2024

YÜKSEK LİSANS TEZİ

Burak YAĞCI



T.C.

ANKARA YILDIRIM BEYAZIT ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

SİBER TERÖRİZMİN İDARE HUKUKUNDA SOSYAL RİSK İLKESİ ÇERÇEVESİNDE İNCELENMESİ

YÜKSEK LİSANS TEZİ

BURAK YAĞCI

YÖNETİM BİLİŞİM SİSTEMLERİ ANA BİLİM DALI

ANKARA, 2024

T.C.
ANKARA YILDIRIM BEYAZIT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

SİBER TERÖRİZMİN İDARE HUKUKUNDA SOSYAL RİSK İLKESİ ÇERÇEVESİNDE İNCELENMESİ

YÜKSEK LİSANS TEZİ

BURAK YAĞCI

YÖNETİM BİLİŞİM SİSTEMLERİ ANA BİLİM DALI

Tez Danışmanı

Prof. Dr. Derya FINDIK

ANKARA, 2024

ONAY SAYFASI

Burak YAĞCI tarafından hazırlanan "Siber Terörizmin İdare Hukukunda Sosyal Risk İlkesi Çerçevesinde İncelenmesi" adlı tez çalışması aşağıdaki jüri tarafından oy birliği ile Ankara Yıldırım Beyazıt Üniversitesi Sosyal Bilimler Enstitüsü Yönetim Bilişim Sistemleri Ana Bilim Dalı E-Devlet ve Kamuda Dönüşüm Programında Yüksek Lisans Tezi olarak kabul edilmiştir.

<table>
<tr><th colspan="2">JÜRİ ÜYESİ</th><th>Kurumu</th><th>İmza</th></tr>
<tr><td colspan="2">Danışman: Prof. Dr. Derya FINDIK</td><td rowspan="2">Ankara Yıldırım Beyazıt Üniversitesi</td><td rowspan="2"></td></tr>
<tr><td>Kabul x</td><td>Red</td></tr>
<tr><td colspan="2">Dr. Öğr. Üyesi Musab Talha AKPINAR</td><td rowspan="2">Ankara Yıldırım Beyazıt Üniversitesi</td><td rowspan="2"></td></tr>
<tr><td>Kabul x</td><td>Red</td></tr>
<tr><td colspan="2">Prof. Dr. Olgun DEĞİRMENCİ</td><td rowspan="2">TOBB Ekonomi ve Teknoloji Üniversitesi</td><td rowspan="2"></td></tr>
<tr><td>Kabul x</td><td>Red</td></tr>
</table>

Tez Savunma Tarihi: 27.12.2024

Ankara Yıldırım Beyazıt Üniversitesi Sosyal Bilimler Enstitüsü Yönetim Bilişim Sistemleri Ana Bilim Dalında Yüksek Lisans Tezi olması için şartları yerine getirdiğini onaylıyorum.

Doç. Dr. Muhammet Enes KALA
Sosyal Bilimler Enstitüsü Müdürü V.

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün aşamalarda patent ve teklif haklarını ihlal edici etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, bu tezde kullanılmış olağan tüm bilgi ve yorumlara kaynak gösterdiğimi beyan ederim.

Tarih: (27.12.2024)

Burak YAĞCI

TEŞEKKÜR

Tez çalışmam boyunca bilgi ve deneyimlerini benimle paylaşarak değerli katkılarda bulunan tez danışmanım Sn. Prof. Dr. Derya FINDIK'a, manevi destekleri ile bu süreç boyunca yanımda olan annem Gülay YAĞCI, babam Akif YAĞCI ve ablam Esra YAĞCI'ya, her daim beni destekleyerek umut ışığım olan ve hukuki bilgisi ile bu teze katkıları için sevgili eşim Av. İrem YAĞCI'ya teşekkürü bir borç bilirim. Tezimi yeni doğacak olan oğlum Ilgaz'a ithaf ediyorum.

ÖZET

Siber Terörizmin İdare Hukukunda Sosyal Risk İlkesi Çerçevesinde İncelenmesi

Siber terörizm, son yüzyılda konvansiyonel savaşların yanında kullanılan hibrit savaş yöntemleri ile birlikte hayatımıza girmiştir. Teknolojik gelişmelerle beraber devletler arası savaşların siber ortama taşınması neticesinde devletlerin kritik altyapılarına, kritik tesis ve varlıklarına, üretim tesislerine, enerji altyapılarına yönelik siber saldırılar artarak siber uzamda yeni bir küresel güç savaşı ortaya çıkarmıştır. Devlet dışı aktörler ve terör örgütleri, internet teknolojilerini kullanarak siyasi hedefler doğrultusunda siber terörizmi etkili bir toplumsal araç olarak belirlemiştir. Devletler için ise, daha az maliyetle rakip olarak gördükleri diğer devletlerin kritik altyapılarına zayiat verme imkânı hasıl olmuştur. Bu bağlamda terörizm neticesinde bireylerin sırf o devletin vatandaşları olmaları dolayısıyla gördükleri maddi ve manevi zararların yine devlet tarafından idarenin sorumluluğu kapsamında tazmin edilmesi hususu gündeme gelmiştir. Diğer taraftan tüm uluslararası hukukta olduğu gibi, Türk hukukunda da yer alan klasik terörizm ve terörle mücadeleden doğan zararların tazminine ilişkin düzenlemelerin, siber saldırılar neticesinde vatandaşların görebileceği zararlara karşı yeterli olmadığı ve bu alanda bir kanun boşluğu olduğu görülmektedir. Bu çalışmada; siber terörizmin tarihi gelişimi içerisinde ana unsurları, siber terörizmde araç olarak kullanılan siber saldırı yöntemleri, devletlerin siber dayanıklılığına yönelik siber güvenlik tedbirleri ile söz konusu alandaki kanun boşluğunun doldurulması amacına hizmet edebilecek nitelikte kanun koyucuya yol gösterecek çözüm önerileri ele alınmıştır.

Anahtar Kelimeler: İdare Hukuku, Siber Saldırı, Siber Suç, Siber Terörizm, Sosyal Risk İlkesi

ABSTRACT

Examination of Cyber Terrorism in the Framework of Social Risk Principle in Administrative Law

Cyber terrorism has entered our lives with hybrid warfare methods used alongside conventional warfare in the last century. As a result of the transfer of interstate wars to the cyber environment with technological developments, cyber attacks on critical infrastructure, critical facilities and assets, production facilities and energy infrastructures of states have increased, creating a new global power struggle in cyberspace. Non-state actors and terrorist organisations have identified cyber-terrorism as an effective social tool to achieve political goals through the use of Internet technologies. It has become possible for states to inflict damage at lower cost on the critical infrastructure of other states that they perceive as rivals. In this context, the question of compensation for the material and moral damage suffered by individuals as a result of terrorism, simply because they are citizens of that state, has come to the fore, under the responsibility of the administration. On the other hand, as in any international law, it can be seen that the regulations regarding the compensation of damages resulting from classical terrorism and the fight against terrorism in Turkish law are not sufficient for the damages that citizens may suffer as a result of cyber attacks, and there is a legal gap in this area. In this study, the main elements of cyber terrorism within its historical development, cyber attack methods used as tools in cyber terrorism, cyber security measures for the cyber resilience of states and proposed solutions that will guide the legislator to fill the legal gap in this area are discussed.

Keywords: Administrative Law, Cyber Attack, Cyber Crime, Cyber Terrorism, Social Risk Principle

İÇİNDEKİLER

ONAY SAYFASI i
BEYAN ii
TEŞEKKÜR iii
ÖZET. iv
ABSTRACT v
İÇİNDEKİLER vi
SİMGELER VE KISALTMALAR DİZİNİ viii
ŞEKİLLER DİZİNİ x
TABLOLAR DİZİNİ xi
GİRİŞ. 1
1. SİBER TERÖRİZM ve TARİHSEL GELİŞİMİ 6
1.1. Siber Terörizm 6
1.2. Terör, Terörizm ve Siber Terörizm İlişkisi 8
1.3. Siber Terörizmin Tarihi Gelişimi ve Teorik Temelleri 17
1.4. Siber Terörizme Yakın Kavramlar 22
2. SİBER SALDIRI TÜRLERİ 67
2.1. Kötü Amaçlı Yazılım İçeren Siber Saldırılar 67
2.2. Ağ ve Sistem Hedefli Siber Saldırılar 103
2.3. İnsan Hataları Kaynaklı Siber Saldırılar 121
2.4. Diğer Siber Saldırı Yöntemleri 125
3. SİBER TERÖRİZM ve ULUSLARARASI HUKUK 134
3.1. NATO Antlaşması Kapsamında Siber Saldırılarla Mücadele 135
3.2. BM Sözleşmesi Kapsamında Meşru Müdafaa ve Kuvvet Kullanımı 136
3.3. Devletlerin Uluslararası Sorumluluğu Kapsamında Siber Saldırılar 139
3.4. Siber Saldırıların Silahlı Saldırı Sayılması Tartışması 142
3.5. Tallinn Manual ve Dava Örnekleri Kapsamında Siber Saldırılar 147
4. İDARE HUKUKUNDA SORUMLULUK ve SİBER TERÖRİZM 157
4.1. İdarenin Sorumluluğu 158
4.2. İdarenin Kusursuz Sorumluluğu 166

4.3. Risk İlkesi Kapsamında İdarenin Sorumluluğu 171
4.4. İdarenin Sorumluluğu Kapsamında Zararın Tazmini 179
4.5. İdarenin Tazminat Sorumluluğuna İlişkin Temel İlkeler.....182
4.6. Siber Terörizm ile Tazminat Yükümlülüğü İlişkisi 188
SONUÇ VE ÖNERİLER 193
KAYNAKLAR.....207

SİMGELER VE KISALTMALAR DİZİNİ

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
API	Application Programming Interface
APT	Advanced Persistent Threat
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
BM	Birleşmiş Milletler
BMGK	Birleşmiş Milletler Güvenlik Konseyi
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CCA	Cyber Caliphate Army
CER	Critical Establishment Resilience Directive
CERT	Computer Emergency Response Team
CIA	The Central Intelligence Agency
CISA	The Cybersecurity and Infrastructure Security Agency
CMK	Ceza Muhakemeleri Kanunu
CRA	Cyber Resilience Act
CSA	Cyber Security Act
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service Attack
DMK	Devlet Memurları Kanunu
DNS	Domain Name System
DORA	Digital Operational Resilience Act
DoS	Denial of Service Attack
ENISA	European Union Agency for Cybersecurity
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IBM	International Business Machines
IDS	Intrusion Detection System
IP	Internet Protocol

ISP	Internet Service Provider
ITU	International Telecommunication Union
İYUK	İdari Yargılama Usulü Kanunu
KGB	Komitet Gosudarstvennoy Bezopasnosti
MitM	Man-in-the-Middle Attack
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCA	National Cyber Security Authority
NIS2	The NIS 2 Directive (EU) 2022/2555
NIST	The National Institute of Standards and Technology
NSA	National Security Agency
P2P	Peer-to-peer
PII	Personally İdentifiable İnformation
PLC	Programmable Logic Controller
RaaS	Ransomware-as-a-Service
SCA	Sons Caliphate Army
SMTP	Simple Mail Transfer Protocol
SOME	Siber Olaylara Müdahale Ekibi
SSL	Secure Sockets Layer
STRATCOM	US Strategic Command
SQL	Structured Query Language
TCK	Türk Ceza Kanunu
UCC	United Cyber Caliphate
URL	Uniform Resource Loader
USOM	Ulusal Siber Olaylara Müdahale Merkezi

ŞEKİLLER DİZİNİ

Şekil 1. Bilgi Güvenliği Politikası Unsurları..... 62
Şekil 2. Yıllık Sağlık Hizmetleri Veri İhlalleri (The HIPAA Journal, 2023b). 95

TABLOLAR DİZİNİ

Tablo 1. Libicki'nin Bilgi Savaşı Biçimlerine İlişkin Yedili Kategorizasyonu (Robinson ve diğer., 2015)..... 52
Tablo 2. Siber Saldırı Türlerinin Sınıflandırılması..... 67
Tablo 3. Kritik Altyapı Türlerine ve Sorumlu Kuruluşlara İlişkin Öneriler..... 198

GİRİŞ

Son yıllarda gelişen bilgi ve iletişim teknolojileri, sağladığı faydaların yanı sıra toplum ve devletler açısından çeşitli riskleri de beraberinde getirmiştir. Öyle ki söz konusu riskler dolayısıyla devletlerin kendi vatandaşlarının alacağı hizmetler üzerinde sağlamakla yükümlü olduğu sorumluluklar doğmuştur. Devletlerin idari işlem ve faaliyetlerini internet üzerinden gerçekleştirmesi ve kamuda dijital dönüşümle birlikte e-devlet hizmetlerinin vatandaşların kritik ve hassas verilerini barındırması siber saldırganların söz konusu sistemleri hedeflemesine yol açmıştır. Bununla birlikte kritik altyapıların bilgi ve iletişim teknolojilerine bağlı ve bağımlı hale gelmesi söz konusu siber saldırıların bilişim sistemlerine yönelmesine yol açmıştır. Bu kapsamda devletlerin yönetim ve bilişim sistemlerini kullanarak siber güvenlik önlemlerini alması bir yükümlülük haline gelmiştir. Siber uzay bağlamında gerçekleştirilen saldırı ve haksız fiiller karşısında idarelerin sorumluluk alanları genişlemiş, kritik altyapıların uzaktan kontrol ve yönetim sistemlerini oluşturan endüstriyel kontrol sistemleri ve SCADA'ların yönetim bilişim sistemleri bağlamında ele alınması gerekli olmuştur.

Siber saldırıların hedefi haline gelen kritik altyapılar, devletlerin ülkesel bütünlüklerine ve kamu güvenliğine ilişkin zafiyetleri ortaya çıkarmakta, bu sebeple günümüzde söz konusu varlık ve tesislerin daha büyük bir öneme kavuştuğu görülmektedir. Kritik altyapılara yönelik siber saldırılar devletlerin siyasi, ekonomik, idari ve sosyal alanlarda sahip olduğu tesislere zarar vermekte, vatandaşların hak kaybı ve menfaat ihlallerine sebep olmaktadır. Bu çerçevede idarenin sorumluluğu bağlamında devletlerin siber uzaydaki tehditlere karşı siber güvenlik önlemlerini alması, siber saldırı ve suçlarla etkin mücadelede bulunması, kamu kurum ve kuruluşlarının siber dayanıklılık kapasitesini artırması ve saldırılardan doğan zararlar dolayısıyla vatandaşlara yönelik hukuki, teknik ve idari siber güvenlik tedbirlerini alması gerekmektedir. Gerekli siber savunma tedbirlerini almayan devletlerin idari işlem ve faaliyetlerini yürüten idareler vatandaşların uğradıkları zararlar dolayısıyla kusursuz sorumluluk ve sosyal risk ilkesi çerçevesinde yaptırıma tabi tutulması gerektiği değerlendirilmektedir.

Araştırma Yöntemi

Bu çalışmada "sistematik literatür taraması" kapsamında uluslararası anlaşma, hukukun genel ilkeleri, uluslararası belge ve davalar incelenmiştir. "Belgesel araştırma yöntemi" kullanılarak uluslararası yasal dokümanlar araştırılmış, resmî belgeler ve yayınlar detaylıca ele alınmıştır. Söz konusu dokümanlar Amerika Birleşik Devletleri ve Birleşik Krallık başta olmak üzere hem Anglo-Sakson Hukuk Sistemi, hem de Avrupa Birliği çalışmaları kapsamında Kıta Avrupası Hukuk Sistemi çerçevesinde tartışılmıştır. Siber terörizm kavramı devletlere göre farklılaşan mevzuat, toplumsal norm ve teamüller doğrultusunda incelenerek buna ilişkin tanımlar ortaya konmuştur. Siber saldırı türleri devletlerin resmi siber güvenlik organları ve strateji politikaları bakımından ele alınmıştır. Sektörde faaliyet gösteren özel firmalar ve siber güvenlik şirketlerinin söz konusu alanda kamuya ve vatandaşlara sundukları çözümler, aktif ve pasif caydırıcılık yöntemleri araştırılarak bu araçlara çalışmada yer verilmiştir. Ülke uygulamaları ve uluslararası kuruluşların çalışmaları kapsamında resmi internet siteleri üzerinden kaynak taraması yapılmış, NIST Cybersecurity Framework, NIST SP (Special Publication), ENISA Cybersecurity Reports, Best Practices, Policy Papers, ITU Cybersecurity Resources, ITU-T (Telecommunication Standardization Sector), CISA Cybersecurity Toolkits & Services, UN Group of Governmental Experts (GGE), NATO Cyber Defence Centre of Excellence (CCDCOE) Database, NATO Cyber Crime Information Sharing veri tabanları kullanılmıştır. İdare hukuku bağlamında meri mevzuat incelenmiş ve "Danıştay Dosya Sorgulama" veri tabanı kullanılarak terörizme ilişkin zararlarda idarenin kusursuz sorumluluğu kararlar doğrultusunda incelenmiştir. Sosyal risk ilkesi kapsamında terör faaliyetlerinden dolayı vatandaşların uğradığı zararlar detaylı şekilde ele alınmıştır. Son olarak siber saldırılara yönelik uygulanabilecek ve uygulanması gereken mevzuat tartışılmıştır. Bu kapsamda "İdare Hukuku", "Siber Saldırı", "Siber Suç", "Siber Terörizm", "Sosyal Risk İlkesi" anahtar kelimeleri temel alınarak bahse konu çalışma ortaya konmuştur.

Problemin Tanımlanması

Çalışmada ele alınacak ana problem; gelişen saldırı teknolojileriyle devletlerin maruz kaldığı kritik altyapılara yönelik siber saldırılar sonucunda vatandaşların uğradığı zararların idare tarafından tazmin edilip edilemeyeceği meselesidir. Bu kapsamda devletlerin

fiziki ve sibere dayalı kritik varlık ve tesislerin tahribata uğratılması, vatandaşların bu sebeple uğradığı maddi ve manevi zararlar, söz konusu zararların idarenin kusursuz sorumluluğu ve sosyal risk ilkesi kapsamında tazminat yükümlülüğü çalışmanın ana odak noktası olmuştur. Siber saldırılar ile ilgili uluslararası hukukta bulunan mevzuat boşluğu dolayısıyla siber saldırılara ve siber terörizm faaliyetlerine ilişkin uygulanabilecek genel hukuk ilkeleri araştırılmıştır. Bunların yetersiz kaldığı durumlarda ise bu alana özgü kuralların ortaya konulması gerekliliği incelenmiştir.

