SİBER GÜVENLİK POLİTİKALARININ

KARŞILAŞTIRMALI BİR ANALİZİ:

TÜRKİYE VE İNGİLTERE ÖRNEĞİ

Gül Nazik ÜNVER

LIVRE DE LYON
2023

Sosyal Bilimler

SİBER GÜVENLİK POLİTİKALARININ

KARŞILAŞTIRMALI BİR ANALİZİ: TÜRKİYE VE İNGİLTERE ÖRNEĞİ

Gül Nazik ÜNVER

LIVRE DE LYON

Lyon 2023

SİBER GÜVENLİK POLİTİKALARININ

KARŞILAŞTIRMALI BİR ANALİZİ: TÜRKİYE VE İNGİLTERE ÖRNEĞİ

Gül Nazik ÜNVER

LIVRE DE LYON

Lyon 2023

Siber Güvenlik Politikalarının Karşılaştırmalı Bir Analizi: Türkiye Ve İngiltere Örneği

Author • Dr. Gül Nazik ÜNVER • Orcid: 0009-0005-5003-1555
Cover Design • Motion Graphics
Book Layout • Motion Graphics
First Published • July 2023, Lyon

ISBN: 978-2-38236-562-5

Publisher • Livre de Lyon
Address • 37 rue marietton, 69009, Lyon France
website • http://www.livredelyon.com
e-mail • livredelyon@gmail.com

ÖNSÖZ

Siber güvenlik uluslararası ilişkilerde çok önemli bir rol oynamakta ve hükümet politikalarında önemli bir unsur olmaya devam etmektedir. Siber güvenlik ve hükümet politikaları arasındaki ilişki, küresel düzeyde siber tehdit ve saldırılardaki artışla bağlantılı olabilmektedir. Siber saldırıların tüm ağlar ve sistemler üzerindeki geniş etkisi nedeniyle, hükümetler bu sorunla mücadele etmek zorundadır. Siber güvenlik, her hükümetin temel politikasında dikkate alması gereken uluslararası bir kavramdır. Siber güvenlik, siber alanda ortaya çıkan sorunları saptama, saldırgandan bir adım önde düşünme ve toplumları siber suçlardan korumaya yönelik etik bir istekle ilgilidir. Bu kitap Türk ve İngiliz hükümetlerinin siber güvenliğe öncelik vermeleri ve bu alanda kendilerini ne ölçüde geliştirmesi gerektiğini anlatmaktadır. Bu kitap esasen, Türk ve İngiliz hükümetlerinin iyi yapılandırılmış siber güvenlik politikaları geliştirmeleri ve uyulması gereken rehber niteliğindeki belgeleri dikkate almaları gerektiğini iddia etmektedir.

Selçuk Üniversitesi Uluslararası İlişkiler Bölümü'nde yürüttüğüm doktora tezinden ortaya çıkan bu kitap, siber güvenlik politikalarını iki farklı ülkeyi baz alarak karşılaştırmalı analizlerini içermektedir. Kitapta, bilgi ve katkılarıyla doktora tezimi tamamlamamı sağlayan değerli tez danışmanım Prof. Dr. Şaban Halis ÇALIŞ'a ve zamanını harcayıp çalışmama yön veren Doç. Dr. Fazlı DOĞAN'a, tez izleme kurul toplantılarında sabır ve anlayışla sunumumu dinleyip, bu çalışma ile ilgili yorumlarını ekleyen Doç. Dr. Rukiye SAYGILI'ya, bu kitabın konu başlığını belirlememde bana cesaret veren değerli Prof. Dr. Nezir AKYEŞİLMEN'e, çalışmamın her anında sorularıma cevap verip, çalışmamın özellikle son safhalarında cesaretlendirici bir ses olan abim Dr. Öğr. Üyesi Muharrem ÜNVER'e teşekkürlerimi sunuyorum. Ayrıca farklı üniversitelerde ve farklı alanlarda olmamıza rağmen birlikte başladığımız doktora sürecinde her zaman birbirimizi destekleyip, birbirimizi motive ettiğimiz ve yeni Dr. Öğr. Üyesi olan canım arkadaşım Fatmanur DEMİRBAŞ'a, her türlü desteği veren ve hayatım boyunca yanımda olan değerli aileme çok minnettarım.

Bu kitabın siber güvenlik, siber güvenlik politikaları, teknoloji çalışmaları ve uluslararası ilişkiler üzerine bundan sonra yapılacak çalışmalarda yararlı bir rehber olmasını ümit ederim.

Gül Nazik ÜNVER
gulunver@outlook.com

ÖZET

Bu çalışmada, siber güvenlik politikaları, Türkiye ve İngiltere örnekleri özelinde karşılaştırmalı olarak ele alınmaktadır. Devletlerin, siber güvenlik politikalarının gelişiminde kendilerine has tarihsel ve özgün koşulları bulunmaktadır. Bununla beraber bu gelişim sürecinde yapısal benzerliklerin de göz ardı edilemeyeceği açıktır. Türkiye ve İngiltere'de siber güvenlik politikalarının gelişiminde de benzerliklerin ve farklılıkların varlığı kaçınılmazdır. Bu çalışmada, ilk olarak, değişik kalkınma düzeylerine sahip devletlerden örnekler vererek, siber güvenlik politikalarının beş boyutta (1. politika ve strateji, 2. kültür ve toplum, 3. eğitim, öğretim ve beceriler, 4. yasal ve düzenleyici çerçeveler, 5. standartlar, organizasyonlar ve teknolojiler) karşılaştırmalı olarak analiz etmenin mümkün olduğunu ve siber politikaların uluslararası düzeyde bir etkileşim içinde olduğunu iddia etmektedir. Bu çalışmada, ikinci olarak, Türkiye ve İngiltere'nin siber alanda artan tehditlere nasıl yanıt verdikleri, karşı stratejilere nasıl yaklaştıkları ve ulusal siber güvenlik politikalarını nasıl tasarladıkları da gösterilmektedir. Bu kapsamda da üçüncü olarak, bu iki ülkenin çeşitli siber güvenlik endeksleri dâhilinde karşılaştırılmasıyla (Küresel Siber Güvenlik Endeksi-GCI), siber alanda ülkeler için en iyi siber politikaların nasıl olabileceği tartışılmakta ve son olarak da bu konuda bundan sonra yapılacak araştırmalara yol gösterici önerilerde bulunulmaktadır.

Anahtar Kelimeler: Siber Alan, Siber Güvenlik, Siber Güvenlik Politikaları, Siber Güvenlik Endeksleri.

ABSTRACT

In this study, cyber security policies are discussed comparatively with the examples of Turkey and England. States have their own historical and unique conditions in the development of their cyber security policies. However, it is clear that structural similarities cannot be ignored in this development process. It is inevitable that there are similarities and differences in the development of cyber security policies in Turkey and England. In this study, firstly, by giving examples from states with different levels of development, cyber security policies are examined in five dimensions (1. policy and strategy, 2. culture and society, 3. education, training and skills, 4. legal and regulatory frameworks, 5. standards, organizations and technologies) and that cyber policies interact at the international level. Secondly, this study shows how Turkey and the UK respond to increasing threats in cyberspace, how they approach counter-strategies and how they design national cyber security policies. In this context, thirdly, by comparing these two countries within various cyber security indices (Global Cyber Security Index-GCI), it is discussed how the best cyber policies can be for countries in the cyber field, and finally, guiding suggestions are made for future research on this subject.

Keywords: Cyber Space, Cyber Security, Cyber Security Policies, Cyber Security Indices.

KISALTMALAR LİSTESİ

AB	**:** Avrupa Birliği
ABD	**:** Amerika Birleşik Devletleri
ARPA	**:** İleri Araştırma Projeleri Ajansı
ARPANET	**:** Gelişmiş Araştırma Projeleri Ajansı Ağı
AU	**:** Afrika Birliği
BDDK	**:** Bankacılık Düzenleme ve Denetleme Kurumu
BDT	**:** Bağımsız Devletler Topluluğu
BGYS	**:** Bilgi Güvenliği Yönetim Sistemi
BİLGEM	**:** Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BİT	**:** Bilgi ve İletişim Teknolojisi
BM	**:** Birleşmiş Milletler
BSI	**:** Federal Bilgi Güvenliği Ofisi
BT	**:** Bilgi Teknolojileri
BTK	**:** Bilgi Teknolojileri ve İletişim Kurumu
CAE	**:** Çin Mühendislik Akademisi
CAS	**:** Çin Bilim Akademisi
CERN/CERT	**:** Bilgisayar Acil Müdahale Ekipleri
CERT-UK	**:** İngiltere Bilgisayar Acil Müdahale Ekipleri
CIP (FOCP)	**:** Kritik Altyapı Koruması
CIRT	**:** Bilgisayar Olay Müdahale Ekipleri
CiSP	**:** Siber Güvenlik Bilgi Paylaşım Ortaklığı
CMA	**:** Bilgisayarın Kötüye Kullanımı Yasası
CMM	**:** Siber Güvenlik Kapasite Olgunluk Modeli
CMX-2017	**:** Crisis Management Exercise 2017
CNI	**:** Kritik Ulusal Altyapı
COBIT	**:** Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri
COMESA	**:** Doğu ve Güney Afrika Ortak Pazarı
CPNI	**:** Ulusal Altyapının Korunması Merkezi
CPS	**:** Kraliyet Savcılık Servisi

CSIRT : Bilgisayar Güvenliği Olay Müdahale Ekibi
CSOC : Siber Güvenlik Operasyon Merkezi
DCMS : Dijital, Kültür, Medya ve Spor Dairesi
DCSS : Savunma Siber Koruma Ortaklığı
(C)DDO : (Cumhurbaşkanlığı) Dijital Dönüşüm Ofisi
DDoS : Dağıtılmış Hizmet Reddi Saldırıları
DNS : Alan Adı Sistemi (Domain Name System)
ECOWAS : Batı Afrika Ülkeleri Ekonomik Topluluğu
ENISA : Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı
GCHQ : Devlet İletişim Merkezi
GCI : Küresel Siber Güvenlik Endeksi
GII : Küresel İnovasyon Endeksi
GSCC : Küresel Siber Güvenlik Kapasite Merkezi
http : Hiper Metni Aktarım Protokolü
ICO : Bilgi Komisyonerliği Ofisi
ICS : Ulusal Bilgi Güvenliği ve Kriptoloji Konferansı
ICT : Bilgi ve İletişim Teknolojileri
IDF : İsrail Savunma Kuvvetleri
IoT : Nesnelerin interneti
INCP : İsrail Ulusal Siber Bürosu
INSEAD : Institut Européen D'administration des Affaires veya Avrupa İşletme Enstitüsü Cornell Üniversitesi
IP : İnternet Protokolü
ISO/IEC : Uluslararası Standardizasyon Örgütü
ISPA : Birleşik Krallık İnternet Servis Sağlayıcıları Derneği
ISS : İnternet Servis Sağlayıcısı
ITU : Uluslararası Telekomünikasyon Birliği
KVKK : Kişisel Verileri Koruma Kanunu
MIIT : Sanayi ve Bilgi Teknolojileri Bakanlığı
NATO : Kuzey Atlantik Antlaşması Örgütü
NCS/NSS : Ulusal Siber Güvenlik Stratejisi
NCSA : Ulusal Siber Güvenlik Otoritesi

NCSC : Ulusal Siber Güvenlik Merkezi
NCSPs : Ulusal Siber Güvenlik Politikaları
NNISCSG : Ulusal Ağ ve Bilgi Güvenliği Koordinasyonu Küçük Grubu
NIS : Ağ ve Bilgi Sistemleri için Yüksek Düzeyde Ortak Güvenlik Önlemleri
NSA : Ulusal Güvenlik Ajansı
NSF : Ulusal Bilim Kurulu
OCSIA : Siber Güvenlik ve Bilgi Güvencesi Ofisi
PCIDSS : Ödeme Kartı Sektörü Veri Güvenliği Standardı
PLA : Çin Halk Kurtuluş Ordusu
RIPA : Soruşturma Yetkileri Yönetmeliği
SCADA : Merkezi Denetim ve Veri Toplama Sistemi
SCITO : Devlet Konseyi Bilgilendirme Ofisi
SGE : Siber Güvenlik Enstitüsü
SIC : Güvenli İnternet Merkezi
SILG : Devlet Bilgilendirme Lideri Küçük Grup
SSB : Savunma Sanayi Başkanlığı
STK : Sivil Toplum Kuruluşları
STMAŞ : Savunma Teknolojileri Mühendislik ve Ticaret Anonim Şirketi
TASE : Tel Aviv Menkul Kıymetler Borsası
TCP : İletim Kontrol Protokolü
TR : Türkiye
TR-CERT : Türkiye Ulusal Bilgisayar Acil Müdahale Ekipleri
TR-BOME : Türkiye Bilgisayar Olayları Müdahale Ekibi Koordinasyon Merkezi
TSK : Türk Silahlı Kuvvetleri
TÜBİTAK-UEKAE : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu-Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
UCLA : Kaliforniya Üniversitesi
UK : Birleşik Krallık

UNIDIR : Birleşmiş Milletler Silahsızlanma Araştırmaları Enstitüsü

URL : Uniform Resource Locator (Tekdüzen Kaynak Konum Belirleyici- Bağlantı Belgeleri)

USOM : Ulusal Siber Güvenlik Müdahale Merkezi

WFS : Dünya Bilim İnsanları Federasyonu

WIPO : Dünya Fikri Mülkiyet Örgütü

www : World Wide Web

TABLO LİSTESİ

ŞEKİL LİSTESİ

GRAFİK LİSTESİ

İÇİNDEKİLER

GİRİŞ

Bu çalışma, stratejik siber güvenlik politikaları uygulayan devletlerin yerel kurumsal yapısındaki farklılıklarına odaklanmaktadır. Bu kapsamda stratejiler belirleyen devletler, siber güvenliği bütüncül bir yaklaşımla ele almaktadır. Buna göre siber güvenliğin ekonomik, sosyal, yasal, politik, eğitim, stratejik, organizasyonel tüm yönlerini değerlendirmektedir. Bu bağlamda İngiltere gibi gelişmiş ve Türkiye gibi gelişmekte olan devletlerin siber alanda[1] kültürel farklılıklarının önemli rolü olduğu bu çalışmada görülmektedir. Buna rağmen, İngiltere ve Türkiye'de uygulanan siber güvenlik politikaları daha esnek bir yaklaşımı benimsemektedir. Bunu özellikle her iki ülkenin siber güvenlik politikalarında ekonomik ve kişisel (bireysel) boyutlarını önemsediği bu araştırma sonucunda görülmüştür. Küresel Siber Güvenlik Endeksi'ne göre, Avrupa'da siber güvenlik etkilerinin ölçüm verilerine dayalı olarak İngiltere listede 1. Sırada yer alırken, Türkiye 11. Sırada yer almıştır.[2] İngiltere'nin stratejileri uygulama açısından Türkiye'den daha iyi olduğu görülmektedir. İngiltere siber güvenlik politikalarını koordine etme ve uygulama konusunda Türkiye'den daha aktiftir. Türkiye siber olayların teknik ve organizasyonel yapıya vereceği zararın önlenmesine odaklanmaktadır. İngiltere ise siber olayların ulusal kritik bilgi altyapılarına ve kilit ağ kaynaklarına yönelik saldırıları önlemek üzere siber alana odaklanmaktadır. Siber güvenlik perspektifinden bakıldığında, Türkiye'nin önceliği kamu ve devletin güvenliği iken, İngiltere'nin önceliği bireyin güvenliği ve insan hakları olmaktadır. Siber güvenlikte Türkiye, kamu kurumlarını teşvik etmekte ve standartlarının artırılmasının farkındalığı üzerine çalışmaktadır.

Bu çalışma da karma yöntem araştırmaları[3] kullanılarak siber güvenlik politikalarının karşılaştırılması, bir politika alanı olarak anlaşılması gerektiğini savunmaktadır. Çalışmada ana iddia ve yardımcı iddiaları sentezlemek

[1] 1982 yılında bilimkurgu yazarı William Gibson tarafından "Neuromancer" adlı bir çizgi romanda ilk kez kullanılan "cyberspace", orijinal anlamını tam karşılamasa da yaygın olarak Türkçe çalışmalarda siber uzay, siber ortam ya da siber alan olarak geçmiştir. Bu çalışmada "cyberspace" kavramı, "siber alan" olarak kullanılmıştır. Detaylı bilgi için bkz. S.W Singer ve Allan Friedman (2013). *Cybersecurity ve Cyberwar: What Everyone Needs to Know,* England: Oxford University, s. 17.

[2] Tablo 6: 2018 Küresel Siber Güvenlik Endeksi'nde Bölgesel ve Küresel Sıralama.

[3] Bu çalışma karma yöntem araştırması olarak çalışmanın nitel ve nicel yaklaşım veya yöntemleri kullanarak nitel yorumlama yapıldığı, nicel veri toplandığı ve çıkarımlarda bulunulduğu bir çalışmadır.

için sayısal verilerden, literatür taramasından ve birincil kaynaklardan faydalanılmıştır. Teorik ve pratikte iki önemli devletin strateji ve politika belgelerinin karşılaştırılmıştır. Bu ülkeler ile ilgili siber güvenlik politika belgeleri araştırılmıştır. Bunun sonucunda, bibliyografik verilerin, devletlerin siber güvenlikte hangi farklı işlevleri ve sosyal meseleleri yerine getirmesinin beklendiği ele alınmıştır.

Bu çalışma kavramsallaştırılan, değişken bir yapıda ve kesişen bir politika alanı olarak siber güvenlik anlayışını Türkiye ve İngiltere arasında karşılaştırmalı olarak incelemektedir. Buna ek olarak bu iki ülkenin siber güvenlik ilişkilerindeki paylaşımlar, küresel siber güvenlik alanının önemli bir yönünü de göstermektedir. Bu alandaki araştırmacıların bu iki ülkeyi göz önünde bulundurarak, devletlerin siber güvenlik alanında iç ve dış yapıda farklı rollerinin daha kapsamlı bir şekilde anlaşılmasına olanak sağlayan araştırma soruları sorulması ve cevaplanması beklenmektedir.

Bu çalışmanın temel araştırma soruları şu şekildedir:

Siber güvenliğin uluslararası alanda kabul edilebilir bir tanımı var mıdır?;

Siber güvenlik politikaları nelerdir?;

Siber güvenlik politikalarında "devletlerin" rolleri nelerdir?;

Mevcut literatür, devletin rolü güvenlik bağlamında nasıl kuramsallaştırmaktadır? Siber güvenlik, politika tartışmalarında ve siyasi uygulamada mevcut ve gelecekteki kavramsallaştırılması için nasıl anlaşılmalıdır?;

Ulusal güvenlik (hem aktif hem de pasif) olarak siber güvenliğin oluşturulmasında devlet nasıl bir rol oynamaktadır?;

Siber güvenlikle ilgilenen ne tür kurumlar vardır?; Görevleri nelerdir?; Nasıl çalışırlar?;

Siber güvenliğin günümüzdeki özel görünümünün toplumsal güvenlik üzerinde nasıl bir etkisi vardır?;

*Siber güvenlik politikalarının çeşitliliği göz önüne alındığında, karmaşık sorunun hangi yönleri için farklı aktörlerin rolleri ve sorumlulukları vardır? ve farklı aktörler arasındaki hangi çekişmeler siber güvenlik politikası alanını yapıland*ırmaktadır?*;*

Toplum için tehdit oluşturan risk kümelenmelerini ve bulaşma etkilerini önlemek için yasal ve düzenleyici çerçeve kapsamında devlet nereye müdahale etmelidir?

Bu çalışma kural koyucu ve uygulayıcı "devletler" üzerinden siber güvenlik politikalarının karşılaştırmalı olarak incelenmesine dayalıdır.

Bu çalışma beş ana bölümden oluşmaktadır*:*

Birinci Bölüm**'de**; güvenlik politikalarına ilişkin literatürün yanı sıra mevcut siber güvenlik tanımlarına odaklanılmıştır. Uluslararası İlişkiler ve Siyaset Bilimindeki siber güvenlik sorunları, aynı zamanda uluslararası güvenlik sorununun da bir parçasıdır. Buna göre özellikle Siber Güvenlik alt bilim dalına yoğunlaşıldığında, uluslararası güvenlik sorununun çözümüne de diğer bileşenleri ile birlikte katkı sunacağı bilinmektedir. Ulusal siber güvenlik stratejilerinin, siber güvenliğin farklı politika alanlarında çok sayıda konuya değindiği belirtilmektedir.

Birinci ana başlık "güvenlik"tir. Güvenlik fikrinin altında yatan temel varsayımlar üzerinde durularak, tartışma ve analiz yapılmıştır; "*genel kabul görmüş bir güvenlik tanımı var mı?, neyin veya kimin güvenliği?, ne için güvenlik?, ne anlamda güvenlik? ve nasıl güvenlik?*" vb. gibi… Burada güvenliğin, insan yaşamının temel bir değeri olduğu düşüncesinden hareket edilmektedir. Esasen, "*uluslararası ilişkilerde güvenlik paradigmaları nelerdir?*" sorusundan yola çıkılmaktadır. Burada konunun üç alt başlıkta incelenmesi uygun görülmüştür: Ulusal Güvenlik, uluslararası güvenlik ve insan güvenliği.

Birinci alt başlık olan ulusal güvenlik, güvenliği devlet açısından incelemektedir. Bu alt başlıkta da belirtildiği üzere; devlet, temelde bir güvenlik düzenlemesine dayalıdır ve yirmi birinci yüzyılda da öyle kalmalıdır. İyi yönetilen bir ulus devlet, kapsamlı bir güvenlik örgütüdür. İşte bu nedenle ulus devlet, en nihayetinde klanların, kabile topluluklarının, özgür şehirlerin, orta çağ loncalarının, dukalıkların, hanedan devletlerinin ve hatta imparatorlukların yerini alarak modern politik örgütlenmenin temel biçimi haline gelmiştir. Dolayısıyla, "ulusal güvenlik" terimi, ulus devletin ayrı ve egemen bir topluluk olarak hayatta kalmasını ve böylelikle vatandaşlarının güvenliğini ve refahını güvence altına aldığı tüm devlet politikalarına atıfta bulunmaktadır. Ulus devlet ile yurttaşları arasındaki karşılıklı güvenlik yükümlülüğü, ulus devletin halkın koruyucusu olma iddiasının dayandığı normatif temeldir. Ulusal güvenlik paradigmasının geçerli olması için, devletin zorlayıcı gücü son çare olarak ve mümkün olduğunca nadiren kullanılmalıdır. Ancak bu her zaman böyle değildir. Liberal demokrasilerde bile, Barry Buzan'ın "savunma ikilemi" olarak adlandırdığı şey, nükleer caydırıcılık ve terörle mücadele önlemlerinin yaşanan örnekleri netleştirdiği ortaya çıkmaktadır. Totaliter ve zayıf, başarısız veya yarı devletlerin deneyimi, ulusal güvenlik paradigmasının sınırlarını göstermek için de incelenmektedir.

İkinci alt başlık uluslararası güvenliktir. Bu bölüm temelde, güvenliği uluslararası toplum açısından incelemektedir. Dolayısıyla uluslararası toplumun

tarihi, düzensizlik sorunu ve bununla birlikte ortaya çıkan güvensizlik ile devam eden bir mücadele olarak sunulmaktadır. Uluslararası güvenliğin sağlanmasındaki birincil sorumluluk, büyük güçler olarak adlandırılan devletlere aittir. Rolleri güç dengesi ve büyük güçlerin birliği açısından değerlendirilmektedir. Bu durumun aksine büyük bir gücün uluslararası bir zorba veya illegal olarak hareket etmeye başladığı durumlarda, uluslararası güvenlik riske girmekte ve felaketle sonuçlanan savaş potansiyeli artmaktadır. Bu ikilemler, askeri müdahale ve nükleer silahların yayılmasının önlenmesi bağlamında uluslararası güvenlik paradigmasının temel sınırlamaları olarak sorgulanmaktadır.

Üçüncü alt başlık insan güvenliğidir. Bu bölüm temelde güvenliği bireyin bakış açısından incelemektedir. Uluslararası sınırları aşan küresel insan topluluğu düşüncesi, uluslararası ilişkiler için önemli bir yapı oluşturmaktadır. Bu yapı, bu çalışmada siber güvenlik bakış açısı ile incelenmiştir. Son olarak, uluslararası ilişkilerin şimdiye kadar, iyi ya da kötü, devlet egemenliği ve çoğul değerler temelinde örgütlenmiş halde kalmasının doğrudan bir sonucu olan insan güvenliği paradigmasının da beklenen sınırları incelenmektedir. Bu noktaya kadar incelenen üç ana güvenlik paradigmasının her biri (ulusal güvenlik, uluslararası güvenlik ve insan güvenliği) farklı güvenlik hedeflerine öncelik vermektedir. Bunu şu sorularla ele almaktadır: "*Devletin ulusal güvenliği önce gelmeli mi?, Devletlerin toplumları içinde genel bir barış ve istikrar koşulunun, üyelerinden birinin ulusal güvenliğinin ihlal edilmesini makul bir şekilde gerektirebileceği durumlar var mı? Ya devlet sistemi içinde genel bir barış ve istikrar durumuna ve ulusal güvenliğe bakılmaksızın, ciddi türden bir insan ıstırabı devam ederse?, Bu tür durumlarda, insan güvenliği bu diğer hususlara üstün gelmeli mi?*" Bu bölümde, insan güvenliğinin çelişkileri ve tutarlılıkları, örnekler üzerinden değerlendirilmektedir.

İkinci ana başlık "siber güvenlik"tir. Bu başlık kavramsal çerçeve ışığında siber güvenliğin tanımı ve geçmişini incelemekte ve bunlar paradigmalar arası tartışmalarda karşılaşılacak temel sorular üzerinden şu şekilde sıralanmaktadır: "*Siber güvenlik kime/neye göre olmalıdır? Güvenli bir siber alan oluşturabilmek için üzerinde durulan amaçlar nelerdir? Siber güvenlik nasıl sağlanmalıdır? Siber kavramı nasıl ortaya çıkmıştır? Siber alan hangi olayda önem kazanmıştır? Siber alanın bir sınırı var mıdır? Ve ortak bir siber güvenlik tanımı yapılabilir mi?*". Bu sorular gibi pek çok soruya yanıtlar verilmeye çalışılmıştır. Yukarıdaki sorulardan yola çıkılarak yapılan araştırmalar, ikinci ana başlığın temel çıkış noktasına olanak sağlamıştır. Ayrıca uluslararası ilişkilerde güvenlik, siber

güvenlik ve temel varsayımlar, siber güvenlikte internet sisteminin işleyişi alt başlıkları ile birinci bölümün teorik çerçevesi oluşmuştur.

İkinci Bölüm'de; Birleşmiş Milletler (BM) kuruluşu olan Uluslararası Telekomünikasyoun Birliği (ITU) endeksleri bu bölümde devletlerin siber güvenlik yaklaşımları açısından bazı örneklerle beraber incelenmiştir. ITU'nin Küresel Siber Güvenlik Gündemi'ne dayanan Küresel Siber Güvenlik Endeksi (GCI), devletlerin siber güvenlik taahhüt düzeyine beş boyutta bakmaktadır: 1. politika ve strateji, 2. kültür ve toplum, 3. eğitim, öğretim ve beceriler, 4. yasal ve düzenleyici çerçeveler, 5. standartlar, organizasyonlar ve teknolojiler. Siber güvenliğin öneminin artması, siber güvenlik stratejilerinin derinden incelenmesi ihtiyacını doğurmuştur. Literatür araştırmasına ve halka açık siber güvenlik stratejilerinin analizine dayanarak, ülkeler siber güvenlik alanı için öngörü metodolojileri uygulamaktadır.

İkinci Bölüm'de birinci ana başlık "siber güvenliğin tarihsel gelişimi"dir. Siber alanda "devletler çıkarlarını anlamak ve tanımlamak için mücadele eder"[4]. Tarihsel olarak bu temel görevi, politika yapıcılar siyasi çıkarımlarla birlikte engelleyebilmekte veya çözüm üretebilmektedirler. Politika yapıcılar için güvenlik sorunları analizinin yanlış şekilde uygulanması feci sonuçlar doğurabilmektedir. ABD liderlerinin 1950'lerdeki Kore Savaşı'ndaki politikaları bunun çarpıcı bir örneğidir. Vietnam Savaşı'nda ise ABD stratejisini yanıltıcı veriler ışığında şekillendirmiş ve bölge insanının acı çekmesine sebep olmuştur. Bilim insanları ve politikacıların farklı yaklaşımları, bazen ciddi ve olumsuz politika sonuçları doğurmaktadır. Bu da ulusal ve uluslararası güvenlik sorunlarını algılama biçimini farklı açılardan incelemeyi gerektirmektedir. Bu nedenle siber güvenlik politika oluşturma sürecinde, uygulamaya yönelik potansiyel sonuçlarını değerlendirmek hayati önem taşımaktadır. Örneğin, Soğuk Savaş stratejik kavramlarının siber güvenlik analizine uygulanması, potansiyel olarak ciddi sorunların olduğu gerçeğini göstermektedir. Çalışma siber güvenliği tarihsel anlamda, devletlerin çıkarları ve ilişkileri üzerinde önemli bir etkiye sahip, büyük ölçüde devlet eyleminin sorunlarını ve uyguladıkları politikaları incelemektedir.

İkinci ana başlık "siber güvenlik politikaları" siber alanın devam eden coğrafi genişlemesini ele almakta olup, gelişen teknolojilerle beraber altyapı ve hizmetlerin birbirine bağlılığını nasıl artıracağını öngörmüştür. Siber alanın

[4] Joseph S. Nye, Jr (2014). "The Regime Complex for Managing Global Cyber Activities", London: Global Commission on Internet Governance *(CIGI) and Chatham House*, No 1, s. 12.

bütünleşik sosyo-teknik sistemlerle bağlantılı bir şekilde hem ulusal hem de uluslararası düzeyde daha fazla politik alana yayılacağını vurgulamaktadır. Bu ana başlık, devlet ve devlet dışı unsurlar arasında daha detaylı kavramsal anlayışlar getirerek siber tehdit engellerini aşmaktadır. Birçok hükümet kendi siber güvenlik stratejilerini oluşturmuştur. Düzenleyici yasal çerçeveye odaklanmakta olan Avrupa Birliği (AB), siber güvenlikle ilgili uluslararası iş birliği ve uygulamalar için bir plan kapsamında Avrupa Konseyi Siber Suç Sözleşmesi'ni (Budapeşte Sözleşmesi) teşvik etmektedir. Öte yandan Anglosfer[5], ulusal siber güvenliğin korunması için özel sektör liderliğine, eğitimli bir işgücüne, sosyal yardıma ve diplomasiye vurgu yapmaktadır. Buna, siber güvenlik mevzuatında bilgi özgürlüğünün altını çizen ve özel sektörün rolünü vurgulayan Amerika Birleşik Devletleri'de (ABD) dâhildir. Devlet bilgilerinin hassasiyeti nedeniyle siber güvenlik hayati öneme sahiptir ve bilgi edinme özgürlüğünden daha öncelikli olmaktadır. Buna yönelik Baltık Devletleri, ulusal siber güvenlik stratejilerinin geliştirilmesinde Kuzey Atlantik Antlaşması Örgütü (NATO) ile sıkı bir iş birliği içerisindedir. 2007 yılında Estonya'da meydana gelen ilk devlet düzeyinde Siber Savaş'tan bu yana, Rusya- Gürcistan (Güney Osetya anlaşmazlığı), Kuzey Kore-ABD, Çin- Hindistan, İran'ın nükleer tesislerine yönelik Stuxnet saldırısı gibi ülkelerde bir takım siber savaş olayları yaşanmıştır. Daha gelişmiş olarak Duqu solucanı, Flame virüsü ve Orta Doğu hükümet sistemlerini hedef alan ve 30.000 Saudi Aramco iş istasyonuna zarar veren Shamoon virüsü gibi bir dizi siber saldırı olayları yer almıştır. Bu saldırılar, siber savaşın zamanla şiddetini artıracağını kanıtlamakta ve yirmi birinci yüzyılda siber alanın güvenliğini sağlamanın ve ülkelerin siber güvenlik politikalarını geliştirmesinin kritik önemini ortaya koymaktadır. Nitekim Birleşik Krallık Kabine Ofisi tarafından Haziran 2009'da hazırlanan "Birleşik Krallık'ın Siber Güvenlik Stratejisi" raporu, siber alanın önemine işaret etmiştir. Her yeni gün, siber güvenliğin önemi artmaktadır. Bazı ülkelerin kamuoyunda güvenlik bilincini artırmak amacıyla savunma ve taarruz yeteneğine sahip siber birimler kurması, eğitim ve tatbikat faaliyetleri gerçekleştirmesi, sempozyumlar, çalıştaylar gerçekleştirmesi ve bu konuda farkındalık bilincinin artması için faaliyetler yapılması gibi birtakım haberler beraberinde gelmektedir.

Siber stratejilerin etkinliğini değerlendirmek için yaygın olarak benimsenen metodolojilerin olmaması, bu yeni siber güvenlik politikası oluşturma döneminin hala ilk günlerinde olduğunu göstermektedir. Siber

[5] İngilizcenin ana dil olduğu, ortak kültürel tarihi bağları paylaşan ülkeler grubudur. Özellikle bu grubun içinde bulunan ülkeler Birleşik Krallık, Amerika Birleşik Devletleri, Kanada, Avustralya ve Yeni Zelanda'dır.

güvenlik stratejisi hazırlayacak veya güncelleyecek ülkelerin bütüncül bir bakış açısına sahip olmaları, önceliklerini belirlemeleri ve siber güvenliğin ulusal öncelikleriyle uyumlu yönlerine daha fazla odaklanmaları çalışmada tavsiye edilmektedir. Bir diğer önemli nokta siber alandaki tehdit ve risklerin yanında fırsatların da dikkate alınması gerçeğidir. Küresel olarak kabul edilen başlıca siber güvenlik stratejileri, özellikle siber güvenliğin çift katlı ikili zincir yapısını (saldırgan siber güvenlik strateji planları ve savunma amaçlı siber güvenlik strateji planları) kabul eden İngiltere, ABD gibi ülkelerden gelmektedir.[6] Politikanın uygulanması, vatandaşlar arasında siber güvenlik bilinci ve siber güvenlik politikalarının güncellenmesi, ulaşılması gereken zorluklar olarak karşımıza çıkmaktadır. Ulusal Siber Güvenlik Politikaları, toplumda siber güvenlik kültürü oluşturulması ve geliştirilmesi gereksinimini anlaşılır hale getirecektir. Devletler-toplumlar ve bireyler güvenliği bir kez alışkanlık haline getirdiğinde, her ülke siber güvenlik konusunda destek olacak ve gelişimine katkı sağlayacaktır.

Üçüncü ana başlık "siber güvenlik politikası hedeflerinin belirlenme süreci ve hükümetlerin aldığı önlemler"dir. 2003 yılında ABD, siber güvenlik politikasının önemini anlayan ve dünyada siber güvenlik politikasına sahip ilk ülke olmuştur. Son on yılda, ulusal siber güvenlik stratejisi belgesini yayınlayan 35 ülke daha eklenmiştir.[7] Siber alanda iletişim, ülkeleri çeşitli zorluklara maruz bırakmaktadır. Bir siber tehdit karşısında hedef ülkenin uygulayabileceği üç temel strateji vardır: Caydırma, Silahsızlanma ve Savunma. Libicki (2009) çalışmasında, silahsızlanma ve caydırıcılık yerine en iyi stratejinin iyi bir savunma olduğu sonucuna varmıştır. İyi bir savunma elde etmek için, bir ulusun stratejik hedefleri ve bunlara ulaşmak için alınacak önlemleri içeren ulusal strateji belgesi geliştirmesi zorunlu olmaktadır. Gelecekteki tüm askeri ve siyasi anlaşmazlıkların bir siber güvenlik boyutu olacaktır. Bu nedenle siber güvenlik stratejisi olmayan, merkezi savunma ve müdahale kabiliyeti olmayan ülkeler zayıf kalacaktır.[8] Bu, devletler tarafından etkili siber güvenlik politikaları hazırlanarak ve uygulanarak çözülebilmektedir. Ulusal siber güvenlik stratejilerinin çeşitli yönleri vardır. Luiijif ve Healey'e (2012) göre, ulusal siber güvenliğin beş görevi vardır: 1) Askeri siber operasyonlar, 2) Siber

[6] Myriam Dunn Cavelty (2005). "The Socio-political Dimensions of Critical Information Infrastructure Protection (CIIP)", *International Journal of Critical Infrastructures,* Sayı 1 (2/3), ss. 258-268.
[7] Global Cybersecurity Index 2018, *ITU,* s. 6-7.
[8] Martin C. Libicki (2009). *Cyberdeterrence and Cyberwar*, US: RVE, s. 59-62.

suçla mücadele, 3) İstihbarat/Karşı istihbarat, 4) Siber güvenlik kriz yönetimi ve kritik altyapı koruması ve 5) İnternet yönetişim ve siber diplomasi olmaktadır.[9]

Dünyada bazı ülkelerin yapmış olduğu Ulusal Siber Güvenlik Strateji Belgeleri'ne bakacak olursak; ABD Ulusal Siber Strateji Belgesi (Siber Alanın Güvenliğine Yönelik Ulusal Strateji) Şubat 2003'te yayınlanmıştır. Ülke genelinde binlerce kişi ile birçok kamu ve özel kuruluş tarafından geliştirilen belge, siber alanın güvenliğinin ancak tüm Amerikan halkının ve özellikle özel sektörün katkısı ile kamu ve özel sektör iş birliği ile mümkün olabileceğini belirtmiştir. Belge, siber güvenliğin sağlanması konusundaki ana sorumluluğu ABD İç Güvenlik Bakanlığı'na vermiş ve üç stratejik hedefi içeren strateji belgesinin, ABD anavatanının korunması için hazırlanan Ulusal Strateji'nin tamamlayıcısı olduğunu vurgulamıştır. [10] Almanya'nın siber güvenlik stratejisi belgesi, kritik bilgi altyapısı koruması ve ulusal kamu sistemleri güvenliğine vurgu yaparak bir Ulusal Siber Güvenlik Konseyi ve Ulusal Siber Müdahale Merkezi kurma gerekliliği üzerinde durmuştur.[11] Fransız siber güvenlik strateji belgesi, siber savunmanın süper gücü olmak, ulusal bağımsızlığa ilişkin bilgileri korumak, ulusal kritik altyapıyı korumak ve siber alanda siber güvenliği sağlamak için stratejik hedefleri ele almıştır.[12] 2009 yılında yayınlanan Avustralya siber güvenlik stratejisi belgesi, tehdit farkındalığı ve müdahalesi, kültürel değişim ve ulusal güvenliğe tehdit oluşturabilecek tüm elektronik sistemlerin esnekliğini ele almıştır.[13] Hollanda'nın siber güvenlik strateji belgesi, kamu-özel ortaklığına, uluslararası işbirliğine önem vermiştir.[14] Genel olarak diğer ülkelerin resmi raporları ve yayınları da incelendiğinde, güvenlik perspektifi kavramları benzerdir. Toplumlar, kuruluşlar, kurumlar, gelişmeler, eylem türleri ve önlemler ile geleceğe yönelik plan ve stratejileri dikkate almaktadır. İletişim ağları, geçmişten bugüne insan toplumunun merkezinde yer almaktadır. Seçkin bir azınlığın deneyimlediği mağara resimleri, sözlü tarihler, yazı, baskı, kütüphaneler ve yaygın okuryazarlık yoluyla gelişen ve süreklilik arz

[9] Ünal Tatar (vd.) (2014). "A Comparative Analysis of the National Cyber Security Strategies of Leading Nations", *9th International Conference on Cyber Warfare and Security* (Ed. Dr. Sam Liles), ss. 211-218.
[10] US White House (February 2003). "The National Strategy to Secure Cyber Space".
[11] Germany (2011). *Cyber Security Strategy for Germany*.
[12] French (2011). *French Network and Information Security Agency (FNISA)*, France's Strategy: Information Systems Defense and Security.
[13] Australia (2020). *Australia's Cyber Security Strategy*.
[14] Netherlands (2011). *The National Cyber Security Strategy (NCSS): Success Through Cooperation*; Gül N. Ünver (2017). "Ulusal Siber Güvenlik Strateji Belgelerinde İnsan Hakları", *Cyberpolitik Journal*, 2 (4), ss. 104-129.

ederek mevcut nesillerin ve dijital bir geleceğin ilk adımlarını göstermektedir. Bu değişim yirmibirinci yüzyılda hızlı bir şekilde ilerlemektedir. Ağların gücü, çok sektörlü uzmanlığa, yeni fikirlerin ve teknolojilerin etkileşimli gelişimine olanak sağladığından, bireyleri ve toplumları beklenmedik ve genellikle benzeri görülmemiş düzeylerde yeniliklere götürmektedir.

Dördüncü ana başlık "küresel salgın ve siber güvenlik ilişkisi"dir. COVID-19 pandemisi, küresel olarak vatandaşların hayatını değiştiren, toplumsal normlar, yaşama ve çalışma şekli açısından "yeni-normal" şeklinde adlandırılan, benzeri görülmemiş olağanüstü bir duruma yol açmıştır. Bir bütün olarak toplum ve iş dünyası üzerindeki olağanüstü etkisinin yanı sıra, pandemi, kurum ve kuruluşları da etkileyen bir dizi görülmemiş siber suçla ilgili olayları da açığa çıkarmıştır. Pandeminin neden olduğu artan endişe de siber suçların gerçekleşmesi olasılığını artırmıştır. Pandemi Nisan 2020'de yayılmaya başladığında, Akamai İnternet trafiğinin yüzde 30 kullanımının arttığını kaydetmiştir.[15] Uzaktan çalışmadan uzaktan eğitime kadar, teknoloji insanları birbirine bağlı tutmada önemli bir rol oynamıştır. Dijital çağın potansiyelini gerçekleştirmesi için güvenilir ve güvenli bir siber alan ülkelerin önceliği olmalıdır. Dünya Sağlık Örgütü tarafından COVID-19'un pandemi ilan edilmesinden ve yeni yönetim sistemlerinin ve aşıların geliştirilmesinden bir yıl sonra, dijital teknolojilere olan bağımlılık hızla artmıştır.

Pandemi sonrasında güvenilir ve güvenli bir siber alan oluşturmaya yardımcı olmak için Küresel Siber Güvenlik Endeksi, pandeminin siber güvenlik çabalarını nasıl etkilediğini, ülkelerin siber güvenlik ve güveni ele almak için nasıl çalıştığını anlamak için önemli bir veri seti sunmaktadır. Örneğin, bazı ülkelerde yasaların onaylanması ve yürürlüğe girmesi, ulusal siber güvenlik stratejilerinin geliştirilmesi veya revize edilmesi, kapasite geliştirme çabalarının sunulması ile ilgili gecikmeler olduğu bildirilmiştir. Ortak anlaşmalar, toplantılar, eğitim vb. artık sadece yüz yüze iletişim ve iş birliği ile yapılmamaktadır. Uzaktan sistemlerle süreçler devam ettirilmektedir. Dünya değişmeye devam ederken, hükümetlerin siber güvenlikle ilgili hangi politika ve uygulamaların mevcut olduğunu değerlendirmeleri önemlidir. Siber güvenlik geliştikçe ve güvenlik politikalarına uyarlandıkça, siber güvenliğin ölçülme şekli de değişmiştir. Siber güvenlik riskine ilişkin artan bir farkındalık vardır.[16] Pandemi, özellikle

[15] Global Cybersecurity Index 2020, *ITU,* s. 1; Martin McKeay (13.04.2020). "The Building Wave of Internet Traffic", [https://www.akamai.com/blog/security/the-building-wave-of-internet-traffic] (er. tar. 12.12.2021).

[16] World Economic Forum, "Global Risk Report 2020- Executive Summary", [http://reports.weforum.org/global-risks-report-2020/executive-summary/] (er. tar. 12.12.2021).

çevrimiçi ortamda güvensizlik yaratmıştır. GCI'da toplanan veriler, yerel bağlamın ve gözlemlerin ileriye dönük bir yol belirlemede kritik olduğu siber güvenlik hakkında daha geniş bir konuşmanın başlangıcını oluşturmaktadır. COVID-19'dan alınan derslerden biri, sağlık veya siber güvenlik gibi toplu eylem sorunlarının disiplinler arası ve bütünsel bir yaklaşımla ele alınması gerektiğidir. Küresel Siber Güvenlik Endeksi'nin tüm temellerini (yasal, teknik, organizasyonel, kapasite geliştirme ve iş birliğine dayalı önlemler) incelemek, insanları gelişmiş iletişim kanalları ile birbirine bağlamayı ve güven inşa etmeyi gerektirmektedir. Ülkeler kendi içinde birlikte çalışmanın ötesinde, gelişmekte olan ve gelişmiş ülkeler gibi siber güvenlik sorunlarını çözme konusunda daha az yetenekli olan az gelişmiş ülkeleri desteklemeleri gerekmektedir. Bugün siber alan kolayca erişilebilmektedir ve jeopolitik sınırların ötesinde bir varlığa sahiptir.

Üçüncü Bölüm; siber güvenlik politikalarının yer aldığı devlet, ekonomi ve toplum arasındaki üç ana gerilim alanını incelemektedir. Bu nedenle, siber güvenlik politikasının merkezinde iki tür soru yer almaktadır: sorumluluğun sınırlarına ilişkin bir soru olarak "*devletin, ekonomik ve toplumsal aktörlerin sorumluluğu nerede başlar ve biter?*", sorumluluklar açısından ise "*bir oyuncunun rollerinin sorumluluklarını üstlenmek için kullanmasına izin verilen araç veya unsur nedir?*" şeklinde cevaplanması gereken soruları içermektedir. Bu politikalar, toplumlarda var olan tematik ittifaklar, devletin farklı bölümleri ve ekonominin çeşitli çıkar grupları arasında bir denge bulmasına imkân sağlamaktadır. Devletin rolüne ilişkin farklı vizyonlar, beş ana boyutta değişen derecelerde yansıtılmaktadır. Böyle bir anlayış, stratejik kararlar almak, politika yönergelerini müzakere etmek ve devletin siber güvenlik etrafındaki değişen rollerini daha fazla araştırmak için sağlam bir temel sağlamaktadır.

Türkiye, üçüncü bölümde incelenen başlıktır. Ulusal strateji bağlamında taslak strateji belgesinin gözden geçirilmesi ve resmi olarak yayınlanması gerekmektedir. Stratejilerin çoğu savunma amaçlı olsa da siber savaşın Stuxnet olayında yaşandığı gibi sadece siber alanda değil fiziksel hasar açısından da riskler taşıdığı küçümsenmemeli ve hükümetin saldırı stratejilerini de geliştirmesi gerekmektedir. Eylem planları ve resmi raporlar kapsamında; her bakanlık ve hükümet yetkilisi kendi siber güvenlik strateji planlarını geliştirmesi gerekmektedir. Çoğunluğu özel sektöre ait olan ve kontrol edilen kritik altyapıların korunması için devletin rolü ve sorumluluğu açıkça belirlenmelidir. Kritik altyapıların korunması için kamu-özel ortaklığına dayalı model geliştirilmeli ve ortak CERT'ler oluşturulması gerekmektedir. Bilgi İletişim

Enstitüsü, Türkiye Bilimsel ve Teknolojik Araştıma Kurumu (TÜBİTAK) ve Devlet İletişim Merkezi (GCHQ) gibi kamu/özel kuruluşlar, özellikle hükümetin dikkatine yönelik çeşitli analiz ve tavsiyeler içeren ulusal raporlar yayınlamaya teşvik edilmesi gerekmektedir. Nesnelerin İnterneti'nin (IoT) ortaya çıkmasıyla, güvenliği ihlal eden her cihazın zararlı olma potansiyeli vardır. Her devletin kendi ayrı bireysel siber güvenlik politikasına sahip olması **b**ir zorunluluk haline gelmiştir. Bu bölüm, Türkiye'nin Ulusal Siber Güvenlik Politikalarını (NCSPs) eleştirel bir şekilde analiz etmektedir. Türkiye'nin Küresel Siber Güvenlik Endeksi'nde yer alan veriler ışığında ulusal siber güvenlik stratejileri incelenmekte ve karşılaştırılmaktadır. Belgeler, türetilen çerçeve ışığında analiz edilmektedir. Ulusun belirli özellikleri (yasal, organizasyonel, ekonomik güç ve siyasi durum vb.) ile siber stratejisinin odak ve içeriği arasındaki ilişkiler incelenmiştir.

Çalışmanın Dördüncü Bölümünde; siber alanda devlet aktörlerinin doğru dengeyi nasıl bulması gerektiğini, tırmanma riskini kontrol etme çabalarını neden sürdürmesi gerektiğini ve hükümetin giderek artan bir şekilde ekonomiden ve toplumdan aktörlerle neden sorumluluk paylaştığını tartışmıştır. Bu çalışmada, siber strateji oluşturma tecrübesi, Küresel Siber Güvenlik Endeksi'nde belirlenen bulgulara göre ülkenin siber güvenlik stratejileri seçilmiştir. Dördüncü bölümde ana başlık "İngiltere"'dir. Bu bölümde, bir önceki bölümdeki bulgular dikkate alınarak, analizin gerçekleştirilmesinde kullanılan her bir ana gösterge İngiltere üzerinden incelenmiştir.

Beşinci Bölüm'de; **çeş**itli kurum ve kuruluşlarda kullanılabilecek sağlam ve kapsamlı siber güvenlik bilgisi sağlamak için Türkiye ve İngiltere'nin önemli ve ortak siber güvenlik politikaları karşılaştırılmakta ve araştırılmaktadır. Bu kapsamlı çalışmada birkaç önemli ortak güvenlik politikası belirlenmiş ve tartışılmıştır. Bu bölümde, Türkiye ve İngiltere'nin beş boyutta siber güvenlik politikaları karşılaştırılmakta ve tartışılmaktadır.

Genel olarak bu çalışma, ülkelerin siber güvenlik taahhütlerini daha iyi anlamayı, boşlukları tespit etmeyi, iyi uygulamaların dâhil edilmesini teşvik etmeyi ve ülkelerin siber güvenlik duruşlarını iyileştirmeleri için faydalı bilgiler sağlamayı amaçlamaktadır. Ayrıca bu çalışma, ulusal düzeyde siber güvenliği yönetmek için kullanılan genel ulusal girişimler ve kaynaklar hakkında bilgi toplamayı, iyi uygulamalara, ortaklara ve bölgesel komşulara karşı kıyaslamayı, ulusal düzeyde koordinasyon ihtiyaçları konusunda çeşitli paydaşlar arasında farkındalık yaratmayı ele almaktadır.

Siber güvenlik alanında eğitimler verilmeli ve eğitimin her kademesinde müfredat desteklenmeli ve güncellenmelidir. Uzmanlaşmış siber güvenlik insan gücüne önem verilmelidir. Özellikle devlet bilgi sistemleri üzerinde yapılan güvenlik denetimleri ve kalem testleri, mevcut ulusal güvenlik politikalarına göre ulusal bir otorite tarafından gerçekleştirilmelidir. İlgili alanda konferans ve sempozyum sayıları umut verici görünürken, siber tatbikatlarda elde edilen siber tatbikat sonuçları kamuoyu için olumsuz bir imaj sergilemektedir. Bununla birlikte, bir ulus siber alanda avantaja sahip olmak istiyorsa, sadece savunmadan ziyade hem savunma hem de saldırı yeteneklerinin geliştirilmesi için çaba sarf etmelidir. Ulusal/uluslararası iş birliği kapsamında; özellikle kritik altyapıların korunması alanında, hükümet ve özel sektör kritik altyapı operatörleri arasında iş birliği yapmalıdır. Siber saldırıların tespiti ve önlenmesi, izleme, analiz ve müdahale gibi tüm faaliyetler, yüksek otoriteye sahip merkezi bir tesis tarafından yönlendirilmeli ve kontrol edilmelidir.

Türkiye ve İngiltere hükümetlerinin hem devlet hizmetlerinin hem de çevrimiçi ticari hizmetlerin güvenilirliğini artırmayı düşünmesi, aynı zamanda özel veya kişisel verilerin genel olarak ele alınması, e-devlet ve e-ticaret hizmetlerine güven konusunda kanıt sağlamak için bir geri bildirim mekanizması geliştirmesi önem arz etmektedir. Bu önlemler, siber saldırı ve siber güvenlik ile hizmet ve teknolojilerde güvenilirliğin anlaşılmasını teşvik etme çabasıyla birlikte ele alınmalıdır. Çalışma da siber güvenlik eğitiminin, teknik ve bilgisayar bilimleri disiplinlerinden öte, her düzeyde (uygun koşullarda) daha birçok eğitim disiplininde genişletilmesi gerektiği vurgulanmaktadır. İlerlemek için işletme yönetimi, felsefe, siyaset bilimi, uluslararası ilişkiler, kamu politikası, savunma ve güvenlik, hukuk, sosyoloji, ekonomi, etik gibi alanlardan birkaçının görülmesi ve müfredatlarında siber güvenlik konusunun geliştirilmesi önemlidir. Ek olarak, kamu ve özel sektörün siber güvenlik eğitimi için temel gereksinimleri belirlemesi gerekmektedir.

Siber güvenliğin sağlanması ve siber güvenlik politikalarının belirlenmesi için gerekli önlemlerin uygulanması, bilgi teknolojisi ve güvenliğin geleceği ile sonraki nesiller için iyi karşılanacak ve iyi yönetilecektir. Bibliyografik veriler, sosyal bilimlerde siber güvenlik konularında yeniden araştırma yapılmasının teknik bilimlerdeki araştırmalara kıyasla etki alanını genişleteceğini ortaya koymaktadır.

BİRİNCİ BÖLÜM

KAVRAMSAL VE TEORİK ÇERÇEVE

Güvenlik "gerçek veya algılanan bir tehdit olmadığında veya mevcut tehditlerin dikkate alınan nesne için bir tehlike oluşturmadığında gerçekleşen bir durum" olarak tanımlamak mümkün olsa da bu tanım bilim insanları için yeterli değildir. Güvenlikten yola çıkarak bu çalışma, güvenlik ve küreselleşmenin etkisiyle siber güvenliği tartışmalı bir kavram olarak açıklamaktadır. Bu çalışma çeşitli güvenlik tanımları ve farklı bağlamlarda doğrudan onunla ilgili bazı kavramları incelemektedir. Güvenlik anlamının açıklığa kavuşturulması, bilim insanları ve politika yapıcılar için önemli olmaktadır.

Bu bölüm, güvenlik kavramının nereden geldiğini ve günlük hayata nasıl yansıdığını uluslararası ilişkiler teorileriyle incelemektedir. Kişisel güvenlik ve devlet güvenliği arasındaki ilişkiyi tartışmakta, güvenlik politikalarını tanımlamakta ve değerlendirmektedir. Ayrıca siber güvenliği teorik ve kavramsal bir çerçevede incelemektedir.

1.1. Kavramsal Çerçeve

1.1.1. Güvenlik

"Güvenlik" kavramı, Fransızca sécurité veya Latince securitas kelimesinden gelmektedir. Çoğu sözlük ve ansiklopedi, tehlikeden, korkudan, yoksunluktan, ilgiden, hatta şüpheden kurtulmak olarak tanımlamaktadır. Aynı zamanda bir koşul, nitelik, değer veya durum olarak tanımlanmaktadır.[17] Yarım asırdan daha uzun bir süre önce Bernard Brodie, güvenliği tanımlamıştır[18]; "Türev değer, yalnızca gerçekleştirilmiş veya gerçekleştirilmekte olan ve

[17] Detaylı bilgi için bkz. Angus Stevenson (2007). *Shorter Oxford English Dictionary on Historical Principles*, 6th Edition, Oxford: Oxford University, s. 2734; "Security and Protection System", [https://www.britannica.com/technology/security-and-protection-system] (er. tar. 05.12.2020); [https://dictionary.cambridge.org/tr/s%C3%B6zl%C3%BCk/ingilizce/security] (er. tar. 05.12.2020); Urs E. Gattiker (2004). *The Information Security Dictionary, Defining the Terms that Define Security for E-Business, Internet, Information and Wireless Technology,* NewYork: Kluwer Academic Publishers.

[18] Bernard Brodie (1949). "Strategy as a Science", *World Politics*, Sayı. 1, No. 4, s. 477.

korunmaya değer olduğu düşünülen diğer değerleri teşvik ettiği ve koruduğu ölçüde anlamlı olmakla birlikte, tehdidin büyüklüğü ile orantılı olarak tüm diğerlerinin öncelikli olarak yerini alabilir." Onun tanımı, askeri güvenlik ile ekonomik refah, istikrar ve bireysel özgürlük gibi diğer değerler arasındaki değiş tokuşa odaklanmaktadır. Brodie bu konuya değindiği süreçte, uluslararası ilişkiler alanındaki teorisyenler, ulusal güvenlik ve ekonomi, sivil özgürlükler ve demokratik siyasi süreç gibi içişlerine büyük önem vermişlerdir. Brodie, ulusal güvenliği hem askeri hem de askeri olmayan yollarla ulaşılması gereken bir hedef olarak görmüştür. Stephen Walt, güvenliği bir hedef olarak görmezden gelmekte ve bunu dar bir şekilde, "askeri gücün tehdidi, kullanımı ve kontrolünün incelenmesi" olarak tanımlamıştır.[19] Ona göre güvenlik çalışmalarının ana odağı savaş olgusu olmalıdır.

Güvenlik arzusu, diğer insanlardan gelecek zarar tehdidine veya olgusuna karşı savunmacı ve kendini koruyan bir tepkidir. Tehdit edici insanlar olmasaydı, güvenliği garanti etme ihtiyacı ortadan kalkardı.[20] Yağmalama, ateş etme, tecavüz, cinayet veya diğer baskılayıcı ve şiddet içeren davranış biçimleri ile mücadele etmek gibi bir sorun olmayacaktı. Kargaşa ve can kaybı muhtemelen yine de olacaktı, ancak bu, diğer insanların saldırısının veya şiddetinin bir sonucu olmayacaktı. Bugüne kadarki insanlık tarihi, "her zaman başkalarına tehdit oluşturacak insanların da olacağı" önermesini güçlü bir şekilde desteklemektedir. Sonuç olarak, güvenlik sorunu devam etmektedir. Tehlike olarak algılanan bir dünyada, güvenlik arzusu siyasi düşünce ve eylemin merkezi bir endişesi haline gelmektedir.

Güvenlik fikri, doğanın güçleri değil, diğer vatandaşlar veya yabancılar tarafından yapılan zararlı eylemler sorununa yöneliktir.[21] İnsanlığın amaçları açısından güvenliğin en önemli noktası Hedley Bull tarafından ele alınmıştır:[22] "Uluslararası politikada güvenlik: ya nesnel güvenlik, yani gerçekte var olan güvenlik ya da hissedilen/deneyimlenen güvenlik anlamına gelen öznel güvenlik" tir. Güvenlik, insan ilişkilerinin bir koşuludur. Güvenlik, diğer insanlarla ilişkilerimizde düzen ve öngörülebilirliktir. Peki, neyin güvenliği? Hobbes'un "doğa durumunda" her insan potansiyel bir tehdittir. Çünkü sınırlı kaynakların

[19] Stephen M. Walt (1991). "The Renaissance of Security Studies", *International Studies Quarterly*, Sayı. 35, No. 2, s. 2.

[20] Robert Jackson (2003). *The Global Covenant: Human Conduct in a World of States,* London: Oxford University, s. 190-192.

[21] Barry Buzan (1984). "Peace, Power, and Security: Contending Concepts in the Study of International Relations", *Journal of Peace Research*, Sayı. 21, No. 2, [https://edisciplinas.usp.br/pluginfile.php/364767/mod_resource/content/1/buzan_1984.pdf].

[22] Hedley Bull (2012). *The Anarchical Society A Study of Order in World Politics* (ed. Andrew Hurrell), 4th Edition, London: Red Globe, s. 32-37.

olduğu bir dünyada hayatta kalma mücadelesi "herkesin herkese karşı savaşıdır". Bir insan daha güçlü olabilir, bir diğeri daha kurnaz olabilir, ancak her biri kendi yolunda diğerine zarar verebilir. Buna göre insanlar arasında hiçbir zaman tam bir güven ve karşılıklı güvenlik olamaz. İnsan durumu, en açık koşullarda bile güvensizdir, çünkü insanoğlu kaçınılmaz olarak- en azından bir dereceye kadar -umursamaz ve güvenilmezdir. En kötü ihtimalle kötü ve kötü niyetli kişilere maruz kalmaktadır. İnsan doğası kusurlu olduğu için mükemmel güvenlik hiçbir insan toplumunda var olamaz.[23] Güvensizlik, ne kadar büyük veya küçük olursa olsun, her zaman mevcuttur veya mümkündür. İstikrarlı, genellikle barışçıl ve müreffeh toplumlarda yaşayan insanlar yine de evlerini korumak için hırsız alarmları kurmaktadırlar. Ayrıca, saldırıya uğrama, tecavüze uğrama ve hatta öldürülme gibi makul bir risk olduğunu hesapladıkları günün belirli saatlerinde belirli alanlardan da kaçınabilmektedirler. Böyle bir davranış, paranoyadan çok sağduyu ortaya çıkarmaktadır. Ve bu, her bireyin veya toplumun en azından bir dereceye kadar güvensiz olduğunu vurgulamaktadır.

Güvenlik teriminin uzlaşmaya dayalı veya tek bir anlamı yoktur. Aksine, oldukça çekişmeli bir alanın çevresini belirlemektedir. Güvenlik nasıl sağlanacak? Kim, hangi tehlikelere karşı güvence altına alınacak? Güvenlik, gündelik söylemdeki ifadelerinden bağımsız olan gerçek bir varoluş durumuna atıfta bulunacaktır. Bu ontolojik güvenlik koşulu, oldukça farklı formlarda tasavvur edilmiştir. Örneğin, Uluslararası İlişkiler teorisinde Realizm ve İdealizm arasındaki büyük tartışmada, ya şimdiki zamanın göreceli bir durumu ya da geleceğin yegâne bir koşulu olarak düşünülmüştür. Ancak her iki durumda da güvenliğe yönelik atıflar belirli bir nesnelliği belirtmeye çalışmıştır. Bu düşünce, güvenlik kavramının incelenmesi gereken yol üzerinde en azından iki sonucu olduğunu vurgulamaktadır. Birincisi, güvenlik nesnel olarak bilinebilen ve bu nedenle özenle ölçülmesi, izlenmesi ve akıl ve bilimsel araştırma yoluyla iyileştirilmesi gereken bir şey olarak düşünülmektedir. İkincisi, güvenlik normatif yaklaşıma ulaşmakta; aktif olarak hedeflenmesi gereken bir "iyi şey" olarak görülmektedir. Böyle bir bakış açısıyla, güvenliğin genel tanımı, belirli bir nesneye yönelik tehditlerin yokluğunda ya da güvenliğin en azından olası olmadığı durumlarda karşılaşıldığı düşünülmektedir.

David Baldwin güvenliği "edinilmiş değerlerde düşük hasar olasılığı" olarak tanımlamıştır.[24] Benzer şekilde, Lawrence Krause ve Joseph Nye için de

[23] J. Jackson Preece (2011). *Security in International Relations*, London: University of London, s. 15.
[24] David A. Baldwin (1997). "The Concept of Security," *Review of International Studies,* Sayı 23, No 1, s. 13.

güvenlik kavramı şudur:[25] "… bir insanın hayatta kalması için gerekli olduğunu düşündüğü temel değerlerin asgari kabul edilebilir seviyelerine yönelik şiddetli tehditlerin yokluğudur." Bu tür güvenlik tanımları, terimin altında yatan özü bir şekilde yakalamaya çalışmaktadır. Ancak, yine de oldukça farklı şekillerde kavramsallaştırılabilmektedir. Belirli bir akademik ve / veya politik proje bağlamında özden güvenlik kavramına geçmek için, ele alınması gereken en önemli soru şudur: kimin için güvenlik? Çoğu durumda cevap, bazılarına ya da tüm bireylere, bazı durumlara ya da tüm durumlara atıfta bulunmaktadır. Bununla birlikte, güvenliğin, örneğin hayvan yaşamı, biyosfer veya fiziksel altyapı gibi çok çeşitli nesnelere eşit ölçüde uygulanabileceği unutulmamalıdır.[26]

Güvenlik kavramının bedensel bütünlük, ekonomik refah, özerklik veya psikolojik refah anlamına gelip gelmediği konusunda net olması gerekmektedir. Sonuçta, farklı nesneler ve değerler, oldukça farklı güvenlik kavramsallaştırmalarını ortaya çıkarmaktadır. Bunların en önemlileri elbette "insan güvenliği" ve "devletin güvenliği"dir. Baldwin güvenlik arayışı ile ilgili birkaç soru önermiştir. Birincisi belirli bir endişe konusuna bağlı olarak, güvenliğe yönelik gerçek tehditlerin tanımlanması gerekmektedir. İkinci olarak, bu tehditleri en aza indirgemek ve hatta ortadan kaldırmak için hangi araç ve stratejilerin kullanılması gerektiğini sorulması gerekmektedir. Tehlikeden kurtulma ve / veya caydırma stratejilerini destekleyen zorlayıcı askeri araçlara geri dönülüyor mu? Yoksa tehditlerin temel nedenlerine yönelik ve dolayısıyla tehlikenin üstesinden gelme ve onu aşma stratejileriyle ilişkili olan gelişimsel araçlar mı tercih ediliyor? Üçüncüsü, güvenliği artırmak için ne kadar kaynak ayrılması ve harcanan kaynakların farklı araçlar ve stratejiler arasında nasıl bölünmesi düşünülmesi gerekmektedir.

Güvenliği sağlamak için en uygun olanlar her zaman devlet kurumları mıdır, yoksa özel ve / veya sivil toplum sektörünün de oynayacağı bir rol var mıdır?[27] Aslında, Soğuk Savaş'ın sona ermesini takiben güvenliğin "yeniden tanımlanması" ile ilgili tartışmanın en büyük kısmının, bu soruları yanıtlamak için farklı yaklaşımların olduğudur.

Güvenlikle ilgili yapılan literatürün bir kısmı Neo-realizm üzerine eğilim göstermiş durumdadır. Neo-realizm, güç yetenekleri ve ölçülebilir riskler

[25] Lawrence B. Krause and Joseph S. Nye (1975). "Reflections on the Economics and Politics of International Economic Organizations", Section IV, *International Organization*, Sayı 29, No 1, s. 330.
[26] Robert Jackson (2005). *The Global Covenant: Human Conduct in a World of States,* London: Oxford University, s. 25-33.
[27] Emma Rothschild (1995). "What is Security?", *Daedalus*, Sayı 124, No 3, s. 55.

tarafından bilgilendirilen maddi bir yaklaşımdır.[28] Ahlaki ikilemler bu tür analizlerde eksik kalabilmektedir. Aynı zamanda kişinin ilgi alanlarının rasyonel arayışlarından uzaklaşması nedeniyle son derece uygunsuz olarak görülme eğilimindedir. Güvenliğe yönelik normatif veya neo-realist yaklaşımlar arasında devam eden tartışma, uluslararası ilişkilerde ve daha genel olarak sosyal bilimlerde çok daha büyük bir metodolojik tartışmanın parçası olmaktadır. Her yaklaşımın avantajları olduğu kadar dezavantajları da vardır. Bunu belirlemek kişinin görüş ve iradesine kalmaktadır.

Uluslararası İlişkiler disiplininde devletin güvenliği ve kişinin güvenliği temelde devlet ve devletlerarasındaki ilişkilerle ilgilidir. Devlet bir güvenlik düzenlemesi olarak ortaya çıktı ve günümüzde de güvenliği sağlayan başat aktör olarak devem etmektedir.[29] Hobbes'un kişisel güvenlik sorununa çözümü, insanları korumak için "Leviathan" olarak adlandırdığı bir siyasi düzen veya hükümdarın yaratılmasıdır. "Leviathan" hükümdar tarafından korunmak için bireysel olarak erkekler ve/veya kadınlar koruma özgürlüklerini değiş-tokuş yapmaya hazır olurlarsa ancak ortaya çıkabilmektedir. Hobbes için devlet, esasen toplu bir güvenlik düzenlemesidir. Ancak kendisinin de belirttiği gibi, kişisel güvensizlik sorununa devletçi çözüm eş zamanlı olarak devletlerarasında yeni bir güvensizlik tehdidine yol açmaktadır:[30]

Devletin güvenliği, bir devletin kendisini dış tehlikelerden ve tehditlerden koruma yeteneğini ifade etmektedir: örneğin, müdahale, abluka, yıkım, işgal, düşman bir yabancı güç veya terörist grup tarafından yapılan diğer bazı zararlı müdahalelere karşı kendini koruması gerekmektedir. Devlet güvenliğinin yöntemleri, evlerdeki hırsız alarmına benzemektedir. Devlet güvenliğinin amacı, devlete ve halkına yönelik saldırıları caydırmak, önlemek veya yenmektir. Devletin ve halkın fikirleri yakından ilişkilidir. Aslında, klasik bir egemenlik tanımı (bir devletin temel niteliği olan), toprak ve nüfus üzerinde etkili bir kontrol oluşturmaktadır. Yine de bazı teorisyenlerin yapmaya çalıştığı gibi, devlet güvenliği ile kişisel güvenlik arasındaki ayrımı yıkmamak çok önemlidir.

Liberal siyaset teorisinde, devlet yalnızca halka ait değildir, aslında halkın bir yaratımıdır. Halk hükümeti, halk yasası, halk ordusu, halk polisi,

[28] David A. Baldwin (1997). "The Concept of Security," *Review of International Studies,* Sayı. 23, No. 1, s. 17-21; Ole Waever, Barry Buzan (vd.) (1993). *Identity, Migration and the New Security Agenda in Europe,* London: Palgrave Macmillan, s. 104.

[29] J. Preece (2011). *Security in International* ..., s. 17.

[30] Thomas Hobbes (2016). *Leviathan* (ed. Marshall Missner), "Chapter 13: the Natural Condition of Mankind as Concerning their Felicity and Misery", London: Routledge, s. 84-85.

halk mahkemeleri, halk hapishaneleri ve hatta halkın idam sehpasıdır. Bu nedenle teoride devlet, kişisel çıkarları, devlet çıkarlarıyla eş anlamlı olan kendi vatandaşlarına tehdit oluşturamamaktadır. Ancak bu teorinin geçerli olması için, devletin zorlayıcı gücü son çare olarak ve mümkün olduğunca nadiren kullanılmalıdır. Başka bir deyişle, devlet ancak zorlayıcı gücü "çoğu insanı marjinal, önemsiz ve dolaylı olarak etkilediği sürece meşrudur".[31] Ancak pratikte, devletin güvenliği, liberal teorinin yapmasını istediği şekilde her zaman halkın güvenliğine dönüşmemektedir. Kendi yetki alanları dâhilindeki toprakların tümü üzerinde etkili bir kontrol uygulayamayan devletlerin nüfusları için kişisel güvenlik sağlanamamaktadır.[32] Bunlara genellikle zayıf' veya başarısız devletler denilmektedir. Kontrolü sürdürmek, ideolojik veya ekonomik hedefleri gerçekleştirmek için kendi halklarını doğrudan ve kasıtlı olarak tehdit eden devletler de vardır. Bunlara genellikle "totaliter" veya "polis devletleri" denilmektedir. Devletin güvenliği ile halkın güvenliği arasındaki ayrım yıkılırsa, bu gibi totaliter ya da polis devletleri durumları yeterince analiz edilemeyebilir.

Vatandaşların bireysel ve toplu olarak kendi güvenliklerini garanti altına almaları devlet aracılığıyla gerçekleşmektedir. Bu şekilde kişisel güvenlik, ulusal güvenliğe bağımlı veya buna benzer hale gelmektedir. Buna karşılık, güvensizlik, devlet / vatandaş ilişkisinin dışında yer alan bir dış tehdit olarak anlaşılmaktadır. Bu nedenle teorik olarak devlet, kişisel çıkarları devlet çıkarlarıyla uyumlu olursa kendi vatandaşlarına tehdit oluşturamamaktadır. Ulusal güvenlik paradigmasının geçerli olması için, devletin zorlayıcı gücü son çare olarak ve mümkün olduğunca nadiren kullanılmalıdır. Diğer bir deyişle, devlet ancak zorlayıcı gücü çoğu insanı ihmal edilebilir düzeyde etkilediği ve dolaylı olarak tam gücü nispeten küçük ve belirsiz bir yasa çiğneme grubuna verildiği sürece meşrudur. İdeal olan budur ve birçok durumda tarihsel gerçekliğe yakından karşılık gelmektedir. 1945'ten bu yana bu tür ülkelerin tarihinin, güvenli bir devletin nihai temeli olan liberal fikrini ortaya koyduğunu söyleyecek kadar ileri gidilebilir.[33] Bu tür devletlerin vatandaşları diğerlerinin yanı sıra Avrupa Birliği üye ülkeleri, Amerika Birleşik Devletleri, Avustralya, Kanada, Japonya ve Yeni Zelanda insanlık tarihindeki en yüksek yaşam standartlarına sahiptir. Bunlar elbette, halkları ortak güvenlik düzenlemelerinden (NATO vb.) olduğu kadar ekonomik birliklerden (Avrupa Birliği ve Kuzey Amerika Serbest Ticaret

[31] R.N. Berki (1986). *Security and Society Reflections on Law*, *Order and Politics,* London: Dent, s. 53; J. Preece (2011). *Security in International …*, s. 18.
[32] Ramesh Sunramanian (2008). *Computer Security, Privacy, and Politics: Current Issues, Challenges, and Solution*s, New York: IRM, s. 324-328.
[33] J. Preece (2011). *Security in International …*, s. 26-7.

Birliği vb.) ve uluslararası düzeyde kurumsallaşmış serbest ticaretten (GATT, WTO) büyük ölçüde yararlanan son derece uluslararasılaşmış ulus devletlerdir. Bu koşul, devletin bireysel özgürlüğün korunduğu güvenli bir toplum yaratma ve sürdürme becerisine çok şey borçlu olmaktadır.

Uluslararası ilişkilerde üç temel güvenlik paradigması vardır: ulusal güvenlik, uluslararası güvenlik ve insan güvenliği. Ulusal güvenlik ve uluslararası güvenlik yaklaşımı, insanlığın gelişmesi için gerekli bir ön koşul olarak devlete ahlaki öncelik vermektedir. Bu iki devlet merkezli yaklaşımın aksine, güvenlikle ilgili üçüncü bir bakış açısı, insanlara ve insanlık toplumuna, ait oldukları devletlerin veya uluslararası toplumun çıkarlarının üzerinde ve ötesinde ahlaki öncelik vermektedir. Güvenlik ile ilgili bu üç yaklaşım şu şekilde alt başlıklar halinde özetlenebilir:

1.1.1.1. Ulusal Güvenlik

Modern devlet, kökeninde önemli bir güvenlik düzenlemesi olmuştur. Günümüzde devletlere atfettiğimiz birçok role rağmen (refah, adalet vb.), güvenlik birincil husus olmaya devam etmektedir. Orta çağın Avrupası'nda ortaya çıkan ilk devletler, derin bir güvensizlikle karakterize edilmiştir. Roma İmparatorluğu'nun sözde "pax romana"sı[34] çoktan geride kalmış ve bunun ardından hem laik hem de dini olan bir dizi rakip otorite var olmuştur. Çeşitli güçlü ve zayıf hükümdarlar, bölge ve nüfus üzerinde kontrol sağlamak için birbirleriyle mücadele etmişlerdir. Belirsiz ve çelişkili yasaları benimsemişlerdir. Birleşik bir yasal düzen yerine, birbiriyle yarışan ve sıklıkla birbiriyle çelişen yasalar ve gelenekler karmaşası var olmuştur. Bazıları Roma hukukunun kalıntılarına, bazıları kilise kanununa, bazıları eski barbar kanunlarına dayanmıştır. Adalet, büyük ölçüde keyfi bir iş olmuştur. Örneğin, öldürülen bir kişinin ailesinin, katilin ailesinden intikam alabildiği "kan davası", ceza hukukunda (artan kısıtlamalarla da olsa), orta çağda kraliyet ayrıcalığı ile ortadan kaldırılıncaya kadar devam etmiştir.[35] Şiddet olağan olmuş ve Thomas Hobbes'un ifade ettiği gibi, "yalnız, fakir, iğrenç, vahşi ve kısa bir insanın hayatı var olmuştur.[36] Devlet, şimdiye kadarki bu kaotik toplumsal duruma düzen ve kontrol dayatmanın bir yolu olarak ortaya çıkmıştır.

---

[34] Avrupa'da milattan sonra birinci ve ikinci yüzyılları karakterize eden uzun barış dönemine verilen isimdir. Detaylı bilgi için bkz. Pax Romana, [https://www.britannica.com/event/Pax-Romana].

[35] J. Preece (2011). *Security in International …*, s. 24.

[36] Hobbes (2016). *Leviathan…,* s. 82.

Ulus devlet, vatandaşların dışarıdan gelecek müdahalelerden bağımsız bir şekilde, kendi amaçlarına göre hareket ettikleri bir davranış biçimidir. Bu genellikle karşılıklı bir düzenleme olarak belirtilmektedir. Ulusal güvenliği bu şekilde anlamak, ulus devlete ve özellikle temsilcilerine yalnızca güç kullanımında ayrıcalık verildiğine ve yalnızca kamu yararı için kullanılan bir güç olduğunda dikkat çekmektedir. Bu nedenle kamu görevlileri hem ulusal güvenliği hem de kişisel güvenliği sağlamaktan sorumludur ve güvenlik görevlerini ihmal etmekten veya yerine getirmemekten sorumlu tutulabilmektedirler. Aynı zamanda vatandaşlar, kendilerine getirilen makul güvenlik taleplerini görmezden geldikleri veya ihlal ettikleri için mahkûm edilebilmektedirler. Ulus devlet ile vatandaşları arasındaki bu karşılıklı güvenlik yükümlülüğü, ulus devletin halkın koruyucusu olma iddiasının genellikle haklı gördüğü normatif temeldir. Bu perspektiften bakıldığında, ulus devlet barışın, düzenin ve iyi yönetişimin sağlayıcısıdır. Dolayısıyla, "ulusal güvenlik" terimi, ulus devletin ayrı ve egemen bir topluluk olarak hayatta kalmasını ve böylelikle vatandaşlarının güvenliğini ve refahını temin ettiği tüm kamu politikalarına atıfta bulunmaya başlamıştır.

"Ulusal Güvenlik" kavramı, tanımı açısından her zaman tartışmalı olmuştur. Soğuk Savaş'ın sona ermesinden sonra yeni paradigmalar ortaya çıktıkça bu belirsizlik artmıştır. Ulusal Güvenlik üzerine çalışanların, güvenlik çalışmaları disiplini içindeki karmaşık konularla başa çıkmak için ulusal güvenlik kavramını daha iyi analiz etmeleri gerekmektedir. Richard Ullman ulusal güvenlik kavramını şu şekilde tanımlamıştır:[37] "Ulusal güvenliğe yönelik bir tehdit, bir devletin sakinlerinin yaşam kalitesini düşürmek için, görece kısa bir sürede ve büyük ölçüde tehdit eden bir eylem veya olaylar dizisidir. Başka bir deyişle, bir devletin hükümetinin veya bir devlet içindeki sivil toplum kuruluşlarının (kişiler, gruplar, şirketler) kullanabileceği mevcut politika seçeneklerini önemli ölçüde daraltmakla tehdit eden durumdur." Bu, bir tanım sunmaktan çok, basitçe tehdit ve ulusal güvenlik arasındaki ilişkileri tanımlamaktadır. Ancak bu açıklama yanıltıcıdır, çünkü geleneksel askeri tehditler olarak algılanan ulusal güvenlik anlamına gelmektedir. Öte yandan Ullman, bir bölgede bulunan sakinlerinin yaşam kalitesinin yalnızca kısa vadede düşünmüş ve sivil toplum kuruluşlarına (kişiler, gruplar, şirketler) atıfta bulunmuştur. Bu, tanımına kendi başına ulusal güvenlikten çok daha geniş bir anlam vermiştir.

[37] Richard H. Ullman (1983). "Redefining Security", *International Security*, Sayı 8, No 1, s. 135.

Ulusal güvenlik yaklaşımının realist savunucuları, genellikle devletlerin hem ana güvenlik kaynağı hem de temel güvenlik tehditleri olduğu bir dünyada yaşanıldığını varsaymışlardır. Ulusal güvenlik sorunu, bu anarşik dünya görüşünden, yani birbirine zarar verebilecek bağımsız ve silahlı devletlerin dünyasından kaynaklanmaktadır. Ulusal güvenlik politikaları, ulusal savunma ve caydırıcılık için silahlı kuvvetler oluşturmaya ve sürdürmeye yöneliktir. Suçlular, isyancılar, teröristler vb. gibi güvenliğe yönelik iç tehditlerle başa çıkmak için tasarlanmış önlemleri de içermektedirler. Ulusal güvenlik paradigması, iki rakip devletin birbirine aktif olarak karşı çıktığı Soğuk Savaş gibi durumları ele almak için iyi bir donanıma sahiptir. Ancak, devlet güvenliği ile kişisel güvenlik arasındaki ayrımı yıkma eğiliminden dolayı "zayıf, başarısız veya totaliter" devletlerin sorunlarını sorgulamak için çok etkili bir konumda değildir. Bu nedenle, örneğin, Schelling gibi realistler Soğuk Savaş sırasında ABD ile SSCB arasındaki silahlanma yarışına dair ikna edici açıklamalar yapmışlardır. Ancak Güney Amerika'nın "Jim Crow" yerel yasalarına karşı sivil haklar savunucularının veya Orta ve Doğu Avrupa'nın komünist ülkelerindeki siyasi muhaliflerin karşılaştığı güvenlik ikilemlerine büyük ölçüde sessiz kalmışlardır.[38]

1.1.1.1.1. Ulusal Güvenlik Politikaları

Ulusal güvenliği sağlamak için alınan politikalar ekonomik, politik veya askeri nitelikte olabilmektedir. Bunlar içeriden ya da dışarıdan yönlendirilmiş olabilmektedir. Ulusal güvenlik önlemleri, şunları içermektedir;[39]

- Etkili silahlı kuvvetlerin sürdürülmesi,
- Terörle mücadele tedbirlerinin uygulanması,
- Sivil ve olağanüstü savunmaların sağlanması,

[38] Bu çalışmada belirtildiği gibi güvenlik iki yolla sağlanabilmektedir: muhtemel koruyucunun caydırıcılığı ya da olası saldırgan tarafındaki çekingenlik. Thomas Schelling gibi bazı realistler, güvenlik politikasının temel bileşeni olarak caydırıcılığı, güvenliği sağlayacak bir unsur olarak düşünmüşlerdir. Örnek vermek gerekirse bu realistler Soğuk Savaş sırasında ABD ile SSCB arasındaki silahlanma yarışına dair ikna edici hesaplar üretmişlerdir. Ancak Güney Amerika'nın "Jim Crow" yasaları ile sivil haklar savunucularının veya Orta ve Doğu Avrupa'nın komünist ülkelerindeki siyasi muhaliflerin karşılaştığı güvenlik ikilemlerinde ise çoğunlukla sessiz kalmışlardır. Detaylı bilgi için bkz. Thomas Schelling (2006). *The Strategy of Conflict*, Cambridge, Massachusetts: Harvard University, s. 53-61, 83-85.

[39] David Campell (1998). *Writing Security United States Foreign Policy and the Politics of Identity,* Minnesota: University of Minnesota, s. 33-41.

- Dış saldırıları ve iç yıkımı tespit etmek ve bunlara karşı koymak için istihbarat kullanmak,
- İttifakları güçlendirmek ve tehditleri izole etmek için diplomasi kullanması,
- Ekonomik gücü iş birliğini teşvik etmek ve siyasi rakipleri izole etmek veya zayıflatmak için kullanmaktır.

Örneğin, Amerika Birleşik Devletleri'nin 2018 Ulusal Güvenlik Stratejisi, "Milletimizi potansiyel tehditlere karşı savunmayı… Federal Hükümetin ilk ve temel taahhüdü" olarak öne sürmüştür.[40] Bunu yapmak için ABD hükümeti, "bir askeri güç olarak cephaneliğindeki her aracı, daha iyi vatan savunmalarını, kanun yaptırımını, istihbaratına yönelik güçlü çabaları kullanacağını" vurgulamıştır. Benzer şekilde, İngiltere İçişleri Bakanlığı da ulusal güvenliğine yönelik herhangi bir tehditten İngiltere'yi korumaktan sorumlu olduğunu ileri sürerek,[41] ulusal güvenlik stratejilerinin ülkesine veya halkına herhangi bir zarar gelmesini önlemek için polis ve güvenlik teşkilatlarıyla birlikte çalıştıklarını beyan etmektedirler.

1.1.1.2. Uluslararası Güvenlik

Çoğulcu veya rasyonalist olarak bahsettiğimiz uluslararası güvenlik savunucuları, çatışma ve iş birliğinin bir karışımı ile karakterize edilen bir dünya görmektedirler. Bu açıdan bakıldığında, devletlerarasındaki ilişkileri "anarşik bir toplum" oluşturmaktadır. Bu nedenle, tek bir otorite veya hükümet kaynağı yoktur. Uluslararası ilişkiler makul bir şekilde düzenli ve amaçlıdır. Uluslararası ilişkiler, hayatta kalma ve birlikte yaşama konusundaki ortak ilgiden kaynaklanan karşılıklı düzenleme ve kısıtlamalara tabidir. Bunu takiben rasyonalistler, güvenliği sağlamaktan sorumlu tek aktörün devlet olmadığı varsayımlarında realistlerden farklıdırlar. Bunun yerine rasyonalistler, güvenliği sağlama sorumluluğunun uluslararası toplumu da kapsadığına inanmaktadır. Güvenliği kavramsallaştırmanın bu şekli, küresel ve giderek kurumsallaşan uluslararası bir toplum fikrinin zemin kazandığı yirminci yüzyılda öne çıkmıştır. En eski somut örneklerinden biri, Birinci Dünya Savaşı'nın ardından 1919'da Paris'te oluşturulan bölgesel yerleşimi korumayı amaçlayan Milletler Cemiyeti Misakının 11. Maddesi'dir.[42] Bu maddeye göre; "Milletler Cemiyet üyesi olan

[40] USA. *National Cyber Strategy* (September 2018), s. 7.
[41] UK. *National Cyber Security Strategy 2016-2021*, s. 37-39.
[42] Milletler Cemiyeti Misakı, s. 6, [http://sam.baskent.edu.tr/belge/] (er. tar. 27.01.2022).

ulusların herhangi birine doğrudan doğruya dokunulsun veya dokunulmasın, her savaş veya savaş tehdidi iş bu vesileyle bütün Cemiyet için bir endişe konusudur. Ulusların barışını etkin bir şekilde korumaya yönelik her türlü önlemleri almakla Milletler Cemiyeti yükümlüdür." Benzer bir durum, 1945 yılında kabul edilen Birleşmiş Milletler Şartı'nın 1. Maddesinde de düzenlenmiştir:[43] "Uluslararası barış ve güvenliği sağlamak ve bu amaçla; barışa yönelik tehditlerin önlenmesi, ortadan kaldırılması ve saldırganlık eylemlerinin veya diğer barış ihlallerinin bastırılması için etkili toplu önlemler almak…" BM'nin amaçları arasındadır.

