T.C.
BATMAN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER ANABİLİM DALI

AVRUPA KONSEYİ SİBER SUÇLAR SÖZLEŞMESİ TEMELİNDE TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKASININ DEĞERLENDİRİLMESİ.

YÜKSEK LİSANS TEZİ

ÖĞRENCİ
Elif Tuğçe ŞİŞMAN

Ocak, 2024
BATMAN

T.C.
BATMAN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER ANABİLİM DALI

AVRUPA KONSEYİ SİBER SUÇLAR SÖZLEŞMESİ TEMELİNDE TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKASININ DEĞERLENDİRİLMESİ.

YÜKSEK LİSANS TEZİ

ÖĞRENCİ
Elif Tuğçe ŞİŞMAN

DANIŞMAN
Doç. Dr. Eray ALIM

Ocak, 2024
BATMAN

TEZ KABUL VE ONAYI

Elif Tuğçe ŞİŞMAN tarafından hazırlanan "Avrupa Konseyi Siber Suçlar Sözleşmesi Temelinde Türkiye'nin Siber Güvenlik Politikasının Değerlendirilmesi" adlı tez çalışması 23/01/2024 tarihinde aşağıdaki jüri tarafından oy birliği ile Batman Üniversitesi Lisansüstü Eğitim Enstitüsü Siyaset Bilimi Ve Uluslararası İlişkiler Anabilim Dalı'nda YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Jüri Üyeleri **İmza**

Başkan

Doç. Dr. Murat CİHANGİR

Danışman

Doç. Dr. Eray ALIM

Üye

Doç. Dr. Ömer BAYKAL

Yukarıdaki sonucu onaylarım.

Dr. Öğr. Üyesi Ömer Murat ÖTER

Lisansüstü Eğitim Enstitüsü Müdürü

TEZ BİLDİRİMİ

Bu tezdeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edildiğini ve tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

DECLARATION PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Elif Tuğçe ŞİŞMAN

09.01.2024

ÖZET

YÜKSEK LİSANS TEZİ

AVRUPA KONSEYİ SİBER SUÇLAR SÖZLEŞMESİ TEMELİNDE TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKASININ DEĞERLENDİRİLMESİ.

Elif Tuğçe ŞİŞMAN

Batman Üniversitesi Lisansüstü Eğitim Enstitüsü
Siyaset Bilimi ve Uluslararası İlişkiler Anabilim Dalı

Danışman: Doç. Dr. Eray ALIM

2024, 64 Sayfa

Jüri
Danışmanın Unvanı Doç. Dr. Eray ALIM
Diğer Üyenin Unvanı Doç. Dr. Murat CİHANGİR
Diğer Üyenin Unvanı Doç. Dr. Ömer BAYKAL

Avrupa Konseyi Siber Suçlar Sözleşmesi Temelinde Türkiye'nin Siber Güvenlik Politikasının Değerlendirilmesi

Bilişim sistemleri vasıtasıyla işlenen suçların artışı, ülkelerin coğrafi sınırları içerisinde kalmayan, dünyayı tek bir yapı gibi görülmesini, uygulanacak yaptırımların da tek ve adil bir sistem içerisinde geliştirilmesini gerekli kılan bir süreci doğurmuştur. Avrupa Konseyi Siber Suçlar Sözleşmesi bu ihtiyaca binaen Türkiye'nin de aralarında bulunduğu üye ülkelerce imzalanmıştır.

Çalışmada üye ülkelerin siber suçlara karşı hazırladıkları hukuki çalışmalar ve söz konusu ülkelerin siber güvenliğe bakış açısı ile Türkiye'nin bu anlamda geldiği nokta karşılaştırmalı olarak incelenmiştir.

Bilişim sistemlerinin kullanılması suretiyle işlenen suçların yanında; sahtecilik, hakaret, dolandırıcılık, özel hayatın gizliliği ve kişisel verilere karşı suçlar, kullanıcı kimlik hırsızlığı, fikri mülkiyet hakkı ve haksız rekabete ilişkin internet ortamı üzerinden işlenen suçlar, banka ve kredi kartlarının kopyalanması ile hesap içeriklerinin elde edilmesi gibi suçların Türk Hukuk Sistemi içerisindeki yerine ve bu hususta eksikliklere değinilmiştir.

Sözleşme, taraf devletlere bilişim suçlarıyla mücadele etmek için gerekli hukuki temel çatıyı sağlamaktadır. Bu araştırmada, sınır aşan soruşturma ve kovuşturmalarda devletlerin birbirleriyle hızlı ve etkili bir şekilde koordinesi üzerine incelemeler yer almaktadır. Türkiye'nin günümüzde siber güvenlik politikasıyla ilgili çalışmalar üzerinde durulmuştur. Yukarıda bahsi geçen yaptırımlardan ziyade teknolojinin doğurduğu eşitsiz gücün ortaya çıkaracağı yeni tehditlerin devletlerin ve bireylerin egemenlik/özgürlük alanları üzerinde yarattığı etki ve çözüm önerilerine yer verilmiştir.

Anahtar Kelimeler: Avrupa Komisyonu, Siber güvenlik, Siber suç, Türkiye, Uluslararası İlişkiler

ABSTRACT

MS THESIS

AN ASSESSMENT OF TURKEY'S CYBER SECURİTY POLİCY BASED ON THE EUROPEAN UNİON CONVENTİON ON CYBERCRİME

Elif Tuğçe ŞİŞMAN

INSTİTUTE OF POLİTİCAL SCİENCES AND INTERNATİONAL RELATİONS OF BATMAN UNİVERSİTY
THE DEGREE OF MASTER OF İN POLİTİCAL SCİENCES AND INTERNATİONAL RELATİONS

Advisor: Assoc. Prof. Eray ALIM

(2024, 64 Pages)

Jury
Advisor's Title Assoc. Prof. Dr. Eray ALIM
Member's Title Assoc. Prof. Dr. Murat CİHANGİR
Member's Title Assoc. Prof. Dr. Ömer BAYKAL

An Assessment of Turkey's Cyber Security Policy Based on the European Union Convention on Cybercrime

The increase in crimes committed through information systems has led to a process that does not remain within the geographical borders of countries, which makes it necessary to see the world as a single structure and to develop the sanctions to be applied within a single and fair system. The Council of Europe Convention on Cybercrime was signed by member states, including Turkey, in response to this need.

In this study, the legal studies prepared by the member states against cybercrimes, the perspective of these countries on cyber security and the point Turkey has reached in this sense are examined comparatively.

In addition to the crimes committed through the use of information systems; the place of crimes such as forgery, defamation, fraud, crimes against privacy and personal data, user identity theft, crimes committed through the internet environment related to intellectual property rights and unfair competition, copying of debit and credit cards and obtaining account contents in the Turkish Legal System and the deficiencies in this regard were mentioned.

The Convention provides the States Parties with the necessary legal framework to combat cybercrime. This research examines the rapid and effective coordination of states with each other in cross-border investigations and prosecutions. Turkey's current cybersecurity policy has been emphasized. Rather than the aforementioned sanctions, the impact of the new threats posed by the unequal power created by technology on the sovereignty/freedoms of states and individuals and solution proposals are included.

Keywords: European Council, Cyber Crime, Cyber Security, International Relations, Turkey.

ÖNSÖZ

Yüksek lisans çalışmam boyunca bilgi ve tecrübesi ile desteğini esirgemeyen kıymetli hocam Doç. Dr. Eray ALIM'a, tarafıma göstermiş olduğu sabrı ve nezaketi için teşekkür ve saygılarımı sunarım.

Elif Tuğçe ŞİŞMAN
BATMAN- 2024

İÇİNDEKİLER

1. GİRİŞ

Türkiye Cumhuriyeti'nin kuruluşundan bu yana ülkenin uyguladığı resmi politikalarını en temel şekilde etkileyen ve yön veren olgulardan biri güvenlik konusudur. İçinde bulunulan coğrafi bölgenin içeriden ve dışarıdan gelecek tehditlere açık bölgede olması sebebiyle güvenliği her zaman ön planda tutmak elzem olmuştur. Ancak geleneksel güvenlik anlayışı, çok katmanlı ve çok yönlü bir takım yeni denklemlerin güvenlik tartışmasına dâhil olmasıyla birlikte yerini yeni güvenlik anlayışlarına bırakmıştır. Küresel dünya düzeninde kavramlardan hangilerinin iç güvenliği hangilerinin ise dış güvenliği etkilediği konusu oldukça belirsizleşmektedir.

Küreselleşme dönemi ile birlikte devletlerin egemenlik alanlarına dair geleneksel kaygılarının yerini yeni sorun alanları doldurmaya başlamıştır. İçinde bulunduğumuz yüzyılda teknoloji bilgisi ve kullanımının ülkelerin güvenlik anlayışlarındaki yeri oldukça önemlidir. Siber saldırılar gelişmiş devletlerin stratejik planlar yürütmesi ve savunma yöntemleri geliştirmesini zorunlu kılan bir tehdit biçimi olarak karşımıza çıkmaktadır. Öyle ki bu yarışta geride kalan ülkelerin geleneksel saldırı ve savaş yöntemleri ile ayakta kalabilmesi mümkün olmayacaktır. Uluslararası platformda üzerinde çalışılan plan ve projeler, hazırlanan yasalar, bağlayıcı bir takım sözleşmeler kapsamlı şekilde incelenmeli ve Türkiye'nin durduğu/durması gerektiği yer araştırılmalıdır.

1.1. Kaynak Araştırması

Uluslararası mevzuat ile ulusal mevzuatın birbirine eklemlendiği, birinin diğerinden bağımsız düşünülemez hale geldiği bu çağda öncelikle ulusal mevzuattaki eksiklikler hızla kapatılmalıdır. Hukuksal çalışmaların yanında teknolojik ilerleme hızı da büyük ölçüde ivme kaydetmelidir. Çalışmamızın temelini bu gereklilikler oluşturacak olup Türkiye'nin siber güvenlik hususunda, Avrupa Konseyi Siber Suçlar Sözleşmesi'nin içeriğine ve uluslararası siber güvenlik anlayışına ne derece uyumlu olduğu, varsa eksiklik ve aksaklıkların neler olduğu ve üzerine ne konulabileceği ile ilgili temel kaygılar değerlendirilecektir. Yapılan diğer çalışmalardan farkı Avrupa Konseyi Siber Suçlar Sözleşmesi'ne üye ülkelerle ve uluslararası siber güvenlik uygulamaları ile mukayeseli değerlendirme içerecek olmasıdır. Ayrıca bu alanda

yapılan çalışmaların sayısı az olduğundan yapılacak yeni çalışmalara açık bir alan olduğu değerlendirilmektedir.

2. SİBER GÜVENLİĞE DAİR TANIMLAR

Soğuk Savaş döneminde kapitalizm ile komünizm mücadelesinde komünizmin çökmesi ile birlikte kapitalizm hızlı bir yükseliş sürecine girmiştir. Bu itici güç ile modernleşme süreci sosyal, kültürel ve siyasal alanlara sirayet etmiştir. Kültürel modernleşme, akıl ve ilerleme ilkeleri üzerine konumlandırılmış ve küreselleşme öncesinde temel argüman olan ulusal devlet sınırlarının yerini uluslararası bir takım normlar almıştır (Heywood, 2015, s.38).

Geleneksel güvenlik anlayışının değişmesiyle beraber teknolojinin başat bir rol almaya başladığı görülmektedir. Güvenlik tehdidi kavramında yaşanan dönüşüm sonucunda 1980'li yılların devlet bekası uygulamaların yerini, artık günümüzde küresel teorilerin savunulduğu güvenlik teorileri almıştır (Aras, 2023, s.474). Küreselleşmenin yükselişe geçtiği yıllarda ise, devletler ve toplumlar kendilerini modern uluslararası sisteme entegre etme sürecine girmişlerdir. Bireylerin önemli birer etken olduğu ve uluslararası alanın önem kazandığı bu yeni yüzyılda siber alan da karşımıza söz konusu uluslararası unsurlardan biri olarak çıkmıştır.

Avrupa Konseyi Siber Suçlar Sözleşmesi'nin ortaya çıkışı Suç Sorunlarına ilişkin Avrupa Komitesi'nin (SSAK- European Committee on Crime Problems) Avrupa Konseyi'ne (AK) 1996 yılında siber suçlar uzman komitesi kurması tavsiyesi iledir (Council of Europe, 2001). Siber güvenliğin teknolojik bir takım ilerlemelere paralel olarak farklı kurum ve kuruluşlar tarafından benzer birçok tanımı olmuştur. Siber güvenlik terimi ilk olarak 1990'lı yıllarda bilgisayar mühendisleri tarafından ağ bilgisayarları ile ilgili güvenlik sorunlarını ifade ederken kullanılmıştır (Hansen ve Nissenbaum, s.1155). O tarihlerden bugüne dek teknik birikim ve yetenek gelişim gösterdiğinden siber alandaki riskler de artış göstermiştir. Bu paralelde, siber saldırganların kimliklerini ve konumlarını gizleyecek teknik olanaklarının da artıyor oluşu, devletlerin teknolojik gelişmeleri öncelemelerine hız kazandırmıştır.

Siber suç, siber saldırı ve benzeri tanımlamalara geçmeden bu tanımlamaların oluşmasına zemin hazırlayan teknoloji kavramını açıklamak yerinde olacaktır.

Teknoloji, Yunanca tekhne (ustalık gerektiren zanaat) ve logia (içindeki düşünceyi aktarmak) kelimelerinden türer ve teknik bir meselenin sistematikleştirilmesi, aktarılması anlamına gelir. Teknoloji toplumun beslenmesi, sağlığı ve konforu gibi amaçlar uğruna kolektif insan bilgisini kullanarak elde edinilen yöntemlerdir (Acemoğlu, Johnson, 2023, s.19).

Teknoloji, ayrılmaz unsuru olan insanla ilişkisi gereği, toplumda politik ve teknik değişkenlik gösteren her alana temas eder (Ünver, 2023, s.26). Günümüz dünyasında bilgi teknolojileri yaşantımızın hemen her alanında artık kilit bir rol oynamaktadır. Kişisel, toplumsal, finansal ve benzeri temas edilen tüm alanlarda bilgi güvenliğine ihtiyaç artmaktadır. Kişisel bilgilerin elektronik ortamda kullanımının önüne geçilemeyeceği bilgi çağında tüm bu bilgilerin güvenliği sadece fiziksel alanda değil, elektronik ortamda da sağlanmalıdır (Henkoğlu ve Yılmaz, 2013, s.454). Bilgi güvenliği bağlamında Avrupa Konseyi'ne taraf devletlere düşen, kişisel verilerin korunmasının öncelikle ulusal düzenlemeler, sonrasında konsey üyeliği kapsamında sağlanmasıdır. Ulusal ve uluslararası hukuk arasında doğacak olan uyumsuzluklar yapılacak olan hukuki ve teknik çalışmalar ile mümkün mertebe giderilmelidir.

Avrupa Konseyi'nin 95/46/EC sayı ve 1995 tarihli "Kişisel verilerin işlenmesi ve bu tür verilerin serbest dolaşımına dair bireylerin korunması hakkındaki direktife" göre; kişisel veriler üye ülkelerin sosyoekonomik ilişkileri gereği paylaşılabilir olmalıdır. Bu paylaşım üye ülkelerin ulusal mevzuatlarında bireysel hak ve özgürlüklere atfedilen değere göre gerekçelendirilmemelidir. Yani üye devletlerin ulusal kanunlarında bireysel hak ve özgürlükler noktasında görülen eksiklikler Konseyin ekonomik ve sosyal çıkarını olumsuz etkileyecek şekilde değerlendirilemez denilmektedir (Council of Eupore, 2001).

Bilişim, bilgisayar ve bilgisayar aracılığıyla sanal ortamda gerçekleştirilen faaliyetler ifadesini de kapsayacak şekilde gerçekleştirilen faaliyetlerdir (Tezcan, 2019, s.288). Bilgi teknolojilerinin güvenliği ile ilgili uluslararası düzeyde kabul gören en geniş sertifikasyon programı, Common Criteria (Ortak Kriterler) olarak bilinen Bilgi Teknolojileri Güvenliği Değerlendirmesi için Ortak Kriterleridir. Bu düzenleme ile amaçlanan, Ortak Kriterler sertifikası bulunan ülkelerin -ki Türkiye de bu ülkelerden biridir- teknoloji ürünlerinin ekstra bir değerlendirmeye ihtiyaç duyulmadan alınıp satılabileceği güvenilir bir rekabet ortamı yaratmaktır (Common Criteria, 2014).

Devletlerin tehdit algıları doğrultusunda ürettiği stratejiler ulusal güvenlik stratejilerini belirler. Dolayısıyla devletler stratejik amaçlarını belirlerken uluslararası düzendeki güç dağılımına uygun olarak hareket ederler. Bu sebeple uluslararası sistemin ne tür tehditleri ön plana çıkardığı üzerine odaklanmaktadırlar (Yalçın, 2017, s.11).

Küresel dünyada güvenlik tehditleri ve güvenliğe dair riskler askeri kaynaklı olmaktan ziyade siyasi ve diplomatik araçların da kullanılması ile aşılabilecektir Siber güvenlik stratejileri de benzer bir yol izlemektedir. Avrupa Birliği Devlet ve Hükümet Başkanları Konseyi'nce 2003 yılında Avrupa Güvenlik Stratejisi kabul edilmiştir. Söz konusu stratejide güvenlik ve refahın, yalnız Avrupa Birliği (AB) sınırları içerisinde değil, uluslararası düzenin çıkarına olacak şekilde biçimlendirilmesinin genel yararı artıracağı değerlendirilmiştir (Büyükbaş, 2006, s.55).

Siber güvenlik terimi çeşitli kurumlarca tanımlanmıştır. Uluslararası Telekomünikasyon Birliği siber güvenliği şöyle tanımlamıştır: "*Siber ortamda kurum, kuruluş ve kullanıcıların siber alandaki varlıklarını muhafaza etmek için kullanılan araçlar, belirlenen politikalar, risk yönetimi ve güvenlik yaklaşımları ile faaliyet ve uygulamaları kapsayan teknolojilerin tamamıdır"* (Ünver, Canbay ve Özkan, 2011, s.1). Ulusal Siber Güvenlik Eğitim Girişimi (NICE) ise siber güvenliği "*bilgi ve iletişim sistemleri ile bu sistemlerin içerisinde yer alan bilgilerin herhangi bir zarara, saldırıya ya da yok edilmeye karşı korunduğu, savunulduğu bir faaliyet ya da süreç"* olarak tanımlamıştır (Karasoy ve Babaoğlu, 2021, s.130).

Ülkemizde siber güvenliğin etkili şekilde sağlanabilmesi için kritik altyapıların belirlenerek öncelikle bu alanların korunması önemsenmiş ve bu itibarla 2013-2014 Eylem Planı'nda bu hususa değinilmiştir. Ülkemizde gerçekleşen üç temel eylem planı ayrı bir bölüm içerisinde incelenecektir. Avrupa Konseyi'nde ise 2004'te başlanan kritik altyapı çalışmalarına günün koşullarına uygun olacak şekilde 2008'de bilgi teknolojileri de eklemlenerek Avrupa Kritik Altyapısının Belirlenmesi ve Koruyucu Tedbirlerin Artırılması Direktifi oluşturulmuştur (Council Directive, 2008/114/EC. s. 75). Siber güvenliğin sağlanması siber saldırı ve tehditlerin etkili şekilde bertaraf edilmesine bağlıdır. Gelişen teknoloji ile siber tehdit türleri ve buna bağlı olarak alınacak tedbirler de artmaktadır. Siber tehditler 1990'larda virüs ifadesi ile hayatımıza girmiş, takip eden on yıllarda solucan ve daha sonrasında Botnets (robot ağ), APT (gelişmiş sürekli tehdit) gibi birçok tanım türemiştir (Taşkın. 2018, s.319).

Türkiye'de gerçekleştirilen ilk siber güvenlik stratejisi 2013 yılında hazırlanmıştır. Türkiye Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda siber ortam "*Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortam*" olarak ifade edilmektedir (T.C. Ulaştırma ve Altyapı Bakanlığı, 2013). Siber ortam kara, deniz, hava ve uzay olmak üzere dört alana etki edebilen yapısı nedeniyle oldukça önemli ve insan eliyle üretilmiş olması yönüyle farklı, beşinci kavram olarak karşımıza çıkar (Çelik. 2018: s. 115). Siber saldırı yapılacak ülkenin sınırlarına dahi girmeden o ülkenin ulaşım, iletişim ve her türden hizmete erişim gibi son derece önemli hizmetlerinin kullanılmasını engellemek son derece güçlü bir silah olarak değerlendirmelidir. Zira NATO, Varşova Zirvesinde müttefiklerine siber savunmanın Nato önderliğindeki operasyonlarında yan rolden başat role getirmenin gerekliliğini vurgulamıştır (Robinson, 2016).

Yukarıda bahsi geçen 2013-2014 Eylem Planında siber güvenlik ;

> *Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi,*

şeklinde ifade bulmuştur (RG, 2013a).

Bilişim sistemleri kullanılarak işlenen suçlarla ilgili olarak geneli kapsayan uluslararası yasal bir düzenleme bulunmamaktadır. Siber terörizmin kapsamı, sınırları net olarak belirlenemeyen yönüyle terörizmin diğer türlerinden ayrılmaktadır. Bu belirsizliğin sonunda çok sayıda şiddet boyutuna erişen eylem gerçekleştirilmiştir. Siber saldırıya uğrayan ülkenin su ve elektronik kaynakları, finansal alanı, savunma sanayi sistemleri gibi sistemleri işlemez duruma getirerek zarara uğradığı örnekler mevcuttur (Doğan ve Abacı, 2021, s.5974).

Siber güvenlik terimi ile bağlantılı çok sayıda teknik terim bulunmakla birlikte çalışmamızın odağı olan Avrupa Konseyi Siber Suçlar Sözleşmesi'nin dört temel tanımı üzerinden devam edelim.

Bilgisayar sistemi bir veya daha fazla yazılım odağında otomatik verileri işleyebilen cihaz veya birbiri ile bağlantısı bulunan cihazlar sistemini ifade eder. Bir

diğer tanım olan **Bilgisayar verisi** ise tanımlanan bilgisayar sisteminin belirli bir amacı/işlevi yerine getirmesini sağlayan bilgi, konsept ve uygun nitelikteki yazılımlar olarak belirtilmiştir. Üçüncü tanım **hizmet sağlayıcı** ise bilgisayar vasıtasıyla iletişim imkanı sağlayan kamu ve özel tüzel kişileri ya da hizmet sağlayan kişi ve kuruluşları ifade eder. Son terim olarak **trafik bilgisi**, bilgisayar sistemlerini kullanmak vasıtasıyla gerçekleşen bir iletişimle ilgili, o iletişim ağının bir parçası olan bilgisayar sistemince üretilen iletişimin izlediği yol, saati, tarihi, boyutunu ve hizmet tipini gösteren bilgisayar verisidir (Council of Europe, 2001).