Araştırma Sorusu

Çalışmanın "ana araştırma sorusu"nu konvansiyonel terör saldırılarında uygulanan hukuk kurallarının siber saldırılara uygulanıp uygulanamayacağı oluşturmaktadır. Söz konusu bağlamda siber uzayda iki farklı hipotez ortaya çıkmaktadır. Bunların ilkini halihazırda mevcut uluslararası normların siber saldırılara uygulanabileceği ancak siber alana ilişkin mahsus özellikler dolayısıyla söz konusu normlara eklemeler yapılması gerektiği oluşturmaktadır. Çalışmada ortaya çıkan ikinci hipotez ise dünya üzerinde siber saldırılara özgü herhangi bir düzenleyici metnin ve ortak bir siber suç tanımına sahip olmamanın getirisiyle siber uzaya özgü kuralları düzenleyen yeni bir sözleşme veya sair düzenlemenin hayata geçirilebilir olmasıdır. Bu çalışmada ilk hipoteze ilişkin olarak mevcut normların siber uzay için eksiklikleri tartışılmış ve ikinci hipotez çerçevesinde siber alana uygulanacak yeni bir sözleşme veya uluslararası anlaşmanın taşıması gereken hususlar ve devletlerin gerçekleştirmesi gereken mevzuat uyum çalışmaları ele alınmıştır.

Söz konusu problem ve araştırma sorusu idarenin klasik terörizmle ilgili zararlardan dolayı kusursuz sorumluluğuna gidilebilen ulusal mevzuatımız incelenmiş ve bu mevzuatın siber terörizme uygulanması bakımından değerlendirmelerde bulunulmuştur. Bu kapsamda idarelerin terör ve terörle mücadelen doğan zararlara ilişkin tazminat sorumluluğu kusursuz sorumluluk çerçevesinde incelenmiştir. Kusursuz sorumluluk bağlamında gündeme gelen terör olayları, toplumsal çatışmalar ve tehlikeli faaliyetler idare hukuku kapsamında sosyal risk ilkesi çerçevesinde idarelerin tazminat sorumluluğunu doğurduğu göz önüne alınarak siber uzaya ilişkin kıyaslama yapılmıştır. Sosyal risk ilkesi çerçevesinde Danıştay kararları temel alınarak devletin idari işlem, eylem ve faaliyetlerini yürüten idarenin vatandaşlara tazminat ödemesi gerekliliği çalışmada tartışma konusu yapılmıştır.

Bununla birlikte çalışmanın ilk bölümünde siber ve siber terörizm kavramları ulusal ve uluslararası yaklaşımlar çerçevesinde incelenmiş, siber terörizme yakın kavramlar bu bağlamda kazandıkları anlamlarla açıklanmıştır. Çalışmanın ikinci bölümünde genel olarak siber saldırı türleri üzerine yoğunlaşılmış, siber uzayda gelişen teknolojilerle beraber günümüze kadar uzanan güncel saldırı türleri ayrıntılı şekilde ele alınmıştır. Söz konusu siber saldırı türleri teknik donanımları bakımından kötü amaçlı yazılımlar içeren siber saldırılar, ağ ve sistemlerin hedeflendiği siber saldırılar ve insan hatası kaynaklı siber saldırılar çerçevesinde üçlü bir sınıflandırmaya tabi tutulmuş, bu türler dışında dördüncü bir grupta söz konusu siber saldırılarda kullanılan diğer yöntemlere de yer verilmiştir. Bahse konu saldırıların bilgisayar ve bilişim sistemleri üzerinde bıraktıkları etkilere değinilerek kritik altyapıları etkilemeleri bakımından uluslararası ölçekte siber saldırı örnekleri ortaya konmuştur.

Üçüncü bölüm çerçevesinde siber terörizmle mücadelede siber güvenliğe ilişkin yaklaşımlar ele alınarak bilgi güvenliğinin unsurları açıklanmıştır. Bununla beraber siber terörizmle mücadele kapsamında uluslararası hukuki yapı, kurum ve kuruluşlar nezdinde değerlendirilmiştir. Bu kapsamda siber terörizmden doğan zararların karşılanmasına dair kıyasen uygulanabilecek uluslararası belgeler tartışılmıştır. Söz konusu kısımda savaş ve çatışmalar hukuku göz önünde bulundurulmuş, bu sebeple öncelikle Kuzey Atlantik Anlaşması Örgütü (NATO) bünyesinde yayımlanan NATO Anlaşması, ilerleyen bölümlerde ise başta Birleşmiş Milletler Şartı ve uzmanlar grubunun çalışmaları olmak üzere çeşitli belgeler incelenmiştir. Birleşmiş Milletler kapsamında Bilgi ve İletişim Teknolojilerinin Suç Amaçlı Kullanımının Önlenmesine İlişkin Kapsamlı Uluslararası Sözleşme incelenerek siberle ilgili, siberle kolaylaşan ve siberin araç olarak kullanıldığı suç tiplerinin ulusal mevzuatımız kapsamında uyumlaştırılmasına ilişkin gerekler ortaya konmuştur. Bilgi ve iletişim teknolojilerinin farklı siber saldırı türlerine vücut vermesi dolayısıyla ortaya çıkan kritik altyapı saldırılarına yönelik uygulanabilecek uluslararası düzenleme maddeleri mercek altına alınmıştır. Bu kapsamda devletlerin siber saldırılara karşı devlet egemenliği ve toprak bütünlüğü doğrultusunda iç işlerine karışmama ilkesinin uygulanması gündeme gelmektedir. Siber saldırılar nezdinde silahlı saldırı eşiğinin belirlenmesi ve devletler nezdinde meşru müdafaa hakkının kullanılabilmesi amacıyla siber uzama uygulanabilecek anlaşma, resmî belge ve sözleşmeler de yine bu bölüm kapsamında ele alınmıştır.

Çalışmanın son bölümünde idare hukuku bağlamında sorumluluk kavramı ele alınmış, ülkemizdeki yasal mevzuat kapsamında idarenin kusurlu ve kusursuz sorumluluğu incelenmiş, idare hukukunda sosyal risk ilkesi etrafında şekillenen terörle mücadeleden doğan zararlara ilişkin tazmin yükümlülüğü siber saldırılar çerçevesinde ele alınmıştır.

Sonuç ve öneriler bölümünde ise gerçekleşebilecek siber saldırılar dolayısıyla ülkemizdeki meri mevzuat kapsamında idare hukukunda terörle mücadeleden doğan zararlara ilişkin idarenin sorumluluğu, vatandaşların hak kaybı ve menfaat ihlalleri siber uzam bağlamında ele alınarak mevcut kanun boşluğunun doldurulması çerçevesinde ülkemiz için hukuki önceliklerin neler olabileceği değerlendirilmiştir. Bilgi ve iletişim teknolojilerinin gelişmesi ile beraber günümüzde sıklıkla karşılaşılan ve vatandaşların çeşitli zararlara uğradığı siber saldırılara ilişkin kanun boşluğu dolayısıyla gerekli mevzuat çalışmalarının yürütülmesi hususu vurgulanmıştır. Söz konusu kısımda Avrupa Birliği kapsamındaki siber güvenlik düzenlemeleri, Amerika Birleşik Devletleri ve Çin Halk Cumhuriyeti tarafından uygulanan kanunlar, kritik altyapılara ilişkin belirli düzeyde kritiklik içeren altyapılara ilişkin mevzuatımızın NIS2 direktifi, AB Direktifleri, Birleşmiş Milletler, Avrupa Güvenlik ve İşbirliği Teşkilatı, NATO ve Uluslararası Telekomünikasyon Birliği düzenlemeleri ile uyumlaştırılması, Avrupa Birliği Siber Dayanıklılık Yasası kapsamında ağa bağlanabilen dijital ürünlerin siber güvenliği bakımından sertifikalandırma ve standardizasyon çalışmaları, CER Direktifi çerçevesinde kritik varlık ve tesislerin korunmasına ilişkin mevzuatın incelenmesi, ülkemizde hayata geçirilmesi önerilen kritik altyapı kurum ve bilgi ağı organizasyonu, kurumsal ağlara ve ikili iş birliklerine vücut veren anlaşmalar, meri mevzuatımız kapsamında idarenin kusursuz sorumluluğu çerçevesinde gidilebilen sosyal risk ilkesinin, siber saldırılar neticesinde karşılaşılan çeşitli zarar türlerine de uygulanması ve mevcut kanun boşluğunun doldurulması bakımından kanun koyucuya yol gösterici hususlar ortaya konulmak istenmiştir.

1. SİBER TERÖRİZM ve TARİHSEL GELİŞİMİ

Bilgi ve iletişim teknolojilerinin gelişip yeni dünya düzeninin sanal ortama taşınmasıyla beraber siber saldırı ve siber terörizm kavramları ortaya çıkmıştır. Bu çerçevede hibrit savaşlar meydana getirilerek konvansiyonel savaşlardan siber savaşlara doğru bir devinim ve dönüşüm gerçekleşmiştir. Bu dönüşüm beraberinde yeni bir terminolojiyi doğurmuştur. Modernleşen dünyada teknolojiye bağımlı hale gelen toplumlarda siber terörizm, siyasi, sosyal, ekonomik ve idari boyutlarına bakıldığında görmezden gelinemeyecek bir statüdedir. Söz konusu terminoloji içerisinde gelişen kavramlar siber uzay kavramı altında kümelenmiştir. Her birinin ayrı bağlamları olsa da ortak bir siber uzay kavramı altında birleşmişlerdir. Bu terminoloji etrafında şekillenen siber terörizm, devletler ve vatandaşlar için kritik öneme sahiptir. Öyle ki klasik terörizm unsurları, yaşadığımız yüzyılda siber saldırı araçları ile desteklenmekte ve siber terörizm ortaya çıkmaktadır.

1.1. Siber Terörizm

Siber terörizme ilişkin uluslararası siber güvenlik literatüründe birçok tanım bulunmaktadır. İnternet teknolojilerinin gelişmesiyle son zamanlardaki tanımlar farklı bir yöne evrilmiştir. Bu kapsamda internet ve ağ teknolojileri kullanılarak terörizme yol açan siber saldırıları içerisinde barındıran "*bir terör örgütüne mensup veya ilintili kişi veya kişiler tarafından ağ (internet) teknolojileri kullanılmak suretiyle siyasi bir amaca ulaşmak maksadıyla girişilen her türlü suç teşkil eden şiddet eylemi, faaliyeti veya planlaması*" tanımı yaygınlık kazanmıştır (İç İşleri Bakanlığı, 2024). Uluslararası literatürde ise genel olarak kullanılan tanımda siber terörizm, "*devletleri veya vatandaşları korkutmak ve baskı altına alarak politik ya da sosyal amaçların gerçekleştirilmesi için, bilgisayar, internet veya depolama aygıtlarındaki bilgilere yönelik bilgisayar yahut bilgisayar sistemleri aracılığıyla ortaya çıkan yasal olmayan saldırılar"* olarak nitelendirilmiştir. Siber terörizm bunun yanı sıra yalan haber yayma, siyasi görüşlerin radikal savunuculuğu, toplumları kontrol etme, terörizmin finansmanı ve teröristler tarafından internette yürütülen diğer faaliyetleri tanımlamak için de kullanılmıştır. Bazı görüşlere göre siber terörizmin esas unsuru önemli derecede fiziksel hasar gerektirdiği için internet aracılığıyla siyasi propagandada bulunmak

siber terörizm olarak tanımlanamaz. Söz konusu propagandanın ancak hacktivizm olarak nitelendirilebileceği ifade edilmiştir (Alexander, 2014). Öyle ki bu görüşe göre internet korsanları siyasi ve sosyal konularda iletmek istedikleri mesajları yalnızca hedef kitleye iletmek maksadıyla internet sitelerine yahut bilgisayar ağlarına yönelik saldırı faaliyetleri gerçekleştirmektedir. Hacktivizm kapsamında saldırıyı gerçekleştiren süjeler, kişilerin özel ve hassas bilgilerini kullanarak zafiyetleri ortaya çıkarmak, bilgileri ele geçirmek veya kullanılamayacak duruma sokmak saikiyle iletmek istedikleri mesajları siber saldırılar aracılığıyla hedef kitlelere göndermektedir (First Line Practitioners, 2024).

Siber terörizm tanımının anlaşılabilmesi için söz konusu tanımda kullanılacak olan kriterler büyük önem arz etmektedir. Bu kriterlerin başlıcaları bilgi teknolojilerinin kullanılması, siber eylemi gerçekleştiren kişinin kimliği ve kimlik bilgilerinden ortaya çıkarılması istenen sonuçtur. Sayılan unsurlar etrafında şekillenen çeşitli siber terörizm tanımları bulunmaktadır. Tanımların içerikleri incelendiğinde ise fikir uyuşmazlıkları ve algısal farklılıklar oluştuğu görülmektedir (Shamsuddin, 2003). Bu konudaki fikir ayrılığının giderilmesi açısından söz konusu kavramı oluşturan "siber" ve "terörizm" terimlerinin muğlak alandan çıkarılması faydalı olacaktır (Nasrat, 2015).

Siber terörizmin tanımlanmasındaki ana unsur olan "siber" teriminin kökü, etimolojik olarak yardım etmek, yönlendirmek, kontrol etmek anlamlarına gelen eski Yunancadaki "kybereo" (κυβερεω) kelimesinden gelmektedir (Oxford University, 2015). Aynı kökten gelen sibernetik (cybernetics) kelimesi ise sinir sistemi gibi otomatik hakimiyet sistemleri etrafında kontrol ve iletişim kuramının yer aldığı bilim dalı olarak tanımlanmıştır (Helvacıoğlu, 2004). Siber terimine ilişkin en önemli tanımlardan birisi Birleşmiş Milletler (BM) tarafından yapılmıştır. Bu tanıma göre siber; "*internete bağlı bilgisayarların, iletişim altyapılarının, çevrimiçi iletişim yapan kişilerin, veri tabanı ve bilgi sistem araçlarının oluşturduğu küresel bir sistem*" olarak nitelenmiştir (Andress ve Winterfeld, 2011). Amerika Birleşik Devletleri (ABD) Ticaret Bakanlığı Ulusal Standartlar ve Teknoloji Enstitüsü (The US Department of Commerce's National Institute of Standards and Technology-NIST) tarafından yapılan tanım ise "*hem bilgi hem de iletişim ağlarını ifade eden olgu*" şeklindedir (NIST, 2015). Bu tanımda öne çıkan unsur, bilgi ağlarının yanı sıra iletişim ağlarının da siber terörizm nitelemesine dahil edilmesidir. 2012 yılında İsviçre'de yapılan World Economic Forum'da (WEF) siber teriminin kapsama alanına kritik endüstrilerdeki internet, bilgisayar

sistemleri, telekomünikasyon ağları, gömülü işlemciler ve denetleyicilerini de aldığı, bu terimin bilgi teknolojisi altyapılarının birbirine bağlı ağını temsil ettiği ifade edilmiştir (World Economic Forum, 2012).

Flutter'e (2018) göre siber kelimesi kapsadığı anlamlar dolayısıyla genel bir terim olarak nitelendirilmiş ve bu ön ek yerine farklı kavramlar ortaya atılmıştır. Bunlardan bazıları "bilgisayar ağı operasyonları", "bilgi operasyonları" ve "bilgi harbi"dir. Flatter (2018), ortaya attığı yeni kavramların teknolojiyle ilişkili suçları tanımlamada daha etkili olacağını ifade etmiştir (Flutter, 2018). Yine bu görüşlerde söz konusu tanımın teknolojik bileşenler altında kategorize edilmesinin konuyu farklı bir noktaya taşıyarak bağlamından uzaklaştırdığını iddia etmiştir (Jantunen ve diğer., 2018). Bunun aksine söz konusu yaklaşımı benimseyerek siber terörizm tanımlarında kullanan akademisyenler de bulunmaktadır (Conway, 2014; Denning, 2006). Correia'ya (2022) göre ise siber ön ekin teknolojik bileşenler altında tanımlanması yaklaşımı, teknolojinin askeri alanı ve teröre ilişkin propagandaların yayılımını dışarıda bırakması sebebiyle kısıtlı bir bağlam sunmaktadır. Bu yaklaşım beraber konvansiyonel suçlarla teknolojinin getirdiği yeni suçlar farklı gruplarda kategorize edildiği ve terör faaliyetlerine ilişkin türleri göz ardı ettiği için eleştirilmiştir. Söz konusu bağlamda değerlendirme yapıldığında toplumlar üzerinde büyük etkiye sahip olan terörizm ve teknoloji kavramlarının birbirine sıkı şekilde bağlı olan ilişkisi reddedilmiş olmaktadır. Correia (2022) bu sebeplerle konvansiyonel terörizm ile siber terörizm kavramları arasında farkı ortaya koymak için kullanılan siber ön ekinin tanımlamalarda kullanılmasını önermektedir (Correia, 2022).

1.2. Terör, Terörizm ve Siber Terörizm İlişkisi

Terör kelimesi köken olarak korkutmak ve yıldırmak anlamlarını karşılamakla beraber Latince'de "*terrere*" sözcüğünden gelmektedir. Terörizme ilişkin bir tanıma ulaşmak için etkileşimli ve belirli politik bir amaca yönelik terör olayları dizisine ihtiyaç bulunmaktadır (Doğrul ve diğer., 2011). Terör terimine ekleme yapılarak oluşturulan terörizm terimiyle sistematik bir yapıda terörizme yol açan eylemlerin politik hedeflere veya bu eylemlere yönelik düşüncelerin icrai olarak harekete geçmesine atıfta bulunulması söz konusu olmaktadır. Diğer bir deyişle terörün kapsamı şiddet vasıtasıyla halkta oluşturulan

korku ve şiddet eylemi iken terörizm politik hedefler için örgütlü, daimî ve sistematik araç olarak kullanılan teröre yönelik eylemleri kapsamı içine almaktadır. Terörizm, şiddetle oluşturulan korku ve panik ortamını meydana getiren süreç olarak nitelendirilirken, terör halk arasında korku ve panik yaratmaya ilişkin çatı bir kavramı ifade etmektedir. Buna binaen teröristler ise, terörizmi hayat döngüsüne yerleştirerek terör eylemlerini meydana getiren saldırganlar olarak nitelenebilecektir (Sağıroğlu ve Alkan, 2018).

