Gazi Üniversitesi
Fen Bilimleri Dergisi
PART C: TASARIM VE TEKNOLOJİ

Gazi University
Journal of Science
PART C: DESIGN AND TECHNOLOGY

GU J Sci, Part C, 11(2): 347-366 (2023)

Türkiye'de Yapılan Siber Güvenlik Faaliyetlerinin ve Eğitim Çalışmalarının Değerlendirilmesi

Hüseyin ÇAKIR[1], Murat TAŞER[2,*]

[1]*Gazi University Faculty of Education, Department of Computer Education and Instructional Technology, Yenimahalle/ANKARA*
[2]*Pamukkale University Hospitals, Chief Directorate, Pamukkale/DENİZLİ*

Article Info

Review article
Received: 22/08/2022
Revision: 08/10/2022
Accepted: 25/10/2022

Keywords

Cyber Security
Cyber Law
Cyber Attacks
Cyber Crimes
Critical Infrastructures

Makale Bilgisi

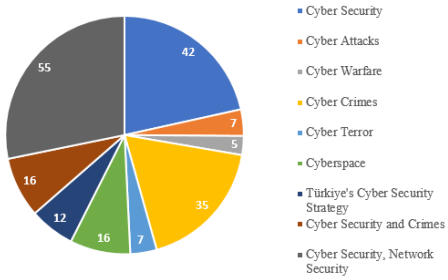
Derleme makalesi
Başvuru: 22/08/2022
Düzeltme: 08/10/2022
Kabul: 25/10/2022

Anahtar Kelimeler

Siber Güvenlik
Siber Hukuk
Siber Saldırı
Siber Suç
Kritik Altyapılar

Grafik Özet (Graphical/Tabular Abstract)

Günümüzde giderek artan siber suçlar, ülkelerin karşı stratejiler geliştirmesini gerektirmiştir. Türkiye'nin de güvenlik açığı oluşmaması adına siber güvenlikte hangi aşamada olduğunu tespit etmesi gerekmektedir (Today, increasing cybercrimes have required countries to develop counter-strategies. Turkey also needs to determine where it stands in cyber security in order to avoid a security gap).



Şekil A: *Çalışmada incelenen yayınlar/**Figure A**:* Publications examined in the study

Önemli noktalar(Highlights)

- *Siber güvenlik sistemleri takibi için daha fazla personel istihdam edilmelidir. / More personnel should be employed to monitor cyber security systems.*
- *Son zamanlarda yapılan çalışmalar Türkiye'de siber güvenlik farkındalığını üst seviyelere taşımıştır. / Recent studies have raised cyber security awareness in Turkey to high levels.*
- *Alınacak önlemlerle, kamu bilişim uzmanlarıyla özel kuruluşların ortak faaliyetlerde bulunmaları kolaylaştırılmalıdır. / It should be facilitated for public informatics experts and private organizations to engage in joint activities through solutions.*

Amaç (Aim): *Araştırmada, Türkiye'de siber güvenlik alanında son yirmi yılda yapılan çalışma, strateji ve politikaların incelenmesi, olumlu ve olumsuz yönlerin ortaya çıkarılması amaçlanmıştır. / This study aims to examine the studies, strategies and policies in the field of cyber security in Turkey in the last two decades and to reveal the positive and negative aspects.*

Özgünlük (Originality): *Çalışmada Türkiye'de siber güvenlik alanındaki tehditler ve geliştirilmesi gereken alanlar değerlendirilmiştir. Eksikliklerin tespiti açısından yol gösterici bir çalışma olmuştur. / The study evaluated the threats and areas that need to be improved in the field of cyber security in Turkey. It has been a guiding study in terms of identifying deficiencies.*

Bulgular (Results): *Türkiye'de siber Güvenlik alanında 2000'li yıllarda alınan yetersiz kısmi önlemlerden sonra 2012 yılında "Siber Güvenlik Kurulu" kurularak ilk ciddi önlemler alınmaya başlanmıştır. Ancak bilişim suçlarının mevzuat boyutu hala yeterince incelenmemiştir. / After the inadequate partial measures taken in the field of cyber security in Turkey in the 2000s, the first serious measures were taken by establishing the "Cyber Security Board" in 2012. However, the legislative dimension of cybercrimes has still not been sufficiently examined.*

Sonuç (Conclusion): *Akademik çalışmaların artması, yerli ve milli yazılımların yaygınlaşması, ASELSAN ve STM gibi firmaların donanım-yazılım ürünlerinin ortaya çıkması, Türkiye'nin yakın gelecekte siber güvenlikte iyi bir seviyede olacağına işaret ediyor. / Increasing academic studies, the expansion of domestic and national software, and the emergence of hardware-software products by companies such as ASELSAN and STM indicate that Turkey will be at a good level in cyber security in the near future.*

*Corresponding author, e-mail: mtaser@pau.edu.tr
DOI: 10.29109/gujsc.1165131

GU J Sci, Part C, 11(2): 347-366 (2023)

Gazi Üniversitesi
Fen Bilimleri Dergisi
PART C: TASARIM VE TEKNOLOJİ

Gazi University
Journal of Science
PART C: DESIGN AND TECHNOLOGY

http://dergipark.gov.tr/gujsc

Türkiye'de Yapılan Siber Güvenlik Faaliyetlerinin ve Eğitim Çalışmalarının Değerlendirilmesi

Hüseyin ÇAKIR[1], Murat TAŞER[2,*]

[1]*Gazi University Faculty of Education, Department of Computer Education and Instructional Technology, Yenimahalle/ANKARA*
[2]*Pamukkale University Hospitals, Chief Directorate, Pamukkale/DENİZLİ*

Makale Bilgisi

Derleme makalesi
Başvuru: 22/08/2022
Düzeltme: 08/10/2022
Kabul: 25/10/2022

Anahtar Kelimeler

Siber Güvenlik
Siber Hukuk
Siber Saldırı
Siber Suç
Kritik Altyapılar

Öz

Araştırmada, Türkiye'de siber güvenlik alanındaki son yirmi yılda yapılan çalışmaların derlenmesi, siber güvenlik strateji ve politikalarının incelenmesi ve elde edilen sonuçlar ile artı ve eksi tarafların belirlenmesi amaçlanmıştır. Araştırmanın amacı çerçevesinde, 2001 yılından günümüze siber güvenlik alanında yayımlanmış kitaplar, Ulusal tez merkezi, Sobiad, Turcademy ve Dergipark'ta yayımlanan tez, dergi ve makaleler ile Türkiye'nin Siber Güvenlik Strateji ve Politikaları incelenmiştir. Çalışmada akademik alanda hangi üniversitelerde siber güvenlik bölümlerinin kurulduğu ve hangi programlarda eğitim öğretim faaliyetinde bulunulduğuna da değinilmiştir. Ayrıca siber saldırılardan en çok etkilenen kurumlar, Türkiye'de siber güvenlik alanında öncü kurum ve kuruluşlara değinilmiş ve bunların politikaları üzerinde durulmuştur. Yine Türkiye'de eksikliği hissedilen önemli konulardan birisi olan siber güvenliğin mevzuatı boyutu ele alınmış, siber güvenlikle alakalı Cumhurbaşkanlığı Mevzuat Bilgi Sistemi üzerinden Kanunlar ve Yönetmelikler incelenmiştir. Son olarak elde edilen önemli sonuçlar, kişisel olarak siber güvenlik alanında yapılması gerekenler ve Türkiye'de siber güvenlik alanındaki tehditler değerlendirilmiştir. Çalışma siber güvenlik alanındaki eksikliklerin tespit edilmesi açısından önemli bir çalışma olmuştur.

Evaluation of Cyber Security Activities and Training Studies in Turkey

Article Info

Review article
Received: 22/08/2022
Revision: 08/10/2022
Accepted: 25/10/2022

Keywords

Cyber Security
Cyber Law
Cyber Attacks
Cyber Crimes
Critical Infrastructures

Abstract

In the research, it is aimed to compile the studies conducted in the last twenty years in the field of cyber security in Turkey, to examine the cyber security strategies and policies, and to determine the positive and negative sides with the results obtained. Within the scope of the research, the books published in the field of cyber security since 2001, the theses in the national thesis center, the articles published in Sobiad, Turcademy and Dergipark, and Türkiye's Cyber Security Strategies and Policies were examined. In the study, it was also mentioned in which universities cyber security departments were established in the academic field and in which programs they were engaged in education and training activities. In addition, the institutions most affected by cyberattacks, the leading institutions and organizations in the field of cyber security in Türkiye were mentioned and their policies were emphasized. Again, the legal dimension of cyber security, which is one of the important issues that are felt to be lacking in Türkiye, has been discussed, and Laws and Regulations related to cyber security have been examined through the Presidential Legislation Information System. Finally, the important results, what needs to be done personally in the field of cyber security and threats in the field of cyber security in Turkey were evaluated. The study has been an important study in terms of detecting the deficiencies in the field of cyber security.

1. GİRİŞ (INTRODUCTION)

Gelişen bilgisayar teknolojisiyle birlikte hayatın her alanı gittikçe daha kolay hale gelmektedir. Ancak teknoloji doğru kullanıldığında kişilerin hayatını kolaylaştırdığı gibi yanlış kullanıldığında da zarar verebilmektedir. İnsanlar bu olumsuz etkilere maruz kalmamak ve kişisel güvenliklerini sağlamak adına alışılagelmiş yöntemlerin de ötesinde veri güvenliği tedbirlerine ihtiyaç duyar hale gelmişlerdir. Kişisel verilerin koruma altına alınması ise siber ortamı tanımakla mümkündür [1].

Dijitalleşen dünyada her geçen gün yeni bir gelişmenin duyurulması, internet kullanımının farklı ortamlarda fazlalaşmasıyla, teknolojinin

*Corresponding author, e-mail: mtaser@pau.edu.tr
DOI: 10.29109/gujsc.1165131

önemi bir kat daha artmıştır. Bireylerin güvenilir ve doğru olmayan teknolojileri bilinçsiz kullanımı, siber suçları gün geçtikçe çoğaltmış, siber güvenlik, siber dünya, siber güç, siber uzay ve kişisel bilgi güvenliği gibi kavramların önemini artırmıştır [2].

Teknolojinin hızla gelişmesiyle birlikte her alanda internet kullanan fakat veri güvenliği konusunda yeterli bilgisi olmayan bilinçsiz bir toplum yetişmektedir. İnsanlar farkında olmadan, teknolojik aletler vasıtasıyla suç işlemeye veya suç oluşturacak unsurlar meydana getirmeye başlamıştır. Sürekli gelişen siber güvenlik ve siber suçlar konularında paralelinde yasal düzenlemelerinde geliştirilmesi gerekmektedir. Özellikle siber ortamda işlenen suçların niteliği ve hangi alanlarda kişiye yaptırım yapılabileceği konularının üzerinde daha çok çalışılması gerekmektedir. Bunun için de bu zamana kadar yapılan yasal düzenlemelerin artıları ve eksilerinin ortaya konulması önemlidir [3].

Konuya ulusal güvenlik açısından bakıldığında, siber caydırıcılık ve siber suçların artarak devam etmesi ülkelerin karşı strateji geliştirme gereksinimini doğurmuştur. Siber güvenlik alanında strateji geliştirme ve ihtiyaç duyulan çalışmaların yapılması açısından Türkiye'nin diğer ülkelere göre hangi aşamada olduğu ve bu noktada yaşanan ulusal sorunların belirlenmesi gerekmektedir. Ayrıca siber güvenlik alanında kurum ve kuruluşların aldıkları önlemlerin ne olduğu, daha çok hangi kurumların etkilenebileceği ortaya konulmalıdır. Akademik anlamda üniversitelerin farkındalık yaratmak adına ne gibi çalışmalar yapması gerektiği de tespit edilmelidir.

Araştırmada, Türkiye'de akademik olarak şimdiye kadar siber güvenlik alanında yapılan çalışmaların yanı sıra gelecek dönem siber güvenlik stratejileri ve politikaları planlamalarına dair çalışmalar da incelenmiştir. Araştırma, bu konuyla alakalı daha önce yayınlananlardan farklı olarak, yayımlanan tüm çalışmaların derlenmesi açısından önem arz etmektedir. Çalışmada öncelikli olarak bazı önemli kavramların tanımları ele alınmıştır.

1.1. Siber Güvenlik (Cyber Security)

Siber güvenlik, siber saldırılara ve uluslararası tehditlere karşı savunma sistemlerinin geliştirilmesidir. Ulaştırma Denizcilik ve Haberleşme Bakanlığı siber güvenlik kavramını, "Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin 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" olarak tanımlamıştır [4].