3. SİBER SALDIRI VE SAVUNMA YÖNTEMLERİ

21. yüzyılda hayatın vazgeçilmez bir unsuru olan bilgisayar, bir çok sektöre hizmet sağlayan ve günden güne genişleyen bir alana yayılmaktadır. Profesyonel veya bireysel olarak sınırsız bir alanda kullanıma açılan bilişim sistemlerinde oluşacak olası güvenlik açığı durumunda, özgürlük sağlayan bu alanın bir suç mekanizması haline gelmesi öngörülemeyen zararları beraberinde getirecektir. İnsanın yaratıcı gücünün teknoloji ile harmanlanması sonucu teknoloji hızlı bir ivme ile hayatlarımızı dönüştürmekte ve bu değişimin derinleşerek etkisini artıracağı bir döneme girilmektedir (Kurzweil, 2020, 19). Bu dönüşüm kaygısından hareketle devletler siber güvenlikle ilgili birbirini takip eden ve birbiri ile temas halinde çalışmalar yürütmektedirler. Devletlerin kritik altyapılarına yönelik gerçekleştirilecek bir siber saldırının zararının boyutları öngörülebilirdir.

Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ ile kritik altyapılar "İşlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim veya endüstriyel kontrol sistemlerini barındıran altyapılar" şeklinde tanımlanmıştır (RG, 2013b). Kritik altyapılar denildiğinde genel olarak ülkenin iletişim, ulaşım, altyapı hizmetleri (doğalgaz, su, elektrik sistemleri) anlaşılabilir.

Bilgi teknolojilerinde yaşanacak güvenlik zafiyetleri, yürütülen hizmetlerde aksamalardan kötüye kullanmaya ve hatta çok daha büyük çaplı ekonomik ve güvenliğe dönük zararlara sebep olabilecektir.

Türkiye'de Siber Olaylara Müdahale Ekipleri (SOME) kurulmuş olup bu ekiplerin siber tehditleri bertaraf etme görevi bulunmaktadır. Türkiye'de siber alanda yapılan kurumsal çalışmalar ayrı bir başlık altında açıklanacaktır.

3.1. Siber Saldırı Yöntemleri

Siber saldırı, yasal ve yasadışı kuruluşların, yetkili hükümet organlarının, şirketlerin, şahısların ve hatta terörist grupların operasyonel hedeflerini gerçekleştirmek amacıyla siber ortamdaki faaliyetleridir. Siber saldırı; meşru ya da değil bir amaca hizmet eden, aktif ya da pasif bir saldırı ile gerçekleşen, büyük ya da küçük etki gözeten, yasal veya yasadışı olabilen saldırı şeklidir (Çifci, 2023, s.107). En sade tabiriyle siber saldırı, zararlı yazılımlar kullanma vasıtasıyla gerçekleştirilen saldırılar olarak tanımlanabilir.

Siber saldırı türleri her geçen gün farklı bir yere ulaştığından teknik anlamda günümüzde geldiği son noktanın takibi zor olmakla birlikte belli başlı siber saldırı türlerini bilmek faydalı olacaktır. Siber güvenlikle bağlantılı terimlerin sayısı oldukça uzun bir listeyi içerdiğinden çalışmanın kapsamı gereği terimsel karşılığı bulunan tüm saldırı türlerine değinilemeyecektir.

3.1.1. Tuzak kapı (Trapdoor)

Yazılım ya da işletim sisteminin kendisinde bulunan bir açık üzerinden kimlik doğrulama sisteminin bertaraf edilmesi yoluyla sağlanan yetkisiz erişimdir (Keleştemur, Koldemir ve Yapıcı, 2018, s.13). En sık kullanılan tuzak kapı yöntemi erişilmesi hedeflenen sistemde dinleme ajanı eklenmiş bir portu açık bırakmak şeklindedir (Arslan, 2017, s.6).

3.1.2. Oltalama (Phishing)

Kişisel ve finans bilgilere erişmek amacıyla yapılan sosyal mühendislik tarzı saldırı türüdür. Bilinen örnekleri;

-Şirket marka ve logolarının kullanımıyla yapılan oltalama (Branded spear),

-Finans kuruluşları ve e-ticaret sitelerinin hizmet sağlayıcılarının taklit edilmesiyle yapılan oltalama (Elektronik posta),

-Siber saldırının gerçek kişi gibi davranıp iletişime geçmek yoluyla gerçekleştirildiği, ülkemizde de sıkça karşılaşılan oltalama (Gone),
-Hedef şahsa ait bilgilerin her bir hedef için kullanılması ile yapılan oltalama (Spear),
-Telefon kullanarak yapılan oltalama türü (Vishing),
-Kısa mesaj yoluyla yapılan oltalama türü (Smishing),

-Sahte bir web sitesine yönlendirme şeklinde yapılan oltalama (pharming) gibi türleri bulunmaktadır (Polat ve Karakaş, 2023, s. 127). Bu yöntem finansal internet sitelerinde olduğu kadar online alışveriş yapılan tüm sitelerde uygulanmakta olup kişilerin şifre güvenliklerine dikkat etmeleri gerekmektedir. Bu tip siber saldırılar genellikle vatandaşı hedef alan dolandırıcılık tipi saldırıları kapsar.

3.1.3. Spam

Günlük bilgisayar kullanımımızda sıkça karşımıza çıkan istenmeyen e-postalardır. Kişisel bilgilere erişim amaçlı olarak tasarlanır. Şahsi bilgilere erişim mümkün olacağı gibi kurumsal şifre ve bilgiler de bu saldırı yöntemiyle ele geçirilebilir. Spamlar genel olarak kullanıcılara arama motorlarının yan profilleri üzerinden saldırı gerçekleştirir. Web sitelerini alt üst etmeye yönelik bir dizi teknik şeklinde ifade edilebilir.

3.1.4. Yerine geçme (Masquerading)

Veri iletme yolu ile gerçek sunucunun yerine geçerek gerçekleştirilen saldırı türüdür. E-posta iletisi kullanıcıyı banka internet adresi yerine, banka internet sitesinin kopyası olan başka bir web sayfası hazırlayarak bu alana yönlendirir, kullanıcının şifre bilgilerini kendi sunucusuna kaydeder. İsrail Filistin savaşında Filistin yanlısı hacktivist grup AnonGhost tarafından roket uyarılarını almak için Android uygulaması görünümüne bürünen casus yazılımlar kullanıldığı iddia ediliyor (Arghire, 2023).

3.1.5. Dos (Deniel of service)

Amaç, hizmetlerin geçici ya da süresiz olarak devre dışı bırakılarak asıl kullanıcıların erişimini engellemektir. Sistemin kullanılamaz hale gelmesine ya da kapanmasına neden olur (Polat ve Karakaş, 2023, s.50). Gerçekleştirilecek olası bir Dos

saldırı sırasında örneğin ülke gündeminde bir genel seçimin olması durumunda siber saldırı sadece finansal kayıplara değil, bunun yanında saldırıya maruz kalan ülkenin demokrasisine de yapılmış bir saldırı olacaktır. Yahut dışarıdan satın alınan bir kritik alyapıya örneğin doğalgaz sistemlerine yapılacak bir saldırı ise doğalgazı üreten ve kullanan ülkeleri etkileyerek daha büyük zararlara neden olabilecektir.

3.1.6. Ddos (Dağınık hizmetdışı bırakma)

Çok sık kullanılan ve üzerine oldukça çalışma bulunan saldırı türlerinden biri olup dağınık hizmet dışı bırakma olarak tanımlanan saldırı türüdür. Serverin kaldırabileceği yükün üzerine çıkan anlık iletilerle sistem yorulur ve saldırıya yanıt veremez hale getirilir (Aslanbakan, 2023, s.91). Dünyanın çeşitli yerlerinden aynı anda yapılan paylaşımlarla protesto eylemi gerçekleştirmek üzere kurulmuştur. Bir hacker grubu olan Anonymous topluluğu Ddos saldırı türünü sıklıkla kullanır. Yapmış oldukları bu eylem hareketine Chanology Projesi demişlerdir. Bir dönem tarikatların internet sitelerine siber saldırı düzenleyen Anonymous "Biz Anonim'iz, Biz Lejyonuz. Bağışlamayız. Unutmayız. Bizi bekleyin." mottosu ile hareket etmeye başlamıştır (Yegen, 2014, s.65). Uluslararası arenada önemli görülen siber saldırılardan birisi Estonya'ya karşı yapılan DDoS saldırısıdır. Rusyaya ait bir siber operasyon olduğu ve siyasi amaçlarla gerçekleştirildiği genel kanısı bulunan bu saldırı ile devlet başkanlığının internet siteleri ile birçok kamu kuruluşu etkilenmiştir (Güldoğan ve Işıklı, 2022, s.293).

Türkiye'yi hedef alan ddos saldırısına bir örnek de Rusya tarafından Türkiye uzantılarının erişimini aksatacak şekilde ve büyük ölçekli olarak gerçekleştirilen ve Türkiye'de Rus uçağının düşürülmesinden sonraki sürece tekabül eden ddos saldırısıdır (Darıcılı ve Özdal, 2017, s.25).

3.1.7. Fidye yazılımı (Ransomware)

Dosyaların ya da bütün bilgisayarın şifrelenmesi ve deşifre etmek için ücret istenmesidir. 2017 siber suçlar raporuna göre fidye yazılımlarının çoğu Kobilere (küçük ve orta ölçekli işletmelere) yöneliktir (Akyeşilmen. 2018, s.79). Fidye yazılımı ile yapılan saldırılara örnek olarak *WannaCry* verilebilir. Gerçekleştirdiği fidye yazılım ile

birçok devleti, şirketleri hatta bireyleri siber tehdit ile karşı karşıya bıraktığı bilinmektedir (Çelik ve Çeliktaş, 2018, s.108).

Fidye yazılımları iki türlü gerçekleştirilmektedir. İlki şifreleyici fidye yazılımıdır. Hedef kişilerin bilgisayardaki önemli dosyaları şifre ile açılacak duruma getirildikten sona şifreye erişim için fidye istenir. Bir diğeri kilitleyici fidye yazılımıdır. Burada da belirli dosyalar değil tüm sistem kilitlenir ve karşılığında yine fidye istenir (Kara, 2019a, s.118).

3.1.8. Casus yazılımları (Spyware)

Kullanıcılara e mail ile Truva Atı olarak ya da bir programa gizlenerek gelebilen, kişisel verileri ulusal ya da uluslararası örgütlerle paylaşma amacı güden saldırı yöntemidir (Akyeşilmen, 2018, s.79). Devletlerin istihbarat örgütlerine satılan yazılımlardan olduğu iddiası mevcuttur. Örneğin dijital casusluk yazılımı olan ve İsrail üretimi olan Pegasus adlı zararlı yazılım dünya gündemine 50'den fazla ülkede tespit edilmesiyle oturmuştur. Bu ülkelerde üst düzey siyasetçi, gazeteci, hukukçu, aktivist kimseleri izlediği iddiaları mevcuttur. Her ne kadar yalanlanmış olsa da Suudi Arabistan hükümeti tarafından Cemal Kaşıkçı'nın cinayetten önceki süreçte izlendiği iddia edilmiştir (Çahmutoğlu, 2021).

3.1.9. Hat çekme (Wire tapping)

Telefon hattına sızarak yasadışı dinleme yapmak olarak tanımlanır. İlk olarak New York polisinin kriminal araştırmalar için kullandığı bu yöntem kötü niyetli kişilerce kişisel bilgilere erişmek maksadıyla siber saldırı türü olarak kullanıldığı bilinmektedir. İstihbarat birimlerinde *kabloya saplama yapmak* şeklinde de tanımlanır. Sıradan iletişim ağlarına çeşitli araç gereç ile fiziksel olarak saplama yaparak bağlantı kurulmasını ifade eder. Bu yolla iletişim trafiği dinlenir. Sadece telefon trafiği değil, bilgisayar sistemleri arasındaki trafik de dinlenebilir (Keleştemur, 2018, s.101). Hukuki bir dinleme yöntemi olmadığından polis teşkilatlarınca delil mahiyetinde kullanılamaz ancak hedeflenen suçlu ya da suç örgütlerine ulaşmada yol katedilmesini sağlamak maksadıyla yapıldığı değerlendirilmektedir. Wire tapping dosyalarının incelemesiyle ilgili çalımalar bulunmaktadır.

3.1.10. Sosyal mühendislik

İnsanların kaygı ve korku gibi zayıflıkları üzerinden hareketle onları manipule edip bilgi ve kayıtlarına erişmeyi hedefleyen siber saldırı yöntemidir. Bireylere farkındalığı artıracak eğitimler verilerek bu faaliyetin önüne geçilebilir (Sağıroğlu ve Akleylek, 2022, s.157). Söz konusu siber saldırı yöntemi ile aldatıcı ilişkiler meydana getirme yolu kullanılır. Sosyal mühendislik saldırılarından korunmak için kullandığımız bilgisayarların güvenlik duvarlarının güvenilir ve etkin olması gerekmektedir. Ancak kişileri aldatma yöntemleri o kadar çeşitlidir ki bazen antivirüs programları yetersiz kalmaktadır. Sosyal mühendislikte kullanılan yöntemlere dair bazı kavramlar vardır:

"*Klavye ile kişisel bilgi giren birisini gözle seyretmek (Omuz Sörfü),

*Saldırganı kurbanın yardım amacıyla aradığı saldırı yöntemi (Ters Toplum Mühendisliği),

*İşe yarar bir bilgi bulmak amacıyla hedef kişinin çöpünü karıştırma (Çöp Dalışı),

*Kişisel bilgilerin bir başkasınca yetkisiz kullanımı (Kimlik Hırsızlığı) ,

*Oltalama olarak öncesinde açıklanan siber saldırı yöntemi de sohbet sitelerinde hedef kişiden bilgi alma yoluyla bir sosyal mühendislik yöntemi olarak değerlendirilebilir.

*Bunların yanında e-postaya gönderilen link yerine telefon numarası verilmesi ve bu numara arandığında bilgi çalınması (Telefon Oltalaması),

*Bir kurum çalışanı gibi görünerek sistemdeki yetkilere zaten sahipmiş gibi davranması (Kimliğe Bürünme),

*Sosyal mühendis tarafından yollanan e posta yoluyla Truva Atı ya da solucan gibi zararlı yazılım gönderme (Online Dolandırıcılık),

*Teknik destek ekibi gibi davranarak verilen talimatları bilgisayarda gerçekleştirmesinin sağlama (Yardım Masası) gibi aldatma unsurlarından oluşur." (Gündüz ve Daş, 2016, s.3).

3.1.11. Ip sahteciliği

Diğer adıyla IP routing, farklı ağların birbirleri ile iletişime geçmek için hangi yolu kullanacaklarının hesaplanmasıdır (Polat ve Karakaş. 2023: s.86). Yönlendirme solucanı da diyebileceğimiz bu saldırı türünün tespit edilmesi zor ve yayılma hızı yüksektir. Bu siber saldırı yönteminde saldırgan gerçek IP adresini gizler ve sahte bir IP adresine sahip görünecek şekilde hareket eder (Güner, 2018, s.2).

3.1.12. Zararlı yazılımlar

Yukarıda açıklanan siber saldırı yöntemleri de birer zararlı yazılım içermekle birlikte doğrudan zararlı yazılım olarak kurgulanan ve diğer dosyalara bulaşma ortak parantezinde değerlendirilebilecek unsurlar zararlı yazılımlar alt başlığı altında açıklanacaktır.

3.1.12.1. Bakteri

Çalıştığı bilgisayarda kendiliğinden çoğalarak çok fazla yer işgal eden ve bu yolla işletimi meşgul eden zararlı yazılım türüdür (Körpe, 2021, s.134). Virüs ve solucan kadar gelişmiş bir saldırı türü olmadığı bilinmektedir.

3.1.12.2. Virüs

Genellikle virüs koruma ve casus yazılım engelleme programı görüntüsü altında bilgisayarlarımıza bulaşan sahte antivirüs yazılımlardır. Harici bellekler, dosya indirme siteleri, spamlar, iletişim ve chat uygulamaları aracılığıyla da virüs bulaşabilmektedir (Çakır ve Kesler, 2012, s.471). 2015 yılında en çok etkilenen ülke İran olmak üzere birçok ülkede devlet kurumları Stuxnet isimli bir virüsten etkilenmişti. Devletlerin bilişim sistemlerine büyük ölçüde zararlar veren bu virüs özellikle nükleer enerji sistemleri etkilemiştir. Virüsün ABD İsrail ortaklığında ve İran nükleer faaliyetlerine zarar vermek üzere oluşturulduğu yönünde iddialar vardır. Bu siber saldırı sonucu İran milyonlarca dolar zarara uğramıştır (Zetter, 2014).

3.1.12.3. Solucan

İnternet ağında kendisini yayabilen ve kendi başına program olarak değerlendirilmesi yönüyle virüslerden ayrılır. Virüs bir dosyaya bulaştığında o virüslü dosya açılmadığı sürece diğer dosyalara bulaşamaz. Solucan ise veri transferi yapan fonksiyonların denetimini ele geçirip önce sisteme bulaşır, daha sonra hızla yayılım gösterir. 15 milyon bilgisayara bulaştığı tahmin edilen Conficker adlı solucan zayıf şifreli kullanıcı hesapları üzerinden taşınabilir bellekler vasıtasıyla 15 milyon bilgisayara bulaştığı tahmin edilmektedir (Arslan, 2017, s.8).

3.1.12.4. Truva atı (Trojan)

İçerisine gizli şekilde yerleştiği bilgisayar sistemine zarar verme amaçlı olan, yararlı bir program gibi görünerek bulunduğu programı kontrol altında tutan zararlı bir yazılımdır (Körpe, 2021, s.134). Uzaktan Erişim Truva Atı (UETA) olarak bilinen saldırı şekli kullanıcı izni olmaksızın kontrolü ele geçirmeye ve kullanıcıya ait bilgilere ulaşmaya imkân sağlayan bir saldırı türüdür. UETA saldırılara karşı şu önlemler alınabilir:

Şüpheli görülen bir trafik varsa portlar üzerinden incelenmeli, uygulama programları arayüzü (API) çağrısı varsa yine şüpheli görülmeli, sıkıştırılmış arşiv dosyalarında (rar uzantısı ve benzeri.) zararlı yazılım içerebileceği göz önüne alınmalı, Domain İsim Servisi (DNS) istekleri şüpheli işlem olabileceğinden dikkat edilmelidir (Kara, 2019b, s. 30).

3.1.12.5. Mantık bombası (Logic bomb)

Amacını gerçekleştirene kadar hareketsiz halde duran, meşru bir yazılımın içerisinde gizlenen ve kurulum aşamasında test edilme ile meydana çıkarılamayan zararlı yazılım türüdür (Dusane ve Pavithra, 2020, s. 3662).

ABD'deki bir güvenlik firması 2013 yılında Güney Kore'de bankalara ve yayın şirketlerine ait bilişim cihazlarında bilgi silinmesi olayının bir mantık bombası ile gerçekleştirildiğini iddia etti. Mantık bombası, zararlı yazılımın birden çok kurban arasındaki yıkımı koordine ederek bilgisayarlardan veri silmeye başlanacak tarihi ve saati belirliyordu (Zetter, 2013).

3.1.12.6. Rootkit

Kötü amaçlı yazılımlara yardımcı olmak amacıyla virüsler veya solucanlarla paketlenen ve virüslerde olduğu gibi sahte antivirüs ve reklam yazılımlarının içerisine gizlenen yazılımlar olarak bilinir. Elde edilen verilere göre LoJax olarak adlandırılan rootkit, Doğu Avrupa'da yüksek profilli hedeflere yönelerek başka yazılımların erişemediği yerlerde kalıcı olarak ulaşmak amacıyla hareket etmektedir (Bıktım, 2018).

3.1.12.7. Köle bilgisayarlar (Botnet)

Zombi bilgisayarlar da denilen bu yazılım türü ile hedeflenen bilgisayar, sisteme daha öncesinden yüklenen bir program aracılığıyla kolayca uzaktan kontrol edilerek zarar verilmektedir (Körpe, 2021, s.134). Genel olarak siber suçlar kapsamında yapılan operasyonlara bakıldığında siber saldırganların eğitim seviyesinin düşük ve yaşlarının küçük olduğu görülmektedir. Devletler, uluslararası siber suç örgütlerinin genç ve üretken kişileri kullanmasının önüne geçmelidir.

İstanbul Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğü ekiplerince yapılan bir operasyonda Bot-Netler (Birden fazla bilgisayarın virüslerle ele geçirilerek uzaktan yönetilmesine olanak sağlayan ağ) sayesinde köle bilgisayarlar oluşturdukları ve oluşturulan bu ağları pazarladıkları ortaya çıktı. Yapılan bu operasyonda gözaltına alınanların büyük çoğunluğunun ortaokul/lise eğitim seviyesinin üzerinde olmadığı ortaya çıktı (Özgür Kocaeli, 2013).

3.2. Siber Saldırı Örnek Olayları

Siber saldırı, herhangi bir mesafeyi engel olarak görmeyen, yarattığı zarar çok kısa sürede yayılan tehlikeli ve yeni bir savaş aracı olarak tanımlanabilir. Siber saldırıların devletler düzeyine çıkması durumunda siber savaş teriminden söz edilebilir ki günümüzde savaşların başlangıç noktasının siber ortamlar olduğu görülmektedir. Teknolojik gücü yüksek yahut bilişim sektöründe insan unsurunu doğru eğitmiş devletlerin gerçekleştirdiği siber saldırıların siber savaşlara sebep olduğu örnekler üzerinde durulacaktır.

Dünya pazarına hâkim olma ya da sadece devlet güvenliğini koruma gibi farklı gayelerle devletlerarasında meydana gelen siber gerilimleri dünya kamuoyunda izlemekteyiz. Siber güvenlik üzerine kurulan bölgesel ve uluslararası örgütlenmelere, Avrupa Konseyi Siber Suçlar Sözleşmesi'nin bu perspektifteki yerini görebilmek açısından kısaca değinilecek olup, öncelikle bu tip örgütlenmelerin kuruluşlarına gerekçe olabilecek bilinen bazı siber saldırıları inceleyelim.

Filistin İsrail örneği siber saldırıların asimetrik boyutunu da gözler önüne sermesi yönüyle önemlidir. Siber saldırı ile ülkelerin gelişmişlik seviyesi, refah düzeyi, savunma sanayiine ayırdıkları pay gibi oldukça yüksek maliyet içeren etkenler büyük oranda devredışı kalabilmektedir. Profesyonel Filistin Siber Ekipleri (Organized Palestinian Cyber Teams) Filistin silahlı kuvvetlere ait ve Hamas'ın çalışmalarını tamamlayıcı siber silahlara sahip bir ekiptir. İsrail'in siber gücü karşısında her ne kadar zayıf kalsa ve İsrail için büyük bir tehdit oluşturmuyor olsa da Filistin siber alandaki yeteneklerini geliştirmeyi hedeflemektedir.

Bir diğer siber ekip ise Filistin İslami Cihad hareketine bağlı siber ekiplerdir. Kudüs Tugayları çatısı altındadır. İsrail'in siber saldırı ve casusluk faaliyetlerine karşı oluşturulmuştur. Bu kurumsal siber ekiplerin haricinde gönüllü filistin siber ekipleri ve Gaza hack timi de dâhil olmak üzere profesyonel olmayan ve oluşum aşamasında olan bir siber örgütlenmenin olduğu görülmektedir (Saada ve Turan, 2021, s.191).

