T.C.

TRAKYA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI

YÜKSEK LİSANS TEZİ

ULUSLARARASI İLİŞKİLERDE DEĞİŞEN GÜVENLİK ANLAYIŞI VE TÜRKİYE'NİN SİBER GÜVENLİK STRATEJİLERİ

ATALAY ÖCAL

TEZ DANIŞMANI

PROF.DR. SİBEL TURAN

EDİRNE 2022

Tezin Adı: Uluslararası İlişkilerde Değişen Güvenlik Anlayışı ve Türkiye'nin Siber Güvenlik Stratejileri

Hazırlayan: Atalay ÖCAL

ÖZET

Soğuk Savaş ve 11 Eylül sonrası dönemde internet kullanımının bireyler düzeyine kadar inmesi birçok faydanın yanı sıra yeni tehditleri ve riskleri de beraberinde getirmiştir. Siber uzay olarak adlandırılan bu yeni rekabet ortamında devletler ve bireyler için çeşitli tehditler ve riskler oluşmaya başlamıştır. İnsanoğlunun her geçen gün siber uzaya daha da bağımlı hale gelmesi bireylerin temel gereksinimlerinden olan güvende olabilme ihtiyacını tetikleyerek bu alanda ki güvenlik kaygılarının oluşmasına sebep olmuştur. Bu rekabetçi ortamda devletlerin temel aktör olarak varlıklarını sürdürmelerinin yanı sıra devlet dışı aktörlerinde ortamda yerini almasıyla geleneksel aktör algılamalarında köklü değişimler yaşanmıştır. Sisteme dahil olan devlet dışı aktörlerin bazılarının kötü emeller gütmesi siber uzay içerisinde güvenliğe yönelik endişeler yaşanmasına yol açmıştır. Başta kamu olmak üzere özel sektör bireyler ekseninde de siber uzay içerisinde güvende olabilme normu hayati bir öneme sahip olmuştur.

Devletler bu ortamda varlıklarının devamını sağlayabilmek için kendi savunma sistemlerini kurarak kargaşanın hâkim olduğu siber uzay içerisinde tehditleri ve riskleri oluşmadan kontrol altından tutabilecek siber güvenlik stratejilerini ve politikalarını belirlemekle yükümlüdürler. Bu stratejilerin ve politikaların belirlenmesi safhasında daha önceden gerçekleşmiş siber saldırıların detaylı analizleri yapılarak, uluslararası ilişkiler perspektifinde ki rolü ve kapsamı çerçevesinde değerlendirilerek olması mümkün siber saldırılara ve tehditlere karşı ulusal bilinç düzeyinin ve güvenlik kapasitesinin artırılmasıyla ilgili faaliyetleri gerçekleştirmesi gerekmektedir. Buna ek olarak siber güvenlik kavramının ana

oluşumlarının iyice kavranması, literatür içerisinde yaşanan kavram kargaşasını kaldıracak ve siber güvenlik kavramının daha net bir biçimde anlaşılmasını sağlayacaktır. Gerçekleşen siber olayların sebeplerinin ve sonuçlarının detaylı analiz edilmesi uluslararası ilişkiler disiplini içerisinde siber güvenlik unsurunun ne denli önemli olduğunu ortaya koyacaktır.

Uluslararası örgütler ve devletler düzeyinde yapılan siber güvenlik politikalarını ve stratejilerini daha net bir biçimde kavrayarak ulusal siber güvenlik ekosistemini kurmak, devletlerin siber güvenlik alanında yapması elzem olan birincil amaçları içerisinde yer almalıdır. Bu çerçevede çalışmada, uluslararası ilişkilerde değişen güvenlik algısı ekseninde Türkiye'nin ulusal siber güvenlik stratejileri ve politikaları analiz edilecektir.

Anahtar Kelimeler: Siber Güvenlik, Siber Uzay, Siber Saldırı, Ulusal Siber Güvenlik Stratejileri, Güvenlik

Title of the Thesis: **Changing Understanding of Security in International Relations and Türkiye's Cyber Security Strategies**

Prepared by: Atalay ÖCAL

ABSTRACT

The decline of internet use to the level of individuals in the post-Cold War and post-September 11 period brought along new threats and risks as well as many benefits. In this new competitive environment called cyberspace, various threats and risks have begun to emerge for states and individuals. The fact that human beings become more and more dependent on cyberspace every day has triggered the need to be safe, which is one of the basic needs of individuals, and has led to security concerns in this area. In this competitive environment, there have been radical changes in the perceptions of traditional actors, as states continue to exist as the main actors, and non-state actors take their place in the environment. The bad intentions of some of the non-state actors involved in the system have led to concerns about security in cyberspace. The norm of being safe in cyber space has been of vital importance on the axis of individuals and the private sector, especially the public.

In order to ensure the continuation of their existence in this environment, states are obliged to establish their own defense systems and to determine cyber security strategies and policies that can keep threats and risks under control before they occur in cyberspace dominated by chaos. At the stage of determining these strategies and policies, it is necessary to carry out activities related to increasing the level of national awareness and security capacity against possible cyber attacks and threats by making detailed analyzes of previous cyber attacks and evaluating them within the framework of their role and scope in the perspective of international relations. In addition, a thorough understanding of the main formations of the concept of cyber security will remove the confusion in the literature and provide a clearer

understanding of the concept of cyber security. Detailed analysis of the causes and consequences of cyber incidents will reveal how important the cyber security element is in the discipline of international relations.

Establishing the national cyber security ecosystem by understanding the cyber security policies and strategies made at the level of international organizations and states more clearly should be among the primary objectives of the states in the field of cyber security. In this framework, in this study, Turkey's national cyber security strategies and policies will be analyzed in the axis of the changing perception of security in international relations.

Keywords: Cyber Security, Cyber Space, Cyber Attack, National Cyber Security Strategies, Security

ÖNSÖZ

"Uluslararası İlişkilerde Değişen Güvenlik Anlayışı ve Türkiye'nin Siber Güvenlik Stratejileri" Başlıklı tez çalışmasında uluslararası ilişkilerde değişen güvenlik algısı perspektifinde Türkiye'nin izlemiş olduğu siber güvenlik stratejilerinin analizi ortaya koyulmaya çalışılmıştır.

Eğitim hayatımda ve tez çalışmanın ortaya çıkmasında değerli bilgi, birikim ve tecrübelerini asla benden esirgemeyen danışman hocam Prof. Dr. Sibel Turan'a en içten teşekkürlerimi sunarım. Ayrıca, her türlü zorlukta koşulsuz, şartsız yanımda kıymetli aileme sabır ve destekleri için teşekkür ederim.

EDİRNE/2022

İÇİNDEKİLER

ÖZET….....i
ABSTRACT…..... iii
ÖNSÖZ v
İÇİNDEKİLER… vi
KISALTMALAR… x
TABLOLAR……...xii
GİRİŞ 1
BİRİNCİ BÖLÜM..... 5
1. ULUSLARARASI İLİŞKİLER DEĞİŞEN GÜVENLİK ALGISI 4
1.1. Tarihsel Süreç İçerisinde Güvenlik Kavramı ve Tanımı..... 5
1.2. Uluslararası İlişkilerde Geleneksel Güvenlik Algısı..... 11
1.3. Soğuk Savaş Dönemi ve 11 Eylül Sonrası Değişen Güvenlik Algısı 14
İKİNCİ BÖLÜM.....17
2. SİBER UZAYIN KAVRAMSAL ÇERCEVESİ.....17
2.1. İnternet Kavramının Ortaya Çıkışı..... 17
2.2. Siber Uzay Kavramı 18
2.3. Siber Tehdit ve Siber Saldırı 20
2.4. Siber Suç ve Siber Terörizm 22
2.5. Hacker Kavramı 24
2.5.1. Hacking 24
2.5.2. Hacker Çeşitleri..... 25
2.5.2.1. Siyah Şapkalı Hacker (Black Hat) 25
2.5.2.2. Beyaz Şapkalı Hacker (White Hat) 25
2.5.2.3. Gri ve Kırmızı Şapkalı Hackerlar (Gray Hat and Red Hat) 26
2.6. Siber Caydırıcılık 26
2.7. Siber İstihbarat ve Casusluk..... 27
2.8. Siber Savaş..... 28
2.9. Hibrit Savaş..... 30

2.10. Siber Güvenlik ve Siber Savunma 32
2.10.1. Kritik Altyapı Sistemlerinin Güvenliği 35
2.10.2. Uluslararası İlişkilerde Siber Güvenlik Kavramı 37
2.10.3.Siber Saldırı Silahları 38
2.10.3.1. Zararlı Yazılımlar 39
2.10.3.2. Bakteri 40
2.10.3.3. Solucanlar 40
2.10.3.4. Virüsler 40
2.10.3.5. Truva Atı 41
2.10.3.6. Mantık Bombası 41
2.10.3.7. Arka Kapı 42
2.10.3.8. Bot, Botnet, Zombi, Köle Bilgisayar 42
2.10.3.9. Kök Kullanıcı Takımı 42
2.10.3.10. Fidye Yazılım 43
2.10.3.11. Casus Yazılımlar 43
2.10.3.12. Gelişmiş Sürekli Tehditler 43
2.10.3.13. Klavye Takipçisi 44
2.10.4. Siber Saldırı Yöntemleri 44
2.10.4.1. Dos ve DDos Saldırıları 45
2.10.4.2. Oltalama, Yemleme ya da Sazan Avlama Saldırıları 46
2.10.4.3. Sosyal Mühendislik 46
2.10.4.4. Yığın e-posta (Spam mail) 47
2.10.4.5. Sıfırıncı Gün Saldırıları (Zero Day) 47
2.10.4.6. Kabloyla Saplama Yapma (Wire Tapping) 47
2.10.4.7. Ip Sahteciliği 48
2.10.4.8. Açık Mikrofon Dinleme Yöntemi 48
2.10.4.9. Oturum Çalma 48
2.10.4.10. Zararlı Yazılımlar 49
2.10.4.11. Tuzak Kapı Saldırıları 49
2.10.4.12. İnternet Servis Saldırıları 49
2.10.4.13.Trafik Analizi Yöntemi 50

2.10.4.14.Kriptografik Sistemlere Yönelik Saldırılar 50
2.10.4.15. Zamanlama Saldırıları 50
2.10.5. Siber Güvenlik Sistemleri 51
2.10.5.1. Kimlik Doğrulama Sistemleri 51
2.10.5.2. Zafiyet Tarayıcısı Sistemler 52
2.10.5.3. Güvenlik Duvarı 53
2.10.5.4. Saldırı Tespit ve Koruma Sistemleri 53
2.10.5.5. Antivirüs 54
2.10.5.6. Yığın E-posta Engelleme Sistemleri 54
2.10.5.7. Veri Kaçağı Önleme Sistemi 54
2.10.5.8. Hava Boşluğu Sistemi (Air Gap) 54
2.10.5.9. Adli Bilişim Sistemleri 55
2.10.5.10. Ağ Erişim Kontrol Sistemleri 55
2.10.5.11. İçerik Filtreleyici Sistemler 55
2.10.5.12. Uç Nokta Güvenliği Sistemi 56
2.10.5.13. Stenografi Sistemi 56
2.10.5.14. Bal Küpü Sistemi 56
2.10.5.15. Güvenlik Veri ve Vaka Yönetim Sistemleri 57
2.10.5.16. Kriptolama Sistemleri 57
2.10.5.17. Sayısal İmza 58
2.10.5.18. Siber Olaylara Müdahale Ekibi 58
2.10.5.19. Elektromanyetik Güvenlik Sistemleri 59
ÜÇÜNCÜ BÖLÜM 60
3. TÜRKİYE'DE YAPILAN SİBER GÜVENLİK ÇALIŞMALARI 60
3.1. 2013-2014 Ulusal Siber Güvenlik Strateji Belgesi 63
3.2. 2016-2019 Ulusal Siber güvenlik Strateji Belgesi 67
3.3. 2020-2023 Ulusal Siber Güvenlik Strateji Belgesi 72
3.4. Türkiye'de ki Kurum ve Kuruluşların Siber Güvenlik Alanında ki Faaliyetleri 75
3.4.1. Bilgi Teknolojileri ve İletişim Kurumu 75
3.4.2. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu 77
3.4.3. Emniyet Genel Müdürlüğü 78

3.4.4. Millî İstihbarat Teşkilâtı 78
3.4.5. Türk Silahlı Kuvvetleri 79
3.4.6. Ulusal Siber Olaylara Müdahale Merkezi 80
3.4.7. Siber Güvenlik Kurulu 80
3.4.8. Afet ve Acil Durum Yönetimi Başkanlığı 81
3.5. Türkiye'de Faaliyet Gösteren Hacker Gruplarının Analizi 82
3.5.1. Ayyıldız Team 83
3.5.2. Turk Hack Team 85
3.5.3. RedHack 86
3.5.4. B3yaz Hacker 86
3.5.5. Cyber Warrior (Akıncılar) 87
3.5.6. Türk Güvenliği 89
3.6. Türkiye'ye Yönelik Yapılan Siber Saldırı Örnekleri 89
3.6.1. Anonymous grubunun Türkiye'ye Yönelik Tehditleri 90
3.6.2. Rus Uçağının düşürülmesi Sonucu Yaşanan Siber Saldırılar 91
3.6.3. Türk Telekom ve Garanti BBVA Bankası Siber Saldırıları 92
3.6.4. E-ticaret Sitelerine Yönelik Siber Saldırı İddiaları 93
3.6.5. Yemeksepeti'ne Yönelik Siber Saldırı 94
3.7. Küresel Siber Güvenlik Endeksinde Türkiye 95

SONUÇ…. 99
KAYNAKÇA 102

KISALTMALAR

ABD: Amerika Birleşik Devletleri

SSCB: Sovyet Sosyalist Cumhuriyetler Birliği

ARPA: The Advanced Research Projects Agency- Gelişmiş Araştırma Projeleri Ajansı

ARPANET: Advanced Research Project Agency Network- Gelişmiş Araştırma Projeleri Ajansı Ağı

MILNET: Military Network- Askeri Ağ

CERN: Conseil Européen pour la Recherche Nucléaire- Avrupa Nükleer Araştırma Merkezi

Http: Hyper Text Transfer Protocol- Hiper Metin Transfer Protokolü

MIT: Massachusetts Institute of Technology- Massachusetts Teknoloji Enstitüsü

PENTAGON: Amerika Birleşik Devletleri Savunma Bakanlığı

SCADA: Supervisory Control and Data Acquisition - Merkezi Denetleme Kontrol ve Veri Toplama Sistemi

TDK: Türk Dil Kurumu

ITU: International Telecommunication Union- Uluslararası Telekomünikasyon Birliği

DCS: Distributed Control System- Dağıtık Kontrol Sistemi

ICS: Industral Control System- Endüstriyel Kontrol Sistemleri

DDOS: Distributed Denial of Service- Dağıtık Hizmet Dışı Bırakma

DOS: Denial Of Service- Dağıtık Hizmet Dışı Bırakma

SOME: Siber Olaylara Müdahale Merkezi

TCK: Türk Ceza Kanunu

UEKAE: Ulusal Elektronik ve Kriptoloji Enstitüsü

MGK: Milli Güvenlik Kurulu

TÜBİTAK: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

SGK: Siber Güvenlik Kurulu

SGE: Siber Güvenlik Enstitüsü

USOM: Ulusal Siber Olaylara Müdahale Merkezi

UDHB: Ulaştırma, Denizcilik ve Haberleşme Bakanlığı

BTK: Bilgi Teknolojileri ve İletişim Kurumu

TİB: Telekomünikasyon İletişim Başkanlığı

EGM: Emniyet Genel Müdürlüğü

MİT: Millî İstihbarat Teşkilâtı

JGK: Jandarma Genel Komutanlığı

APT: Advanced Persistent Threat- Gelişmiş Sürekli Tehdit

İLTAREN: İleri Teknoloji Araştırma Enstitüsü

YTE: Yazılım Teknolojileri Araştırma Enstitüsü

TSK: Türk Silahlı Kuvvetleri

NATO: The North Atlantic Treaty Organization- Kuzey Atlantik Antlaşması Örgütü

ODTÜ: Orta Doğu Teknik Üniversitesi

MASAK: Mali Suçları Araştırma Kurumu

MEBS: Muhabere Elektronik ve Bilgi Sistemleri

AFAD: Afet ve Acil Durum Yönetim Başkanlığı

KAUBA: Avrupa Birliği Kritik Altyapı Uyarı Bilgi Ağı

TBMM: Türkiye Büyük Millet Meclisi

KVKK: Kişisel Verilerin Korunması Kanunu

-TABLOLAR-

Tablo 1: Siber Ortamın Bileşenleri 19
Tablo 2: Siber Tehditleri 21
Tablo 3: Siber Suç, Siber Terör ve Siber Savaşın Temel Özellikleri 29
Tablo 4: Savaşların Tarihsel Süreci 31
Tablo-5: Siber Güvenlik Nedir? 32
Tablo 6: CIA Üçlüsü 34
Tablo 7: Zararlı Yazılımlar Tablosu 39
Tablo 8: Siber Saldırı Yöntemleri 44
Tablo 9: Kimlik Doğrulama Sistemleri 51
Tablo 10: Bal Küpü Sistemi 57
Tablo 11: 2016-2019 Ulusal Siber Güvenlik Stratejik Eylem Planı 71
Tablo 12: 2020-2023 Ulusal Siber Güvenlik Stratejisi Oluşturulurken Belirlenen Ana Hedefler 73
Tablo 13: 2020-2023 Ulusal Siber Güvenlik Strateji Belgesinin Hedefleri 74
Tablo 14: 2017 Yılı Küresel Siber Güvenlik Endeksi… 97
Tablo 15: 2018 Yılı Küresel Siber Güvenlik Endeksi 98

GİRİŞ

1648 Vestfalya Antlaşmasıyla beraber uluslararası sistemde devletler en güçlü aktör konumuna gelmişlerdir. Değişen ve dönüşen bu sistemde devletlerin üzerinde hiçbir güç otoritesinin bulunmadığı ve kargaşanın hâkim olduğu ortamda ise devletin birincil görevinin varlığının devamını temin edecek olan güvenliğini sağlama hususu olduğu kabul edilmiştir. Fakat güvenlik kavramının net bir tanımının ve çizgisinin olmayışı bu kavram özelinde yaklaşımların çeşitlenmesine ve farklılaşmasına yol açmıştır.

Geleneksel güvenlik anlayışında ulusal ve uluslararası güvenliğe yapılan vurgu, Soğuk Savaş döneminin bitişi sonrası gerçekleşen küreselleşme olgusunun beraberinde getirdiği etnik çatışmalar, terörizm, çevre sorunları, bölgesel çatışmaların yanı sıra internet kullanımının bireyler düzeyine kadar inip yaygınlaşmasıyla birlikte siber kaygılarda oluşturmuştur. Siber uzay olarak adlandırılan bu yeni rekabet sahasında ortam ulus devletlerin kontrolünden çıkıp, etkin aktörlerin arttığı bir ortam haline gelmiştir. Klasik tipte ki güvenlik anlayışını bırakmak zorunda kalan uluslararası örgütler, devletler, kurum ve kuruluşlar mevcutlarında bulunan kritik altyapılarını ve bilgi sistemlerini siber tehditlere karşı koruyabilmek adına siber güvenlik olgusu üzerine çalışmalarını artırmak zorunda kalmışlardır. Siber uzayda yaşanabilecek olası siber saldırıların etkilerini minimum düzeyde tutabilmek amacıyla kritik altyapıların ve sistemlerin analiz edilmesi ve bunların güvenliklerinin tesis edilmesinin yanında hukuki ve stratejik eylemlerin oluşturulması gereklilik halini almıştır.

21.yüzyılla birlikte bilgi ve iletişim teknolojilerinde yaşanan gelişmeler sonucu bu teknolojilerin gelişiminde ve yayılmasında süratli bir ivmelenme süreci yaşanmıştır. Bireylerden kurum ve kuruluşlara kadar hemen hemen herkes için bu teknolojiler hayatın ayrılmaz birer parçası haline gelmişlerdir. Temelde çok büyük faydalar sağlayacağı düşüncesiyle oluşturulmuş bu siber ortam kötü niyetli kullanıcıların

amaçları doğrultusunda yaptıkları kötücül faaliyetler sonucu siber ortamı güvensizliğin hâkim olduğu bir yapıya dönüştürmüştür.

Siber ortam yaşanan bu gelişmeler neticesinde siber saldırılara ve tehditlere açık hale gelmiş bir ortama dönüşmüştür. Oluşan bu yeni kargaşa ortamında bireyler, kurumlar, kuruluşlar, devletler ve uluslararası örgütler siber güvenlik ve savunmaya yönelik faaliyetlerini artırmışlardır. Günümüzde siber güvenlik kavramı en önemli gündem unsurlarından biri haline gelmiştir. Gelecekte de yaşanan gelişmeler ışığında siber güvenlik kavramının önemi giderek daha da artacaktır.

Çalışmanın birinci bölümünde, 1648 Vestfalya Antlaşmasıyla birlikte oluşturulan geleneksel devlet eksenli güvenlik anlayışının süreç içerisinde günümüze kadar yaşamış olduğu değişim ve dönüşüm analiz edilmiştir. Ayrıca günümüz güvenlik kavramının oluşumu, kavramın tarihi kökenleri ve dönüşümü gibi hususlara da değinilecektir. Son olarak da Soğuk Savaş dönemi sonrası ve 11 Eylül Saldırıları sonrası dünyada değişen güvenlik algıları üzerinde durulacaktır.

Çalışmanın ikinci bölümünde, siber uzay kavramı ve bu kavramın bileşenlerini oluşturan siber suç, siber tehdit, siber caydırıcılık, siber casusluk, siber güvenlik ve savunma, hacker kavramı, siber saldırı yöntemleri ve siber savunma yöntemleri üzerinde detaylı bir şekilde durulacak olup, konunun daha net anlaşılabilmesi için kavramsal çerçevesi çizilecektir. Ayrıca uluslararası ilişkilerde siber uzay kavramının yeri ve önemi hususunda analiz yapılacaktır.

Çalışmanın üçüncü ve son bölümünde ise, Türkiye'nin kronolojik bir sıra içerisinde siber uzayla tanışması ve bu alanda yaptığı çalışmaları ortaya koyulacaktır. Türkiye'nin Estonya'da yaşanan büyük siber saldırılar sonucu siber uzayda almış olduğu güvenlik önlemleri ve yayınlamış olduğu strateji planları ele alınacaktır. Türkiye'de ki kurum ve kuruluşların siber uzay içerisinde ki görev ve sorumlulukları

ayrıca ortaya koyulacaktır. Türkiye'nin yaşamış olduğu siber saldırılar ve bu saldırıların sonuçları irdelenecek olup Türkiye'de faaliyet gösteren hacker gruplarının potansiyelleri ve etkileri ortaya koyulmaya çalışılacaktır. Son olarak ise, Türkiye'nin siber güvenlik adına yaptığı tüm çalışmalar değerlendirilip Küresel Siber Güvenlik Endeksi ışığında dünyada ki diğer rakiplerine göre konumu ve bu sıralamada ki yıllara göre olan değişimi ele alınıp, Türkiye özelinde ulusal siber güvenlik bilincinin oluşturulması amaçlanmaktadır.

Bu çalışma oluşturulurken kitaplar, güncel bilimsel makaleler, dergiler ana kaynakça yapısını oluştururken birincil kaynak olarak Türkiye Cumhuriyeti'nin yapmış olduğu mevzuatlar ve siber güvenlik strateji belgelerinden yararlanılmıştır. Ayrıca çalışma güncel veriler ışığında oluşturulması gerektiği için internet tabanlı açık kaynaklar, gazeteler, haberler ve kurum, kuruluşların demeçlerinden faydalanılmıştır. Çalışmanın oluşturulma aşamasında siber güvenlik alanında faaliyet gösteren kurum ve kuruluşlarla görüşme sağlanmaya çalışılsa da dünyada yaşanan koronavirüs salgını sebebiyle görüşmeler için olumlu geri dönüşler alınamamıştır.

"Uluslararası İlişkilerde Değişen Güvenlik Anlayışı ve Türkiye'nin Siber Güvenlik Stratejileri" başlıklı çalışmada hedeflenen amaçlardan biri, siber uzay kavramı ve bu kavramın bileşenlerinin ne olduğu, siber güvenlik kavramının uluslararası ilişkiler disiplini içerisinde ki yeri ve önemini okuyuculara aktarabilmek ve bu konuyla ilgili olarak bilincin ve farkındalığın oluşmasına katkı sağlamaktır. Türkiye'de geçmişte yaşanmış siber saldırılar ışığında gelecekte yaşanması muhtemel olaylar için alınması gereken tedbirlerin ve önlemlerin bireyden başlayarak tüm topluma kadar yayılıp, ulusal siber güvenlik bilincinin oluşturulması hedeflenmektedir. Yapılan bu çalışma çerçevesinde Türkiye Cumhuriyeti ve vatandaşları özelinde siber güvenlik kavramı perspektifinde olumlu katkılar sunması amaçlanmaktadır.

1.ULUSLARARASI İLİŞKİLERDE DEĞİŞEN GÜVENLİK ALGISI

Güvende olma arzusu, yeme, içme ve barınma gibi temel insani gereksinimler arasında yer almaktadır. Abraham Maslow'un ihtiyaçlar hiyerarşisi sisteminde fizyolojik ihtiyaçların ardından insanın en temel ikincil ihtiyacı olarak yer almaktadır. İnsanın güvende olma arzusu giderilmeden bir sonraki basamak ihtiyaçlarının giderilebilmesi olanaksız olmaktadır. Fizyolojik ihtiyaçları karşılanabilen bir bireyin güvende olma ihtiyacı karşılanmadan bir sonraki ihtiyaçları olan sevgi, aitlik, saygı gibi sosyal ihtiyaçları oluşmamaktadır. Maslow'un da çalışmasında belirttiği gibi güvende olabilmek kişiliğin getirmiş olduğu temel bir ihtiyaçtır.[1]

Tarihin her anında önemli olan güvenlik temelde kişinin güvenliğiyle başlamış olup, insanların toplumsal yaşama geçmeleriyle beraber toplumsal güvenlik anlayışına dönüşmüştür. Toplumsal güvenlik hem kişilerin hem de içinde bulundukları toplulukları bakımından yaşamlarının vazgeçilmez bir unsuru olmuştur. İnsanların ve toplulukların yerleşik hayatı oluşturmalarıyla beraber ilişkilerinde huzur, emniyet ve düzen gereksinimi oluşmuştur. Bu çerçevede toplumsal kuralların devamlılığının tesisi için görevli kişi ve kurumlar kurulmuştur. Devletler oluşturdukları kanunlar vasıtasıyla güvenliğin ve kamusal düzenin devamı için kişilerin özgürlüklerini sınırlayabilen önlemler alabilmektedirler. Demokratik toplum anlayışında refah ve güven içinde yaşayabilme arzusu kişisel önceliklerde en ön sırada yer almaktadır.[2]

---

[1] Sedat KULA, Bekir ÇAKAR "Maslow İhtiyaçlar Hiyerarşisi Bağlamında Toplumda Bireylerin Güvenlik Algısı ve Yaşam Doyumu Arasındaki İlişki", *Bartın Üniversitesi İ.İ.B.F. Dergisi*, Cilt no:6, Sayı :12, yayın yılı: 2015 s:194.

[2] Ahmet Hamdi Aydın, "Toplumsal Güvenlik ve Yerel Siyaset", *Yerel Siyaset*, 1. Baskı, Okutan Yayıncılık, İstanbul 2008, s.307.

Küreselleşmeyle beraber bireylerin ve devletlerin güvenliklerine yönelik tehdit ve tehlikelerde çeşitlenmiştir. Terörist faaliyetler, nükleer felaketler, salgın hastalıklar, çevresel sorunlar, siber saldırılar ve göç gibi farklı düzeylerde ve etki alanlarına sahip tehdit ve tehlikeler güvenlik sorunlarına neden olarak toplumsal yaşamı etkilemiştir. Güvenlik kavramı hem devletler hem de bireyler ekseninde tehdit ve tehlikeler ile mücadelede kullanılan bir kavram olması sebebiyle toplumsal yaşamın kalbinde yer almaktadır. Toplumsal düzenin oluşturulması ve bu düzenin sürdürülebilir kılınması için güvenlik unsuru bu yapının olmazsa olmazları içerisinde yer almaktadır. Kişilerin ya da devletlerin herhangi bir siyasi oluşum içerisinde benliklerini tehdit ve tehlikelerden uzak hissetmeleri güvenlik yapısının ulaşmak istediği asıl amaçtır.[3] Bu amaca ulaşmadaki uygulanan tehdit ve tehlikelerle mücadele yöntemi, dönemin ve ortamın algılayışına göre farklılıklar göstermektedir. Uluslararası ilişkiler disiplini içerisinde de tarihsel süreçte tehdit ve tehlikelere paralel olarak güvenlik algılamasında değişimler ve dönüşümler gerçekleşmiştir.

1.1. Tarihsel süreç içerisinde güvenlik kavramı ve tanımı

Güvenlik kavramı geçmişten günümüze kadar insan yaşamının her alanında birey merkezli bir yapı olarak varlığını devam ettirmektedir. Maslow'un da ihtiyaçlar hiyerarşisi çalışmasında yer verdiği gibi güvende olma ihtiyacı hayatın her alanında farklı biçimleriyle kendine yer bulmaktadır.[4] Temel gereksinimler içerisinde yer alan güvenlik; devlet, toplum ve birey düzeyinde değişkenlere sahiptir. Bu yüzden güvenliğin çok yönlü ve esnek bir kavramsal yapısı vardır. En temelde Türk Dil Kurumu sözlüğüne bakıldığında güvenlik;

> *"Toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu"*

[3] Salih Elmas, "Modern *Toplumun Güvenlik Çıkmazı: Tehdit, Risk ve Risk Toplumu perspektifinde Güvenlik*", Uluslararası Stratejik Araştırmalar Kurumu Yayınları, Ankara 2013, s.34.
[4] Sedat Kula, Bekir Çakar, *a.g.m*. s.194.

Olarak tanımlanmaktadır.[5] Bu tanımlama bağlamında güvenlik unsurunun fiziksel ve psikolojik boyutlarının bulunduğu anlamlandırılabilmektedir. Tarihsel süreç içerisinde ağırlıklı olarak güvenliğin fiziksel boyutu ele alınmıştır ve bu yaklaşım çerçevesinde devletlerin güvenlik algılarının temelinde kendi fiziki sınırlarını diğer devletlere karşı koruma algısı oluşturmuştur.[6]

Güvenlik kavramına ilk bakıldığında, güvenlik kavramının tartışmalı bir kavram olduğu göze çarpmaktadır. Bu tartışmanın sebebi olarak ise güvenlik kavramının ortak bir tanımının yapılamayacağına dair kuşkular yatmaktadır. Uluslararası ilişkiler disiplini içerisinde bazı uzmanlar ve devlet adamları güvenlik olgusunu tanımlamaya çalışırken günün şartları çerçevesinde tanımlamalar yapmaya çalışmışlardır. Ayrıca her devletin güvenliği tanımlarken kendi güvenlik riskleri çerçevesinde bir tanımlama yapacağı aşikardır. Bu perspektif içerisinde her bir devlet için tehdit algılamaları farklılaşacağından dolayı birbirine benzer fakat derinliğinde birbirinden ayrışan güvenlik tanımları görülmektedir.