Siber ortamda oluşan saldırılar bazen ulusal siber güvenliği tehdit edebilmektedir. Geçmişte yüz yüze yapılan savaş artık yerini dijitalleşen ve kodlar üzerinden yapılan saldırılara bırakmıştır. Siber saldırılarda ilk hedef alınan yerler ise kritik altyapılardır. Kişisel veriler de dâhil olmak üzere bilginin gizliliğinin, bütünlüğünün veya erişilebilirliğinin bozulması durumunda; ekonomik zarar oluşmasına, kritik tesislerin işlevlerini yerine getirmesini engellenmesine, kamu düzenini bozulmasına veya can kaybına yol açılmasına sebebiyet veren bilişim altyapı sistemlerine kritik altyapılar denir. Ulusal siber güvenliğin sağlanması ve kritik altyapıların korunması ülkelerin ana görevlerinden biri haline gelmiştir. Bu yüzden son yıllarda uluslararası düzeyde siber güvenlik çalışmalarına ağırlık verilmektedir [5].

Türkiye'de siber güvenlik alanında yapılan çalışmalar ise henüz yeterli seviyede değildir. Bu durum 2020 yılı için Türkiye'nin siber güvenlik alanında ulusal siber güvenlik indeksinde 45. sırada olmasından anlaşılmaktadır [6]. Bu da Türkiye'nin bu konuda birçok ülkenin gerisinde kaldığını göstermektedir. Araştırmada kurumların siber güvenlik alanındaki çalışmaları incelenmiş ve yeterlilikleri sorgulanmıştır. Ek olarak Türkiye'de siber güvenlik alanında yayınlanmış akademik çalışmaların incelenmesi ve eksikliklerin belirlenmesi hedeflenmiştir. Araştırma bu anlamda eksik olan alanların tespit edilmesi adına önemli bir çalışmadır. Konuyla ilgili incelemelere geçmeden önce aşağıda siber güvenlik alanındaki tehditler hakkında bilgi verilmiştir.

1.2. Siber Suç ve Geçmişten Günümüze Suç Türleri (Cybercrime and Types of Crime from Past to Present)

Bilgisayar, cep telefonu, kredi kartı gibi gündelik yaşamda sıklıkla kullanılan araçlarla da işlenebildiği için geniş bir alana yayılan siber suçların, niteliğini ve sınırlarını belirlemek zor olmaktadır. Bu yüzden siber suçlara dair literatürde birçok tanım bulunmaktadır [7]. Siber suç kavramı, global elektronik ağlar aracılığıyla yürütülen yasa dışı olan veya belirli bir tarafça kabul edilen bilgisayar faaliyetleri" olarak açıklanırken, aynı zamanda sosyal normları ve kuralları ihlal eden yasa dışı eylemler, sapkınlıklar ve sakıncalı eylemler olarak da karşımıza çıkmaktadır [8].

Wall'a göre siber suçlar; izinsiz giriş yapma şeklinde (Virüs), aldatma ve hırsızlık yoluyla (kredi kartı dolandırıcılığı), cinsel bir materyalle (porno ve

müstehcenlik) ve bireylere zarar verme yoluyla (zorbalık, terör ve taciz) olmak üzere dörde ayrılmıştır [9]. Tablo1'de detayları verilen bir başka çalışmada, siber suçlar şu şekilde tanımlanmıştır [10]:

Tablo 1. Siber suç türleri (Types of cybercrime)

Suç Türü	Tanımı
Dolandırıcılık	Kişisel fayda ve kazanç için izinsiz, yetkisiz olarak çıktıları değiştirmek, yok etmek, kötüye kullanmak, verileri değiştirmek.
Hırsızlık	Veri ve yazılım hırsızlığı.
Lisanssız yazılım kullanımı	Kopya yazılım, korsan yazılım.
Siber Terörizm	Sanal ortamda teröre yönlendirmek.
Özel iş	Menfaat için bilgi işlemleri izinsiz kullanmak.
Kişisel verilerin kötüye kullanımı	Resmi olmayan kayıtları bilgisayar ortamında kişisel çıkar amaçlı kullanım.
Hacklemek	Yetkisiz erişimle bilgisayar sistemini ele geçirmek
Sabotaj	Kasıtlı olarak bilgisayara zarar vermek.
Pornografi	İzinsiz indirilen pornografik verilerin tanıtılması.
Casusluk	Kişisel verileri çevrim içi yollarla elde edip kişisel bilgisayarlara saldırmak.
Virüs	Bilgisayar sistemini bozmak için yapılan zararlı yazılım.
Çevrim içi hizmet reddi	Çevrim içi bilgisayara zarar vermek için e-posta göndermek virüslerle bilgisayarın kullanılması.

Ulusal Beyaz Yaka Suçları Merkezinin 2013 yılı raporunda siber suç olarak altıya ayrılmıştır:

- Sosyal zorbalık (Cyber-Bullying),
- İnternet sahtekârlığı (Internet Fraud),
- Siber takip (Cyberstalking),
- Sosyal medyanın suç amaçlı kullanımı (Criminal use of Social Media),
- Sağlık hizmet dolandırıcılığı (Healthcare Fraud),
- Kara para aklama (Money Laundering).

ABD doktrininde on iki siber suç türüyle en kapsamlı sınıflandırma yapılmıştır. Bunlar; hizmetlere veya verilere karşı işlenen hırsızlıklar, mülkiyete karşı hırsızlıklar, maddi hırsızlıklar, bankamatik kartı hırsızlıkları, manyetik kart şifre eylemleri, giriş ihlalleri, insan hatalarından kaynaklanan ihlaller, veri sahtekârlığı, evrak sahtekârlığı, sır ihlalleri, sabotaj ve gasp olarak tanımlanmıştır [11].

Bilişim Suçları Türk Ceza Kanununda ise şu şekilde belirtilmiştir: Bilişim sistemine hukuka aykırı olarak girme, kalmaya devam etme ve veri nakli yapma, sistemi engelleme, bozma, verileri değiştirme ya da yok etme, banka veya kredi kartlarının kötüye kullanma [12].

1.3. Siber Saldırı Tanımı ve Örnekleri (Cyber Attack Definition and Examples)

Alkan siber saldırıyı "hedef seçilen şahıs, şirket, kurum, örgüt ve devlet gibi yapıların bilgi ve iletişim sistemlerine ve kritik altyapılarına yapılan planlı ve koordineli saldırılar" olarak tanımlamıştır [13]. Ulaştırma Denizcilik ve Haberleşme Bakanlığına göre ise siber saldırı; "Ulusal siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler" olarak tanımlanmıştır [4].

Siber saldırılar sadece bilgisayar sistemine sızma, zarar verme ve bilgi çalma şeklinde olmamaktadır. Aynı zamanda kritik askeri, haberleşme, enerji ve ulaşım sistemlerine zarar verme/ele geçirme yöntemleriyle asimetrik ve hibrit bir savaş haline gelmiştir. Günümüzde artan bu saldırılar, yakın geçmişten itibaren devletler tarafından da kabul edilmeye başlanmıştır. Bununla ilgili yapılan akademik çalışmaların son yıllarda giderek arttığı

gözlenmektedir. Gerek özel ve gerek kamu kuruluşları olmak üzere farkındalık eğitimleri verilmeye ve bu konuda deneyimli personeller yetiştirilmeye devam edilmektedir. Eylül 2016'da yapılan toplantıda Türkiye'nin dört yıllık süreçte nasıl bir siber güvenlik çalışması yapacağı, 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ile beş ana eylem altında kırk bir alt eylem ile değerlendirilmiştir. Sonuç olarak, siber güvenliğin ulusal güvenlikle aynı olduğu, siber uzayda yer alan teknolojilere karşı önlemler alınması ve etkinliklerin artırılması kararı alınmıştır.

Siber saldırı yöntemlerini, internet üzerinden saldırı yoluyla, donanım/yazılım hataları oluşturma yoluyla ve kritik ağ sistemlerine erişim yoluyla olmak üzere üç ana başlıkta toplamak mümkündür. Bilinen diğer yöntemler kısaca şunlardır [2]:

- Veri dolandırıcılığı (Data Diddling),
- Yanlış veri girişi, kritik verilerin veya kayıtların değiştirilmesi,
- Salam tekniği (Salami Techniques): Bankacılıkta küsuratlı rakamların başka bankaya aktarılması,
- Süper darbe (Super Zapping): Ağ kullanıcılarının şifrelerini çalma yöntemiyle normal güvenlik denetimlerini devre dışı bırakacak kadar ayrıcalıklara sahip olmak,
- Truva atı (Casus Yazılımlar): Arka kapılar kullanarak sisteme erişmek, keylogger gibi programlarla şifrelere, klavye verilerine, kişisel verilere erişmek,
- Zararlı yazılımlar,
- Mantık Bombaları (Logic Bombs): Program içerisine zararlı kod ekleyip sistemi veya ağları çökertmek veya kullanılamaz hale getirmek,
- Oltalama (Phishing): Sahte web sitesinden alışveriş yapılması sonucu kredi kartı bilgilerini ele geçirmek,
- Bukalemun (Chamelon): Zararsız gibi görünen programlarla bilgisayardaki tüm gizli dosyaları ve şifreleri ele geçirmek,
- İstem dışı elektronik posta (Spam): Web sayfalarından elde edilen bilgilerle alıcılara ticari amaçlı istenmeyen e-posta göndermek,
- Çöpe dalma (Scavenging): Sistemdeki silinmiş bilgileri geri getirmek,
- Yerine geçme (Masquerading): Hileyle erişim yetkisi olan birinin yerine geçmek,
- Sistemi kırmak (Hacking),
- Sosyal mühendislik: Kişilerin güvenini kazanarak bilgi toplamak tekniklerdir.

Siber saldırıları yapan saldırganlar üç ayrı sınıfta değerlendirilir. Bunlardan ilki amatörlerdir. İnternette hazır kalıplar ve kodlardan derlemeler yaparak, işletim sistemlerine saldırılar yaparlar. Bu tarz saldırganlar başlangıçta kendilerini başarılı gibi gösterseler de hedef bilgisayar veya işletim sistemi hakkında bilgi sahibi değillerdir. Her ne kadar bilgisiz ve donanımsız saldırılar yapsalar da korunmasız bir bilgisayar sistemi üzerinde kalıcı etkiler bırakabilirler. İkincisi; siber korsan olarak da bilinen beyaz, gri ve siyah şapkalı olarak tanımlanan hackerlardır. Hackerlar yeterli bilgiye sahiptir ve istediklerinde çok ciddi zararlara yol açabilirler. Kurum ve kuruluşlar, sistemlerine zarar vermeye çalışan bu tarz hackerlara karşı sistem açıklarını bulan kişilere maddi ödüller vermektedir. Üçüncüsü organize gruplardır. Hedef alınan devletin düşmanları tarafından desteklenirler. Bu siber suçlular, organize bir şekilde bir araya gelerek bilgileri manipüle etmeyi, kurumlara ciddi zararlar vermeyi, istihbarat toplamayı ve sabotaj yapmayı amaçlarlar. İyi eğitimlidirler ve sadece belli hedeflere odaklanırlar. Amacı belli olmayan saldırılara girişmezler [14]. Özellikle üçüncü olarak sayılan organize grupların düzenlediği saldırılar, bazen ülkelerin ulusal güvenliğini tehlikeye sokmaktadır. Ülkelerin bu konuyla ilgili özel olarak kurulmuş/görevlendirilmiş, sürekli denetim ve gözetleme faaliyetlerinde bulunan, acil eylem planları oluşturulmuş kurumlarının bulunması gerekmektedir. Konunun öneminin daha iyi anlaşılabilmesi için Türkiye'de gerçekleşen siber saldırılardan bazıları aşağıda verilmiştir:

<u>2008 yılında kritik tesislerden Bakü-Tiflis-Ceyhan boru hattına siber saldırı</u>

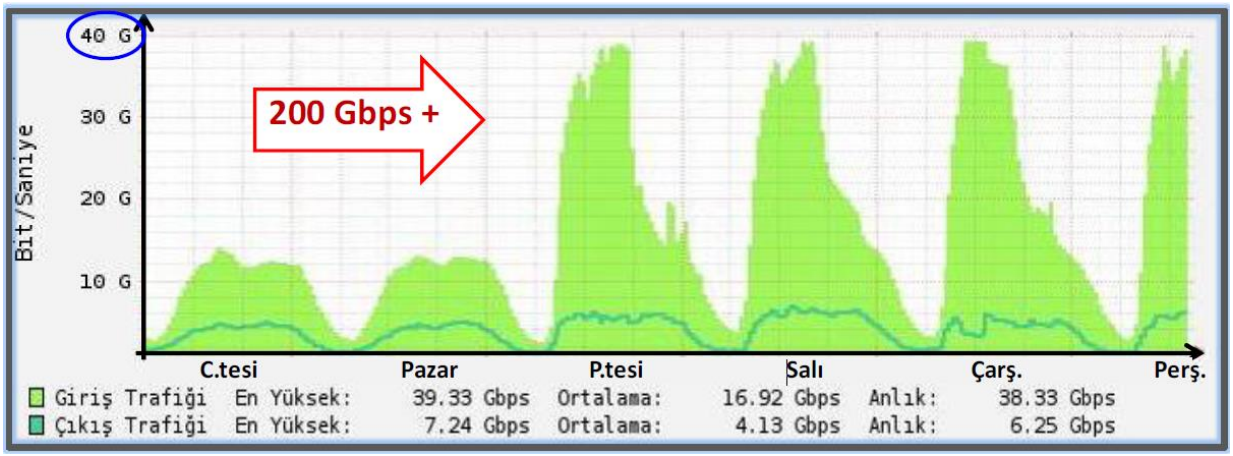
5 Ağustos 2008 tarihinde petrol boru hattında meydana gelen patlamada sabotaj yapılmasından şüphelenilmesi üzerine çalışma yapılmış ve araştırma sonucunda olayın teknik bir arızadan kaynaklandığı duyurulmuştur. Patlama sosyal medyada da siber saldırı olarak anılmıştır. Saldırganların güvenlik kameralarını kullanarak sisteme bağlandığı, boru hattı güvenlik sistemine Windows alarm düzenini değiştiren kötücül yazılım yerleştirerek saldırıyı gerçekleştirdikleri iddia edilmiştir. Alarm çalışmadan basınç artırılıp boru patlatılmıştır. Patlama zamanı ve 60 saat güvenlik kamerası görüntüleri silinmiştir. Patlamanın neden olduğu anlaşılınca sinyal karıştırıcı kullanılarak, kızılötesi olarak ağa bağlanılmıştır. Boru hattında yürüyen siyah üniformalı iki kişi görüntülenmiştir. Saldırının ülkemiz ekonomisine zararı 7,5 milyon dolar, şirket ve ortaklarına zararı 75 milyon dolar ve Azerbaycan'a maliyeti 1 milyar dolardan fazladır [15].