İsrail ise dijital diplomasi alanında dünyanın en gelişmiş ülkelerinden biri olarak kabul ediliyor. 2016 yılı Dijital Diplomasi raporunda küresel olarak sekizinci sırada yer alırken, İsviçre, Almanya, Japonya, Kanada, Avusturya, İspanya ve İsveç gibi gelişmiş ülkeleri geride bırakmıştır (Saada ve Turan, 2021, s.192). Diğer taraftan İsrail, yapay zekâ uygulamaları kullanarak canlı olarak tespit edilen her şeyin imha edildiği, teknolojinin insanlık suçunda bir araç olarak çok rahat kullanıldığı bir süreci göstermiştir. Geleceğin güvenlik stratejileri yapay zekâ, insansız araçlar ve robotik sistemler düzeyinde güvenlik kapasitesini artırırken etik ve mahremiyet problemlerini de beraberinde getireceği öngörülmektedir (Gemici ve Ercan, 2023, s.31). Teknoloji ile gelen tüm iyileştirmelerin yanı sıra siber alanın uluslararası hukuk kurallarını çiğneme kabiliyeti de oldukça yüksektir. Siber güvenliği diğer güvenlik sektörlerinden ayıran şey sürekli güncellenerek yeni tehditler yaratıyor olmasıdır ki bu siber güvenliğe daha net bir perspektiften bakmamız gerektiğinin de işaretidir.

İsrail Filistin Savaşında, kendilerini hacktivist olarak tanımlayan bilgisayar korsanları siyasi olarak destekledikleri taraf için siber saldırılarda bulunmaktadır. Jerusalem Post ve benzeri haber sitelerine defalarca saldırılar gerçekleştirilmiştir (Euronews, 2023). Klasik savaş tekniklerinde saldırganın bulunup yok edilebileceği yahut bombardıman altına alınarak bertaraf edilebileceği beceriler, söz konusu siber saldırı olduğunda aynı kolaylıkla gerçekleştirilemeyecektir.

İzzeddin el-Kassam Tugayları tarafından gerçekleştirilen ve Aksa Tufanı operasyonu ile başlayan İsrail- Filistin savaşı öncesinde Filistinli siber ekipler İsraillilere yönelik önemli bilgiler elde etmişlerdir. Filistinli siber ekiplerin Aksa Tufanı planlaması sırasında İsrail'in zayıflıklarını ve sırlarını içeren bir veri tabanına sahip oldukları bilinmektedir. Siber saldırının Kassam Tugayları'nın siber birliği olan ve İsrailli yetkililerce gölge askerler olarak bilinen ekip tarafından yapıldığı değerlendiriliyor (Independent, 2023).

İsrail ise İran akaryakıt sistemine siber saldırı gerçekleştirdiğini duyurdu. Tahran'da akaryakıt istasyonlarının büyük kısmında hizmetler aksadı. İsrail ordu radyosundan yapılan yayında *"Bu siber saldırı İslam Cumhuriyeti'nin ve uzantılarının bölgedeki saldırganlığına bir yanıttır. Hamaney, ateşle oynamanın bir bedeli vardır"* ifadeleri kullanıldı (Ntv, 2023).

ABD Merkezi İstihbarat Teşkilatının istatistiklerine göre İran siber güçte dünya sıralamasında 5. en güçlü ülke konumundadır. İran siber kuvvetlerinde 2400 kişi çalışıyor ve 12 bin kişilik yedek kuvvetleri bulunmaktadır (Asl, 2017, s.340). İran nükleer faaliyetleri uluslararası siber güvenlik arenasında çok sayıda ülkeyi tedirgin etmektedir. Bu itibarla daha önce bahsedildiği gibi Stuxnet adlı bir siber saldırıya uğramıştır.

Yeni bir örnek olarak, 1999 Kosova Savaşı sırasında Nato güçleri Çin Büyükelçiliğini (Belgrad) yanlışlıkla jetler ile vurunca Çin Kızıl Korsanlar Birliği çok kısa bir süre içerisinde karşı atak olarak ABD'nin kurumsal internet sitelerine siber saldırılar düzenlemiştir. 2001 yılında ise Amerikan casus uçağı ile Çin jetinin çarpışması sonucunda Çin'li hackerlar Beyaz Saray'ın internet sitesine saldırı düzenlemişlerdir (Altun, 2017, s.30). Bu olaya literatürde Hainan Adası olayı da denilmektedir. Amerika, Çin siber saldırılarına karşı kritik altyapılarını korumak gerektiği bilincindedir. Çin'in Amerikaya karşı siber faaliyetlerinin diğer adı Titan Rain

olarak bilinmektedir. Amerika savunma sistemlerine ait askeri ağdan yaklaşık 20 terabayt boyutunda veri çalınmıştır. Titan Rain siber saldırıları Amerikanın kurumsal savunma sitelerinin yanında finansal ortaklarına karşı da yürütülmektedir (Çifci, 2023, s.134).

ABD'nin siber stratejilerini geliştirmek adına hazırladığı strateji metinleri bulunmaktadır. Bunlardan 2015 yılında yayınlanan Siber Strateji Belgesi daha önceki isimlendirmeler olan "siber uzay güvenliği" ya da "siber güvenlik" tanımlamalarına göre daha genel bir stratejik nitelik taşımaktadır. Yeni siber stratejiye dönük somut adımlara yer verilen bu belge üç temel amaç üzerine kurulmuştur. Abd çıkarlarına zarar veren siber saldırıları engellemek, dönemin başkanı Obama'nın Birleşmiş Milletler (BM) ülkeleriyle hareket edecek savunma planı direktifi oluşturmak ve Siber Görev Güçleri (Cyber Mission Force) oluşturarak operasyonel hareket etmek (Göçoğlu ve Aydın, 2019, s.240).

ABD Temsilciler Meclisi Başkanının 2022 yılında Tayvan ziyaret planı, Çin-Tayvan gerilimi nedeniyle Çin Hükümetinin rahatsız etmiş ve bu konuyla ilgili ABD Başkanı Joe Biden ile Çin Devlet Başkanı Şi Cinping görüşme yapmıştır. Yapılan bu görüşmede Çin Devlet Başkanı Şi Cinping'in ABD Başkanı Joe Biden'a "Ateşle oynayan, kendini yakar" dediği belirtildi (Anonymous, 2022). Çin Halk Cumhuriyeti 2050 yılını hedefleyerek aldığı stratejik kararda elektronik liderliği ele geçireceğini, bu amaca mavi ordu adını verdiği siber birimini oluşturarak ulaşacağını duyurmuştur (Akkaş ve Ravanoğlu, 2022, s.56).

Devletlerin yaşadığı siber saldırılardan öğrenerek siber güvenlik çalışmalarını daha kapsamlı hale getirmeleri ve proaktif hareket etmeleri son derece önemlidir. Bu hususta önemli bir örnek olarak Colonial Pipeline olayını inceleyelim. Uluslararası yankı uyandıran bu siber saldırı ABD'yi bazı eyaletlerinde Ohal (Olağanüstü hal) ilanına götüren kısa ve etkili bir süreci kapsamaktadır. Darkside olarak bilinen bir hacker grubu yaptığı siber saldırı ile Amerika'nın en büyük yakıt tedarik zinciri olan Colonial Pipeline'ı kesintiye uğratmıştır. Kesintiyi sonlandırmak için fidye isteyen hacker grubunun bu saldırısının Fidye yazılımı (Ransomware) olduğu söylenebilir. Yakıt kıtlığına sebep olan ve yaklaşık beş gün süren bu durum tüketicilerde panik yaratmıştır. Bu saldırı siber güvenlik politikaları çatısı altında oldukça önemlidir. Çünkü bu saldırının ardından ABD siber güvenlikle ilgili bir dizi yasa, kararname ve direktif yayımlamıştır (Wood, 2023).

Çin Halk Cumhuriyeti ise çevrimiçi sansür sistemi çok yüksek olan, güvenlik duvarlarını etkin şekilde uygulayan ülkelerin başında gelir. Çin'in siber alanda uyguladığı bu yüksek güvenlik seddine Great Wirewall of China denmektedir. Çin'de internet kullanıcıları ülkenin büyük güvenlik duvarını aşmak için hemen her erişim için VPN (*Virtual Private Network*) kullanırlar (Economist, 2018). Çin ayrıca 2035 yılını hedef alan şehirleşme, teknoloji, ekonomi gibi alanlarda bir dizi master plan yapmaktadır. Ekonominin dijitalleştiği alanlarda yapay zekâ, akıllı şehir uygulamaları, küresel düzeyde veri standardı oluşturma hedeflerinin yanında teknoloji ihracatında da uluslararası standartları belirlemek gibi iddialı hedefler, Batı tarafından bakıldığında teknolojik soğuk savaş anlamı taşımaktadır (Küçüksolak, 2023, s.295).

2022 yılının Şubat ayında Ukrayna-Rusya Savaşının başlamasının akabinde Ukrayna'yı destekleyen gönüllü hacker grupları Ukrayna Başbakanı Mykhailo Fedorov'un çağrısı ile Telegram uygulaması üzerinden birleşmişlerdir. Federov Bilişim Teknolojileri Ordusu kurulmasını planladığını ve gönüllülere eğitim desteği vereceğini duyurmuştur. Bu durum, dünya savaş tarihinde hackerlardan destek istenen ilk örnek olması yönüyle önemlidir (Paltacı, 2022, s.7). Yine Rusya ile ilgili olarak, Estonya ve Gürcistan saldırısı Rus Savunma Bakanlığı'na bağlı elektronik harp birlikleri tarafından gerçekleştirildiği değerlendirilmektedir. Rusya, iç ve dış güvenlikteki kurumsal yapılanma, ayrıca siber eğitimlere verdiği önem bağlamında önde gelen ülkelerden olduğunu söylemek yanlış olmayacaktır.

IŞİD (Irak Şam İslam Devleti) terör örgütü ise farklı bir örnekle karşımıza çıkmaktadır. Söz konusu örgüt, misyonunu gerçekleştirmek için diğer terör örgütlerinden farklı bir yöntem deneyerek interneti doğrudan kullandı. Benzer nihai hedeflere sahip diğer gruplardan farklılaştıran, yeni üyelerden faydalanmalarının ve misyonlarını daha önce hiçbir militan grubun yapamadığı şekilde ilerletmelerinin bir yolunu bulan terör örgütü internet üzerinden üye sağlamıştır. IŞİD, internet operasyonlarını kontrol eden medya yayılım ekibi, siber iletişim ekibi, işe alım görevlileri ve bilgisayar korsanları gibi işbirliği içerisinde çalışan timler kurmuştur. Bilgisayar korsanlarını mühendis veya geliştirici olarak konumlandırmıştır (Baumberger, 2019, s.6).

3.3. Siber Savunma Sistemleri

Devletlerin görevleri arasında siber saldırılara karşı daha güçlü ve güvenli bir sistem geliştirmeleri, özellikle kritik altyapıları korumak üzerine kurulu çalışmalar yapmaları da bulunmaktadır. Geleneksel devlet anlayışında devletin görevleri daha kısıtlı bir alanda iken günümüz toplumlarında daha çok güvenlik açığı oluşmaktadır. Zira siber güvenlik artık bir faaliyetten ziyade bir milli güvenlik meselesi olarak değerlendirilmelidir (Çifci, 2023, s.187).

Gelişmekte olan ülkelerde siber güvenlik, siber müdahale biçimleri ve siber savunmaya dönük yapılanma henüz beklenilen seviyeye erişememiştir. Bir disiplin olarak değerlendirirsek henüz gelişim aşamasında olan bu yeni alan için büyük devletler teknik ve operasyonel anlamda ciddi fonlar ayırmaktadırlar. Önceki başlıklarda açıklandığı üzere siber alandaki çalışmalarını bakanlık yapılanması altında gerçekleştiren ülkeler mevcuttur. Bilişim sektöründe istihdam edilen personel sayısı da belirleyici etkenlerden birisi olacaktır.

Örneğin ABD, olası siber saldırılara karşı bir savunma yöntemi olarak Savunma Üçlüsü (The Defensive Triad) adını verdiği bir savunma sistemi geliştirmiştir. Clinton, Bush ve Obama başkanlık süreçlerinde de var olan ve siber saldırılara karşı devletler bazında bir strateji planı olan Savunma Üçlüsünün temel aldığı üç sektör vardır. Kazayağının ilk aşamasını internet omurgası (çok sayıda şirketin sahip olduğu ağların tamamı) oluşturur (Clarke ve Knake, 2010, s.160). Eyaletlerdeki ağları birbirine bağlayan ve bir nevi emniyet sibobu görevi gören bu sistem, olası siber saldırının bir anda her yere bulaşabilir olmasının önüne geçmek üzere tasarlanmıştır.

Savunma üçlüsünün diğer iki ayağını ise güvenli bir elektrik sistemi ve gizli bilgi içeren ve sadece Savunma Bakanlığı'nın kullanımında olan kısıtlı bilgisayar ağıdır (Clarke ve Knake, 2010, s.167).

Türkiye'de ise 2012 yılında Türk Silahı Kuvvetleri (TSK) bünyesinde kamusal alan ile koordineli faaliyet gösteren TSK Siber Savunma Merkezi Başkanlığı kurulmuş ve 2013'te TSK Siber Savunma Komutanlığına dönüştürülmüştür. Komutanlık NATO Siber Olaylara Müdahale Merkezi ile koordineli hareket etmektedir (Uslu, 2016).

İnternet ortamında karşılaşılacak tehditlerin artması paralelinde alınacak tedbirler de artmaktadır. Gerçekleştirilen ve gerçekleştirilmesi planlanan siber

saldırılara yönelik alınacak bir dizi savunma yöntemi bulunmaktadır. Bunlardan bazıları; Güvenlik Duvarı, Saldırı Tespit ve Önleme Sistemi, Hava Boşluğu, Kimlik Doğrulama, Zafiyet Taraması, Ağ Erişim Kontrol Sistemidir. Şifreleme sistemi, sayısal imza, uç nokta güvenlik sistemi, kripto sistemler gibi daha bir çok savunma sistemi de bulunmaktadır.

3.3.1. Güvenlik duvarı

İnternet ağına bağlanmak buradan gelecek siber tehditlere karşı hazırlıklı olmayı beraberinde getirir. Bu korumasız alanda bilgisayarlarımıza virüs yayılabilir yahut casus bir yazılım bilgisayarımıza yüklenmiş olabilir. Kişisel verilerimizin güvenliği için antivirüs programları yüklemenin yanında güvenlik duvarı yazılımı da bulunmalıdır. Bu sayede internete erişim yapmak isteyen zararlı yazılımlar tespit edilerek önenebilmektedir. Ayrıca güvenlik duvarları siber saldırılara ve sisteme bulaşmak isteyen tehlikeli yazılımlara karşı koruyucu rol üstlenecektir (Zeydan, 2006, s.4).

3.3.2. Kimlik doğrulama

Her geçen gün gelişmekte olan bilişim teknolojileri kişisel verilerin paylaşımını zorunlu hale getirmekte ve kişisel bilgilere erişimi daha mümkün kılmaktadır. Kişisel erişimi daha kolay kıldığından bazı tehlikeleri de beraberinde getirmektedir. Kişisel bilgilerin çalınması riskinin öngörülmesi ve uygun tedbirlerin alınması gerekmektedir.

2007 yılında Resmi Gazete yayınlanan tebliğ metninde *"Müşterilere uygulanan kimlik doğrulama mekanizması birbirinden bağımsız en az iki bileşenden oluşur. Bu iki bileşen; müşterinin "bildiği", müşterinin "sahip olduğu" veya müşterinin "biyometrik bir karakteristiği olan" unsur sınıflarından farklı ikisine ait olmak üzere seçilir."* ifadesi ile iki faktörlü doğrulama uygulamaya dâhil edilmiştir (Çivi ve Çekiç, 2015, s.49).

3.3.3. Zafiyet taraması

Güvenli bir bilişim alanı oluşturmak için, ağ ve sistemlerin rutin olarak test edilmesi, bulunan zafiyetlerin belirlenerek giderilmesi bir gerekliliktir. Güvenlik politikalarında güvenlik tehdit kaynaklarınca kullanılabilecek zafiyetleri bulup

gidermek, güvenlik zaafiyeti taraması ve test edilmesi ile mümkün olur (Saygılı ve Koyuncu, 2010, s.1).

3.3.4. Saldırı tespit ve önleme sistemi (IDS)

Bilişim sistemlerinin güvenliğine karşı tehdit içeren olay ve ihlallerden koruyan sisteme Saldırı Tespit Önleme ya da İzinsiz Giriş Tespit Sistemi (instrusion detection system - IDS) denilmektedir. IDS geliştirmek için uyarlanabilirlik, esneklik, hızlılık nedenleriyle yapay zekâ tabanlı teknikler uygundur ve diğer tekniklerin önüne geçmektedir (Karasoy ve Gezici, 2023, s.181). Yapay zeka teknolojileri ve devamı olan akıllı sistemler önümüzdeki yıllarda meslek ve piyasaları da dönüştürerek devrim yaratacaktır. Bu devrim, sahip olunacak bilgi miktarının büyük oranda artmasıyla teknolojik alanda gerçekleşecek olup, toplumsal yansımalarının ne derece olumlu olacağı bir başka tartışma konusudur (Acemoğlu, 2023, s.7).

3.3.5. Ağ erişim kontrol sistemi

Kablosuz ağ teknolojileri, son dönemdeki teknolojik ilerlemelerle birlikte kablolu erişimlerin yerini alarak erişim hareket alanını genişletmiştir. Veri girişinin yapıldığı alanlarda kontrol noktası oluşturulması gereklidir.

Güvenlik zincirinin en zayıf halkasının insan olması nedeniyle kullanıcı faktörünün olumsuz etkilerini en aza indirgemek elzemdir. Bu sebeple kullanılan antivirüs ve güvenlik duvarı yazılımları haricinde ağ erişimi sağlanan cihazlara güvenlik kontrolü yapan cihazlar da yerleştirilmektedir (Bulut, Aydın ve Zaim, 2023, s.217).

4. SİBER GÜVENLİĞİN TÜRKİYE MEVZUATINDAKİ YERİ VE ULUSLARARASI HUKUKTAKİ REFERANSLARI

Küreselleşme, bilginin toplum yapısını değiştirmesi ile başlayan ve bilişim dünyasında meydana gelen değişmelerin tetiklediği bir süreç olarak karşımıza çıkmaktadır. Küreselleşme çağında bilim, öngörülü bir ilerleme hattında ve kümülatif bir büyüme eğilimi ile ilerlemekte ancak Avrupa perspektifinden bakıldığında bunun büyümeden ziyade bir dönüşüm ve farklılaşma süreci olduğu görülmektedir. Bu durum ise farklı bilgilerin aynı zamanda olanaklı olabileceği gerçeğini doğurmuştur (Foucoult,

2018, s.77). Bilgi toplumu olma yolunda ilerleyen Türkiye gibi ülkeler için yeni düzene ayak uydurabilmek uluslararası hukuka olan inanca bağlı olarak mümkün olacaktır.

Sosyal, ekonomik ve benzeri alanlarda bir gereklilik olarak karşımıza çıkan hukukun üstünlüğü, uluslararası meselelerde de esaslı bir yer teşkil etmektedir. Hukukun temeli insanlık tarihi ile paralel olarak çok eskilere dayanmakla birlikte, hukukun üstünlüğü kavramsal olarak Friedrich A. Hayek tarafından 100 yıl kadar önce özgürlüklerin korunması temel argümanı üzerine formüle edilmiştir (Gözlügöl, 2013, s.1425).

Hukukun üstünlüğü kavramını içinde yaşadığımız yüzyılda uluslararası ilişkiler bağlamından uzak düşünemeyiz. Uluslararası hukuku farklı referans noktaları üzerinden tanımlayacak olursak; örneğin, Foucoult'nun Fons Elders'le söyleşisinde bahsettiği üzere Chomsky, uluslararası hukuku tanımlarken onun çok zayıf bir araç olduğunu dile getirir. Bununla ilgili olarak, devletlerin ve onların temsilcilerinin yaratımı olan, mevcut güç yapılarını halkların örgütlenmelerine karşı korumak üzerine kurulu bir düzen ifadesini kullanır (Foucoult, 2018, s. 90).

Bilişim suçları, teknolojinin gelişme hızıyla paralel olarak çeşitlenerek artmaktadır. Kendini güncelleyerek değişen, kapsamı genişleyen bu suç türleri ile mücadele etmek için sağlam temellere dayanan hukuki bir altyapının bulunması şarttır. Sadece kişisel kullanımda değil, kamu kurumlarında da internet araçlarının yürütülen işin ayrılmaz bir parçası olarak kullanılması bir takım suistimalleri de beraberinde getirmektedir (Turan ve Külcü, 2014, s.19). Teknolojik ilerlemenin hız kazandığı, toplumları hızlı bir gelişim sürecinin içine alan bu çağda sosyal uzlaşıyı, güvenliği ve adaleti sağlamak önceki yüzyıllardaki gibi zamana yaygın ve ağır gelişim ve dönüşümlerle mukayese edilemeyecek denli yüksek ivme kazanmış durumdadır. Öyle ki, toplum içerisinde elektronik sistemleri kullanan hemen her bireye mağduriyet yaşatabilecek olan siber suç unsurları ile mücadele, yapısı gereği sadece içerisinde bulunulan ülkeyi değil, uluslararası işbirliğini de gerekli kılmaktadır.

Çalışmamızın bu bölümünde bilişim hukukunun gelişimi sürecindeki yasal düzenlemeler ulusal ve uluslararası olmak üzere iki bölümde anlatılmak yerine, daha anlamlı olacağı inancı ile birbirini tetikleyen ulusal ve uluslararası mevzuat hikâyesi ve gelişim süreci çerçevesinde açıklanmaya çalışılarak Türkiye'de uluslararası mevzuata karşılık hangi reaksiyonların alındığı üzerinde durulacaktır.

Bilişim suçları Avrupa Konseyi Siber Suçlar Sözleşmesi'ne üye ülkeler arasında adli bir koordinasyon ve yeknesaklık gerektirdiğinden ülkeler arası adli dayanışmaya ihtiyaç duyulmaktadır (Turan, 2023, s.704). Bu ihtiyaca binaen uluslararası hukuku korumak ve geliştirmenin bahse konu sözleşmeye üye ülkelerin görevlerinden olduğu görülmektedir. Türkiye'nin de dâhil olduğu Avrupa Konseyi Siber Suçlar Sözleşmesi gereğince uluslararası hukukun uygulanmasında bilhassa teknolojiyi içerisine alan hususlarda sürekli olarak mevzuat güncelleme gerekliliği bulunmaktadır. Teknolojinin gelişme hızı ve bilişim suçlarının ileri yönlü evrilme eğilimi suçluların bulunarak cezai infazlarının gerçekleştirilmesinde ülkeler arası işbirliği gerektirmekte, bu bağlamda kanunlar yeni düzenlemeler yolu ile açılarak detaylandırılmaktadır. 5237 sayılı Türk Ceza Kanunu (TCK) ilk olarak 765 kanun sayısı ile 1926'da düzenlenmiştir. Toplumun değişen yapısı ve gereklerine uygun olarak bir dizi değişiklik ve ek ile 2005'te bugünkü halini alarak uygulanmasına devam edilmiştir (RG, 1926).