Küresel uluslararası toplum, insan yaşamını tehdit edebilecek olağandışı durumlarla karşılaşmazsa bu bağlamda güvensizlik içeriden gelmeye başlamaktadır. Güvensizlik genellikle uluslararası toplumun diğer üyelerinin (yani devletlerin) eylemlerinin bir sonucudur. Ancak güvensizlik aynı zamanda terörist gruplar gibi devlet dışı aktörler tarafından da yaratılabilir. 11 Eylül saldırılarını izleyen dönemde ABD'nin öncülüğünde "teröre karşı savaşı" küresel alanda meşrulaştıran böyle bir devlet dışı dinamik olmuştur. Bu açıdan bakıldığında uluslararası güvenlik, bir bütün olarak uluslararası toplum için bir iç sorun teşkil etmektedir. Bu bağlamda, silahlı kuvvet kullanımı, özünde uluslararası toplumun rasyonel ve işbirlikçi yapısını tehdit eden aktörlerin bertaraf edilmesi açısından bir iç sorun olarak düşünülebilir. Ayrılık, irredantizm, savaş, fetih, işgal, toplu sınır dışı etme, soykırım ve uluslararası hukuku ihlal eden diğer eylemlerin tümü; uluslararası toplumdaki genel barış, düzen ve hukuka uygunluk koşulunu bozma tehdidinde bulunmaktadır. Bu tür ihlallere yönelik uluslararası hukuk ve yaptırım, devlet içindeki iç hukuk uygulamasına benzemektedir. Yani, toplum içinde (bu durumda uluslararası toplum) genel bir barış ve istikrar koşulunu korumayı amaçlamaktadır. Böylece o toplumun üyeleri (esas olarak devletler) günlük yaşamlarına devam edebilirler. Bununla birlikte, uygulamada bu tür bir yaptırım oldukça tartışmalı bir konudur. Çünkü potansiyel olarak uluslararası toplumun bir üyesi, kendi ulusal güvenliği adına tüm uluslararası toplumun güvenliğini hiçe sayıp feda edebilir. ABD önderliğindeki askeri güçlerin 2003'te Irak'ı işgal etmesi buna iyi bir örnek olmaktadır. Bağımsız ve egemen Irak devletine yönelik yapılan Bush yönetiminin askeri saldırısı ve ardından Irak'ı işgal etmesi, diğer devletlerce uygun görülmemiştir. Bu işgale yönelik Amerika'ya, Birleşmiş Milletler Güvenlik Konseyi tarafından yetki ve izin verilmemiştir. Bu ve diğer nedenlerden dolayı uluslararası hukuk alanındaki birçok uzman bu eylemleri yasa dışı olarak değerlendirmiştir. Buna

[43] Birleşmiş Milletler Antlaşması ve Uluslararası Adalet Divanı Statüsü, s. 5, [https://www.ombudsman.gov.tr/] (er. tar. 11.08.2022).

karşılık, 1990-91 Körfez Savaşı, hem daha önceki BM Güvenlik Konseyi yetkisi ile yapıldığı hem de uluslararası toplum üyeleri tarafından neredeyse evrensel destek aldığı için genellikle meşru uluslararası kanun yaptırımının birkaç örneğinden biri olarak gösterilmektedir.[44]

1.1.1.3. İnsan Güvenliği

Genellikle dayanışmacı ya da devrimci olarak adlandırılan insan güvenliği savunucuları, kişisel güvenliği uluslararası ilişkilerin temel bir sorunu olarak görmekteler ve sadece ilgili devletin iç siyasi meselesi olmadığını düşünmektelerdir. İnsan güvenliği genellikle güvenlik sorularına yeni bir bakış açısı olarak sunulmaktadır. Immanuel Kant, yer veya yargı yetkisi dışında diğer insanlara karşı evrensel bir görevin var olduğuna inanmıştır. Kant, tüm erkeklerin ve kadınların kamu otoriteleri tarafından bireysel insanlar olarak tanınması ve korunmasına yönelik meşru iddiasını kastettiği "evrensel bir insan hakkı" nı tanımlamıştır. Benzer şekilde, insan hakları hukuku, insanlığa karşı suçlar doktrini, savaşmayanların uluslararası insancıl hukuka göre hakları (savaş hukuku), soykırım yasağı, "insan güvenliği" terimi ortaya çıkmadan önce, kişisel güvenlik devletlerin güvenliğinin ötesinde korunması için var olmuştur.[45]

İnsan güvenliğinin somutlaştırdığı düşünce, özünde kişinin güvenliği, devletin güvenliği ve toplum güvenliğinin temelde birbirine bağlı olmasından kaynaklanmaktadır. Dünyadaki herhangi bir erkek, kadın veya çocuk güvensiz ise, o zaman kimse güvende değildir.[46] Bir devlette kişisel güvensizliğe tahammül etmek, güvensizliğin diğer devletlere ve dolayısıyla uluslararası topluma yayılma riskini artırmaktadır. Örneğin, bir devletteki insan veya azınlık hakları ihlalleri, diğer devletlerde sığınmacılar için bir sorun yaratan ve bunun sonucunda Birleşmiş Milletler Mülteciler Yüksek Komiserliği gibi uluslararası kuruluşlar için bir endişe konusu oluşturan, sınırları aşan mülteci akışlarını tetikleyebilmektedir. Benzer bir zincir etkisi, terörizm, iç savaş veya uluslararası sınırları aşmakla yıldırmaya çalışan diğer tehditler konusunda da görülebilmektedir.

İnsan güvenliği savunucularının çağdaş güvenlik düzenlemelerine yönelttikleri eleştiri, hukuki sınırlardan bağımsız olarak varlığını sürdüren

[44] P.W Singer ve Allan Friedman (2013). *Cybersecurity and Cyberwar: What Everyone Needs to Know,* England: Oxford University, s. 20-21.
[45] Immanuel Kant (2015). *Ahlak Metafiziğinin Temellendirilmesi,* Ankara: Türkiye Felsefe Kurumu, s. 17-19.
[46] J. Preece (2011). *Security in International* ..., s. 21.

insanların birbirine bağlılık ilkesinden kaynaklanmaktadır. Devletler içindeki işkence, terörizm, etnik temizlik, soykırım ve diğer ağır insan hakları ihlalleri, tüm insanların güvenliği sağlanacaksa tolere edilmemelidir. Devletler, bu temel insani yükümlülükten kaçmak için uluslararası eşit egemenlik ve müdahale etmeme ilkelerinin arkasına saklanmamalı, bunları durdurmak için birlikte hareket etmelilerdir. İnsan güvenliği paradigması, uluslararası ilişkilerde giderek daha etkili hale gelmektedir.

1.1.2. Siber Güvenlik

"Siber güvenlik" geniş bir kavramdır. Genel olarak, elektronik ağların bütünlüğüne, kullanım amaçlarına ve ilgili tüm veri ve sistemlere atıfta bulunmaktadır. Bu, kişisel sistemlerdeki sağlıktan, askeri ağların elektronik savaşından korunmasına kadar her şeyi içerebilmektedir. Aynı zamanda hem kişinin kendi ağlarını savunması hem de bir düşmana karşı saldırı yeteneklerinin geliştirilmesi veya kullanılması anlamına gelebilmektedir.[47] Bu literatürdeki tartışma da iki farklı düzeyde gerçekleşmektedir.

İlki, tehdidin niteliği ve onu ele almanın potansiyel araçları hakkında bir tartışmadır. İkincisi, siber güvenliğin ontolojisi, epistemolojisi ve kavramın evrimi hakkında bir meta-tartışma vardır.

İkincisi, ilkini, belirli siyasi gündemleri ilerletmek için esnek bir şekilde tanımlanmış ve spekülatif tehditlerin sunulduğu sürekli bir tehditte olma durumu olarak tasvir etmiştir. Büyük ölçüde realist varsayımlarla bilgilendirilen bu literatürdeki politika çalışmaları, tipik olarak ilk tartışmanın içinde yer alırken, akademik literatürdeki çalışmalar tipik olarak konstrüktivizmdir ve güvenlik söyleminin meta tartışmalarıyla ilgilenmektedir. Örneğin Der Derian, hem "Dijital Çağ"ın ortaya çıkmasının hem de 11 Eylül 2001 saldırılarının farklı şekillerde "ulusal güvenliğin anlamını ve söylemini dönüştürdüğünü" savunmuştur.[48] Der Derian, her ikisini de siber alanın iletişim gücünden ve diğer iletişim teknolojisi biçimlerinden yararlanan, dönüştürücü söylemsel değişimin iki tarzı olduğu kanaatindedir.

Dijital dünyanın kısaltması olarak interneti sık sık kullanırken, siber alan aynı zamanda bu bilgisayarların arkasındaki insanları ve bağlantılarının

[47] Özellikle ABD hükümetinin kullanımında farklı terimlerin ve ilgili kavramların kapsamlı bir incelemesi için bkz. Myriam Dunn Cavelty (2008). *Cyber-Security and Threat Politics: U.S. Efforts to Secure the Information Age*, New York: Routledge.

[48] James Der Derian (1990). "The (S)pace of International Relations: Simulation, Surveillance and Speed", *International Studies Quarterly*, s. 298-300.

toplumlarını nasıl değiştirdiğini de kapsamaktadır. O halde siber alanın en önemli özelliklerinden biri, sistem ve teknolojilerinin insan yapımı olmasıdır. Bu nedenle siber alan, fiziksel veya dijital olduğu kadar bilişsel alan tarafından da tanımlanmaktadır. Siber alan küresel olabilir, ancak hem hükümette hem de medyada sıkça kullanılan "devletsiz" veya "küresel ortaklar" gibi değildir. Tıpkı insanların dünyayı yapay olarak "uluslar" dediği, bölgelere ayırdığı ve insan türünü "milliyetler" dediği, çeşitli gruplara ayırdığı gibi, benzer şekilde siber alan için de bu ayrım yapılabilmektedir. Coğrafyaya bağlı fiziksel altyapıya ve kullanıcılara dayanmaktadır. Dolayısıyla egemenlik, milliyet ve mülkiyet gibi insani kavramlara da tabii olmaktadır. Başka bir deyişle, siber alanın bölünmeleri, Amerika'yı Kanada'dan veya Kuzey'i Güney Carolina'dan ayıran anlamlı ve aynı zamanda hayali çizgiler kadar gerçektir. Ancak siber alan, tıpkı yaşam gibi sürekli gelişmektedir.

Teknolojinin ve onu kullanan insanların melez birleşimi, siber alanın boyutundan ve ölçeğinden ona rehberlik etmeye çalışan teknik ve politik kurallara kadar her şeyi çeşitlendirmektedir. Birçoğuna göre siber alanın coğrafyası diğer ortamlardan çok daha değişkenlik göstermektedir. Dağlar ve okyanusları hareket ettirmek zordur, ancak siber alanın bazı kısımları bir düğmeye basılarak açılıp kapatılabilmektedir. Temel özellikler aynı kalmakta, ancak topografya sürekli değişim halindedir. Bugünün siber alanı, 1982 siber alanıyla hem aynı hem de tamamen farklılık arz etmektedir. Örneğin, siber alanı oluşturan donanım ve yazılım, başlangıçta sabit kablolardan ve telefon hatlarından çalışan bilgisayarlar için tasarlanmıştır. Bugün, bilgisayar kullanımının giderek artan bir yüzdesi masaüstü bilgisayarlar yerine mobil cihazlara ve iPad'leri kullanmaktadırlar. Siber alan teknolojisi ile birlikte, ondan beklentiler de aynı şekilde gelişmektedir. Öyleyse interneti oluşturan şey daha da temel ve hızlı bir şekilde gelişmektedir. Aynı anda çok daha büyük hal almakta (her gün küresel dijital bilgi arzına yaklaşık yirmi milyon terabit eklenmektedir) ve çok daha kişisel hale gelmektedir. Çevrimiçi bilgiyi pasif bir şekilde almak yerine, bireysel kullanıcılar siteleri oluşturmakta ve kişisel kullanımlarına göre uyarlamaktadır. Sonuçta çevrimiçi olarak kendileri hakkında daha fazlasını açığa çıkarabilmektedirler. Bu siteler, Amerika'daki Facebook ve Çin'deki RenRen gibi sosyal ağlardan, Twitter ve Çin eşdeğerleri Tencent ve Sina gibi mikro bloglara kadar uzanmaktadır. Nitekim Çin'deki mikrobloglar (Weibo olarak adlandırılır), 2012'de beşyüzelli milyonun kaydedildiği ölçüde yükselmiştir. Bu nedenle, siber alan bir zamanlar sadece bir iletişim ve ardından e-ticaret alanı iken (yılda 10 trilyon dolara ulaşabilen satış), "kritik altyapı" dediğimiz şeyi

içerecek şekilde genişlemiştir. Bunlar, tarım ve gıda dağıtımından bankacılık, sağlık, ulaşım, su ve elektriğe kadar modern uygarlığımızı yöneten temel sektörlerdir. Bunların her biri bir zamanlar birbirinden ayrı durmuştur. Ancak şimdi hepsi birbirine bağlı ve bilgi teknolojisi yoluyla, genellikle "Merkezi Denetim ve Veri Toplama Sistemi (SCADA)" aracılığıyla siber alana bağlı olmuştur. Bunlar, kritik altyapının diğer süreçlerini izleyen, değişimi ayarlayan ve kontrol eden bilgisayar sistemleridir.[49]

Siber güvenlik kavramının tanımlanmasının zor olmasının nedeni, genişleyen küresel doğası ve bugünün siber alanında neredeyse tanınmaz olması gerçeğinde de yatmaktadır. ABD Savunma Bakanlığı, siber alanın vaftiz babası olarak kabul edilebilmektedir. Geçmişi, ARPANET gibi ilk bilgi işlem ve orijinal ağlar için yaptığı fonlara kadar uzanmaktadır.[50] Yine de ABD zaman geçtikçe ayak uydurmakta zorlanmaya başlamıştır. Yıllar boyunca, siber alan olarak düşündüğü şeyin ondan fazla farklı tanımını yayınlamıştır. Bunlar, dijitalleştirilmiş bilgilerin bilgisayar ağları üzerinden iletildiği kavramsal ortamdan; siber alanın yalnızca iletişim için ve büyük ölçüde hayali olduğunu ima ettiği, elektronik ve elektromanyetik spektrumun kullanımı ile karakterize edilen bir alan olduğu, bilgisayar ve füzelerden güneş ışığına kadar her şeyi kapsadığı için reddedilmiştir. ABD yine yapmış olduğu bir tanıma göre siber alanı "internet, bilgisayar sistemleri, telekomünikasyon ağları, gömülü işlemciler ve denetleyiciler dâhil olmak üzere birbirine bağlı bilgi teknolojisi altyapılarından oluşan bilgi ortamındaki küresel etki alanı adını vermişlerdir. Özünde siber alan, bilginin çevrimiçi olarak depolandığı, paylaşıldığı ve iletildiği bilgisayar ağlarının (ve arkasındaki kullanıcıların) alanıdır. Ancak siber alanın tam olarak mükemmel bir şekilde ifade edilmiş tanımını bulmaya çalışmak yerine, bu tanımların ulaşmaya çalıştığı şeyi ortaya çıkarmak daha yararlıdır.

"Siber alan ve onu benzersiz kılan temel özellikler nelerdir?" Siber alan her şeyden önce bir bilgi ortamıdır. Oluşturulan, saklanan ve en önemlisi paylaşılan dijitalleştirilmiş verilerden oluşmaktadır. Bu, sadece fiziksel bir yer olmadığı ve dolayısıyla her tür fiziksel boyutta ölçüme meydan okuduğu anlamına gelmektedir. Ancak siber alan tamamen sanal değildir. Verileri depolayan bilgisayarların yanı sıra akışına izin veren sistemleri ve altyapıyı içermektedir.

[49] Reardon ve Choucri (2012). "The Role of Cyberspace in International Relations…", s. 9-12; Lorenzo Cavallaro ve Dieter Gollmann (2013). *Information Security Theory and Practice,* New York: Springer.

[50] P.W Singer ve A. Friedman (2013). *Cybersecurity and Cyberwar: What Everyone…,* s. 11. İkinci bölümde siber güvenliğin tarihsel gelişimi alt başlığında "ARPANET" incelenmektedir.

Bu, ağa bağlı bilgisayarların internetini, kapalı intranetleri, hücresel teknolojileri, fiber optik kabloları ve alan tabanlı iletişimleri içermektedir.

Dartnell, siber alanın güçlü mesajları, bireylerin kimliklerindeki değişimi teşvik edebileceği ve dolayısıyla siyasi sınırları ve aktörleri yeniden şekillendirebileceği bir araç olarak nasıl kullanılabileceğini tartışmıştır.[51] Bu süreci, "güvenliğin kalbinde yer alan öz ve güvenlik kavramlarını dönüştürmek" olarak tanımlamıştır. Der Derian'a göre bugünkü "siber güvenlik" modası, bu sürecin bir sonucudur. Dartnell'e göre, baş aktörler taktiksel davranan devletler değil, stratejik olarak "ulusötesi ideolojik radikalizmi" yaymayı uman devlet dışı aktörlerdir.[52]

Hansen ve Nissenbaum'un yaklaşımı, siber alanın ulusal güvenlik bağlamında nasıl tanımlandığına yararlı bir şekilde dikkat çekmiş ve bunun meydana geldiği birkaç önemli mekanizmayı aydınlatmıştır. Tüm güvenlik tehditlerini basitçe sosyal söylemin ürünleri olarak ifade etmişler, siber güvenliği diğer güvenlik sorunlarından ayırmamışlardır. Bu nedenle siber güvenlik, ne dereceye kadar siyasi güdümlü sürekli tetikte olma durumudur? Ya da meşru dış tehditlere ölçülü bir yanıt olduğunu belirlemek için kullanılmamakta mıdır? Bu, politika yapıcılar için kritik bir ayrımdır; siber tehdit, diğer güvenlik endişelerine göre daha etkisi ön planda ise, bu politika sürecini ve savunma kaynaklarının tahsisini bilgilendirmek için olmalıdır. Teorik bir perspektiften bakıldığında, literatür güvenlikleştirme için önemli mekanizmalar belirlemiş olsa da, bu süreci yönlendirebilecek bürokratik veya örgütsel çıkarları keşfetmede başarısız olmuştur.[53] Aslında siber alan, bu kavramların her birine güçlü bir şekilde bağlıdır. Ancak, hangisinin en uygun analitik çerçeveyi sunduğunu söylemek kolay değildir. Siber alan bir ağ, sosyal medya gibi yeni teknolojik yenilikler için bir platform, bir iletişim kanalı ve bir bilgi deposudur. Telekomünikasyon veya bilgisayarlar gibi diğer teknolojilere kavramsal olarak nasıl bağlanması gerektiği açık değildir. Ayrıca, siber alan teknolojisi, ilgili uygulamaları ve teknik standartları ile ağları oluşturan bireysel kullanıcılar arasındaki uygun sınırların nerede olduğu da belirsizdir. Bunlar birinci dereceden kavramsal bulmacalardır ve akademisyenlerin ve politika yapıcıların daha fazla dikkatini gerektirmektedir.

---

[51] Michael Dartnell (2003). "Weapons of Mass Instruction: Web Activism and the Transformation of Global Security," *Millennium,* Sayı 32, No 3, s. 478.

[52] Dartnell (2003). "Weapons of Mass Instruction: Web Activism and the Transformation…", s. 486.

[53] Lene Hansen ve Helen Nissenbaum (2009). "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly*, Sayı 53, No 4, s. 1163-1165.

Bilgisayar mühendisleri ve uzmanların siber güvenliği inceleme nedenleri, teknik sistemlerin güvenliğini artırma amacından kaynaklanmaktadır. Siber güvenlik için ITU'nin yaptığı tanım; bilgi ve iletişim teknolojileri güvenlik hedefinin üç birleşiminden oluşmaktadır. Bu üç birleşim, "gizlilik", "ulaşılabilirlik" ve "bütünlük"tür. Buradaki anahtar kavram, ulusal yasalar veya uluslararası anlaşmalar, standartlar, organizasyonlar, kültürel ve toplumsal yapı, teknolojilerdir. Temel amaç farklı aktörler arasında "güven" ve "beklentilerin" istikrarını sağlamak olan politik ve stratejik "düzenleme"dir. Devletin rolüne çok az odaklanma eğiliminde olan teknik yönelimli siber güvenlik, sosyal bilimler literatüründe ele alınan bilgi paylaşımı ve diğer örgütsel önlemler konularında "sığ" kalmaktadır. Devlet ve onun bürokratik birimleri, güvenlik garantörü, yasa koyucu ve düzenleyici veya güvenlik ortağı olarak karşımıza çıkmaktadır.

Dijital sürekliliğin insan faaliyetinin tüm alanlarına girmesi ve benzeri görülmemiş düzeyde teknolojik yenilik ve karşılıklı bağımlılık, siber güvenliği tek başına, teknik bir sorun veya ayrı bir politika alanı olarak incelemeyi imkânsız hale getirmiştir. Son yıllarda, siber güvenlik, birden çok disiplinin ve politika alanının kesiştiği noktada yer almaktadır: dijital erişim ve bağlanabilirlik, dayanıklılık, ceza adaleti, diplomasi, uluslararası güvenlik ve savunma, dijital ekonomi ve ticaret ile yeni teknolojiler. Dördüncü Sanayi Devrimi'nin[54] kazanımlarını elde etmekte olan uluslarla birlikte, siber güvenlik küresel politikanın yadsınamaz bir gereksinimi haline gelmiştir. Bu, tüm hükümeti ve hatta bazen tüm toplumu kapsayan ulusal siber güvenlik stratejilerinin benimsenmesinde veya özellikle ilgili yasaları olmayan gelişmekte olan ülkelerde ulusal siber suç mevzuatının geliştirilmesi veya uyarlanarak revize edilmesinde önemli bir artışa neden olmuştur. Devletler bir bütün olarak hükümet ve sivil sektör de dâhil olmak üzere birçok rutin ve günlük işlev için siber alan ve bilgi sistemlerine bağımlıdır.

[54] Birinci Sanayi Devrimi, üretimi mekanize etmek için su ve buhar gücünü kullanmıştır. İkinci Sanayi Devrimi, seri üretimi sağlamak için elektrik gücünü kullanmıştır. Üçüncü Sanayi Devrimi, üretimi otomatikleştirmek için elektronik ve bilgi teknolojilerini kullanmıştır. Dördüncü Sanayi Devrimi ise Nesnelerin İnterneti (IoT) yoluyla birbirine bağlanabilirlik, gerçek zamanlı verilere erişim ve siber-fiziksel sistemlerin gelişimi sayesinde dijital teknolojiye verilen önemin somutlaştırılmış halidir. Önceki endüstriyel devrimlerle karşılaştırıldığında, Dördüncü Sanayi Devrimi, doğrusal bir hızdan ziyade üstel bir hızda gelişmektedir. Bu hızla gelişen ve değişen sistemin genişliği ve derinliği, tüm üretim, yönetim ve yönetişim sistemlerinin dönüşümünü müjdelemektedir. Detaylı bilgi için bkz. Klaus Schwab (2018). *Dördüncü Sanayi Devrimi*, World Economic Forum, İstanbul: Optimist Yayıncılık; "The 4th Industrial Revolution: What it Means, How to Respond", [https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/] (er. tar. 09.04.2022).

Açık ve kolay bilgi alışverişi için tasarlanmış bir interneti kullanan Türkiye veya İngiltere'nin yüksek düzeyde ağa sahip toplumu, yirmi birinci yüzyıl siber alanında siber saldırıya maruz kalabilmektedir.

Çalışmada kavramsal çerçevenin yanısıra, problemi ortaya koymak için kullanılan kavramların referans katkısı açısından da desteklenmesi amacıyla teorik çerçeve sunulacaktır. Çalışmanın teorik çerçevesi şu alt başlıklar halinde verilecektir: Uluslararası İlişkiler'de Güvenlik, Siber Güvenlik ve Temel Varsayımları, Siber Güvenlik'te İnternet Sisteminin İşleyişi.

1.2. Teorik Çerçeve

1.2.1. Uluslararası İlişkiler'de Güvenlik

Güvenlik, insan yaşamının temel bir değeridir. Güvende olmak, tehlike ya da korkudan rahatsız olmamaktır. Thomas Hobbes'un Leviathan[55]'da belirttiği gibi, güvenlik olmadan "sanayiye yer yoktur… bilim ve sanat yoktur, toplum yoktur ve en kötüsü, sürekli korku ve şiddetli ölüm tehlikesi vardır; güvenliğin olmadığı insanın hayatı, yalnız, fakir, vahşi ve kısa" olmaktadır. Gelişmiş Batılı devletlerin vatandaşları, Dünya Ticaret Merkezi'ne 11 Eylül'de yapılan saldırı veya 7 Temmuz'da Londra Metrosu'na yapılan bombalamalar gibi bazı olağanüstü olaylarla karşılaşılana kadar güvenliklerinin rutin olarak sağlandığını kabul etmişlerdir. Onlara göre güvensizlik, on yedinci yüzyıl İngiliz İç Savaşı sırasında Hobbes için olduğu gibi günlük yaşamın bir gerçeği olmuştur. Böylesi son derece güvensiz koşullar, özellikle günlük yaşamın temel meşguliyetinin güvenlik ve hayatta kalmaya dönüştüğü savaş koşullarında belirgindir.[56]

Şiddetli çatışma yaşamış bölgelerden birisi de Yugoslavya'dır. Yugoslavya'da bölünme savaşları sırasında özellikle Saraybosna'da bombalanmış bir sokak pazarının görüntüsü, bireyi ve toplumu endişe, korku, güvensizlik, kargaşanın eşiğine sürüklemiştir. İnsanlar böyle bir kargaşada barınak bulma arayışına düşmüştür. Güvenliğe ulaşamayanlar sokaklarda ya yaralı kalmıştır ya da ölümle sonuçlanmıştır. Bunun gibi sahneler çeşitli zamanlarda Bağdat, Beyrut, Gazze, Mogadişu, Grozni, Belfast, Ruanda ve dünyanın pek çok şehrinde de görülmüştür.

---

[55] Hobbes (2016). *Leviathan*…, s. 84-85.

[56] Jef Huysmans (1998). "Security! What Do You Mean? From Concept to Thick Signifier", *European Journal of International Relations*, Sayı 4, No 2, s. 227-231.

Mearsheimer'in, "Back to the Future: Instability in Europe after the Cold War"[57] adlı çalışmasında, Soğuk Savaşın[58] son bulmasının ardından, etnik çatışmaların ve aşırı milliyetçiliğin sonucunda geniş alanda istikrarsızlığa ve çatışmalara neden olacağını belirtmiştir. Mearsheimer, geçmişte çok kutuplu güç dengesi sisteminde yapılagelen politikaların geleneksel yönden dönüşmesinin muhtemel olduğunu savunmuştur.[59] Bu nedenle Soğuk Savaş'ın egemen iki kutuplu güç sisteminin sebep olduğu zaman için barış ve istikrar dönemi denilmiştir. Bu sistemin çökmesiyle, bir ilişki türü olarak uluslararası ilişkilerde on yedinci yüzyıldan beri felaketlere yol açan büyük güç rekabetine dönüleceği varsayımında bulunmuştur.

Güvensizlik, savaş ve savaş tehdidi ile ilişkilidir; güvenlik barış ve istikrarla ilişkilidir. Güvenlik, insan yaşamı için gerekli bir öncü olduğundan, kendi başına temel bir iyiliktir hem kişisel hem de politik bir unsurdur.[60] Savaş trajedisini ilk elden yaşamış olan Hobbes ve diğer düşünürler, daha ayrıcalıklı koşullarda güvenliğin tüm insani değerlerin en temelini oluşturduğunu hatırlatmaktadır. Güvenlik, bireysel ve toplu yaşamlarımızı üzerine inşa ettiğimiz temeldir.

Güvenlik nasıl olmalıdır? Bu soruya yanıt bulmak için her ülkenin kendi güvenliğine bakmak gerekmektedir. Genel itibariyle bireyin güvenliğini sağlamakla yükümlü devlet, tehlikelerden uzak tutmak için bariyerler, siperler, surlar, polis kuvvetleri, silahlı kuvvetler vb. oluşturarak korumaktadır. Güvenliğin tersi savunmasızlık ve emniyetsizliktir. Tehlikeye maruz kalmak, tehlikede ve risk altında vb. olmaktır. Güvenlik herkesin yalnızca diğerlerinin özgürlüğüne saygı duymasını ve onları rahat bırakmasını gerektirmektedir. Güvenlik, kadınların ve erkeklerin birbirlerini tehdit etmediği veya zarar vermediği her yerde ve her zamanda sağlanması gerekmektedir. Eğer insanlar başka insanların

---

[57] John J. Mearsheimer (1990). "Back to the Future: Instability in Europe After the Cold War", *International Security*, Sayı 15, No 1, ss. 5-56.

[58] Soğuk Savaş'ın sona ermesiyle tetiklenen entelektüel ortamda güvenlik, en çok tartışılan konulardan biri haline gelmiştir. İyimserler yirminci yüzyılın sonunda, çeşitli şekillerde liberal demokrasiye, ulus ötesi kapitalizme, uluslararası örgütlere veya yeni bir barış ve iş birliği çağını başlattığını ilan etmişlerdir. Kötümser olanlar, etnik çatışmaların ve silahların yayılmasıyla anarşik bir geleceğe dair uyarılar vermiştir. Detaylı bilgi için bkz. Keith Krause ve Michael C. Williams (1997). *Critical Security Studies: Concepts and Cases*, "From Strategy to Security: Foundations of Critical Security Studies", Minnesota: University of Minnesota, s. 33-60; Waever, Buzan (vd.) (1993). *Identity, Migration…,* s. 171.

[59] John Mearsheimer (1990). "Back to the Future: Instability…", s. 5-7,37-39.

[60] Ole Waever (1996). "European Security Identities", *Journal of Common Market Studies*, Sayı 34, No 1, s. 103-105.

özgürlüğünü ihlal ederse, bu durumda hiç kimse kendi arzularından veya hırslarından vazgeçmeye hazır değildir. Aksi halde malları ele geçirecek olanları veya başka şekillerde değer verdiği şeylerden (yaşam, özgürlük, mülkiyet vb.) onları soyacak olanları uzak tutmak için kapılarını kilitlerler ve evlerine alarm sistemleri kurarlar. Güvensizlik, bazı insanlar kendilerini sınırlamadığında ve başkaları tarafından sınırlanamadığında ortaya çıkmaktadır. Güvenlik iki yolla sağlanabilir: ya muhtemel koruyucunun caydırıcılığı ya da olası saldırgan tarafındaki çekingenlik.[61]

Thomas Schelling gibi bazı teorisyenler, güvenlik politikasının temel bileşeni olarak caydırıcılığın güvenilirliğine öncelik vermiştir.[62] Caydırıcılık, güvenliğe ulaşmanın en önemli yollarından biridir. Caydırıcılık politikaları, devletler tarafından ulusal güvenlik stratejilerinin bir parçası olarak yaygın şekilde kullanılmaktadır. Ekonomik yaptırımlar, konvansiyonel silahlar ve kitle imha silahları veya bunların herhangi bir kombinasyonu caydırıcı olarak kullanılabilmektedir. Bu tür bir güvenlik yaklaşımı hem ABD hem de SSCB'nin bir tarafın nükleer saldırısının diğer tarafın derhal misilleme ve imhayla sonuçlanacağını bildiği "karşılıklı imha" gibi Soğuk Savaş politikalarında özetlenmiştir. Ancak caydırıcılık teorisinin de zayıf yönleri vardır. Caydırıcılık, saldırganların kendilerine zarar vermekten kaçınmaya istekli olduklarını varsaymaktadır. Ancak bu mantık her zaman geçerli olmayabilir. Bazı hükümetler (örneğin totaliter devletler) askeri personellerini ve sivil nüfuslarını güvende tutma konusunda diğerlerinden (örneğin liberal demokrasiler) daha az endişe duyabilmektedir. Benzer şekilde, tehdit algıları da caydırıcıyla ilgisi olmayan diğer etkilere göre değişebilmektedir (örneğin, diplomatik yanlış anlamalar ve/veya karşıt siyasi ideolojiler). Caydırıcılık politikaları rakip devletler arasında silahlanma yarışına yol açabilir ve bu da gerçek savaş riskini azaltmaktan ziyade artırabilmektedir. Bu şekilde, caydırıcılık politikaları Barry Buzan'ın "savunma ikilemi"[63] olarak adlandırdığı şeyi üretebilir, burada askeri güç ulusal güvenliği desteklemek yerine alt üst etmektedir.

"Her zaman krallar ve egemen otoriteye sahip kişiler, bağımsızlıkları nedeniyle, sürekli kıskançlık içindedir… silahlarını göstererek ve gözleri

[61] Robert Jackson (2005). *The Global Covenant Human Conduct in a World of States,* London: Oxford University, s. 192.

[62] Thomas Schelling (2006). *The strategy of conflict*, Cambridge, Massachusetts: Harvard University, s. 36-39.

[63] Detaylı bilgi için bkz. Barry Buzan (2007). *People, States and Fear: National Security Problem in International Relations,* Bölüm 7: Defence Dilemma, 2. Baskı, UK: ECPR, ss. 217-233.

birbirine sabitlenmiş olarak; krallıklarının sınırlarında kaleleri, garnizonları, silahları ve komşuları üzerinde sürekli casusluk yapması bir savaş duruşudur."

Paradoksal olarak, "Leviathan" devlet içindeki kişisel güvenlik sorununu çözdüğü anda, devletlerarasında yeni bir güvensizlik sorunu ortaya çıkarmaktadır. Devletlerarasındaki bu güvenlik ikilemi, bugüne kadar ve günümüz dâhil uluslararası ilişkilerin belirleyici bir özelliği olmuştur. Bu, Hedley Bull'un "anarşik bir toplum" olarak tanımladığı çok sayıda bağımsız egemen devletin varlığının sonucudur.[64] Bununla birlikte, devletin güvenliği ile kişinin güvenliği arasında önemli bir ayrım vardır. Kişisel güvenlik, insanlığın gelişmesi için temel bir ön koşuldur. Başkalarına kasten zarar vererek zarar ilkesini ihlal etmemeleri koşuluyla, insanları başkalarından zarar görme korkusu olmadan kendi çıkarlarını, hedeflerini, hırslarını vb. takip etme özgürlüğü sağlamaktadır. Kişisel güvenlik, başkalarının zarar görmesine karşı kişisel korumadır. Elbette başkalarının tüm olası zararlarını ortadan kaldırmak imkânsızdır. Hırsız alarm sistemi düşünüldüğünde; en karmaşık hırsız alarmı bile, güvenliği ihlal etmeye kararlı olanlar tarafından aşılabilmektedir. Ancak bir hırsızlık alarmı kurulursa, birçok hırsız caydırılacak, diğerleri engellenecektir. Alarmı geçmeyi başaranlar, yerel polis gücü tarafından takip edilecek ve belki de yakalanacak, suçlanacak ve mahkûm edilecektir. Bu nedenle, hırsız alarmının kusursuz olmadığı bilinmesine rağmen, bireyler onun sağladığı güvenlik ile evinde daha rahat olmaktadır.

Thomas Hobbes gibi diğer teorisyenler, aksi bir durumda tehdit oluşturacak olan insanları engelleyen zihinsel bir durum olan çekingenliğe öncelik vermişlerdir.[65] Caydırıcılık ve çekingenlik birbiriyle alakasız değildir. Çekingenlik, caydırıcılığın istenen sonucudur. Bu nedenle, güvenliği sağlamak bir saldırıyı önlemek amacıyla, olası bir saldırganın zihninde korku uyandırmakla ilgilidir.

Denize açılıp gemiden sağ olarak tek başına çıkan Robinson Crusoe[66] gibi izole bireyler, diğer insanlardan gelen saldırılara karşı tamamen güvendedirler. Çünkü etrafta onlara saldıracak insan yoktur. Ancak çok az birey tek başına, hiçbir etkileşim, iletişim ve iş birliği olmayan bir adada yalnız yaşamayı (tek bir gemi enkazından kurtulan kişinin hayatı gibi) çekici bulabilmektedir. Bu, insan nezaketinden, şefkatinden, arkadaşlığından, sevgisinden veya ailesinden yoksun bir hayattır. Güvenlik, insan ilişkilerinin temel bir değeridir. Güvenliğin

[64] Hedley Bull (2012). *The Anarchical Society A Study of Order in World Politics*, (ed. Andrew Hurrell), 4th Edition, London: Red Globe.
[65] Hobbes (2016). *Leviathan…,* s. 83.
[66] Daniel Defoe (2019). *Robinson Crusoe*, Akşit Göktürk (Çev.), Ankara: Yapı Kredi Yayınları.

gerekliliği, insanların birlikte yaşamak istemesinden ve dolayısıyla birbirlerine karşı savunmasız olmalarından kaynaklanmaktadır. Güvenlik, aksi bir durumda muhtemelen başarılamayacak olanı; saldırganlara karşı nispeten güvenli, gelişen bir toplumu mümkün kılmaktadır. Toplum içinde kişi hiçbir zaman tamamen güvende olamaz. Bu yüzden güvenlik politikalarına ihtiyaç duyulmaktadır. Bu tür politikalar genellikle, kamu yararı için bu temel görevi yerine getirmek üzere hazırlanmış; donanımlı polis ve askeri güçlerin oluşturulmasını ve sürdürülmesini içermektedir.

Bir disiplin türü olarak Uluslararası İlişkilerde güvenliğe yönelik yaklaşımlardan biri normatiftir. Normatif bir güvenlik görüşü, değerlere, fikirlere ve kimliklere dayandırılan görüştür. Bu yaklaşımın açık sonucu, güvenliğin temelde normatif olarak görülmesi gerektiğidir. Çünkü onsuz insan hayatı, hayatta kalmak için temel bir mücadeleye indirgenmektedir. Bu normatif görüş Buzan, Bain ve daha az ölçüde Hough'un temel metinlerinde de belirgindir.[67] Güvenliğe normatif şekilde yaklaşıldığında, örneğin devletin güvenliği ile kişinin güvenliği üzerine yapılan analizin rakip değerleri arasında seçim yapmak zor olmaktadır. Bu seçimler yalnızca güvenlik politikasının amaçları veya hedefleri ile değil, aynı zamanda bunları takip etmek için kullanılan araçlarla da ilgili olması gerekmektedir. Bu nedenle, güvenlik politikasının kendisi, çözümlerinin kolay olamayacağı bir dizi ahlaki ikilem olarak görülmektedir.[68]

1.2.2. Siber Güvenlik ve Temel Varsayımları

Uluslararası siber politika bağlamında, uluslararası ilişkilerin realist teorileri en çok siber güvenlik ve siber savaşla ilgili konulara uygulanabilmektedir. Realist teoriler, devletlerin güvenlik konusundaki çıkarlarını geliştirmek için siber teknolojileri nasıl kullandıklarını ve diğer devletlerin siber yeteneklerine nasıl tepki verebileceklerini açıklamaya yardımcı olabilmektedir.

Realizm; caydırıcılık, kriz yönetimi ve çatışma teorileri, siber alanın istikrar mı yoksa istikrarsızlaştırıcı mı olduğunu, siber teknolojilerin yeni

[67] Detaylı bilgi için bkz. Barry Buzan (2007). *People, States and Fear*..., s. 15-32; William Bain (2012). *The Empire of Security and the Safety of the People,* London: Routledge; Peter Hough (2018). *Understanding Global Security,* 4th Edition, London: Routledge; Jef Huysmans (1998). "Security! What Do You Mean?: From Concept to Thick Signifier", *European Journal of International Relations,* Sayı 4, No 2, ss. 226-255; Stephen M. Walt (1991). "The Renaissance of Security Studies", *International Studies Quarterly*, Sayı 35, No 2, ss. 211-239.

[68] J. Jackson Preece (2011). *Security in International Relations*, London: University of London, s. 17.

bir çatışma veya barış kaynağı olup olmayacağını ve devletlerin siber silah yarışına girip girmeyeceğini anlamak için kullanılabilmektedir. Realizm, siber alanın gelişmesinin ve büyümesinin devletleri baltaladığını ve yeni uluslararası aktörleri güçlendirdiğini iddia eden teorisyenlere de meydan okuyabilir.[69] Buna karşılık, liberal uluslararası ilişkiler teorileri, siber alana erişimin siyasi fikirlerin gelişmesini ve yayılmasını, sivil toplumun örgütlenmesini ve ulus ötesi sosyal ağların gelişimini nasıl teşvik edebileceğini açıklamaya yardımcı olabilmektedir.

Liberalizm, siber alana erişimin ve kontrolün devlet davranışını şekillendirebileceğini ve uluslararası siyaseti etkileyebileceğini öne sürmektedir. Liberal kurumsal teoriler, siber güvenlik, siber alan yönetimi ve siber silahların kontrolü ile ilgili konularda devletlerarasında iş birliğini teşvik etmeye yönelik uluslararası çabalara ilişkin anlayışa uygulanabilmektedir. Liberalizm, sivil toplum kuruluşları, etnik ve ulusal gruplar, siber suçlular ve siber terörizm gibi uluslararası devlet dışı aktörlerin davranışlarını açıklamaya da yardımcı olabilmektedir.[70]

Konstruktivistler, yirmi yıl boyunca siber güvenlik politikaları üzerine akademik çalışmalara hâkim olmuşlardır. Akademik dergilerde yer alan makalelerin yarısı konstrüktivizm üzerinedir. Comor, Deibert, Herrera, Der Derian, Murphy, Hansen and Nissenbaum vb. siber güvenliği incelemiş ve yaklaşım olarak konstrüktivizme yönelmişlerdir.[71] Bazı yazarlar, bir "Küresel Sivil Toplum" için olasılıkların, çevrimiçi olarak kurulan sosyal ilişkilerin "gerçek" dünyada oluşturulan kişilerarası bağlar ve kimliklerden çok daha zayıf ve geçici olmasını vurgulamaktadırlar. Bundan ötürü her zaman küresel sivil toplumun sınırlı olacağını savunmaktadırlar.

---

[69] Nazlı Choucri (2012). *Cyberpolitics in International Relations,* London: The MIT, s. 25-28.

[70] Reardon ve Choucri (2012). "The Role of Cyberspace in International Relations…", s. 7.

[71] Detaylı bilgi için bkz. Edward Comor (2001). "The Role of Communication in Global Civil Society: Forces, Processes, Prospects," *International Studies Quarterly*, ss. 389-408; Ronald J. Deibert (2003). "Black Code: Censorship, Surveillance, and the Militarization of Cyberspace", *Millennium*, ss. 501-530; James Der Derian (1990). "The (S)pace of International Relations: Simulation, Surveillance and Speed", *International Studies Quarterly*, ss. 295-310; Lene Hansen ve Helen Nissenbaum (2009). "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly*, Sayı. 53, No. 4, ss. 1155-1575; Geoffrey L. Herrera (2003). "Technology and International Systems", *Millennium*, ss. 559-593; Emma C. Murphy (2009). "Theorizing ICTs in the Arab World: Informational Capitalism and the Public Sphere," *International Studies Quarterly*, Sayı 53, No 4, ss. 1131-1153.

Murphy, çevrimiçi etkileşimleri sığ olarak nitelendirmekte ve vatandaşların genellikle siyasi tartışma ve ifadeden çok, sanal ortamda eğlenceye ilgi duyduğunu söylemektedir. Murphy, siber alanın dünyasında Habermasçı bir "kamusal alan" yaratılmasını kolaylaştırdığını, rasyonel tartışma ve ifade için devlet otoritesinin önemli bir eleştirisi olarak hizmet edebilecek, bölgede daha önce hiç var olmayan bir çevrimiçi sivil politik forum oluşturduğunu savunmaktadır.[72]

Comor, çevrimiçi ilişkilerin geçiciliği ve gerçek topluluk bağlarına olan farklılıkları hakkında güçlü bir argüman sunmaktadır. Comor'a göre kimlikler, internet üzerinden kurulan "görece aracılık eden" ilişkilere çok dirençli olabilmektedir. Comor, siber alanın yerel kültür, bölgesel kimlikleri aşma ve bunları küresel olanlarla değiştirme yeteneği konusunda şüpheci yaklaşmıştır.[73] Yine de bu teorisyenler literatürde önceki varsayımlar üzerine önemli mantıksal noktaları ortaya koyarken, bu iddiaları çürütmüşlerdir. Ayrıca, ulus ötesi sosyal bağların hâlihazırda var olduğu durumları ve bu bağların siber alandan nasıl etkilenebileceğini tam olarak belirlememişlerdir.[74]

Konstruktivistler, çeşitli faaliyetlerin ulusal güvenliğe yönelik tehditler olarak etiketlenmesinin maddi olarak belirlenmekten çok özneler arası yorumlamanın bir ürünü olduğunu savunmaktadırlar. Ayrıca, konstruktivistler siber güvenlik sorunuyla ilgilenme konusundaki daha büyük istekleri, realistlerin siber alan üzerinde çalışma konusundaki isteksizliğini yansıtıyor olabilirler.[75]

Realistler, uluslararası ilişkilerde itici güç olarak iktidarın devletlerarasında dağılımına odaklanmaktadır. Realistler dünya siyasetini, anarşi koşulları altında devletlerarasında güvenliklerini en üst düzeye çıkarmak ve hayatta kalmalarını garanti altına almak için bir mücadele olarak sınıflandırırlar. Realizm, iç politikanın, devlet dışı aktörlerin ve devletin dışındaki diğer güçlerin uluslararası davranışın belirlenmesinde önemli bir rol oynamasına izin ver(ebil)mektedirler. Fakat bu güçler devletlerin önceliğine ve uluslararası politikada devlet çıkarlarına meydan okuyamamaktadır.[76] Her devlet kendisini korumak için

[72] Emma C. Murphy (2009). "Theorizing ICTs in the Arab World: Informational Capitalism…", s. 1131-1138.
[73] Edward Comor (2001). "The Role of Communication in Global Civil Society: Forces…", s. 389-392.
[74] Reardon ve Choucri (2012). "The Role of Cyberspace in International Relations…", s. 9.
[75] Reardon ve Choucri (2012). "The Role of Cyberspace in International Relations…", s. 6.
[76] Reardon ve Choucri (2012). "The Role of Cyberspace in International Relations…", s. 5.

daha yüksek bir otoriteye güvenemeyeceğinden son tahlilde, kendilerini diğer devletlerin avlarından korumaya çalışmaktadırlar. Bunu da kendi çabalarına bağlı bir şekilde yapmaktadırlar.

Liberal uluslararası ilişkiler teorisi, devlet tercihlerini şekillendirmede ve dolayısıyla devlet davranışını etkilemede "sosyal fikirlerin, çıkarların ve kurumların" oynadığı role odaklanmaktadır. Liberalizm, hem yerel siyasal kurumlar ve kültür gibi yerel toplumu hem de uluslararası devlet dışı aktörlerin ve sosyal süreçlerin işleyişini ele almaktadır. Liberalistler, devlet tercihlerini ve davranışlarını hem yerel hem de uluslararası sivil toplum tarafından sınırlandırılmış ve etkilenmiş bir şekilde görmektedirler.

Konstruktivistler, maddi köklü çıkarlar ve güç ilişkilerinden ziyade uluslararası ilişkilerin sosyal olarak yapılandırılmış doğasına odaklanarak gerçekçilik, liberalizm ve kurumsallıktan ayrılmaktadırlar. Konstruktivistler, uluslararası siyasetin yapı uygulamalarının çoğunun maddi güçlerden ziyade sosyal olarak inşa edilmiş kimliklere, dünya görüşlerine ve fikirlere dayandığını iddia etmektedirler. Bu nedenle, bu etkileşim yapıları ve kalıpları, aktörler için dünyanın doğası hakkındaki fikir ve varsayımlarındaki değişikliklere göre şekillenmektedir. Sonuç olarak, "iletişimsel eylem" yoluyla fikir alışverişi, temeldeki maddi koşullardaki herhangi bir değişiklikten bağımsız olarak uluslararası ilişkiler üzerinde önemli bir etkiye sahip olabilmektedir.[77]

Murphy, Comor ve Deibert, siber alanı küresel kapitalizm ve ticarileşme için potansiyel bir araç olarak görmüş ve bunları değişen derecelerde sivil toplum için bir tehdit olarak tanımlamışlardır. Murphy, bazı bölgelerde kamusal alanın, uluslararası kapitalizmin hâkim olduğu daha geniş bir küresel alana yerleştirilmiş olduğunu varsaymıştır. Murphy, "erdemli olmayan" kimlik temelli ulus ötesi grupların kamusal alan üzerindeki etkisini değerlendirmiştir. Bu gruplar, daha "erdemli" sivil toplum gruplarının yapabildiği siber teknolojiyle güçlenebildiğini düşünmüştür.[78]

Teoriye değerli bir katkıyı özellikle, Deibert'in siber alanın teknik ve maddi unsurlarına ve bu siyasi yarışmalarla ilişkisine odaklanması oluşturmuştur. Deibert, güçlü ticari aktörleri internetin açık mimarisini bozmakla tehdit eden uluslararası bir güç olarak görmüştür. Deibert'in, siber alan mimarisinin açıklığını tehdit eden şekillerde tartışıldığı iddiası örneğin, vaka analizi için çok

[77] Nazlı Choucri (2012). *Cyberpolitics in International Relations,* London: The MIT, s. 155-158; Reardon ve Choucri (2012). "The Role of Cyberspace in International Relations…", s. 5.

[78] E. C. Murphy (2009). "Theorizing ICTs in the Arab World: Informational Capitalism…", s. 1135-1139.

uygundur.[79] Teknoloji daha geniş bir aktörler yelpazesine ve değer verdikleri şeylere yayıldıkça ve etkilendikçe, bu aktörler siber alanın mimarisine itiraz edecek ve özel ilgi alanlarını geliştirmek için onu teknik düzeyde yeniden tasarlamaya çalışacaklardır.

1.2.3. Siber Güvenlik'te İnternet Sisteminin İşleyişi

Siber güvenlikte internet sisteminin işleyişi şu şekilde çalışmaktadır:[80] "Herhangi bir düşünce kuruluşunun Brookings Enstitüsü'nün bilgilendirici ve eğlenceli web sitesini ziyaret etmek istediğinizi varsayalım. Esasen, cihazınızdan Brookings tarafından Washington'daki kontrol edilen bir bilgisayarla konuşmasını istediniz. Makineniz, o bilgisayarın nerede olduğunu öğrenmeli ve iletişimi sağlamak için bir bağlantı kurmalıdır. Bilgisayarınızın bilmesi gereken ilk şey, Brookings web sayfasını barındıran sunucuları nasıl bulacağınızdır. Bunu yapmak için, internetteki uç noktalar adres olarak hizmet veren "İnternet Protokolü (IP)" numarasını kullanmaktır. Büyük olasılıkla internet servis sağlayıcınız veya herhangi bir ağ ile otomatik olarak bir IP adresi atanmıştır. Yönlendiricisinin adresini veya daha geniş İnternet yolunu da bu IP ile bilmektedir. Dahası, bilgisayarınız bir "Alan Adı Sistemi (DNS)" sunucusunun adresini bilmektedir.

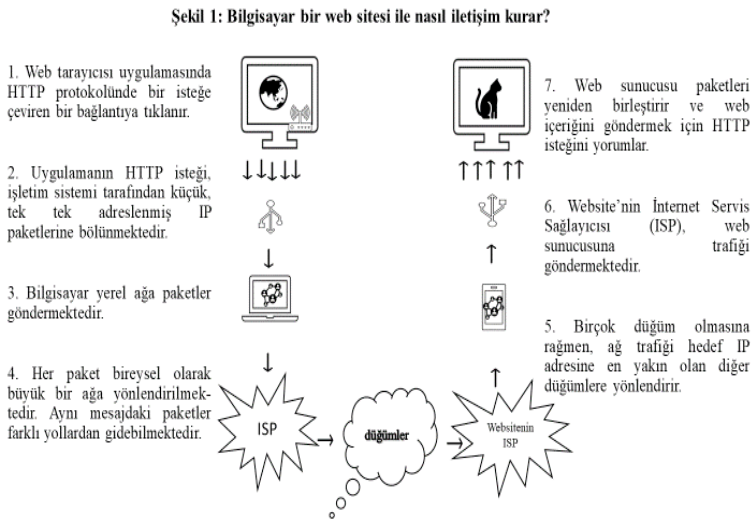
DNS, bilgisayarların alan adlarını (Brookings.edu gibi) karşılık gelen IP adreslerine (192.245.194.172 gibi makine verileri) bağladıkları protokol ve altyapıdır. DNS küreseldir ve merkezi değildir. Mimarisi bir ağaç olarak düşünülebilir. Ağacın "kökü", DNS için yönlendirme noktası görevi görmektedir. Bunun üzerinde üst düzey alanlar vardır. Bunlar, ".uk", ".gov" gibi ülke kodları ve ".com" ve ".net" gibi diğer alan adlarıdır. Bu üst düzey alanların her biri daha sonra alt bölümlere ayrılmaktadır.

Pek çok ülke, sırasıyla iş yeri ve akademik kurumları belirtmek için "gov. tr, edu.tr, co.uk ve ac.uk" gibi belirli ikinci düzey alanlara sahiptir. Brookings etki alanına ulaşmak için, bilgisayarınız DNS sistemini bir dizi çözümleyici aracılığıyla sorgulayacaktır. Temel fikir, ağacın seviyelerine çıkmaktır. Kökten başlayarak, Educause tarafından yönetilen ".edu" kaydına işaret edilecektir. Educause, ". edu"da kayıtlı her alan adının listesini tutan iki binden fazla eğitim kurumunun kuruluşudur. Bu listeden, bilgisayarınız daha sonra Brookings'in

[79] Ronald J. Deibert (2003). "Black Code: Censorship, Surveillance, and the Militarization of Cyberspace", *Millennium*, s. 502, 507, 513.
[80] P.W Singer ve A. Friedman (2013). *Cybersecurity and Cyberwar: What Everyone…,* s. 21-24.

dâhili ad sunucusunun belirli IP adresini öğrenecektir. Bu, Brookings etki alanının içinden içerik veya uygulamalarla ilgili belirli sorguları ele almasına izin verecektir. Daha sonra Brookings isim sunucusu, onu barındıran makinenin IP adresini geri döndürerek bilgisayarınızı aradığı belirli içeriğe yönlendirecektir.'' Gerçekte bu süreç biraz daha karmaşıktır. Örneğin, sunucular genellikle verileri gelecekte kullanılmak üzere önbelleklerde depolar. Böylece her sorgunun köke gitmesi gerekmez ve protokol, tahmin edilebilir şekilde belirli hata koşullarını içermektedir. Bununla birlikte, her şeyin nasıl çalıştığına dair bir fikir vermektedir. Artık bilgisayarınızda verilerin konumu vardır. Peki, bu veriler bilgisayara nasıl ulaşacaktır?

Şekil 1: Bilgisayar Bir Web Sitesi ile Nasıl İletişim Kurar?



Brookings'teki sunucunun, makineye veri göndermesi gerektiğini ve verilerin oraya ulaşması gerektiğini bilmesi gerekmektedir. Şekil 1, bilgisayarın istediği paketlere bölerek ve internet üzerinden göndererek bir web sayfasını nasıl talep ettiğini göstermektedir. Öncelikle, uygulamanın "katmanında", tarayıcının birey tarafından fare ile tıklanması; içeriğin nasıl isteneceğini ve teslim edileceğini tanımlayan Köprü Metni Aktarım Protokolündeki (HTTP) bir komut olarak yorumlanmaktadır. Bu komut daha sonra taşıma ve ağ katmanlarına aktarılmaktadır. Aktarım, verileri paket büyüklüğünde parçalara ayırmaktan, tüm parçaların hatasız bir şekilde ulaştığından ve yukarıdaki uygulama katmanı için doğru sırada yeniden birleştirildiğinden sorumludur.

Ağ katmanı, internette paketler arasında gezinmek için en iyisini yapmaya çalışır. Gönderilmeye ve alınmaya çalışılan veriler birer bilgi paketi olarak düşünülürse; bunların paketlenmesinden ve alınmasından taşıma katmanı sorumluyken, ağ da bunları kaynaktan hedefe taşımaktan sorumlu olmaktadır. Hedefe ulaştığında, paketler yeniden birleştirilir, kontrol edilir ve ardından uygulamaya geri gönderilir. Ancak paketler, internet üzerinden hedeflerine ulaşacaklarını nasıl bilmektedir? Bilgisayarın aradığı web sitesini bulmasına yardımcı olan DNS gibi, internet ağlarının organizasyonu da bir hiyerarşi olarak düşünülebilmektedir.

Her bilgisayar, bir internet servis sağlayıcısının (ISS) tüm müşterilerini birbirine bağlayan bir ağın parçasıdır. İnternet servis sağlayıcıları, esasen internete, e-posta veya web siteleri gibi diğer ilgili hizmetlere erişim sağlayan kuruluşlardır. İnternet servis sağlayıcıların birçoğu özel, kâr amacı gütmeyen şirketlerdir. Ama internet erişimi sunmaya başlayan geleneksel telefon ve kablo TV firmaları ise devlete veya topluluğa aittir. Bu ağlar, sırayla, küresel internette Otonom Sistemler (AS) adı verilen düğümler oluşturmaktadır.

Otonom Sistemler, internet bağlantılarının mimarisini tanımlamaktadır. Trafik, yerel olarak Otonom Sistemler üzerinden yönlendirilmekte ve bu kuruluşun politikaları tarafından kontrol edilmektedir. Her Otonom Sistemin bir dizi bitişik IP adresi bloğu vardır. Bugün internette 40 binden fazla Otonom Sistem düğümü vardır ve ara bağlantıları zaman içinde değişmektedir. Bu ölçek göz önüne alındığında, her şeyi aynı şekilde yönlendirmek için küresel bir yaklaşım imkânsız hale gelmektedir.[81]

Tüm bu siber çalışmaların arkasındaki şaşırtıcı rakamlar, tehditlerin ölçeğini ve kapsamını göstermektedir: "Fortune 500"[82] dergisinde her yıl yayımlanan beş yüz şirketin neredeyse yüzde 97'si saldırıya uğramıştır (muhtemelen yüzde 3'ünün de hacklenmiş olduğu bilinmemektedir) ve yüzden daha fazla hükümet çevrimiçi alanda siber güvenlikte kendini ve vatandaşlarını korumak için politikalar hazırlamaktadır. Alternatif olarak sorunlar, siber alanın ürettiği zorlu siyasi konular aracılığıyla kavramsallaştırılabilir: WikiLeaks ve NSA'da izleme gibi skandallar, Stuxnet gibi yeni siber silahlar ve Arap Baharı

[81] P.W Singer ve A. Friedman (2013). *Cybersecurity and Cyberwar: What Everyone…,* s. 24.

[82] Detaylı bilgi için bkz. "The Darknet Index: Fortune 500 Reranking the Fortune 500 Using Darknet Intelligence" (2017). [https://owlcyberdefense.com/], ss. 1-22; Allan Levine (2018). *Shielding Fortune 500 Companies from Cyberattacks*, [https://internationalfinance.com/shielding-fortune-500-companies-from-cyberattacks/] (er. tar. 27.01.2022).

devrimlerinden kişisel mahremiyet konusundaki endişelere kadar her şeyde sosyal ağların oynadığı rol giderek artmaktadır.

Birçok ülkenin liderleri tarafından yinelenen "siber güvenlik risklerinin yirmi birinci yüzyılın en ciddi ekonomik ve ulusal güvenlik zorluklarından bazılarını ortaya çıkardığını" belirtmek gerekmektedir. Bilgi çağının tüm umut ve vaatlerine rağmen, yirmi birinci yüzyıl aynı zamanda bir "siber endişe" çağı olmaktadır. Dış Politika[83] dergisi, dünyanın gelecekte nereye gittiğine dair bir ankette siber alanı "ortaya çıkan en büyük tehdit" olarak tanımlarken, Boston Globe[84] geleceğin zaten burada olduğunu iddia etmiştir: "kanlı, dijital siper savaşı" ile sonuçları devam edecek olan bir "siber dünya savaşı". Bu korkular, dünyanın en hızlı büyüyen endüstrilerinden biri olan siber güvenliğin ortaya çıkmasıyla belirgin bir hale gelmiştir. Çeşitli yeni devlet daireleri ve bürokrasilerinin kurulmasına yol açmıştır (ABD İç Güvenlik Bakanlığı'nın Ulusal Siber Güvenlik Bölümü, başlangıcından bu yana her yıl iki veya üç katına çıkarak büyümektedir).[85] Aynı şey ABD Siber Komutanlığı (USCYBERCOM) ve görevi siber alanda savaşlar yapmak ve savaşları kazanmak olan yeni askeri birimler olan Çin "Bilgi Güvenliği Üssü" gibi dünyanın dört bir yanındaki silahlı kuvvetler için de geçerlidir. Daha sonra ele alınacağı üzere, siber alanın bu yönleri gerçek riskler ortaya çıkarmaktadır. Ancak bu riskleri hükümetlerin nasıl algıladıkları ve bunlara nasıl yanıt verdikleri, yalnızca Bilgi ve İletişim Teknolojisi için değil, gelecek için daha da önemli olabilmektedir.

Siber güvenlik, hızlı teknolojik gelişme ile devlet ve devlet dışı unsurlar tarafından siyasi ve stratejik yapısı arasında ilerlemektedir. Devletlerin, toplumların ve özel sektörlerin bu alan için sorumlulukları, yasal sınırları ve kabul edilebilir davranış kurallarını tanımlamaya yönelik çeşitli girişimleri vardır. Devletler siber alanı stratejik hedeflerine göre şekillendirmekte ve bunu tarihsel gelişim ışığında uluslararası güvenlik açısından incelemektedir.[86]

---

[83] Paul M. Nakasone ve Michael Sulmeyer. "How to Compete in Cyberspace", *Foreign Affairs*, (Publication Date 25.08.2020), [https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity] (er. tar. 22.11.2020).

[84] Boston Globe, "Cyber War has Already Begun" (13.03.2017), [https://www.bostonglobe.com/opinion/2017/03/13/cyber-war-has-already-begun/dYE1vkpT1W3zKdhjxwH1QP/story.html] (er. tar. 22.11.2020).

[85] P.W Singer ve A. Friedman (2013). *Cybersecurity and Cyberwar: What Everyone…, s.* 3.

[86] Myriam Dunn Cavelty ve Andreas Wenger (2022). *Cyber Security Politics Socio-Technological Transformations and Political Fragmentation,* NewYork ve London: Routledge, s. 4.

Gelecek bölüm tarihsel çerçevede siber güvenlik, siber güvenlik politikaları, hükümetlerin bu konuda aldığı önlemler, küresel salgın döneminde yaşanan sebep ve sonuçların siber alanda yansımasını incelemektedir. Ayrıca farklı ülkelerden siber güvenlik politikaları ve hükümetlerin bu konuda yaptığı çalışmalara yer verilecektir.

İKİNCİ BÖLÜM

TARİHSEL GELİŞİM

Hızla büyüyen ve en büyük teknoloji sektörlerinden birisi Siber Güvenlik'tir. Siber güvenlik, bir yandan günlük yaşamı kolaylaştırmakta ve yaşam standartlarını yükseltmektedir. Diğer yandan kişisel, ulusal ve küresel güvenliğe dair yeni güvenlik açıkları ve tehditleri beraberinde getirmektedir. Siber alana erişim yaygınlaştıkça, güvenlik unsurlarının öneminin artması şaşırtıcı değildir. Bu bölümde amaç, siber güvenlik ve siber güvenlik politikaları tartışmalarını tarihsel açıdan bilgilendirmek ve gerek ulusal gerekse uluslararası düzeyde daha tutarlı, kapsamlı ve ileriye dönük bir politika müdahalesi için gerekçe oluşturmaktır. Bu bölüm, siber güvenlik politikasındaki benzerlik ve ayrılıkları görmek için bazı ülkelerdeki siber güvenlik politikalarını genel çerçevede sunmaktadır. Bu karşılaştırmanın ilk kısmı kısa tarihsel bir genel bakış sağlamaktır. Daha sonra, verilen bilgiler ışığında ülkelerin siber alan ve siber güvenlik hakkında ne ifade ettiklerini görmek için benzerlikler ve farklılıklar değerlendirilmektedir. Son olarak çalışma, her iki yargı alanındaki politikalardan alınan tavsiyeleri ve dersleri ortaya koyacaktır.

2.1. Siber Güvenliğin Tarihsel Gelişimi

Bilginin paylaşıldığı ve iletildiği teknolojik yeniliklerle birlikte gelişen telgrafın icadından yirmi birinci yüzyıla değin, elektronik iletişim ağlarında büyük ilerlemeler kaydedilmiştir. Elektronik iletişim ağlarının tarihsel süreci, bazılarının geriye dönüp "Victorian İnternet"[87] adını verdiği bir cihazla ön plana

[87] Tom Standage, on dokuzuncu yüzyıl dünyasının Viktorya dönemi interneti ile ilgili uçaklar ve televizyonlar gibi şeylerden bahsetmiştir. Teknolojik ilerlemelerden ve bunun toplum üzerindeki etkilerinden bahsetmiştir. Telgraf ve internetin tarihi ile ilgili olan tartışma, 1746 yılında Abbe Nollet'in ünlü deneyinden (elektrik hikâyesiyle başlayan ve bir mil uzunluğundaki keşişlerin zincirin bir ucundan diğer ucuna elektriğin geçebileceğini başarıyla gösterdiği deney) başlayarak, telgrafın yayılması ve "Viktoryan İnternet" dünyasına dönüşümüyle gerçekleşmiştir. Ayrıca Standage; mucitler, politikacılar, savaş stratejilerini belirleyenler ve hükümetler açısından uzak mesafelerde verimli bir iletişim aracına hızlı bir şekilde ulaşılabildikleri takdirde kazanacak bir şeylerinin olduğunu ileri sürmüştür. Detaylı bilgi almak için bkz. Tom Standage (2014). *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-line Pioneers*, 2nd Edition, USA: Bloomsbury.

çıkmaktadır. Bu eski teknolojinin etkileri, zamanın meraklılarını ve ilgililerini cezbetmiştir. İnterneti eski telgraflar ve daha sonra telefon ağları gibi önceki iletişim ağlarından ayıran şey, uygulamada devre anahtarlama yerine paket anahtarlama olmasıdır. Paketler, küçük dijital veri zarflarıdır. Her paketin başlangıcındaki (esasen zarfın dışında) ağ kaynağı, paket içeriğinde bazı temel bilgiler hakkında ayrıntılar içeren bir başlık olmaktadır. Veri akışlarını daha küçük bileşenlere bölerek, her biri bağımsız ve merkezi olmayan bir şekilde teslim edilebilmekte ve ardından uç noktada yeniden birleştirilebilmektedir. Ağ, her paket geldiği anda yönlendirmekte, dinamik açıdan hem esneklik hem de dayanıklılık oluşturmaktadır. Paket anahtarlama bilgisayarlar arasında daha güvenilir, daha verimli bağlantılar sağlamak için geliştirilmiştir.[88] 1970'lerde bu teknoloji, iki bilgisayar arasındaki iletişim özel bir devre veya önceden yapılmış bant genişliği gerektirmiştir. Doğrudan bağlantı, hiçbir veri aktarılmadığında bu kaynakların başkaları tarafından kullanılamayacağı anlamına gelmiştir. Bu konuşmaları daha küçük parçalara bölerek, birden çok farklı konuşmadan gelen paketlerle aynı ağ bağlantıları paylaşılmıştır. Bu, iki makine arasındaki ağ bağlantılarından birinin iletişimin ortasında kesilmesi durumunda, herhangi bir bağlantı kaybı olmaksızın bir iletimin otomatik olarak yeniden yönlendirilebileceği anlamına gelmiştir (fakat hiçbir zaman başlayacak bir bağlantı olmamıştır).[89]

Dijital anlamda ilk bilgisayar 1943 yılında çok gürültülü ve çok büyük boyutta inşa edilmiştir. 1940-1950 yıllarında dünyada sadece birkaç bilgisayar üretilmiştir ve birçok insan bilgisayarın varlığından haberdar olmamıştır. 1950'lerde telefon dolandırıcılığı akımı başlamıştır.[90] 1960'larda bilgisayarlar devasa ana bilgisayarlar olarak üretilmeye devam etmiştir. 1969'da, Kaliforniya Üniversitesi'ndeki (UCLA) araştırmacılar Stanford Araştırma Enstitüsü'nde bir bilgisayara giriş yapmaya çalışmışlardır. Bireysel makinelerin her biri, gerçek ağ bağlantısını idare eden bir "Arayüz Ağ İşlemcisi" ile bağlanacağına inanılmıştır. Ancak "log" kelimesine "g" harfini yazamadan, ağın Stanford tarafındaki bilgisayar çökmüştür. Bu, bilgisayar ağı üzerinden internete dönüşecek ilk gerçek kelime olmuştur. "Lo and behold" gibi derin bir açıklamanın başlangıcı yerine, "lo" bir sistem başarısızlığının ürünü olmuştur. Ancak, İleri Araştırma

[88] P.W Singer ve A. Friedman (2013). *Cybersecurity and Cyberwar: What Everyone…, s.* 17.

[89] Barry M. Leiner (vd.) (2009). "A Brief History of the Internet", Sayı 39, No 5, s. 21-23, [http://www.isoc.org/internet/history/brief.shtml] (er. tar. 14.10.2020).

[90] Michael Warner (2012)." Cybersecurity: A Pre-History". *Intelligence and National Security*, Sayı 27, No 5, s. 782.

Projeleri Ajansı (ARPA) [91] tarafından finanse edildiği şekliyle adlandırılan ARPANET projesi, sonunda bilgisayarların verileri ve bununla birlikte diğer her şeyi paylaşma şeklini değiştirmiştir.[92] Bu ağ, ilk "Lo" nun evi ve modern siber çağın başlangıcı olan "ARPANET" olarak ortaya çıkmıştır.

ARPA, Pentagon'da geliştirilen bir organizasyondur. Bilgisayarlar 1960'ların sonlarında üretimi artmış ve mevcut olandan daha fazla sayıda araştırmacı onları kullanmak istemiştir. ARPA için bu, ülke çapında farklı kurumlardaki kişilerin, kullanılmayan bilgisayar zamanından yararlanmalarına olanak tanımanın yollarını bulmak anlamına gelmiştir. Üniversiteler arasında özel ve pahalı bağlantılara sahip olmaktansa, hesaplama ve veri bağlantıları ağı olmuştur. 1971 yılında ilk "elektronik posta" gönderilmiştir. Florida Üniversitesi'nden Stanford'a olan ilk 1969 bağlantısı, 1972'de kırk düğümü birbirine bağlayacak şekilde büyümüştür. Kısa süre sonra dünyanın her yerinden daha fazla üniversite ve araştırma merkezi bu ilk ağa katılmış veya alternatif olarak kendi ağlarını oluşturmuştur.

Modern internetin amaçları doğrultusunda, tek bir ağdaki makineler arasında gönderilen bir dizi paket "internet" olarak sayılmamaktadır. İnternet, birçok farklı ağın, bu durumda ARPANET'in ötesinde kısa süre sonra ortaya çıkan ancak bağlantısız kalan diğer çeşitli bilgisayar ağlarının bağlanması anlamına gelmiştir. Burada öne çıkan zorluk, farklı ağların çok farklı temel teknolojiler kullanması olmuştur. Teknik sorun, bu farklılıkların soyutlanmasına ve verimli iletişime izin verilmesine yani 1973'te çözüm bulunmasına kadar devam etmiştir. O zamanlar Stanford'da profesör olan Vint Cerf ve ARPA'dan Robert Khan ortak bir aktarım protokolü fikrini geliştirmişlerdir. Bu "protokol", iletişim bağlantısının her bir ucunun diğerinden yapması gereken beklentileri oluşturmuştur. Bu paketler, ses dalgalarından radyo dalgalarına, cam elyaf

[91] ARPA, 1960 yılında askeri operasyonları belirlemek için TRANSIT adlı GPS'in bir sürümü üzerinde çalışan kuruluşlardan biriydi. 1972'de ajansın adı DARPA (Defense Advanced Research Projects Agency, "Savunma" için "D" eklenmiştir.) olarak değiştirilmiştir. DARPA, ABD Savunma Bakanlığı'nda ileri teknolojilerin bir koludur. DARPA ajansı, Sovyetler Birliği'nin 1957'de Sputnik uydusunu fırlatmasından sonra kurulmuştur. Uzaya gönderilen ilk uydu, ABD'nin teknolojik olarak geride kaldığına dair endişeleri ateşlemiştir. Ajansın amacı, yeni teknolojileri denemek, mümkünse operasyonel olarak hazır hale getirmek ve yeni bir şeyler yapmak için mevcut askeri teknolojilerin ötesine ulaşmaktır. Bunun için DARPA navigasyon, gizli, insansız hava araçları, gece görüşü ve ağ iletişimi gibi son yirmi yılda savaşın çehresini değiştiren ve gelecekte de değiştirmeye devam edecek birçok çalışmaya imza atmaktadır. Detaylı bilgi için bkz. "DARPA", [https://www.darpa.mil/about-us/about-darpa] (er. tar. 14.10.2020).

[92] P.W Singer ve A. Friedman (2013). *Cybersecurity and Cyberwar: What Everyone…, s.* 16.

üzerindeki ışık darbelerine kadar her türlü ağ üzerinden gönderilebilmektedir. Bu tür Taşıma Kontrol Protokolleri veya TCP'ler her tür paket protokolü üzerinde kullanılabilmektedir. Ancak şimdi yalnızca modern internette "İnternet Protokolü" veya "IP" adı verilen bir tür kullanılmaktadır.[93] Bu protokol, bir ağlar ağının oluşturulmasını mümkün kılmıştır.

İnsanlar araştırma için makineleri paylaştıkça birbirlerine mesaj yoluyla basit dosyalar göndermeye başlamışlardır. Bu durum zorlaşmış ve 1972'de BBN adlı teknik danışmanlık firmasında Ray Tomlinson[94], mesajları okumak, oluşturmak ve göndermek için temel bir program yazmıştır. Bu aynı zamanda internet genişlemesinde kârın ortaya çıktığı dönem olmuştur. Örneğin, bu noktada Vint Cerf, telekomünikasyon firması olan MCI'ye katılmıştır. 1983 yılında, internetteki ilk ticari e-posta hizmeti olan MCI postayı başlatma çabalarına öncülük etmiştir. Bu gelişmeler esnasında siber kelimesi ilk kez ortaya atılmıştır.

William Gibson, kelimeyi ilk kez 1982 çalışmasında "sibernetik" ve "alan" ın bir karışımı olarak kullanmıştır. İki yıl sonra türün devrim yaratan romanı Neuromancer'de bunu "Her ulusta milyarlarca meşru operatörün her gün tecrübe ettiği bir rızaya dayalı halüsinasyon... Düşünülemez karmaşıklık. Işık çizgileri, zihnin boşluğunda, veri kümelerinde ve takımyıldızlarında yer alan bir metafor" olarak bahsetmiştir.

1980'lerin sonlarında, yeni ortaya çıkan interneti yönetmenin araştırma topluluğunun işi olmadığı tespit edilmiştir. Ticari aktörler, interneti destekleyen gerekli ağ hizmetlerini sağlayabilmekte ve aynı zamanda hevesli tüketiciler haline gelebilmektedir. Bu nedenle Beyaz Saray Bilim ve Teknoloji Ofisi, hizmetlerini genişletmek ve ticarileştirmek için bir plan geliştirmiştir. Planlamacılar, ticari devir tesliminin son aşamalarının 1990'ların sonlarına kadar tamamlanmadığı on yıllık bir süreç öngörmüşlerdir.[95]

1989'da Al Gore[96], ağın daha hızlı özelleştirilmesi çağrısında bulunan bir tasarıyı Kongre'ye sunmuştur. Kongre'nin işleri hızlandırmak için yaptığı bu hamle, internetin genişlemesi için çok önemli olmuştur. Gore 1994'te Başkan

[93] B. M. Leinervd. (2009). "A Brief History …", s. 24.
[94] B. M. Leinervd. (2009). "A Brief History …", s. 24.
[95] P.W Singer ve A. Friedman (2013). *Cybersecurity and Cyberwar: What Everyone…, s*. 17-9.
[96] 1993-2001 yılları arasında ABD'nin kırkbeşinci başkan yardımcısı olarak görev yapan Amerikalı bir politikacıdır. Gore, Bill Clinton'ın 1992'deki seçim kampanyasında aday arkadaşıydı. Detaylı bilgi için bkz. [https://www.britannica.com/biography/Al-Gore] (er.tar. 14.10.2020).

Yardımcısı olduğunda, Ulusal Bilim Kurulu (NSF), bölgesel bağlantılarının resmi kontrolünü özelleştirmeye başlamıştır.[97] Bu özelleştirme, daha sonra interneti demokratikleştiren ve yaygınlaştıran çeşitli yeni buluşlar ve gelişmelerle aynı zamana denk gelmiştir.

1990 yılında, İsviçre'deki Avrupa Nükleer Araştırma Merkezi'nde (CERN) bir araştırmacı bilgileri, bir dizi harflerin belirsiz bir şekilde bağlantılı olduğu bilgisayardaki belgelerle yeni bir ağ ara yüzü oluşturmuştur. Bu Hiper Metni Aktarım Protokolü (HTTP)'dür. Bilgisayara bağlantılı belgeleri (URL) tanımlamak için eşlik eden bir sistemle Tim Berners-Lee, World Wide Web'i (www) icat etmiştir. Singer ve Friedman'ın belirttiğine göre, Berners-Lee bunu akademik bir konferansta sunmaya çalıştığında, buluşu resmi bir panel yapmak için yeterince değerli görülmemiştir. Bunun yerine, bir koridorda üzerine bir posteri tutmaya mahkûm edilmiştir.

1991'de ilk "web sitesi" yapılmıştır. Birkaç yıl sonra, Illinois Üniversitesi'ndeki araştırmacılar hem web tasarımını basitleştiren hem de genel halk için yeni "web sörfü" uygulamasını tanıtan Mosaic (1993-1997 yılları arasında kullanılan web tarayıcısı) web tarayıcısını tanıtmıştır.[98]

1996 yılında gizlilik becerisi ortaya çıkmış ve makro virüsleri piyasaya sürülmüştür. Bu durum anti virüs yazılımlarında yeni risklere karşı koruma yollarını bulmayı gerektirmiştir.[99] 2000'lerde kredi kartlarına yönelik hacklemeler yaşanmıştır. Bu sorun birçok güvenlik açığını da beraberinde getirmiştir. 2013 yılına kadar otuz trilyonun üzerinde kişisel web sayfası kullanılmıştır.[100] 2023'te insanlar bilgisayarsız neredeyse hiçbir işi yapamamaktadırlar. Bilgisayarlı saatlerle uyanırlar, bilgisayarla ısıtılan suda duş alırlar, bilgisayarla evinden ayrılmadan sipariş verirler, hatta bilgisayar tarafından kontrol edilen bir araba ile işe giderler ve bir bilgisayarda dün geceki spor skorlarına bakabilirler. Dahası, internet sadece posta göndermek veya bilgi toplamaktan oluşmamaktadır. Artık elektrik tesislerinin bağlanmasından oyuncak satın alımlarını takip etmeye kadar her şeyi yönetmektedir.

Ağ, bulut ve siber güvenliğin çözümleri olarak bilinen Cisco, 2013 yılı başında 8,7 milyar cihazın internete bağlandığını belirtmiş ve bu sayının 2020

[97] "Timeline of Computer History", [https://www.computerhistory.org/timeline/1989/] (er. tar. 14.10.2020).
[98] P.W Singer ve A. Friedman (2013). *Cybersecurity and Cyberwar: What Everyone…, s.* 20.
[99] M. Warner (2012). "Cybersecurity: A Pre…", s. 795.
[100] P.W Singer ve A. Friedman (2013). *Cybersecurity and Cyberwar: What Everyone…, s.* 1-3.

yılında kırk milyara ulaştığı vurgulamıştır.[101] 2023'te bu sayı çok daha fazla olacaktır. Kısaca ticaretten iletişime, günümüz uygarlığına güç veren kritik altyapıya kadar uzanan alanların tümü, küreselleşmiş bir ağ haline gelen sistem üzerinde çalışmaktadır. Tüm bu çalışmaların yükselişiyle, son derece önemli ancak kısa dönemli bilgisayar ve internet tarihinde belirleyici bir noktaya ulaşılmıştır: Siber Alan.

Siber alanın iyi tarafı, hızlı ve genellikle beklenmedik sonuçlarla fiziksel alana doğru dalgalanıyorsa, olumsuz tarafı da öyle dalgalanmaktadır. Facebook, Twitter, YouTube, Google ve diğer her şey, birçok yönden demokratik batıdaki modern yaşamın tanımı olarak belirtilmektedir. Birçoğu için, konuşma özgürlüğüne sahip işleyen bir internet ve seçtiğimiz sosyal ağlarla iyi bir bağlantı, sadece modernitenin değil, uygarlığın da bir işareti olmaktadır. Bunun nedeni, insanların "video ekranına bağımlı olmaları veya başka bir patronluk gösteren psikolojik tanıya sahip olmaları" değildir.

İnternet iş, kültür ve kişisel ilişkiler için merkezi platformdur. Bu hizmetlerin günümüz toplumundaki merkeziyetini yanlış anlamak, temel bir hata yapmanın ötesine geçmemektedir. İnternet hayata lüks bir katkı değildir; bilerek veya bilmeyerek çoğu insanın hayatında yer alan önemli bir noktadır. Bu durum internette kullanıcıların artmasıyla tehditleri de beraberinde getirmektedir. Devletler bu tehditleri manipüle edebilmek için güvenlik önlemlerini alması gerekmektedir. Gibson'un ilk kez Sibernetik kelimesini yazması ve internetin büyümesi ile güvenlik açıklarının ortaya çıkması "Siber Güvenlik" disiplininin oluşmasına zemin hazırlamıştır. Siber güvenlik ve siber güvenlik politikaları, hızlı bir sosyo-teknik dönüşüm, siyasi güç ve otoritenin parçalanmasıyla giderek farklı boyutlar kazanmıştır. Siber güvenlik, önümüzdeki on yılda ortaya çıkması muhtemel karmaşıklığın artışına bağlı olarak, siyasi alanda daha da etkili hale gelecektir.

2.2. Siber Güvenlik Politikaları

"Siber Güvenlik Politikası Nedir?" sorusunun yanıtı karmaşıktır ve *Mali* çalışmasında buna şöyle değinmektedir:[102] "Siber güvenlik politikası, siber alanın güvenliği ve operasyonları ile ilgili strateji, politika ve standartları içermelidir. Siber Güvenlik; tehdidi önleme, güvenlik açığını azaltma,

[101] P.W Singer ve A. Friedman (2013). *Cybersecurity and Cyberwar: What Everyone…, s.* 2; "The Center for Internet Security", [https://www.cisecurity.org/] (er. tar. 12.09.2022).
[102] Prashant Mali. (2016). "Critical Analysis of National Cyber Security Policies of UK, India, USA & Germany", *Chevening Fellowship in Cybersecurity Project*, s. 3.

caydırıcılık, uluslararası angajman, olay müdahalesi, esneklik, küresel bilgi ve iletişim altyapısının güvenliği ve istikrarı ile ilgili olduğu için bilgisayar ağı operasyonları, bilgi güvencesi, kanun yaptırımı, diplomasi, askeri ve istihbarat misyonları dahil kurtarma politikaları ve faaliyetlerini kapsamalıdır." Siber alan, ülkeler ve vatandaşları için alternatifler sunmaktadır. Yani hükümette artan bilgi birikimi ve şeffaflık, sivil toplumun zenginleştirilmesi, entelektüel ve ekonomik büyümeyi de beraberinde getirmiştir.[103] Ancak bu geri dönüşlerle birlikte casusluk, veri hırsızlığı ve dolandırıcılık gibi siber suçlar, devlet dışı aktörler, kritik altyapıyı tehdit eden ve Fikri Mülkiyet Hakları hırsızlığı ile endüstriyel, savunma ile ilgili casusluk yapan saldırganlar gibi yeni tehditleri de ortaya çıkarmıştır.[104]

Ukrayna elektrik şebekesi saldırısı[105] ve Bangladeş Bankası soygunu[106] gibi siber saldırılar, büyük enerji ve bankacılık kuruluşlarının kritik operasyonlarını sarsmıştır. Bu tür olaylar ve bildirilmeyen pek çok diğerleri, siber güvenliği dünya çapındaki hükümetler için bir öncelik haline getirmiştir. Birçok ülkeyi Ulusal Siber Güvenlik Politikaları (NCSPs) geliştirmeye yönlendirmiştir. Ulusal siber güvenlik stratejisi bir vizyon şekillendirmektedir. Devletlerin risklerini anlamak ve yönetmek için öncelikleri, ilkeleri ve yöntemleri formüle etmektedir.[107]

Ulusal Siber Güvenlik Politikaları, politik/sosyal vizyon veya istek olarak, stratejik açıdan oraya ulaşmak için ne yapılması gerektiği ve bunun nasıl yapılacağı konusunda daha net bir planlama olarak görülebilmektedir. Ancak her ikisinin de örtüşen özellikleri vardır. Bazı ülkelerde, çaba kritik altyapıyı korumaya yönelik olabilirken, diğerleri fikri mülkiyeti korumaya odaklanabilmektedir.