<u>2011 yılı Telekomünikasyon İletişim Başkanlığı (TİB) saldırısı</u>

5651 sayılı kanunun, internette temel hak ve özgürlükleri ihlal ettiğini savunan *Anonymous* adlı grup 09 Haziran 2011 tarihinde kurum sitesine saldırmış, erişimi engelleyerek devre dışı bırakmıştır. Siteye erişim ancak gece yarısından sonra sağlanabilmiştir. Kısıtlamaların kaldırılmasına yönelik bir saldırı olsa da kamuoyunda yer almıştır [16].

2015 – 2016 yılında internet saldırıları

Saldırı ".tr" uzantılı siteler hedef alınarak 14-24 Aralık 2014 ve 12-17 Aralık 2015 tarihlerinde yapılmıştır. Orta Doğu Teknik Üniversitesi (ODTÜ) ve E-Devlet başta olmak üzere bankalar da dâhil birçok kamu kurumu sisteminde yavaşlama ve çökme sorunları oluşmuştur (Şekil 1). Saldırıyı Türkiye'de birçok bilgisayarı ele geçirdiğini söyleyen *Anonymous* grubu üstlenmiştir.



Şekil 1. 12-17 Aralık 2015 tarihi ağ trafiği [16] (Network traffic on December 12-17, 2015)

2015 ülke genelinde elektrik kesintisi

Türkiye tarihinde ilk kez yaşanan bir başka olayda ülke genelinde elektrik kesintisi yaşanmıştır. 31 Mart 2015 tarihinde Türkiye genelinde elektrikler 10 saatten fazla kesilmiştir. Saat 10 sularında Türkiye Elektrik İletim Anonim Şirketinin Ankara Gölbaşındaki ve Sakarya'daki ana ve yedek kontrol odalarındaki bilgisayarlar aynı anda alarm vermiştir. Kısa süre içinde Türkiye'nin elektrik frekans sistemi çökmüştür. Kesintinin ülkenin enterkonnekte sistemine yapılan siber saldırıdan kaynaklandığı öne sürülmüştür [17].

1.4. Araştırmanın Amacı (Purpose of the Research)

Yapılan araştırmalarda Türkiye'de siber güvenlik alanında yeterli sayıda çalışma olmadığı görülmüştür. Eksik noktaların belirlenmesi amacıyla çalışmaların nitelikleri ve özellikleri bakımından derleme yapılmasına ihtiyaç duyulmuştur. Makalede Siber Güvenlik terimi çerçevesinde son yirmi yıldaki yapılan çalışmalar derlenerek, siber güvenlik strateji ve politikalarının incelenmesi ve elde edilen sonuçlar ile Türkiye'de siber güvenlik alanındaki çalışmaların artı ve eksi yönlerinin değerlendirilmesi amaçlanmıştır. Çalışmanın amacına ulaşmak için aşağıda belirtilen alt amaçlar izlenmiştir.

- Türkiye'de siber güvenlik alanında yer alan kurumlar ve çalışmaları nelerdir?
- Siber güvenlik çerçevesinde yapılan yasal düzenlemeler nelerdir?
- Siber güvenlik alanında akademik eğitim faaliyetlerine yönelik çalışmalar nelerdir?
- Türkiye'de yüksek lisans ve doktora seviyesinde siber güvenlik alanında yapılan tez çalışmaları nelerdir? Hangi konular üzerinde çalışılmıştır?
- Siber güvenlik alanında yazılmış olan kitap çalışmaları ve konuları nelerdir?

2. MATERYAL VE METOT (MATERIALS AND METHODS)

Türkiye'de siber güvenlik önemi yeni anlaşılmaya başlanan bir kavramdır. Siber suç, siber saldırı, siber hukuk ve siber uzay gibi konuların işlendiği alandaki akademik çalışmalar son zamanlarda giderek artmaktadır. Kurum ve kuruluşlarda da siber güvenlik konusunda çalışmalar yapılmaya başlanmıştır. Alan yazı incelendiğinde, yeterli çalışma olmadığı, gelişmekte olan bir alan olduğu görülmektedir. Siber güvenlik alanında ilgili yayınlara ulaşılırken, yayımlanmış kitaplar, Ulusal tez merkezi, Sobiad, Turcademy ve Dergipark'ta yayımlanan tez, dergi ve makaleler incelenmiştir. Literatür incelemesinde Siber Saldırı, Siber Savaş, Siber Güvenlik, Siber Suç, Siber Terör ve Siber Uzay anahtar kelimeleri doğrultusunda YÖK Ulusal Tez Merkezinden, 2004 yılından 2021 yılına kadar yayımlanan 104 Yüksek Lisans Tezi ve 9 Doktora

Tezine ulaşılmıştır. Araştırmada bazı tezlere ulaşılamamıştır. Bu tezler istihbarat açısından güvenlik sebebiyle gizlenen Harp Akademisi araştırmalarıdır. Araştırmaya katkıda bulunabilecek çalışmalar aşağıda belirtilen hususlarda önem arz ettiği için ayrıntılı olarak incelenmiştir:

- Kamu ve özel kurumlar açısından kritik altyapıların önemi [18],
- Siber güvenliğin altyapı sorunları, ulusal güvenliğin sağlanması konusundaki zorluklar, kritik altyapıların önemi ve kamu politikalarının siber güvenliğe etkisi [19],
- Ulusal siber güvenlik stratejisi ve politikalarının oluşturulması noktasında kişi, kurum ve kuruluşlara yol gösteren bir kaynak olması [16],
- Siber güvenliğin hukuki altyapısı, eksiklikleri ve gereklilikleri [3],
- İletişim çağı ile gelen internetin etkileri, sosyal mühendislik kavramları ve bilişimin gücü [20],
- İşletmelerin ve kurumların teknoloji ile birlikte istihdam sorunları ve siber güvenlik altyapıları [21],
- NATO ülkeleri siber güvenlik stratejileri ve alınan önlemler [22],
- Covid 19 etkisi ve stratejinin sınırlılıkları [23],
- Sosyal medyada siber suç farkındalık düzeyinin ölçülmesi [24].

Tablo 2. Çalışma kapsamında incelenen yayınlar (Publications examined within the scope of the study)

Sıra	Konu	Türü	Sayı
1	Siber Güvenlik	Tez, Makale, Dergi	42
2	Siber Saldırı		7
3	Siber Savaş		5
4	Siber Suç		35
5	Siber Terör		7
6	Siber Uzay		16
7	Türkiye'nin Siber Güvenlik Stratejisi	Belge ve Planlar	12
8	Siber Güvenlik ve Suçlar	Kanun	16
9	Siber Güvenlik, Ağ Güvenliği	Kitap	55
Toplam			**195**

Ek olarak 2001 yılından 2021 yılına kadar 20 yıllık süreçte siber güvenlik alanında 55 adet basılmış kitap incelenmiştir. Ayrıca ulusal siber güvenlik konusuyla ilgili olabilecek yayımlanmış stratejiler, dokümanlar ve raporlar araştırılarak 12 adet çalışmaya ulaşılmıştır. Akademik olarak hangi üniversitelerde ve programlarda siber güvenlik bölümlerinin kurulduğu ve eğitim öğretim faaliyetinde bulunulduğu araştırılmıştır. Ek olarak Türkiye'de siber güvenlik alanında öncü olan ve/veya siber saldırılardan en çok etkilenen kurumlara değinilmiş ve bunların politikaları üzerinde durulmuştur. En önemli konulardan birisi de siber güvenliğin mevzuatı boyutudur. Çalışmada Cumhurbaşkanlığı Mevzuat Bilgi Sistemi üzerinden Türkiye'deki şimdiye kadar düzenlenmiş siber güvenlikle alakalı çok sayıda Kanun ve Yönetmelik incelenmiştir. Son olarak tez, makale, dergi, kitap, strateji ve politikalarda elde edilen önemli sonuçlar, kişisel olarak siber güvenlik alanında yapılması gerekenler ve Türkiye'de siber güvenlik alanındaki tehditler değerlendirilerek çalışma sonuçlandırılmıştır.

3. BULGULAR (RESULTS)

3.1. Türkiye'de Siber Güvenlik Alanında Yer Alan Kurumlar ve Çalışmaları (Institutions in the Field of Cyber Security in Türkiye and Their Studies)

Siber güvenlik ve siber suçlar alanında yürütülen asayiş ve hukuk çalışmaları tek başına yeterli olmamıştır. Bu konularda çalışan birçok kurum olmakla birlikte aynı zamanda alanında uzman ve çözüm üretebilecek kurum ve kuruluşların varlığına da ihtiyaç duyulmuştur. Bu ihtiyaçtan dolayı özellikle ulusal güvenliğin sağlanması amacıyla güvenilir yerli yazılım ve donanımlarla çalışan çeşitli kurum ve kuruluşlar kurulmuştur.

Tablo 3. Siber güvenlik alanında çalışma yapan kurumlar (Organizations working in the field of cyber security)

İstihbarat Çalışmaları	Kritik Altyapı Çalışmaları	Özel Girişimler
Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı	BTK	Savunma Teknolojileri Mühendislik ve Ticaret A.Ş. (STM)
Jandarma Genel Komutanlığı Bilişim ve Teknik İstihbarat Başkanlığı	Afet ve Acil Durum Yönetimi Başkanlığı (AFAD)	Hava Elektronik Sanayi (HAVELSAN)
Siber Güvenlik Komutanlığı İstihbarat Daire Başkanlığı	TÜBİTAK	Askeri Elektronik Sanayi (ASELSAN)
Siber Suçlarla Mücadele Şube Müdürlüğü	Milli İstihbarat Teşkilatı (MİT)	
Milli İstihbarat Teşkilatı (MİT)	Türk Silahlı Kuvvetleri Siber Savunma Komutanlığı	

3.1.1. Bilgi Teknolojileri ve İletişim Kurumu (Information and Communications Technologies Authority)

Bilgi Teknolojileri ve İletişim Kurumu (BTK) 4502 sayılı kanun ile "Telekomünikasyon Kurumu" adıyla 27 Ocak 2000 tarihinde kurulmuştur. Daha sonra adı "Bilgi Teknolojileri ve İletişim Kurumu" olarak değiştirilmiştir. Siber suçlarla mücadele bu kurum tarafından sivil toplum kurum ve kuruluşlarıyla iş birliği halinde yürütülmektedir. Türkiye'nin ilk sektör düzenleyici kurumu olan BTK, telekomünikasyon sektörünü denetlemektedir. Türkiye'de siber güvenlik noktasında ana omurgayı BTK oluşturmaktadır [25].

Kurum kurulduğu günden bugüne kadar sektöre yön veren, önemli Stratejik Planlar belirlemiştir. 2010-2012 Stratejik Planı ile IPv6'ya geçiş süreci, E-Devlet uygulamalarının artırılması, Teknoparkların kurulması, Elektronik ve mobil imza kullanım alanlarının genişletilmesi, tüketicilerin bilgilendirilmesi kapsamında kurum internet sayfalarının genişletilmesi, tüketici şikâyetlerinin dinlenmesi ve çözüm üretilmesi gibi önemli kararlar alınmış ve uygulanmıştır.

2013-2015 Stratejik Planı ile Ulusal siber güvenliğin arttırılmasına yönelik çalışmalar yapılması, kayıtlı elektronik posta düzenlemelerinin güncellenmesi ve hizmet sağlayıcılarının denetlenmesi, ihtiyaç duyulan alanlarda yeni düzenlemeler yapılması, yeni nesil şebekelere geçiş sürecinin tanımlanması ve uygulanması, spektrum serbestleşmesi, spektrum ticareti düzenlenmelerinin tamamlanması ve uygulanması, altyapıya dayalı rekabetin desteklenmesi yönünde düzenlemeler yapılması kararları alınmıştır.