ABD Savunma Bakanlığı (The US Department of Defense) tarafından yayınlanan ulusal sözlükte terör; "*politik, dini veya ideolojik amaçları olan hükümetleri veya toplumları zorlamak veya korkutmak için yasa dışı şiddetin bilinçli şekilde kullanımı veya yasa dışı şiddet tehdidi*" olarak kullanılmıştır. Federal Soruşturma Bürosu (FBI) tarafından yapılan tanım da bu tanımla paralel şekilde düzenlenmiştir (Department of Emedrgency and Military Affairs, 2024). 2001 yılında yayımlanan "Terörizmi Durdurmak ve Engellemek İçin Gerekli Uygun Araçları Sağlayarak Amerika'yı Birleştirme ve Güçlendirme Yasası (The USA Patriot Act)" bağlamında terör faaliyetleri içerisinde ulaşım araçlarının kaçırılması, tehdit aracı olarak kullanılması ve komplo kurulması fiillerine yer verilmiştir. "Korunan" olarak nitelenen varlıklara karşı şiddet eylemlerine teşebbüs ve kamu güvenliğini tehdit edici şekilde veya önemli ölçüde mala zarar vermek amacıyla silah ve tehlikeli aygıt kullanımı şeklinde faaliyetlerin olmasının bir davranışın terör eylemi olarak nitelendirilmesinde ana faktör olduğu belirtilmiştir (USA Patriot Act, 2001). Terör eylemlerinin genel olarak bir toplumda yerleşik olan siyasi düşünceye karşı mevcut statükoyu devirme ve bunun için toplum üzerinde korku ve panik yaratma amacı içerdiğini göz önünde bulundurmak terörün anlaşılmasında faydalı olacaktır. Ülkemizde teröre ilişkin mevzuatlarda yapılan tanımlara bakıldığında 3713 sayılı "Terörle Mücadele Kanunu"nun ilk maddesinde terörün "*cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir.*" şeklinde tanımlandığı görülmektedir (Terörle Mücadele Kanunu, 1991).

Söz konusu tanımlar çerçevesinde genelleme yapıldığında terörizm kavramı, toplumda korku yaratarak paniğe sürüklemek şeklinde nitelendirilebilir. Bozdemir (1981) terörizmi: "*Terörizm, siyasi amaçlar için, örgütlü, sistemli ve sürekli terör kullanımını içeren bir yöntemle kendini tanımlayan stratejik bir yaklaşım*" şeklinde tanımlamaktadır (Bozdemir, 1981). Bu tanıma benzer şekilde Denning'e (2000) göre terörizm: "*bir kişi veya organize bir grubun, toplumları veya hükümetleri sindirmek veya zorlamak amacıyla, genellikle ideolojik veya politik nedenlerle insanlara veya mülke karşı yasadışı güç veya şiddet kullanma tehdidi*" olarak nitelendirilmiştir (Denning, 2000).

Siber terörizmin terörizmle olan ilişkisini anlayabilmek için öncelikle terörizmin unsurlarını ortaya çıkarmak büyük bir önem arz etmektedir. Terörizmin tanımlanmasında da aynı siber terörizmde olduğu gibi siber güvenlik bağlamında yer alan paydaşlar arasında çeşitli ihtilaflar yaşanmıştır. Toplumların savaşa karşı bakış açıları, bağımsızlık mücadeleleri, örf ve ananeleri, ideolojik, siyasi ve dinsel olarak yaşam tarzlarının farklı yapıda olması, üzerinde fikir birliği olan yeknesak bir terörizm tanımının belirlenememesine yol açmıştır. Terörün tanımı, bu nitelendirmeyi yapan kişiler veya topluma göre şekillendiği için terörizm toplumsal bir unsur olarak kabul edilmektedir (Anderson, 2013). Enders ve Sandler'e (2012) göre terörizm, savaşla ilgisi olmayan toplumun geniş kesimlerini korkutmak vasıtasıyla politik ve toplumsal kitleleri hedef alan kişi veya gruplar tarafından eyleme geçmeden önce tasarlanmış şiddet gösterisi yahut tehdididir (Enders ve Sandler, 2012).

Terörizmin yapısal olarak iki temel unsur üzerinde inşa edildiği görülmektedir. Bunlardan ilki şiddet unsuru, diğeri ise politik ve sosyal sebep unsurudur (Sandler, 2015). Terörizm faaliyeti içerisindeki saldırganlar, terörizme yol açan taleplerini yerine getirtmek veya ulaşmaya çalıştıkları hedefleri elde etmek için toplumda korku ve panik oluşturup insanlık dışı eylemlerle siyasi değişimi amaçlayabilmektedir. Terörizme ilişkin hazırlanan kampanyalar, meşruiyeti sağlamak adına kanunlarla vatandaşlarının temel haklarını ve kamu güvenliğini sağlamakla yükümlü kılınmış hükümetlerde çok daha fazla görülmektedir (Eubank ve Weinberg, 1994). Taylor ve Hewer, terörizme ilişkin yaptıkları nitelemede bu kavramı hükümetlerin vatandaşları üzerinde uyguladıkları cebri davranış ve uygulamaları meşrulaştırmak için kullandıkları belirteç ifadesini kullanmışlardır. Dünya üzerinde doğu ve batı olarak kutuplaşan devletlere bakıldığında terörizme bakış açıları arasında farklılar

olduğu görülecektir. Öyle ki Ortadoğu'da seküler sayılamayacak dini görüşlerle siyaset arasındaki ilişkiye bakıldığında toplumun normlarını etkileyen bir yapı olduğu görülmektedir. Buna rağmen Batı'ya bakıldığında dini inanışlarla politika arasında sert bir ayrım olduğu ve demokratik bir düzenin olduğu değerlendirilmektedir (Correia, 2022). Bu iki kutbun mevcut inanç ve ideolojileri terör kavramına ilişkin farklı bakış açılarına sahip olmalarına neden olmaktadır (Nikfar, 2020). Aynı zamanda tek bir terör kavramı üzerinde uzlaşının da bu kutupları hassasiyet duydukları yapılar nedeniyle rahatsız edebilecektir. Terör eylemi olarak kabul edilen fiiller ve davranış biçimleri bu noktada farklı olabilmektedir (Correia, 2022). Örneğin Birleşik Krallık'ta mukim olmayan ve terör faaliyetinde bulunan kişilerin, mahkeme tarafından kovuşturmasının çeşitli problemlere yol açabileceği görüşü bulunmaktadır. Söz konusu farklılıklardan dolayı şiddet ve kesinti fiillerinin Birleşik Krallık'taki siber güçler tarafından kolaylıkla işlenebileceği göz önüne alındığında bu problemlerin daha da arttığı görülmektedir. Birleşik Krallık'taki meri mevzuata bakıldığında 2006 Terörizm Yasası (Terrorism Act) ve 2008 Terörle Mücadele Yasası (Counter-Terrorism Act) terörizmle ilişkili yasal olmayan faaliyetleri ayrıntılı şekilde ortaya koyan mevzuatlar olarak ön plana çıkmaktadır. 2006 yılındaki ilk düzenlemede terörizm "*halkı ve/veya mülkiyeti sindirmek veya siyasi yahut dini ideolojileri ilerletmek için halka ve/veya mülkiyete karşı bir şiddet eylemi ya da tehdidi*" şeklinde tanımlanmıştır (United Kingdom Government, 2006; United Kingdom Government, 2008). Söz konusu tanımın eleştirildiği nokta, terörizm içeren eylemlerin hangi fiillerle işlenildiği ve kanunilik ilkesi üzerindeki etkisinin muğlak olmasıdır. Bu muğlaklık terörist davranışlarda bulunan faillerin işledikleri fiillerin kanunda suç olarak tanımlandığının farkına varılamayacağı noktasında olumsuz şekilde yorumlanmaktadır. Ancak tanım belirsiz olsa dahi siber terörizm tanımında bu nitelendirmenin etkili olduğu ve mevcut durumda meşru olan bir mevzuata uygun olmasının önem arz ettiği değerlendirilmektedir (Correia, 2022).

Söz konusu terörizm tanımlamalarında ön planda tutulan beş özellikten bahsedilmektedir. Bunların ilki cebir yani zor kullanma, ikincisi politik hedef, üçüncüsü terörün köken olarak ifade ettiği korku salma, dördüncüsü tehdit etme ve sonuncusu kamuoyu üzerinde veya üçüncü kişilerde uyandırılan psikolojik etkidir (Nasrat, 2015). Ergil (2014) bu özellikleri dikkate alarak terörizme dair şu şekilde bir tanım yapmıştır: "*saldırıların yöneltildiği hedeflerden daha büyük bir kitleyi, korkutulan sivil ve masum kurbanlar aracılığı ile yıldırıp, korkutarak, yasa-dışı stratejik ve siyasal amaçlarını*

gerçekleştirmek için bir grubun veya devletin, bilinçli ve planlı bir biçimde şiddet kullanması veya şiddet kullanma tehdidinde bulunmasıdır" (Ergil, 2014). Marie-Helen isimli ceza hukukçusuna göre terörizm; "*ideolojik, dini veya siyasi nedenlerle bir hükümeti korkutmak veya baskı altına almak amacıyla kritik altyapı sistemlerine (örneğin, su, enerji, iletişim) saldırı düzenlemesi.*" olarak nitelenmektedir (Maras, 2012). Araştırmacı Rod Stork'a (1999) göre ise terörizme ilişkin tanım şöyle olmalıdır: "*devlet veya devlet destekli gruplar tarafından gerçekleşen ve halk arasında korku yaratmak amacıyla askeri ve sivil mallara zarar vermek*." (Stark, 1999). Bu tanımda, toplumda korku ve panik yaratmanın terörizm için olmazsa olmaz unsur olduğu vurgulanmaktadır. Diğer dikkat edilecek unsur ise askeri mal kavramına bu tanımda yer verilmesidir.

Siber terörizmin geçmişinin çok eski olmaması ve niteliği itibariyle farklı bileşenleri bünyesinde barındırması sebebiyle evrensel olarak kabul edilen uluslararası bir siber terörizm tanımı bulunmamaktadır. Ancak bazı devlet ve toplumlar çeşitli tanımlar üzerinde fikir birliğine varmıştır. Yine de bu fikir birliği karşılaşılan bazı somut olaylarda fikir ayrılığına dönüşebilmektedir. Öyle ki somut olaylar özelinde bu tanımın uygulanabilmesi konusunda ihtilaflar ortaya çıkabilmektedir. Bu sebeple siber terörizme ilişkin tanımlarda farklı görüşlerin değerlendirilmesi gerekmektedir (Doğrul ve diğer., 2011).

Siber terörizm anlamsal ve yapısal olarak farklı şekillerde tanımlanmıştır. Bazı yazarlara göre siber terörizm yalnızca bir yöntem olarak tanımlanmakta veya teröristlerce hedeflere yönelik olarak kullanılan saldırı aracı olarak nitelendirilmektedir. Diğer bazı yazarlar ise siber terörizmi terörizmin bir çeşidi olarak sınıflandırmaktadır. Bu sınıflandırmanın ilkinde saldırı yahut hedefe yönelik siber terörizm oluşurken ikincisinde siber terörizm araç olarak kullanıldığı şekliyle karşımıza çıkmaktadır. Conway'a göre, siber terörizm "*internet kullanılarak ve/veya internet altyapılarına karşı gerçekleştirilen terör eylemleri*" olarak tanımlamaktadır. Denning (2000), siber terörizmi "*terörizm ve siber uzayın yakınlaşması*" şeklinde tanımlamaktadır (Cassim, 2012). Buradan anlaşılması gereken siber terör fiillerinin politik veya sosyal amaçlarla planlanan şekilde hayata geçirilebilmesi için hükümetleri ve toplumu panikletmek saikiyle yapıldığında bilgisayarlara, bilgisayar ağlarına ve sistemlerdeki bilgilere yönelik yasal olmayan saldırılar ve saldırı tehditleri olduğudur. Buna ek olarak siber terörizme örnek verilen olaylara bakıldığında büyük yıkım yaratan patlamalar, ekonomik zayiat, ulaşımın aksatılması, kişilerin vücut bütünlüğüne verilen

zararlar ile vatandaşların temel ihtiyaç kaynaklarına yönelik saldırılar dikkat çekmektedir. Bunların en önemlileri arasında kritik altyapılar ve devletlere ait kritik tesisler sayılmaktadır (Nasrat, 2015). Denning (2000), teröristlerin konvansiyonel yöntemlerle şehirlere saldırılar düzenlemesi gibi terörizm biçimlerini uygulanabilir hale sokmak amacıyla da siber uzaydan faydalanabileceklerini veya mesajlarını kamuoyuna yayarak onlara destek veren terör yanlısı kişileri işe almak için interneti kullanabileceklerini söylemektedir (Cassim, 2012).

Pollit (2013), siber terörizm kavramını "*bilgiye, bilgisayar sistemlerine, bilgisayar programlarına ve verilere karşı, alt ulusal gruplar veya gizli ajanlar tarafından savaşçı olmayan hedeflere karşı şiddetle sonuçlanan önceden tasarlanmış, politik olarak motive edilmiş saldırı*" olarak tanımlamaktadır (Pollitt, 2013). Bu tanıma göre meydana getirilen saldırılar fiziksel, bedensel zararlara hatta ölüme dahi yol açabilmektedir. Örneğin kritik altyapılara yönelik siber saldırılar nükleer patlamalara, uçak ve tren gibi ulaşım araçlarında kazalara, su kütlelerindeki ciddi kirliliklere, elektronik altyapıda ve iletişimde enterferansa, büyük miktarlı ekonomik kayıplara neden olabilmektedir (Cassim, 2012). Burada dikkat edilecek diğer unsurlar ise şiddet ve gizli ajan unsurları ile önceden tasarlanmış planlı fiillerin hayata geçirilmesi unsurudur (Nasrat, 2015).

Siber terörizm bu örneklerde belirtildiği üzere devletlerin ulusal güvenliklerine ilişkin kurum, kuruluş ve kritik altyapı sektöründe hizmet veren özel sektöre yönelerek vatandaşların yaşam standartlarını düşüren saldırıları kapsamaktadır. Saldırıların hedefi kamuoyunda ve toplum nezdinde terör ve panik havası oluşturmaktır. Teröristler bunun yanı sıra suç işlemede araç olarak bilgi teknolojilerini kullanmakta, planlama, finans, lojistik ve istihbarat girişimleri için siber uzaydaki muğlaklıktan faydalanmaktadır. Söz konusu metotlarla teröristler, örgütsel amaçlarını güvenceye almak için bilgisayar teknolojisini kullanmaktadır. Buna rağmen siber saldırılar hizmetleri aksatması veya finansal açıdan sorun yaratması durumunda siber terörizm kapsamında değerlendirilmemektedir (Cassim, 2012). Siber terörizm kavramına ilişkin söz konusu nitelendirmeler konvansiyonel terörizm tanımı ekseninde gelişerek bir devletin, toplumun yahut kuruluşun siyasi, demografik veya finansal işleyişini bozma, toplumdaki fiziksel şiddet eylemlerinin etkisini propagandalarla artırma ve toplumu isyana sürükleme faaliyetlerini içerisinde bulundurmaktadır (Foltz, 2004)

Siber terörizm terimi çerçevesinde doktrinde iki farklı görüş savunulmaktadır. İlkinde siber terörizmin tehlike yaratma kapasitesinin ciddi tehditlere yol açmayacağı savunulurken, ikinci savunulan görüşe göre bu alanın terörizmin yeni görünümü olduğu ve devletlerin kritik altyapılarına zarar verebilecek fiziksel hasara yol açabilecek potansiyele sahip olduğu ifade edilmektedir (Nasrat, 2015). Holt'a (2012) göre siber terörizm terör eylemine neden olan davranışı kapsayarak fiziksel hasarı dışarıda bırakmalıdır (Holt, 2012). Söz konusu tanımlar geniş anlamlarıyla fiziksel etkileri kapsam dışında bırakarak söz konusu eylemlerin gerçekleştirilmesine ilişkin motivasyon ve saiklere odaklanmaktadır (Correia, 2022). Bu tanımların karşısında yer alan görüşe göre ise farklı bir yaklaşım benimsenerek siber terörizme ilişkin eylemlerin bilgisayar veya bilgisayar ağlarına yönelik fiziksel veya enterferansa neden olan etkisinin bulunması gerekliliği ifade edilmiştir (Holt, 2012; Denning, 2006). Gordon ve Ford (2002) ise siber terörizmi Denning'in önerdiği şekliyle tanımlamışlardır. Bu çerçevede teknolojik gelişmeler günden güne ilerledikçe ve insanlar tarafından çok daha erişilebilir bir boyuta ulaştıkça siber terörizmi Denning'in (2006) tanımladığı şekilde ele almanın kamu güvenliği ve kamu düzeni için tehlike oluşturduğu değerlendirilmektedir. Bu tanımlarla birlikte ulusal kolluk birimlerinin siber terörizme neden olan eylemleri tespit etme, soruşturma ve engelleme konusunda yanlış yönde yaklaşım benimsemesine neden olunabilecektir (Correia, 2022). Birleşik Krallık'ta siber terörizme ilişkin yapılan yasal tanımda diğer tanımlardan daha uyumlu bir yaklaşım benimsenmeye çalışılmıştır. Bu bağlamda ikili araç sınıflandırılması göz önünde tutularak şu tanım oluşmuştur: "*siber terörizm, halka karşı siyasi, sosyal veya dini ideolojileri ilerletmeyi amaçlayan siber etkin faaliyetleri ve ayrıca halka, mülklere ve/veya sistemlere yönelik zararı tehdit etmeyi veya kolaylaştırmayı amaçlayan siber bağımlı faaliyetler*". Bu tanım doğrultusunda siber terörizmin geleneksel terörizmle çakışma potansiyeline sahip olduğu değerlendirilmektedir (Shamsuddin, 2003). Söz konusu tanımda diğer tanımlara kıyasla daha sade ve netlik içeren öğeler kullanılmaya çalışılmıştır. Bu doğrultuda siber terörizm alanında yer alan çeşitli süjeler söz konusu tanımda fikir birliği sağlayarak bu yaklaşımı benimsemişlerdir. Bu tanımdaki amaç, sektörde faaliyet gösteren paydaşların siber terörizme karşı mücadelesinde, tehditleri tespit etmesi ve engellemesinde yol gösterici olmaktır (Correia, 2022). Yine söz konusu tanımlamalar doğrultusunda sonuç olarak ortaya çıkan husus uluslararası boyutta siber terörizm ile ilgili yaklaşım farklılıkları olduğu ve ortak bir siber terörizm kavramı üzerinde uzlaşma sağlanamadığıdır (Nasrat, 2015).