En genel haliyle güvenlik kavramına bakıldığında güvenlik;[7]

"*Güvensizlik ihtimallerinin ortadan kaldırılması durumu*"

Olarak tanımlanmaktadır. Fakat bu tanımlama özelinde unutulmaması gereken husus güvenliğin beklenti ve algılar çerçevesinde gelişen ve çoğu zaman geçmişten gelen tecrübelerden beslenen bir kavram olduğudur. Ayrıca güvenlik kavramı, yeni

[5] Türk Dil Kurumu Sözlükleri, Güvenlik nedir? *https://sozluk.gov.tr/,* (Erişim Tarihi:17.01.2022).
[6] Çağrı Erhan, "Soğuk Savaş sonrası ABD'nin Güvenlik Algılamaları", "*Uluslararası Güvenlik Sorunları ve Türkiye*", Derleyenler: Refet Yinanç, Hakan Taşdemir, Seçkin Yayıncılık, Ankara 2002, s. 58.
[7] Beril Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 4.Baskı, Yeni yüzyıl Yayınları, İstanbul 2020, s. 29.

gelişen tehdit ve risklere karşı esnek bir yapıda olup farklı anlamlar taşıyabilen bir kavramdır.[8]

Etimolojik olarak bakıldığında güvenlik kavramı Latince kökenli se (olmaksızın) ve Cura (endişe) kelimelerinden türetilmiş bir kavramdır. "*Endişe olmaksızın*" yani "*securitas*" kavramı tarihin farklı zamanlarında çeşitli coğrafyalarda farklı şekillerde karşımıza çıkmıştır. Güvenlik kavramı, psikoloji ve felsefe literatüründe ilk defa Cicero ve Lucretius aracılığıyla gündeme getirilmiştir. 1.yüzyıl ile birlikte siyasi bir kavram yapısında "*Pax-Romana*" kavramından bahsedilmiştir. Kavramın bir başka oluşumu ise Thucydides'in oluşturduğu ve Thomas Hobbes tarafından şekillendirilen otoriter ve güçlü devlet anlayışının şekillendirilmesiyle oluşmuştur. Günümüzün güvenlik kavramının bu üç düşüncenin birleşimiyle oluşturulduğu söylenmektedir. İlk aşamada Atinalıların, imparatorluklarını ayakta tutma çabaları, ikinci aşamada Romalıların siyasi ve dini bir yapıda oluşturdukları "*securitas*" kavramı, üçüncü aşamada ise Hobbes'un felsefi bir düşünce yapısında oluşturmuş olduğu Leviathan'dır.[9]

Günümüzün güvenlik anlayışına yakın olarak "*securitas*" kelimesini ilk defa Cicero kullanmıştır. M.Ö 1.yüzyılın sonlarında "endişeden uzak olma, kayıtsızlık" anlamlarında ki "*Securus*" kelimesinden türetilerek "*securitas*" olarak oluşturulduğu düşünülmektedir. Cicero "*securitas*" kelimesini felsefi bir anlayışla mutlu hayat biçiminde oluşturmuştur. Cicero'nun bu anlayış yapısına göre kişilerin mutlu olabilmeleri ve toplumda ki prestijlerini sağlamaları ancak korkunun olmayışı yani güvende olabilme durumuyla ilişkilendirilmiştir. Cicero'nun tanımlamalarına ek olarak Roma imparatoru Ausgustus Cesar Roma'da barış ve huzur ortamını "*securitas*" kelimesiyle açıklamıştır. Cesar'ın bu kullanımı

[8] *a.g.e.* s.28.
[9] Hans Günter Brauch, "Güvenliğin Yeniden Kavramsallaştırılması: Barış, Güvenlik, Kalkınma ve Çevre Kavramsal Dörtlüsü", *Uluslararası İlişkiler Dergisi*, Cilt 5, Sayı 18 (Yaz 2008), s.3.

kelimeye siyasi bir yapı katmıştır.[10] Bu anlayışla "*securitas*" kavramının merkeze oturtulduğu imparatorların koruması altında güvende olunduğu anlamında "*Pax-Romana*" Roma Barışı kavramı oluşturulmuştur. Teolojik açıdan "*securitas*" kavramı Augustinus ve Tertullianus tarafından ele alınmış ve şüphe karşıtlığından doğan inancın güvencesi biçiminde bir anlam kazandırılmıştır. Roma imparatorluğu dönemi boyunca "*securitas*" kavramı "*Pax-Romana*" kavramıyla kullanılmıştır. Fakat Batı Roma imparatorluğunun yıkılmasının ardından teolojik anlamıyla Orta çağ boyunca olumsuz bir anlamda kullanılan bir kelime oluşmuştur.[11]

Orta Çağın sonlarına doğru Avrupa kıtasında savaşlarda ateşli silahların kullanılmasıyla beraber güvenlik kavramı ve güvenliğin sağlanmasına yönelik düşünce yapısı yeniden oluşmaya başlamıştır. Güvenlik kavramının teolojik yapısı 16. ve 17.yüzyılda gerçekleşen Reform hareketleri ve bilimsel buluşlar aracılığıyla değişmiştir.[12] Güvenlik kavramı, daha önce ki tanımlamalarının aksine çağın gereksinimlerine uygun bir biçimde Thomas Hobbes tarafından oluşturulmuştur. Hobbes, güvenlik kavramını oluştururken Thucydides'den etkilenmiştir. Thucydides'in yenilginin önlenmesi için her türlü yolun kullanılabileceği fikri Hobbes tarafından detaylıca irdelenmiştir. Hobbes yaptığı çalışmaların sonucu olarak insanları doğa hali ve toplum hali olarak iki parçada ele almış ve bu perspektifte siyaset teorisini oluşturmuştur. Teorisine göre insanoğlu doğasından kaynaklı olarak kötü ve bencil bir yapıdadır. Teorisini biraz daha derinleştiren Hobbes herkesin herkesle savaş durumunda olduğu bir ortam söz konusudur ve bu anarşik ortam son derece güvensizdir. Böyle bir doğal yaşam ortamında insanlar birbirleri için tehlike unsuru olmakta ve bu durum güvensizliği doğurmaktadır. Bu güvensizlik durumunun ortadan kaldırılabilmesi için bireylerin egemenliklerini bir üst otoriteye devrederek bütün yetki ve gücü siyasi bir merkezde toplamalarıyla mümkün olacağını belirtmiştir. Bu husus da toplum sözleşmesi olarak kurguladığı

[10] J. Frederik M. Arends, "Homeros'dan Hobbes ve Ötesine: "Güvenlik" Kavramının Avrupa Geleneğindeki Boyutları", *Uluslararası İlişkiler Dergisi*, Cilt 6, Sayı 22 (Yaz 2009), s.207-213.
[11] *Aynı Yerde.*
[12] Beril Dedeoğlu, *a.g.e*. s.49-51.

ve mutlak devleti simgeleyen ölümlü tanrı "*Leviathan*" sembolünü oluşturmuştur. Hobbes, bu yol ile bireylerin barış ve güvenlik arzularının karşılanabileceğini belirtmiştir. Fakat Hobbes'in belirtmiş olduğu devlet yapısında kişilerin özgürlüklerinin sınırlandırılabildiği belirtilmelidir. Hobbes'in kurguladığı güvenlik teorisinde devletin çıkarları ve güvenliği ön plandadır ancak bu yolla kişilerin güvenliklerinin sağlanabileceğinden söz edilmektedir.[13]

15.yüzyılın ikinci yarısıyla beraber güvenlik kavramı çağın gerekliliklerine uygun olacak şekilde evrilmiştir. Hobbes'un ortaya koymuş olduğu düşünce yapısı varlığını sürdürürken bunun yanında modern anlamda güvenlik kavramı ortaya çıkmaya başlamıştır. Güvende olabilme arzusu devrimler, savaşlar, krizler ve ideolojilerde yaşanan değişimler sonucunda yeni tür tehdit unsurlarıyla karşı karşıya kalmıştır. Bu süreçte güvenlik kavramı, Amerikan anayasasında özgürlüklerle ilintilenmiş, Fransız ihtilalinde ise dört ana insan hakkından biri olarak literatürde yerini almıştır. 19.yüzyılla beraber güvenlik kavramı ulusal ve küresel çapta çeşitli ayrışmalara ve kavrayışlara sebep olmuştur.[14]

Günümüzdeki güvenlik kavramının temeli kuramsal perspektiften 19.yüzyılın ikinci yarısından süre gelerek incelenebilmektedir. İki dünya savaşı ve sonrasını içeren dönemde güvenlik alanında yapılan çalışmalarda tehditlerin azaltılması ve bu tehditlerin bertarafı noktasında nasıl bir yöntem izlenmesi gerektiği üzerine çalışmalar yapılmıştır. Bu süreç içerisinde uluslararası işbirliği, demokrasi, silahsızlanma ve kolektif güvenlik gibi konularda çalışmalar yapılmıştır. Güvenlik politikalarının oluşturulması hususunda sivil hakları, demokratikleşme süreçleri ve ekonomi yönetimi üzerine konulara yer verilmiştir.[15]

---

[13] J. Frederik M. Arends, *a.g.m.* s.213.
[14] *Aynı yerde.*
[15] Zerrin Ayşe Bakan, Soğuk Savaş Sonrasında Yeni Güvenlik Teorileri ve Türkiye'nin Güvenlik Algılamaları, *21. Yüzyıl Dergisi,* Ekim/Kasım/Aralık 2007, s. 37-42.

İkinci Dünya Savaşı sonrası ve Soğuk Savaşı kapsayan dönem içerisinde güvenlik algısıyla ilgili iki kutuplu bir dünya düzeninin sonuçlarının irdelendiği bir dönemi kapsamaktadır. Bu dönemde yapılan çalışmalarda iki hegamon gücün mücadelesi ve bu mücadelenin bir sonucu olarak ortaya çıkan nükleer yarışın güvenlik üzerine etkilerine yönelik çalışmalar yapılmıştır. Yapılan çalışmalarda askeri tehditler ve çözümleri üzerine odaklanılmıştır. Bu dönemin göze çarpan güvenlik konusu askeri güç ve gücün maksimizasyonu ana güvenlik konusu olmuştur. Soğuk Savaşın bitiminin akabinde güç ve nükleer silahlar temelli güvenlik anlayışı terk edilmiştir. Bu dönemde ekonomik gelişmenin ve siyasal bütünleşmenin güvenlik üzerine etkisine vurgu yapılmıştır. Göç, kimlik, uluslararası suçlar ve askeri özelliği olmayan sorunlar güvenlik çalışmaları kapsamında ele alınmıştır. Bu dönem içerisinde geleneksel anlayış eleştirel bir bakışla ele alınmıştır. Dönemin önemli çalışmacıları arasında Barry Buzan, Ole Waever, Booth ve Ayoob yer almaktadır. Bu yeni akımda, değişen koşullar ekseninde devlet merkezli olmayan, sadece askeri konulardan ibaret olmayan post pozitivist temelli ve eleştirel teoriye dayalı yeni bir akım yaratılmıştır.[16] Dönemin önemli teorisyenlerinde olan Ole Waever'a göre güvenlik;

"*Güvenli, emniyetli olmak, tehdit altında olmamak*"

Gibi geleneksel bir anlama sahip olmasının yanında kavrama ulusal güvenlik ve güvenlik politikaları gibi imgesel anlamlarda yüklemiştir. Fakat güvenliğin kavramsallaştırılmasının geleneksel anlamı kullanılmasıyla ilgili olmadığını belirtmiştir. Tarihsel açıdan güvenliğe bakıldığında ise devletlerin birbirlerini tehdit ettiği, iradelerini birbirlerine dikte etmeye çalıştıkları ve egemenliklerini savundukları bir alan olarak ileri sürmüştür.[17]

[16] *Aynı Yerde.*
[17] Ole Waever "Securitization and Desecuritization", *International Security Volume 3: Widening Security*, Editörler: Barry Buzan, Lene Hansen, Londra Sage Publibations, Londra 2007, s. 69.

Ullman'a göre ise güvenlik kavramının yalnızca askeri unsurlar üzerinden tanımlanmasının yanıltıcı ve tehlikeli olabileceğini vurgulamıştır. Bu bakış açısıyla sadece askeri risklere odaklanmanın devletlerin çok daha büyük riskleri görmezden gelebileceğini ve bu durumun güvenlik riskine yol açacağını vurgulamıştır. Bu bakışın yanı sıra böyle bir yaklaşımın uluslararası ilişkilerin askerileştirilmesine sebep olacağını belirtmiş ve bu durumunda küresel güvensizlik ortamına neden olacağını açıklamıştır.[18]

Günümüzde güvenlik çalışmalarının üzerinde durduğu konular küresel ısınma, açlık, uluslararası terörizm, bölgesel savaşlar, salgın hastalıklar, çevresel felaketler, siber güvenlik tehditleri gibi konulara doğru evrilmiştir. Bu açıdan bakıldığında süreç içerisinde düşünürler güvenlik kavramının merkezine insanların güvenlik anlayışlarına paralel olarak çeşitli unsurlar yerleştirmişlerdir. Yaşanan bu durum neticesinde farklı dönemlerde farklı güvenlik anlayışları ortaya çıkmıştır.

1.2. Uluslararası ilişkilerde geleneksel güvenlik algısı

Vestfalya düzeninin kurulmasıyla beraber Orta Çağın feodal sistem yapısı kaldırılıp yerine devlet hâkim yönetici ve ulus egemen bir sistem oluşturulmuştur. Yaşanan bu tarihsel dönüşüm modern devlet yapısına doğru giden bir süreci yaratmıştır. Bu dönüşüm süreciyle birlikte yerel, bölgesel güç unsurlarının birbirine entegre olduğu ve sınırları belirli bir merkezi yapı sistemi oluşturulmuştur. Hâkim modern devlet yapısının yükselişiyle beraber uluslararası sistemde yeniden yapılandırılmıştır. Hâkim olan modern devletin gücünü koruyabilmesi için hakimiyetinin korunabilmesi uluslararası istikrarın belirleyici unsuru olmuştur. Bu yöntem ile dönem içerisinde çatışmalar ve savaşlar minimum

[18] Richard H. Ullman, "Redefining Security", International Security, Cilt:8 No:1, Yaz 1983, ss. 129-130.

düzeyde tutulabilmiştir. Vestfalya düzeninin kurulması haricinde Fransız ihtilali ve akabinde oluşan Napolyon savaşları tehdit ve risk algısının yeniden yorumlanmasında önemli bir unsurdur. Yaşanan bu yeni tehdit ve risk ortamında devletler benliklerini koruyabilmek adına diplomatik ve askeri unsurların devreye alınmasının önemli olduğunun kanısına varmışlardır.[19] Bu şekilde devletin hakimiyeti yolunda toprak bütünlüğüyle birlikte ulus kavramının da önemli olduğu vurgulanmış ve devletler uluslararası sistemin belirleyici aktörleri olmuşlardır. Güvenlik, askeri ve stratejik anlamda algılandığı süre boyunca devletlerin birinci vazifeleri olarak anlamlandırılmıştır. Realist perspektifte güvenliği gücün artırılmasının bir sonucu biçiminde açıklamıştır.

Birinci Dünya Savaşı'nın ortaya çıkması devletlerin izlediği güç temelli politikalarının uluslararası sistemin ve kendi güvenliklerinin korunmasında yetersiz kaldığı düşüncesini ortaya çıkarmıştır. Savaş sonrası uluslararası barış ve güvenliği yeniden oluşturabilmek için uluslararası hukuk normlarından ve örgütlerden oluşacak bir yapının oluşturulması düşüncesi hâkim olmuştur. Bunun yanında dönemin Amerikan Başkanı W. Wilson'un ortaya attığı On Dört İlke prensibi de yaşanabilecek saldırıları ortak bir yapıda engellemek ve dünya barışını sağlamak gibi prensiplerini de içermekteydi. Wilson'un bu yaklaşımı Immanuel Kant'ın Liberal bakışının bir yansıması olarak algılanmıştır. İdealist teorisyenler hukuka ve ortak evrensel değerlere saygılı, Milletler Cemiyeti ve benzeri uluslararası örgütlerin hâkim olduğu bir uluslararası sistemin oluşturulması fikrini savunmuşlardır. İdeal bir dünya düzeni yaratılması olgusu etrafında birleşilmiştir.[20] Ne yazık ki 1930'lar ile Almanya ve İtalya'da güçlenen faşist yönetimlerin iktidarları ele geçirmeleri ve ekonomik temelli yaşanan güç mücadeleleri idealist bir düşünce sistemiyle düzenin ve güvenliğin sürdürülebilir olamayacağı algısını ortaya çıkarmıştır. İki savaş arası dönemde yaşanan idealist

[19] Barry Buzan, Lene Hansen, "The *Evolution of International Security Studies*", Cambridge University Press, New York 2009, ss.23-24.
[20] Güngör Şahin, *Soğuk Savaş Sonrası Değişen Güvenlik Anlayışı Bağlamında NATO*, (Trakya Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalı, Basılmamış Doktora Tezi), Edirne 2015, ss.45-46.

temelli düşünce yapısının başarısızlığı uluslararası sistemi güç ve çıkar ilişkileri merkezli realist bir bakış açısına dönüştürmüştür.[21]

Realist bakış açısı, güç, çıkar ve insan doğası temelli olup devleti ana aktör olarak konumlandırmaktadır. Realizmin güvenlik anlayışının merkezinde daimi bir güvensizlik algısı ve güvende olamama durumu yatmaktadır. Bu perspektif ile realizm devletlerin askeri güçleri ve çıkarları doğrultusunda daima tehdit ve risklere karşı hazırlık içerisinde olmaları gerektiğini ve bu yöntem ile varlıklarıyla ulusal güvenliklerini koruyabileceklerini savunmaktadır. Sürekli anarşinin hâkim olduğu sistem yapısında varlığını ve söylemlerini kabul ettirebilmenin yolunun güç ve kapasite artırımıyla mümkün olacağını belirtmiştir. Bu yolla realizm bireyin güvenliğinin sağlanabilmesi yolunda devletin ulusal güvenliğinin hâkim kılınması prensibini ortaya atmıştır. Soğuk Savaş döneminin yaratmış olduğu ortam realizmin güç ve kapasite artırımının süreklilik arz ettiği fikrine uygun olarak gelişmiştir.[22] Ancak Soğuk Savaş dönemi içerisinde de realizm fikri dönüşüme uğramıştır. Kenneth Waltz, 1979 yılında yayımlamış olduğu "Theory *of International Politics*" isimli kitabıyla dış politikayı sadece insan doğasına ve devlet kapasitesine indirgeyen görüşe, dış politikayı sadece birey eksenli değerlendiren Liberalizme ve üretim biçimiyle sınıf çatışmasını temel alan Markist görüşü eleştirmiştir. Waltz, uluslararası sistemin yapısını anarşik kabul edip, devletlerin amaçlarının varlıklarının devamını sağlamak ve hakimiyetlerini korumaları olarak belirtmiştir.[23] Neorealist bakış açısıyla realizm arasında güvenliğin sağlanması konusunda benzerlikler olmasının yanında temel bazı farklılıklar vardır. Örnek verilecek olursa realizm devletlerin güç mücadelelerini insanın doğası gereği olduğu anlayışından yola çıkarak değerlendirmektedir. Ancak Neorealizm'de devletlerin güç mücadelelerinin olduğu olgusunu kabul edip bunun temelinde yatan olgunun ise devletlerin içerisinde bulundukları anarşik

[21] Mustafa Aydın, "Uluslararası İlişkilerde Yaklaşım, Teori ve Analiz", *Uluslararası İlişkiler Dergisi*, Cilt:51, No:1, 1996, s. 92.
[22] Atilla Sandıklı, Bilgehan Emeklier, "Güvenlik Yaklaşımlarında Değişim ve Dönüşüm" s.6-7.
[23] Tayyar Arı, "*Uluslararası İlişkiler Teorileri: Çatışma, Hegemonya, İş birliği,* 8. Baskı, Mkm Yayıncılık, Bursa 2013, ss.157-164.

ortamda ki tehdit ve risklerden kaynaklandığı düşüncesini ortaya atmaktadırlar. Her iki anlayışında güvenlik politikalarının temelinde temel aktör devlet ve güç mücadelelerinin kaynağında var olan güvensizlik ortamının oluşturduğunu belirtilmektedir. Neorealistler sistem içerisinde ki güvensizlik ortamında yaratılacak hegemon bir güç aracılığıyla yok edilebileceğini savunmaktadırlar.[24] Soğuk Savaş döneminin gevşemeye başlamasıyla beraber devlet ve devlet dışı aktörlerin çoğalması sonucu sistemin yeniden yorumlanması gerekmiştir. Bu yorumlama küresel çapta varlığın devamı ve güvenliğin sağlanması hususunda ekonomi, kültür, siyaset gibi birçok alanda güvenliğin oluşturulmasını da beraberinde getirmiştir.[25]

1.3. Soğuk Savaş dönemi ve 11 Eylül Saldırısı sonrası değişen güvenlik algısı

Soğuk Savaş'ın bitmesinin ardından güvenlik kavramı en fazla üzerinde çalışılan konulardan biri olmuştur. Bu dönem içerisinde ortaya çıkan görüşlerde bir kesim Liberalizm ve uluslararası örgütlerin katkılarıyla barış ve işbirliğinin tesis edileceğini ortaya atmış, diğer kesim ise medeniyetler arası veya etnik kökenli çatışmaların artacağını ve silahların yayılması sonucu gelecekte anarşik ortamın oluşacağını söylemişlerdir. Fakat yaşanan bu yeni dönemle birlik tehditlerin ve risklerin hem nitelik hem de nicelik olarak başkalaşmasıyla birlikte güvenlik kavramının yeniden analiz edilmesi gerekmiştir. Güvenlik kavramının yeniden analizi hususunda eski dar düşünce kalıpları bir kenara atılıp, kavramın derinlemesine bir analizinin yapılması gerekmiştir. Sistemin yapısal dönüşümü iki

[24] John Baylis, "Uluslararası İlişkilerde Güvenlik Kavramı", "*Uluslararası İlişkilerde Çatışmadan Güvenliğe*", Editörler: Mustafa Aydın, Hans Günter Brauch, Mitat Çelikpala, 2. Baskı, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2012, s.155.
[25] Beril Dedeoğlu, *a.g.e*. s.78

kutupluluğu ortadan kaldırarak birden çok aktörün sistem içerisinde etkin olduğu bir hale bürünmüştür.[26]

Güvenlik kavramı askeri güvenlik anlayışından çıkıp daha karmaşıklaşmış ve bilgi güvenliğinden çevre güvenliğine kadar çok geniş bir alana kadar yayılmıştır. Bu genişleme sonucu devletler, devlet dışı aktörler ve bireylerde güvenlik kavramının oluşturulma safhasında ki analiz düzeylerinde değişimi olarak yerini almışlardır.[27] Bu yeni anlayış kavramı yolsuzluk, etnik çatışmalar, çevre sorunları, uluslararası uyuşturucu trafiği, insan kaçakçılığı, siber saldırılar, mali suçlar gibi çeşitli risk ve tehditler üzerine odaklanmaya itmiştir. Kavramın bu biçimde genişlemesi devlet temelli güvenlik anlayışlarını bir kenara atarak bireyleri güvenliğin merkezine oturtmuştur. Güvenlik kavramının bu yeni anlayışında denetime açıklık, hesap verebilirlik, şeffaflık, hukukun üstünlüğü vb. ilkeleri de benimsemesi beklenmektedir.[28]

Güvenlik sorunları Soğuk Savaş boyunca daima askeri güç perspektifiyle ele alınmış ve askeri güç unsurları devletlerin temel politikalarını oluşturmuştur. Devlet merkezli ve güç temelli uluslararası anarşik sistem yapısı bu dönemde etkili olsa da Soğuk Savaş sonrası dönemde küreselleşmenin de tetiklemesiyle tehdit ve risk algılamalarında çeşitlilikler oluşmuştur. Güvenlik kavramının çeşitlenmesi sonucu kültürel, nüfus, çevre, enerji sorunları ve ekonomik etkenler gibi kavramlar analiz düzeylerinde kendilerine yer bulmuşlardır.[29]

11 Eylül 2001 Tarihinde yaşanan terör saldırıları sonucunda güvenlik algılamalarında köklü bir değişim ve dönüşüm yaşanmıştır. Gerçekleşen bu terör

---

[26] Keıth Krause, Mıcheal Wıllıams*, "From* Strategy to Security: Foundations of Critical Security Studies", *Critical Security Studies: Concepts and Cases*, Unıversıty of Minnesota Press, 1997, s.33.
[27] Ergin Ergül, *Küresel Köyde Suç ve Adalet*, 1.Baskı, Adalet Yayınevi, Ankara 2008, s.176.
[28] Bedri Şahin, Değişen Dünya Düzenine Bağlı Olarak Değişen Uluslararası Güvenlik Algısı, *İmgelem,* Cilt :4, Sayı:6, 2020, s.197.
[29] Bedri Şahin, *a.g.m*. s. 198.

saldırıları güvenlik olgusunun kapsamına örgütlü suçlar, terör, uyuşturucu, insan kaçakçılığı, dini ve etnik çatışmalar, yasadışı göç, kitle imha silahlarının yaygınlaşması ve başarısız devletlerin varlığı gibi yeni risk ve tehditleri de eklemiştir.[30]

[30] *Aynı yerde.*

2.Siber Uzayın Kavramsal Çerçevesi

2.1.İnternet kavramının ortaya çıkışı

İnternet kavramı ABD ve SSCB'nin Soğuk Savaş dönemindeki askeri ve ideolojik rekabetinin bir ürünü olarak ortaya çıkmıştır. ABD bu dönemde teknolojik olarak üstünlük sağlayabilmek amacıyla bilimsel araştırmaların yapılabilmesi için ABD Savunma Bakanlığı Pentagon'a bağlı Gelişmiş Araştırma Projeleri Ajansı (*The Advanced Research Projects Agency* ARPA)'yı kurdu.[31] Daha sonraki süreçte 1962 yılında ajansın çalışma alanı büyüyüp üniversitelerin ve özel kuruluşlarında dahil edilmesiyle yeni bir yapı olarak ortaya çıkmaya başlamıştır. Bu yeni yapıda bağımsız olan bilgisayarların birbirleriyle iletişim kurabilmeleri için ARPANET (*Advanced Research Projects Agency Network*) ismiyle bir sistem oluşturulmuştur.[32] Sistem içerisindeki ilk veri transferi 1969 yılında gerçekleştirilmiştir. Pentagon tarafından kurulan bu sistem daha sonrasında INTRANET adıyla anılmıştır. Beklenenden çok daha hızlı bir gelişme gösteren bu sistemin askeri kısmı MILNET olarak ayrılmış, sivil kullanımlar için oluşturulan kısımına da INTERNET adı verilmiştir. INTERNET tüm ağların birleştirilmesiyle oluşmuş en büyük ağ olarak tanımlanmaktadır.[33]Internet'in ticari amaçlar için kullanımı 1 Ocak 1983 tarihinde TCP/IP (*Transmission Control Protocol and Internet Protocol)* protokolünün kurulmasıyla başlamıştır. İnternetin günümüzdeki yapısının oluşmasını sağlayan olay ise CERN'de çalışan İngiliz fizikçi Bernes Lee'nin laboratuvardaki elektronik belgelere kolayca uzaktan erişimi ve birden çok kullanıcının bu belgelere erişerek eksikleri giderebilmesi amacıyla ortaya çıkmıştır.[34] Bu amaç doğrultusunda 1989 yılında World Wide Web (www) ve Hypertext olarak bilinen http sistemini icat etmiştir. Robert Knake Clarke,[35] internetin

---

[31] Nezir Akyeşilmen, *Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik*, 1.Baskı, Orion Yayınları, Ankara 2018, ss. 26-27.
[32] *A.g.e.*ss.26-27.
[33]İstanbul Teknik Üniversitesi Bilgi İletişim Daire Başkanlığı, *İnternetin Tarihçesi*,7 Eylül 2013, *https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/internet'in-tarih%C3%A7esi,* (Erişim Tarihi: 07.01.2021).
[34] *A.g.e.* (Erişim Tarihi: 07.01.2021).
[35] Robert Knake Clarke ABD yönetiminin üst kademelerinde yıllarca görev yapmış bir güvenlik uzmanıdır.

askeri bir icat olmadığını aslında bunun 60`lı yıllarda MIT, Stanford ve Berkeley üniversitelerinde okumuş olan hippilerin icadı olduğunu öne sürmüştür.[36]Bugün hayatımızın ayrılmaz bir parçası olan ve hızla gelişen internet kavramının yararlarının yanında denetim zorluğu gibi sebeplerden dolayı kötü niyetli kullanıcıların yarattığı kargaşa ortamından kaynaklı birçok zararı da vardır.

2.2.Siber uzay kavramı

Siber alanı anlamak hususunda öncelikli olarak siber uzay kavramını anlayabilmek yararlı olacaktır. Siber uzayın tanımlanmasıyla ilgili olarak dünyada ortak bir kavram yapısı bulunmamaktadır. Gelişen teknoloji ile beraber siber uzayında kapsama alanı daha da artmakta, oluşan bu sonuç neticesinde ise kavramı tanımlayabilmek daha da zorlaşmaktadır. Siber uzay olarak tanımladığımız alanda dünyamızın içinde yer aldığı boşluk olan uzay akla gelmemelidir. Bu yüzden siber uzay kavramı siber ortam ya da siber alan şeklinde de literatürde tanımlanmaktadır. Siber uzay (Cyberspace) kavramı ilk olarak Amerikalı bilim kurgu yazarı William Gibson'ın 1982 yılında yayımladığı "*Burning Chrome*" adlı kitabında yer almıştır.[37] Yazar, siber uzayı sadece çağrışımdan ibaret olan anlamsız bir kelime olarak tanımlamıştır. Siber uzayı oluştururken yazar "*Şifre, önemsiz şey, sıfır*" anlamı oluşturabilecek "Cipher" (veya cypher) kelimesi ile oluşturup daha sonrasında "cyber" olarak nitelendirmiştir.[38] Siber uzayın net bir tanımlaması olmadığından çeşitli tanımlamaları bulunmaktadır. Bunlardan bazıları; P.W.Sınger ve Allan Frıedman'ın kitabında yer alan tanımlamaya göre siber uzay

> *"İçerisinde verilerin çevrimiçi olarak saklandığı, paylaşıldığı ve iletildiği, bilgisayar ağları ile kurulmuş bir sanal alemdir."*[39] *Bir başka siber uzay tanımına göre "İnternet ağları, kapalı askeri ağlar, enerji sistemleri ağları,*

[36] Robert Knake Clarke, *Siber Savaş*, Çeviren: Murat Erduran, İstanbul K.Ü Yayınları, İstanbul 2011, s. 45.
[37] Hasan Çiftçi, *Her Yönüyle Siber Savaş*, 2. Basım, Tübitak Yayınları, 2017 Ankara, s.3.
[38] *A.g.e.* s.3.
[39] P.W.Sınger- Allan Frıedman, *Siber Güvenlik ve Siber Savaş*, Çeviren: Ali Atav, Ankara 2015, s.29.

yazılım tabanlı sistemler gibi içerisinde yazılım ve donanım bulunduran yapılar bütünü"[40]

Olarak tanımlanmaktadır. Amerika Birleşik Devletleri Savunma Bakanlığı (Pentagon)'na göre ise siber uzayın tanımı

"İnternet ağları, bilgisayar sistemleri, dahili işlemci ve denetleyicileri içeren birbirleriyle etkileşim halindeki küresel bir yapıdır."[41]

Salih Bıçakçı'nın tanımlamasına göre basitçe siber uzay

"İnsanların birbirlerine bağlı ağlar aracılığıyla etkileşime geçtiği ya da sistemlerin kendi aralarında iletişime geçtiği fiziksel olmayan alan."[42]

Bilgi ve iletişim teknolojilerinin hızla geliştiği günümüzde bu tanımlamalar yetersiz kalmaktadır. Etkili bir tanım yapabilmek için siber uzayın tüm unsurlarını içine alan bir tanımlama yapılmalıdır. Bu türden tanımlarında yapılabilmesi ancak siber ortamı oluşturan bileşenlerin neler olduğunun belirtilmesiyle mümkün olmaktadır. Siber ortam sadece internet tabanlı olmayıp birden çok unsuru içermektedir. Siber ortamı oluşturan unsurlara bakıldığında yazılım, donanım ve iletişim altyapısı yer almaktadır.

Tablo-1: Siber Ortamın Bileşenleri[43]

Siber Ortamın Bileşenleri
Yazılım: İşletim ve veri tabanı yönetim sistemleri, Uygulama yazılımları, Yönetim yazılımları, Gömülü işlemciler
Donanım: Sunucular, Kripto sistemleri, SCADA sistemleri ve sensörleri
İletişim Altyapısı: Kablolu/kablosuz iletişim ağları, Telsiz sistemleri, Uydu sistemleri, Telekomünikasyon sistemleri ve internet

Kaynak: Hasan Çiftçi, *Her Yönüyle Siber Savaş*, 2. Basım, TÜBİTAK Yayınları, 2017 Ankara, s.5

[40] Ali Burak Darıcılı, *Siber Uzay ve Siber Güvenlik,* 1.Baskı, Dora, Bursa 2017, s.31
[41] Hasan Çiftçi, *a.g.e.,* s.4.
[42] Salih Bıçakçı, *21.yüzyılda Siber Güvenlik*, 1.Baskı, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2013, s.4.
[43] Hasan Çiftçi, *a.g.e.,* s.5.

Pantfinder'e göre yapılan bir başka tanımlamaya göre siber ortam içerisinde kendine özgün dört bileşen bulunmaktadır. Bu bileşenler, bilgi, fiziksel sistem, yazılım ve insanlardır. Bilgi ve onu kullanan insanlar siber ortam içerisindeki en önemli iki bileşendir.[44] Tüm bu veriler ışığında bütün siber uzay unsurlarını içine alabilen Türkiye'de ki siber uzay tanımı ise

> *"Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortamdır."*[45]

2.3. Siber tehdit ve siber saldırı

Siber uzay içerisinde olağan faaliyetleri tehlikeye atan ya da zarar veren unsurlar tehdit olarak değerlendirilmektedir. Tehditlerin amacı sistemlerin ya da verilerin gizliliği, erişilebilirliği veya bütünlüğünün bozulmasına yönelik faaliyetleri içermektedir. 2016-2019 Ulusal Siber Güvenlik Strateji Belgesine göre tehdit

> *"Bir kurumun ya da sistemin zarar görmesiyle neticelenecek istenmeyen bir olayın olma potansiyeli"*[46]

Olarak tanımlanmaktadır. Bilgi Teknolojileri ve İletişim Kurumunun daha kapsamlı siber tehdit tanımlamasına bakıldığında siber tehdit

> *"Siber uzaya yönelik her türlü yıkıcı, bozucu, engelleyici ve ele geçirici faaliyet ile siber saldırıların çeşitli araçlar ve yöntemler vasıtasıyla kullanılması"*[47]

---

[44] Nezir Akyeşilmen, *a.g.e.,* s.57.
[45] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, *2016-2019 Ulusal Siber Güvenlik Stratejisi (2016), http:/www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.odf.,* (Erişim Tarihi: 03.02.2021), s.7.
[46] *A.g.e.,* s.7.
[47] *A.g.e.* s.7.

Olarak tanımlanmaktadır. Siber tehditler zararlı faaliyetler sonucunda oluşabileceği gibi bazen de bilinçsiz kullanıcılar tarafından da gerçekleşebilir. Siber tehditlere bakıldığında her tehdittin bir motivasyonu, aktörleri ve hedefleri mevcuttur.[48]

Tablo-2: Siber Tehditler[49]

	Motivasyon	**Aktör**	**Hedef**
Hacktivizm	Politik değişim, Egoizm	Aktivist, hacktivist ve bireyler	Ülkeler, işletmeler ve bireyler
Siber Suç	Ekonomik, finansal	Suçlular	İşletmeler, kişiler ve çeşitli kazançlar
Siber Sabotaj	Bilgi çalma	Milletler ve organizasyonlar	Devletler, organizasyonlar ve bireyler
Siber Terörizm	Politik değişim, korku, politik, dini veya ideolojik amaçlar	Teröristler, milletler	Altyapılar, genel hedefler, Organizasyonlar ve bireyler
Siber Savaş	Politik veya sosyal değişimler	Milletler, bireysel bilgisayar korsanları, Terörist gruplar	Kritik altyapılar, ülkeler, askeri güçler, kritik Hedefler

Kaynak: Güzin Ulutaş, "Siber Güvenlik", *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık,* Derleyenler: Şeref Sağıroğlu- Mustafa Alkan, Grafiker Yayınları, Ankara 2018, s.93

Siber saldırılar günümüzde internete bağlı unsurların artmasıyla beraber giderek artmaktadır. Siber saldırılar, siber güvenlik için en büyük risk faktörünü oluşturmaktadır. Siber saldırı 2016-2019 Ulusal Siber Güvenlik Strateji Belgesinde şu şekilde tanımlanmaktadır.

> *"Ulusal siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük ya da erişilebilirliğini ortadan kaldırmak maksadıyla siber uzay içerisinde ki kötü niyetli kişi, kişiler, örgütler veya bilişim sistemleri tarafından faaliyetlerdir."*[50]

Siber saldırının amacına bakıldığında siber uzay içerisindeki fiziki yahut sanal organizmayı yazılım, donanım ve kritik altyapı sistemlerinin çoğunlukla da bu

[48] Güzin Ulutaş, "Siber Güvenlik", *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık,* Derleyenler: Şeref Sağıroğlu- Mustafa Alkan, Grafiker Yayınları, Ankara 2018, s.93.
[49] *A.g.e.,* s.93.
[50] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, *2016-2019 Ulusal Siber Güvenlik Stratejisi (2016),* s.8. *http:/www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.odf* (Erişim Tarihi: 03.02.2021).

sistemler içerisindeki verileri veya kullanıcıları hedef almaktadır.[51] Siber saldırılar aslında asimetrik savaşın bir türü olup, bir ülkenin kritik altyapılarına zarar verebilme potansiyeline sahiptirler.