2016-2018 Stratejik Planı ile Şebeke yatırımları ve rekabetin desteklenmesi, tüketici memnuniyetinin sağlanmasının teşvik edilmesi, elektronik haberleşme güvenliği ve siber güvenlik konularında yetkinliğin artırılması, e-dönüşüm sürecinin desteklenmesi, alan adı tahsisinde etkinliğin artırılması, uluslararası gelişmelerin takip edilerek Türkiye'ye yönelik çalışmalar yapılması gibi kararlar alınmıştır.

2019-2023 Stratejik Planı ile güvenlik temelli Ar-Ge faaliyetlerinin desteklenmesi, bilgi teknolojileri ve internetin bilinçli kullanımı konusunda farkındalık faaliyetlerinin yürütülmesi, internetin bilinçli kullanımı için oluşturulan teknik araçların etkinliğinin sağlanması, yasal olmayan internet içeriği ile mücadele edilmesi, siber güvenliğe yönelik uzman insan gücünün nicelik ve niteliğinin artırılması, ulusal siber güvenliğin sağlanması için ihtiyaç duyulan denetleme ve düzenleme faaliyetlerinin sürdürülmesi gibi siber güvenliği ilgilendiren önemli kararlar alınmıştır [26].

3.1.2. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (Scientific and Technological Research Council of Turkey)

Kuruluş amacı; "Türkiye'de müspet bilimlerde araştırma ve geliştirme faaliyetlerini ülke kalkınmasındaki önceliklere göre geliştirmek, özendirmek, düzenlemek ve koordine etmek; mevcut bilimsel ve teknik bilgilere erişmek ve erişilmesini sağlamak" olarak belirlenen Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK), bu amaç doğrultusunda Ulusal Siber Güvenlik konusunda çalışmalar yapmak üzere Bilişim ve Bilgi Güvenliği İleri Araştırmalar Merkezinin (BİLGEM) bünyesinde 1997 yılında bir laboratuvar kurmuştur. Burada Microsoft/açık kaynak kodlu işletim sistemleri, e-posta sunucuları, aktif ağ cihazları, veri tabanları ve saldırı tespit sistemleri gibi savunma ürünleri hakkında detaylı çalışmalar yapılmıştır. Genelkurmay

Başkanlığı'nındesteğiyle 2001 yılında kurulan Ortak Kriter Merkezi, bilişim sistemi ürünlerinin güvenlik kriterlerini ve seviyelerini incelemiş, kripto cihazlar için Haberleşme Güvenliği testleri yapmıştır. 2006 yılından sonra akıllı kart güvenliği üzerine Yan Kanal Analizi ve Tersine Mühendislik konularında uzmanlaşan kurum, altyapısıyla dünyada önemli test merkezlerinden biri haline gelmiştir [27].

2005 yılında Bilgi Sistemleri Güvenlik Programı ile kamu kurum ve kuruluşlarının ihtiyaçlarını karşılamak için TÜBİTAK BİLGEM Ağ Güvenliği kurulmuştur. Burada kritik kamu kurum personellerine ve üniversitelerin bilişim sistemlerinde çalışan görevlilere eğitimler verilmiştir. Yine TÜBİTAK BİLGEM bünyesinde kurulan Siber Güvenlik Enstitüsü ise kritik altyapıların akıllı sistemler karşısında güvensiz hale gelmesinden dolayı Türkiye genelindeki enerji, su, haberleşme, finans gibi kritik altyapıların korunması yönünde güvenlik testleri yapmıştır. Bilişim sistemlerinin güvenliği konusunda çalışmalar devam etmektedir.

Bugüne kadar üç adet ulusal siber güvenlik tatbikatı gerçekleştirilmiştir. İlki 2008 yılında, ikincisi 2011 yılında, Üçüncüsü ise 2013 yılında gerçekleştirilmiştir [27]. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı ile kritik altyapı tesislerinin korunması ve güvenli yazılımlarının geliştirilmesi görevi TÜBİTAK'a verilmiştir. Siber güvenlik ürünleri ve hizmet sağlayıcılarının sertifikalandırılması da Türk Standartları Enstitüsü ile birlikte TÜBİTAK sorumluluğuna verilmiştir.

3.1.3. Afet ve Acil Durum Yönetimi Başkanlığı (Disaster and Emergency Management Presidency)

Siber güvenlik alanında çalışma yapan kurumlardan birisi de 17 Haziran 2009'da kurulan Afet ve Acil Durum Yönetimi Başkanlığı (AFAD)'dır. Her ilde valiye bağlı olarak çalışan AFAD, Eylül 2014'te 2014-2023 Kritik Altyapıların Korunması Yol Haritasını yayımlamıştır. Güvenlik irtibat görevlisinin atanması, eğitim programının oluşturulması ve uygulanması, Kritik Altyapı Koruma Planının hazırlanması, AB Kritik Altyapı Uyarı Bilgi Ağı çalışmalarına destek verilmesi ve yetkili otoritelerin belirlenmesi bu yol haritasında belirlenen gereksinimlerdir. Fakat belgede olası bir siber güvenlik krizinin nasıl yönetileceğine açıklık getirilmemiştir [28].

AFAD'ın önemli görevleri vardır. Bilhassa kritik altyapıların korunması, ilgili kurumlar arasında koordinasyonun sağlanması ve altyapılara yönelik ihtiyaç duyulan verilerin hazırlanması görevinin AFAD tarafından yürütülmesi önem arz etmektedir [29]. Kurumun siber güvenlik konusunda çalışmaları, Bilgi Sistemleri ve Daire Başkanlığı tarafından yürütülmektedir.

3.1.4. Ulusal Siber Olaylara Müdahale Merkezi (Computer Emergency Response Team)

28447 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" ve 5809 sayılı "Elektronik Haberleşme Kanunu" gereğince, 27.05.2013 tarihli Bakanlar Kurulu Kararıyla siber saldırın etkilerini azaltmak veya ortadan kaldırmak için BTK'ya bağlı olarak Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur. Bu merkezin görevleri aşağıda verilmiştir [30].

- Ülkemizdeki siber olaylara müdahale konusunda koordinasyon ve kontrol faaliyetlerini yürütmek,
- Tespit edilen siber tehditlerle ilgili olarak ülke çapında alarm, uyarı ve duyuru yapmak,
- Siber güvenlik olaylarına maruz kalan bilişim sistemlerine koruyucu tedbirler almak,
- Siber güvenlik çalışmalarında suç teşkil eden eylemlere karşı adli makamlar ve kolluk kuvvetleriyle koordine olarak hareket etmek,
- Yerli ve milli Siber Olaylara Müdahale Ekipleri (SOME) İletişim Platformu (SİP) üzerinden sektörel güvenlik bildirimlerini (alarm, duyuru, mesaj ve ihbar) göndermek,
- Zararlı internet adreslerini tespit etmek, zararlı yazılımları kontrol etmek, port taraması yapan internet adreslerinin erişimlerini engellemek,
- Siber tehditleri azaltmak ve bertaraf etmek,
- Özel kuruluşlar ile kamu kuruluşları arasında iş birliği yapmak ve farkındalığı artırmak,
- Ulusal ve uluslararası sivil, askeri güvenlik tatbikatlarına katılım sağlamaktır.

3.1.5. Siber Güvenlik Kurulu (Cyber Security Board)

2012/3842 sayılı Bakanlar Kurulu Kararı ile "siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla" Siber Güvenlik Kurulu kurulmuştur. Kurulun görevlerinden bazıları aşağıda verilmiştir [31]:

- Siber Güvenlik için ihtiyaç duyulan politika, strateji ve eylem planlarını hazırlamak.
- Kamu kurumlarının veri güvenliğini sağlamaya yönelik usul ve esasları hazırlamak.

- Siber Güvenlik için kamu kurumlarında ihtiyaç duyulan teknik altyapının oluşturulmasını, etkinliğini ve test edilmesini sağlamak.
- Ulusal iletişim altyapısı, sistemleri ve veri tabanlarının güvenliğini sağlamak.
- Kritik alt yapılara yönelik siber tehdit ve saldırıları izlemek, müdahale ve önleme sistemlerini oluşturmak.
- İhtiyaç duyulan merkezleri kurmak, bu sistemlerin denetimi, işletimi ve güçlendirilmesiyle ilgili çalışmalar yapmak.
- Siber Güvenliğin sağlanması adına milli çözümler ve siber saldırılara müdahale araçları geliştirmek.
- Ulusal Siber Güvenliğin sağlanması için uzman personel temini, eğitimi ve bu konuda diğer ülkeler ve uluslararası kuruluşlarla iş birliği yapmak.

3.1.6. Türk Silahlı Kuvvetleri Siber Savunma Komutanlığı (Turkish Armed Forces Cyber Defense Command)

Türkiye'nin ülkeyi dışardan gelecek siber saldırılara karşı korumak amacıyla oluşturulan ve Siber Savunma Komutanlığı olarak bilinen ilk siber ordusu, Savunma Bakanlığı, TÜBİTAK ve ODTÜ iş birliği ile Genelkurmay Başkanlığı bünyesinde 2010 yılında kurulmuştur. 2013 yılında Ulusal Siber Güvenlik Stratejisinin yayınlanmasıyla resmileşerek görevleri tanımlanmıştır. Bu görevler şunlardır [1]:

- Türk Silahlı Kuvvetlerinin (TSK) siber ortamdaki tüm sistemlerinin siber savunmasını sağlamak.
- Siber olaylara 7/24 müdahale edecek şekilde hazır bulunmak.
- NATO tarafından veya ulusal olarak icra edilen tatbikatlara katılmak.
- Bilinçlendirme ve eğitim faaliyetleri yürütmek.
- Kurumun kullandığı ağlarda siber güvenlik denetlemeleri yapmak.

2014 yılında Siber Savunma Proje Tanımlama Dokümanı hazırlanmış ve Millî Savunma Bakanlığına sunulmuştur. TSK için milli yazılım ve donanım altyapısı sağlanmıştır. Kasım 2014'te NATO destekli Siber Koalisyon Tatbikatı yapılmıştır. 2020 yılı itibariyle milli yazılımlar ve Siber Savunma Merkezi projeleriyle siber ordu güçlendirilmiştir.

3.1.7. Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı (General Directorate of Security, Department of Combating Cybercrime)

Emniyet Genel Müdürlüğü (EGM) bünyesinde ilk olarak 1998'de Bilgisayar Suçları ve Bilgi Güvenliği Kurulu kurulmuştur. Bu kurul bilişim suçlarının kapsamı, bilişim ve ağ teknolojileri hakkında bilgi sahibi olunması, ulusal ve uluslararası mevzuatın incelenmesi ve suç unsuru olabilecek faktörlerin belirlenmesi amacıyla çalışmalar yapmıştır. Bu kuruldan bir yıl sonra Bilgi Suçları Çalışma Gurubu kurulmuştur.

2001 yılında ise siber suçlarla mücadele kapsamında Bilişim Suçlarıyla Mücadele Daire Başkanlığı kurulmuştur. 2003 yılında ismi değiştirilerek Siber Suçlarla Mücadele Daire Başkanlığı olmuştur. 81 ilde şubesi olan bu başkanlık çok kapsamlı ve etkili bir şekilde çalışmalarına devam etmektedir.

Siberay, Ocak 2020'de Siber Suçlarla Mücadele Daire Başkanlığı bünyesinde başlatılan bir projedir. Siber zorbalığı engellemek, teknoloji bağımlılığı konusunda çocukları ve gençleri bilinçlendirmek, güvenli internet kullanımını sağlamak projenin esas amaçlarıdır. Özellikle çocukları bilinçlendirmeyi hedef alan proje Emniyet Müdürlüğü Çocuk Şubesi uzman pedagoglarıyla çalışmaktadır. BTK, Gazi Üniversitesi, Milli Eğitim Bakanlığı Talim ve Terbiye Kurulu Başkanlığı ve İçişleri Bakanlığı'na bağlı çeşitli Daire Başkanlıkları projeye katkıda bulunan diğer kuruluşlardır.