Siber alanda Bilgi ve İletişim Teknolojisi (BİT), cihazlarının ve ağlarının dünya çapında dağıtımı ile desteklenen, insanlar, yazılımlar ve hizmetler arasındaki etkileşimlerden oluşan karmaşık bir ortam olduğu önceki bölümlerde belirtilmiştir. Teknolojik gelişmelerin getirdiği sayısız fayda nedeniyle

[103] Leanne Hirshfield (vd.) (2015). "The Role of Human Operators' Suspicion in the Detection of Cyber Attacks", *International Journal of Cyber Warfare and Terrorism*, 5(3), ss. 28-44.
[104] Prashant Mali (2016). "Critical Analysis…", s. 3.
[105] Robert M. Lee (vd.) (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid*, Washington, DC: E-ISAC.
[106] Sara Peters (2016). "Malware At Root Of Bangladesh Bank Heist Lies To SWIFT Financial Platform", [https://www.darkreading.com/attacks-breaches/malware-at-root-of-bangladesh-bank-heist-lies-to-swift-financial-platform] (er. tar. 13.12.2021).
[107] Madeline Carr (2016). "Public-Private Partnerships in National Cyber-Security Strategies", *International Affairs*, 92 (1), ss. 43-62.

günümüzde siber alan, vatandaşlar, şirketler, kritik altyapı, ordu ve hükümet grupları arasında net sınırlar çizmeyi zorlaştıracak şekilde kullanılan ortak bir havuz olduğu bilinmektedir. Öngörülebilir gelecekte siber alanın daha karmaşık olması ve ona bağlı ağlarda ve cihazlarda birçok kat artış olması politika yapıcılar tarafından beklenmektedir.

Birçok hükümet kendi siber güvenlik stratejilerini ve düzenlemelerini ayrı ayrı oluşturmuştur. AB sağlam bir yasal ve düzenleyici çerçeveye odaklanmaktadır. Avrupa Konseyi Siber Suçlar Sözleşmesini (Budapeşte Sözleşmesi veya Sözleşme) açıklayacak olan siber güvenlikle ilgili uluslararası iş birliğini desteklemektedir. Öte yandan Anglosphere[108], ulusal siber güvenliğin sürdürülmesi için özel sektörün lider rolünü, eğitimli bir işgücünü, sosyal yardım ve diplomasiyi vurgulamaktadır. Buna, siber güvenlik mevzuatında bilgi özgürlüğünün altını çizen ve özel sektörün rolünü vurgulayan Amerika Birleşik Devletleri'de dâhildir. Yine de hükümet bilgilerinin hassasiyeti nedeniyle, siber güvenlik hayati öneme sahiptir ve bilgi özgürlüğünden daha öncelikli olma eğilimindedir. Baltık Devletleri, ulusal siber güvenlik stratejilerinin geliştirilmesinde Kuzey Atlantik Antlaşması Örgütü (NATO) ile sıkı bir iş birliği içindedir.

BİT, siber alanda yer alan ve orada bulunan kritik sektörlerden biridir. Türkiye ve İngiltere hükümetlerinin ekonomisi için en önemli büyüme katalizörlerinden biri olarak ortaya çıkmıştır. Bu sektör, ülkelerin ekonomisini beslemenin yanı sıra; istihdam, yaşam standardı, çeşitli sosyo-ekonomik parametrelere doğrudan ve dolaylı katkı sağlayarak halkının yaşamlarını da olumlu yönde etkilemektedir.

[108] Avrupa entegrasyonuna İngilizlerin katılımı, yüksek düzeyde bir politika ikilemi olarak ortaya çıkmıştır. Bu ikileme sebep olan temel faktör, çakışan birtakım hedeflerin Avrupa şüpheciliği ile bütünleşerek, ortak hedeflere ulaşmada çözümsüzlükleri de beraberinde getirmesiydi. Bu şüphecilik, Avrupa entegrasyonundan bağımsız olarak İngiliz siyasetinin hâkim olduğu İngiliz milliyetçiliğini daha net bir şekilde ortaya çıkarmıştır. Detaylı bilgi için bkz. Ben Wellings (2014). "Euroscepticism and the Anglosphere: Traditions and Dilemmas in Contemporary English Nationalism", *JCMS*, s. 7. "Anglosphere", İngilizce konuşulan dünyanın heryerindeki (Avustralya, Kanada, Yeni Zelanda, Birleşik Krallık, ABD, Avrupa ve Asya'nın diğer gelişmiş uluslarının) ortak kültürel, tarihi bağları paylaşan ülkelerin oluşturduğu bir kavramdır. Anglosphere kavramı ile bu ülkelerin, ayırt edici üstün özelliklerinin olduğuna inanılmaktadır. James C. Bennet (2007). *The Anglosphere Challenge: Why the English-Speaking Nations Will Lead the Way in the Twenty-First Century*, Maryland: Rowman & Littlefield, s. 54-55. Böyle bir organizasyon, çeşitli şekillerde "İngilizce Konuşan Birlik" veya "Anglosphere" olarak adlandırılmıştır. Andrew Mycock ve Ben Wellings (2011). "The Anglosphere: Past, Present and Future", *Stanford University,* [https://www.thebritishacademy.ac.uk/] (er. tar. 27.01.2023).

Sektör, küresel çapta ülkelerin imajını dünya standartlarında teknoloji çözümleri ve BİT iş hizmetleri sağlamada evrensel bir oyuncuya dönüştürmede önemli bir rol oynamıştır. Devlet, BİT tabanlı ürünlerin ve BİT destekli kamu hizmetlerinde (vatandaş hizmetleri, vatandaş kimlik belirleme, kamu dağıtım sistemleri vb.), sağlıkta (tele tıp, uzaktan danışma, gezici klinikler vb.), eğitimde (e-öğrenme, sanal sınıflar vb.) ve finansal hizmetlerde (mobil bankacılık, ödeme ağ geçitleri vb.) daha fazla benimsenmesinde önemli bir itici güç olmuştur. Bu tür girişimler, kurumsal ve özel katılım ile büyük ölçekli BİT altyapısının oluşturulmasına yol açan ulusal programların daha fazla benimsenmesini sağlamıştır.

Ülkelerdeki BİT sektörünün büyümesi, hızlı sosyal dönüşüm ve kapsayıcı büyüme için iddialı planları beraberinde getirmiştir. Böyle bir odaklanma, ülkelerde küresel olarak ağa bağlı ortama uygun bir siber güvenlik eko-sisteminin oluşturulmasını sağlamaktadır.

Siber alan ister kasıtlı ister tesadüfi, insan yapımı veya doğal olsun, çok çeşitli olaylara karşı savunmasızdır ve siber alanda alınıp verilen veriler, hem ulus-devletler hem de devlet dışı aktörler tarafından kötü amaçlarla kullanılabilir. Bir ulus devletin altyapısını veya altında yatan ekonomik refahı hedefleyen siber saldırılar, mevcut devlet kaynaklarını etkili bir şekilde azaltabilmekte ve destek yapılarına olan güveni zayıflatabilmektedir. Ulusal öneme sahip siber ile ilgili bir olay herhangi bir biçimde olabilmektedir: Organize bir siber saldırı, bilgisayar virüsü, solucanlar veya herhangi bir kötü amaçlı yazılım kodu gibi kontrolsüz bir istismar, önemli siber sonuçları olan bir ulusal felaket, bilgi altyapısına veya önemli varlıklara büyük zarar verebilecek diğer ilgili olaylar.

Büyük ölçekli siber olaylar, kritik bilgi sistemlerinin işleyişine zarar vererek hükümet, kamu ve özel sektör kaynaklarını ve hizmetlerini olumsuz etkileyebilmektedir. Böylesine büyük kesintilerden kaynaklanan sorunlar, yaşamları, ekonomiyi ve ulusal güvenliği tehdit edebilmektedir. Hızlı tanımlama, bilgi alışverişi, soruşturma ve koordineli yanıt ve iyileştirme, kötü niyetli siber faaliyetlerinin neden olduğu hasarı azaltabilmektedir. Kişilere, işletmelere ve hükümete yönelik siber tehdit örneklerinden bazıları kimlik hırsızlığı, kimlik avı, sosyal mühendislik, haktivizm, siber terörizm, mobil cihazları hedefleyen bileşik tehditler ve akıllı telefon, güvenliği ihlal edilmiş dijital sertifikalar, gelişmiş kalıcı tehditler, hizmet reddi, bot ağları, tedarik zinciri saldırıları, veri sızıntısı vb. olabilmektedir.[109]

[109] National Cyber Security Policy (2013), s. 2, [https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/India_2013_National_cyber_security_policy-2013] (er. tar. 03.09. 2020).

Bilgi altyapısının korunması ve siber güvenliğin sağlanması; bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinden kaynaklanmaktadır. Hükümetlerin, siber alanı koruma çabalarını destekleyebilmesi ve sürdürebilmesi adına bir platformun oluşturulması için siber güvenlik zorluklarını ele alan çeşitli faaliyetleri ve programları bulunmaktadır. Siber alanın dinamik doğası nedeniyle, artık bu eylemlerin Ulusal Siber Güvenlik Politikası altında, entegre bir vizyon ve uygulama için bir dizi sürdürülebilir ve koordineli stratejiyle birleştirilmesine ihtiyaç duyulmaktadır.

Siber güvenlik politikası büyüyen bir alandır. Bireyler, küçük, orta ve büyük işletmeler ile devlet ve hükümet dışı kuruluşlar dâhil olmak üzere tüm BİT kullanıcılarına ve sağlayıcılarına hitap etmektedir. Siber alanın güvenliği ile ilgili eylemleri tanımlamak ve yönlendirmek için şemsiye bir çerçeve görevi görmektedir. Aynı zamanda bireysel sektörlerin ve kuruluşların ihtiyaçlarına uygun siber güvenlik politikaları tasarlamalarına da olanak tanımaktadır.

Politika bilgileri, bilgi sistemlerini ve ağları etkili bir şekilde korumak için genel bir bakış sağlamaktadır. Hükümetin ülkedeki siber alanın korunmasına yönelik yaklaşımı ve stratejisi hakkında bir fikir vermektedir. Ayrıca ülkenin bilgi ve bilgi sistemlerini korumada, kamusal ve özel sektörde tüm kilit oyuncuların iş birliğine dayalı çalışmasını sağlamak için bazı işaretlerin ana hatlarını çizmektedir. Bu nedenle bu politika, ülkenin siber alanının güvenlik duruşunu iyileştirmek için belirli eylemlere ve programlara yol açan bir siber güvenlik çerçevesi oluşturmayı amaçlamaktadır. Güvenli bir siber alan oluşturabilmek için siber güvenlik politikalarında şunlar vurgulanmaktadır:[110]

- Açıkça tanımlanmış roller ve sorumluluklarla, ülkedeki siber güvenlikle ilgili tüm konuları koordine edecek bir ulusal ağa dayalı siber güvenlik politikalarını belirlemek,
- Tüm kuruluşların siber güvenlik girişimlerini uygulamak ve siber olaylardan kaynaklanan acil durum müdahalelerini karşılamak için belirli bir bütçe ayırmasını sağlamak,
- Kuruluşları siber güvenlikle ilgili bilgi altyapısı kurmaya, güçlendirmeye ve yükseltmeye teşvik edecek mali planlar ve teşvikler sağlamak,
- Teknoloji geliştirme, siber güvenlik uyumluluğu ve pro-aktif eylemler için teşvikler yoluyla siber olayların meydana gelmesini ve tekrarını önlemek,
- Bilgi paylaşımı, siber güvenlik olaylarını tespit etme ve müdahale etme ve yenileme çalışmalarında iş birliği için bir mekanizma oluşturmak,

[110] Cyber Security Strategy Documents, [https://ccdcoe.org/cyber-security-strategydocuments.html] (er. tar. 04.09.2020).

- Kuruluşları, güvenilir BİT ürünlerinin tedariki için yönergeler benimsemeye teşvik etmek ve yerel olarak üretilmiş güvenlik açısından etkileri olan BİT ürünlerinin tedarikini sağlamak,
- Bilgi güvenliği ve uyumluluğunda küresel en iyi uygulamaların benimsenmesini teşvik etmek ve böylece siber güvenlik duruşunu geliştirmek,
- Uygunluk değerlendirmesi ve siber güvenlik en iyi uygulamaları, standartları ve yönergelerine uygunluğun belgelendirilmesi için altyapı oluşturmak (örneğin, ISO 27001 ISMS sertifikasyonu, IS sistem denetimleri, Sızma testi / Güvenlik açığı değerlendirmesi, uygulama güvenlik testi, web güvenliği testi),
- Risk değerlendirme ve risk yönetimi süreçlerinde, iş sürekliliği yönetiminde ve siber kriz yönetim planında küresel güvenlik uygulamalarının hükümet içindeki ve kritik sektörlerdeki tüm kuruluşlar tarafından en iyi şekilde uygulanmasını sağlamak, kesinti riskini azaltmak ve güvenliği artırmak,
- Tüm kuruluşları, iş planlarında bütünleşmiş bir bilgi güvenliği politikaları geliştirmesi ve bu politikaları uluslararası en iyi uygulamalara göre uygulaması yönünde teşvik etmek gerekmektedir. Bu tür politikalar, güvenli bilgi akışı için standartlar ve mekanizmalar oluşturmayı (işlem sırasında, işleme, depolama ve geçiş sırasında), kriz yönetimi planını, proaktif güvenlik duruş değerlendirmesini ve hukuki olarak etkinleştirilmiş bilgi altyapısını içermelidir.

ITU tarafından oluşturulan endekste belirtildiği üzere yukarıda bahsedilen siber güvenlik gündeminin beş boyutunun genel olarak iyileştirildiğini ve güçlendirildiğini görmek gerekmektedir. Ancak ITU, bu beş boyutun siber kapasitedeki bölgesel boşlukların devam ettiğine dair dikkat çekmektedir. Bir ulus olarak kapasite ve siber güvenlik duruşunun daha iyi anlaşılmasını sağlamak için olayları tespit etmenin yeterli olmadığı ve etkili ölçümlerin gerekli olduğu Küresel Siber Güvenlik Endeksi ve Uluslararası Telekomünikasyon Birliğinin çalışmaları tarafından not edilmiştir.

Küresel anlamda siber güvenlik faaliyetleri yapılmakta, ortak programlar ve çalıştaylar düzenlenmektedir. GCI ilk olarak 2015 yılında ITU tarafından dünya çapında siber güvenliğin durumu hakkında farkındalık oluşturarak Filistin Devleti ile birlikte 194[111] üye devletin siber güvenlik alanlarını belirlemelerine ve iyileştirmelerine yardımcı olmak, ülkeleri harekete geçmeye teşvik etmek amacıyla başlamıştır. 194 üye devletin katılımı ile bildirilen verilere dayanmakta

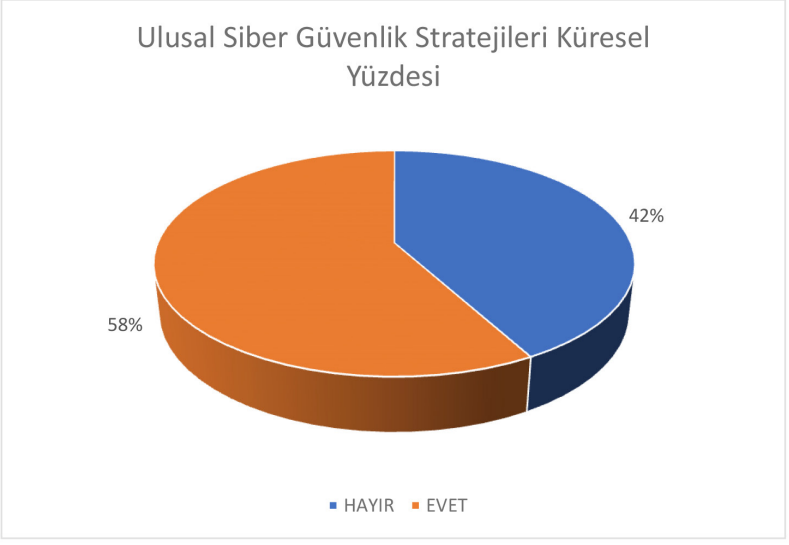
[111] 2018 Küresel Siber Güvenlik Endeksi'nde 193 üye devletlerin katılmasına rağmen, 2020 yılında bu üye devletlere Filistin'de eklenmiştir. Detaylı bilgi için bkz. Global Cybersecurity Index 2020, *ITU,* s. vi.

olan Küresel Siber Güvenlik Endeksi'nde amaç siber güvenliğe olan bağlılığı ölçmek ve ülkelerin ulusal düzeyde siber güvenlik angajmanlarında nerede durduğuna dair anlık bir görüntü sağlamaktır. Siber güvenlik riskleri, öncelikleri ve kaynakları geliştikçe Küresel Siber Güvenlik Endeksi, ülkeler tarafından alınan siber güvenlik önlemlerinin daha doğru bir görüntüsünü vermek için de uyarlanmıştır.

Siber Güvenlik Stratejilerinin içeriği, metrikler ve ölçümler ışığında revize edilmektedir. Gelişen tehditler ve öğrenilen dersler siber güvenlik stratejilerinin uygulanmasını şekillendirmektedir. Küresel olarak ulusal siber güvenlik stratejilerine ilişkin ikili ölçekteki anket sonuçları Grafik 1'de verilmiştir.

Grafik 1:[112] Küresel Olarak Ulusal Siber Güvenlik Stratejileri

HAYIR	EVET
42 %	58%

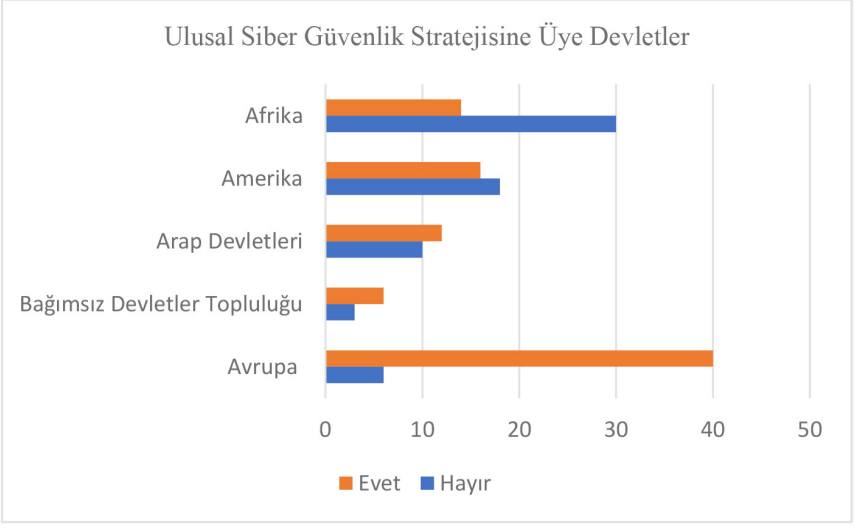


2018 yılı verilerine göre 193 ülkenin katılımıyla gerçekleşen siber güvenlik çalışmaları, ITU'nin GCI'nde detaylı olarak incelenmiştir. Yirmi beş farklı göstergeden oluşmaktadır. Bu göstergelerden bazıları, dünya çapında belirli siber güvenlik faaliyetlerinin durumunu somutlaştırmaya yardımcı olan taahhütlerle ilgilidir. En güçlü taahhütlerden biri, ülkenin dijital ağlarına yönelik saldırılara nasıl hazırlanacağını ve bunlara nasıl yanıt vereceğini açıklayan bir

[112] Global Cybersecurity Index 2018, *ITU, s*. 18.

siber güvenlik stratejisinin ana hatlarını belirlemektir. Buna göre, Grafik 1'de ülkelerin çoğu (%58), Ulusal Siber Güvenlik Stratejisi'ne (NCS) sahip olduğunu bildirmiştir. Fakat Grafik 1'de verilen bu ikili ölçekte azımsanmayacak kadar ulusal düzeyde siber güvenlik strateji belgesi olmayan ülkelerin yüzdelik dilimi %42 olarak belirtilmiştir. Bu kritik alanda, özellikle hükümetlerin dijital riskleri, öncelik olarak gördüğünü ifade ettiği için hükümetlerin siber güvenlik stratejilerine daha fazla çaba göstermesi gerekmektedir.

Grafik 2:[113] Ulusal Siber Güvenlik Stratejilerinde Üye Devletlerin İkili Ölçek Sonuçları



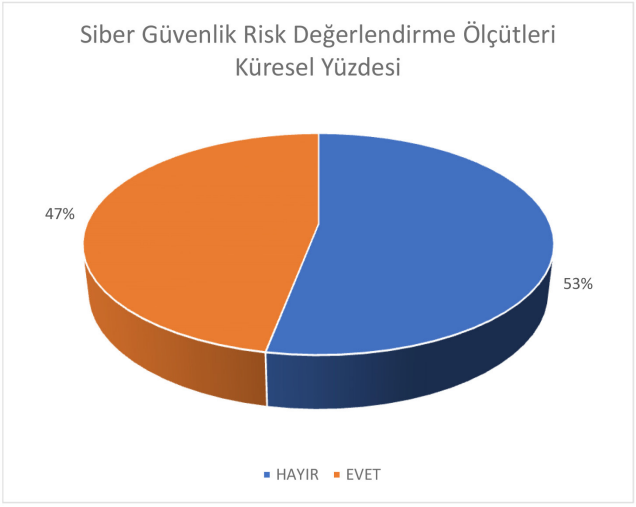
Grafik 1'de küresel olarak analiz edilen değerler, Grafik 2'de bölgesel olarak analiz edilmektedir. Grafik 2'de, Avrupa ve Bağımsız Devletler

[113] 2018 GCI verilerine göre, Avrupa 46 ülke, Bağımsız Devletler Topluluğu 9 ülke, Asya-Pasifik 38 ülke, Arap Devletleri 21 ülke, Amerika 35 ülke ve Afrika 44 ülke siber güvenlik endeksine katılmıştır. Afrika bölgesindeki 44 üye devletten 33' GCI'ne yanıt vermiştir, ancak yalnızca 31'i anketi gerçekleştirmiştir. Amerika bölgesindeki 35 üye devletten 31'i GCI'ne yanıt vermiştir, ancak yalnızca 18'i anketi gerçekleştirmiştir. Arap Devletleri bölgesindeki 21 üye devletten 20'si GCI'ne yanıt vermiştir, ancak Filistin Devleti dâhil yalnızca 16'sı anketi gerçekleştirmiştir. Asya-Pasifik bölgesindeki 38 üye devletten 26'sı GCI'ne yanıt vermiştir, ancak yalnızca 24'ü anketi gerçekleştirmiştir. Bağımsız Devletler Topluluğu bölgesindeki 9 üye devletten 7'si GCI'ne yanıt vermiştir ve 7 ülke de anketi gerçekleştirmiştir. Avrupa bölgesindeki 46 üye devletten 38'i GCI'ne yanıt vermiştir, ancak yalnızca 31'i anketi gerçekleştirmiştir. Detaylı bilgi için bkz. Global Cybersecurity Index 2018, *ITU*, s. 18, 24.

Topluluğu[114] bölgeleri, kendi bünyelerindeki ülkelerde ulusal stratejilere sahip olma oranı açısından ("Evet" oranının "Hayır" oranından fazla olması) yüksek olması ile öne çıkarken, Afrika Bölgesi'ndeki ülkeler en düşük oranı göstermektedir. Arap Devletleri'nde ise bu oran birbirine yakın seyretmektedir. Ulusal siber güvenlik stratejisine üye olan devletlere bakıldığında Grafik 2 ölçeğinde belirtilen en çok "Evet" yüzdelik dilimi Avrupa'da iken, en çok "Hayır" yüzdelik dilimi Afrika'da olmuştur. Ülkelerin siber alanda eksik olduğu noktalarda güvenlik duruşunu iyileştirmek için belirli eylemlere ve programlara yol açan bir siber güvenlik çerçevesi oluşturması gerekmektedir. Siber güvenlik politikaları, güvenli alanı sağlamak için önemlidir. Bu nedenle güvenli bir siber alan oluşturabilmek ve siber güvenlik politikalarına üye olan devletlerin sayısını artırmak hedeflenmelidir.

Grafik 3:[115] Küresel Olarak Siber Güvenlik Metrikleri

HAYIR	EVET
53%	47%

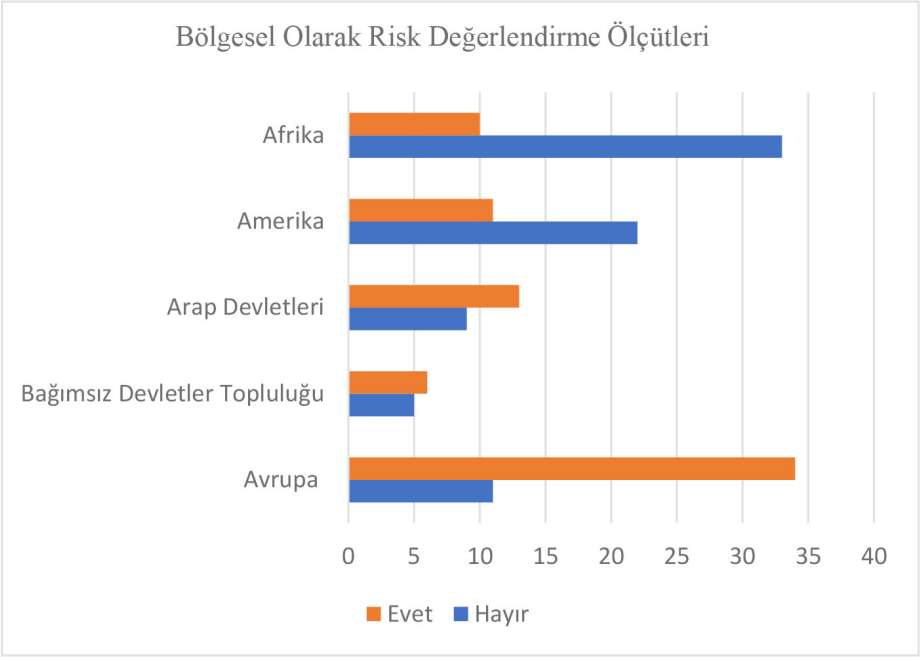


[114] GCI 2020 verilerine göre Bağımsız Devletler Topluluğu'nda dokuz ülke vardır: Ermenistan, Azerbaycan, Belarus, Kırgızistan, Türkmenistan, Tacikistan, Kazakistan, Rusya Federasyonu ve Özbekistan'dır. GCI 2018 yılında yapılan çalışma da ise Bağımsız Devletler Topluluğu dokuz ülke olarak belirtilmesine karşın, bunlardan sadece üçü incelemeye tabii tutulmuştur. İncelemede yer alan bu üç ülke, Rusya Federasyonu, Kazakistan ve Özbekistan'dır. Detaylı Bilgi için bkz. Global Cybersecurity Index 2018, *ITU, s*. 29-30.

[115] Global Cybersecurity Index 2018, *ITU, s*. 18.

Grafik 3'te, 193 ülkenin yüzde 47'sinde (91 ülke) siber güvenlik alanında risk değerlendirme ölçütlerine önem verildiği görülmektedir. Bu değer 2017 yılında ülkelerin yalnızca yüzde 21'inde görülmekteydi. Buna göre siber güvenliğin küresel düzeyde risk değerlendirmesine yönelik çalışmaların ciddi oranda artış gösterdiği anlaşılmaktadır. Ulusal bir siber güvenlik programının temel unsurlarının performansına ilişkin metriklerini geliştirmek, uygulamak, izlemek ve güncellemek siber güvenlik yönetişimi ve risk yönetimi açısından önemli iyileştirmelerdir.

Grafik 4:[116] Bölgesel Açıdan Risk Değerlendirme Ölçütleri



Bölgelere göre ölçümler çubuk grafiği olan Grafik 4'te, birçok Avrupa Bölgesi ülkelerinin nispeten siber güvenlik risk değerlerini ölçmek için yüksek kabul düzeyinde olduğu görülmektedir. Avrupa'yı ardısıra Arap Devletleri izlemekte olup, Grafik 4'ten de anlaşılacağı üzere Arap Devletleri'nin, Avrupa Bölgesi ülkelerini referans aldığı düşünülmektedir. Diğer bölgeler (Afrika, Amerika, Bağımsız Devletler Topluluğu) risk değerlendirmesi açısından iyileştirmeye ihtiyaç duymaktadır.

[116] Global Cybersecurity Index 2018, *ITU, s*. 18.

Küresel Siber Güvenlik gündemi ilk defa 2007 yılında başlamıştır. İnternet bağlantısıyla o yıl, bir milyar insan çevrimiçi olmuş ve oluşturulan 255 eksabaytlık veri miktarının kullanılabilir depolama alanını aşacağına dair endişeler ortaya çıkmıştır. Bugün, akıllı telefonlar günlük hayatı yeniden şekillendirmiş ve sosyal medya daha geniş bir topluma etki etmiştir. Günümüzde 3,5 milyar insan çevrimiçi durumda ve dijital dünyanın bulut bilişim sayesinde kullanılamayan depolama riski olmaksızın 44 zettabayt olduğu tahmin edilmektedir.[117] Buna ek olarak BİT'nin yaygınlaşması, daha geniş ulusal ekosistemi etkileyerek e-devlet hizmetleri gibi yeni organizasyonel olanaklara, Endüstri 4.0 (Dördüncü Sanayi Devrimi) ve daha geniş dijital ekonomi gibi ekonomik ve üretken paradigmalara hayat vermiştir. Buna karşılık BİT'nin yaygınlaşması yeni sorunları ve devletlerin güvenlik açıklarını da ortaya çıkarmıştır. Burada etki eden faktör, ortak güvenlik politikaları ve stratejileri belirlemenin zor olmasıdır.

ITU Küresel Siber Güvenlik Gündemi'ne dayanan GCI, taahhüt düzeyine beş boyutta bakmaktadır: organizasyonel önlemler, iş birliğine dayalı önlemler, kapasite geliştirme, yasal önlemler ve teknik önlemler.[118] Belirlenen bu beş boyut, ulusal bir siber güvenlik kültürünün doğal yapı taşlarını şekillendirdikleri için Küresel Siber Güvenlik Endeksi'nin göstergelerinin temelini oluşturmaktadır. Siber güvenlik hem dikey hem de yatay olarak tüm sektörleri kapsayan bir uygulama alanına sahiptir. Bu beş boyut, ülke düzeyinde bir endeks ve küresel siber güvenlik hazırlığı sıralamasıdır.

2.2.1. Organizasyonel Önlemler (Uyum Stratejisi)

Organizasyonel önlemler, ülkelerin siber güvenlik faaliyetlerinde, yönetişim ve koordinasyon mekanizmalarını incelemektedir. Organizasyonel önlemler, siber güvenliği yürütmenin en üst düzeyinde sürdürülmesini sağlamayı ve çeşitli ulusal kuruluşlarla ilgili kuruluşları sorumlu hale getirmeyi hedeflemektedir. Organizasyonel önlemler (ulusal stratejiler, sorumlu ajanslar ve siber güvenlik ölçümleri dâhil), herhangi bir ulusal girişimin uygun şekilde uygulanması için önemlidir. Geniş stratejik hedefler, uygulama, dağıtım ve ölçümde her şeyi kapsayan bir planla birlikte ulus devlet tarafından belirlenmelidir. Ulusal ajanslar stratejiyi uygulamak ve sonucu değerlendirmek için hazır bulunmalıdır. Ulusal bir strateji, yönetişim modeli ve denetim organı olmadan, farklı sektörlerdeki çabalar çatışmakta ve siber güvenlik gelişiminde

[117] Global Cybersecurity Index 2020, *ITU,* s. 1.

[118] Global Cybersecurity Index 2014, *ABI Research,* [https://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf] (er.tar. 22.01.2022).

etkin bir uyum sağlama çabalarını engellemektedir. Organizasyon yapıları, ulusal düzeyde siber güvenlik geliştirmeyi içeren kurum ve stratejilerin varlığına göre değerlendirmektedir.

Ulusal bir siber güvenlik stratejisine sahip olmak, siber güvenlik duruşu için olumlu bir ilk adımdır, ancak düzenli güncellemeler gerekmektedir. Ulusal bir siber güvenlik stratejisine sahip birçok ülke, siber güvenlik tehditlerinde ve önceliklerinde planlı olarak değişiklik ve düzenleme yapmamaktadır. 2020 yılı GCI verilerine dayalı olarak ulusal siber güvenlik stratejisine sahip 98 ülkeden sadece 60'ı yaşam döngüsü değerlendirmelerini stratejilerinin bir parçası olarak dâhil etmektedir.[119] Benzer şekilde, çoğu ülkede siber alanla ilişkili riskleri, ulusal düzeyde değerlendirmek için ölçütler mevcut değildir. Bu ölçütlerin eksikliği, ülkelerin mevcut riskleri değerlendirmesini, siber güvenlik müdahalelerine öncelik vermesini ve ilerlemeyi zorlaştırabilmektedir. Yeterli kurumsal önlemlerin olmaması, ulusal siber güvenlik yönetişiminde net sorumlulukların ve hesap verebilirliğin eksikliğine sebep olabilmektedir. Bu da etkili hükümet içi ve sektörler arası koordinasyonu zayıf bırakabilmektedir.

2.2.2. İşbirliğine Dayalı Önlemler

Siber suç ulusal sınırlar veya sektörel ayrımlarla sınırlı değildir. Siber suç küresel bir sorundur. Siber güvenlik, artan ağ bağlantıları ve ilişkili altyapılar ile ulus ötesi bir konu olmaya devam etmektedir. Küresel siber ekosistemin güvenliği, tek bir paydaş tarafından garanti edilemez veya yönetilemez.[120] Erişim ve etkiyi genişletmek için ulusal, bölgesel ve uluslararası iş birliğine ihtiyaç duyulmaktadır. Siber güvenlik iş birliğinin tipik hedefleri arasında minimum güvenlik önlemlerinin uyumlaştırılması, bilgi uygulama paylaşımı ve davranış normlarının kodlanması yer almaktadır. Bu nedenle, siber suçlarla mücadele, tüm sektör ve disiplinlerden (ikili ve çok taraflı anlaşmalar, uluslararası forumların/derneklerin katılımı, kamu özel ortaklıkları, kurumlar arası ortaklıklar, en iyi uygulamalar vb.) girdilerle çok paydaşlı bir yaklaşım gerektirmektedir.

ITU siber güvenliğin pratik yönlerinden en fazla sorumluluğu olan Birleşmiş Milletler kuruluşudur. ITU Genel Sekreteri, BM Genel Sekreterine üç ayda bir siber alanda oluşa(n)cak tehdit değerlendirmelerini sunmaktadır. ITU,

[119] Global Cybersecurity Index 2020, *ITU, s*. 10.
[120] Global Cybersecurity Index 2020, *ITU, s*. 20.

bir siber saldırı durumunda bir kaynak üssü olarak uzmanlardan oluşan bir veri tabanını tutmakta ve Küresel Siber Güvenlik gündemini yönlendirmektedir.[121]

Uluslararası ilişkiler teorisi bakış açısından, ITU'nin BM siber güvenlik ile ilgili faaliyetlerindeki rolü özellikle dikkate değerdir. ITU, 194 üye devlet tarafından kullanılan bir örgütsel platform ve özerk normlu bir girişimciliktir. Bürokrasisi, yani siber suçu en önemli üç önceliğinden biri olarak gören Genel Sekreteri, geleneksel ana vekil ilişkisinin ötesinde hareket etmektedir. Organizasyonel bir platform olarak Tunus'taki Dünya Bilgi Toplumu Zirvesi, Uluslararası Telekomünikasyon Birliği'nin 140 ülke tarafından onaylanan Eylem Hattı C5 (Karar 36 Antalya 2006) "Bilgi ve İletişim Teknolojilerinin kullanımında güven ve güvenlik oluşturulması" ndan sorumlu olması için faaliyete geçmiştir.[122]

Tunus gündemine cevaben Uluslararası Telekomünikasyon Birliği Genel Sekreteri Hamadoun I. Toure, Mayıs 2007'de Küresel Siber Güvenlik Gündemini başlatmıştır.[123] Üst düzey uzmanlar grubu, Küresel Stratejik Raporunu yayınlamadan önce 2007 ile 2008 yılları arasında üç toplantı gerçekleştirmiştir. Küresel Stratejik Rapor beş boyuta odaklanmaktadır: (i) yasal önlemler, (ii) teknik ve prosedürel önlemler, (iii) organizasyon yapıları, (iv) kapasite geliştirme ve (v) uluslararası iş birliği. ITU, Küresel Siber Güvenlik Gündemini "siber güvenlik için uluslararası bir çerçeve" olarak tanımlamaktadır.[124]

İkili ve çok taraflı anlaşmalar, normların ve davranışların kodlanmasında, siber güvenlik konusunda uluslararası iş birliğinin geliştirilmesinde çok önemli olduğu görülmektedir. Daha fazla iş birliği, çok daha güçlü siber güvenlik yeteneklerinin geliştirilmesine, çevrimiçi olarak tekrarlanan kalıcı tehditlere çözüm bulunmasına ve kötü niyetli bireylerin daha iyi araştırılıp onların yakalanmasına ve kovuşturulmasına yardımcı olabilmektedir.

---

[121] ITU Corporate Annual Report 2008, s. 16,43; United Nations (2008). *International Telecommunication Union*, "ITU Global Cybersecurity Agenda: High Level Experts Group, Global Strategic Report", Geneva: United Nations, s. 95; United Nations. "Internet Governance Forum", *About the Internet Governance Forum*, [http://www.intgovforum.org/cms/aboutigf] (er. tar. 12.05.2021).

[122] Hamadoun Toure (2011). "ITU's Global Cybersecurity Agenda", in the Quest for Cyber Peace, *International Telecommunication Union and World Federation of Scientists*, s. 104.

[123] Detaylı bilgi için bkz. ITU Rev. 36 Antalya (2006). [https://www.itu.int/oth/R0B06000017] (er. tar. 15.05.2021); H. Toure (2011). "ITU's Global Cybersecurity…", s. 104.

[124] United Nations. International Telecommunication Union. (March 2010). "Cybersecurity for all, Global Cybersecurity Agenda: A Framework for International Cooperation", Geneva: United Nations.

Ulusal ve uluslararası iş birliği, ortaklık sayısı, iş birliği çerçeveleri ve bilgi paylaşım ağları temelinde değerlendirilmektedir. Siber güvenliğin toplu eylem sorunu göz önüne alındığında, bazı ülkeler sadece ikili anlaşmaların değil, aynı zamanda çok taraflı anlaşmaların da imzalanması sağlamaya çalışılmıştır. Küresel Siber Güvenlik Endeksi'nin bu yinelemesi, çok taraflı anlaşmaların, hükümetlerin ve bölgesel kuruluşların üç veya daha fazla taraf arasındaki anlaşmalarını vurgulamaktır.

Küresel Siber Güvenlik Gündemi'nin ITU tavsiyeleri, üye devletlerin Siber Suçlara İlişkin Budapeşte Sözleşmesi'ni[125] benimsemelerini, model mevzuat geliştirmelerini ve örnek olarak kullanmalarını hedeflemektedir. Diğer bir öneri ise, koordinasyon için ulusal bir liderin veya ulusal siber güvenlik konseyinin varlığı ile CERT'nin varlığı gibi organizasyonel yapılara dayanan bir Siber Güvenlik Hazırlık Endeksinin oluşturulmasıdır. Aynı zamanda, ulusal altyapı koruması için bir çerçeve sunmakta ve 57/239 sayılı Genel Kurul kararında ana hatları çizilen bir siber güvenlik kültürünün ne anlama gelebileceğine dair bir kavramsallaştırma önermektedir.[126]

Küresel Siber Güvenlik Gündemi, iş birliği ve verimlilik için tasarlanmıştır. İlgili tüm paydaşlar arasındaki iş birliğini teşvik etmekte ve tekrarlı sorunlardan kaçınmak için mevcut girişimleri temel almaktadır. Küresel Siber Güvenlik Gündemi, siber tehditlere karşı gerçek anlamda ilk küresel çok paydaşlı, kamu ve özel sektör ittifakıdır. 2008'de ITU ve Siber Tehditlere Karşı Uluslararası Çok Taraflı Ortaklık hususlarında resmi olarak katılımcı ülkeler tarafından Malezya'da (GCA'nın Cyberjaya'daki teknoloji genel merkezi) bir mutabakat zaptı imzalanmıştır.[127] Birçok ülke (99) bilgi paylaşımı ve kapasite geliştirme konusunda anlaşmalar imzalamış veya onaylamıştır.[128]

---

[125] 2001 yılında Avrupa Konseyi Siber Suç Sözleşmesi olarak imzalanan ve 2004 yılında yürürlüğe giren Budapeşte Sözleşmesi, siber suçlara açıkça odaklanan ilk uluslararası antlaşma olmuştur. Anlaşmanın amaçları üç yönlüdür: 1) siber suçlarla ilgili ulusal yasaları uyumlu hale getirmek 2) bu suçların soruşturulmasını desteklemek ve 3) siber suçlarla mücadelede uluslararası işbirliğini arttırmak. Detaylı bilgi için bkz. Jennifer Daskal ve Debrae K. (2020). "Budapest Convention: What is it and How is it Being Updated?" [https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/].

[126] UN, ITU (March 2010). *Cybersecurity for all, Global Cybersecurity Agenda…,* s. 76, 120-121.

[127] H. Toure (2011). "ITU's Global Cybersecurity…", s. v.

[128] Global Cybersecurity Index 2020, *ITU, s*. 21.

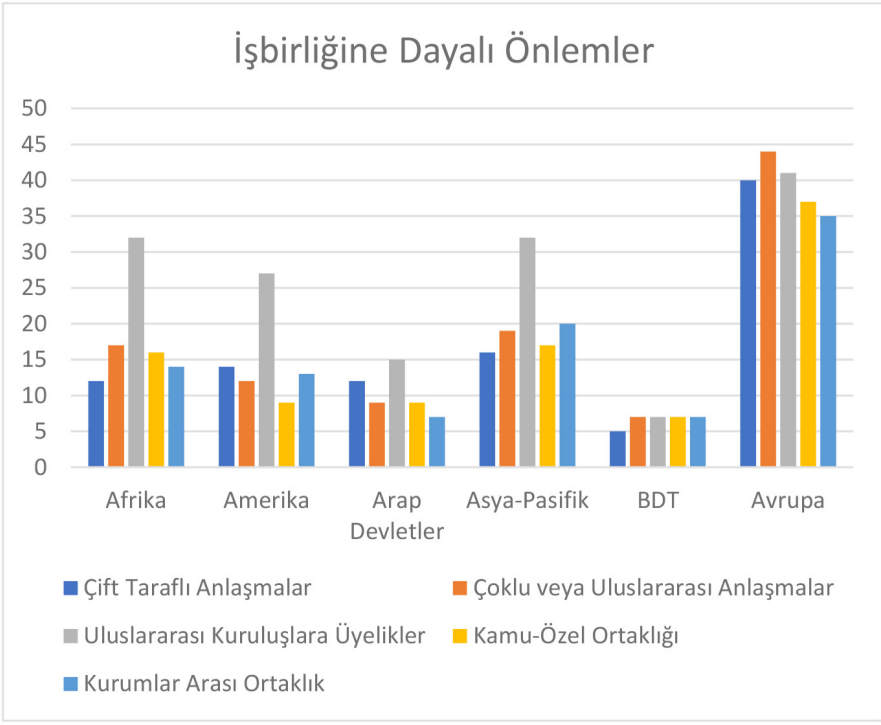
Tablo 1:[129] Bölge Bazında İş Birliği Sütunundaki Göstergelere Bağlılık

	Afrika	Amerika	Arap Devletleri	Asya-Pasifik	BDT	Avrupa
Çift Taraflı Anlaşmalar	12	14	12	16	5	40
Çoklu veya Uluslararası Anlaşmalar	17	12	9	19	7	44
Uluslararası Kuruluşlara Üyelikler	32	27	15	32	7	41
Kamu-Özel Ortaklığı	16	9	9	17	7	37
Kurumlar Arası Ortaklık	14	13	7	20	7	35

Tablo 1'de altı ayrı bölgenin (Afrika, Amerika, Arap Devletleri, Asya-Pasifik, Bağımsız Devletler Topluluğu ve Avrupa) uluslararası forumlara katılım açısından iş birliği göstergeleri verilmiştir. Genel olarak Avrupa ülkeleri tüm kategorilerde önde çıkmaktayken, Avrupa'yı Asya-Pasifik ülkeleri takip etmektedir. İş birliğine dayalı anlaşmalar ve ortaklıklar en az Bağımsız Devletler Topluluğu'nda görülmektedir. Uluslararası forumlara katılım tüm bölgelerde yüksek olmasına rağmen, bazı ülkeler az sayıda ikili anlaşmaya, kurumlar arası ortaklıklara ve kamu-özel ortaklıklarına sahiptir. Uluslararası ortaklık, iş birliği, kamu-özel ortaklığı, ikili ve çok taraflı anlaşmalara bakılırsa, bölge bazında en çok Avrupa ülkeleri siber güvenlik konusunda iş birliği uygulamıştır.

[129] Global Cybersecurity Index 2018, *ITU, s*. 48.

Grafik 5:[130] Bölge Bazında İş Birliği Sütunundaki Göstergelere Bağlılık



Grafik 5'te uluslararası kuruluşlara katılım tüm bölgelerde güçlüyken, çift taraflı anlaşmalar, kurumlar arası ortaklıklar ve kamu-özel ortaklıklar daha az sayıda gösterilmektedir. Avrupa bölgesindeki 46 üye devletten sadece ikisi siber güvenlik konusunda çok taraflı anlaşmaya sahip değildir. Tüm bölgeler, tüm göstergelerde ortalama ülke sayısını göstermektedir.

İki veya daha fazla ülke arasındaki resmi iş birliğinin ötesinde uluslararası faaliyetlere katılmak, ülkelere siber güvenlik tehditleriyle mücadele için iyi uygulamaları ve yeni yaklaşımları anlama fırsatları sunmaktadır. Son iki yılda 140 ülke, siber güvenlik konferansları, çalıştaylar, ortaklıklar ve diğer ülkelerle yapılan sözleşmeler gibi uluslararası etkinliklere katılmıştır. Ülkeler, diğer ülkelerle iş birliğinin ötesinde, özel sektörle de iş birliği yapmaktadır. Kamu ve özel sektör ortaklıkları, eyleme geçirilebilir istihbarat paylaşımından, iyi uygulamaların paylaşılmasına, Ar-Ge ihtiyaçları ve önceliklerinin iletilmesine kadar siber güvenlik çabaları için kritik öneme sahiptir.[131]

[130] Global Cybersecurity Index 2018, *ITU, s*. 48.
[131] Global Cybersecurity Index 2020, *ITU, s*. 21-22.

İşbirliğine dayalı önlemlerde diğer birçok teknolojinin yanı sıra akıllı cihazlar, M2M[132] iletişimleri, bulut tabanlı hizmetler ve yeni nesil ağ bağlantıları toplumları ilerletmektedir. Dijital teknoloji ve internet bağlantısı, önemli avantajlar sundukları için sistematik olarak özel ve kamu sektörüne entegre edilmektedir: üretkenlik, hız, maliyet azaltma ve esneklik.

Küresel sağlık acil durumu, iklim değişikliği, yaşlanan nüfus veya gelecekteki diğer zorluklar için dijital teknolojiler, dünyayı ileriye taşımada cazip bir araç sunacaktır. 2030'da "Sürdürülebilir Kalkınma Hedefleri" geliştirildiğinde, öngörülen dünya nüfusunun yüzde 90'ının (7,5 milyar insanın) çevrimiçi olacağı,[133] 24,1 milyar[134] Nesnelerin İnterneti (IoT) cihazına bağlı olacağı tahmin edilmektedir. Sürdürülebilir Kalkınma Hedefleri'ne yönelik çabalar devam ettikçe, dijital çözümlerin güvenli olmasını sağlamak için siber güvenlikte iş birliğine yönelik adımlara ihtiyaç duyulacaktır.

2.2.3. Kapasite Geliştirme Önlemleri (Siber Güvenlik Kapasitesinin Geliştirilmesi)

Kapasite geliştirme (kamu bilinçlendirme kampanyaları, siber güvenlik uzmanlarının belgelendirilmesi ve akreditasyonu için çerçeve, siber güvenlikle

[132] Son zamanlarda giderek daha önemli hale gelen Endüstri 4.0 (Dördüncü Sanayi Devrimi) ile ilgili yeni bir kavram olan M2M, makinadan makinaya gerçekleşen bir iletişim şeklidir. Makinadan makinaya kavramı iki cihazın birbiriyle bilgi alışverişinde bulunmasına, örneğin iletişim kurmasına ve veri göndermesine izin veren herhangi bir teknolojiyi temsil etmektedir. Makineler veya cihazlar arasında gerçekleşen iletişim otonomdur, bu veri alışverişinin gerçekleşmesi için insan müdahalesine gerek yoktur. M2M bağlantısı, Nesnelerin İnterneti (IoT) ile ilgilidir. Her ikisi de aynı kavramın parçasıdır ve birbirini tamamlamaktadır. IoT sayesinde, bir makine sistemi veya birbiriyle ilişkili cihazlar kablosuz olarak bağlanabilir. Bu sayede bulutta otomatik olarak veri alışverişi ve analizi yapılabilir. Kısacası, IoT, birçok M2M cihazını entegre ederek ve tüm bu verileri işlemek için bulut web platformlarını kullanarak etkinleştirilmektedir. Detaylı bilgi için bkz. "M2M or Machine to Machine communication, what is it?", "What is the M2M Communication?" (2019). [https://www.atriainnovation.com/en/m2m-communication-what-is-it/] (er. tar. 22.11.2022).

[133] Steve Morgan (18.07.2019). "Humans On The Internet Will Triple From 2015 To 2022 And Hit 6 Billion", [https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/] (er. tar. 12.11.2021).

[134] 2019'un sonunda 7,6 milyar aktif IoT cihazı vardı. Bu sayının 2030 yılında %11 bileşik yıllık büyüme oranı ile 24,1 milyara çıkacağı tahmin edilmektedir. Detaylı bilgi için bkz. "Global IoT Market Will Grow to 24.1 Billion Devices in 2030, Generating $1.5 Trillion Annual Revenue" (19.05.2020). [https://www.prnewswire.com/news-releases/global-iot-market-will-grow-to-24-1-billion-devices-in-2030--generating-1-5-trillion-annual-revenue-301061873.html] (er. tar. 12.11.2020).

ilgili profesyonel eğitim kursları, eğitim programları veya akademik müfredat vb.) ilk üç boyut (yasal, teknik ve organizasyonel) ile ilişkilidir. Siber güvenlik, çok sayıda sosyo-ekonomik ve politik sonuçları olmasına rağmen, çoğunlukla teknolojik bir perspektiften ele alınmaktadır. Sistematik ve uygun çözümler için sektörler arasında farkındalık, bilgi birikimini artırmak ve nitelikli profesyonellerin gelişimini teşvik etmek üzere insani ve kurumsal kapasite geliştirme esastır. Kapasite geliştirme, araştırma ve geliştirme, eğitim ve öğretim programları, sertifikalı profesyoneller ve kamu sektörü kurumlarının sayısına göre değerlendirilmektedir.

Tablo 2:[135] Bölge Başına Kapasite
Geliştirme Sütunundaki Göstergelere Bağlılık

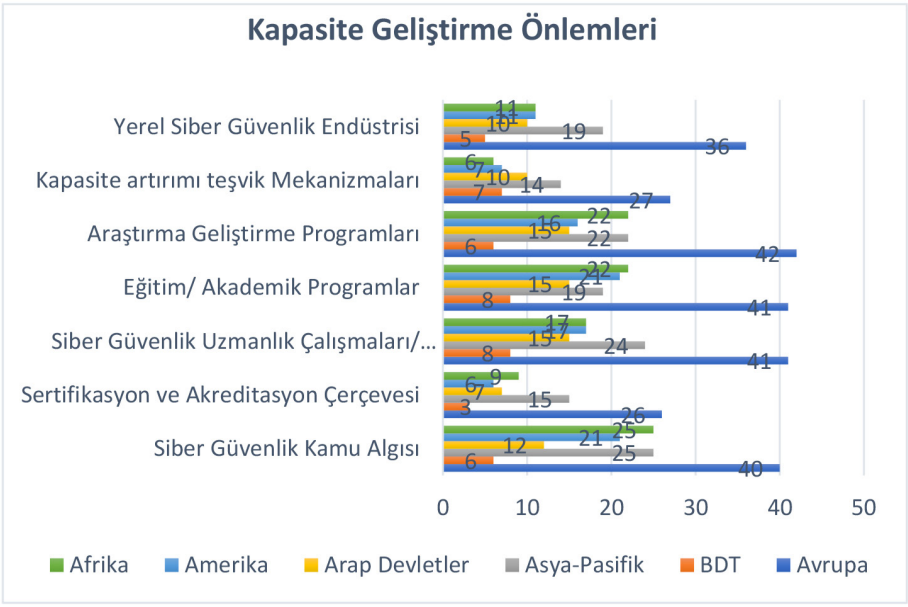
Bölgeler	Siber Güvenlik Kamu Algısı	Setifikasyon ve Akreditasyon **Çerçevesi**	Siber Güvenlik Uzmanlık **Çalışmaları/** Kursları	Eğitim/ Akademik P Programlar	Araştırma Geliştirme Programları	Kapasite artırımı teşvik Mekanizmaları	Yerel Siber Güvenlik Endüstrisi
Avrupa	40	26	41	41	42	27	36
BDT	6	3	8	8	6	7	5
Asya-Pasifik	25	15	24	19	22	14	19
Arap Devletleri	12	7	15	15	15	10	10
Amerika	21	6	17	21	16	7	11
Afrika	25	9	17	22	22	6	11

Tablo 2'de altı ayrı bölgenin (Afrika'dan 44 ülke, Amerika'dan 35 ülke, Arap Devletleri'nden 21 ülke, Asya-Pasifik ülkelerinden 38'i, Bağımsız Devletler Topluluğu'ndan 9 ülke ve Avrupa'dan 46 ülke) kapasitelerinin geliştirilmesine yönelik göstergeleri verilmiştir. Avrupa bölgesinde 46 devletin 41'i siber güvenlik eğitimleri/kursları/programlarında etkili olmuştur. Bağımsız Devletler Topluluğu'nda 9 devletin sadece 1'i siber güvenlik eğitimleri/ kursları/ programlarında etkin değildir. Asya-Pasifik'te 38 ülkeden 25'i kamu algısı bilincine sahiptir. Amerika bölgesinde 35 ülkeden yalnızca 21'i siber güvenlik kamu algısı ve eğitim/akademik programlar alanlarında etkilidir. Arap Devletleri'nin 22'sinden yalnızca 15'i siber güvenlik, araştırma geliştirme eğitimleri / kursları ve programlarında etkili olduğu görülmektedir.

[135] Global Cybersecurity Index 2018, *ITU, s*. 44.

Bölge bazında Avrupa ülkeleri (46 ülkeden en fazla katılım, iki kategoride 41 ülke de olmuştur) tüm kategorilerde daha fazla ülke katılımı gösterirken, Afrika ülkeleri (44 ülkeden en fazla katılım siber güvenlik ve kamu algısı üzerine 25 ülke de olmuştur) kendi içlerinde en az katılımı göstermektedir. Bölge bazında en az Bağımsız Devletler Topluluğu ülkelerinin kapasite geliştirmeye yönelik siber güvenlik çalışmaları görülmektedir. Genel olarak bölgeler en az etkiyi sertifikasyon ve akreditasyon çerçevesi üzerine göstermişlerdir.

Grafik 6:[136] Bölgesel Açıdan Kapasite Geliştirme Önlemleri



2018 yılı GCI verilerine göre Grafik 6'da Avrupa bölgesinin (mavi) çoğu göstergede yüksek taahhüt seviyelerini diğer bölgelere kıyasla koruduğunu göstermektedir. Uluslararası forumlara katılım tüm bölgelerde yüksek olmasına rağmen, ülkeler az sayıda ikili anlaşmaya, kurumlar arası ortaklıklara ve kamu-özel ortaklıklarına sahiptir. Uluslararası ortaklık, iş birliği, kamu-özel ortaklığı, ikili ve çok taraflı anlaşmalara bakılırsa; bölge bazında en çok Avrupa ülkeleri siber güvenlik konusunda iş birliği uygulamıştır.

Dünya Ekonomik Forumu, "her gün yaklaşık bir milyon insanın siber alanda ilk kez çevrimiçi olduğunu ve dünya nüfusunun üçte ikisinin bir mobil

[136] Global Cybersecurity Index 2018, *ITU, s*. 44.

cihaza sahip olduğunu" tahmin etmektedir.[137] İnternet ve dijital dünya, benzeri görülmemiş fırsatlar getirse de operasyonel kararlar ve teknoloji seçenekleri ele alınırken, çoğu zaman engelliler ve yaşlılar dikkate alınmamaktadır. 2021'de 65 yaş ve üzeri tahminen 752 milyon kişi vardır.[138] Bu sayı, engellilere ve yaşlılara odaklanan farkındalık kampanyaları yürüten ülke sayısıyla karşılaştırıldığında önemli ölçüde düşük çıkmaktadır. 194 ülkeden sadece yüzde 18'i engelliler için farkındalık oluşturmakta ve yüzde 25'i yaşlılar için kampanyalar yürütmektedir.[139]

COVID-19 sürecinde engelli kişiler ve yaşlılar için kişi izleme uygulamaları gibi dijital hizmetleri kullanma teşvik edilmiştir. Buna karşın, bu iki belirli nüfus için farkındalık yaratmaya çalışan az sayıda ülke olması endişe vericidir. İş ve ekonomik büyümeyi teşvik etmek, dayanıklı altyapı oluşturmak, kapsayıcı ve sürdürülebilir sanayileşmeyi teşvik etmek, yeniliği teşvik etmek, ülkeler içinde ve arasında eşitsizliği azaltmak, ulusal yetenekleri artırmayı amaçlayan süreçleri, becerileri, kaynakları, araştırma ve gelişmeleri güçlendirmek için siber güvenlik kapasitesinin geliştirilmesi gerekli olmaktadır.

2.2.4. Yasal ve Düzenleyici Çerçeve

Devletin, yasa koyucu ve düzenleyici olarak işlevinde bazı rolleri vardır. Bir yandan, toplum ve ekonomi karşısındaki hiyerarşik işlevini netleştirmek için gerekli yasal temeli ortaya çıkarmaktadır. Bunu, örneğin siber suçla mücadelede veya kritik altyapıların (kesintileri topluma ciddi şekilde zarar verebilecek olanlar) düzenlenmesinde yapmaktadır. Öte yandan, vatandaşlar ve işletmeler arasındaki ilişkiyi sağlamak için yasal çerçeveyi de oluşturmaktadır. Bu, ürün sertifikalarındaki güvenlik düzenlemeleri veya dijital bileşenlere sahip ürünler için üreticilerin sorumluluğuna ilişkin mevzuat ile olmaktadır. Bu rolün nasıl ve ne ölçüde icra edildiği, ekonomi ve devlet arasındaki tarihsel olarak gelişmiş ilişkilere bağlıdır. Uluslararası çalışmalar, özellikle ceza hukuku iş birliği etrafında uluslararası boyut da büyük önem taşımaktadır. Devlet kurumları hem ilgili ekonomiye hem de sivil topluma yardımcı olan uluslararası çerçeveleri savunarak toplumun destekçisi/temsilcisi olarak hareket etmektedir.

[137] World Economic Forum, "Global Risk Report 2020 - Executive Summary", [http://reports.weforum.org/global-risks-report-2020/executive-summary/] (er. tar. 12.12.2021).
[138] United Nations, "Department of Economic and Social Affairs Population Dynamics", *World Population Prospects 2019*, [https://population.un.org/wpp/DataQuery/] (er. tar. 22.11.2021).
[139] Global Cybersecurity Index 2020, *ITU, s*. 16.

Siber yasa, dijital dünyayı yöneten yasadır ve bilgilerin güvenliğini ve mahremiyetini, zararlara ilişkin suçları düzenlemektedir. İç kaynaklar, siber tehditte bulunan özel veya kamu kurumlarının çalışanları ve müşterilerdir. Dış kaynaklar ise, hackerlar, suç/terör grupları veya örgütleri, istihbarat ve soruşturma kurumlarıdır. Varlıklara yönelik tehditler farklı türlerde ve değişen yoğunluklarda ve etki değerlerinde olabilmektedir. Varlıklar, veri, bilgi, bilgi kaynakları, programlar, donanım, ağ vb. gibi dâhili veya harici olabilmektedir. BİT sistemlerinin güvenliğine yönelik tehdit birçok kaynaktan ve farklı şekillerde olabilmektedir. Bilişim teknolojilerindeki hızlı gelişmeler göz önüne alındığında siber yasalar önemli hale gelmiştir. Devletler, bu gelişmelerle ilişkili bilgisayar suçlarına ve ilgili ceza hukuku sorunlarına yanıt verebilmektedir.

Yirmi birinci yüzyılın en ciddi sorunları siber saldırı, güvenlik ve tehditlerdir. Suç faaliyetlerinin artan karmaşıklığı ve ölçeği, zararlı eylemlerin potansiyelini artırmaktadır.

Yasal ve düzenleyici çerçeveler, siber alanda yasa dışı faaliyetleri neyin ortaya çıkardığını belirleyen mevzuatın oluşturulmasını ve bu tür mevzuatın araştırılması, kovuşturulması ve uygulanmasında gerekli usule ilişkin araçların tanımlanmasını; bir dizi ulusal paydaş için siber güvenlik temellerinin ve uyum mekanizmalarının oluşturulmasını ve uluslararası yükümlülüklerle tutarlılığı sağlamak için prosedürler geliştirmesini içermelidir.[140]

GCI, aşağıda verilen bilgilerin varlığını ölçerek bir ülkenin yasal çerçevesi içindeki siber güvenlik müdahalelerinin envanterini sunmaktadır:[141]

- Kamu ve özel sektör paydaşlarının uyması gereken temel gereksinimler;
- Zararlı eylemleri yasaklayan yasal araçlar;
- Veri koruma mevzuatı[142] (örneğin bir kuruluşu bir siber güvenlik ihlalini ifşa etmeye veya yıllık denetim gereklilikleri oluşturmaya zorlayabilecek bir düzenleme biçimini alabilmektedir.);
- Çevrimiçi kimlik ve veri hırsızlığı (Ülkeler yasa dışı erişim konusunda harekete geçmiş olsa da çevrimiçi kimlik ve veri hırsızlığı mevzuatı hala yeterince dikkat çekmemektedir. Özellikle mevcut dijital ortama geçişle birlikte çevrimiçi

[140] Global Cybersecurity Index 2020, *ITU, s*. 3.
[141] Global Cybersecurity Index 2020, *ITU, s*. 3-4.
[142] 133 ülke koruma ve mahremiyet düzenlemelerini kanun haline getirmiştir. Koruma ve mahremiyet düzenlemeleri 15 ülke de taslak aşamasındadır ve 46'sında herhangi bir düzenleme bulunmamaktadır. Mevcut düzenlemeye sahip birçok ülke, yeni anlaşmaları ve normları yansıtacak şekilde mevzuatlarında güncellemeler yapmıştır. Detaylı bilgi için bkz. Global Cybersecurity Index 2020, *ITU, s*. 4.

kimlik koruması büyük ölçüde önemli olmaktadır. Dünya nüfusu, sosyal medya ve iş uygulamaları aracılığıyla çevrimiçi olarak değişmiştir. Çalınan bir kimlik hem özel hem de profesyonel olarak günlük yaşamı tehlikeye atabileceğinden önemli ölçüde güvenliğe ihtiyaç duymaktadır.);

- Çevrimiçi taciz ve ırkçılık[143]

Yasal önlemler (mevzuat, düzenleme ve spamın kontrol altına alınması dâhil ilgili yasa), bir ulus devlete suçların soruşturulması ve kovuşturulması, yasaya uyulmaması veya yasaların ihlali durumunda yaptırım uygulanması yoluyla temel yanıt mekanizmaları kurma yetkisi vermektedir. Bir yasal çerçeve, daha fazla siber güvenlik yeteneğinin üzerine inşa edilebileceği asgari davranış temelini belirlemektedir. Temel olarak amaç, bölgesel/uluslararası düzeyde uygulamaları uyumlu hale getirmek ve siber suçlara karşı uluslararası mücadeleyi basitleştirmek için yeterli mevzuata sahip olmaktır. Hukuki bağlam, siber güvenlik ve siber suçlarla ilgilenen yasal kurum ve çerçevelerin sayısına göre değerlendirilmektedir. [144] Yirmi birinci yüzyıda birçok zorluk çevrimiçi güveni aşındırmakta ve dijital toplumun tam potansiyelinde çalışmasını engellemektedir. Örneğin, siber suçlardan kaynaklanan küresel kayıpların 2020'de 1 trilyon ABD doları iken[145], 2021'de 6 trilyon ABD dolarına[146] kadar çıkmıştır. Toplumu korumak, güvenli bir dijital ortamı teşvik etmek için yasal

[143] Çevrimiçi taciz, kalıcı bir sorun olmaya devam etmektedir: 2020 yılında ABD'nde "Amerikalıların yüzde kırk biri kişisel olarak bir tür çevrimiçi taciz yaşamıştır". Avrupa Birliği'ndeki her on kadından en az biri çevrimiçi tacize maruz kalmıştır. 32 ülkedeki yetişkinlerle yapılan bir ankette, her beş yetişkinden biri çevrimiçi nefret söylemi yaşadığını bildirmiştir. Bir ülkede yasal olan başka bir ülkede cezalandırıcı bir suç oluşturabileceğinden, neyin suç oluşturduğuna ilişkin eşik, ülkeler arasında büyük ölçüde değişmektedir. Bununla beraber bazı ülkeler çevrimiçi ırkçı davranışları öne çıkaran hükümler yazmaya karar vermişlerdir. Detaylı bilgi için bkz. European Comission. "Let's put an end to Violence against Women", [https://ec.europa.eu/info/sites/default/files/aid_development_cooperation_fundamental_rights/factsheet_lets_put_an_end_to_violence_against_women_en.pdf] (er. tar. 11.11.2021); Jacqueline Beauchere (13.11.2020). "Microsoft Study: Online Risks that sow hate and Division are Growing", [https://blogs.microsoft.com/on-the-issues/2020/11/13/microsoft-study-online-risks-world-kindness-day/#_edn1] (er. tar. 22.11.2021).

[144] Global Cybersecurity Index 2018, *ITU, s*. 9.

[145] Zhanna Malekos Smith and Eugenia Lostri. "The Hidden Costs of Cybercrime", s. 3, [https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf] (er. tar. 23.11.2021).

[146] Steve Morgan. "Cybercrime To Cost The World $10.5 Trillion Annually By 2025", (13.11.2020). [https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/] (er. tar. 10.11.2021).

ve düzenleyici bir çerçevenin geliştirilmesi önemli olmaktadır. Siber güvenlikle ilgili herhangi bir ulusal çabanın başlangıcında yasal ve düzenleyici çerçeveler yer almalıdır.

2.2.5. Teknik Önlemler

Teknoloji (Bilgisayar Olay Müdahale Ekipleri (CIRT)[147] veya Bilgisayar Acil Müdahale Ekipleri (CERT)[148]), siber tehditlere karşı birincil savunma alanlarıdır. Teknoloji, ülkelerin olaylara merkezi bir temas noktası kullanarak ulusal düzeyde yanıt vermelerini sağlamakta ve hızlı, sistematik eylemi teşvik ederek ülkeleri deneyimlerden öğrenme ve siber güvenlik direnci oluşturma konusunda güçlendirmektedir. Ulusal bir CERT/CIRT/CSIRT; siber tehditleri belirleme, savunma, yanıt verme, yönetme ve siber alan güvenliğini artırma yeteneklerini sağlayan ulusal sorumluluğa sahip bir savunma alanını ifade etmektedir. Bu yeteneğin, CIRT seçim bölgelerinden veya diğer kaynaklardan gelen güvenlik olaylarının ikincil raporlamasını incelemek yerine, kendi istihbaratının toplanmasıyla birleştirilmesi gerekmektedir.

Devlet CERT/CIRT/CSIRT, yalnızca devlet kurumlarını etkileyen bilgisayar güvenliği veya siber güvenlik olaylarına yanıt veren bir kuruluştur. CERT hizmetlerini yalnızca kamu sektöründen bileşenlere sağlamakta ve sektörel bir CERT/CIRT/CSRIT, bilgisayar güvenliği veya siber güvenlik olaylarına yanıt veren bir kuruluş olmaktadır. Belirli bir sektörü etkileyen sektörel CERT'ler genellikle sağlık, kamu hizmetleri, acil servisler ve finans sektörleri gibi kritik sektörler için kurulmaktadır. Kamu sektörüne hizmet veren devlet CERT'inden farklı olarak sektörel CERT, hizmetlerini yalnızca tek bir sektördeki bileşenlere hizmet sağlamaktadır.[149]

Standartlar uygulama çerçevesi, istenmeyen postaları ele almak için kullanılan teknik mekanizmalar ve yetenekler, çevrimiçi çocuk koruması vb. kullanım teknik önlemlerin içerisinde yer almaktadır. Siber saldırıları tespit etmek ve bunlara yanıt vermek için uygun teknik becerilere sahip olmayan ülkeler savunmasız kalmaya devam etmektedir.

BİT geliştirme ve kullanımı, yalnızca güvenlik ortamında başarılı olabilmektedir. Bu nedenle ülkelerin, yazılım uygulamaları ve sistemleri için

---

[147] "CIRT (Cyber Incident Response Team)". [https://www.gartner.com/en/information-technology/glossary/cirt-cyber-incident-response-team] (er. tar. 10.11.2021).

[148] Peter Sullivan. "Computer Emergency Response Team (CERT)", [https://whatis.techtarget.com/definition/CERT-Computer-Emergency-Readiness-Team] (er. tar. 10.11.2021).

[149] Global Cybersecurity Index 2018, *ITU, s*. 69.

kabul edilen minimum güvenlik ölçütleri ve akreditasyon şemaları oluşturması ve kurması gerekmektedir. Bu çabaların, siber olaylarla başa çıkmak amacıyla ulusal bir organın, yetkili bir devlet kurumunun ve olayları izlemek, uyarmak ve bunlara müdahale etmek için ulusal bir çerçevenin oluşturulmasıyla tamamlanması gerekmektedir. Teknik unsurlar, siber güvenlikle başa çıkmak için pratik mekanizmaların sayısına göre değerlendirilmektedir.

Afrika bölgesinin teknik alanda yetersizliği bilinmesine rağmen, 2018 Küresel Siber Güvenlik Endeksi'nden bu yana altı ek CIRT geliştirilmiştir. Bölge ulusal CIRT'e sahip 13 ülkeden 19'a yükselmiştir. Amerika bölgesi 21 CIRT'e sahiptir. Arap Devletleri bölgesinde ulusal CIRT'i olan 17 ülke vardır. Ancak, Avrupa'da altı ülke ulusal CIRT'lerden yoksundur.[150]

Ulusal CIRT'ler ulusal düzeydeki sorunları ele alırken, sektöre özgü CIRT'ler sağlık, ulaşım, telekomünikasyon, kamu hizmetleri gibi belirli bir sektörün siber güvenlik ihtiyaçlarını ele almaktadır. CIRT türleri, diğerlerinin yanı sıra çok uluslu şirketlere, büyük şirketlere, özel üniversitelere ve diğer CIRT türlerine hizmet etmektedir. İnternet kullanıcılarının sayısına göre dünyanın dört bir yanındaki ülkelere bakıldığında, internet kullanıcılarının yüzde 95'inden fazlası hem ulusal siber güvenlik stratejisine hem de ulusal CIRT'ye sahip ülkelerde bulunmaktadır.[151]

Tablo 3:[152] Bölge Başına Teknik Sütundaki Göstergelere Bağlılık

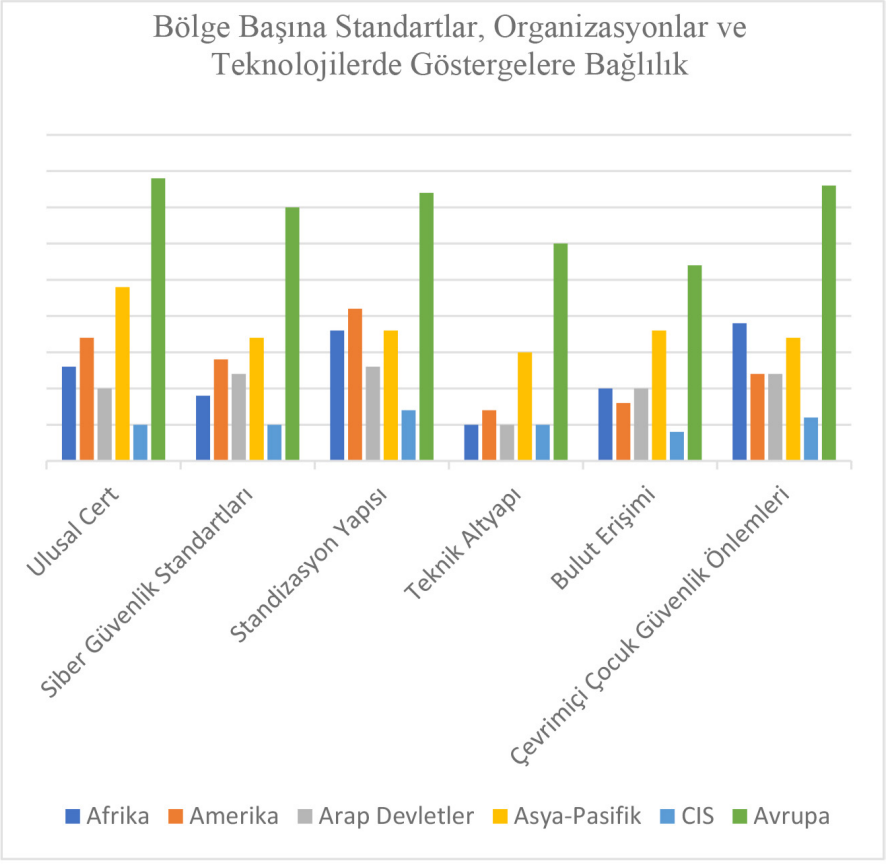
Bölgeler	Ulusal CERT	Siber Güvenlik Standartları	Standardizasyon Yapısı	Teknik Altyapı	Bulut Erişimi	Çevrimiçi Çocuk Güvenlik Önlemleri
Afrika	13	9	18	5	10	19
Amerika	17	14	21	7	8	12
Arap Devletler	10	12	13	5	10	12
Asya-Pasifik	24	17	18	15	18	17
BDT	5	5	7	5	4	6
Avrupa	39	35	37	30	27	38

Tablo 3'te altı ayrı bölgenin (Afrika, Amerika, Arap Devletleri, Asya-Pasifik, Bağımsız Devletler Topluluğu ve Avrupa) ortalama ülke sayılarının verilerine dayalı teknik sütundaki göstergeleri verilmiştir. 2018 yılı verilerine

[150] Global Cybersecurity Index 2020, *ITU, s*. 7.
[151] Global Cybersecurity Index 2020, *ITU, s*. 10.
[152] Global Cybersecurity Index 2018, *ITU, s*. 36.

göre, Afrika bölgesinde 44 ülkeden sadece 5 devletin teknik alt yapısı vardır. Amerika'da 35 ülkeden yalnızca 8'i bulut erişimine sahiptir. Arap Devletleri'nde 22 ülkenin 13'ü standizasyon yapısında etkin olurken, bu sayı Asya-Pasifik'te 38 ülkeden yalnızca 18'i etkin olmuştur. BDT'nde 9 devletin 2'sinde, Avrupa bölgesindeki 46 devletin 9'unda standizasyon yapısı mevcut değildir.

Grafik 7:[153] Bölge Başına Teknik Sütundaki Göstergelere Bağlılık



Tablo 3 ile birlikte çubuk Grafik 7'de gösterildiği gibi, Afrika bölgesi teknik altyapıda lider olmamasına rağmen, Çevrimiçi Çocuk Güvenlik Önlemlerine dâhil olan 19 üye devlete sahiptir. Amerika ve Arap ülkelerinin her biri eşit sayıda 12 üye devlete sahiptir. Asya-Pasifik'te 17 ve BDT'nda Çevrimiçi Çocuk Koruma önlemleri olan 6 üye devlet vardır. Avrupa diğer bölgelere kıyasla ulusal

[153] Global Cybersecurity Index 2018, *ITU, s*. 36.

CERT, siber güvenlik standartları, standizasyon altyapısı, teknik altyapı, bulut erişimi ve çevrimiçi çocuk güvenlik önlemlerinde lider olduğu görülmektedir.

2020 yılı sonunda 131 ülke, 2018 Küresel Siber Güvenlik Endeksi'nden bu yana kurulan 10 yeni CIRT dâhil olmak üzere Ulusal Bilgisayar Olay Müdahale Ekipleri kurmuştur. Pek çok ülke Bilgisayar Olay Müdahale Ekipleri uygulanmasında ilerleme kaydetmiş olsa da özellikle de az gelişmiş ülkeler CIRT'ın kurulmasında önemli engellerle karşılaşmaktadır. 2023'te birçok ülke bu boyuta önem vermesine rağmen; kaynak, teknolojik bilgi, siber güvenlik ekosistemi, araştırma ve geliştirme, önceliklendirme ve siyasi irade eksikliği, siber güvenlik sorunlarına yönelik teknik önlemlerdeki çabaları engelleyebilmektedir.[154]

2.3. Siber Güvenlik Politikası Hedeflerinin Belirlenme Süreci ve Hükümetlerin Aldığı Önlemler

Günlük yaşamlar, temel haklar, sosyal etkileşimler ve ekonomiler, teknolojilerinin "sorunsuz bir şekilde çalışmasına" bağlı kalmıştır.[155] Hükümetler teknolojinin sorunsuz şekilde çalışmasını, ulusal güvenliğin tehdit edilebileceği bir ortam olarak görmeye başlamışlardır. 2009 yılında, gelişmiş bilgi ve iletişim teknolojisine güvenmeye başlayan büyük işletmeler veya kuruluşlar olmuştur. Demiryollarından perakendeciliğe uzanan birçok sektör hem müşteriler hem de tedarikçilerle temel iş iletişimlerini sürdürmek için yüksek performanslı BİT sistemlerine bağlıkalmışlardır.

Finans sektöründe, her gün yüz milyarlarca dolar değerinde işler, küresel veri ağları üzerinden, kamuya açık ve özel olarak işlem görmektedir. Kamu sektöründe önemli kurumlar, kritik altyapı, sağlık, eğitim ve sosyal hizmetler sunmak için siber tabanlı sistemlere güven duymaktadır. Toplumların BİT sistemlerine ve ağlarına bağımlılığı daha da artacağı tahmin edilmektedir. Bu nedenle, küresel ekonominin artık geniş bant destekli bir siber bilgi karmaşasına bağlı olduğunu söylemek abartı olmaz. Bu durum bağımlılıkla birlikte siber alanda maruz kalma, savunmasızlık ve istismar gibi sürekli genişleyen bir dizi sorunuda beraberinde getirmektedir. Çatışma modu geliştikçe, saldırılara karşı gereken yöntem ve taktikler de gelişmiştir. Nitekim temel değişkenler zaman, yer, yer, yön, sayılar ve yetenekler nispeten sabit kalmıştır.

---

[154] Global Cybersecurity Index 2020, *ITU, s*. 7.

[155] European Commission (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, s. 2, [http://ec.europa.eu/digitalagenda/en/cybersecurity] (er. tar. 18.05.2021).

Siber saldırıların sayısındaki artış, siber güvenliğe olan ilginin artmasına neden olmaktadır. Basit bir örnekle, daha iyi bilinen internet arama motorlarından birinde siber güvenlik kelimesinin arama sıklığı, Mart 2016'dan Haziran 2019'a kadar yirmiden yüze yükselmiştir.[156] Başka bir deyişle, siber güvenlik kelimesi giderek daha popüler bir arama haline gelmiştir. Tesadüfen, siber güvenlik arayan kullanıcılar bu alandaki kursları ve eğitim fırsatlarını arama eğiliminde olmuşlardır. Yani, daha fazla insan siber güvenliğin öneminin farkında ve bilgilerini geliştirmenin yollarını aramıştır.

Ağ ve bilgi sistemleri için yüksek düzeyde ortak güvenlik önlemleri ile ilgili NIS Yönergesi[157], AB'nde yeni bir siber güvenlik kültürünün geliştirilmesinde muazzam bir role sahiptir. NIS Yönergesi sayesinde, AB üye ülkeleri siber olaylar hakkında bilgi alışverişinde bulunmakta, en iyi siber güvenlik uygulamalarını paylaşmakta, iş birliği yapmakta ve daha iyi koordine olmaktadır. NIS Yönergesi kapsamında temel hizmetlerin operatörleri (örneğin; bankalar, telekomünikasyon AB'nin Siber Alandan Kaynaklanan Tehditlere Yönelik Kapsamlı Yaklaşımı ve Kriz Müdahalesi Genel Müdürü, Avrupa Harici Eylem Servisi 25 şirket, enerji sağlayıcıları, hastaneler vb.) ciddi siber güvenlik olaylarından etkilendiklerinde ulusal makamları bilgilendirmek ve riskleri belirlemek için risk değerlendirme planları hazırlamakla yükümlüdür.[158]

Ağ ve bilgi sistemlerinin güvenliğini sağlamadaki sorumluluklar büyük ölçüde temel hizmetlerin operatörlerine ve dijital hizmet sağlayıcılarına ait olmaktadır. Dijital ekonomide ve toplumda, siber tehditler ve siber güvenlik olayları olarak farklı becerilerden uzmanların bir araya getirilmesi gerekmektedir. Ayrıca iş birliği ve bilgi alışverişine her zamankinden daha fazla ihtiyaç vardır. Bilişim sistemlerine yönelik saldırılar hakkında Yönergenin 2013 yılında kabul edilmesiyle, siber saldırılara ceza hukuku tepkisini iyileştirmeye yönelik bir adım atılmış olmaktadır. Bu, bilgi sistemlerine yönelik saldırılar alanında cezai suçların ve yaptırımların tanımlanmasına ilişkin asgari kuralları

[156] European Commission (2016). "Joint Framework on countering hybrid threats: a European Union response", [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN] (er. tar. 09.05.2021); European Commission (2017). "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en] (er. tar. 09.05.2021).

[157] Ağ ve Bilgi Sistemleri Güvenliği Yönergesi (the NIS Directive), AB'deki genel siber güvenlik seviyesini artırmak için yasal önlemler sağlamaktadır. Siber güvenlikle ilgili AB çapında mevzuatın ilk parçasıdır. AB'nde genel siber güvenlik seviyesini artırmak için yasal önlemler sağlamaktadır. Detaylı bilgi için bkz. [https://digital-strategy.ec.europa.eu/en/policies/nis-directive] (er. tar. 09.05.2021).

[158] [https://digital-strategy.ec.europa.eu/en/policies/nis-directive] (er. tar. 20.11.2021).

belirlemekte ve yetkililer arasında iş birliğini geliştirmek için operasyonel tedbirler sağlamaktadır.

İnternetin sınırsız doğası göz önüne alındığında, Avrupa Konseyi'nin Siber Suçlara ilişkin Budapeşte Sözleşmesi tarafından sağlanan uluslararası iş birliği çerçevesi, siber suçları ele alan farklı ulusal yasalar için en uygun yasal standardı kullanma fırsatı sunmaktadır. Şu anda sözleşmeye olası bir protokol eklenmesi araştırılmaktadır. Bu da elektronik kanıtlara sınır ötesi erişim konusunu uluslararası bağlamda ele almak için yararlı bir fırsat sağlayabilir.[159]

ITU'nin BM siber güvenlik ile ilgili faaliyetlerindeki rolü özellikle dikkate değerdir. *2.2.2. İşbirliğine Dayalı Önlemler* alt başlığında verilen bilgide ITU'nin siber güvenliğin sağlanması için çok taraflı anlaşmaların ve iş birliği yapmanın önemine değinilmiştir. ITU'nin stratejisi iki yönlü olarak tanımlanabilmektedir: birincisi üye devletler tarafından belirlenen geniş gündemi ilerletmeye çalışmakta ve ikincisi belirli girişimlere odaklanmaktadır. İkincisi ile ilgili olarak, örneğin "Çevrimiçi Çocuk Koruması", sosyalleşme etkilerinin potansiyel olarak daha geniş siber güvenlik gündeminde olumlu etkiler oluşturabilmesi için güven inşa edilebilecek bir yer ve tüm devletlerin hak ettiği bir çaba olarak tanımlanmıştır. Ayrıca, Haydarabad'daki 2010 Dünya Telekom Geliştirme Konferansı'nda BM Genel Sekreteri, devletlerin siber teröristleri ve saldırganları cezasız olarak ülkelerinde barındırmamaları gerektiğini vurgulamıştır. Bu açıklamalar, üye devletlere yapılan resmi bir talep değil, konuşmanın sadece bir parçası olmuştur.

Clarke ve Knake'in, "Cyberwar" adlı çalışmalarında, benzer bir öneriye sahip olduklarını belirtmek gerekmektedir: "Bir çatışma başladığında onu sınırlamak yerine, siber saldırıların savaşları başlatmasını engellemek gerekmektedir." Bu tüm uluslara, benzer bir beyanda bulunanlara veya bir anlaşma imzalayan uluslara uygulanabilmektedir.[160] ITU devletler için bir örgütsel platform olarak hizmet vermektedir. Dahası ITU, Dünya Bilim İnsanları Federasyonu (WFS)[161] ve BM'nin siber güvenlik faaliyetleriyle ilgili olarak kayda değer bir rol oynamaktadır.

---

[159] "Cybersecurity Risks, Progress, and the Way Forward in Latin America and Caribbean", *2020 Cybersecurity Report*, [www.cybersecurityobservatory.org] (er. tar. 09.05.2021).

[160] Richard A. Clarke ve Robert Knake (2010). *Cyber War: The Next Threat to National Security and What To Do About It,* NewYork: Ecco, s. 239.

[161] Dünya Bilim İnsanları Federasyonu dolaylı bir şekilde ITU'yı organizasyonel bir platform olarak kullanmıştır. 2001'de Federasyon, evrensel bir siber alan düzeni önermiştir. Detaylı bilgi için bkz. Tim Maurer (2011). *Cyber Norm Emergence at the United Nations An Analysis of the Activities at the UN Regarding Cyber,* Cambridge: Belfer Center for Science and International Affairs, s. 30-31.