2.4. Siber suç ve siber terörizm

Siber suçları belirgin kılan özellikleri klasik suçların bilgisayarlara, bilgisayar sistemlerine ve bilgisayar ağlarına taşınmış hali olmasıdır. Siber suçlar ile ilgili birçok tanımın yapılmasının yanında ceza ve adalet uzmanlarınca net bir tanımı ortaya koyulamamıştır. Siber suçlar ile ilgili en kapsamlı ve uzlaşılmış tanımları; Birleşmiş Milletlerin 2000 yılında ki

> *"Bilişim sistemi güvenliğinin ya da veri işleminin hedef alan ağ aracılığıyla gerçekleştirilen eylemler"*[52]

Tanımı ve Avrupa Konseyi Siber Suçlar Sözleşmesi (2004)'de siber suç

> *"Yetkisiz erişim, sisteme ve veriye müdahale, bilişim sistemi aracılığıyla sahtekarlık ya da dolandırıcılık suçları yanında, bilgisayar ve veriye yönelik fiillere ilave olarak, bilişim sistemlerinin kullanılmasıyla ve özellikle internetin yaygınlaşması ile birlikte niceliksel ortaya çıkan çocuk pornografisi, telif haklarına ilişkin ihlaller, yabancı düşmanlığının ve ırkçılığın önlenmesine ilişkin hükümlerde siber suçtur."*[53]

Şeklinde tanımı yapılmıştır.

Avrupa Konseyi Siber Suçlar Sözleşmesi ile birlikte siber suçlar çeşitli sınıflandırmalara tabi tutulmuştur;

---

[51] Mustafa Şenol, "Hibrit Savaş Kapsamında Siber Savaş ve Siber Caydırıcılık*", Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık,* Derleyenler: Şeref Sağıroğlu- Mustafa Alkan, Grafiker Yayınları, Ankara 2018, s.194

[52] Mustafa Şenol, *a.g.e.,* s.194

[53] *A.g.e.*, s.195

- Bilgisayar veri ve sistemlerinin gizliliği, erişilebilirliğini veya bütünlüğünü bozmaya yönelik eylemler,
- Bilgisayar aracılığıyla yapılan her türlü sahtecilik ve dolandırıcılık eylemleri,
- İnternet ağı içerikleriyle ilgili olarak çocuk pornografisiyle ilgili eylemler,
- Telif haklarının ve benzer hakların ihlali sonucu oluşan suçlar,[54]

Tüm bu siber suç tanımları ve sınıflandırmalarına rağmen siber suçların kavramsallaştırılmasıyla ilgili ortak bir görüş ya da içerik unsuru ortaya atılamamıştır.

Siber terörizm kavramının daha iyi anlaşılabilmesi için öncelikle terörizmin kelime kökenine bakmak gerekmektedir. Fransızca "*terreur*" sözcüğünden dilimize "*terör*" biçiminde geçen terim, Latince kökenli olup "*korkudan titreme*", "*yıldırma*" anlamlarından oluşmaktadır. Uluslararası alanda kabul görmüş bir terör tanımı bulunmamaktadır. Ancak bir tanımlama yapılacak olursa terör, şiddet aracılığıyla yaratılmış korku ortamını ve bu korkunun kendisini ifade ederken; terörizm kavramı ise ideolojik amaçlar için sistematik bir şekilde gerçekleştirilin terör faaliyetleri olarak tanımlanmaktadır.[55] Uluslararası ortamda uzlaşılmış bir terörizm tanımı olmadığı gibi siber terörizm tanımının da ortak bir tanımı bulunmamaktadır. Genel olarak siber terörizm ideolojik hedefleri gerçekleştirebilmek amacıyla, devletleri ve vatandaşlarını korkutarak, baskı oluşturma yoluyla hükümetlerin politikalarını değiştirmek için bilgisayarlara, ağ sistemlerine, veri tabanlarına bilgi ve iletişim teknolojilerinde ki kabiliyetleri vasıtasıyla gerçekleştirilen tehditler ve zarar verici eylemler olarak tanımlanabilir.[56] Teröristler için siber uzay; denetimden uzak oluşu, saldırı maliyetlerinin ucuz oluşu, propaganda için kitlelere çabuk erişim ve herhangi bir sınırının bulunmamasından dolayı cazip bir ortam olmuştur. Siber terörizm ve siber suç birbirinden ayrı unsurlardır. Bu ayrım saldırganın eylemi yapma motivasyonu ile alakalıdır.[57] Siber suçta saldırganlar bilgi ve iletişim teknolojileri aracılığıyla maddi ya da manevi menfaat sağlamayı ilke edinmişlerdir. Fakat siber terörizmde ise

---

[54] Haydar Çakmak- Taner Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya,* Ankara 2009, s.33
[55] Yıldıray Yalman, "Siber Terör, Terörizm ve Mücadele", *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık,* Derleyenler: Şeref Sağıroğlu- Mustafa Alkan, Grafiker Yayınları, Ankara 2018, s.259
[56] Mustafa Şenol, *a.g.e.,* s.195
[57] Gabriel Weimann, "*Cyber Terroism, How Real Is The Treat?",* United States Institute of Peace, Special Report 119, 2004, s.4

saldırganlar belirli ideolojiler doğrultusunda hareket edip fiziksel veya ruhsal açıdan zarar verme eğilimindelerdir.[58]

2.5.Hacker kavramı

Hacker kelimesi İngilizce kökenli bir kelimedir. TDK`daki karşılığı ise

> *"Bilişim teknolojileri konusundaki bilgi ve becerilerini gizli verilere ulaşmak, ağlara zarar verici kötü niyetli işler için kullanan kimse" olarak tanımlanmıştır.*[59]

Hackerler için farklı birçok tanımlama bulunmaktadır. Bilgisayar ve haberleşme teknolojilerini iyi kullanan, yazılım alanında yüksek beceriye sahip olan ve onları geliştirip, kullanabilen kişilerdir.[60]Hackerler bağımsız bilgisayarlara ve büyük ağlara girebilecek beceriye sahiptirler. Bir kez eriştiklerinde gizli bilgileri çalabilir, kötü amaçlı yazılım yükleyebilmektedirler.[61]Hackerlar, internet açıklarından faydalanıp şifreleri kırabilir, sistemlere izinsiz girebilir, ulusal ve uluslararası güvenlik belgelerine erişip bunları çalabilirler.

2.5.1.Hacking

Hacking bir sistem veya ağdaki, gizli ve ulaşılamaz bilgilerin sisteme sızmalarla çalınması işlemidir. Sistemin güvenlik duvarlarının aşılarak sisteme izinsiz giriş yapılması ve sistemin yetkili unsurlarının devre dışı bırakılmasıdır. *Hacking* işlemi yapan *hacker* sistem veya ağ üzerinde izinsiz dolaşabilir, bilgisayarlara erişimi kısıtlayabilir, bilgileri çalıp üstünde değişiklikler yapabilmektedir.[62]

---

[58] Yıldıray Yalman, *a.g.e.,* s.260

[59] TDK, Online sözlük, *http://www.tdk.gov.tr/?option=com_karsilik&view=karsilik&kategori1=abecesel&kelime2=H* (Erişim Tarihi: 03.04.2020).

[60] Kaspersky, *Hacker Nedir? https://www.kaspersky.com.tr/blog/hacker-ne-demektir/611/*about:blank (Erişim Tarihi:03.04.2020).

[61] *A.g.e.,* (Erişim Tarihi: 03.04.2020).

[62] Emniyet Genel Müdürlüğü, *Hacker Nedir? Hacking nedir? Siber suçlar Nelerdir? http://siberguvenlikhaberleri.blogspot.com/2014/05/hacking-nedir.html,* (Erişim Tarihi: 04.04.2020).

2.5.2. Hacker çeşitleri

Richard A. Clarke, *Hackerın* bilişim sistemlerine sızmaya yönelik çalışmaları yasadışı kabul edilirken, devlet adına yapıldığında yasal olduğunu belirtmiştir. Hackerlar, eylemlerinin türlerine göre ve kimin adına bu eylemi yaptıklarına göre çeşitli sınıflandırmalar yapılmaktadır. Genellikle şapka renklerine göre iyi veya kötü niyetli olmak üzere sınıflandırılmıştır. Beyaz renk masumiyeti, Siyah renk kötülüğü ve gri renk ise niyetlerinin net olmadığını belirtmiştir. Kırmızı şapkalılar ise tamamen bu sınıflandırma dışında kendini marjinal bir yerde görmektedir.

2.5.2.1.Siyah şapkalı hacker (Black Hat)

En riskli hacker çeşididir. Amaçları; güvenlik zafiyeti olan noktaları bulup gizli bilgileri ele geçirmek, üzerlerinde değişiklik yapmak veya sistemi tamamen erişilemez, çalışamaz hale getirmektir. Siyah şapkalı hackerlar büyük maddi zararlara yol açmışlardır. Ayrıca kritik bilgileri ele geçirip şantaj, fidye gibi yöntemlerle bu bilgileri kullanmışlardır[63].

2.5.2.2. Beyaz şapkalı hacker (White Hat)

Bu grup hackerlar sistemlerin zafiyetlerini ve açıklarını bulup kurum, kuruluş veya devletlere bu durumdan nasıl kurtulunabileceği konusunda yardımcı olmaya çalışmaktadırlar. Bu tarz hackerlar yeteneklerini kurum, kuruluş ve devletlere yardım etmek için çaba harcamaktadırlar.[64]

---

[63]Ufuk Eriş, *Türkiye`de Kırıcı (Hacker) Kültürü*, Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi, Sayı:2, Eylül 2011, *https://dergipark.org.tr/en/download/article-file/83912,* (Erişim Tarihi 03.04.2020).

[64]Norton Antivirüs, *What is the Difference Between Black, White and Grey Hat Hackers? https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html* (Erişim Tarihi 08.04.2020).

2.5.2.3.Gri ve kırmızı şapkalı hackerlar (Gray Hat and Red Hat)

Gri şapkalı hackerlar duruma göre hareket ederler ve pazarlık esastır. Bazen iyi bazen ise kötü niyetli hackerlardır. Bu sebeple oldukça dikkat edilmeli, menfaatleri doğrultusunda değişikliğe gidebilmektedirler[65].

Kırmızı şapkalı hackerlar ne beyaz ne de siyah şapkalı hacker özelliği göstermektedirler, belli bir hacker kültürü, amacı, ideolojileri olduğunu iddia etmektedirler. Redhack örneği bu kategoride tanımlanmaktadır.

2.6. Siber caydırıcılık

Caydırıcılık Türkçe literatürde "*korkutarak cesaret kırmak ve vazgeçirmek*" anlamlarına gelen "*caydırmak*" sözcüğünden türemiştir. TDK sözlüğüne bakıldığında caydırıcılık "*Bir saldırganlığı önlemek ve engellemek için önlem alma işi*" biçiminde açıklanmaktadır.[66] Uluslararası ilişkiler literatüründe caydırıcılık bir devletin ya da topluluğun, aleyhine gerçekleşebilecek olaylardan kaçınabilmesi için aldığı tedbirler biçiminde tanımlanmaktadır. Caydırıcılık başka bir deyişle sorunun tırmanarak askeri güç unsurlarının kullanılmasını engelleme faaliyetleri de denilmektedir.[67] Genel kabul gören Schulze'ın caydırıcılık anlayışına göre caydırıcılık rasyonel seçimlere dayanmaktadır. Caydırıcılıkta, unsurlar yapacakları eylemlerin maliyetlerini ve faydalarını hesap ederek en düşük maliyetli olanı seçerler.[68] Siber caydırıcılık ile ilgili tanımlamalarda siber caydırıcılık;

> *"Siber uzayda bilişim sistemleri ve bunlara bağlı altyapılara saldıracak olan saldırganın bu işe başlamadan saldırıdan vazgeçirilmesi"*[69]

Olarak tanımlanmaktadır. Libicki, Siber caydırıcılığı,

---

[65]*A.g.e.,* (Erişim Tarihi 08.04.2020).
[66] Türk Dil Kurumu Online Sözlüğü, *https://sozluk.gov.tr/*, (Erişim Tarihi: 08.04.2020.)
[67] Vahit Güntay, "Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu: Siber Savaş Örneği", *Güvenlik Bilimleri Dergisi*, Cilt No:6, Sayı:2, Kasım 2017, s.91
[68] Sevda Korhan, "Uluslararası İlişkilerde Siber Güvenlik: Caydırıcılık, Güç ve Diplomasi", *Yeni Küresel Tehdit Siber Saldırılar*, Derleyen: Fulya Köksoy, Ankara, Ekim 2020, s.54
[69] Mustafa Şenol, *a.g.e.,* s.209

"Siber uzayda saldırganların faaliyetlerini boşa çıkarma veya cezalandırma yöntemiyle saldırıdan vazgeçirme prensibi"

Olarak tanımlamıştır.[70] Siber caydırıcılık konusunda yapılan eleştiri siber saldırının nereden gelebileceğini bulmanın zor oluşu yönündedir. Çünkü siber caydırıcılık politikaları başarısız olma ihtimali yüksek olan politikalar olarak adlandırılmaktadır. Bu yüzden siber caydırıcılık politikalarının güvenilirliği tartışmalıdır. Bunun aksine siber savunma yeteneklerinin geliştirilmesi siber saldırıları etkisiz hale getirip bunu boşa çıkarıp bir daha bu yola başvurulmaması gerektiğini gösterecektir.[71]

2.7. Siber istihbarat ve casusluk

İstihbarat ve casusluk faaliyetleri insanlık tarihi boyunca mücadele içinde bulunan ülke, devlet yahut topluluklar üzerinde hakimiyet sağlama ya da rekabette bir adım öne geçebilmek için yürütülmüş faaliyetlerdir. Bu kavramların kökü ne kadar eskiye dayansa da günümüz teknolojik ilerlemeleriyle birlikte farklı bir mücadele sahasına taşınmış ve aynı orantıda da yöntemleri farklılaşmıştır. Siber istihbarat kavramı birden çok bileşeni içerdiği için karmaşık olmakla beraber tanımlanacak olursa

"Liderler, devletler, örgütler, şirketler ya da bireylerin siber uzay içerisinde rekabette oldukları güçlerin gizli ve hassas verilerinin bilgi teknolojileri aracılığıyla yasadışı yollarla elde etmesidir".[72]

Klasik istihbarat yöntemleriyle karşıt unsurların bilgilerini ele geçirebilmek maliyetli ve zahmetli bir süreç iken bilgi ve iletişim teknolojileri aracılığıyla maliyeti ve zahmeti minimum düzeye inmiştir. Siber casusluğun tanımına bakıldığında

[70] Martin Libicki, *Cyberdeterrence and Cyberwar, Santamonica,* CA: Rand Cooperation, 2009, s.29-30
[71] Yavuz İduğ, Ferhat Çalışkan, Talip Güler, "Siber Caydırıcılık ve Türkiye'nin İmkân ve Kabiliyetleri", *6. Uluslararası Bilgi Güvenliği ve Kripto Konferansı Bildiriler Kitabı*, Ankara, 2013, s.288
[72] Nezir Akyeşilmen, *a.g.e.,* s.231

> *"Aktörlerin sahip olduğu sanal ortamdaki bilgi varlıklarının; sistemlerde bulunan açıklıklar, zafiyetler mevcut tehditler ve siber saldırılar vasıtasıyla yazılım ve donanım unsurları üzerinden belirli bir fayda için ele geçirme ya da bilgi sızdırma"*[73]

Olarak tanımlamaktadır. Siber istihbarat ve siber casusluk faaliyetleri neticesinde ileride karşılaşılabilecek geleneksel ya da siber savaşta düşman güçlerine karşı bilgi üstünlüğü sağlanabilmektedir.

2.8.Siber savaş

Siber savaşında diğer tanımlarda mevcut olan sorunlar gibi anlaşılmış net bir tanımı bulunmamaktadır. Siber savaşın tanımlamasına bakıldığında;

> *"Ulusal bir amacı gerçekleştirmek için mevcut bir savaşı desteklemek amacıyla düşman unsurlarının her türlü bilişim sistemlerine ve kritik altyapılarına karşı gerçekleştirilen engelleme, imha etme veya kendi çıkarı için kullanma faaliyetlerini içinde barındıran siber saldırılar bütünü"*[74]

Olarak tanımlanmaktadır. Uluslararası alanda en yaygın tanımlama Richard Clarke'ın yapmış olduğu siber savaş tanımıdır. Clarke'a göre

> *"Bir devlet tarafından, bir devleti adına veya o devleti desteklemek üzere başka bir ülkenin bilgisayar veya bilişim ağlarına veri eklemek, değiştirmek, bozmak veya bilgisayarları, ağ üzerindeki cihazları ya da bilgisayar sisteminin kontrol ettiği nesneleri kesintiye uğratmak veya onlara hasar vermek amacıyla yetkisiz giriş yapılmasıdır."*[75]

---

[73] Şeref Sağıroğlu, "Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler", *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*, Derleyenler: Şeref Sağıroğlu- Mustafa Alkan, Grafiker Yayınları, Ankara 2018, s.25

[74] Vahit Güntay, *a.g.e.*, s.97

[75] Rıchard Clarke- Robert Knake, *Siber Savaş*, İstanbul 2011, s.119

R. Clarke ayrıca siber savaşın tanımlamasını yaptıktan sonra siber savaşın şu özelliklerine değinmiştir;

- Siber savaş gerçek bir savaştır.
- Siber savaş çok hızlı gerçekleşmektedir.
- Siber savaş küresel bir kapsamdadır.
- Siber savaş konvansiyonel savaştan önce meydana gelmektedir.[76]

Siber uzayda gerçekleşen siber savaş yöntemleri şu şekilde sıralanabilir; 1) komuta- kontrol savaşı, 2) Bilgisayar korsanlığı savaşı, 3) İstihbarat merkezli savaş, 4) Elektronik savaş, 5) Ekonomik bilgi savaşı,[77]

Siber savaş, siber terörizm ve siber suçlarla aynı yöntemleri ve yolları izlese de motivasyon ve amaçları doğrultusunda ayrışmaktadır. Ayrıca siber savaş bu kavramlara nazaran daha koordineli ve daha yoğun siber saldırıları içinde barındırmaktadır. Bir başka perspektiften bakılacak olursa da siber suçlar ve siber terörizm faaliyetleri bireyler ya da gruplar tarafından yapılırken siber savaşın tarafları devlet ya da örgütler biçimindedir. Siber savaşlar devletler ve örgütler eksenli oluşan bir kavramdır.[78]

Tablo-3: Siber Suç, Siber Terör ve Siber Savaşın Temel Özellikleri[79]

Eylemin	**Siber Suç**	**Siber Terör**	**Siber Savaş**
Niteliği	Doğrudan	Sembolik	-Doğrudan -Sembolik
Şiddeti	Az yoğun	Yoğun	En yoğun
Motivasyonu	Kişisel Kazanç	Siyasi	-Siyasi -Doğrudan savaş kabiliyetini azaltmak -Casusluk

[76] *A.g.e.,* s.23
[77] Haydar Çakmak- Taner Altunok, *a.g.e.,* s.45
[78] Oona Hathaway, Rebecca Crootof, "The Law of Cyber-Attack", *California Law Review*, Cilt: 100,2012, s.833
[79] *A.g.e.*, s.49

Failleri	-Bireyler -Organize suç örgütleri -Anonim	-Terörist örgütler -Hangi örgüt olduğu tahmin edilebilir	-Failin kim olduğu tam olarak bilinmese de kaynaklandığı devletler bilinir.
Hedefleri	Kazanç sağlanacak hedefler	-Kritik tesisler -Güvenlik birimleri -Hükümet temsilcilikleri	-Kritik tesisler -Ekonomik ve endüstriyel altyapılar -Güvenlik birimleri -Hükümet temsilcilikleri -Askeri altyapılar
Kaynağı	Ülke içinden ya da dışından	Ülke içinden ya da dışından	Ülke dışından

Kaynak: Haydar Çakmak- Taner Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya,* Ankara 2009, s.49

2.9. Hibrit savaş

2000'li yıllar ile beraber askeri ve güvenlik otoriteleri tarafından konuşulup, tartışılmaya başlanan hibrit tehditler ve hibrit savaş terimi ilk kez 2014 yılında Rusya-Ukrayna arasında ki çatışmalarda görülmüş ve o zamandan beri oldukça konuşulmaya başlanmıştır. Hibrit savaşın tanımına bakıldığında

> *"Elektronik savaşın yöntemlerinden daha kapsamlı bir organizasyon gerektiren, konvansiyonel güç unsurlarıyla eşgüdümlü ilerleyen bileşke savaş türüne hibrit savaş"*[80]

Denilmektedir. Birden çok çalışmada hibrit savaş, opersayonel siber savaş kavramı yerine de kullanılmaktadır. Fakat hibrit savaş, operasyonel siber savaşa kıyasla özel durumları ve farklı müdahale biçimlerinide kapsamaktadır.[81] Hibrit savaş ile ilgili

[80] Vahit Güntay, *a.g.e.,* s.101
[81] Ali Bilgin Varlık, "Savaşı Tanımlamak, Terminolojik Bir Yaklaşım", *Avrasya Terim Dergisi*, Cilt:1, Sayı:2, 2013, s.125

birçok tanım ve tartışma bulunmasına rağmen genel kabul gören tanımı Frank Hoffman tarafından yapılmıştır. Hoffman'a göre

> *"Hibrit savaş, faaliyet alanında konvansiyonel yetenekler, düzensiz taktikler, terör eylemleri ve suç oluşturan düzen bozucu unsurları içinde barındıran bir savaş yöntemidir."*[82]

Hibrit savaş yöntemlerinde düşmanın tamamen saf dışı bırakılması mümkün görünememektedir. Bunu başarabilmek için düşman unsurlarının tamamıyla siber uzaya bağımlı bir yapıda bulunması gerekmektedir.

Tablo-4: Savaşların Tarihsel Süreci[83]



Kaynak: Mustafa Şenol, "Hibrit Savaş Kapsamında Siber Savaş ve Siber Caydırıcılık*", Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık,* Derleyenler: Şeref Sağıroğlu- Mustafa Alkan, Grafiker Yayınları, Ankara 2018, s 186

Hibrit savaşın temel amacı bir bölgenin ele geçirilmesi veya kontrol altına alınması olmayıp, hibrit savaşı uygulayan tarafın mevcut bütün yeteneklerini kullanarak düşman üzerinde istediği baskıyı kurarak, karşı tarafın karar alma mekanizmalarına zarar vererek, yönetim boşluğu oluşturup, düşmanda kargaşa ve panik havası yaratma amacı taşımaktadır. Bu amaca yönelik operasyonlarda ise düşman unsurlarının zayıf olan unsurları seçilerek daha da zayıflatılır ya da yok edilir.[84]

Hibrit savaşı kendine doktrin olarak edinen Rusya Federasyonu "2008 Gürcistan", "2014 Kırımın İlhakı" operasyonlarında hibrit savaş yöntemlerini etkin ve verimli bir şekilde kullanmıştır. Rusya Federasyonu'nun bu yeni savaş konsepti

[82] Mustafa Şenol, *a.g.e.*, s.188
[83] *A.g.e.*, s.186
[84] *A.g.e.*, s.186

NATO ve müttefikleri başta olmak üzere her an Rusya Federasyonu tehlikesi altında olabilecek olan ülkelerin birincil gündem maddeleri olarak yerini almıştır.[85]

2.10. Siber güvenlik ve siber savunma

Bilgi ve iletişim teknolojilerinin hızla değişmesi ve dönüşmesi siber uzay içerisinde de güvenlik kavramını gündeme getirmiştir. Hem siber uzayın karmaşık ve anarşik olan yapısı hem de farklı disiplinlerin ve aktörlerin güvenlik anlayışlarındaki farklılıklar net bir siber güvenlik kavramının ortaya koyulabilmesi mümkün olmamıştır. Sonuç olarak bugün literatürde siber güvenlik anlayışları farklı birçok tanım bulunmaktadır. Siber güvenlik ile amaçlanan asıl düşünce verinin güvenliğidir. Siber güvenlik nedir? sorusuna cevap olarak farklı disiplinlerden farklı tanımlamalar yapılmıştır.

Tablo-5: Siber Güvenlik Nedir?[86]

Siber güvenlik Nedir?
1) Yazılımlara, bilgisayarlara ve ağlara yapılabilecek siber saldırıların risklerini azaltmayı amaçlar. Bu amaca uygun olarak sızmaları bulan, virüsleri ve yetkisiz erişimleri kısıtlayan kriptolu haberleşmeyi sağlayan unsurları kapsar.
2) Araçların, kararların, güvenlik konseptlerinin, güvenlik önlemlerinin, kılavuzların, risk yönetim yaklaşımlarının, önlemlerin, içinde bulunduğu bütüncül bir yapıdır. Amaç siber uzay içerisinde ki kurum, tüzel kişilerin çıkarlarını korumaktadır.
3) Siber uzayın içerisinde oluşabilecek siber saldırılardan korunmasıdır.
4) Bilgi ve iletişim sistemlerinin oluşturmuş olduğu ekosistemi saldırıdan, tahripten veya yetkisiz erişimden koruyabilmek adına yapılması gereken

[85] Salih Bıçakçı, "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", *Uluslararası İlişkiler Dergisi*, Cilt:9, Sayı:34,2012, s.210
[86] Güzin Ulutaş, *a.g.e.,* s.90

eylemler bütünüdür. Bu yöntemle gizliliği, bütünlüğü ve erişilebilirliğini sağlamayı amaçlar.
5) Elektronik verinin izinsiz veya yasadışı kullanımına karşı korunma durumudur ya da bunu sağlayabilmek için alınan tedbirler bütünüdür.

Kaynak: Mustafa Şenol, "Hibrit Savaş Kapsamında Siber Savaş ve Siber Caydırıcılık*", Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık,* Derleyenler: Şeref Sağıroğlu- Mustafa Alkan, Grafiker Yayınları, Ankara 2018, s.186

Yukarıda ki tablodan da anlaşılabileceği gibi siber güvenlik kavramının farklı disiplinler için farklı tanımlamaları bulunmaktadır. Fakat bu tanımlamaların hiçbiri bütüncül bir yaklaşımla oluşturulmuş tanımlar olmadığından tam olarak kavramı açıklayamamaktadır. Bütüncül ve kapsayıcı bir bakış açısıyla oluşturulmuş tanımlardan biriside dünyada uluslararası alanda bilgi ve iletişim teknolojilerinde yetkili merci olan Uluslararası Telekomünikasyon Birliği (ITU)'nın yapmış olduğu siber güvenlik tanımına göre

> *"Siber uzayın bütün katman ve boyutlarından gelebilecek tüm tehdit ve saldırılara karşılık, kullanıcıların mevcudiyetlerinin korunması amacıyla oluşturulmuş araçlar, politikalar, güvenlik kavramları, yöntemler, risk yaklaşımları, eğitim ve teknolojiyi de içinde barındıran faaliyetler bütünü"* [87]

Olarak tanımlanmıştır. Bu tanımlamayla ITU siber güvenlik veriyi ve verilerin niteliklerini korumayı, bilişim sistemlerini siber tehdit ve saldırılara karşı savunmayı ve bu sistemlerin güvenlik açıklıklarını en aza indirmeyi amaçlamıştır. Türkiye'nin 2016-2019 Ulusal Siber Güvenlik Strateji Belgesinde siber güvenlik tanımlaması da aynı ITU'nun yapmış olduğu tanımlama gibi bütüncül ve kapsayıcı bir şekilde oluşturulmuştur. 2016- 2019 Ulusal Siber Güvenlik Strateji Belgesine göre Türkiye'nin siber güvenlik tanımlaması ise

> *"Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korumasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük*

[87] ITU-T Recommendations, ITU (2008) "Overview *of Cybersecurity*", *http:/hande.itu.int/11.1002/1000/9136-en?locatt=format:pdf&auth* (Erişim Tarihi: 05.02.2021).

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 döndürülmesini amaçlamaktadır."

Siber güvenliğin hedef ve amaçları kullanıcılara ve çeşitli paydaşlara göre farklılıklar göstermektedir. Fakat nihai amaç olarak ise siber uzayın tüm kullanıcılar ve paydaşlar için güvenli bir yere dönüştürülmesidir. Siber güvenliğin sağlanması hususunda birçok farklılıklar ve öncelikler bulunmasına rağmen temelde siber güvenliğin amacı CIA olarak bilinen verinin gizliliği (*confidentiality*), bütünlüğü (*integrity*) ve erişilebilirliğinin (*availability*) sağlanmasıdır.

Tablo-6: CIA Üçlüsü[88]

CIA Üçlüsü
Gizlilik: Verilerin korunmasını, mahremiyetini ve yetkisiz erişimini içerir.
Bütünlük: Sistemin ve içerisinde ki mevcut verinin yetkisiz bir şekilde değiştirilmesidir.
Erişilebilirlik: Sistemlerin olağan çalışma durumlarının korunmasıdır.

Kaynak: P.W.Sınger- Allan Frıedman, *Siber Güvenlik ve Siber Savaş*, Çeviren: Ali Atav, Ankara 2015, s.57

Elbette ki siber güvenliği sadece gizlilik, bütünlük ve erişilebilirlik kavramlarıyla açıklamak yanlış olacaktır. Kavramlara ek olarak bu unsurları bütünleyici şekilde 3A formülünü de açıklamakta fayda olacaktır. 3A formülüne göre; Kimlik doğrulama (authentcation), Yetkilendirme (authorization) ve İnkâr edememe (non- repudiation) aşamaları da etkili bir siber güvenlik yapısının oluşturulmasındaki temelleri oluşturmaktadır.[89] 3A'ya göre kimlik doğrulama, bilişim sistemine giren

[88] P.W. Sınger- Allan Frıedman, *a.g.e.,* s.57
[89] Nezir Akyeşilmen- İbrahim Kurnaz, "Küresel Siber Güvenlik: Kavramsal ve Kuramsal Bir Analiz", *Yeni Küresel Tehdit Siber Saldırılar*, Derleyen: Fulya Köksoy, Ankara, Ekim 2020, s.10

gerçek ya da tüzel kişinin kimliğinin teyit edilmesidir. Yetkilendirme, bilişim sistemini kullanan kişilerin yetkileri kadar işine yarayabilecek verilerin sunulmasıdır. İnkâr edememe ise bilişim sisteminde kullanıcının yaptığı işlemlerin ispatlanması ve reddedilememesidir.

Siber savunma ve siber güvenlik kavramları benzerlikler taşısalar da ayrıldıkları temel noktaları vardır. Siber savunma kavramına bakıldığında düşman unsurlarına yapılan bir taarruzda siber uzaydan gelebilecek tehdit ve saldırıların olumsuz etkilerinin önlenmesi ve sistemlerin olağan çalışmalarına devam edebilmesi için alınan tedbirlerin bütünüdür. Siber savunma ve siber güvenlik arasındaki temel ayrım siber güvenlik barış şartları içinde saldırı ve tehditlere karşı alınan tüm önlemler olurken, siber savunmada ise mevcut olan bir çatışma veya savaş sırasında sistemlerin korunması için alınan tüm tedbirleri kapsamaktadır.[90]

2.10.1 Kritik altyapı sistemlerinin güvenliği

Bilgi ve iletişim teknolojilerinde ki hızlı değişim ve dönüşüm süreci hayatımızın her alanına etki etmektedir. Her geçen gün daha da bağımlı hale geldiğimiz siber uzayda avantajlarının yanı sıra kötü niyetli kullanıcıların yaratmış olduğu dezavantajları da mevcuttur. Yaşanan bu hızlı değişim ve dönüşüm sürecinden kritik altyapı sistemleri de etkilenmiştir. Bu sistemlere uygulanan teknolojik entegrasyonun sonucu olarak iş süreçleri ve hizmetlerde ki verimlilik oldukça artmıştır. Fakat bu faydaların yanı sırada sistemler dışarıdan müdahalelere açık bir hale gelmiştir. Son zamanlarda siber saldırı ve tehditlerin hedefinde kritik altyapı sistemleri yer almaktadır. Kritik altyapı sistemlerine baktığımızda içinde barındırdığı verilerin gizliliği, erişilebilirliği veya bütünlüğünde bozulma meydana geldiğinde can kayıplarına, büyük ekonomik zararlara ulusal güvenliğin ya da kamu düzeninin bozulmasına sebep olabilecek hayati sistemler olarak tanımlanmaktadır.[91]

---

[90] Myriam Dunn Cavelty, "Cyber-Security and Threat Politics", *US Efforts to Ensure The Information Information Age*, New York: Routledge, 2008, ss.12-13

[91] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, *2016-2019 Ulusal Siber Güvenlik Stratejisi (2016), http:/www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.odf.*, (Erişim Tarihi: 03.02.2021), s.8.

Kritik altyapı sistemleri kavramı ilk kez Amerika Birleşik Devletleri Başkanlık Komisyonunca 1996 yılında hazırlanan "Kritik Altyapıların Korunmasıyla İlgili Raporda" yer bulmuştur. İlgili raporda kritik altyapı sistemlerinin devletin ve ekonominin işleyişinde önemli bir yeri olduğunun ve söz konusu sistemlere yapılacak fiziksel ya da siber saldırılarda ulusal güvenliğe ciddi zararlar vereceği belirtilmiştir. Ayrıca kritik altyapı sistemlerinin kamu ve özel sektör tarafından yönetilen haberleşme, enerji, finans, su sistemleri, ulaşım ve acil durum servislerini kapsadığı fakat sadece bu sistemlerle de sınırlı olmadığı belirtilmiştir.[92]

Kritik altyapı sistemleri ülkeden ülkeye çeşitlilik göstermek ile birlikte genelde ulaşım, savunma, finans, haberleşme, eğitim, sağlık, elektrik, su altyapıları gibi hayati sistemleri kapsamaktadır. Türkiye'de 20/06/2013 tarihli Siber Güvenlik Kurulu kararınca kritik altyapı sektörleri; "Elektronik haberleşme, enerji organizasyonları, su yönetimi sistemleri, kritik kamu hizmetleri, ulaştırma, bankacılık ve finans sektörleri olarak belirtilmiştir.[93]

Kritik altyapı sistemlerinin operatörler tarafından uzaktan verilerin incelenmesi ve sistemlerin yönetilmesi gerekmektedir. Bu ihtiyacı karşılayabilmek içinde günümüzde teknolojik cihazlardan yardım alınmaktadır. Kritik altyapı sistemlerinde kullanılan cihazlar ikiye ayrılmaktadır. Bu sistemler "Merkezi Denetleme Kontrol ve Veri Toplama Sistemi (Supervisory Control and Data Acquisition- SCADA) ve Dağıtık Kontrol Sistemi (Distributed Control System, DCS)'dir. Bu sistemlerin genel adı ise literatürde Endüstriyel Kontrol Sistemleri (Industral Control System- ICS) olarak tanımlanmaktadır. Endüstriyel Kontrol Sistemleri tek bir yerden operatörlerin sistem ile ilgili verileri inceleyebilmesine ve yönetilebilmesine olanak sağlamaktadır. Fakat bir ağ bağlı bir şekilde yönetilebilen bu sistemler güvenlik açısından da çok büyük risk oluşturmaktadır. Ağ aracılığıyla bu sistemlere yapılabilecek siber saldırılar hayatlarımızı olumsuz yönde etkileyebilir

[92] Bilge Karabacak, "Kritik Altyapılara Yönelik Siber Tehditler ve Türkiye için Siber Güvenlik Önerileri", *Siber Güvenlik Çalıştayı,* Bilgi Güvenliği Derneği, Ankara, 29 Eylül 2011, s.1
[93] Nezir Akyeşilmen, *a.g.e.,* s.175

hatta felaketlere sebep olabilirler. Bu sebeplerden dolayı kritik altyapı sistemlerinin siber saldırılardan korunması hayati bir önem taşımaktadır.[94]

2.10.2. Uluslararası ilişkilerde siber güvenlik kavramı

Teknolojide yaşanan gelişmeler tarihin her anında insan hayatını değiştirmiş ve dönüştürmüştür. Bilgi ve iletişim teknolojilerinde yaşanan hızlı ilerlemeyle beraber mesafelerin bir önemi kalmamış ve insanların birbirleriyle olan etkileşimleri artmıştır. Bu etkileşimi sağlayan ise yazılım, donanım ve elektronik diğer unsurların içinde bulunduğu siber uzay alanıdır. Bu yeni alan toplumsal ilişkilerde giderek daha da baskın bir hal almaktadır. İçinde bulunulan siber uzay alanı fiziksel sınırları ortadan kaldırıp devletlerin klasik güvenlik anlayışlarını ortadan kaldırmıştır. Devletler ve vatandaşları siber tehdit ve saldırılara açık bir hale gelmişlerdir. Siber uzaya uyum sağlamaya çalışan devletler geleneksel güvenlik anlayışlarını terk ederek sınırları belirsiz olan bu alana uyum sağlayabilmek adına siber saldırılara yönelik etkili siber savunma mekanizmaları kurmaya çalışmışlardır.