4.1. 5273 sayılı Türk Ceza Kanununda Bilişim Suçları

1991 yılında yürürlüğe giren 3756 sayılı Kanun, 765 sayılı Kanunun revize edilmiş hali olup, bilişim suçlarına günün koşullarına uygun ve ayrıntılı şekilde yer vermiştir (Mahmutoğlu, 2013, s.891). Bilişim Alanında Suçlar başlığı bu düzenleme ile yeni bir başlık altında düzenlenmiştir. 525. Maddesinde bilgisayar sistemlerinde bulunan bir veriyi başkasına zarar vermek üzere kullanan, nakleden, çoğaltan, tahrip eden, değiştiren, silen, sistemin işlemesine engel olan veya yanlış biçimde işlemesini sağlayan kişilere hapis ve para ceza verilmesini öngörmüştür (RG, 1991).

Türk hukuk sisteminde bilişim suçlarıyla ilgili düzenlemeler incelendiğinde 5237 sayılı Türk Ceza Kanununu temel metin olarak değerlendirmek yanlış olmayacaktır. Genel olarak internet üzerinden işlenen suçlar temelinde ilgili kanunun dokuzuncu bölümü incelendiğinde, dolaylı olarak bilişim sistemleri kullanılmak suretiyle Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar başlığı altında Haberleşmenin Gizliliğinin İhlali, Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması, Kişisel Verilen Kaydedilmesi, Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme gibi alt başlıklar altında hükme bağlanmıştır. İlgili kanunun onuncu bölümünde ise doğrudan bilişim kullanma vasıtasıyla işlenen suçlar "Bilişim Alanındaki Suçlar" başlığı altında aşağıdaki şekilde açıklanmıştır.

"Bilişim sistemine girme

MADDE 243. - (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

Sistemi engelleme, bozma, verileri yok etme veya değiştirme

MADDE 244. - (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.

Banka veya kredi kartlarının kötüye kullanılması

MADDE 245. - (1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis cezası ve adlî para cezası ile cezalandırılır.

(2) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan yedi yıla kadar hapis cezası ile cezalandırılır."(TCK, 2004).

TCK Madde 243'te ifade edildiği üzere "hukuka aykırı olarak bilişim sistemine giren" denilmekle bilişim suçunun gerçekleşmesinden önce bu alanda hukuksuz olarak bulunmak dahi müeyyidelendirilmiştir. Kanunda bilişim ağı kullanılmak suretiyle işlenebilecek diğer suçlar 125, 132 ila 138, 142/2-e, 158/1-f, 226, 228, 286 gibi maddelerinde belirtilmektedir. Örneğin madde 135'te ifade edilen Kişisel Verilerin Korunmasına İlişkin Suçlar, Siber Suç Sözleşmesi içerisinde yer almamakta fakat kişisel verilerin korunmasına ilişkin Avrupa Konseyi Sözleşmesinde bulunmaktadır. Birebir Siber Suç Sözleşmesi içerisinde başlıklandırılmamış, fakat siber güvenlikle ilintili konulara çalışmamız boyunca yer verilecektir.

Şerefe Karşı Suçlar başlığı ile 125. maddede geçen hakaret suçunun, 132-138. Maddelerde söz edilen Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar başlığı altında (Haberleşmenin Gizliliğini İhlali, Verileri Yok Etme gibi), Mal Varlığına Karşı Suçlar başlığında 142.maddesinin 2-e bendinde yazılı Hırsızlık suçunun, 158.maddenin 1-f bendinde geçen dolandırıcılık suçunun, Genel Ahlaka Karşı İşlenen Suçlar başlığında 226. Maddede Müstehcenlik ve benzeri suçların, 228. maddede kumar oynanması için yer ve imkân sağlama suçunun ve 286. Maddede soruşturma ve kovuşturma sürecinde izinsiz ses ve görüntü kaydı alınması suçlarının bilişim sistemlerinin kullanılması yoluyla işlenmesi halinde işlenen suç nitelikli olarak nitelendirilerek, suça karşılık gelen cezai müeyyidelerin de kanunda artırıldığı görülmektedir.

Bilişim alanında işlenen suçlar başlığı altında bulunmayan fakat bilişim alanı kullanılmak suretiyle işlenen bu gibi suçlar için ceza sürelerinin artırıldığı görülmektedir (Çakmakkaya ve Akpınar, 2018, s.124). TCK'nın 157. Maddesi Dolandırıcılık suçunun tanımı ve ceza süresini (1-5 yıl) örgörmekte iken Nitelikli Dolandırıcılık başlığı altındaki 158. Maddesinin 1. Fıkrası f bendinde dolandırıcılık suçunun *"Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle,"* işlenmesi halinde ceza süresi suçun nitelikli hale gelmesi sebebiyle 3-10 yıl olarak belirlenmiştir. Görüldüğü gibi bilişim alanındaki suçlar başlığı altında en yüksek ceza süresi 7 yıl iken ilgilinin bilişim suçu kullanmak suretiyle dolandırıcılık suçu işlemesi durumunda ceza üst sınırı 10 yıla kadar çıkabilmektedir. Dolandırıcılık suçunda bizzat kişileri hedef alan hileli davranış, baskı ve aldatma söz konusudur.

Bilişim suçlarında ise hileli davranışın muhatabı doğrudan kişiler değil, bilişim sisteminin kendisidir.

Avrupa Komisyonu bilişim suçları tasnifini "elektronik ağlar vasıtasıyla işlenen klasik suçlar", "elektronik medya üzerinde yayınlanan yasa dışı içeriğe ilişkin suçlar" ve "elektronik ağlara has suçlar" şeklinde düzenlemiştir (Hekim ve Başıbüyük, 2013, s.137).

4.2. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

2007 tarih ve 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile internet ortamında işlenen suçlarla mücadele amaçlanmaktadır.
İnternet ortamında işlenen suçlarla ilgili hukuksal çerçevede tarama yapıldığında en kapsamlı metin olarak görebileceğimiz bu Kanun doğrudan internet ortamında işlenen bir takım suçları kapsamaktadır. Söz konusu kanunun 2. maddesinde Bilgi Teknolojileri ve İletişim Kurumu (BTK) yetkili ve sorumlu kılınmıştır. 8. maddesinde belirtildiği üzere içerik kaldırma ve erişim engelleme kararları Türk Ceza Kanununda yer alan intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu kullanım ve sağlık için tehlikeli madde temin edilmesi, müstehcenlik, fuhuş, kumar için yer temini suçlarıyla ilgili olarak uygulanır. Kanunun uygulama alanı bulduğu birkaç başlık daha bulunmakla birlikte araştırma konumuzdan uzak olması sebebiyle değinilmeyecektir.

Bahse konu Kanunun 10. maddesinde Bilgi Teknolojileri ve İletişim Kurumuna *bilişim şuurunu geliştirmeye yönelik çalışmalar yapmak* görevi verilmiştir. Aynı maddenin bir diğer bendinde ise *"Bilişim ve internet alanındaki uluslararası kurum ve kuruluşlarla işbirliği ve koordinasyonu sağlamak*." ve bu görevi yerine getirirken 8. maddede belirtilen ve aşağıda yazılı olan suçların görüntülü, sesli ya da yazılı internet ortamında işlenmesi halinde yetkili kimselere yardımda bulunarak koordinasyon içerisinde hareket etmek görevi yüklenmiştir:

> *"*Yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması*

**Cumhurbaşkanlığı veya millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması".* (RG, 2007).

Bu kanunda geçen erişim engellenmesi kararının gereği, bildirilmesinden itibaren 4 saat, kararın Sulh Ceza Hâkimine sunulması için 24 saat, kararın açıklanması için ise 48 saat içerisinde yapılmalıdır denilmektedir. Siber alanda suçluya erişmenin zorlukları göz önüne alındığında yaptırıma bağlamak üzere sürelerin kısa tutulması ilk incelemede anlamlı görülmektedir. Diğer yandan, tek kararda birden fazla site hakkında erişim engelleme kararının verilmesi ve mahkeme onaylama süresinin kısa tutulmasının hukuki olmadığı görüşü yaygındır. Ayrıca engellenen adreslerin hangi gerekçelere dayanılarak engellendiğinin kararda belirtilmemesi, gerekçeli karar hakkının ihlal edildiğine dair eleştirileri de beraberinde getirmektedir (Özkaya, 2022, s.122). Kanun, içerik sağlayıcısını internette sağlayıcının kendisi tarafından üretilmiş her şeyden sorumlu tutmaktadır. Dolaylı olarak, bağlantısını sağladığı ve diğer kullanıcıların kullanımına sunduğu içeriklerden ise içeriğe ulaşılması "amaçlanması" durumunda sorumlu tutulmaktadır ki burada içerik sağlayıcının amacının ne olduğu, hangi hükümlere tabi tutulacağı veya bu amacın nasıl tespit edileceğine dair mevcut kanun maddelerinde açık bulunduğu görülmektedir. TCK'nın 20.maddesinde ifade edilen *Cezai sorumlulukta şahsilik* ilkesine aykırı görülen içerik sağlayıcısına yüklenen her türlü içerikten sorumlu tutulması, içerik sağlayıcı bu veriyi bizzat üretmemiş ise yasal dayanaktan yoksun duruma düşmektedir. Türk hukuk sisteminde pek kabul görmeyen objektif sorumluluk tanımlaması ile ifade edilebilecek bu durum 5237 sayılı TCK'da sözü geçen maddeye aykırı görülmektedir (Özel, 2007).

Kanun, erişim sağlayıcı olarak adlandırdığı gerçek veya tüzel kişileri de bu hususta sorumlu tutmaktadır. Kullanıcının hukuka aykırı olarak içerik paylaşımında bulunduğunu bilmesi halinde erişimi engellemekle yükümlüdür. Erişimin engellenmesi ve bilhassa içeriğin kaldırılması kararları uygulamada demokratik yaklaşımı negatif yönde etkilediği görüşlerinin bulunması sebebiyle bir takım sorunlara yol açmaktadır. Bu hususta BTK'nın 2011 tarihli ve 14/461 sayılı Kurul Kararı ile *Güvenli İnternet Hizmetine İlişkin Usul ve Esaslar* isimli düzenlemesinde çocuk profili ve aile profili uygulamaları yer almıştır. Bu uygulamanın BTK tarafından internet sansürüne bir kılıf olarak hazırlandığı ve internet erişimini yasal olduğu halde sınırlandırma amacı güdüldüğü değerlendirmesi ile 15 Mayıs 2011'de Türkiye'de yaklaşık 30 ilde "İnternetime dokunma" eylemleri gerçekleştirilmiştir (Sert, 2012, s.134).

4.3. 6698 sayılı Kişisel Verilerin Korunması Kanunu

Kişisel verilerin korunması ile ilgili yasal düzenlemeler Avrupa'da 1970'li yıllarda hazırlanmaya başlanmıştır. Kişisel verilerin ulusal düzeyde korunmasına yönelik hazırlanan ilk yasal düzenleme 1973 yılında İsveç Veri Yasasıdır. Takiben 1977'de Federal Almanya, Veri Koruma Yasasını kabul edilmiştir (Küzeci, 2010, s.97). 1970'lerde önem kazanmaya başlayan veri güvenliği konusu Türkiye'de çeşitli yasal düzenlemelere konu olmuş ise de Kişisel Verilerin Korunması Kanunu 2016 yılında yürürlüğe girmiştir. Öncesinde 2010 yılında Türkiye Cumhuriyeti Anayasasında yapılan anayasa değişikliği ile Özel Hayatın Gizliliği ve Korunması Hakkı başlıklı 20. Maddesine kişisel verilerin korunması hususu;

> *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar."* şeklinde eklenmiştir (RG, 2016).

2016 tarihli 6698 sayılı Kişisel Verilerin Korunması Kanununda kişisel veri, *gerçek kişiye ilişkin her türlü bilgi* olarak tanımlanmıştır. Kişisel veriler korunması birtakım ilkelere dayandırılmıştır. Bunlar hukuka ve dürüstlük kurallarına uygunluk, doğruluk ve güncellik, açıklık ve meşru amaçlara uygunluk, işlendiği amaca bağlantılılık ve ölçülülük, gereken süre ile sınırlılık ilkeleridir.

İlgili Kanun 9.maddesinde, Türkiye'nin taraf olduğu uluslararası sözleşmelere atıf yaparak, kişisel verinin yurtdışına aktarılması izni verilip verilmeyeceğini belirlerken, söz konusu ülke ile tarafı olunan uluslararası sözleşmelerin bulunuyor olmasını belirleyici kılmıştır.

Kanun 20.maddesinde Kişisel Verileri Koruma Kurumu'na (KKVK), *kişisel verilere dair uluslararası gelişmeleri izlemek ve değerlendirmek, uluslararası kuruluşlarla iş birliği yapmak* gibi görevler yüklemektedir.

Avrupa Konseyi'nin 1981 tarihinde kişisel verilerin korunması konusunda tek bağlayıcı uluslararası metin olan ve Türkiye'nin de aralarında bulunduğu yedi üye devlet tarafından imzalanan *108 sayılı Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşmenin* konusu hem özel hem de

kamu sektöründe elektronik olarak işlenen verilerin güvenliğidir. Sözleşme taraf devletler için asgari düzeyde bir zemin oluşturarak daha ayrıntılı çalışmaları ülkelerin kendi iç mevzuatlarına bırakmıştır (Küzeci, 2010, s.138).

4.4. 7418 sayılı Basın Kanununa ek Dezenformasyon Yasası

Türk Dil Kurumu'nun tanımlamasında dezenformasyon kelimesi *bilgi çarpıtma* olarak açıklanmış olup Fransızca aslından dilimize doğrudan aktarılmıştır. Enformasyon kelimesinin zıddı olarak anlam bulan bu kelime *bir bilginin kasıtlı veya kasıtsız olarak yanlış sunulması, deforme edilmesi* anlamında kullanılmaktadır. 2022 tarih ve 7418 sayılı Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına dair Kanun ile internet ortamında işlenen suçlara dönük bir takım düzenlemeler yapılmıştır (Resmi Gazete, 2022). Kanun 5187 sayılı Basın Kanununda revizyona giderek medya kuruluşu tanımlaması içerisinde internet ortamında haber yapan haber sitelerini eklemleyerek bu mecralardaki gazetecilerin Basın Kartı alabilmelerinin önünü açmıştır. Bu durum Basın Kanunu kapsamında yapıcı bir çalışma olarak okunmakla birlikte Kanunun üzerinde çokça durulan, mecliste ve toplum içerisinde tartışma götüren tarafı *Halkı yanıltıcı bilgiyi alenen yayma* başlığı aşağıdaki şekildedir:

> *Md.29. "Sırf halk arasında endişe, korku veya panik yaratmak saikiyle, ülkenin iç ve dış güvenliği, kamu düzeni ve genel sağlığı ile ilgili gerçeğe aykırı bir bilgiyi, kamu barışını bozmaya elverişli şekilde alenen yayan kimse, bir yıldan üç yıla kadar hapis cezasıyla cezalandırılır."*

Muhalif kesimlerce "Sansür Yasası" olarak lanse edilen kanun, yasanın yürürlüğe girme tarihinin seçim öncesi dönem olması sebebiyle hükümetin elini kuvvetlendireceği, ifade özgürlüğünü kısıtlayacağı, gazeteciler hakkında soruşturmaların artacağı ve net olmaması sebebiyle savcı ve hâkimler tarafından niyet okumasına sebep olabileceği yönünde eleştiriler almıştır (Oymak, 2022, s.510).

İletişim Başkanlığı'na bağlı Dezenformasyonla Mücadele Merkezi'nin (DMM) düzenli aralıklarla hazırlayarak internet üzerinden paylaştığı Dezenformasyon Bülteni, internet ortamında çıkan manipülatif haberlere dönük bir karşı sav niteliğindedir. Hazırlanan bu bültenlerde yer alan ve savunması yapılan asılsız haberler incelendiğinde, neredeyse tamamına yakınının hükümete karşı çıkan haberlere cevap niteliğinde olduğu, dezenformasyona maruz kalan diğer kesimlere dönük yanıtlara yer verilmediği

görülmektedir. Konuya devletin temel dinamiklerini korumak ve savunmak perspektifinden bakıldığı, Dezenformasyonla Mücadele Yasasında (RG, 2010) ifade edildiği gibi "kamu barışını bozmaya dönük eylemler" teması sebebiyle güvenlik perspektifinden yanıtlandığı yönünde iyimser bir bakış ile yaklaşılacaktır.

Özellikle çok uluslu toplumlarda toplumsal dinamiği sağlam bir zemine oturtmak için ifade özgürlüğünün ayrımcılığa sebep olmayacak şekilde formüle edilmesi gerekmektedir. Nefret söyleminin herkesçe kabul gören tek bir tanımı olmasa da Avrupa Birliği Bakanlar Kurulu'nun tavsiye kararını baz alalım. Bu kararda nefret söylemi için;

> *"Irkçı nefreti, yabancı düşmanlığını, Yahudi düşmanlığını veya azınlıklara, göçmenlere ve göçmen kökenli insanlara yönelik saldırgan ulusalcılık ve etnik merkezcilik, ayrımcılık ve düşmanlık şeklinde ifadesini bulan, dinsel hoşgörüsüzlük dâhil olmak üzere hoşgörüsüzlüğe dayalı başka nefret biçimlerini yayan, kışkırtan, teşvik eden veya meşrulaştıran her türlü ifade biçimi" denilmiştir* (Avrupa Konseyi, 1997). İfade özgürlüğü, kişi ve grupların hak ve özgürlüklerinin korunması ile ifade özgürlüğünün özünün kısıtlanmaması aralığında kalabildiği müddetçe anlam bulacaktır.

2016 yılında Avrupa Komisyonu tarafından çevrimiçi nefret söylemi ile mücadele kapsamında "Çevrimiçi Nefret Söylemi ile Mücadele İçin Etik Kurallar" kabul edilmiştir. Kurala katılan şirketlere erişimin engellenmesi ve içeriğin kaldırılması kararı verme yetkisi sağlayan bu kural metin, sansür yasası benzeri bir hukuksuzluğa sebep olabileceği yönü ile eleştirilmektedir (Çubukçu, 2020, s.170).

İfade özgürlüğünün sınırları konusunda Siber Suç Sözleşmesine üye ülkelerin ilgili yasaları ile Türkiye Dezenformasyon Yasası arasında mukayese yapacak olursak özellikle Almanya ve Fransa'da çok daha katı uygulamalar görmekteyiz. Almanya'da uygulanan Sosyal Ağ Uygulama Yasası (Network Enforcement Act- NetzDG) 2015 yılından itibaren ülkeye kabul edilen mültecilere karşı sorumlu kamu görevlilerini hedef alan nefret söylemleri sonrasında yürürlüğe girmiştir. Kanun, hızlı şekilde hazırlandığı ve demokratik söylemlere tehdit niteliğinde olduğu gerekçesiyle eleştirilmiştir (Çubukçu, 2020, s.171).

Siber güvenlik kapsamında Türkiye mevzuatı kanunlar çerçevesinde incelenmiş olup Bilgi Teknolojileri ve İletişim Kurumu çalışmaları kapsamında

hazırlanan yönetmelikler, tebliğ ve Kurul kararları gibi uygulamaya dönük alt düzenlemelere bu bölümde değinilmemiştir.

5. AVRUPA SİBER SUÇ SÖZLEŞME METNİNİN İÇERİK İNCELEMESİ

Toplumların ayakta kalabilmek için süregelen mücadelelerini bir arada var olma arzusu yönlendirmektedir. Toplum içerisinde yaşamanın ön şartı ise güvende olma duygusudur. Bu duygu toplumların tarih sahnesinde nice savaşlar yaşamasına neden olmuştur (Bauman, 2021, s.19). Devletlerin ayakta kalabilmek için temelde ihtiyaç duydukları şey yönetilenlerin faydasına olacak şekilde yönetim anlayışı belirlemektir. Hal böyle iken asırlar boyunca savaştan geriye kalan zamanlarda uluslararası anlaşmalar imzalanmış ve anlaşmaların getirdiği olumlu ya da olumsuz pek çok neticeler oluşmuştur. Büyük bedeller ödenerek çizilen devlet sınırlarına yönelen güvenlik açıkları zaman içerisinde şekil değiştirmiştir. Siber güvenlik, bilgi çağı öncesindeki geleneksel güvenlik kaygılarında olduğu gibi tahmin edilebilir değildir. İnternet alanında gelecek saldırılara karşı mücadele etmenin büyük bir bilgi birikimi gerektirmesi, siber saldırının nereden geleceğinin bilinememesi ve siber saldırılarda belirli devlet sınırlarının olmaması siber güvenlik meselesinin çıkmazlarından bazılarıdır (Akyeşilmen, 2018, s.109). Bu yeni tehdit biçimine karşı ne tür önlemler alınacağı konusunda bilgi birikimimizi artırarak bilgi çağı toplumları içerisinde yer edinebilmek oldukça önemlidir.

Avrupa Konseyi Birinci Dünya Savaşı ve İkinci Dünya Savaşı arasındaki dönemde Avrupa'da ortaya çıkan diktatörlükler ve demokrasi karşıtı fikirlere karşı bir duruş olarak, insan hakları ve özgürlükler noktasında ortak bir siyasi değerde buluşmak amacıyla oluşturulmuştur (Cevizliler ve Öncü, 2013, s.9). Konseyin oluşumunun ilk aşamalarında 1949 Ağustos ayında üyeliği kabul edilen Türkiye, o zamandan itibaren organizasyonun uluslararası düzeydeki hükümet çalışmalarında önemli rol oynamıştır (Schwimmer, 2001, s.1). Avrupa Birliği üyesi olma yolunda nice adımlar atan Türkiye, Avrupa Konseyi çerçevesinde imzalanan sözleşmeler noktasında oldukça istikrarlı bir ilerleme kaydetmektedir. Bilişim suçlarının doğası gereği suçun faili ile mağduru arasında oluşan mesafe, tek bir tanım ve çözüm üzerinde buluşma noktasında zorlukları beraberinde getirmektedir. Bilişim suçlarının mukayeseli hukukta yeknesak bir tanımı olmamakla birlikte mevcut tanımlar da açık ve yeterli tanımlamalar değildir. Belirtilen

bilişim suçlarının işlendiği bilişim araç ve sistemlerinin de çok teknik ve sürekli değişken olduğu görülmektedir. Önceki başlıklarda belirtildiği üzere TCK bilişim suçlarını tanımlamadan, tasnifleyerek açıklarken Bilgi Teknolojileri ve İletişim Kurumu'nun bilişim suçu tanımı "*bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış"* şeklindedir (Bilgi Teknolojileri ve İletişim Kurumu, 2019). Avrupa Konseyi Siber Suçlar Sözleşmesi'nde de siber suç tanımına yer verilmemiş, metin siber suçla mücadele ve mücadelede işbirliği üzerine kurgulanmıştır. Tek bir tanımı yapılamayan ve çerçevesi oldukça geniş olan bir kavram ve bu kavram etrafında şekillenen güvenlik konusu üzerine düzenlenen Avrupa Konseyi Siber Suçlar Sözleşmesi, sürekli değişen ve gelişen bilişim dünyasında gelecek tehlikelere karşı uluslararası işbirliği öngörmesi açısından değerlidir.