3.2. Siber Güvenlik Faaliyetleri Çerçevesinde Yasal Düzenlemeler (Legal Regulations Within the Framework of Cyber Security Activities)

Dünya'da, teknolojinin hızlı gelişimiyle ve bilgisayar kullanımının yaygınlaşmasıyla siber suçlar cezasız kalmaya başlamıştır. Siber dünya yeni savaş alanı haline gelmiş ve devletler de bu yönde önlem almak zorunda kalmıştır. Türkiye'de de son yıllarda ulusal bir sorun haline gelen siber güvenlik saldırıları sonucunda, siber suçlar konusunda hukuksal olarak düzenleme yapılması ihtiyacı ortaya çıkmıştır. Siber suçlar kısmında da değinilen onuncu kısım haricindeki Türk Ceza Kanununda yer alan ve bilgisayar yoluyla işlenen suçlar aşağıda verilmiştir [12]:

1-Kişisel Verilerin Kaydedilmesi Suçu (madde 135) "Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.",

2-Kişisel Verilerin Hukuka Aykırı Olarak Ele Geçirilmesi veya Verilmesi (madde 136) "Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.",

3-Verilerin Yok Edilmesi Suçu (madde 138) "Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü

olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.”,

4-Haberleşmenin Gizliliğini İhlal Suçu (madde 132) “Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat artırılır.”,

5-Haberleşmenin Engellenmesi (madde 124) “Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi halinde, altı aydan iki yıla kadar hapis veya adlî para cezasına hükmolunur.”,

6-Hakaret Suçu (madde 125) “Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden (...) veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldıran kişi, üç aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Mağdurun gıyabında hakaretin cezalandırılabilmesi için fiilin en az üç kişiyle ihtilat ederek işlenmesi gerekir. Fiilin, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi halinde, yukarıdaki fıkrada belirtilen cezaya hükmolunur.”,

7-Bilişim Sistemi kullanılarak İşlenen Hırsızlık Suçu (madde 142/2/e) *“Bilişim sistemlerinin kullanılması suretiyle işlenmesi.”,*

8-Bilişim Sistemi kullanılarak İşlenen Dolandırıcılık Suçu (madde 158/1/f) “Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlemesi.”,

9-Müstehcenlik Suçu (madde 226) “Bir çocuğa müstehcen görüntü, yazı veya sözleri içeren ürünleri veren ya da bunların içeriğini gösteren, okuyan, okutan veya dinleten, bunların içeriklerini çocukların girebileceği veya görebileceği yerlerde ya da alenen gösteren, görülebilecek şekilde sergileyen, okuyan, okutan, söyleyen, söyleten, bu ürünleri, içeriğine vakıf olunabilecek şekilde satışa veya kiraya arz eden, bu ürünleri, bunların satışına mahsus alışveriş yerleri dışında, satışa arz eden, satan veya kiraya veren, bu ürünleri, sair mal veya hizmet satışları yanında veya dolayısıyla bedelsiz olarak veren veya dağıtan, bu ürünlerin reklamını yapan kişi, altı aydan iki yıla kadar hapis ve adlî para cezası ile cezalandırılır.”

Türk Ceza Kanunu dışında yapılan düzenlemelere ise aşağıda yer verilmiştir:

5846 sayılı Fikir ve Sanat Eserleri Kanunu Madde 2/1’in 7 Haziran 1995 tarihinde değişiklik yapılan hali “Herhangi bir şekilde dil ve yazı ile ifade olunan eserler ve her biçim altında ifade edilen bilgisayar programları ve bir sonraki aşamada program sonucu doğurması koşuluyla bunların hazırlık tasarımları” şeklindedir [32]. Bu maddeyle bilgisayar programları, hazırlık aşamasında bilgisayar ara yüzünden erişilen bilgiler de eser olarak tanımlanmış, bunlara yönelik fiillerde suç olarak sayılmıştır.

5070 sayılı Elektronik İmza Kanunu Madde 17 “Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile bu elektronik sertifikaları bilerek kullananlar, iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adlî para cezasıyla cezalandırılır.” ile elektronik sertifikalar üzerinde yapılan değişiklikler de suç olarak kabul edilmiştir [33].

5651 sayılı kanun ile içerik sağlayıcının, yer sağlayıcının ve erişim sağlayıcının yükümlülükleri tanımlanmış ve işlenen suçlarla nasıl mücadele edilmesi gerektiği belirlenmiştir [34]. Madde 8/1’ de *“İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak içeriğin çıkarılmasına ve/veya erişimin engellenmesine karar verilir.”* ifadesi yer almaktadır. Bahsedilen suçlar; uyuşturucu madde kullanılmasını kolaylaştırma, intihara yönlendirme, müstehcenlik, fuhuş, çocukların cinsel istismarı, kumar oynanması için yer ve imkân sağlama, sağlık için tehlikeli madde temini, Atatürk aleyhine işlenen suçlar kanunu ve Spor Müsabakaları bahis oyunları kanununda yer alan suçlardır.

Yukarıda belirtilen suçlar dışında mevzuatta değinilmesi gereken, siber suç kapsamına alınabilecek diğer hükümler ise aşağıda verilmiştir.

Kritik altyapıların korunmasına yönelik ihtiyaç duyulan hükümlere 1 nolu Cumhurbaşkanlığı Kararnamesi’nde yer verilmiştir. Cumhurbaşkanlığı dijital dönüşüm ofisine sorumluluklar verilmiş; ofis, kritik altyapıların belirlenmesine ilişkin çalışmalar gerçekleştirmek, bilgi güvenliği yönetim sistemleri kurmak, işletmek ve teknik standartlara ilgili usul esasları konusunda yetkilendirilmiştir. Güvenlik ve Dış Politikalar Kurulu kararlarıyla da siber güvenlik politikaları konusunda strateji geliştirme görevi verilmiştir [35]. Ayrıca özel kanunlarda da internet aracılığıyla işlenebilen suçlara yer verilmektedir. İlgili mevzuat hükümleri şunlardır:

1632 sayılı Askeri Ceza Kanununa göre internet ve iletişim araçlarıyla işlenebilen birçok suç türü vardır. Kanunun 58. maddesine göre; *“Her kim, Türk Ceza Kanununun 153, 161 inci maddelerinde yazılı suçlardan birisini ve 155 inci maddede yazılı halkı askerlikten soğutmak yolunda neşriyatta ve telkin atta bulunmak ve nutuk irat etmek fiillerini işleyecek olursa milli mukavemeti kırmak*

cürmünden dolayı mezkur maddelerde gösterilen cezalarla cezalandırılır." hükmünün yanı sıra amirlere ya da emirlere itaatsizliğe yönlendirmek veya güncel olarak incelendiğinde sosyal medya hesaplarından askeri bilgi ve belgelerin paylaşılması, fotoğraf ve konum paylaşımı ile yer tespit edilmesinin sağlanması internet yoluyla işlenebilen suçlar kapsamında yer alır [36].

2935 sayılı Olağanüstü Hal Kanunu ile güvenlik, asayiş ve kamu düzenini korumak kapsamında sınırlamalar getirme yetkisi il ve bölge valilerine verilmiştir. Kanunun 25.maddesi 2.bendinde yer alan şu hüküm *"Özel maksatla kamunun telaş ve heyecanını doğuracak şekilde asılsız, mübalağalı havadis ve haber yayan veya nakledenler, fiilleri başka bir suç oluştursa bile ayrıca üç aydan bir yıla kadar hapis ve beş bin liradan az olmamak üzere ağır para cezasıyla cezalandırılırlar. Eğer fiil, fail tarafından bir yabancı ile anlaşma sonucu işlenmiş ise hapis cezası bir yıldan ve ağır para cezası otuz bin liradan aşağı olamaz. Bu suçlar basın ve yayın organları vasıtasıyla işlenirse fail ve mesulleri hakkında verilecek cezalar bir misli artırılarak hükmolunur."* ile internet üzerinden ve sosyal medya hesaplarından yalan haber yapan veya gerçeğe aykırı beyanda bulunan kişilerin de cezalandırılabileceği anlaşılmaktadır [37].

Ağır cezalar içeren 3713 sayılı Terörle Mücadele Kanunu 7. maddesinde yer alan "…Terör örgütünün; cebir, şiddet veya tehdit içeren yöntemlerini meşru gösterecek veya övecek ya da bu yöntemlere başvurmayı teşvik edecek şekilde propagandasını yapan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır. Bu suçun basın ve yayın yolu ile işlenmesi hâlinde, verilecek ceza yarı oranında artırılır. Ayrıca, basın ve yayın organlarının suçun işlenmesine iştirak etmemiş olan yayın sorumluları hakkında da bin günden beş bin güne kadar adli para cezasına hükmolunur…" hükmü, bireysel olarak sosyal medyada veya internette yayın yaparak suç unsuru oluşturan kişileri de kapsamaktadır [38].

5352 sayılı Adli Sicil Kanunu 11. maddesinde yer alan; "Adlî sicil ve arşiv bilgileri gizlidir. Bu bilgiler, görevlilerce açıklanamaz ve bu Kanun hükümlerine göre verilen kişi, kurum ve kuruluşlarca veriliş amacı dışında kullanılamaz." hükmü ile kişisel bilgilerin açıklanmaması gerektiği belirtilmektedir [39]. Son zamanlarda bu konular yüzünden özellikle kamu personelleri tarafından Cumhurbaşkanlığı İletişim Sistemine (CİMER) birçok başvuruda bulunulduğu görülmektedir. Bilgisayar veya internet yoluyla bu bilgilerin paylaşılması veya kullanılması siber suçlar kapsamında değerlendirilebilir.

4125 sayılı seçimlere yönelik kanunda yer alan yayın yasaklarına uymamak hükmünün, bilgisayar veya internet yoluyla çiğnenmesi de yasaktır [40]. 3192 sayılı Bankacılık Kanununda bankanın itibarını zedeleyecek, şöhretine ya da servetine zarar verebilecek asılsız haber yaymanın internet ve bilgisayar yoluyla işlenmesi de suç kapsamına girmektedir [41].

6502 sayılı Tüketicilerin Korunması Kanuna göre internette reklam alan/verenlerin, Rekabet Kurulu ilkelerine, kamu düzenine, genel ahlaka, kişilik haklarına uygun, dürüst ve doğru olmaları, tüketiciyi aldatmamaları, yanıltıcı reklam vermemeleri gerekmektedir. Ayrıca kamu sağlığını bozacak, çocuk, hasta, yaşlı ve özürlüleri istismar edecek reklam ve ilanlar ile örtülü reklam yapılamaz hükmü yer almaktadır [42].

3.3. Siber Güvenlik Alanında Akademik Eğitim Faaliyetlerine Yönelik Çalışmalar (Studies on Academic Training Activities in the Field of Cyber Security)

Son yıllarda dünyada teknolojinin gelişmesiyle birlikte güvenlik zafiyetleri artmaktadır. Küreselleşen dünyada ülkemizin bu gelişen teknoloji ve değişimlere karşı ayak uydurması biraz zaman alsa da akademik anlamda farkındalık çalışmaları uzun yıllardır devam etmektedir.

Günümüzde 11'i Devlet Üniversitesi, 12'si Vakıf Üniversitesi olmak üzere toplam 23 üniversitede Siber Güvenlik bölümü açılmış olup akademik eğitime devam edilmektedir. Üniversiteler ve buralarda açılan bölümlere bakıldığında farklı olarak sadece Yıldız Teknik Üniversitesinin Siber Güvenlik ve Kriptografi Anabilim Dalı bölümü açtığı, diğer üniversitelerde Siber Güvenlik adı altında eğitime devam edildiği görülmektedir.

Tablo 4. Siber güvenlik eğitimi veren üniversiteler (Universities offering cyber security education)

Sıra	Üniversite Adı	Şehir	Bölüm Adı
1	Üsküdar Üniversitesi	İstanbul	Siber Güvenlik
2	Kadir Has Üniversitesi	İstanbul	Siber Güvenlik
3	Işık Üniversitesi	İstanbul	Siber Güvenlik
4	Alparslan Türkeş Bilim ve Teknoloji Üniversitesi	Adana	Siber Güvenlik
5	Marmara Üniversitesi	İstanbul	Siber Güvenlik
6	İstanbul Ticaret Üniversitesi	İstanbul	Siber Güvenlik
7	Orta Doğu Teknik Üniversitesi	Ankara	Siber Güvenlik
8	Gebze Teknik Üniversitesi	Kocaeli	Siber Güvenlik
9	Antalya Bilim Üniversitesi	Antalya	Siber Güvenlik
10	Sabancı Üniversitesi	İstanbul	Siber Güvenlik
11	Bahçeşehir Üniversitesi	İstanbul	Siber Güvenlik
12	Koç Üniversitesi	İstanbul	Siber Güvenlik
13	Düzce Üniversitesi	Düzce	Siber Güvenlik
14	Yıldız Teknik Üniversitesi	İstanbul	Siber Güvenlik
15	Yıldız Teknik Üniversitesi	İstanbul	Siber Güvenlik ve Kriptografi
16	TOBB Ekonomi ve Teknoloji Üniversitesi	Ankara	Siber Güvenlik
17	Hacettepe Üniversitesi	Ankara	Bilgi Güvenliği
18	Sakarya Üniversitesi	Sakarya	Siber Güvenlik
19	Milli Savunma Üniversitesi	Ankara	Siber Güvenlik
20	Süleyman Demirel Üniversitesi	Isparta	Siber Güvenlik
21	İstanbul Teknik Üniversitesi	İstanbul	Siber Güvenlik
22	Yaşar Üniversitesi	Ankara	Siber Güvenlik
23	Ahmet Yesevi Üniversitesi	Ankara	Siber Güvenlik