Yaşanan teknolojik gelişmelerle beraber uluslararası ilişkiler disiplininde de karar alma süreçleri, bilgi paylaşımı ve diplomatik süreçler olarak üç aşamada etkileneceği düşünülmektedir. İlk olarak uluslararası politika alanında ki paydaşları çoğaltarak karar alma süreçlerinin içinden çıkılamayacak bir hale getirmektedir. İkincisi, doğru ya da yanlış tüm bilgileri yaydığı için bu bilgilerin idare edilebilirliğini ve sonuçlarını etkilemektedir. Üçüncü olarak ise, vatandaşlara ve devletlere diplomatik hizmetleri hızlı ve ucuz bir biçimde sunmaktadır.[95]

Siber uzayı ticari, ekonomik ve kültürel gibi düşük politika (*Low Politics*) alanı olarak değerlendiren devletler, 2007 Estonya Siber Saldırısı, 2010 İran Stuxnet Saldırısı gibi yıkıcı siber saldırıların ardından siber uzayın öneminin ve etkilerini anlayıp askeri, güvenlik ve strateji gibi yüksek politika (*High Politics*) alanı içine dahil

[94] Cristina Alcara, Sherali Zeadally, "Cyber İnfrastructure Protection: Requirements and Challenges For The 21st Century", *International Journal of Critical Infrastucture Protection*, Sayı:8, 2015, ss.54-55
[95] Nezir Akyeşilmen, *a.g.e.,* s.175

edilmişlerdir.[96] Siber uzay ortamı bireyler başta olmak üzere devlet dışındaki aktörleri de süreçlere dahil ederek devletlerin bu alandaki egemenliklerini zedeleyici bir yapıya bürünmüştür. Ayrıca, dünyada siber tehdit ve saldırılara karşı ortak bir görüş olmadığı için karara varılmış bir siber güvenlik sözleşmesi bulunmamaktadır. Bunun bir başka nedeni olarak ta siber uzayı etkin kullanan bazı devletlerin çıkarlarına aykırı düşeceği için bu tür bir anlaşmaya da yanaşmamaktadırlar. Uluslararası ilişkiler açısından değerlendirilecek olursa da gelecekte siber uzay rekabetinin yoğunlaşacağı, süreçlerde devlet dışı aktörlerinde yer alacağı ve daha tanımları konusuna bir uzlaşı bulunmayan bu yeni mücadele alanında yakın gelecekte siber güvenliğin sağlanması için bir uluslararası anlaşmanın imzalanmasının mümkün olmadığı değerlendirilmektedir.[97]

2.10.3. Siber saldırı silahları

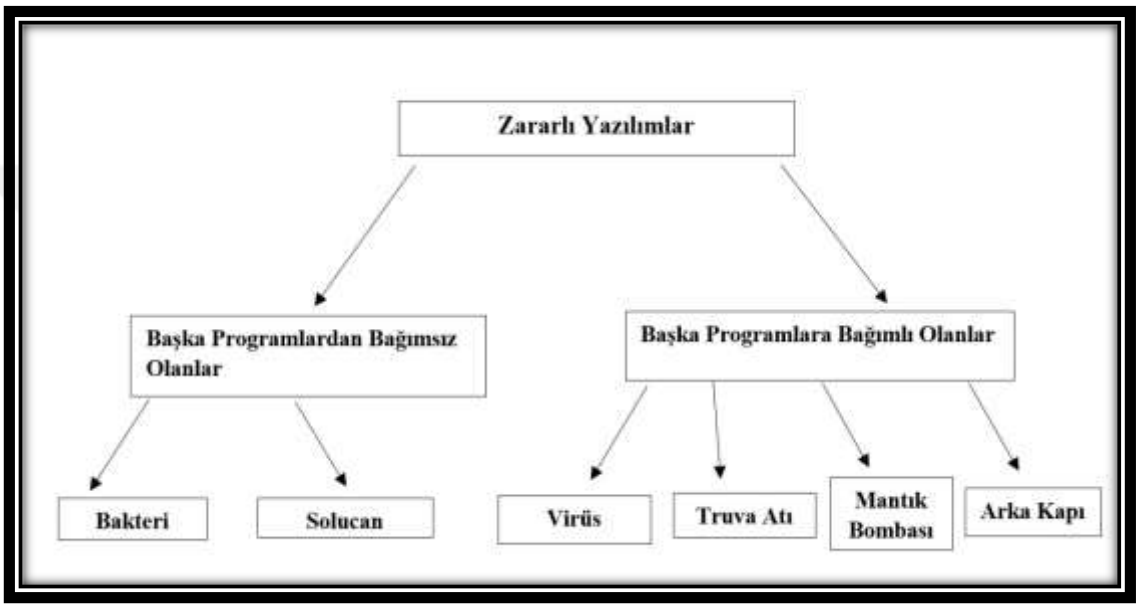
Silahların genel tanımlamalarına bakıldığında silahlar, insanlara, sistemlere ya da yapılara zarar vermek veya yok etmek amacıyla kullanılan araçlar biçiminde tanımlanmaktadır. Silahlar saldırı ya da savunma amacıyla kullanılabilmektedir. Geleneksel silahlarla ilgili hem ülkelerin hem de çeşitli örgütlerin tanımlamaları ve düzenlemeleri olmasına rağmen siber silahlar ile ilgili olarak herhangi bir tanımlama ya da düzenleme bulunmamaktadır. Yeni bir güç mücadelesi alanı olarak tanımlanan siber uzay içerisindeki siber silahlarda gün geçtikçe daha da önem kazanmaktadır.

Siber silahlarla ilgili olarak bir tanımlama yapılacak olursa, siber silahlar düşman bilgi ve iletişim teknolojilerindeki verilerin gizliliğini, erişilebilirliğini ve bütünlüğünü bozarak zarar vermek veya yok etmek üzere tasarlanmış yazılım unsurlarıdır.[98] Siber silahlar direk olarak düşmana bir zarar vermese de düşmanın kullandığı bilişim sistemlerine zarar vererek dolaylı olarak ciddi hasarlara yol açmaktadır. Ayrıca, siber silahlar geleneksel silahlara kıyasla daha az maliyetli ve daha çok zarar verebilme potansiyeline de sahiptirler. Fakat siber silahların

[96] *A.g.e.,* s.176
[97] Muharrem Gürkaynak, Âdem Ali İren, "Reel Dünya'da Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Dergisi,* Cilt: 16, Sayı:2, 2011, ss.275-276
[98] Hasan Çiftçi, *a.g.e.,* s.168

üretilebilmesinde bilgi ve iletişim teknolojilerinde uzmanlaşmış, teknik bilgiye sahip insan gücüne ihtiyaç vardır.[99]

Tablo-7: Zararlı Yazılımlar Tablosu



Kaynak: Hasan Çiftçi, *Her Yönüyle Siber Savaş*, 2. Basım, TÜBİTAK Yayınları, 2017 Ankara, s.168

2.10.3.1. Zararlı yazılımlar

Bilgi ve iletişim teknolojilerine zarar verici, akışını bozucu ve veri hırsızlığına yönelik amaçlar için tasarlanmış virüs, kurtçuklar, bakteri, mantık bombası, Truva atı, arka kapı vb. siber silah türleri zararlı yazılım olarak adlandırılmaktadır.[100]

[99] Stefano Mele, "Cyber- Weapons: Legal and Strategic Aspects", *Machiavelli Editions*, Version 2.0, *https://www.files.ethz.ch/isn/168388/cf4eaaaf89e17df399d1d580beade36a.pdf*, 2013, (Erişim Tarihi: 06.04.2021), ss.7-10.

[100] Malware Definition, *https://techterms.com/definition/malware#:~:text=Short%20for%20%22malicious%20software%2C%22,actions%20on%20a%20computer%20system.,* (Erişim Tarihi: 08.04.2020.)

2.10.3.2. Bakteri

Bakteriler, belirli bir programdan bağımsız olarak kendi kendilerini çoğaltabilen ve birçok farklı türünü kendi kedine yazabilen zararlı yazılımlardır. Çoğalan tipteki versiyonlarında bulaştıkları sistemde çok fazla disk alanı kaplayıp, işlem sürelerini geciktirirler. Bakteriler virüslerin aksine başka bir programa ihtiyaç duymazlar ve programlara, dosyalara bulaşmazlar.[101]

2.10.3.3. Solucanlar, kurtçuklar (Worms)

Solucanlar virüslere benzeseler de yayılma biçimi olarak farklılık göstermektedirler. Solucanlar bir dosya aracılığıyla bulaşmak yerine ağ vasıtasıyla kendi kedine yayılıp, bulaşırlar. Solucanlar, gizlenmek zorunda kalmadan ağlar üzerinden ilerlemektedirler.[102] Solucanlar güvenlik açıklarından yararlanarak çoğalırlar ve saniyeler içinde milyonlarca bilgisayara bulaşabilme potansiyeline sahiptirler. Dünyada en çok tanınan solucanlar, Morrıs, Blaster, Sebig, Nimda, Slammer, Conficker, Stuxnet, Duqu'dur.[103]

2.10.3.4. Virüsler

Virüsler, kendi kendilerine çoğalabilme yeteneğine sahip, sisteme yerleşebilmek için bir programa gereksinim duyan, sistemler üzerindeki veriyi yok etme ya da sistemi çökertme potansiyeli olan zararlı bir yazılım çeşididir.[104]

Virüsler çeşitli şekillerde gruplandırılmaktadır. Bunlar;[105]

- Yerleşik virüsler
- Ön yüklemeli virüsler
- Makro virüsler
- Çok şekilli virüsler

---

[101] Hasan Çiftçi, *a.g.e.,* s.169
[102] Worm Definition, TechTerms, *https://techterms.com/definition/worm.,* (Erişim Tarihi:06.04.2021)
[103] Hasan Çiftçi, *a.g.e.,* s.169
[104] Virus Definition, TecTerms, *https://techterms.com/definition/virus.,* (Erişim Tarihi: 06.04.2021)
[105] Hasan Çiftçi, *a.g.e.,* s.170

- Çok parçalı virüsler

Virüsleri virüs yapan unsur ise yayılma biçimleridir. Virüsler solucanlar gibi ağ vasıtasıyla yayılım göstermezler. Virüslerin bulaşabilmesi için USB gibi taşınabilir bir bellek vasıtasıyla bilgisayardan bilgisayara taşınması gerekmektedir. Aksi takdirde gizlenemezler ve antivirüs programları tarafından tespit edilme ihtimalleri artmaktadır.

2.10.3.5. Truva atı (Trojan Horse)

Çanakkale'de bulunan ve tarihteki örneğinden esinlenerek geliştirilmiş bir zararlı yazılımdır. Truva atı ağ aracılığıyla özellikle ücretsiz programlar, e-mail eklentileri, oyunlar, dosyalar vasıtasıyla kendini gizleyen ya da geçerli bir program içerisinde sızan zararlı bir yazılımdır.[106] Örneğin, bir müzik dosyası olduğu düşünülen bir dosya açıldığında gizlenen Truva atı yazılımı aktive olarak amaçlanan görevleri yerine getirmeye başlamaktadır.[107] Virüslerin aksine bir programdan diğer programa kendini kopyalayabilme yeteneği bulunmaktadır.[108] Truva Atı saldırıları bilişim sistemlerini tehlikeye atan en önemli tehditlerden biridir. Zararlı bir yazılımı Truva Atı yapan en büyük özelliği bulaşma yöntemidir.[109]

2.10.3.6. Mantık bombası (Logic Bomb)

Mantık bombaları, belirli zamanlamayla veya belirli olaylar gerçekleştiğinde çalışan bir zararlı yazılım türüdür. Mantık bombaları sistemlerde gizlenerek aktive olacağı günü beklerler. Aldatıcı, bozucu veya yıkıcı durumlar günü geldiğinde harekete geçirilen zararlı yazılım türüyle sağlanmaktadır.[110]

---

[106] Trojan Horse, TechTerms, *https://techterms.com/definition/trojanhorse*., (Erişim Tarihi: 08.04.2021)
[107] Şeref Sağıroğlu, *a.g.e.,* s.31
[108] Trojan Horse, TechTerms, *a.g.e.*
[109] Hasan Çiftçi, *a.g.e.,* s.171
[110] *A.g.e.,* s.172

2.10.3.7. Arka kapı (Back Door)

Arka kapı yöntemi, sadece saldırganın bildiği kimlik doğrulama mekanizmalarına takılmadan sistem açıklarından yararlanarak oluşturulmuş, gizli bir şekilde sistemi yönetme veya giriş noktasına verilen tanımdır.[111]

2.10.3.8. Bot, botnet, zombi, köle bilgisayar

Sistemlere yüklenen bir program aracılığıyla uzaktan kontrol edilebilen ve saldırganların amaçları doğrultusunda yönlendirilen sistemlere Botnet denilmektedir. Sistemin kullanıcısının herhangibir haberi olmadan sistemi saldırganın amaçları doğrultusunda hareket eder.[112] Köleleştirilmiş bilgisayar kullanarak saldırganlar bir köle ordusu oluşturmaktadırlar. Köle bilgisayarlar sayesinde saldırganlar spam mailler ve reklamlar yollayabilir ya da DDOS saldırıları gerçekleştirebilirler. Botnet zararlı yazılımları web sitesi eklentileri aracılığıyla, zararlı kod içeren spam mail eklentileriyle ya da internetteki ücretsiz korsan yazılımlar aracılığıyla sistemlere yüklenmektedir.[113]

2.10.3.9. Kök kullanıcı takımı (Rootkit)

Kök kullanıcı takımı, sistemde yapılan işlemleri, dosyaları ya da sistem bilgilerini işletim sisteminden gizleyerek gerçekleştiren bir zararlı yazılım türüdür. İlk olarak çok kullanıcının mevcut bulunduğu sistemlerde ki normal kullanıcıların programlarını ve sistem bilgilerini gizlemek için kullanılmasına rağmen günümüzde daha çok sistemleri ele geçiren bir zararlı yazılım türü olarak kullanılmaktadır. İşletim sistemlerinde çekirdek düzeylerinde faaliyet gösterdikleri için tespit edilebilmeleri oldukça zordur. Sistemlere bulaşan kök kullanıcı takımlarını bulmak ve yok etmek için özel programların kullanılması gerekmektedir.[114]

---

[111] *A.g.e.,* s.172
[112] Murat Güngör, *Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma*, (T.C. Kalkınma Bakanlığı, Bilgi Toplumu Dairesi Başkanlığı, Basılmamış Uzmanlık Tezi), Ankara 2015, s.45
[113] Nezir Akyeşilmen, *a.g.e.,* s.77
[114] Hasan Çiftçi, *a.g.e,* s.173

2.10.3.10. Fidye yazılımı (Ransomware)

Fidye yazılımlar, en tehlikeli zararlı yazılım türlerinden olup birçok sistemi etkilemiştir. Genellikle oltalama yöntemiyle zararlı yazılım bulunduran web siteleri aracılığıyla yayılım göstermektedir. Bu zararlı yazılım bilişim sistemlerine girmesinin ardından sistem içerisindeki tüm dosyaları şifrelemeye başlar ardından saldırgan tarafından mağdura bir mail yollanarak belirli bir süre zarfında bildirilen bir miktar parayı hesaba transfer etmesi söylenir. Transfer yapıldıktan sonra saldırgan mağdura dosyaları açacağı şifreyi gönderir, transfer gerçekleşmez ise sistemdeki tüm verileri silebilme ihtimalide bulunmaktadır. Bu fidye yazılım yönteminin çeşitli versiyonları da mevcuttur. En çok bilinen fidye yazılım örnekleri Wanna Cry ve Petya'dır.[115]

2.10.3.11. Casus yazılımlar (Spyware)

Casus yazılımlar sistem kullanıcısının haberi olmadan verileri toplamak amacıyla geliştirilmiş istihbarat amaçlı yazılım ya da donanımlardır. Bunlar, belirli komutları yerine getirmenin yanında sistemdeki etkinlikleri takip ederler, gizlerler ve raporlayabilirler.[116] Bu türden zararlı yazılımlar mail yoluyla Truva Atı görünümünde ya da web sitelerinden sistemlere yüklenebilirler. Casus yazılımlardan korunmak için en son sürüm antivirüs ve antispyware programları kullanmalı ve kullandığımız internet tarayıcılarının ve işletim sistemlerinin güvenlik yazılımlarının güncelliğine dikkat edilmelidir.[117]

2.10.3.12. Gelişmiş sürekli tehdit (Advanced Persistent Threat- APT)

Gelişmiş Sürekli Tehdit, İleri Düzey Sürekli Saldırı, İleri Düzey Kalıcı Tehdit, Hedef Odaklı saldırı gibi çeşitli isimlendirmeleri bulunmaktadır. Bu zararlı yazılımlar hedefe özel olarak geliştirilmiş kapsamlı saldırı yığınlarını içinde bulunduran bir saldırı yöntemidir. Geliştirilmesi, bulaştırılması ve kullanılması özel uğraş gerektirip daha önceden belirlenmiş özel bir hedefe yönelik zararlı yazılımlardır. Özel ve detaylı

---

[115] Şeref Sağıroğlu, *a.g.e.,* s.29
[116] Spyware, TechTerms, *https://techterms.com/definition/spyware.*, (Erişim Tarihi: 08.04.2021)
[117] Şeref Sağıroğlu, *a.g.e.,* s.28

bir analiz gerektirdiği için bilgi ve iletişim teknolojilerinde uzmanlaşmış insan gücüne ihtiyaç vardır. Çok karmaşık yöntemlerle geliştirildikleri için tespiti ve yok edilmesi oldukça zor zararlı yazılımlardır. Bu zararlı yazılımlardan en ünlüleri Stuxnet, Shady Rat, Lurid, Night Dragon, Flame'dir.[118]

2.10.3.13. Klavye takipçisi (Keylogger)

Sistem içerisine yerleştirilen bir zararlı yazılım aracılığıyla tüm klavye hareketleri kaydedilip, belirli aralıklarla zararlı yazılımın yöneticisine ulaştırılır. Klavye takipçisi taşınabilir bir bellek yardımıyla, mail aracılığıyla ya da zararlı web siteleri tarafından sisteme yüklenebilmektedir. Şifreler ya da hassas bilgiler klavye takipçileri aracılığıyla çalınabilmektedir. En tehlikeli zararlı yazılımlardan bir tanesidir.[119]

2.10.4. Siber saldırı yöntemleri

Siber saldırılar, çeşitli devlet organizasyonlarına, yasal ya da yasadışı kuruluşlara, terörist organizasyonlara, şirketlere ya da şahıslara yönelik belirli amaçlar ve hedefler doğrultusunda siber uzay aracılığıyla yapılan saldırılardır. Siber saldırganlar, siber uzay içerisinde ki yazılım, donanım ve altyapı unsurlarını kendi amaçları doğrultusunda hedef almaktadırlar. Siber saldırganlar siber silahlar aracılığıyla çeşitli siber saldırı yöntemleri kullanmaktadırlar.[120]

Tablo-8: Siber Saldırı Yöntemleri

Siber Saldırı Yöntemleri
• Kabloyla Saplama Yapma (Wire Tapping)
• Tuzak Kapı (Trap Door)
• Hizmet Dışı Bırakma (Denial of Servıce- Dos)

[118] *A.g.e.,* ss.28-29
[119] Nezir Akyeşilmen, *a.g.e.,* s.78
[120] Hasan Çiftçi, *a.g.e*, s.151

• Dağıtık Hizmet Dışı Bırakma (Distributed Denial of Servıce- DDOS)
• İnternet Servis Saldırıları
• Kriptografik Saldırılar
• Zamanlama Saldırıları
• Trafik Analizi
• Ip Sahteciliği (Ip Spoofing)
• Zararlı Yazılım Kullanımı (Virüs, Solucan, Truva Atı, vb)
• Yığın Mail Gönderme (Spam)
• Oturum Çalma
• Açık Mikrofon Dinleme
• Sosyal Mühendislik (Social Engineering)
• Ağ Tarama (Network Scanning)
• Yerine Geçme (Masquerading)
• Oltalama (Phishing)

Kaynak: Hasan Çiftçi, *Her Yönüyle Siber Savaş*, 2. Basım, TÜBİTAK Yayınları, 2017 Ankara, s.157

2.10.4.1. Dos ve DDos saldırıları- Servis dışında bırakma saldırıları (Distributed Denail of Service Attacks)

Saldırganlar tarafından hedef olarak belirlenen bir web sitesini erişilmez kılmak veya hizmet vermeyecek duruma getirebilmek için yapılan saldırılardır. Bu saldırı türünde Botnet bilgisayarlar kullanılarak aynı anda hedeflenen bir web sitesinde talep yoğunluğu yaratarak sistem işlevsiz hale getirilmektedir.[121] Uluslararası siber çatışmalarda kullanılan en yaygın saldırı türüdür. Bu türe örnek olacak en iyi olay 2007 yılında Estonya'ya gerçekleştirilen DDos atakları serisidir.

Dos ve DDos saldırılarında kullanılan yöntemler şu şekildedir;[122]

[121] Şeref Sağıroğlu, *a.g.e.,* s.31
[122] Hasan Çiftçi, *a.g.e,* s.159

- Sistemlerin ağ bant genişliği, disk alanı ya da işlemcilerinin kaynaklarının tüketilmesi,
- Yönlendirici verilerin bozulması,
- Sistemlerin oturum bilgilerinin bozulması,
- Kullanıcılar ile sistem arasındaki iletişim altyapısının kesilmesi,

2.10.4.2. Oltalama, yemleme yada sazan avlama saldırıları (Phishing)

Bu tür saldırılarda amaç kullanıcıların kandırılarak insani zafiyetler sonucu bilgileri, şifreleri, kredi kartı numaraları vb. bilgilerin bir şekilde elde edilmeye çalışılmasıdır. Oltalama da kullanıcılara başka bir olay oluyormuş gibi kandırıp verilerini alıp gizli amaçlar doğrultusunda kullanılmaktadır.[123] Kullanıcılara genelde bir bankadan ya da güvenilir bir web sitesinden mesaj yoluyla veya mail aracılığıyla bir link gönderilir, gönderilen bu link ile bilgisayara kötücül yazılım yüklenir ya da bir web sitesine yönlendirilir.[124]

2.10.4.3. Sosyal mühendislik (Social Engineering)

Günümüzde ki en yaygın saldırı türlerinden bir tanesidir. Bu saldırı yönteminde temel amaç sistemlerin ya da ağların suiistimali yerine, insan zafiyetleri ya da zayıflıklarını kullanarak verileri elde etme amacındadır. Sosyal mühendislik yöntemi bir nevi sanal dolandırıcılık yöntemidir. Saldırganlar kullanıcıların güvenlerini sağlayıp onları ikna ederek kullanıcıların verilerine ulaşırlar.[125]

Yaygın olarak kullanılan sosyal mühendislik yöntemleri şu şekildedir;[126]

- Saldırganın güvenilir bir kaynaktan olduğuna ikna edilir,

---

[123] Hakan Hekim, "Oltalama (Phishing) Saldırıları", *Siber Suçlar, Tehditler, Farkındalık ve Mücadele*, Derleyenler: Fatih Tombul, Murat Güneştaş, Oğuzhan Başıbüyük, Global Politika ve Strateji, Ankara, 2015, s.58.
[124] Şeref Sağıroğlu, *a.g.e.,* s.31
[125] Nezir Akyeşilmen, *a.g.e.,* s.80
[126] Hasan Çiftçi, *a.g.e.,* s.166

- Saldırılacak sistemin atıklarında (eski donanım vb) araştırma yapmak,
- Kullanıcıların tanıdığı kişilerin isimlerini kullanarak bir yakınlık oluşturma,
- Başkasının yerine geçme,
- Gizlice zor bir durum yaratılarak kullanıcının bu durumdan kurtulmasına yönelik dostça görünerek yardımcı olmak,

2.10.4.4. Yığın mail (Spam Mail)

Yığın mail saldırılarında çok sayıda kişiye birbirine benzeyen içeriklere sahip maillerin gönderilmesiyle oluşturulmaktadır. Ağırlıklı olarak yasadışı ürünlerin tanıtımlarını yapmak için kullanılırlar. Yığın mailleri oluşturan kişiler mail veri setlerini web sitelerinden, sosyal medya sitelerinden ya da kurum, kuruşların müşteri listelerinden toplamaktadırlar. Özellikle son zamanlarda yığın mailler aracılığıyla kimlik hırsızlığına sebebiyet verecek oltalama saldırıları da yapılmaktadır.[127]

2.10.4.5. Sıfırıncı gün saldırıları (Zero Day)

Bu saldırı türünde siber güvenlik uzmanları tarafından daha bulunamamış ya da yayımlanmamış sistem açıklıklarına sıfırıncı gün açıklığı denilmektedir. Bu saldırı türünde sistemi yazan yazılımcıların fark edemediği bazı açıklıklar sayesinde saldırganlar sistemlere erişim sağlayabilmektedir. Sistem açığının keşfedilmesinin ardından sisteme bir güvenlik güncelleştirilmesi yapılarak sorun ortadan kaldırılmaktadır.[128]

2.10.4.6. Kabloyla saplama yapma (Wire Tapping)

Bu saldırı yönteminde güvenliği alınmamış ağ kablolarına özel cihazlarla fiziksel olarak yeni hat çekilerek ağ üzerinde bağlantı sağlanmaktadır.[129] Bu yöntem

---

[127] Şeref Sağıroğlu, *a.g.e.,* s.33
[128] *A.g.e.,* s.32
[129] Mithat Yıldız, *Siber Suçlar ve Kurum Güvenliği*, (T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Bilgi İşlem Daire Başkanlığı, Basılmamış Denizcilik Uzmanlık Tezi), Ankara 2014, s.31

ile ağ üzerinde tüm veri akışı incelenerek kaydedilebilmektedir. Özellikle İsrail yaptığı siber operasyonlarda düşman veri akışını dinlemek için sık sık bu yönteme başvurmaktadır.[130]

2.10.4.7. IP sahteciliği

Ip sahteciliği yönteminde sistemin gerçek ıp adresi saptırılarak gizlenmek veya başkasının yerine geçmek için kullanılan saldırı yöntemidir. Bu saldırı türü özellikle saldırganların hedefledikleri sisteme saldırırken kullandığı bir yöntemdir. Saldırganlara anonimlik sağlayarak kimliklerinin deşifre olması engellenmiş olur. Ayrıca, Ip adresi temelli kimlik doğrulama sistemlerinde güvenilir kullanıcıların Ip adreslerini kullanarak sisteme sızılıp verilere erişebilmektedir.[131]

2.10.4.8. Açık mikrofon dinleme yöntemi

Zararlı bir yazılım vasıtasıyla sistem sahibinin izni olmadan, sistemde ki mevcut kamera ve mikrofon aracılığıyla ortam dinlemesinin yapılması faaliyetidir. Açık mikrofon dinleme yönteminin en ünlü saldırısı GhostNet saldırısıdır. Bu saldırıda zararlı yazılımın elçilik ve devlet kurumlarının sistemlerine yüklenerek toplanan verilerin Çin'e iletildiği iddia edilmiştir.[132]

2.10.4.9. Oturum çalma (Session Hijacking)

Bu saldırı yönteminde sunucular ve istemciler arasında oturumun çeşitli siber saldırı yöntemleri ile ele geçirilip, karşı sisteme izinsiz giriş yapabilme yeteneğinin kazandırılması biçiminde yapılmaktadır. Bu saldırıda, saldırgan kullanıcı ve sunucu arasına girip ortadaki adam yöntemiyle tüm veri trafiğini inceleyebilmektedir.[133]

---

[130] Hasan Çiftçi, *a.g.e.,* s.58
[131] Hasan Çiftçi, *a.g.e.,* s.164
[132] *A.g.e.,* s.165
[133] *A.g.e.,* s.165

2.10.4.10. Zararlı yazılımlar

Sistemlere saldırıda bulunabilmenin bir başka yöntemi de hedeflenen sisteme zararlı yazılım (Virüs, Truva Atı, Solucan vb.) yüklemek ya da yüklenmesine yardımcı olmaktır.[134] Zararlı yazılımlar kendilerine özgü yöntemler ile hedef sistemlerde yerini alırlar. Zararlı yazılımlar hedef sistemde ki verilerin gizliliğine, erişilebilirliğine ya da bütünlüğüne zarar verici faaliyetlerde bulunmaktadırlar.[135]

2.10.4.11. Tuzak kapı saldırıları

Hedef sisteme yüklenen yazılım ya da sistem içerisinde bulunan yazılımın güvenlik açıklıkları gibi yöntemlerle kimlik doğrulama prosedürlerini aşarak gizlice sisteme erişmeyi sağlayan saldırı yöntemidir. Bu yazılımlar işletim sistemleri ya da uygulamalar vasıtasıyla sisteme yerleştirilebilirler. Tuzak kapı yazılımlarının tespit edilebilmeleri çok zordur.[136]

2.10.4.12. İnternet servis saldırıları

İnternete bağlı olan sistemler, çeşitli internet protokolleri ve servisleri vasıtasıyla birbirleriyle iletişime geçerler. İnternette ki protokollerin (Http, Dns, Tcp/Ip, Telnet vb.) açıklıklarından ya da bu protokolleri kullanan programların zafiyetlerinden yararlanarak hedef sisteme saldırma yöntemidir.[137]

---

[134] Enis Karaarslan, Gökhan Akın, Hüsnü Demir, "Kurumsal Ağlarda Zararlı Yazılımlarla Mücadele Yöntemleri", *Çanakkale On Sekiz Mart Üniversitesi Akademik Bilişim Konferansı*, Çanakkale 2008, s.1
[135] *A.g.e.,* s.164
[136] Hasan Çiftçi, *a.g.e.,* s.158
[137] *A.g.e.,* s.160

2.10.4.13. Trafik analizi yöntemi

Trafik Analizi, ağ trafiklerinde ki iletişimler tespit edilip bu iletişimlerin analizini yaparak değerli bilgileri elde etme yöntemidir. Bu yöntemde ağ içindeki gelip- giden verilerden ziyade bu verinin örüntüsüne ya da Bıg datasına bakılarak bir sonuca varılmaktadır.[138] Bu yöntemle mesajlar kriptolu ya da çok sayıda olsa da uygulanabilmektedir. Ağırlıklı olarak askeri istihbarat birimleri tarafından düşmanın iletişim altyapısından veri sızdırmak için kullanılmaktadır.[139]

2.10.4.14. Kriptografik sistemlere yönelik saldırılar

Bu saldırı yönteminde şifrelenmiş mesaj ya da verilerin şifrelerinin çözümlenmesi amacıyla yapılan saldırılardır. Ağırlıklı olarak kriptolama sistemlerinin zafiyetlerinin araştırılarak şifrelerin çözümlenmesi amaçlanmaktadır. Kriptografi genel olarak bilgilerin anlaşılabilir hallerinden anlaşılamaz hale çevrilmesiyle oluşturulan yöntemdir. Kriptoanaliz ise kriptografik sistem ve yaklaşımları analiz ederek şifreleri çözebilme yöntemidir.[140]

2.10.4.15. Zamanlama saldırıları

Bu saldırı yöntemi kriptografik saldırıların ayrı bir türüdür. Şifreleme için harcanan sürenin analizi yapılarak kripto sisteme baskı yapılması amacıyla paralel bir ağ ile yapılan saldırılara denilmektedir. Sistemlerde her bir işlem belirli süreler içinde gerçekleşmektedir. Bu sürenin uzaması veya kısalması işlenen veriye bağlı olarak değişmektedir. Verileri işlemeye harcanan sürelerin analiz yapılarak kriptolama sisteminin özelliklerine ve içindeki veriye ulaşılması amaçlanır.[141]

---

[138] Emin Ulaşanoğlu, Ramazan Yılmaz, Alper Tekin, *Bilgi Güvenliği: Riskler ve Öneriler*, Bilgi Teknolojileri ve İletişim Kurumu, Ankara 2010, s.21
[139] Hasan Çiftçi, *a.g.e.,* s.163
[140] Şeref Sağıroğlu, *a.g.e.,* s.33
[141] Hasan Çiftçi, *a.g.e.,* s.163

2.10.5. Siber güvenlik sistemleri

Bilgi ve iletişim teknolojilerinin yaygınlaşmasıyla birlikte kötü niyetli kişilerinde bu alandaki faaliyetleri artmaya başlamıştır. Özellikle kritik altyapı sistemleri saldırganlar tarafından hedef olarak belirlenmesi, hayatı olumsuz yönde etkileyebilecek olayların yaşanabilme riskini ortaya çıkarmıştır. Yaşanabilecek bu olumsuzluk durumlarında kamu düzeni ve güvenliği ciddi anlamda zarar görebilecektir.