Avrupa Birliği çerçevesinde ise siber güvenlik çalışmalarına dayanak olan temel kuruluş Avrupa Ağ ve Bilgi Güvenliği Ajansıdır (ENISA). ENISA 2004 tarihinde Avrupa Konseyi'nin 460 sayılı Tüzüğü ile kurulmuş, 2008 tarihinde ise genişletilmiştir. AB uluslarının yetkili kuruluşların çalışmalarını birleştirmek ve koordine etmekle yetkilendirilmiştir (ENISA, t.y.). AB Siber Güvenlik Yasası bahse konu ajansı merkeze alarak birçok görev yüklenmiştir. Siber güvenlikle alakalı bir uzmanlık merkezi olarak değerlendirilmesi ve AB'ye üye devletlerin siber güvenlik politikalarının geliştirilmesi gibi önemli görevleri bulunmaktadır. AB uyum sürecinde Türkiye, Ulusal Siber Güvenlik Kurulu'nu ENISA örneği üzerinden kurgulamaktadır. Zira Türkiye'nin de taraf olduğu Avrupa Konseyi Siber Suçlar Sözleşmesi ile Avrupa Birliği çerçevesindeki siber güvenlik yasa ve çalışmaları birbirinden bağımsız düşünülememektedir.

ENISA, siber güvenlik alanında 2015 Ekim ayını Siber güvenlik ortak bir sorumluluktur! sloganı ile Avrupa Siber Güvenlik Ayı ilan etmiştir. Ayrıca farkındalık kazandırma ve teknolojilerde siber güvenlik alanında kamu-özel ortaklığı kurulmasını amaçlamaktadır. Zira ENISA, Avrupa Komisyonu ve paydaşlar (hükümetler, üniversiteler, sivil toplum kuruluşları, meslek örgütleri vb.) ile Avrupa genelinde geniş bir ağa sahiptir (Kutlu, Kahraman ve Dinçer, 2020).

Sanal Ortamda İşlenen Suçlar Sözleşmesi (doktrindeki adı ile Avrupa Konseyi Siber Suçlar Sözleşmesi) Avrupa Konseyi'ne üye ve üye olmayan ülkeler arasında 23.11.2001 tarihinde Budapeşte'de imzalanmış ve 01.07.2004'te 5 ülkenin onayı ile

siber suçlarla ilgili yasal prosedürü kapsayan ana metin haline gelerek yürürlüğe girmiştir (Council of Europe, 2001). Avrupa Konseyi Siber Suçlar Sözleşmesi'ne üye ülkelerin imza ve onay tarihleri değişmekle birlikte metni Türkiye'nin de aralarında bulunduğu 46 Avrupa Konseyi'ne üye ülke ile 24 Avrupa Konseyi'ne üye olmayan ülke imzalamıştır. Türkiye'nin sözleşmeyi imza tarihi 2010, yürürlüğe alma tarihi ise 2015'tir.

Siber güvenliğin sağlanması noktasında atılan uluslararası ilk önemli adım olan Avrupa Konseyi Siber Suçlar Sözleşmesi incelendiğinde, üye ülkelerin siber güvenlik konusunda birlik içerisinde hareket etmeleri sözleşmenin en temel amacı olarak karşımıza çıkmaktadır. Bilgisayar sistemlerinin üye ülkelerin toplumsal yapılarına uygun gizlilik ve güvenlik kuralları çerçevesinde işletilmesinin sağlanması, sağlanamadığı yahut art niyetli kişilerce ihlal edildiği durumlarda yasal yaptırımlara bağlanması metnin temel dinamiğini oluşturmaktadır. İyi işleyen bir uluslararası işbirliğinin koşulu olarak ortak bir ceza siyasetinin belirlenmesi de ihtiyaç olarak görülmektedir (RG, 2014).

Tüm bu amaçları gerçekleştirmek adına Avrupa Konseyi Siber Suçlar Sözleşmesi'nde bir takım yardımcı sözleşme metinlerine başvurulmuştur. 1950 Avrupa Konseyi İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi ile 1966 Birleşmiş Milletler Uluslararası Medeni ve Siyasi Haklar Sözleşmesi insan haklarına saygı hususunda yardımcı metin olarak değerlendirilmiştir. Kişisel verilerin korunması ile ilgili olarak 1981 Kişisel Verilerin Otomatik İşlenmesine İlişkin Olarak Bireylerin Korunması Konusunda Avrupa Konvansiyonu, Çocuk hakları konusunda 1989 Birleşmiş Milletler Çocuk Hakları Konvansiyonu ile 1999 Uluslararası Çalışma Örgütü Çocuk İşçilerin Kötü Durumları Konvansiyonu ve 1997 tarihli İkinci Zirve Toplantısı, Avrupa Konseyi toplantılarına ait tavsiye kararlarıdır (Council of Europe, 2001). Bahsi geçen toplantı metinleri doğrultusunda kişisel verileri amacına uygun kullanma ve insan haklarına saygılı olma prensibine bağlı bir sözleşme metni ortaya çıkmıştır.

Sanal ortamda işlenen suçlarla ilgili üye devletlerin iç hukuk düzenlerinde yeknesaklık sağlanması amacıyla Avrupa Suç Sorunları Komitesine (CDPC) bağlı çalışmalar ile bilgi teknolojileri standart ve değerlerine ortak bir bakış açısı getirebilmek amacıyla toplanan İkinci Zirve Eylem Planı siber güvenliğin gelişiminde ırkçı tutumlar

sergilenemeyeceği yönündeki tavsiye kararlarıyla zenginleştirilmiştir (Council of Europe, 2001).

Avrupa Konseyi Siber Suçlar Sözleşmesi 48 maddeden oluşmakta ve bilgisayar üzerinden işlenecek suç ve eylemler, ağ güvenliği gibi temel argümanları içermektedir. Ulusal Düzeyde Alınacak Önlemler ana başlığı altında ilkin Maddi Ceza Hukukuna yer verilmiş olup taraf ülkelerin ilgili ceza kanunlarında olması gereken alt başlıklar şu şekilde sıralanmıştır:

"Bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar" başlığı altında Yasadışı Erişim, Yasadışı Araya Girme, Verilere Müdahale, Sistemlere Müdahale, Cihazların Kötüye Kullanımı konularına yer verilmiştir. *"Bilgisayarla bağlantılı suçlar"* başlığı altında Bilgisayarlarla ilişkili sahtecilik fiilleri, Bilgisayarlarla ilgili dolandırıcılık alt başlıklarına yer verilmiş olup sahtecilik fiilleri verilerin orijinalliğini bozmak, değiştirmek, yeni veri eklemek, silmek, erişimi engellemek gibi durumlarla ilişkilendirilmiş, sahtekârlık fiilleri ise yapılan bu müdahalelerden haksız menfaat sağlamak ile ilişkilendirilmiştir. Hile, art niyet, zararın boyutu gibi kıstaslarla taraf ülkelere yorumlama hakkı vermektedir.

"İçerikle İlişkili Suçlar" başlığında Çocuk pornografisiyle ilişkili suçlarda reşit olmayanlar ve reşit görünmeyenlerin katılımına dair görüntüler suç sayılmış olup taraf ülkelere 16 yaşından küçük olmamak kaydıyla daha düşük yaş sınırı belirleyebilecekleri ifade edilmiştir.

Sözleşmenin 9. Maddesinde çocuk pornografisi tanımı *"cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımı, cinsel anlamda müstehcen bir eyleme reşit görünmeyen bir kişinin katılımı ve cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımını gösteren ve gerçek olmasa da gerçek gibi algılanan görüntüler içeren pornografik materyaller"* olarak tanımlanmıştır. Bilişim teknolojileri aracılığıyla gerçekleşen en yaygın çocuk istismarı türü çocuk pornografisi olmakla birlikte Türkiye mevzuatında açık bir tanımı bulunmamaktadır (Hekim ve Başıbüyük, 2013, s.141). Türkiye'de çocuk istismarı konusuna TCK madde 103'te değinilmiş, fakat bilişim sistemleri üzerinden gerçekleştirilebilecek istismara dönük bir yaptırım öngörülmemiştir. TCK madde 226 'da ise basın yoluyla müstehcenlik suçu tanımlanmış fakat yine çocuk pornografisi tanımlanmamış ve müeyyidelendirilmemiştir.

Birleşmiş Milletler tarafından kabul edilen 1989 Çocuk Hakları Sözleşmesi 1990 yılında Türkiye tarafından imzalanmış, 4058 sayılı Kanunla kabul edilerek yürürlüğe girmiştir (RG, 1994). Avrupa Konseyi Siber Suçlar Sözleşmesi metnine tekrar dönecek olursak, Maddi Ceza başlığı altındaki bir diğer alt başlık, *"Telif Haklarının ve Benzer Hakların İhlaline ilişkin suçlar"* olup 1971 tarihli Paris Yasası, Fikri Mülkiyet Haklarının Ticari Yönlerine ilişkin sözleşme ve WIPO Telif Hakları Anlaşması temelinde üye ülkelerin alacağı yasama tedbirlerine ilişkindir. Avrupa Konseyi Siber Suçlar Sözleşmesi içeriğinde bulunmasına rağmen çalışma alanımızla doğrudan ilgili olmadığından bu husus detaylandırılmayacaktır.

Bahse konu ana başlık altındaki son alt başlık ise, *"İlave Yükümlülük ve Yaptırımlar"* şeklinde tanımlanmıştır. *Teşebbüste Bulunmak ve Yardım ya da Yataklık Etmek, Kurumsal Yükümlülük, Yaptırımlar ve Önlemler* kenar başlıkları ile açıklanan bu kısımda, sözleşme metninde suç olarak belirlenen hususlarda şahsi ve kurumsal yardım ve yataklık yapan özel ve tüzel kimseler için devletlerin iç hukuklarında yasal düzenleme ve tedbirlerin alınmasını öngörmektedir.

Avrupa Konseyi Siber Suçlar Sözleşmesi'nin ikinci kısmı usul hukuku ile ilgili olup, üye devletlerce alınacak tedbirler ile ilgili kıstas sadece sözleşmede tanımlı cezai suçlarla sınırlı tutulmamıştır. Sözleşmede geçen cezai suçlar, bilgisayar sistemi kullanmak vasıtasıyla işlenen suçlar ve suç delillerinin elektronik alanda toplanması biçiminde üç ana maddede düzenlenmiştir.

Sözleşme, Şartlar Ve Tedbirler başlıklı 15. Maddesinde üye ülkelerden 1950 Avrupa Konseyi İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi ile 1966 Birleşmiş Milletler Uluslararası Medeni ve Siyasi Haklar Sözleşmesine, ayrıca uluslararası geçerliliği olan insan hakları belgelerine ölçülülük ve orantılılık çerçevesinde iç hukukta uygulama alanı yaratma teminatı istemektedir.

Sözleşmenin 16. Ve 17. Maddelerinde ise, depolanan bilgisayar verilerinin korunmasının gerekmesi durumunda (kişi mülkiyetinde bulunan bir bilgisayar verisi ise 90 gün boyunca) söz konusu veriyi süratle koruma, veri kaybını engelleme ve istenirse kısmen açıklama tedbirlerini taraf ülkelere yüklemektedir.

Sözleşme 19. maddede taraf ülkelerden birinin kendi ülkelerinde bir bilgisayar sistemine ait yetkisiz bir bilgisayar verisinin bulunduğuna olan inançlarını

gerekçelendirmeleri halinde; Bilgisayar sisteminin tamamına ya da bir kısmına yahut depolama cihazına el koyma, ilgili veriyi kopyalama, muhafaza altına alma, erişilemez hale getirme ve kaldırma yetkilerine sahip kılınmıştır. Bu maddeye dönük değerlendirme ilgili başlık altında açıklanacaktır.

Trafik verilerinin gerçek zamanlı toplanması başlığı altındaki 20. Maddede toplama, kaydetme, yetkili makamlarla işbirliği yapma konusunda taraf devletlere görev yüklenmiştir.

Avrupa Konseyi Siber Suçlar Sözleşmesi'ne ifade edilen tüm bu suç konularıyla ilgili taraf ülkelerin yargılama yetkisinde suçun;

Taraf ülkenin kendi sınırları içerisinde,

Taraf ülkeye ait bir gemi veya uçakta,

Herhangi bir devletin yerel yargı alanı dışında işlenmiş olması durumunda taraf ülkenin kendisi tarafından müeyyidelendirilmesi öngörülür (Council of Europe, 2001).

Sözleşmenin üçüncü bölümü uluslararası işbirliği konusunda olup ayrı başlık altında incelenecektir.

6. TÜRKİYE'DE KURUMSAL SİBER GÜVENLİK ÇALIŞMALARI

2012 yılına kadar siber güvenlik faaliyetlerinden TÜBİTAK sorumlu iken 2012/3842 sayılı Bakanlar Kurulu kararı ile ulusal siber güvenlik kurulu yürürlüğe girmiş ve sorumlu organ olarak Ulaştırma ve Altyapı Bakanlığı belirlenmiştir. (Ünver, 2023, s.132). 6518/2004 sayılı kanun ile 2008 tarihli 5809 sayılı Elektronik Haberleşme Kanunu'na madde eklenerek siber güvenlik kurulu düzenlenmiş, Bilgi Teknolojileri ve İletişim Kurumu'na siber güvenlik ile ilgili yeni görevler verilmiştir. Bahse konu maddede siber güvenlik kurulunun görevleri aşağıdaki gibi tanımlanmıştır.

"Siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak,

Kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak

Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek

Kanunlarla verilen diğer görevleri yapmak" (Bilgi Teknolojileri ve İletişim Kurumu, 2017).

6.1. Cumhurbaşkanlığına Bağlı Kurumsal Çalışmalar

Cumhurbaşkanlığına bağlı olarak faaliyet gösteren Dijital Dönüşüm Ofisi 2018 yılında Cumhurbaşkanlığı Hükümet Sistemine geçilmesini takiben 1 sayılı Cumhurbaşkanlığı kararnamesi ile kurulmuştur (RG, 2018). Ofis, kamu kurumlarının yürüttüğü kurumsal iş ve işlemlerin dijital ortama adapte edilmesi ve çağın koşullarına uygun güncel teknolojik gelişmelerle kurumsal işleyişin revize edilmesi üzerine çalışmalar yapmaktadır. Bir dizi çalışma yürüten Ofis, 81 ilde 81 Siber Kahraman, HackIstanbul, Kamunet ağı gibi projeler geliştirmeye devam etmektedir (TC. Cumhurbaşkanlığı, 2020).

Siber Güvenlik Kurulu çatısı altında Cumhurbaşkanlığına bağlı ve sorumlu bir diğer kuruluş ise Güvenlik ve Dış Politikalar Kuruludur. Kurulun ulusal ve bölgesel çalışmaları takip etmek, Siber güvenlik üzerine politika ve stratejiler geliştirerek önerilerde bulunmak gibi görev ve yetkileri bulunmaktadır (RG, 2018). Cumhurbaşkanlığına bağlı 9 kurul çalışmakta fakat Güvenlik ve Dış Politikalar Kurulunun görev alanının geniş olması sebebiyle dış politika aktörleri olan Dış İşleri Bakanlığı, Milli Savunma Bakanlığı gibi bakanlıklarla işbirliği halinde çalışmaktadır. Bu bağlamda kurulun bakanlıklardan bilgi ve belge talep edebilmesi diğer kurullar arasındaki öncelikli durumuna da örnek teşkil etmektedir (Gündoğdu, 2023, s.245).

Dijital Dönüşüm Ofisi bünyesinde hazırlanan ve birkaç yıllık sürelerle hazırlanan siber güvenlik eylem planları, siber tehditlerle daha etkin mücadele edebilmek, ulusal ve uluslararası çalışmaları takip ederek Türkiye'nin siber güvenlik misyonunu ileriye taşımak amaçlarıyla hazırlanmıştır. 2012-2013, 2016-2019 ve 2020-2023 yıllarını kapsayacak şekilde hazırlanan bu strateji ve eylem planlarına kısaca değinelim.

6.1.1. Ulusal siber güvenlik stratejisi ve 2013-2014 eylem planı

Ulusal siber güvenlik stratejisi ve 2013-2014 eylem planının amacı, kurumsal anlamda bilişim teknolojileri üzerinden sağlanan hizmetlerin güvenliği ile kritik altyapı

sistemlerinin güvenliğini sağlamaktır. Ayrıca, meydana gelecek siber tehditlerin kontrol altında tutulması yönünde stratejik hedefler belirlemek, siber suçların araştırmasını sağlamak da belirlenen amaçlardandır. Söz konusu eylem planı incelendiğinde kişisel ve kurumsal anlamda siber alan bilgi ve bilinç seviyesinin ayrıca yetişmiş personel sayısının henüz yeterli düzeyde olmadığı vurgulanmıştır. Bilişim sektöründeki yerli üretim eksikliği de bir başka ihtiyaç alanı olarak değerlendirilmiştir.

2013-2014 döneminde planlanan stratejik eylemler;

*Siber alanda mevzuat eksikliklerinin giderilmesi,

*Siber güvenlik terminolojisini içeren bir sözlük oluşturulması,

*Uluslararası hukuk kuralları çerçevesinde siber alanın, günün teknolojik gelişmelerinin gerisinde kalmayacak şekilde düzenlenmesi,

*Ulusal düzeyde gerçekleşecek siber saldırılara karşı ise Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulması, sektörel ve kurumsal bazda Siber Olaylara Müdahale Ekipleri (SOME) oluşturulması,

*Yerli teknolojiyi geliştirme ve bilinçlendirme faaliyetlerinin yürütülmesi gibi alt eylemler planlanmıştır (Ulaştırma ve Altyapı Bakanlığı, 2013).

6.1.2. 2016-2019 Ulusal e-devlet stratejisi ve eylem planı ve 2016-2019 ulusal siber güvenlik stratejisi ve eylem planı

Bir önceki eylem planı ve yürütülen faaliyetler doğrultusunda, yapılan iş ve işlemlerin gerçekleşme durumları ile değerlendirmeler üzerinde durulmuştur. Ayrıca Ortak Akıl Platformu oluşturularak Türkiye'de siber güvenliğin bulunduğu durum değerlendirilmiş, bilişim çalışanları, üniversiteler, kritik altyapı işletmecileri gibi sektörde bilgi sahibi uzman kişilerin katılımı ile toplantılar gerçekleştirilmiştir.

Güvenlik Stratejisi ve Eylem Planı hazırlanırken bu çalışmalara ilave olarak, tüm dünya üzerinde yapılan siber güvenlik stratejileri göz önüne alınmış, siber güvenlik alanında gelişmiş ülkelerin organizasyon yapıları ve siber saldırılara karşı geliştirilen çözüm önerileri dikkate alınmıştır.

Bir önceki eylem planıyla benzer amaçlar taşıyan bu strateji ve eylem planında siber güvenlik kuruluna üye kurumlar ile düzenleyici ve denetleyici kurumlar da listelenmiştir.

6.1.3. Ulusal siber güvenlik stratejisi ve eylem planı (2020-2023)

Siber güvenlik misyonunu daha ileriye taşımayı hedefleyen bu eylem planı ile siber tehditlerde ortaya çıkan eğilimler, ulusal ve uluslararası uygulamalar dikkate alınarak belirli hedefler ortaya konulmuştur. Siber tehditlere karşı daha etkin müdahale ederek ulusal becerilerin geliştirilmesi ve hatta Türkiye'nin siber güvenlik hedeflerinin uluslararası düzeyde en üst seviyelere taşınması hedeflenmiştir (Dijital Dönüşüm Ofisi, 2020).

Cumhurbaşkanlığı 2023 yıllık programında Dijital Dönüşüm Ofisine 2023 yılında siber güvenlik mevzuatını hazırlamaktan uluslararası siber rekabet üzerine çalışmalar yapmaya, yerli siber güvenlik modeli oluşturulmasından siber güvenlik eğitim öğretim meslek okulları müfredatının genişletilmesine kadar bir dizi görev verilmiştir. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanı Ali Taha Koç, Teknopark Mesleki ve Teknik Lisesi'nin kendi türü liseler içerisinde yüzde 1'lik dilime girerek en yüksek puanlı liseler arasında bulunduğunu açıklamıştır. Aynı zamanda devlet üniversitelerinde de siber güvenlik meslek yüksekokulları açılmaya başlanmıştır. Söz konusu strateji ve eylem planında ulusal faaliyetlerin yanı sıra uluslararası siber güvenlik çalışmaları temelinde ikili ve çoklu işbirliklerinin artırılması ve bu bağlamda çalışmalar yapılmasının öngörülmektedir.

Bir önceki eylem planında (2016-2019) uluslararası siber faaliyetlerin takip edilerek Türkiye'deki siber güvenlik çalışmalarının genişletilmesi amacı ile hareket edilmiş iken 2020-2023 eylem planında bu alanda uluslararası bir marka haline gelmek hedeflenmektedir. "Ulusal Güvenlik İçin Siber Güvenlik" mottosu ile 8 strateji hedefi belirlenmiştir. Bunlar; kritik altyapıların korunması ve güçlülüğünün artırılması, ulusal kapasitenin geliştirilmesi, organik siber güvenlik ağı oluşturulması, yeni nesil teknoloji güvenliği, siber suçlarla mücadele, yerli ve milli teknolojilerin geliştirilmesi, siber güvenliğin milli güvenliğe entegrasyonu, uluslararası iş birliğinin geliştirilmesi başlıkları altında düzenlenmiştir (Ulaştırma ve Altyapı Bakanlığı, 2020).

Dijital Dönüşüm Ofisi projelerinden olan Türkiye Siber Güvenlik Kümelenmesi ise milli siber güvenlik ürünlerinin tanıtımı ve yaygınlaştırılması amaçları doğrultusunda hareket eden bir platformdur. Kurumsal ilerlemenin özel sektöre de yayılması ve topyekûn bir siber öğrenim sürecinin geliştirilmesi hedeflenerek uluslararası teknoloji platformunda toplumun bilincini geliştirmek hedeflenmektedir.

6.2. Ulaştırma ve Altyapı Bakanlığına Bağlı Kurumsal Çalışmalar

2018 tarihinde yayımlanan 703 no'lu Kanun Hükmünde Kararname ile öncesinde Ulaştırma, Denizcilik ve Haberleşme Bakanlığı adı ile çalışmalarına devam eden bakanlık, teşkilat yapısında yapılan bazı değişiklerle birlikte Ulaştırma ve Altyapı Bakanlığı adını almıştır (Resmi Gazete, 2018). Bakanlığa bağlı genel müdürlüklerden olan Haberleşme Genel Müdürlüğü siber güvenlik alanında faaliyetler yürütmektedir. 2013 yılında kurulan Siber Olaylara Müdahale Ekipleri (SOME) ilgili bakanlığın kuruluş yönetmeliği ile siber güvenlik eylem planları çerçevesinde hazırlanmıştır.

Siber Olaylara Müdahale Ekipleri bilişim sistemlerinde kullanılan verilerin gizliliği, bütünlüğü ve erişilebilirliğinde meydana gelebilecek risklerin kaynak, neden ve sonuçlarının tespitine yönelik siber faaliyetler yürütür. SOME'ler kurumsal boyutta 28818 sayılı Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev Ve Çalışmalarına Dair Usul Ve Esaslar Hakkında Tebliğ ile tanımlanmış, ayrıca tebliğ metninde diğer kurum ve kuruluşların da kendi yapılanmalarına karşı oluşacak siber saldırılara karşı kendi bünyelerinde SOME oluşturabilecekleri bildirilmiştir. Ulusal Siber Olaylara Müdahale Merkezi (USOM) ise aynı metinde siber saldırılara karşı müdahale etme üzere kurulmuş ve gelen ihbarları değerlendiren ana merkez olarak kurulmuştur (RG, 2013b).