Bu kavram üzerine yapılan bazı tanımlarda öncekilerden farklı olarak bilgisayar sistemleri ana unsur olarak yer almaktadır. Bunlardan birisi de FBI tarafından yapılan "*siyasi, sosyal ya da ideolojik programlarını onaylatmak için bir hükümet veya halkı etkilemek amacıyla şiddet, yıkım ve/veya hizmetleri kesmekle halk içinde karışıklık ve belirsizliğe neden olan olarak korku yaratan bilgisayar ve telekomünikasyon gücü kullanarak işlenen bir suç*" tanımıdır (U.S. Army Training and Doctrine Command, 2005). Burada göze çarpan unsurlar belirli bir hedefe yönelik olarak korku yaratma maksatlı hareketlerdir. Tereshchenko (2013), siber terör tanımını "*büyük ölçekli yıkım, cinayet veya hak ihlali amacıyla, bilgi teknolojisi kullanımı yoluyla bir ülke ve halkına korku yaratarak, gerçekleştirilen kasıtlı bir eylem*" şeklinde yapmıştır (Tereshchenko, 2013). Dikkat edilmesi gereken ana unsurun fiilin işlenmesinde iradilik içeren kast öğesi olduğu vurgulanmıştır. Söz konusu tanım değerlendirildiğinde ceza hukuku bağlamında mefhumu muhalif yorumla siber terörizmin taksirle işlenemeyeceği çıkarımı yapılabilecektir.

Siber terörizme ilişkin sektörde bu denli fazla tanımın bulunması karşısında bunun sebebini araştıran Luiijf (2014) "*kökenlerinin kolluk kuvvetleri, uluslararası çalışmalar, terörle mücadele, bilgi güvenliği gibi oldukça farklı uzmanlık alanlarına dayanması*" şeklinde olayı özetlemektedir (Luiijf, 2014). Yine bu niceliksel sebebiyle bahse konu terimi kullanırken doğru kullanım şekliyle açıklığa kavuşturmanın önemine değinilmiştir (O'Brien, 2021). Siber terörizmin kategorize edilerek yapıldığı tanımlar hangi faaliyetlerin siber terörizm ekseninde değerlendirileceğine ilişkin yaklaşımlar öne sürmektedir. Bu tanımlamaların savunulduğu zamanlar üzerinden belli bir müddet geçtiği için işlevsellik problemi ortaya çıkmıştır. Öyle ki yeni teknolojilerle beraber siber terörizmin amaç ve araç olarak kullanıldığı suçların artmasıyla söz konusu terimin günümüz teknoloji ortamında tanımlanması gerekli olmuştur (Correia, 2022).

Plotnek ve Slay'a (2021) ait olan siber terörizmle ilgili en geniş tanımlardan birisi de: "*siber terörizm, sosyal veya ideolojik hedefler peşinde sivil, hükümet veya hükümet dışı hedefleri korkutmak veya zorlamak için siber uzayı gerçek dünya sonuçlarına neden olmak amacıyla kullanma niyetiyle devlet dışı aktörler tarafından önceden tasarlanmış saldırı veya tehdit"* şeklindedir (Plotnek ve Slay, 2021). Söz konusu saldırıların gerçek dünyadaki sonuçlarının fiziksel, psikolojik, politik, ekonomik, ekolojik veya siber uzamın dışında meydana gelen diğer çıktıları da içerdiği ifade edilmiştir. Tanımda siber terörizme ilişkin

failleri, faillerin suçu işlemedeki motivasyonunu, suç işleme saiklerini, suçta kullanılan araçları, neticenin etki ettiği alanı ve genişliği açıklanmaktadır. Daha önceki tanımlarda ise bu tanımdan farklı olarak siber terörizme yol açan eylemlerin kapsamı doğrultusunda terör davranışlarının etkilediği alan geniş şekilde yorumlanmamıştır (Foltz, 2004; Holt, 2012). Yine daha önce yer tanımlarda yalnızca fiziksel olarak etkisi bulunan davranışlara yer verilmiştir (Cassim, 2012). Ancak bu tanımlardan, siber terörizme ilişkin faaliyetlerin ekonomik ve psikolojik etkisinin olabileceği sonucu da çıkmaktadır. Söz konusu tanımlamada siber terörizmin birçok alan üzerindeki etkisine değinildiği için geniş yorumlandığı söylenebilir (Correia, 2022). Tanımın, Birleşik Krallık Terörizm Yasası'ndaki tanımda ve sonrasında ekleme yapılarak 2006 yılında oluşturulan yeni terörizm tanımıyla uyumsuz olduğu görülmektedir (The Crown Prosecution Service, 2022). Terörizm Yasası kapsamında ilk haliyle terörizm tanımı: "*hükümeti etkilemek, halkı ya da halkın bir bölümünü korkutmak için düzenlenmiş dini veya ideolojik amaçlarla gerçekleştirilen bir hareket veya tehdit*" şeklinde yapılmıştır. 2006 yılında bu tanıma ekleme yapılarak "*ya da bir uluslararası hükümet organizasyonunu etkilemek amacıyla*" şeklinde yeni bir tanım yapılmıştır. Söz konusu tanımlar arasındaki farklılığın ana sebeplerinden biri de konuya yaklaşımdaki farklılıklar ve coğrafi olarak farklı siyasi geçmişlerin olmasıdır. Plotnek ve Slay'nın da Avustralya menşeli bilim insanları olmasından dolayı söz konusu farklılıklar oluşmaktadır (Correia, 2022). Birleşik Krallık'ta bu yasaların üzerine 2008 yılında Terörizmle Mücadele Kanunu (Counter-Terrorism Act) yayımlanmış ve bu Kanunda polisin terör olaylarına karşı yetkileri artırılarak terör eylemleri kapsamında şüpheli olarak sorgulanan şahısların tutukluluk süreleri uzatılmıştır. 2011 yılında Terörizmin Önlenmesi ve Soruşturma Önlemleri Yasası (Terrorism Prevention and Investigation Measures Act) yürürlüğe sokulmuştur (United Kingdom Government, 2011). Bu yasa kapsamında yabancı uyruklu olup terör tehdidi oluşturan kişilerin sınır dışı edilememe ve soruşturmaya tabi tutulamama sorunundan dolayı çeşitli tedbirler alınmıştır. 2015 yılında Terörizmle Mücadele ve Güvenlik Yasası (Counter Terrorism and Security) terörizme açık olan savunmasız kişileri koruyucu bir yapı getirerek güvenlikle ilgili devlet otoriteleri ve makamlarına yükümlülük getirmiştir (United Kingdom Government, 2015). Bu çerçevede "Kanal Programı" adında bir çalışma grubu oluşturularak meşru bir altyapı meydana getirilmiştir. 2019 yılında Terörizmle Mücadele ve Sınır Güvenliği Yasası (Terrorism and Border Security Act) kabul edilerek Birleşik Krallık sınırları dışında terörizm tehdidi içeren bir bölgeye gitme yahut ikamet etme yeni bir suç olarak tanımlanmıştır (United Kingdom

Government, 2019). Burada düzenleme yapılan bir diğer alan da bilgi edinme suçudur. İnternette terörizme ilişkin görüntülerin, yazılı veya sözlü dokümanların kayıt edilme amaçlı olarak indirilmesi yahut aktarılması bu suçun kapsamına alınmıştır. Sonuç olarak son düzenlemeyle konvansiyonel terör siber terörizme doğru bir devinim yaşayarak internet ortamına radikal bir geçiş yaşanmıştır. Bu yolla aktarılan bilgiler, devletlerin ve vatandaşların siber terörizme yönelik saldırılara açık hale gelmesine yol açmaktadır. Aynı zamanda internet ortamında işlenen suçların artmasına da ortam hazırlamaktadır.

1.3. Siber Terörizmin Tarihi Gelişimi ve Teorik Temelleri

"Sibernetik" kelimesinin literatürde ilk kez kullanılması 1948 yılında “Sibernetik” adlı kitabında Norbert Wiener adlı matematikçi bilgin tarafından gerçekleşmiştir (NTNU, 2024) Sibernetik kavramı, Yunanca “κυβερνήτης” yani yönlendirme sanatı, dümenci, pilot ve hükümet kelimeleriyle aynı kökten türemiştir (Tabansky, 2011). 1940’lı yıllara gelindiğinde bilgisayarlar ortaya çıkmış ve sibernetik kelimesi toplum tarafından çok daha fazla duyulmaya başlanmıştır. Bu çerçevede siber terimi de bilgisayara ilişkin güvenlikle ilgili konularda literatüre girmiştir (Dunnigan, 2003). Yirminci yüzyılın ortalarında Norbert Wiener tarafından sibernetik terimi kullanılana kadar olan süreçte siber terimi yapay zekâ içerikli makinelerde ve canlılardaki sistemlerin yapısal olarak çalışmaları olarak nitelendirilmiştir (Wiener, 1948). Siber terimi de sibernetik kelimesinin kısaltılması amacıyla kullanılmıştır (Çakmak ve Altunok, 2009). 1980’li yıllara gelindiğinde, zamanın en popüler romanlarından olan ve yazarlığını William Gibson’ın yaptığı Neuromancer isimli kitaptaki siberpunk düşünce akımı sibere yönelik bakış açısını etkilemiştir. Siberpunk kavramının literatüre girmesiyle bu kültürden de etkilenilerek fütürizm ve distopya terimleri ile bağlantı kurulmuştur. Bu bağlantının çıkış zamanına paralel olarak ABD askeri kuvvetlerinin benimsediği yeni yaklaşımlarda dezenformasyona yönelik savaşlar ve konvansiyonelden sibere yönelen yeni savaş alanlarının ortaya çıktığı görülmüştür (Gibson, 1984). Sibernetik kelimesi, yine 80’li yılların popüler film endüstrisi içerisinde robotik makinelerin yanı sıra biyolojik makineleri de popüler bir duruma sokmuştur. Söz konusu fiziksel oluşumun doğal ve yapay sistemlere sahip olması “siborg” terimini doğurmuştur. Bu terim 80’li yıllarda kullanıldığı anlamda ilk kez 1960 yılında Manfred Clynes tarafından insani özellikleri içeren suni fonksiyonel bir yapı için kullanılmıştır. Biyolojik fonksiyonları

olan "Siborg", teknolojik aletler tarafından yönlendirilen yapay insan-makine yapısını temsil etmiştir (Jose ve Meera, 2015). Bu gelişmeler doğrultusunda "siber terör" terimini ilk kez literatüre sokan kişi ise 1980'lerde Kaliforniya Güvenlik ve İstihbarat Enstitüsü araştırmacısı olan Barry C. Collin'dir. Collin sibernetik ile terörizmi tek potada eriterek ortaklaşa bir tanım yapmak istemiştir. Bu çerçevede yaptığı tanımda "*sibernetik ve terörizmin yakınlaşması*" ifadesini kullanmıştır (O'Brien, 2021). Ancak bu tanım sonrasında siber güvenlik uzmanlarınca üzerinde uzlaşılan bir tanım haline gelmemiştir.

90'lı yıllara gelindiğinde dünya üzerinde yaşanan terör olayları sonucunda siber terörizm çok daha fazla konuşulur hale gelmiştir. Özellikle ABD'nin içinde bulunduğu olaylarda siber terörizm sesli olarak dile getirilmeye başlanmıştır. 1993 yılında ABD'nin New York eyaletinde yer alan Dünya Ticaret Merkezi'ne yönelik saldırı ve yine 1995'te Oklahoma City katliamı siber terörizmin terörizmle ilişkili olduğuna yönelik emareleri çoğaltmıştır. 1997 yılına gelindiğinde ABD Savunma Bakanlığı siber güvenlik alanında iç sistemlerini analiz ederek önceden haber vermeksizin bir tatbikat gerçekleştirmiştir (Soesanto, 2020). Yine aynı sene içerisinde "Marsh Komisyonu Raporu" yayımlanarak kritik altyapılara ilişkin korunma ve caydırıcılık ile siber tehdit ekosistemi ortaya konulmuştur (The White House, 1997). 1998 yılında "ABD Büyükelçilik Saldırıları" olarak adlandırılan Tanzanya ve Kenya'nın başkentleri Darüsselam ile Nairobi'de yer alan ABD büyükelçiliklerine yapılan saldırılar sonrasında siber uzay içerisinde terörizm kavramı potansiyel bir tehdit unsuru şeklinde değerlendirilmeye başlanmıştır (Defense Intelligence Agency Office for Counterterrorism Analysis, 1999). 1999 yılında ABD Savunma İstihbarat Teşkilatı adına hazırlanan Donanma Yüksek Lisans Okulu'na ait siber terörizm araştırma çalışmasında bu alanda sayıca çok fazla tanım ortaya konmuştur (Soesanto, 2020). Bunlardan birisi de "*destek faaliyetlerinde bilgi teknolojisinin terörist kullanımı"*nın siber terörizm olarak nitelendirilmediği şeklindeki ifadedir. Ancak dar anlamda siber terör "*siyasi, dini veya ideolojik hedefler peşinde hükümetleri veya toplumları korkutmak veya zorlamak için dijital mülkün yasadışı olarak yok edilmesi veya bozulması*" şeklinde ifade edilmiştir (Luiijf, 2014). Bu dönemde ABD'de söz konusu tanımlarla ilişik tutulan somut olaylara bakıldığında "Bilgisayar Dolandırıcılığı ve Kötüye Kullanımı Yasası (18 USC 1030)" çerçevesinde siber saldırıların silahlı saldırı veya saldırganlık eylemi olarak kabul edilmeleri büyük bir sorun olarak ortaya çıkmıştır. Bu dönemde siber terörizmi askeri saldırı operasyon eylemlerinden, siber suçlardan ve hacktivizmden ayrı tutmak konusunda zorluklar

yaşanmıştır. 2012 yılında Jonalan Brickey'in siber terörizmi "*terörizm yapmak için siber kullanımı veya siyasal değişim arayışında şiddet veya şiddet tehdidi yoluyla korku yaratmak ve sömürmek için siber uzayda militan operasyonlar yürütmek, yıkıcı militan operasyonlar yapmak için siber yeteneklerin kullanılması*" olarak tanımlaması da söz konusu dönemin etkilerinin göstergesidir. Yine 2014 yılında Daniel Cohen tarafından yazılan siber terörizmin vaka çalışmalarıyla ilgili kitapta örneklerin büyük bir kısmının hacktivizm, siber suç ve askeri saldırı operasyonlara ilişkin olması bu dönemdeki tanımlardan etkilenildiğini göstermektedir (Soesanto, 2020).

Siber Terörizmin Teorik Temelleri

Siber teröristler tarafından kullanılan çeşitli yöntemlerden bazıları olan nefret içerikli ifadeler, askeri ve sivil içerikli propagandalar, toplumun düşünceleri üzerinde meydana getirilen manipülasyonlar ve kasıtlı iletişim gibi faaliyetlerin hayata geçirilmesi amacıyla siber alan araç olarak kullanılmaktadır. Siber terörizmin teorik temelleri bakımından literatürde bu temelleri incelemek adına kullanılan iki teori karşımıza çıkmaktadır. Söz konusu teorilerin siber terörizmle ilgili eylemlerin engellenmesi ve öncül tedbirler alınması, siber terörizme yol açan faaliyetlerin tespiti ve incelenip üzerinde kovuşturma yapılması hususlarında bu konuda faaliyette bulunan tüm paydaşlara fayda sağlayacağı tahmin edilmektedir. Yine bu teorilerin siber terörizm saldırılarında araç olarak kullanılan faillerin suçu işlemedeki düşünce yapılarını ortaya koymada etkili olacağı değerlendirilmektedir (Correia, 2022).

Rutin Aktivite Teorisi

Rutin Aktivite Teorisi, 1979'da Cohen ve Felson tarafından "Social Change and Crime Rate Trends: A Rutine Activity Approach" adlı makalede ortaya atılmıştır. Daha önceki dönemlerde yer alan kriminolojik teorilerin genel özelliği itibariyle suçluların kişilik özelliklerine ve onları suça yönelten etkenlere ilişkin araştırma eğilimleri suçu oluşturan durumları göz ardı etmelerine yol açmıştır (Haava, 2017). Diğer taraftan bu teorinin durumsal olaylar üzerinde ortaya çıkması, suçlunun üzerindeki bireysel dikkatten uzaklaşılarak suç işlemeyi etkileyen durumsal faktörler üzerine yoğunlaşılmasına neden olmuştur (O'Brien ve Yar, 2008).

Söz konusu teorinin oluşması için üç ana faktörün ortaya çıkması gerektiği savunulmuştur. Bunlar; motive olmuş suçlu, uygun hedef ve yetenekli koruyucu yokluğu olarak sıralanmıştır. Teorinin temelleri siber terörizme kıyasen uygulandığında fiziksel alana tekabül eden kısmın siber uzay olarak nitelendirilebileceği ifade edilmektedir (McQuade, 2006; LeClair ve diğer., 2016). Daha önce üniversite öğrencileri üzerinde yapılan bir araştırma göstermiştir ki, kişisel bilgisayarlarında çeşitli siber saldırı türlerine yönelik güvenlik yazılımlarını kullanmayan öğrencilerin bilgisayar yoluyla işlenen suçlara karşı daha dirençsiz oldukları gözlemlenmiştir (Choi, 2008). Buradan çıkarım yapılarak koruyucuya ilişkin sadece fiziksel bir yapının değil, güvenlik yazılım eksikliğinin koruyucu eksikliği faktörü içerisinde değerlendirilebileceği düşünülmektedir. Bu minvalde orijinal rutin aktivite teorisinin kıyasen söz konusu alana da uygulanabileceği görülmüştür (Correia, 2022). Söz konusu deneysel çalışma öğrencilerin bilgisayar korsanlığına ilişkin zafiyetlerini ölçse bile araştırma bulguları siber terörizme ilişkin faaliyetlerde siber suça yönelik rutin aktivite teorisinin uygulanması için daha önce belirtilen üç faktörün netliğe kavuşturulması gerekliliğini ortaya koymaktadır (Suler, 2004). Buna örnek vermek gerekirse kullanıcıların bilgisayarlarında yazılımsal güvenliğe sahip olmaması durumunda veya engellenen web sitelerinin bulunması durumunda zafiyetin siber terörizm faaliyetlerinde bulunacak kişilerin motivasyonu artırarak hedeflere yönelik terörün şiddetini artırmasıdır (Correia, 2022).