Siber tehdit ve saldırılara karşı mücadele verilirken siber savunma sistemlerinin de etkin ve verimli bir şekilde işleyişlerine devam etmesi gerekmektedir. Bu sayede tam anlamıyla etkin bir siber savunma şemsiyesi oluşturulabilir. Siber tehdit ve saldırılara karşı korunma sistemlerine bakıldığında;

2.10.5.1. Kimlik doğrulama sistemleri

Sisteme giriş yapmak isteyen kullanıcının kim olduğunun teyit edilmesi, sisteme giriş yapılabilmesi için ilk aşamadır.

Tablo-9: Kimlik Doğrulama Sistemleri

Kullanıcı Bilgisi	Kullanıcı tarafından bilinen şifreler
	Zamana ve sorgu sırasına göre üretilen şifreler
Kullanıcı Kişi veya Konum Bilgisi	Kullanıcıyı doğrulayıcı elektronik simge ya da akıllı kart
	Kullanıcının kaynak adresinin doğrulanması
	Kullanıcının fiziksel konumuna dayalı doğrulama
	Kullanıcının elektronik simge ya da akıllı kartının kriptografik yöntemlerle sistem tarafından tanınması

Kullanıcının Özellikleri	Kullanıcının fizyolojik özelliklerine yönelik doğrulama (Retina taraması, Parmak izi, Yüz şekli, Ses)
	Kullanıcının vücudunu tanımlayıcı sistemin fiziksel olarak yerleştirilmesi

Kaynak: Hasan Çiftçi, *Her Yönüyle Siber Savaş*, 2. Basım, Tübitak Yayınları, 2017 Ankara, s.227

Kimlik doğrulama sistemlerinden olan iki aşamalı kimlik doğrulama sisteminde de kullanıcıların şifrelerinin yanı sıra ek bir erişim kontrol adımı eklenerek kullanıcının farklı bir şekilde sisteme girmesi amaçlanır. Bu sisteme örnek olarak internet bankacılığı sisteminde kullanıcının şifresi yanında tanımlı cep telefonu numarasına sms şifre gönderilmesi gösterilebilir.[142]

2.10.5.2. Zafiyet tarayıcısı sistemler

Zafiyet, bir yazılım, donanım, sistem, tasarım ve üretim süreçlerinden kaynaklanan, mantık, tasarım, bakım ya da test süreçlerinde oluşabilecek hatalardan kaynaklanan sistem güvenliğini tehlikeye atabilecek unsurlara denilmektedir.[143] Zafiyet tarayıcısı sistemleri ise sistemlerin, ağların, uygulamaların var olabilecek zafiyetlerini analiz ve tespit edebilen yazılımlardır. Bu yazılımlar zafiyet ile ilgili açıklıkları bulurken, saldırganların eylemlerine ilişkin delilleri de tespit edebilirler. Sistemlerde yapılan taramalar sonucunda, risklerin ortadan kaldırılıp, maksimum güvenlik seviyesine ulaşılması amaçlanmaktadır. Ayrıca tüm bu süreç sonunda yazılımdan sistem ile ilgili olarak bir "zafiyet raporu" elde edilmektedir.[144]

[142] Şeref Sağıroğlu, *a.g.e.,* s.32
[143] The Goverment of The Hong Kong Special Administrative, *Region an Overview of Vulnerability Scanners*,2008, *https://slidelegend.com/an-overview-of-vulnerability-scanners_5a0cdbd91723dd746a0fae27.html.*, (Erişim Tarihi: 10.09.2021.), s.2.
[144] Şeref Sağıroğlu, *a.g.e.,* s.30

2.10.5.3. Güvenlik duvarı (Firewall)

Bir ağ içerisinde yetkisiz olarak içeriden ve dışarıdan gelebilecek istekleri ya da işlemleri, standardize edilmiş kurallar doğrultusunda önleyen ya da bloklayan, sistemleri kendileri dışındaki işlemlerden korumak için tasarlanmış yazılım, donanım veya her ikisinin birleşiminden oluşan siber güvenlik çözümüdür.[145]

Güvenlik duvarları ağ trafiğini birden çok güvenlik işleviyle birlikte kontrol ederler. Bunlar;

- Paket Filtreleme
- Uygulama Filtreleme
- Durumsal Denetim
- Tüm Yöntemlerin Birleştirilmesi[146]

2.10.5.4. Saldırı tespit/ koruma sistemi (IDS/ IPS)

Bir sisteme, sunucuya ya da ağ sistemine yapılabilecek, yetkisiz erişimleri veya sızmaları tespit ederek buna karşı bir uyarı alarmı üreten sistemlerdir. Herhangi bir sistemin gizliliğine, erişilebilirliğine ya da bütünlüğüne yönelik saldırıları tespit eder. Koruma sistemleri de yapılan siber saldırıyı durdurmaya yönelik çalışan sistemlerdir.

Saldırı Tespit/Koruma Sistemleri iki temelde oluşmaktadır;

- Ağ tabanlı saldırı tespit/koruma tespitleri
- Bilgisayar tabanlı saldırı tespit/koruma sistemleri[147]

---

[145] US CERT- MS ISAC, Local Goverement Cyber Security: Beginner Guide To Firewalls, 2006, https://flmanagers.com/wp-content/uploads/2021/01/Cybersecurity-for-Local-Government-Guide.pdf., (Erişim Tarihi: 12.11.2021.), s.3.
[146] Hasan Çiftçi, *a.g.e.,* s.229
[147] Şeref Sağıroğlu, *a.g.e.,* s.32

2.10.5.5.Antivirüs sistemleri

İşletim sistemi olan tüm cihazlarda kullanılabilen bir siber güvenlik çözümüdür. Bu yazılımlar, virüslerin ve zararlı yazılımlar imza kodlarına bakarak güvenilirliğini teyit ederek sistemin zarar görmesini önlemektedir. Antivirüsler imza kodlarına bakmak dışında programların ya da dosyaların analizlerini inceleyerek şüpheli hareketleri tespit etmektedir.[148]

2.10.5.6.Yığın mail engelleme sistemleri

Kullanıcılara zarar vermek veya reklam yapmak amaçlı gönderilen maillerin sisteme girmesini ya da kullanıcı mail kutusuna gitmesini engelleyen sisteme denilmektedir.[149]

2.10.5.7. Veri kaçağı önleme sistemi

Bu güvenlik sisteminde kullanımda olan, hareketli olan ve geri kalan verinin önem derecelerine göre sınıflandırılması, takip edilmesi ve korunmasını sağlayan siber güvenlik sistemidir. Bu sistemler değerli verilerin kurumlardan çalınmasını engellemek amacıyla kurulur. Ayrıca sistemde kullanıcıların hangi verileri kaydetmesi, yazdırması ya da yollaması engellenebilir veya bu işlemlerin kayıtları tutulabilir.[150]

2.10.5.8. Hava boşluğu sistemi (Air Gap)

Hava Boşluğu Sisteminde, gizlilik dereceleri farklı iki ağ arasında güvenli bir biçimde veri aktarılmasını sağlamaktadır. Bu sistemde iki ağ arasında fiziksel bir

[148] Hasan Çiftçi, *a.g.e.,* s.231
[149] Şeref Sağıroğlu, *a.g.e.,* s.33
[150] Hasan Çiftçi, *a.g.e.,* s.232

bağlantı olmayıp, iki ağ arasında kurulan hava boşluğu ile verilen güvenli bir biçimde aktarımı sağlanır.[151]

2.10.5.9. Adli bilişim sistemleri

İletişim ağları ve veri depolama sistemlerinde ki delil sayılabilecek verileri yasal bir zeminde toplamaya ve incelemeye yarayan donanım ve yazılım unsurlarına adli bilişim sistemleri denilmektedir.[152]

Genellikle kullanılan adli bilişim sistemleri şu şekildedir;

- İmaj alma,
- Yazma engelleme,
- Adli analiz yazılımı,
- Veri kurtarma yazılımları,
- Parola kırma sistemleri,
- Şifreleme analiz sistemleri,
- İmaj dönüştürme,[153]

2.10.5.10. Ağ erişim kontrol sistemleri (Network Access Control-NAC)

Bu sistem, ağa ya da ağ üzerindeki verilere erişim sağlamak için sistemlerde güvenlik araçlarını kontrol eden sisteme denilmektedir. Bir sistem ağ bağlamadan önce işletim sisteminin güncelliği, antivirüs yazılımlarının güncelliği, bazı dosyaların varlığı aşamaları analiz edip teyit ederek sisteme ağ giriş yetkisi vermektedir.[154]

---

[151] *A.g.e.,* s.232
[152] US-CERT, *Computer Forensics*, 2008, *https://www.cisa.gov/uscert/sites/default/files/publications/forensics.pdf.,* (Erişim Tarihi: 16.12.2021.), s.1.
[153] *A.g.e.,* s.233
[154] Hasan Çiftçi, *a.g.e.,* s.234

2.10.5.11.İçerik filtreleyici sistemler

Ağ ya da sisteme giren ve sistemden çıkan trafiği analiz ederek istenmeyen geçişleri engelleyen sistemdir. Bazı dosya türleri, internet adresleri ve belirli kelimeler bu sistem aracılığıyla filtrelenebilir.[155]

2.10.5.12. Uç nokta güvenliği sistemi (Endpoint Security)

Bu güvenlik sisteminde temel prensip her sistemin kendini korumasını yetebilecek kadar güvenlik yazılımına sahip olması ve bu güvenlik yazılımları eş güdümlü bir şekilde çalışması amaçlanmaktadır. Genel olarak uç nokta güvenlik sistemlerinde güvenlik duvarı, antivirüs, saldırı tespit/ korunma sistemi, ağ erişim kontrol yazılımı, şifreleme yazılımı, veri kaçağı önleme yazılımı gibi yazılımların eş güdümlü olarak çalışmasıyla sistem kurulur.[156]

2.10.5.13. Stenografi sistemi

Stenografi veri gizleme bilimidir. Veriler şifrelenmez gizlenir. Bu sistemin şifrelemeye göre en önemli avantajı veriyi gören kimsenin gördüğü şeyde önemli bir veri olduğunu fark edememesidir.[157]

2.10.5.14. Bal küpü sistemi (Honeypot)

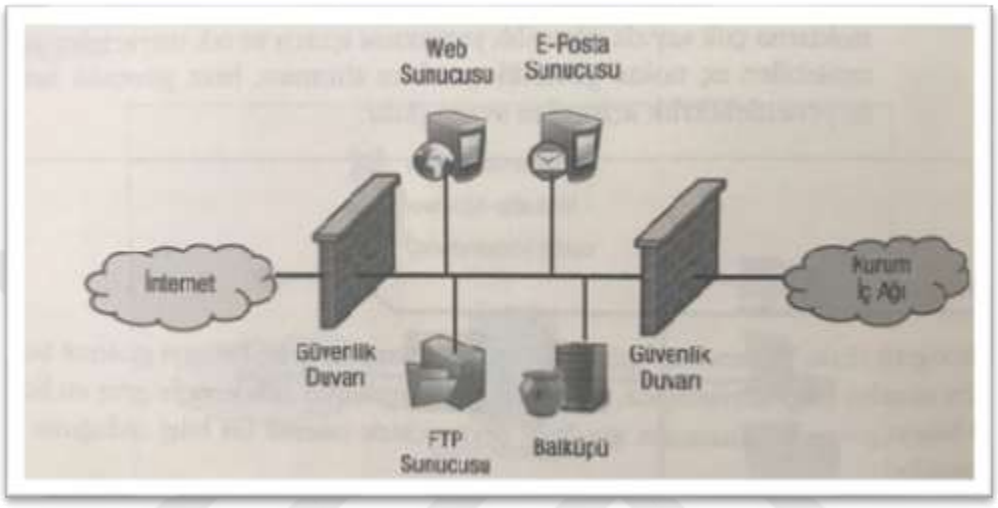
Sistemlere ya da verilere erişmek isteyen saldırganları bulmak amacıyla, sistemin bir parçası gibi olan fakat tuzak olarak kurulan sistemlere denilmektedir.[158]

---

[155] *A.g.e.,* s.234
[156] *A.g.e.,* s.235
[157] Hasan Çiftçi, *a.g.e.,* s.235
[158] The Goverment of The Hong Kong Special Administrative, "*Honeypot Security*", Şubat 2008, *https://docplayer.net/3431533-Honeypot-security-february-2008-the-government-of-the-hong-kong-special-administrative-region.html.,* (Erişim Tarihi: 12.11.2021.), s.2.

Bu sistem üzerinde kasıtlı olarak bazı zafiyetler bırakılarak, güvenlik sistemlerinin aşan saldırganların yakalanması amaçlanmaktadır.[159]

Tablo-10: Bal Küpü Sistemi



Kaynak: Hasan Çiftçi, *Her Yönüyle Siber Savaş*, 2. Basım, TÜBİTAK Yayınları, 2017 Ankara, s.236

2.10.5.15. Güvenlik veri ve vaka yönetim sistemleri (SIEM)

Bir kurum veya kuruluş da tutulan kayıtların sadece siber vaka gerçekleştiğinde analiz edilmesi uygun değildir. Sistemlerde saniyeler içinde binlerce rutin vaka gerçekleşmekte, her bir vaka tek tek incelenememektedir. Bu sebeplerden dolayı siber vakalarda ki belirli tutarlılıklar eşleştirilip ve daha önceden tanımlanan durumlar gerçekleştiğinde uyarı amaçlı bir alarm üretilmesi gerekmektedir. Tüm bu ihtiyaçların karşılanabilmesi için güvenlik veri ve vaka yönetim sistemleri geliştirilmiştir. Bu sistemler kayıtları toplayıp, analiz ederek daha önceden tanımlanan durumlardan biri gerçekleştiğinde uyarıcı alarm üreten sistemlerdir.[160]

2.10.5.16. Kriptolama sistemleri

Sistemlerin, ağların, veri tabanlarının ve dosyaların güvenliğini sağlayabilmek için içerisindeki verilerin şifrelenmesi yöntemidir. Bazı kriptolama sistemlerine bakılacak olursa;

[159] Hasan Çiftçi, *a.g.e.,* s.236
[160] Hasan Çiftçi, *a.g.e.,* s.236

- Dosya- dizin kriptolama yazılımları, (7-Zip, TrueCrypt)
- Veri tabanı kriptolama yazılımları (Netlib, Vormetric vb.)
- Mail kriptolama yazılımları (PGP)
- Ağ trafiği kriptolama yazılımları (Ipsec, Virtual Private Network- VPN)
- Sabit disk kriptolama yazılımları (Bitlocker, PGP)[161]

2.10.5.17. Sayısal imza (Digital Signature)

Verilerin güvenliği için onun şifrelenmesinin ve bütünlüğünün korunması yanında o veriyi işleyenin kim olduğu, verinin başkası tarafından değiştirilip değiştirilmediği ve tamamının ya da bir kısmının silinmediği bilinmelidir. Bu yüzden sayısal imza yöntemiyle kullanıcının gerçek yetki sahibi kullanıcı olduğu teyit edilmektedir.[162]

Sayısal imza yöntemi üç ana güvenlik prosedürünü sağlar;

- **Kimlik doğrulama (authentication):** Kullanıcının kimliği doğrulanır.
- **Bütünlük (integrity):** Verinin değişikliğe uğramadığı teyit edilir.
- **İnkâr edememe (non-repudiation):** Gizli anahtar sadece kendisinde bulunan kullanıcı verilerini inkâr edemez.

Türkiye Cumhuriyetin 'de "5070 sayılı Elektronik İmza Kanunu" ile birlikte belirlenen şartları yerine getiren sayısal imzalar, elle atılan ıslak imzalar ile aynı geçerliliğe sahip olmuşlardır.[163]

2.10.5.18. Siber olaylara müdahale ekibi (SOME)

2016- 2019 Ulusal Siber Güvenlik Strateji Belgesine göre siber olay;

> *"Bilişim ve Endüstriyel kontrol sistemlerinin ya da bu sistemlerce işlenen verilerin gizliliği, erişilebilirliği ya da bütünlüğünün ihlal edilmesi veya ihlal edilme girişimleri"*

[161] *A.g.e.,* s.237
[162] Kemal Ermiş, "Sayısal İmza ve Elektronik Belge Yönetimi", *Bilgi Dünyası,* Cilt: 7, Sayı:1, 2006, ss.122-123.
[163]Hasan Çiftçi, *A.g.e.,* s.238

Olarak tanımlanmıştır.[164] Siber Olaylara Müdahale Ekipleri kurumlara doğrudan ya da dolaylı yollar ile yapılan siber saldırı ve tehditlere karşı tüm önlemleri alma ya da aldırma, siber olaylarla mücadele edebilecek organizasyonları oluşturma ve olayları kayıt altına alıp, veri güvenliğine yönelik çalışmaları yapma ya da yaptırma görevlerinden sorumludur. Ayrıca, siber olayların azaltılması, önlenmesi, kurum ve kuruluşların bilgi ve iletişim sistemlerinin kurulması, işletilmesi ve geliştirilmesiyle ilgili olarak birimlere öneriler sunmakla yükümlüdür. Somelerde önemli olan husus etkili eşgüdümün sağlanması ve nitelikli teknik güvenlik personelinin istihdam edilmesidir.

Siber Olaylara Müdahale Ekipleri üç ana grupta hizmet verirler.

- Tepki Servisleri
- Önleyici Servisler
- Güvenlik Kalite Yönetimi Servisleri[165]

2.10.5.19. Elektronik güvenlik sistemleri (TEMPEST)

Bu türden güvenlik sistemleri elektromanyetik kuvvetlendirme aracılığıyla çalışmaların zafiyete uğratılmasına, sinyallerin düşmanlar tarafından yakalanmasına yönelik koruma sağlarken aynı zamanda yapılandırılmış enerji saldırılarına karşıda etkin bir sistemdir. Önemli verilerin işlendiği sistemlerin yaydığı elektromanyetik dalgaların araştırılması, tespit edilmesi, incelenmesi ve kontrol altında tutulabilmesini içeren güvenlik sistemleri bütünüdür.[166]

[164] 2016-2019 Ulusal Siber Güvenlik Strateji Belgesi, s.7
[165] *A.g.e.,* s.8
[166] Hasan Çiftçi, *a.g.e.,* s.242

3) TÜRKİYE'DE YAPILAN SİBER GÜVENLİK ÇALIŞMALARI

Türkiye'nin siber uzay ile ilgili olarak yapmış olduğu ilk çalışmalar 1991 yılına kadar dayanmaktadır. 6 Haziran 1991'de Türk Ceza Kanunu'nda 3756 sayılı kanun ile "Bilişim Alanında ki Suçlar" başlığı altında yer alan bir bilgisayardan, verilerin yasadışı yollarla elde edilmesi, çoğaltılması veya başka bir ortama aktarılmasının ceza unsuru olarak tanımlanmasıyla yerini almıştır.[167] Eylül 2004 yılına gelindiğinde 5237 sayılı TCK ile tanımın kapsamı genişletilerek bilişim alanında ki suçlar yerini siber suç kavramına bırakmıştır. 2006 yılında 3713 sayılı Terörle Mücadele Kanunu kapsamında yapılan değişiklikler sonucu siber suç kavramı terör suçları içerisine alınmıştır. Bu kanunun 243 ve 244. Maddelerinde siber suç, bilişim sistemine sızma, sistemi bozma, engelleme, sistem içerisinde ki verileri yok etme ve değiştirme maddelerine ek olarak bilişim sistemleri aracılığıyla işlenebilecek diğer suçların listesini de içermektedir. Yapılan bu yasal mevzuatların dışında Devlet Planlama Teşkilatı kamu hizmetlerinin vatandaşa internet aracılığıyla sağlanabilmesi için "e-Türkiye inisiyatifi Eylem Planı 2002", "e-Dönüşüm Türkiye Projesi ve Kısa Dönem Eylem Planı (2003-2004)" ve e-Dönüşüm Türkiye Projesi 2005 Planı" eylemlerini açıklamıştır.[168] Dünyada yaşanan büyük çaplı siber saldırılar ve gün geçtikçe artan siber tehditlere karşı Türkiye bilgi ve iletişim altyapısını korumak için çeşitli çalışmalar yapmaya başlamıştır. Bu önlemlerden ilki 2008 yılında TÜBİTAK Ulusal Elektronik ve Kriptoloji Enstitüsü (UEKAE) öncülüğünde bir çalışma grubu kurulmuştur. Bu ekibin içerisinde kamu kurum ve kuruluşlarından temsilciler yer almıştır. Çalışma grubunun yaptığı faaliyetler sonucunda 2009 yılında "Ulusal Sanal Ortam Güvenlik Politikası" yapılmıştır.[169] Belge içerisinde bir eylem planı ve politika stratejileri bulunmasa da Türkiye'ye yönelik tehditleri, açıklıkları ve riskleri belirttiği için önemlidir. Bu belgenin bir diğer önemi ise Türkiye'nin siber güvenlikle alakalı hazırlamış olduğu ilk resmî belge olma özelliğini taşımaktadır. TR-BOME tatbikatı ve

[167] Salih Bıçakçı, Doruk Ergun, Mitat Çelikpala, *Türkiye'de Siber Güvenlik,* EDAM Siber Politika Kağıtları Serisi, Yıl:2015, Sayı:1, ss.30-31
[168] *A.g.e.*ss.30-31
[169] Mehmet Emin Erendor, *Türkiye'nin Siber Güvenlik Politikası, Yeni Küresel Tehdit Siber Saldırılar*, Derleyen: Fulya Köksoy, Nobel Yayınları, Ekim 2020, s.306

Ulusal Sanal Ortam Güvenlik Politikasının kabulünün ardından siber saldırı ve tehditlerin küresel boyutta ciddi etkileri olmaya başlamıştır. Milli Güvenlik Kurulu (MGK) 27 Ekim 2010 tarihli toplantısında siber saldırılar ve tehditleri değerlendirmiştir. Kurul toplantısında siber saldırı ve tehditleri şu şekilde ifade etmiştir;[170]

> "*Siber tehdidin küresel düzeye ulaştığı ve bu tehdidin ulusal güvenliğe etkileri kapsamlı olarak ele alınmıştır. Bu bağlamda, siber tehdidin engellenmesi açısından milli düzeyde yapılan çalışmalar değerlendirilmiştir."*

Siber saldırılar ve tehditler Türkiye'nin ulusal düzeyde algıladığı güvenlik sorunları haline gelmiş ve "Milli Güvenlik Siyaset Belgesi" içerisinde yer almasına karar verilmiştir. Türkiye bu şekilde siber saldırı ve tehditlere karşı önlemler almak için bir kararlılık ve irade koyduğunu göstermiştir.

Türkiye'de özellikle siber güvenlik eksenli yasal düzenlemeler 11.06.2012 tarihinde Bakanlar Kurulu'nun 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" yürürlüğe girmesiyle başlamıştır. Alınmış olan bu Bakanlar Kurulu kararının öncesinde Türkiye'de siber güvenlikle ilgili yetkili merci TÜBİTAK iken kararın yürürlüğe girmesinin ardından siber güvenlikle ilgili yetkili kurum Ulaştırma ve Altyapı Bakanlığı olmuştur.[171] Karar ile birlikte Siber Güvenlik Kurulu oluşturulmuştur. Ayrıca kararla Siber Güvenlik Kurulu ile birlikte Ulaştırma ve Altyapı Bakanlığı'nın yetkileri ve sorumlulukları belirlenmiştir.

---

[170] Milli Güvenlik Kurulu Genel Sekreterliği, 27 Ekim 2010 tarihli toplantı, *https://www.mgk.gov.tr/index.php/27-ekim-2010-tarihli-toplanti.*, (Erişim Tarihi: 14.02.2021)

[171] Volkan Göçoğlu, *Türkiye'nin Siber Güvenlik Politikası: Karar Verme Yaklaşımları Çercevesinde Bir Analiz", Güvenlik, Teknoloji ve Yeni Tehditler,* Derleyen: Ali Burak Darıcılı, 1.Basım, Nobel Yayınları, Mart 2020, s.92

2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" ile siber güvenliğe yönelik olarak Ulaştırma ve Altyapı Bakanlığı'na çeşitli görevler ve sorumluluklar verilmiştir;[172] "

- *Siber güvenliğin tesisi hususunda politikalar, stratejiler ve eylem planları hazırlamak,*
- *Kamu kurum ve kuruluşlarının verilerinin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması amacıyla usul ve esasları hazırlamak,*
- *Kamu kurum ve kuruluşlarında siber güvenliğin sağlanması yolunda teknik altyapının oluşturulması, yapılanların doğruluğu ve test edilmesinin sağlanması,*
- *Kritik altyapıları ve sistemleri belirleyerek bunlara yapılabilecek siber saldırılara ve tehditlere karşı izleme, müdahale ve önleme sistemlerini oluşturup ilgili merkezleri kurmaya, kurdurmaya ve denetlemeye yönelik çalışmalarda bulunmak,*
- *Siber saldırı ve tehditlere karşı her türlü yerli çözümlerin geliştirilmesine ve üretilmesine teşvikler verilmesi,*
- *Kritik kurum ve mevkiler için yeterli sayıda uzmanın temini, eğitimi ve yetiştirilmesi konularında gerekli planlamayı yapmak,*
- *Ulusal siber güvenlik farkındalığının oluşturulması için çalışmalar yürütmek,*
- *Siber Güvenlik Kurulu'nun sekretarya görevini yürütmek."*

2012/3842 sayılı " Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" ile kurulan Siber Güvenlik Kurulu , Ulaştırma ve Altyapı Bakanı Başkanlığında, Bilgi Teknolojiler ve İletişim Kurumu Başkanı, Mali Suçlarla Mücadele Başkanı, Telekomünikasyon İletişim Kurumu Başkanı, Genelkurmay Muhabere ve Elektronik Bilgi Sistemleri Başkanı ve ihtiyaç halinde Ulaştırma ve Altyapı bakanının belirleyeceği bakanlık ve kamu kurumlarının üst düzey temsilcilerinden oluşmasına karar verilmiştir.

Siber Güvenlik Kurulunun görevleri;[173]

- Siber güvenlikle alakalı politikaları, stratejileri ve eylem planlarını belirlemek ve uygulanması yönünde gereken kararları almak,
- Kritik altyapıların ve sistemlerin belirlenmesi doğrultusunda çalışmalarda bulunmak,

[172] T.C. Resmî Gazete, Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar (2012), Karar Numarası:28447, *https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm* 20 Ekim 2012, (Erişim Tarihi: 12.04.2020).
[173] *Aynı yerde.*

- Siber güvenlikle ilgili hükümlerde istisnai tutulabilecek kurum ve kuruluşları belirlemek,
- Kanunlarla belirlenen diğer sorumluluklarını yerine getirmek.

3.1 2013-2014 Ulusal siber güvenlik strateji belgesi

Siber Güvenlik Kurulu'nun Aralık 2012 yılında yaptığı ilk toplantısının ardından Ulaştırma ve Altyapı Bakanlığı önderliğinde çeşitli kurum, kuruluşlar ve sivil toplum kuruluşlarının destekleriyle 2013-2014 Ulusal Siber Güvenlik Strateji Belgesi 20 Haziran 2013'de Resmî Gazete 'de yayınlanarak yürürlüğe girmiştir. Bu strateji belgesi ulusal çapta siber güvenliğin sağlanması yolunda üzerine sorumluluk düşen paydaşlara çeşitli zamanlar içerisinde yükümlülükler yüklemektedir. 2013-2014 Ulusal Siber Güvenlik Strateji Belgesi Türkiye'de siber güvenlik ekosisteminin kurulması hedefiyle oluşturulmuş ilk kapsamlı belge olma özelliğini taşımaktadır.

2013-2014 Ulusal Siber Güvenlik Strateji Belgesi'nin oluşturulma amaçları şu şekilde ifade edilmektedir;[174]

- *Kamu kurum ve kuruluşlarında ki bilgi ve iletişim sistemlerinin güvenliğinin sağlanması,*
- *Kamu veya özel sektörün işlettiği kritik altyapıların ve sistemlerin güvenliğinin sağlanması,*
- *Siber olayların olası etkilerinin minimum düzeyde tutulmasına ve yaşanan olayların ardından sistemlerin normal çalışma rutinine dönebilmesini sağlamaya yönelik çalışmalar yapmak,*
- *Oluşan siber olayların sorumlularının adli makamlarca ve kolluk kuvvetlerince araştırılmasının ve soruşturulmasının sağlanması maksadıyla altyapı sistemlerinin oluşması,*

2013-2014 Ulusal Siber Güvenlik Strateji Belgesi'nde Türkiye'nin mevcut siber güvenlik riskleri şu şekilde belirtilmektedir;[175]

[174] T.C. Resmî Gazete, Ulusal Siber Güvenlik Stratejisi (2013-2014), 20 Haziran 2013, Karar Numarası: 28683, *https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm*,s.6 *(*Erişim Tarihi: 12.04.2020*).*

[175] (2013-2014) Ulusal Siber Güvenlik Stratejisi (2013), s.12

"1. Siber uzayın anonimlik ve inkâr edebilirlik imkanları sunması, siber saldırıların maliyetlerinin çoğu zaman çok ucuz ve siber silahların kolay elde edilebilir olması, herhangi bir zamanda ve herhangi bir yerden sistemlere yönelik kasıtlı veya kasıtsız siber saldırı yapabilme imkanının sunulması ve asimetrik bir tehdit oluşturması,

2.Siber uzayın bütünleşik ve kesintisiz haberleşme altyapısı sayesinde kötücül yazılımlar vb. tehditler sonucu tüm bilişim sistemlerinin birbirlerine zarar verebilme potansiyellerinin bulunması,

3.Günümüzde kritik altyapıların ve sistemlerinin birçoğunun bilgi ve iletişim teknolojileri aracılığıyla kontrol ediliyor olması,

4.Kritik altyapıların ve sistemlerin mevcut bilgi ve iletişim altyapısının çoğunun internete bağlı olarak hizmet vermesi,

5.Ulusal düzeyde siber güvenliğin sağlanması noktasında vatandaşların siber güvenlik bilincinin yetersiz seviyede olması,

6.Siber güvenlik konusunda paydaş olan kurum ve kuruluşlar arasındaki ulusal koordinasyonun yeterli seviyede olmayışı,

7.Kişilerin veya kurumların toplum önünde itibarlarını kaybetmesi korkusuyla siber saldırıları saklamaları,

8.Siber güvenlik olaylarının araştırılması ve soruşturulması safhasında ki ulusal ve uluslararası mevzuat eksiliğinden kaynaklı sıkıntıların yaşanması,

9.Kurum ve kuruluşlarda siber güvenlik yönetimi altyapısının yeterli seviyede olmaması,

10.Siber güvenlik alanında kişi, kurum ve kuruluşların yeterli düzeyde bilgisinin ve farkındalığının olmayışı,

11.Siber güvenlik konusunda kurum ve kuruluşlarda yapılanmaların eksiliği ve sadece bilgi işlem bölümlerin bu konuda sorumlu tutulması yanlışlığının yapılması,

12.Bilgi işlem bölümlerinin çalışanlarının yeterli seviyede siber güvenlik bilgi ve tecrübesinde olmayışı,

13.Kurum ve kuruluşların denetim süreçlerinde siber güvenlikle ilgili denetim adımlarının yeterli düzeyde olmayışı,

14.Donanım ve yazılım konusunda yerli ürünlerin yeterli düzeyde olmayışı,"

2013-2014 Ulusal Siber Güvenlik Strateji Belgesi'nde Türkiye'nin mevcut siber güvenlik riskleri ortaya koyulmuş, çeşitli kurum ve kuruluşlarının veri sağlayıcıları, bilgi sistemleriyle kamu veya özel sektör aracılığıyla işletilen kritik altyapıların ve sistemlerin siber güvenliğinin sağlanması için sorumlu olan mekanizmalara çeşitli görevler verilmiştir.