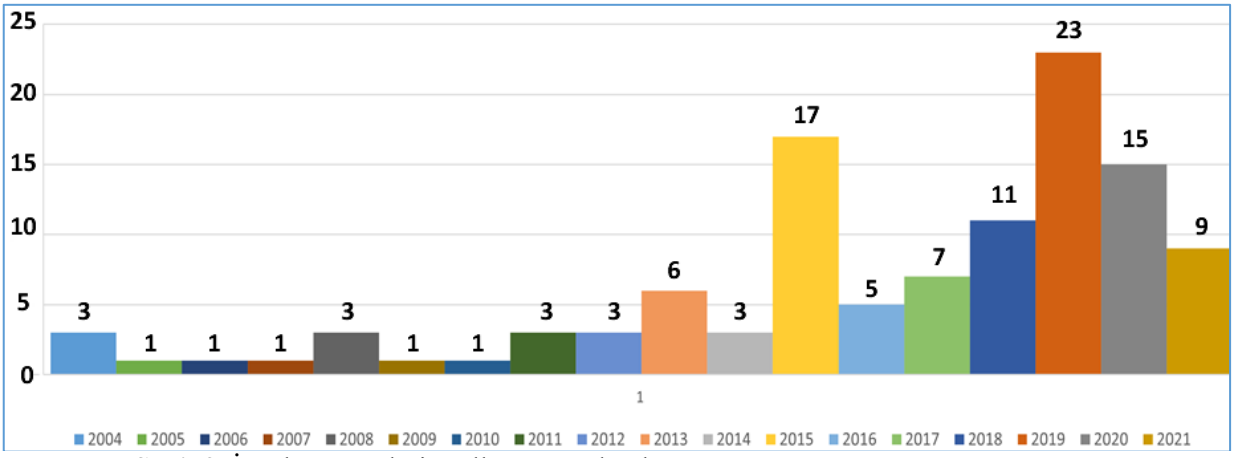
Siber güvenlik alanında açılan bölümlerin hangi düzeyde olduğu incelendiğinde ise iki üniversitede (Yaşar Üniversitesi, Marmara Üniversitesi) Anabilim dalı olarak bölüm açılmış olup Lisans eğitimi verilmektedir. Dokuz üniversitede Yüksek Lisans düzeyinde eğitim faaliyeti verilmekte, iki üniversitede (İstanbul Ticaret Üniversitesi, Kadir Has Üniversitesi) ise Doktora düzeyinde eğitim verilmektedir. Yüksek Lisans ve Doktora alanındaki eğitim veren üniversite bölümlerinin 20 tanesi Tezli olarak, 16 tanesi Tezsiz olarak öğrenci kabul etmekle birlikte 12 tanesi doğrudan Türkçe, 6 tanesi doğrudan İngilizce, 5 tanesi Türkçe-İngilizce öğrenci kabul etmektedir.

3.4. Türkiye'de Siber Güvenlik Alanında Yapılan Tez Çalışmaları (Thesis Studies on Cyber Security in Türkiye)

Çalışma kapsamında Türkiye'de siber güvenlik alanında yapılan tezler araştırılmıştır. YÖK Tezler sayfasından 2004 ve 2021 yılları arası ve aşağıda belirtilen anahtar kelimeler üzerinden yapılan aramalar neticesinde 113 teze ulaşılmıştır. Arama yapılan anahtar kelimeler Siber Güvenlik (Cyber Security), Siber Hukuk (Cyber Law), Siber Terör (Cyber Terrorism), Siber Saldırı (Cyber Attacks), Siber Savaş (Cyber Attack), Siber Suç (Cyber Crimes), Siber Uzay (Cyber Space) şeklinde sıralanabilir.

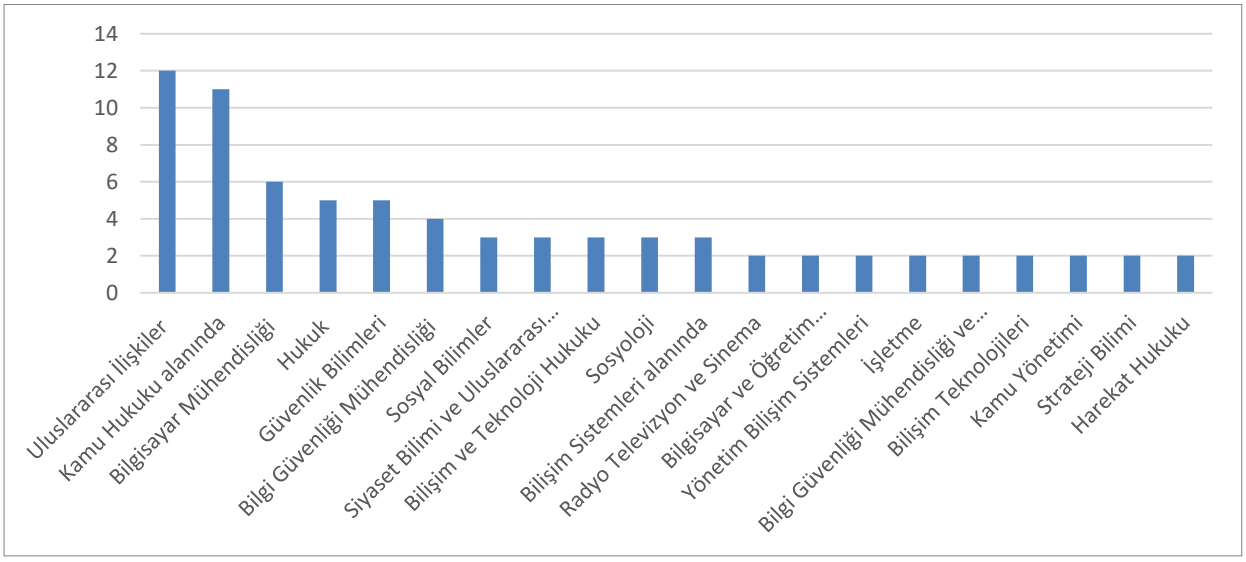
Tezlerin 80 tanesinin (%71) devlet üniversitesi, 33 tanesinin (%29) ise vakıf üniversitesi bölümlerinde yayınlandığı tespit edilmiştir. Vakıf üniversitelerinin Siber Güvenlik alanında yaptığı çalışmalar çok olmasına karşın yayınlanan tez oranlarına bakıldığında devlet üniversiteleri bu konuda açık ara öndedir. Türkiye'de Siber Güvenlik alanında yayınlanan tezlerin %92 si (104 adet) Yüksek Lisans Tezi, %8 i (9 adet) Doktora Tezidir. Bu konu da Yüksek Lisans ile başlayıp giderek artan çalışmalar olduğunu ve Siber Güvenlik farkındalık çalışmalarının sonuç vermeye başladığını söylemek mümkündür. Türkiye'de Siber Güvenlik alanında incelenen tezlerin üniversitelere göre dağılımı incelendiğinde ise; 12 tez ile Gazi Üniversitesinin ilk sırada olduğu görülmektedir. İstanbul Bilgi Üniversitesi 6 tez, Marmara Üniversitesi ve İstanbul Üniversitesi 5 tez, Selçuk Üniversitesi ve Harp Akademisi Komutanlığı 4 tez, Erciyes Üniversitesi, Ankara Üniversitesi, İstanbul Teknik Üniversitesi,

Polis Akademisi, Kara Harp Okulu Komutanlığı, Bahçeşehir Üniversitesi, Fırat Üniversitesi ve Hacettepe Üniversitesi 3 tez yayımlamıştır. Yayımlanan tezlerin 2004–2021 yılları arasında dağılımı incelendiğinde 2018 ve sonrasında ciddi bir artış gözlemlenmektedir. Özellikle 2013 yılı ve öncesinde siber güvenlik, siber ortam, siber uzay kavramlarının yeterli derecede incelenmediği görülmektedir. 2021 yılı tezleri Covid 19 pandemisi sebebiyle YÖK Ulusal Tez Merkezinde beklemede olduğu için bu tezlerin tamamına ulaşılamamıştır.



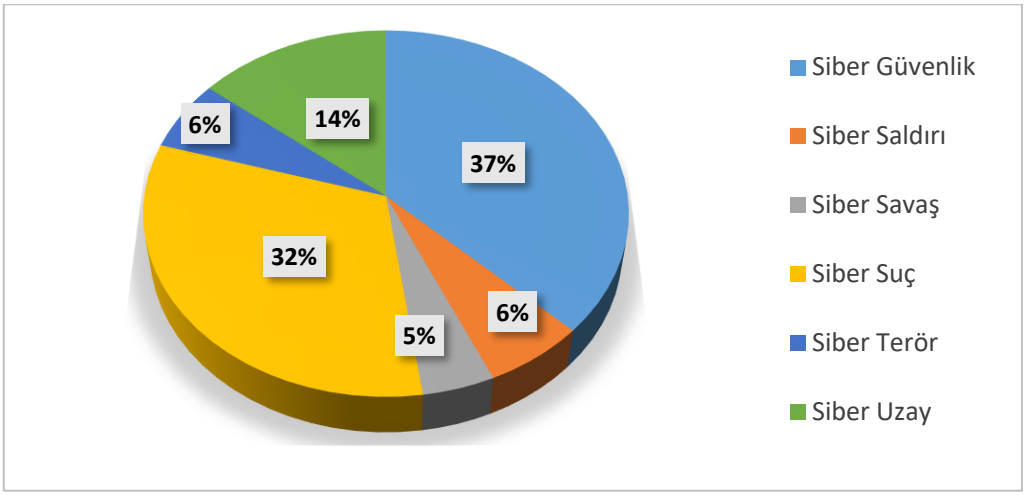
Şekil 2. İncelenen tezlerin yıllara göre dağılımı (Distribution of analyzed theses by years)

İlerleyen süreçte 2021 yılında yayımlanan tezlerde artış gözlemlenebilecektir. Tezlerin enstitülerine göre dağılımı incelendiğinde 57 tane Sosyal Bilimler Enstitüsü, 23 tane Fen Bilimleri Enstitüsü, 9 tane Bilişim Enstitüsü, 5 tane Lisansüstü Eğitim Enstitüsü, 4 tane Stratejik Araştırmalar Enstitüsü, üçer tane Güvenlik Bilimleri ve Savunma Bilimleri Enstitülerinde tez yayımlandığı görülmektedir.



Şekil 3. Tezlerin anabilim dalına göre dağılımı (Distribution of theses by department)

Anabilim Dalına göre incelendiğinde ise en fazla tez 12 adet ile Uluslararası İlişkiler alanında yayımlanmıştır. Kamu Hukuk'u alanında 11 tane, Bilgisayar Mühendisliği alanında 6 tane, Hukuk alanında 5 tane, Güvenlik Bilimleri ve Bilgi Güvenliği Mühendisliği alanında 4 tane, Sosyal Bilimler, Siyaset Bilimi ve Uluslararası İlişkiler, Bilişim ve Teknoloji Hukuku, Sosyoloji, Bilişim Sistemleri alanlarında 3'er tane tez yayımlanmıştır. Tezler konularına göre sınıflandırıldığında ise en çok Siber Güvenlik alanında tez yazıldığı görülmektedir. Siber Suç tez yazımında çok tercih edilen diğer bir konudur.