Uzay Geçiş Teorisi

Uzaya Geçiş Teorisi, teori kriminolojisinde konvansiyonel terörizm ortamındaki eylemlerden siber alandaki eylemlere geçişte siber suçlu davranışlarını anlamak için kullanılmıştır (Correia, 2022). Bu teori, 2008 yılında Schmalleger ve Pittaro'nun editörü olarak görev yaptığı Prentice Hall yayınevinde yayınlanan “İnternet Suçları” adlı kitapta Karuppanan tarafından kaleme alınmıştır. Hindistan’daki Kriminoloji ve Suç Bilimleri baş direktörü olarak görev yapan Karuppanan tarafından ortaya atılan bu teori, insanların mekanlar arası geçişlerinde davranışlarında farklılaşmanın olduğunu savunmaktadır. Söz konusu teori incelenmesi gereken yedi unsurdan oluşmaktadır. Bunlar; siber ortamda oluşturulan esnek kimlik, suçluların sosyal bağlantıları, fiziksel suç alanından siber alana geçişteki rahatlık, suçlular üzerindeki tehdit oranının düşmesi, fiziksel ortamda bastırılmış olan suç işleme eğiliminin siber ortama aktarılması, siber alandaki kurallar ve değerler arasındaki sınırların net olmaması ve yakalanma olasılığı düşük olan suç fırsatlarıdır

(Jaishankar, 2007). Karuppanan tarafından öne sürülen ilkeler teorisi konvansiyonel suçlarla yeni düzendeki siber suçlar ilişkisinin daha iyi şekilde anlaşılmasını sağlayarak siber terörizmi kavramada önemli sacayaklarını oluşturan üç özelliği ön plana çıkarmaktadır. Bu sac ayaklarından ilki kimliğin gizlenmesidir. Bu özellik sayesinde siber teröristler siber uzayda rahatça hareket edebilmekte ve kimliklerini anonimleştirerek gizleyebilmektedir (Suler, 2004; Agustina, 2015). İkinci sacayağı ise siber terör eylemlerini gerçekleştiren faillerin anonim ortamda herhangi bir ceza almadan, soruşturma veya kovuşturma kapsamında tespit edilmeden suça ilişkin fiilleri siber ortamda idame ettirmelerine olanak sağlanmasıdır. Bu fiillerin devamlılığına sebep olan ana unsur siber caydırıcılığın olmamasıdır (Suler, 2004). Üçüncü ve son özellik ise siber alanın niteliği itibariyle, fiziksel olarak suçun işlendiği alanlarla gri bir ortamda değişim ve geçişkenlik özelliğinin bulunmasıdır. Siber taraf siyah bir ortam olarak düşünüldüğünde terörist faaliyetlerin bu ortamda çok daha rahatlıkla uygulanabildiği ve aynı zamanda düşük maliyetlerle çok daha büyük etkilere yol açabileceği değerlendirilmektedir. Bu husus finansal açıdan terörizmin amaçladığı sonuçlara ulaşılması noktasında avantaj sağlamaktadır. Propaganda ve siber terör faaliyetini gerçekleştirecek grupların üye sayılarını artırmak amacıyla anonim olarak siber alanın sağladığı perdeleme hususu burada ön plana çıkmaktadır (Shandler ve diğer., 2021). Anonim olma özelliğinden dolayı siyah alan olarak nitelendirilebilecek siber uzayda işlenen suçların azaltılması ve siber terörizmi canlı tutan dinamiklerin söndürülmesi adına öncül ve ardıl tedbirlerin alınması gerektiği açıktır.

Terörizme yönelik davranışlar fiziki olarak engellenerek caydırıcılığın artırılmasıyla bu fiilleri işleyen faillerin siber uzayda da aynı düzenlemelerin uygulanabileceğine yönelik düşüncelerinin değiştirilmesi söz konusu olabilecektir. Bu durumda siber terör faaliyetlerinin devletlerin ulusal düzenleyici ve denetleyici kurumlarından ve terörizmle mücadele eden kuruluşlardan gizlenebileceği karanlık ortamı aydınlatabilecektir (Stalans ve Finn, 2016). Bu kapsamda siber terörizmle mücadele eden devlet organlarının uluslararası kuruluşlarla iş birliği içerisinde çıkaracağı mevzuat ve pratikteki uygulamaların ne denli önemli olduğu ortaya çıkmaktadır.

2020 yılında ortaya çıkan ve sonrasında da küresel etkileri devam eden COVİD-19 pandemisi sürecinde dijital ortamın eskiye nazaran çok daha etkin olarak kullanılmasıyla siber ortamın avantajları ön plana çıkmıştır (Blair, 2020). Terörizmin fizikselden dijitale

dönüşümüyle birlikte, siber uzayda söz konusu siber saldırıların artması ve siber saldırganların sayıca yükselmesiyle suçluların yakalanması zor bir hale gelmiştir (Shandler ve diğer., 2021). Küresel çapta etkisi olan devletler siber güvenlik önlemlerine ilişkin ulusal savunma ödeneklerini artırarak yeni bir savaş alanı doğduğunun farkına varmıştır. Öyle ki bu alanda devletler arası siyasi ve askeri rekabet günden güne artmaktadır.

1.4. Siber Terörizme Yakın Kavramlar

Siber terörizm içerisinde bulunduğu bağlamda birçok kavramla ilişkili olarak anlam değişimine uğramaktadır. Bu kavramlar siber uzay içerisinde kendilerine yer bularak birbirlerini doğrudan etkilemektedir. Bu sebeple iç içe geçmiş söz konusu terimlerin açıklığa kavuşturulması gerekmektedir. Örnek vermek gerekirse siber terörizme yol açıcı fiilleri işleyen kişi yahut gruplar siber suçları işlerken hacktivizme ilişkin davranışlarda da bulunabilmektedir. Buna benzer olarak, devletler arasında yaşanan siber casusluk süreci içerisinde etkin bir istihbarat sürecine ilişkin olarak da yüksek düzeyli bilgi savaşları yürütülebilmektedir (Alkhouri, 2019). Söz konusu kavramlar arasındaki sınırların belirlenmesi gerekliliği faillerin işledikleri fiiller bakımından hukuki ve cezai yaptırımlara ilişkin önemi ortaya koymaktadır. Özellikle birden fazla hareketle kümülatif şekilde oluşan davranışlar, suçların cezalandırılması bakımından gerçek veya fikri içtimaya ilişkin hükümlerin uygulanmasına neden olabilmektedir. Bu bakımdan yargısal boyutuyla da söz konusu terimsel ayrımların yapılması önem kazanmaktadır.

Siber Uzay (Siber Alem)

Siber uzay terimi ile birlikte onunla aynı anlama gelen diğer bazı kavramlar da kullanılmaktadır. Bunlara örnek vermek gerekirse “siber alan”, “siber alem”, “siber dünya”, “sanal vatan”, “siber uzam”, “ungoverned space”, “infosphere”, “terra nullius” gibi kelime grupları söylenebilir (Jeutner, 2019). Söz konusu terimler için yapılan tanım “*herhangi bir fiziksel biçimde var olmayan ve insanların, yazılımların, servislerin internete bağlı teknoloji cihazları ve ağlar aracılığıyla etkileşimi sonucu ortaya çıkan karmaşık ortam*” şeklindedir (ISO/IEC, 2012). Bir diğer tanım ise “*yerel bir özel ağ veya dünya çapındaki interneti oluşturan bilgisayarlar, ağlar, iletişim yolları, yazılımlar, veriler ve kullanıcılar topluluğu. Yazılımın içinde çalıştığı, verilerin manipüle edildiği ve değiş tokuş edildiği dijital ortam*”

şeklinde söz konusu dijital ortamda bulunan varlıkların sıralanması ile oluşturulmuştur (SimplicityVoip Glossary, 2024).

Siber uzay Andress ve Winterfeld'in (2011) tanımında "*siber savaş veya siber tehditlerin oluştuğu kara, hava, deniz, denizaltı ve uzayda operasyon yürütülen bütün alanları kapsayan alan*" olarak nitelendirilmiştir (Andress ve Winterfeld, 2011). Bu tanımdan daha ayrıntılı şekilde Kuehl (2009) tarafından yapılan bir diğer tanım; "*bilgi-iletişim teknolojilerini kullanan birbirine bağlı ağlar aracılığıyla bilgi oluşturmak, depolamak, değiştirmek, değiş tokuş etmek ve kullanmak için elektronik ve elektromanyetik spektrumun kullanımıyla ayırt edici ve benzersiz karakteri çerçevelenen bilgi ortamı içindeki küresel alan*" şeklindedir (Kuehl, 2009). ABD Ulusal Güvenlik Başkanlık Yönergesi ve İç Güvenlik Başkanlık Yönergesinde siber uzay teriminin tanımı yapılmıştır: "*birbirine bağlı bilgi teknolojisi altyapıları ve internet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü işlemciler ve kontrolörleri içeren kritik sektörlerdir*". Yine Amerikan Hava Kuvvetleri tarafından yapılan siber uzay tanımı: "*ağ sistemleri ve fiziksel yapılar üzerinde veri depolamak, değiştirmek ve geliştirmek amacıyla elektronik ve elektromanyetik spektrumun kullanılması*" şeklindedir (Nasrat, 2015). Birleşmiş Milletler tarafından siber alanda oluşturulan sözlükte siber uzay "*net olarak bilinen internete, çevrimiçi konferans kuruluşlarına, bilgi depolama ile işleme aygıtlarına ve iletişim altyapısına bağlı küresel sistem*" olarak nitelendirilmiştir (Yayla, 2013a). Kuzey Atlantik Anlaşması Örgütü (North Atlantic Treaty Organization-NATO) kapsamında yapılmış olan tanım ise "*ağ teknolojilerinin ürünü olan bir sayısal dünya olarak insan ve bilişim teknolojilerinin bir arada olduğu sanal dünya*" şeklindedir. Burada göz önünde bulundurulması gereken nokta NATO'nun bilişim teknolojisinin yanı sıra insan faktörüne de tanımda yer vermiş olmasıdır. Bu yönden bakıldığında insan faktörü çerçevesinde siber uzayın sanal bir ortam olsa da beşerî tarafının da bulunduğu gerçeğidir. Çünkü insan faktörü olmadan söz konusu bilişim sistemleri ve otonom araçlar harekete geçemeyecektir (CertBy LAB, 2018). NIST tarafından yapılan tanım: "*internet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü işlemciler ve denetleyiciler dahil olmak üzere bilgi sistemleri altyapılarının birbirine bağlı ağından oluşan bilgi ortamı içindeki küresel bir etki alanı*" şeklindedir (NIST, 2012). Pentagon ise "*internet sistemleri, bilişim ağları, saklı işlemcileri de kapsayan birbirleri ile doğrudan bağlantılı bilgi teknolojilerinden meydana gelen yeryüzüne yayılmış bir ortamdır*" şeklinde bir tanım yapmıştır (Darıcılı, 2017).

Siber uzayla ilgili yabancı ülkelerin yaptığı tanımlara bakıldığında Belçika'nın "Cyber Security Strategy: Securing Cyberspace" strateji planında bu tanımı *"iletişim ve bilgi sistemlerinin birbirine bağlanmasıyla oluşturulan küresel çevre*" şeklinde yaptığı görülmüştür (Government of Belgium, 2012). Kanada tarafından yapılan tanım "*birbirine bağlı bilgi teknolojisi ağları ve bu ağlardaki bilgiler tarafından yaratılan elektronik dünya*" şeklindedir (MPS, 2010). Almanya'nın "*küresel ölçekte veri düzeyinde birbirine bağlı tüm BT sistemlerinin sanal alanı*" (BMI, 2011) olarak tanımladığı siber uzay Çekya'nın tanımında biraz daha ayrıntılı aktarılarak "*bilgi sistemleri ve hizmetleri ile elektronik iletişim ağları tarafından oluşturulan, bilgilerin yaratılmasına, işlenmesine ve değiş tokuşuna olanak sağlayan dijital ortam*" şeklinde nitelendirilmiştir (NCKB, 2015). Burada göze çarpan husus oluşturulan dijital ortamda bilgiye ilişkin fiillerin tahdidi olarak sayılmış olmasıdır. Genel olarak bakıldığında ise birbirine paralel olan tanımların tercih edildiği görülmektedir.

Ülkemizde bu alanda yapılan tanımlara bakılacak olursa, 2020-2023 Ulusal Siber Güvenlik Strateji ve Eylem Planının tanımlar bölümünde siber uzayın "*doğrudan ya da dolaylı olarak internete, elektronik haberleşme ve bilgisayar ağlarına bağlı olan tüm sistem ve hizmetler*" olarak tanımlandığı görülecektir (Ulaştırma ve Altyapı Bakanlığı, 2020). İçişleri Bakanlığı ve Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı (Siber Ay) tarafından yapılan tanım ise "*tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam*" şeklindedir (Siber Ay Sözlüğü, 2024). Burada gerçek olmayan sanal bir ortamdan bahsedilmiştir. Söz konusu kavram kapsamı içerisine internet ortamını almakla birlikte aslında kumanda edilebilen cihazlar (telefon, TV vb.) ile birlikte kayıt alınabilen ses, görüntü gibi içerikleri de kapsamaktadır (Siber Ay, 2024).

Siber uzay için söz konusu tanımların oluşmasında temel alınan ilk olaylar ABD ile SSCB arasındaki soğuk savaş döneminde meydana gelmiştir. Bahse konu dönemde ve 1947-1991 yılları arasında hibrit savaşların bir ayağının uzay ve askeri teknolojiye taşındığı bilinen bir gerçektir (Darıcılı, 2017). Soğuk Savaş söz konusu alanlarda ağırlık kazanmışken 1957 yılında ABD'de "İleri Araştırma Proje Ajansı (Advanced Research Projects Agency-ARPA)" kurulmuştur. Bu kuruluşun ana hedeflerinden bir tanesi de savaş söz konusu

olduğunda bilgisayar sistemlerinde meydana gelecek zafiyetlerin saldırganlarca tespit edilmesinden önce kritik bilgi ve verilerin diğer bilgisayarlara aktarılmasıdır (Aslay, 2017). 1960 yılına gelindiğinde ARPA'nın başına getirilen "defence (D)" ile birlikte "Savunma Araştırmaları Proje Ajansı (Defence Advanced Research Projects Agency-DARPA)" oluşumunu tamamlamış, (DARPA, 2024) 1969 yılında nihayet "ARPANET" 60'lı yılların başındaki ilk halinin üzerine yapılan çalışmalarla geliştirilerek bu alanda siber uzay terimi literatüre girmiştir (ICANN, 2024).

Siber uzay terimi ilk kez William Gibson isimli Kanadalı yazarın 1982 yılında yayınladığı ve siberpunk türündeki "Burning Chrome" isimli hikâye kitabında kullanılmıştır (Aithor, 2024). Bu terimin kullanıldığı bir diğer kitap aynı yazarın kısa hikayelerinden biri olan ve 1984 yılında yayınlanan "Neuromancer" romanıdır. Söz konusu kitapta hırsız olan Case'in siber uzaydaki işverenlerinin matrix adı verilen sistemlerine bir jak vasıtasıyla gizli şekilde bağlanması konu edilmektedir. Burada öne çıkan husus, insan ile makine arasında teknolojik olarak bir dönüşümün ortaya konulmuş olmasıdır (Seviş ve Şeker, 2016). Gibson söz konusu kitapta siber uzayı; "*milyarlarca meşru kullanıcı tarafından her gün tecrübe edilen uzlaşılmış bir halüsinasyon ve tasavvur edilemez karmaşa*" olarak tanımlamıştır (Gibson, 1984).

Siber uzay, bilgisayar sistemlerinin fiziksel unsurlarını içerisinde barındırır ancak yalnızca söz konusu sistemlerden ibaret değildir. Aynı zamanda ağ yapısının içeriğindeki sosyal etkileşimleri de bünyesinde barındırmaktadır (Sağıroğlu ve Alkan, 2018). Bu açıdan bakıldığında siber uzayın hibrit bir ortam olduğu söylenebilir. Söz konusu yapıda ağlar içerisinde küresel ağ bağlanma talebi olduğunda bağlanılabilecek ağ internettir (Maurer, 2011). Küresel çapta bilgisayar ağının kurulduğu bu elektronik ortam dörtlü sacayağı üzerine kuruludur. İlk sacayağını fiziksel altyapı unsuru oluşturmaktadır. Bu kısımda telekomünikasyon sektöründeki uydular, yönlendiriciler, anahtarlar gibi haberleşmeyi sağlayan fiziki yapılar bulunmaktadır. Kablo sistemleri, endüstriyel kontrol sistemleri ve Gözetleyici Kontrol ve Veri Toplama Sistemi (Supervisory Control and Data Acquisition-SCADA) askeri sistem içindeki insansız hava aracı (İHA), silahlı insansız hava aracı (SİHA) gibi araçlar ve kapalı intranetler fiziksel altyapılara örnek olarak verilebilecektir. İkinci sacayağı olan mantıksal yapılar yazılım olarak nitelendirilebilir. Teknolojinin gelişmesiyle birlikte cihazların yazılımları özellikle de cep telefonu gibi mobil yazılımlar, bilgisayar

işletim sistemleri ve tarayıcılar bu yapılara örnek verilebilir. Yazılımın buradaki fonksiyonu fiziksel yapı içindeki unsurların haberleşmesini ve icrai olarak harekete geçebilmesini sağlayacaktır. Üçüncü sacayağı yani bilgi kısmında ise internet ortamına aktarılan ve içerik sağlayıcıların ürettiği, sosyal medya platformlarında paylaşılan yazışma, yorum gibi sözel içerikler ile fotoğraf, resim, video gibi görsel içerikler bulunmaktadır (Sağıroğlu ve Alkan, 2018). Aynı zamanda haberleşmeye ilişkin trafiği yöneten mantıksal yönerge ve yazılımlar (DNS veya ISP gibi) siber uzayın kod katmanını oluşturmaktadır. Bilişsel katman için ise enformasyon operasyonları olarak nitelendirilebilecek ve dezenformasyona yol açıcı içeriklerle stratejik olarak tasarlanmış iletişim biçimleri örnek olarak verilebilir (Eldem, 2021). Dördüncü ve son sacayağı ise beşerî unsur olarak nitelendirilebilecek insan unsurudur. Bu unsur diğerleri arasında en önemli unsuru oluşturmaktadır. Öyle ki siber uzayda bilgi ve veriyi işleyen, kullanan, değiştiren veya başkalarına aktaran insandır (Sağıroğlu ve Alkan, 2018). Siber uzay ağ yapısından oluşması itibariyle zamansal ve mekânsal sınırların bulunmadığı bir alandır. Bu sınırsızlık, uluslararası hukuk normlarının mülkilik ve şahsilik ilkeleri doğrultusunda suç faillerine yönelik uygulanmasına engel olmaktadır. Bunun yanı sıra suç olarak tanımlanacak fiillerin hangi fiiller olduğu konusunda da muğlaklık oluşturmaktadır. Yine devletlerin mevzuatları ve mevzuatlarını uygulama biçimlerinin farklılığı neticesinde farklı soruşturma ve yargılama prosedürleri ortaya çıkmaktadır (Yayla, 2013a).