Bu stratejik siber güvenlik eylem planında 7 ana başlık altında 29 eylem yönergesi, 86 alt eylem yönergesi ve 31 sorumlu kurum, kuruluş ve organizasyon yer almaktadır.[176] 2013- 2014 Ulusal Siber Güvenlik Strateji Belgesi'nin eylem planında şu hususlara değinilmiştir;

1. Yasal Çalışmaların ve Düzenlemelerin oluşturulması,
    - Siber Güvenlik Kurulu'nun çalışmalarına başlaması ve gerekli usul ve esaslarının çerçevesinin çizilmesi,
    - Yasal düzenlemelerin yapılması noktasında siber güvenlik alanında ki ulusal ve uluslararası mevzuatların analiz edilmesi,
    - Siber güvenlik alanı özelinde sözlük ve terminolojilerin oluşturulması,
    - Siber güvenliğin tesisi hususunda gerekli mevzuat ve yönetmelik çalışmalarının oluşturulup siber güvenlik kuruluna sunulması,

2. Adli Olaylara Yardımcı Olabilecek Çalışmaların Yapılması,
    - Siber olayların gerçekleşmesinin ardından suçluların yakalanması sürecine yardımcı olabilecek güvenilir deliller elde edilmesini sağlayan günün şartlarına uygun olarak kayıt sistemlerinin kurulması,
    - Kritik altyapılar ve sistemlerde uluslararası standartlara uygun siber olaylar kayıt sistemlerinin kurulması,

3. Ulusal Siber Olaylara Müdahale Merkezinin Kurulması,
    - Ulusal koordinasyonu ve uluslararası işbirliğini gerektiren konularda 7/24 faaliyet gösterecek olan Ulusal Siber Olaylara Müdahale Merkezi (USOM)'un oluşturulması,
    - Kurumsal ve sektörel bazlı Siber Olaylara Müdahale Ekipleri (SOME)'lerin kurulması ve işletilmesi,
    - SOME'ler doğrudan USOM'un koordinasyonunda ve onun sağladığı destek ile çalışması,

[176] (2013-2014) Ulusal Siber Güvenlik Stratejisi (2013), s.17

4. Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi,
    - Kritik altyapıların ve sistemlerin risk analizlerinin yapılarak sektörel acil eylem planlarının oluşturulması,
    - Kamuda bilgi güvenliğinin sağlanması amacıyla ihtiyaçlar doğrultusunda güvenlik programı oluşturulması,
    - Siber güvenlik alanında eğitim faaliyetlerinin artırılması,
    - Belirli aralıklarla siber saldırılara hazırlık düzeyinin ölçülmesi maksadıyla siber güvenlik tatbikatlarının yapılması,
    - Yazılım güvenliği programının faaliyete geçirilmesi,
    - Siber tehditlerin önlenmesine yönelik projelerin hayata geçirilmesi,
    - Siber güvenlik alanında ki ürünlerin ve hizmetlerin sertifikasyon işlemlerinin yetkili kurumlarca yapılması,
    - Adli bilişim alanında hizmet veren gerçek ve tüzel kişilerde olması gereken minimum standartların belirlenmesi ve sertifikalandırılması,
    - İş sürekliliğini sağlayan ve veri yedekleyen sistemlerin kurulması,
    - Veri sızmasına yönelik test altyapısının geliştirilmesi ve uygulanması,
    - Kamu kurum ve kuruluşlarında veri kısıtlaması getirilerek verilere olan erişim seviyelerinin kademelendirilmesi,
    - Açık kaynak koduna sahip ürün ve sistemlerin kullanımının yaygınlaştırılması,

5. Siber Güvenlik Alanında Nitelikli İnsan Kaynağının Yetiştirilmesi,
    - Siber güvenlik alanında çalışmalar yapacak akademisyenlerin desteklenmesi,
    - Üniversitelerde siber güvenlik farkındalığının artırılması amacıyla eğitimlerinin artırılması,
    - Siber güvenlik uzmanlığına yönlendirme programlarının yürütülmesi,
    - Kullanıcıların siber güvenlik konusunda farkındalığının oluşturulması,
    - Ulusal ve uluslararası boyutta siber güvenlik etkinliklerinin organize edilmesi,

6. Siber Güvenlik Alanında Yerli Ürün ve Teknolojilerin Geliştirilmesi,
    - Araştırma- Geliştirme (Ar-Ge) faaliyetlerini destekleyici yapıların oluşturulması,
    - Alana özel Araştırma-Geliştirme (Ar-Ge) laboratuvarlarının yapılması,
    - Siber güvenlikte yerli ürün ve teknolojilerin geliştirilmesi ve desteklenmesi,

7. Ulusal Güvenlik Mekanizmalarının Kapsamının Geliştirilmesi,
    - Ulusal siber güvenliğin milli güvenliğin sağlanmasında önemli bir yapı taşı olduğu,
    - Siber olaylar gerçekleştiğinde kurumların sorumlulukları ve koordinasyonunun belirlenmesi,
    - Türkiye'yi hedef alabilecek siber tehditlerin analizinin yapılması,

3.2. 2016-2019 Ulusal siber güvenlik strateji belgesi

Değişen ve dönüşen siber uzayda artan güvenlik riskleri ve kazanılan tecrübeler doğrultusunda zamanın koşullarına uygun olacak şekilde Ulusal Siber Güvenlik Strateji Belgesi'nin revize edilmesi gerekmiştir. Bu çerçevede Ulaştırma ve Altyapı Bakanlığı önderliğinde eski strateji planındaki sorumlu olan kurum ve kuruluşlarla 10 Mart-7 Nisan 2015 tarihleri arasında eski plana yönelik yedi adet değerlendirme toplantısı gerçekleştirilmiştir.[177] Bu değerlendirmelerin sonucu olarak eski strateji planındaki gerçekleştirilen faaliyetler, karşılaşılan güçlükler ve ileri dönük olarak görüşleri alınarak not edilmiştir. Toplantıların akabinde 73 kurum ve kuruluştan toplam 126 uzmanın katılımıyla Ortak Akıl Platformu oluşturulmuştur. Bu platformda Türkiye'nin siber güvenlik alanında ki güçlü ve zayıf tarafları ve yapılması gereken

[177] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, *2016-2019 Ulusal Siber Güvenlik Stratejisi (2016), http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf* s.6.(Erişim Tarihi:22.04.2020).

eylemler belirlenmiştir.[178] Tüm bu yapılanların yanı sıra dünyadaki çeşitli ülkelerin ulusal siber güvenlik strateji belgeleri analiz edilip çeşitli başlıklar altındaki çözümleri incelenmiştir. Tüm bu çalışmaların sonucu olarak 2016- 2019 Ulusal Siber Güvenlik Strateji Belgesi yayınlanmıştır. Hazırlanan bu strateji belgesi devlet eksenli bir siber güvenlik anlayışının yerine siber uzayın ülke içerisindeki tüm paydaşlarını kapsayacak şekilde çok yönlü bir bakış açısı ile oluşturulmuştur. Milli güvenliğin sağlanması hususunda siber güvenlik faaliyetlerinin önemi ayrıca vurgulanmıştır.

Tüm bu yapılan faaliyetler ışığında strateji belgesinde, ulusal siber güvenliğin sağlanabilmesi hususunda şu ilkeler belirtilmiştir;[179]

1. Siber güvenlik, risk yönetimini temel alan etkili ve sürekli analize dayalı yöntemler vasıtasıyla sağlanacaktır. Ortaya çıkan risklerin ele alınarak kabul edilebilir bir seviyeye indirgenerek yönetilmesi amaçlanmaktadır.
2. Siber güvenliğin sağlanması hususunda tüm paydaşların riskleri ve bu riskleri nasıl yöneteceklerini bilmeleri önemlidir. Bu çerçevede siber farkındalığın artırılması için eğitim ve deneyim kazanımları şarttır.
3. Siber saldırı ve tehditler sonucu doğabilecek zararlardan en az seviyede etkilenebilmek için bu faaliyetlere karşı hazırlık ve süreklilik planlarının bulunması gerekmektedir.
4. Siber güvenliğin sağlanması ve etkin bir şekilde sürdürülebilmesi için kamu, özel sektör, sivil toplum kuruluşları, üniversiteler ve bireylerin dahil olduğu işbirliği ekosisteminin yanı sıra uluslararası işbirlikleri de tesis edilmelidir.
5. Siber uzayın güvenliği sağlanırken, hukukun üstünlüğü, ifade özgürlüğü, insan hakları ve mahremiyetin korunmasıyla ilgili prensipleri göz ardı etmemesi gerekmektedir.
6. Tüm paydaşlar siber uzay içerisindeki sorumluluklarını yerine getirirken şeffaf ve hesap verebilir olmalıdırlar.
7. Siber güvenlik önlemlerinin riskler ile orantılı bir biçimde oluşturulması gerekmektedir.

[178] Aynı yerde.
[179] 2016-2019 Ulusal Siber Güvenlik Stratejisi (2016), *a.g.e.* s.11

8. Siber güvenlik ihtiyaçlarının karşılanmasında yerli ürün ve hizmetlerin kullanılması teşvik edilmeli ve bunların geliştirilmesine yönelik projeler desteklenmelidir.

2016-2019 Ulusal Siber Güvenlik Strateji Belgesi'nde siber uzayda Türkiye için öngörülen siber güvenlik risk unsurları şu şekilde belirtilmiştir;[180]

1. Kritik altyapılara ve sistemlere yönelik yapılabilecek Dos ve DDos benzeri saldırılar sonucu enerji, su, telekomünikasyon, ulaştırma gibi önemli hizmetlerin aksaması,
2. Yapılacak siber saldırılar sonucunda kamuya ve kişilere ait özel bilgilerin gizliliği, erişilebilirliği veya bütünlüğünün zarar görmesi,
3. Ar-Ge faaliyetinde bulunan ve üretim yapan kurum ve kuruluşların hassas bilgilerinin gizliliğinin, erişilebilirliğinin ya da bütünlüğünün bozulması,
4. Propaganda faaliyeti amaçlı yapılan siber saldırılar sonucu kurum ve kuruluşların kamuoyu önünde itibarlarının zarar görmesi ya da verilerinin gizliliğinin, erişilebilirliğinin ya da bütünlüğünün bozulması,
5. İnternet üzerinde hizmet veren kuruluşların Dos veya DDos saldırılarına uğraması sonucu hizmetlerinde yaşanan aksaklıktan dolayı maddi kayba uğraması veya verilerinin gizliliğinin, erişilebilirliğinin ya da bütünlüğünün zarar görmesi,
6. Finans ve bankacılık hizmeti veren kuruluşlarının müşterilerinin, hassas bilgilerinin yapılan saldırılar sonucu ele geçirilmesi sebebiyle itibar kaybına uğraması ve toplum nezdinde internet üzerinde sağlanan finans ve bankacılık işlemlerine yönelik güven kaybı oluşması,
7. Toplumun siber uzaya olan bağımlılığı ve siber güvenlikle ilgili yeterli bilgi düzeyine sahip olamaması gibi etkenlerden dolayı kötücül yazılım, oltama, kimlik hırsızlığı, dolandırıcılık gibi saldırılara maruz kalmaları,
8. Kurum ve kuruluşlarda spam eposta, kötücül yazılım ve türevi saldırılar sebebiyle dolandırıcılığa maruz kalması,
9. Kurum ve kuruluşlarda bireysel hatalar veya doğal afetler sonucunda bilişim sistemleri vasıtasıyla verilen hizmetlerin kesintiye uğraması,

[180] 2016-2019 Ulusal Siber Güvenlik Stratejisi (2016), *a.g.e.* ss.11.12.

2016-2019 döneminde var olan risklerin belirlenmiş ilkeler aracılığıyla minimum düzeye indirilebilmesini hedefleyen stratejik amaçlar şu şekilde belirtilmiştir;[181]

1) Ulusal düzeyde etkili olan kritik altyapıların ve sistemlerinin envanterinin oluşturulması ve varsa güvenlik zafiyetlerinin giderilip, belirli periyotlar çerçevesinde güvenlik seviyelerinin denetimlerinin yapılması,
2) Uluslararası standartlara uygun bir biçimde siber güvenlik alanında denetimini de içerek olan bir mevzuatın oluşturulması,
3) Sektör içerisinde yer alan düzenleyici kurumların siber güvenlik alanında ki düzenleme ve denetleme bilinçlerinin ve kabiliyetlerinin artırılması,
4) Kritik altyapıların ve sistemlerin sadece saldırılara karşı değil, bireysel hatalara ve afetlere de karşı korunmasına yönelik düzenlemelerin yapılması gerekmektedir.
5) Her kurum ve kuruluşun kendi bilgi güvenliğini oluşturabilecek yönetim yapısına ve kabiliyetine ulaşması,
6) Kurumların ve kuruluşların yöneticilerinin siber güvenlik konusunda bilinç düzeyinin artırılması,
7) Siber güvenlik konusunda yetkili personel yetiştirilmesi ve bu alanda çalışmak isteyen araştırmacılara, öğrencilere ve personellere teşvikler verilmesi,
8) Toplumun bütününe yönelik yazılı ve görsel medyada siber güvenlik farkındalığının oluşturulması için çalışmalarda bulunulması,
9) Kamu kurum ve kuruluşlarında siber güvenlik alanında uzman personelin görev alabilmesi için mevzuat desteğinin sağlanması,
10) Siber güvenlik ile ilgili sağlıklı iletişimi sağlayabilecek merkezi bir kamu otoritesinin oluşturulması,
11) Ulusal siber güvenlik ağı içerisinde danışmanlık hizmetlerinin verilmesi,
12) Yazılım ve donanım unsurlarının açıklık analizi ve sertifikasyon faaliyetinin yapılması,

[181] 2016-2019 Ulusal Siber Güvenlik Stratejisi (2016), *a.g.e.* ss.13-14.

13) Siber güvenlik alanında dışa bağımlılığı azaltmak için Ar-Ge çalışmalarına önem verilerek yerli ürünlerin üretilmesi,
14) Tehditlerin saldırıları gerçekleştiremeden yok edilmesi için etkin bir siber savunma yapısının oluşturulması,
15) Siber uzayda ki kimlik belirsizliğini ortadan kaldırmaya yönelik etkin kayıt yönetimi ve Ipv6 teknolojilerinin yaygınlığının artırılması,

Belirtilmiş stratejik hedeflere ulaşmak amacıyla yapılması gereken eylemler beş stratejik eylem başlığı altında raporda toplanmıştır. Beş stratejik eylem planına bakıldığında;[182]

Tablo 11: 2016-2019 Ulusal Siber Güvenlik Stratejik Eylem Planı

2016-2019 Ulusal Siber Güvenlik Stratejik Eylem Planı
1)Siber Savunma Kapasitesinin Güçlendirilmesi, Kritik Altyapıların ve Sistemlerin Korunması: Bu kapsamda devleti, ulusal ekonomiyi, kritik altyapıları ve toplumu etkileyebilecek siber riskleri azaltmaya yönelik çalışmaları içermektedir.
2) Siber suçlarla Etkin Mücadele: Kurum, kuruluşları ve bireyleri etkileyen, genellikle maddi kayba sebep olan siber riskleri azaltmaya yönelik çalışmaları içermektedir.
3) Siber Farkındalık ve Nitelikli İnsan Kaynağının Oluşturulması; Toplumun tamamına siber güvenlik alanıyla ilgili farkındalık kazandırılmasıyla amacıyla çalışmaları içermektedir. Ayrıca nitelikli insan kaynağının oluşturulması hususunda siber güvenlik uzmanlarının yetiştirilmesi amaçlanmaktadır.
4) Siber Güvenlik Ekosisteminin Geliştirilmesi; Ekosistem içerisinde yer alan tüm paydaşlarla koordineli bir şekilde siber güvenlik alanıyla ilgili ihtiyaç ve taleplerin belirlenip, karşılanmasını kapsamaktadır.
5) Siber Güvenliğin Milli Güvenliğin Bir Unsuru Haline Getirilmesi; Milli güvenliği tehdit edebilecek kapsamlı siber saldırıların verebileceği zararı kontrol edilebilir seviyede tutmaya dönük çalışmaları içermektedir. Belirtilmiş stratejik hedeflere ulaşmak amacıyla yapılması gereken eylem planları raporda toplanmıştır.

KAYNAK: T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, *2016-2019 Ulusal Siber Güvenlik Stratejisi (2016), http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf* s.6.(Erişim Tarihi:22.04.2020).

[182] 2016-2019 Ulusal Siber Güvenlik Stratejisi (2016), *a.g.e.* s.15.

2016-2019 Ulusal Siber Güvenlik Strateji Belgesi'nde uygulanacak olan stratejilerin sadece kamuya değil özel sektör kuruluşlarına da görev ve sorumluluklar yüklediği, eğitim ve farkındalık konularında topluma yönelik ayrıca çalışmaların yapılmak istendiği ve tehditlerin saldırıya geçemeden etkin bir siber savunma kabiliyetiyle yok edilmesinin amaçlandığı değerlendirilmektedir. Bu belge ile birlikte Türkiye yapmış olduğu siber güvenlik çalışmalarıyla uluslararası camiada konumunu iyi bir noktaya taşımıştır.

3.3.2020-2023 Ulusal siber güvenlik strateji belgesi

COVID-19 küresel salgınıyla beraber dünyada olduğu gibi Türkiye özelinde de yeni çalışma model ve yöntemlerine geçilmiştir. İnsanların evlerinde bulundukları bu zaman içinde hem iş hem de sosyal faaliyetleri amacıyla siber uzay içerisinde yoğun olarak yer almışlardır. Yeni oluşan bu durum beraberinde güncel risk ve tehditlerin de oluşmasına zemin hazırlamıştır. Türkiye özelinde mevcut olan 2016-2019 Ulusal Siber Güvenlik Strateji Belgesi'nin hem hedeflenen sürecinin son bulması hem de gelişen risk ve tehditlere yönelik güncel bir strateji belgesinin oluşturulması ihtiyacı ortaya çıkmıştır. Tüm bu ihtiyaçlara paralel olarak Türkiye'nin 2023 vizyonu kapsamında "Ulusal Siber Güvenlik Stratejisi 2020-2023" adıyla güncel bir ulusal siber güvenlik strateji belgesi yetkili makamlarca oluşturulmuştur. Bu belgenin içeriğine bakıldığında; koranavirüs salgını içerisinde başta sağlık hizmetleri olmak üzere kritik altyapı ve sistemlere yönelik olarak siber tehditlerin ve saldırıların arttığı rapor edilmiştir.[183] Mevcut ortamın oluşturduğu yeni dijital hayat beraberinde siber uzay içerisinde ki kullanıcılara yönelikte çeşitli çalışmaların yapılması gerektiğini ortaya koymuştur. Güncel risk ve tehdit ortamında ulusal siber güvenliğin sağlanabilmesi için

[183] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı,*2020-2023 Ulusal Siber güvenlik Stratejisi (2020),* s.16*, https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf,* (Erişim Tarihi:07.02.2021)

risklerin düşük düzeyde, yönetilebilir ve kabul edilebilir bir yapıda oluşturulması amaçlanmaktadır.[184]

2020-2023 Ulusal Siber Güvenlik Strateji Belgesi'nin oluşturulma safhalarında geçmiş dönemde ki stratejilerde yer alan ve süreklilik arz eden hususlar gözden geçirilmiş, mevcut bulunan plan ve durumlar incelenip çeşitli iyileştirmeler yapılmıştır. Yapılan durum analizinin sonucu olarak strateji belgesinin oluşturulmasında 8 başlıkta çeşitli hedefler belirlenmiştir.

Tablo 12: 2020-2023 Ulusal Siber Güvenlik Stratejisi Oluşturulurken Belirlenen Ana Hedefler

2020-2023 Ulusal Siber Güvenlik Stratejisi Oluşturulurken Belirlenen Ana Hedefler
1) Kritik altyapıların ve sistemlerin korunması ve dayanıklılık seviyelerinin artırılması,
2) Mevcut ulusal kapasitenin geliştirilmesi
3) Yeni nesil teknolojilerin güvenliği
4) Güçlü bir siber güvenlik ağının oluşturulması
5) Siber suçlarla etkin bir mücadele
6) Yerli teknolojilerin geliştirilmesi ve desteklenmesi
7) Siber güvenliğin milli güvenliğin bir unsuru olduğu vurgusu
8) Uluslararası iş birliğinin artırılması ve geliştirilmesi

KAYNAK: T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı,*2020-2023 Ulusal Siber güvenlik Stratejisi (2020)*, s.16, *https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf*, (Erişim Tarihi:07.02.2021)

Belirlenen bu 8 ana stratejik hedefler kapsamında eylemlerin oluşturulması için ulusal paydaşların katılımlarıyla 19 Şubat 2020 tarihinde bir hazırlık çalıştayı gerçekleştirilmiştir. Yapılan analizler ve gerçekleştirilen hazırlık çalıştayıyla beraber

[184] 2020-2023 Ulusal Siber güvenlik Stratejisi (2020), *a.g.e.*s.17.

8 ana hedef kapsamında 38 adet eylem ve 71 adet uygulama adımı strateji planı içeriğinde yer almıştır.[185] Türkiye'nin 2023 yılı vizyonu kapsamında oluşturulmuş olan 2020-2023 Ulusal Siber güvenlik Strateji Belgesi'nde "Ulusal Siber Güvenlik Hedeflerimiz" başlığı altında 2020-2023 yılları arasında belirlenen hedefler şu şekildedir.

Tablo 13: 2020-2023 Ulusal Siber Güvenlik Strateji Belgesinin Hedefleri

2020-2023 Ulusal Siber Güvenlik Strateji Belgesinin Hedefleri
• Kritik altyapıların ve sistemlerin siber güvenlik unsurlarının 7/24 esasına göre korunması,
• Ulusal düzeyde siber güvenlik alanında ki en son teknolojilere sahip olunması,
• Operasyonal ihtiyaçlar için yerli teknolojik unsurların geliştirilmesi,
• Siber olaylara müdahalede olayın öncesi, olayın gerçekleştiği an ve sonrası olarak bir bütün içerisinde etkin bir siber savunma anlayışının geliştirilmesine devam edilmesi,
• Siber olaylara müdahale ekiplerinin yetkinlik seviyelerinin ölçülmesi ve izlenmesi,
• Siber olaylara müdahale ekiplerinin kabiliyetlerinin artırılması,
• Kurum ve kuruluşların veri paylaşımlarının güvenli bir biçimde sağlanması,
• Kaynağı ve hedefi yurtiçinde bulunan veri trafiğinin yurtiçinde kalması,
• Kritik altyapılarda ve sistemlerde düzenlemeye ve denetlemeye yönelik siber güvenlik anlayışının geliştirilmesi,
• Kritik altyapılarda ve sistemlerde bilgi teknolojileri ürünlerinde üretici bağımlılığının önüne geçilmesi,
• Yerli ürün ve hizmetlere geçilmesi,
• Toplumun tüm kesimi tarafından siber uzayın güvenle kullanılması,
• Kurum ve kuruluşlarda bilgi güvenliği bilincinin artırılması,
• Çocukların siber uzaydaki kötü içerik ve unsurlardan korunması,
• Siber güvenlik alanında uzmanlaşmak isteyen bireyler için projeler üretilip bu alanda ki nitelikli insan kaynağının güçlendirilmesi,
• Siber güvenlik alanında eğitimin ve eğitim içeriklerinin kapasitesinin artırılması,
• Ulusal ya da uluslararası düzeyde ki paydaşlarla bilgi alışverişi ve iş birliğinin artırılması,

[185] 2020-2023 Ulusal Siber güvenlik Stratejisi (2020), a.g.e.s.10.

• Siber suçların minimum seviyede tutulması ve caydırıcılığının artırılması,
• Siber uzayda bilgilerin doğruluğunun ve güncelliğinin sağlanarak spekülatif bilgilerin önüne geçilmesine yönelik mekanizmaların oluşturulması,

KAYNAK: T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı,*2020-2023 Ulusal Siber güvenlik Stratejisi (2020)*, s.16, *https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf,* (Erişim Tarihi:07.02.2021)

Daha önce ki strateji belgelerine kıyasla 2020-2023 Ulusal Siber Güvenlik Strateji Belgesi'nde siber uzayda işlenen çocuk istismarı suçu ve çocukların siber uzayda korunmasıyla ilgili olarak ayrı bir başlık altında önemli bir vurgu yapılmıştır.[186] Ayrıca belge içerisinde etkili bir siber güvenlik ağ yapısının oluşturulabilmesi için tüm paydaşların iş birliğinde organik bir yapı içerisinde siber güvenlik ekosisteminin yaratılması amaçlanmaktadır.[187] Türkiye nezdinde siber güvenlik kavramı milli güvenliğin tesisinde son derece önemli olup, bu önemini ise her geçen gün süratle artırmaktadır. Türkiye'nin 2023 yılı vizyonu kapsamında siber uzay içerisinde önemli bir aktör olmak ve siber savunma kabiliyetleri bakımından caydırıcı bir güç olarak siber uzay içerisinde yer alma amacı mevcuttur.

3.4. Türkiye'de ki kurum ve kuruluşların siber güvenlik alanındaki faaliyetleri

3.4.1.Bilgi Teknolojileri ve İletişim Kurumu

2000 yılında Telekomünikasyon Kurumu adıyla kurulup, 2008 yılında "5809 sayılı Elektronik Haberleşme Kanunu" çerçevesinde "Bilgi Teknolojileri ve İletişim Kurumu (BTK)" adıyla kurum yeniden yapılandırılmıştır. Ulaştırma ve Altyapı bakanlığınca belirlenen politikalar aracılığıyla telekomünikasyon sektörünü

[186] 2020-2023 Ulusal Siber güvenlik Stratejisi (2020), *a.g.e*.s.28.
[187] 2020-2023 Ulusal Siber güvenlik Stratejisi (2020), *a.g.e*.s.29.

düzenleyen ve denetleyen bir kurumdur. Kurum ayrıca bilgi teknolojilerinden yükümlü kamu otoritesidir[188]. Kurum bu görevini Telekomünikasyon İletişim Başkanlığı (TİB) aracılığıyla yürütmektedir. 2005 yılında kurulmuş olan Telekomünikasyon İletişim Başkanlığı direkt olarak Bilgi Teknolojileri ve İletişim Kurumu Başkanına rapor vermesinin yanı sıra Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Milli İstihbarat Teşkilatından birer temsilci bulundurmaktadır.[189]

BTK'ya 06 Şubat 2014 tarihinde Resmî Gazete 'de yayımlanan "6518 sayılı kanunla mevcut elektronik haberleşme kanununa eklenen bazı maddelerle siber güvenlikle ile yeni görevler verilmiştir. Bu görevler içerisinde bilginin ve haberleşmenin güvenliğinin sağlanması, yetkisiz erişime karşı şebeke güvenliğinin artırılması, elektronik haberleşmenin milli güvenliğin bir unsuru olduğu ve bu yönde mevzuatın belirttiği tedbirlerin alınması, Bakanlar Kurulu, Bakanlık ve Siber Güvenlik Kurulu tarafından siber güvenlik ile ilgili görevleri Telekomünikasyon İletişim Başkanlığı ve diğer alt birimleri aracılığıyla yürütmesi belirtilmiştir.[190] Telekomünikasyon İletişim Başkanlığı telekomünikasyon sistemleri aracılığıyla yapılan iletişimin ve sinyalin takibi, değerlendirilmesi, gözetlenmesi ve kayıt edilmesinden sorumludur. Ulusal siber güvenlik ağı içerisinde TİB kurum ve kuruluşlar arasındaki siber saldırıların tespiti ve engellenmesi için koordinasyon sağlamaktadır.[191]

---

[188] Bilgi Teknolojileri ve İletişim Kurumu, *Mevzuat, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2813&MevzuatTur=1&MevzuatTertip=5.,* (Erişim Tarihi:6.07.2021)

[189] Salih Bıçakçı, Doruk Ergun, Mitat Çelikpala., *a.g.e.* s.33

[190] Bilgi Teknolojileri ve İletişim Kurumu, *Mevzuat.*

[191] Salih Bıçakçı, Doruk Ergun, Mitat Çelikpala, *a.g.e.* s.33

3.4.2. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) ulusal siber güvenliğin tesisi için ilk çalışmalarına 1997 yılında Ağ Güvenliği Grubu ismiyle kurduğu birim vasıtasıyla başlamıştır. Bu birimde açık kaynak kodlu işletim sistemleri, veritabanları ve sunuculara yönelik güvenlik açıklıklarının tespitiyle beraber sızma testleri üzerine çalışmalarda bulunulmuştur. Kurum ilerleyen zamanlarda bu konularda ki uzmanlığını artırarak dünyada ki sayılı test merkezlerinden biri olmuştur.[192] Kurum içerisinde kriptolu haberleşme cihazlarının güvenlik testleri, akıllı kart teknolojilerinin güvenlik testleri, tersine mühendislik ve yan kanal analizi gibi testler gerçekleştirilmektedir. TÜBİTAK, Ağ Güvenliği Grubuyla beraber Türk Silahlı Kuvvetleri'nin siber güvenlik alanında ki ihtiyaçlarının karşılanmasının yanı sıra grup Türk Silahlı Kuvvetleri iş birliği ile NATO tatbikatında da yer almıştır.[193]

2012 yılına gelindiğinde TÜBİTAK BİLGEM bünyesinde, Yazılım Teknolojileri Araştırma Enstitüsü (YTE), Siber Güvenlik Enstitüsü (SGE) ve İleri Teknoloji Araştırma Enstitüsü (İLTAREN) kurulmuştur. TÜBİTAK 2012 yılıyla beraber siber güvenlikle ilgili sorumlu olduğu tüm yetkisini 2012/3842 sayılı Bakanlar Kurulu Kararı ile Ulaştırma ve Altyapı Bakanlığına devretmiştir. Ayrıca TÜBİTAK bakanlıkla beraber Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve yurt içerisinde ki ağ trafiğini toplayıp analiz eden Bal Küpü sisteminin işletmesini gerçekleştirmektedir.[194]

---

[192] Salih Bıçakçı, Doruk Ergun, Mitat Çelikpala, *a.g.e.* s.34
[193] TÜBİTAK, *Tarihçe Siber Güvenlik Enstitüsü, https://sge.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce.,* (Erişim Tarihi: 06.07.2021)
[194] Salih Bıçakçı, Doruk Ergun, Mitat Çelikpala, *a.g.e.* s.35

3.4.3 Emniyet Genel Müdürlüğü

Emniyet Genel Müdürlüğü bünyesinde ilk olarak "Bilgisayar Suçları ve Bilgi Güvenliği Kurulu" 1998 yılında kurulmuştur. Kurulan bu kurul bilişim suçlarının belirlenmesi, ulusal ve uluslararası yapıların incelenmesi, bilişim araçlarıyla işlenen suçların belirlenmesi gibi konularda çalışmalarda bulunmuştur.[195] Yapılan bu çalışmalar neticesinde 1999 yılında "Bilgi Suçları Çalışma Grubu" kurulmuştur. 2013 yılında Emniyet Genel Müdürlüğü bünyesinde siber suçlarla etkin bir şekilde mücadele edilmesi amacıyla "Siber Suçlarla Mücadele Daire Başkanlığı" kurulmuştur. Kurulan başkanlığın görevleri arasında siber suçlarla mücadele, siber suçlarla ilgili olarak toplumun bilinç düzeyinin artırılması, siber suçlarla mücadelede uluslararası iş birliğinin artırılması, siber suçlar alanında uzman personel yetiştirilmesi gibi görevleri bulunmaktadır.[196]

3.4.4. Millî İstihbarat Teşkilâtı

Millî İstihbarat Teşkilâtı (MİT) Türkiye'ye yönelik siber güvenlik tehditlerinin eyleme geçmeden yok edilmesi için gerekli olan istihbarati bilgiyi toplamakla yükümlü olan kurumlardan biridir. MİT'e bu yetki 26 Nisan 2014 tarihinde yürürlülüğe giren yasa ile verilmiştir. Bu yasa ile MİT'in görevi şu şekilde tanımlanmaktadır.[197]

> *"Dış istihbarat, milli savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri*

---

[195] Salih Bıçakçı, Doruk Ergun, Mitat Çelikpala, a.g.e. s.46

[196] Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı, *Hakkımızda, https://www.egm.gov.tr/siber/hakkimizda2*., (Erişim Tarihi: 27.07.2021)

[197] T.C. Resmi Gazate, Devlet İstihbarat Hizmetleri ve Milli istihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun, Karar Numarası:6532, 17 Nisan 2014, *https://www.resmigazete.gov.tr/eskiler/2014/04/20140426-1.htm.,* (Erişim Tarihi: 27.07.2021)

toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak"

3.4.5. Türk Silahlı Kuvvetleri

Türkiye'de siber tehdit kavramı özellikle Estonya ve Gürcistan'da yaşanan siber saldırıların ardından siber tehditler milli güvenliği tehdit eden kritik unsurlar olarak tanımlanmıştır. Gerek NATO nezdinde yapılan çalışmalar gerekse de Türkiye'de yapılan çalışmalar Türk Silahlı Kuvvetleri bünyesinde bir siber savunma komutanlığının oluşturulmasını gündeme getirmiştir. Kurulması planlanan bu komutanlık Türkiye'yi siber saldırılara karşı korumayı amaçlamıştır. Komutanlık, Millî Savunma Bakanlığı, TÜBİTAK ve Orta Doğu Teknik Üniversitesi iş birlikteliğinde Genelkurmay Başkanlığı yapısı içinde görev yapacak bir biçimde tasarlanmıştır. Fakat ilerleyen yıllarda Siber Güvenlik Kurulu'nun kurulmasıyla komutanlık yapısı yerini Siber Savunma Merkezi Başkanlığı olarak revize etmiştir.[198] Bu yapılanma Türkiye'nin siber savunma ihtiyacını karşılamak yerine Türk Silahlı Kuvvetleri'nin siber güvenlik ihtiyaçlarının karşılanması hususunda görev almıştır. 2013 yılıyla beraber Ulusal Siber Güvenlik Strateji Belgesi'nin ilan edilmesine müteakip Türk Silahlı Kuvvetleri Siber Savunma Komutanlığının kuruluşunu duyurmuştur. Bu komutanlığın görevleri şu şekilde belirtilmiştir;[199]

1) Türk Silahlı Kuvvetleri'nin siber uzay içerisindeki tüm sistemlerinin siber güvenliğinin sağlanması,
2) Siber saldırı ve tehditlerle 7/24 esasına göre mücadele edilmesi,
3) NATO kapsamında gerçekleştirilen siber tatbikatlara katılmak,
4) Türk Silahlı Kuvvetleri bünyesinde siber farkındalık ve eğitim çalışmalarını yürütmek,
5) Türk Silahlı Kuvvetleri bünyesindeki ağlara ve sistemlere düzenli aralıklarla siber güvenlik denetimleri ve testleri yapmaktır.

---

[198] Salih Bıçakçı, Doruk Ergun, Mitat Çelikpala, *a.g.e.,* s.44
[199] *A.g.e.,* s.45

3.4.6. Ulusal Siber Olaylara Müdahale Merkezi

Ulusal Siber Olaylara Müdahale Merkezi (USOM) 2013-2014 Ulusal Siber Güvenlik Strateji Planı çerçevesinde 2014 yılında kurulmuştur. Telekomünikasyon İletişim Başkanlığı denetimi altında olan USOM Türkiye'ye yönelik siber tehdit ve saldırılara karşı 7/24 görev esasına göre çalışmaktadır. Strateji belgesine göre USOM koordinatörlüğünde kritik altyapı sistemlerine sahip sektörlerde Siber Olaylara Müdahale Ekipleri (SOME)'nin kurulması öngörülmüştür.[200] Kurulan somelerin her türlü yasadışı faaliyete gerekli kamu kurumuna ve USOM'a iletmesi gerekmektedir. Someler kuruldukları kurum ve kuruluşun siber saldırılara karşı güvenlik tedbirlerini almak, olaylara müdahale etmek ve olayları kayıt altına almakla sorumludur. USOM, Somelerle koordineli bir şekilde çalışarak büyük çaplı siber saldırılara karşı koymak için çalışmaktadır. Ayrıca usomlar, sektörel somelere eğitim verme, somelerin saldırılara karşı koyamadıklarında onlara destek olma ve uluslararası kendine denk kuruluşlarla iş birliği kurma görevlerini yürütmektedir.[201]

3.4.7. Siber Güvenlik Kurulu

2012 yılında 3843 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" ile kurulmuş bir kuruldur. Bu karar şu şekildedir;[202]

> "*Siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla: Ulaştırma ve Altyapı Bakanının başkanlığında*

[200] Ulusal Siber Olaylara Müdahale Merkezi, USOM, *USOM Hakkında*, *https://www.usomgov.tr/hakkimizda.html* (Erişim Tarihi: 22.04.2020)
[201] Bilgi Teknolojileri ve İletişim Kurumu, *USOM-SOME, https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi*., (Erişim Tarihi: 14.07.2021)
[202] Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar (2012),

Dışişleri, İçişleri, Milli Savunma , Ulaştırma ve Altyapı Bakanlıkları müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı MEBS Başkanı, BTK Başkanı, TÜBİTAK Başkanı, MASAK Başkanı, TİB Başkanı ile UAB Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşan Siber Güvenlik Kurulu Kurulmuştur."