"Siber İstikrar ve Siber Barış İlkeleri Üzerine Erice Deklarasyonu"[162] serbest bilgi ve fikir akışını, ortak bir siber davranış kuralını ve uyumlu küresel yasal çerçeveyi, siber suçlulara karşı yasa uygulama çabalarını ve daha dayanıklı sistemler geliştirmeyi vurgulayan siber barış kavramını açıklamaktadır.[163] ITU Genel Sekreteri, norm girişimci rolünde olan Dünya Bilim İnsanları Federasyonu'nun bir örgüt olarak siber barışla ilgili ilkelerin belirlenmesinde önemli bir rol oynamaktadır.[164] Siber barışla ilgili Federasyon tarafından formüle edilen beş ilke şunlardır: [165]

1. Her hükümet, çalışanlarının iletişime erişimini sağlamaya kendini adamalıdır.
2. Her hükümet, insanlarını siber alanda korumaya adayacaktır.
3. Her ülke kendi topraklarında teröristleri / suçluları barındırmamayı taahhüt edecektir.
4. Her ülke, diğer ülkelere ilk siber saldırı başlatan ülke olmayacağını taahhüt etmelidir.
5. Her ülke, siber alanda barışı sağlamak için uluslararası iş birliği çerçevesi içinde birbirleriyle iş birliği yapmaya kendini adamalıdır.

ITU; varlıklar, insanlar, mali, teknik ve kuruluşların bilgileri de dâhil olduğu kaynakların siber güvenlik endişesi içerisinde olduğunu açıklamıştır. Bu nedenle, bu tür bir güvenlik önlemi, tehditlere karşı korumayı ve hasar görmüş hizmetleri / işlevleri makul bir süre ve parayla geri yüklemeyi içermelidir.[166]

Oxford Üniversitesi'ndeki Küresel Siber Güvenlik Kapasite Merkezi (GSCC) ise, hükümetlerden, sivil toplumlardan ve akademilerden gelen ikiyüzün

[162] 1982 tarihli Erice Beyanı'nda şöyle yazmaktadır: "İnsan yaşamının kültürünü, tarihini, yapısını üçüncü dünya savaşından veya eşi görülmemiş felaket bir savaştan korumak için etkili bir süreç başlatmak ve gereken temel faktörleri belirlemek hayati önem taşımaktadır. Bunu başarmak için, barış hareketini tek taraflı bir eylemden karşılıklı anlayışa dayalı teklifleri içeren gerçek bir uluslararası eyleme dönüştürmek gerekmektedir." Detaylı bilgi için bkz. World Federation of Scientists "The Erice Statement", [http://www.federationofscientists.org/WfsErice.php] (er. tar. 15.05.2021); H. Toure (2011). "ITU's Global Cybersecurity…", s. 110-111.

[163] Tim Maurer (2011). *Cyber Norm Emergence ...,* s. 31.

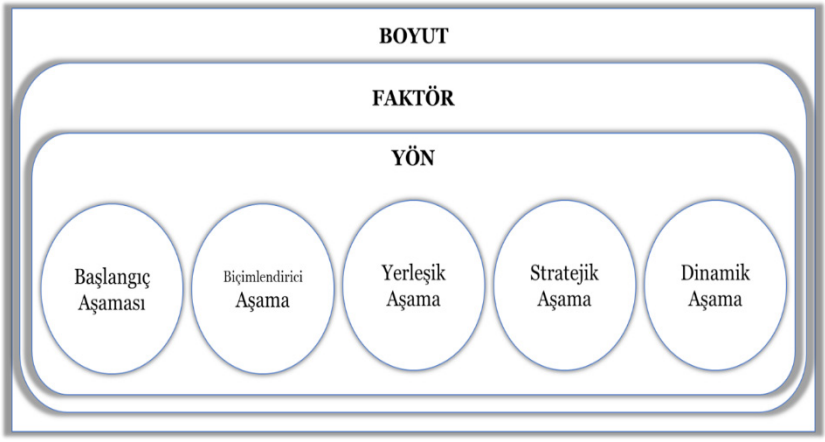
[164] H. Toure (2011). "ITU's Global Cybersecurity…", s. 79.

[165] H. Toure (2011). "ITU's Global Cybersecurity…", s. 79-80.

[166] Hamadoun I. Toure (ed.) (2014). "ITU the Quest for Cyber Confidence", [http://www.itu.int/] (er. tar. 07.06.2021).

üzerinde uluslararası uzmanla istişare halinde Uluslar İçin Siber Güvenlik Kapasite Olgunluk Modeli'ni (CMM) geliştirmiştir.[167]

Şekil 2: [168] Siber Güvenlik Kapasite Olgunluk Modelinin Beş Aşaması



CMM, bir ülkenin siber güvenlik yeteneklerinin olgunluk düzeyinin değerlendirmesini ve siber güvenlik erişim derecelerine karşılık gelen aşamaların belirlenmesini hedeflemektedir. Şekil 2'de Boyut, Faktör ve Yön olmak üzere üç derece tanımlanmıştır.

Boyut tüm derece ve aşamaları: bir bütün olarak CMM tarafından değerlendirilen ulusal siber güvenlik kapasitesini en geniş şekliyle kapsamaktadır. Her Boyutun, çekirdek kapasiteleri bir dizi "faktörden" oluşmaktadır. Bu üç model, siber güvenlik kapasitesinin kanıtlanıp analiz edilebileceği farklı modelleri temsil etmektedirler.

Faktör: Beş Boyut içinde faktörler, siber güvenlik kapasitesine sahip olmanın ne anlama geldiğini açıklamaktadır. Bunlar, ulusal kapasitenin temel

[167] Siber Güvenlik Kapasite Olgunluk Modeli (CMM), bir ülkenin siber güvenlik kapasitesini gözden geçirmek için tasarlanmış yöntemsel bir çerçevedir. CMM, bir ülkenin siber güvenlik sağlamasında etkili olması için ihtiyaç duyduğu ulusal kapasite genişliğini oluşturan beş boyuttan oluştuğunu düşünmektedir: 1. Siber güvenlik politikası ve stratejisi geliştirmek, 2. Toplum içinde sorumlu siber güvenlik kültürünü teşvik etmek, 3. Siber güvenlik bilgisi ve yetenekleri oluşturmak, 4. Etkili yasal ve düzenleyici çerçeveler oluşturmak ve 5. Standartlar ve teknolojiler aracılığıyla riskleri kontrol etmek. Detaylı bilgi için bkz. Global Cyber Security Capacity Centre 2021, University of Oxford, [https://gcscc.ox.ac.uk/the-cmm#/] (er. tar. 08.05.2021).

[168] "Cybersecurity Risks, Progress, and the Way Forward in Latin America and Caribbean", *2020 Cybersecurity Report*, s. 40, [www.cybersecurityobservatory.org] (er. tar. 09.05.2021).

unsurlarıdır ve daha sonra olgunluk aşaması için ölçülmektedir. Faktörlerin tam listesi, bir ülkenin tüm siber güvenlik kapasitesi ihtiyaçlarını bütünsel olarak birleştirmeyi amaçlamaktadır. Çoğu faktör, faktör göstergelerini daha kısa parçalar halinde (kanıt toplama ve ölçmeyle doğrudan ilgili olan) yapılandıran bir dizi "yönden" oluşmaktadır. Ancak, kapsam olarak daha sınırlı olan bazı faktörlerin belirli yönleri yoktur.

Yön: Bir Faktörün birden fazla bileşene sahip olduğu durumlardır. Yönler, göstergeleri anlaşılması daha kolay olan daha küçük kümelere ayırmak için kurumsal bir yöntemdir. Yönlerin sayısı, faktör içeriğinde ortaya çıkan temalara ve faktörün genel karmaşıklığına bağlıdır.

Aşama: Aşamalar, bir ülkenin siber güvenlik kapasitesinin belirli bir "faktörü veya yönü" ile ilişkili olarak ilerleme derecesini tanımlamaktadır. Bir değerlendirme yoluyla belirlenen beş olgunluk aşaması, en temelden (Başlangıç) en gelişmişe (Dinamik) kadar değişmektedir. Beş aşama şu şekilde tanımlanmaktadır (bkz. Şekil 2):[169]

• Başlangıç: Bu aşamada ya siber güvenlik olgunluğu yoktur ya da doğası gereği çok embriyoniktir. Siber güvenlik kapasitesi geliştirme konusunda ilk tartışmada yer alır. Ancak somut bir eylem gerçekleştirilmemektedir. Bu aşamada siber güvenlik kapasitesinin gözlemlenebilir bir kanıtı yoktur.

• Biçimlendirici Aşama: Bazı yönler büyümeye ve formüle edilmeye başlanmıştır. Ancak geçici, düzensiz, yetersiz tanımlanmıştır.

• Yerleşik Aşama: Görüntünün unsurları yerinde ve işlemektedir. Bununla birlikte, kaynakların göreceli tahsisine ilişkin iyi düşünülmüş bir değerlendirme yoktur. Bu yöndeki göreceli yatırımla ilgili çok az ödünleşim kararı alınmıştır. Ancak görünüş, işlevsel ve tanımlanmıştır.

• Stratejik Aşama: Bu aşamada, yönün hangi göstergelerinin önemli olduğu ve belirli bir organizasyon veya devlet için hangilerinin daha az önemli olduğu konusunda seçimler yapılmıştır. Stratejik aşama, bu seçimlerin devletin veya kuruluşun özel koşullarına bağlı olarak yapıldığı gerçeğini yansıtmaktadır.

• Dinamik Aşama: Bu aşamada, tehdit ortamının teknolojik karmaşıklığı, küresel çatışma veya bir endişe alanındaki önemli bir değişiklik (siber suç veya gizlilik vd.) gibi hâkim durumlara bağlı olarak stratejiyi değiştirmek için açık mekanizmaları vardır. Dinamik kuruluşlar, stratejileri adım adım değiştirmek

[169] "Cybersecurity Risks, Progress, and the Way Forward in Latin America and Caribbean", *2020 Cybersecurity Report*, s. 40, [www.cybersecurityobservatory.org] (er. tar. 09.05.2021).

için yöntemler geliştirmektedirler. Hızlı karar verme, kaynakların yeniden tahsisi ve değişen çevreye sürekli uyum sağlama bu aşamanın özellikleridir. CMM, bir ülkenin alınan önlemlere (veya eylemsizliğe) bağlı olarak, bir ülkenin iyileştirebileceği veya olumsuz duruma düşebileceği mevcut siber güvenlik kapasitesini inceleyerek bu aşamalara göre ülkeyi kıyaslamaktadır.

Tablo 4:[170] Siber Güvenlik Kapasite Olgunluk Modelinin Beş Boyutu

BOYUT 1 *Siber Güvenlik Politikası ve Stratejisi*	**B.1.1.** Ulusal Siber Güvenlik Stratejisi **B.1.2.** Olay Müdahale **B.1.3.** Kritik Altyapı (CI- Critical Infrastructure) Koruması **B.1.4.** Kriz Yönetimi **B.1.5.** Siber Savunma **B.1.6.** İletişim Yedekliliği (Communications Redundancy)
BOYUT 2 *Siber Kültür ve Toplum*	**B.2.1.** Siber Güvenlik Zihniyeti **B.2.2.** İnternette Güven **B.2.3.** Çevrimiçi Kişisel Bilgilerin Korunması Hakkında Kullanıcı Anlayışı **B.2.4.** Raporlama Mekanizmaları **B.2.5.** İletişim ve Sosyal Medya
BOYUT 3 *Eğitim, Öğretim ve Beceriler*	**B.3.1.** Farkındalık Yaratma **B.3.2.** Eğitim Çerçevesi **B.3.3.** Mesleki Eğitim Çerçevesi
BOYUT 4 *Yasal ve Düzenleyici Çerçeveler*	**B.4.1.** Yasal Çerçeveler **B.4.2.** Ceza adalet sistemi **B.4.3.** Siber Suçlarla Mücadelede Resmi ve Gayri Resmi İş birliği Çerçeveleri
BOYUT 5 *Standartlar, Organizasyonlar ve Teknolojiler*	**B.5.1.** Standartlara Uyum **B.5.2.** İnternet Altyapısı Esnekliği **B.5.3.** Yazılım Kalitesi **B.5.4.** Teknik Güvenlik Kontrolleri **B.5.5.** Kriptografik Kontroller **B.5.6.** Siber Güvenlik Pazarı **B.5.7.** Sorumlu İfşa (Responsible Disclosure)

Tablo 4'e göre olgunluk seviyelerinin değerlendirilmesi, siber güvenliğin temel ve belirli yönlerine karşılık gelen beş boyutla özdeşleşmiştir: (i) Siber Güvenlik Politikası ve Stratejisi; (ii) Siber Kültür ve Toplum; (iii) Eğitim, Öğretim ve Beceriler; (iv) Yasal ve Düzenleyici Çerçeveler; (v) Standartlar,

[170] "Cybersecurity Risks, Progress, and the Way Forward in…", s. 41-42.

Organizasyonlar ve Teknolojiler. Bunlar ayrıca, her boyutta siber güvenlik kapasitesine sahip olmanın ne anlama geldiğini tanımlayan ve olgunluğun nasıl artırılacağını gösteren bir dizi faktöre ayrılmıştır. Her ülkenin siber güvenlik görünüşü beş boyuta göre ilgili olgunluk düzeylerini listeleyen bir özet tabloyla açıklanmaktadır. Yukarıdaki tablo, boyutları oluşturan faktörlerin ayrıntılarını vermektedir.[171]

Tablo 5:[172] Küresel İnovasyon Endeksi, İnovasyon Çıktı Alt-Endeksi Sıralaması 2016-2020

Ülke	2016	2017	2018	2019	2020
Türkiye	42	43	50	49	53
İngiltere	3	5	4	4	3

Küresel İnovasyon Endeksi (GII), INSEAD (Institut Européen d'Administration des Affaires veya Avrupa İşletme Enstitüsü), Cornell Üniversitesi ve Dünya Fikri Mülkiyet Örgütü (WIPO) ve ortakları tarafından oluşturulan küresel bir endekstir. GII, mevcut ABD doları cinsinden dünya nüfusunun %90'ından fazlasını ve dünya GSYİH'sinin (Gayri Safi Yurtiçi Hâsıla) %95'inden fazlasını temsil eden yüz yirmiden fazla ülke için ayrıntılı ölçümler sağlamaktadır. İnovasyon Çıktıları Alt Endeksi iki çıktı sütunundan oluşmaktadır: 1. Bilgi ve teknoloji çıktıları, 2. Yaratıcı çıktılar.

Tablo 5'te siber güvenlik pazarında küresel paya sahip İngiltere ve Türkiye'nin GII puanları, 2016-2020 yılları arası puanları sırasına göre gösterilmektedir.[173]

Siber güvenlik sektöründe baskın olmak ile GII puanları arasında bir ilişki olmasa da Türkiye'nin siber güvenlik sektöründeki yeniliklerden faydalanabilmesi ve yararlanabilmesi için ilk 20'ye girme taahhüdüne sahip olması gerekmektedir. Stratejik belgeler hiyerarşisinde, siber güvenlik stratejileri, ulusal güvenlik veya savunma stratejilerinin bir parçasıdır ve siber güvenliğin bir bütün olarak toplum üzerindeki her şeyi kapsayan etkisi nedeniyle diğer birçok kurumun stratejileriyle bağlantılıdır. Burada alt başlıklar halinde bazı ülkelerin siber güvenlik politikaları ve hükümetlerin aldığı önlemlere yer verilmiştir.

[171] "Cybersecurity Risks, Progress, and the Way Forward…", s. 41-42.
[172] Global Innovation Index, "Innovation Output Sub-Index Rankings", [https://www.globalinnovationindex.org/Home] (er. tar. 30.05.2021).
[173] Global Innovation Index, "Innovation Output Sub-Index Rankings".

Verilen bilgiler ışığında ülkelerin ve bölgelerin siber güvenlik stratejilerine ve siber politika hedeflerinin uygulanmasında önemli olan kurumlara genel bir bakış sağlayacaktır.

2.3.1. Amerika Birleşik Devletleri (ABD) Örneği

ABD'de güvenlik sistemlerinin bilgisayar cihazlarına ve bilgi sistemlerine entegrasyonu, ulusal güvenliklerinin korunmasına büyük ölçüde yardımcı olmuş ve bu durum Amerikan refahını da artırmıştır. Amerika'da siber güvenlik, ulusal güvenlik sistemleri ve ekonomisine, toplumun savunma sistemlerine yönelik yapılan çabaların sonucu olarak gelişmiştir.

ABD'de siber güvenlik, yüzeysel olarak teknik bir konu olmasına rağmen, ekonomik ve politik bir sorun olduğu konusunda da artan bir görüş vardır. Amerika'da ileri teknolojik sistemlerin uygulanması sonucu, sürdürülebilirlik ile üretimini nispeten artırmıştır. ABD merkezli kuruluşlar, siber koruma cihazlarının uygulanması, verilerinin ve kimlik bilgilerinin yeterli şekilde korunmasıyla pazarlardaki tüketicilerin güvenliğini sağlamıştır. Bu tür eylemler aracılığıyla, Amerikan hükümet sistemleri ve kuruluşları, verilerine yerleştirilen güvenlik ölçümleri aracılığıyla müşterilerine hesap verebilirlik ve güvenilirlik hususlarını güvence altına almıştır.

Amerikan temel siber güvenlik çıkarları aşağıdaki üç yönü içermektedir:[174]

İlk olarak, temel altyapının güvenliği. Amerikan ekonomik, politik ve askeri operasyonları büyük ölçüde bir web ağına bağlıdır. Bu nedenle finans, telekomünikasyon, enerji, ulaşım, su temini ve acil servis tesislerinin siber terörizm ve diğer siber saldırılardan korunması hayati bir ulusal çıkar haline gelmektedir. ABD'nin 2011 yılı başlarında eğitim, istihbarat ve komuta kontrolü gibi ABD askeri operasyonlarını destekleyen düzinelerce başka ülkede işletilen on beş bin ağı ve yedi milyon bilgisayarı vardır. Bu sayı bugün ABD'de çok daha yüksektir. Bu, ABD'nin siber güvenlik endişelerine diğer ülkelere göre daha duyarlı olduğunun göstergesidir.

İkinci olarak, diğer ülkelerin ağ sistemlerine erişim de dâhil olmak üzere siber alanda hareket özgürlüğünün olmasıdır. Örneğin, Ulusal Güvenlik Ajansı'nın "Prism Projesi"[175], tüm dünyada birçok ülkenin telekomünikasyon ve ağ sistemlerinin verilerini izlemekte ve bu verileri toplamaktadır. ABD, bu tür

[174] Cuihong Cai (2016). "Global Cybersecurity Environment: Perspectives of the US and China in Comparison", *Securing CyberSpace International and Asian Perspectives,* (Ed. Cherian Samuel ve Munish Sharma), New Delhi: Pentagon, ss. 328-329.

[175] Prism Projesi sayfa 86'da detaylı olarak bahsedilmektedir.

faaliyetlerin kendi ulusal mevzuatına uygun olduğunu ve yasal ulusal çıkarlarını korumanın özüyle terörle savaştığını savunmuştur.

Üçüncü olarak, ticari ve teknik sırların güvenliğidir. İnternetin anonim bir ortam olması ve bağlanabilir olması, veri ve bilgi hırsızlığı için kolaylık sağlamaktadır. Amerikan işletmelerinin siber bilgi hırsızlığı nedeniyle her yıl yüz milyarlarca ABD doları zarara uğrattığı söylenmektedir. Bu nedenle fikri mülkiyet haklarını, teknik patentleri ve ticari sırları korumak, ABD'nin önemli bir siber güvenlik çıkarı haline gelmektedir. Siber alandaki bu temel ulusal çıkarlara dayalı olarak ABD, önleyici bir siber güvenlik stratejisi uygulamaktadır. Dünyadaki lider konumunu desteklemek için siber caydırıcılığa ulaşmayı ve önleyici siber alan stratejisi yoluyla siber alanda baskın pozisyon sağlamayı hedeflemektedir.

2011 yılında ABD Savunma Bakanlığı tarafından yayınlanan ilk Siber Uzay Operasyon Stratejisi'nde beş boyut önerilmiştir. Beş boyutun ilk ikisi özellikle önleyici siber alan stratejisini yansıtmıştır. İlk olarak siber alan, kara, deniz, hava ve alan ile "operasyon sahası" olarak listelenmiştir. Siber alan ilk kez askeri harekât kategorisine dâhil edilmiştir. İkincisi, Amerikan ağ sistemi üzerindeki işgali ve diğer düşmanca eylemleri daha etkili bir şekilde önlemek ve saldırmak için pasif savunma, aktif savunmayla yer değiştirmiştir. ABD, siber alanı bir savaş alanı olarak almayı öneren ilk ülkedir. Siber Komutanlık ve siber savaş uygulamasını ilk gerçekleştiren ülke olmuştur.[176]

Dünyanın en büyük iki ekonomik gücü olan Çin ve Amerika Birleşik Devletleri, ekonomik üretkenlikleri, sosyal geçim kaynakları ve ulusal güvenlikleri için küresel siber alana bağımlıdır. Hem hükümetler hem de endüstri, bilgi sistemlerinin güvenliği ve güvenilirliği konusunda giderek daha fazla endişe duymaya başlamıştır. "California Üniversitesi Küresel Çatışma ve İş birliği Enstitüsü" ve "ABD Deniz Harp Okulu" yakın zamanda iki çalıştaya destek vermiştir. Bunlar, Çin'deki siber güvenliğin siyasi, ekonomik ve stratejik boyutlarını tartışmak için Çinli ve Batılı bilim adamlarını, politika analistlerini ve bilim adamlarını bir araya getirmiştir. Çalıştaydaki konular araştırma bulguları, endüstriyel düzenleme, kanun yaptırımı, askeri, stratejik yapı, yasal ve düzenleyici çerçeve konularını kapsayan politika sorunları gibi, çok çeşitli konuları kapsamaktadır. Tartışmaların yanı sıra ortak endişeleri de vurgulamaktadırlar.

---

[176] Cuihong Cai (2016). "Global Cybersecurity Environment: Perspectives…", ss. 328-329.

Son yıllarda küresel bilgi sistemlerinin güvenliği ABD-Çin ilişkilerinde tartışmalı bir konu haline gelmiştir. ABD hükümeti, tescilli ekonomik verileri ve hassas ulusal güvenlik bilgilerini hedef alan Çin müdahalelerinin arttığını iddia etmektedir. Aynı zamanda, küresel olarak kötü niyetli faaliyetlerin büyük bir kısmı ABD'de bulunan ana bilgisayarlardan kaynaklanmaktadır. Hem ABD Savunma Bakanlığı hem de Çin Halk Kurtuluş Ordusu (PLA), siber alanı yeni bir çatışma alanı olarak görmekte ve ihtiyatla bakmaktadırlar.[177]

2.3.2. Çin Örneği

Amerika Birleşik Devletleri'ndeki popüler algının aksine, Çin'in siber güvenliğe yönelik, koordineli bir politika yaklaşımı yoktur. Siyasi güç Çin Komünist Partisi'nde merkezileşmiş olsa da, Çin yönetimi bölgesel ve işlevsel olarak ikiye bölünmüştür. Çin, karmaşık düzenleyici kurumlar, politikaların tutarsız uygulanması ve uyumsuz çıkarlar peşinde koşan kamu ve özel sektör aktörleri ile mücadele etmek zorundadır.

Çinli paydaşlar arasında Komünist Parti, devlet kurumları, akademi, kritik altyapı operatörleri ve endüstriyel tedarikçileri yer almaktadır. Ulusal Bilgi Teknolojileri (BT) geliştirme politikası için Devlet Bilgilendirme Lideri Küçük Grup (SILG) 1993'te kurulmuş ve 2001'de Zhu Rongji altında yeniden oluşturulmuştur. Rutin işleri Devlet Konseyi Bilgilendirme Ofisi (SCITO) tarafından yürütülmüştür. Ancak 2008'de dağılmıştır. Özellikle siber güvenlik için, Ulusal Ağ ve Bilgi Güvenliği Koordinasyonu Küçük Grubu (NNISCSG), SILG altında alt grup olarak 2002 yılında oluşturulmuştur.

NNISCSG organı, Çin'in ulusal sivil siber güvenlik stratejisini ("Belge 27") hazırlamıştır. Bu organ siber güvenlikle ilgili başlıca politikaları ve ulusal stratejileri (ağlar, infosec standartları ve infosec beş yıllık planı) belirlemiştir. On yılın ilk bölümünde strateji oluşturma ve politika planlamasını tamamladıktan sonra, bu organ 2008'de dağılmış ve 2009'da yeniden oluşmuştur. Ancak o zamandan beri halka açık bir toplantı kaydı yoktur.[178]

Kamu Güvenliği Bakanlığı, siber suçlardan ve kritik altyapı korumasından sorumludur. Ülke çapında araştırma laboratuvarları ağına sahiptir. Sanayi ve Bilgi Teknolojileri Bakanlığı (MIIT), bir bilgi güvenliği koordinasyon bölümüne

[177] Jon Lindsay (2012 Raporu). "China and Cybersecurity: Political, Economic, and Strategic Dimensions", *IGCC Workshop Report on China and Cybersecurity*, San Diego: University of California, s. 1.

[178] J. Lindsay (2012 Report). "China and Cybersecurity: Political, Economic…", s. 1-4.

sahiptir ve telekom ve internet güvenliğinden sorumludur. Çin'in sivil siber güvenlik seçkinleri, profesyonel, teknik açıdan bilgili bireylerden oluşan bir gruptur. Siber güvenlik görevlilerinin "birinci nesli", Çin Mühendislik Akademisi (CAE) akademisyenleri ve Çin Bilim Akademisi (CAS) üyeleri tarafından çokça temsil edilmektedir. Mevcut birçok yetkili, bu kıdemli akademisyenlerin/yetkililerin vesayeti altındadır. [179]

Çin'in 2003 yılında yayınlanan ve başlangıçta sınıflandırılan ancak daha sonra daha geniş çapta ilan edilen sivil ulusal siber güvenlik stratejisi, "Belge 27: Bilgi Güvenliği Güvencesi Çalışmasını Güçlendirmeye Yönelik Görüşler" olarak bilinmektedir. "Aktif savunma" ilkesini benimsemekte ve kritik altyapı koruması, kriptografi, yerli inovasyon, yetenek geliştirme, liderlik ve finansman için politika temelleri belirlemektedir. 2008'de dağılması, Çin'in sivil siber güvenlik politikası arenasında "kaosa" yol açmıştır.[180]

Çin'in yayınlanan bir değerlendirme raporuna göre, 2011 yılında, Çin'de her gün yaklaşık sekiz milyar beş yüz otuz bir milyon bilgisayar, günlük ağa bağlı bilgisayarların yüzde 5,7'sini oluşturan ve 2010 yılına göre yüzde 48'lik bir büyüme oranına ulaşan zararlı yazılım ve programların saldırısına uğramıştır. Bir banka web sitesi örneği olan Yazılım Test Merkezi, en düşük puan olan bir değerlendirme anketinde sadece 31,98 puan (tam not 100 puan) almıştır. Başka bir anket, iki bin beş yüz kişinin yüzde 60'ının kişisel bilgilerinin çalındığını göstermiştir. Yüzde 66'dan fazlası yasa dışı davranışlarla mücadele çabalarını yoğunlaştırmak gerektiği konusunda hemfikir olmuştur. Buna göre Çin'in internet bilgi güvenliğindeki durumunun oldukça önemli olduğu, internet ortamları altında bilgi sızmasının ciddi bir mesele olduğu bir gerçektir. Bu nedenle mahremiyetin ve kişisel verilerin korunması, güçlendirilmesi gerektiği konusuna önem verilmiştir.

Çin, en fazla ağ kullanıcısına sahip olan ülkelerin başında gelmektedir. Çin, dünyanın en büyük e-ticaret pazarına dönüşmüştür. Siber alanın istikrarlı ağ bağlantılarını korumak, Çin'in ekonomik kalkınmayı ve sosyal ilerlemeyi teşvik etmesine, uluslararası rekabet gücünü güçlendirmesine ve yeni stratejik fırsatları artırmasına yardımcı olmaktadır. Ancak, ABD ve bazı Batılı ülkelerle karşılaştırıldığında, Çin'de ağ teknikleri, ağ ürünü rekabet gücü ve ağ uygulamalarının araştırma ve geliştirme (Ar-Ge) kapasitesi hala zayıftır.

---

[179] J. Lindsay (2012 Report). "China and Cybersecurity: Political, Economic…", s. 6.
[180] J. Lindsay (2012 Report). "China and Cybersecurity: Political, Economic…", s. 6-7.

Çin'in karşı karşıya olduğu uluslararası siber güvenlik baskılarının iki temel teşvik edici faktörü vardır: Snowden'in ortaya çıkardığı Prism[181] projesi ve yeni teknolojinin hızla gelişmesi. Prism projesinin yayınlanması, AB dâhil her ülkenin, ABD'nin teknik avantajlarını kötüye kullanma yeteneği konusunda önceden var olan güvenlik endişesini tetiklemiştir. Çin için 2013, ulusal siber güvenlik tehditlerinin daha net hale geldiği başlangıç yılıdır. Bu yıl boyunca, Prism projesine ek olarak, Stuxnet virüsü hakkında sonraki derinlemesine raporların yanı sıra Doğu ve Kuzey Afrika'dan Güney Amerika'ya yayılan kitlesel gösteriler, ülkenin siber alanda büyük zorlukla karşı karşıya olduğunun bir başka kanıtı olmuştur.

Çin'in temel siber güvenlik çıkarları şu özelliğe sahiptir:[182] İnternet, özellikle sosyal medyanın hızla gelişmesiyle birlikte, düşük maliyetli ve yüksek verimli bir bilgi yayma platformu olmasının yanı sıra siber kamuoyunun da büyük etki alanı olmaktadır. Çin, sanayileşmiş bir toplum olma yolunda geçiş aşamasındadır. Bu süreçte yeni ve eski toplumsal çelişkiler iç içedir. Bu nedenle Çin Hükümeti, siber kamuoyunun sosyal ve politik istikrarı üzerindeki olumsuz etkilerinden kaçınma perspektifinden siber alanı uygun şekilde yönetmesi gerekmektedir. Bu nedenle, Çin örneğinde en büyük siber tehdit, onun sosyal ve politik istikrarını etkileyen bir faktördür.

- Siber alanda herhangi bir hükümet karşıtı veya anti-sosyal faaliyet;
- Toplumu istikrarsızlaştıran söz ve eylemlerin yayılması;
- Etnik nefreti ve terörizmi teşvik eden siber alan faaliyetleri;

[181] Prism, Amerika Ulusal Güvenlik Ajansı'nın (NSA) çeşitli Amerikan internet şirketlerinden internet iletişim verilerinin topladığı programın kod adıdır. 2008 tarihli Amerikan FISA Değişiklik Yasası'nın 702. Bölümü uyarınca Google gibi internet şirketlerine yapılan taleplere dayalı olarak depolanmış internet iletişim verilerini toplamıştır. Program, Dış İstihbarat Gözetim Yasası (FISA) uyarınca ABD Dış İstihbarat Gözetim Mahkemesi'nin (FISA Mahkemesi veya FISC) denetimi altında yürütülmüştür. Prism projesi NSA yüklenicisi Edward Snowden tarafından kamuoyuna sızdırılmış ve kitlesel veri toplama kapsamının halkın bildiğinden çok daha büyük olduğu konusunda uyarmıştır. Açıklamalar The Guardian ve The Washington Post tarafından 6 Haziran 2013 tarihinde yayınlanmıştır. ABD hükümet yetkilileri, Guardian ve Washington Post'da PRISM'e yönelik eleştirilere itiraz etmişlerdir ve bu programı, izinsiz olarak yerel hedeflerde kullanılamayacağını iddia ederek savunmuşlardır. Detaylı bilgi için bkz. "PRISM (surveillance program)", ss. 1-24. [https://www.sindark.com/genre/PRISM%20(surveillance%20program).pdf] (er. tar. 1.10.2022).

[182] Cuihong Cai (2016). "Global Cybersecurity Environment: Perspectives…", s. 328-329.

• Her türlü yıkım, bölünme veya sabotaj eyleminin planlanması, organizasyonu ve uygulanması;

• Ağ üzerinden Çin'in toprak bütünlüğünü ve siyasi güç hedefleyen şiddetli ayrılıkçı terör saldırıları ve bilgi ağına yönelik kamuoyu saldırıları, Çin rejiminin konsolidasyonunu, siyasi sistemin istikrarını ve tüm halkların birlik ve uyumunu baltalayabilecek eylemler, diğer eşdeğer eylemlerle birlikte, ulusal güvenliğe yönelik tehditlerin birincil kategorisine girmektedir.[183]

Çin'in kendi sansür altyapısı büyük ölçüde düzenli olduğundan, ülke yurtdışında bir filtreleme ve gözetim teknolojileri sağlayıcısı haline gelmiştir. Siber tehditlerin, özellikle de sivil toplumun karşı karşıya olduğu durumların incelenmesinde, Çin hükümetinin insan haklarına ilişkin politika ve uygulamalarının siber güvenlik üzerinde olumsuz bir etkisi olduğu giderek daha açık hale gelmiştir. Siber alanda uzun süredir devam eden insan hakları sorunları yaşanmakta ve siber güvensizlik için önemli bir katalizör oluşturmaktadır. Siber alanı güvence altına alma çabaları, insan hakları endişelerinin daha fazla bütünleştirilmesini ve bunları ele almaya çalışan sivil toplum aktörlerine yönelik tehditlerin analizini gerektirmektedir. Çünkü bu unsurlar Çin hükümetinin kendi kapsamlı siber stratejisinde kilit faktörlerdir.[184]

2.3.3. Doğu Avrupa Ülke Örnekleri (Estonya- Letonya- Litvanya- Polonya- Çek Cumhuriyeti- Macaristan-Ukrayna)

Estonya'nın siber güvenlik konusundaki stratejik belgeleri ve siber güvenliği sürdürmeye yönelik kurumsal yapıları, olgun ve kapsamlı siber güvenlik kültürü ve politikaları ile olmuştur. Bu, tüm siber güvenlik mimarisinin uyumunu sağlayan stratejik planlamanın önde geldiği bir ülkedir. 2007'deki bir dizi kapsamlı bilgisayar korsanlığı saldırısına yanıt olarak, Estonya, 2008'de ulusal siber güvenlik stratejisi benimseyen dünyadaki ilk ülkelerden birisi olmuştur. Estonya'nın 2007'de karşılaştığı bilgisayar korsanlığı olayı, bir ülkenin dijital altyapısına siyasi amaçlı bir saldırı olarak tespit edilen ilk "siber savaş" olarak adlandırılmıştır. Bu "siber savaş"tan sonra Estonya Savunma Bakanlığı ulusal bir siber güvenlik stratejisi hazırlamıştır. Estonya, BİT kullanımını ve

[183] Cuihong Cai (2016). "Global Cybersecurity Environment: Perspectives…", s. 329-330.

[184] J. Lindsay (2012 Raporu). "China and Cybersecurity: Political, Economic…", s. 30.

akıllı çözümlerin geliştirilmesini kolaylaştıran bir ortam yaratmak için Dijital Gündem'i 2020 yılında yayınlamış ve başlatmıştır.[185]

Estonya, Baltık ülkelerinde en kapsamlı kurumsal siber güvenlik politikalarına sahiptir. Estonya'nın genel siber güvenlik politikalarını koordine etme sorumluluğu, 2011 yılında Estonya Savunma Bakanlığı'ndan Ekonomi ve İletişim Bakanlığı'na devredilmiştir. Kurumlar arası bir organ olarak, Estonya'nın Siber Güvenlik Hükümeti Güvenlik Komitesi, kurumlar arası iş birliği ve ülkenin siber güvenlik stratejisi hedeflerinin uygulanmasını denetlemek için politika ve stratejiler belirlemektedir. Savunma Bakanlığı, ulusal savunma alanında siber savunma için koordinasyon makamıdır. 2008'den bu yana, Estonya savunma kuvvetleri, NATO'nun ve ulusların siber savunma yeteneklerini geliştirmeye odaklanan uluslararası bir askeri organizasyon olan NATO Siber Savunma Merkezi'ne de ev sahipliği yapmaktadır.[186]

Letonya'nın 2014-2018 Siber Güvenlik Stratejisi 2014 yılında kabul edilmiştir. Strateji, Letonya siber alandaki BİT güvenlik olaylarını vurgulamıştır. Ülkenin gelecekte artan siber güvenlik risklerine maruz kalabileceğini belirlemiştir. Strateji aynı zamanda devletin, belediye kurumlarının ve kamunun, elektronik iletişim hizmetleri sağlayıcıları ile kritik BİT altyapısının denetçilerinin temel güvenlik gereksinimlerini belirleyen Bilgi Teknolojilerinin Güvenliği Yasasına da hitap etmektedir. Her iki belge de kritik altyapı ve kamu hizmetlerine öncelik veren Letonya'nın siber güvenliğinin ve ulusal güvenliğinin korunmasına yönelik bütünleşmiş bir yaklaşımı vardır. Letonya Ulusal Bilgi Teknolojisi Güvenlik Konseyi, ulusal siber güvenlik politikalarının geliştirilmesini ve politikaların amaç ve önlemlerinin uygulanmasını koordine etmektedir. Konsey, kamu ve özel sektör arasında bilgi alışverişi ve iş birliği için merkezi ulusal otoritedir. Savunma Bakanlığı, bilgi teknolojisi güvenliği, siber alanı koruma politikalarının geliştirilmesini ve uygulanmasını koordine etmektedir. Letonya'nın siber güvenlik politikalarını da uygulayan diğer bakanlıklar, CERT gibi kuruluşları da vardır.[187]

Litvanya, siber güvenlikle ilgilenen ilk kurumları oluşturmuştur. Siber güvenlikle ilgili kapsamlı bir yasayı yakın zamanda çıkarmıştır. Litvanya, 2011 yılında kapsamlı bir siber güvenlik stratejisi yayınlamış, ancak uygulanmasına

[185] Detaylı bilgi için bkz. 2013 yılı Estonya için 2020 yılı Digital Agenda.

[186] Dusko Tomic, Eldar Saljic ve Danilo Cupic (2018). "Cybersecurity Policies of East European Countries", (Ed. E. Carayannis vd.), NY: Springer International Publishing AG, *Handbook of Cyber-Development, Cyber-Democracy and Cyber-Defense*, s. 5-6.

[187] D. Tomic, E. Saljic ve D. Cupic (2018). "Cybersecurity Policies of East European,,,", s. 6.

ilişkin bilgiler sınırlı kalmıştır. Bununla birlikte, Litvanya parlamentosu, siber güvenliği ulusal çıkarların önceliği ilan eden bir ulusal güvenlik stratejisini onaylamıştır. Litvanya'nın siber alanının güvenliğini sağlamak için, Litvanya hükümeti 2011-2019 için Elektronik Bilgi Güvenliği Geliştirme Programını onaylamıştır.

Programın üç ana hedefi vardır: (1) devlete ait bilgi kaynaklarının güvenliğini güçlendirmek, (2) kritik bilgi altyapısının verimli bir şekilde çalışmasını sağlamak, (3) Litvanya vatandaşlarının, sakinlerinin ve ülkede kalan kişilerin siber güvenliğini sağlamak. Bu hedefler 2014 yılında onaylanan Litvanya siber güvenlik yasasına taşınmış ve bu yasa tarafından içeriği geliştirilmiştir. Bu yasanın önemli sonuçları arasında ulusal siber güvenlik politikalarının koordinasyonunun Millî Savunma Bakanlığı'na devredilmesi, yeni bir operasyonel Ulusal Güvenlik Konseyi'nin kurulması yer almıştır. Siber güvenlik stratejisi, kamu-özel sektör ortaklıklarının değerini ve ihtiyacını kabul etmektedir. Ancak henüz resmi veya sistematik bir iş birliği mevcut değildir.[188] 2018 ve 2021 yıllarında Ulusal Siber Güvenlik Strateji belgeleri yayınlamıştır.[189]

Polonya, siber güvenlik stratejisi yayınlamış ve uygulamıştır. Siber güvenlik, Polonya'nın ulusal güvenlik çabalarının ayrılmaz bir parçası haline gelmiştir. Bu, diğer ulusal stratejik belgelerinde sıklıkla bahsedilmektedir. Polonya stratejik belgelerindeki siber güvenlik konusuna ilk olarak 2007 yılında Polonya Cumhuriyeti Ulusal Güvenlik Stratejisi'nde değinmiştir. Belge, siber güvenlik ile ülkenin iyi çalışma yeteneği arasında doğrudan bir ilişki olduğunu belirtmiştir. Daha sonra, Polonya Cumhuriyeti Ulusal Güvenlik Sisteminin Geliştirilmesi Stratejisi 2011-2022, Polonya'daki siber alan koruması ile ilgili konuları detaylandırmış ve geliştirmiştir. Ancak, siber güvenliğe adanan ilk belge olan Siber Uzay Koruma Politikası 2013 yılına kadar yayınlanmamıştır. 2015 yılında Polonya Ulusal Güvenlik Bürosu bir siber güvenlik doktrini yayınlamıştır. Belge siber alanda ulusal güvenliği geliştirmek için tamamlanması gereken çalışmaları da ortaya koymuştur. Doktrin devlet kurumlarının, özellikle de güvenlik kurumları, silahlı kuvvetler, özel sektör ve STK'lar için görevlerin haritasını çıkarmıştır. Ulusal Güvenlik Bürosu, Yönetim ve Sayısallaştırma Bakanlığı, İç Güvenlik Ajansı ve siber güvenlik hedeflerine ulaşmaktan sorumlu CERT ile birlikte ana varlık olarak işlev görmektedir.[190]

[188] D. Tomic, E. Saljic ve D. Cupic (2018). "Cybersecurity Policies of East European,,,", s. 7.

[189] Lithuania (2018). *National Cyber Security Strategy*; Lithuania (2021). *Key Trends and Statistics of the National Cyber Security Status of Lithuania*.

[190] D. Tomic, E. Saljic ve D. Cupic (2018). "Cybersecurity Policies of East European,,,", s. 8.

2005 yılında onaylanan Çek Ulusal Bilgi Güvenliği Stratejisi, Çek Cumhuriyeti'nin ulusal siber alanını düzenlemeye yönelik ilk girişimidir. 2011 yılında Ulusal Güvenlik Stratejisi, siber güvenliği Çek hükümetinin ana önceliklerinden biri olarak tanımlamış ve siber tehditleri bölgesel çatışmalar, terörizm ve kitle imha silahlarıyla aynı güvenlik tehdidi düzeyine yerleştirmiştir. Çek Cumhuriyeti, 2011-2015 için siber güvenlik stratejisini ve eylem planını onaylamıştır. Strateji, öncelikle Çek Cumhuriyeti'ndeki BİT sistemlerini korumayı ve siber saldırıların neden olduğu hasarı azaltmayı amaçlamıştır. 2015 yılında Çek hükümeti, 2015-2020 için güncellenmiş ulusal siber güvenlik stratejisini onaylamıştır. On yılın ikinci yarısına yönelik bu strateji, mümkün olan en yüksek siber güvenlik seviyesine ulaşmak için kapsamlı bir dizi önlem içermektedir. Çek Cumhuriyeti'nde sivil kurumlar siber güvenlik politikasını uygulamakla görevlidir. Ulusal siber güvenliğin genel sorumluluğu, ülkenin Ulusal Güvenlik Otoritesine aittir. Ulusal Güvenlik Otoritesi bünyesindeki bir kurum olan Ulusal Siber Güvenlik Merkezi, ülkenin ulusal ve uluslararası siber alanda erken uyarı sisteminin bir parçasıdır. Ayrıca, İçişleri Bakanlığı siber güvenlik konularını siyasi düzeyde desteklerken, Savunma Bakanlığı siber güvenlik konularını yalnızca NATO ile iş birliği içerisinde ele almaktadır.[191]

Slovakya, 2009-2013 yılları arasında Ulusal Bilgi Güvenliği Stratejisini (NSIS) kabul etmiştir. Slovak Cumhuriyeti, 2008 yılında siber güvenlik için yasal bir çerçeve geliştirmiştir. Strateji, Slovakya'nın sınıflandırılmamış kamu yönetimi bilgilerinin güvenliğini sağlamaktan sorumlu kurumu olan Maliye Bakanlığı tarafından hazırlanmıştır. 2012 yılında Slovakya Ulusal Siber Güvenlik Stratejisini başlatmıştır. Karşılıklı iletişim, bilgi güvenliği konusunda stratejik ve teknik materyaller hazırlayan, danışmanlık ve koordinasyon rolü üstlenen Maliye Bakanlığı Bilgi Güvenliği Komitesi tarafından sağlanmaktadır. Bazı özel konular Güvenlik Konseyi, İçişleri Bakanlığı ve Savunma Bakanlığı tarafından denetlenmektedir. Slovakya Savunma Bakanlığı'nın ulusal siber güvenlik yönetiminde doğrudan bir rolü yoktur.[192]

2013 yılında **Macaristan**, siber alanda ülkenin egemenliğini korumanın ulusal bir çıkar olduğunu açıkça belirten bir ulusal siber güvenlik stratejisi yayınlamıştır. Siber alanda ortaya çıkan tehdit ve saldırıların müttefik iş birliği gerektiren bir düzeye gelebileceğinin farkında olmuştur. Macaristan'da siber bağlantılı politikaların koordinasyonundan ve uygulanmasından sorumlu ana

[191] D. Tomic, E. Saljic ve D. Cupic (2018). "Cybersecurity Policies of East European,,,", s. 8.
[192] D. Tomic, E. Saljic ve D. Cupic (2018). "Cybersecurity Policies of East European,,,", s. 9.

kurum Ulusal Siber Güvenlik Koordinasyon Konseyi'dir. Siber güvenlikle görevli ek kurumlar; Siber Güvenlik Kurumu (Ulusal Kalkınma Bakanlığı bünyesinde bir kurum), Ulusal Güvenlik Ofisi, Kamu Yönetimi, Adalet Bakanlığı ve CERT.[193]

Ukrayna, son yıllarda kritik altyapısına yönelik büyük çaplı saldırılara yanıt olarak 2016 yılında Ulusal Siber Güvenlik Stratejisini benimsemiş ve uygulamıştır. 2016 yılında Ulusal Siber Güvenlik Koordinasyon Merkezi'nin kurulması ve siber suç mevzuatının Budapeşte Sözleşmesi gerekliliklerini ve özellikle internet servis sağlayıcıları üzerindeki en iyi uygulamaları karşılayacak şekilde önerilen güncellemesi, ülkenin siber direncini artırmada iki ana adım olmuştur. Hizmetlerin giderek dijitalleşmesi ve internete duyulan güven, siber alanın evrimini beraberinde getirerek, bilgisayar sistemlerine karşı ve bu sistemler aracılığıyla dünya genelindeki hükümetler için önemli güvenlik sorunlarını da ortaya çıkarmıştır. Ukrayna'da, yerel seçimlerin yapılacağı gün Ukrayna büyük televizyon kanallarına yapılan saldırıların ardından Aralık 2015'te Ukraynalı elektrik şirketlerine yönelik büyük ölçekli siber saldırılarla en belirgin şekilde ortaya çıkmıştır. Tehdit ortamı analizi aynı zamanda diplomatlara, kolluk kuvvetlerine, savunma aktörlerine, devlet kuruluşlarına, kitle iletişim araçlarına, politikacılara, kamuoyundaki şahsiyetlere yönelik hedefli saldırılara ve "fiziksel" dünyayı etkilemek için internet üzerinden yanlış bilgilendirme kampanyalarına başlamıştır.[194] Bir Çin deyiminin dediği gibi: "Su bir tekneyi taşıyabilirken, onu alabora da edebilir." Başka bir deyişle, bir devlet siber alana yoğun bağımlılığından büyük ölçüde faydalanabilmekte ve bunu yaparken bu ortam aracılığıyla oluşturulan saldırılar, suçlar ve terör eylemleri tarafından alabora olmaya karşı daha savunmasız hale getirebilmektedir. Siber alanı güvence altına alma görevi, modern zamanlarda ulusal güvenlik, kamu güvenliği ve ekonomi için en ciddi zorluklardan biri olarak değerlendirilmektedir.

Rusya'nın Ukrayna'ya yönelik askeri saldırganlığı siber alanda da çeşitli şekillerde kendini göstermiştir. 2022 yılının başından bu yana, Ukraynalı işletmelere, devlet kurumlarına ve diğer kuruluşlara karşı birçok hizmet reddi (DDoS) saldırısı düzenlenmiş ve saldırganların içeriği kendi mesajlarıyla değiştirdiği web sitelerinin tahrifatı yapılmıştır. İşgalin başlangıcından bu yana en kapsamlı saldırı 28 Mart'ta Ukrayna'nın en büyük telekom şirketi

[193] D. Tomic, E. Saljic ve D. Cupic (2018). "Cybersecurity Policies of East European,,,", s. 9.
[194] D. Tomic, E. Saljic ve D. Cupic (2018). "Cybersecurity Policies of East European,,,", s. 10.

olan Ukrtelekom'a yapılmış ve müşterilerin yaklaşık yüzde seksenini saatlerce internetsiz bırakmıştır.

Siber saldırılar çoğunlukla yanlış bilgi yaymak için yapılmıştır. Örneğin, iki yerel yönetimin web siteleri ele geçirilmiş ve Kiev'in teslim olduğuna dair mesajlar yayınlanmıştır. Ukrayna Cumhurbaşkanı Volodymyr Zelensky'nin sahte bir videosu ile güvenliği ihlal edilmiş Ukrayna haber portallarına yayılmıştır.[195] 1 Mart 2022 tarihli kararında Avrupa Parlamentosu, AB'nin siber güvenlik de dâhil olmak üzere Ukrayna'nın savunma kapasitelerini güçlendirmeye katkısını artıracak tüm kararların derhal ve tam olarak uygulanması çağrısında bulunmuştur. Ayrıca Parlamento, AB, NATO ve benzer düşüncedeki diğer ortakları Ukrayna'ya siber güvenlik yardımlarını yoğunlaştırmaya çağırmıştır.[196] Ukrayna-Rusya savaşı nedeniyle siber güvenlik açıkları meydana gelmiş ve saldırılar hem siber alanda hem de uluslararası alanda güvenliğe yönelik derin izler bırakmıştır.

Doğu Avrupa ülkeleri olarak incelenen yedi ülkedeki ulusal siber güvenlik stratejilerine ilişkin bu genel bakış, bölgenin siber güvenlik stratejilerinin kapsamlı hale geldiğini ortaya koymaktadır. Siber güvenlik, ülkelerin nesnelerin nasıl korunması gerektiğine, birincil tehditleri ve riskleri nasıl algıladıklarına, tehdit ve risklerin kaynaklarını nasıl tanımladıklarına göre farklılık göstermektedir. Bu farklılıklara göre ülkeler iki kategoriye ayrılabilmektedir. Siber güvenlik konularını militarize eden ülkeler kategorisine Polonya, Estonya, Litvanya ve bir dereceye kadar Letonya dâhildir. Siber güvenlik söylemini militarize etmiş olan bu ülkeler, belirli referans nesnelerini belirlemede ve bu nesnelerin savunmasını ulusal öncelikler olarak ifade etmede daha kesindir. Bu eğilim, siber güvenliği en yüksek ulusal güvenlik düzeyine yükseltmektedir. BİT ve hükümet bilgi kaynaklarının korunmasına odaklanmaktadır. Polonya, Estonya ve Litvanya, siber güvenlik sorunlarını devletin düzgün işleyişine yönelik tehditler olarak belirleme ve yabancı devletlerden gelen saldırıları bu tür tehditlerin en tehlikeli kaynakları olarak belirleme eğilimindedir.

Slovakya ve Çek Cumhuriyeti'nde uygulananlar gibi bazı stratejiler daha esnek bir yaklaşımı desteklemekte ve siber güvenlik politikasının ekonomik ve kişisel (bireysel) boyutlarını vurgulamaktadır. Ayrıca sivil kurumların siber güvenliği sağlamaktan sorumlu olduğu Çek Cumhuriyeti, Slovakya ve Macaristan ülkeleridir. Bu bağlamda bu ülkelerde siber güvenlik sivil odaklı

[195] Republic of Estonia (2022). "Russian Aggression in Ukraine-is it also a Cyber War?", *Trends and Challenges in Cyber Security*.

[196] European Parlamento (Haziran 2022). "Russia's war on Ukraine: Timeline of Cyber-Attacks", *EPRS*, s. 5.

olarak nitelendirilebilmektedir Askeri kurumlar Estonya, Litvanya, Letonya ve Polonya'da siber güvenlik politikalarını koordine etme ve uygulama konusunda daha aktiftir.[197]

2.3.4. Almanya Örneği

Almanya uzun yıllar boyunca, siber alandaki güvenlik tehditlerinin politik, diplomatik ve askeri yaklaşımlar üzerinden teknolojik kontrolünü vurgulayan, siber güvenliğe yönelik önleyici ve mühendislik bir yaklaşım izlemiştir. Buna göre, teknik odaklı Federal Bilgi Güvenliği Ofisi (BSI), Almanya'nın ulusal siber güvenlik mimarisinde öncü bir rol oynamıştır. Ordu, siber savunma yeteneklerini 2016'da genişletmiş ve yeniden düzenlemiştir. 2016 yılında Almanya hükümeti, ulusal siber savunma mimarisini, devlet ve sanayi arasındaki iş birliğini ve bireysel kullanıcı ajansını güçlendirmeyi amaçlayan üçüncü siber güvenlik stratejisini sunmuştur.

2.3.5. Japonya Örneği

Japonya siber alandaki en büyük devletlerden biridir. 2016 yılında, internet kullanıcılarının sayısı 100 milyonun üzerindedir. Bu sayı vatandaşların yüzde 82,8'ini oluşturmuştur. Bu veri günümüzde çok daha yüksektir. Bu nedenle Japonya'da siber güvenlik, dikkate alınması gereken en önemli konulardan biri haline gelmektedir.[198]

17 Aralık 2013'te yayınlanan Ulusal Güvenlik Stratejisi, siber alanın istikrarını vurgulamaktadır. Ayrıca, ulusal güvenliğe ilişkin temel politikalar olarak "strateji, deniz, uzay, siber alan ve enerji" dâhil olmak üzere ulusal güvenlikle ilgili alanlardaki politikalar için kılavuzlar sunmaktadır. Strateji belgesi "siber alanı korumanın… ulusal güvenliği güvence altına almak için hayati olduğunu" söylemektedir. Japonya, Siber Güvenlik Temel Yasasını 12 Kasım 2014'te kabul etmiştir. Uzay Temel Yasası ve Okyanus Temel Yasası gibi bazı önemli temel yasalar da hemen hemen aynı zamanda kabul edilmiştir.[199] Japonya, gelişmiş bir BT ülkesi olarak siber güvenliği teşvik etmektedir. Japon

[197] D. Tomic, E. Saljic ve D. Cupic (2018). "Cybersecurity Policies of East European,,,", s. 9-10.

[198] Yasuaki Hashimoto (2016). "Cybersecurity Policy in Japan", *Securing CyberSpace International and Asian Perspectives,* (Ed. Cherian Samuel ve Munish Sharma), New Delhi: Pentagon, s. 295.

[199] Siber Güvenlikle ilgili bu temel yasanın ana noktaları hakkında detaylı bilgi için bkz. Yasuaki Hashimoto (2016). "Cybersecurity Policy…", ss. 296-297.

Hükümeti Ulusal Güvenlik Stratejisi, Ulusal Siber Güvenlik Stratejisi, Siber Güvenlik Temel Yasası ve güvenlikle ilgili çeşitli kuruluşlar oluşturmuştur. Daha güvenli siber alan için ikili, çok taraflı, bölgesel ve küresel iş birliği esastır. Japonya bu noktada siber güvenlikle ilgili birçok faaliyet ve sistem geliştirmektedir.

2.3.6. Afrika Örneği

Afrika'nın birçok ülkesi, yirminci yüzyılda sömürgeciliğin sona ermesine tanık olmuştur. Bağımsız devletler, bölgesel ekonomik ve siyasi uyumu, dış politika hedeflerinin ve kalkınma stratejilerinin temel bir bileşeni olarak benimsemeye başlamışlardır. Bölgesel uyum arayışı, iş birliğinin yanı sıra, serbest ticaret ve ortak pazarların gelişimi gibi ekonomik hedeflerin de altını çizmiştir. Bölgesel uyum arayışı, Afrika kıtasını oluşturan beş coğrafi alt bölgede (Güney Afrika, Orta Afrika, Doğu Afrika, Kuzey Afrika ve Batı Afrika) çeşitli bölgesel hükümetler arası kuruluşların kurulmasına yol açmıştır.

Afrika şu anda elli beş egemen devletten oluşmakta (30.2044.049 milyon kilometrekare kara kütlesi) ve bir milyarın üzerinde insan nüfusu ile Asya'dan sonra dünyanın en büyük ve en kalabalık ikinci kıtası olarak sınıflandırılmaktadır. Afrika Birliği ("AU" elli dört üye devlet vardır), Afrika'da önde gelen bölgesel hükümetler arası örgüttür. Fas, AU'ya üye olmayan tek egemen devlettir.

Afrika'da internet kullanıcı nüfusu, olağanüstü oranlarda büyümeye devam etmektedir. İstatistiksel veriler, Afrika'daki internet kullanıcılarının nüfusunun 2000 yılında 4.514.400 milyondan Kasım 2015 yılında 330.965.359 milyona yükseldiği düşünülmektedir. Bu sayı Afrika nüfusunun yaklaşık yüzde 28,6'sını temsil ettiğini göstermektedir. Öngörülebilir gelecekte hala devam eden bu olağanüstü büyüme, Afrika ülkelerinde telekomünikasyon pazarlarının serbestleştirilmesi, mobil ve kablosuz internet teknolojilerinin yaygınlaşması ve geniş bant kapasitesinin artan kullanılabilirliği gibi faktörlerle bağlantılıdır. Bununla birlikte, Afrika devletlerinde internetin yayılması, siber güvenliği güçlendirme ihtiyacına ilişkin ciddi endişeleri de beraberinde getirmiştir. Örneğin, Afrika'daki en büyük internet kullanıcı nüfusuna sahip olan Nijerya'nın siber suçlar nedeniyle yıllık 13 milyar ABD dolarının üzerinde kayıp yaşadığı tahmin edilmektedir. Güney Afrika'da siber suçlar nedeniyle yılda 5,7 milyar dolardan fazla para kaybettiği bildirilmiştir.

Siber güvenliği sağlamak ve siber suç endişelerini gidermek için Afrika'daki hükümetler arası kuruluşların bazıları, siber güvenlik yönetişiminin

bölgeselleşmesini teşvik etmektedir. Ayrıca üye devletlerde siber güvenlik yasalarının uyumlaştırılmasını kolaylaştırmak için bağlayıcı ve bağlayıcı olmayan yasal çerçeveler geliştirmektedir. Alt-bölgesel düzeyde, ECOWAS (Batı Afrika ülkeleri Ekonomik Topluluğu) Ağustos 2011'de Siber Suçlarla Mücadele Yönergesi'ni model olarak kabul ederken, COMESA (Doğu ve Güney Afrika Ortak Pazarı) Ekim 2011'de model olarak Siber Suç Yasası'nı kabul etmiştir. Mart 2012'de Bilgisayar Suçları ve Siber Suçlara İlişkin Model Yasası ve Haziran 2014'te Siber Güvenlik ve Kişisel Verilerin Korunması Sözleşmesi kabul edilmiştir.[200]

Afrika Birliği Sözleşmesi, üye devletlerin kendi ulusal yasalarındaki hükümlerini uygulamalarında, kendi belirledikleri düzenlemelere göre uygulama hakkına sahiptir. Ocak 2016 itibariyle, Afrika kıtasının 55 Eyaletinden 30'u siber güvenlik yasaları, 14'ü ise ulusal siber güvenlik politikaları oluşturmuştur. Öte yandan, 16 Devlet CERT kurmuştur. 2016 yılına kadar 55 Afrika ülkesi arasından siber güvenlik politikası, siber güvenlik yasası ve CERT'i olmayan 21 ülke vardır. Geriye kalan 22 ülkede ise tam siber güvenliğe dair bir çalışma (siber güvenlik yasası, siber güvenlik politikaları, strateji belgeleri, CERT) bulunmamaktadır. 12 ülke siber güvenlik kültürünü geliştirmektedir. Afrika'da siber güvenliğe yönelik ulusal düzenleme yapan ülkeler; Güney Afrika, Bostwana, Fas, Ruanda, Sudan, Tunus, Uganda, Mauritus Cumhuriyeti, Mısır, Gana, Kenya, Nijerya'dır.[201]

Siber güvenlik yönetişimi için geniş çapta kabul gören küresel bir yaklaşımın yokluğu, ikili ve bölgesel yönetişim düzenlemelerinin çoğalmasına yol açmıştır. Bununla birlikte, internetin küresel doğası göz önüne alındığında, ikili ve bölgesel siber güvenlik yönetişim düzenlemeleri, geniş çapta kabul görmüş bir küresel siber güvenlik yönetişim düzenlemesinin yerini almamıştır. İkili ve bölgesel düzenlemeler yargısal sınırlamalarına rağmen, siber güvenlik yönetiminde küresel fikir birliği oluşturmak için platformlar sağlayabilmektedir. Özellikle bölgesel yönetişim düzenlemeleri, yasal uyumun kolaylaştırılması ve üye ülkelerde mümkün olan iş birliğinin teşvik edilmesi için bir temel sağlayabilmektedir. Bu hedeflere ulaşılması, öncelikle bölgesel yönetişim düzenlemesinin nasıl yapılandırıldığına bağlıdır. Üye devletlerin bu tür bir düzenlemeden doğan bağlayıcı yükümlülüklerin yerel uygulamasını zamanında

[200] Uchenna Jerome Orji (2016). "Regionalising Cybersecurity Governance in Africa: an Assessment of Responses", *Securing CyberSpace International and Asian Perspectives,* (Ed. Cherian Samuel ve Munish Sharma), New Delhi: Pentagon, s. 203-215.

[201] Uchenna Jerome Orji (2016). "Regionalising Cybersecurity Governance in Africa…", s. 213.

üstlenme kabiliyeti ve ilgili bölgesel yönetimin kabiliyeti bu hedeflere ulaşmak için diğer hususlardır.

Afrika'da bağlayıcı olmayan model yasaların ve bağlayıcı bölgesel siber güvenlik yasalarının yaygınlaşması, kıtanın siber güvenlik yönündeki farkındalığını artırmaktadır. Bu da güvenli bir küresel bilgi toplumunun gelişimini teşvik etme konusundaki ilgisinin sinyallerini verdiği söylenebilir. Ancak, istenen sonuçların elde edilmesi, vurgulanan konuların ele alınmasına yönelik sürekli bir çaba gerektirecektir.[202] Örneğin ITU belgelerinde beş aşamada incelenen Nijerya'da, yasa ve politika boyutu siber güvenlik sorunlarını incelemektedir. Ancak bu boyutların Nijerya'da iyileştirilmesi gerekmektedir. İnternet servis sağlayıcıları da bir araya gelmeli ve ülkedeki altyapı eksikliğini gidermek için bir yol önermelidir. Afrika'daki ülkeler siber alanı koruyabilirse, bu ülkeler kendi ekonomilerini, politikalarını ve teknolojilerini destekleyebileceklerdir.[203]

2.3.7. İsrail Örneği

İsrail'deki ulusal siber güvenlik stratejisi ve politikası 2000'lerin başında başlamıştır. Dünya çapında ilk örneklerden biri olan İsrail'de merkezi bir kritik altyapı koruması sağlanmıştır. 2002 Karar B/84 yasasında yer alan düzenleme "Ulusal Bilgi Güvenliği Otoritesi" tarafından, ticari, kamu kuruluşları ve kamu hizmetleri için siber güvenlik yönergelerini zorunlu kılmıştır.

Ulusal Bilgi Güvenliği Kurumu tarafından denetlenen kuruluşlar, zorunlu güvenlik talimatlarını finanse etmek ve uygulamakla yükümlüdür. Bu da, Tel Aviv Menkul Kıymetler Borsası'nın (TASE) siber güvenliğin yeniden düzenlenmesi yönündeki isteksizliğini artırmıştır. Ayrıca İsrail'de siber güvenlik politikasının karşı karşıya kaldığı yinelenen zorlukları göstermektedir.[204] Uzmanlar ekibi tarafından hazırlanan "Ulusal Siber Girişim Raporu", 2011 İsrail Siber Güvenlik Stratejisi'ni kabul etmiştir. Ulusal Siber Strateji, İsrail'de siber güvenliği artırmaya çalışırken, uluslararası arenada siber alanın, makro-ekonomik ve stratejik faydalarını da araştırmaktadır. İsrail Ulusal Siber Bürosu (INCB), ulusal siber politika çabalarını koordine etmek ve teşvik etmek için kurulmuştur.

---

[202] Uchenna Jerome Orji (2016). "Regionalising Cybersecurity Governance in Africa…", s. 215.

[203] Detaylı bilgi için bkz. Nwosu John Nwachukwu (2022). "Nigeria Cyber Security Analysis for a Secure Nation", *INOSR Experimental Sciences,* Sayı 8(1), s. 36.

[204] Lior Tabansky ve Isaac Ben Israel (2015). "The Israeli National Cybersecurity Policy Focuses on Critical Infrastructure Protection (CIP)", *Cybersecurity in Israel*, Springer Briefs in Cybersecurity UK: Springer Cham, ss. 35-42.

İsrail siber güvenlik politikası (2014-2015) adımları, Ulusal Siber Güvenlik Otoritesinin (NCSA) kurulmasına yol açan politika tasarımını yeniden düzenlemiştir. İsrail'in ulusal siber güvenlik duruşu, teknik olmayan yönlerden değişmiştir. Ayrıca İsrail Savunma Kuvvetleri'ndeki (IDF) siber güvenlik gelişmeleri, insan sermayesi gelişimi ve doktrinel görüşler gelişmiştir. Yabancı kaynaklar tarafından İsrail'e atfedilen siber saldırılardan Orchard ve Stuxnet Operasyonu, siber güvenliğin sağlanmasında etkinlik, ilişkilendirme ve caydırıcılık zorluklarını göstermektedir. NCSA tasarımı, güvenlik ihtiyaçları ve temel özgürlükler arasındaki gerilimi azaltırken, kapsamlı ulusal siber güvenliği geliştirmektedir. NCSA'yı kurma süreci, çok sayıda yasal, örgütsel ve diğer çabaları içermiştir. Ülke çapında siber güvenlik ve siber güç, BİT sistemlerinin dayanıklılığını artırmak için bilimsel, teknik ve ekonomik becerilerden ziyade karmaşık ahlaki ve organizasyonel gerilimleri azaltmaya bağlıdır.

2.3.8. İsviçre Örneği

İsviçre'nin siber güvenlik politikası iki strateji ile formüle edilmiştir: (1) MELANI[205], siber güvenlikte en önemli oyuncu olmaya devam etmiş ve NCS (İsviçre'nin siber risklere karşı korunması için ulusal strateji) aracılığıyla etkisini daha da genişletmeyi başarmıştır. MELANI'nin yanında, (2) FOCP (CIP) alanında kilit bir sistem haline gelmiş ve "Ulusal Kritik Altyapı Koruması" stratejisinin ana koordinatörü olarak konumlanmıştır. Her iki strateji İsviçre'nin mevcut siber güvenlik yaklaşımını oluşturmakta ve uygulamaktadır. İsviçre siber güvenlik politikasını şekillendiren faktörlerden bazıları şunlar olmuştur:[206]

---

[205] Ulusal Siber Güvenlik Merkezi (NCSC), İsviçre'nin siber güvenlik yetkinlik merkezidir. Bu alanda ilk temas noktası olan merkez, işletmeler, kamu idareleri, eğitim kurumları ve genel halk için siber sorunları ile ilgilenmektedir. İsviçre'nin siber risklere karşı korunmasına yönelik ulusal stratejinin eşgüdümlü uygulanmasından da sorumludur. Federal Yönetimde Siber Risklere Karşı Koruma Yönetmeliği 1 Temmuz 2020'de yürürlüğe girmiştir. NCSC'nin oluşturulması ve genişletilmesi için yasal temel sağlamakta ve ilgili makamların yapısını, görev ve sorumluluklarını düzenlemektedir. Ulusal Bilgisayar Acil Müdahale Ekibi (GovCERT) ile birlikte Bilgi Güvencesi Raporlama ve Analiz Merkezi (MELANI), teknik uzmanlık merkezi olarak NCSC'ye entegre edilmekte ve daha da genişletilmektedir. Detaylı bilgi için bkz. "National Cyber Security Centre (NCSC)-Switzerland", [https://www.cybersecurityintelligence.com/national-cyber-security-centre-ncsc-switzerland-4181.html] (er. tar. 3.10.2022).

[206] Myriam Dunn Cavelty (2014). *Cybersecurity in Switzerland*, NewYork: Springer, s. 73.

• Uluslararası Düzey: MELANI ne kadar uzun süre var olur ve çalışırsa, dışarıdan gelen etkiler o kadar az olmaktadır. MELANI'nin kurulmasından bu yana İsviçre, güçlü bir kamu-özel ortaklıklarına dayanan kendi siber güvenlik kimliği için çalışmaktadır. ABD ve Birleşik Krallık'taki politika gelişmelerinden etkilenmiş olsa da MELANI ve yapısı, siber olayları ele almada oldukça benzersiz bir yol olmuştur.

• Dâhili Düzey: Bu dönemde Federal yönetimde en az iki (potansiyel) fay hattı vardır. MELANI esas olarak özel sektör ile operasyonel olay-tepki konularına odaklanmıştır. Kritik altyapıların "siber olmayan" ve "siber olan" unsurları arasındaki ayrımın çok yapay olduğunu kabul ederek, FOCP'nin görevleri ve MELANI'nin görevleri, İsviçre'de 2012 yılında siber risk stratejisi belgesinde uyumlu hale getirilmiştir.

• İş Düzeyi: MELANI aracılığıyla özel sektörün endişeleri ve istekleri önemlidir.

• Odaklanılan Olaylar: Stuxnet gibi büyük siber olaylar, İsviçre'de küresel siber güvenlik tartışmasını da değiştirmiştir. Her şeyden önce, tartışma askeri-stratejik yönlere daha fazla odaklanmıştır. Ancak, İsviçre toplumu bu eğilimlerden çok fazla etkilenmemiştir. Genel siber hazırlığın düşük olduğu yargısına varılsa da İsviçre siber güvenlik camiasında, kamu-özel ve kamu-kamu ortaklığına dayalı politika yaklaşımının doğru olduğuna dair büyük bir inanç vardır.[207]

Siber güvenlik politikalarının hükümetler tarafından yönetilmesi, bir yandan devam eden sosyo-teknik dönüşümlerin hızlanması, diğer yandan ilgili siyasi tepkilerin değişen dinamikleri tarafından ortaklaşa üretilmesi gibi hususlar, yirmibirinci yüzyılda daha da karmaşık olacağı ve öneminin artacağını göstermektedir. Siber güvenlik ve bu alanda uygulanması gereken politikalar, bu bölümde incelenen bölgeler ve ülkeler için bir öncelik olduğu anlaşılmıştır. Ayrıca diğer ülkeler de dâhil olmak üzere küresel olarak hükümetler ve bilgi güvenliği firmaları için bir temel oluşturmaktadır. Hükümetler bazen siber güvenlik endişelerine küresel bağlamı veya politika tekliflerinin sonuçlarını tam olarak dikkate almadan tepki vermektedirler. Siber güvenlikle ilgili bazı yasalar, düzenlemeler ve diğer gereksinimler, ulusal güvenlik çıkarlarını desteklemek adına çıkarılmıştır.

Tüm şirketler, ticari işlemleri güvenli bir dijital altyapıda kullanmak istemektedir. Altyapının sürekli canlılığını ve sektörlerinin büyümesini sağlamak

[207] M. D. Cavelty (2014). *Cybersecurity…,* s. 73-74.

için teknoloji şirketleri, ürünlerinin ve sistemlerinin DNA'sına güvenlik tasarlama ve yerleştirme konusunda teşvik edilmektedir. Hükümetler sırasıyla ekonomik büyüme, refah, verimlilik ve koruma için güvenli bir küresel dijital altyapı hedeflemektedir. Endüstri ve hükümetler, siber güvenliği artırmak ve doğru politika çerçevesini geliştirmek için birlikte çalışırken, altı yol gösterici ilkeye uymaları gerekmektedir:[208]

- Kamu-özel ortaklıklarından yararlanmak ve mevcut girişimler ve kaynak taahhütleri üzerine inşa etmek;
- Günümüz siber ortamının sınırsız, birbirine bağlı ve küresel doğasını yansıtmak;
- Ortaya çıkan tehditlere, teknolojilere ve iş modellerine hızla uyum sağlayabilmek;
- Etkin risk yönetimine dayalı olmak;
- Kamu bilincini artırmayı amaçlamak;
- Doğrudan kötü aktörlere ve onların tehditlerine karşı siber güvenlik politikaları geliştirmek ve uygulamak.

2.4. Küresel Salgın ve Siber Güvenlik İlişkisi

17 Kasım 2019, korona-virüs pandemisi (COVID-19 salgını) olarak bilinen salgının başlangıç tarihidir.[209] COVID-19 hızla büyümüş ve küresel bir kriz haline gelmiştir. COVID-19 dünyanın birçok ülkesinde yüz milyonlarca vatandaşın toplu karantinaya alınmasına neden olmuştur. Dünya Sağlık Örgütü (WHO), COVID-19 salgınının dünya çapında yaklaşık 172 milyondan fazla insanın bu salgına yakalandığını onaylamıştır. Salgından dolayı, 3.718.683'ten fazla ölüm olduğunu belirtmiştir. Bu vakaların sayısı Türkiye'de 5.282.594 iken İngiltere'de 4.511.673 olmuştur.[210]

COVID-19 dünyaya yayıldıkça, teknoloji odaklı bir toplum için ikincil bir önemli tehdide yol açmıştır. Ayrım gözetmeyen ve hedefli, siber saldırı ve siber suç kampanyasını da beraberinde getirmiştir. Salgın dört yıl sonra beklenen dijital dönüşümün hızlanmasını üç ay gibi bir sürede yaşatmıştır. "Her şeyin dijitalleşmesi" çağına geçiş, profesyonel ve kişisel yaşamları derinden ve

[208] J. Lindsay (2012 Raporu). "China and Cybersecurity: Political, Economic…", s. 14.
[209] UNODC (2020). "COVID-19: Cyber Threat Analysis", *Cybercrime Global Program*.
[210] WHO, "WHO Coronavirus (COVID-19) Dashboard", [https://covid19.who.int/] (er. tar. 06.06.2021).

yeniden şekillendirmiştir. Salgının en yıkıcı ortamında bile, internet ve küresel dijital altyapı temel hizmetlerin sağlanmasını mümkün kılmıştır.

Toplumun tüm düzeylerine ve dünyanın bilinen tüm endüstriyel, ticari ve konut sektörlerine meydan okuyacak küresel bir krize girileceğini düşünmek dahi olanaksızdı. 2020'nin başlarında COVID-19 salgınının neden olduğu kriz, çoğu birey için genellikle görünmeyen veya en iyi ihtimalle zor algılanabilen hayati olarak altyapıya bağımlılığı artırmıştır. Gıda tedarik zincirleri, ulaşım araçları, ödemeler ve finansal işlemler, eğitim faaliyetleri, hükümet prosedürleri, acil servisler, su ve enerji gibi günlük temel ihtiyaçlar, dijital teknolojilere her zamankinden daha bağımlı hale gelen bir teknoloji ile onları siber tehditlere karşı daha duyarlı hale getirmiştir. Özellikle 2021 yılı COVID-19 küresel salgını, BİT temel hizmetlerin sunulmasında toplumlara derinlemesine etki etmiş ve hayatın önemli bir parçası olduğu gerçeğini vurgulamıştır.

COVID-19 salgını, bilgi ve iletişim teknolojisinde internet bağlantısının ve siber güvenliğin genişlemesindeki ilerlemeye karşı düşünme fırsatı sunmaktadır. Kriz sırasında siber alanda artan bağımlılık, toplumların ve ekonomilerin sürekli dönüşümünde ve küresel olarak siber güvenliğin sağlanmasında ileriye dönük dersler çıkarma ihtiyacının altını çizmektedir.

Siber güvenlik politikaları, vatandaşların gizlilik ve erişilebilirliği dâhil olmak üzere dijital alandaki haklarını korumanın yanı sıra dijital teknolojiye olan güvenlerini ve kullanım rahatlığını güçlendirmek için temeldir. Bu modern zaman salgını, kriz zamanlarında beklenilenden fazla yeni zorlukları ortaya çıkarmıştır. Siber saldırıların neden olduğu ekonomik hasarın, bazı ülkelerin yıllık gayri safi yurtiçi hasılasının (GSYİH) yüzde 1'inden fazla olduğu tahmin edilirken, kritik altyapıya yönelik saldırıların yıllık GSYİH'nın yüzde 6'sına ulaşan zararlara neden olduğu düşünülmektedir. COVID-19 salgını ve artan dijitalleşme süreci, bilgi ve iletişim teknolojisindeki dijital alanın güvenlik açıklarını daha da ortaya çıkarmaktadır. Her yıl internete ilk kez bağlanan milyonlarca yeni kullanıcı olmaktadır. Bu da uzun dönemli bilgisayar kullanıcıları olan dijital müşteriler kadar teknoloji meraklısı olmayan yeni müşterilerin kaynaşmasını sağlamaktadır. Bu, yüksek riskli bir ortamı beraberinde getirmektedir. Bu nedenle, birey-toplum ya da devlet sadece bu tür saldırıların hedefi olmakla kalmamakta, önemli bir kaynağı da olmaktadır.

Tarih topluma, bu tehditlere başlangıçta karşı koymanın en etkili yönteminin, kurumsal ve kişisel yaşamın tüm düzeylerine yönelik önlem ve farkındalık olduğunu öğretmiştir. Pandemi, bu konuda geçmişte nadiren görülen yüksek bir zorluğu beraberinde getirmektedir. Pandemi küreseldir ve konumu,

ırkı, etnik kökeni, dini, sosyal kökeni, cinsiyeti, engelliliği, geliri veya diğer herhangi bir statüsü olmaksızın herkesi etkilemektedir.

Küresel salgın, insanların günlük rutinlerini yeni bir gerçekliğe uyarlamak zorunda kalmasıyla dünya çapında kitlesel bozulmaya neden olmuştur: evden çalışma, sosyal etkileşim ve fiziksel aktivite eksikliği ve hazırlıklı olmama korkusu.[211] Bu durumlar birçok kişiyi bunaltabilmekte ve bir saldırının kurbanı olma şansını artırabilecek stres ve endişeye neden olabilmektedir. Ayrıca, çalışma ortamlarındaki ani değişiklik, şirketlerin yeni çalışma yapılarını geliştirmek zorunda kalmasına ve potansiyel olarak birlikte çalışabilirlik adına kurumsal varlıkları eskisinden daha az koruma altına almasına neden olmuştur.

COVID-19 başladığından beri dolandırıcılık ve kötü amaçlı yazılım saldırıların sayısını artırmıştır. Nisan 2020'de Google'ın her gün virüsle ilgili 18 milyon kötü amaçlı yazılım ve kimlik avı e-postasını engellediğini belirtmiştir.[212]

2021 yılı verilerine göre siber suçlular, korona-virüsle ilgili kimlik avı saldırılarıyla küresel pandemiden yararlandıkları şekilde, para ve kişisel bilgileri çalmak için aşıdan yararlanmaya çalışmışlardır. Ekim 2020 ile Ocak 2021 arasında yapılan bir analizde araştırmacılar, bilgisayar korsanlarının hedeflenen kimlik avı saldırılarında aşıyla ilgili e-postaları giderek daha fazla kullandığını vurgulamışlardır. İlaç şirketleri aşıları geliştirmek ve test etmek için acele etmiş, bilgisayar korsanları da oltalama kampanyalarında haber kapsamının yarattığı ivmeden yararlanmak için faydalanmıştır. Bu saldırılar, ekonomik açıdan yüksek talep gören malların (Kişisel Koruma Ekipmanı, koronavirüs test ilaçları vb.) satışını, COVID-19 ile ilgili hisse senetlerine potansiyel olarak yüksek kârlı yatırımları, kamu temsilcilerinin kimliğine bürünmelerini ve yardım konularını hedef almaktadır. Saldırganların, özellikle, pandeminin neden olduğu bozulmadan en iyi şekilde yararlanmaya çalıştıkları belirlenmiştir. Ayrıca, saldırılara karşı koruma sağlamak için çeşitli yönergeler ve öneriler de yayınlanmıştır. Bu yönergeler artan tehdidi azaltmak için zorunludur. Ancak temellerini güçlendirmek için öncelikle başlatılan siber saldırılara ilişkin esas bir anlayış olması gerekmektedir.[213]

---

[211] Harjinder Singh Lallie (vd.) (2021). "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic", *Computers & Security*, Sayı 105, s. 3.

[212] SHI, Fleming (2020). "Threat spotlight: Coronavirus-related phishing", [https://blog.barracuda.com/2020/03/26/threatspotlight-coronavirus-related-phishing] (er. tar. 06.06.2021).

[213] SHI, Fleming (2021). "Threat Spotlight: Vaccine-related phishing", [https://smartermsp.com/threat-spotlight-vaccine-related-phishing/] (er. tar. 06.06.2021).

COVID-19'un toplum üzerindeki etkisi ve enfeksiyon oranları arttıkça, bir yandan işlerin durdurulması neticesinde iş gücü ihtiyacında azalma görülmüştür. Fakat diğer yandan farklı iş alanlarında emek-yoğun işgücüne ihtiyaç, giderek arttığı için olumsuz bir karmaşayı da beraberinde getirmiştir. İş gücü hızla uzaktan çalışmaya geçmekte ve bunu desteklemek için teknolojiye ihtiyaç duymaktadır. Hızlı bir biçimde uzaktan çalışmaya geçiş, BİT altyapı gereksinimlerini ve saldırı yüzeyini değiştirerek önemli etkilere neden olabilmektedir. Bu da genel BİT operasyonlarını desteklemeye veya değişen riske uyum sağlamak için süreçleri ve teknolojileri hızla değiştirmeye neden olmuştur. Potansiyel olarak önemli güvenlik faaliyetlerini kesintiye uğratabilmektedir.[214]

Dünya Ekonomik Forumu'nun 2020 Küresel Riskler Raporu'na göre, kritik altyapı ve veri dolandırıcılığı veya hırsızlığına yönelik siber saldırı riski, meydana gelme olasılığı en yüksek on risk arasında yer almıştır. Bu raporda son COVID-19 riskleri, dijital çalışma modellerinde şu anki ve sürekli geçişi nedeniyle siber saldırıları üçüncü en büyük endişe olarak tanımlamaktadır.[215] Mevcut veriler bu endişeleri desteklemektedir;[216] Siber suç zararlarının 2021 yılına kadar 6 trilyon Amerika dolarına ulaşacağı tahmin edilmiştir. Bu, dünyanın üçüncü büyük ekonomisinin GSYİH'sına denk gelmektedir. Finansal maliyetin yanı sıra, siber suçlar ve siber saldırılar, kullanıcıların dijital ekonomiye olan güvenini zayıflatmaktadır. Bu alanda yapılan anketler, internet erişimine sahip küresel nüfusun yüzde 50'den daha azının teknolojinin hayatlarını iyileştireceğine güvendiğini, veri gizliliğine ilişkin artan ve derin bir güven eksikliğini göstermiştir. Bu eğilimler, son beş yılda BİT kullanımında muazzam bir genişlemeye tanık olan İngiltere ve Türkiye için özellikle geçerlidir. Bu iki ülke dijital ekonomiye doğru daha fazla ilerleme sağlarken, dijital güveni sağlama ihtiyacı da artmıştır. Dijital güvenlik risk yönetimi ve gizlilik koruma protokolleri, artan veri odaklı bir ekonomide hükümetler, özel sektör ve bireysel kullanıcılar tarafından paylaşılan sorumlulukları oluşturmaktadır. Bu salgın, olaylar ve siber saldırılar arasında en iyi şekilde tanımlanabilecek gevşek, doğrudan ve ters bir ilişki olduğunu göstermiştir.

---

[214] "Managing the Impact of COVID-19 on Cyber Security", s. 2, [https://www.pwccn.com/en/issues/cybersecurity-and-privacy/covid-19-impact-mar2020.html] (er. tar. 05.06.2021).

[215] WEF (World Economic Forum). 2020. COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications, [https://www.weforum.org/reports/covid-19-risks-outlook-a-preliminary-mapping-and-its-implications] (09.05.2021).

[216] Cybersecurity Risks, Progress and the Way Forward in Latin America and Caribbean, 2020 Cybersecurity Report, [www.cybersecurityobservatory.org] (er. tar. 9.05.2021), s. 28-29.

Gelecek bölümde Türkiye'nin siber alanlarındaki yasal düzenlemeleri, teknik altyapı, kurumsal altyapı, uluslararası iş birliğini inceleyerek karşılaştırmalı bir analizini sunacaktır. Üçüncü ve Dördüncü Bölüm ülkelerin siber güvenlik politikalarına nasıl başladığı ve bu sürecin nasıl ilerlediği üzerine bir tartışma oluşturacaktır. Ayrıca;

- Ülkelerin internet erişimi ve siber ortamda güvenlik politikalarını nasıl bir süreç içerisinde başlayıp, nasıl stratejik belgeler oluşturma gereği duydukları,
- Siber güvenlik politikası hedeflerinin belirlenme süreçleri ve bu hükümetlerin aldığı önlemler tartışılacak,
- Gelişmişlik modeline göre beş faaliyet kategorisi incelenecek (politika ve strateji; kültür ve toplum; eğitim, öğretim ve beceriler; yasal ve düzenleyici çerçeveler; standartlar, organizasyonlar ve teknolojiler),
- Siber güvenlikle ilgili karar verme süreçlerine değinilecek,
- Türkiye ve İngiltere hükümetlerinin siber güvenlik politikası sorunlarıyla nasıl başa çıktığı ya da nasıl çık(a)madığı tartışılacaktır.

ÜÇÜNCÜ BÖLÜM

SİBER GÜVENLİK POLİTİKALARI: TÜRKİYE ÖRNEĞİ

Türkiye'de internet, 1990'ların başında savunma, araştırma ve akademi dünyasında etkisini göstermiştir. Bireylerin ve toplumların genel anlamda güvendiği iletişim altyapısının yenilikçileri, kurucuları ve onun üzerinden sağlanan hizmetler, Türkiye'de Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından temsil edilmektedir.