6.3. Sanayi ve Teknoloji Bakanlığına Bağlı Kurumsal Çalışmalar

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK), bilim ve teknolojiyi teşvik etmeyi amaçlamakta olup Sanayi ve Teknoloji Bakanlığının kuruluşlarından biridir. TÜBİTAK bazı platform ve yazılımlar üzerinden siber alanda çalışmalar yürütmektedir. Yürütülen bu çalışmalardan ilki ORION (Veri Güvenlik Platformu) ajan yazılımlar ile hassas verilere izinsiz erişim senaryolarına karşı çözümler

üreten veri kaçağı önleme sistemidir. Bir diğer uygulama olan DERBENT (Güvenli Uzaktan Erişim Sistemi) olup Anti virüs, Loglama Ajanları gibi alanlarda çalışmalar yürütür. Üçüncü faaliyet alanı olan SİBERLAB (Sanal Siber Güvenlik Laboratuvarı Altyapısı) uygulama odaklı eğitimler, tatbikatlar ve analiz laboratuvarları tasarımları ile hızlı erişimi olanaklı kılmaktadır. MERGE-n ise bir web uygulaması olup yerli siber güvenlik ürünlerinin kullanımlarının yaygınlaştırılmasını amaçlamaktadır (Tübitak, 2023).

6.4. Bilgi Teknolojileri ve İletişim Kurumu Bünyesinde Yürütülen Çalışmalar

Bilgi Teknolojileri ve İletişim Kurumu bilişim sektöründeki rekabetin oluşturulması, internet ve siber güvenlik alanında çalışmalar yürütülmesi gibi amaçlar doğrultusunda çalışmaktadır.

2013 yılında kurulan ve SOMElerle ilgili olarak yukarıda bahsedilen Ulusal Siber Olaylara Müdahale Merkezi (USOM) 2016'da doğrudan Bilgi Teknolojileri ve İletişim Kurumuna bağlanmıştır. Türkiye'de SOME sayısı ekip bazında 1000'in üzerine ulaşmış durumda olup USOM siber güvenlik uzmanı sayısı ise 3000'lere ulaşmış durumdadır. Yerli üretim AZAD, AVCI ve Kasırga yazılımları da kurumsal çalışmalarda siber suçla mücadele kapsamında kullanılmaktadır (Bilgi Teknolojileri ve İletişim Kurumu, 2023, s.84).

Bilgi Teknoloji ve İletişim Kurumu Avrupa Komisyonu mevzuatı kapsamında çalışmalara dâhil olmaktadır. AB mevzuatı çerçevesinde elektronik haberleşme anlayış ve tecrübelerinin paylaşılmasını sağlayan bir platform olan Avrupa BEREC çalışmalarına Türkiye'yi temsilen BTK gözlemci üye sıfatıyla katılım sağlamıştır (Bilgi Teknolojileri ve İletişim Kurumu, 2023, s.67).

Siber güvenlik çalışmalarında öncü konumda bulunan kurum, gündelik tedbirlerin yeterli olmayacağı öngörüsü ile hareket ederek çalışmalarını 4 ana program kapsamında yürüteceğini açıklamıştır. Bunlar; Kapasite İnşası Programı (İnsan kaynağı ve Eğitim), Hızlı Tespit Erken Müdahale Programı (teknolojik önlemler), Siber Tehdit İstihbaratı Edinimi ve Paylaşımı Programı (işbirliği ve iletişim), Kritik Altyapıların ve Verilerin Korunması Programı olarak açıklanmıştır.

6.5. Güvenlik Güçleri Çerçevesinde Kurumsal Çalışmalar (EGM, TSK)

2012 yılında TSK Siber Savunma Merkezi Başkanlığının kurulmasının ardından 2013'te bu kurum TSK Siber Savunma Komutanlığı adını almıştır. Türk Silahlı Kuvvetleri ve Genelkurmay Başkanlığı'nı olası siber saldırılara karşı korumak olarak tanımlanan misyon, sadece siber saldırılara karşı savunma işlevi gördüğünü gösterir niteliktedir (Orak, 2021, s.221). 2018 yılına gelindiğinde Türk Silahlı Kuvvetleri'ne ait siber güvenlik çalışmalarını ilerletmek maksadıyla Siber Savunma Merkezi Projesi (SİSAMER) kurulmuştur. Milli yazılım oluşturarak "dijital hudut"ların etkin korunmasını sağlamayı temel alan SİSAMER, TSK'nın çalışmalarını ileri seviyeye taşıması yönüyle önemlidir (Mavi Vatan, 2023).

2023 yılında Estonya Talin koordinatörlüğünde (NATO Siber Savunma Mükemmeliyet Merkezi) gerçekleştirilen 2023 Kilitli Kalkan Tatbikatına Türkiye ve Kore Cumhuriyeti takım halinde katılmıştır. 38 ülkenin yer aldığı söz konusu sanal tatbikata, TSK Siber Savunma Komutanlığı katılım göstermiştir (Milli Savunma Bakanlığı, 2023).

Emniyet Genel Müdürlüğü çatısı altında siber suçlarla mücadele etmek ve toplumda farkındalık oluşturmak, siber suçluların bulunmasında uluslararası işbirliğini artırmak gibi amaçlar doğrultusunda çalışmalar yürüten birimin adı Siber Suçlarla Mücadele Daire Başkanlığıdır. İlk olarak 2011 yılında Bilişim Suçlarıyla Mücadele Daire Başkanlığı olarak kurulmuş, 2013 yılında ismi Siber Suçlarla Mücadele Daire Başkanlığı olarak değiştirilmiştir (Emniyet Genel Müdürlüğü, 2023).

Avrupa Konseyi Siber Suç Program Ofisi (iPROCEEDS-2 Projesi) kapsamında 2022 yılında Antalya'da düzenlenen 7. Uluslararası Siber Suçlar Çalıştayı farklı ülkelerin karşılaştığı siber tehditlere karşı geliştirilen mücadele örnekleri ile ülkeler arası bilgi paylaşımında bulunulmuştur (Emniyet Genel Müdürlüğü, 2022).

7. ULUSLARARASI ADLİ YARDIMLAŞMA VE ULUSLARARASI SORUMLULUK

Uluslararası hukuk kuralları devletlerarası ilişkilerden doğan zarar ve eylemleri bertaraf etme ihtiyacı ile ortaya çıkmıştır. Küresel dünya düzeninde devletlerin ve uluslararası organizasyonların birbirlerine zarar vermesi, bilhassa siber alanda verilerin

erişilebilirlik imkânının artmasına paralel olarak daha kolay hale gelmiştir. Uluslararası düzlemde siber suçlarla mücadele mekândan bağımsız yapısı gereği uluslararası işbirliğini zorunlu kılmaktadır. Siber suç kaynaklarına erişim ulusal sınırları aştığı ölçüde işbirliği ve ortak çalışmalar zaruridir.

Siber güvenlik kapsamında Avrupa Birliği çerçevesindeki sözleşmelerle ile NATO arasında siber saldırılara karşı alınacak önlemler noktasında her ne kadar yeknesaklık görünse de Birleşmiş Milletler Genel Kurulu saldırı tanımını "*Saldırı, bir devletin diğer bir devletin egemenliğine, ülke bütünlüğüne veya siyasi bağımsızlığına karşı veya işbu tanımda belirtildiği üzere, Birleşmiş Milletler Andlaşması ile bağdaşmayan diğer herhangi bir tarzda silahlı kuvvet kullanılmasıdır*." şeklinde yapmaktadır (BM Enformasyon Merkezi, 1974). Bu noktada uzmanlar siber saldırının silahlı bir saldırı sayılıp sayılamayacağı üzerinde tartışmaktadır. Çatışma hukuku konusunda temel metinlerden olan Cenevre Sözleşmesinde saldırı eylemine hasma karşı işlenen şiddet eylemleri denilmiş ve tanım fiziki bir savaş aleti/silah ile daraltılmamıştır. Silahlı saldırıya eşdeğer zaiyat verebilecek siber saldırıların, BM sözleşmesi madde 51'de belirtilen meşru müdafaa hakkı kapsamında değerlendirilmesi öngörülmektedir (Çifci, 2023, s.85). Bu noktada devletlerin siber savunma stratejilerinde ve gelişmişlik düzeylerinde denklik olmadığı gerekçesi ile geride kalan ülkelerin meşru müdafaa hakkını kullanırken ortaya çıkan dezavantaj giderilmelidir.

Ulusların siber savunma alanında başvuru metni olarak değerlendirdiği, bağlayıcı olmayan fakat bilimsel değer taşıyan Tallinn Kılavuzu diğer adıyla Tallinn El Kitabı, NATO İşbirliğine Dayalı Siber Savunma Mükemmeliyet Merkezi (CCDCOE) tarafından ilk olarak 2013 yılında yayımlanmıştır. 2013 Siber Savaşa Uygulanabilen Uluslararası Hukuk ve 2017 Talin el kitabı 2.0 uluslararası siber saldırıları karşı koymanın hukuki zeminini oluşturmaktadır. Siber saldırıları da diğer saldırı türleri gibi kuvvet biçimi olarak görme gerekliliğinden ve devletlerin bu hususta meşru müdafaa hakkı bulunması gerektiğinden bahseder. 2021 yılında revize edilen metin, Tallinn Manual 3.0 Projesi adı ile bilimsel değerini korumaya devam etmektedir. (NATO İşbirlikçi Siber Savunma Mükemmeliyet Merkezi).

Ulusların karşılaştırmalı olarak siber güvenliğe karşı duruşları ile yürüttükleri çalışmaları tek tek inceleyerek kıyaslamak oldukça zor olacaktır. Bu görevi üstlenerek yıllık çalışmalar yapan ve belirli endeksler çerçevesinde devletlerin siber güvenlikte

bulunduğu noktayı gözler önüne seren, genel kabul görmüş bir çalışma bulunmaktadır. Uluslararası Telekomünikasyon Birliği her yıl tüm dünyada kabul gören ve devletlerin siber güvenlik kabiliyetleri ile mevzuatlarındaki gelişmeleri değerlendiren bir Global Siber Güvenlik Endeksi hazırlamaktadır. Endeksin 2021'de yayımlanan sonuçlarına göre Türkiye önceki yıllara göre yükselme eğilimine devam ederek Avrupa ülkeleri arasında 6., dünya genelinde ise 11. sıradadır. Ulusal ve uluslararası hukuki süreçlerde iş birliği alanında ise kaydedilen gelişmelerin değerlendirmesinde 100 üzerinden 97,50 puan almıştır. Birleşmiş Milletler Küresel Siber Güvenlik Endeksi çalışmasında ise devletlerin siber savunma kapasiteleri incelenerek bir sıralama oluşturulmuştur. Siber saldırılara karşı en hazırlıklı ülkeler sıralamasında Singapur'u Amerika Bireşik Devletleri takip etmektedir. İlk 10 ülke sıralaması Malezya, Umman, Estonya, Mauritius, Avustralya, Gürcistan, Fransa ve Kanada şeklinde devam etmektedir (Euronews, 2017). Görüldüğü gibi refah seviyesi en üst sıralarda yer almayan ülkeler de siber güvenlikle ilgili sıralamada üst sıralarda bulunmaktadır. Bu durum teknolojik aklın nerede bulunacağının değişkenlik göstermesi ve ülkelerin yaşadığı siber saldırılardan bir takım dersler çıkarması şeklinde açıklanabilir. Rusya, endekse 11'nci sıradan girerken, Hindistan 25'inci, Almanya ve Çin 34'üncü sırada yer aldı. Türkiye ise 43'üncü sırada kaldı.

Uluslararası sorumluluk konusunda *"Devletin Milletlerarası Hukuka Aykırı Eylemlerinden Sorumluluğuna ilişkin Taslak Maddeler"* metninde uluslarası örgütlerin kendisine yüklenen ve uluslararası hukuk uyarınca bir yükümlülüğü ihlâl eden eylemleri örgüte uluslararası sorumluluk yüklemektedir. Ancak uluslararası hukukta devletin suçu gibi bir tanımlama ve düzenleme bulunmadığından devletlere cezai sorumluluk yüklemek mümkün olmayacaktır. Bağlı olduğu kuruluşlar çerçevesinde hareket etmekte zorlanan ve uluslararası hukuk kurallarına aykırı hareketleri bulunan devletlere karşı yegâne yaptırım söz konusu sözleşme ve kuruluşlardan uzaklaştırmak şeklinde olabilecektir.

7.1. Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Uluslararası İşbirliği

Siber saldırı yöntemlerinin karmaşık bir hale gelmesi ile sınır aşan siber saldırılar devletlerin bu alanda güvenlik kaygısı yaşamasına sebep olmaktadır. Meydana gelecek saldırının yaratacağı hasar ve nereden geldiğinin tespiti için uluslararası işbirliği

şarttır. Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Uluslararası İşbirliği, sözleşmenin 23 ila 28. maddelerinde ifade bulmuştur. Suçlu iadesi söz konusu olduğunda suçlu iade edecek ve alacak olan taraf devletlerarasında başkaca antlaşma yok ise suçun cezai karşılığının bir yıl ve daha fazla hapis cezası gerektirmesi durumunda iade işlemi gerçekleştirilebilecektir (md. 24). Taraf devletlerden en az ikisi arasında iadeye konu soruşturma/kovuşturma durumu oluşmuş ise elektronik ortamda delil toplanması ile ilgili en geniş ölçüde ve en hızlı şekilde yardımlaşmada bulunacaklardır (md.25).

Devletlerarası işbirliği konusunda yardımcı kuruluşlardan biri, Avrupa Suç Sorunları Komitesi (CDPC) tarafından Avrupa Konseyi'nin suç önleme üzerine tavsiye ve raporlar hazırlama, anlaşma düzenleme gibi hususlarda Konseye üye devletlerarasında işbirliği oluşturmayı amaçlamaktadır. Bahse konu komite önderliğinde Avrupa Konseyi üye devletler adına hazırlanan anlaşmalar genel olarak terör, siber suçlar, organize suçlar gibi suç alanlarını kapsamaktadır (Tuncay, 2018, s.30).

Taraf devletlerarasında karşılıklı mevzuata dayalı uluslararası antlaşmalar yok ise yine bu sözleşme hükümlerine göre hareket edilecektir (md. 26). Bu madde taraf devletlerarasında teknolojik, kültürel, hukuksal uzlaşmazlıklara ve yeknesaklık sorununa bir çözüm niteliğinde okunabilir. Sözleşme, her ne kadar taraf -devletlerin kendi ihtiyaçlarına göre- iç mevzuatlarında olduğu kadar geniş olmayan bir çerçeve sunmakla yetinmiş ise de, Avrupa Konseyi Genel Sekreterliğinin yeknesaklık konusunda çözüm odağı olarak görevli kılındığı görülmektedir. Olası soruşturma/kovuşturma durumunda sözleşmenin taraf ülkelerden beklentisi, merkezi makamlar belirlenerek bu makamlar üzerinden iletişim kurulması, işbirliği hususunda herhangi bir talep olması durumunda iletişimin Uuluslararası Polis Teşkilatı olan Interpol üzerinden kurulması şeklindedir (md.27). Ayrıca Türkiye'de uluslararası mevzuata tekabül edecek şekilde 2013 yılında isim değiştirerek yeniden yapılanan, merkezde Siber Suçlar Daire Başkanlığı ve bünyesinde illerde siber şube müdürlük ve amirlikleri çalışmalar yürütmektedir.

Bilişim suçlarıyla mücadelede Interpol/Europol bünyesinde High- Tech Crime olarak tanımlanan, bilgisayar ağlarına zarar vermek için ileri teknoloji yöntemlerinin kullanılması ileri teknoloji suçu olarak ifade edilir. Bilgisayarlara veya bilgisayar ağına saldırmak için elektronik ve dijital tabanlı teknolojiyi kullanan suçları ifade eder. Bu suçlulara karşı Avrupa Konseyi Siber Suçlar Sözleşmesi'nde devletlerin ortak

menfaatleri göz önünde bulundurularak operasyonel faaliyetler yürütülmektedir (Europol). 2010 yılına gelindiğinde Europol içinde, Avrupa Komisyonu, Eurojust ve AB ülkelerinin siber suçla mücadele birimlerinin en tepesindeki kişilerden oluşan, Avrupa Siber Suç Timi (European Cybercrime Task Force-EUCTF) adında bir platform oluşturulmuştur. Esas amaç, bilişim suçlarıyla mücadelede işbierliği ve uyumu arttırarak çalışmalar yürütmek ve teknolojik ilerlemeden kaynaklı problemlere çözüm bulmaktır (Aliusta ve Benzer, 2018, s.37).

Avrupa İnsan Hakları Mahkemesi Avrupa Konseyi çerçevesinde mutlak surette değinilmesi gereken bir kuruluştur. Avrupa Konseyi'nin bir organı olmasa da bir materyali olarak çalışmalar yürüten Mahkeme, temel olarak Avrupa Konseyi'nden bağımsız çalışır. Fakat Konsey'in amaçları açısından organik bir bütünlük içerisinde ve esas araçlarından birisi olarak tasarlanmıştır. Bu organik bağ nedeniyle Avrupa Konseyi ile etkileşim ve iletişim alanında çalışmalar yürütür (Elban, 2008, s.169).

Avrupa Konseyi İnsan Hakları ve Hukukun Üstünlüğü birimince Uluslararası cezalara yönelik işbirliği alanında Avrupa Konseyi araçlarının uygulanması ilgili sorulan soruları cevaplamayı hedefleyen PC-OC (Problemes Criminels- Operation of onventions) uygulaması cezai işbirliği alanında oldukça önemli bir rol oynamaktadır. Bu şeffaf platform üzerinde Avrupa Konseyi çerçevesinde yürütülen toplantı genel faaliyetleri, kanun uygulayıcıları için hukuki standartlar ve ülke bilgileri, Avrupa İnsan Hakları Mahkemesi ile ilgili içtihadi bilgiler, PC-OC'nin önceki ve gelecekteki toplantıları da dâhil olmak üzere genel faaliyetleriyle ilgili bilgiler, PC-OC'nin faaliyetleri doğrultusunda yararlı diğer linkler bulunmaktadır (Avrupa Konseyi, 2017).

7.2. Türkiye Tarafında Uluslararası İşbirliği Konusu

Türk Hukuk Sistemi içerisinde ceza yasasının temel metinlerinden olan ve cezai müeyyideleri belirleyen Türk Ceza Kanunu 18. Maddesinde Geri Verme başlığı ile "suçluların iadesi" konusuna yer vermiştir. Suçluların iadesine dair uluslararası düzeydeki çalışma 1959 yılında Avrupa Konseyi tarafından hazırlanan ve tarafı bulunduğumuz sözleşmelerden olan Suçluların İadesine Dair Avrupa Sözleşmesidir (RG, 1959).

Avrupa Konseyi sözleşme yükümlülüklerini denetlemek amacıyla oluşturulan Avrupa İnsan Hakları Mahkemesi (AİHM) Türkiye'nin dâhil olduğu kuruluşlardandır.

İnsan hakları, eşit muamele, ayrımcılık ve işkence yasağı gibi konularda etkin mücadeleyi amaçlayan bu kuruluşun ulusal izdüşümü olarak 2016 yılında Türkiye İnsan Hakları ve Eşitlik Kurumu kurulmuştur (Sezgin, 2021, s.7).

6706 Sayılı Cezai Konularda Uluslararası Adli İşbirliği Kanunu uluslararası alanda işbirliği konusunda yapılan çalışmalara karşılık gelecek şekilde hazırlanmıştır. Kanun incelendiğinde iadeye konu olamayacak hususların kanunda belirlenmiş olması ile anlaşılmaktadır ki bilişim suçları kanun kapsamı içerisinde bulunup iadeye konu sebeplerden birisidir.

2016 yılında yürürlüğe giren Kanun Genel Hükümler, Adli Yardımlaşma, İade, Soruşturma ve Kovuşturmanın Devri, İnfazın Devri, Hükümlü Nakli gibi bölümler altında düzenlenmiştir. Bahse konu kanunda uluslararası adlî işbirliği tanımı *"cezaî konularda bir devletin adlî mercilerinin diğer bir devletin adlî mercileri adına yerine getirdiği işlemler"* şeklinde tanımlanmıştır (RG, 2016). Türk Ceza Kanununda tek maddede kısaca açıklanmış olan suçlu iadesi konusu 6706 sayılı kanun ile hukuki boşlukları doldurarak detaylandırıldığı görülmektedir. Örneğin Adli İş Birliği Taleplerinin Reddi başlığı altında c bendinde *"Talebe konu kişinin ırkı, etnik kökeni, dini, vatandaşlığı, belli bir sosyal gruba mensubiyeti veya siyasî görüşleri nedeniyle bir soruşturma veya kovuşturmaya maruz bırakılacağına veya cezalandırılacağına ya da işkence veya kötü muameleye maruz kalacağına dair inandırıcı nedenlerin bulunması"* şeklindeki ifadeden anlaşılacağı üzere Türkiye'de bulunan yabancı bir kimsenin cezasının infaz edilebilmesi amacıyla bir başka ülke ya da ülkelerce iade talebinin yanıtlanması belirli hukuki kıstaslara dayandırılmıştır. Bu kanun maddesinin söz konusu suçlu veya suçluların ülkemizde barınması, saklanması konusunun önüne geçerek uluslararası işbirliği bağlamında güncel ve olumlu bir düzenleme olarak okunabilmesinin yanı sıra suçlu iadesinde hukuka aykırı olarak cezalandırılacağına dair bir neden görülmesi durumunda suç isnat edilen kişinin temel hak ve hürriyeti de gözetilmiştir. Diğer yandan kötü muameleye maruz kalacağına dair inandırıcı nedenin hukuki ve nesnel temellere dayandırılması keyfi ve taraflı uygulamaların önüne geçmek bakımından önemlidir.

Aynı kanunda olumlu yorumlanabilecek ve suçlunun iadesinin reddini gerekli kılacak diğer bir ifade: *"Talebe konu fiilin sırf askerî suç, düşünce suçu, siyasî suç veya siyasî suçla bağlantılı bir suç olması,"* şeklindedir. Failin işlediği fiil ve meydana

getirdiği zarar bağlamından uzaklaşmadan ve failleri ülkeler arası çekişmelere konu etmeden uygulama alanı bulması hukukun temel ilkelerine verilen öneme örnek teşkil edecek niteliktedir.

Türkiye'nin iade koşullarındaki inisiyatifi kanun içerisinde yukarıda bahsedildiği şekilde ifade edilmiş olup suçluyu talep eden ülke veya ülkelerin iade talebinin kabul edilmeyebileceği durumlar açıklanmıştır. İade durumunun, *kişinin kendisini ve ailesini fiilin ağırlığı ile orantısız şekilde mağdur edeceği* öngörülüyorsa Türkiye söz konusu suçluyu iade etmeyebilecektir.

Suçlu iadesiyle ilgili olarak TCK, suçun işlendiği yer hususunda karma teori uyguladığından, başka ülkelerde işlenen suç sonuçlarının Türkiye'de vuku bulması halinde, Türkiye'de işlenmiş bir suç gibi değerlendirileceğinden mevzuatın uluslararası işbirliğine uygunluğu su götürmemektedir (Tezcan, 2019, s.289). Karşılıklılık ilkesi gereği Sözleşmeye taraf ülkelerin iç mevzuatlarının da uyumlu olması gerektiği düşünülmektedir.