Siber Tehdit

Siber tehdit, NIST tarafından yapılan tanımda "*yetkisiz erişim, bilgilerin yok edilmesi, ifşa edilmesi, bilgilerin değiştirilmesi ve/veya bilgilerin reddedilmesi yoluyla bir bilgi sistemi aracılığıyla kurumsal operasyonları (misyon, işlevler, imaj veya itibar dahil), kurumsal varlıkları veya bireyleri olumsuz etkileme potansiyeline sahip herhangi bir durum, olay veya hizmet. Ayrıca, bir tehdit kaynağının belirli bir bilgi sistemi güvenlik açığından başarıyla yararlanma potansiyeli"* olarak nitelendirilmiştir (NIST Glossary, 2024). Kanada Siber Güvenlik Merkezi ise siber tehdidi "*bir sistemin veya içerdiği bilgilerin kullanılabilirliğini, bütünlüğünü veya gizliliğini değiştirerek bir bilgi sisteminin güvenliğini tehlikeye atmayı veya genel olarak dijital yaşamı bozmayı amaçlayan bir faaliyet*" olarak açıklamaktadır. Ayrıca siber tehdit içerikli ortamı da söz konusu alanda faaliyet gösteren aktörlerin kötü amaçlı fiilleri işledikleri sanal ortam olarak tasvir etmiştir. Siber tehdit

aktörleri bilişim sistemlerinin zafiyet alanlarından faydalanarak bu sistemdeki kişilerin verilerine, teknolojik aygıtlarına, sahip oldukları sistemlere ve bağlı oldukları ağlara erişim sağlamakta, kötü amaçlar için kullanım sağlamaktadır (Canadian Centre for Cyber Security, 2022). Söz konusu sistemlerdeki bilgileri de dezenformasyona uğratarak farklı hedeflere yöneltebilmektedirler. Bu hedefler devletlere ilişkin olabileceği gibi vatandaşlara yönelik korku ve panik ortamına neden olmak ve vatandaşların devlete olan güveninin kaybolmasına yol açacak nitelikler kazanabilmektedir. Söz konusu davranışlarla siber saldırganlar kamu düzeni ve güvenliğinin sarsılmasına yol açabilmektedir.

Bilgisayar Korsanlığı (Hacking) ve Hacktivizm

Bilgisayar korsanlığı (hacking), Ritchie ve Thompson tarafından MIT (Massachusetts Institute of Technology) Bell Labs'da 1960'lı yıllarda yürüttükleri çalışmalar kapsamında ortaya çıkan bir tabirdir. Bu ikili söz konusu terimi "*bir problemi çözmek, bir ürünü geliştirmek ya da bir fonksiyonu geliştirmek için zekice çözümler bulmak*" şeklinde tanımlamıştır (Pitts, 2017). Zamanla gelişen teknolojiyle birlikte değişen bilişim sistemleri vasıtasıyla ise hacking; "*verilere ve sistem kaynaklarına yetkisiz erişim elde etmek için bir sistemdeki veya ağdaki zayıflığı belirleme ve kullanma sürecidir*" olarak ifade edilmiştir. Bilgisayar korsanlığı, fiili gerçekleştiren kişinin bilişim sistemlerine rıza dışı girmesi şeklinde de kısaltılabilir. Sistemdeki gizli verilere ilişkin erişim amacıyla mevcutta bulunan parolaların yeterli güvenlikte olmamasından faydalanma buna örnek gösterilebilir (GreyCampus, 2024). Bu saldırı türünde sistemlerdeki açıklık ve zafiyetlere karşı virüsler, parola kırıcılar, zararlı yazılımlar araç olarak kullanılabilmektedir. Bilgisayar korsanlığı saldırılarının temel amacı bilgisayar ve bilişim sistemlerinin barındırdığı veri ve bilgilerin ele geçirilmesi, silinmesi veya tahrifata uğratılmasıdır. Bu kapsamda mağdur olarak siber saldırılardan zarar gören kişilerin hak kaybı ve menfaat ihlali söz konusu olmaktadır (BTK, 2022). Söz konusu saldırıları gerçekleştiren hackerlar; web siteleri, bilgisayar veya bilişim sistemleri üzerinde hakimiyet kurarak gizli bilgilere erişim sağlamakta, erişilen verileri ifşa etmekte, kredi kartı bilgilerini ele geçirerek ekonomik kazanç sağlamaktadır. Bu saldırılar milli istihbarat, siyasi itibar, ekonomik tahribat, kritik altyapılara yönelik yıkıcı faaliyetler ve diğer saiklerle gerçekleştirilebilmektedir. Bunlar haricinde siber terörizme yol açacak faaliyetlerin devlet destekli gruplar veya özel amaçlarla oluşturulan sivil siber birlikler tarafından gerçekleştirilmesi sırasında da bilgisayar korsanlığı saldırıları önemli bir yer tutmaktadır. Devletler arası siber savaşta ve ticari rekabet ortamında mali kazanç sağlama

noktasında söz konusu saldırı tipi diğer saldırı türleriyle entegre şekilde kullanılabilmektedir.

Bilgisayar korsanlığı saldırıları günümüzde nesnelerin interneti (IoT) teknolojisinin gelişimiyle yaygınlaşmıştır. Bunun yanı sıra bilgisayarlara ait web kameraları kullanıcıları izleme, mesajlara erişim sağlama, ekran görüntüsü alma, göz atma geçmişlerine yetkisiz şekilde erişebilme gibi faaliyetleri de gerçekleştirmektedir. Web kameralarını hedef alan Uzaktan Erişim Truva Atı (RAT) olarak isimlendirilen kötü amaçlı programlar sayesinde kameraya erişim elde edilebilmektedir. Yönlendiriciler üzerinden iletimi sağlanan verilerin ve erişim sağlanan ağların da yine hackerlar tarafından ulaşılan sistemler olması yönlendiricileri hacking faaliyetlerine karşı açık hedef haline getirmektedir. Yönlendiricilerin ele geçirilmesi genellikle hackerlar tarafından Dağıtılmış Hizmet Reddi (DDoS) saldırıları, Etki Alan Adı Sistemi (DNS) sahteciliği veya kripto madenciliği şeklindeki kötü niyetli fiillerle gerçekleştirilmektedir. E-postalarla gönderilen link, ek veya bağlantılarla kötü niyetli yazılımlar ve fidye yazılımları yayılarak bilgisayar korsanlığı ile bütünleşik şekilde siber saldırılar gerçekleştirilebilmektedir. Bu vasıtayla mağdur durumunda olan kullanıcılara kimlik avı saldırıları gerçekleştirilerek bilgisayar korsanlığına bütünleşik şekilde yıkıcı siber saldırılar kullanılmaktadır. Son zamanlarda hızlı enjeksiyon saldırısı (jailbreak) olarak adlandırılan ve kullanıcıların telefonlarındaki resmi aplikasyon mağazalarında yer almayan uygulamaları ya da diğer yazılımları telefona indirmek için cihazdaki işletim sistemi kısıtının kaldırılması da yaygın yöntemler arasında yer almaktadır. Öyle ki bu saldırılarda büyük dil modellerine (LLM) yönelik güvenlik sistemleri istismar edilerek sahte unsurların üretilmesi sağlanmaktadır (Kara, 2011). Bu durum hukuki açıdan bakıldığında kullanıcıların cihazı geliştiren şirketle arasında yaptığı matbu lisans sözleşmelerinin ihlali anlamına gelmekte ve büyük bir güvenlik açığının da habercisi olmaktadır. Bilgisayar korsanları, cihaz içerisinde yer alan tüm verileri ele geçirerek yaptıkları siber saldırılarla birbirine bağlı ağlara ve sistemlere de zarar verebilmektedir. Burada ikili bir ayrımda bulunularak ilk kategoride kötü niyetlice bilişim sisteminin hacklenmesi “siyah şapka korsanlığı”, iyi niyetli şekilde sistemlerdeki noksanlıkların tespiti ve bunların düzeltilmesi için yasal ve bilinçli olarak hackleme işlemlerinde bulunmak ise “beyaz şapka korsanlığı” olarak nitelendirilmektedir (Alkhouri, 2019). Son olarak ortaya çıkan ve “gri şapka korsanlığı” olarak nitelenen üçüncü kategoriyi ise gerçekleştirilen fiillerin kamu yararına yönelik yapıldığı gri alanı temsil eden hackerlar oluşturmaktadır.

Yukarıda değinilen örnekler doğrultusunda bilgisayar korsanlığı türlerine aşağıda yer verilmektedir:

Siyah Şapkalı Hackerlar (Black Hat Hackers)

Siyah şapkalı hackerlar "kötü adamlar" olarak nitelendirilmek ile birlikte kendilerini kırıcı (cracker) şeklinde isimlendirmektedirler (Lockhart, 2007). Söz konusu hackerlar, bilişim sistemleri ve bilgisayar ağları üzerindeki güvenlik zafiyetlerini tespit ederek mali kazanç, kişisel ve özel itibar elde etmek, kurumsal ve ticari alanlarda bilgi hırsızlığı ve devletlerarası casusluk gibi faaliyetleri yürütmektedir. Yine bu gruplar kritik ağlara ve sistemlere yönelik hedefler belirleyerek bu hedeflere ait sistemlerin çalışmasını engelleyebilmektedir. Bununla beraber hassas ve kişisel bilgilerin terör gruplarınca ele geçirilmesini sağlayarak terörün finansmanı için çalışmalar yapabilmektedir. Bu bağlamda kritik altyapılara ilişkin saldırılarla konvansiyonel savaşlarda devletlerin avantaj sağlaması için siber saldırılar gerçekleştirilebilmektedir (Fortinet, 2024a). Diğer taraftan siber güvenlik olaylarına neden olan saldırıların da siyah şapkalı hackerlara karşı verilen mücadele vasıtasıyla önlendiği ve yok edildiği görülmektedir (Hatcher, 2014).

Beyaz Şapkalı Hackerlar (White Hat Hackers)

Siyah şapkalıların aksine beyaz şapkalı hacker grupları kötü niyetli saldırıları bertaraf etmek adına ve kötücül yazılımları engellemek için çalışmalar yürütmektedir. Bu kategorideki hackerlar uluslararası literatürde "iyi adamlar" olarak tanımlanmakta ve siber saldırılara karşı savunma sistemlerine yönelik geliştirme ve iyileştirme çalışmalarıyla birlikte proaktif şekilde siber saldırıların önlenmesine ilişkin faaliyetler yürütmektedir. Beyaz şapkalı hackerlığa "etik bilgisayar korsanlığı" da denilmektedir. Söz konusu hackerlar ağ güvenlik seviyesini değerlendirip test ederek teknik araştırma ve geliştirme işlemlerini yapmaktadır. Kullanılan teknikler masanın diğer tarafında yer alan siyah şapkalı hackerlarla hemen hemen aynıdır. Burada farklı olan kısım ise etik olarak karanlık taraf yerine aydınlık tarafta yer almalarıdır (Fortinet, 2024a). Söz konusu tarafta çalışan beyaz şapkalı hackerlar bilgisayar veya bilişim sistemi sahiplerinin kanuna uygun rızasıyla siber güvenlik uzmanlığını kullanmaktadır. Sistemlere erişim sağlayarak önceden siber saldırı tiplerini bu sistemler üzerinden denetleme ve test etme görevleri bulunmaktadır. Bu denemeler siber literatürde sızma testi (pentest) olarak adlandırılmaktadır. Bu hackerlar, sistemlerde

meydana gelen açıklık ve zafiyetleri tarayarak sistemlere ait koruyucu katmanları güçlendirir (Eshan, 2018). Yine yapılan testlerde kurum, kuruluş ve özel sektör şirketlerinin siber güvenliğe ilişkin dayanıklıkları ortaya çıkmakta, yapısal güvenlik önlemleri alınması için tespitler yapılmaktadır. Bununla beraber bilgi, birikim ve donanımlarını kuruluşlara aktararak donanımsal ve yazılımsal güvenlik tedbirlerini almaktadırlar (Porterfield, 2017). Geri besleme (feedback) ya da dönüt alacak şekilde test etme yöntemleriyle sistem güvenliğini artıran uygulamalar yapmaktadırlar (Smith, 2015).

Beyaz şapkalı hackerlar geneline bakıldığında köken olarak siyah şapkalı eski hackerlardan oluşmaktadır. Siyah şapkalı hackerlar karanlık taraf (dark side) olarak adlandırılan ortamda kazandıkları tecrübeler sonrası devletlerin kendi hukuk sistemlerindeki cezai yaptırımlara tabi tutulmakta daha sonrasında ıslah amaçlı çeşitli görevlerde çalıştırılabilmektedir. Verilen bu görevlerin başında da halihazırda yaptığı işi karanlık taraf için değil, aydınlık taraf olarak nitelendirilebilecek ortamda yapmasıdır. Kamu ve özel sektörde siber güvenlik uzmanı olarak çalışan hackerların birçoğu bu şekilde her iki tarafı gören ve bilen kişilerden oluşmaktadır (Hatcher, 2014). Bunların dışında kamu kurum ve kuruluşları ile şirketlerde görev alan ve sızma testi uygulayan çalışanlar bulunmaktadır. Bu çalışanlara sızma testçisi (penetration tester) denilmektedir. Sızma testçileri, kurum, kuruluş veya şirketlerin erişim izni dahilinde bilişim sistemlerine ve ağlara sızarak siber güvenlik dayanıklılıklarını ölçmektedir (Oriyano, 2017). Gerçek siber saldırı seviyesinde saldırılar yaparak sızma testleri ile sistem açıklıkları ve zafiyetleri tespit edilmektedir (Vitula, 2015). Teknik kapasitenin yükseltilmesi ve potansiyel tehlikelerin farkına varılması açısından sızma testleri büyük önem arz etmektedir (Raj, 2015).

Gri Şapkalı Hackerlar (Gray Hat Hackers)

Gri şapkalı hackerlar ise lafzen nitelendirdiği şekilde ne siyah ne de beyaz tarafta yer alan, bu iki tarafın tam ortasında bulunan grubu temsil etmektedir. Siyah şapkalı hackerlara benzer şekilde uluslararası hukuku, kural ve ilkeleri ihlal ederek siber saldırı faaliyetleri yürütmekle birlikte onların aksine herhangi bir mali kazanç elde etme amaçları bulunmamaktadır. Gerçekleştirdikleri eylemleri kamu yararı maksatlı yapmaktadırlar. Örnek verilecek olursa bir sistemdeki güvenlik açığından farkındalık yaratmak adına yararlanırlar ancak beyaz şapkalıların aksine bunu herkese açık şekilde gerçekleştirirler.

Yani sistemlere ilişkin güvenlik açıklıkları hakkında bir uyarı misyonu üstlenmektedirler. Böylece kamu ve özel sektörün dikkatini çekmektedirler (Gibson, 2015). Bu grup hackerlara örnek olarak verilebilecek olan Khalil Shreateh isimli hacker 2013'te Facebook için açıklık ve zafiyetler tespit etmiştir. Bu zafiyetleri Facebook'a iletmiş ve noksanlıkların giderilmesi amacıyla girişimde bulunmuştur. İlk uyarıyı dikkate almayan bu sosyal medya platformu sonrasında kurucu Mark Zuckerberg'in sayfasına da bu kişi tarafından erişim sağlanınca söz konusu zafiyetin büyüklüğü anlaşılarak açıklık kapatılmıştır (Porterfield, 2017). Yine gri hacker gruplarının da süjesi olarak içerisinde yer aldıkları gruplara örnek olarak Anonymous, LulzSec ve Wikileaks verilebilir. Bu gruplar devletlere ait hassas olarak nitelendirilebilecek gizli bilgileri herkesin ulaşabileceği çeşitli platformlarda yayımlamıştır. Bahse konu bilgi sızdırma operasyonlarının amacı siyasi olarak bilgisi sızdırılan devletleri zor duruma düşürmektir (Fortinet, 2024a).

Bilgisayar korsanlığı örneklerine bakılacak olursa, dünya üzerinde yaşanan en çarpıcı örneklerden biri 1991 yılında meydana gelen Çöl Fırtınası (Desert Storm) siber saldırısı ön plana çıkmaktadır. Bu siber saldırı, ABD-Irak savaşı sırasında klasik savaş unsurları bakımından ABD'nin üstün geldiği bir dönemde ABD Savunma Bakanlığı ve kuvvet komutanlıklarının bilgisayarlarına sızılarak erişim sağlanması ile meydana getirilmiştir (AFCEA, 2012). Çöl fırtınası siber saldırısı savunma sanayi sistemlerinde kullanılan uçak sensörlerinin istihbari faaliyetlerine yönelmiştir. Bu vasıtayla kritik hedeflere ilişkin bilgi toplayan sistemler üzerinde yönetimsel kontrol sağlanarak konvansiyonel savaşın düşük maliyetli araçlarla tersine çevrilmesi imkânı doğmuştur (United States General Accounting Office,1997).

1999 yılında ABD'ye ait Marshall Uzay Uçuş Merkezi hedeflenerek gerçekleştirilen siber saldırıda Ulusal Havacılık ve Uzay Dairesine (NASA) ait sistemlere erişim sağlanmıştır. Marshall Uzay Uçuş Merkezi sistemine saldırganlarca sağlanan erişimle uzay araçlarının uçuş bilgileri de çalınmıştır. Bu saldırı neticesinde yirmi bir gün boyunca NASA çalışamamış ve uzay istasyonunda problemler ortaya çıkmıştır. Öyle ki uzay istasyonunun sıcaklık ve nem de dahil kritik veri ve bilgileri çalınarak iki milyon civarında yazılım ele geçirilmiştir. Siber saldırı bununla sınırlı kalmamış Amerika Birleşik Devletleri Savunma Bakanlığı'nın genel merkez binası (Pentagon) da hedeflenerek silahlarla ilgili sistemlere yetkisiz şekilde erişim sağlanma girişiminde bulunulmuştur. Söz konusu saldırının yalnızca

on beş yaşında ufak bir çocuk tarafından gerçekleştirilmesi siber alemde şaşkınla karşılanmış ve NASA sistemlerinin ele geçirilmesi kuruluş açısından önemli bir güvenlik zafiyeti şeklinde yorumlanmıştır (ABCNEWS, 2000).