Bu bölüm, siber güvenlik politikasındaki benzerlik ve ayrılıkları görmek için Türkiye'deki siber güvenlik politikası ve stratejisi, siber kültür ve toplum, eğitim, öğretim ve beceriler, yasal ve düzenleyici çerçeveler, standartlar, organizasyonlar ve teknolojileri alt başlıklar halinde sunmaktadır. Bu çalışma, Türkiye'de siber güvenliği daha iyi anlamak için önde gelen BM kuruluşu olan ITU'nin verilerini, ulusal stratejik belgelerini, siber güvenlik endekslerini, siber güvenliğe yönelik kurum ve kuruluşlarını ve bu alanda yapılan diğer çalışmalarını incelemektedir. Son olarak çalışma, siber alanında politikalardan alınan tavsiyeleri ve dersleri ortaya koyacaktır.

3.1. Türkiye'de Siber Güvenlik

Siber güvenlik bir devlete, bölgeye veya belirli bir sosyal organizasyona ait olmayıp, tüm dünyada ağı kullanan veya ağ tekniğinden büyük ölçüde etkilenen her grup veya bireyi ilgilendirmektedir. Siber güvenlik alanı, belirli bir özne tarafından algılanan siber güvenlik tehdidi ile ilgilidir. Küresel siber güvenlik alanı, dünyadaki ülkelerin güvenliğini, istikrarını ve gelişimini etkileyen siber ile ilgili mevcut koşulları ve olayları ifade etmektedir.

Siber güvenlik alanının kapsamı büyük veya küçük olabilmekte ve siber güvenlik alanına yönelik tehditlerin ciddiyeti de değişiklik göstermektedir. Aslında siber güvenlik alanı öznel bir durumdur ve söylem inşasıyla ilgilidir. Siber alandaki tüm aktörler saldırı başlatma kapasitesine sahiptir. Ağ ortamında coğrafi bir kavram yoktur. Bu nedenle saldırı kapasitesi coğrafi mesafe ile sınırlı değildir. Ağ ortamına yönelik tehditler hızlı ve etkin bir şekilde çözümlenemez. Ağ ortamında caydırıcı politikaları etkin bir şekilde yapmak da imkânsız

olmaktadır. Siber güvenlik, güç yapısının dengesizliği, kurum ve normların eksikliği ve yetersiz karşılıklı güven gibi bazı ortak özelliklere de sahiptir. Tablo 6'da Türkiye'nin dünya ülkeleri arasındaki sıralamasına bakacak olursak; Küresel Siber Güvenlik Endeksi'nde değerlendirmeye katılan ülkeler arasında 20. sırada yer almıştır.

Tablo 6:[217] 2018 Küresel Siber Güvenlik Endeksi'nde Bölgesel ve Küresel Sıralama

Üye Devlet	Puan	Bölgesel Sıralama (Avrupa Bölgesi)	Küresel Sıralama
Türkiye	0.853	11	20
İngiltere	0.931	1	1

Tablo 6'da 2018 yılı Küresel Siber Güvenlik Endeksi'nde verilen bilgilere dayalı olarak, Türkiye, Avrupa ülkeleri arasında sıralamada 11. sırada yer almıştır. İngiltere 1. sırada yer alarak diğer ülkelerin önüne geçmiştir. Burada belirtilen "Puan 0 ile 1" arasında verilen değerlere göre ölçülmüştür. Bölgesel ve Küresel sıralamada ülkeler için en düşük puan 0 iken, en yüksek puan 1 olmaktadır. "Sıralama" ise ülkelerin siber güvenlik etkinliğine göre ölçülmüştür. Değerlendirmeye katkı sağlamamış ülkelerin verileri 2018 Küresel Siber Güvenlik Endeksi'nde yer almamıştır.

"0 ile 1" arasında bir ölçeğe sahip olan önceki yinelemelerden farklı olarak, 2020 Küresel Siber Güvenlik Endeksi'nin yinelemesi, her bir sütunun 20 puan ağırlıklı olduğu "0 ile 100" arasında bir ölçek olmaktadır. Bileşik ağırlıklı indeks olarak, her bir gösterge, alt gösterge ve mikro gösterge, gösterge grubuna göreli önemi verilen bir ağırlık ile atanmaktadır. Ağırlık, final puanları üzerinde önemli bir etkiye sahip olabilmekte ve farklı teknikler farklı sıralamalar üretebilmektedir. Verilere katılan ülkelerin yanıtları, ITU ekibi tarafından doğrulanan anket verilerine göre rapor edilmektedir. Gösterge grupları, ağırlıklı aritmetik ortalamalar kullanılarak toplanmıştır. Bu, bir alanda düşük puan alan bir ülkenin, puanlarının bir kısmını başka yerlerde iyi yaparak telafi edebileceği anlamına gelmektedir.

2020 Küresel Siber Güvenlik Endeksi'nde "küresel puan ve sıralamalar" için ankete katılan ülkeler içerisinde Türkiye "97,49 Puan" ve "11. Sırada"

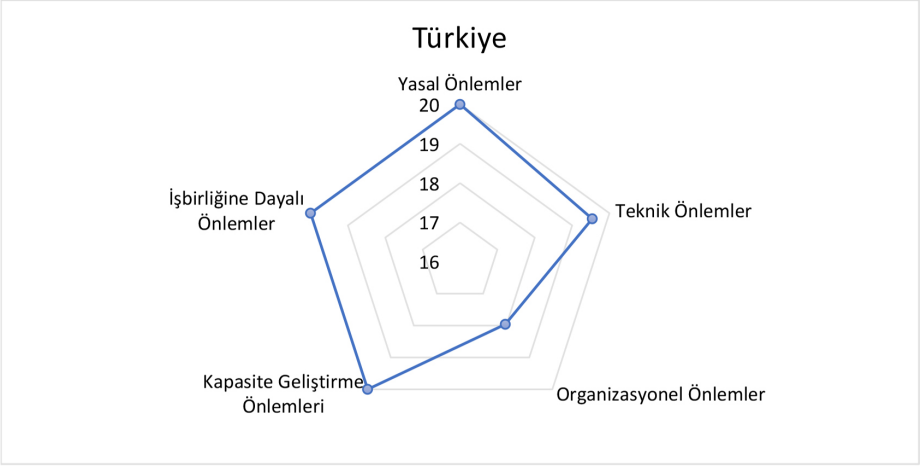
[217] Global Cybersecurity Index 2018, *ITU, s*. 60.

yer almaktadır.[218] Birinci sırada yer alan Amerika'nın 2020 yılı Küresel Siber Güvenlik Endeksi'ne göre puanı 100'dür. Ankette son sırada yer alan ülkeler Mikronezya, Vatikan ve Yemen 0 puan alarak 182. sırada yer almaktadırlar.

Bölgesel incelendiğinde küresel siber güvenlikte puan ve sıralamalar değişmektedir. Buna göre, Türkiye'nin Grafik 8'de siber güvenlik kapasite olgunluk "genel puanı 97,5" iken, siber güvenlik kapasite olgunluk sıralaması ise Avrupa ülkeleri arasında 6. olmaktadır.[219]

Grafik 8:[220] Siber Güvenlik Kapasite
Olgunluk Modelinin Beş Boyutu'nda Türkiye

Genel Puan	Yasal Önlemler	Teknik Önlemler	Organizasyonel Önlemler	Kapasite Geliştirme Önlemleri	İşbirliğine Dayalı Önlemler
97.5	20	19.54	17.96	20	20



Organizasyonel önlemler, siber güvenlik hedeflerinin ve stratejik planların tanımlanmasının yanı sıra, bunların uygulanmasını sağlamak için organizasyonel rollerin, sorumlulukların ve hesap verme sorumluluklarının resmi bir tanımını içermektedir. Bu önlemler, etkili bir siber güvenlik duruşunun uygulanmasını ve detaylandırılmasını sağlamak için vazgeçilmezdir. Uygulama, teslimat ve ölçümde her şeyi kapsayan bir planla birlikte devlet tarafından geniş stratejik hedefler belirlenmelidir. Ulusal ajanslar stratejiyi uygulamak ve sonucu değerlendirmek için hazır bulunmalıdır. Ulusal bir strateji, yönetişim modeli

[218] Global Cybersecurity Index 2018, *ITU, s*. 25.
[219] Global Cybersecurity Index 2020, *ITU, s*. 30.
[220] Global Cybersecurity Index 2020, *ITU, s*. 127-128.

ve denetim organı olmadan, farklı sektörlerdeki çabalar çatışabilmekte ve siber güvenlik gelişiminde etkin bir uyum sağlama çabalarını engelleyebilmektedir. Hassas radar grafiğine göre Grafik 8'de Türkiye organizasyonel ve teknik önlemlerde birtakım iyileştirmelere ihtiyaç duymaktadır. Yasal önlemler, iş birliğine dayalı önlemler ve kapasite geliştirme önlemleri açısından yirmi ve yirmiye yakın bir puanda olduğu için Küresel Siber Güvenlik Endeksi'nin yapmış olduğu çalışmaya göre Türkiye'nin ideal noktada olduğu bilinmektedir.

Türkiye'de ulusal güvenlik, ulusal ve toprak bütünlüğü ile anayasal düzenin güvence altına alındığı, ekonomik ve sosyal ilerlemenin sürdürüldüğü bir koşul olarak algılanmaktadır. Bu tanımda belirtilen ulusal çıkardır. Bir ülkenin ulusal çıkarları, bir taraftan güvenlik politikalarını yönlendirirken, diğer taraftan tarih ve coğrafya güvenlik algılarını şekillendirmektedir.

Türkiye'nin hayati güvenlik çıkarları geleneksel olarak "Yurtta sulh, cihanda sulh" olarak algılanmış ve kategorik olarak şu bağlamda tanımlanmıştır: "toprak ve ulusal bütünlüğün korunması, meşru hakların, egemenliklerin ve özgürlüklerin savunulması." Burada güvenlik durumu, komşularla ilişkilerin, komşu istikrarsızlıkların ve yayılma potansiyeli olan rahatsızlıkların ve iç düzenin doğasının bir katsayısı olmaktadır. Türkiye'nin güvenlik çıkarları giderek ekonomik odaklı olmaya yönelmiştir. Türkiye'de siber güvenliğe duyulan endişe alanının kapsamı ise ekonomik çıkarların, siyasi ve tarihsel bağlantıların kapsamı ile orantılı hale gelmiştir.

Siber güvenliğin ulusal düzeydeki en önemli yönü stratejik yönetimdir. Kapsamlı bir analiz için ilk aşama, ülkenin siber güvenlik stratejisi olmalıdır. Yirmi birinci yüzyılda siber savaşlar ve siber alanda güvenliğin sağlanması en önemli stratejik önceliktir. Bu nedenle, ulusal bir strateji geliştirmek, hayati önem taşımaktadır. Konu ile ilgili çalışma, Türkiye'de siber güvenlik hakkında çeşitli düzeylerde yapılmıştır. Örnekler arasında Dünya Bilgi Toplumu Zirvesi'nde kabul edilen "Tunus Raporu"[221] ve "Türkiye Dokuzuncu Kalkınma Planı"[222] yer almaktadır.

[221] Tunus Raporu şu noktalara dikkat çekmektedir; "Bilgi kaynakları ve teknolojileri suç için kullanılmaktadır. Terörizm, bilgi teknolojilerini etkin kullanmaktadır." Bu nedenle bilgi teknolojilerinin kötüye kullanılması önlenmeli, ancak suistimali önlenirken insan hakları dikkate alınmalıdır. Detaylı bilgi için bkz. WSIS (2005). *Report of the Tunis phase of the World Summit on the Information Society* (WSIS), Tunis: WSIS.

[222] Kalkınma, hukukun üstünlüğünün yanı sıra ekonominin büyümesi, bilgi ve iletişim teknolojilerinde ilerleme sağlanması, uluslararası rekabetin artması, sürdürülebilir büyüme ve insani gelişme gibi kavramları içeren çok boyutlu bir anlayışla tanımlanmaktadır. Büyüme ve gelişme çabalarının bu tanıma uyan bütüncül bir bakış açısı ile sürdürüleceği görülmektedir. Detaylı bilgi için bkz. Dokuzuncu Kalkınma Planı (2007- 2013). [https://www.sbb.gov.tr/kalkinma-planlari/] (er. tar. 23.05.2021). E-devlet

Türkiye toplumunun bir bilgi toplumuna dönüşümü, 2007-2013 yıllarını kapsayan Türkiye Dokuzuncu Kalkınma Planı'dır. Kamu hizmetlerinin elektronik ortamda sağlanması, günlük yaşama büyük kolaylık getirmektedir. Nitekim suç örgütleri de bilgi teknolojisinden faydalanmaktadır.[223] Bu çalışmanın ikinci bölümünde bahsedilen Estonya'ya yönelik siber saldırıların, gelecekte e-devlet uygulamaları için yeterli güvenlik önlemleri alınmazsa potansiyel sorunların ortaya çıkabileceğini küresel ölçekte göstermiştir.

Dokuzuncu Kalkınma Planı'nın ardından, "program dönemi gelişme eksenleri" ve "kamu hizmetlerinde kalite ve etkinliğin artırılması" konusu altındaki iki bölüm siber güvenliğe atılan diğer adımlardır.[224] Bunlar, e devlet uygulamalarının güvenliğinin ve yaygınlaştırılmasının etkinliğini artıran bölümlerdir:[225]

2017 yılı Ocak ayında "Siber Yıldız" adlı çevrimiçi bir siber güvenlik yarışması düzenlenmiştir.[226] Bu yarışmada için katılımcı sayısı yaklaşık yirmi yedi bin iken, yarışmacı sayısı onbeş bin civarında olmuştur. Yarışma, ülkedeki siber güvenlik uzmanlarını belirlemiş ve başarılı rakiplerden bazıları Türkiye Ulusal Bilgisayar Acil Müdahale Ekipleri (TRCERT) tarafından işe alınmıştır. TRCERT, Ekim 2017'de NATO CMX-2017[227] Kriz Yönetimi Tatbikatı'na ve Kasım 2017'de Ulusal Siber Savunma Tatbikatı'na katılmıştır.

Güvenli İnternet Merkezi (SIC), internetin doğru ve güvenli kullanımı konusunda farkındalığı artırmak amacıyla kurulmuştur. SIC, bir "İnternet Yardım Hattı" ve ailelerin internetten en iyi şekilde nasıl yararlanabilecekleri konusunda tavsiye bulabilecekleri bir web sitesi olan "Güvenli Web"i işletmektedir. SIC, bilgi ve iletişim teknolojilerine sınırlı erişimi olan çocuklara

---

uygulamalarının teşvik edilmesi Dokuzuncu Kalkınma Planı'na dâhil edilmiştir (s. 51, madde 314).

[223] Dokuzuncu Kalkınma Planı (2007- 2013), s. 53, madde 323.

[224] Resmî Gazete, Karar 2007/12300, [https://resmigazete.gov.tr/eskiler/2007/06/20070621-2.htm] (er. tar. 23.05.2021); Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, *Orta Vadeli Program (2012- 2014),* [https://www.sbb.gov.tr/wp-content/uploads/2018/11/Orta_Vadeli_Program2012-2014.pdf] (er. tar. 23.05.2021).

[225] Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, *Orta Vadeli Program (2012-2014)*, s. 61-62, [https://www.sbb.gov.tr/wp-content/uploads/2018/11/Orta_Vadeli_Program2012-2014.pdf] (er. tar. 23.05.2021).

[226] Ulusal Siber Olaylara Müdahale Merkezi (USOM) tarafından organize edilen Siber Yıldız, Türkiye'de siber gelişme ve yetenekleri belirlemek için yarışma düzenlemektedir. Detaylı bilgi için bkz. [https://www.siberyildiz.com/] (24.05.2021).

[227] Crisis Management Exercise 2017, NATO, [https://www.nato.int/cps/en/natohq/news_147373.htm] (er. tar. 09.11.2021); Tania Laţici (2020). *Understanding EU-NATO Cooperation Theory and Practice*, European Parliament Briefing: European Parliamentary Research Service (EPRS).

ve gençlere, teknolojiyi yakından deneyimleyebilecekleri ve sunduğu fırsatları öğrenebilecekleri bir platform sunmaktadır. Çocuklar için internetin güvenli kullanımı konusunda farkındalık yaratan "Fragman, Teknolojik Deneyim Alanı", "Robotik Kodlama Alanı", "Sanal Gerçeklik Alanı", "İnternet Alanının Bilinçli ve Güvenli Kullanımı, Eğitim Alanı" ve "Yarışma Alanı" olmak üzere beş aşamadan oluşmaktadır. SIC ayrıca çocuklar için oyunlar, etkinlikler, yarışmalar ve eğitimler içeren özel bir web sitesi işletmektedir.

SIC, "yarat, bağlan ve saygı duy: daha iyi bir internet seninle başlar" ana temasıyla "Güvenli İnternet Günü" etkinliğini düzenlemiştir. BTK ve Bahçeşehir Üniversitesi, 12-18 yaş arası gençleri oyun tasarlamaya teşvik etmek için bir masa oyunu yarışması başlatmıştır. Bu etkinlikte Facebook ve Google, öğrencilere dijital oyunlar ve daha güvenli internet konusunda atölye çalışmaları yapmıştır.[228] Günümüzde de okullarda, kurum ve kuruluşlarda siber güvenlik ile ilgili birçok eğitim verilmektedir.

Bu çalışmanın ikinci bölümünde "Siber Güvenlik Politikalarının Belirlenme Süreci ve Hükümetlerin Aldığı Önlemler" başlığı altında verilen Tablo 5'e göre; 2016-2020 yıllarını kapsayan Küresel İnovasyon Endeksi, İnovasyon Çıktı Alt-Endeksi Sıralaması'nda 120'den fazla ülkenin siber güvenlik pazarında küresel paya sahipliği ölçülmüştür. Bu ülkeler arasında Türkiye'nin GII puanları, İngiltere ile karşılaştırılınca daha geride olduğu anlaşılmıştır. 120'den fazla ülke arasında 2016-2020 yılları verilerine göre İngiltere en iyi 3. ve en son 5. sıraları, Türkiye en iyi 42. ve en son 53. sıraları arasında olduğu görülmektedir.[229]

Bu bilgiler ışığında, Türkiye'nin siber güvenlik sektöründeki yeniliklerden faydalanabilmesi ve yararlanabilmesi için ilk 20'ye girmesi gerekmektedir. Burada alt başlıklar halinde Türkiye'nin siber güvenlik politikasını beş boyutta incelemek yerinde olacaktır. Verilen bilgiler ışığında bu alt başlıklar, Türkiye'nin siber güvenlik stratejilerine ve siber politika hedeflerinin uygulanmasında önemli olan kurumlara genel bir bakış sağlayacaktır.

3.1.1. Politika ve Strateji

Ulusal stratejide belirlenen hedeflere ulaşmak için belirli programları ve yol haritalarını sağlayan stratejik planlar olmalıdır. Bu gösterge ile stratejik planlar ve ulusun stratejik konuları ele almak için oluşturduğu resmi raporlar, ulusun güvenli bir siber alana ulaşma potansiyelini belirlemek için değerlendirilmektedir. Türkiye Ulusal Siber Güvenlik Strateji Belgesi geliştirme

[228] Global Cybersecurity Index 2018, *ITU, s*. 47-48.
[229] Global Innovation Index, "Innovation Output Sub-Index Rankings".

sürecine bakıldığında, Devlet Planlama Teşkilatı tarafından şu politika belgeleri yayınlanmıştır:[230]

- E-Türkiye Girişimi Eylem Planı 2002,
- E-Dönüşüm Türkiye Projesi Kısa Vadeli Eylem Planı (2003-2004),
- E-Dönüşüm Türkiye Projesi 2005 Eylem Planı, Bilgi Toplumu Stratejisi (2006-2010),
- Bilgi Toplumu Stratejisi Eylem Planı (2006-2010),
- Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2013-2014,
- Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2016-2019 ve
- Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023.

Bu dönemde içerisinde birçok çalıştay, seminer, sempozyum ve derslerde siber güvenlik eğitim ve öğretim, faaliyet raporları olarak verilmiştir. 11 Temmuz 2006 tarihli Bilgi Toplumu Stratejisi ve Ek Eylem Planı, Yüksek Planlama Kurulu tarafından onaylanmış, 28 Temmuz 2006 tarih ve 26242 sayılı Resmî Gazete'de yayımlanmıştır.[231] Bu belge, ulusal siber güvenlikle ilgili beş eylem planına sahiptir ve bunlar:

- "Kişisel Bilgilerin Güvenliği ve Gizliliği" kategorisi, Eylem Planı 88, sorumlu kuruluş Türkiye Bilimsel ve Teknolojik Araştırma Kurumu-Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (TÜBİTAK-UEKAE) tarafından Ulusal Bilgi Sistemleri Güvenlik Programı'nın oluşturulması için 2007 yılından itibaren 24 aylık bir süre belirlemiştir.
- "Bilgi Güvenliğine İlişkin Yasal Düzenlemeler" Eylem Planı 87, Adalet Bakanlığı sorumlu kuruluşu tarafından aşağıdaki hususlara yönelik yasal düzenlemelerin yapılmasını öngörmüştür:[232] "Ulusal güvenlikle ilgili tüm bilgilerin elektronik ortamda korunması", "devlet bilgi güvenlik sistemlerinin korunması", "Kişisel Verilerin Korunması".
- "Vatandaş Odaklı Yaklaşım" kategorisi, Eylem Planı 27, tüm kamu kurumlarının web sitelerinin içerik, güvenlik, kimlik yönetimi ve kullanılabilirlik standartlarını sağlamasını gerektirmektedir. Bunun için 27 Ocak 2009 tarihinde

---

[230] Bilge Karabacak ve Sevgi Özkan (2009). "Critical Infrastructure Protection Status and Action Items of Turkey", *International Conference on E-Government Sharing Experiences*, [https://fuse.franklin.edu/facstaff-pub/40/] (er. tar. 20.06.2022).

[231] SPO Information Society Strategy Action Plan (2006-2010). *Assessment Report*, No 5, Ankara.

[232] H. Şentürk (vd.) (2012). "Cyber Security…", s. 116-117; SPO Information Society Strategy Action Plan (2006-2010). *Assessment Report*, No 5, Ankara, s. 32, 46.

yapılan toplantıda "Kamu Kurumlarının İnternet Sitelerine İlişkin Standartlar ve Öneriler" adlı bir rehber hazırlanmış ve kamuoyuna tanıtılmıştır.

- "Bilgi ve İletişim Teknolojilerinin İşletmeler Tarafından Benimsenmesi" kategorisi, Eylem Planı 26, Türk Standartları Enstitüsü tarafından e-ticaret güvenlik altyapısı gereksinimlerini belirlemiştir.
- "Sosyal Dönüşüm" kategorisi, "İnternet Güvenliği" adlı 10. Eylem Planı, "5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" sonuçlarının Adalet Bakanlığı tarafından izlenmesini gerekli kılmıştır.

Türkiye Bilgi Güvenliği Derneği'nin girişimiyle 16 Haziran 2012 tarihinde Ankara'da "Siber Güvenlik Stratejisi Çalıştayı" düzenlenmiştir. Bu derneğin üyeleri öncelikle bir taslak belge hazırlamış, daha sonra özel ve kamu kurumlarıyla paylaşmıştır. Bu belge daha sonra seksenden fazla Bilgi Teknolojileri güvenlik profesyoneli ile kamu ve özel kuruluşlardan uzmanların katılımıyla bir çalıştayda tartışılmış, bu çalıştayda taslak strateji belgesi revize edilerek Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na sunulmuştur. Türk Strateji Belgesi; ulus toprağını, vatandaşlarını, tüm varlıklarını, bugününü ve geleceğini korumak için siber alan güvenliğinin sağlanmasının zorunlu olduğunu belirtmektedir. Belge ayrıca şu önemli noktalara da değinmektedir:[233]

- Ulusal Siber Güvenlik Kurulu'nun kurulması,
- Ulusal siber güvenlik risk analizinin yıllık performansı,
- Ulusal Siber Tehdit ve Zafiyet Analiz Merkezi Laboratuvarı'nın kurulması,
- Siber Güvenlik Mükemmeliyet Merkezi'nin kurulması,
- Kritik altyapıları yöneten resmi/özel kuruluşların TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ile uyumlu olması şartı,
- Siber güvenlik bilincini artırma ihtiyacı, üniversite programlarında çekirdek "Siber Güvenlik ve Savunma" dersi önerisi.

Belgenin amacı, Türkiye'nin siber alandaki saldırılara karşı ülkeyi hazırlaması ve güçlü bir şekilde atacağı adımları belirlemesidir. Belirlenen adımlar şunlardır:[234]

[233] H. Şentürk (vd.) (2012). "Cyber Security…", s. 115-116.
[234] H. Şentürk (vd.) (2012). "Cyber Security…", s. 116.

- Ulusal Siber Güvenlik Stratejisinin hazırlanması,
- Yasal düzenlemeler
- Ulusal siber yeteneklerin geliştirilmesi
- Ulusal Siber Olaylara Müdahale Teşkilatının Kurulması
- Eğitim ve Farkındalık Faaliyetleri
- Kritik Altyapıların Korunması
- Uluslararası iş birliği
- Kamu Kurumlarının Siber Güvenliği

Türkiye'de devlet düzeyinde 19 yılı aşkın bir süredir siber güvenlik konularına önem verilmiş ve "E-Dönüşüm Türkiye Projesi" ile resmi başvuru ve eylemleri 2003 yılına kadar başlatılmaya çalışılmıştır. Telekomünikasyon Birliği Türkiye'de 2000 yılında kurulmuş ve 2008 yılında BTK'ya dönüştürülmüştür.[235] TÜBİTAK bünyesinde Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) kurulmuştur. BİLGEM bünyesinde 2012 yılında açılan Siber Güvenlik Enstitüsü (SGE), faaliyetlerine günümüzde devam etmektedir. Bir diğer resmi politika belgesi ise 2008 yılında on dokuz devlet kurumunun iş birliği ile hazırlanan ve 2009 yılında Başbakanlığa sunulan "Ulusal Siber Güvenlik Politikası"dır.[236]

Siber güvenlikle ilgili en belirgin ve önemli adımlar, Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2013-2014, Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2016-2019 ve Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023'dür. Söz konusu strateji ve eylem planları; kamu kurumlarını temsil eden kurum ve kuruluşlar, kritik altyapı işletmecileri, BİT sektörü, üniversiteler ve sivil toplum kuruluşlarından uzmanlarla, toplantılar, çalıştaylar, seminerler ve konferanslar düzenleyerek olmuştur. Strateji ve eylem planı uygun şekilde geliştirmek için çok çeşitli paydaşlardan iş birliği ve anlaşma sağlamak gerekmektedir. Tunus raporu, Dokuzuncu Kalkınma Planı ve Orta Vadeli Program (2012-2014) örnek olarak siber güvenlik konusunun hem ulusal hem de uluslararası açıdan önemli bir alan olarak değerlendirildiğini göstermektedir.

TÜBİTAK, 2003-2023 yılları arasını kapsayan yeni bilim ve teknoloji politikalarını belirlemek üzere "Vizyon 2023" adı verilen bir projeyi tasarlamıştır. Vizyon 2023 kapsamında on panel ve iki kesişen tematik alan olarak

[235] Salih Bıçakçı, D. Ergun ve M. Çelikpala (2016). "Türkiye'de Siber Güvenlik", (ed. Sinan Ülgen), *Türkiye'de Siber Güvenlik ve Nükleer Enerji*, İstanbul: EDAM, s. 26.

[236] "E-dönüşüm Türkiye", [http://www.bilgitoplumu.gov.tr/bilgi-toplumu/e-donusum-projesi/] (er. tar. 30.05.2021).

kurulmuştur. Proje ağırlıklı olarak stratejik teknolojileri ve öncelikli araştırma ve geliştirme alanlarını belirlemeyi amaçlamıştır. Vizyon 2023 kapsamında on panel ve iki kesişen tematik (eğitim ve insan kaynakları, çevre ve sürdürülebilir kalkınma) alan kurulmuştur. Siber güvenlik çalışmaları, Bilgi ve İletişim Paneli, Savunma, Havacılık ve Uzay Endüstrileri Paneli olmak üzere iki panel altında gerçekleştirilmiştir. Kriptoloji, Bilgi ve İletişim Paneli altındaki 32 teknoloji alanından biri olmuştur. Ayrıca siber savaş, kriptoloji, web güvenliği ve bilgi güvenliği de kritik teknoloji konuları olarak değerlendirilmiştir.[237]

3.1.1.1. Siber Alan Tehditleri ve Siber Suçlarla Mücadele

Sistemlerin giderek çevrimiçi olduğu ve bilişim teknolojilerinin hayatın kaçınılmaz bir parçası olduğu dünyada, siber saldırı teknikleri bir bireye, gruba, şirkete, kuruma veya bir ülkeye zarar vermenin şüphesiz en etkili ve en ucuz yöntemi haline gelmiştir. Bu nedenle siber tehdidin şiddeti artarak devam etmektedir. Siber suçlar sadece dünya için değil Türkiye için de büyük tehdit olmaktadır.[238]

Norton Siber Suç Raporu verilerine göre 2012 yılında Türkiye'nin de arasında bulunduğu birçok devlet beş yüz elli altı milyondan fazla zarara uğramış, birçok insan siber suç nedeniyle mağdur olmuştur. Bu durum Türkiye'de yaklaşık on milyondan fazladır. Genel olarak mağdurların toplam maliyetinin yüz on milyar Amerikan Doları civarında olduğu belirtilmiştir.[239] Bu nedenle Norton Siber Suç Raporu, ülkelere olduğu kadar şirketlere karşı da "suç" olarak kullanılabilecek siber saldırı araçlarını ya da eylemlerini hedeflemektedir. Kötü amaçlı yazılımdan koruma çözümleri, bu tehditlere karşı önlemler olarak bahsedilmektedir. Bazı aktivistler, hackleme eylemleriyle seslerini duyurmak için interneti bir araç olarak kullanmaktadır.[240]

2009 McAfee Sanal Kriminoloji Raporu, ülkelerin yalnızca rakiplerinin siber alandaki faaliyetleri hakkında bilgi toplamakla kalmayıp, aynı zamanda karmaşık siber saldırı teknikleri geliştirdiğini belirtmiştir. Saldırgan siber yetenekleri olduğu bilinen ülkeler Çin, Rusya, ABD, İsrail ve Fransa'dır. Kuzey

---

[237] TÜBİTAK (2004). "Ulusal Bilim ve Teknoloji Politikaları 2003-2023 Strateji Belgesi".

[238] On Birinci Kalkınma Planı (2019-2023). "Siber Güvenlik ve Mahremiyet", s. 5.

[239] Norton (2012). *2012 Norton Cybercrime Report*, [https://www.relianceacsn.co.uk/the-2012-norton-cybercrime-report/] (er. tar. 23.05.2021).

[240] Hactivist, hacker ve aktivistin birleştirilmesiyle üretilen, böyle bir kişiye hitap etmek için kullanılan bir terimdir. Detaylı bilgi için bkz. S. Bıçakçı, D. Ergun ve M. Çelikpala (2016). "Türkiye'de Siber…", s. 51.

Kore, İran, Tayvan, Brezilya ve Hindistan'ın da saldırgan programları olduğu bilinmektedir. McAfee Sanal Kriminoloji Raporu'na göre, ABD'nin saldırı gücü puanı 10 üzerinden 8, siber savunma gücü puanı 1, Kuzey Kore'nin sırasıyla 2 ve 7 olduğu iddia edilmiştir.[241]

RedHack, 29 Mart 2012'de Türkiye polis teşkilatı web sitesinin yaklaşık yüzde doksanını hackleyen bu türden bir aktivisttir.[242] 2011 yılında Millî Eğitim Bakanlığı'nın Öğretmen Atama Sitesi hacklenmiş ve hackerlar açılır pencere yardımıyla "Güvenlik 0" mesajı vermiş(ler)dir.[243] RedHack, 20 Nisan 2012'de İçişleri Bakanlığı'nın alt web sitesini hackleyerek İçişleri Bakanlığı'nın tüm dosyalarını indirdiğini iddia etmiştir.[244] Yine 2012 yılı Anneler Günü'nde Aile Bakanlığı hacklenmiştir.[245] 2012 yılında RedHack örgütü Dışişleri Bakanlığı sayfasını da hedef almıştır.[246] 2012 yılı Türkiye Öğrenci Seçme ve Yerleştirme Merkezi (ÖSYM) web sitesine koordineli olarak RedHack ve Anonymous tarafından saldırıya uğramış ve ÖSYM web sitesinin bu gruplar tarafından saldırıya uğraması üzerine kurumun itibarı zedelenmiş ve kullanıcıların web sitesine erişimi engellenmiştir.[247]

2013 yılında Polis Teşkilatı'da hacklenmiştir. Emniyet Genel Müdürlüğü'nün PolNet sistemini RedHack hackladığini duyurmuştur. PolNet ve Emniyet Genel Müdürlüğü'nün resmi internet sitesine erişiminin kesilmesi nedeniyle sınır kapılarının giriş-çıkışlarında kuyruk oluşmuş ve Emniyet hizmet sunamamıştır. Fakat Emniyet yetkilileri hacklenme iddialarını yalanlamış, internet sitelerinin kontrollü olarak devre dışı bırakıldığını ve PolNet'in internet bağlantısı olmadan kapalı bir ağ üzerinden çalıştığını bu nedenle hacklenmesinin

---

[241] Dave DeWalt (2009). "McAfee Virtual Criminology Report 2009", Virtually Here: The Age of Cyber Warfare, [http://conflictsincyberspace.blogspot.com/2009/12/mcafees-virtual-criminology-report-2009.html] (er. tar. 12.06.2022).

[242] S. Bıçakçı, D. Ergun ve M. Çelikpala (2016). "Türkiye'de Siber …", s. 53-56.

[243] Milliyet (2011). "Şok! MEB'in Sitesi Hacklendi", [https://www.milliyet.com.tr/teknoloji/sok-mebin-sitesi-hacklendi-1353574] (er. tar. 23.05.2021).

[244] NTV (2012). "İçişleri Bakanlığı "hack"lendi", [https://www.ntv.com.tr/turkiye/icisleri-bakanligi-hacklendi,3kdtZFzt00msI4WP1eiu4A] (er. tar. 23.05.2021); "İçişleri "bizi seviyor musun" diye "hack"lendi", Milliyet, [https://www.milliyet.com.tr/siyaset/icisleri-bizi-seviyor-musun-diye-hack-lendi-1530889] (er. tar. 23.05. 2021).

[245] Milliyet (2012). "Aile Bakanlığı'nı RedHack hackledi", [https://www.milliyet.com.tr/gundem/aile-bakanligi-ni-redhack-hackledi-1539999] (er. tar. 23.05.2021).

[246] NTV (2012). "Redhack Dışişleri Bakanlığı'nı hack'ledi", [https://www.ntv.com.tr/turkiye/redhack-disisleri-bakanligini-hackledi,iECCMBunCE2i7A16_PkFVg] (er. tar. 23.05.2021).

[247] Cumhuriyet (2012). "ÖSYM'nin sitesi çökertildi", [https://www.cumhuriyet.com.tr/haber/osymnin-sitesi-cokertildi-357600] (er. tar. 22.05.2021).

mümkün olmadığını belirtmiştir.[248] Daha birçok Türk Devlet sitesinin hacklendiği gazetelerde yer almıştır.[249] 2015 yılında Türkiye Diyanet Vakfı ve ona bağlı Kadın, Aile, Gençlik Merkezi resmi twitter hesapları da hacklenmiştir.[250] Bu eylemler, hizmetlerin engellenmesine ek olarak itibar kaybına da yol açmıştır.

Dünya çapında da birçok devlet, devlet adamları veya kamu kurumları hacklenen listeler arasında yer almıştır. F-35 Savaş Uçaklarının verilerinden, Apple Şirketine; ABD Savunma Bakanlığı sitesinden 1,6 milyon müşterisinin hesabına girilen PayPal sitesine, dönemin İsrail Savunma Bakanı Naftali Bennett'in twitter hesabından Mark Zuckerberg'in kendi Facebook hesabına ve daha birçok kişiler ya da kurumlar hacklenenler arasında olmuştur.[251] 2020 yılında web sitesi olan Kişisel Verileri Koruma Kurumu'ndan Vatan Bilgisayar'ın internet sitesini kullanan yirmi yedi bin müşterisinin verileri hacklendiğini duyurmuştur.[252]

Siber alanda faaliyet gösteren bilgi ve işlem sistemlerinin korunması için hem sivil hem de askeri tedbirlere ihtiyaç olduğu düşünüldüğünde, bir ülkenin siber alanda hacklenme olayları ile ilgili yaşadıkları durumlara karşılık yapılacak müdahalelerin de analiz edilmesi gerekmektedir. Askeri

[248] Milliyet (2013). Türkiye'deki GBT, ehliyet, pasaport, trafik, ruhsat vb. gibi çoğu alanda hizmet vermesini sağlayan PolNet sistemidir. "Emniyetin PolNet'i çöktü Türkiye'de hayat durdu", [https://www.milliyet.com.tr/gundem/emniyetin-polnet-i-coktu-turkiye-de-hayat-durdu-1759603] (er. tar. 23.05.2021).

[249] Milliyet (2013). "76 Türk Devlet Sitesi Hacklendi", [https://www.milliyet.com.tr/teknoloji/76-turk-devlet-sitesi-hacklendi-1665235] (er. tar. 23.05.2021).

[250] Milliyet (2015). "Diyanet'i hackliediler", [https://www.milliyet.com.tr/gundem/diyanet-i-hackliediler-2029945] (er. tar. 23.05.2021); "Atatürk'ün hackerlarından Diyanet'e hack şoku", Milliyet, 2015, [https://www.milliyet.com.tr/gundem/ataturkun-hackerlarindan-diyanete-hack-soku-2029752] (er. tar. 23.05.2021).

[251] HaberTürk (2017). "F-35 savaş uçağı verileri hacklendi!", [https://uzmanpara.milliyet.com.tr/haber-detay/gundem2/f-35-savas-ucagi-verileri-hacklendi/74000/74783/] (er. tar. 23.05.2021); Cumhuriyet (2017). "PayPal'dan açıklama: 1,6 milyon kişinin bilgileri hacklendi!", [https://www.cumhuriyet.com.tr/haber/paypaldan-aciklama-16-milyon-kisinin-bilgileri-hacklendi-880275] (er. tar. 23.05.2021); Milliyet (2020). "İsrail Savunma Bakanı'na hacker şoku! İstiklal Marşı paylaşıldı", [https://www.milliyet.com.tr/dunya/israil-savunma-bakanina-hacker-soku-istiklal-marsi-paylasildi-6160630] (er. tar. 23.05.2021); Milliyet (2018). "Apple 16 yaşındaki genç tarafından hack'lendi", [https://www.milliyet.com.tr/teknoloji/apple-16-yasindaki-genc-tarafindan-hacklendi-2726648] (er. tar. 23.05.2021); Milliyet (2018). "Mark Zuckerberg'in kendi Facebook hesabı bile hack'lendi", [https://www.milliyet.com.tr/mark-zuckerberg%E2%80%99in-kendi-facebook-hesabi-bile-hack%E2%80%99lendi-molatik-9532/] (er. tar. 23.05.2021).

[252] Milliyet (2020). "27 bin kişinin verisi hacklendi", [https://www.milliyet.com.tr/ekonomi/27-bin-kisinin-verisi-hacklendi-6328491] (er. tar. 23.05.2021).

siber güvenlik strateji belgesi, doktrin, kavram ve eylem, savunma ve taarruz siber güvenlik komutanlığı, CERT, uzman siber güvenlik personeli, eğitim kurumu, ulusal/uluslararası programlara katılım düzeyi vb. varlığı bu kapsamda değerlendirilebilmektedir.

Devlet, sınırları içinde fiziki güvenliği sağlamak için önemli bir sorumluluğa sahiptir. Bununla birlikte, bir saldırgan siber saldırılarla fiziksel hasar oluşturabileceğinden, dijital güvenlik bir ülkenin savunması kapsamında olması önem arz etmektedir. Bu hasar sadece pahalı araçları değiştirmek veya devlet web sitelerini kapatmak için para israfına neden olmakla sınırlı değildir. Siber silahları diğer silah sistemleriyle karşılaştırırken, siber güç maliyet, etki ve menzil avantajları yanında oldukça hümanist bir sistem olarak ortaya çıkmaktadır. Bununla birlikte, Stuxnet'ten[253] daha karmaşık bir siber silah, savaş başlıklı bir füzeden daha fazla hasara neden olabilmektedir. Temmuz 2012'de Savunma Sanayi Başkanlığı (SSB), devlete ait bir şirket olan Savunma Teknolojileri Mühendislik ve Ticaret Anonim Şirketi (STM A.Ş.) ile bilgi güvencesi ve siber savunma yeteneklerinin geliştirilmesi için bir fizibilite sözleşmesi imzalamıştır.[254]

"Entegre Siber Güvenlik Sistemi" başlıklı proje, kavramı doğrulama amacıyla siber savunma sistemleri, yazılımları ve süreçleri hakkında test yapılarak prototip ve ağ destekli yetenek fizibilite raporu üretmeyi hedeflemiştir. Bu aynı zamanda bir kavramın mevcut olduğu anlamına gelmektedir. Savunma Sanayi Başkanlığı, Türkiye'deki siber güvenlik şirketlerini geliştirmek, zenginleştirmek ve Türkiye Siber Güvenlik Kümelenmesi oluşturmak amacıyla 2018 yılında bir girişim başlatmıştır. Türkiye'nin önde gelen şirketleri Siber Güvenlik Kümelenmesi'ne üye olmuştur.[255] Türkiye'de altmış bir aktif

[253] Stuxnet, 2010 yılında İran'da bir bilgisayarda keşfedilen kötü amaçlı yazılımdır. Haziran 2010'da "Stuxnet" adlı bir siber solucanın Natanz'daki İran nükleer tesisini vurduğuna dair bilgi, siber savaş için bir dönüm noktası olmuştur. Stuxnet, dünya çapında kritik altyapılar için siber güvenlik sorunlarına ilişkin farkındalığı artırmıştır. Yeni siber tehditlerin ortaya çıkmasına sebep olan bu politik ve stratejik bağlam, bu solucanın yarattığı caydırıcı etki olmuştur. Detaylı bilgi için bkz. Marie Baezner, Patrice Robin (2017). "Hotspot Analysis: Stuxnet", *Center for Security Studies (CSS)*, s. 5-14; Jamess Farwell &Rafal Rohozinski (2011). "Stuxnet and the Future of Cyber War", *Survival Global Politics and Strategy,* Sayı 53, No 1, s. 23-40.

[254] Savunma Sanayi Başkanlığı, [https://www.ssb.gov.tr/WebSite/contentlist.aspx?PageID=39&LangID=2] (er. tar. 28.04.2022).

[255] Türkiye Cumhuriyeti Savunma Sanayi Başkanlığı, "Türkiye Siber Güvenlik Kümelenmesi", [https://www.ssb.gov.tr/Website/contentList.aspx?PageID=2584&LangID=1] (er. tar. 28.05.2021).

teknoloji geliştirme bölgesi (bilim ve teknoloji parkları yani teknoparklar) bulunmaktadır.[256]

Siber güvenlik teknolojileri kullanılarak hem hedefli hem de hedefsiz siber saldırılar gerçekleştirilebilmektedir. Ülkelerin kara, deniz, hava ve uzay gibi diğer savaş alanlarında olduğu gibi siber güvenlik kabiliyetlerini artırdıkları ve siber silahlar geliştirdiği bilindiğinde; bu kaçınılmaz yarışın gerisinde kalmak çok önemli bir hata olmaktadır. Bu nedenle, ABD ve diğer ülkelerde olduğu gibi yoğun siber savaş hazırlıklarına paralel olarak Türkiye'nin, yeni yüzyılın kritik tehdidine karşı hızla kendini uyarlaması ve siber tehditlere karşı mücadele geliştirmesi gerekmektedir. Yirmi birinci yüzyıl siber savaşlarına yerini sağlamlaştırmak isteyen bir millet için önerilerin dikkate alınması ve zamanında hayata geçirilmesi gerektiğine inanılmaktadır. On yıl öncesinde Türkiye'deki önlemler, kuruluşların farklı stratejileriyle sınırlı kalmıştır. Örneğin, bir sızma testi yaptırmak, kuruluşlar için sadece bir seçenek olmaktan öteye gidememiş ve çok yaygın olarak uygulanmamıştır. Konuyla ilgili diğer çalışmalar arasında Türkiye'deki Siber Güvenlik Tatbikatları da olmuştur.

25-28 Ocak 2011 tarihleri arasında ilk Ulusal Siber Güvenlik Tatbikatı 41 farklı enstitü / firmanın katılımıyla gerçekleştirilmiştir.[257] Türkiye'nin Ulusal Siber Güvenlik Strateji Belgesi 2013-2016, 2016-2019 ve son olarak 2020-2023 tarihleri arasını kapsayan üç ayrı siber güvenlik üzerine çalışmaları olmuştur. Teknolojik gelişmeler açısından Türkiye'de siber güvenlik ve veri mahremiyeti ile ilgili olası risklerin önlenebilmesi ve teknolojileri geliştirme yeteneğini iyileştirmesi gerekmektedir. Ayrıca nitelikli insan kaynağının sağlanması ve mevzuat altyapısını değişen teknolojik koşullara göre güncel tutulması gerekmektedir.[258] 2019 yılı 12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi'ne göre Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin (DDO) kamu kurum ve kuruluşları ve kritik altyapı sektörlerine hizmet veren özel kuruluşlar tarafından uygulanmak üzere Bilgi ve İletişim Güvenliği Rehberi (Kılavuz) hazırlanması öngörülmüş ve daha sonra bu konuda çalışmalar yapılmıştır.[259]

---

[256] Hasan Çiftçi (2019). *Technology Foresight and Modeling: Turkish Cybersecurity Foresight 2040*, PhD Thesis, Ankara: METU, s. 124.

[257] Faruk Aydın (2012). *Cyber Security in the National Protection of Turkey*, Master Thesis, Ankara: Cankaya University, s. 47.

[258] On Birinci Kalkınma Planı (2019-2023). "Küresel Gelişmeler ve Eğilimler", s. 11.

[259] Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi.

2019-2023 dönemi Türkiye On Birinci Kalkınma Planı'nda teknolojik dönüşümün sağlanması vurgulanmaktadır. Bunun için kamu kurumları ve özel sektörlerde siber güvenliğe yönelik adımlar atılması On Birinci Kalkınma Planı'nda önemli bir husus olmuştur. Kalkınma Planı'nda Türkiye Cumhuriyeti, siber güvenliğe dair teknolojik yenilikleri sağlaması, siber alanda nitelikli insan sayısındaki boşluğu doldurması, ilerleyen teknoloji ile beraber siber kabiliyetini geliştirerek veri güvenliğine yönelik riskleri ortadan kaldırması, siber güvenlik eğitimlerinin düzenlenmesi ve bu konuda farkındalığın artırılması, yasal ve düzenleyici çerçevesini oluşturması gerektiğine dair bilgiler verilmiştir.[260]

2019-2023 dönemi On Birinci Kalkınma Planı, Bilgi ve İletişim Teknolojileri hedefleri tahmini olarak verilmiştir. Buna göre BM-ITU Küresel Siber Güvenlik Endeksi'nde 2018 yılı ile 2023 yılının karşılaştırılması yapılmıştır. 2018 yılı BM-ITU 175 devlet arasında endekse göre Türkiye 20. sıradayken, 2023 yılının Aralık ayına kadar kalkınma planına göre 14. sırada olacağı tahmin edilmektedir.[261]

3.1.2. Kültür ve Toplum

Siber alan, birbirinden farklı bireyleri büyük bir küresel ailede birleştiren, farklı insanlarla ve yerlerle anlık ve gerçek zamanlı ilişkiler sürdürmektedir. Siber alanda kullanıcıların etkileşimleri ve davranışlarıyla oluşturulan siber kültür ve toplum kavramı, çeşitli topluluklar ve ülkeler arasında kültürlerarası iletişimi teşvik etmektedir. Çeşitli ülkelerden çok sayıda insan bilgi paylaşmak için dijital medyayı kullanırken, siber alan kültürlerarası iletişimi ve çok kültürlülüğü anlamak için yeni bir ortam sağlamaktadır. Pereira, teknolojik cihazlar aracılığıyla kültürel iletişim olan siber kültür kavramını, iletişimin bir ağdaki kültürel davranışları içerdiğini ve bu ağdaki iletişimin kültürel etkisini ve kontrolünü açıklamıştır.[262] Ayrıca, çeşitli kültürlerden kullanıcılar çevrimiçi olarak etkileşime girdiğinde, insanların farklılaşması ve mekâna yansıması, çevrimiçi alanda kültürlerarası iletişim ve yabancı kültür müzakeresi konusunda yeni bir anlayış sunmaktadır.

Siber güvenlik kültürü kavramı, Türkiye'de organizasyonun işgücünün siber güvenlikle ilgili tutumlarını, bilgilerini, varsayımlarını, normlarını ve değerlerini ifade etmektedir. Bunlar, organizasyonun amaçları, yapısı,

[260] On Birinci Kalkınma Planı (2019-2023) s. 7, 66, 109, 110, 183.
[261] On Birinci Kalkınma Planı (2019-2023). "Planın Hedefleri ve Politikaları", s. 111.
[262] Luís Moniz Pereira (2018). "Cyberculture, Symbiosis, and Syncretism", *Springer-Verlag*, No. 33, ss. 447-452.

politikaları, süreçleri ve liderliği tarafından şekillendirilmektedir. İyi bir siber güvenlik kültürü hem kültürün kurumsal belirleyicilerinin (politika, süreç, liderlik, sosyal normlar vb.) hem de kültürün bireysel belirleyicilerinin (tutumlar, bilgi, varsayımlar vb.), siber güvenlik bilincine sahip davranışlarda kendini gösteren, kurumun siber güvenliğe yaklaşımıyla uyumlu olduğu bir kültürdür.

İnsanlar hem siber saldırılara en iyi tepki veren hem de siber güvenlik zincirlerinin en zayıf halkasıdır. Bu nedenle, çalışanların ilk savunma hattı olma bilgisine ve içgüdüsüne sahip olduğu bir ortamı teşvik etmek çok önemlidir. İyi bir siber güvenlik kültürü oluşturmak, saldırıları ve ihlalleri önlemenin ötesine geçmektedir.

Interpol'e göre, COVID-19'un yarattığı hapsedilme, endişe ve korku duygusu, artan siber güvenlik tehditleri için mükemmel ortamı geliştirmiştir. Interpol'ün Siber Suç Tehditlerine Müdahale ekibi, önemli kuruluşlara ve virüs müdahalesiyle uğraşan altyapıya yönelik fidye yazılımı saldırılarının sayısında önemli bir artış tespit etmiştir.[263] Birçoğunun sıklıkla uzaktan çalışmaya devam edebileceği bir gelecekte, kuruluşların iş güçlerinin doğru davranışları benimsemesini sağlamak için daha kapsamlı bir yaklaşım düşünmesi gerekmektedir. Liderlerin farkındalık yaratmanın ötesine geçmeleri ve bir siber güvenlik kültürü aracılığıyla davranış değiştirmeye odaklanmaya başlamaları gerekmektedir.

Türkiye'de semboller, alışkanlıklar, kurallar, eserler ve diğer toplumsal yeteneklerin toplamı insan kültürünün nitelikleridir. Türkiye'de siber alanda kültürel bilgi işaret sistemleri için kodlanmıştır. Bu sistemlerde ifade edilen düşünce ve kavramlar bireyden ayrılarak bağımsız, kişisel olmayan bir varoluş kazanmaktadır. Kültür sayesinde medeniyetler, nesiller boyunca tarihlerini belgeleyebilir ve oluşturabilirler. Kültürün sembolik unsurları ve bu sembollerin sosyo-tarihsel anlamlar kazandırma biçimleriyle ilgili olmuştur. Türkiye'de kültür bir toplumu pekiştiren çeşitli bilgi, inanç ve etik kod biçimlerine atıfta bulunmaktadır. Olumlu ve olumsuz sloganlar ve eylemler, düşünceleri semboller ve şekillerle anlatma, geleneksel bilgiyi açığa çıkarma, dini söylemler, kurallar, partizanlık vb. gibi birçok unsur kültür ve toplum konusuna girmektedir.

2003 yılında, Birleşmiş Milletler Genel Kurulu, küresel bir siber güvenlik kültürünün oluşturulması kararını kabul etmiştir.[264] Devletleri, bilgi sistemleri

[263] Ashleigh Fowler ve Tom Everard. "What is Cyber Security Culture and why does it Matter for your Organisation?" [https://www.paconsulting.com/insights/what-is-cyber-security-culture-and-why-does-it-matter-for-your-organisation/] (er. tar. 12.06.2022).

[264] UNGA (2003). "Creation of a Global Culture of Cybersecurity", [https://digitallibrary.un.org/record/482184] (er. tar. 02.06.2022); UNGA (2018). "Advancing responsible State behaviour in cyberspace in the context of international security", [https://undocs.org/A/C.1/73/L.37] (er. tar. 02.06.2022).

ve ağlarını geliştiren, sahiplenen, sağlayan, yöneten, hizmet veren ve kullanan Hükümetler, işletmeler, diğer kuruluşlar ve bireysel kullanıcılar gibi tüm katılımcılar tarafından bilgi teknolojilerinin uygulanması ve kullanımında toplumları genelinde bir siber güvenlik kültürü geliştirmeye davet etmiştir. Siber güvenlik kültürüyle ilgili küresel kelimesi, yaklaşımın evrenselliğini, kurumsallığını, yerel ve uluslararası siber güvenlik düzeylerinin geniş kapsamını yansıtmaktadır.

Siber güvenlik politikalarında belirtilen faaliyetler, programlar ve projeler, ulusal siber güvenliğin sağlanması için ortak bir amaca hizmet etmektedir. Bunu başarmak için kültürel bağ, toplum yapısı, büyük bir uyum ve iş birliği gerekmektedir. Özellikle kritik altyapıların siber saldırılara karşı korunması için de uluslararası iş birliğine ihtiyaç duyulmaktadır. Ulusal iş birliğine örnek olarak, 2009 yılında BTK tarafından birçok kamu ve özel kuruluşun katılımıyla spam e-postaya karşı çalışma projesi gerçekleştirilmiştir. Proje sonunda spam mailleri ileten IP adresi sayısı yüzde 99 oranında azalmış ve günlük toplam spam mail sayısı 6,5 milyardan 394 milyona gerilemiştir.[265]

On üçüncü e-devlet yuvarlak masa toplantısında öne çıkan konulardan biri de kamu bilincinin yanı sıra kamu ve özel sektörün güvene dayalı iş birliğinin gerekliliği olmuştur. Türkiye Siber Güvenlik Yol Haritası temalı birçok kurumun katılımıyla 2012 yılında Ankara'da gerçekleştirilmiştir.[266] Türkiye Cumhuriyeti Resmî Gazetesi'nde siber güvenlik endeksi araştırması, Malezya ile Türkiye arasında siber güvenlik teknolojileri alanında olası iş birliğini içeren bir mutabakat zaptı olan uluslararası iş birliğine ilişkin bir bulguyu ortaya çıkarmıştır.[267] Olumsuz bir örnek, Kasım 2011'de Londra'da düzenlenen Siber Uzay Konferansı olmuştur.[268] Siber saldırılara karşı küresel düzeyde koordineli müdahalenin vurgulandığı konferansa katılan 60 ülke arasında Türkiye yer almamıştır.[269]

Uluslararası düzeyde siber güvenlik kültürü, devletler ve hükümetler arası kuruluşlar arasındaki ilişkiler tartışmalıdır. Jeopolitik olarak savunmasızdır ve uluslararası güvenliğin korunması için son derece önemlidir. BM Genel Kurulu

[265] Emin Ulaşanoğlu vd. (2010). "Bilgi güvenliği: Riskler ve Öneriler", *Bilgi Teknolojileri ve İletişim Kurumu*, s. 34.
[266] H. Şentürk vd. (2012). "Cyber Security…", s. 120.
[267] Resmî Gazete (16.06.2008). "2008/13685 Türkiye Cumhuriyeti-Malezya Ekonomik ve Ticaret Ortak Komitesi İkinci Dönem Toplantısı Mutabakat Zaptının Onaylanması Hakkında Karar".
[268] Symantec, "Global Internet Security Threat Report Trends for 2008", Sayı 14, (April 2009), [https://docs.broadcom.com/doc/istr-12-april-volume-17-en] (er. tar. 19.06.2022).
[269] H. Şentürk vd. (2012). "Cyber Security…", s. 120.

Birinci Komitesi'nin 73. Oturumu'nda yaptığı, iki jeopolitik muhalif olan Amerika Birleşik Devletleri ve Rusya Federasyonu tarafından aynı maddeye ilişkin iki karar taslağının başlatıldığı çalışma bunun iyi bir örneğidir. Her iki karar da siber alanda devletlerin sorumlu davranış standartlarını geliştirme ihtiyacını tanımlamaktadır. Ancak farklı amaçlar ve uygulama mekanizmaları vardır.[270] Uluslararası siyasetteki bu tür eğilimlerin arkasındaki nedenleri araştırmaya ve küresel siber güvenlik kültürüyle ilgili uluslararası söylemin senaryolarını tahmin etmeye ihtiyaç vardır. Türkiye'de siber güvenliği tesis etmek üzere ulusal siber güvenlik kültürünün oluşturulması ve toplumda bu konuda farkındalığın artırılması gerekmektedir.

3.1.3. Eğitim, Öğretim ve Beceriler

Siber Güvenlik Programları, stratejik planların belirli programlara ve ulusal ölçekteki projelere gerçekleştirilmesini analiz etmenin temel göstergesidir. Özellikle farkındalık artırıcı akademik faaliyetler, eğitim programları, tatbikatlar, araştırma geliştirme projeleri, kritik altyapının korunmasına yönelik özel savunma programları, risk yönetimi, veri tabanları veya web portalları gibi zafiyet analizleri ve uluslararası girişimlere katılım bu kapsamda değerlendirilebilecek konulardır. Devlet Planlama Teşkilatı'nın "Bilgi Toplumu Stratejisi ve Ek Eylem Planı 88", Ulusal Bilgi Sistemleri Güvenlik Programını belirlemektedir. Program, TÜBİTAK-UEKAE tarafından yürütülen 2005 Türkiye'nin Dönüşümü Projesi'nin devamı niteliğindeki bir proje olmuştur. Proje kapsamında;

- "Koordinasyon" maddesinde Ulusal Bilgisayar Olayları Müdahale Ekibi Koordinasyon Merkezi'nin kurulması,
- "Eğitim" maddesinde kamu kurumlarında görev yapan bilgi işlem personelinin eğitimi,
- "Dokümantasyon" maddesinde, kamu kurumlarına yönelik bilgi sistemleri güvenliği ile ilgili rehberlik dokümanlarının hazırlanması ve Bilgi Güvenliği Portalı üzerinden paylaşılması,
- "Yönetim" maddesinde seçilen kamu kurumlarına Bilgi Güvenliği Yönetim Sisteminin Bilgi Güvenliği Yönetim Sistemi (BGYS) kurulması,

[270] Paziuk Andrii ve Mitsik Vsevolod (2019). "Global Cybersecurity Culture in the International Discourse Values and Principles", s. 104, [http://journals.uran.ua/visnyknakkkim/article/view/175488] (er. tar. 22.06. 2022).

- "İzleme" maddesinde Siber Uzay Savunma Sistemi'nin kurulması ve uygulanması amaçlanmıştır.[271]

Bilgi Toplumu Stratejisi Eylem Planı Beşinci Değerlendirme Raporu'nda üniversite personeline siber güvenlik eğitimi verildiği; TR-BOME kullanıcı farkındalık eğitimi, CERT kurulum ve yönetimi eğitimi, olay müdahale ve sistem analizi eğitimi gibi ücretsiz çevrimiçi kurslar sağlamak için çalışmaktadır. BGYS Projesi için Başbakanlık ve Adalet Bakanlığı gibi birçok devlet dairesi ve bakanlığın risk analizi tamamlanmıştır. Ulusal Bilgi Güvenliği Kapısı projesi kapsamında (https://bilgiguvenligi.org.tr/) adresindeki web sitesinde siber güvenlik konularında teknik makaleler, standartlar ve rehberlik dokümanları ile bilgi güvenliği belgeleri yayınlanmaktadır. Ayrıca özel eğitim kurumları tarafından verilen çok sayıda siber güvenlik eğitim programı bulunmaktadır. Örneğin, Bilgi Güvenliği Akademisi tarafından 2011 yılının Temmuz ayında ilk kez bir siber güvenlik yaz kampı düzenlenmiştir. 20 kişilik bir üniversite öğrencisi grubuna beş hafta boyunca yoğun bir eğitim verilmiştir. Bilgi güvenliği bilgi ve deneyimlerini paylaşmak için etik hackerlar tarafından yönetilen bir çevrimiçi kütüphane olan (http://www.CEHTurkiye.com) gibi ücretsiz programlar da bulunmaktadır.[272]

Siber Güvenlik Tatbikatları kapsamında ilk CERT tatbikatı 20-21 Kasım 2008 tarihlerinde sekiz kamu kuruluşunun katılımıyla gerçekleştirilmiştir. Bilgi Sistemleri Güvenliği Tatbikatı başlıklı ikincisi ise 25-28 Ocak 2011 tarihleri arasında finans, elektronik haberleşme, eğitim, iç güvenlik ve savunma gibi farklı sektörlerden 41 kamu ve özel kurum ve bakanlığın katılımıyla gerçekleştirilmiştir. Üç günlük tatbikat sırasında, dağıtılmış hizmet reddi ve web sitesi güvenlik denetimleri dâhil olmak üzere 450'den fazla senaryo test edilmiştir. 2012 yılının ikinci döneminde de sadece internet servis sağlayıcıları ve GSM operatörleri için önemli bir CERT çalışması gerçekleştirilmiştir.[273]

Halkın farkındalığını artırmak amacıyla 23 Şubat 2010 tarihinde ilk kez bir güvenlik farkındalık günü gerçekleştirilmiştir. Ayrıca hükümet tarafından öğrenciler ve velileri tarafından bilgi sistemlerinin güvenli kullanımı hakkında faydalı bilgiler sağlayan bir kitapçık yayınlanmıştır. Konferans ve sempozyumla ilgili olarak Türkiye'de yeterli sayıda bu tür etkinlikler düzenlenmektedir.

---

[271] Bilgi Güvenliği Derneği, *SETA Medya*, [https://bilgiguvenligi.org.tr/] (er. tar. 22.06.2022).

[272] Kâmil Burlu (vd.) Certified Ethical Hacker, [http://www.CEHTurkiye.com] (er. tar. 22.06.2022).

[273] H. Şentürk (vd.) (2012). "Cyber Security…", s. 119-120.

2008'den beri devam eden Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (ISC), Siber Güvenlik ve Savunma ana temasıyla Mayıs 2012'de beşinci organizasyonunu gerçekleştirmiştir. Her yıl düzenlenen bu konferans, 19-20 Ekim 2022 tarihleri arasında 15. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (ISC) olarak yapılmıştır. Sunumların ve makalelerin tümü ISC web sitesinde (http://www.iscturkey.org) çevrimiçi olarak yayınlanmaktadır.[274] Diğer örnekler, Kamu Kurumları Bilgi Teknolojileri Güvenliği Konferansı 2011 yılında altıncı panelini, Eylül 2011'de ikincisini Ulusal Siber Güvenlik Çalıştayı, Ocak 2012'de Siber Güvenlik Hukuku Çalıştayı, Aralık 2011'de Siber Güvenlik Konferansı gerçekleştirmiştir.[275]

28 Temmuz 2006 tarihli Resmî Gazete'de 2006-2010 Bilgi Toplumu Stratejisi ve Eylem Planı yayınlanmıştır. Bu eylem planı ile siber güvenlik alanında 2010 yılından itibaren beş yıllık bir referans belgesi olduğundan ve ileriye dönük çalışmalara ışık tutması gerektiğinden bahsedilmiştir. Resmî Gazete'de 11 Haziran 2012 tarihli Bakanlar Kurulu kararıyla Türkiye'de "Siber Güvenlik Kurulu" kurulmuştur.[276] Siber Güvenlik Kurulu ile ulusal siber güvenlik stratejisi ve eylem planı hazırlanmasına karar verilmiştir. Bu karar, siber güvenlik alanında atılan en etkili adımdır. İlgili belge ile siber güvenliğin sürdürülebilmesi açısından üniversitelerin siber güvenlik uzmanı yetiştirebilmelerini tavsiye etmektedir.

2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı, Resmî Gazete'de yayınlanmıştır.[277] Şemsiye olarak görülen bu belge, hem 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nın hem de 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı'nın konularını kapsamıştır. 2015-2018 Eylem Planı'nda, "Bilgi Güvenliği ve Kullanıcı Güveni" alt başlığında eğitim, öğretim ve becerilerden bahsedilmektedir. Buna göre;

- Nitelikli insan kaynağını artırmak ve toplumda güvenli internet kullanımı konusunda farkındalık yaratmak amacıyla eğitim çalışmaları yapmak,
- Kurum ve kuruluşlar arasında iş birliği sağlamak ve siber güvenlik eğitimleri vermek,

[274] ISC Turkey, [http://iscturkey.org/] (er. tar. 22.06.2022).
[275] H. Şentürk vd. (2012). "Cyber Security…", s. 119.
[276] Resmî Gazete (20 Ekim 2012). "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar", Karar Sayısı 2012/3842.
[277] Resmî Gazete (6 Mart 2015). "2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı", Karar No 2015/4.

• Hukuki altyapının sağlanması ile siber güvenlik alanında asgari standartların hızla belirlenmesini öngörmüştür.

2020-2023 Ulusal Strateji Belgesi ve Eylem Planı'nda siber suçlarla mücadele için "Ulusal Siber Suç Stratejisi" hazırlanacağı belirtilmiştir. Bilişim suçlarına yönelik ihtisas mahkemelerinin kurulacağına yönelik bilgiler bu Eylem Planı'nda yer almıştır.[278] Türkiye'de siber güvenliği sağlamak için hukuki altyapının oluşması, mahkemelerin kurulması, bu alanda uzmanların yetiştirilmesi ve eğitim çalışmalarının yapılması önem arz etmektedir.

3.1.4. Yasal ve Düzenleyici Çerçeveler

Kullanılan modelin temel taşlarından biri düzenlenmediği takdirde en önemli sorun alanı olarak ortaya çıkan mevzuattır. Türkiye'de özel bir siber güvenlik yasası mevcut değildir.[279] Bakanlar Kurulu Kararı 20 Ekim 2012 tarihinde Resmî Gazete'de yayımlanarak yürürlüğe giren 2012/3842 sayılı Kanun, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın sorumlu mercii tarafından uygulanacak Türk ulusal siber güvenlik faaliyetlerinin uygulanması, yönetimi ve koordinasyonu konusunda birtakım sorumluluklar belirlemektedir.[280] Karar aynı zamanda Ulusal Siber Güvenlik Kurulu'nu da oluşturmaktadır.

5809 sayılı "Elektronik Haberleşme Kanunu" ile Bilgi Teknolojileri ve İletişim Enstitüsüne aşağıdaki maddeleri içeren sorumluluklar atanmaktadır:[281] "Bilgi güvenliği ve iletişimin gizliliğini korumak", "Yetkisiz erişime karşı sayaç sistemi sağlamak", "hizmet kalitesi ve elektronik haberleşme sektöründe, kamu düzeninde ve hizmetlerde milli güvenliğin uygulanmasına yönelik yasal düzenlemelerin emrettiği tedbirleri almak". Mevzuatın öngördüğü gerekli tedbirlerin alınması görevi Ulusal Bilgi Teknolojileri ve İletişim Kurumu tarafından yürütülmektedir.

---

[278] T.C. Adalet Bakanlığı (Nisan 2021). İnsan Hakları Eylem Planı Uygulama Takvimi, s. 54, 60, 104, 106.

[279] Neslihan Kasap ve Stéphanie Beghe Sönmez, "Cybersecurity in Turkey, [https://www.lexology.com/library/detail.aspx?g=39d8fdbc-ed93-4e91-b520-4a804a4b2f7f#:~:text=Turkey%20does%20not%20have%20any,breach%20of%20data%20protection%20law.] (er. tar. 26.05.2021).

[280] Resmî Gazete (20.10.2012). "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar", Karar Sayısı 2012/3842, Sayı 28447, [https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm].

[281] Resmî Gazete, "5809 Sayılı Elektronik Haberleşme Kanunu", [https://www.resmigazete.gov.tr/eskiler/2008/11/20081110M1-3.htm] (er. tar. 16.04.2021).

Türk hukukunda siber güvenliğin net bir tanımı yoktur. Siber güvenlik bir kavram olarak çeşitli düzenlemelerde kullanılmasına rağmen gerek tüzük gerekse içtihat yoluyla henüz tam tanımı yapılmamıştır.[282] Siber güvenlik ve veri gizliliği arasındaki ayrım herhangi bir otorite tarafından belirlenmemiştir. Siber güvenlik gereksinimleri, veri gizliliği yükümlülüklerine uyma açısından tanımlanmasına devam edilmektedir. Bununla birlikte, düzenleyici otoriteler tarafından çeşitli tanımlar kullanılmıştır.

BTK şu tanımı benimsemiştir; "Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıklarının güvenlik özelliklerinin, siber ortamların güvenlik risklerine dayanabilecek şekilde oluşturulmasını ve sürdürülmesini sağlamayı amaçlar. Siber güvenliğin ana hedefleri gizlilik, erişilebilirlik, bütünlüktür."[283]

Veri sorumluları, kişisel verilerin hukuka aykırı olarak işlenmesini veya erişilmesini önlemek ve korunmasını sağlamak için uygun bir güvenlik düzeyini sağlamak için gerekli teknik ve organizasyonel önlemleri almakla yükümlüdür. Kişisel Verilerin Korunması Kanunu (KVKK), alınması gereken teknik ve organizasyonel önlemleri açıkça belirtmemektedir. Bunlar vaka bazında değerlendirilmelidir. 6698 Sayılı KVKK[284] dâhil olmak üzere veri koruma mevzuatı, kişisel verilerin güvenliğine ilişkin genel gereklilikler içermektedir. Siber güvenlik ihlalleri bu nedenle veri koruma yasasının ihlaline yol açabilmektedir. 20 Haziran 2013 tarihinde Bakanlar Kurulu, ulusal siber güvenlik stratejisi hakkında kamu ve özel sektör tarafından işletilen BİT sistemleri ve kritik BİT altyapısı aracılığıyla devlet tarafından sağlanan hizmetlerin, işlemlerin ve verilerin korunmasını sağlamayı amaçlayan bir eylem planı şeklinde hazırlanması gerektiğini Resmî Gazete'de yayımlanmıştır.[285] Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, tanımların, ilkelerin, siber güvenlik risklerinin ve stratejik siber güvenlik amaçlarının ve eylemlerinin sunulduğu bir 2016-2019 ulusal bir siber güvenlik stratejisi ve eylem planı hazırlamıştır. Bu plan, Türkiye'nin siber güvenlik mevzuatını uluslararası standartlara göre şekillendirmeyi ve siber güvenlik alanında koordinasyonu sağlayan bir kamu otoritesi kurmayı hedeflemiştir.

[282] Mehmet Bedii Kaya (2019). "Hukuki Açıdan Bilişim Suçları, Siber Güvenlik ve Adli Bilişim", (Ed. Şeref Sağıroğlu, Mustafa Şenol), *Siber Güvenlik ve Savunma: Problemler ve Çözümler*, Ankara: Grafiker Yayınları, 1. Baskı, s. 255-258.

[283] M. B. Kaya (2019). "Hukuki Açıdan Bilişim Suçları, Siber Güvenlik…", s. 217.

[284] Resmî Gazete (Kabul Tarihi 24.03.2016). "6698 Sayılı Kişisel Verilerin Korunması Kanunu", Sayı 29677, Cilt 57.

[285] Resmî Gazete (20 Haziran 2013 tarihli ve 28683 Sayılı Karar). "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"nın kabulü, [https://www.resmigazete.gov.tr/eskiler/2013/06/20130620.htm] (er. tar. 22.12.2021).

Türkiye Cumhuriyeti'nin 2019 yılı On Birinci Kalkınma Planı, ulusal güvenliği artırmak ve birincil sektörlerde (örneğin kimya sanayi, ilaç ve tıbbi techizat, elektronik, otomotiv ve raylı sistem aracı vb.) teknolojik dönüşümü sağlamaya önem vermiştir. Bu doğrultuda Türkiye'nin siber güvenlik ve veri gizliliği teknolojilerini geliştirmesi, nitelikli insan sayısındaki boşluğu doldurması, idari yapılarını geliştirmesi ve mevzuatını sürekli gelişen teknolojiye ayak uydurması kalkınma planının temel konuları oluşturmuştur.[286] Öte yandan 2018 yılında kurulan DDO, kamu hizmetlerinde dijitalleşmenin sağlanması ve kamuoyunun bilinçlendirilmesi amacıyla siber güvenlik ve veri güvenliği alanında bir dizi çalışma ve proje yürütmektedir.[287]

5 Temmuz 2019 tarihinde Cumhurbaşkanlığı tarafından yayınlanan Bilgi ve İletişim Güvenliği Önlemlerine İlişkin Cumhurbaşkanlığı Genelgesi'nde, verilerin yerelleştirilmesi için gereksinimler ve bulut hizmetlerinin kullanımına ilişkin sınırlamalar dâhil, kritik verilerin güvenliğinin artırılmasına yönelik bir dizi önlem yer almaktadır. Genelge öncelikle kamu kurum ve kuruluşlarını ilgilendirdiği gibi, bankacılık ve finans, elektronik haberleşme, ulaşım, enerji, su yönetimi ve kritik kamu hizmetleri gibi kritik altyapı sektörlerinde hizmet veren özel kuruluşları da ilgilendirmektedir.[288] Genelge ayrıca, DDO'nun kamu kurum ve kuruluşları ile kritik altyapı hizmetleri sunan kuruluşlar tarafından uygulanmak üzere Bilgi ve İletişim Güvenliği Kılavuzu hazırlaması öngörülmüştür. Bu kurumların mevcut bilgi sistemleri, kılavuzda belirlenecek ilkelerle kademeli olarak uyumlu hale getirilmesi amaçlanmıştır.

KVKK, bağlayıcı olmayan teknik ve organizasyonel önlemlere ilişkin yönergeler yayınlamıştır. Bu yönergeler, kişisel verileri işleyenler tarafından atılması gereken birkaç adım önermektedir. Uygun bir güvenlik duvarı yerleştirilmelidir. Tüm uygulamalar ve yazılımlar, güncel tutulmaları gerektiği anlamına gelen siber saldırılara karşı korunmalıdır. Kişisel verileri içeren sistemlere erişim sınırlandırılmalıdır. Çalışanlar, bilgiye yalnızca bilmesi gerekenler temelinde erişebilmelidir. Kaba kuvvet algoritmasının kullanılması, güçlü parolaların kullanılması gerekliliği ve en yaygın saldırılara karşı koruma sağlamak için parola giriş denemelerinin sayısında sınırlamalar da önerilmektedir.

---

[286] Resmî Gazete, (20 Haziran 2013 Tarihli ve 28683 Sayılı Karar). "Ulusal Siber Güvenlik…".

[287] Resmî Gazete (10 Temmuz 2018 Tarihli ve 30474 Sayılı Karar). [https://cbddo.gov.tr/mevzuat/1-nolu-cbk/] (er. tar. 22.12.2021).

[288] Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri 12 Sayılı Genelgesi (2019). [https://cbddo.gov.tr/mevzuat/2019-12-sayili-bilgi-guvenligi-tedbirleri-cumhurbaskanligi-genelgesi/] (er. tar. 17.01.2022).

Sistemi periyodik olarak gözden geçiren ve kötü amaçlı yazılımları tespit eden anti-spam ürünleri kullanılmalıdır. Veri sızıntısı programlarının bütünleşmesi de koruyucu bir önlem olarak kabul edilmesi öngörülmelidir. Yönergeler ayrıca verileri korumak için teknik yöntemler olarak takma isimlendirme, mikro birleştirme, küresel kodlama, farklılaştırılmış şifre sistemleri, kısmi gizleme ve değişkenlerin iade edilmesini önermektedir.[289]

Türkiye, kritik altyapıya yönelik siber tehditleri ele alan özel bir mevzuata sahip değildir. Ancak sektöre özel düzenlemeler, finansal hizmet sistemleri gibi ilgili sektörlerde kritik altyapının korunmasına yol açmaktadır. Ayrıca, elektronik haberleşme hizmetleri, elektronik ağlar, altyapı ve enerji tesisleri sağlayan kuruluşlar için ISO/IEC 27001 standardının kullanılması zorunludur. Ayrıca, bankacılık sektöründe Tebliğ, verilerin korunması için iki faktörlü kimlik doğrulama yönteminin kullanılmasını zorunlu kılmakta ve risk analizinin bankanın ilgili birimi tarafından yapılmasını zorunlu kılmaktadır. Yönetmelik uyarınca siber güvenlik eğitimi verilmesi de zorunlu hale gelmelidir.[290]

Türk Ceza Kanunu, telefon görüşmelerine erişmeyi veya bunları kaydetmeyi veya özel postaya müdahale etmeyi ve açmayı suç saymaktadır.[291] Bunun ilke olarak elektronik haberleşmeyi de kapsaması gerekirken, mevzuatta bu konuda açık hükümler bulunmamaktadır. Bununla birlikte, elektronik iletişimin gizliliğinin de korunduğu genel olarak kabul edilmektedir. Bunun yeni siber güvenlik yasası kapsamında açıkça sağlanması beklenmektedir.

5271 sayılı Türk Ceza Muhakemesi Kanunu'nda, özel iletişimin gizliliğine ilişkin tek istisna, yasa dışı faaliyetlerde bulunduğundan şüphelenilen kişilerin iletişimlerine erişilebileceği öngörülebilmekte ve Cumhuriyet savcısının izni ile soruşturma ihtiyacı için kayıt altına alınabilmektedir.[292]

---

[289] Data Protection in Turkey, [https://www.kvkk.gov.tr/Icerik/5389/Data-Protection-in-Turkey] (er. tar. 17.01.2022), National Data Protection Authority, [https://www.dlapiperdataprotection.com/index.html?t=authority&c=TR&c2=GB] (er. tar. 17.01.2022).

[290] Türk Standartları Enstitüsü, "ISO/IEC 27001 Kişisel Verilerin Korunması Kanunu & ISO 27701 Kişisel Veri Yönetim Sistemi", [https://tse.org.tr/IcerikDetay?ID=2311&ParentID=9423] (er. tar. 17.06.2022).

[291] Türk Ceza Kanunu, Kişisel Verilerin Korunması 5237 Sayılı TCK, Madde 135 ve 136, [https://www.kisiselverilerinkorunmasi.org/mevzuat/5237-sayili-turk-ceza-kanunu/] (er. tar. 21.06.2022).

[292] Resmî Gazete (17.12.2004 Tarihli Ceza Muhakemesi Kanunu). Sayı 25673, [https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5271&MevzuatTur=1&MevzuatTertip=5] (er. tar. 21.06.2022).

Ağları veya verileri siber tehditlere karşı korumak amacıyla özel iletişime erişime izin veren bir yasa yoktur. Meta verilere erişimi düzenleyen herhangi bir yasa yoktur. 5070 sayılı "Elektronik İmza Kanunu" başlıklı Kanun, güvenli elektronik imzaya ilişkin teknik ölçütlerin yanı sıra Elektronik Sertifika Hizmet Sağlayıcılarının yetkilendirilmesi ve denetimine ilişkin hususları düzenlemektedir. 2007 yılında çıkarılan 5651 sayılı "İnternet Ortamında Yapılan Yayınların ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesinin Düzenlenmesi" başlıklı Kanun, internet aktörlerini içerik, konum, erişim ve erişim sağlayıcıları ve içerik denetimi açısından düzenlemektedir. Elektronik Ticaret Kanun Tasarısı, istenmeyen elektronik postalara ilişkin ikincil mevzuat yapma yetkisini, "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesine ve Mahremiyetin Korunmasına İlişkin Yönetmelik" yazışmaların gizliliğini, trafik verilerinin işlenmesini ve konum tespitini düzenlemektedir. İstenmeyen Elektronik İletilere İlişkin Yönetmelik Taslağı, spam SMS'lerin engellenmesine yönelik prosedürleri belirlemektedir. İnternetin Güvenli Kullanımına İlişkin Taslak İlke ve Prosedürler, operatörlerin güvenli internet hizmeti sunmasını düzenlemektedir. Devlet Planlama Teşkilatı Strateji Belgesi Eylem Planı 87, "Bilgi Güvenliğine İlişkin Düzenlemeler" başlıklı, mahremiyetin, sınıflandırılmış bilgilerin ve devlet bilgi güvenliği sistem ve ağlarının korunmasına yönelik mevzuatı belirlemektedir. Bu kapsamda Kişisel Verilerin Korunması Kanun Tasarısı 22 Nisan 2008 tarihinde TBMM'ye sunulmuş ancak onaylanmamıştır.[293] 5237 sayılı Türk Ceza Kanunu kapsamında suç olarak kabul edilen siber faaliyetler;[294]

- Bilgi sistemlerine yasadışı veya yetkisiz erişim sağlamak,
- Bilgi sistemlerini engellemek ve verileri değiştirmek veya yok etmek;
- Banka veya kredi kartlarının uygunsuz kullanımını sağlamak;
- Suçları işlemek için cihazlar, yazılımlar, şifreler veya diğer güvenlik kodlarını oluşturmak veya bir araya getirmek;

[293] Resmî Gazete (20.10.2012). "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar", Karar Sayısı. 2012/3842, Sayı 28447, [https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm](er.tar.21.06.2022); Resmî Gazete (23.05.2007). 5651 sayılı "İnternet Ortamında Yapılan Yayınların ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesinin Düzenlenmesi", Sayı 26530; Resmî Gazete (10.11.2008). "5809 Elektronik Haberleşme Kanunu", Sayı 27050.

[294] Resmî Gazete (26.09.2004 Tarihli Türk Ceza Kanunu). Sayı 25611, Tertip 5, Cilt 43, [https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5].

• Bunları üretmek, ithal etmek, teslim etmek, nakletmek, depolamak, kabul etmek, satmak, tedarik etmek, satın almak veya taşımak. Bu suçlar, bir yıldan üç yıla kadar hapis cezası ile cezalandırılabilmektedir (madde 134).

Kanuna aykırı olarak kişisel veri toplayan kişiler bir yıldan üç yıla kadar hapis cezasına çarptırılmaktadır. Veriler hassas kişisel veri ise fail hapis cezasına çarptırılmak suretiyle yargılanmaktadır. Kişisel verileri yasa dışı olarak aktaran veya kişisel verileri kamuya açık hale getiren kişiler iki ile dört yıl arası hapis cezasına çarptırılmaktadır (madde 136). Saklama süresi sona erdikten sonra verileri silmekle yükümlü olan ancak bunu yapmayan kişiler bir yıldan iki yıla kadar hapis cezasına çarptırılmaktadır (madde 138).[295]

DDoS saldırıları "bir bilişim sisteminin işleyişinin engellenmesi" fiiline karşılık geldiğinden, Türk Ceza Kanunu244/1 maddesi ile öngörülen suça karşılık gelmektedir. 5237 sayılı Türk Ceza Kanunu'nun 244/1. maddesi uyarınca "Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır."[296]

Yasal çerçeve bağlamında; 2012/3842 sayılı Bakanlar Kurulu kararı ile kurulan Ulusal Siber Güvenlik Kurulu'nun yürürlüğe girmesinden sonra, çoğu mevzuat değişikliğinin ve diğer köklü faaliyetlerin daha hızlı gerçekleşeceği düşünülmüştür. Türk Ceza Kanunu'ndaki mevcut üç bilişim suçunun kapsamı, ileri teknoloji içeren suçları kapsayacak şekilde genişletilmelidir. Ulusal yasalar Avrupa Siber Suçlar Sözleşmesi'ne paralel olarak uyarlanmalıdır. Genç ve eğitimli nüfusa sahip, özellikle yazılım mühendisliği konusunda yetenekli bir ülke olarak, üretim süreçlerinde gerekli güvenlik standartları ve ilgili ölçütler uygulanarak daha güvenli yazılım ve donanım sistemlerinin geliştirilmesi zorunlu hale getirilmelidir. Kişisel Verilerin Korunması Kanun Tasarısı yürürlüğe geçirilerek siber güvenlik alanında daha ileri adımlar atılmaktadır. Ayrıca dikkat edilmesi gereken bir diğer husus, internet servis sağlayıcılarına bilgi güvenliği ihlallerini önleme yetkisi ve yükümlülüğünün verilmesi de yasal ve düzenleyici çerçeve hususunda önem arz etmektedir.

Üçüncü Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı nihai raporu ile uyumlu olarak, siber suçların analizi için bir adli enstitü (adli bilişim eğitimleri) ve yeni bir yönetişim (e-yönetişim) modeli oluşturulmuştur. 2012 Siber Güvenlik Hukuku Çalıştayı sonuç bildirgesinin de gösterdiği gibi, bu

[295] Resmî Gazete, 26.09.2004 Tarihli Türk Ceza Kanunu, Sayı 25611, Tertip 5, Cilt 43.
[296] Sacit Yılmaz (2011). "5237 Sayılı Türk Ceza Kanunu'nun 244. Maddesi'nde Düzenlenen Bilişim Alanındaki Suçlar", *TBB Dergisi*, Sayı 92, ss. 62-100.

belgede açıklanan ve analiz edilen mevcut düzenlemeler siber güvenlik hukuki altyapısını desteklemek için yeterlidir. Ancak alandaki mevcut tüm ihtiyaçları karşılamaya yeterli değildir. Sorumlu otorite ve kuruluşlar bağlamında, kurulan Ulusal Siber Güvenlik Kurulu en kısa sürede toplanmalı ve siber güvenlik konusunda uzun süredir devam eden stratejik eylemleri başlatmalıdır.

Kritik altyapılar için Ortak Olay Müdahale Merkezleri kurulmuştur. Araştırma ve geliştirme için devlet teşvikleri, ulusal olarak kritik siber güvenliği içerecek şekilde genişletilmelidir. Devam eden ve gelecekteki tüm siber güvenlik programları belirli kuruluşlara atanmalı ve program denetimleri merkezi bir üst makam tarafından yapılmalıdır.