27 Haziran 2023'te Siber Suçlar Sözleşmesi Komitesinin yaptığı bir toplantıda siber suçlarla ilgili uluslararası işbirliğinin sadece bilgisayar sistemlerine karşı ve bilgisayar sistemleri aracılığıyla işlenen suçlar için değil, konusu bilişimle ilgili olmamakla birlikte herhangi bir suça ilişkin elektronik ortamdaki kanıtlar için de geçerli olacağı kılavuz bir metin ile duyurulmuştur (Cybercrime Convention Committee, 2023).

Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi ve pratik uygulamasına dönük telekomünikasyon dinlemeleri ile ilgili R85 10 sayılı, güvenlik alanında kişisel verilerle ilgili R87 15 sayılı, bilgisayar suç tanımlarında devletlere yönerge sağlayan R89 9 sayılı ve telekomünikasyon ve bilgi teknolojileri ile ilgili Bakanlar Komitesi Tavsiye Kararları Avrupa Konseyi Siber Suçlar Sözleşmesi'ne üye devletlerce dikkate alınacaktır (RG, 2014).

Avrupa Konseyi Siber Suçlar Sözleşmesi içeriğinde belirtildiği üzere sanal ortamda işlenen suç konusunda uluslararası işbirliğini artırmak amacıyla BM, OECD, AB ve G8 çalışmalarını ve gelişmeleri takip etmek ve bu hususstaki anlayışı artırmak noktasında da bahse konu sözleşmeye üye devletlerle mutabakata varılmıştır (RG, 2014).

8. SONUÇLAR VE ÖNERİLER

Devletlerin siber güvenlik yarışında artık sadece siber savunma değil, bir adım daha ilerisi düşünülerek siber saldırılar üzerine bir yarış içerisinde olduğu görülmektedir. Milli güvenliği sağlamak adına siber alanda edinilen bilgiler ve siber casusluk faaliyetleri bir takım etik sorunlarını da beraberinde getirmektedir. Günümüzde güvenliği sağlamak argümanının gelişmiş devletlerin yegâne hedefi olmadığı açıktır. Üstünlük elde etme gayreti kendisini siber alanda da açık şekilde göstermektedir.

Avrupa Konseyi Siber Suçlar Sözleşmesi genel bir hat çiziyor olsa da devletlerin iç hukuklarında cezai müeyyideler birebir örtüşmemektedir. Sözleşme cezada yeknesaklık, caydırıcılık gibi bir takım temel hedefler gütmektedir. Türkiye özelinde cezaların caydırıcılığı, ceza sürelerinin yeterli olup olmadığı tartışılmalıdır. Çalışmaya konu sözleşmeye uyulup uyulmadığı konusunda bir denetim mekanizmasının fiilen mümkün görünmediği, siber saldırının nereden geldiği ve nasıl hızlıca bertaraf edilebileceği hususlarının ülkelerin teknoojik gelişmişlik seviyesine göre farklılık gösterdiği de bilinmektedir.

8.1. Sonuçlar

Bilişim sektörünün verileri somut veriler olmadığı için siber alanda yapılan çalışmalar bir kat daha zorlaşmaktadır. Örneğin Avrupa Konseyi Siber Suçlar Sözleşmesi madde 19'da belirtildiği üzere "verinin bahse konu bilgisayar sisteminde depolandığına *inandıklarına dair gerekçelerinin bulunması* ifadesi" taraf ülkelerin demokrasi inançları ve birbirlerine olan güvenleri noktasında havada kalmaktadır. İleri teknoloji üreten ve kullanan devletlerin artniyetli yaklaşımları daha düşük teknolojilere sahip ülkeleri dezavantajlı duruma getirebilecektir. Benzer şekilde 20. Maddede "trafik verilerinin eş zamanlı toplanması" ifadesi de teknik imkânları eşit olmayan ülkeler için yeknesaklığın nasıl sağlanacağı yönündeki çalışmaları beraberinde getirecektir. Tüm bunlar önümüzde duran eşitsizlikler ve sorunlar olarak değil, teknolojiyi geliştirmekte birer itici güç olarak değerlendirilirse batının teknolojik gelişmişlik seviyesine erişmek mümkün olabilecektir.

Devletlerin güvenlik kaygılarında birer etken olan coğrafi konumları, sömürgeciliğe yatkınlıkları, yeraltı ve yerüstü doğal zengin ve kaynakları gibi birçok faktör devletlerin refah seviyelerini etkileyen ve onları güçlü devlet konumuna getiren etkenlerdir. Ancak güvenliğin sağlanmasındaki diğer faktörlerden azade olarak teknolojik gelişme, devletlerin kendi kaderini değiştirecek farklar yaratabilme kapasitesini yaratır. Bu kapasite eğitimle güçlendirildiğinde bahşedilen diğer güçleri galebe çalabilecek seviyelere erişebilir.

Bir dizi ulusal ve uluslararası düzenleme yapan ve hedef ve öncelikleri farklı olan ülkeleri siber alanda aynı noktada buluşturmak zordur. Siber suçlulukla mücadelede büyük sorunlardan biri de, bu alanda devletlerin topyekün mücadele anlayışının olmamasının getireceği zararlar olarak ifade edilebilir. Öyle ki bir kaç ülkenin bile siber suç mevzuatı konusunda düzenleme yapmaması siber suçlulara korunaklı bir alan açılması açısından sorun teşkil edecektir. Suçlu iadesinin mümkün olabilmesinin ön koşulu suçun işlendiği ülke ile iade edilerek cezalandırılacağı ülkenin her ikisinin de iç hukukunda siber suçlarla ilgili yaptırım öngörülmesine bağlıdır. Birleşmiş Milletler, Avrupa Konseyi, NATO ve benzeri birçok kuruluş belirli tanımlamalar yapmış olsa da yeknesaklık konusunda sorunların çözülmesine uluslararası ve tek bir siber güvenlik terminolojisinin oluşturulması ile başlanabileceği değerlendirilmektedir.

Siber suçlular herhangi bir mekândan herhangi bir devlet ya da örgüte saldırı düzenleme gücü ile diğer suçlulardan ayrılmaktadır. Uluslararası genel geçer bir siber mücadele anlayışı olmadığı müddetçe etkin mücadeleden söz edilemeyecektir. Aksine devletlerin kendi mevzuatları ve çıkarları ile ters düşebilir olduğundan genel geçer bir siber güvenlik hukukun olması da neredeyse imkânsızdır. Örneğin Amerika Birleşik Devletleri siber alanda uluslararası hukuk normlarını kendi içişleyişindeki menfaatlere uygun bulmadığından çalışmamıza konu sözleşmeye üye olmamıştır.

8.2. Öneriler

Siber güvenliğin teknolojinin geldiği son noktada sağlayacağı faydalar ile güvenlik zafiyeti durumunda yaratacağı hasarlar günümüzde güvenlik meselesinin

temeline oturtulmalı ve teknolojik yarışta geri kalmadan bu alana gereken değer verilmelidir.

Bir Avrupa Birliği'nin idari denetiminden sorumlu Avrupa Komisyonunun, birlik üyesi ülkelerin ihtiyaçlarını temel alan yaklaşım sergilemesi son derece normaldir. Türkiye Avrupa ile ilişkili bir ülke olmasının yanında jeopolitik konumu gereği Amerika ve Asya ile de bağlantı kurma kabiliyeti çok yüksek olan bir ülkedir. Avrupa perspektifinden siber güvenlik anlayışı geliştirmek devletin siber politikalara bakış açısını kısır döngü içerisine sokabilir. Ekonomi ve güvenlik alanlarında Rusya ve Çin'le, Ortadoğu coğrafyasında İran, Irak, Suriye ile önemli bağları bulunan Türkiye, her alanda olduğu gibi siber güvenlik alanında da çok yönlü düşünmeye ve dünyanın farklı noktalarındaki siber politikaları takip etmeye mecburdur. Geleceğe dönük çalışmalar yapmak içinde bulunduğumuz çağın rekabetçi yapısı nedeniyle son derece gereklidir. ABD ve Rusya gibi ülkelerin siber güvenlik çalışmaları incelendiğinde, bu ülkelerin öngörülerinin daha geniş ve hatta güvenlik kaygılarının daha fazla olduğunu Avrupa'ya göre çok daha önceki tarihlerde başladıkları çalışmalardan görebilmekteyiz. Zira bağımsız güvenlik politikaları geliştirmek, ülkelerin kaderlerine yön vermede önemli bir etkendir.

Siber alanda hem devletler hem de özel sektör araştırma ve geliştirme faaliyetlerine hız kazandırmalıdır. Teknolojik ilerleme günü gününe takip edilebilir ve yakalanabilir bir süreci ifade etmese de siber savunmaya yönelik çözümler ülkeyi belki ciddi bir siyasi krizin içerisinden alabilecektir. Türkiye'deki siber güvenlik yöneticilerinin Avrupa Komisyonu içerisindeki çalışmaya konu sözleşmeden hareketle alanında uzman kişiler arasından seçilmesi, farkındalık yaratma eğilimi yüksek yöneticilerle hareket edilmelidir. Yine siber güvenlik organizasyonları içerisinde olası siber saldırılara karşı geliştirilecek formül ve çabuk yanıt verme gibi risk yönetimi konularında da uzman kişiler istihdam edilmelidir.

Hukuksal boyuttaki Türkiye'deki eksikliklere bakacak olursak 5237 sayılı kanunun 226. maddesi müstehcenlik suçu ile ilgilidir. Suç teşkil eden müstehcenlik eylemleri tanımlanıp yaptırıma bağlanmış ise de çocuk pornografisinin ayrı bir suç tipi olarak düzenlenmemiş olması Türk Hukuku açısından önemli bir eksiklik olarak okunabilir. Avrupa Konseyi Siber Suçlar Sözleşmesi'nde açıkça ifade edilen bu konu ile ilgili henüz mevzuatımızda bir çalışma görülmemektedir. Birleşmiş Milletler 1989

tarihli Çocuk Hakları Sözleşmesi 1990 yılında Türkiye tarafından imzalanmış, 4058 sayılı kanunla yaklaşık 4 sene sonra yürürlüğe girmiş olup çocuk pornografisi ile ilgili sadece *"önlemek amacıyla ulusal düzeyde ve ikili ile çok taraflı ilişkilerde gerekli her türlü önlemi almak"* tan öte bir ifade bulunmamaktadır.

Sistemdeki güvenlik açıkları kullanılarak veri gizliliği bozulan ve tehdit unsuru haline gelen durumlara karşı devletler farkındalık seviyelerini çeşitli eğitimlerle arttırmalıdır.

9. KAYNAKLAR

Acemoğlu, D. ve Johnson, S. (2023). *İktidar ve teknoloji. Bin yıllık mücadele*. Çeviren: Cem Duran. 1. baskı, İstanbul: Doğan Yayınları.

Akkaş, H.H. ve Ravanoğlu, G.A. (Ed). (2022). *Değişen dünyada küreselleşme ve ulus devlet.* İstanbul: Efe Akademi Yayınları.

Akyeşilmen, N. (2018). *Disiplinlerarası bir yaklaşımla siber politika ve siber güvenlik*. Ankara: Orion kitapevi.

Aliusta, C. ve Benzer, R. (2018). Avrupa siber suçlar sözleşmesi ve Türkiye'nin dahil olma süreci. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 4(2), s.35-42, Erişim Bilgisi: https://dergipark.org.tr/tr/download/article-file/645923 [Erişim Tarihi: 1 Aralık 2023].

Altun, Ö. G. A. (2017). Abd-Çin rekabeti bağlamında siber savaş. *International Journal of Academic Value Studies*, 3(9), ss24-34, Erişim Bilgisi: https://javstudies.com/files/javstudies_makaleler/1525107318_3-Altun%20ALTUN_24-34.pdf [Erişim Tarihi: 19 Aralık 2023].

Aras, F.Ç. (2023). Türkiye'de yeni sınır güvenliği paradigması: Göç, güvenlik ve göç yönetimi. *Van Yüzüncü Yıl Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 61, s. 469-487. Erişim Bilgisi: https://dergipark.org.tr/en/download/article-file/3352005. [Erişim Tarihi: 7 Kasım 2023].

Arghire, I. (2023). "Casus yazılım, İsrail roket uyarı uygulaması kılığına girerken yakalandı". Erişim Bilgileri: https://www.securityweek.com/spyware-caught-masquerading-as-israeli-rocket-alerting-applications/ [Erişim Tarihi: 4 Aralık 2023].

Arslan, M. E. (2017). Siber güvenlik ve siber saldırı türleri. Gazi Üniversitesi. Erişim Bilgisi: https://www.academia.edu/31827545/S%C4%B0BER_G%C3%9CVENL%C4%B0K_VE_S%C4%B0BER_SALDIRI_T%C3%9CRLER%C4%B0_CYBER_SECURITY_AND_CYBER_ATTACK_TYPES_03_05_2016 [Erişim tarihi: 26.12.23].

Asl, S. S. (2017). Siber terörizm ve ulusal güvenlik: Örnek ülke İran. İstanbul: Tasam Yayınları. Erişim Bilgisi: https://tasam.org/tr-TR/Icerik/54663/siber_terorizm_ve_ulusal_guvenlik_ornek_ulke_iran [Erişim Tarihi: 7 Aralık 2023].

Aslanbakan, E. (2023). *Bilgi güvenliği ve uygulamaları: Hacking yöntemleri.* 5. Basım, İstanbul: Pusula yayıncılık ve iletişim.

Avrupa Konseyi Bakanlar Kurulu kararı. (1997). Erişim Bilgisi: https://www.echr.coe.int/documents/d/echr/FS_Hate_speech_TUR [Erişim Tarihi: 1 Ekim 2023].

Avrupa Konseyi. (2017). İnsan hakları ve hukukun üstünlüğü ceza hukuku birimi. Erişim Bilgileri: https://rm.coe.int/16807011be [Erişim Tarihi: 27 Ekim 2023].

Bauman, Z. (2021). *Küreselleşme. Toplumsal sonuçları*. Çeviren: Akın Emre Pilgir. 10. Basım, İstanbul: Ayrıntı Yayınları.

Baumberger, G. (2019). ISIS online: Analyzing ISIS's use of the internet as a method of legitimation. *The Student Journal of Theological Studies*, Volume 2, İssue 1, Article 2, s.1-14. Erişim Bilgisi: https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=1024&context=saysomethingtheological [Erişim Tarihi: 4 Eylül 2023].

Bıktım, E. (2018). UEFI Rootkit saldırılarına dikkat. Erişim Bilgisi: https://www.cnnturk.com/teknoloji/uefi-rootkit-saldirilarina-dikkat [Erişim Tarihi: 14 Kasım 2023].

Bilgi Teknolojileri ve İletişim Kurumu. (2017). 5809 sayılı Elektronik ve haberleşme kanunu'na eklenen ek madde 1 Siber Güvenlik Kurulu. Erişim Bilgileri: https://www.btk.gov.tr/siber-guvenlik-kurulu [Erişim Tarihi: 01.11.2023].

Bilgi Teknolojileri ve İletişim Kurumu. (2019). Bilişim hukuku ve bilişim suçu. Erişim Bilgisi: https://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu#:~:text=Bili%C5%9Fim%20Su%C3%A7lar%C4%B1%20ise%20bilgileri%20otomatik,i%C5%9Flenen%20su%C3%A7lar%20%C5%9Fekliyle%20de%20tan%C4%B1mlanabilir. [Erişim Tarihi: 25 Temmuz 2023].

Bilgi Teknolojileri ve İletişim Kurumu. (2023). Bilişim hukuku ve bilişim suçu. Erişim Bilgisi: https://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu#:~:text=Bili%C5%9Fim%20Su%C3%A7lar%C4%B1%20ise%20bilgileri%20otomatik,i%C5%9Flenen%20su%C3%A7lar%20%C5%9Fekliyle%20de%20tan%C4%B1mlanabilir. [Erişim Tarihi: 25 Temmuz 2023].

BM Enformasyon Merkezi, (1974/3814). Birleşmiş Milletler Genel Kurul kararı. Erişim Adresi: https://inhak.adalet.gov.tr/Resimler/Dokuman/2312020095336bm_31.pdf [Erişim Tarihi: 3 Ekim 2023].

Bulut, A., Aydın, M.A. ve Zaim, A.H. (2023). Sıfır güven ağ erişim mimarisinde kullanıcı güvenliğinin sağlanması. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi*, 22(43), s.215-232, Erişim Bilgisi: https://doi.org/10.55071/ticaretfbd.1102276 [Erişim Tarihi: 8 Aralık 2023].

Büyükbaş, H. (2006). Avrupa güvenlik strateji belgesi ve Türkiye. *Ankara Üniversitesi SBF Dergisi*, 61(01), s. 37-66, Erişim Bilgisi: https://doi.org/10.1501/SBFder_0000001383 [Erişim Tarihi: 12 Kasım 2023].

Clarke, R.A. ve Knake, R.K. (2010). *Cyber war: The next threat to national security and what to do about it*. New York: Harper Collins Publishers.

Common Criteria. About the common criteria. Erişim Bilgisi: https://www.commoncriteriaportal.org/ccra/index.cfm [Erişim Tarihi: 25 Temmuz 2023].

Councıl Dırectıve. (2008). "On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection", *Official Journal of the European Union*, 345(82), s.75-82, Erişim Bilgisihttps://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF [Erişim Tarihi: 20 Temmuz 2023].

Council of Europe. (2001). "Avrupa siber suçlar sözleşmesi", Erişim Bilgisi: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 [Erişim Tarihi: 25 Temmuz 2023].

Cybercrime Convention Committee. (2023). Erişim Bilgisi: https://www.coe.int/en/web/cybercrime/-/t-cy-confirms-broad-scope-of-powers-for-the-collection-of-electronic-evidence-and-international-cooperation%C2%A0 [Erişim Tarihi: 11 Ekim 2023].

Çahmutoğlu, E. (2021). "Dünyayı tehdit eden casus yazılım: Pegasus." Erişim Adresi: https://www.aa.com.tr/tr/analiz/dunyayi-tehdit-eden-casus-yazilim-pegasus/2314321 [Erişim Tarihi: 05 Kasım 2023].

Çakır, S. ve Kesler, M. (2012). Bilgisayar güvenliğini tehdit eden virüsler ve antivirüs yazılımları. *Akademik Bilişim'12* - XIV. Akademik Bilişim Konferansı Bildirileri, 469-476.

Çakmakkaya, B.Y. ve Akpınar, T. (2018). Bilişim suçları ile mücadelede karşılaşılan sorunlar. *Balkan ve Yakın Doğu Sosyal Bilimler Dergisi,* 04 (03), s.123-129, Erişim Bilgisi: http://ibaness.org/bnejss/2018_04_03/14_Cakmakkaya_and_Akpinar.pdf [Erişim Tarihi: 1 Ocak 2024].

Çelik, S. (2018). Siber uzay ve siber güvenliğe multidisipliner bir yaklaşım. *Academic Review of Humanities and Social Sciences.* Vol1, s. 110-119, Erişim Bilgisi: https://dergipark.org.tr/en/download/article-file/567921 [Erişim Tarihi: 10 Eylül 2023].

Çelik, S., ve Çeliktaş, B. (2018). Güncel siber güvenlik tehditleri: Fidye yazılımlar. *Cyberpolitik Journal*, 3(5), 105-132.

Çubukçu, A. (2020). Almanya'nın sosyal ağ yasasının nefret söylemi içeriklerinin kaldırılması bakımından incelenmesi: Türkiye için öneriler. *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi* 3(2), s.164-181, Erişim Bilgisi : https://dergipark.org.tr/en/download/article-file/942164 [Erişim Tarihi: 5 Kasım 2023].

Çifci, H. (2023). *Her yönüyle siber savaş*. 3.basım, Ankara: Tübitak Popüler Bilim Kitapları.

Çivi, G. ve Çekiç, N. (2015). INTERSECT- Kullanıcı kimlik doğrulama ve onaylama sistemi. *GİDB Dergi(02)*, s. 47-52, Erişim Bilgisi: https://dergipark.org.tr/tr/pub/gidb/issue/53676/717547 [Erişim Tarihi: 8 Aralık 2023].

Darıcılı, A.B. ve Özdal, B. (2017). Enformasyon savaşı bağlamında Rusya Federasyonu-Türkiye ilişkilerinin analizi. *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi*, 4(1), s. 19-40. Erişim Bilgisi: https://doi.org/10.17336/igusbd.305525 [Erişim Tarihi: 1 Aralık 2023].

Doğan, A. ve Abacı, F. (2021). Türkiye'de siber terörizme karşı bilişimlerinin kullanımı. *Uluslararası Toplum Araştırmaları Dergisi*, 18 (42), Erişim Bilgisi: https://dergipark.org.tr/tr/download/article-file/1656045 [Erişim Tarihi: 12 Kasım 2023].

Dusane, P.S. ve Pavithra, Y. (2020). Logic bomb: an insider attack. *International Journal of Advanced Trends in Computer Science and Engineering.* Volume 9, No.3, s. 3662-3665, Erişim Bilgisi: https://www.warse.org/IJATCSE/static/pdf/file/ijatcse176932020.pdf [Erişim Tarihi: 23 Aralık 2023].

Economist. (4 Ocak 2018). "China's great firewall is rising". Erişim Bilgileri: https://www.economist.com/china/2018/01/04/chinas-great-firewall-is-rising?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=18151738051&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gad_source=1&gclid=EAIaIQobChMIrurkuJK3gwMVCBAGAB0MPgXYEAAYASAAEgJpZfD_BwE&gclsrc=aw.ds [Erişim Tarihi: 29 Aralık 2923].

Elban, H.K. (2018). Avrupa Konseyi ve İnsan Hakları Avrupa Mahkemesi ilişkileri. *TBB Dergisi*, 77, s.167-190, Erişim Bilgisi: http://tbbdergisi.barobirlik.org.tr/m2008-77-436 [Erişim Tarihi: 1 Aralık 2023].

Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Dairesi Başkanlığı. (2022). 7. Uluslararası siber suçlar çalıştayı. Erişim Bilgisi: https://www.egm.gov.tr/siber/genel-bilgiler-general-information [Erişim Tarihi: 3 Aralık 2023].

Emniyet Genel Müdürlüğü. (2023). Siber suçlarla mücadele daire başkanlığı. Erişim Bilgileri: https://www.egm.gov.tr/siber.

ENISA. (t.y.). ENISA yetkisi ve düzenleyici çerçeve. Erişim Bilgileri: https://www.enisa.europa.eu/about-enisa/regulatory-framework [Erişim Tarihi: 15 Aralık 2023].

Euronews. (2017). "Küresel siber güvenlik endeksi açıklandı.". Erişim Bilgileri: https://tr.euronews.com/business/2017/07/05/kuresel-siber-guvenlik-endeksi-aciklandi [Erişim Tarihi: 05.10.2023].

Euronews. (2023). “Siber aktivistler İsrail-Gazze savaşını internete taşımaya çalışıyor”. Erişim Bilgileri: https://tr.euronews.com/2023/10/11/siber-aktivistler-israil-gazze-savasini-internete-tasimaya-calisiyor [Erişim Tarihi: 3 Ocak 2024].

Europol. (t.y.). High tech crime. Erişim Bilgileri: https://www.europol.europa.eu/crime-areas/cybercrime/high-tech-crime [Erişim Tarihi: 24 Ekim 2023].