Bir diğer bilgisayar korsanlığı olayı 2000 yılında Avustralya'nın Queensland şehrindeki Maroochydore nehri yakınında gerçekleşmiştir. Söz konusu siber saldırı "Maroochy Shire" olarak adlandırılmış ve kanalizasyon suyunun dökülmesi ile sonuçlanmıştır. Saldırı daha önce bahse konu tesislerde çalışan bir personel tarafından hizmet sözleşmesi ile ilgili problemler üzerine gerçekleştirilmiştir. Bu saldırıda çalıntı kablosuz radyo, SCADA denetleyicisi ve kontrol yazılımı kullanılarak Maroochydore nehrine ve yakınlarından geçen kıyı sularına yaklaşık bir milyon litre kanalizasyon suyunun salınmasına yol açmıştır. SCADA sistemlerinin komuta ve kontrol mekanizması ele geçirilerek pompalama istasyonlarının mevcut verileri değiştirilmiştir. Queensland şehri söz konusu siber saldırı dolayısıyla olumsuz etkilenmiş ve yerleşim bölgesindeki sızıntı günler süren uğraşlar sonucu ancak temizlenmiştir. Bu temizleme işlemi hem büyük bir maliyete sebep olmuş hem de çıkan koku ve yayılan hastalıklarla vatandaşların sağlığı olumsuz etkilenmiştir. Bununla birlikte Avustralya Çevre Koruma Ajansı tarafından yapılan açıklamada saldırı neticesinde deniz canlılarının da olumsuz etkilenerek birçoğunun öldüğü ve nehir suyu renginin koyulaştığı ifade edilmiştir (Risdata, 2000).

2003 yılında ABD ile Kanada'nın hedef alındığı ve önemli üretim tesisleri ile petrol rafinelerinin hizmet kesintisine uğradığı siber saldırılarda vatandaşları etkileyen boyutuyla elektrik kesintileri yaşanmıştır. Bunun yanı sıra söz konusu saldırı ABD'de yaklaşık 10 milyar dolar mali zarara sebep olurken Kanada'nın ise 2,5 milyar dolar zarara uğradığı hesaplanmıştır. Söz konusu siber saldırı tedarik zincirini de etkilemiş, petrol iletim ve dağıtımında yaşanan problemler nedeniyle karayolu ulaşımı sekteye uğramıştır. Diğer taraftan elektrik hatlarındaki kopmalar sebebiyle demiryolu ve elektrikli şehir ulaşımı işlemez hale gelmiştir. Bu devletlerdeki önemli sanayi tesislerinde üretim durma noktasına gelmiş ve ekonomik kayba uğramışlardır (U.S.-Canada Power System Outage Task Force, 2004).

Bilgisayar korsanlığına ilişkin faaliyetler, karşı tarafın bilgisayar sistemlerine girme yani erişim için bu sistemlerde kalma ve fiili olarak işlemde bulunmanın yanı sıra yasal

olmayan şekilde şifrelerin kırılarak ya da elde edilerek donanımsal yahut yazılımsal uygulamaları kullanma şeklinde de meydana gelebilmektedir (Andini, 2021). Bilgi toplama, verilere ulaşma ve kopyalama hedefiyle bilgisayar sisteminin açıklıklarından yararlanarak donanımsal yapıya internet vasıtasıyla rızasız erişim söz konusu olmaktadır. Bu yetkisiz girişi yapan ve sistemde kalan kişilere ise hacker denilmektedir.

Daha önce kısaca değinilen ve siber terörizmden ayırt edilmesi gereken bir kavram olarak nitelenen hacktivizm ise; "*siyasi amaçların peşinde, yasadışı veya yasal olarak belirsiz dijital araçların şiddet içermeyen kullanımı*" olarak tanımlanmaktadır (Gardner ve Thomas, 2014). Bir diğer tanım ise "*dijital dataların siyasi bir amacı benimsetmek amacıyla insanları kendi amaçları doğrultusunda yönlendirmek için kullanılmasıdır*" şeklindedir. Hactivizm ile siber terörizm arasındaki temel fark burada hedeflenen unsurun korku ve panik yaratmak olmasıdır (Alkhouri, 2019). "Hack" ve "aktivizm" sözcüklerinin bir araya gelmesiyle oluşan "Hacktivizm" terimi ilk defa 1996'da Cult of the Dead Cow isimli grubun "Omega" adlı üyesi tarafından ortaya konmuştur. Hacktivist faaliyetler çeşitli olaylara karşı protestoda bulunmak isteyen grupların siyasi olarak eylemde bulunması olarak ortaya çıkabilmektedir. Ancak internet kullanımının günden güne artmasıyla hacktivist faaliyetler klasik ortamından uzaklaşarak sanal ortama taşınmıştır (Trendmicro, 2015). Sanal ortamda hacktivizmin tanımlanmasında göz önünde bulundurulması gereken en önemli faktörler siber savaşın aksine hareketin devlet dışı bir aktör tarafından gerçekleştirilmesi, siyasi veya sosyal bir amaç doğrultusunda ilerleme amacı ve söz konusu eylemin siber terörizmin aksine toplumda fiziksel veya ruhsal bir yıkıma neden olmaması yahut asli amaç olarak bunun hedeflenmemesidir (First Line Practitioners, 2024). Siyasi bir gündem yaratma amacı güdülmesi, şiddet içermeyen ancak suç içeren bir fiilde bulunulması hacktivizmin ana unsurlarıdır. Hacktivistler, siyasi hedeflere aracı olmak ve bazı düşünceleri desteklemek adına siber saldırılar düzenleyen gruplardır. Bu gruplar hedef olarak tüm sektörleri seçebilmekte fakat bazı durumlarda grup ideolojisine ve siyasi görüşlerine uygun olmadığını değerlendirdikleri çeşitli kurum ve kuruluşlara karşı da siber saldırı faaliyetinde bulunabilmektedir (Fowler, 2016). Bu eylemler doğrultusunda kurum, kuruluş yahut özel sektörde faaliyet gösteren şirketlerin ekonomik kayıplara uğramasının yanında aynı zamanda itibar kayıplarına uğraması da söz konusu olmaktadır.

1950'li yıllarda bilgisayar korsanlığı kendini göstermiş olsa da, hacktivizmin popüler olduğu ilk olay 1989 yılında nükleer faaliyetlere karşı eylem ve protestoda bulunmak isteyen Avustralyalı bir bilgisayar korsanının NASA ve ABD Enerji Departmanı bünyesinde yer alan bilgisayarlara sızma olayıdır. 1990'lı yılların sonlarına gelindiğinde 'Hong Kong Sarışınları' adlı protestocu grubun internete ilişkin ücretlere karşılık herhangi bir ücret ödemeden bir hak olarak gördükleri internete erişim hakkı doğrultusunda Çin hükümetinin bilgisayar ve bilişim sistemlerine yönelik hackleme faaliyeti ile söz konusu terim daha da popüler hale gelmiştir. Bu grupların yasal olmamalarına rağmen halk tarafından destek görmeleri neticesinde etik olarak varlıkları sorgulanmıştır. Hactivist faaliyetler protestocu davranışlarla halkın ve medyanın farkındalığını artırmak için bir araç görevi de üstlenmektedir. Coğrafi ve siyasi sınırlardan bağımsız bir konumda bulunduğu için hacktivistlerin kendi belirledikleri bağımsız amaçları gerçekleştirebilmeleri bilişim sistemleri ve bilgisayar kullanılarak daha da kolaylaşmaktadır (Marlenec, 2021).

Dünya üzerinde hacktivist eylemlere bakıldığında özellikle Ortadoğu merkezli olarak tüm dünyada terör faaliyetlerinde bulunan IŞİD'e ilişkin saldırılar ön plana çıkmaktadır. Son dönemlerde IŞİD ile yakından ilişkili olan ve IŞİD terör eylemlerini siber saldırılarla destekleyen hacker grupları tarafından gerçekleştirilen eylemler artmıştır. Konvansiyonel terörün yanı sıra internet ve ağ ortamında meydana getirilen savaş ve saldırı ortamı söz konusu terör faaliyetlerini destekleyerek kaotik bir ortama sebep olmaktadır. Bu örneklerden Cyber Caliphate Army'nin (CCA), IŞİD'e yardım eden ilk siber terör gruplarından birisi olduğu söylenmektedir. CCA tarafından 2015 yılında gerçekleştirilen siber saldırıların ana amacı IŞİD'i destekleyerek terörizmin artışına yol açmak olmuştur (Andini, 2021). Yine bu örgüte ait çarpıcı siber saldırılardan birisi, United States Central Command (USCENTCOM) resmi hesaplarına karşı Twitter ve YouTube'da gerçekleştirilen saldırılardır. Ayrıca Newsweek adlı siyasal haberler yapan derginin Twitter hesaplarına CCA tarafından siber saldırıda bulunulmuştur (Alkhouri, 2016). İslami Siber Ordu (ICA) tarafından yapılan bir diğer siber saldırı ise Azerbaycan'ın en önemli bankalarından biri olan Amrah Bank'a yönelik yapılan saldırıdır. Bu saldırıda söz konusu bankanın web sitesine zarar verilerek IŞİD'e ait logo, bayrak ve Usame Bin Ladin'e ait görseller sitede yasa dışı şekilde paylaşılmıştır (Giantas, 2018).

ABD tarafından Musul ve Irak'taki telekomünikasyon altyapısının çoğu 2003 yılındaki Irak savaşının ardından yerleştirilmiş ve bu gelişmeyle IŞİD tarafından potansiyel olarak hackleme faaliyetleri artmıştır. 2016 yılında IŞİD'in birçok yeri hedef almasında bu altyapının gelişmesi önemli bir faktör olmuştur. Yine aynı yıl Newsweek dergisinde yapılan haberde IŞİD'in Batı dünyasının internet ve haberleşmeye yönelik altyapısını hedef alarak siber saldırılarda bulunma amacının olduğu ifade edilmiştir. Bu gelişmeler üzerine ABD Savunma Bakanı Ashton Carter verdiği bir brifingde "Irak ve Kürt güçlerinin Musul şehrini yeniden ele geçirmelerine yardımcı olmak için siber saldırıların kullanılacağı" ifadelerini kullanmıştır. Carter, ABD ordusunun siber saldırılara yönelik olarak önlemler aldığını ve IŞİD'e karşı elektronik harp mücadelesinde gelişme kaydettiklerini açıklamıştır. CCA'nın bir sonraki hedefinin Google olduğu ancak teknik olarak bunu gerçekleştiremeyip bunun yerine Hintli yerel ölçekte bir firma olan Add Google Online'ın web sitesine siber saldırıda bulunduğu aktarılmıştır (Newsweeka, 2016).

CCA'nın siber uzayda gerçekleştirdiği bir diğer siber saldırının İngiltere'de Solar UK isimli bir enerji şirketine yönelik olduğu ve şirketin web sayfasının IŞİD yanlısı görüntüler ve sloganlarla değiştirildiği belirtilmiştir. CCA tarafından yapılan açıklamada, Solar UK şirketine yapılan saldırının örgütün liderlerlerinden Junaid Hussain'e karşı yapılan insansız hava aracı saldırısına cevaben intikam amaçlı yapıldığı aktarılmıştır (Newsweekb, 2016).

2016 yılının Şubat ayında kurularak faaliyete geçen Sons Caliphate Army (SCA) isimli örgüt tarafından bireysel ve kurumsal Twitter ve Facebook hesaplarına yapılan 15.000 civarı siber saldırının örgütleri tarafından gerçekleştirildiği ifade edilmiştir (Andini, 2021). Bunun yanı sıra SCA, Central Bank of Bangladesh'e ait web sitesini hacklediğini belirtmiştir. Yine diğer bir hackleme faaliyeti olarak İngiltere Premier Lig futbol ekiplerinden Arsenal'in Arapça resmî web sitesine gerçekleştirilen saldırıyı da söz konusu örgüt üstlenmiştir. Bu sitede mezhepsel savaşların bir tetikleyicisi olarak Şii karşıtı propagandayla karışıklık ve kaos çıkarmaya yönelik video paylaşımında bulunulmuştur (Alkhouri, 2016).

Siber terörizme yönelik faaliyet gösteren bir diğer terör örgütü de 2016 yılı mayıs ayında birden fazla grubun belirli hedefler doğrultusunda birleşerek oluşturduğu koordineli olarak IŞİD'in siber terörizm faaliyetlerine destek veren United Cyber Caliphate (UCC)

isimli örgüttür. Bu örgüt; Cyber Caliphate Army, Sons Caliphate Army ve Kalashnikov E-Safety Team olmak üzere üç hacker topluluğunun bir araya gelmesiyle meydana gelmiştir. UCC örgütü siber saldırı operasyonu gerçekleştirmesinin yanı sıra IŞİD'in bir yayın organı gibi çalışmaktadır. Öyle ki bu yapılanma Telegramda grupların oluşturduğu ölüm listelerini de yayınlamıştır (Andini, 2021).

2020 yılında İsrail'de meydana gelen olayda kritik su altyapılarına yönelik siber saldırı gerçekleştirilmiştir. Söz konusu saldırı ile Galilee ve Mateh Yehuda'daki su pompa istasyonlarına erişim sağlanmak istenmiştir. Bu saldırı göstermiştir ki su kritik altyapılarına yapılan siber saldırılar dolayısıyla tarım sektöründe çalışan vatandaşlar doğrudan etkilenebilmektedir (ZDNET, 2020b). Diğer taraftan söz konusu saldırılar bununla sınırlı kalmamış ve 2020 yılının Nisan ayında yine İsrail'deki su arıtma tesislerine erişim sağlanmıştır. İsrail Ulusal Siber Müdürlüğü (INCD) ve Su İdaresi tarafından yapılan açıklamalarına göre siber saldırganlarca yetkisiz erişim sağlamak üzere hedeflenen unsurlar su arıtma tesisinin operasyonlarını yöneten sistemler, SCADA sistemi içeren klor kontrol cihazları ve kanalizasyon sistemleri olmuştur (ZDNET, 2020a). Söz konusu siber saldırı ile tesiste olması gereken klor seviyesinin üstünde bir miktar klor ana su şebekesine salınarak vatandaşların kullandığı şebeke suyundan zarar görmeleri hedeflenmiştir (ZDNET, 2020b). Bu siber saldırı kritik altyapılara yönelik saldırılardan toplumun can ve mal kayıpları dolayısıyla olumsuz etkilenebileceğini göstermektedir.

Bir diğer olay da 2021 yılının şubat ayında ABD'nin Florida eyaletinde meydana gelmiştir. Söz konusu siber olayda Oldsmar su arıtma tesisine yönelik siber saldırı gerçekleştirilerek SCADA sistemlerine uzaktan erişim sağlanması hedeflenmiştir. Söz konusu saldırıda su kanallarının temizlenmesinde kullanılan sodyum hidroksit (NaOH) oranını artırılarak (milyonda 100 parçadan (ppm) 11.100 ppm'e) şebeke suyuna salınım yapılmak istenmiştir (ICP, 2021a).

Bununla birlikte bahse konu hacking saldırılarına karşı devletlerin ve vatandaşların güvenli şekilde korunması amacıyla uygulanması gereken aktif ve pasif caydırıcılık önlemleri ve siber savunma yöntemleri aşağıdaki şekilde sıralanabilir (Fortinet, 2024a).

- Yazılım Güncelleme
- Parola Güçlendirme

- HTTPS Şifrelemesi
- Reklam ve Spam İçerikli Bağlantılara Karşı Dikkatli Olma
- Yönlendiricide ve Akıllı Cihazlarda Varsayılan Kullanıcı Adı ve Parolayı Değiştirme
- Antivirüs Programları Kullanma
- VPN (Sanal Özel Ağ) Kullanma
- Birinci Taraf Kaynaklardan Dosya İndirme
- İki Faktörlü Doğrulama Kullanma
- Kimlik Avına Karşı Koruma Teknikleri Güncelleme
- Varsayılan Olarak Yönetici Girişi Kullanmama

Siber Casusluk

Casusluk kelimesi gözetlemek manasına gelen "spigare" ve "epier" kelimelerinin etimolojik kökeninin birleşmesinden meydana gelmektedir (Gözübüyük, 1970). Gözetleme faaliyeti, tarihi süreç içerisinde düşman kuvvetlerinin hareketlerini araştırma, gizli araştırmalar yürütme şeklinde savaş hukuku kapsamında kullanılmıştır. Casus terimi, La Haye Kara Savaşı Kuralları Sözleşmesinde "*uluslararası silahlı çatışmalar hukuku çerçevesinde çatışan taraflardan birinin harekât alanı içinde karşı tarafa iletmek üzere gizli bir biçimde bilgi toplamasını belirlemekte olup bu tür eylemlerde bulunan kişiler*" olarak nitelendirilmektedir. Casusluğun oluşabilmesi için ön koşul söz konusu fiilin gizli ya da gerçek olmayan bir sebeple yapılması ve saldırıda bulunulan tarafın hareket alanı sınırları çerçevesinde olmasıdır. Bu fiil icrai bir hareketi içerebileceği gibi bilgi toplama gibi pasif bir faaliyeti de içerebilir (Pazarcı, 2018).

Siber casusluk; "*rekabetçi bir şirkete veya devlet kurumuna karşı avantaj elde etmek için sınıflandırılmış, hassas verileri veya fikri mülkiyeti çalan bir siber saldırı biçimi*" şeklinde tanımlanmaktadır (Broadcom, 2024). Ekonomik üstünlük, siyasi hedefe ulaşma veya hâkim durum elde etmek için kişisel bilgi ve verileri kötü niyetli olarak ele geçiren veya yayımlayan bir siber casus tarafından meydana getirilen faaliyet olarak da tanımlanabilir. Bu faaliyetler kişilerin veya şirketlerin kamuoyu nezdindeki itibarına zarar verici şekilde yapılabilmektedir. Diğer bir tanıma göre siber casusluk "*avantaj elde etmek veya hassas bilgileri parasal bir ödül için satmak amacıyla bir düşman veya rakip hakkındaki hassas bilgilere erişim sağlayarak bilgisayarların veya dijital iletişim*

faaliyetlerinin kasıtlı olarak kullanılması" şeklindedir (Coleman, 2008). Yine siber casusluk için yapılan bir diğer tanım "*verileri sızdırmak veya dahili, özel, gizli bilgileri ifşa etmek için bir kuruluşun mahremiyetini ve güvenliğini ihlal eden etik olmayan eylem*" gizlilik ve güvenlik ekseninde nitelenmiştir (SimplicityVoip Glossary, 2024).