Siber Güvenlik Kurulu'nun faaliyet alanı; siber güvenlikle ilgili politika, strateji ve eylem planlarını onaylamak, kritik altyapıların ve sistemlerinin belirlenmesiyle alakalı konuları karara bağlamak ve kanun tarafından verilen sorumluluklarını yerine getirmek şeklinde belirtilmektedir.[203]

3.4.8. Afet ve Acil Durum Yönetim Başkanlığı (AFAD)

5902 sayılı kanun ile beraber T.C. İçişleri Bakanlığı Afet ve Acil Durum Yönetimi Başkanlığı (AFAD) Türkiye'de siber kriz yönetimi ve kritik altyapıların korunmasıyla alakalı çalışmalardan sorumlu kurum olmuştur. AFAD'ın görev tanımı kanunda hem afet esnasında hem de afetlerden sonra ki durumda afetler ile mücadele eden kurum ve kuruluşlar arasındaki koordinasyonu sağlamak ve bu yapıyı düzenleyecek politika ve stratejileri geliştirmek olarak tanımlamaktadır. AFAD bu perspektifte bir strateji planı hazırlarken afetleri doğal afetler ve teknolojik afetler olarak iki gruba ayırmıştır. Kritik altyapıların ve sistemlerin korunması ile siber güvenlik konuları teknolojik afetler sınıflandırmasında yer almaktadır.[204]

[203] Bilgi Teknolojileri ve İletişim Kurumu, *Siber Güvenlik Kurulu, https://www.btk.gov.tr/siber-guvenlik-kurulu.*, (Erişim Tarihi: 26.07.2021)
[204] Salih Bıçakçı, Doruk Ergun, Mitat Çelikpala, *a.g.e.*, s.43

AFAD 2014 yılında "2014-2023 Kritik Altyapıların Korunması Stratejisi'ni yayınlamıştır. Bu stratejide ihtiyaçlar ve yapılması gereken eylemler belirlenmiştir. Belirtilen ihtiyaçlar şu şekildedir;[205]

- Yetkili mercilerin belirlenmesi,
- Yetkili koordinasyon otoritesinin belirlenip, kritik altyapıların ve sistemlerin tespit edilmesi,
- Avrupa Birliği Direktiflerine uygun taslak ve yönetmeliklerin hazırlanması,
- Kritik altyapıların ve sistemlerin korunmasında ulusal düzeyde koordinasyon ve iş birliğinin sağlanması,
- Çeşitli eğitim programlarının oluşturulması ve uygulanması,
- Ulusal düzeydeki kritik altyapıların ve sistemlerin korunması amacıyla koruma planı hazırlanması,
- Sistemlerin Avrupa Birliği Kritik Altyapı Uyarı Bilgi Ağı (KAUBA)'na entegre edilmesi,
- Yapılan çalışmaların raporlanması,

AFAD tarafından belirtilen bu strateji belgesinde AFAD'ın siber güvenlik krizini nasıl yöneteceğiyle ilgili herhangi bir bilgiye rastlanamamıştır.

3.5. Türkiye'de faaliyet gösteren hacker gruplarının incelenmesi

Türkiye kökenli hacker grupları küresel çapta gerçekleştirilen siber saldırılarda etkin bir biçimde yer almaktadır. Türk hackerların yeteneklerinin çözümlenebilmesi ülke içerisinden gelebilecek potansiyel tehditlerin saptanmasında önemlidir. Devletler özellikle kritik altyapı sistemlerinde geleneksel internet bağlantılarını değiştirerek, yerel ve az cihazın bağlı olduğu hatlar kullanmaya doğru gitmektedir.

[205] T.C. İçişleri Bakanlığı Afet ve Acil Durum Yönetimi Başkanlığı, *2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi*, Eylül 2014, *https://www.afad.gov.tr/kurumlar/afad.gov.tr/2535/files/123-20141010111330-kritikaltyapi-son.pdf.*, (Erişim Tarihi: 02.08.2011)

Türkiye'de faaliyet gösteren hackerların profiline bakıldığında;[206]

- Türkiye'de ki hackerların yaşları 14 ve 45 yaş aralığında olmakla birlikte genel ağırlık olarak 18-25 yaş aralığında olmaktadır.
- Hackerlar üniversitelerin bilgi ve iletişim teknolojileriyle alakalı bölümlerinden mezun olmasalar da genellikle lise veya üniversitelerin farklı bölümlerinden mezunlardır.
- Hackerlığa yeni giriş yapanlar yeteneklerini hacker forumlarından elde ederek ve genellikle basit hack araçları kullanarak geliştirirler.
- Hackerların %90'lık kısmı erkek iken %10'luk kısmı kadınlardan oluşmaktadır.
- Genellikle ailelerinin gelir seviyeleri orta ve düşük gelir seviyesinde oluşmaktadır.
- Ters mühendislik ve sosyal mühendislik saldırılarında etkindirler.
- Hackerların ağırlıklı yaşadıkları bölge genellikle Marmara bölgesidir.

Türkiye'de internetin vatandaşların hizmetine sunulmasıyla birlikte belirli fikir ve düşünceler doğrultusunda çeşitli hacker grupları ortaya çıkmıştır. Bu kısımda öne çıkan yedi hacker grubu incelenecektir. Bunlar; Ayyıldız Team, Turk Hack Team, Redhack, B3yaz Hacker, Cyber Warrior (Akıncılar) ve Türk Güvenliği.

3.5.1. Ayyıldız Team

İnternet sitelerinde ki verilere göre Ayyıldız Team 2002 yılında kurulmuştur. Amaçlarının Türkiye'ye yönelik internetten yapılabilecek siber saldırılara karşı gönüllülük esası çerçevesinde karşı koymaya yönelik bir organizasyondur. Türkiye

[206] Salih Bıçakçı, Doruk Ergun, Mitat Çelikpala, *a.g.e.*, s.51

Cumhuriyeti devletine, devlet adamlarına, manevi değerlere ve ülkenin bütünlüğüne yönelik siber uzaydan gelebilecek saldırılara karşı tesis edilmişlerdir.[207]

Ayyıldız Team'in hedeflerine bakıldığında;[208]

- Türkiye Cumhuriyeti'ne yönelik siber saldırılarla mücadele etmek.
- Türkiye aleyhine ve düzeni bozucu her türlü yayın yapan sitelerin ve sistemlerim yayın faaliyetlerine son vermek.
- Türkiye Cumhuriyeti'nin faydasına yönelik faaliyetlerini sürdüren sitelere ve sistemlere teknik destek sağlamak.
- Türkiye Cumhuriyeti'ni temsil eden gov.tr, pol.tr, edu.tr, bel.tr uzantılı internet sitelerini korumak.
- Propaganda faaliyetleri aracılığıyla Türkiye Cumhuriyeti'ni dünya milletleri arasında prestijli bir konuma getirmek.
- Gerektiğinde yönetim kurulu kararıyla Türkiye'ye yönelik sözlü, yazılı ve fiili saldırılara karşı cevap vermek.
- Kamuoyunun bilgilendirilmesi amacıyla information admin eliyle yazılı açıklamalarda bulunmak.

Ayyıldız Team'in hack faaliyetlerine yönelik Zone-H sitesinde 13.579 bildirim mevcuttur.[209] Ayyıldız Team ağırlıklı olarak devlet hedeflerine paralel hareket eden kendi ifadesiyle devletçi bir hacker grubudur.[210] Ayyıldız Team yaptığı saldırılarda Türkiye Cumhuriyeti'ni korumaya yönelik saldırılar yapmaktadır. Bunun yanında Türkiye'ye yönelik gerçekleştirilen siber saldırılarda gönüllü

[207] Ayyıldız Team, Tarihimiz, *https://www.ayyildiz.org/ayyildiz-tim-tarihi.html*., (Erişim Tarihi: 5.08.2021.)
[208] Ayyıldız Team, Vizyon-Misyon, *https://www.ayyildiz.org/misyon-vizyon.html*., (Erişim Tarihi: 5.08.2021.)

[209] Ayyıldız Team, Zone-H, *http://www.zone-h.org/archive/notifier=Ayy%25C4%25B1ld%25C4%25B1z%2520Tim.*, (Erişim Tarihi:26.08.2021)
[210] Salih Bıçakçı, Doruk Ergun, Mitat Çelikpala, *a.g.e.*, s.52.

olarak karşı saldırılar yapıp düşmanı yıldırmaya ya da hedefini gerçekleştirmemeye yönelik olarak çalışmaktadır.[211]

3.5.2. Turk Hack Team

Turk Hack Team en eski ve en kapsamlı hacker gruplarından biridir. 2002 yılında kurulmuş bir oluşumdur. "Arsenik" rumuzlu hacker tarafından kurulduğu bilinmektedir. Turk Hack Team internet siteleri aracılığıyla hackerlığa merakı olanları eğitmeyi amaçlamaktadır. Milliyetçi çizgilerini korumalarının yanında dini unsurlara da yer vermektedirler. Grubun üyeleri kendilerini "Vatanını Seven Müslümanlar" olarak tanımlamaktadır. Ulusal çıkarlar doğrultusunda hareket edip, Türk ulusunun siber güvenlik alanında yeterli yeteneklere kavuşabilmesi amacıyla çalıştıklarını söylemektedirler.[212]

Grubun kendi internet sitelerinde açıkladıkları hedefleri şu şekildedir;[213]

1) *Turk Hack Team ulusal çıkarlar doğrultusunda çalışmaktadır.*
2) *Turk Hack team bireylere milliyetçiliği ve vatan sevgisini aşılamaya çalışmaktadır.*
3) *Türk ulusunun siber güvenlik alanında yeterli kabiliyete ve beceriye kavuşabilmesi amacıyla çalışır.*
4) *Hack'in zevk için değil misyon için yapılmalıdır.*
5) *Toplum yararına yayın yapan siteler yardımcı olup, onların çıkarlarını göz etmektedir.*
6) *Türk diline, İslam dinine, ülkemize, örf ve adetlerimize karşı yayın yapan internet sitelerinin yayın hayatına son vermek."*

---

[211] Gamze Akkuş, *Anonymous Resmi Hedefe Saldırdı, Ayyıldız Team Karşı Atakla Cevap Verdi*, Hürriyet, 10 Haziran 2011, *https://www.hurriyet.com.tr/ekonomi/anonymous-resmi-hedef-e-saldirdi-ayyildiz-tim-karsi-atakla-yanit-verdi-17996737.*, (Erişim Tarihi: 26.08.2021)

[212] Turk Hack Team, *https://www.linkedin.com/company/turkhackteam/?originalSubdomain=tr.*, (Erişim Tarihi: 6.08.2021.)

[213] Turk Hack Team, *Misyon*, *https://www.turkhackteam.org/misyon.html.*, (Erişim Tarihi: 6.08.2021)

Turk Hack Team'in çok büyük bir botnet ağını kontrol ettiği düşünülmektedir. Zone-H sitesinde Turk Hack Team'in farklı yazımlarla birçok kaydı bulunmaktadır.[214] Bu farklılıklar grubun yeteneklerini anlamayı zorlaştırmaktadır.[215]

3.5.3. RedHack

Redhack 1997 yılında "Halk için Hack" sloganıyla kurulmuş bir hacker grubudur. Redhack ideolojisini eşit, adil ve emek sömürüsünün bulunmadığı bir dünya biçiminde tanımlamaktadır. Kendilerini kızıl hackerlar olarak tanımlayıp, Marksist ideolojiyi benimsediklerini bildirmektedirler. Zone-H kayıtlarına göre 2008 yılından itibaren Redhack'in yapmış olduğu siber saldırılar bulunmaktadır.[216] Hacker grubu kendini duyurmaya Ankara Emniyet Müdürlüğüne yaptıkları siber saldırıyla ve gizli belgeleri yayınlamakla başlamıştır. 2013 yılıyla beraber Gezi Parkı olaylarında da yaptığı şiddetli saldırılarla da popülerliğini artırmıştır. Çeşitli devlet kurumlarında ki görevlilerin kişisel bilgilerini yayınlamıştır. 2013 yılında Redhack'e yönelik yapılan operasyonlarda çeşitli tutuklamalar yapılmış fakat delil yetersizliği sebebiyle serbest bırakılmışlardır.[217]

Redhack'in uluslararası hacker gruplarıyla iş birliği yaptığı bilinmektedir. Bu iş birliklerinden biri 2013 yılında Anonymous ile beraber İsrail İstihbarat Servisi'ne bir siber saldırı düzenlenmişlerdir.[218]

---

[214] Turk Hack Team, Zone-H, *http://www.zone-h.org/archive/notifier=turkhackteam/page=3.,* (Erişim Tarihi: 11.09.2021)
[215] Salih Bıçakçı, Doruk Ergun, Mitat Çelikpala, *a.g.e.,* s.55
[216] RedHack, Zone-H, *http://www.zone-h.org/archive/notifier=RedHack.,* (Erişim Tarihi:06.08.2021).
[217] Salih Bıçakçı, Doruk Ergun, Mitat Çelikpala, *a.g.e.,* s.53
[218] Yiğit Turak, RedHack Özelinde Siber Olaylar ve Siber Suçlar, İstanbul Bilgi Üniversitesi 2014, *http://www.yigitturak.com/wp-content/uploads/RedHackIncelemesi.pdf.,* (Erişim Tarihi: 22.08.2021).

3.5.4. B3yaz Hacker

Bu hacker grubunun etkinlikleriyle ilgili olarak çok fazla bir bilgi bulunmamaktadır. Grup isimlerini beyaz hackerların farklı bir yazılış şekliyle belirterek üreticilere güvenlik açıklarını bildiren zararsız hacker grubu olduğunu belirtmektedir. Grup şirketlere sızma testi hizmetleri sunma yoluyla hackleme yapmaktadır. Firmalar bu testlerin güvene dayalı biçimde yapılmasını istedikleri için genelde hacker gruplarını tercih etmezler. Grubun amaçlarına bakıldığında ilk olarak yaptıkları saldırılarla internet sitelerinin güvenlik seviyelerini test etmek ikinci olarak ise grubun değer yargılarına ters düşen içeriklere yönelik internet sitelerine saldırmayı içermektedir.[219] Zone-H kayıtlarına göre bu isim ve bu ismin çeşitli varyasyonlarında 540 adet saldırı kaydedilmiştir.[220]

3.5.5. Cyber Warrior (Akıncılar)

Cyber Warrior hacker grubu 1999 yılında illegal port adıyla kurulmuştur. Daha sonra Cyber Warrior ismiyle yeniden teşkilatlanma sürecine girmiştir. İhtiyaç duyduğunda gönüllü toplama çağrılarında bulunmaktadır.[221]

Grubun gönüllülerinde aradığı özellikleri şu şekildedir;[222]

> *"1) Din, örf, adet ve ananelerimize sadık,*
>
> *2) Türk milliyetçileri*

[219] Salih Bıçakçı, Doruk Ergun, Mitat Çelikpala, a.g.e., s.54
[220] B3yaz Hacker, Zone-H, *http://www.zone-h.org/archive/ip=123.30.191.186.*, (Erişim Tarihi: 22.08.2021.)
[221] Cyber Warrrior (Akıncılar), Sitemizin Çizgisi, *https://www.cyber-warrior.org/.*, (Erişim Tarihi: 15.08.2021)
[222] Cyber Warrrior (Akıncılar), Neler Yaptık? *https://www.cyber-warrior.org/.*, (Erişim Tarihi:15.08.2021.)

3) Üyeler arasında bir kardeşlik bağı sağlayacak kişiler,

4) Üyeler Arasında başka bir üyeye küfür, argo söz, ağır laf etmeyecektir."

Cyber Warrior grubu kendi internet sitelerinde 2007 yılında yürürlüğe giren bilişim suçları yasasının ortaya çıkması hususunda yer aldıklarını ifade etmektedir. Buda hacker grubunun Türk karar mercilerine yakın bir durumda olduğunu göstermektedir.[223]

Cyber Warrior'un başlıca görevleri şu şekilde sıralanmıştır;[224]

1) İnançlarımıza ve ahlaki değerlerimize yönelik saldırı yapan ve satanist, pornografik içeriklere sahip internet siteleriyle mücadelemiz esastır.
2) Türk karşıtlığı yayınlar ve toplum vicdanını derinden etkileyen durumlarla mücadele esastır.
3) Politikalarımıza uygun yayınlar gerçekleştiren kurum, site, grup ya da oluşumlara güvenlik ve diğer alanlarda teknik destek vermek.
4) Bizim değerlerimize saldırmadığı sürece hiçbir yayın mücadelemizin kapsamına girmez.

Cyber Warrior grubu Türkiye'de faaliyet gösteren hiçbir siteye saldırmadıklarını belirtmiştir. Grubun Türk polisiyle farklı seviyelerde bağlantıları bulunduğu iddia edilmektedir.[225] Zone-H sitesine göre 7895 saldırısı bulunmaktadır. Grubun mensuplarının çeşitli ülkelere yaptıkları saldırıların yanı sıra saldırılarını İsrail, Mısır, Avusturya ve Ermenistan üzerinde yoğunlaştırmışlardır.[226]

---

[223] Cyber Warrrior (Akıncılar), Sitemizin Çizgisi, *https://www.cyber-warrior.org/.*, (Erişim Tarihi:15.08.2021.)

[224] Cyber Warrrior (Akıncılar), Neler Yaptık? *https://www.cyber-warrior.org/.*, (Erişim Tarihi:15.08.2021.)

[225] Salih Bıçakçı, Doruk Ergun, Mitat Çelikpala, *a.g.e.*, s.56

[226] Cyber Warrior, Zone-H, *http://www.zone-h.org/archive/notifier=Cyber-Warrior.*, (Erişim Tarihi: 19.09.2021.)

Erişilebilen kayıtların çoğunda grubun devletle güçlü ilişkiler kurduğu ve devletin amacına yönelik hizmetlerde bulunduğu görülmektedir. Buda hacker grubunu devlet destekli bir grup olduğu iddiasını oluşturmaktadır.[227]

3.5.6. Türk Güvenliği

Türk Güvenliği hacker grubu "Agd_Scorp" kullanıcı adlı hacker tarafından 2006 yılında kurulmuştur. Bu hacker grubu adını fuse.microsoft.com, The Register ve Vodafone'a yapılan saldırılar neticesinde uluslararası mecrada duyurmuştur. Türk Güvenliği grubunun faal bir internet sitesinin olmaması yanında kurucusu Agd_Scorp'un açıklamalarıyla hedef ve amaçları şekillenmiş bir gruptur. Fakat net bir ideolojisi bulunmamaktadır.[228] Zone-H kayıtlarında Türk Güvenliği adına 225 kayıt, Agd_Scrop adına ise 424 kayıt bulunmaktadır. Grubun yaptığı saldırılar ağırlıklı olarak SQL enjeksiyonu saldırılarını içermektedir.[229] Türk Güvenliği özellikle Suriye Elektronik Ordusu (SEA) Türkiye'ye yönelik yaptığı saldırılara çok yoğun karşılık vermiştir ve SEA'nın sitesini hacklemiştir. Türk Güvenliği grubunun SEA'nın sitesine bıraktığı mesajlar grubun milliyetçi eğilimde bir grup olduğunu göstermektedir.[230]

3.6. Türkiye'ye yönelik yapılan siber saldırı örnekleri

Bilgi ve iletişim teknolojileri günümüzde toplumların ve ekonomilerin ayrılmaz bir parçası haline gelmiştir. Ülkelerin kalkınmalarında önemli bir unsur olan bu

[227] Salih Bıçakçı, Doruk Ergun, Mitat Çelikpala, *a.g.e.,* s.56
[228] Türk Güvenliği, *https://twitter.com/turkguvenligi.,* (Erişim Tarihi:26.08.2021)
[229] Türk Güvenliği, Zone-H, *http://www.zone-h.org/archive/notifier=turkguvenligi.info.,* (Erişim Tarihi: 26.08.2021)
[230] Salih Bıçakçı, Doruk Ergun, Mitat Çelikpala, *a.g.e.,* s.58

teknolojiler, kamu kurumlarından, özel sektöre kadar tüm hizmet türlerinde kullanımı ve bu sistemlere olan bağımlılığı giderek artmaktadır. Bu kullanım ile gelişen bağımlılık sürecinde bu teknolojilerde ki güvenlik unsurunu ön plana çıkararak toplumların ulusal güvenlik meselelerinden biri haline getirmiştir. Bu teknolojilerde yaşanabilecek bir güvenlik zafiyeti kamu düzenini ciddi bir biçimde etkileyecektir. Türkiye açısından duruma bakıldığında ise nüfusunun çoğunluğu interneti etkin bir biçimde kullandığı bir ülke olduğu için yararlarının yanında siber uzayda birçok güvenlik zafiyeti gerçekleşmektedir. Türkiye dünyada siber saldırıya en çok maruz kalan ülkeler arasında yer almaktadır. Bu bölümde Türkiye'ye yönelik yapılan siber saldırı örnekleri ve alınan önlemler değerlendirilecektir.

3.6.1. Anonymous grubunun Türkiye'ye yönelik tehditleri

Uluslararası bir hacker grubu olan Anonymous tarafından 6 Haziran 2011'de kendi internet siteleri ve Youtube yüklenen bir video aracılığıyla Türkiye'yi açık bir şekilde siber saldırıyla tehdit etmiştir. "Operation Turkey" adıyla başlatacakları saldırının amacının Türkiye'de internet kullanımına yönelik uygulanan sansüre karşı bir tepki koymak ve Türk hükümetini bu işlemden vazgeçirme isteği olduğunu bildirmişlerdir. Grup saldırıya katılacak gönüllülerin kimliklerinin ifşa olmaması için teknik kılavuzlar yayımlamıştır. Ayrıca saldırıyı oluşturacak sistemin Türkçe sürümü ve Türkçe yönlendirmeleri de içeren bir versiyonu yapılmıştır. Saldırı yönteminin DDos (Dağıtık Servis Dışı Bırakma) olacağı ve binlerce bilgisayarla eşgüdümlü bir şekilde yapılacağı grubun sosyal medya hesaplarından duyurulmuştur.[231]

[231] CHIP Online, Türkiye Operasyonu Başlıyor! 9 Haziran 2011, *https://www.chip.com.tr/haber/turkiye-operasyonu-basliyor_27402.html.,* (Erişim Tarihi: 28.09.2021)

9 Haziran 2011'de Bilgi Teknolojileri ve İletişim Kurumu (BTK) ve Telekomünikasyon İletişim Başkanlığı (TİB) internet sitelerine yönelik yoğun bir siber saldırı başlatılmıştır. 5 dakikalık bir erişim sorunu harici kurumların internet sitelerinde herhangi bir sorun olmadığı duyurulmuştur. Saldırının etkisiz olmasının en büyük sebebi saldırının önceden bildirilmesi ve kurumların bu yönde yaptığı yoğun hazırlıklar olmuştur.[232]

3.6.2. Rus uçağının düşürülmesi sonucu yaşanan siber saldırılar

24 Kasım 2015 tarihinde Suriye rejiminin kontrolü altındaki bölgeden havalanan Su-24 tipi bir Rus savaş uçağının Türk hava sahasını ihlal etmesi ve yapılan uyarılara rağmen bu ihlaline devam etmesi sonucu değişen angajman kuralları çerçevesinde Türk Hava Kuvvetleri tarafından Rus savaş uçağı düşürülmüştür. Rus savaş uçağının düşürülmesinin ardından gerginleşen Türkiye- Rusya ilişkilerinden sonra Türkiye'ye yönelik olarak çok yoğun siber saldırılar başlatılmıştır.[233]

Türkiye'de ki "tr." Uzantılı internet adreslerine yönelik olarak çok yoğun siber saldırılar gerçekleştirilmiştir. 14-24 Aralık 2015 tarihleri arasında gerçekleştirilen saldırılar kapsamında .tr uzantılı sitelere erişim sağlanamamıştır.[234] Saldırıların kapsamı veri hırsızlığı olmayıp, DDos (Dağıtık Servis Dışı Bırakma) saldırıları biçiminde gerçekleştirilmiştir. ".tr" alan adlarının sunucularının yönetiminden sorumlu olan Orta Doğu Teknik Üniversitesi (ODTÜ) yaptığı açıklamada saldırının

[232] Hasan Çiftçi, *a.g.e.,* s.207
[233] Ntv Haber, Rus Savaş Uçağı Sınırı İhlal Etti., 24.11.2015, *https://www.ntv.com.tr/turkiye/rus-savas-ucagi-dusuruldu,_mP74HrTmEe3cc8qXBIqrA.,* (Erişim Tarihi: 25.08.2021)
[234] Hasan Çiftçi, *a.g.e.,* s.208

uluslararası literatüre geçecek büyüklükte bir saldırı olduğunu ve zararın en aza indirilmesi için uzman ekipler tarafından müdahale edildiği bildirilmiştir.[235]

Yapılan bu siber saldırıları Anonymous yayınladığı bir videoyla üstlenmiştir. Anonymous yaptığı açıklamada Türkiye'nin terör örgütü DEAŞ ile petrol ticareti yaptığı ve terörizmi finanse ettiği için bu saldırıların gerçekleştirildiğini açıklamıştır. Fakat gerek saldırıların yoğunluğu gerekse de saldırıların profesyonelliği açısından devlet destekli bir saldırı olduğu düşünülmektedir. Siber saldırılarıyla ünlü Rusya'nın Rus uçağının düşürülmesinin ardından Türkiye'ye gerek finansal gerekse de itibari zarar vermek amacıyla bu saldırıları gerçekleştirdiği uzmanlar tarafından iddia edilmektedir.[236]

3.6.3. Türk Telekom ve Garanti BBVA bankası siber saldırıları

27 Ekim 2019 tarihinde yurtdışı kaynaklı olarak kamu kurumlarına, GSM operatörlerine ve finans şirketlerine yönelik olarak erişim engellemesi saldırıları yapılmıştır. DDos (Dağıtık Servis Dışı Bırakma) yöntemi kullanılarak saldırılar gerçekleştirilmiştir. Siber saldırılar sebebiyle Türkiye'de internet bağlantılarında kopmalar, kesilmeler ve yavaşlamalar meydana gelmiştir.[237]

---

[235] Merve Kara, Türkiye Siber Saldırı Altında: Bilmeniz Gerekenler, Webrazzi, 25 Aralık 2015, *https://webrazzi.com/2015/12/25/turkiye-siber-saldiri-altinda-bilmeniz-gerekenler/.,* (Erişim Tarihi: 25.08.2021)

[236] Sertan Akçalı, Mehmet Bilge Kağan Onacan, *Türkiye'de Siber Saldırı Olayları ve Siber Savunma Yeteneklerinin Gelişimi,* Jass Studies: The Journal of Academic Social Science Studies, Sayı:78, Kış 2019, s.360.

[237] TRT Haber, *Türkiye'ye yönelik siber saldırılar bertaraf edildi,* 28 Ekim 2019, *https://www.trthaber.com/haber/turkiye/turkiyeye-yonelik-siber-saldirilar-bertaraf-edildi-437841.html.,* (Erişim Tarihi: 26.08.2021)

Garanti BBVA'dan yapılan açıklamada;[238]

> *"Dijital hizmetlerimize yönelik yoğun internet trafiği nedeniyle dijital kanallarımızda erişim sıkıntısı yaşamaktayız. İnternet servis sağlayıcılarımızla beraber sorunu gidermek için çalışıyoruz. Müşterilerimizin yaşadığı mağduriyet için özür dileriz."*

Banka siber saldırıya uğradığını doğrulamıştır.

Siber saldırılara maruz kalan bir diğer şirket olan Türk Telekom üst düzey yöneticisinin yaptığı açıklamada;[239]

> *"Dünyada pek çok kurumun ve devletin maruz kalabileceği gibi bizde siber saldırılara maruz kaldık, uzmanlarımız tarafından zamanında müdahale edilerek saldırılar durdurulmuştur."*

Şeklinde siber saldırıya uğradıklarını doğrulayan bir açıklama gelmiştir.

Yapılan bu saldırılar sonucunda finansal işlemlerin yapılamamasından dolayı çok büyük bir maddi zarar oluşmuştur. Yapılan araştırmalar neticesinde saldırılar sonucu herhangi bir verinin çalınmadığı anlaşılmıştır.[240]

3.6.4. E-ticaret sitelerine yönelik siber saldırı iddiaları

6 Aralık 2019 tarihinde bir internet sitesinden yayılan haber sonrasında mesajlaşma uygulaması WhatsApp aracılığıyla dolaşan bir ses kaydında;

---

[238] Aynı yerde.

[239] Deutsche Welle, *Türkiye'de internet erişimi ve bankalara siber saldırı,* 28.Ekim 2019, *https://www.dw.com/tr/t%C3%BCrkiyede-internet-eri%C5%9Fimi-ve-bankalara-siber-sald%C4%B1r%C4%B1/a-51014514.*, (Erişim Tarihi: 26.08.2021)

[240] Haber Türk, Türkiye DDos Saldırısı Altında! Garanti ve Türk Telekom'dan Açıklama Geldi,28.10.2019, *https://www.haberturk.com/son-dakika-garanti-ve-turk-telekom-na-siber-saldiri-aciklamamasi-haberler-2535014-teknoloji.*, (Erişim Tarihi: 26.08.2021)

"Hepsiburada, Trendyol, Morhipo ve Defacto gibi e-ticaret sitelerinin siber saldırıya maruz kaldığı ve müşteri bilgileri ile müşterilerin kredi kartı bilgilerinin çalındığı bildirilmiştir."

Birçok e-ticaret sitesinde "Efsane Cuma" gibi indirimlerin olduğu ve satış rekorlarının kırıldığı bir dönemde böyle bir iddianın dolaşması sitelerin müşterilerini panikletmiştir. Yapılan araştırmalar sonucunda hackerlar daha önce iflas edip, faaliyetine son veren bir e-ticaret sitesinin müşteri bilgilerini ele geçirdiği ve başka e-ticaret sitelerinde de bu kullanıcı adı ve şifreleri deneyerek hesaplara erişmeyi denedikleri ortaya çıkmıştır. Hackerlar yaptıkları denemeler sonucu herhangi bir finansal duruma erişememişlerdir. Söz konusu sitelerden olan Hepsiburada.com ve Defacto.com.tr yaptıkları açıklamalarda sistemlerine yönelik herhangi bir siber saldırı olmadığını ve herhangi bir verinin çalınmadığını açıklamışlardır. Ayrıca müşteri kredi kartı bilgilerini veri tabanlarında tutmadıklarını ve güvenle alışverişlerine devam edebileceklerini bildirmişlerdir.[241]

Yoğun bir şekilde alışverişin yapıldığı bu tür dönemlerde ortaya çıkan siber saldırı iddiaları herhangi bir saldırı olmasa bile müşterileri paniğe sevk ederek firmalara güvensizlik oluşmasına ve bunun sonucu olarak maddi kayıplara sebep olmaktadır. Alınan önlemlerin yanında müşterilerinde bu konularda bilgilendirilmesi önem arz etmektedir.

3.6.5. Yemeksepeti'ne yönelik siber saldırı

Türkiye'de faaliyet gösteren yemek siparişi internet sitesi Yemeksepeti 25 Mart 2021 tarihinde büyük çaplı bir siber saldırıya uğramıştır. Diğer siber saldırılara kıyasla bu saldırıda internet sitesinin veritabanından müşterilerin önemli bilgileri çalınmıştır.

---

[241] HaberTürk, *e-ticarette ortalığı bir ses kaydı karıştırdı,*06.12.2019, *https://www.haberturk.com/hepsiburada-trendyol-morhipo-ve-defacto-hacklendi-mi-iste-gercek-2547156-ekonomi.*, (Erişim Tarihi: 26.08.2021)

Çalınan bilgiler içerisinde müşterilerin Adı, Soyadı, Doğum Tarihi, cep telefonu numaraları, e-posta adresleri, açık adresleri ve SHA-256 Algoritmasıyla maskelenmiş şifreleri çalınmıştır. Yaşanan bu siber saldırı verilerin değeri açısından son zamanlarda yaşanmış en büyük etki bırakan siber saldırılar arasında yerini almıştır. Şirketten yapılan açıklamada siber saldırıya uğradıkları açıklanırken çalınan veriler arasında müşterilerin kredi kartı bilgilerinin bulunmadığı açıklanmıştır.[242] Saldırıyı gerçekleştiren siber korsanların kim ya da kimler olduğu saptanamamıştır. Bu ve benzeri siber saldırılar şirketlerin itibarlarını zedelemelerinin yanında müşterilerinde oluşan güvensizlik duygusuyla da maddi açıdan şirketleri zarara uğratmaktadır.[243]

3.7. Küresel Siber Güvenlik Endeksinde Türkiye

Birleşmiş Milletler Uluslararası Telekomünikasyon Birliği (ITU) 2013 yılından beri belirli zamanlarda ülkelerin siber güvenlik yapılarını çeşitli kriterler ile ortaya koymaktadır. Oluşturulan Küresel Siber Güvenlik Endeksi 194 ülkeyle belirli kıstaslarda yapılan anketlerin bir sonucudur. Küresel Siber Güvenlik Endeksi 2017 ve 2018 yıllarında yayınlanmış olup, son güncel hali küresel salgın sebebiyle gecikmiştir ve 2021 yılının 2. Çeyreğinde yayınlanması planlanmaktadır.[244]

Küresel Siber Güvenlik Endeksi 5 temel grup içerisinde 25 farklı değerlendirmeyle, grupların sahip olduğu farklı ağırlıklı puan oranlarıyla hesaplanan bir rapordur. 5 temel değerlendirme grubuna bakıldığında bunlar;

- Yasal Tedbirler
- Teknik Tedbirler

---

[242] Ntv Haber, *Yemeksepeti'ne siber saldırı: Önemli kullanıcı bilgileri çalındı,* 27.03.2021, *https://www.ntv.com.tr/teknoloji/yemeksepetine-siber-saldiri,ZKF1OyPIaUCXEonX0A2Mew.,* (Erişim Tarihi: 26.08.2021)

[243] Haber Türk, Yemeksepeti'ne Siber Saldırı, 27.03.2021, *https://www.haberturk.com/yemeksepeti-ne-siber-saldiri-haberler-3019953-teknoloji.,* (Erişim Tarihi:11.09.2021)

[244] Nezir Akyeşilmen, *a.g.e.,* s.138

- Organizasyonel Tedbirler
- Kapasite Artırımları
- İşbirlikleri

Küresel Siber Güvenlik Endeksinin amacı; küresel siber güvenlik kültürünü geliştirmek, ülkelerin siber güvenlikteki mevcut yeteneklerini ortaya koymak, ülkelerin siber güvenlik alanındaki eksik oldukları kısımları geliştirmesine teşvik etmek, ülkelerin siber güvenlik gelişmişliklerini küresel ve bölgesel bir bakış ile değerlendirmek gibi amaçlara sahiptir.[245]

Küresel Siber Güvenlik Endeksinde puanlandırmada kullanılan 5 temel gösterge vardır. Bu 5 temel göstergenin içermiş olduğu kapsama bakıldığında;[246]

1) Yasal Ölçütler: siber suç mevzuatı, siber güvenlikle ilgili yasal düzenlemeler, koruma ve engelleme mevzuatı,
2) Teknik Ölçütler: CERT/CIRT/CSIRT standart uygulama süreçleri, yetkili merciler, teknik güç ve işleyiş, siber güvenlik için bulut teknolojilerinin varlığı, sanal dünyada çocukları korumaya yönelik uygulamalar,
3) Organizasyonel Ölçütler: Ulusal siber güvenlik stratejileri, organizasyonel kuruluşlar, siber güvenlik kıstasları,
4) Yapısal Kapasite Ölçütleri: vatandaşlara yönelik farkındalık faaliyetleri, siber güvenlik çözümlerinin sertifikasyonu ve akreditasyonu işlemleri, siber güvenlik alanında eğitim ve teşvik programları,
5) İşbirliği Ölçütleri: ulusal yada bölgesel anlaşmaların varlığı, uluslararası siber güvenlik alanında faaliyet gösteren derneklere katılım durumu, kamu ve özel sektörün işbirliği potansiyeli, uluslararası örgütler veya kuruluşlarla yapılan işbirliği faaliyetleri

[245] ITU, Global Cybersecurity Index, *https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx.*, (Erişim Tarihi: 25.07.2021)
[246] ITU, Global Cybersecurity Index 2018, *https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf*,s.9, (Erişim Tarihi: 13.03.2021)

Küresel Siber Güvenlik Endeksi'nin ilk raporu olan 2017 yılında yayınlanan raporda Türkiye için yapılan değerlendirmelerde aldığı ağırlıklı puanlara göre 5 temel grupta; yasal tedbirlerde orta, teknik tedbirlerde geçer, organizasyonel tedbirlerde geçer, kapasite artırımında orta ve işbirliği yapmada ise düşük puan almıştır. Türkiye'nin notları toplamı değerlendirilmesine bakıldığı zaman orta seviye olarak belirtilmiştir. Bu verilere göre Türkiye Avrupa Bölgesinde 0.581 puanla 14. Sırada, Küresel ölçekte ise yine aynı puanla 164 katılımcı ülke arasında 43.sırada yer almıştır. 2017 yılında yayınlanan raporda Türkiye'ye yönelik ayrıca bir değerlendirme bulunmamaktadır.[247]

Tablo 14: 2017 Yılı Küresel Siber Güvenlik Endeksi

Üye Ülkeler	**Puan**	**Dünya Sıralaması**
Singapur	0.925	1
ABD	0.919	2
Malezya	0.893	3
Umman	0.871	4
Estonya	0.846	5
Moritus	0.830	6
Avustralya	0.824	7
Gürcistan	0.819	8
Fransa	0.819	8
Kanada	0.818	9
Rusya Federasyonu	0.788	10
Japonya	0.786	11
…..	…..	….
Belarus	0.592	39
Tunus	0.519	40
Hırvatistan	0.590	41
Romanya	0.585	42
Türkiye	**0.581**	**43**
…..	…..	…..