Türk Hukuku, bulut bilişimle ilgili güvenlik sorunlarını henüz özel olarak ele almamıştır. 2013 yılında BTK tarafından bir bilgilendirme notu yayınlanarak 2014 yılında Türk Standartları Enstitüsü tarafından bulut bilişim sistemlerine yönelik taslak standartların yayınlanmasına yol açmıştır.[297] Bunlar henüz kesinleşememiştir ve dolayısıyla bağlayıcılığı da bulunmamaktadır.

BTK tarafından hazırlanan 2019-2023 Strateji Planı, bulut bilişim hizmetlerinin geliştirilmesi ve yaygınlaştırılması için gerekli yasal ve idari düzenlemelerin yapılacağını belirtmektedir. Bulut hizmetlerinin kullanımı, bir Türk kuruluşu tarafından işlenen kişisel verilerin Türkiye dışında bulunan bulut sunucularda saklanmasının, bu verilere kişiler tarafından erişilemese dahi uluslararası bir veri aktarımı olarak değerlendirileceği ölçüde KVKK kapsamında dolaylı olarak düzenlenmektedir. Bu nedenle, kişisel verilerin Türkiye dışına aktarılmasına ilişkin KVKK kurallarına uyulması gerekecektir. KVKK kapsamında kişisel veriler, ilgili kişinin açık rızası alınmadıkça veya kuruluş kanunla belirlenen istisnalardan birine dayanmadıkça yabancı ülkelere aktarılamamaktadır. Bankacılık sektöründe, Taslak Yönetmelik, bankaların özel bulut bilişim hizmetlerinden yararlanabileceklerini öngörmektedir. Ancak bulut hizmetleri sağlayıcısının sunucularının Türkiye sınırları içinde bulunması halinde bundan yararlanabileceklerini belirtmektedir.

[297] Bulut bilişim kavramı, altyapı, platform gibi kaynaklar veya yazılımla ilgili hizmetler, minimum yönetim çabası veya hizmet sağlayıcı etkileşimi ile hızlı bir şekilde sağlanabilen internet üzerinden mevcut olabilen modern BİT'nin bir olgusudur. Bulut bilişim mimarisi, herhangi bir model için bulut hizmeti sağlayıcılarının bilginin depolanması, işlenmesi ve taşınması için hayati bir rol oynamaktadır. Detaylı bilgi için bkz. Lipi Akter (vd.) (2013). "Information Security in Cloud Computing", *International Journal of Information Technology Convergence and Services (IJITCS)*, Sayı 3, No 4, ss. 13-22; Türk Standartları Enstitüsü, "ISO/IEC 27017 Bulut Hizmetlerinde Bilgi Güvenliği Yönetim Sistemleri (BBYS)", [https://www.tse.org.tr/IcerikDetay?ID=2311&ParentID=9423] (er. tar. 17.06.2021).

BTK, bilgi sistemlerinin korunmasına ilişkin karar ve eylemlerde bulunmaya yetkili düzenleyici kurumdur. Ancak, KVKK siber güvenlik açısından şu anda gereklilikler getiren genel mevzuat olduğundan, bağlayıcı kararlar vermeye ve idari para cezası vermeye yetkili düzenleyici bir makamdır. Siber suçların Türk Ceza Kanunu'nda tanımlandığı ölçüde, savcılar ve ceza mahkemeleri de bu tür suçlarla ilgili soruşturma, ifade ve yaptırım uygulama yetkisine sahiptir. KVKK, veri güvenliğini sağlama yükümlülüğünün yerine getirilmemesi durumunda on beş bin ile bir milyon lira arasında değişen bir para cezası ile sonuçlanabileceğini öngörmektedir.[298]

Bankacılık sektöründe Bankacılık Düzenleme ve Denetleme Kurumu'nun (BDDK) da bankanın gelirine göre hesaplanan cezalar için uygulama yetkisi bulunmaktadır. Ancak bu resmi bir üst sınıra tabi değildir ve BDDK tarafından ihlal bazında belirlenebilmektedir.

Tazminat davaları, taraflar arasında sözleşme ilişkisi varsa haksız fiil veya sözleşmeden doğan sorumluluk da dâhil olmak üzere hukukun genel ilkeleri temelinde açılabilmektedir. Veri ihlalinin kişisel verileri etkilemesi durumunda, KVKK açıkça veri sahiplerinin verilerinin kanuna aykırı olarak işlenmesi halinde tazminat hakkını öngörmektedir. Veri ihlali fikri mülkiyet haklarının ihlali ile sonuçlanmışsa, fikri mülkiyet hukuku temelinde de tazminat talep edilebilmektedir. Bir şirket, yöneticilerinin kurum içinde yeterli siber güvenlik önlemlerini uygulamaması nedeniyle zarara uğramışsa, bu, görevlerin ihlali olarak nitelendirilebilmekte ve Türk Ticaret Kanunu uyarınca yöneticilere karşı sorumluluk iddialarının temelini oluşturabilmektedir.[299] Ayrıca çoğu şirket, kendi çalışanlarına dahi olsa internete erişim sağladıkları sürece, 5651 sayılı İnternet Kanunu ve ilgili yönetmelikler kapsamında üç yıl boyunca internet "log" kayıtlarını tutmakla yükümlü olabilmektedir.[300]

Telekomünikasyon sektöründe, BTK tarafından 2008 yılında yayınlanan Elektronik Haberleşme Sektöründe Ağ ve Bilgi Güvenliği Yönetmeliği, ağ ve güvenlik ihlallerine ilişkin kayıtların iki yıl süreyle tutulmasını şart koşmaktadır. Bankacılık sektöründe bankalar veri ve logların kayıtlarını tutmakla yükümlüdür.

---

[298] Resmî gazete (24.03.2016 tarihli Kişisel Verilerin Korunması Kanunu), Sayı 29677, No 6698, Tertip 5, Cilt 57, Beşinci Bölüm, Madde 18b.

[299] Data Protection in Turkey, [https://www.kvkk.gov.tr/Icerik/5389/Data-Protection-in-Turkey], National Data Protection Authority, [https://www.dlapiperdataprotection.com/index.html?t=authority&c=TR&c2=GB] (er. tar. 17.06.2021).

[300] Resmî Gazete, "04.05.2007 Tarihli İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkındaki 5651 No'lu Kanun", [https://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm] (er. tar. 17.06.2021) .

Ancak kayıtların ne kadar süreyle saklanması gerektiği şu anda belirsizdir. İnternet Yasası kuruluşların tüm e-ticaret ve çağrı merkezi işlemlerinin daha sonra kanıt amacıyla kullanılabilecek günlüklerini tutmasını şart koşmaktadır. KVKK uyarınca, bir veri ihlali veya siber saldırı tespit edildikten sonra mümkün olan en kısa sürede ilgili veri sahipleri bilgilendirilmelidir. KVKK kapsamında düzenli olarak siber güvenlik hakkında rapor verme zorunluluğu yoktur.[301]

Yasal önlemler (mevzuat, düzenleme ve spam mevzuatının kontrol altına alınması dâhil), bir devlete, suçların soruşturulması ve kovuşturulması ve kanuna uyulmaması veya kanunun ihlali durumunda yaptırım uygulanması yoluyla temel yanıt mekanizmaları kurma yetkisi vermektedir.

3.1.5. Standartlar, Organizasyonlar ve Teknolojiler

Türkiye, Uluslararası Standardizasyon Örgütü'nün (ISO) bir üyesi olduğundan, veri güvenliği alanında ISO/IEC 27001 standardında belirtilen şartlara uyulması gerekmektedir. ISO/IEC 27001, elektronik iletişim hizmetleri, elektronik ağlar ve altyapı ve enerji tesisleri sağlayan kuruluşlar için Türk hukukunda da geçerli ve zorunlu olan ortak bir standarttır.[302] Türkiye, ISO'nun bir üyesi olduğundan, veri güvenliği alanında ISO/IEC 27001 standardında belirtilen şartlara uyulması gerekmektedir. Bankacılık sektöründeki kurum ve kuruluşların, veri güvenliği ve bütünlüğünü sağlamak için BDDK tarafından yıllık olarak denetlenen Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri (COBIT) standartlarına uymaları gerekmektedir. Verilerin sürdürülebilirliği ve kriptografisi ile ilgili olarak ISO/IEC 23001 ve ISO/IEC 19790 standartları kullanılmış olmasına rağmen, bunlar zorunlu değildir.[303] Uygulamada, e-ticaret sektörünü destekleyen ödeme sistemi sağlayıcıları, çevrimiçi ödeme kayıtlarını ve kredi kartı numaraları gibi hassas verileri güvende tutmak için kredi kartı

[301] Resmî Gazete (2008). "Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği", Madde 17/2 ve Madde 29, [https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=19880&mevzuatTur=KurumVeKurulusYonetmeligi&mevzuatTertip=5] (er. tar. 17.06.2021).

[302] Türk Standartları Enstitüsü, "ISO/IEC 27001 Kişisel Verilerin Korunması Kanunu & ISO 27701 Kişisel Veri Yönetim Sistemi", [https://tse.org.tr/IcerikDetay?ID=2311&ParentID=9423] (er. tar. 17.06.2021).

[303] ISO/IEC 23001 (2020). Information Technology, "Part 10: Carriage of Timed Metadata Metrics of Media in ISO base Media File Format", [https://www.iso.org/standard/78824.html] (er. tar. 19.05.2021); [https://tse.org.tr/IcerikDetay?ID=2059] (er. tar. 19.05.2021).

kuruluşlarının dayattığı Ödeme Kartı Sektörü Veri Güvenliği Standardı'na (PCI DSS) uymaktadır.[304]

Standartlar, organizasyonlar ve teknolojiler açısından birçok sektörde siber güvenlik ve bilgi teknolojilerini geliştirmek, hükümet ve düzenleyici otoriteler için umut verici hedefler belirleyen çeşitli strateji ve kalkınma planlarının yayınlanmıştır. Bununla birlikte ülkede dijitalleşmeye yönelik artan bir eğilim olmuştur. Türk kamu otoriteleri, verimliliği, bütünlüğü ve sürdürülebilirliği artırmak için dijital platformları kullanmaya başlamıştır. Bunun en güncel örneklerinden biri Posta, Telgraf ve Telefon Kurumu tarafından verilecek elektronik çevrimiçi apostil hizmetleridir.[305]

Türk hükümeti siber güvenliği geliştirmeleri için kamu kurumlarını teşvik etmekte ve siber güvenlik standartlarının ve farkındalığının artırılması için çalışmaktadır. Bu doğrultuda, Savunma Sanayii Başkanlığı öncülüğünde tüm kamu kurumları, akademi ve özel sektör temsilcilerinin katkılarıyla Türk siber güvenlik ekosistemini geliştirmek amacıyla "Türkiye Siber Güvenlik Kümesi" kurulmuştur.[306]

Bir şirketin ISO 27001 standardına uymadığı, ISO yetkilendirilmiş denetçiler tarafından yapılan bir inceleme sonucunda tespit edilirse, belgelendirmesi askıya alınabilmekte veya iptal edilebilmektedir. Enerji sektöründe Enerji Piyasası Düzenleme Kurumu gibi kendi düzenleyici otoritesi tarafından ISO 27001 standardına uymak zorunda olan şirketlere, uyulmaması durumunda doğrudan yetkili düzenleyici tarafından idari para cezası uygulanabilmektedir. Bu yalnızca aşırı durumlarda geçerli olmakla birlikte, Türk düzenleyici kurumları, yasalara, düzenlemelere veya düzenleyici kararlara uyulmaması durumunda bir kuruluşun faaliyet ruhsatını askıya alma veya iptal etme yetkisine de sahiptir.[307]

2012 Ekim ayına kadar siber güvenlikten sorumlu merci TÜBİTAK ajansı olmuştur. 20 Ekim 2012 tarihi itibari ile Bakanlar Kurulu Kararı No. 2012/3842 Resmî Gazete'de yayımlanan sorumlu makam Ulaştırma, Denizcilik ve Haberleşme Bakanlığı olmuştur. Karar aynı zamanda Dışişleri ve Dışişleri

[304] PCI Security Standards Council (2018). "PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard", USA: PCI DSS v3.2.1 Quick Reference Guide.

[305] "Elektronik Apostil Sistemi" (2018). [https://www.ptt.gov.tr/Sayfalar/Kurumsal/DuyuruDetay.aspx?DetayId=26] (er. tar. 15.06.2021).

[306] "Türkiye Siber Güvenlik Kümelenmesi", [https://www.siberkume.org.tr/Index] (er. tar. 19.06.2022).

[307] Türk Standartları Enstitüsü, "ISO/IEC 27001 Kişisel Verilerin Korunması Kanunu & ISO 27701 Kişisel Veri Yönetim Sistemi", [https://tse.org.tr/IcerikDetay?ID=2311&ParentID=9423] (er. tar. 17.06.2021).

Bakanlıklarının üyelikleri ile Ulusal Siber Güvenlik Kurulu, İçişleri ve Savunma Bakanlığı ile Millî İstihbarat Teşkilâtı, Kamu Düzeni ve Güvenliği, Genelkurmay Başkanlığı, TÜBİTAK, BTK, Mali Suçları Araştırma Kurulu, Telekomünikasyon ve Haberleşme Komisyonu ve Bakanlıkça gerekli görülecek diğer müsteşar ve üst düzey yöneticilerden oluşmaktadır.

İki akredite CERT bulunmaktadır: Biri devlet tarafından yönetilen "TR-BOME", diğeri araştırma ve eğitim amacıyla işletilen TÜBİTAK'a ait olan "ULAK-CSIRT"tır.[308] TR-BOME uluslararası arenada da faaliyet göstermektedir.[309] TR-BOME, "Uluslararası Siber Savunma Çalıştayı, Güz 09- ICDW09" tatbikatında Türkiye'yi temsil etmiş ve 2009 NATO Tatbikatı Siber Koalisyon'una aktif olarak katılmıştır. Ulusal Bilgi Sistemleri Güvenliği Programı kapsamında kurulan CERT Koordinasyon Merkezi, ülke genelindeki kamu/özel kurumların bilgisayar güvenlik olaylarına müdahale etme becerisi kazanmasına yardımcı olma sorumluluğuyla görevlendirilmiştir.[310]

Siber Uzay Savunma Merkezi, Ulusal Bilgi Sistemleri Güvenliği Programı kapsamında Ankara'da kurulmuş bir araştırma merkezidir. Trafik verileri ve siber saldırılar hakkında istatistik toplayan sistemlere sahiptir. Faaliyetleri, kamu kurumlarına yönelik tehdit tespiti, siber saldırıların profillemesi ve raporlanması, uyarı ve tedbir alınması, botnet tespiti ve imhasına odaklanmaktadır.[311]

Çevre ve Şehircilik Bakanlığı, veri güvenliği, bilgi teknolojileri, akıllı altyapılar vb. alanlarında çeşitli iyileştirmeler sunan 2019-2022 akıllı şehirler strateji planını yayınlamıştır.[312] Akabinde 2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı yayınlanmıştır.[313] Birçok büyükşehir belediyesi, akıllı şehirler sistemi, toplu taşıma ve bayi makinelerinde ödeme sistemleri için veri toplama üzerinde çalışmaktadır. Amaç, halka açık yerlerde ödemeler için bir şehir kartını tanıtmaktır. Bu durum, artan siber güvenlik önlemlerine duyulan ihtiyacı beraberinde getirmektedir. Önemli gelişmelerden bir diğeri de tapu kayıt

[308] Resmî Gazete (20.10.2012). "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar", Karar Sayısı. 2012/3842, Sayı. 28447, [https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm] (er. tar. 15.06.2022)

[309] TR-BOME KM (Türkiye Bilgisayar Olayları Müdahale Ekibi- Koordinasyon Merkezi), (Ed. Mehmet Eriş) [http://ulakbim.tubitak.gov.tr] (er. tar. 15.06.2022); H. Şentürk vd. (2012). "Cyber Security…", s. 118.

[310] H. Şentürk (vd.) (2012). "Cyber Security…", s. 118.

[311] H. Şentürk (vd.) (2012). "Cyber Security…", s.118-119.

[312] Akıllı Şehirler Stratejisi ve Eylem Planı 2019-2022, Türkiye Çevre ve Şehircilik Bakanlığı Coğrafi Bilgi Sistemleri Müdürlüğü.

[313] Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı 2020-2023, Türkiye Çevre ve Şehircilik Bakanlığı.

sistemiyle ilgili olup, tapu kütüklerinin çevrimiçi kayıt tutmaya ve tapu işlemleri için çevrimiçi ödeme kabul etmeye başlamasıdır. Ticaret sicili başvuruları veya veri sorumlusu siciline kayıt gibi bir dizi başka birçok formalitede artık çevrimiçi sistemler üzerinden yapılmaktadır.

Türk veya yabancı sermayeli Türk kuruluşları veya yerel bir şube aracılığıyla iş yapan yabancı kuruluşlar, Türkiye'de iş yapan tüm kuruluşlar için yasal yükümlülükler aynıdır. Bununla birlikte, yabancı sermayeli Türk kuruluşları ve Türkiye'de iş yapan yabancı kuruluşlar, Türkiye'de üretilen verileri, KVKK kapsamında kısıtlamalarla karşılaşacakları Türkiye dışındaki yargı alanları ile pekiştirmeye ihtiyaç duyacaktır. BTK, Türkiye'nin telekomünikasyon düzenleyici ve denetleyici kurumu olarak siber güvenlik konularını düzenlemeye yetkilidir. BTK'nın kararları şirketler üzerinde doğrudan bağlayıcı olmakla birlikte, otorite ayrıca tavsiyeler ve yönergeler de yayınlamaktadır. BTK'nın tavsiyelerine göre, verilerle ilgilenen her kuruluş, bilgi sistemlerindeki zayıflıkları belirlemek için yıllık sızma testleri yapmalıdır. Bu test bankacılık sektöründe gereklidir, ancak Yönetmelik uyarınca, testin yıllık olarak bağımsız bir firma tarafından yapılması zorunlu hale gelmektedir. BTK ayrıca veri güvenliğini artırmak ve veri sızıntısı riskini en aza indirmek için veri sınıflandırması, veri yönetişim projeleri ve kriptoloji yöntemlerinin benimsenmesini tavsiye etmektedir.[314]

Siber güvenlik çerçevesi oluşturmak ve siber saldırılara karşı dayanıklılığı belirlemek için AB çapında bir sertifika sistemi sağlanmıştır. 2019 yılı AB Siber Güvenlik Yasası, Avrupa Parlamentosu'nda onaylanmıştır.[315] KVKK ve Ödeme Sistemleri Kanunu büyük ölçüde AB mevzuatına göre modellendiğinden, Türkiye'nin gelecekteki siber güvenlik kodunun Siber Güvenlik Kanunu'na benzer olması beklenmektedir. Siber güvenlik uzmanlarıyla yapılan toplantılarda BTK yetkilileri, örnek olarak büyük ölçüde Siber Güvenlik Yasası'na atıfta bulunmaktadır.

Genel olarak, Türkiye'deki siber güvenlik ekosistemi, özellikle kamu ve bankacılık sektöründe, sağlık, telekomünikasyon ve enerji gibi kritik özel sektörlerden daha fazla strateji, plan ve proje hazırlanması gerekmektedir. Bununla birlikte, siber güvenlik konularıyla ilgilenen Türk kamu yetkilileri,

[314] Bilgi Teknolojileri İletişim Kurumu (BTK) (12 Haziran 2019). "Kişisel Veriler ve Kişisel Bilgi Güvenliği", [https://internet.btk.gov.tr/kisisel-veriler-ve-kisisel-bilgi-guvenligi] (er. tar. 23.06.2022).

[315] "The EU Cybersecurity Act: a new Era dawns on ENISA", [https://www.enisa.europa.eu/news/enisa-news/the-eu-cybersecurity-act-a-new-era-dawns-on-enisa] (er. tar. 17.06.2021).

piyasa oyuncularından geri bildirim almaya ve onları yeni düzenlemeleri şekillendirme sürecine dâhil etmeye oldukça açık olmaları gerekmektedir. Bu alanda, süreçte mümkün olan en kısa sürede düzenleyici makamlarla ilişki kurmak, ihtiyaçlarını bu makamlara bildirmek ve önerilen düzenlemelerle ilgili yapıcı geri bildirim sağlamak önemlidir. Türkiye'nin taahhüdü, Türkiye'nin siber güvenlik vizyonuna ulaşma arzusu, kararlılığı ve gerçek adımları ile ilgili tüm itici güçleri kapsamaktadır. Eylem planında siber tehditlerin iletişim, ulaşım, enerji, bankacılık, finans ve sağlık olmak üzere tüm sektörleri olumsuz etkileyebileceği belirtilmiştir. Bu nedenle siber alanda artan tehditlerle mücadele için tedbirlere hız verilmesi önem taşımaktadır.

Türkiye Ulaştırma ve Altyapı Bakanlığı, sivil toplum kuruluşları, üniversiteler, kamu ve özel sektör ile koordineli olarak 2020-2023 dönemi için bir eylem planı hazırlamıştır.[316] Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, stratejik hedeflerle ilgili olarak 40 eylem ve 75 uygulama adımı içermektedir. Planın temel amaçları, kritik altyapının siber güvenliğini korumak, operasyonel ihtiyaçlara yönelik ulusal teknolojik araçlar geliştirmek ve siber tehditlerle mücadele eden ekiplerin yetkinliklerini artırmaktır. Türkiye, siber güvenliği artırma çabalarının bir parçası olarak USOM'un açılışını yapmıştır. USOM, devlet tarafından işletilen BTK bir yan kuruluşu olmaktadır. USOM, BTK tarafından kurulan ve siber güvenlik uzmanlarını eğitmek için bir veri merkezi ve bir akademi de içeren bir ağın parçasıdır.[317] Dönemin Ulaştırma ve Altyapı Bakanı Adil Karaismailoğlu, Avcı, Azad ve Kasırga adlı yerli uygulamalar ile Türkiye'nin 325.000 siber saldırıyı önleyebildiğini söylemiştir.[318]

Bakan tarafından yayınlanan yazılı açıklamaya göre BTK tarafından geliştirilen Avcı yazılımı, komuta kontrol merkezinin zararlı yazılımlardan etkilenebilecek tehditleri ve sistemleri izlemesine olanak tanımaktadır. Azad ise yapay zekâ ile bilgisayarları tespit etmekte ve Kasırga internetteki açık

[316] Ulusal Siber Güvenlik Eylem Planı 2020-2023, [https://hgm.uab.gov.tr/haberler/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023-yayimlandi?PageSpeed=noscript] (er. tar. 17.06.2021); Ulusal Siber Güvenlik Eylem Planı 2020-2023, Cumhurbaşkanlığı Genelgesi, [https://teftis.ktb.gov.tr/Eklenti/78925,20201229-9pdf.pdf?0] (er. tar. 17.06.2021).

[317] USOM (2013). "Siber Olaylara Müdahale Ekipleri Kurulum Adımları", [https://www.usom.gov.tr/duyuru/2015/01/siber-olaylara-mudahale-ekipleri-kurulum-adimlari.html].

[318] Adil Karaismailoğlu (2020). "Yerli ve milli imkânlarla geliştirdiğimiz KASIRGA, AVCI ve AZAD uygulamaları ile son 3 yılda Türkiye'yi hedef alan 325 bin siber saldırı engellendi", T.C. Ulaştırma ve Altyapı Bakanlığı, [https://www.uab.gov.tr/haberler/turkiye-nin-siber-guvenligi-emin-ellerde] (er.tar. 19.06.2021).

kaynakları denetlemektedir. Karaismailoğlu, GCI 2019 raporunda, Türkiye'nin bu alanda dünyanın en güvenli 20 ülkesinden biri haline geldiğini belirtmiştir.[319] Türkiye Cumhurbaşkanı Erdoğan bir açılış töreninde yaptığı konuşmasında, konuyla ilgili önceki yaptığı yorumlarının altını çizmiştir; "Gün geçtikçe yaygınlaşarak ve gelişerek hayatımızın ayrılmaz bir parçası haline gelen bilgi ve iletişim teknolojileri bize birçok fırsat sunarken siber güvenlik risklerini de beraberinde getiriyor".

Cumhurbaşkanı, 2023 hedeflerinin bir parçası olarak, birçok alanda olduğu gibi siber güvenlik alanında da Türkiye'yi uluslararası düzeyde daha ileriye taşıyacaklarını sözlerine eklemiştir. Ayrıca devletlerin vatandaşlarının dijital verilerini ve hizmetlerini koruma sorumluluğu ile ilgili çalışmaların önemini vurgulamıştır. Cumhurbaşkanı, "Yaklaşık 7 yıl önce Ulusal Bilgisayar Acil Müdahale Merkezi'nin kurulmasıyla aslında bu yönde ilk adımı attık… Mevcut ihtiyaç ve tehditleri göz önünde bulundurarak ülkemizin siber güvenlik politikalarına ilişkin kapsamlı ve bütüncül bir yaklaşımla yeni bir strateji belirlemek üzere harekete geçtik. Stratejimizi, son dönemde diğerlerinin yanı sıra dijital altyapılar ve siber güvenlik alanlarında engellerle karşılaştığımızdan, bazıları alenen, bazıları açıktan gizli kalarak yerli ve milli bir yaklaşımla şekillendirdik" demiştir.[320]

Cumhurbaşkanı, Türkiye'nin ilk iletişim uydusunun 2022'de uzaya fırlatma planını da açıklamıştır. "Kendi ulusal siber güvenlik teknolojilerimizi geliştirerek güçlü ve caydırıcı bir altyapı inşa ediyoruz. Yönlendirme teknolojisi üzerine hedefimiz doğrultusunda mavi vatandan siber alana her alanda egemen haklarımızı savunacağız" demiştir. [321] Florida'da SpaceX firmasına ait Cape Canaveral'daki fırlatma merkezinden 8 Ocak 2021'de Türksat 5A ve 19 Aralık 2021'de Türksat 5B uydusu uzaya gönderilmiştir. İlk sinyali alınan Türksat 5B uydusunun Falcon 9 roketiyle başarılı şekilde gerçekleştiği belirlendi. Bakan Karaismailoğlu, 2023 yılında TUSAŞ, ASELSAN CTECH firmaları ile tamamen terli ve milli olan Türksat 6A'nın uzaya fırlatılacağını söylemiştir.[322]

---

[319] A. Karaismailoğlu (2020). "Yerli ve milli…"; Türkiye Bilişim Derneği Küresel Gelişmeler Raporu (2019). [https://www.tbd.org.tr] (er.tar.19.06.2021).

[320] "Türkiye'yi, bilgi ve iletişim teknolojilerinde dünyanın en önde gelen ülkeleri arasına sokacağız" (2020). [https://www.tccb.gov.tr/haberler/410/116592/-turkiye-yi-bilgi-ve-iletisim-teknolojilerinde-dunyanin-en-onde-gelen-ulkeleri-arasina-sokacagiz-] (er. tar.19.06.2021).

[321] "Turkey reveals its three-year cybersecurity plan", *TRT World* [https://www.trtworld.com/magazine/turkey-reveals-its-three-year-cybersecurity-plan-42820] (er. tar. 20.05.2021).

[322] TRT Haber, "Türksat 6A 2023'te uzayda olacak" [https://www.trthaber.com/haber/gundem/turksat-6a-2023te-uzayda-olacak-729744.html] (er. tar. 11.03.2023).

BİT geliştirme ve kullanımı güvenlik ortamında başarılı olabilmektedir. Bu nedenle ülkelerin, yazılım uygulamaları ve sistemleri için kabul edilen minimum güvenlik kıstasları ve akreditasyon şemaları oluşturması ve kurması gerekmektedir. Bu çabaların, siber olaylarla ilgilenen ulusal bir organın, yetkili bir devlet kurumunun ve olayları izlemek, uyarmak ve bunlara müdahale etmek için ulusal bir çerçevenin uygulanmasıyla tamamlanması gerekmektedir.

DÖRDÜNCÜ BÖLÜM

SİBER GÜVENLİK POLİTİKALARI: İNGİLTERE ÖRNEĞİ

Yirmi birinci yüzyılın küresel iletişim sistemi, en büyük ve en karmaşık süreklilik gösteren bir sistem olmaktadır. Bireylerin ve toplumların genel anlamda güvendiği iletişim altyapısının yenilikçileri, kurucuları ve onun üzerinden sağlanan hizmetler, Birleşik Krallık'ta İnternet Servis Sağlayıcıları Derneği (ISPA) tarafından temsil edilmektedir.

Bu bölüm, siber güvenlik politikasındaki benzerlik ve farklılıkları görmek için İngiltere'deki siber güvenlik politikası ve stratejisi, siber kültür ve toplum, eğitim, öğretim ve beceriler, yasal ve düzenleyici çerçeveler, standartlar, organizasyonlar ve teknolojileri alt başlıklar halinde sunmaktadır. Çalışma, İngiltere'de siber güvenliği daha iyi anlamak için önde gelen BM kuruluşu olan ITU'nin verilerini, ulusal stratejik belgeleri, siber güvenlik endekslerini, siber güvenliğe yönelik kurum ve kuruluşları ve bu alanda yapılan diğer çalışmaları incelemektedir.

4.1. İngiltere'de Siber Güvenlik

Haziran 2009'da yayınlanan Birleşik Krallık Siber Güvenlik Stratejisi Belgesi, siber alanda güvenlik, esneklik ve dayanıklılık olarak ana temaları ele almaktadır. Yirmi birinci yüzyılın en büyük tehdidini siber güvenlik riskleri olarak belirlemekte, uluslararası koordinasyona, merkezi bir Siber Güvenlik Ofisi'nin kurulmasına ve mevcut doktrinel, siyasi ve yasal eksikliklerin belirlenmesi gerekliliğine dikkat çekmektedir.[323] 2011 yılında yayınlanan strateji belgesi, Birleşik Krallık'ı küresel alanda iş yapmak için en güvenli yerlerden biri haline getirmeyi amaçlamaktadır. Belge, İngiltere'nin siber suç birimi ve ulusal kritik altyapı koruma merkezi planlarını da özetlemektedir.[324]

İngiltere, 2009 yılında ilk ulusal stratejisi olan İngiltere Siber Güvenlik Stratejisini sunmuştur: "Siber Alanda Güvenlik, Güvenlik ve Dayanıklılık".

[323] Cabinet Office (Haziran 2009). *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyberspace*.

[324] Cabinet Office (2011) *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, [https://www.gov.uk/government/] (er. tar. 11.03.2023).

Ardından 2011-2015 dönemi için ikinci bir strateji olan İngiltere Siber Güvenlik Stratejisi'ni ortaya çıkarmıştır: "Dijital Bir Dünyada İngiltere'yi Koruma ve Teşvik Etme". Bununla birlikte, 2016'da başlatılan üçüncü strateji, İngiltere'nin siber güvenlik politikasında önemli bir değişikliğe işaret etmiştir. İngiltere'nin ulusal siber güvenlik politikasına yönelik hedeflerini detaylandıran mevcut çerçeveyi de oluşturmuştur.

Ulusal Siber Güvenlik Stratejisi 2016-2021[325], hükümetin İngiltere'nin siber tehditlere karşı güvenli, dirençli olması ve dijital dünyada müreffeh ve kendinden emin olması vizyonunu ortaya koymuştur. Vizyona üç kapsayıcı hedef eşlik etmiştir:

- Birincisi Savunma; İngiltere'yi gelişen siber tehditlere karşı savunmak, olaylara yanıt vermek ve İngiltere ağlarının, verilerinin, sistemlerinin dayanıklılığını ve korunmasını sağlamak için araçlara ulaşmak önem teşkil etmektedir. Bu hedef aynı zamanda vatandaşların, işletmelerin ve kamu sektörünün kendilerini savunma yeteneğini de kapsamaktadır.
- İkincisi Caydırıcılık: Suçluları takip etme ve kovuşturma ile birlikte saldırganları tespit etme, anlama, araştırma ve bozma becerisini kazanarak İngiltere'nin siber alandaki her türlü saldırganlığa karşı dirençli olmasını sağlamak ve böylece suçluları sorumlu tutmaktır. Bu hedef aynı zamanda siber alanda saldırgan yetenekler kullanma becerisini de içermektedir.
- Üçüncüsü Geliştirme: Kamu ve özel sektörde sürdürülebilir kalkınmaya ve becerilerin korunmasına yatırım yapmak ve siber güvenlik endüstrisinde, gelecekteki tehdit ve zorlukların karşılanmasına, üstesinden gelinmesine yardımcı olacak, dünya lideri bilimsel araştırma ve geliştirme ile desteklenen yeniliği teşvik etmektir.

Bu kapsayıcı hedefler, İngiltere'nin etkisini uygulamak, ülkenin ekonomik ve güvenlik çıkarlarıyla uyumlu siber alanın küresel evrimini şekillendirmesine yardımcı olan ortaklıklara yatırım yapmak için uluslararası eyleme yönelik destekleyici çalışmalardır. 2016-2021 ulusal stratejisi, ağırlıklı olarak merkezi hükümet için kilit bir role sahip müdahaleci bir strateji olmuştur. 2016-2021 Ulusal Siber Güvenlik Strateji Begesi, İngiliz hükümetinin siber güvenliğe

[325] İngiltere (2016-2021). "UK National Cyber Security Strategy" [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf] (er. tar. 12.11.2021).

yaklaşımını basitleştirmeyi, ulusal ve küresel ortaklıkları teşvik etmeyi amaçlamıştır.[326]

İngiltere'de siber alanı oluşturan hizmetlere ve bilgilere güven, her geçen gün artmaktadır.[327] İnternette gezinirken, alışveriş yaparken veya çevrimiçi sosyal ağ kurarken insanlar bunun farkında olabilirler. Ya da güvendikleri hizmetleri destekleyen ağ bağlantılı faaliyetin ve hükümetin, iş dünyası ve ulusal altyapı çalışmalarının bu yeni insan faaliyeti alanına ne kadar kritik derecede bağımlı olduğunun farkında olmayabilirler. Her iki durumda da siber alanın etkin işleyişi hayati önem taşımaktadır. "Digital Britain" raporunda:[328] "Dijital dünya, hayatımızın bir gerçeğidir" diye belirtilmiştir. Bu belge, hükümetin güvenliğini, emniyetini, dayanıklılığını sağlamak ve sunduğu fırsatlardan yararlanmak için ne yapacağını açıklayan bir rapordur.

İngiltere'nin siber alana bağımlılığı arttıkça, siber alanın güvenliği ulusun sağlığı için her zamankinden daha kritik hale gelmektedir. Siber alan, Ulusal Güvenlik Stratejisi'nde belirtilen tehditlerin ve itici güçlerin neredeyse tamamının üstesinden gelmektedir. Tüm toplumu etkilemekte, uluslararası sınırları aşmakta, büyük ölçüde anonim olmakta ve onu destekleyen teknoloji hızla gelişmeye devam etmektedir.[329] İngiltere'de siber alanı kullananlara yönelik tehditler, kimlik avından kredi kartı dolandırıcılığına ve kurumsal casusluğa kadar uzanmaktadır. Tüm bunlar, kuruluşları, bireyleri, kritik altyapıyı ve hükümet işlerini etkileyebilmektedir.

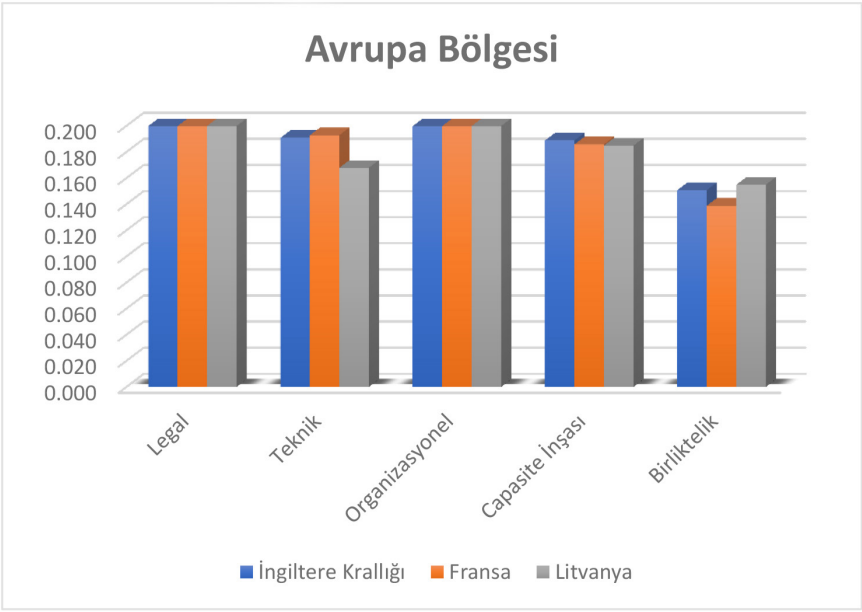
Tablo 7:[330] Avrupa Bölgesi

Üye Ülkeler	GCI Puanı	Yasal Önlemler	Teknik Önlemler	Organizasyonel Önlemler	Kapasite Geliştirme Önlemleri	İşbirliğine Dayalı Önlemler
İngiltere	0,931	0,200	0,191	0,200	0,189	0,151
Fransa	0,918	0,200	0,193	0,200	0,186	0,139
Litvanya	0,908	0,200	0,168	0,200	0,185	0,155

[326] Erik Silfversten (vd.) (2020). "Cybersecurity A State-of-the-art Review: Phase 2", *Final Report,* UK: RAND Europe, s. 146-147.
[327] UK (2009). *Cyber Security Strategy of the United Kingdom*, London: TSO.
[328] Detaylı bilgi için bkz. "Digital Britain Final Report "7650" (2009), London: TSO.
[329] UK (2009). *The National Security Strategy of the United Kingdom: Update 2009 Security for the Next Generation*, London: TSO.
[330] Global Cybersecurity Index 2018, *ITU,* s. 30.

Tablo 7'de verilen Avrupa Bölgesi'nden 3 ayrı ülkenin siber güvenlik kapasite olgunluk modelinin beş boyutu 0 ile 1 arasında bir ölçekte karşılaştırmalı olarak incelenmektedir. Bu doğrultuda Avrupa Bölgesi'nden bu üç ülkenin birbirine yakın GCI puanı vardır. Tablo 7'de İngiltere, Fransa ve Litvanya, beş sütunun tamamında puanları almaktadır. Bu üç ülke yasal ve organizasyonel önlemlerde aynı puanı almıştır.

Grafik 9:[331] Avrupa Bölgesi

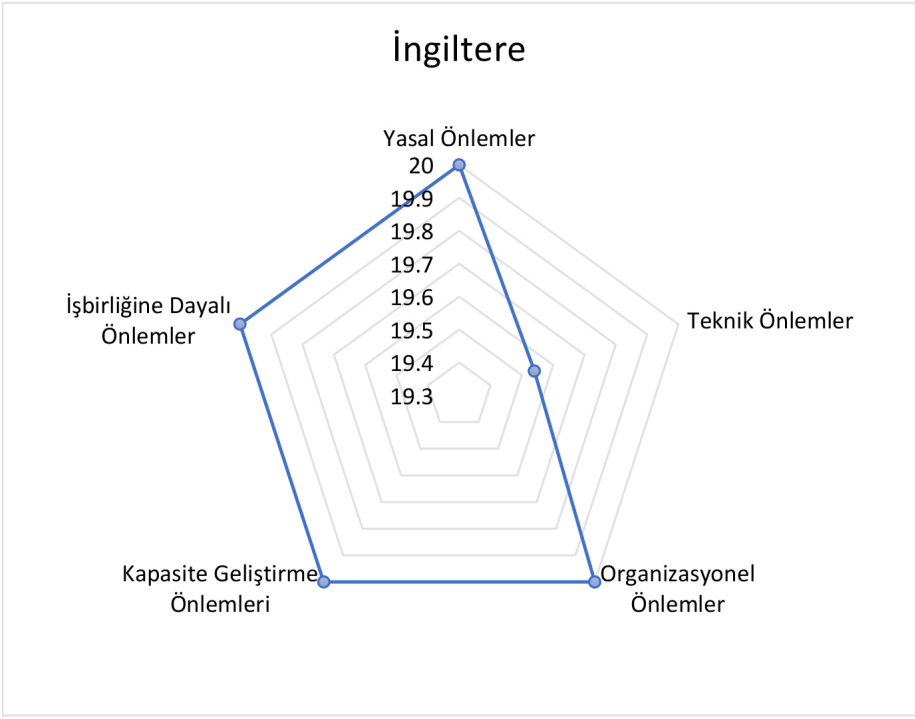


Grafik 9'da İngiltere, Fransa ve Litvanya, beş sütunun tamamında benzer puanları almaktadır. Yasal ve organizasyonel temellerde, tümü maksimum puan (0.2) almaktadır. Tüm ülkeler, teknik ve kapasite geliştirme sütunlarında yüksek ancak maksimum olmayan puanlar ile iş birliğine dayalı önlemler sütununda en düşük (ancak yine de yüksek) puanları göstermektedir. İngiltere, yasal önlemler sütununda ve organizasyon ayağında en yüksek puana sahip olarak ilk sırada yer almaktadır. İngiltere, Bilgisayarın Kötüye Kullanımı Yasası da (CMA) dâhil olmak üzere, siber suçlarla mücadele etmelerini sağlayan bir dizi yasal araca sahiptir.

[331] Global Cybersecurity Index 2018, *ITU,* s. 30.

Grafik 10:[332] İngiltere ve Kuzey İrlanda (Büyük Britanya)

Genel Puan	Yasal Önlemler	Teknik Önlemler	Organizasyonel Önlemler	Kapasite Geliştirme Önlemleri	İşbirliğine Dayalı Önlemler
99,54	20	19,54	20	20	20



Daha öncede belirtildiği gibi, 2020 Küresel Siber Güvenlik Endeksi'nin yinelemesi, her bir sütunun 20 puan ağırlıklı olduğu 0 ile 100 arasında bir ölçek olmaktadır. Bileşik ağırlıklı indeks olarak, her bir gösterge, alt gösterge ve mikro gösterge, gösterge grubuna göreli önemi verilen bir ağırlık atanmaktadır. Ağırlık, final puanları üzerinde önemli bir etkiye sahip olabilmekte ve farklı teknikler farklı sıralamalar üretebilmektedir. Verilerin altında yatan tüm ülke yanıtları, ITU ekibi tarafından doğrulanan anket verilerine göre rapor edilmektedir. Gösterge grupları, ağırlıklı aritmetik ortalamalar kullanılarak toplanmıştır. Bu, bir alanda düşük puan alan bir ülkenin, puanlarının bir kısmını başka yerlerde iyi yaparak telafi edebileceği anlamına gelmektedir.

[332] Global Cybersecurity Index 2020, *ITU, s*. 128.

2020 Küresel Siber Güvenlik Endeksi'nde ankete katılan ülkeler içerisinde Grafik 10'da İngiltere 99,54 puan ve 2. sırada yer almaktadır.[333] Bölgesel düzeyde anket çalışmaları incelendiğinde İngiltere 99,54 puan ile 1. sırada yer almaktadır.[334] Üçüncü bölümde verilen bilgiler ışığında, Türkiye ise bölgesel sıralamada 6. ve genel puanı 97,5'tu. Buna göre İngiltere beş boyutun dördünden tam puan (20) alırken, Türkiye üçünden tam puan (20) almıştır. Grafik 8 ile Grafik 10 karşılaştırıldığında; İngiltere, Türkiye'ye göre siber güvenlik kapasite olgunluk modelinde daha ileri olduğu görülmüştür.

Siber güvenlik kapasite olgunluk modelinin beş boyutu açısından grafik incelendiğinde İngiltere 20 ve 20'ye yakın puanlar aldığı gözlemlenmiştir. 2020 Küresel Siber Güvenlik Endeksi'ne göre ülkeler, "yoğun" bir sıralama yöntemi kullanılarak nihai puanlarına göre sıralanmıştır. Hassas radar grafiğine göre İngiltere teknik önlemlerde birtakım iyileştirmelere ihtiyaç duymaktadır. Yasal önlemler, İşbirliğine dayalı önlemler, kapasite geliştirme önlemleri ve organizasyonel önlemlerde yirmi ve teknik önlemlerde yirmiye yakın olduğu için ideal noktaya çok yakın olduğu görülmektedir.

Grafik 8'de Türkiye ve Grafik 10'da İngiltere'ye baktığımızda, eşdeğer konuma ulaşabilmeleri ve yirmi puanına erişmeleri için özellikle teknik önlemlerde birtakım iyileştirmelere ihtiyaçları olduğu anlaşılmaktadır. Grafik 10'da verilen bilgilere göre, İngiltere siber güvenlik politikaları kapsamında, beş boyutta toplanan kanıtlara dayanarak, CMM'nin ile ele alınan faktörlerin çoğu için ülkedeki siber güvenlik kapasitesi, yerleşik ve stratejik bir olgunluk aşaması arasında yer almaktadır. Ancak, "Strateji ve Politika" ve "Yasal ve Düzenleyici Çerçeveler" belirli faktörler için olgunluk daha yüksek (dinamik) bir aşamada görünmektedir. Ancak, CMM'nin konuşlandırılması sırasında izlenen yönteme göre, atanacak olgunluk aşaması için belirli bir aşamaya ilişkin göstergelerin tam olarak sağlanması gerekmektedir. Ayrıca, her iki grafikte gösterildiği gibi, bir dizi faktör için daha yüksek bir olgunluk aşamasında faaliyeti gösteren bazı göstergeler vardır. Aksi takdirde, gösterge verileri tamamlanan en yüksek aşamada tanınmaktadır.[335]

İngiltere'de siber güvenlik üzerine düzenli senaryo ve gerçek zamanlı siber tatbikatlar yapılmaktadır. Ulusal siber güvenlik stratejisini özellikle yerel düzeyde tam kapsamıyla uygulayacak bir mekanizma henüz mevcut değildir. Ulusal düzeyde siber olayların merkezi bir kaydı İngiltere Bilgisayar

[333] Global Cybersecurity Index 2020, *ITU, s*. 25.
[334] Global Cybersecurity Index 2020, *ITU, s*. 30.
[335] Maria Bada (ed.) (2016). *Cybersecurity Capacity Review of the United Kingdom*, Oxford: Oxford University, s. 16.

Acil Müdahale Ekipleri (CERT-UK) tarafından oluşturulmuştur ve CERT-UK tarafından tutulmaktadır. Ancak olay müdahalesi için merkezi bir sorumluluk yoktur ve tüm olayların rapor edilmesini sağlayacak net bir düzenleme (ya da bu tür siber olayları teşvik edecek bir düzenleyici rejim) yoktur. Koordinasyonla ilgili olarak, olaya müdahale sorumluluğu her bir kamu idaresi birimi, devlet dairesi ve bakanlık içinde tahsis edilmiştir. İngiltere Bilgisayar Acil Müdahale Ekipleri'nin (CERT-UK) desteklediği Siber Güvenlik Bilgi Paylaşım Ortaklığı (CiSP) platformunun kamu ve özel sektör arasında bilgi paylaşımını desteklemeye yardımcı olması beklenirken, bu mekanizma hala gelişmektedir. Nasıl ki paylaşılan bilginin doğası değişken ise operasyonel faydalar da değişken olabilmektedir. Kapasiteyi artırmak için, özellikle de hem Kritik Ulusal Altyapı (CNI) kuruluşlarının güvenlik duruşlarını güçlendirmelerine yardımcı olmak hem de İngiltere ulusal güvenlik duruşunu güçlendirebilecek bu alanda iş birliği için daha fazla mekanizmaya ihtiyaç vardır. Bu bağlamda yerel ve uluslararası düzey de dâhil olmak üzere, olay müdahalesi için tüm sektörler arasında çok seviyeli ulusal koordinasyona öncelik verilmesi, olay müdahalesi ve raporlamaya ilişkin düzenlemelerin taslağının oluşturulmasının yanı sıra, yerel olarak daha düşük hükümet düzeylerindeki olayları yakalamak için tanımlanmış bir mekanizmanın geliştirilmesi gerekmektedir.[336]

Düzenleyici olaylara müdahale açısından, düzenleyiciler ilgili bakanlıklar ve kurumlarla iş birliği yapmaktadır. Ancak gerekli esnekliğin farklı yorumları nedeniyle siber güvenlik olaylarına müdahale yönetmeliğine her zaman yeterince uyulmamaktadır. Bu nedenle, CNI varlıklarının listelenmesine öncelik verilmesi ve tehdit ortamındaki değişiklikleri yakalamak için düzenli olarak yeniden değerlendirilmesi gerekmektedir.

- Risk faktörünün sürekli değerlendirilmesini yapmak;
- Ağ ve sistem bağımlılıklarını değerlendirmek için düzenli denetim uygulamaları yapmak;
- CNI, kamu ve özel sektör arasındaki bilgi paylaşımına ilişkin resmi koordinasyonu güçlendirmek;
- Mevcut mevzuatı değiştirerek veya gerektiğinde yeni yasal düzenlemeler yaparak Kritik Ulusal Altyapı ile ilgili yasal çerçeveyi optimize etmek için prosedürleri yürütmek önem teşkil etmektedir.

[336] Maria Bada (2016). *Cybersecurity*..., s. 7-8.

Kriz yönetimi üzerine tatbikatların önemi kabul edilirken, özellikle yerel düzeyde bu tür tatbikatlara yapılan yatırım, muhtemelen bu tatbikatların değerini paydaşlara iletmedeki zorluktan dolayı yetersiz kalmaktadır. Bu nedenle, özellikle yerel düzeyde kriz yönetimi tatbikatlarına öncelik vermek ve tatbikatların değerini iletmek önemli olmaktadır.[337]

Devlet düzeyinde, siber güvenlik bir endişe kaynağıdır. Ancak geleneksel olarak kişisel bilgileri ele alan ve işlemeyen bölümler gibi devlet düzeylerindeki bölümler arasında farklılıklar vardır. Özellikle, yerel düzeyde riskler ve tehditler konusunda bir anlayış eksikliği bulunmaktadır. CERT-UK ve Devlet İletişim Merkezi (GCHQ) gibi siber güvenlik odaklı ajanslar, siber güvenlik zihniyetini benimseme konusunda en usta ve ikna edici olarak kabul edilmektedir. İngiliz halkı siber güvenlik tehditlerinin giderek daha fazla farkına varmaktadır. Bireyler bu tehditleri nasıl ele alacakları konusundaki anlayışları ile internet kullanıcılarının rutin uygulamaları arasında büyük farklılıklar vardır ve birçoğu internetin kabul edilen iyi uygulamaları günlük kullanımlarına dâhil etmemektedir. Genellikle endüstrinin dâhil olduğu veya endüstri tarafından yönetilen birçok girişimin olduğu bilinse de bu girişimler toplumun tüm gruplarını hedef almadığından dolayı, bunun toplum üzerinde sınırlı bir etkiye sahip olduğunu görmek doğaldır. Ortaya çıkan bir diğer hususta, uzmanlar ve toplumun diğer üyeleri arasındaki siber güvenlik kavramları arasındaki boşluk ve bu farklılığın uygulamaları nasıl etkileyebileceği olmuştur. Uzmanların genellikle sıradan bir kullanıcıdan gerçekçi olmayan beklentileri olmaktadır. Kuruluşların kendilerini yaygın siber saldırılara karşı korumalarına yardımcı olmak için koordineli, devlet destekli, endüstri destekli bir program olan "Cyber Essentials"[338] gibi farkındalık çalışmaları vardır. Siber güvenlik uygulamalarını eğitmek ve iyileştirmek için programlar ve materyaller kullanıma sunulmaktadır. Okullarda farkındalığı artırmaya yönelik artan bir çaba var olmaktadır. Bununla birlikte, İngiltere'deki bireylerin çoğunluğu çevrimiçi ortamda olası risklerin tam olarak farkında değildir. Çevrimiçi ortamda olası risklere karşı zamanla artan farkındalık bile toplumun siber alanda güvenli olduğunu göstermemektedir. Farkındalık olsa da uzmanlar tarafından uygun eylemlerin anlaşılmadığı veya uygun eylemlerin alınmadığı konusunda bir durum söz konusudur.[339]

Mevcut kapasitenin geliştirilmesine ilişkin olarak, kamu sektörünün, ulusal siber güvenlik stratejisiyle bağlantılı çeşitli hedef grupları kapsayacak şekilde

[337] Maria Bada (2016). *Cybersecurity*..., s. 9.
[338] NCSC (04.2021). "Cyber Essentials: Requirements for IT Infrastructure", UK: Cyber Essentials, ss. 1-17.
[339] Maria Bada (2016). *Cybersecurity*..., s. 10-11.

mevcut bilinçlendirme programlarını sürdürmesi ve genişletmesi gerekmektedir. Devletin alt kademelerinde riskler ve tehditler konusunda farkındalığı artırmak ve ayrıca özel sektörü bilinçlendirme eğitimi vermeye teşvik etmek gerekmektedir. İngiltere'de, özellikle genç kullanıcılar tarafından çevrimiçi hizmetlerin kullanımı artmaktadır. Ancak bu hizmetlerin güvenliğine yönelik alanda, buna karşılık gelen bir güven artışı olması gerekmemektedir. Çeşitli paydaşlar, güvenli hizmet sunumundan bağımsız olarak insanların çevrimiçi hizmetlere güvenme eğiliminde olduğunu ve bu desteklenmeyen güvenin siber güvenlik çabalarına zarar verebileceğini belirtmiştir. Bazı şirketler hizmetlerini çevrimiçi ortama taşımak için önemli bir çaba gösterse de, bu hizmetlerin güvenliği konusunda güven oluşturmaya yönelik eşgüdümlü bir program yoktur. Ayrıca, e-devlet hizmetlerine güveni teşvik edecek eşgüdümlü bir program bulunmamaktadır. Maria Bada'nın editörlüğünü yaptığı çalışma da, İngiltere'de yapılan görüşmeler sonucu yerel çevrimiçi hizmetlerin ulusal düzeyde sunulanlardan daha güvenilir olabileceği ileri sürülmüştür.[340] Bu nitelikteki bir inceleme, bu tür görüşlerin sağlam temellere dayanıp dayanmadığını araştırmak önem teşkil etmektedir.

4.1.1. Politika ve Strateji

Siber Alan ve İngiltere Ulusal Güvenliği, siber güvenlik sorununa genel bir bakış sağlamaktadır. Toplum her alanda bilgi ve iletişim teknolojisine giderek daha fazla bağımlı hale gelmektedir. Bağımlılıkla birlikte maruz kalma ve kötüye kullanım, suç ve hatta saldırıya karşı savunmasızlık ortaya çıkmaktadır. Suçlular ve aşırılık yanlıları, toplumun bu kadar bağımlı hale geldiği aynı küresel teknolojik ortaklıklardan yararlanabilmektedir. Siber güvenlik, küresel bilgi ve iletişim teknoloji altyapısından yararlanan herkesin koordineli, yetenekli ve karşılıklı olarak güçlendirici bir yanıt gerektiren bir sistem olmasına karşın, hızlı gelişen ve karmaşık bir güvenlik sorununu da beraberinde getirmektedir. 1990'ların başından beri siber politika çalışmaları yürüten İngiltere, politika ve planlamayı desteklemek amacıyla 1994'teki İngiltere siber ilişkili öngörü programını yayınlamıştır.[341]

Modernite kavramsal olarak korkunun, belirsizliğin, teknolojik değişimin ve küreselleşmenin hızlanmasına eşlik etmiştir. Toplumlar güvenlik ve acımasız bir güvenlik arayışı içinde olan bir risk toplumunda yaşamaktadır.[342] Bu varoluşsal kaygının ortasında, Neoliberal siyasetin yükselişi, vatandaşların ve kuruluşların

[340] Maria Bada (2016). *Cybersecurity*..., s. 11.
[341] John Michael Schmidt (2015). "Policy, Planning, Intelligence and Foresight in Government Organizations", *Foresight*, 17(5), ss. 489-511.
[342] Anthony Giddens (1990). *The Consequences of Modernity,* UK: Polity, s. 23-25.

kendi suç risklerini yönetmeleri gerektiği bir "kontrol kültürü" getirmiştir. Bu tür bir sorumluluk, küçültülmüş devletin uzaktan yönettiği Neoliberal yönetişim yaklaşımının temel bir özelliğidir. Siber güvenlik alanı, bu düzenleyici modele çok uygun görünmektedir. Çünkü siber alan, doğası gereği, hükümetlerin insan davranışını düzenleme, vatandaşları ve işletmeleri koruma becerisine meydan okumaktadır.[343] Geç modernite içinde zaman ve mekânın uzaklaşmasını özetler ve siber suç, ondan gelen bir düzensizlik biçimi olmaktadır. Modernite içinde zaman ve mekânın uzaklaşmasını özetler ve siber suç, ondan gelen bir düzensizlik biçimidir. Siber alan, suç mağduriyetini değiştirmektedir. Bazıları tarafından "mekânsal-karşıtı" olarak tanımlanan siber alanda, bir kişi birçok kişiye aynı anda ve herhangi bir mesafeden saldırabilmektedir.[344]

Çalışma da, neoliberal etkinin yükselişini de göstermek önemlidir. İngiltere'de, suçun önlenmesi ve kontrol edilmesinde birey ve devlet sorumluluğunun kökenleri yaklaşık elli yıl öncesine dayanmaktadır. Toplu olarak, bazı özel hareketler, ilerlemeler ve değişiklikler bu sorumluluğun geliştiği zemini oluşturmaktadır:[345] hükümet artan mesafe ve artan suçtan kaynaklanan güvensizlikten, suçun önlenmesine yönelik stratejik geçişten ve suç mağduriyetiyle kaynaklanan yaklaşımdan kaçınmaktadır. Bu değişim üzerinden tarihsel bir rota çizmek, siber güvenlik için bireylerin sorumluluğu etrafındaki hükümet söyleminin daha bağlamsal olarak anlaşılmasını sağlayacaktır.

İngiltere yaklaşık elli yıl öncesinde derin sosyal ve mekânsal değişimden kaynaklı suçların ortaya çıktığı bir dönem yaşamıştır. Toplumsal doku bozulmuş, zaman ve mekân ayrılmış ve böylece sivil toplum daha geçirgen ve savunmasız hale gelmiştir.[346] Önceleri suç ve kabalık en çok yoksulları etkilemiştir. Orta sınıflar ile suç arasındaki sosyal mesafe büyük ölçüde azalmış ve beraberinde bakış açısı ve perspektif olarak yeni sonuçlar doğurmuştur.[347] Güvensizlik artmaya başlamıştır. Kasıtsız olarak devletin artan suça stratejik tepkisi yalnızca halkın endişesini artırmıştır. Ciddi suçlara odaklanması ve daha küçük suçlara toleranslı olması, birçoğunun İngiltere için inzivaya girdiğini düşünmesine

---

[343] Ulrich Beck (1992). *Risk Society: Towards a New Modernity*, London: SAGE, s. 2-7.
[344] Anthony Giddens (1990). *The Consequences ...,* s. 32.
[345] Neil MacEwan (2017). *Responsibilisation, Rules and Rule-following concerning Cyber Security: Findings from Small Business Case Studies in the UK*, PhD Thesis, UK: University of Southampton, s. 7.
[346] Anthony Giddens (1990). *The Consequences ...,* s. 17-20.
[347] David Garland (2001). *The Culture of Control: Crime and Social Order in Contemporary Society*, Oxford: Oxford University, s. 152.

neden olmuştur. İlerleyen yıllarda İngiltere'de internetin hayata girmesiyle siber alanda yapılan suçlar artmış ve bu alanda hükümetin çalışmaları başlamıştır.

İngiltere'deki hükümetin siber ilişkiler üzerine öngörü çalışmaları, doğrudan kabineye rapor veren bir merkezi hükümet kuruluşu tarafından yürütülmektedir. Ayrıca Savunma Bakanlığı, "Geliştirme, Kavramlar ve Doktrin Merkezi" ve "Birleşik Krallık Savunma Bilim ve Teknoloji Laboratuvarı" altında öngörü faaliyetlerini yürütmektedir.[348] Siber Güven ve Suç Önleme Projesi 2004 yılında İçişleri Bakanlığı Suç Azaltma, Polislik, Toplum Güvenliği ve Terörle Mücadele Bakanlığı bünyesinde bilim insanı ve çeşitli sektörlerden toplam 260 uzmanın katılımıyla gerçekleştirilmiştir. Projenin amacı, gelecekteki teknolojiler üzerinde araştırmalar yapmak, siber güven tesis etmek ve siber suçları önlemek için eylemler oluşturmaktır.[349]

Hiçbir hükümet ulusal düzeyde bir siber güvenlik politikası ve stratejisi veya politika ve stratejik uygulamadan sorumlu bir organ oluşturmamıştır.[350] Bir politika alanı olarak siber güvenlik hala gelişmektedir. Bununla birlikte, siber güvenlik koordinasyonu için kapsayıcı bir devlet organı tayin etmenin ve ulusal bir siber güvenlik stratejisi ve politikasına sahip olmanın önemi ne kadar vurgulansa yetersiz kalmaktadır. Bu önlemleri alan hükümetlerin siber olaylarla ve saldırılarla başa çıkması diğer ülkelere nazaran daha kolay olmaktadır. Bu boyut, hükümetin bir siber güvenlik stratejisi tasarlama, üretme, koordine etme ve uygulama kapasitesini araştırmaktadır.

İngiltere, kapsamlı bir siber güvenlik stratejisine sahiptir. Bu strateji, güçlü bir siber güvenlik yasal çerçevesi ve iki CERT ile tamamlanmaktadır. İngiltere Bilgisayar Acil Durum Müdahale Ekipleri (CERT-UK) temel olarak kritik altyapı operatörlerini desteklerken, GovCertUK devlet kurumlarını desteklemektedir. Diğer ilgili kurumlar arasında Milli Güvenlik Kurulu ve Siber Güvenlik ve Bilgi Güvencesi Dairesi bulunmaktadır. İngiltere ayrıca, özel sektörün aktif olarak katıldığı iyi gelişmiş bir kamu-özel sektör ortaklıkları sistemine sahiptir. Bu işbirlikçi yaklaşım, siber güvenlik stratejisi tarafından da güçlü bir şekilde desteklenmektedir. Örneğin Ulusal Altyapının Korunması

---

[348] Hasan Çiftçi (2019). *Technology Foresight and Modeling: Turkish Cybersecurity Foresight 2040*, PhD Thesis, Ankara: METU, s. 48; Cabinet Office (2011) The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf] (er. tar. 22.06.2022).

[349] Hasan Çiftçi (2019). *Technology Foresight and Modeling…,* s.48.

[350] Maria Bada (2016). *Cybersecurity…*, s. 18.

Merkezi (CPNI), sektörü kapsayan, sektöre özel bilgi alışverişi sağlamaktadır.[351] Böyle merkezlerin oluşu siber güvenlik alanında ilerleme kaydetmek isteyen ülkeler için referans niteliği taşımaktadır.

Strateji, güçlü bir ilkeler beyanı ve İngiltere'nin karşılaştığı siber güvenlik tehditlerinin bir değerlendirmesini içermektedir. Stratejide yer alan uygulama planı, temel belirlenen hedeflere dayanmaktadır. CPNI, İngiltere'nin kritik altyapısının korunmasıyla görevlendirilmiştir. CPNI'nın merkezi belgesi, 2010 yılında kabul edilen, Kritik Altyapının Doğal Tehlikelerden Kaynaklanmasına Karşı Dayanıklılığının Artırılmasına İlişkin Stratejik Çerçeve ve Politika Bildirimidir.[352]

İngiltere'de siber güvenlik politikası ve stratejisi, hükümet genelinde bir siber güvenlik gündemini yaygınlaştırmak için çok önemlidir. Çünkü siber güvenlikte diğer önemli politika alanlarına göre öncelik verilmesi, kilit siber güvenlik devlet aktörlerinin yetkilerini belirlediğinden ve kaynakların ortaya çıkan mevcut siber güvenlik sorunlarına yardımcı olduğundan, devlet genelinde bir siber güvenlik gündemini yaygınlaştırmak ve temelde incelemek önem teşkil etmektedir. İngiltere'deki bazı kuruluşlar, büyük ölçüde üç ilke etrafında yapılandırılabilen siber güvenlik sorumluluğuna sahiptir:[353]

- Kabine Ofisine ait olan politika koordinasyonu, geliştirme ve uygulama;
- Devlet İletişim Merkezi'ne (GCHQ), İngiltere ve Ulusal Siber Güvenlik Stratejisi'ne bağlı olan ulusal güvenlik;
- İstihbarat ve Savunma Bakanlığı tarafından yönetilen siber savunma.

Siber sorumluluğa sahip politika yapıcılar şunlardır: Başbakan (Milli Güvenlik Kurulu- Ulusal Güvenlik Stratejisinin Uygulanması), Kabine Ofisi, Dijital, Kültür, Medya ve Spor Dairesi (DCMS), Uluslararası Ticaret Departmanı, Eğitim Bakanlığı, İşletme, Enerji ve Sanayi Stratejisi Departmanı, Dışişleri ve Milletler Topluluğu Ofisi, Ev ofisi, Savunma Bakanlığı ve Ulaştırma Bakanlığı. Ulusal güvenlik perspektifinden temel siber güvenlik sorumluluğu, 2016-2021 Ulusal Siber Güvenlik Stratejisi aracılığıyla ulusal siber güvenlik otoritesi olarak hareket etmek üzere tek bir organ olarak kurulan İngiltere Ulusal

[351] "EU Cybersecurity Dashboard A Path to a Secure European Cyberspace" (2015), [https://cybersecurity.bsa.org/] (er. tar. 13.12.2021).
[352] Cabinet Office (2010). *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*, s. 8, [http://www.cabinetoffice.gov.uk/] (er. tar. 14.12.2021).
[353] Erik Silfversten (vd.) (2020). "Cybersecurity A State…", s. 147.

Siber Güvenlik Merkezi (NCSC) aittir.[354] Kuruluşundan bu yana ulusal siber olayları izlemekten, pratik rehberlik yoluyla bilgi paylaşmaktan ve sistematik güvenlik açıklarıyla mücadele etmekten sorumludur. [355]

Birden fazla paydaş, Ulusal Güvenlik Stratejisini hükümet genelinde uygulamaktadır. Strateji için bir gözden geçirme ve yenileme süreci vardır, ancak yıllık bazda değildir. Ulusal Siber Güvenlik Merkezi (NCSC), Birleşik Krallık'ın siber güvenlik ortamı konusundaki ulusal otoritesi olmak üzere GCHQ'nun bir parçası olarak 2017'de kurulmuştur. Buna göre, bilgi paylaşımı, sistemik güvenlik açıklarının ele alınması ve ulusal siber güvenlik konularında liderlik sağlanması önemli unsurlar arasında olmuştur.

2014 yılında yürürlüğe giren Devlet Güvenlik Sınıflandırmaları Politikası, 1989 yılı Resmi Sırlar Yasası da dâhil olmak üzere yerel kanunların gerektirdiği bilgiler için üç kademeli bir sınıflandırma sistemini detaylandırmıştır. Bilginin hassasiyetine ve bilgilerin ifşa edilmesiyle ilgili risk seviyesine göre üç sınıflandırma seviyesi ile belirlenmektedir. Sınıflandırma seviyeleri, bilgilerin ifşa edilmesiyle ilgili risk seviyesi dikkate alınarak belirlenmektedir. Politika daha sonra belirli güvenlik gereksinimlerini sınıflandırma düzeyine göre planlamaktadır. İngiltere'de Savunma Siber Koruma Ortaklığı (DCPP), savunma tedarik zinciri içinde siber güvenliği geliştirmek için kurulmuştur. Uygulama, farkındalık ve orantılı olarak standartlara odaklanmaktadır.[356]

CPNI, "Stratejik Çerçeve ve Kritik Altyapının Doğal Tehlikelerden Kaynaklanmasına Karşı Dayanıklılığının Artırılmasına İlişkin Politika Bildirimi" de dâhil olmak üzere politika belgelerinde "kritik altyapı koruması" için uygun bir tanım sağlamaktadır. İngiltere'nin Bilgi Güvencesi Ulusal Teknik Otoritesi tarafından güvenlik standartlarına ilişkin bazı ek gönüllü rehberlik sağlanmasına rağmen, İngiltere genellikle uluslararası sertifikasyon planlarını tanımaktadır. Haziran 2014'te Hükümet, Siber Gereklilikler Tablosu (Cyber Essentials Scheme)[357] olarak bilinen yeni bir siber güvenlik standardı yayınlamıştır. 1 Ekim 2014'ten itibaren İngiltere Hükümeti, hassas ve kişisel bilgi işleme sözleşmeleri için teklif veren tüm tedarikçilerin Siber Gereklilikler Tablosu'na göre sertifikalandırılmasını zorunlu kılmıştır.[358]

---

[354] İngiltere (2016-2021). "UK National Cyber Security Strategy".
[355] Erik Silfversten (vd.) (2020). "Cybersecurity A State…", s. 148.
[356] Prashant Mali, "Critical Analysis…", s. 5.
[357] Detaylı bilgi için bkz. NCSC (04.2021). "Cyber Essentials: Requirements for IT Infrastructure", UK: Cyber Essentials, ss. 1-17; Kabine Ofisi (25.05.2016). "Procurement Policy Note-Cyber Essentials Scheme", UK: Crown Commercial Service, ss. 1-11.
[358] Kabine Ofisi (25.05.2016). "Procurement Policy Note…", ss. 1-11.

İngiltere Hükümeti, 2010 yılında bir Ulusal Siber Güvenlik Stratejisi (NSS) geliştirmiş ve siber saldırıları "Aşama 1" tehdidi olarak derecelendirmiştir.[359] Bu strateji, güvenlik ile mahremiyete ve temel haklara saygıyı dengeleyen bir şekilde tehditlerle mücadele etmeyi amaçlamıştır. İngiltere hükümeti, yurtiçinde ve uluslararası alanda, siber alanın yeniliklere, özgür fikirlere, bilgi ve ifade akışına açık bir alan olarak kalmasını sağlamaya çalışmıştır. Bu strateji yapısı, riskleri azaltmaya, işletmeler ve bireyler için güvenilir bir dijital ortamın faydalarını sağlamaya odaklanmıştır. İngiltere Siber Güvenlik Stratejisi 2011-2015 yılları arasında özgürlük, adalet, şeffaflık ve hukukun üstünlüğü gibi temel değerler tarafından yönlendirilen eylemlerin refahı, ulusal güvenliği ve güçlü bir toplumu geliştirdiği canlı, esnek ve güvenli bir siber alandan büyük ekonomik ve sosyal değer ortaya çıkarmaktır. Stratejinin İngiltere için hedefleri şunlardır:[360]

1) siber suçlarla mücadele etmek ve siber alanda iş yapmak için dünyanın en güvenli yerlerinden biri olmak;

2) siber saldırılara karşı daha dirençli olmak ve siber alandaki çıkarları daha iyi koruyabilmek;

3) İngiliz halkının güvenli bir şekilde kullanabileceği ve toplumları destekleyen açık, istikrarlı ve canlı bir siber alanın şekillendirilmesine yardımcı olmak ve

4) tüm siber güvenlik hedeflerini desteklemek için gerekli olan ortak bilgi, beceri ve yeteneğe sahip olmak.

2022-2030 yıllarını kapsayan "Birleşik Krallık Ulusal Siber Güvenlik Strateji Belgesi'nde" Birleşik Krallık hükümeti:[361]

- Tehditleri anlamak,
- Yasa yapmak ve yasaları uygulamak,
- Ulusal standartları belirlemek ve saldırgan siber operasyonlar yürütmek de dâhil olmak üzere düşman aktörlerin tehditlerine karşı koymak için gerekli istihbaratı bir araya getirmek konusunda benzersiz bir konuma sahip

[359] İngiltere (2010). "A Strong Britain In An Age Of Uncertainty: The National Security Strategy", [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf] (er. tar. 12.11.2021).
[360] Maria Bada (2016). *Cybersecurity*..., s. 19.
[361] Cabinet Office (2022). *Government Cyber Security Strategy: Building a Cyber Resilient Public Sector 2022-2030.*

olduğu belirtilmiştir. Hükümet bu strateji aracılığıyla ulusal siber yetenekleri güçlendirmeye yatırım yapacağını vurgulamıştır.

İngiltere'de devlet daireleri ve kamu sektörü kuruluşları kendi ağlarını ve sistemlerini korumaktan sorumludur. Önemli verilerin sahibi ve bir hizmet sağlayıcısı olarak hükümet, bilgi varlıkları için koruma sağlamak üzere sıkı önlemler almaktadır. Devletin vatandaşlara, işletmelere ve kuruluşlara kendilerini çevrimiçi ortamda korumak için ne yapmaları gerektiği konusunda tavsiyelerde bulunma ve bilgi verme konusunda da önemli bir sorumluluğu vardır. Siber politikanın çoğu alanı ve bu stratejide belirtilen önlemlerin çoğu, ulusal güvenlik, dış ilişkiler ve savunma, telekomünikasyon, ürün standartları ve güvenliği, tüketicinin korunması gibi konularla ilgilidir. Ancak bu stratejinin geliştirilmesi ve uygulanması hala Kuzey İrlanda, İskoçya ve Galler hükümetlerinin girdilerine, eylemlerine ve yatırımlarına bağlıdır. Bu, özellikle eğitim, güvenlik ve kendi kamu sektörleri de dâhil olmak üzere belirli kritik sektörlerin siber dayanıklılığı gibi bu stratejinin "ekosistem" ve "direnç" sütunları içinde yer alan politika alanlarıyla ilgili olduğu aşikârdır. Tüm ülke genelinde en büyük etkiyi sağlamak için Birleşik Krallık'ın dört ülkesi arasında koordinasyon ve iş birliği önemli olmaktadır. Bu, Kabine Ofisi ve diğer Birleşik Krallık hükümet dairelerinin, öncelikler ve planlar hakkında bilgi paylaşmak için Galler, İskoçya ve Kuzey İrlanda hükümetleri ile düzenli katılımını gerektirmektedir. Bu aynı zamanda tekrardan kaçınmaya ve kamu finansmanından en iyi değeri elde etmeye yardımcı olmaktadır. Hükümetler, kendi siber stratejilerini ve planlarını geliştirmeye devam ederek bunları Birleşik Krallık hükümetinin bu stratejisiyle uyumlu hale getirmesi hedeflenmektedir.[362]

4.1.2. Kültür ve Toplum

Sürekli ve hızla değişen dinamik bir dünyada mevcut dijital teknolojiler kültürel açıdan bireylerin ve toplulukların yaşamları üzerinde büyük bir etkiye sahiptir. Son otuz yılda, iletişim ve bilgi işlemin teknolojik yakınsaması ilerlemiştir. İnternet, World Wide Web (www) ve mobil iletişim, günümüz toplumunun ve üyelerinin her birinin yaşamının içsel bir unsuru haline gelmiştir. Günlük yaşam deneyimleri, insanların binlerce yıldır içinde yaşadıkları alışılmış gerçekliklerden önemli ölçüde farklı olan yeni bir gerçekliğe dönüşmüştür. İngiltere'de BİT platformlarının yaygın kullanımının, insanların varlığının ayrılmaz bir parçası haline gelen sanal siber alanı oluşturduğu ve düzenlediği

[362] Cabinet Office (2022). *Government Cyber Security Strategy: Building a Cyber Resilient Public Sector 2022-2030.*

açıktır. Ancak siber alan alışılmış gerçekliğin yerini almaz, onu tamamlar ve onun ayrılmaz bir parçası olur. En önemli değişiklik, ayrı bir varlık olarak geleneksel insan kavramının, tüm dünyayla bağlantılı bir bilgi organizması olarak insanın yeni bir ontolojik benlik algısı ile değiştirilmesiyle ilgilidir.

Küresel siber bilginin bütünlüğü, dünya ekonomisinin günlük işleyişi ve hükümetlerin, kuruluşların, insanların güvenliği ve refahı için de kritik öneme sahiptir. Kamu kurumları saldırıya uğrayabilmekte, ticari yönden dolandırılabilmekte ve bireyler çeşitli saldırılara maruz kalabilmektedir. Çeşitli platformlarda oluşan dijital iletişim ve kültür, zaman ve mekân kısıtlaması olmadan kullanıcının bağlantısını teşvik etmiştir. İngiltere'de 2007 ve 2008 yılları arasında yaklaşık 830.000 işletme, çevrimiçi olarak veya bilgisayarla ilgili bir güvenlik açığı yaşamıştır. 2007'de kişisel kimlik dolandırıcılığının yaklaşık yüzde kırkı (84.700 civarında olay) çevrimiçi olarak gerçekleşmiştir.[363]

Herhangi bir siber güvenlik analizinin ilk adımı siber tehditlerin aralığını (BİT ağları aracılığıyla veya bunlara yapılan güvenlik zorlukları kastedilmektedir) belirlemek olmalıdır. 2007 yılı itibariyle, toplam İngiltere nüfusunun üçte ikisi internet kullanmıştır:[364]

- İngiltere'nin farklı bölgelerinde erişimde önemli farklılıklar (%51-69) olmuştur.
- Geniş bant sağlayıcılarında büyüme oranı giderek artmıştır. 2004'ten bu yana yüzde 45'lik yıllık büyüme oranı, tüm hane halkının yüzde 52'sinde erişimi sağlamış veya evlerdeki internet bağlantılarının yüzde 83'üne ulaşmıştır.
- 2007 yılında internete bağlı çocuklu hanelerin yüzde 92'sinde geniş bant sağlanmıştır.
- 2007 yılında 2,7 milyon internet bağlantılı ev hala dar bantla idare etmiş; resim yükleme ve video akışı gibi yüksek bant genişliğine sahip hizmetlerine erişim sağlamak zor olmuştur.
- Cinsiyet farkı ortalama olarak daralmış, ancak yaşlı kadınların internet erişimi sağlama olasılığı, yaşlı erkeklerden çok daha az olmuştur.
- Çevrimiçi nüfus ortalamadan daha genç, daha eğitimli ve daha zengindir. İnternet kullanmayanlar daha yaşlı, daha fakir, daha az eğitimli, engelli veya bazı etnik azınlıklardan olma eğilimindekiler olarak kalmıştır.

---

[363] Paul Cornish, Rex Hughes ve David Livingstone (2009). *Cyberspace and the National Security of the United Kingdom: Threats and Responses*, London: Chatham House Report, s. 3.

[364] P. Cornish, R. Hughes ve D. Livingstone (2009). *Cyberspace and the National Security…,* s. 3-5.

• 2007 yılında 16-24 yaşındakilerin yüzde doksanı internete erişim sağlamakta iken 65 yaş üzerindekiler yüzde yirmi beş erişim sağlamıştır.

• En düşük internet erişim düzeyine sahip demografik gruplar artık en yüksek büyüme oranlarına sahip olmuştur. Bu, internet kullanıcıları ile internet kullanmayanlar arasındaki "erişim boşluğunun" (sadece internet erişimiyle tanımlandığı şekliyle) daraldığı anlamına gelmektedir.

• Daha geniş bir erişim tanımını, "geniş bir uygulama yelpazesini her istediği zaman kullanabilecek beceriye ve kaynaklara sahip olmak" olarak kullanıldığında, ikincil bir dijital uçurum açılmıştır.

• İngiltere'de en sık erişim noktası ev olmaya devam etmektedir. Ancak internet kullanıcılarının çoğunluğu birden fazla yerde erişimleri olduğunu söylemektedir.

Dünya politikasına yön veren ülkelerin, konumlarını kaybetmemek ve ilerlemek için modern çağın gerektirdiği stratejik önlemleri almaları gerekmektedir. Birleşik Krallık Kabine Ofisi, "Birleşik Krallık Siber Güvenlik Stratejisi" olarak hazırlanan 2009 yılı raporu, şu ifadeyle bu gerekliliği vurgulamaktadır. *"...tıpkı on dokuzuncu* yüzyılda ulusal güvenliğimiz ve refahımız için denizleri*n güvence altına almamız ve yirminci yüzyılda havayı güvence altına almamız gerektiği gibi, yirmi birinci yüzyılda da siber alandaki avantajımızı da güvence altına almalıyız..."* İngiltere Siber Güvenlik Stratejisi siber tehdidi yirmi birinci yüzyılın birincil riski olarak tanımlamaktadır. Bu kapsamda uluslararası koordinasyon, merkezi bir siber güvenlik ofisi kurulmasına karar vermiştir. Siber güvenlik ofisinin sadece teknolojide değil, aynı zamanda hukuk ve politik düzenlemelere de gereksinim olduğunu belirtmiştir.[365]

2013 yılında, Birleşik Krallık nüfusunun %78'i internet kullandığını söylemiştir. İngiltere'deki internet kullanıcılarının bu büyük oranı, ortak bir internet kültürünün yükselişinin habercisi midir? Veya internet hakkındaki inançlar ve tutumlar, genel nüfus arasında olabilecek görüşler kadar çeşitli midir? 2013 OxIS araştırmasının analizi, Britanya'daki çoğu kullanıcının her biri, internette tutumlar ve inançlar hakkındaki sorulara benzer şekilde yanıt veren bireylerden oluşan beş kümeye veya kültüre ayrılabileceğini göstermiştir.

Bilgi devrimi, diğer herkesle kolayca iletişim kurma ve sayısız bilgi ve bilgi biçimine herhangi bir endişe duymadan erişme kapasitesini getirmiştir. Ek olarak, yapay zekâdaki önemli ilerlemelerin bir sonucu olarak, günümüzün

[365] UK (2009). "Cyber Security Strategy of the United Kingdom Safety, Security and Resilience in Cyber Space", UK: Cabinet Office, s. 5

dijital teknolojileri diğer ülkelerde olduğu gibi İngiltere'de giderek daha akıllı ve kişisel hale gelmektedir. Neredeyse her insan deneyiminin etkileşimi, büyük verilere bağlı karmaşık bir kabuk aracılığıyla sağlanmaktadır.[366] Bu kabuk bireye, çok çeşitli kararlar almak için gerekli olan, yalnızca o kişi için hazırlanmış bağlam odaklı bilgiler sağlamaktadır. Böylece, insan koşulları ve insan davranışlarının ilkeleri değiştiği için dünya görüşleri hem doğrudan (fiziksel) hem de sanal alanlara bağlı kalarak kültür ve toplumun yapısını değiştirmektedir. İngiltere'de beş kültürün her birinin kendine özgü yapısı vardır. Bunlar şu şekilde tanımlanmaktadır:[367]

- e-Mersives; bu kullanıcı grubu, çevrimiçi dünyada rahat ve doğal olarak evlerinde çevrimiçi olmaktan mutludur. İnterneti bir kaçış olarak kullanmaktan, çevrimiçi zaman geçirmekten, insanlarla tanışabilecekleri ve bir topluluğun parçası olabilecekleri bir yer olarak düşünmekten memnunlardır. Günlük yaşamlarının ve işlerinin bir parçası olarak internete girmişlerdir. Birleşik Krallık'taki internet kullanıcılarının yalnızca yaklaşık %12'sini oluşturmuşlardır.
- Tekno-pragmatistler; bu kullanıcı grubu, zamandan tasarruf etmek ve hayatlarını kolaylaştırmak için interneti kullanmaya odaklandıkları merkezilikle öne çıkmışlardır. E-mersives kullanıcı grubu gibi, interneti kontrol altında hissetmekteler ve interneti günlük yaşamlarının, işlerinin verimliliğini artıran araçsal nedenlerle kullanmaktalar. E-mersives'in aksine, pragmatistler interneti bir kaçış olarak görmemekteler ve çoğu zaman sadece eğlence olsun diye internete girmemektelerdir. Pragmatistler, Birleşik Krallık'taki internet kullanıcılarının yaklaşık %17'sini oluşturmuşlardır.
- Siber bilgili (bilgisayarlar veya internet konusunda bilgili; teknolojik olarak bilgili); bu kullanıcı grubu, internet hakkında bazı kararsız görüşlere, karışık duygulara ve inançlara sahip olduklarını ifade etmişlerdir. Her zaman kontrolü kendilerinde hissetmek yerine, teknolojik kontrolü kaybedebileceklerini ve bu da kendilerini zaman ve mahremiyetten alıkoyabileceğini düşünmektelerdir. Birleşik Krallık'taki internet kullanıcılarının yaklaşık beşte birini (%19) temsil etmişlerdir.
- Siber ılımlılar; interneti zaman geçirmek için iyi bir yer, bilgi bulmak veya alışveriş yapmak için etkili bir yol veya sosyal ilişkilerini sürdürmek ve geliştirmek için iyi bir yol olarak gördüklerinde daha ılımlı olduklarını gösteren

[366] Anthony M. Townsend (2013). *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia,* NewYork: W. W. Norton & Company.
[367] William H. Dutton (vd.) (2013). "Cultures of the Internet: The Internet in Britain", *Oxford Internet Survey*, s. 4.

tutum ve inanç kalıpları tarafından en açık şekilde tanımlanmaktalardır. Öte yandan, internetin kendilerini ahlaksız materyallere maruz bırakma, mahremiyetlerine tehdit oluşturma veya zamanlarını boşa harcama riskinden de aynı şekilde korkmamaktalardır. Bunlar, kullanıcıların %37'sini oluşturan İngiltere'deki en büyük tek internet kullanıcısı kümesidir.

- Adigital; bu grup internetin kendilerini daha verimli hale getirdiğini düşünmüyorlar. Yalnızca zaman geçirmek veya gerçek dünyadan kaçmak için çevrimiçi olmaktan da keyif almıyorlar. Bu kültürün üyelerine göre, internet muhtemelen kendi kontrolleri dışında, potansiyel olarak başkaları tarafından kontrol ediliyormuş gibi algılanmaktadır. Bu adijital kültür, Birleşik Krallık'ın çevrimiçi nüfusunun yaklaşık %14'ünü kapsamaktadır.