Foucoult, M. (2018). *Özgürlük ve bilgi. Fon Eldersle söyleşi*. Çeviren: Utku Özmakas. İstanbul: Sel Yayıncılık.

Gemici, E. ve Ercan, M. (2023*). 21. yüzyılda küresel ve bölgesel aktörlerin güvenlik stratejileri ABD, AB, Almanya, Çin, Fransa, İngiltere, Rusya, Türkiye, NATO*. İstanbul: Efe Akademi Yayınları.

Göçoğlu, V., Aydın, M.D. (2019). Siber güvenlik politikası: Abd, Rusya ve Çin üzerine karşılaştırmalı bir analiz. *Güvenlik Bilimleri Dergisi*, 8(2), s.229-252, Erişim Bilgisi: https://dergipark.org.tr/tr/download/article-file/854161 [Erişim Tarihi: 20 Aralık 2023].

Gözlügöl, S. V. (2013). Uluslararası hukuk boyutuyla hukukun üstünlüğü. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi,* 17(2), s.1423-1454. Erişim Bilgisi: https://dergipark.org.tr/en/pub/ahbvuhfd/issue/48109/608415. [Erişim Tarihi: 17 Eylül 2023].

Güldoğan, M.V., Işıklı, Ş. (2022). Siber savaşta mütekabiliyet. *Academic Journal of Information Technology* 13(51), s. 288-319, Erişim Bilgisi: https://dergipark.org.tr/en/download/article-file/2744210 [Erişim Tarihi: 23 Aralık 2023].

Gündüz, M. Z. Ve Daş, R. (2016) Sosyal mühendislik: yaygın ataklar ve güvenlik önlemleri Erişim Bilgisi: https://www.bingol.edu.tr/documents/Sosyal%20M%C3%BChendislik-yayg%C4%B1n%20Ataklar%20ve%20G%C3%BCvenlik%20%C3%96nlemleri.pdf [Erişim Tarihi: 16 Ekim 2023].

Güner, M. A. (2018). Yaygın ağ saldırıları ve genel hatlarıyla ağ savunması. Erişim Bilgisi:https://www.researchgate.net/profile/Mahmut-Alperen-Guener/publication/348098380_Yaygin_Ag_Saldirilari_ve_Genel_Hatlariyla_Ag_Savunmasi/links/5fef05c3a6fdccdcb81ec923/Yaygin-Ag-Saldirilari-ve-Genel-Hatlariyla-Ag-Savunmasi.pdf [Erişim Tarihi: 10 Eylül 2023].

Hansen, L., Nissenbaum, H. (2009) Digital disaster. *Cyber Security and the Copenhagen School, International Studies Quarterly*, Volume: 53, s.1155-1175. Erişim Bilgisi: https://nissenbaum.tech.cornell.edu/papers/Digital%20Disaster.pdf [Erişim Tarihi: 10 Eylül 2023].

Hekim, H., Başıbüyük, O. (2013). Siber suçlar ve Türkiye’nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi,* 4 (2), s. 135-158, Erişim Bilgisi: https://www.acarindex.com/dosyalar/makale/acarindex-1423936102.pdf [Erişim Tarihi: 5 Kasım 2023].

Henkoğlu, T., Yılmaz, B. (2013). Avrupa Birliği bilgi güvenliği politikaları. *Türk Kütüphaneciliği* 27, 3, s. 451-471, Erişim Bilgisi: https://dergipark.org.tr/en/download/article-file/811421 [Erişim Tarihi: 12 Eylül 2023].

Independent Gazetesi. (4 Kasım 2023). "Hamas siber saldırısıyla' İsrail ordusunun sırlarını hackledi". Erişim Bilgisi:https://www.indyturk.com/node/671951/d%C3%BCnya/%E2%80%98hamas-siber-sald%C4%B1r%C4%B1s%C4%B1yla%E2%80%99-i%CC%87srail-ordusunun-s%C4%B1rlar%C4%B1n%C4%B1-hackledi [Erişim Tarihi: 21 Aralık 2023].

Küçüksolak, Ö. (2023). Teknolojik soğuk savaş: ABD-Çin rekabetinin dijital merkantilizm üzerinden analizi. *Marmara Üniversitesi Siyasal Bilimler Dergisi*, 11(2), 284-308. Erişim Bilgisi: https://doi.org/10.14782/marmarasbd.1345741 [Erişim Tarihi: 15 Aralık 2023].

Körpe, Ö. (Ed.). (2021*). Harpte yeni kavramlar: operatif sanat, teknoloji ve harp hukukundaki yansımalar*. İstanbul: Millî Savunma Üniversitesi Yayınları.

Heywood, Andrew. (2015). *Siyasi ideolojiler: bir giriş*. Baskı, Ankara: Adres yayınları.

Kara, İ. (2019a). İnterpol fidye yazılım saldırısı ve analizi. *İleri Teknoloji Bilimleri Dergisi*, 8(2), s. 117-128, Erişim Bilgisi: https://dergipark.org.tr/tr/pub/duzceitbd/issue/51527/566286 [Erişim Tarihi: 27 Aralık 2023].

Kara, İ. (2019b). Truva atı zararlı yazılımlarının tespit, teknik analiz ve çözüm önerileri. *Bilgi Yönetimi Dergisi* 2(1), s. 28-33, Erişim Bilgisi: https://dergipark.org.tr/en/download/article-file/726511 [Erişim Tarihi: 20 Aralık 2023].

Karasoy, H. ve Babaoğlu, P. (2021). Türkiye'de siber güvenlik: yasal ve kurumsal altyapı. *Yasama Dergisi* (44), s. 123-155, Erişim Bilgisi: https://dergipark.org.tr/tr/pub/yasamadergisi/issue/68393/1005110 [Erişim Tarihi: 15 Aralık 2023].

Karasoy, H. ve Gezici, H.S. (2023). Bombalardan baytlara: siber güvenliğin ulusal güvenlikteki rolü ve yapay zekânın siber güvenlikteki önemi. *Uluslararası Yönetim Akademisi Dergisi*, 6(1), s. 173-188, Erişim Bilgisi: https://doi.org/10.33712/mana.1254015 [Erişim Tarihi: 15 Aralık 2023].

Keleştemur, A. (2018). Siber istihbaratın kamu güvenliği için rolü ve önemi, Yüksek Lisans Tezi*,, İstanbul Gedik Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul, 100-101.

Keleştemur, A., Koldemir, B., Yapıcı, M. (2017) Deniz taşımacılığında siber güvenliği tehdit eden unsurlar ve koruma önlemleri üzerine bir çalışma. *III. Ulusal Liman Kongresi.*

Kurzweil, R. (2020). *İnsanlık 2.0. Tekilliğe doğru biyolojisini aşan insan*. Çeviren: Mine Şengel. 6. Baskı, İstanbul: Alfa Basım.

Kutlu, Ö., Kahraman, S. Ve Dinçer, S. (2020). Avrupa Birliği'ne uyum sürecinde Türkiye'nin siber güvenlik politikalarının analizi. 13. Uluslararası Kamu Yönetimi Sempozyumu Bildirileri.

Küzeci, E. (2010), Kişisel verilerin korunması, Doktora Tezi, *Ankara Üniversitesi Sosyal Bilimler Enstitüsü*, Ankara, 97-138.

Milli Savunma Bakanlığı. (2023). Kilitli kalkan-2023 (Locked shields-2023) tatbikatı, Erişim Bilgisi: https://www.hvkk.tsk.tr/News/Article/hvkk/1685 [Erişim Tarihi: 19 Aralık 2023].

Mahmutoğlu, F. S. (2013). Türk ceza kanununda yer alan bilişim alanındaki suçlar ve karşılaşılan sorunların yargı kararları ışığında değerlendirilmesi. *İÜHFM C. LXXI,* S. 1, s. 891-890, Erişim Bilgisi: https://dergipark.org.tr/tr/download/article-file/97790 [Erişim Tarihi: 3 Ocak 2024].

Mavi Vatan. (2023). "TSK siber savunma merkezi (SİSAMER) projesi". Erişim Bilgileri: https://mavivatan.net/tsk-siber-savunma-merkezi-sisamer-projesi/ [Erişim Tarihi: 03.10.2023].

NATO İşbirlikçi siber savunma mükemmeliyet merkezi. (t.y.). Tallinn El Kitabı. Erişim Bilgileri: https://ccdcoe.org/research/tallinn-manual/ [Erişim Tarihi: 14 Aralık 2023].

Ntv. (18 Aralık 2023). "İran'daki siber saldırıları İsrailli grup üstlendi". Erişim Bilgileri: https://www.ntv.com.tr/dunya/irandaki-siber-saldirilari-israilli-grup-ustlendi,Odg4fI8dVUqTvGB2nSiumQ [Erişim Tarihi: 25 Aralık 2023].

Orak, M. (2021). Siber ordular ve siber savaşlar. *Kaytek Dergisi*, 3(2), s. 214-226, Erişim Bilgisi: https://dergipark.org.tr/en/download/article-file/2194137 [Erişim Tarihi: 13 Ekim 2023].

Oymak, H. (2022). Kamuoyunda dezenfornasyon yasası olarak bilinen, 7418 sayılı "Basın kanunu ile bazı kanunlarda değişiklik yapılmasına dair kanun' un getirdikleri. *Yeni Medya Dergisi,* Güz (13), s. 504-514, Erişim Bilgisi: https://dergipark.org.tr/tr/download/article-file/2860682 [Erişim Tarihi: 10 Kasım 2023].

Öncü, A.S. ve Cevizliler, E. (2013). Avrupa bütünleşmesi için önemli bir adım: ''Avrupa Konseyi'' ve Türkiye'nin konseye üyeliği meselesi. *Akademik Bakış*, 7 (13), s. 15-44, Erişim Bilgisi https://dergipark.org.tr/tr/download/article-file/73830 [Erişim Tarihi: 1 Kasım 2023].

Özel, C. (2007). 5651 sayılı internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun üzerine düşünceler. Erişim Bilgisi:

https://www.hukuki.net/hukuk/index.php?article=2165 [Erişim Tarihi: 19 Kasım 2023].

Özgür Kocaeli Gazetesi. (11 Ocak 2013). "Köle bilgisayar şebekesi çökertildi". Erişim Bilgileri: https://www.ozgurkocaeli.com.tr/haber/4376634/kole-bilgisayar-sebekesi-cokertildi [Erişim Tarihi: 12 Kasım 2023].

Özkaya, Y. (2022). 5651 sayılı kanun kapsamında suç işlenmesinin önlenmesi amacıyla internet erişiminin engellenmesi. *Bilişim Hukuku Dergisi* (1). s.81-140, Erişim Bilgisi: https://dergipark.org.tr/en/download/article-file/1748691 [Erişim Tarihi: 14 Kasım 2023].

Paltacı, B.M. (2022). Ukrayna-Rusya savaşı bağlamında siber güvenlik ekosisteminde yaşanan gelişmeler ve değerlendirmeler. *Orta Doğu Ve Orta Asya-Kafkaslar Araştırma Ve Uygulama Merkezi Dergisi*, 2(2), s.1-19. Erişim Bilgisi: https://dergipark.org.tr/tr/pub/odak/issue/74381/1227279 [Erişim Tarihi: 2 Aralık 2023].

Polat, A. C. ve Karakaş, B. (2023). *A'dan z'ye siber güvenlik.* 1.Baskı, İstanbul: Ezgi Matbaacılık.

Robinson, N. (2016). NATO: Siber savunmada vites değiştiriyor. Natoreview. Erişim Bilgileri: https://www.nato.int/docu/review/tr/articles/2016/06/08/nato-siber-savunmada-vites-degistiriyor/index.html [Erişim Tarihi: 11 Aralık 2023].

Saada, M. A. ve Turan, Y. (2021). Israeli-Palestinian cyber conflict, *Eskişehir Osmangazi Üniversitesi İİBF Dergisi*, 16(1), s. 186 – 204, Erişim Bilgisi: https://dergipark.org.tr/tr/pub/oguiibf/issue/60025/869178 [Erişim Tarihi: 20 Aralık 2023].

Sağıroğlu, Ş. ve Akleylek., V. (2022). Siber güvenlik ve savunma. Siber güvenlik ontolojisi, tehditler ve çözümler. [Retrieved from https://bilgiguvenligi.org.tr/BGD/SiberGuvenlikSavunmaKitapSerisi_No_6.pdf] [Erişim Tarihi: 4 Kasım 2023].

Saygılı, S., & Koyuncu, M. Ücretsiz ve açık kaynak kodlu araçlar kullanılarak geliştirilen ağ güvenlik açığı tarayıcısı. Erişim Bilgileri: https://savassaygili.com/wp-content/uploads/2016/01/savenum-sunumu.pdf [Erişim Tarihi: 23 Aralık 2023].

Schwimmer, W. (2001). The future path of Turkey within the council of Europe, *Journal Of Internatıonal Affairs* 6 (2), Erişim Bilgisi: https://dergipark.org.tr/en/download/article-file/816828 [Erişim Tarihi: 4 Kasım 2023].

Sert, N.Y. (2012). Online aktivizm araçları yoluyla oluşturulan etkilerin metafor kullanılarak açıklanması. *Akdeniz İletişim Dergisi,* s.126-140, Erişim Bilgisi: https://dergipark.org.tr/tr/download/article-file/788670 [Erişim Tarihi: 2 Ocak 2024].

Sezgin, A.A. (2021). TBMM, Avrupa Konseyi ve insan hakları. *İnsan Hakları Araştırma ve Uygulama Merkezi ve UNESCO Felsefe ve İnsan Hakları Kürsüsü Bülteni*, Maltepe Üniversitesi. (10), s. 6-7. Erişim Bilgisi: http://acikerisim.maltepe.edu.tr/xmlui/bitstream/handle/20.500.12415/8480/TBMM%20Avrupa%20Konseyi%20ve%20%c4%b0nsan%20Haklar%c4%b1.pdf?sequence=1&isAllowed=y [Erişim Tarihi: 4 Eylül 2023].

Taşkın, C. (2018). *Ağ Teknolojileri ve Telekomünikasyon*. 4.Basım, İstanbul: Pusula 20 Teknoloji ve Yayıncılık.

T.C. Cumhurbaşkanlığı. (2020). Dijital Dönüşüm Ofisi. Erişim Bilgileri: https://cbddo.gov.tr/projeler/#3166 [Erişim Tarihi: 2 Aralık 2023].

T.C. Resmî Gazete, (1 Mart 1926). 765 sayılı kanun. Erişim Adresi: https://www.mevzuat.gov.tr/mevzuatmetin/5.3.765.pdf [Erişim Tarihi: 11 Ekim 2023].

T.C. Resmî Gazete, (26 Kasım 1959). 7376 sayılı kanun. "Suçluların İadesine Dair Avrupa Sözleşmesi". Erişim Adresi: https://diabgm.adalet.gov.tr/arsiv/sozlesmeler/coktaraflisoz/ak/turkce/024_tur.pdf [Erişim Tarihi: 10 Ekim 2023].

T.C. Resmî Gazete, (14 Haziran 1991). 3756 sayılı kanun. Erişim Adresi: https://www.resmigazete.gov.tr/arsiv/20901.pdf [Erişim Tarihi: 19 Ekim 2023].

T.C. Resmî Gazete, (11 Aralık 1994). 22138 sayılı çocuk haklarına dair sözleşmenin onaylanmasının uygun bulunduğu hakkında kanun. Erişim Bilgileri: https://www5.tbmm.gov.tr/tutanaklar/KANUNLAR_KARARLAR/kanuntbmmc078/kanuntbmmc078/kanuntbmmc07804058.pdf [Erişim Tarihi: 10 Ekim 2023].

T.C. Resmî Gazete, (26 Eylül 2004). 5237 sayılı Türk ceza kanunu. Erişim Adresi: https://www.resmigazete.gov.tr/eskiler/2004/10/20041012.htm [Erişim Tarihi: 15 Ekim 2023].

T.C. Resmî Gazete, (4 Mayıs 2007). 5651 sayılı internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun. Erişim Adresi: https://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm [Erişim Tarihi: 20 Ekim 2023].

T.C. Resmî Gazete, (07 Mayıs 2010). 5982 sayılı kanun. Erişim Adresi: https://www.resmigazete.gov.tr/eskiler/2010/05/20100513-1.htm [Erişim Tarihi: 7 Ekim 2023].

T.C. Resmî Gazete, (2013a) Bakanlar Kurulu kararı. Erişim Adresi https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm [Erişim Tarihi: 13 Ekim 2023].

T.C. Resmî Gazete, (2013b). Siber olaylara müdahale ekiplerinin kuruluş, görev ve çalışmalarına dair usul ve esaslar hakkında tebliğ. Erişim Adresi:

https://dergipark.org.tr/en/download/article-file/816828 [Erişim Tarihi: 11 Ekim 2023].

T.C. Resmî Gazete, (2014). Sanal ortamda işlenen suçlar sözleşmesi. Erişim Adresi: https://www.resmigazete.gov.tr/eskiler/2014/08/20140809-5-1.pdf [Erişim Tarihi: 5 Aralık 2023].

T.C. Resmî Gazete, (07 Nisan 2016). 6698 sayılı kişisel verilerin korunması kanunu. Erişim Adresi: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5 [Erişim Tarihi: 11 Kasım 2023].

T.C. Resmî Gazete, (05 Mayıs 2016). 6706 sayılı kanun. Erişim Adresi: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6706.pdf [Erişim Tarihi: 11 Ekim 2023].

T.C. Resmî Gazete, (10 Temmuz 2018). 2018/ 30474 sayılı 1 sayılı Cumhurbaşkanlığı kararnamesi. Erişim Adresi: https://www.mevzuat.gov.tr/MevzuatMetin/19.5.1.pdf [Erişim Tarihi: 12 Kasım 2023].

T.C. Resmî Gazete, (07 Eylül 2018). 703 sayılı Khk. Erişim Adresi: https://www.resmigazete.gov.tr/eskiler/2018/07/20180709M3-1.pdf [Erişim Tarihi: 11 Kasım 2023].

T.C. Resmî Gazete, (13 Ekim 2022). 7418 sayılı kanun. Erişim Adresi: https://www.resmigazete.gov.tr/eskiler/2022/10/20221018-1.htm#:~:text=MADDE%20217%2FA%2D%20(1,y%C4%B1la%20kadar%20hapis%20cezas%C4%B1yla%20cezaland%C4%B1r%C4%B1l%C4%B1r [Erişim Tarihi: 11 Ekim 2023].

Tezcan, D. (2019). Bilişim suçlarında uluslararası adli yardımlaşma. Ceza Hukuku ve Veri Koruma Boyutuyla Bilişim Hukuku Sempozyumu, *Yaşar Hukuk Dergisi*, C.1 S.2, s. 287-294.

Tuncay, İ. (2018). Avrupa Suç Sorunları Komitesi (CDPC). Adalet Bakanlığı Uluslararası Hukuk Bülteni. Erişim Bilgileri: https://diabgm.adalet.gov.tr/Resimler/Dokuman/2622020105111i_tuncay.pdf [Erişim Tarihi: 22 Eylül 2023].

Turan, H. (2023). Bilişim suçlarında uluslararası adli yardımlaşma: Hukuki Açıdan Türkiye Üzerine Bir Değerlendirme. *Avrasya 7th International Conference on Social Sciences*– Budapest, 704-711.

Turan, M. ve Külcü, Ö. (2014). Türkiye'de bilişim suçlarının tanımlanması ve yaşanan ihlallere yönelik içerik analizi. *Türk Kütüphaneciliği* 28, 1, s.18-46, Erişim Bilgisi: https://dergipark.org.tr/en/pub/tk/issue/48826/621977 [Erişim Tarihi: 1 Ocak 2024].

Tübitak. (2023). Bilgem. Erişim Bilgileri: https://bilgem.tubitak.gov.tr/siber-guvenlik/ [Erişim Tarihi: 3 Kasım 2023].

Ulaştırma ve Altyapı Bakanlığı. (2013), Ulusal siber güvenlik stratejisi ve 2013-2014 eylem planı. Erişim Adresi: https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf [Erişim Tarihi: 12 Aralık 2023].

Ulaştırma ve Altyapı Bakanlığı. (2020), Ulusal siber güvenlik stratejisi ve eylem planı (2020-2023). Erişim Bilgileri: https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf [Erişim Tarihi: 5 Aralık 2023].

Uslu, U. (4 Haziran 2016). "Türk ordusunun yeni "kuvveti" siber savunma". Erişim Bilgileri : https://www.aa.com.tr/tr/turkiye/turk-ordusunun-yeni-kuvveti-siber-savunma/584061# [Erişim Tarihi: 27 Kasım 2023].

Ünver, G.N., (2023). *Siber güvenlik politikalarının karşılaştırmalı bir analizi: Türkiye Ve İngiltere örneği.* Livre de Lyon yayıncılık. Erişim Bilgileri: https://play.google.com/books/reader?id=OQDZEAAAQBAJ&pg=GBS.PA25&hl=tr [Erişim Tarihi: 8 Ekim 2023].

Ünver, M. Canbay, C. ve Özkan, H. B. (2011). *Kritik altyapıların korunması*. 1. Baskı, BTK Yayınları.

Wood, K. (7 Mart 2023). "Colonial pipeline fidye yazılımı saldırısına siber güvenlik politikasının yanıtları". Erişim Bilgileri: https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/ [Erişim Tarihi: 17 Aralık 2023].

Yalçın, H. B. (2017). *Ulusal güvenlik stratejisi Abd, İngiltere, Fransa, Rusya, Çin.* İstanbul: Seta Kitapları. [Retrieved from https://setav.org/assets/uploads/2017/04/UGS_pdf.pdf]

Yegen, C. (2014). Dijital aktivizmin bir türü olarak hacktivizm ve "redhack*"*. *Intermedia International E-Journal*, 1(1), 118-132.

Zetter, K. (21 Mart 2013). Logic bomb set off South Korea cyberattack. Erişim Bilgileri: https://www.wired.com/2013/03/logic-bomb-south-korea-attack/ [Erişim Tarihi: 8 Kasım 2023].

Zetter, K. (3 Kasım 2014). An unprecedented look at stuxnet, the world's first digital weapon. Erişim Bilgileri: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ [Erişim Tarihi: 8 Kasım 2023].

Zeydan, Ö. (2006). Kişisel bilgisayarlar ve internet güvenliği. XI." Türkiye'de İnternet" Konferansı, TOBB Ekonomi ve Teknoloji Üniversitesi, Ankara.

10. ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Elif Tuğçe ŞİŞMAN

Uyruğu : Türkiye Cumhuriyeti

Doğum Yeri ve Tarihi : Osmancık/ 19.12.1988

Telefon :

e-mail : eliftugce188@gmail.com

EĞİTİM

Derece		Adı, İlçe, İl	Bitirme Yılı
Lise	:	**Eryaman Lisesi, Etimesgut, Ankara**	**2005**
Üniversite	:	**Kocaeli Üniversitesi, Umuttepe, Kocaeli**	**2013**
Yüksek Lisans	:	**Polis Akademisi Güvenlik Bilimleri Enstitüsü, Gölbaşı, Ankara**	**2016**

İŞ DENEYİMLERİ

Yıl	Kurum	Görevi
2016-halen	**Emniyet Genel Müdürlüğü**	**Büro Amiri**