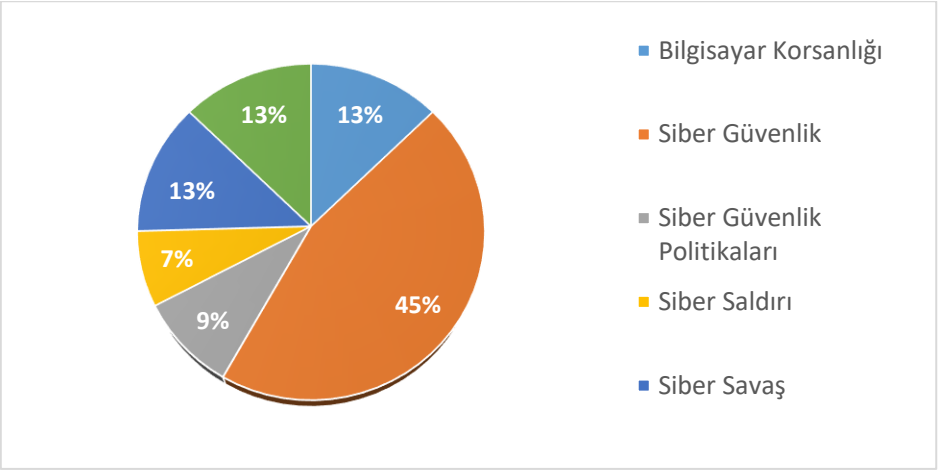
Şekil 4. Tezlerin konularına göre dağılımı (Distribution of theses by subject)

Genel hatlarıyla tezlerde elde edilen sonuçlar aşağıda verilmiştir:

- Ulusal güvenlik ve milli değerlerin korunması için gelecekteki teknolojilere uyum sağlanması ve ihtiyaç duyulan konularda çözümler üretilmesi,
- Kurumların kendi bünyelerinde gerekli tedbirleri almaları ve ihtiyaç duyulan güvenlik kurallarını belirlemeleri gerektiği,
- En tehlikeli siber suçun interaktif dolandırıcılık olduğu,
- En az bilinen siber suç bot-net/DDoS saldırıları olduğu,
- Sanal bahis ve kumarın çok fazla arttığı,
- Siber suçlar konusunda eğitim seviyesinin yetersiz olduğu,
- Türkiye'nin gelişmiş ülkelere göre siber güvenlik alanında geri kaldığı,
- Siber suçların eğitim seviyesi ile aynı oranda arttığı,
- Kişisel güvenlik önlemlerinin siber saldırılar için yetersiz kaldığı,
- Cinsiyetin farkındalık açısından bir etkisinin olmadığı,
- Yazılım kullanma, sanal bahis ve DDoS saldırılarının siber suç olarak görülmediği fakat en tehlikeli suçlardan birisi olduğu,
- Türkiye'nin siber hukuk alanında mevzuatını güncellemede geri kaldığı,
- Türkiye'nin siber güvenlik eylem planlarını uygulamada geri kaldığı,
- Özel sektörler ile sağlanan siber orduların siber güvenliği destekleyemediği,
- Okullarda verilen eğitimlerde eski usullerin kullanılması ve öğrencilerin siber güvenliği yanlış yerlerden, sosyal medyadan öğrenmesinin uygun olmadığı,
- Siber saldırıların şirket, kurum ve kuruluşlara son zamanlarda çok ciddi zararlar verdiği ve mevzuat hükümlerinin yetersizliğinden kişilerin yargılanamadığı,
- Türk hukuk sistemi bilişim suçlarının tasniflenmesinde eksiklikler olduğu,
- Gelişen teknolojiler ile siber uzayı daha çok hayatımızda hissedeceğimiz ve yakın gelecekte bu teknolojilerin olası zararlarının artacağı,
- Sosyal medya uygulamalarının mahremiyet kavramının ortadan kalkmasına ve kişisel bilgilerin kolaylıkla dolandırıcıların eline geçmesine yol açtığı,
- Kritik altyapılara yapılan siber saldırılara karşı yetersizlikler olduğu,
- Kurumların kendilerini güncellemede sorunlar yaşadığı,
- Gelişen akıllı ev, akıllı şehir teknolojilerinin olası etkileri,
- Siber güvenlik ile gelen siber terörün ülke açısından olası etkileri,
- Kablosuz ağ güvenliğinin farkındalığının yetersiz olduğu,
- Siber güvenlik politikalarının güncellenmesi gerektiği.

3.5. Siber Güvenlik Alanında Yazılmış Olan Kitaplar (Books Written on Cyber Security)

Türkiye'de Siber Güvenlik alanında yayımlanan kitaplar incelendiğinde toplamda 55 adet kitaba erişilmiştir. Siber Güvenlik alanında ülkemizde yayımlanan kitapların konusuna göre dağılımları Şekil 5' te verilmiştir:



Şekil 5. Kitapların konularına göre dağılımı (Distribution of books by subject)

Şekilden de görüleceği üzere yazılan kitaplarda en çok Siber Güvenlik konusu tercih edilmiştir. Siber Güvenlik konusunun genel anlamda anlatımını yapan kitapların yanı sıra savunma, politika, hukuk ve savaş boyutuna dair kitaplar da yayınlanmıştır. Tezlerde olduğu gibi kitaplarda da Siber Suç konusu Siber Güvenlikten sonra en çok tercih edilen konu olmuştur. Kitapların yazıldığı yıllara göre dağılımları incelendiğinde ise 2019 yılına kadar düzenli bir artış yaşandığı görülmektedir. Çalışma kapsamında yapılan araştırmalarda son yıllarda bu konuda yazılan kitap sayısında büyük bir artış yaşanmadığı görülmüşür.

Tablo 5. Siber güvenlik alanında yazılan kitaplar (Books written in the field of cyber security)

Sıra	Kitap Adı	Yıl
1	Siber İstihbarat	2001
2	Bilgisayar ve Ağ Üzerinden İşlenen Siber Suçlarla Mücadelenin Hukuksal ve Güvenlik Boyutu	2005
3	Siber Uzay'da Güvenlik ve Türkiye	2006
4	Avrupa Konseyi Siber Suçlar Sözleşmesi Taslağı	2006
5	Siber Suçların Cezalandırılması ve Türkiye'deki Durum	2008
6	Siber Uzayda Macera Dolu Bir Yolculuk	2008
7	Suç Terör ve Savaş Üçgeninde Siber Dünya	2009
8	Okul Zorbalığı ve Siber Zorbalık	2011
9	Siber Savaş Ulusal Güvenliğe Yönelik Yeni Tehdit	2011
10	Her Yönüyle Siber Savaş	2012
11	Türk Ceza Kanunda Bilişim Suçları	2012
12	Siber Güvenlik: Rapor	2012
13	Siber Güvenlik	2013
14	21.Yüzyılda Siber Güvenlik	2013
15	Siber Güvenlik: Rapor	2013
16	Güncel Tehdit Siber Suçlar	2014
17	Anonymous Hacker Dünyasının ve Küresel Siber Ayaklanmanın İç Yüzü	2014
18	Bilişim Suçları ve İnternet İletişim Hukuku	2014
19	Truva Atı Siber Kıyamet	2014
20	5. Uluslararası Bilgi ve Kriptoloji Konferansı: Siber Güvenlik ve Savunma: Bildiriler Kitabı	2014
21	Siber Güvenlik ve Elektronik Bileşenleri	2015
22	Siber Savaş ve Ulusal Güvenlik Stratejisi	2015
23	İnternet ve Gençlik İlişkisinin Bugünü ve Geleceği	2015
24	Siber Suçlar: Tehditler Farkındalık Mücadele	2015
25	Siber Güvenlik ve Siber Savaş	2015
26	Uygulamalarla Siber Güvenliğe Giriş	2015
27	Siber Savaş ve Ulusal Güvenlik Stratejisi	2015
28	Türkiye'de Siber Güvenlik ve Nükleer Enerji	2016
29	Avrupa Birliği'nin Siber Güvenlik Politikası	2017
30	Siber Ortamda Güvendeyim	2017
31	Geleceğin Endüstrileri: [Robotlar, Nesnelerin İnterneti, Genomlar, Büyük Veri, Dijital Para, Hassas Tarım, Siber Güvenlik]	2017
32	Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık	2018
33	Siber Kırılma: Hacker El Kitabı	2018
34	Disiplinler arası Yaklaşımla Siber Politika & Siber Güvenlik	2018
35	Siber Güvenlik: -Hacking- Atölyesi	2018
36	Siber Güvenlik Bibliyografyası	2018
37	Siber Politika ve Siber Güvenlik	2018
38	APT ve Siber Saldırı Analizi	2019
39	Siber Güvenlik ve Savunma: Problemler ve Çözümler	2019
40	Herkes İçin Siber Güvenlik	2019
41	Mükemmel Silah: Siber Çağda Savaş, Sabotaj ve Korku	2019
42	Siber Güvenlik Operasyonları Merkezi: SGOM ve SOME'ler İçin Analiz, Tasarım, Kurulum ve İşletim Rehberi	2019
43	Siber Güvenlik: Saldırı & Savunma Stratejileri	2019
44	Siber Ortamda Güvendeyim	2019
45	Uygulamalı Siber Güvenlik ve Hacking	2019
46	Dijital Dönüşüm: Siber Güvenlik	2019
47	Siber Mücadeleye Giriş: <Guvende_Misin.V101/>	2019
48	Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi	2019
49	Siber Güvenlik ve Savunma: Standartlar ve Uygulamalar	2019
50	Siber Güvenlik Kapsamında Kültür ve Turizm Bakanlığında Bilgi Güvenliği ve Yol Haritası Önerisi	2019
51	Zararlı Yazılımlar: Siber Kitle İmha Silahları	2019
52	Ağ ve Yazılım Güvenliği	2020
53	Etik Hackerlığa Giriş 2	2020
54	Siber Casusluk: Siber Casusluk Yöntemleri ve Karşı Tedbirler	2021
55	Kablosuz Ağ Güvenliği	2021

4. SONUÇLAR (CONCLUSIONS)

Çalışma kapsamında yapılan siber suç araştırmalarından, dolandırıcılık, sahtekârlık, yasa dışı para toplama, müstehcenlik, pornografi, kamu malına zarar verme, zimmet, tehdit, komplo, teşebbüs ve terör benzeri suçların gerçek dünyada işlenebilen suçlar olduğu gibi sanal dünyada da rahatlıkla işlenebilen suç türleri olduğu görülmüştür. Siber suçlar kategorisine almak için bilgisayar veya internet ortamında işlenmesi yeterlidir. İnternet üzerinden işlenen suçları bağımsız bir kategori yapmak uygun değildir.

Siber güvenlik alanında en büyük zafiyetlerden bir tanesi ortak internet kullanımı ve wi-fi paylaşımlarıdır. Kontrol altına alınmadığı sürece işletme sahiplerine yasal sorumluluklar yüklenmesi kaçınılmazdır. Örneğin; bir kafede oturan müşteri, işletmenin wi-fi şifresini öğrenip bir kamu kurum ve kuruluşunun sitesine sızıntı yaparak ciddi bir zarar verebilir, bunun sonucunda ağa sızmaya çalışan kişi arandığında o kafenin işletme sahibi üzerine kayıtlı wi-fi sayesinde işletme sahibi bu suçtan sorumlu tutulabilir. Bu yüzden kullanılan wi-fi denetlenebilir olmalıdır.

Yapılan çalışmalar, günümüzde siber saldırılarda en çok kullanılan yöntemlerden birinin de sosyal mühendislik yöntemi olduğunu göstermektedir. Bu yöntemle kişilerden sohbet veya ikna yoluyla bilgileri öğrenilmekte, başka bir alanda bu bilgiler kullanılarak kişiler mağdur edilmektedir. Bu tarz saldırılardan korunmak için ise aşağıdaki basit yöntemler izlenebilir:

- Güvenlik duvarını sürekli açık tutmak,
- Anti virüs ve anti spyware yazılımı kullanmak,
- İşletim sistemini ve tarayıcıyı açıklara karşı sürekli güncel tutmak,
- Tüm bilgisayar ve ağ sistemini şifreli kullanmak,
- Kablosuz ağları şifreli ve gerekirse Mac filtreli kullanmak,
- Parolaların korunması için güçlü bir şifreleme yapmak,
- Verileri sürekli yedekleyip güncel tutmak,
- İki faktörlü doğrulama yapmak,
- Sosyal medyada az veri paylaşımı yapmak,
- E-posta ve tarayıcıyı özel veriler paylaşırken gizli modda kullanmak.

Araştırma sonuçları göstermektedir ki bir kurumu veya kuruluşu tam olarak siber saldırılara karşı korumak mümkün değildir. Güvenliği sürekli güncel tutarak, sistemli bir şekilde önlemler alarak, çalışmalara devam edilmelidir. Teknik ekip her zaman saldırılara karşı hazır durumda bulunmalıdır. Her ne kadar çok güvenlik önlemleri alınsa da iyi hazırlanmış, planlı ve zamanlı bir siber saldırı her zaman başarılı olacaktır. Siber saldırılar yoluyla erişilen kişisel bilgiler sayesinde kurum veya kuruluşun itibarı zedeleneceği gibi, erişimin engellenmesi sonucu maddi zararlarda oluşabilir. Bazı siber saldırılar tamamen keyfidir. Saldırganlar, kurumlardan maddi bir çıkar veya veri beklentisinde olmayıp kendilerini geliştirmeyi amaçlamaktadırlar.

Türk Ceza Kanununda siber güvenlik faaliyetlerinin yasal düzenlemeleri kapsamında birçok madde bulunmaktadır. Hukuksal açıdan incelediğimizde siber güvenliğin ve siber suçların mevzuat yönünün yeterince irdelenmemesinin ve yapılan çalışmalardaki yetersizliklerin, siber saldırılar, tehditler ve siber suçlara karşı net bir siber hukuk sistemi kurulamamasına yol açtığı görülmüştür. Bu açık yüzünden adalet ve ceza sisteminde de aksaklıklar yaşandığı görülmektedir. Bununla beraber kanuni düzenlemelerde sürekli değişiklikler ve güncellemeler yapılarak bilgisayar ve ağ sistemleri üzerinde işlenebilen bütün suçlar siber güvenlik alanına dâhil edilmeye başlanmıştır.