İnternet kullanımı, siyasete ve hükümete katılım ile pozitif olarak ilişkilendirilmiştir. Bununla birlikte, iki faaliyet alanı önemli ölçüde farklılık göstermektedir. Devlet faaliyetleriyle ilgili olarak, daha fazla hizmet gitgide daha kolay çevrimiçi tedarike doğru ilerlemektedir. Ayrıca, nüfusun tamamı potansiyel olarak dijital hale gelen bir veya daha fazla devlet hizmetine ihtiyaç duymaktadır. Bu nedenle, zaman içinde halkın artan bir bölümünün çevrimiçi olarak sağlanan devlet hizmetlerini kullanması beklenmiştir. Buna karşılık, bankacılık hizmetleri, hesap bakiyelerine bakmak gibi yalnızca birkaç hizmete erişen milyonları içerebilmektedir. Bununla birlikte, Birleşik Krallık'ta önceki yıllara değin dijital devlet hizmetlerinin alınmasında önemli bir ilerleme kaydedilmiştir.[368]

İngiltere Siber Güvenlik Stratejisi genel olarak, "insanların siber alanı güvenli bir şekilde kullanmak ve daha donanımlı hale gelmeleri için her düzeyde siber güvenlik eğitimini iyileştirmenin en iyi yollarına bakma" planını içermektedir. Ayrıca "riskleri anlayan ve insanların siber alanı kullanmasını ve her düzeyde siber güvenlik becerilerini geliştirmesini sağlayan bir kültür inşa etme" taahhüdü de vardır. Uygulamada İngiltere, "çevrimiçi güvenli kal" programı da dâhil olmak üzere bölgedeki en gelişmiş siber güvenlik eğitim girişimlerinden bazılarını uygulamıştır.[369] Bu boyut, çeşitli paydaşlar tarafından algılandığı şekliyle, bireysel ve kurumsal düzeyde sorumlu bir siber kültür ve toplumun önemli unsurlarını gözden geçirmektedir. Siber güvenliği destekleyen önemli kültürel ve sosyal yönler arasında, e-devlet ve e-ticaret gibi internet

[368] William Dutton (vd.) (2013 Report). "Cultures of the Internet…", s. 31.
[369] "EU Cybersecurity Dashboard A Path to a Secure European Cyberspace" (2015). [https://cybersecurity.bsa.org/] (er. tar. 13.12.2021).

hizmetlerine duyulan güven düzeyi ve bu hizmetleri sağlayan tüm kuruluşlar tarafından kişisel bilgilerin ele alınmasında gizliliğe önem veren uygulamalarda bağlılığına duyarlı olarak yer almaktadır.

Tüm siber güvenlik uzmanlarının, siber güvenlikle ilgili sorunlar için kullanıcıları suçlamaktan kaçınması gerekmektedir. Bunun yerine, uzmanların kullanılabilir sistemler ve programlar oluşturması önemli olmaktadır. Ayrıca kullanıcıların tehditlerden, iyi uygulamalardan haberdar olmalarını ve iyi uygulamaları çevrimiçi rutin davranışlarına nasıl dâhil edeceklerini bilmelerini sağlamaları gerekmektedir. Siber güvenlik zihniyeti, bir yatkınlık ve bazı durumlarda, kişinin eylemlerini hem bireysel düzeyde hem de kurumsal bir alanda iyi siber güvenlik öncelikleriyle uyumlu hale getirmede tutarlı, rutinleştirilmiş bir davranış modeli olarak anlaşılmaktadır. Siber güvenlik zihniyeti, bireysel kullanıcıların, uzmanların ve siber güvenlik ekosistemindeki diğer aktörlerin çevrimiçi güvenliklerine yönelik tehditlere karşı direncini artıran alışkanlıkları da dâhil olmak üzere değerlerinden, tutumlarından ve uygulamalarından oluşmaktadır.[370]

Siber güvenlik, İngiltere hükümeti genelinde bir öncelik olarak kabul edilmiştir. Bu nedenle, ülkede siber güvenlik zihniyetinin oluşturulmasında riskler ve tehditler rol oynamaktadır. Devlet düzeyinde, siber güvenlik yaygın bir endişe kaynağı olmuştur. İngiltere CERT-UK ve Devlet İletişim Merkezi (GCHQ) gibi çoğunlukla siber güvenliğe odaklanan ajanslar, aktif olarak bir siber güvenlik zihniyetini teşvik etmektedir. Ancak daha fazla çalışma yapılması gerekmektedir. Örneğin, İngiltere devlet dairelerine "Siber Güvenlik için 10 Adım"[371] hakkında tehditler üzerine bilgi verilmiştir. Siber güvenliğin dili tüm bölümlerde belirgindir.

Özel sektör içinde yüksek riskli uygulamalar belirlenmektedir. Ancak, çeşitli endüstriler arasında farklılıklar vardır ve bir organizasyonun ölçeği de bu anlayış farklılığına katkıda bulunmaktadır. Daha büyük kuruluşlar, siber güvenlik risklerinin daha çok farkındadır. Bu nedenle risk yönetimi yaklaşımlarında siber güvenliğe öncelik verme olasılıkları daha yüksektir. KOBİ'ler ise siber tehdit algılarına öncelik verilmediği için aynı siber güvenlik zihniyetine sahip değillerdir. Çalışanların proaktif bir zihniyete sahip olduğu sektörler vardır. Genel olarak işletmeler siber güvenlik konusunda endişelidir. Ancak çoğu zaman yapabilecekleri ve yapmaları gereken eylemlerden emin değillerdir.

[370] Maria Bada (2016). *Cybersecurity*..., s. 28.

[371] Detaylı Bilgi için bkz. Kabine Ofisi. "Reducing the Cyber Risk in 10 Critical Areas", [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/395716/10_steps_ten_critical_areas.pdf] (er.tar. 16.12.2021).

Şirketler, siber güvenlik kapasitelerini geliştirmeye proaktif olarak katılmak yerine, genellikle bir iş sorunu veya saldırı olduğunda tepki vermektedirler. O halde olaylar, siber güvenlik uygulamalarının kullanılmasının ana nedenidir.

İngiltere'de bireylerin çoğu, çevrimiçi ortamda olası risklerin tam olarak farkında değildir. Farkındalık olsa da uygun eylemlerin mutlaka anlaşılmadığı veya alınmadığı konusunda tartışmalar vardır. Uzmanların genellikle sıradan bir kullanıcıdan gerçekçi olmayan beklentileri vardır. Kullanıcıları parola sıfırlama gibi siber güvenlik uygulamalarına uymadıkları için suçlamak yerine, kullanıcıların uyması daha kolay uygulamalar geliştirmeye ve tehditlerin geniş bir şekilde anlaşılmasını sağlamak için daha fazla kaynak ayırmaya ve bunları ele almak için araçlara ihtiyaç vardır. İngiltere'de sivil toplumda büyüyen bir farkındalık hareketi vardır. Ancak daha siber güvenli bir zihniyete geçişin gerçekleştirilmesi uzun vadeli bir hedef olmaya devam etmektedir.

4.1.3. Eğitim, Öğretim ve Beceriler

İngiltere'de çeşitli hükümet paydaşları, özel sektör ve bir bütün olarak nüfus için siber güvenlik eğitimi, öğretimi ve becerilerinin kullanılabilirliğini ve kalitesini gözden geçirmektedir. Özellikle, mevcut eğitim tekliflerini ve siber güvenlik eğitiminin ulusal gelişimini, kamu ve özel sektörde eğitim ve öğretim girişimlerini, kurumsal yönetim, bilgi ve standartları değerlendirmektedir. Bu boyut, kamu ve özel sektör ihtiyaçları için yeterli ve sürdürülebilir siber güvenlik becerileri arzını sağlamak adına yüksek kaliteli siber güvenlik eğitim ve öğretim seçeneklerinin ve bunların mevcudiyetinin önemine değinmektedir. Bilgi güvenliği ve siber güvenlik alanında okullarda ve üniversitelerde mevcut eğitim teklifleri, özel sektör ve bunun ötesindeki eğitim teklifleri hakkında fikirleri ele almaktadır.

Siber Şampiyonlar,[372] İngiltere'deki okullara, gençlik kuruluşlarına ve ilgi gruplarına dijital okuryazarlık ve çevrimiçi güvenlik bilinci konusunda en iyi uygulamaları teşvik etmek için oluşturulmuş kâr amacı gütmeyen bir kuruluştur. Program, Siber Şampiyonlar ağları, genç profesyonel gönüllüler ve yerel toplulukları için bir fark yaratmaya ve gelecek nesillerin becerilerini artırmaya teşvik eden, giderek artan sayıda özel ve kamu sektörü kuruluşu tarafından desteklenmektedir. İngiltere Siber Güvenlik Zorlukları (Cybersecurity Challenge UK),[373] ödüllendirici bir kariyer olarak siber güvenlik bilincini artıran

[372] "Cyber Champions", [https://www.cyberchampions.org/] (er. tar. 12. 11. 2021).
[373] "Cybersecurity Challenge UK", [https://cybersecuritychallenge.org.uk/] (er. tar. 12. 11. 2021).

ve daha fazla insanı mesleğe katılmaya teşvik eden öğrenme ve gelişim fırsatları oluşturmaktadır. Okulların programı, öğretmenler ve işverenlerle ortaklaşa tasarlanmıştır ve özel okulların programı, 14-17 yaşındaki sınıfların sektöre gelecekteki girişlerini kolaylaştıracak akademik seçimler yapmalarına yardımcı olmak için ders planları ve destekleyici materyaller sunmaktadır.

Kamu ve özel sektör eğitimi iş birliği içindedir. Her iki sektörden alınan beceri setlerini oluşturmaya çalıştığı için sürekli olarak değişen çevreye uyum sağlamaktadır. Ayrıca hükümet, diğer sektörlerle ortaklıklar kurmakta, kolluk kuvvetlerini eğitmek için faaliyetlere fon sağlamaktadır. Eğitim ve beceriler arasında bir fark vardır. Siber güvenlik becerileri konusunda eğitim almış uzman kadrolar olsa da bu kadro İngiliz toplumunun ihtiyaçlarını yeterince karşılayamayacak kadar küçüktür. Sonuç olarak, şu anda eğitim ve uygulamalı eğitimin birleştirilmesi ihtiyacını vurgulayan algılanan bir beceri eksikliği vardır.[374] Bu nedenle, siber güvenlik ve beceri geliştirme programlarına daha fazla yatırım yapılması gerekmektedir.

Siber güvenlik devam eden bir süreç olduğundan, ülkelerin ulusal siber güvenlik stratejilerinin değişen risk ortamı göz önüne alındığında hala geçerli olup olmadığını, hala ulusal hedefleri yansıtıp yansıtmadığını ve hangi ayarlamaların gerekli olduğunu anlamaları için ulusal siber güvenlik stratejilerini düzenli olarak gözden geçirmeleri gerekmektedir. Özellikle COVID-19 pandemisi çocukları çevrimiçi eğitime zorlamıştır. İnsanların çalışma ortamını evlerine taşımıştır. Ayrıca çocukları ve büyükleri, çevrimiçi ortamda korumaya yönelik mekanizmalar geliştirmek ülkelerin hayati öncelikleri arasında yer almıştır.[375] İnternet, özellikle çocukların eğitimine ve büyümesine önemli faydalar sağlarken, onları çevrimiçi risklere de maruz bırakmaktadır.

Çoğu ülke, çocuklar, ebeveynler ve eğitimciler için özel eğitim materyalleri, bilgilendirici oyunlar ve kılavuzlar içeren web siteleri ve sosyal medya oluşturma gibi çabalarla çocukların çevrimiçi korunmasını destekleyen girişimlerde bulunmuştur. Bu ülkelerden birisi de İngiltere'dir.

İngiltere'de siber güvenlik konusunda, modüler biçimde mesleki eğitim de dâhil olmak üzere, ilköğretimden mezuniyet sonrasına kadar ulusal ve kurumsal seviyelerde eğitim teklifleri bulunmaktadır. Herkese açık olan Devlet İletişim Merkezleri (GCHQ) çevrimiçi eğitiminin lansmanı, siber güvenlik eğitimine ilgiyi artırma niyetini göstermiştir. İngiltere'de Ulusal Siber Güvenlik Stratejisi,

---

[374] "Cybersecurity …", [https://cybersecuritychallenge.org.uk/].
[375] Global Cybersecurity Index 2020, *ITU, s*. 16, 23, 133.

eğitimi siber güvenlik becerilerinin geliştirilmesinin anahtarı olarak kabul etmektedir.[376]

İnternet ve bunun üzerine inşa edilen dijital eğitim ve iletişim, İngiltere'ye ve İngiltere'nin eğitim faaliyetlerine büyük faydalar sağlamaya yardımcı olmaktadır. Bununla birlikte hem suçlu hem de devlet tarafından yönetilen kötü niyetli aktörler, aktif olarak İngiltere'nin siber savunmalarındaki güvenlik açıklarından yararlanmaya devam etmektedir. Kasıtlı veya kazara meydana gelen siber olay riski, kuruluşlar ve bireyler tarafından kullanılan ağların, sistemlerin ve cihazların birbirine giderek daha fazla bağlı olması ve dijital hizmetlerin artan kullanımı nedeniyle tehditlerde çoğalmaktadır.

Kuruluşlar ve özellikle eğitim kuruluşları, siber risklerini azaltmak için adımlar atması gerekmektedir. Siber Farkındalık eğitim kampanyası İngiltere'de başarılı olmasına rağmen, henüz yeterli kurum ve kişiye ulaşamamaktadır. İngiliz hükümetinin tavsiye ve rehberliğin neden yeterli kitleye ulaşmadığını anlamak için daha fazlasını yapması ve bu erişimi artırması gerekmektedir. 2022 yılı Haziran ayında yayınlanmış son Ulusal Strateji Belgesi'nde İngiltere siber toplum yaklaşımını desteklemek için gerekli yapıları, ortaklıkları ve ağları güçlendirmenin önemini vurgulamıştır.[377]

4.1.4. Yasal ve Düzenleyici Çerçeveler

İngiliz hükümeti, internetin artan merkeziliğinden, çocuklar ve toplumun diğer önemli kesimleri için algılanan risklerden kaynaklanan sorunlarla ilgilenmeye çalıştıkça, internetin yasal düzenlemesi giderek daha tartışmalı bir konu haline gelmiştir. Kullanıcılar, tüketici sahtekârlığı ve ürün yanlış beyanına karşı yasalar gibi mevcut yasalara ve düzenlemelere tabi olduklarından, birçoğu dijital olmayan bir dünya için yazılmış yasaların çevrimiçi ortama pek uymadığını ve ulusal sınırların ötesinde uygulanması zor olduğunu düşünmektelerdir. Tartışmanın bir kısmı, internetin yeni düzenleyici yaklaşımlara ihtiyaç duyduğu yerle ilgilidir.

Yasal önlemler, siber güvenlikteki yasal müdahaleleri ölçmektedir. İngiltere için Yasal ve Düzenleyici Çerçeveler siber güvenlikle ilgili ulusal maddi hukuku daha iyi yansıtacak şekilde güncellenmiştir. Telekomünikasyon Geliştirme Bürosu Yönetim Danışma Grubu tavsiyelerine dayanarak, usul hukuku artık

[376] Maria Bada (2016). *Cybersecurity…*, s. 36.
[377] Cabinet Office. (2022). *Government Cyber Security Strategy: Building a Cyber Resilient Public Sector 2022-2030.*

Küresel Siber Güvenlik Endeksi'nde ölçülmemektedir.[378] Bunun yerine, kimlik hırsızlığı, çevrimiçi tacizler, ırkçılık dahil olmak üzere çeşitli alanlarda daha fazla netlik vurgulanmaktadır. Uluslararası deneyim, yasal ve düzenleyici çerçevelerin siber güvenliğin sektörler arasında yaygınlaştırılmasında oynadığı önemli rolü doğrularken, siber tehditlerden etkilenen bireylere ve kuruluşlara önleme, azaltma ve anlaşmazlık mekanizmaları sunmaktadır. Bu boyut, İngiliz hükümetinin, BİT güvenliği konularına özel bir vurgu yapmaktadır. Ayrıca siber güvenlikle doğrudan ve dolaylı olarak ilgili ulusal mevzuatı ve bunlara eşlik eden yönetmelikleri tasarlama ve yürürlüğe koyma kapasitesini incelemektedir.

1990 yılında ilk hukuksal düzenleme bilişim suçlarına yönelik Bilgisayarları Kötüye Kullanma Yasası (Computer Misuse Act)[379], İngiltere hükümeti tarafından çıkarılmıştır. Bilgisayar yazılımları, verilere yetki olmadan erişilmesi veya girilmesi, bilgisayara izinsiz olarak erişim sağlanması gibi birçok suça yönelik yapılan durumlar bu mevzuat kapsamında suç sayılmaktadır. 1998 yılında İngiltere Veri Koruma Yasası (Data Protection Act)[380] çıkarmıştır. İngiltere Kraliçe'sinin emri ile 2009 yılında ilk siber güvenlik strateji belgesini yayınlamıştır. Ardından Siber Güvenlik Ofisi kurulmuştur.[381]

2010 yılında beş yıllık süreci kapsayacak strateji ve savunmanın siber alanda gözden geçirilmesi üzerine çalışmalar yapmıştır. Bu çalışmaları belgelendirmek kaydıyla Siber Suç Stratejisi (Cyber Vrime Strategy) yayınlanmıştır. 2011 yılında Birleşik Krallık, dijitalleşen çağa ayak uydurmak ve krallığı bu siber alana taşımak için yeni bir strateji belgesi yayınlamıştır. Savunma Strateji Belgesi ile askeri alanda çalışma yapılması planlanmış ve iki temel merkez kurulması amaçlanmıştır. Bu merkezler Küresel Operasyonlar için Güvenlik Kontrol Merkezi ve Siber Operasyonlar Çalışma Grubu'dur. Ardından 2012 yılında siber güvenlik strateji belgesinde verilen amaçlara ilişkin ilerleme raporu, 2013 yılında Brileşik Krallık Ulusal Siber Güvenlik Strateji Belgesi (gelecekteki planlar ve başarılar), 2014 yılında Birleşik Krallık Ulusal Siber Güvenlik Strateji Belgesi (ilerleme ve ileriye dönük planlar) adlı ilerleme

---

[378] Global Cybersecurity Index 2020, *ITU, s*. 132.

[379] "Computer Misuse Act 1990", [https://www.legislation.gov.uk/ukpga/1990/18/contents] (er. tar. 28.12.2022).

[380] "Data Protection Act 1998", [https://www.legislation.gov.uk/ukpga/1998/29/contents] (er. tar. 28.12.2022).

[381] "2010 to 2015 Government Policy: Cyber Security" [https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security] (er. tar. 28. 12. 2022).

raporları yayınlamıştır. 2015 yılında İngiltere "2010'dan 2015'e Hükümet Politikası: Siber Güvenlik" çalışması yayınlamıştır.[382]

Ulusal Suç Ajansı (NCA),[383] çeşitli yerel ve uluslararası siber güvenlik ortaklarıyla yakın iş birliği içinde çalışarak İngiltere'nin siber suçla mücadelesine liderlik etmeye ve koordine etmeye devam etmektedir. Webstresser[384] araçları sunan suçlular, genellikle bu tür araçların yasal ağ stres testi etkinliği ve DDOS saldırıları gibi yasa dışı etkinlikler için kullanılma yeteneğinden kaynaklanan alanlardan yararlanmaya çalışmaktadırlar.

2018 yılı Nisan ayında, NCA ve Hollanda Ulusal Polisi, uluslararası kanun uygulayıcı ortaklarla iş birliği içinde, "Webstresser" hizmetiyle bağlantılı İngiltere'deki en büyük bankalar da dâhil olmak üzere, dünya çapında 4 milyon DDoS saldırısıyla bağlantılı bir web sitesini kapatan uluslararası bir operasyonu başarıyla yönetmiştir. Önemli bir suç sitesi kapatılmış ve arkasındaki karmaşık suç grubu durdurulmuştur.

Hukuki tedbirler kapsamındaki sorular, başlangıçta Budapeşte Siber Suçlar Sözleşmesi gibi sözleşmelerin tavsiyelerini takiben geliştirilmiştir. Bununla birlikte, cevaplar artık yalnızca uygulanan ulusal yasaları vurgulamaya odaklanmaktadır. Bununla birlikte, uluslararası sözleşmelerin etkisi ve bağlayıcı taahhütler oluşturmadaki rolü göz önüne alındığında, Budapeşte Sözleşmesi gibi uluslararası sözleşmeler artık uluslararası işbirliği önlemleri faaliyetleri kapsamında ölçülmektedir.[385] İnsanlar giderek daha fazla çevrimiçi olduğu için çeşitliliği ve içermeyi de destekleyen güvenilir bir siber alan, sosyal mühendislik ve mahremiyetin yanı sıra taciz, zorbalık, çocuk pornografisi ve ırkçılık vb. gibi konuların incelenmesini gerektirmektedir.

---

[382] "2010 to 2015 Government Policy: Cyber…".

[383] National Crime Agency (NCA), (2017). *Annual Report and Accounts 2016–17*, London: OGL, [https://assets.publishing.service.gov.uk/].

[384] Webstresser.org, dağıtılmış hizmet reddi (DDoS) saldırıları olarak bilinen şekliyle büyük kesintilere neden olabilecek yazılımlar satmıştır. Bu tür saldırılar, internet sunucularında trafiği artırarak, web sitelerin ve çevrimiçi hizmetlerin zarar görmesine neden olmaktadır. Anthony Cuthbertson (25.04.2018). *Independent*, [https://www.independent.co.uk/life-style/gadgets-and-tech/news/webstresser-internet-ddos-europol-nca-cybersecurity-a8321751.html] (er. tar. 13.12.2021); AB'nin kolluk kuvvetleri istihbarat teşkilatı "Europol", Webstresser.org adlı sitenin, bankalardan devlet kurumlarına, polis güçlerine ve oyun sitelerine kadar çeşitli web sitelerine 4 milyondan fazla saldırı yaptığını belirtmiştir. Mathew J. Schwartz (26.04.2018). "Police Seize Webstresser.org, Bust 6 Suspected Admins", [https://www.bankinfosecurity.com/police-seize-webstresserorg-bust-6-suspected-admins-a-10920] (er. tar. 13.12.2021).

[385] Global Cybersecurity Index 2020, *ITU,* s. 132.

Uluslararası Siber Politika Birimi, İngiltere'nin Dışişleri Bakanı tarafından oluşturulan internet yönetişim aracıdır.[386] İngiliz siber stratejisi, esas olarak, uluslararası siber hukuk için bir çerçeve oluşturmak, uluslararası iş birliğine ve ayrıca siberdeki güçlü aktörle ikili ilişkiler geliştirmeye odaklanmaktadır.

BİT güvenliği mevzuatı, siber güvenliği ele alan kapsamlı BİT güvenliği yasal ve düzenleyici çerçeveleri uygulandığından ve İngiltere'de dijital ortamda bireylerin ve kuruluşların haklarını koruyan mevzuat kabul edildiğinden dolayı ileri düzeydedir ve hatta (Grafik 10'da görüldüğü gibi) dinamik bir aşamaya ulaşmıştır. İnsan haklarına saygı gösterirken bilgisayarla ilgili suçlarla mücadele etmek için ceza adaleti sistemi içinde kapsamlı bir yapı mevcuttur. Ülke, mahremiyet ve veri koruma konusunda uluslararası kuruluşlarla birlikte çalışmaktadır. İngiltere, İnsan Hakları Yasası gibi uluslararası anlaşmaları ve bunların tespitini, soruşturulmasını ve kovuşturulmasını kolaylaştırarak, mahremiyet ve veri korumasına karşı suçlarla mücadele etmek için uygun mevzuatın kabul edilmesine yönelik diğer anlaşmaları onaylamıştır.[387]

İngiltere'de siber güvenliği ele alan kapsamlı BİT güvenliği yasal ve düzenleyici çerçeveleri uygulanmış, bireylerin ve kuruluşların dijital ortamda haklarını koruyan mevzuat kabul edilmiştir. Siber suçlarla ilgili farklı mevzuat girişimleri vardır.

29 Haziran 1990 tarihli Bilgisayarın Kötüye Kullanımı Yasası (CMA), aşağıdaki gibi bilgisayar kötüye kullanımı suçlarını içermektedir:[388] bilgisayar ve materyaline yetkisiz erişim; başka suçların işlenmesi veya işlenmesini kolaylaştırmak amacıyla yetkisiz erişim; bilgisayarın çalışmasını bozma niyetiyle veya dikkatsizce yapılan yetkisiz eylemler. Siber suçlar için geçerli olan mevzuat hükümleri, aşağıdakiler gibi daha geniş mevzuatta yer almaktadır:

a) 1913 tarihli Sahtecilik Yasası, md. 1[389];
b) Dolandırıcılık Yasası 2006, md. 1-8[390];

---

[386] Maria Bada (2016). *Cybersecurity*..., s. 44.
[387] Maria Bada (2016). *Cybersecurity*..., s. 44-45.
[388] United Kingdom (1990). "Computer Misuse Act 1990" [https://www.legislation.gov.uk/ukpga/1990/18/contents] (er. tar. 28.12.2022).
[389] Siber suçlar için geçerli olan mevzuat hükümleri, 1913 tarihli Sahtecilik Yasası'na atıfta bulunmaktadır. Detaylı bilgi için bkz. United Kingdom "Forgery Act 1913" [https://www.legislation.gov.uk/ukpga/1913/27/contents/enacted] (er. tar. 28.12.2022).
[390] United Kingdom (2006). "Fraud Act 2006", [https://www.legislation.gov.uk/ukpga/2006/35/contents] (er. tar. 28.12.2022).

c) 1978 tarihli Çocukların Korunması Yasası, md. 1[391];

d) Telif Hakkı, Tasarımlar ve Patentler Yasası 1988, md. 1-8, md. 56 ve md. 262.[392]

1998 tarihli İnsan Hakları Yasası, GCHQ gibi kamu kurumlarının Avrupa İnsan Hakları Sözleşmesi kapsamında vatandaşların haklarını korumasını şart koşmaktadır.[393] İletişim operasyonlarının dinlenilmesi, 2000 sayılı Soruşturma Yetkileri Yönetmeliği (RIPA) kapsamında yetkilendirilmiştir.[394] Müdahaleye yalnızca Dışişleri Bakanı tarafından izin verilebilmektedir. Bir durdurma emri çıkarılmadan önce, Dışişleri Bakanı bir arama emrinin belirli gerekçelerle gerekli olduğuna ve durdurmanın belirtilmek istediği şeyle orantılı olduğuna inanmalıdır. Bu gerekçeler, müdahalenin gerekli olduğu yönündedir:[395] ulusal güvenlik çıkarları ve İngiltere'nin ekonomik refahı için ciddi suçların önlenmesi veya tespitine destek olarak müdahale edebilmektedir. RIPA ayrıca, ele geçirilen materyalin ve ilgili iletişim verilerinin kullanımını sınırlamak için önlemlerin yerinde olmasını gerektirmektedir.

RIPA, iki bağımsız yetkinin, GCHQ'nun faaliyetlerini denetleyen kıdemli yargıçların, İletişimin Durdurulması Komiserinin ve İstihbarat Hizmetleri Komiserinin işlevlerini belirlemektedir. GCHQ, bu Komisyon üyeleri ile iş birliği yapmak ve ihtiyaç duyabilecekleri tüm bu tür belgeleri ve bilgileri ifşa etmekle yükümlüdür.[396]

İngiltere, Avrupa İnsan Hakları Sözleşmesi (1998) gibi uluslararası anlaşmaları ve bunların tespitini, soruşturulmasını ve kovuşturulmasını kolaylaştırarak, mahremiyet ve veri korumasına karşı cezai suçlarla mücadele etmek için uygun mevzuatın kabul edilmesine yönelik diğer anlaşmaları onaylamıştır.[397]

2009 yılında İngiltere'nin ilk siber güvenlik strateji belgesi olan Birleşik Krallık'ın Siber Güvenlik Stratejisi Siber Alanda Güvenlik, Emniyet ve

[391] United Kingdom (1978). "Protection of Children Act 1978", [https://www.legislation.gov.uk/ukpga/1978/37/contents] (er. tar. 28.12.2022).
[392] United Kingdom (1988). "Copyright, Designs and Patents Act 1988", [https://www.legislation.gov.uk/ukpga/1988/48/contents] (er. tar. 28.12.2022).
[393] United Kingdom (1998). "Human Rights Act 1998", [https://www.legislation.gov.uk/ukpga/1998/42/contents] (er. tar. 28.12.2022).
[394] United Kingdom (2000). "Regulation of Investigatory Powers Act 2000", [https://www.legislation.gov.uk/ukpga/2000/23/contents] (er. tar. 28.12.2022).
[395] Maria Bada (2016). *Cybersecurity*..., s. 44.
[396] Maria Bada (2016). *Cybersecurity*..., s. 45.
[397] Maria Bada (2016). *Cybersecurity*..., s. 45.

Dayanıklılık[398] suç örgütleri ve saldırılara karşı savunma planları üzerine yoğunlaşmıştır. 2010 yılı Ulusal Güvenlik Stratejisi ve Stratejik Savunma ve Güvenliğin Gözden Geçirilmesi Belgesi'nde İngiltere, beş yıllık güvenlik açıklarına yönelik önlemlerin alınması kapsamı üzerinde durmuştur.[399]

Kraliyet Savcılık Servisi (CPS), 2013-2014 CPS Güvenlik ve Bilgi risk yönetimi politikasını geliştirmiştir. Bu politika, bilgi risk yönetimini mümkün olduğunca mevcut iş ve proje riskine entegre etmeyi amaçlamaktadır. Belirli tehditler, bir ISO 27001 güvence programı aracılığıyla yönetilmektedir.[400]

Nisan 2016'da Birleşik Krallık Siber Güvenlik Strateji Belgesi 2011-2016 Yıllık Raporu yayınlanmıştır. Kasım 2016'da İngiltere siber güvenlik belgesi olan 2016-2021 yıllarını kapsayan Ulusal Siber Güvenlik Strateji Belgesini yayınlamıştır. Bu belgeyi yayınlamasından bir ay sonrasında Siber Güvenlik Düzenlemesi ve Teşvikler İnceleme belgesini yayınlamıştır.[401]

2016'dan bu yana İngiliz hükümeti, siber tehditlerle mücadelede, Birleşik Krallık toplumu ve ekonomisinin dayanıklılığını artırmada önemli ilerleme kaydetmiştir. Ulusal Siber Güvenlik Strateji (2016-2021) belgesiyle, hükümetin çalışmaları daha çok Birleşik Krallık'a yönelik siber tehditleri incelemek olmuştur.

Ulusal Siber Güvenlik Merkezi'nden tavsiye ve rehberlik sağlanması ve Genel Veri Koruma Yönetmeliği, 2018 Veri Koruma Yasası ve 2018 Ağ ve Bilgi Sistemleri Yönetmeliği'nin uygulanması yoluyla siber risk yönetiminde iyileştirmeler sağlanmıştır. Covid-19 salgını ile birlikte İngiltere'de bilgi depolama, paylaşımlı iletişim ve güvenlik gibi temel kurumsal ihtiyaçları karşılamak için kullanılan dijital servislerin kullanımı ve bağımlılığı tüm ekonomi ve toplum genelinde artış göstermiştir. Bu durum, İngiltere'ye önemli faydalar sağlamıştır. Ancak kuruluşlara ve daha geniş ekonomiye yönelik siber risklerin kapsamını da artırmıştır. Hükümet, 2016 Düzenleme ve Teşvikler İncelemesinde belirtilen önceki yaklaşımının, gerekli değişikliği yeterli hız ve

---

398 Detaylı bilgi için bkz. Cabinet Office (June 2009). *Cyber Security Strategy of the United Kingdom Safety, Security and Resilience in Cyber Space*.

399 UK (2010). "A Strong Britain In An Age Of Uncertainty: The National Security Strategy"; Cabinet Office (2010). *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*.

400 "Audit and Risk Committee Minutes" (11.2020), [https://www.cps.gov.uk/publication/minutes-cps-audit-and-risk-committee/arc-minutes-october-2020] (er. tar. 28.12.2022).

401 "2022 Cyber security Incentives and Regulation Review" [https://www.gov.uk/government/publications/2022-cyber-security-incentives-and-regulation-review/2022-cyber-security-incentives-and-regulation-review] (er. tar. 28.12.2022).

ölçekte sağlamadığı açıktır. Ekonomi ve toplum genelinde siber direnci artırmak için hükümetin daha proaktif ve müdahaleci olması gerekmektedir.

Mart 2021'de yayınlanan Entegre Güvenlik, Savunma, Kalkınma ve Dış Politika İncelemesi,[402] İngiltere'nin on yılda dünyadaki rolüne ilişkin vizyonunu ve 2025'e kadar atacağı adımları açıklamaktadır.

Mayıs 2022'de İngiltere, 2022 Sivil Nükleer Siber Güvenlik Stratejisi belgesini yayınlamıştır.[403] Son olarak yayınladığı 2022-2030 Ulusal Siber Güvenlik Strateji Belgesi'nde Birleşik Krallık, 2030'da ulusal hedefleri desteklemek için siber alanda ve siber ortam aracılığıyla çıkarlarını koruyabilen ve geliştirebilen lider, sorumlu ve demokratik bir siber güç olmaya devam edeceğini vurgulamaktadır.[404]

4.1.5. Standartlar, Organizasyonlar ve Teknolojiler

İngiltere'de sorumlu makam ve resmi raporlar, bir ülkenin ulusal siber güvenlik için gerekli organizasyonel yapıları oluşturup oluşturmadığını analiz etmenin en temel göstergesidir. Önemli konulardan biri, genel ulusal siber güvenlikten sorumlu olacak tek bir merkezi otoritenin belirlenmesidir. Bu otorite kamu ve özel sistemlerin, kritik altyapıların akreditasyon, denetim, standartlar, şartname ve koruma gibi siber güvenlik görevleri olan diğer kuruluşların tüm çaba ve faaliyetlerini uyumlu hale getirmelidir. Ülkenin siber güvenlik yeteneklerini geliştirmek için, siber güvenlik teknolojilerinin araştırma ve geliştirmesini yapan uzmanlaşmış enstitülerin, laboratuvarların ve merkezlerin varlığı da önemlidir.

İngiltere'nin ilk ticari internet servis sağlayıcısı olan Pipex, 1990 yılında kurulmuştur. Pipex, Mart 1992'den itibaren çevirmeli internet erişimi sağlamıştır. JANET[405] gibi ağlar ve özel iş ağları da bu dönemde kullanılmıştır. 1995 yılına

---

[402] "Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy", [https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy] (er. tar. 28.12.2022).

[403] UK, "2022 Civil Nuclear Cyber Security Strategy", London: OGL.

[404] Cabinet Office. (2022). *Government Cyber Security Strategy: Building a cyber resilient public sector 2022-2030.*

[405] Janet, Birleşik Krallık'ın Ulusal Araştırma ve Eğitim Ağıdır. Devlet tarafından finanse edilen tüm araştırma ve yenilikleri birbirine bağlamakta ve kendisi de devlet tarafından finanse edilmektedir. Janet, Birleşik Krallık'taki tüm Ar-Ge çalışmalarının temel dayanaklarından biridir. Janet, Birleşik Krallık'ın tüm ülkelerinde faaliyet göstermektedir. Janet ayrıca, Ar-Ge için daha önemli bir bilgi işlem ve veri depolama hizmetleri kaynağı olan büyük bulut sağlayıcılarına yüksek bant genişliğine sahip

gelindiğinde, NTL (Ağ Test Labarotuarları)[406] ülkenin farklı yerlerinde birkaç şirketi satın almasıyla beraber kablo operatörlerinin bağlantısı başlamıştır. Günümüzde, ağırlıklı olarak kablo ağına sahip Virgin Media da dâhil olmak üzere yaklaşık kırk bağımsız ağ operatöründen oluşan sabit geniş bant altyapısı mevcuttur. Ek olarak, ülke çapında yerel veya bölgesel olarak konumlandırılmış yüzden fazla sabit kablosuz erişim ağı vardır.[407]

İngiltere'de bant genişliği hem gigabit başına fiyat hem de güvenilirlik açısından hızla gelişmeye devam etmiştir. Önce müzik, ardından video büyük ölçekte geniş bant dağıtımına geçmiştir. İngiltere lider bir dijital ekonomi haline gelmiş, akıllı telefonlar ve Wi-Fi uygun fiyatlı bir eğlence olarak herkesin kolay erişmesine olanak tanımıştır.

İlk İngiltere Siber Güvenlik Stratejisi hükümet tarafından Haziran 2009'da oluşturulmuştur. İngiltere'nin ilk Ulusal Güvenlik Stratejisi'nin yayınlanması, Soğuk Savaş'ın gizli durumundan günümüzün yüksek düzeyde kamu korumacı durumuna resmi bir geçişe işaret etmiştir. Hükümet, endüstri, kamuoyu ve uluslararası ortakların sorumluluğu paylaştığı "siber güvenliğe tutarlı bir yaklaşım" ihtiyacını vurgulamıştır. Siber Güvenlik Stratejisinin ardından, siber güvenlikle mücadelede koordineli bir yaklaşım geliştirmekten sorumlu iki yeni kurum oluşturulmuştur.[408]

2010 Ulusal Güvenlik Stratejisinin ardından, Stratejik Savunma ve Güvenlik İncelemesi, dört yıl içinde yeni Ulusal Siber Güvenlik Programına 650 milyon £ ek fon ayırmıştır. Bu, İngiltere'nin kritik ulusal altyapısının yaklaşık yüzde sekseninin özel olarak işletildiği göz önüne alındığında çok önemlidir.[409]

---

bağlantı sağlamaktadır. Janet Güvenlik Operasyonları Merkezi (SOC), Janet altyapısını korumanın yanı sıra, sorumlu oldukları araştırma, eğitim ve yeniliklerin bütünlüğünü koruyabilmeleri için üniversitelere ve diğer kurumlara koruma, tehdit analizi, danışmanlık ve diğer hizmetler sağlamaktadır. SOC ayrıca ulusal güvenlik kurumları ve uluslararası meslektaşlarıyla da çalışmaktadır. Detaylı bilgi için bkz. "Janet: the UK's Research & Education Network", [https://www.infraportal.org.uk/infrastructure/janet-the-uks-research-education-network] (er. tar. 28.12.2022).

406 NTL bir IP adresi sağlamaktadır. Ağ bağlantılı makinelerin adreslerini NTL'nin sunucusundan atanan adrese dönüştüren bir mekanizmaya sahip olmak gerekmektedir. Bu işleme Ağ Adresi Çevirisi denir. Kablo ile modem paylaşımı düşünüldüğünde NTL ön koşuldur. Detaylı bilgi için bkz. [https://www.networklab.co.uk/cmodem/basics.html] (er. tar. 29.12.2022).

407 ISPAUK, "Celebrating 25 Years of United Kingdom Internet", 2020, s.6,[https://www.ispa.org.uk/wp-content/uploads/ISPA-25th-Anniversary-Report] (er. tar. 29.12.2022).

408 "Cyber Security in the UK" (September 2011). *UK: The Parliamentary Office of Science and Technology,* No 389, s. 1, [www.parliament.uk/] (er. tar. 15.04.2021).

409 "Cyber Security in the UK" (September 2011). *UK: The Parliamentary…,* s. 1.

Siber Güvenlik Ofisi, 2009 yılında kurulmuş ve 2010 yılında Siber Güvenlik ve Bilgi Güvencesi Ofisi (OCSIA) olmuştur. OCSIA, Kabine Ofisinde yer almış ve Ulusal Siber Güvenlik Programının finansmanı dâhil olmak üzere Birleşik Krallık hükümeti tarafından yürütülen siber güvenlik programlarını koordine etmiştir. Siber Güvenlik Operasyon Merkezi (CSOC) 2009 yılında kurulmuştur. CSOC, GCHQ (siber saldırı ve tehditlere karşı korumak amacıyla İngiliz hükümeti tarafından görevlendirilen siber güvenlik ve istihbarat kurumu) bünyesinde yer almaktadır ve siber tehditlerin analizi ve kapsamlı durumsal farkındalık sağlamaktan sorumludur. CPNI, ulusal altyapı kuruluşlarına ve işletmelere siber dâhil koruyucu güvenlik önlemleri konusunda rehberlik sağlamaktadır. CESG (GCHQ'nun bilgi güvenlik kolu), Ulusal Bilgi Güvencesi Teknik Otoritesidir. CESG, GCHQ bünyesinde yer almaktadır. Hükümet, savunma ve kilit altyapı müşterilerine, çeşitli bilgi güvenliği hizmetleri sağlamaktadır. CERT bir dizi kamu ve özel sektör kuruluşunda bulunmaktadır.[410]

Teknik sütun, CIRT'ın nasıl çalıştığını daha iyi yansıtacak şekilde yeniden yapılandırılmıştır. Bu boyutta şunlar yer almaktadır: Bilgisayar Olayı Müdahale Ekibi- Devlet ve Ulusal Bilgisayar Olay Müdahale Ekipleri (National CIRT)[411] tek bir göstergede birleştirilmiştir.

Tüm ülkeler için Küresel Siber Güvenlik Endeksi'nde CIRT sertifikası, siber olayla mücadele kapasitesi hakkında bilgi sağlamada önemli bir unsur olmaktadır. Küresel Siber Güvenlik Endeksi'nin gelecekteki yinelemeleri, Bilgisayar Olay Müdahale Ekipleri için Güvenlik Olgunluk Modellerini keşfetmede daha derine ineceği öngörülmektedir.[412]

İngiltere Mart 2021'de yayınlanan Entegre Güvenlik, Savunma, Kalkınma ve Dış Politika İncelemesi ile daha rekabetçi bir dünya için daha donanımlı olmasını, ulusal refahını ve stratejik avantajlarını artırmayı hedeflemektedir.

2022 yılı Haziran ayında yayınlanan son Ulusal Strateji Belgesi'nde İngiltere hükümetinin ve daha geniş ekonominin ihtiyaçlarını karşılayan kaliteli ürün ve hizmetler sunarak sürdürülebilir, yenilikçi ve uluslararası düzeyde rekabetçi bir siber ve bilgi güvenliği sektörünün büyümesini teşvik etmek gerektiğini savunmuştur.[413] Bilgi Komisyonerliği Ofisi (ICO), Birleşik Krallık

---

410 "What we do", [https://www.ncsc.gov.uk/section/about-ncsc/what-we-do] (er. tar. 29.12.2022).

411 "National CIRT", [https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx] (er. tar. 29.12.2022).

412 Global Cybersecurity Index 2020, *ITU, s*. 133.

413 Cabinet Office (2022). *Government Cyber Security Strategy: Building a Cyber Resilient Public Sector 2022-2030.*

Genel Veri Koruma Yönetmeliği kapsamındaki siber güvenlik yükümlülükleri konusunda kuruluşlara tavsiyelerde bulunmaktadır.

. İngiltere'nin 2025 vizyonu, bilim ve teknolojideki yenilikleri benimsemeleri gerektiğini kabul etmektedir. Ulusal Siber Strateji bu yaklaşım üzerine kurulmuştur ve yayınlanması, "Integrated Review" stratejik hedefi kapsamındaki bilim ve teknoloji yoluyla stratejik avantajın sürdürülmesi taahhütlerinden biri olmuştur.[414]

Bu çalışma kapsamında Türkiye ve İngiltere örnekleri önceden belirlenmiş beş boyuta dayalı olarak derinlemesine analiz edilmiştir. Bu analizde siber güvenliğe yönelik siyasi ve stratejik yaklaşımlar dikkate alınmıştır. Gelecek bölümde ise bu yaklaşımlar göz önünde bulundurularak belirlenen beş boyut ile her iki ülke örneğindeki siber güvenlik politikalarının karşılaştırmalı analizi yapılmıştır. Söz konusu iki devlet kısa ve orta vadede ağ teknolojileri kapsamında özellikle politik, ekonomik ve askeri kapasitelerini geliştirmek için etkili bir siber savunma ve saldırı kapasitesi oluşturmaya çalışmışlardır. 2000'lerin başı ile birlikte şekillenmeye başlayan resmi siber güvenlik strateji belge ve doktrinlerinin, küreselleşen, ticarileşen ve sivilleşen internet teknolojisinden istifade ettiği gözlemlenmiştir. Bu saye de ulusal siber güvenlik alanlarını denetleyen hukuki altyapı ve ulusal siber güvenlik kurumlarının faaliyetleri incelenerek değerlendirilmiştir.

[414] "National Cyber Strategy 2022 (HTML)", [https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022] (er. tar. 29.12.2022).

BEŞİNCİ BÖLÜM

TÜRKİYE VE İNGİLTERE'NİN SİBER GÜVENLİK POLİTİKALARININ KARŞILAŞTIRILMASI

Bu bölüm, uluslararası ilişkiler açısından siber alanın neden olduğu yeni tartışma konularını ele almak suretiyle, Türkiye ve İngiltere'nin siber güvenlik stratejilerini karşılaştırmalı olarak analiz etmek amacıyla hazırlanmıştır. Bu çalışma kavramsallaştırılan, değişken ve farklılaşan bir yapıdaki siber güvenlik anlayışını Türkiye ve İngiltere arasında karşılaştırmalı olarak incelemektedir. Buna ek olarak bu iki ülkenin siber güvenlik ilişkilerindeki paylaşımlar, ortaklıklar küresel siber güvenlik ortamının önemli bir yönünü de göstermektedir.

Bu bölümde birinci karşılaştırma boyutu politika ve strateji başlığı altında, siber güvenlik ve siber suç olaylarına ilişkin alınacak kararlarda hangi kurumlara ne tür görevler düştüğü değerlendirilmektedir.

İkinci karşılaştırma boyutu olan kültür ve toplum başlığı altında; siber güvenlik kültürünün, organizasyonun işgücünün siber güvenlikle ilgili tutumlarını, bilgilerini, varsayımlarını, normlarını ve toplumların değerlerini incelemektedir.

Üçüncü karşılaştırma boyutu olan eğitim, öğretim ve beceriler başlığı altında ise ülke genelinde siber güvenliğin sağlanması amacıyla yürütülen eğitim faaliyetleri ve bu doğrultuda verilen bilinçlendirme eğitimlerinden bahsedilmektedir. Türkiye ve İngiltere hükümetlerinin hem devlet hizmetlerinin hem de çevrimiçi ticari hizmetlerin güvenilirliğini artırmayı düşünmesi, aynı zamanda özel veya kişisel verilerin genel olarak ele alınması, e-devlet ve e-ticaret hizmetlerine güven konusunda kanıt sağlamak için bir geri bildirim mekanizması geliştirmesi önem arz etmektedir. Bu önlemler, siber saldırı ve siber güvenlik ile hizmet ve teknolojilerde güvenilirliğin anlaşılmasını teşvik etme çabasıyla birlikte ele alınmalıdır. Çalışma da siber güvenlik eğitiminin, teknik ve bilgisayar bilimleri disiplinlerinden öte, her düzeyde (uygun koşullar sağlandığı takdirde) daha birçok eğitim disiplininde genişletilmesi gerektiği vurgulanmaktadır. İlerlemek için işletme yönetimi, felsefe, siyaset bilimi,

uluslararası ilişkiler, kamu politikası, savunma ve güvenlik, hukuk, sosyoloji, ekonomi, etik gibi alanlardan birkaçının görülmesi ve müfredatlarında siber güvenlik konusunun eklenmesi ve geliştirilmesi önemlidir. Ayrıca, kamu ve özel sektörün siber güvenlik eğitimi için temel gereksinimleri belirlemesi gerekmektedir.

Dördüncü karşılaştırma boyutu olarak ülkelerin siber güvenlik konusundaki siyasi ve hukuki perspektiflerinde uygulamaya koydukları stratejik planlar ve mevzuatlar üzerinde durulmuştur. Yasal ve düzenleyici çerçeveler başlığı altında, siber güvenliğe yönelik siyasi çalışmalar değerlendirilmektedir.

Beşinci karşılaştırma boyutu olan standartlar, organizasyonlar ve teknolojiler başlığı altında ise; ülkelerin siber güvenlik konusundaki bilimsel çalışmaları ve bu çalışmalara dayalı olarak geliştirilen teknolojik üretim faaliyetlerine değinilmiştir. Ayrıca iş birliği faaliyetleri kapsamında ülkelerin uluslararası arenadaki iş birliği girişimlerine de ağırlık verilmiştir. Ülkelerin kritik altyapı tesisleri, acil müdahale birimleri, sektörel müdahale ekibi, kurumsal müdahale ekibi, ulusal müdahale birimleri ve kurumlara yönelik standartlar değerlendirilmektedir.

5.1. Karşılaştırmada Yaklaşım ve Kriterler

Siber güvenlik politikalarına veya stratejilerine yönelik olarak çeşitli uluslararası kuruluşların geliştirdiği boyutlar bu çalışma kapsamında daha sistematik olarak gruplandırılmaktadır. Beş temel karşılaştırma boyutuyla ülkelerin siber güvenliğe yönelik tüm politik ve stratejik yaklaşımları analiz edilmektedir. Yapılan karşılaştırma sonuçlarından yola çıkarak Türkiye'nin siber güvenlik politikalarına yönelik çeşitli çıkarımlarda bulunulmuştur. Ancak siber güvenliğin doğası, siber saldırı ve siber suç tekniklerinin sürekli değişim göstermesi nedeniyle; önerilen politik çıkarımların kesin sonuç verip vermeyeceğinin kestirilmesi oldukça zordur. Nitekim Türkiye ve İngiltere için yapılacak çıkarımlarda Türkiye ve İngiltere'nin toplumsal, kültürel ve hukuki yapısı gözetilmeye çalışılmıştır. Tüm bu boyutlar göz önünde bulundurularak, etkin bir siber güvenlik sağlayabilmek için kurumlar arası etkili iletişime dayanan bir yönetim yapısına ait politikalar belirlenmeye çalışılmıştır. Elde edilen bulgular, politika yapıcılar ile kamu ve özel kurum yöneticileri açısından oldukça önemli çıkarımlara sahip olduğu öne sürülebilir.

Karşılaştırmada önemli kısıtları içeren BİT güvenliği mevzuatı, siber güvenliği ele alan kapsamlı BİT güvenliği yasal ve düzenleyici çerçeveleri

uygulandığından ve İngiltere'de dijital ortamda bireylerin ve kuruluşların haklarını koruyan mevzuat kabul edildiğinden dolayı ileri düzeydedir. Türkiye için ise bu mevzuat mikro çapta birtakım revizyonlarla kullanılabilir ve sürdürülebilir bir yapıya getirildiği takdirde, insan hak ve özgürlüğüne yönelik önemli kapsayıcılıkları beraberinde getirecektir. İnsan haklarına saygı gösterirken bilgisayarla ilgili suçlarla mücadele etmek için ceza adaleti sistemi içinde kapsamlı bir yapı mevcuttur. Buna yönelik mahremiyet ve veri koruma konusunda uluslararası kuruluşlarla birlikte çalışmalar devam etmekte olup, taslak mevzuat güncellenmektedir. İngiltere'de İnsan Hakları Yasası gibi uluslararası anlaşmaları ve bunların tespitini, soruşturulmasını ve kovuşturulmasını kolaylaştırarak, mahremiyet ve veri korumasına karşı suçlarla mücadele etmek için uygun mevzuatın kabul edilmesine yönelik diğer anlaşmaları onaylamıştır.[415] Bu hususta Türkiye, ilgili mevzuata ilişkin, genel yapıya uygun yasal sözleşmeleri takip edebilmesi gerekmektedir.

Siber tehditler artık bilgisayar sistemlerine verdikleri zararla sınırlı değildir. Bir ülkenin haberleşme sistemlerine, bilgisayar sistemlerine, enerji ve ulaşım alt yapılarına, askeri komuta ve kontrol sistemlerine kritik sayılabilecek düzeyde zarar verdiği gibi ayrıca, asimetrik bir savaş türü olarak da karşımıza çıkmaktadır. Bu nedenle siber tehditlerin önümüzdeki yıllarda önemli tehditlerden biri olacağı düşüncesi, tüm dünya tarafından kabul görmeye başlamıştır. Dolayısıyla ülkelerin siber güvenliğe yaklaşımının bilgi güvenliğinin çok ötesinde bir güvenlik algısına sahip olduğu söylenebilir. ITU'ye göre siber güvenlik, siber saldırılara karşı alınması gereken önlemler bütünüdür. Kurum, kuruluş ve kullanıcıların varlıklarını korumak için geliştirdikleri araçlar, politikalar ve uygulamalar; yazılı belgeler, elektronik ortam belgeleri, etkinlikler, eğitimler ve bilişim alanında kullanılan güvenlik teknolojileri siber güvenliğin unsurları arasındadır.[416]

5.2. Türkiye ve İngiltere'nin Siber Güvenlik Stratejilerinin Analizi

Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve Eylem Planları, siber alanı oluşturan bilgi sistemlerinin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak için, saldırıların ve bunlara karşı yanıt mekanizmalarının tespit edilmesi ve önlemlerin alınması üzerine siber güvenliğe odaklanmıştır. İngiltere'ye göre

[415] Maria Bada (2016). Cybersecurity…, s. 44-45.

[416] International Telecommunication Union (2008). "Series X: Data Networks, Open System Communications and Security, Overview of Cybersecurity", *ITU-T Recommendation*, 10 (1), s. 8-12.

siber güvenlik, hem İngiltere'nin siber alandaki çıkarlarının korunmasını hem de siber alanın sunduğu birçok fırsattan yararlanarak daha geniş bir İngiliz güvenlik politikasının oluşturulmasını kapsamaktadır.

Türkiye'de ulusal siber güvenlik stratejilerine yönelik olağan ve olağanüstü toplantılar sonucunda alınan kararlar NCS'nin resmi internet sitesinde paylaşılmaktadır. Siber güvenlik konusu ilk olarak 27 Ekim 2010 tarihli toplantıda gündeme getirilmiş ve "Siber tehdidin küresel boyutu ve bu tehdidin ulusal güvenliğe etkileri" ayrıntılı olarak ele alınmıştır. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nın amacı;

- Kamu kurum ve kuruluşlarının bilgi teknolojileri ve bunların sunumunda kullanılan sistemler vasıtasıyla sağladığı her türlü hizmet, işlem ve verilerin güvenliğinin sağlanması,
- Kamu veya özel sektör tarafından işletilen kritik altyapılara ait bilgi sistemlerinin güvenliğinin sağlanması,
- Siber güvenlik olaylarının etkilerinin en düşük seviyede kalmasını sağlayacak altyapıyı oluşturmak, olaylardan sonra sistemlerin en kısa sürede normal işleyişine dönmesi için stratejik siber güvenlik aksiyonlarını belirlemek,
- Ceza makamı ve kolluk kuvvetlerinin daha etkin soruşturma yapabilmesini sağlamaktır.

Afet ve Acil Durum Yönetimi Başkanlığı, siber tehditler ve kritik altyapı çökmeleri konusunu teknolojik afet (insan kaynaklı afet) başlığı altında değerlendirmiştir. Bu kapsamda kritik altyapılar Afet ve Acil Durum Yönetimi Başkanlığı tarafından; "çevrenin, toplumsal düzenin ve kamu hizmetlerinin yürütülmesinde kısmen ya da tamamen işlevini yerine getiremediğinde olumsuz etkilenmesi sonucu vatandaşların sağlığı, güvenliği ve ekonomisi üzerinde ciddi etkileri olacak ağ, varlık, sistem ve yapıların bütünü" olarak tanımlanmıştır. Kalkınma Bakanlığı 2012 Yılı Yatırım Programı'nda yer alan "Kritik Altyapılarda Bilgi Güvenliği Yönetimi Projesi" ve "Ulusal Siber Güvenlik Strateji Belgeleri", "Kritik Altyapıların Bilgi Güvenliği" konuları önemli bir adım olmuştur. Türkiye'de kritik altyapıların çevresel tehdit ve tehlikelere (deprem, sel vb.) karşı korunmasına yönelik yasal düzenleme bulunmamaktadır.[417] Ulusal Siber Güvenlik Stratejisi'nin dördüncü eylem planında, Ulusal Siber Olay Müdahale Merkezi ile Sektörel ve Kurumsal Siber Olay Müdahale Ekiplerinin

[417] AFAD (2014). *2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi,* Ankara: T.C. Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı.

kurulması görevi, NCSC sorumluluğundaki kritik sektörlerin düzenlenmesi ve denetlenmesinden sorumlu kurumlara verilmiştir.

Türkiye'de ilkokul ve lise öğrencilerine; "Siber Suçlar ve İnternet Güvenliği, Sosyal Ağlar, Siber Zorbalık, Siber Saldırılar, Siber Uzay Farkındalığı vb." eğitimler verilmektedir. Siber güvenlik alanında doktora ve yüksek lisans yapacak bazı öğrencilere burs verilmesine Yüksek Öğretim Kurumu tarafından karar verilmiş ve buna ilişkin bir komisyon kurulmuştur. Ayrıca TÜBİTAK tarafından düzenlenen siber güvenlik yaz kampı ve üniversiteler arası siber güvenlik yarışması USOM'da başarılı öğrencilere iş imkânı sağlamaktadır. Birçok üniversitede siber güvenlik ve bilgi güvenliği programları adı altında lisansüstü programlar başlamıştır. Ulusal ve uluslararası Ar-Ge çalışmaları yapılmakta, yüksek lisans ve doktora tez çalışmaları yapılmakta, ürün/yöntem geliştirilmekte, güncel yayınlar yapılmakta ve çalıştaylar/konferanslar düzenlenmektedir.

Uluslararası iş birliklerini geliştirmek, siber güvenlik alanındaki kapasiteyi artırmak, siber saldırılara karşı müdahale kabiliyetlerini geliştirmek, kurum içi, kurumlar arası ve uluslararası iş birliğini geliştirmek, koordinasyonu sağlamak ve bu konudaki farkındalık düzeyini artırmak amacıyla BTK tarafından 2012, 2013, 2014, 2019 ve 2022 yıllarında Siber Kalkan Tatbikatları düzenlenmiştir.

İngiltere'de her gün milyonlarca insanın siber alan tarafından sağlanan hizmetlere ve bilgilere ihtiyaç duyduğunu ve siber alanın etkin kullanımının hayati önem taşıdığı vurgulanarak hükümet tarafından yayınlanan Digital Britain (United Kingdom Government, 2009) raporunda ifade edilmiştir. Haziran 2009'da "dünyanın önde gelen dijital bilgi ekonomilerinden biri olma konumunu sürdürmek" hedefine ulaşmanın bir gereği olarak ilk strateji belgesi yayınlanmıştır. Bu belge, İngiltere Hükümetinin siber alanın güvenliğini sağlamak ve siber alanın sağladığı fırsatlardan yararlanmak için ne yapacağını bildirmektedir.[418] Ulusal Güvenlik Stratejisinde İngiltere; ulusal güvenliği tehdit edebilecek aktörleri istikrarsız ülkeler, ülkeler arası olası çatışmalar, sınır aşan organize suçlar ve doğal afetler olarak tanımlarken, tehdit edilebilecek alanları ise nükleer ve diğer kitle imha silahları, siber alan, kamuoyu, kültür ve bilgi olarak tanımlamıştır.[419] Ulusal Güvenlik Strateji Raporu, farklı ülkelerin İngiltere'ye

[418] United Kingdom Cabinet Office (2009a). *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber space*, London: United Kingdom Government.

[419] United Kingdom Cabinet Office (2009b). *The National Security Strategy of the United Kingdom: Update 2009, Security for the Next Generation*, London: United Kingdom Government.

yönelik siber saldırılar başlattığını açıkça belirtmiştir. Rapor siber güvenliğin, en yüksek ulusal güvenlik risklerinden biri olarak görülmesi gerektiğinin altını çizmiştir. İngiltere'nin siber güvenlik stratejisinde dört hedef vardır. Bunlar:

- Siber suçları önlemek ve İngiltere'yi siber alanda ticaret yapmak için en güvenli ülkelerden biri yapmak,
- İngiltere'yi siber saldırılara karşı daha dirençli hale getirmek ve ülkenin siber alandaki çıkarlarını korumak,
- Vatandaşların güvenle kullanabileceği açık, istikrarlı ve sağlam bir siber alanın şekillenmesine yardımcı olmak,
- Tüm siber güvenlik hedeflerine temel teşkil edecek bilgi, yetenek ve kapasiteye sahip olmaktır.

Birleşik Krallık'ta siber suçlar, 1990 tarihli CMA ile düzenlenmektedir.[420] Üç bölüm ve 18 bölümden oluşan CMA'da; bilgisayara izinsiz girilmesi, sistemde değişiklik yapılması veya benzeri müdahalelerde bulunulması suç sayılmaktadır. İlk bölümde, bir bilgisayara veya içindeki herhangi bir veriye veya programa kasıtlı olarak yetkisiz erişim suç olarak kabul edilmektedir. İkinci bölümde ise birinci bölümün kastı altında, kendisi veya bir başkası tarafından işlenecek başka bir suçun işlenmesini kolaylaştırmak amacıyla siber suç işlenmesidir. Üçüncü bölümde, herhangi bir bilgisayardaki içeriğin izinsiz olarak değiştirilmesi veya bilgisayarın çalışmasının aksaması veya bilgisayara veya içindeki program veya verilere erişimin engellenmesi veya bunlarda değişiklik yapılması suç olarak kabul edilmiştir.

İngiltere'deki kritik altyapı, "ülke ekonomisini önemli ölçüde etkileyen, toplumun önemli bir bölümünü ve hükümetin işleyişini önemli ölçüde hasara uğratan, Birleşik Krallık'ın ekonomik, siyasi ve sosyal hayatını etkileyen varlık, hizmet ve sistemler" olarak belirtilmiştir. İngiltere'nin kritik altyapı tesisleri, dokuz sektörde kategorize edilmiştir: İletişim, Acil Durum Hizmetleri, Enerji, Finansal Hizmetler, Gıda, Kamu Hizmetleri, Sağlık, Ulaşım ve Su.[421] Birleşik Krallık'ta kritik bilgi altyapısını koruma sorumluluğu İçişleri Bakanlığı'na ait olsa da uzman desteği sağlamak ve katkıda bulunmakla görevli birçok kurum vardır. Bu katkı ve destekler CPNI tarafından koordine edilmektedir. CPNI, kritik altyapı sahipleri ve operatörleri için güvenlik tehditlerine nasıl yanıt verileceği ve bu durumların nasıl yönetileceği konusunda tavsiyelerde bulunmak

[420] Bkz. Dördüncü Bölüm, Yasal ve Düzenleyici Çerçeveler.
[421] CPNI (2020). Center for the Protection of National Infrastructure.

üzere Ortak Güvenlik Olaylarına Müdahale Ekibi'ni (CSIRT-UK) kurmuştur. İngiltere'nin siber güvenlik strateji belgesinde kamu, özel sektör ve devletin sorumlulukları açıkça belirtilmiştir.[422] Görevleri kısaca şunlardır:

Halka Ait Görevler;

- Temel düzeyde çevrimiçi tehditlerden nasıl korunacağını bilmek,
- Kişisel ve hassas bilgileri internet ortamına koymamaya özen göstermek,
- İşyerinde veya evde tehditlerin tespit edilmesinde yardımcı olmak,
- Özel sektör ve devlet ile ilgili işlemleri gerçekleştirirken şifrelerin korunması gibi görevlerini yerine getirmek, bilgisayarları tehditlerden koruyacak yazılımların, işletim sistemlerinin ve antivirüs programlarının güncellenmesinin önemini anlamak ve siber alandaki sorumlulukların bilincinde olmak.

Özel Sektöre Ait Görevler

- Siber alanı ticari açıdan hassas bilgileri, fikri mülkiyeti ve müşteri bilgilerini koruyacak şekilde kullanmak ve tehditlerden haberdar olmak,
- Siber alanda karşılaşılabilecek tehditlerin bertaraf edilmesi için devlet ve kolluk kuvvetleri ile iş birliği içinde çalışmak,
- İngiltere, dünyada canlı ve yenilikçi siber güvenlik hizmetlerine yönelik artan ihtiyacı karşılamak için sermaye sağlamak,
- Gelecekte ihtiyaç duyulacak siber güvenlik yeteneklerinin sağlanması için mükemmeliyet merkezleri oluşturmak ve yatırım yapmak.

Devlete Ait Görevler;

- Yüksek riskli tehditleri tespit etme ve önleme kapasitesini artırmak,
- Siber alanda uluslararası mutabakat içinde "davranış normlarının" şekillenmesine yardımcı olmak,
- Kritik altyapı tesislerini ve devlet sistemlerini güçlendirmek,
- Siber güvenlik konusunda çalışanların kadrolarının arttırılması,
- Kanunun uygulanması ve siber suçların önlenmesi,
- Kamuoyu farkındalığının artırılması,
- Özel sektörü bilinçlendirmek,
- İş olanaklarından yararlanmak.

[422] United Kingdom Cabinet Office (2009a). *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber space*, London: United Kingdom Government.

İngiltere'de siber güvenlik stratejisinin yayınlanmasının ardından, takip eden her yılın sonunda Bakanlar Kurulu tarafından ilerleme raporları kamuoyuna duyurulmaktadır. İngiltere stratejisi, diğer girişimlerin yanı sıra siber güvenlik becerilerini eğitim sistemine dâhil etmek, siberle ilgili mesleklerdeki cinsiyet farkını dengelemek, 14-18 yaşındakiler için eğitim ve öğretim programları sağlamak gibi çeşitli düzeylerde eğitim ve öğretim yoluyla beceri eksikliğini gidermektedir. İngiltere'deki Eğitim Bakanlığı, okullarda bilgi işlem becerilerini teşvik etmek için yatırım yapmıştır. Bu da konu alanının daha iyi anlaşılmasını saglayacaktır.

İngiltere siber güvenlik stratejisi ile ilgili olarak; eğitim, kapasite geliştirme ve farkındalık konularında çeşitli uygulamalar geliştirilmiştir. Siber güvenlik stratejisi kapsamında eğitim sürecinde Araştırma Merkezleri, Üniversite İş birliği, Eğitim Müfredatı, Askerlik/Polislik gibi kurumlarda eğitim ve bilinçlendirme odaklı eğitimler verilmesi amaçlanmıştır. İlköğretim düzeyinde farkındalık, üniversiteler için eğitim materyali, ayrılan bütçenin artırılması gibi konulara odaklanılmıştır. Tüm okullarda eğitim materyalleri, üniversitelere kaynak desteği, ayrılan bütçenin artırılması gibi konulara daha fazla ağırlık verilmiştir.

İngiltere hükümeti siber güvenlik stratejisinin dördüncü hedefi olan "tüm siber güvenlik hedeflerinin temelini oluşturacak bilgi, yetenek ve kapasiteye sahip olmak" amacına ulaşmak için, sektörler genelinde tutarlı bir araştırma gündemi izlemiş ve tehditleri, güvenlik açıklarını ve riskleri derinlemesine analiz etme yaklaşımını tercih etmiştir.[423] Strateji gereği üç yeni araştırma enstitüsü kurulmuştur. Bunlar kritik altyapıların doğru çalışmasını sağlamak için Birleşik Krallık Hükümeti tarafından sağlanan fonlarla kurulan, "Siber Güvenlik Bilimi Araştırma Enstitüsü", "Otomatik Program Analizi ve Doğrulama Araştırma Enstitüsü", yenilikçi siber güvenlik araştırması ve güvenlik açığı azaltmak için "Güvenilir Endüstriyel Kontrol Sistemleri Araştırma Enstitüsü"dür.[424]

Ulusal Siber Güvenlik Strateji Belgelerini karşılaştırmalı bir yapıda kullanan bu çalışma, kritik altyapının korunmasında, araştırma ve geliştirmeye bağlılıkta ve gelişmiş ulusal ve uluslararası iş birliğinde farklılıkları ve benzerlikleri dikkate almaktadır. Bu değerlendirmeler sonucunda her iki ülkenin siber güvenlik politikaları Tablo 8'deki gibi karşılaştırmalı olarak ifade edilmektedir.

---

[423] United Kingdom Cabinet Office (2011). *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, London: United Kingdom Government.
[424] CPNI (2020). Center for the Protection of National Infrastructure.

Tablo 8: Türkiye ve İngiltere Siber Güvenlik Politikalarının Karşılaştırmalı Analizi

Karşılaştırma Kriterleri	**Türkiye**	**İngiltere**
Ulusal strateji belgelerinin yapılması ve uygulanması	Var	Var
Siber güvenlik eğitimleri verilmesi ve eğitim programlarının güçlendirilmesi	Var	Var
Siber güvenlik tatbikatları yapılması	Var	Var
Kullanıcıların bilinçli olması	Yok	Var
Uluslararası iş birliği ve kamu-özel ortaklığının sağlanması	Var	Var
Özel sektör ve kamu kurum- kuruluşlarına siber güvenlik farkındalık eğitimleri verilmesi	Var	Var
Kritik altyapının korunması ve ulusal kriz yönetimi	Var	Var
Bilgisayar Acil Müdahale Ekiplerinin Kurulması (CERT) Bilgisayar Olay Müdahale Ekiplerinin Kurulması (CIRT)	Var	Var
Ulusal bağımsızlığa ilişkin bilgileri korumak, ulusal kritik altyapıyı korumak ve siber alanda siber güvenliği sağlamak	Var	Var
Hem uluslararası güvenlik hem de ulusal güvenlikle ilgilenen siber politika ve faaliyetlerde yer alan askeri, istihbarat ve diğer devlet kurumlarının hassas bir ağı	Var	Var
İç ve dış politika koordinasyonu	Var	Var
Bilgi güvenliğinde yasal boşluklar	Var	Var
Daha çok teknik önlem ve organizasyonel önlemine odaklanmaktadır.	Var	Yok
Daha çok siber saldırıların önlenmesi olarak siber alana odaklanmaktadır.	Yok	Var
Bu ülkenin önceliği kamu ve devletin güvenliğidir.	Var	Yok
Bu ülkenin önceliği bireyin güvenliği ve insan haklarıdır.	Yok	Var
Siber suçla mücadele	Var	Var
Ulusal risk değerlendirme yaklaşımının izlenmesi	Yok	Var
Mevcut politikalar, mevzuat ve kapasiteler dikkate alınması	Var	Var
Şeffaf bir yönetim yapısı geliştirmek	Var	Var
Paydaşların belirlenmesi	Var	Var
Güvenilir bir bilgi paylaşım ortamı sağlamak	Yok	Var
Güvenlik ve gizliliğin dengelenmesi	Var	Var
Siber ağlar ve iletişim sistemlerinin fiziksel güvenliğini sağlamak	Var	Var

Ülkeler genelinde kritik altyapılar hem özel sektörde hem de kamu sektöründe yer almaktadır. Bu nedenle maksimum iş birliği için en üst seviyede

stratejilerin üretilmesinde her iki taraf açısından da fayda vardır. Siber Güvenlik Strateji Belgeleri, hükümetin tek başına siber güvenlik sorumluluklarını üstlenemeyeceği ve tüm paydaşların ortak çabası olması gerektiği konusunda hemfikirdir.

Yukarıdaki Tablo 8, her iki ülkenin stratejik hedeflerini özetlemektedir. Ortak temalar çeşitli hedefleri kapsamasına rağmen, her stratejinin kendine özgü hedefleri vardır. Örneğin, Türkiye'nin stratejisi, bireylerin teknolojiyi kullanmasıyla ilişkili riskleri anlamalarını ve Türkiye toplumunun dijitalleşmesindeki kapsayıcı değişikliklerle ilgili gelecekteki zorlukların üstesinden gelmek için bunu güvenli bir şekilde kullanabilmelerini amaçlamaktadır. İngiltere'deki ulusal stratejinin temeli, ekonomiyi, vatandaşları ve ulusal değerleri teşvik etmek için eğitim ve uluslararası iş birliğidir. Türkiye'nin stratejisi, kritik altyapıların siber saldırılara karşı dayanıklı olmasını sağlamaktır. Türkiye'nin stratejisi, siber güvenlik bilincini teşvik etmeyi ve farkındalık yaratmayı amaçlamaktadır. Türkiye'nin siber güvenlik ilkeleri verimlilik, dayanıklılık ve öngörüdür. İngiltere'nin ilkeleri ise çok kapsamlıdır ve bazıları koruma, hesap verebilirlik ve iş birliğine odaklıdır.

Siber suçun yarattığı sorunlar küreseldir ve paydaşların hem ulusal hem de uluslararası düzeyde iş birliği yapmasını gerektirir ve bu, uluslararası forumlar, ikili ve çok taraflı anlaşmalar ve diğerleri arasında kamu-özel sektör ortaklığı gibi farklı yollarla sağlanabilmektedir. Ayrıca, diğer ülkeler arasında uluslararası iş birliğini, kamu-özel sektör ortaklığını, kapasite geliştirmeyi, araştırma ve geliştirmeyi teşvik etmek gibi Türkiye ve İngiltere benzer güçlere sahiptirler. Hem uluslararası güvenlik hem de ulusal güvenlikle ilgilenen siber politika ve faaliyetlerde yer alan askeri, istihbarat ve diğer devlet kurumlarının hassas bir ağı olması siber güvenliği sağlamada bir diğer önemli faktördür. Uluslararası iş birliği; küresel internet, özgürlük, güvenlik, açıklık ve sağlamlık arasındaki doğru denge ile sürdürülebilir bir yapıdadır. Türkiye ve İngiltere küresel iş birliğini teşvik etmek için mevcut veya gelecekteki eylem planlarını açıkça ifade etmişlerdir. Hükümetler görüşleri, ülkelerin siber güvenliğinde önemli bir rol oynadığından, stratejilerde belirtildiği gibi bakanlıklar arası güçlü bir iş birliği, hayati önem taşımaktadır. Devlet bakanlıklarının bağlanabilirliğini göstermenin iyi bir yolu, bir organizasyon yapısı tasarlamaktır.

Türkiye'nin siber ağ yapısı, yerel siber suç seviyelerinin artması, Batı yazılımlarına yaygın bağımlılık ve eşit olmayan yasal rejimler ve yaptırımlar gibi çeşitli kendine özgü risklerle karşı karşıya olmuştur. Ulusal güvenlik cephesinde, her iki devlet de siber alan da kendi ulusal güvenlik çıkarlarını

desteklemek için yeni teknik olanakları en iyi nasıl tasarlayacakları ve uyarlayacakları konusunda kendilerini geliştirmektedirler. Lakin mikro ölçekte internet ortamında gizlilik ve veriler için koruma eksikliği söz konusudur. Kamu bilgi güvenliğinde yasal boşluklar vardır. Ülkelerin mevcut bilgi güvenliği vurgusu yeterli değildir. Kurumları ve hukuk sistemi eksiktir. Bilgi güvenliği strateji ve planları yetersizdir. İnternet teknolojilerinin daha da geliştirilmesi gerekmektedir. Daha fazla uluslararası iş birliğine ihtiyaç vardır. Siber alanın güvenliği yaygın, uluslararası bir sorundur. Ancak ülkeler arasında farklılıklar olduğu için her ülkenin her şeyi aynı tarzda yapması mümkün değildir. İnternet güvenliği konusunda her ülkenin kendine göre sorunları vardır. Siber alanın güvenliği konusu çok hassas olduğu için bu zamana dek yapılan tartışmalar yeterince kapsamlı değildir. Uluslararası iş birliği sayesinde temel ilke ve kuralları belirleyebilmek, çalışacak mekanizmayı kurabilmek önem arz etmektedir. Odaklanacak konular arasında siber güvenlik, gizlilik ve verilerinin korunması yer alabilir.

Siber alanda ulusal çıkarların önceliği farklı olsa da siber altyapının güvenliğinin sağlanması, uluslararası ağ bağlantısının sürdürülmesi, Türkiye için önemli bir temel olan siber terörizm ve siber suçlara karşı mücadele konularında Türkiye ve İngiltere ortak çıkarlara sahip olduğu görülmektedir. Bununla birlikte, İngiltere'nin siber güvenlik çıkarlarını zedeleyebilecek küresel endişeleri ile Türkiye'nin siber güvenlik çıkarlarına ilişkin öncelikli yerel endişeleri görüş farklılıkları içermekte olup, mevcut küresel siber alan üzerinde "çok paydaşlı" yönetişim modelinin sürdürülüp sürdürülmeyeceği veya reforme edilip edilmeyeceğine ilişkin tartışmalar gibi, siber güvenlik kurumları hakkında görüş farklılıklarına yol açmaktadır. Türkiye ve İngiltere, temel siber güvenlik çıkarları konusundaki anlayışlarında farklılık göstermektedir. Bu da siber güvenlik ortamı hakkında farklı düşüncelerin yanı sıra siber alanda karşılıklı güven eksikliğine neden olmaktadır.

Bu çalışma sonucunda elde edilen en önemli bulgulardan biri, kamu ve özel sektörün siber güvenlik konusunun önemini ve siber güvenliği stratejik düzeyde planlamanın gerekliliğini kavrayamamış olmasıdır. Bu nedenle ulusal siber güvenliğin sağlanmasına yönelik çalışmalara ihtiyaç vardır. İngiltere gibi gelişmiş ve Türkiye gibi gelişmekte olan devletlerin siber alanda kültürel farklılıklarının önemli rolü olduğu bu çalışmada görülmektedir. Buna rağmen, İngiltere ve Türkiye'de uygulanan siber güvenlik politikaları daha esnek bir yaklaşımı benimsemektedir. Bunu özellikle her iki ülkenin siber güvenlik politikalarında ekonomik ve kişisel (bireysel) boyutlarını önemsediği

bu araştırma sonucunda görülmüştür. Ulusal Siber Güvenlik politikaları karşılaştırmalı olarak incelendiğinde;

- Türkiye, İngiltere ile kıyaslandığında amaç, vizyon, misyon, temel ilkeler, stratejik amaç ve hedeflerinin belirlenmemiş olması,
- Stratejik planlama kapsamında vatandaşların, özel sektörün, kamu kurum ve kuruluşlarının görevleri belli bir şekilde açıklanmaması,
- Eylem planlarının hayata geçirilmesi için gereken süre Türkiye için aşılmış olması,
- Türkiye'de İngiltere'ye nazaran Siber suçlarla mücadelede mevcut yasaların yetersiz olması,
- İngiltere'de siber suçlarla mücadele kapsamında görev yapan kolluk ve yargı personeline verilmesi gereken eğitimlere yer verilirken, Türkiye'de bunun daha kısıtlı olması,
- İngiltere ile kıyaslandığında Türkiye'de kamu-özel sektör iş birliğine yeterince önem verilmemesi,
- Türkiye'de eğitim ve bilinçlendirme ile ilgili konuların 2000'lerin başlarında olmaması, fakat sonradan bu konuların üzerinde durularak özellikle 2020 sonrası dönemde popüler hale gelmesi,
- Türkiye'de ve İngiltere'de yazılım ve donanıma ilişkin ürün geliştirme standartları belirlenmesinin önemli olması,
- Türkiye'de stratejik planlamayı gerçekleştirmek için bütçeleme yapılmaması, fakat İngiltere stratejik planlamalar için belli bir bütçeleme yapmış ve yapmaktadır.
- Türkiye'de NCSC hazırlandığı tarihten 2020'ye kadar geçen süreçte stratejik belgenin ilerleyişini gösteren bir raporun yayınlanmadığı tespit edilmiştir. 2020-2023 Ulusal Siber Güvenlik Strateji Belgesi ile daha kapsamlı bir raporlama yapılmaktadır.

Küresel Siber Güvenlik Endeksi'ne göre, Avrupa'da siber güvenlik etkilerinin ölçüm verilerine dayalı olarak İngiltere listede 1. Sırada yer alırken, Türkiye 11. Sırada yer almıştır.[425] İngiltere'nin stratejileri uygulama açısından Türkiye'den daha iyi olduğu görülmektedir. İngiltere siber güvenlik politikalarını koordine etme ve uygulama konusunda Türkiye'den daha aktiftir. Türkiye siber olayların teknik ve organizasyonel yapıya vereceği zararın önlenmesine odaklanmaktadır. İngiltere ise siber olayların ulusal kritik

[425] Tablo 6: 2018 Küresel Siber Güvenlik Endeksi'nde Bölgesel ve Küresel Sıralama.

bilgi altyapılarına ve kilit ağ kaynaklarına yönelik saldırıları önlemek üzere siber alana odaklanmaktadır. Siber güvenlik perspektifinden bakıldığında, Türkiye'nin önceliği kamu ve devletin güvenliği iken, İngiltere'nin önceliği bireyin güvenliği ve insan hakları olmaktadır. Siber güvenlikte Türkiye, kamu kurumlarını teşvik etmekte ve standartlarının artırılmasının farkındalığı üzerine çalışmaktadır.

Uluslararası siyasetteki siber güvenlik alanındaki eğilimlerin arkasındaki nedenleri araştırmaya ve küresel siber güvenlik kültürüyle ilgili uluslararası söylemin senaryolarını tahmin etmeye ihtiyaç vardır. Bu kapsamda 2020 Küresel Siber Güvenlik Endeksi'e göre, ankete katılan ülkeler içerisinde İngiltere 99,54 puan ile 2. sırada yer almaktadır.[426] Bölgesel düzeydeki anket çalışmaları incelendiğinde ise İngiltere yine aynı puan ile bu kez 1. sırada yer almaktadır.[427] Türkiye ise bölgesel sıralamada 6. sıradadır. Genel puanı 97,50'dir. Bu anket çalışmasında değerlendirmede yer alan beş boyutun dördünden İngiltere tam puan alırken, Türkiye bu beş boyutun ancak üçünden tam puan alabilmiştir. Burada, İngiltere, Türkiye'ye nispeten siber güvenlik kapasite olgunluk modelinde daha ileri bir konumda yer almaktadır.

Türkiye ve İngiltere'nin siber güvenlik politika eylemleri dâhilinde çeşitli yönlere odaklandığı görülmektedir. Tablo 8'de verilen bilgilere dayalı olarak verilen bilgiler ışığında; Türkiye ve İngiltere'de uygulanan politikalar daha esnek bir yaklaşımı desteklemekte ve siber güvenlik politikasının ekonomik ve kişisel (bireysel) boyutlarını vurgulamaktadır. Bu bağlamda bu iki ülkede siber güvenlik sivil odaklı olarak nitelendirilebilmektedir. Standartlar, organizasyonlar ve teknolojiler açısından İngiltere, siber güvenlik politikalarını koordine etme ve uygulama konusunda daha aktiftir.

Siber güvenlik politikası, esas olarak devletin siber güvenlikteki çeşitli rollerini (ve böylece yarı devlet ve devlet dışı unsurların rolleri de dâhil olmak üzere) tanımlamalar etrafında ilerlemektedir. İngiltere, siber alandaki olayların teknik ve organizasyonel önlemine odaklanmaktadır. Türkiye ise ulusal kritik bilgi altyapılarına ve kilit kaynaklara yönelik siber saldırıların önlenmesi konularına odaklanmaktadır. Bununla birlikte değişen sosyal ve politik koalisyonlar, birkaç nesil siber güvenlik stratejilerinde fark edilebilen yeni siyasi kararlara yansımaktadır. Farklı ülkelerde siyasi etkileşim konuları benzer olsa da, farklı rollerin somut tezahürü, farklı çıkar gruplarının gücüne ve kurumlar arasında tarihsel olarak gelişen rollerin dağılımına ve güven ilişkilerine bağlıdır.

[426] Global Cybersecurity Index 2020, *ITU, s*. 25.
[427] Global Cybersecurity Index 2020, *ITU, s*. 30.

Türkiye'de hem uluslararası hem de iç güvenlikle ilgili olarak siber güvenlik politika ve faaliyetlerde yer alan askeri, istihbarat ve diğer devlet kurumlarının hassas bir ağı vardır. Türkiye ve İngiltere, siber alana yönelik ve siber alan yoluyla ortaya çıkan risklerin doğası hakkında farklı bakış açılarına sahiptir. Bunlar, "bilgi güvenliğinin" internet üzerindeki kontrolleri içermekle beraber, bilgi ağlarını düzenlemek için ideal politikalara ilişkin görüş farklılıkları olabilmektedir. Bunda kültürel ve coğrafi farklılıklar etkin olabilir. Bununla birlikte, yerel siyasi ve ekonomik faktörlerin siber güvenlik dinamikleri için büyük önem taşıması ile iç ve dış politika koordinasyonu çabalarını karmaşıklaştırması bakımından iki ülke benzerdir. Her iki ülkedeki siber güvenlik uzmanları, hükümetlerinden tutarlı bir politika yanıtı almaya çalışırken hayal kırıklığı yaşayabilmektedir.

Türkiye'de sivil siber güvenlikte, ekonomik veya uluslararası ilişkiler uzmanlığı olmayan, teknik odaklı profesyonel bir kadro ile yürütülmekteydi. Mevcut koordinasyon ve liderlik eksikliği, politikada bir durgunluğa yol açmış ve üst düzey bir koordinatör yapısı ihtiyacı doğmuştur. Siber politika yapıcıların çoğu, ekonomi veya uluslararası ilişkilerde çok az deneyime sahip olarak, akademide teknik araştırmalar yapmak için zaman harcamıştır. Son yapılan çalışmalarla bu konunun üzerinde durularak ve birçok ekonomi, hukuk ve uluslararası ilişkiler uzmanı ile görüşülmüştür. Siber güvenlik dersleri üniversitelerde de okutulmaya, bu alanda çalışmalar yapılmasına ve birçok uzmanın bu alanda gelişmesine önem verilmeye başlamıştır.

Türkiye ve İngiltere'nin de siber güvenlik politikaları alanında bilişsel farklılıkları vardır. İngiltere küresel siber güvenlik ortamını "tehditler" perspektifinden tanımlarken, Türkiye bunu "gelişme" perspektifinden tanımlama eğilimindedir. Tehdit temelli yaklaşım, onu "diğerlerinin" perspektifinden tanımlamakta ve kalkınma temelli yaklaşım, siber alanın gelişimini arttırmanın yanı sıra toplumun iç istikrarını garanti altına almak için daha çok kendi ihtiyaçlarına odaklanmaktadır. Bu nedenle, sosyal-politik istikrar Türkiye'nin temel ulusal çıkarı olarak kabul edilmektedir. Türkiye'nin siber güvenlik talepleri ile siber güvenliği sağlama konusundaki gerçek kapasitesi arasındaki fark, Türkiye'nin siber güvenliğe karşı savunmacı bir tavır almasına neden olmaktadır.

2020 Küresel Siber Güvenlik Endeksi'ne göre ülkeler, "yoğun" bir sıralama yöntemi kullanılarak nihai puanlarına göre sıralanmıştır. Dördüncü Bölüm'de yer alan hassas radar grafiğine bakıldığında, İngiltere teknik önlemlerde birtakım iyileştirmelere ihtiyaç duymaktadır. Yasal önlemler, İşbirliğine dayalı önlemler, kapasite geliştirme önlemleri ve organizasyonel önlemlerde yirmi ve

teknik önlemlerde yirmiye yakın olduğu için ideal noktaya çok yakın olduğu görülmektedir. Aynı zamanda, Grafik 8'de Türkiye ve Grafik 10'da İngiltere'ye baktığımızda ise, her iki üklenin eşdeğer konuma ulaşabilmeleri ve tam puana erişmeleri için özellikle teknik önlemlerde birtakım iyileştirmelere ihtiyaçları olduğu görülecektir. Ancak, "Strateji ve Politika" ve "Yasal ve Düzenleyici Çerçeveler" gibi belirli faktörler için olgunluk düzeyi daha yüksek (dinamik) bir aşamada görülmektedir.