Kaynak: ITU Global Cybersecurity Index 2017

[247] ITU, Global Cybersecurity Index 2017, *https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf*,s.47. (Erişim Tarihi: 13.03.2021)

Küresel Siber Güvenlik Endeksi'nin 2.raporu 2018 yılında yayınlanmıştır. 2018 yılında ki rapora bakıldığında Türkiye yine aynı ölçütlerde yapılan puanlandırmada notunu oldukça yükseltmiştir. Bu raporda Türkiye 0.853 puanla Avrupa Bölgesinde 11. Sırada, Küresel ölçekte ise 20.sırada yer almıştır.[248] İki raporun karşılaştırmalı analizi yapıldığında Türkiye'nin büyük bir yükseliş yaptığı görülmektedir. Bu yükselişin sebeplerine bakıldığı zaman; 2016-2019 Ulusal Siber Güvenlik Strateji Belgesi'nin yayınlanması, küreselde yer alan başarılı örneklerin analizi yapılarak yeni bir rol haritasının oluşturulması, Avrupa Konseyi ile yapılan Budapeşte sözleşmesinin yürürlüğe girmesi, Türkiye Büyük Millet Meclisi tarafından onaylanan Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesi ve siber güvenlik alanında gerçekleştirilen eğitim ve bilinçlendirme çabaları Türkiye'nin bu yükselişi yakalamasında etkili olmuştur. Ayrıca 2018 yılı raporu içerisinde Türkiye'nin yapmış olduğu çalışmalarla ilgili olarak ayrı bir bölüm oluşturulmuştur.

Tablo 15 :2018 Yılı Küresel Siber Güvenlik Endeksi

Üye Ülkeler	**Puan**	**Dünya Sıralaması**	**Üye Ülkeler**	**Puan**	**Dünya Sıralaması**
İngiltere	0.931	1	Japonya	0.880	14
ABD	0.926	2	Moritus	0.880	14
Fransa	0.918	3	G. Kore	0.873	15
Litvanya	0.908	4	Umman	0.868	16
Estonya	0.905	5	Katar	0.860	17
Singapur	0.898	6	Gürcistan	0.857	18
Malezya	0.893	8	Finlandiya	0.856	19
Kanada	0.892	9	**Türkiye**	**0.853**	**20**
Norveç	0.892	9	Danimarka	0.852	21
Avustralya	0.890	10	Almanya	0.849	22
Lüksemburg	0.886	11	Mısır	0.842	23
Hollanda	0.885	12	Hırvatistan	0.840	24
Suudi Arabistan	0.881	13	İtalya	0.837	25

Kaynak: ITU Global Cybersecurity Index 2018

[248] ITU, Global Cybersecurity Index 2018, *https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf*,s.60, (Erişim Tarihi: 13.03.2021)

SONUÇ

Soğuk Savaş sonrası dönemde güvenlik algısında yaşanan değişimin bir sonucu olarak toplumlarda artan internet kullanımıyla beraber siber uzay içerisinde de güvende olabilmek önemli bir konu haline gelmiştir. Kritik altyapılar ve sistemler, ulaşım, su nakil hatları, enerji nakil hatları, finans ve telekomünikasyon süreçlerinde yaşanan dijitalleşme olgusu birçok avantajının yanında siber uzay içerisine dahil olan bu sistemler içinde güvenlik endişelerini de beraberinde getirmiştir. Gelişen ve dönüşen bu ortam içerisinde başta devletler olmak üzere uluslararası örgütler, kurum ve kuruluşlar siber uzayda güvende olabilmek adına çeşitli birimler oluşturup, siber güvenlik hususunda strateji planları ortaya koymuşlardır.

Küreselleşmeyle birlikte fiziksel sınırların kalktığı siber uzayda çok yönlü bir siber güvenlik politikasının izlenmesi hayati bir öneme sahip olmuştur. Bilgi ve iletişim teknolojilerinde yaşanan hızlı değişim ve dönüşüm sürecinin çok dikkatli takip edilmesi ve bu konuda siber güvenlik politikalarının sürekli revize edilmesi güvenliğin sağlanmasında çok önemli bir noktayı işaret etmektedir.

21.yüzyılla beraber devletler siber uzay içerisinde hâkim güç olmanın ve bu ortamda güvende olabilmelerinin oldukça önemli bir durum olduğunun bilincindelerdir. Devletler için siber uzay içerisinde güvende olabilmek milli güvenliğin sağlanması noktasında oldukça önemli bir olgudur. Bu sebeple ordular siber uzay içerisinde hareket kabiliyetlerini artırmaya yönelik çalışmalar yapmaktadır. Bu husus da mevcut geleneksel silahların yanında siber silahlarında etkin bir biçimde kullanılabilmesi savaş alanında destekleyici bir unsurdur.

Siber uzay içerisindeki aktörlerin anonimlik avantajını kullanarak yaptıkları eylemler bu yapı içerisinde ki faillerinin bulunmasını zorlaştırmaktadır. Sistemin bu yapısı sebebiyle saldırının kaynağı sorunu uluslararası hukuk açısından failin

cezalandırılması, yaptırımların yapılması ve tedbirlerin alınması gibi hususları da etkilemektedir. Bir diğer nokta ise tehditlere karşı alınan önlemlerin ne derecede alınması gerektiği, tehdidin kim olduğu ve ne gibi önlemlerin alınması gerektiği konusunu da zorlaştırmaktadır.

Geleneksel saldırı yöntemlerine kıyasla siber saldırıların maliyetlerinin düşük olması siber uzayda ki saldırıların artmasına yol açmaktadır. Bu çerçevede kritik altyapılara ve sistemlere yönelik yapılabilecek siber saldırılarda maliyetinin düşük fakat zararın oldukça büyük olduğu gerçeği ortaya çıkmaktadır. Bu gerçekten hareketle kötü niyetli kullanıcılar tarafından siber saldırılar cazip bir unsur olmaktadır. Cazipliğinin yaratmış olduğu bir noktada siber uzay içerisine terör faaliyetlerinin taşınması olmaktadır. Siber terörizm olarak adlandırılan bu oluşumla mücadele için uluslararası arenada ortak bir fikir birliği çerçevesinde çalışmak gerekmektedir. Devletlerin mevcut terör tanımı üzerinde anlaşamamış olmaları yakın gelecekte de siber terörizm faaliyetlerinin katlanarak artacağı düşüncesini oluşturmaktadır.

Siber uzayın sağlamış olduğu en büyük fayda verilerin çok kolay ve hızlı bir şekilde paylaşılmasıdır. Bilişim çağında kritik öneme sahip olan bilgilerin korunması ve erişilebilirliğinin, bütünlüğünün, gizliliğinin sağlanabilmesi veriye sahip unsurlar için hayati bir öneme sahiptir. Bilginin kaynağından hedefine yönelik gittiği sayısal yol içerisinde bilgilerin güvenliğinin sağlanması siber güvenlik açısından kritik bir konudur.

Kurum ve kuruluşlarda yöneticilerden çalışanlara kadar geniş bir yelpazede siber güvenlik alanıyla ilgili bilinçlendirme ve farkındalık çalışmaları yapılmalıdır. Kurum ve kuruluşlar içerisindeki en büyük riski bilinçsiz kullanıcılar oluşturmaktadır. Bu sebeple bilinçli, eğitimli ve nitelikli personelin varoluşu siber güvenlik ekosisteminin oluşturulabilmesinde kilit bir öneme sahiptir. İlkokuldan başlayarak öğrencilere bilinçli internet kullanımı ve siber güvenlik eğitimleri verilmelidir. Üniversiteler

bünyesinde siber güvenlik çalışmaları yaygınlaştırılmalı ve bu alanda akademisyenler yetiştirilmelidir. Kurum ve kuruluşlarda siber güvenlik birimleri oluşturulmalı ve bu birimlerde nitelikli personeller istihdam edilmelidir.

Sonuç olarak, bilgi ve iletişim teknolojileri günümüzün olmazsa olmazları arasında yer almaktadır. Bu teknolojilerin birçok faydasının yanında kötü niyetli kullanıcıların sebep olduğu olumsuzluklarda unutulmayacak bir gerçektir. Siber güvenlik ekosisteminin oluşturulabilmesinde bireylerden devletlere kadar herkes üzerine düşen sorumluluğu yerine getirmelidir. Bu teknolojik dönüşümü yakalayan ve hâkim olan toplumlar geleceğin etkin güçleri olacaklardır. Bu hususda Türkiye'de bu dönüşüm sürecinden en etkili şekilde yararlanarak başat güçler arasında yerini almalıdır.

KAYNAKÇA

AKÇALI, Sertan & ONACAN, Kağan Bilge, "Türkiye'de Siber Saldırı Olayları ve Siber Savunma Yeteneklerinin Gelişmi", *Jass Studies: The Journal of Academic Social Science Studies*, Sayı 78, Kış 2019.

Akkuş, Gamze, *Anonymous Resmi Hedefe Saldırdı, Ayyıldız Team Karşı Atakla Cevap Verdi*, Hürriyet, 10 Haziran 2011, *https://www.hurriyet.com.tr/ekonomi/anonymous-resmi-hedef-e-saldirdi-ayyildiz-tim-karsi-atakla-yanit-verdi-17996737.*, (Erişim Tarihi: 26.08.2021).

AKYEŞİLMEN, Nezir & KURNAZ, İbrahim, "Küresel Siber Güvenlik: Kavramsal ve Kuramsal Bir Analiz", Yeni Küresel Tehdit Siber Saldırılar, Editör: Fulya Köksoy, 1.Baskı, Nobel Yayınları, Ankara 2020.

AKYEŞİLMEN, Nezir, *Disiplinlerarası Bir Yaklaşım ile Siber Politika ve Siber Güvenlik,* Orion Kitabevi, Ekim 2018.

Alcara, Cristina & Sherali, Zeadally, "Critical İnfrastructure Procteion: Requirements and Challenges For The 21st Century", *International Journal of critical Infrastructure Protection,* Sayı:8, 2015.

ARENDS, J. Frederik, "Homeros'tan Hobbes ve Ötesine: Güvenlik Kavramının Avrupa Geleneğindeki Boyutları", *Uluslararası İlişkiler Dergisi,* Cilt 6, Sayı 22, Yaz 2009.

ARI, Tayyar, *Uluslararası İlişkiler Teorileri: Çatışma, Hegemonya, İşbirliği*, 8.Baskı, MKM Yayıncılık, Bursa 2013.

AYDIN, Hamdi Ahmet, "Toplumsal Güvenlik ve Yerel Siyaset", *Yerel Siyaset,* 1.Baskı, Okutan Yayıncılık, İstanbul 2008.

AYDIN, Mustafa, Uluslararası İlişkilerde Yaklaşım, Teori ve Analiz, *Uluslararası İlişkiler Dergisi,* Cilt 51, No 1, 1996.

Ayyıldız Team, Tarihimiz*, https://www.ayyildiz.org/ayyildiz-tim-tarihi.html.,* (Erişim Tarihi: 5.08.2021).

Ayyıldız Team, Vizyon-Misyon, *https://www.ayyildiz.org/misyon-vizyon.html.,* (Erişim Tarihi: 5.08.2021).

Ayyıldız Team, Zone-H, *http://www.zone-h.org/archive/notifier=Ayy%25C4%25B1ld%25C4%25B1z%2520Tim.,* (Erişim Tarihi:26.08.2021).

B3yaz Hacker, Zone-H, *http://www.zone-h.org/archive/ip=123.30.191.186.,* (Erişim Tarihi: 22.08.2021.)

BAKAN, Zerrin Ayşe, "Soğuk Savaş Sonrasında Yeni Güvenlik Teorileri ve Türkiye'nin Güvenlik Algılamaları", *21.Yüzyıl Dergisi*, Ekim/Kasım/Aralık 2007.

BAYLİS, John, "Uluslararası İlişkilerde Güvenlik Kavramı", *Uluslararası İlişkilerde Çatışmadan Güvenliğe*, Editörler: Mustafa Aydın, Hans Günter Brauch, Mitat Çelikpala, 2.Baskı, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2012.

BIÇAKCI, Salih & ERGUN, Doruk & ÇELİKPALA, Mitat, "Türkiye'de Siber Güvenlik", *EDAM Siber Politika Kağıtları Serisi*, Sayı 1, 2015.

BIÇAKCI, Salih, 21.Yüzyılda Siber Güvenlik, 1.Baskı, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2013.

Bıçakçı, Salih, "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", *Uluslararası İlişkiler Dergisi*, Cilt:9, Sayı:34, 2012.

Bilgi Teknolojileri ve İletişim Kurumu, *Mevzuat, https://www.mevzuat.gov.tr /mevzuat?MevzuatNo=2813&MevzuatTur=1&MevzuatTertip=5.,* (Erişim Tarihi: 6.07.2021)

Bilgi Teknolojileri ve İletişim Kurumu, *Siber Güvenlik Kurulu, https://www.btk.gov.tr/siber-guvenlik-kurulu.,* (Erişim Tarihi: 26.07.2021).

Bilgi Teknolojileri ve İletişim Kurumu, *USOM-SOME, https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi*., (Erişim Tarihi: 14.07.2021).

BRAUCH, Hans Günter, "Güvenliğin Yeniden Kavramsallaştırılması: Barış, Güvenlik, Kalkınma ve Çevre Kavramsal Dörtlüsü", *Uluslararası İlişkiler Dergisi*, Cilt 5, Sayı 18, Yaz 2008.

BUZAN, Barry & Hansen, Lene, *The Evolution of International Security Studies*, Cambridge Unıversity Press, New York 2009.

Cavelty, Myriam Dunn, "Cyber- Security and Threat Politics", *US Efforts to Ensure The Information Age*, New York: routledge, 2008.

CHIP Online, Türkiye Operasyonu Başlıyor! 9 Haziran 2011, *https://www.chip.com.tr/haber/turkiye-operasyonu-basliyor_27402.html.*, (Erişim Tarihi: 28.09.2021).

CLARKE, Richard A. & Robert K. KNAKE, *Cyber War – The Next Threat to National Security and What to Do About It*, HarperCollins, Nisan 2010.

Cyber Warrior, Zone-H, *http://www.zone-h.org/archive/notifier=Cyber-Warrior.*, (Erişim Tarihi: 19.09.2021.)

Cyber Warrrior (Akıncılar), Neler Yaptık? *https://www.cyber-warrior.org/.*, (Erişim Tarihi:15.08.2021).

Cyber Warrrior (Akıncılar), Neler Yaptık? *https://www.cyber-warrior.org/.*, (Erişim Tarihi:15.08.2021).

Cyber Warrrior (Akıncılar), Sitemizin Çizgisi, *https://www.cyber-warrior.org/.*, (Erişim Tarihi: 15.08.2021)

Cyber Warrrior (Akıncılar), Sitemizin Çizgisi, https://www.cyber-warrior.org/., (Erişim Tarihi:15.08.2021).

ÇAKMAK, Haydar & ALTUNOK, Taner, Suç, Terör ve Savaş Üçgeninde Siber Dünya, 1. Baskı, Barış Platin Kitapevi, Ankara 2009.

ÇİFTÇİ, Hasan, *Her Yönüyle Siber Savaş*, 2. Basım, TÜBİTAK Yayınları, Ankara 2017.

DARICILI, Ali Burak, *Siber Uzay ve Siber Güvenlik*, 1.Baskı, Dora Yayınları, Bursa 2017.

DEDEOĞLU, Beril, Uluslararası Güvenlik ve Strateji, 4. Baskı, Yeniyüzyıl Yayınları, İstanbul 2020.

Deutsche Welle, *Türkiye'de internet erişimi ve bankalara siber saldırı,* 28.Ekim 2019, *https://www.dw.com/tr/t%C3%BCrkiyede-internet-eri%C5%9Fimi-ve-bankalara-siber-sald%C4%B1r%C4%B1/a-51014514.*, (Erişim Tarihi: 26.08.2021)

ELMAS, Salih, *Modern Toplumun Güvenlik Çıkmazı: Tehdit, Risk ve Risk Toplumu Perspektifinde Güvenlik*, Uluslararası Stratejik Araştırmalar Kurumu Yayınları, Ankara 2013.

Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı, *Hakkımızda, https://www.egm.gov.tr/siber/hakkimizda2*., (Erişim Tarihi: 27.07.2021).

Emniyet Genel Müdürlüğü, *Hacker Nedir? Hacking nedir? Siber suçlar Nelerdir? http://siberguvenlikhaberleri.blogspot.com/2014/05/hacking-nedir.html,* (Erişim Tarihi: 04.04.2020).

ERENDOR, Mehmet Emin, "Türkiye'nin Siber Güvenlik Politikası", Yeni Küresel Tehdit Siber Saldırılar, Editör: Fulya Köksoy, Nobel Yayınları, Ankara 2020.

ERGÜL, Ergin, *Küresel Köyde Suç ve Adalet*, 1. Baskı, Adalet Yayınevi, Ankara 2008.

ERHAN, Çağrı, "Soğuk Savaş Sonrası ABD'nin Güvenlik Algılamaları", *Uluslararası Güvenlik Sorunları ve Türkiye*, Derleyenler: Refet Yinanç, Hakan Taşdemir, Seçkin Yayıncılık, Ankara 2002.

ERİŞ, Ufuk, "Türkiye'de Kırıcı (Hacker) Kültürü", *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi*, Sayı 2, Eylül 2011.

Ermiş, Kemal, "Sayısal İmza ve Elektronik Belge Yönetimi", *Bilgi Dünyası,* Cilt: 7, Sayı:1, 2006.

GÖÇOĞLU, Volkan, "Türkiye'nin Siber güvenlik Politikası: Karar Verme Yaklaşımları Çerçevesinde Bir Analiz", Güvenlik, Teknoloji ve Yeni Tehditler, Editör: Ali Burak Darıcılı, 1.Baskı, Nobel Yayınları, Bursa 2020.

Güngör, Murat, Ulusal *Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma,* (T.C. Kalkınma Bakanlığı, Bilgi Toplumu Dairesi Başkanlığı, Basılmamış Uzmanlık Tezi), Ankara 2015.

GÜNTAY, Vahit, "Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu: Siber Savaş Örneği", *Güvenlik Bilimleri Dergisi*, Cilt 6, Sayı 2, Kasım 2017.

Gürkaynak, Muharrem & İren, Ali Âdem, "Reel Dünya'da Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Dergisi, Cilt: 16, Sayı:2, 2011.

Haber Türk, Türkiye DDos Saldırısı Altında! Garanti ve Türk Telekom'dan Açıklama Geldi,28.10.2019, *https://www.haberturk.com/son-dakika-garanti-ve-turk-telekom-na-siber-saldiri-aciklamamasi-haberler-2535014-teknoloji.,* (Erişim Tarihi: 26.08.2021).

Haber Türk, Yemeksepeti'ne Siber Saldırı, 27.03.2021, *https://www.haberturk.com/yemeksepeti-ne-siber-saldiri-haberler-3019953-teknoloji.,* (Erişim Tarihi:11.09.2021).

HaberTürk, *e-ticarette ortalığı bir ses kaydı karıştırdı,*06.12.2019, *https://www. haberturk.com/hepsiburada-trendyol-morhipo-ve-defacto-hacklendi-mi-iste-gercek-2547156-ekonomi.,* (Erişim Tarihi: 26.08.2021).

Hathaway, Oona & Crootof, Rebecca, "The Law of Cyber-Attack", *California Law Review,* Sayı:100, 2012.

Hekim, Hakan, "Oltalama (Phishing) Saldırıları", *Siber Suçlar, Tehditler, Farkındalık ve Mücadele*, Derleyenler: Fatih Tombul, Murat Güneştaş, Oğuzhan Başıbüyük, Global Politika ve Strateji, Ankara, 2015.

ITU, Global Cybersecurity Index 2017, *https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf*,s.47. (Erişim Tarihi: 13.03.2021).

ITU, Global Cybersecurity Index, *https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx* (Erişim Tarihi: 13.03.2021)

ITU,Global Cybersecurity Index 2018, *https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf*,s.9, (Erişim Tarihi : 13.03.2021).

İduğ, Yavuz & Çalışkan, Ferhat & Güler Talip, "Siber Caydırıcılık ve Türkiye'nin İmkân ve Kabiliyeti", 6. Uluslararası Bilgi Güvenliği ve Kripto Konferansı Bildirileri Kitabı, Ankara, 2013.

İstanbul Teknik Üniversitesi Bilgi İşlem Daire Başkanlığı, *İnternetin Tarihçesi,* 7 Eylül 2013, *https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/internet'in-tarih%C3%A7esi*, (Erişim Tarihi: 07.01.2021).

KARA, Merve, Türkiye Siber Saldırı Altında: Bilmeniz Gerekenler, Webrazzi, 25 Aralık 2015, *https://webrazzi.com/2015/12/25/turkiye-siber-saldiri-altinda-bilmeniz-gerekenler/.*, (Erişim Tarihi: 25.08.2021).

Karaarslan, Enis & Akın, Gökhan & Demir, Hüsnü, "Kurumsal Ağlarda Zararlı Yazılımlarla Mücadele Yöntemleri", *Çanakkale On Sekiz Mart Üniversitesi Akademik Bilişim Konferansı*, Çanakkale 2008.

KARABACAK, Bilge, "Kritik Altyapılara Yönelik Siber Tehditler ve Türkiye İçin Siber Güvenlik Önerileri", *Siber Güvenlik Çalıştayı*, Bilge Güvenliği Derneği, 29 Eylül 2011 Ankara.

Kaspersky, *Hacker Nedir? https://www.kaspersky.com.tr/blog/hacker-ne-demektir/611/*about:blank (Erişim Tarihi:03.04.2020).

KORHAN, Sevda, "Uluslararası İlişkilerde Siber Güvenlik: Caydırıcılık, Güç ve Diplomasi", Yeni Küresel Tehdit Siber Saldırılar, Editör: Fulya Köksoy, 1.Baskı, Nobel Yayınları, Ankara 2020.

KRAUSE, Keıth & WILLIAMS, Mıcheal, "From Strategy to Security: Foundations of Critical Security Studies", *Critical Security Studies: Concepts and Cases*, Unıversıty of Minnesota Press, 1997.

KULA, Sedat Bekir ÇAKAR "*Maslow İhtiyaçlar Hiyerarşisi Bağlamında Toplumda Bireylerin Güvenlik Algısı ve Yaşam Doyumu Arasındaki İlişki*", *Bartın Üniversitesi İ.İ.B.F. Dergisi*, Cilt no:6, Sayı :12, yayın yılı: 2015

Libicki, Martin, "Cyber detterence and Cyberwar", Santa Monica, CA: Rand Cooperation, 2009.

Malware Definition, *https://techterms.com/definition/malware#:~:text=Short%20for%20%22malicious%20software%2C%22,actions%20on%20a%20computer%20system.*, (Erişim Tarihi: 08.04.2020.)

Malware Definition, *https://techterms.com/definition/malware#:~:text=Short%20for%20%22malicious%20software%2C%22,actions%20on%20a%20computer%20system.*, (Erişim Tarihi: 08.04.2020.)

Mele, Stefano, "Cyber- Weapons: Legal and Strategic Aspects", *Machiavelli Editions*, Version 2.0, *https://www.files.ethz.ch/isn/168388/cf4eaaaf89e17df399d1d580beade36a.pdf*, 2013, (Erişim Tarihi: 06.04.2021).

Milli Güvenlik Kurulu Genel Sekreterliği, 27 Ekim 2010 tarihli toplantı, *https://www.mgk.gov.tr/index.php/27-ekim-2010-tarihli-toplanti.*, (Erişim Tarihi: 14.02.2021).

Norton Antivirüs,*What is the Difference Between Black, White and Grey Hat Hackers?,https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html* (Erişim Tarihi 08.04.2020).

Ntv Haber, Rus Savaş Uçağı Sınırı İhlal Etti., 24.11.2015, *https://www.ntv.com.tr/turkiye/rus-savas-ucagi-dusuruldu,_mP74HrTmEe3cc8qXBIqrA.*, (Erişim Tarihi: 25.08.2021).

Ntv Haber, *Yemeksepeti'ne siber saldırı: Önemli kullanıcı bilgileri çalındı,* 27.03.2021, *https://www.ntv.com.tr/teknoloji/yemeksepetine-siber-saldiri,ZKF1OyPIaUCXEonX0A2Mew.*, (Erişim Tarihi: 26.08.2021).

RedHack, Zone-H, *http://www.zone-h.org/archive/notifier=RedHack.,* (Erişim Tarihi:06.08.2021).

SAĞIROĞLU, Şeref, "Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler", *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*, Editörler: Şeref Sağıroğlu, Mustafa Alkan, Grafiker Yayınları, Ankara 2018.

SANDIKLI, Atilla & EMEKLİER, Bilgehan, Güvenlik Yaklaşımlarında Değişim ve Dönüşüm", *BİLGESAM*.

SINGER, Peter Waren & FRIEDMAN, Allan, *Siber Güvenlik ve Siber Savaş*, 1. Baskı, Buzdağı Yayınları, Ankara 2015.

Spyware, TechTerms, *https://techterms.com/definition/spyware.,* (Erişim Tarihi: 08.04.2021).

ŞAHİN, Bedri, Değişen Dünya Düzenine Bağlı Olarak Değişen Uluslararası Güvenlik Algısı, *İmgelem,* Cilt 4, Sayı 6, 2020.

ŞAHİN, Güngör, *Soğuk Savaş Sonrası Değişen Güvenlik Anlayışı Bağlamında NATO,* Trakya Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Anabilim Dalı, Basılmamış Doktora Tezi, Edirne 2015.

ŞENOL, Mustafa, "Hibrit Savaş Kapsamında Siber Savaş ve Siber Caydırıcılık", *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*, Editörler: Şeref Sağıroğlu, Mustafa Alkan, Grafiker Yayınları, Ankara 2018.

T.C. İçişleri Bakanlığı Afet ve Acil Durum Yönetimi Başkanlığı, *2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi*, Eylül 2014, *https://www.afad.gov.tr/kurumlar/afad.gov.tr/2535/files/123-20141010111330-kritikaltyapi-son.pdf.,* (Erişim Tarihi: 02.08.2011).

T.C. Resmî Gazete, Devlet İstihbarat Hizmetleri ve Milli istihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun, Karar Numarası:6532, 17 Nisan 2014, *https://www.resmigazete.gov.tr/eskiler/2014/04/20140426-1.htm.,* (Erişim Tarihi: 27.07.2021).

T.C. Resmî Gazete, Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar (2012), Karar Numarası:28447, *https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm* 20 Ekim 2012, (Erişim Tarihi: 12.04.2020).

T.C. Resmî Gazete, Ulusal Siber Güvenlik Stratejisi (2013-2014), 20 Haziran 2013, Karar Numarası: 28683, *https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm, (*Erişim Tarihi: 12.04.2020*).*

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, *2016-2019 Ulusal Siber Güvenlik Stratejisi (2016), http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf*.(Erişim Tarihi:22.04.2020).

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, *2020-2023 Ulusal Siber güvenlik Stratejisi (2020), https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf,* (Erişim Tarihi:07.02.2021)

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ulusal Siber Güvenlik Stratejisi (2016-2019), *http:/www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.odf*, (Erişim Tarihi: 03.04.2020).

The Goverment of The Hong Kong Special Administrative, "*Honeypot Security*", Şubat 2008, *https://docplayer.net/3431533-Honeypot-security-february-2008-the-government-of-the-hong-kong-special-administrative-region.html.,* (Erişim Tarihi: 12.11.2021.).

The Goverment of The Hong Kong Special Administrative, *Region an Overview of Vulnerability Scanners*, 2008, *https://slidelegend.com/an-overview-of-vulnerability-scanners_5a0cdbd91723dd746a0fae27.html.,* (Erişim Tarihi: 10.09.2021.).

Trojan Horse, TechTerms, *https://techterms.com/definition/trojanhorse*., (Erişim Tarihi: 08.04.2021).

TRT Haber, *Türkiye'ye yönelik siber saldırılar bertaraf edildi,* 28 Ekim 2019, *https://www.trthaber.com/haber/turkiye/turkiyeye-yonelik-siber-saldirilar-bertaraf-edildi-437841.html.,* (Erişim Tarihi: 26.08.2021).

Turak, Yiğit, *RedHack Özelinde Siber Olaylar ve Siber Suçlar*, İstanbul Bilgi Üniversitesi 2014, *http://www.yigitturak.com/wp-content/uploads/RedHackIncelemesi.pdf.*, (Erişim Tarihi: 22.08.2021).

Turk Hack Team, *https://www.linkedin.com/company/turkhackteam/?OriginalSubdomain=tr.*, (Erişim Tarihi: 6.08.2021).

Turk Hack Team, *Misyon, https://www.turkhackteam.org/misyon.html.*, (Erişim Tarihi: 6.08.2021)

Turk Hack Team, Zone-H, *http://www.zone-h.org/archive/notifier=turkhackteam/page=3.*, (Erişim Tarihi: 11.09.2021).

TÜBİTAK, *Tarihçe Siber Güvenlik Enstitüsü, https://sge.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce.*, (Erişim Tarihi: 06.07.2021)

Türk Dil Kurumu Çevrimiçi Sözlüğü, Hacker Nedir? *http://www.tdk.gov.tr/?option=com_karsilik&view=karsilik&kategori1=abecesel&kelime2=H* (Erişim Tarihi: 03.04.2020).

Türk Dil Kurumu Online Sözlüğü, Caydırıcılık Nedir? *https://sozluk.gov.tr/*, (Erişim Tarihi: 08.04.2020.)

Türk Dil Kurumu Sözlükleri, Güvenlik Nedir? *https://sozluk.gov.tr/?q=g%C3%BCvenlik&aranan=*, (Erişim Tarihi:17.01.2022)

Türk Güvenliği, *https://twitter.com/turkguvenligi.*, (Erişim Tarihi:26.08.2021).

Türk Güvenliği, Zone-H, *http://www.zone-h.org/archive/notifier=turkguvenligi.info.*, (Erişim Tarihi: 26.08.2021).

Ulaşanoğlu, Emin & Yılmaz, Ramazan & Tekin Alper, *Bilgi Güvenliği: Riskler ve Öneriler*, Bilgi Teknolojileri ve İletişim Kurumu, Ankara 2010.

ULLMAN, Richard, "Redefining Security", *International Security*, Cilt 8, No 1, Yaz 1983.

Ulusal Siber Olaylara Müdahale Merkezi, USOM, *USOM Hakkında*, *https://www.usomgov.tr/hakkimizda.html* (Erişim Tarihi: 22.04.2020)

ULUTAŞ, Güzin, "Siber Güvenlik", *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*, Editörler: Şeref Sağıroğlu, Mustafa Alkan, Grafiker Yayınları, Ankara 2018.

US CERT- MS ISAC, Local Goverement Cyber Security: Beginner Guide To Firewalls, 2006, https://flmanagers.com/wp-content/uploads/2021/01/Cybersecurity-for-Local-Government-Guide.pdf., (Erişim Tarihi: 12.11.2021.).

US-CERT, *Computer Forensics*, 2008, *https://www.cisa.gov/uscert/sites/default/files/publications/forensics.pdf.,* (Erişim Tarihi: 16.12.2021.).

Varlık, Ali Bilgin, "Savaşı Tanımlamak, Terminolojik Bir Yaklaşım", Avrasya Terim Dergisi, Cilt:1, Sayı:2, 2013.

Virus Definition, TecTerms, *https://techterms.com/definition/virus.,* (Erişim Tarihi: 06.04.2021).

WAEVER, Ole, "Securitization and Desecuritization", *International Security Volume 3: Widening Security*, Editörler: Barry Buzan, Lene Hansen, Londra Sage Publibations, Londra 2007.

Weimann, Gabriel, "Cyber- Terorism, How Real Is The Treat? *Unıted States Institu of Peace,* Special Report 119, Washighton D.C., 2004.

Worm Definition, TechTerms, *https://techterms.com/definition/worm.,* (Erişim Tarihi:06.04.2021)

YALMAN, Yıldıray, "Siber Terör, Terörizm ve Mücadele", Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık, Editörler: Şeref Sağıroğlu, Mustafa Alkan, Grafiker Yayınları, Ankara 2018.

Yıldız, Mithat, *Siber Suçlar ve Kurum Güvenliği*, (T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Bilgi İşlem Daire Başkanlığı, Basılmamış Denizcilik Uzmanlık Tezi), Ankara 2014.