Türkiye'de elektronik haberleşme sahaları, enerji santralleri, su santralleri, ulaşım hizmetleri, bankacılık ve finans hizmetleri ile süreklilik göstermesi gereken bazı kritik hizmetler veren kamu kurumlarının kritik altyapı tesisleri olarak belirlenerek siber güvenlik çalışmalarında yer alması gerektiği görülmektedir. Siber güvenlik sisteminin takibi için personel yetersizliği sorunun çözülmesi gerekmektedir. Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığında siber soruşturma alanında ihtiyaç duyulan personel alımlarının hızla yapılarak, siber suçlar ile daha iyi başa çıkılacağı düşünülmektedir. Ar-Ge laboratuvarları kurulması, proje teşviki ile kamu, özel kuruluşlar ve üniversite bilişim uzmanlarının faaliyetlerde bulunmaları önündeki yetersizlikler hakkında da acil çalışmalar yapılmalıdır.

Türkiye'nin siber güvenlik çalışmaları incelendiğinde 1990'lı yılların sonunda yapılan yasal düzenlemeler sonrasında siber suçlarla nasıl mücadele edileceği konusunda temel bir altyapı oluşturulduğu görülmektedir. Devamında teknolojinin hızla artması ile zafiyetlerin oluşmaması için kısmi önlemler alınmaya çalışıldığı görülmüştür. Yapılan çalışmaların yetersizliği 2000'li yıllarda daha net anlaşılmış ve bu kapsamda 2012 yılında "Siber Güvenlik Kurulu" kurularak ciddi önlemler alınmaya başlanmıştır. Türkiye'nin 2012 yılında oluşturulan Siber Güvenlik Organizasyonu ve Yol Haritasının beş ana başlık etrafında toplandığı görülmektedir. Bunlar; Siber

Güvenlik Kurulu kurulması, yasal düzenlemeler yapılması, altyapısının güçlendirilmesi, yeteneklerin geliştirilmesi ve ulusal iş birliğinin sağlanmasıdır. 2013 yılında Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı kabul edilerek siber güvenlik alanında ilklere imza atıldığı görülmüştür. Resmi ve özel güvenlik alanında yapılan çalışmalarda eksikliklere bakıldığında tam bir sistematik bilgi paylaşımı olmaması, yerli ve milli yazılımların kullanışlı olmaması gibi sorunlar olduğu görülmektedir.

Siber güvenlik donanım ürünleri incelendiğinde, kullanılan yazılımdan kaynaklanan kod hatalarının olması, işletim sistemi hatalarının olması, güncelleme olmaması gibi güvenlik açıklarının güvenlik zafiyetlerine sebebiyet verdiği görülmektedir. Ayrıca henüz büyük bir saldırının olmamış olması yüzünden şirketlerin ucuz maliyet için genelde görünürde kaliteli ama donanımsal olarak eksikliklerle dolu ucuz güvenlik donanımlarını tercih ettikleri görülmüştür. Yakın bir gelecekte büyük şirketler saldırıların hedefi olduğunda konunun önemi, iyi bir yolla olmasa da daha iyi anlaşılabilir.

Yapılan araştırmalar neticesinde siber güvenlik çalışmalarının ülkeler açısından ne kadar zaruri olduğunun yeni farkına varıldığı ve farkındalık eğitimlerinin artmaya başladığı görülmektedir. Türkiye'de siber güvenlik farkındalığının geliştirilmesi için akademik anlamda eğitim çalışmaları yapan kurumların Yüksek Lisans, Doktora Programlarının yanı sıra BTK ve Udemy gibi kurumların siber güvenlik eğitimleri verdikleri görülmüştür. Ayrıca bu kurum ve kuruluşların toplumda bilinç oluşturmak adına afiş, dergi, gazete, kamu spotu gibi farklı alanlarda reklamlar yayımladıkları görülmüştür.

Sonuç olarak günümüzde gelişen teknolojiler ve yapılan çalışmalar Türkiye'de siber güvenlik alanında farkındalığı üst seviyelere taşımıştır. Özellikle son zamanlarda yapılan akademik yayınların sayısı giderek artmaktadır. Bununla birlikte yerli ve milli yazılımların çoğalması, ASELSAN başta olmak üzere STM gibi şirketlerin donanımsal ve yazılımsal ürünler ortaya çıkarması, yakın gelecekte siber güvenlik konusunda Türkiye'nin iyi bir seviyede olacağını düşündürmektedir.

ETİK STANDARTLARIN BEYANI
(DECLARATION OF ETHICAL STANDARDS)

Bu makalenin yazarları çalışmalarında kullandıkları materyal ve yöntemlerin etik kurul izni ve/veya yasal-özel bir izin gerektirmediğini beyan ederler.

The authors of this article declares that the materials and methods they use in their work do not require ethical committee approval and/or legal-specific permission.

YAZARLARIN KATKILARI (AUTHORS' CONTRIBUTIONS)

H.Ç. ve M.T. çalışmanın derlenmesi ve yazımını birlikte yapmışlardır. Ayrıca yazarlar makalenin tamamını tartışmış ve son halini onaylamışlardır.

H.Ç. and M.T. compiled and wrote the manuscript together. The authors also discussed and approved the final version of the manuscript.

ÇIKAR ÇATIŞMASI (CONFLICT OF INTEREST)

Bu çalışmada herhangi bir çıkar çatışması yoktur.

There is no conflict of interest in this study.

KAYNAKLAR (REFERENCES)

[1] Bıçakcı, S., Ergun, F. D. ve Çelikpala, M. (2015). Türkiye'de siber güvenlik. Ekonomi ve Dış Politika Araştırma Merkezi (EDAM) Siber Politika Kâğıtları Serisi, 1, 1-35.

[2] Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi. International Journal of Multidisciplinary Studies and Innovative Technologies, 24-28.

[3] Alioğlu, S. D. (2019). Siber Saldırılar ve Ülkelerin Siber Güvenlik Politikaları (Yüksek Lisans Tezi). İstanbul: İstanbul Bilgi Üniversitesi.

[4] Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi. Ankara: Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

[5] Ak, T. (2019). İç Güvenlik Yönetimi Açısından Kritik Altyapıların Korunması. ASSAM Dergisi, 97-131.

[6] Düveroğlu, E. (2020). A Comparative Analysis Of Critical Infrastructure Cyber Security Policies: Best Practices From The Us, Eu And Turkey (Yüksek Lisans Tezi). Ankara: Bilkent Üniversitesi.

[7] Gedik, D. (2018). Siber Güvenlik ve Terörizmin Evrilişi: Türkiye Üzerine Etkiler (Yüksek Lisans Tezi). Düzce: Düzce Üniversitesi.

[8] Thomas, D. & Loader, B. (2000). Cybercrime: Law Enforcement. London.

[9] Wall, D. (2001). Cybercrimes and the Internet. in D. Wall (Ed.). Crime and the Internet / London: Routledge.

[10] Furnell, S. (2002). Cybercrime: Vandalizing The Information Society. London: Addison-Wesley.

[11] Avşar, B. Z. ve Öngören, G. (2010). Bilişim Hukuku. İstanbul: Türkiye Bankalar Birliği.
[12] Türk Ceza Kanunu (2004). Resmi Gazete (Sayı: 25611). Erişim adresi: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf.
[13] Alkan, M. (2012). Siber Güvenlik ve Siber Savaşlar. TBMM İnternet Komisyonu (s. Siber Güvenlik Siber Savaşlar). Ankara: https://meclishaber.tbmm.gov.tr.
[14] Taner, C. (2019). Herkes için Siber Güvenlik. İstanbul: Abaküs Yayınları.
[15] Kurt, S. ve Erinç, M. B. (2021). PKK Tarafından Enerji Nakil Hatlarına Yönelik Olarak Gerçekleştirilen Saldırıların Türkiye' nin Enerji Güvenliğine Etkileri. Uluslararası İlişkiler Çalışmaları Dergisi, 1(1), 1-27.
[16] Şenol, M. (2020). Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve Politikalarının Oluşturulması Çerçevesinde Caydırıcılık (Doktora Tezi). İstanbul: İstanbul Teknik Üniversitesi.
[17] Kurtoğlu, Ramazan, (2017). Küresel Para Oyunları ve Psiko-Siber Savaş, İstanbul: Destek Yayınları.
[18] Güngör, M. (2015). Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma (Uzmanlık Tezi). Ankara: Bilgi Toplumu İdaresi Başkanlığı Yayını.
[19] Göçoğlu, V. (2018). Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi (Doktora Tezi). Ankara: Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü.
[20] Barışkan, M. A. (2017). Türkiye'deki Siber Güvenlik Bilinci ve Sosyal Mühendislik Ataklarına Karşı Savunma Önlemlerinin Geliştirilmesi (Yüksek Lisans Tezi). İstanbul: İstanbul Üniversitesi.
[21] Korkusuz, A. (2020). Kurumlarda Siber Güvenlik ve Siber Riskler (Yüksek Lisans Tezi). İstanbul: Bahçeşehir Üniversitesi.
[22] Akyazı, U. (2016). Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler. 6.Uluslararası Siber Güvenlik ve Kriptoloji Konferansı. Ankara: http://www.iscturkey.org/assets/files/2016/03/2013-paper105.pdf.
[23] Akdağ, İ. (2021). Siber Güvenlik ve Türkiye: Örgütsel Yapı, Uygulamalar ve Gelecek (Doktora Tezi). Ankara: Hacettepe Üniversitesi.
[24] Arpaci, I. ve Aslan, O. (2022). Development of a scale to measure cybercrime-awareness on social media. Journal of Computer Information Systems, 1-11.
[25] Darıcılı, A. B. (2019). Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Potansiyel Siber Güvenlik Stratejisi. TESAM Akademik Dergisi, 11-33.
[26] Btk (2021). Stratejik Planlar. https://www.btk.gov.tr/uploads/pages/yayinlar-stratejik-planlar/bilgi-teknolojileri-ve-iletisim-kurumu-2019-2023-stratejik-plani-published-revised-at-27-05-19.pdf adresinden alındı.
[27] Tübitak Bilgem. (2021). Siber Güvenlik Enstitüsü. https://sge.bilgem.tubitak.gov.tr/tr/kurumsal/ sge-tarihcesi adresinden alındı.
[28] Bıçakcı, S. (2019). Siber Güvenlik ve Savunma. Güvenlik Portalı: https://trguvenlikportali.com/arastirma2/guvenlik-yazilari/ adresinden alındı.
[29] Demirci, K. (2021). Kritik Altyapılarda Siber Güvenlik ve AFAD Üzerinden Bir Değerlendirme. Nazilli İktisadi ve İdari Bilimler Fakültesi Dergisi, 2(2), s. 54-64.
[30] Usom. (2021). Usom görevleri. https://www.usom.gov.tr/hakkimizda adresinden alındı.
[31] Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar. (2012, 20 Ekim). Resmi Gazete (Sayı:2012/3842). Erişim adresi: https://www.resmi gazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf.
[32] Fikir ve Sanat Eserleri (1951, 13 Aralık). Resmi Gazete (Sayı: 7981). Erişim adresi: https://www.mevzuat.gov.tr/mevzuatmetin/1.3.5846.pdf.
[33] Elektronik İmza Kanunu (2004, 23 Ocak). Resmi Gazete (Sayı: 25355). Erişim adresi: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5070.pdf.
[34] İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun. (2007, 4 Mayıs). Resmi Gazete (Sayı: 26530). Erişimadresi: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf.
[35] Cumhurbaşkanlığı Kararnamesi (2018, 10 Temmuz). Resmî Gazete (Sayı: 30474). Erişim adresi: https://www.mevzuat.gov.tr/MevzuatMetin/19.5.1.pdf.
[36] Askeri Ceza Kanunu (1930, 15 Haziran). Resmî Gazete (Sayı: 1520). Erişim adresi: https://www.mevzuat.gov.tr/mevzuatmetin/1.3.1632.pdf.
[37] Olağanüstü Hal Kanunu (1983, 27 Ekim). Resmi Gazete (Sayı: 18204). Erişim adresi: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2935.pdf.
[38] Terörle Mücadele Kanunu (1991, 12 Nisan). Resmi Gazete (Sayı: 20843 (Mükerrer)). Erişim adresi: http://www.mevzuat.gov.tr/mevzuatmetin/1.5.3713.pdf.

[39] Adli Sicil Kanunu (2005, 1 Haziran). Resmî Gazete (Sayı: 25832). Erişim adresi: https:// www.mevzuat.gov.tr/MevzuatMetin/1.5.5352. pdf.
[40] Seçimlerin Temel Hükümleri ve Seçmen Kütükleri Hakkında Kanun ile Siyasi Partiler Kanunu ve Milletvekili Seçimi Kanununda Değişiklik Yapılmasına İlişkin Kanun (1995, 28 Ekim). Resmi Gazete (Sayı: 22447 (Mükerrer)). Erişim adresi: https://www. mevzuat.gov.tr/MevzuatMetin /1.5.4125.doc.
[41] Bankacılık Kanunu (2005, 1 Kasım). Resmî Gazete (Sayı: 25983 (Mükerrer)). Erişim adresi: https://www.mevzuat.gov.tr/Mevzuat Metin/1.5.5411.pdf.
[42] Tüketicilerin Korunması Kanunu (2013, 28 Kasım). Resmi Gazete (Sayı: 28835). Erişim adresi: https://www.mevzuat.gov.tr/mevzuat metin/1.5.6502.pdf.