Çalışma, ulusal bir siber güvenlik stratejisi hazırlamayı veya güncellemeyi planlayan ülkelere yol gösterici olacaktır. Bu çalışma, karşılaştırmalı analizleri akademik amaçlarla yapmıştır ve siber güvenlik politikalarındaki boşlukları kapatmak için bir basamak görevi görebilir. Politika eylem planlarının geliştirilmesi, uygulanması, güncellenmesi söz konusu olduğunda, İngiltere'nin stratejileri uygulama açısından Türkiye'den iyi olduğu gözlemlenmiştir. Güvenlik stratejisine karşı savunmacı bir yaklaşıma sahip olduktan sonra bile, yeteneklerini kullanmayı çok iyi başarmıştır. Her iki ülke varlıklarını saldırgan bir şekilde gelecek tehditlere karşı korunmasını sağlama uzmanlığına sahiplerdir. Bu nedenle, bu yeni siber dünyada diğer ülkelere kıyasla kaynaklarının uçucu, belirsiz, karmaşık ve savunmasız siber tehditlerden daha iyi korunmasını başarıyla sağlamaya çalışmaktadırlar.

Türkiye ve İngiltere, ihtiyaçlarına göre stratejilerini önceliklendirip geliştirecek olsa da karşılaştırmalı analizin bulgularına dayanarak dikkate alınması gereken kilit alanlar vardır ve bunlar için aşağıda öneriler sunulmuştur:

- Bir Ulusal Siber Güvenlik Strateji Belgesi, "siber güvenlik" teriminin açık bir tanımını içermelidir. Eksik veya muğlak bir tanım, terimle ilgili çok az anlayış olduğunu gösterir ve siber güvenliğin önemli yönlerinin ihmal edilmesine yol açabilir. Henüz terimin evrensel bir tanımı olmasa da bir Ulusal Siber Güvenlik Strateji Belgesi geliştiricileri, ulusun mevcut durumunun ötesine bakmalı ve siber güvenliğin dinamik doğası nedeniyle ortaya çıkan tehditleri dikkate almalıdır.
- Stratejinin hedefleri, sorumlu aktörler ve bunlara ulaşmada gerçekçi zaman çizelgeleri ile kısa, orta ve uzun vadeli hedeflere bölünmelidir. Açık uçlu hedefler, stratejinin vizyonunun ve hedeflerinin gerçekleştirilememesine yol açabilmektedir.
- Strateji geliştirme metodolojisi tanımlanmalıdır. Bu, stratejinin geliştirilmesine yönelik olası yaklaşımların ve çerçevenin gözden geçirilmesine ve sürece gereken önemin verilmesine yardımcı olur.

- Başarıları, zorlukları ve tavsiyeleri belirten stratejinin yıllık ilerleme raporunun sağlanması önemlidir.
- Strateji ile birlikte uygulama ve değerlendirme planları geliştirilmelidir.
- Strateji, siber güvenliğin her yönünü ele aldığından emin olmak için temel bir çerçeveye dayanmalıdır.
- Stratejinin risk yönetimi yaklaşımı iyi tanımlanmalıdır.

Ülkelerin Ulusal Siber Güvenlik Stratejilerindeki ortak kapsayıcı ilkeler, hedefler, kapsamlı yaklaşım ve uyarlanmış öncelikler; kapsayıcılık, ekonomik ve sosyal refah, uygun politika araçları seti ve güvenilir ortamdır. Stratejiler en üst düzeyde büyük ölçüde desteklenmiştir ve siber saldırıların kaçınılmaz olduğu ve Hükümetin tek başına siber güvenliği sağlayamayacağı anlayışı vardır, bu nedenle özel sektörle, özellikle kritik altyapı sahipleri ile iş birliğine ihtiyaç vardır. Ayrıca, saldırıları önlemek ve herhangi bir saldırı durumunda toparlanmak için yeterli planların olması gerekir. Ayrıca, kapasite geliştirme ve siber güvenlik bilincinin artırılması, stratejinin başarısı için önemli faktörler olarak iyi bir şekilde kaydedilmiştir. Ulusal Siber Güvenlik Stratejisi, siber güvenlik becerilerindeki eksikliği gidermek ve araştırma ve desteklemeyi teşvik etmek için farkındalık, eğitim ve öğretime yatırım yapılması gerektiğini ifade etmiştir.

Ulusal Siber Güvenlik Strateji Belgesi tasarlarken ve geliştirirken, ülkeler ulusal çerçevedeki boşlukları belirlemeli; politika, yönetmelik, mevzuat, paydaşların rolleri ile sorumlulukları kapsamındaki boşlukların üstesinden gelmek için eylem hatları geliştirmelidir. Tüm bunlar ülkeden ülkeye farklılık gösterebilecektir.

Mevzuat ve yönetmeliklerde İngiltere'de, Türkiye'den farklı olarak siber güvenliğin daha ciddiye alındığı, yasa ve süreçlerin amaca uygunluğunun gözden geçirildiği görülmektedir. Ancak, uygulama planı, değerlendirme planı, kaynak tahsisi, risk yönetimi ve yıllık strateji değerlendirmesi gibi bir stratejinin başarısı için kritik olan kilit faktörlerin ya eksik ya da yetersiz ifade edildiği görülmüştür. İngiltere, stratejisinde siber güvenlik standartlarını yönlendirmek için Genel Veri Koruma Yönetmeliği kullanmaya atıfta bulunmuştur.

Siber güvenliğin ortak bir sorumluluk olması, ulusal ve uluslararası düzeyde birlikte çalışmanın önemi gibi bakış açıları benzer olsa da siber güvenlik kavramının anlaşılmasında küresel ve yerel anlamda farklılıklar bulunmaktadır. Rollerin ve sorumlulukların net olmaması, siber güvenlik becerilerinin eksikliği, dijitalleşmeye bağımlılık ve kaynakların tahsis edilmemesi gibi bazı zorluklar

belirlenmiştir. Tüm stratejiler hem saldırı hem de savunma önlemleri alarak ülkeleri korumaya yönelik önlemlere sahipken; İngiltere, ülke ağında siber güvenliği ve İletişim Hizmet Sağlayıcıları ile beklenen angajman düzeyini iyileştirmek için belirli teknik önlemler belirlemiştir. Her ülkenin kendine özgü özelliği nedeniyle, olaylara müdahalenin düzeyi ve yöntemi farklılık göstermektedir. Bu da müdahale ekiplerinin farklı şekillerde konuya yaklaşımını göstermektedir.

SONUÇLAR

Güvenliğin gerçek doğasının tanımını ve içeriğini dikkatlice inceleyerek ortaya çıkarmak bu çalışmada, birinci bölümün oluşmasına zemin hazırlamıştır. Her bir uluslararası ilişkiler kuramı, güvenlik kavramının genel hatlarını tartışmaktadır. Güvenlik kavramına yönelik yaklaşımlar üç kategoriye ayrılabilmektedir. Bunlar; "ulusal güvenlik", "uluslararası güvenlik" ve "insan güvenliği" olarak ifade edilebilir. Özellikle, realist düşünce okulu ulusal güvenliğe odaklanırken, liberal teoriler çoğunlukla uluslararası güvenlikle ilgili mülahazalarla ilgilenmektedir. Buna ek olarak, yapılandırmacılık ve eleştirel teori, geleneksel uluslararası ilişkiler teorilerini özgürleştirme vaadiyle insani güvenlik kavramını ortaya çıkarmaktadır. Bu bağlamda, bu çalışmada da belirtildiği gibi, devlet güvenliğini, uluslararası kuruluşların işlev ve kapsamını ve vatandaşların refahını doğrudan etkileyen kritik altyapıların korunmasının, söz konusu uluslararası ilişkiler teorilerinin güvenlik çalışmalarına yaklaşımında temel bir husus olması beklenmektedir.

Bu çalışma, güvenlik tanımlarını analiz etmekte, fakat veriler ışığında salt güvenlik tanımlarının pratik açıdan yeterli olmadığını göstermektedir. Birinci ana başlık, tehditlerin farklı boyutlarını yansıtan güvenlik kavramını incelemektedir. İlgili uluslararası ilişkiler kavramları ve teorileri üzerine farklı analizlerle değerlendirme imkânı sağlanmıştır. Bu ana başlıkta verilen bilgiler güvenlik çalışmalarının karmaşık alanını açıklığa kavuşturmuş ve düzenlemiştir. Elde edilen veriler ışığında hem ulusal hem de uluslararası düzeyde daha fazla politika alanına yayılan güvenlik ve alt bilim dalı olan siber güvenlik kavramları incelenmiştir. Siber güvenlik kavramları, gelişen teknolojilerin altyapıların ve hizmetlerin birbirine bağlılığını nasıl artıracağını göstermiştir. Devlet ve ayrıca devlet dışı unsurlar siber alanda güvensizlik seviyesinin azalmasına katkıda bulunabilmektedir. Devletlerin kırmızı-çizgiler oluşturması, stratejik istikrarı desteklemesi ve siber alanda sorumlu devlet davranışı normları geliştirmesi gerekmektedir. Yine de siber tehditlere karşı bireysel tepkilerinin etkinliği, toplum haricinde bireylerinde karşılıklı etkileşimlerine bağlı olabilmektedir. Devletler ve toplumsal yapılar, siber alanda kamu otoritesinin nasıl kullanılacağını müzakere etmelidir. Siber güvenlik için istikrarlı bir yönetişim çerçevesi, devletlerin etkileşimlerinde siber alanda politikalarını belirleyecek bir anlayış geliştirdiği takdirde ortaya çıkabilmektedir. Ayrıca toplumsal yapılar teknoloji, bilgi, mahremiyet ve güvenlik etrafındaki normatif alanda, yani güvenli bir

ortamda hareket ettiği ölçüde siber güvenliğin etkinliğinden söz edebiliriz. Bu nedenle, bu tür ilişkiler mümkün olduğu kadar netleştirilmelidir, ancak bu kolay bir iş olmayacaktır.

Dünyanın birçok yerinde ulusal güvenlik, geleneksel yaşam ve mülkiyet koruması anlayışının ötesine geçmiştir ve toplumların ekonomik refahını, normlarını ve değerlerini korumaya çalışan daha geniş ve daha katmanlı bir anlayışı kapsamaktadır. Ulusal güvenliğin kapsamı genişlemeye devam ederken, uluslararası güvenlik stratejileri ve teknolojilerinin inşa edildiği evrendeki her şey yenilenmeye ve değişmeye devam etmektedir. Teknoloji ilerledikçe ve bilgi akışı hızlandıkça, istikrarlı sosyal denge zorlaşmaktadır. Toplumlar sürekli olarak bu dengeyi yeniden ölçme ve yeniden kurma arayışındadır. Tartışmalar ve siber alanın belirsizliği politika yapıcılar için öngörülebilirliğin kapsamını sınırlamaktadır. Siber güvenlik ile ilgili problemler, hızlı sosyo-teknik dönüşümün, siyasi güç ve otoritenin değişmeye başladığı bir dünyada, yirmi birinci yüzyılın en önemli ulusal güvenlik sorunlarından biri olarak ortaya çıkmıştır. Siber güvenliğin ontolojik politikasıyla ilişki kurmak, farklı bir analiz türünün yolunu açmaktadır. Bu yaklaşım şunu hatırlatmaktadır: "Ortada açığa çıkarılmayı bekleyen bariz bir bağlam yoktur, eldeki malzeme için bariz analitik dayanak sağlayan hiçbir teori yoktur, bunun yerine, analizi yeni bir yöne götürme potansiyeline sahip sonsuz ilişkilendirme ve yan yana koyma fırsatları vardır."[428] Bu "ontolojik açılım", siber güvenliğin heterojen, dönüştürücü ve en önemlisi çoklu doğasına karşı eleştirel bir analitik duyarlılık sağlamaktadır. Bu siber güvenliğin aslında geleneksel güvenlik hesaplarına nasıl meydan okuyabileceğini göstermektedir. Bu durum da siber güvenlik politikalarının alanına ve onunla akademik ilişki kurmak için yeni yollar açmaktadır.

BİT'in teori ve politika üzerindeki etkileri kabul edilirse, siyasi olaylar olarak farklı siber ortamların nasıl ve hangi koşullar altında ortaya çıktığı tartışılmalıdır. Devlet ve devlet dışı unsurların, siber güvenlik uygulamalarının yeni politik alanları nasıl ortaya çıkardığını, böylece güvenlik politikasındaki geleneksel kavramların mekânsallığına nasıl meydan okuduğunu incelemek gerekmektedir. Son yıllarda siber güvenlik, hayatın bir parçası olmakta ve giderek daha fazla ilgi görmektedir. Buna rağmen, siber güvenlik ile ilgili literatür oldukça sınırlıdır. Ayrıca, mevcut literatür siber güvenliğe geleneksel güvenlik çalışmalarına uygun olarak yaklaşmakta, dolayısıyla mevcut güvenlik anlayışlarını sürdürmektedir. Siber güvenliği teorileştirme ve anlamlandırma

[428] Lien M. Elisabeth (2015). *Becoming Salmon. Oaklve: University of California*, s. 5, [http://www.uc.edu/book.php?isbn=9780520280571] (er. tar. 05.05.2021).

yöntemleri, bu çalışmada verilen bilgiler ışığında sorunları ele alma ve bunlarla yaşama becerileri için önemlidir. Elde edilen veriler ışığında güvenlik ve siber alan arasındaki bağlantının güvenlik politikasına dönüştürme yollarını aramak, mevcut literatür için katkı sağlayabilir. Siber güvenlik hakkındaki bilimsel literatür, güvenlik araştırmalarındaki mevcut tartışmaları sürdürmektedir. Siber güvenlik için;

1. Temelde en iyi uygulama, ulusal bir stratejinin geliştirilmesidir. Bu stratejiler, ülkelerin siber güvenlik çabalarını organize edebilecekleri bir politika çerçevesi sağlamaktadır. Bir strateji geliştirme süreci aynı zamanda geniş bir şekilde, hükümetler arası koordinasyon için bir mekanizma sağlayabilmektedir.

2. Devlet kurumları arasında siber güvenlik konusunda açık ve net sorumluluklar veren bir organizasyon yapısının kurulması gerekmektedir. Bu örgütsel uygulamanın önemli bir yönü, merkezi bir koordinasyon otoritesinin oluşturulmasıdır. Siber güvenlik birçok kurumun sorumluluğundadır ve zaman zaman gereksinimleri örtüşebilmektedir.

3. Siber alanda yaşanan olağanüstü devrim, bağımlılığı artırmakta ve hayatın her alanında olumlu ve olumsuz olarak yerleşmektedir. Küreselleşme ve demografik değişiklikler, insanlığın gıda, hammadde, su ve enerji gibi temel ihtiyaçları üzerinde çatışma riskini artırmaktadır. Aynı zamanda terörizm, kitle imha silahları, uyuşturucu kaçakçılığı, radikal dini hareketler, ulusötesi suç örgütleri, doğal afetler, yasadışı göç, mülteci hareketleri ve insan ticareti uluslararası bir karaktere bürünmekte ve günlük yaşamı büyük ölçüde etkilemektedir. Birçok ülkede adil yönetişim arayan toplumlar taleplerini daha yüksek sesle dile getirmekte ve bireyler, devlet odaklı bilginin etkisini azaltan BİT sayesinde daha fazla farkındalık kazanmaktadırlar. Devlet idareleri, toplumları, kendi argümanları konusunda ikna etmekte zorlanmakta ve vatandaşlar farklı bilgi kaynaklarına yönelebilmektedirler. Bu süreçte, devletlerin iç işlerine müdahale etmeme ilkesi test edilmekte, egemenlik kavramı geleneksel tanımını yitirmekte ve ortak egemenlik kavramı yeni alanlara doğru genişlemektedir. Kendi kendini belirleme ilkesi gelişmiş ülkelerde bile ön plana çıkmakta ve insanlar uluslararası zorlukların üstesinden gelmek için uluslararası kurumların etkinliğini ve meşruiyetini daha yoğun bir şekilde sorgulamaktadırlar.[429] Dolayısıyla devletler kendi politikalarını yaparak

[429] Nigâr Ağaoğulları Yalınkılıç (vd.). *Turkey in a Changing Global ve Regional Security Environment: Analysis ve Recommendations*, "Global Relations Forum", İstanbul: Cenkler Basımevi, 2015, s. 1.

siber güvenlik ile ilgili eylemleri tanımlamak ve yönlendirmek için kapsayıcı bir çerçeve yapısı oluşturmaktadırlar. Ayrıca kurum ve kuruluşların ihtiyaçlarına uygun siber güvenlik politikaları tasarlamalarına da olanak tanımaktadırlar. Bu nedenle siber güvenlik politikaları, ülkelerin siber alanlarının güvenli duruşunu iyileştirmek için belirli eylemlere ve programlara yol açan bir siber güvenlik çerçevesi olmaktadır.

Çalışmanın ikinci bölümünde, siber güvenliğin tarihsel gelişmeleri ve politikalarının belirlenme süreçleri tartışılmış; devletlerin bu konudaki kısıtlama ve stratejik çalışmaları incelemiş; küresel alanda siber güvenlik politikaları arasında doğru dengeyi nasıl bulmaları gerektiği ele alınmış; hükümetlerin neden daha fazla sorumluluk almaları gerektiği tartışılmıştır. Bu çalışmadaki siber güvenlik politikaları analizlerinin büyük bir kısmına kılavuzluk eden şey, bu stratejik bağlam ve önde gelen büyük güçlerin yerel kurumsal yapısındaki farklılıklardır. Ancak aynı zamanda, bireysel görüşler, bir yanda geleneksel (ABD, Çin, İsrail, Japonya, İngiltere) ve gelecek vadeden (Türkiye, Doğu Avrupa ülkeleri) demokrasiler arasındaki siber güvenlik politikalarındaki ilginç farklılıklara ve diğer yanda siber alanda karar verme de uluslararası kültürel farklılıkların önemli rolüne işaret etmektedir. Siber güvenlik politikaları küresel düzeyde giderek daha fazla müzakere edilmekte ve bu nedenle farklı bölgelerin ve kültürlerin siber alanda teknoloji ve siyasetin etkileşimi hakkında nasıl düşündüklerini daha iyi anlamamız gerekmektedir.

Çalışmanın üçüncü bölümünde Türkiye'de ulusal siber güvenlik stratejilerine ilişkin genel bakış, siber güvenlik stratejisinin bütünleşik ve kapsamlı hale geldiğini ortaya koymaktadır. Stratejiler, siber güvenliğe kolektif bir yaklaşımla yaklaşmakta ve siber güvenliğin ekonomik, sosyal, yasal, politik, stratejik, organizasyonel ile ilgili yönlerini kapsamaktadır.

Çalışmanın dördüncü bölümünde, İngiltere'nin siber güvenlik politika eylemleri dâhilinde çeşitli yönlere odaklandığı ifade edilmektedir. Bu bağlamda İngiltere'nin siber alanda ileri bir vizyon ortaya koyduğu görülmektedir.

Çalışmanın beşinci bölümünde, her iki ülkenin siber güvenlik alanında faaliyetlerinin karşılaştırmalı analizi yapılarak benzer ve farklı yönleri ile işbirlikçi faaliyetleri detaylı anlatılmaktadır. Standartlar, organizasyonlar ve teknolojiler açısından İngiltere, siber güvenlik politikalarını koordine etme ve uygulama konusunda daha aktiftir. Siber güvenlik politikası, esas olarak devletin siber güvenlikteki çeşitli rollerini (ve böylece yarı devlet ve devlet dışı unsurların rolleri de dâhil olmak üzere) tanımlamalar etrafında ilerlemektedir. İngiltere, siber

alandaki olayların teknik ve organizasyonel önlemine odaklanmaktadır. Türkiye ise ulusal kritik bilgi altyapılarına ve kilit kaynaklara yönelik siber saldırıların önlenmesi konularına odaklanmaktadır. Beşinci bölümde de bu bilgilere dayalı olarak her iki ülkenin siber güvenlik politikalarının karşılaştırılmalı analizi verilmiştir. Bununla birlikte değişen sosyal ve politik koalisyonlar, birkaç nesil siber güvenlik stratejilerinde fark edilebilen yeni siyasi kararlara yansımaktadır. Farklı ülkelerde siyasi etkileşim konuları benzer olsa da, farklı rollerin somut tezahürü, farklı çıkar gruplarının gücüne ve kurumlar arasında tarihsel olarak gelişen rollerin dağılımına ve güven ilişkilerine bağlıdır.

Bu çalışmadan çıkarılabilecek öneriler şunlardır:

- Türkiye ve İngiltere'nin kritik altyapı sistemlerine uygun yasa ve mevzuatlar yapılmalıdır. Bu şekilde, kritik altyapı koruma alanı yasal bir perspektife oturtulacaktır.
- Türkiye ve İngiltere'nin kritik altyapı sektörlerini artırması gerekmektedir. Bu sayede farklı sektörler için sektörel ve kurumsal CIRT sayısı artırılacak ve birçok altyapı koruma altına alınacaktır.
- Stratejiler; kritik altyapıların korunması ve kontrolü; eğitim, öğretim ve beceriler; standartlar, organizasyonlar ve teknolojiler için kurulan yeni kurumlar veya sektörel ve kurumsal CIRT'ler, kritik altyapıların geliştirilmesi ve güvenliği için özel olarak bütçe ayırmalıdır. Bu sayede gerekli yatırımlar yapılabilmekte ve acil durumlar anında aksiyon alınabilmektedir.
- Yasal ve Düzenleyici çerçeve oluşturulmalı, tüm kamu ve özel sektörleri düzenlemelidir.
- Eylem planlarının gerçekleştirilebilir olup olmadığına ilişkin ayrıntılı yıllık raporlar hazırlanmalı ve kamuoyuna duyurulmalıdır. Bu şekilde gerçekçi hedefler belirlenebilir ve önceki hatalardan da haberdar olunabilir.

Genel olarak bu çalışma siber güvenlik politikasının temel özelliklerini literatürdeki tasviri ve politika belgelerinin analizi yoluyla incelemiştir. Çalışma, siber güvenlik politikasının çeşitli olduğunu ve devletlerin karşılaştırılmasında Küresel Siber Güvenlik Endeksi'nin beş ana boyutu ışığında incelenmesinin önemini göstermektedir. Teorik olarak incelenen güvenlik kavramı, tarihsel olarak gelişen devlet üzerinden günümüze yansıtılmakta ve bunu bir alt dalı olarak siber güvenlik alanından örneklerle detaylandırmaktadır. Hükümet eylemlerinin çeşitliliğinin tanınması (hükümetlerin düzenlediği strateji belgeleri ve bu konuda yapılan faaliyetler), daha sonra genel bir stratejiye yol açabilecek

stratejik seçeneklerin geliştirilmesi için sağlam bir temel oluşturmaktadır. Siber güvenlik politikası için genel bir strateji, çeşitli hedeflerin birbirine karşı nasıl tartışıldığı konusunda net ilişkiler oluşturmalı ve devletin çeşitli rollerinde yerine getirdiği hedefi açıkça tanımlamalıdır. Sonuçlar her ülkelerde farklı görünse de siber güvenlik politikasının yer aldığı gerilim alanları aynı kalmaktadır.

Siber güvenlik teknolojileri kullanılarak hem hedefli hem de hedefsiz siber saldırılar gerçekleştirilebilmektedir. Yirmi birinci yüzyıl siber savaşlarına yerini sağlamlaştırmak isteyen bir millet için önerilerin dikkate alınması ve zamanında hayata geçirilmesi gerektiğine inanılmaktadır. Teknolojik gelişmeler açısından Türkiye'de siber güvenlik ve veri mahremiyeti ile ilgili olası risklerin önlenebilmesi ve teknolojileri geliştirme yeteneğini iyileştirmesi gerekmektedir. Ayrıca nitelikli insan kaynağının sağlanması ve mevzuat altyapısını değişen teknolojik koşullara göre güncel tutulması gerekmektedir.

2022 yılına bakıldığında çalkantılı, makroekonomik ve jeopolitik risklerle dolu bir yıl olduğu görülmektedir. Ukrayna'da yaşanan savaş, hızla artan enflasyon ve siber güvenliğe yönelik başarısızlıkları oluşturan, birbirleriyle iç içe girmiş risklerin bir bütünü olarak karşımıza çıkmıştır. Bunun Türkiye, İngiltere ve dünyanın geri kalanındaki devletler için siber güvenlik üzerinde derin bir etkisi olmuştur. 2023 ve sonraki yıllarda, boyutu veya sektörü ne olursa olsun tüm kurum ve kuruluşlar bir siber saldırıya veya veri ihlaline kurban gitme riskiyle karşı karşıya olduğundan, siber güvenlik her zamankinden daha önemli bir hale gelmektedir.

Çalışmanın *Giriş*'inde bazı destekleyici sorulara yer verilmiştir. Bu sorulara metin içerisinde cevaplar bulunmaya çalışılmıştır. Çalışmanın orjinalliğine ve özgün değerine bakıldığında, özellikle iki ülkenin yaklaşımlarının karşılaştırıldığı değerlendirmeler önem kazanmaktadır. İki farklı gelişmiş ve gelişmekte olan ülkenin, mevcut durum ve ileriye dönük yapabilecekleri olası siber güvenlik hamleleri ile ilgili bilgilendirici bir çalışma olmaktadır. Bu açıdan yol gösterici bir nitelik taşımaktadır. Siber güvenlik politikalarında daha önce yapılan çalışmalarda ABD, Rusya, Çin vb. gibi büyük ve gelişmiş ülkeler analiz edilmiş ve analiz edilmeye devam etmektedir. İngiltere gibi gelişmiş bir ülkenin siber güvenlik politikalarını, bu ülkeyle ilgili yapılan çalışmaların yetersizliği nedeniyle tercih edilmiştir. İngilizce kaynak taraması yapılmış olup hem Türkiye hem de İngiltere için fayda sağlayacak nitelikte orijinal bir çalışma ortaya konulmaya çalışılmıştır. Buna bağlı olarak bu çalışmanın özgün bir kaynak olduğu beyan edilebilir.

Küresel iş birliğine temelde ışık tutan 23 Kasım 2001 tarihinde Avrupa Konseyi Siber Suç Sözleşmesi, farklı ulusal yasalar için en uygun yasal standardı

kullanma fırsatı sunmaktadır. 29 Aralık 2020 tarihinde Türkiye ve İngiltere, Serbest Ticaret Anlaşması imzalamıştır.[430] Türk ve İngiliz hükümetleri ticareti serbest kılmak için anlaşmaya varmışlardır. Savunma, sanayi sektörü ve özel olarak savaş uçağı ve insansız hava araçları gibi katma değeri yüksek teknoloji yönelik projelerde birlikte çalışması iki ülkeye de yarar sağlayacaktır.

Türkiye ve İngiltere gibi ülkelerin siber güvenlik politikalarının stratejik açıdan kesiştiği ve değişkenlik gösterdiği alanlar bu çalışma da çeşitli risk unsurları dikkate alınarak incelenmiştir. Burada Türkiye'nin siber güvenlik ilkeleri verimlilik, dayanıklılık ve öngörüdür. İngiltere'nin siber güvenlik ilkeleri ise bunların yanısıra çok daha kapsamlı olarak korumacılık, hesap verilebilirlik ve iş birliğine odaklı çalışmadır. Her iki ülke bu değişkenliklerin yanısıra diğer ülkelerle de uluslararası iş birliğini, kamu-özel ortaklığını, kapasite geliştirmeyi ve Ar-Ge'yi teşvik etmek gibi ortak faaliyetleri benimsemiştir. Siber güvenlik politikalarında belirtilen faaliyetler, programlar ve projeler, ulusal siber güvenliğin sağlanması için ortak bir amaca hizmet etmektedir. Bunu başarmak için kültürel bağ, toplum yapısı, büyük bir uyum ve iş birliği gerekmektedir. Özellikle kritik altyapıların siber saldırılara karşı korunması için de uluslararası iş birliğine ihtiyaç duyulmaktadır. Buna bağlı olarak Türkiye ve İngiltere küresel iş birliğini de teşvik etmek üzere mevcut ve gelecekteki eylem planlarını açıkça ifade etmişlerdir.

Elde edilen veriler ışığında şunlar söylenebilir: Bu çalışmanın sonuçları, siber güvenlik yaklaşımlarının karşılaştırmalı bir analiz olarak sunulması ve beş ana unsur üzerinden analiz edilmesi, siber güvenliğin daha iyi anlaşılmasına yol açacaktır. Uluslararası düzeyde siber güvenlik konularıyla ilgilenen devletlerarasındaki iş birliğinin önündeki engellerin açıklanmasına katkıda bulunacaktır. Ayrıca, siber güvenliğe farklı yaklaşımların tanımlanması, belirli bir devletin siber alandaki eylemlerini açıklayıcı etki oluşturmaktadır. Devletler, siber güvenlik yaklaşımları olarak dikkate aldıkları nesneleri, potansiyel ve aktif düşman unsurları algılamadaki siber güvenlik üstünlükleri, siber güvenlik alt yapısının gelişimine bağlı olarak ortaya çıkmaktadır. Bu çalışmanın, gelecekte yapılacak çalışmalarda siber güvenlik politikaları ve iş birliği modellerini analiz etmek için yararlı bir rehber olması umulmaktadır.

[430] T.C Ticaret Bakanlığı (10.03.2022). BREXIT ve Birleşik Krallık STA [https://ticaret.gov.tr/dis-iliskiler/brexit-ve-birlesik-krallik-sta] (er. tar. 22. 05.2023).

KAYNAKÇA

AKTER, Lipi (vd.) (2013). "Information Security in Cloud Computing", *International Journal of Information Technology Convergence and Services (IJITCS)*, Sayı 3, No 4, ss. 13-22.

AKYEŞİLMEN, Nezir (2018). *Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik*, İstanbul: ORION.

ARI, Tayyar (2013). *Uluslararası İlişkiler Teorileri. Çatışma ve Hegemonya İşbirliği*, 8. Baskı, Bursa: MKM.

ASTILLEROS, Pablo ve William Mertka (2018). *Cybersecurity Guidelines and Best Practices for Emergency Services*, Belçika: EENA Document.

AYDIN, Faruk (2012). *Cyber Security in the National Protection of Turkey*, Master Thesis, Ankara: Cankaya University.

AYOOB, Mohammed (1991). "The Security Problematic of the Third World", *World Politics*, Sayı 43, No 2, ss. 257- 283.

BADA, Maria (Ed.) (2016). *Cybersecurity Capacity Review of the United Kingdom*, Oxford: Oxford University.

BAEZNER, Marie ve Patrice Robin (2017). "Hotspot Analysis: Stuxnet", *Center for Security Studies,* CSS, ss. 5-14.

BAIN, William (2003). *Between Anarchy and Society: Trusteeship ve the Obligations of Power,* Oxford: Oxford University.

BAIN, William (2012). *The Empire of Security and the Safety of the People,* London: Routledge.

BALDWIN, David A. (1997). "The Concept of Security," *Review of International Studies,* Sayı 23, No 1, ss. 5- 26.

BAYLIS, John (2008). "Uluslararası İlişkilerde Güvenlik Kavramı", *Uluslararası İlişkiler Dergisi,* Cilt 5, Sayı 18, ss. 69- 85.

BAYRAKTAR, Gökhan (2015). *Siber Savaş ve Ulusal Güvenlik Stratejisi,* İstanbul: Yeniyüzyıl.

BAYUK, Jennifer L. (vd.) (2012). *Cybersecurity Policy Guidebook*, USA: Wiley.

BECK, Ulrich (1992). *Risk Society: Towards a New Modernity*, London: SAGE.

BENNET, James C. (2007). *The Anglosphere Challenge: Why the English-Speaking Nations Will Lead the Way in the Twenty-First Century*, Marylve: Rowman & Littlefield.

BERKI, R. N. (1986). *Security and Society Reflections on Law*, *Order and Politics*, London: Dent.

BETTS, Richard K. (1982). *Surprise Attack: Lessons for Defense Planning*, Washington: Brookings Institution.

BETZ, David J. ve Tim Stevens (2013). "Analogical Reasoning and Cyber Security", *Security Dialogue*, Sayı 44, No 2, ss. 147-164.

BIÇAKÇI, Salih (2013). *21. Yüzyılda Siber Güvenlik*, (Ed. Mustafa Aydın), İstanbul: İstanbul Bilgi Üniversitesi.

BIÇAKÇI, Salih, D. Ergun ve M. Çelikpala (2016). "Türkiye'de Siber Güvenlik", (ed. Sinan ÜLGEN), *Türkiye'de Siber Güvenlik ve Nükleer Enerji*, İstanbul: EDAM.

BİRDİŞLİ, Fikret (2011). "Ulusal Güvenlik Kavramının Tarihsel ve Düşünsel Temelleri", *Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, Cilt 1, Sayı 31, ss. 149-169.

BLATCH, Maria (vd.) (2018). *The State of Cybersecurity Report*, USA: ACC Foundation.

BOOTH, Ken (1991). "Security and Emancipation", *Review of International Studies,* Sayı 17, No 4, ss. 313-326.

BOOTH, Ken (1997). "Security and self: Reflections of a Fallen Realist", (Ed. K. Krause ve M. C. Williams), *Critical Security Studies: Concepts and Cases*, Minnesota: University of Minnesota, ss. 83-119.

BOZDAĞLIOĞLU, Yücel (2007). "Yapılveırmacı Yaklaşım (Konstruktivizm)", *Uluslararası İlişkiler*, *Giriş, Kavramlar ve Kuramlar*, (Ed. Haydar Çakmak), Ankara: Platin.

BRODIE, Bernard (1949). "Strategy as a Science", *World Politics*, Sayı 1, No 4, ss. 467 – 488.

BUCHANAN, J. M. (1984). *Politics without Romance: A Sketch of Positive Public Choice Theory and Its Normative Implications*, (Ed. J.M. Bunchanan ve R. D. Tollison), The Theory of Public Choice II, USA: The University of Michigan.

BUCKLAND, Benjamin S. Fred Schreier ve Theodor H. Winkler (2015). "Democratic Governance Challenges of Cyber Security", *Geneva Security Forum, DCAF,* No 1, ss. 1-50.

BULL, Hedley (2012). *The Anarchical Society A Study of Order in World Politics,* (Ed. Verew Hurrell), 4. Baskı, London: Red Globe.

BUZAN, Barry (1984). "Peace, Power, and Security: Contending Concepts in the Study of International Relations", *Journal of Peace Research*, Sayı 21, No 2.

BUZAN, Barry; Ole Waever ve Jaap De Wilde (1998). *Security A New Framework For Analysis,* London: Boulder, Lynne Rienner.

BUZAN, Barry (2007). *People, States and Fear: National Security Problem in International Relations,* 2. Baskı, UK: ECPR.

CAI, Cuihong (2016). *Global Cybersecurity Environment: Perspectives of the US and China in Comparison*, "Securing CyberSpace International and Asian Perspectives", (Ed. Cherian Samuel ve Munish Sharma), New Delhi: Pentagon, ss. 319-332.

CAMPELL, David (1998). *Writing Security United States Foreign Policy and the Politics of Identity,* Minnesota: University of Minnesota.

CARR, Madeline (2016). "Public-Private Partnerships in National Cyber-Security Strategies", *International Affairs*, Sayı 92 (1) ss.43-62.

CARR, Madeline ve Feja Lesniewska (2020). "Internet of Things, Cybersecurity and Governing Wicked Problems: Learning from Climate Change Governance", *International Relations*, Sayı. 34 (3), ss. 391–412.

CAVALLARO, Lorenzo ve Dieter Gollmann (2013). *Information Security Theory* and *Practice,* New York: Springer.

CAVELTY, Myriam Dunn (2005). "The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP)", *International Journal of Critical Infrastructures,* Sayı 1 (2/3), ss. 258-268.

CAVELTY, Myriam Dunn (2008). *Cyber-Security and Threat Politics: U.S. Efforts to Secure the Information Age*, New York: Routledge.

CAVELTY, Myriam Dunn (2014). "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities", *Science and Engineering Ethics*, Sayı 20, No 3, ss. 701-715.

CAVELTY, Myriam Dunn (2014). *Cybersecurity in Switzerland*, NewYork: Springer.

CAVELTY, Myriam Dunn ve Egloff, F. J. (2019). "The Politics of Cybersecurity: Balancing Different Roles of the State", *St Antony's International Review*, Sayı 15, ss. 37–57.

CAVELTY, Myriam Dunn ve Vereas Wenger (2020). "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics and Networked Science", *Contemporary Security Policy*, UK: Routledge, Sayı 41, No 1, ss. 5-32.

CAVELTY, Myriam Dunn ve Vereas Wenger (2022). *Cyber Security Politics Socio-Technological Transformations and Political Fragmentation,* NewYork and London: Routledge.

CHEN, Hsin-I (2017). "Intercultural Communication in Online Social Networking Discourse", *Language and Intercultural Communication*, Sayı 17 (2), ss. 166-189.

CHOUCRI, Nazlı (2012). *Cyberpolitics in International Relations,* London: The MIT.

CLARKE, Richard A. ve Robert Knake (2010). *Cyber War: The Next Threat to National Security and What To Do About It,* NewYork: Ecco.

COMOR, Edward (2001). "The Role of Communication in Global Civil Society: Forces, Processes, Prospects," *International Studies Quarterly*, ss. 389-408.

CORNISH, Paul, Rex Hughes ve David Livingstone (2009). *Cyberspace and the National Security of the United Kingdom: Threats and Responses*, London: Chatham House Report.

ÇALIŞ, Şaban Halis (2002). "Ulus, Devlet ve Kimlik Labirentinde Türk Dış Politikası", (Ed. Şaban H. Çalış, İhsan Dağı, Ramazan Gözen), *Türkiye'nin Dış Politika Gündemi Kimlik Demokrasi Güvenlik*, Liberte.

ÇİFTÇİ, Hasan (2019). *Technology Foresight and Modeling: Turkish Cybersecurity Foresight 2040*, PhD Thesis, Ankara: METU.

DAMGARD, Ivan (Ed.) (1999). *Lectures on Data Security Modern Cryptology in Theory and Practice,* New York: Springer.

DARTNELL, Michael (2003). "Weapons of Mass Instruction: Web Activism and the Transformation of Global Security," *Millennium,* Sayı 32, No 3, ss. 477-499.

DEFOE, Daniel (2019). *Robinson Crusoe*, (Çev. Akşit Göktürk), Ankara: Yapı Kredi Yayınları.

DEIBERT, Ronald J. (2003). "Black Code: Censorship, Surveillance, and the Militarization of Cyberspace", *Millennium*, ss. 501-530.

DEIBERT, R. ve Rohozinski, R. (2010). "Risking Security: The Policies and Paradoxes of Cyberspace Security", *International Political Sociology*, Sayı 4, ss. 15–32.

DER DERIAN, James (1990). "The (S)pace of International Relations: Simulation, Surveillance and Speed", *International Studies Quarterly*, Sayı 34, No 3, ss. 295-310.

DILLON, Michael (1996). *Politics of Security: Towards a Political Philosophy of Continental Thought*, London: Routledge.

DILLON, Michael ve Verew W. Neal (Ed.) (2008). *Foucault on Politics, Security and War,* New York: Palgrave Macmillan.

DUTTON William H. (vd.) (2013). *Cultures of the Internet: The Internet in Britain,* University of Oxford, Oxford Internet Survey Report.

DÜVEROĞLU, Efe (2020). *A Comparative Analysis of Critical Insfracture Cyber Security Policies: Best Practices From the Us, EU and Turkey,* Yüksek Lisans Tezi, Ankara: Bilkent Üniversitesi.

EGLOFF, Florian (2015). "Cybersecurity ve the Age of Privateering: A Historical Analogy", Oxford: Cyber Studies Programme *Working Paper Series* No 1, ss.1-14.

ERIKSSON, Johan ve Giampiero Giacomello (2006). "The Information Revolution, Security and International Relations: (IR)relevant Theory?" *International Political Science Review* 27 (3).

FARWELL, James P. ve Rafal Rohozinski (2011). "Stuxnet and the Future of Cyber War", *Survival Global Politics and Strategy*, Sayı 53, No 1, ss. 23-40.

GARLAND, David (2001). *The Culture of Control: Crime and Social Order in Contemporary Society*, Oxford: Oxford University.

GATTIKER, URS E. (2004). *The Information Security Dictionary, Defining the Terms that Define Security for E-Business, Internet, Information and Wireless Technology,* NewYork: Kluwer Academic Publishers.

GEERS, Kenneth (2011). *Strategic Cyber Security. NATO Cooperative* Cyber Defence Centre Of Excellence Talinn, Estonia: CCD COE Publication.

GIDDENS, Anthony (1990). *The Consequences of Modernity,* UK: Polity.

GLUSCHKE, Guido; Mesut Hakkı Caşın ve Marco Macori (Ed.) (2018). *Cyber Security Policies and Critical Infrastructure Protection,* Germany: Institute for Security ve Safety (ISS) .

GLUSCHKE, Guido; M. Caşın ve M. Macori (Ed.) (2018). *Cyber Security Policies and Critical Infrastructure Protection,* "Critical Infrastructure Security Paradigm and Modern Protection Policies", (Ed. Robert Radvanovsky), Germany: Institute for Security and Safety (ISS).

GLUSCHKE, Guido; M. Caşın ve M. Macori (Ed.) (2018). *Cyber Security Policies and Critical Infrastructure Protection,* "Strengthening the Legal Framework for the Physical Security of Nuclear Materials for the Future of Nuclear Renaissance: Risks, Ossortunities and the Case of Turkey", (Ed. Mesut Hakkı Caşın), Germany: Institute for Security and Safety (ISS).

GOLDMAN, Michael S. (2014). "Asslying the Historical Lessons of Surprise Attack to the Cyber Domain: The Example of the United Kingdom", (Ed.

Emily O. Goodman ve John Arquilla), *Cyber Analogies,* California: Naval Postgraduate School, ss. 15-25.

HASHIMOTO, Yasuaki (2016). "Cybersecurity Policy in Japan", *Securing CyberSpace International and Asian Perspectives,* (Ed. Cherian Samuel ve Munish Sharma), New Delhi: Pentagon, ss. 295-305.

HANSEN, Lene ve Helen Nissenbaum (2009). "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly*, Sayı 53, No 4, ss. 1155-1575.

HEKİM, Hakan ve Oğuzhan Başıbüyük (2013). "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları" (Cyber Crimes and Turkey's Cyber Security Policies), *Uluslararası Güvenlik ve Terörizm Dergisi*, Cilt 4, Sayı 2, ss.135 – 158.

HERRERA, Geoffrey L. (2003). "Technology and International Systems", *Millennium*, ss. 559-593.

HERRING, Susan C. (1996). *Computer-Mediated Communication: Linguistic, Social, and Cross-Cultural Perspectives*, Amsterdam/Philadelphia: John Benjamins Publishing Company.

HERZ, John (1950). "Idealist Internationalism and the Security Dilemma", *World Politics*, Sayı 2, No 2, ss. 157 – 180.

HIRSHFIELD, Leanne (vd.) (2015). "The Role of Human Operators' Suspicion in the Detection of Cyber Attacks", *International Journal of Cyber Warfare and Terrorism*, Sayı 5(3), ss. 28-44.

HOBBES, Thomas (2016). *Leviathan*, (Ed. Marshall Missner), London: Routledge.

HOUGH, Peter (2018). *Understanding Global Security,* 4. Baskı, London: Routledge.

HUYSMANS, Jef (1998). "Security! What Do You Mean?: From Concept to Thick Signifier", *European Journal of International Relations*, Sayı 4, No 2, ss. 226-255.

JACKSON, Robert (2005). *The Global Covenant: Human Conduct in a World of States,* London: Oxford University.

KANT, Immanuel (2015). *Ahlak Metafiziğinin Temellendirilmesi,* Ankara: Türkiye Felsefe Kurumu.

KAYA, Mehmet Bedii (2019). "Hukuki Açıdan Bilişim Suçları, Siber Güvenlik ve Adli Bilişim", (Ed. Şeref Sağıroğlu ve Mustafa Şenol), *Siber Güvenlik ve Savunma: Problemler ve Çözümler*, 1. Baskı, Ankara: Grafiker Yayınları.

KNASS, Kenneth J. (2009). *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions,* New York: Information Science Reference.

KRAUSE Lawrence B. ve Joseph S. Nye (1975). "Reflections on the Economics and Politics of International Economic Organizations", Section IV, *International Organization*, Sayı 29, No 1, ss. 323-342.

KRAUSE, Keith ve Michael C. Williams (1997). *Critical Security Studies: Concepts and Cases,* Minnesota: University of Minnesota.

KRAUSE, Keith ve Michael C. Williams (1997). *Critical Security Studies: Concepts and Cases,* "From Strategy to Security: Foundations of Critical Security Studies", Minnesota: University of Minnesota, ss. 33-59.

KRAUSE, Keith ve Jennifer Milliken (2009). "Introduction: The Challenge of Non-State Armed Groups", *Contemporary Security Policy,* Sayı 30, No 2, ss.202-220.

KREMER, Jan-Frederik and Benedikt Müller (2014). *Cyberspace and International Relations Theory, Prospects and Challenges*, NewYork: Springer.

KREMER, Steve (vd.) (2019). *Cybersecurity: Current Challenges and Inria's Research Directions,* Fransa: White Book.

LALLIE, Harjinder Singh (vd.) (2021). "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks During the Pandemic", *Computers & Security*, Sayı 105.

LATICI, Tania (2020). "Understanding EU-NATO Cooperation Theory and Practice", European Parliament Briefing: European Parliamentary Research Service (EPRS).

LEE, Robert (vd.) (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid*, Washington DC: E-ISAC.

LEINER, Barry M. (vd.) (2009). "A Brief History of the Internet", Sayı 39, No 5, ss. 22-31.

LEVIN, Ilya ve Dan Mamlok (2021). "Culture and Society in the Digital Age", *Information 2021*, Sayı 12, No 68, ss. 1-13.

LEWIS, James Verew (2016). *Advanced Experiences in Cybersecurity Policies and Practices An Overview of Estonia, Israel, South Korea, and the United States*, USA: Inter-American Development Bank.

LIBICKI, Martin C. (2009). *Cyberdeterrence and Cyberwar*, US: RVE.

LINDSAY, Jon (2012 Report). "China and Cybersecurity: Political, Economic, and Strategic Dimensions", *IGCC Workshop Report on China and Cybersecurity*, San Diego: University of California, ss. 1-36.

LUKE, Timothy W. (1991). "The Discipline of Security Studies and the Codes of Containment: Learning From Kuwait", *Alternatives,* Sayı 16, No 3, ss. 315-344.

MACEWAN, Neil (2017). *Responsibilisation, Rules and Rule-Following Concerning Cyber Security: Findings from Small Business Case Studies in the UK*, PhD Thesis, UK: University of Southampton.

MALI, Prashant (2016). "Critical Analysis of National Cyber Security Policies of UK, India, USA & Germany", *Chevening Fellowship in Cybersecurity Project*, ss.1-19.

MALEC, Mieczyslaw (2003). *Security Perception: Within and Beyond The Traditional Assroach*, California: Naval Postgraduate Thesis.

MAURER, Tim (2011). *Cyber Norm Emergence at the United Nations An Analysis of the Activities at the UN Regarding Cyber,* Cambridge: Belfer Center for Science and International Affairs.

MCLUHAN, Marshall (1964). *The Medium is the Message*, Understanding Media: The Extensions of Man.

MEARSHEIMER, John J. (1990). "Back to the Future: Instability in Europe after the Cold War", *International Security,* Sayı 15, No 1, ss. 5-56.

MORGAN, Steve (16.10.2017). "Cybercrime Damages $6 Trillion By 2021", *Cybersecurity Ventures Official Annual Cybercrime Report*, *Cybercrime Magazine.*

MURPHY, Emma C. (2009). "Theorizing ICTs in the Arab World: Informational Capitalism and the Public Sphere," *International Studies Quarterly*, Sayı 53, No 4, ss. 1131-1153.

NADIKATTU Rahul Reddy (2020). "Cyber Security in America", *Vivekananda Journal of Research,* Sayı 9/1, ss. 166-174.

NCSC (04.2021). "Cyber Essentials: Requirements for IT Infrastructure", UK: Cyber Essentials.

NWACHHUKWU, Nwosu John (2022). "Nigeria Cyber Security Analysis for a Secure Nation", *INOSR Experimental Sciences*, Sayı 8(1), ss. 30-37.

NYE, Joseph ve Sean Lynn-Jones (1988). "International Security Studies: A Report of a Conference on the State of the Field", *International Security*, Sayı 12, No 4, ss. 5-27.

NYE, Joseph S. Jr. (2011). "Nuclear Lessons for Cyber Security?" Harvard: *Strategic Studies Quarterly*, Sayı 5, No 4, ss. 18-38.

NYE, Joseph S. Jr (2014). "The Regime Complex for Managing Global Cyber Activities", London: Global Commission on Internet Governance *(CIGI) and Chatham House*, No 1, ss. 1-15.

ORJI, Uchenna Jerome (2016). "Regionalising Cybersecurity Governance in Africa: an Assessment of Responses", *Securing CyberSpace International and Asian Perspectives,* (Ed. Cherian Samuel ve Munish Sharma), New Delhi: Pentagon, ss. 203-218.

PEREIRA, Lus Moniz (2018). "Cyberculture, Symbiosis, and Syncretism", *Springer-Verlag*, No 33, ss. 447-452.

PREECE, J. Jackson (2011). *Security in International Relations*, London: University of London.

PUYVELDE, Damien Van ve Aaron F. Brantly (2019). *Cybersecurity Politics, Governance and Conflict in Cyberspace*, New York: Wiley.

REARDON, Robert ve Nazlı Choucri (2012). "The Role of Cyberspace in International Relations: A View of the Literature", *ISA Annual Convention.*

ROTHSCHILD, Emma (1995). "What is Security?", *Daedalus*, Sayı 124, No 3, ss. 53-98.

ROWLEY, Christina ve Jutta Weldes (2012). "The Evolution of International Security Studies and the Everyday: Suggestions from the Buffyverse", *SPAIS*, No 11-12, ss. 1-36.

RUDOLPH, Christopher (2003). "Globalization and Security", *Security Studies,* Sayı 13, No 1, ss. 1-32.

SCHELLING, Thomas (2006). *The Strategy of Conflict*, Cambridge, Massachusetts: Harvard University.

SCHMIDT, John Michael (2015). "Policy, Planning, Intelligence and Foresight in Government Organizations", *Foresight*, 17(5), ss. 489-511.

SCHWAB, Klaus (2018). *Dördüncü Sanayi Devrimi,* World Economic Forum, İstanbul: Optimist.

SILFVERSTEN, Erik (vd.) (2020). "Cybersecurity A State-of-the-art Review: Phase 2", *Final Report,* UK: RVE Europe.

SINGER P.W ve Allan Friedman (2013). *Cybersecurity and Cyberwar: What Everyone Needs to Know,* England: Oxford University.

StANDage, Tom (2014). *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-line Pioneers*, 2. Baskı, USA: Bloomsbury.

STEWENSON, Angus (2007). *Shorter Oxford English Dictionary on Historical Principles*, 6. Baskı, Sayı 2, Oxford: Oxford University.

SUNRAMANIAN, Ramesh (2008). *Computer Security, Privacy, and Politics: Current Issues, Challenges and Solutions,* New York: IRM.

ŞENTÜRK, Hakan (vd.) (2012). "Cyber Security Analysis of Turkey", *International Journal of Information Security Science*, Sayı 1, No 4, ss. 112-125.

TABANSKY, Lior, Isaac Ben Israel (2015). "The Israeli National Cybersecurity Policy Focuses on Critical Infrastructure Protection (CIP)", *Cybersecurity in Israel*, SpringerBriefs in Cybersecurity UK: Springer, Cham, ss. 35-42.

TATAR, Ünal (vd.) (2014). "A Comparative Analysis of the National Cyber Security Strategies of Leading Nations", *9th International Conference on Cyber Warfare and Security*, (Ed. Sam Liles), ss. 211-218.

TIKK, Eneken ve Mika Kerttunen (2020). *Routledge Hvebook of International Cybersecurity*, 1. Baskı, NY: Routledge.

TOMIC, Dusko; Eldar Saljic ve Danilo Cupic (2018). "Cybersecurity Policies of East European Countries", (Ed. E. G. Carayannis (vd.)), NY: Springer International Publishing AG, *Handbook of Cyber-Development, Cyber-Democracy and Cyber-Defense*.

TOURE, Hamadoun (2011). "ITU's Global Cybersecurity Agenda, in The Quest for Cyber Peace", *International Telecommunication Union and World Federation of Scientists*.

TOWNSEND, Anthony M. (2013). *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*, NewYork: W. W. Norton & Company.

ULAŞANOĞLU, Emin (vd.) (2010). "Bilgi Güvenliği: Riskler ve Öneriler", *Bilgi Teknolojileri ve İletişim Kurumu*.

ULLMAN, Richard H. (1983). "Redefining Security", *International Security*, Sayı 8, No 1, ss. 129-153.

UZELAC, Aleksvera (2008). "Recognising Networks in Cultural Field", *Network Models in Real and Virtual Sphere*, No 8, ss. 133-155.

ÜNVER, Gül N. (2017). "Ulusal Siber Güvenlik Strateji Belgelerinde İnsan Hakları", *Cyberpolitik Journal*, 2 (4), ss. 104-129.

ÜNVER, Gül N. (2018). "Siber Çatışmaların Tanımlama Sorunu", *Cyberpolitik Journal*, Sayı. 3, No. 5, ss. 23-44.

ÜNVER, Gül Nazik (2023). "Cyber Security Policies of Türkiye and England During the Pandemic Period", 7th Bosphorus International Conference On Cybersecurity, Cyberpolitics And Social Sciences (5-8 July 2023), Poland: University of Szczecin.

VISHIK, Claire (vd.) (2016). "Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms", Chapter 11, *International Cyber Norms: Legal, Policy & Industry Perspectives,* (Ed. Anna-Maria Osula ve Henry Rõigas), Talinn: NATO CCD COE Publications.

WAEVER, Ole; Barry Buzan (vd.) (1993). Identity, Migration and the new Security Agenda in Europe, London: Palgrave Macmillan.

WAEVER, Ole (1996). "European Security Identities", *Journal of Common Market Studies*, Sayı 34, No 1, ss. 103-132.

WALICZKO, Tomasz (2020). "WeChat- a Chinese Cyber-Culture Phenomenon", *Modern Management Review,* ss.143-155.

WALKER, R. B. J. (1990). "Security, Sovereignty, and the Challenge of World Politics", *Alternatives*, Sayı 15, No 1, ss. 3-27.

WALT, Stephen M. (1991). "The Renaissance of Security Studies", *International Studies Quarterly*, Sayı 35, No 2, ss. 211-239.

WALTZ, Kenneth (2004). "Neorealism: Confusions and criticisms. Journal of Politics ve Society", *Journal of Politics & Society*, Sayı 15/1, ss. 2-6.

WAMALA, Frederick (2011). *The ITU National Cybersecurity Strategy Guide*, ITU.

WAMER, Michael (2012). "Cybersecurity: A Pre-History". *Intelligence and National Security*, Sayı 27 (5), ss. 781-799.

WELLINGS, Ben (2014). "Euroscepticism and the Anglosphere: Traditions and Dilemmas in Contemporary English Nationalism", *JCMS*, ss. 1–17.

WILLIAMS, Michael C. (1998). "Identity and the Politics of Security", *European Journal of International Relations,* Sayı 4, No 2, ss. 204-225.

YALINKILIÇ, Nigâr Ağaoğulları (vd.) (2015). *Turkey in a Changing Global and Regional Security Environment: Analysis and Recommendations*, Global Relations Forum, İstanbul: Cenkler Basımevi.

YILMAZ, Sacit (2011). "5237 Sayılı Türk Ceza Kanunu'nun 244. Maddesi'nde Düzenlenen Bilişim Alanındaki Suçlar", *TBB Dergisi*, Sayı 92, ss. 62-100.

Ulusal Strateji Belgeleri, Alınan Kararlar ve Raporlar:

ABI Research (2014). *Global Cybersecurity Index.*

AFAD (2014). *2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi.* Ankara: T.C. Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı.

AustralIa (2020). *Australia's Cyber Security Strategy.*

BUDAPEST, Convention on Cybercrime (23.11.2001). *European Treaty Series*, No 185.

CABINET OFFICE (2010). *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*.

CABINET OFFICE (25.05.2016). *Procurement Policy Note- Cyber Essentials Scheme*, UK: Crown Commercial Service, ss. 1-11.

CABINET OFFICE. *Reducing the Cyber Risk in 10 Critical Areas*.

CABINET OFFICE (Haziran 2009a). *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space*, London: United Kingdom Government.

CABINET OFFICE (2009b). *The National Security Strategy of the United Kingdom: Update 2009, Security for the Next Generation*, London: United Kingdom Government.

CABINET OFFICE (2011). *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, London: United Kingdom Government.

CABINET OFFICE (2014). *The UK Cyber Security Strategy Report on Progress and Forward Plans: December*.

CABINET OFFICE (2014a). *Cyber Security is Essential in Today's Marketplace Release*, 5th November, HMSO.

CABINET OFFICE (5.11.2015). *Cyber Insurance Joint Statement*, HMSO.

CABINET OFFICE (2015a). *UK Cyber Security: The role of Insurance in Managing and Mitigating Risk*, HMSO.

CABINET OFFICE (2015b). *Cyber Security Insurance: New steps to make UK World Centre. Release*.

CABINET OFFICE (2015c). *10 Steps to Cyber Security: Executive Companion*, HMSO.

CABINET OFFICE (2016). *Expanding the Cyber First Programme*, London: Minister for Cabinet Office.

CABINET OFFICE (2016a). *Keeping Britain safe from Cyber Attacks*, London: Minister for Cabinet Office.

CABINET OFFICE (2016b). *Procurement Policy Note- Cyber Essentials Scheme*.

CABINET OFFICE (2022). *Government Cyber Security Strategy: Building a Cyber Resilient Public Sector 2022-2030*.

CPNI (2020). *Center for the Protection of National Infrastructure*.

Digital Britain Final Report cm 7650 (2009). London: TSO.

ENGLAND. Cyber Security of the UK's Critical National Infrastructure, Third Report of Session 2017-19, England: House of Lords.

FRENCH (2011). *French Network and Information Security Agency (FNISA),* "France's Strategy: Information Systems Defense and Security".

GERMANY (2011). *Cyber Security Strategy for Germany*.

ITU (2017). *Global Cybersecurity Index.*

ITU (2018). *Global Cybersecurity Index.*

ITU (2020). *Global Cybersecurity Index.*

İNGİLTERE (2010). A Strong Britain In An Age Of Uncertainty: The National Security Strategy.

İNGİLTERE (2016). *UK National Cyber Security Strategy*.

LITHUANIA (2018). *National Cyber Security Strategy*.

LITHUANIA (2021). *Key Trends ve Statistics of the National Cyber Security Status of Lithuania*.

NETHERLANDS (2011). *The National Cyber Security Strategy (NCSS): Success Through Cooperation.*

On Birinci Kalkınma Planı (2019-2023). "Siber Güvenlik ve Mahremiyet". On Birinci kalkınma Planı (2019-2023). "Küresel Gelişmeler ve Eğilimler". PCI SecurIty Standards CouncIl (2018). "PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard", USA: PCI DSS v3.2.1 Quick Reference Guide.

SPO (2006-2010). "Information Society Strategy Action Plan", *Assessment Report*, No 5, Ankara.

T.C. Adalet Bakanlığı (Nisan 2021). İnsan Hakları Eylem Planı Uygulama Takvimi.

TÜBİTAK (2004). "Ulusal Bilim ve Teknoloji Politikaları 2003-2023 Strateji Belgesi".

Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi.

Türk Ceza Kanunu, Kişisel Verilerin Korunması 5237 Sayılı TCK, Madde 135 ve 136.

Türkiye Cumhuriyeti Savunma Sanayi Başkanlığı, "Türkiye Siber Güvenlik Kümelenmesi".

Türk Standartları Enstitüsü, "ISO/IEC 27001 Kişisel Verilerin Korunması Kanunu & ISO 27701 Kişisel Veri Yönetim Sistemi".

Türk Standartları Enstitüsü, "ISO/IEC 27017 Bulut Hizmetlerinde Bilgi Güvenliği Yönetim Sistemleri (BBYS)".

TÜBİTAK ve BTK. (2011) I. Ulusal Siber Güvenlik Tatbikatı Sonuç Raporu.

TÜRKİYE (Haziran 2012). *Ulusal Siber Güvenlik Stratejisi*.

TÜRKİYE (2016-2019). *Ulusal Siber Güvenlik Strateji Belgesi*.

TÜRKİYE (2019). *Bilişim Derneği Küresel Gelişmeler Raporu.*

TÜRKİYE (2020-2023). *Ulusal Siber Güvenlik Eylem Planı.*

TÜRKİYE, *Ulusal Siber Güvenlik Eylem Planı 2020-2023, Cumhurbaşkanlığı Genelgesi.*

UK Furman Report (2019). "Unlocking Digital Competition Report of the Digital Competition Expert Panel", UK: OGL, [https://www.gov.uk/government/publications/unlocking-digitalcompetition-report-of-the-digital-competition-expert-panel].

UK. National Cyber Security Strategy 2016-2021.

UK (2009). *Cyber Security Strategy of the United Kingdom*, London: TSO.

UK (2009). *The National Security Strategy of the United Kingdom: Update 2009 Security for the Next Generation,* London: TSO.

UK (2009). *Cyber Security Strategy of the United Kingdom Safety, Security ve Resilience in Cyber Space*, UK: Cabinet Office.

UK (2016-2021). "UK National Cyber Security Strategy".

UK (2010). "A Strong Britain In An Age Of Uncertainty: The National Security Strategy".

UK (2020). "Cyber experts step in as criminals seek to exploit Coronavirus fears", National Cyber Security Centre United Kingdom.

UK "2022 Civil Nuclear Cyber Security Strategy", London: OGL.

Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı 2020-2023, Türkiye Çevre ve Şehircilik Bakanlığı.

UK "Forgery Act 1913".

UK (1990). "Computer Misuse Act 1990".

UK (1978). "Protection of Children Act 1978".

UK (1988). "Copyright, Designs ve Patents Act 1988".

UK (1998). "Human Rights Act 1998".

UK (2000). "Regulation of Investigatory Powers Act 2000".

UK (2006). "Fraud Act 2006".

UK (Eylül 2011). *The Parliamentary Office of Science and Technology,* "Cyber Security in the UK", POSTnote No 389, [www.parliament.uk/].

UN (2008). *International Telecommunication Union*, ITU Global Cybersecurity Agenda: High Level Experts Group, Global Strategic Report. Geneva: United Nations.

UN (Mart 2010). *International Telecommunication Union*, Cybersecurity for all, Global Cybersecurity Agenda: A Framework for International Cooperation, Geneva: United Nations.

UNODC (2020). "COVID-19: Cyber Threat Analysis", Cybercrime Global Program.

UNODC (2020). "COVID-19: How to Stay Safe from Cybercriminals Exploiting the Pandemic".

US White House (February 2003). *The National Strategy to Secure Cyber Space*.
USA (Eylül 2018). *National Cyber Strategy*.
WSIS (2005). Report of the Tunis phase of the World Summit on the Information Society (WSIS). Tunus: WSIS.

İnternet Adresleri:

___[www.scmagazine.com/home/security-news/].
___[https://www.britannica.com/biography/Al-Gore].
___[https://dictionary.cambridge.org/tr/s%C3%B6zl%C3%BCk/ingilizce/security].
___[https://www.siberyildiz.com/].
___[https://www.oxfordmartin.ox.ac.uk/cyber-security/].
___[https://tse.org.tr/IcerikDetay?ID=2059].
___[https://www.networklab.co.uk/cmodem/basics.html].
___"Audit ve Risk Committee Minutes" (11.2020),
[https://www.cps.gov.uk/publication/minutes-cps-audit-ve-risk-committee/arc-minutes-october-2020].
___"Bilgi Güvenliği Derneği", *SETA Medya*, [https://bilgiguvenligi.org.tr/].
___ "Birleşmiş Milletler Antlaşması ve Uluslararası Adalet Divanı Statüsü",
[https://www.ombudsman.gov.tr/].
___"CIRT (Cyber Incident Response Team)",
[https://www.gartner.com/en/information-technology/glossary/cirt-cyber-incident-response-team].
___ "Communication from the Commission to the European Parliament, The European Council and the Council", *16. Progress Report*, Brüksel,
[https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2015:614:FIN].
___Corporate Information Governance (2018). "Information Security Policy: England", [https://www.england.nhs.uk].
___"Cyber Champions", [https://www.cyberchampions.org/].
___"Cybersecurity Challenge UK", [https://cybersecuritychallenge.org.uk/].
___ "Cybersecurity Risks, Progress, and the Way Forward in Latin America and Caribbean", *2020 Cybersecurity Report*, [www.cybersecurityobservatory.org].
___"Crisis Management Exercise 2017", *NATO*, [https://www.nato.int/].
___ "Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri 12 Sayılı Genelgesi" (2019). [https://cbddo.gov.tr/mevzuat/2019-12-sayili-bilgi-guvenligi-tedbirleri-cumhurbaskanligi-genelgesi/].

___ "Data Protection in Turkey", [https://www.kvkk.gov.tr/Icerik/5389/Data-Protection-in-Turkey].
___"E-Dönüşüm Türkiye", [http://www.bilgitoplumu.gov.tr/bilgi-toplumu/e-donusum-projesi/].
___"Elektronik Apostil Sistemi" (2018), [https://www.ptt.gov.tr/].
___ "EU Cybersecurity Dashboard A Path to a Secure European Cyberspace" (2015), [https://cybersecurity.bsa.org/].
___" E&T", [https://eandt.theiet.org/].
___ "Global IoT Market Will Grow to 24.1 Billion Devices in 2030, Generating $1.5 Trillion Annual Revenue" (19.05.2020), [https://www.prnewswire.com/].
___Global Cyber Security Capacity Centre 2021, University of Oxford, [https://gcscc.ox.ac.uk/the-cmm#/].
___" ISC Turkey", [http://iscturkey.org/].
___ ITU Rev. 36 Antalya (2006), [https://www.itu.int/oth/R0B06000017].
___ ITU Cyber Security Guide for Developing Countries (2006), [https://www.itu.int/].
___ ITU Cyber Security Guide for Developing Countries (2007), [https://www.itu.int/].
___ITU (2008). "Series X: Data Networks, Open System Communications and Security, Overview of Cybersecurity", *ITU-T Recommendation*, 10 (1), ss. 8-12.
___ ITU (2008). *Corporate Annual Report*.
___ITU (2009). *Cyber Security Guide for Developing Countries*, [https://www.itu.int/].
___ITU (2011). *National Cyber Security Strategy Guide*, [https://www.itu.int/].
___ITU (2011). *The Quest For Cyber Peace*, (Ed. Hamadoun I. Touré), [https://citizenlab.ca/].
___ITU (2012). *Readiness Assessment for Establishing a National CIRT*, [https://www.itu.int/].
___ITU (2012). *HIPCAR Assessment Cybercrimes*, [https://www.itu.int/].
___ITU (2013). *ICB4PAC Assessment Eletronic Crime*, [https://www.itu.int/].
___ITU (2014). *Understanding Cyber Crime*, [https://www.itu.int/].
___ITU (2014). The Quest for Cyber Confidence, (Ed. Hamadoun I. Touré), [https://www.itu.int/].
___ITU (2015). Global Cyber Security Index (GCI)v1, [https://www.itu.int/].
___ITU (2017). *Global Cybersecurity Index (GCI)v2*, [https://www.itu.int/].

___ ITU (2018). *Global Cybersecurity Index (GCI) v3*, [https://read.itu-ilibrary.org/].

___ ITU (05.2020). *Connect 2030-An Agenda to Connect all to a Better World*, [https://www.itu.int/en/mediacentre/backgrounders/Pages/connect-2030-agenda.aspx].

___ITU (2020). *Global ICT Regulatory Outlook,* [https://itu.foleon.com/itu/global-ict-regulatory-outlook-2020/home/].

___ ITU (2020). *Tech v COVID-19: Managing the Crisis", ITU News 03,*
[https://www.itu.int/en/myitu/Publications/2020/09/09/13/13/ITU-News-Magazine-No3-2020].

___ ITU (2020). *Economic Experts Roundtable, Economic Impact of COVID-19 on Digital Infrastructure*, GSR-20 Discussion Paper, [https://www.itu.int/en/ITU-D/Conferences/GSR/2020/Pages/default.aspx].

___ ITU (2021). *ICT trends ve developments in Europe, 2017-2020, Digital trends in Europe 2021.*

___"Janet: the UK's Research & Education Network",
[https://www.infraportal.org.uk/infrastructure/janet-the-uks-research-education-network].

___"M2M or Machine to Machine Communication, What is it?", "What is the M2M Communication?" (2019), [https://www.atriainnovation.com].

___"Managing the Impact of COVID-19 on Cyber Security", [https://www.pwccn.com/en/issues/cybersecurity-and-privacy/covid-19-impact-mar2020.html].

___Milletler Cemiyeti Misakı, [http://sam.baskent.edu.tr/belge/], ss. 3-11.

___National Cyber Security Centre (NCSC)- Switzerland,
[https://www.cybersecurityintelligence.com/national-cyber-security-centre-ncsc-switzerland-4181.html].

___National Cyber Security Policy (2013), [https://www.itu.int/en/ITU-D/Cybersecurity], ss. 1-9.

___National Data Protection Authority, [https://www.dlapiperdataprotection.com/].

___National Cyber Security Strategy Guidelines (Tallinn 2013), [https://ccdcoe.org/].

___National CIRT, [https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx].

___ NIS Directive [https://digital-strategy.ec.europa.eu/en/policies/nis-directive].

___ “Pax Romana”, [https://www.britannica.com/event/Pax-Romana].
___“PRISM (Surveillance Program)”,
[https://www.sindark.com/genre/PRISM%20(surveillance%20program).pdf].
___Security and Protection System,
[https://www.britannica.com/technology/security-and-protection-system].
___ SSB,
[https://www.ssb.gov.tr/WebSite/contentlist.aspx?PageID=39&LangID=2].
___“T.C. Ulaştırma ve Altyapı Bakanlığı” (2019).
[https://www.uab.gov.tr/haberler/global-siber-guvenlik-endeksine-gore-turkiye-avrupa-da-11-dunya-genelinde-ise-20-siraya-yukseldi].
___“The Center for Internet Security” [https://www.cisecurity.org/].
___“The Internet of Things: a Movament not a Market”, [https://cdn.ihs.com/].
___“The EU Cybersecurity Act: a new Era Dawns on ENISA”, [https://www.enisa.europa.eu/].
___ The Center for Internet Security, [https://www.cisecurity.org/].
___“The Darknet Index: Fortune 500 Reranking the Fortune 500 Using Darknet Intelligence” (2017), [https://owlcyberdefense.com/], ss. 1-22.
___ Timeline of Computer History,
[https://www.computerhistory.org/timeline/1989/].
___“Türkiye Siber Güvenlik Kümelenmesi”, [https://www.siberkume.org.tr/Index].
___“Türkiye’yi, Bilgi ve İletişim Teknolojilerinde Dünyanın en önde Gelen Ülkeleri Arasına Sokacağız” (2020). [https://www.tccb.gov.tr/].
___ What is Cybersecurity?
[https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html].
___“What we do?”, [https://www.ncsc.gov.uk/section/about-ncsc/what-we-do].
___“What is a Botnet?”,
[https://www.paloaltonetworks.com/cyberpedia/what-is-botnet].
___ “2022 Cyber Security Incentives and Regulation Review”
[https://www.gov.uk/government/publications/2022-cyber-security-incentives-ve-regulation-review/2022-cyber-security-incentives-ve-regulation-review].
___“2010 to 2015 Government Policy: Cyber Security”, [https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security].
AYTAR, Ahmet K. (2015). “ABD Ulusal Güvenlik Strateji Belgesi ve Türkiye”,

[http://www.turkishnews.com/tr/content/2015/02/16/abd-ulusal-guvenlik-strateji-belgesive-turkiye/].

BEAUCHERE, Jacqueline. (13.11.2020). "Microsoft Study: Online Risks that sow hate and Division are Growing", [https://blogs.microsoft.com/].

BOSTON GLOBE "Cyber War has Already Begun", (Publication Date. 13.03.2017), [https://www.bostonglobe.com/].

BTK, Bilgi Teknolojileri İletişim Kurumu (12 Haziran 2019). "Kişisel Veriler ve Kişisel Bilgi Güvenliği", [https://internet.btk.gov.tr/kisisel-veriler-ve-kisisel-bilgi-guvenligi].

BURLU, Kâmil (vd.). Certified Ethical Hacker, [http://www.CEHTurkiye.com]. Cyber Security Strategy Documents, [https://ccdcoe.org/cyber-security-strategydocuments.html].

CCSA (2021). "How COVID-19 is Changing the World: a Statistical Perspective Volume III", [https://data.unicef.org/].

CLAYTON, Mark (2011). "The New Cyber Arms Race", [https://www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race].

Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, *Orta Vadeli Program (2012-2014),* [https://www.sbb.gov.tr/]

CUTHBERTSON, Anthony (25.04.2018). *Independent*, [https://www.indepe ndent.co.uk/life-style/gadgets-and-tech/news/webstresser-internet-ddos-europol-nca-cybersecurity-a8321751.html].

DASKAL, Jennifer ve Debrae K. (2020). "Budapest Convention: What is it and how is it Being Updated?" [https://www.crossborderdataforum.org/].

DEWALT, Dave (2009). "McAfee Virtual Criminology Report 2009", Virtually Here: The Age of Cyber Warfare, [http://conflictsincyberspace.blogspot.com/2009/12/mcafees-virtual-criminology-report-2009.html].

Dokuzuncu Kalkınma Planı (2007- 2013). [https://www.sbb.gov.tr/kalkinma-planlari/].

ERİŞ, Mehmet. TR-BOME KM (Türkiye Bilgisayar Olayları Müdahale Ekibi-Koordinasyon Merkezi), [http://ulakbim.tubitak.gov.tr].

European Comission. "Let's put an end to Violence Against Women", [https://ec.europa.eu/].

European Commission (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, [http://ec.europa.eu/digitalagenda/en/cybersecurity].

European Commission (2016). "Joint Framework on Countering Hybrid Threats: a European Union Response", [https://eur-lex.europa.eu/].

European Commission (2017). "Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU", [https://eur-lex.europa.eu/].

FOWLER, Ashleigh ve Tom Everard. "What is Cyber Security Culture and Why does it Matter for your Organisation?", [https://www.paconsulting.com/insights/what-is-cyber-security-culture-and-why-does-it-matter-for-your-organisation/].

"Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy",[https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy].

ISPAUK (2020). "Celebrating 25 Years of United Kingdom Internet", [https://www.ispa.org.uk/wp-content/uploads/ISPA-25th-Anniversary-Report].

ISO/IEC 23001 (2020). Information Technology, "Part 10: Carriage of Timed Metadata Metrics of Media in ISO base Media File Format", [https://www.iso.org/].

KARABACAK, Bilge ve Sevgi Özkan (2009). "Critical Infrastructure Protection Status and Action items of Turkey", *International Conference on e-Government Sharing Experiences*, [https://fuse.franklin.edu/facstaff-pub/40/].

KARAİSMAİLOĞLU, Adil (2020). "Yerli ve milli imkânlarla geliştirdiğimiz KASIRGA, AVCI ve AZAD uygulamaları ile son 3 yılda Türkiye'yi hedef alan 325 bin siber saldırı engellendi", *T.C. Ulaştırma ve Altyapı Bakanlığı*, [https://www.uab.gov.tr/haberler/turkiye-nin-siber-guvenligi-emin-ellerde].

KASAP, Neslihan ve Stéphanie Beghe Sönmez, "Cybersecurity in Turkey", [https://www.lexology.com/library/].

KLIMBURG, Alexander (2012). *National Cybersecurity Framework Manual*, NATO, [https://ccdcoe.org/].

LEVINE, Allan (2018). "Shielding Fortune 500 Companies from Cyberattacks"
[https://internationalfinance.com/shielding-fortune-500-companies-from-cyberattacks/].

LIEN, M. Elisabeth (2015). *Becoming Salmon,* Oakland: University of California,
[http://www.uc.edu/book.php?isbn=9780520280571].

MCKEAY, Martin (13.04.2020). "The Building Wave of Internet Traffic", [https://www.akamai.com/].

McKinsey (2020). "How COVID-19 has pushed Companies over the Technology Tissing Point and Transformed Business Forever", [https://www.mckinsey. com/].

MORGAN, Steve. (18.07.2019) "Humans On The Internet Will Triple From 2015 To 2022 and Hit 6 Billion", [https://cybersecurityventures.com/].

MORGAN, Steve. (13.11.2020). "Cybercrime To Cost The World $10.5 Trillion Annually By 2025", [https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/].

MYCOCK, Verew ve Ben Wellings (2011). "The Anglosphere: Past, Present and Future", *Stanford University,* [https://www.thebritishacademy.ac.uk/].

NAKASANE, Paul M. ve Michael Sulmeyer (25.08.2020). "How to Compete in Cyberspace", *Foreign Affairs*, [https://www.foreignaffairs.com/].

NCA (National Crime Agency) (2017). *Annual Report and Accounts 2016–17*, London: OGL, [https://assets.publishing.service.gov.uk/].

NORTON (2012). *2012 Norton Cybercrime Report*, [https://www.relianceacsn. co.uk/the-2012-norton-cybercrime-report/].

PETERS, Sara (2016). "Malware At Root Of Bangladesh Bank Heist Lies To SWIFT Financial Platform", [https://www.darkreading.com/].

SCHWARTZ, Mathew J. (26.04.2018). "Police Seize Webstresser.org, Bust 6 Suspected Admins",[https://www.bankinfosecurity.com/police-seize-webstresserorg-bust-6-suspected-admins-a-10920].

SHI, Fleming (2020). "Threat Spotlight: Coronavirus-Related Phishing",[https:// blog.barracuda.com/2020/03/26/threatspotlight-coronavirus-related-phishing].

SHI, Fleming (2021). "Threat Spotlight: Vaccine-Related Phishing", [https:// martermsp.com/threat-spotlight-vaccine-related-phishing/].

SIMONPIETRI, Antoine (2004). "A Guide to Designing a National Strategy for the Development of Statistics", *Paris 21*, [http://siteresources.worldbank. org/].

SMITH, Zhanna Malekos ve Eugenia Lostri (2020). "The Hidden Costs of Cybercrime", ss. 1-38, [https://www.mcafee.com/].

SULLIVAN, Peter. "Computer Emergency Response Team (CERT)",[https:// whatis.techtarget.com/definition/CERT-Computer-Emergency-Readiness-Team].

Symantec (04.2009). "Global Internet Security Threat Report Trends for 2008", Sayı 14, [https://docs.broadcom.com/doc/istr-12-april-volume-17-en].

T.C. Ticaret Bakanlığı (10.03.2022). BREXIT ve Birleşik Krallık STA [https://ticaret.gov.tr/dis-iliskiler/brexit-ve-birlesik-krallik-sta].

The Fourth Industrial Revolution: What it Means, How to Respond, [www.weforum.org/].

TOURE, Hamadoun I. (ed.) (2014). "ITU the Quest for Cyber Confidence", [http://www.itu.int/].

UNGA (2003). "Creation of a Global Culture of Cybersecurity",
[https://digitallibrary.un.org/record/482184].

UNGA (2018). "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", [https://undocs.org/A/C.1/73/L.37].

UNIDIR (2001). "Disarmament as Humanitarian Action A Discussion on the Occasion of the 20th Anniversary of the United Nations Institute for Disarmament Research", Geneva: UNIDIR, [https://www.ungeneva.org/en/unidir].

UN. "Internet Governance Forum", *About the Internet Governance Forum*, [http://www.intgovforum.org/cms/aboutigf].

VERII, Paziuk ve Mitsik Vsevolod (2019). "Global Cybersecurity Culture in the International Discourse Values and Principles", [http://journals.uran. ua/visnyknakkkim/article/view/175488], ss. 103-107.

WAXMAN, Matthew C. (2011). "Cyber-Attacks and the Use of Force: Back to the Future of Article" 2(4), Sayı 36, [https://digitalcommons.law.yale.edu/], ss. 421-459.

WEF (World Economic Forum) (2020). "COVID-19 Risks Outlook: A Preliminary Massing and Its Implications", [www.weforum.org/reports/covid-19].

WHO, "WHO Coronavirus (COVID-19) Dashboard", [https://covid19.who.int/].

World Economic Forum, "Global Risk Report 2020- Executive Summary",
[http://reports.weforum.org/global-risks-report-2020/executive-summary/].

Gazeteler:

Cumhuriyet (2012). "ÖSYM'nin sitesi çökertildi",
[https://www.cumhuriyet.com.tr/haber/osymnin-sitesi-cokertildi-357600].

Cumhuriyet (2017). "PayPal'dan açıklama: 1,6 milyon kişinin bilgileri hacklendi!",

[https://www.cumhuriyet.com.tr/haber/paypaldan-aciklama-16-milyon-kisinin-bilgileri-hacklendi-880275].

HaberTürk (2017). "F-35 savaş uçağı verileri hacklendi!",
[https://uzmanpara.milliyet.com.tr/haber-detay/gundem2/f-35-savas-ucagi-verileri-hacklendi/74000/74783/].

Milliyet (2011). "Şok! MEB'in Sitesi Hacklendi", [https://www.milliyet.com.tr/teknoloji/sok-mebin-sitesi-hacklendi-1353574].

Milliyet (2012). "Aile Bakanlığı'nı RedHack hackledi",
[https://www.milliyet.com.tr/gundem/aile-bakanligi-ni-redhack-hackledi-1539999].

Milliyet (2013). "Emniyetin PolNet'i çöktü Türkiye'de hayat durdu", [https://www.milliyet.com.tr/gundem/emniyetin-polnet-i-coktu-turkiye-de-hayat-durdu-1759603].

Milliyet (2013). "76 Türk Devlet Sitesi Hacklendi",
[https://www.milliyet.com.tr/teknoloji/76-turk-devlet-sitesi-hacklendi-1665235].

Milliyet (2015). "Diyanet'i hacklediler", [https://www.milliyet.com.tr/gundem/diyanet-i-hacklediler-2029945];

Milliyet (2015). "Atatürk'ün hackerlarından Diyanet'e hack şoku",
[https://www.milliyet.com.tr/gundem/ataturkun-hackerlarindan-diyanete-hack-soku-2029752].

Milliyet (2018). "Apple 16 yaşındaki genç tarafından hack'lendi",
[https://www.milliyet.com.tr/teknoloji/apple-16-yasindaki-genc-tarafindan-hacklendi-2726648].

Milliyet (2018). "Mark Zuckerberg'in kendi Facebook hesabı bile hack'lendi",
[https://www.milliyet.com.tr/mark-zuckerberg%E2%80%99in-kendi-facebook-hesabi-bile-hack%E2%80%99lendi-molatik-9532/].

Milliyet (2020). "İsrail Savunma Bakanı'na hacker şoku! İstiklal Marşı paylaşıldı", [https://www.milliyet.com.tr/dunya/israil-savunma-bakanina-hacker-soku-istiklal-marsi-paylasildi-6160630].

Milliyet (2020). "27 bin kişinin verisi hacklendi", [https://www.milliyet.com.tr/ekonomi/27-bin-kisinin-verisi-hacklendi-6328491].

NTV, "İçişleri Bakanlığı hack'lendi",
[https://www.ntv.com.tr/turkiye/icisleri-bakanligi-hacklendi,3kdtZFzt00msI-4WP1eiu4A].

NTV (2012). "Redhack Dışişleri Bakanlığı'nı hack'ledi", [https://www.ntv.com.tr/turkiye/redhack-disisleri-bakanligini-hackledi,iECCMBunCE2i7A16_PkFVg].

Resmî Gazete, 26.09.2004 Tarihli Türk Ceza Kanunu, Sayı 25611, Tertip 5, Cilt 43,
[https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5].

Resmî Gazete, 17.12.2004 Tarihli Ceza Muhakemesi Kanunu, Sayı 25673,[https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5271&MevzuatTur=1&MevzuatTertip=5].

Resmî Gazete, Karar 2007/12300,
[https://resmigazete.gov.tr/eskiler/2007/06/20070621-2.htm].

Resmî Gazete, "5809 Sayılı Elektronik Haberleşme Kanunu",
[https://www.resmigazete.gov.tr/eskiler/2008/11/20081110M1-3.htm].

Resmî Gazete (24.03.2016). "6698 Sayılı Kişisel Verilerin Korunması Kanunu", Sayı 29677, Cilt 57.

Resmî Gazete, "04.05.2007 Tarihli İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkındaki 5651 No'lu Kanun",
[https://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm].

Resmî Gazete (23.05.2007). 5651 sayılı "İnternet Ortamında Yapılan Yayınların ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesinin Düzenlenmesi", Sayı. 26530.

Resmî Gazete (16.06.2008). 2008/13685 Türkiye Cumhuriyeti-Malezya Ekonomik ve Ticaret Ortak Komitesi İkinci Dönem Toplantısı Mutabakat Zaptının Onaylanması Hakkında Karar.

Resmî Gazete (10.11.2008). 5809 Elektronik Haberleşme Kanunu, Sayı. 27050.

Resmî Gazete, "Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği",
[https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=19880&mevzuatTur=KurumVeKurulusYonetmeligi&mevzuatTertip=5].

Resmî Gazete (2012). Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, [http://www.resmigazete.gov.tr/].

Resmî Gazete, 20 Haziran 2013 Tarihli ve 28683 Sayılı Karar, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın Kabulü",
[https://www.resmigazete.gov.tr/eskiler/2013/06/20130620.htm].

Resmî Gazete (6 Mart 2015). "2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı", Karar No 2015/4.

Resmî Gazete, 24.03.2016 Tarihli Kişisel Verilerin Korunması Kanunu, Sayı 29677, No 6698, Tertip 5, Cilt 57, Beşinci Bölüm, Madde 18b.

Resmî Gazete, 10 Temmuz 2018 Tarihli ve 30474 Sayılı Cumhurbaşkanlığı Kararnamesi,
[https://cbddo.gov.tr/mevzuat/1-nolu-cbk/].

TRT Haber (11.03.2023). "Türksat 6A 2023'te Uzayda Olacak".
[https://www.trthaber.com/haber/gundem/turksat-6a-2023te-uzayda-olacak-729744.html].

TRT World (30.12.2020). "Turkey Reveals its Three-year Cybersecurity Plan",
[https://www.trtworld.com/magazine/turkey-reveals-its-three-year-cybersecurity-plan-42820].