5237 sayılı TCK'nın "Devlet sırlarına karşı suçlar ve casusluk" başlığı altında 326'ncı ve 339'uncu maddeler arasında düzenlenen suçlara bakıldığında burada casusluğun hangi fiillerle işlenebileceği açıkça ifade edilmiştir. Öyle ki burada sayılan fiillerle ilgili genel bir tanım yapılacak olursa "*devletin güvenliği veya iç veya dış siyasal yararları bakımından, niteliği itibarıyla, gizli kalması gereken bilgileri veya yetkili makamların kanun ve düzenleyici işlemlere göre açıklanmasını yasakladığı ve niteliği bakımından gizli kalması gereken bilgileri siyasal veya askerî casusluk maksadıyla temin etmek veya açıklamak*" şeklinde bir tanım oluşturulabilir (Türk Ceza Kanunu, 2004).

Siber casusluk kavramı kurumsal casusluğun bir görünüm biçim olarak da nitelenebilir. Siber casusluk faaliyeti sonrasında şirketlerin uğradığı zararlara bakıldığında müşterilerin güveninin yanı sıra şirketin hissedarlarının da güvenini büyük oranda azalttığı görülmektedir. Rekabetçi bir ortamda şirketlerin pazarlama stratejilerini ele geçirerek piyasadaki etkinliklerini azaltıp hâkim durumda etkin piyasa gücüne sahip şirket olma noktasında avantaj yakalama durumuna erişilebilmektedir (Malwarebytes, 2024). Burada önemli olan hususlar kişilerin bilgilerinin rıza dışı ele geçirilmesi ve sadece kişilere karşı değil aynı zamanda devlete ve kritik kurumlara karşı da kötü niyetli bir hedef potansiyelinin bulunmasıdır. Siber casusluk faaliyetleri, devletlere ait kurum ve kuruluşların bünyesinde barındırdıkları vatandaşlara ait kişisel bilgileri ele geçirme amacı gütmektedir. Finansal çıkar elde etme amacının yanı sıra vatandaşların devlete ait güven ve bağlılık duygularını zedeleyici bir etkisi de bulunmaktadır. Siber casusluk faaliyetleri sonucunda oluşan olumsuz etkiler kümülatif şekilde büyüyerek bir siber savaşın meydana gelmesine yol açabilir. Bunların yanı sıra gelişen teknolojiyle devletlerin yerli ve milli seviyede kendi ürettikleri cihaz, yazılım ve donanımsal uygulamalar ele geçirilerek askeri ve endüstriyel devlet sırları ifşa edilebilmektedir.

Birleşmiş Milletler Şartına göre casusluk güç kullanma seviyesinde olmayan bir faaliyettir (Wortham, 2012). Casusluk faaliyetinde bulunan kişilerin kovuşturmaya tabi

tutulması için yabancı bir ülkenin yargılama alanında yakalanması gerekmektedir. Öyle ki devletlerin sahip oldukları casusları yakalandıkları ülkede yargılamasının o devletçe talep edildiği durumlarda iade edilmesi ve bu isteğin kabul edilmesi çok da olası değildir. Konvansiyonel casusluğa bakıldığında bu fiili işleyen casuslar yabancı bir ülkenin sınırları içerisinde yakalandıklarında yargılama yapılabileceği gibi siber casusluk durumunda da aynı şekilde yabancı bir ülke sınırları içerisinde yakalanırsa yargılamaya tabi tutulabilir.

Diğer taraftan siber casusluk faaliyetleri çoğunlukla herhangi bir efor sarf etme ihtiyacı duyulmadan bilgisayar ağ ve sistemleri üzerinden casusların bulundukları ülkede gerçekleştirilmektedir. Bu sebeple de siber casuslar normal casuslara göre yakalanma ve gözaltına alınma konusunda daha avantajlı konumdadır. Soruşturma veya kovuşturmadan kaçınma fırsatı, siber casusluğun bir casusluk türü olduğu gerçeğine halel getirmez. Bundan dolayı konvansiyonel olarak nitelenebilecek casusluklara uygulanan ulusal ve uluslararası kanunlar siber casusluğa da uygulanabilir (Weissbrodt, 2013).

Bazı uzmanlara göre siber casusluk konvansiyonel casusluğa göre daha ele alınır şekilde incelenmelidir. Öyle ki siber casusluk alanı geleneksel casusluktan daha müdahaleci bir alandır. Bu alanda büyük veri olarak nitelendirilen veriyi saklama ve işleme kapasitesinin yanı sıra devlet dışı aktörlerin siber casusluk faaliyetinde bulunma kabiliyetinin olduğu ifade edilmektedir (Melnitzky, 2012). Bu görüşü destekleyen akademisyenlere göre somut olaya göre bazı durumlarda siber casusluk BM Antlaşması 2/4 gereğince kuvvet kullanma veya kuvvet kullanma tehdidi olarak değerlendirilebilir. Karşıt görüşlü ve azınlıkta kalan bazı yazarlara göre ise siber casusluğun niteliği gereği farklı bir yapısı olmasından dolayı konvansiyonel casusluktan ayrı bir kanuna tabi olması gerektiği savunulmuştur (Wortham, 2012). Melnitzky'e göre siber casusluk etkileme kapasitesi göz önünde bulundurulduğunda silahlı saldırı olarak nitelendirilebilir. Öyle ki fiili olarak siber casusluk da silahlı saldırı potansiyeline sahip olması dolayısıyla silahlı saldırı olarak değerlendirilebilir (Melnitzky, 2012). Buchan'ın "Cyber Espionage and International Law" adlı kitabının sekizinci bölümü BM Şartı 51.madde kapsamında meşru müdafaa ve zorunluluk unsuru doktrinlerinin politik ve finansal siber casusluk eylemleri için uygulanabilirliğini incelemektedir. Savunulan görüşe göre devletlerin sadece fiili veya yakın bir silahlı saldırı tehdidine maruz kaldıkları durumda meşru müdafaada bulunabilecekleri ifade edilmektedir. Burada ana amaç siber casusluk eylemlerini meşru yani diğer bir deyişle haklı kılmaktır. Meşru müdafaanın niteliği

gereği gereklilik ve orantılılık unsuru çerçevesinde uygulanmasının siber casusluk eylemlerine karşı da geçerli olacağı değerlendirilmiştir. Yine zorunluluk durumunda uygulanacak karşı koymanın da devletlerin veya toplumun ciddi bir tehlikeyle karşı karşıya kalması durumunda fiiliyata geçirileceği ifade edilmiştir. Bölümün sonunda siber casusluğa ilişkin "lex specialis" o alana özgü bir mevzuatın oluşturulması gerektiği değerlendirilmiştir (Buchan, 2019).

1998 yılında ABD'de meydana gelen Ayışığı Labirenti (Moonlight Maze) bilgisayar korsanlığı siber saldırısı bu yıllarda gerçekleştirilen en önemli siber casusluk faaliyetlerinden biri olarak gösterilmektedir. ABD Savunma Bakanlığı, Ulusal Havacılık ve Uzay Dairesi (NASA), Enerji Bakanlığı ve Dışişleri Bakanlığı ile askeri personellerin bilgisayarlarına gerçekleştirilen saldırı, devlet destekli siber casusluğun dünyadaki ilk örnekleri arasındadır. Söz konusu saldırı sonucunda ABD tarafından yapılan açıklamalarda bilgisayar korsanlarının bir yıldan uzun bir süre boyunca bahse konu kurumların bilgisayarlarına yetkisiz erişim sağlayarak bir gelişmiş kalıcı tehdit (APT) saldırısı düzenlediği aktarılmıştır. Bu siber saldırının etkisini artırılması amacıyla sosyal mühendislik, hedef odaklı kimlik avı ve güvenlik zafiyetlerini kötüye kullanma siber saldırı yöntemleri bir arada kullanılarak savunulması zor bir kompleks yapı inşa edilmiştir. Bununla beraber arka kapı gibi saldırı yöntemleri entegre şekilde kullanılarak personellerin sistem girişlerinde saldırıyı fark etme şansı azaltılmıştır. ABD'li yetkililer, bu siber saldırının gösterdiği emarelerin Rusya tarafından devlet eliyle desteklenen bilgisayar korsanları tarafından yapıldığını iddia etmiştir. Söz konusu saldırıda, ABD Savunma Bakanlığının sahip olduğu kritik veriler ile uydu teknoloji projeleri, füze savunma sistemlerine ilişkin teknik kılavuzlar ve uzay araştırma teknolojilerini barındıran sistemler istihbarat faaliyetleri kapsamında çalınmıştır. Saldırının etkisiyle bu tarihten itibaren savunma sanayisine ayrılan bütçe gibi siber güvenlik tedbirlerine de öncelik verilmiş, siber zafiyetlerin ve kırılganlıkların onarılması için kapsamlı çalışmalar başlatılmıştır. Bu çerçevede siber strateji ve politikalar geliştirilerek siber kapasite inşası kuvvetlendirilmiştir (Aktaş, 2023).

Siber Şiddet

Siber şiddet son zamanlarda internet ortamında sosyal medya kullanımının artmasıyla sıklıkla karşılaşılan bir terim haline gelmiştir. Bu terim için yapılan ve sık

kullanılan tanımlardan birisi "*duygusal, psikolojik veya fiziksel zarara neden olmak için çevrim içi ortamda zarar verici, incitici veya tehlikeli materyallere erişim ve bunların dağıtımı*" şeklindedir (Attrill, 2015). Siber şiddet tanımından da görüleceği üzere zorba yöntemler kullanılan cebri bir uygulamadır. En yaygın görülen türleri ise siber taciz ve siber zorbalıktır. Bilgi ve iletişim teknolojileri söz konusu şiddet biçimlerinin kullanılmasında aracı görevi görmektedir. Siber taciz internet ortamında yapılabildiği gibi e-posta veya çevrimiçi mesajlaşma şeklinde de ortaya çıkabilmektedir. Bu taciz şeklinde belirli bir kişiye yönelik ağır duygusal travmalara yol açabilecek nitelikte tekrarlı davranışlar bulunmaktadır. Mağdur konumunda bulunan kişiler çoğu zaman fiziki olarak zarar görme korkusu da yaşamaktadır. Özellikle de "CyberVawg" olarak adlandırılan yani kadınlara yönelik siber şiddet en sık karşılaşılan siber şiddet türüdür. Avrupa Toplumsal Cinsiyet Eşitliği Enstitüsü tarafından 2017'de yayımlanan dokümanda bu şiddet biçiminin istenmeyen cinsel içerikli e-postalar, metin veya çevrim içi mesajlar, sosyal ağlar, web sitelerinde veya internet sohbet odalarında uygunsuz veya saldırgan yaklaşımlar, nefret söylemi yani bir bireyi kimliği, cinsiyeti ve cinsel yönelim veya engellilik gibi diğer özellikleri üzerinden aşağılama, hakaret, tehdit veya hedef gösteren dil şeklinde somut olaylar özelinde ortaya çıktığı aktarılmıştır (University of Ljubljana Faculty, 2017).

Bunun yanı sıra çevrim içi taciz olarak adlandırılan bir diğer taciz türünde de belirli başlı fiiller yer almaktadır. Bunların başında saldırgan isimlerle anılmak, fiziksel olarak tehdit edilmek, uzun süre tacize maruz kalmak, takip edilmek ve bilerek utandırılmak (slut shaming) gelmektedir (Madden ve diğer., 2014). Bu sayılan davranışlar siber saldırganlık modeli etrafında çeşitlenen davranışlardır. Hedef olarak seçilen kitleye olan yaklaşım niyet tabanlı bir modelle değerlendirilmelidir. Niyet ise oluşturulmak istenen zararın amacının ne olduğuna ilişkindir (Prentice ve diğer., 2015). Siber takip (cyberstalking) kapsamında tekrarlanan zincirleme fiillerden oluşan rahatsız edici içerikler, aynı kişi tarafından internet ortamında yahut mesaj, e-posta, metin yoluyla yayılmaktadır (University of Ljubljana Faculty, 2017). Yine siber flörtün kötüye kullanılması veya istismarı (cyber dating abuse-CDA) flört edilen kişilerin davranışlarını izleme ve kontrol etmek için izleme teknolojisinin kullanılması, sosyal medya ve e-posta hesaplarının şifre kırıcılarla ele geçirilmesi, konum takip sistemleri ve uygulamalarının kötüye kullanılması şeklinde meydana gelmektedir (Backe ve diğer., 2018). Siber flört istismarı için yapılan tanım "*bir kişinin flört partnerinin teknoloji ve sosyal medya aracılığıyla kontrol edilmesi, taciz edilmesi, takip edilmesi ve*

kötüye kullanılması" şeklindedir (Zweig ve diğer., 2014). Söz konusu flört bir ilişkiye dayanıyorsa ilişki sırasında veya ilişkinin bitmesiyle sözlü tehditler ve çevrim içi ortamda saldırganlık gibi hususlar ortaya çıkabilmektedir (University of Ljubljana Faculty, 2017). Saldırganlık olarak nitelendirilen fiili açıklamak gerekirse, kimlik hırsızlığına benzer bir şekilde ilişkideki kişiye karşı çeşitli platformlarda gerçek dışı bilgi yayma gibi mağdura zarar vermeyi hedefleyen davranışları içerdiği söylenebilecektir (Jonason, 2021). Bununla beraber "bilerek utandırılmak (slut-shaming)", özellikle kadınların ve kız çocuklarının sosyal medyada cinsellikle ilgili konularda davranış, giyim ve görünümleri konusunda eleştirilmesi, aşağılanması veya zorbalığa uğraması olarak tanımlanmaktadır (VeryWellFamily, 2023). Söz konusu utandırma yöntemi ergenlik çağındaki kız çocuklarında psikolojik olarak kötü bir etki bırakmakla birlikte ilerleyen evrelerde intiharla dahi sonuçlanabilmektedir. Bu sebeple siber suçlarla ilgili hususların uluslararası sözleşmeler ve anlaşmalar çerçevesinde sibere dayalı (cyber dependant) olarak değil siberle ilişkili ve siberin araç olarak kullanıldığı (cyber enabled) diğer suçlarla birlikte aynı bağlamda değerlendirilerek mevzuatsal çalışmaların yapılmasının yerinde olabileceği değerlendirilmektedir.

Siber tacizlerin önemli ve diğer bir boyutunu da şiddetin cinsel yönüyle ilgili siber şiddet biçimleri oluşturmaktadır. Görsellere rıza dışı erişim ve dağıtım başlığı altında müstehcen görüntülerin ve videoların internet ortamında servis edilmesi, intikam pornosu adı verilen ve özellikle eski partner ve eşlerin birbirlerine ait müstehcen görüntülerini, telefon numaralarını, sosyal medya hesaplarını pornografik öğeler içeren sitelerde karşı tarafı küçük düşürme amaçlı paylaşması, izin alınmadan çekilen cinsel görüntüler (sürüngen çekim, creepshot), rıza ile alınmış ancak sonradan intikam amaçlı olarak izinsiz şekilde paylaşılan görüntüler, dijital olarak kaydedilen rıza dışı cinsel eylemler, özel bilgileri araştırmak, manipüle etmek ve yayımlamak (doxing) söz konusu terim kapsamında yer almaktadır. Bunların yanı sıra tehdit etme ve karşı tarafı sindirme amaçlı kimliğin çalınarak o kimliğe bürünme (impersonation) davranışı kullanıcıların itibarını zedelemektedir. Buna ek olarak hacking faaliyetleri ile bilgisayarların web kameralarını ele geçirme işlemi de siber taciz ve şiddet kapsamında değerlendirilmektedir. Söz konusu eylemler sömürü, zorlama veya tehditle sonuçlanmaktadır. Daha ileri boyutlarıyla failler mağdurlara yönelik olarak cinsel içerikli şantajda bulunabilmektedir. Siber tacizler istenmeyen pornografi olarak adlandırılan ve genellikle kadınların sosyal medya hesaplarına gönderilen cinsel organ

fotoğrafları gibi erotik materyallere maruz kalma şeklinde de ortaya çıkmaktadır (University of Ljubljana Faculty, 2017).

2012'de Almanya'da siber şiddet üzerine yapılan bir araştırmada erkeklere ve çocuklara nazaran kadınların çevrim içi siber şiddete maruz kalma durumunun istatistiki olarak çok daha fazla olduğu saptanmıştır (Staude-Müller ve diğer., 2012). Bir diğer çalışmaya göre ise Fascendini ve Fialova (2011) siber şiddetin kadınlar üzerinde sıklıkla uygulanmasına ilişkin beş önemli unsuru belirlemiştir (Fascendini ve Fialova, 2011). Bunların ilki siber şiddette kullanılan araçların kimliği saklayıcı yapıda yani "anonim" olmasıdır. Bu unsur sayesinde suçu oluşturan fiili işleyen fail kimliğini gizleyerek mağdurun kendisini tanımasını engellemektedir. Burada adeta bir kimliği perdeleme eylemi söz konusu olmaktadır. Diğer bir temel unsur "uzak eylem mesafesi" olarak nitelendirilmiştir. Öyle ki bu unsur fiziki bir temasta bulunmaksızın failin hedefine ulaşabilmesine imkân tanımaktadır. Üçüncü unsur olan "otomasyon", fail tarafından suç işlenirken çevrim içi ortamın bağlamsal anlamda sağladığı avantajı ifade eder. Diğer bir unsur olan "ulaşılabilirlik" unsuru herkes tarafından istenildiği zaman ulaşılabilir olan ortamı ve mağduru rahatsız etmek için zaman ve mekândan bağımsızlığı tanımlar. Son unsur olan "yayılma-süreklilik" ise failin mağdura yönelik oluşturduğu fiil ve rahatsız edici ortamın onun istediği süre boyunca internet ortamında devam etmesi, farklı mecralarda paylaşılabilmesini nitelemektedir. Bu şekilde fail istediği sosyal medya platformlarında mağdura yönelik psikolojik baskı kurarak ulaşmak istediği hedefe ilişkin avantajlı bir konum elde eder (Akman, 2023).

Uluslararası Af Örgütü (Amnesty İnternational) tarafından 2017 yılında yapılan bir araştırma doğrultusunda yaşları 18-55 arasında değişen kadınlar hedef kitle kullanılarak bir anket çalışmasında bulunulmuştur. Söz konusu anket Birleşik Krallık, ABD, Yeni Zelanda, İspanya, İtalya, Polonya, İsveç ve Danimarka'da uygulanmıştır. Bu ankette katılımcılara çevrim içi tacize ilişkin sorular yöneltilmiştir. Ankete katılan kadınların toplam %23'ü en az bir kere halihazırda çevrim içi tacize uğradığını belirtmiştir. Birleşik Krallık'ta bu oran %22 iken, İtalya ve Danimarka'da %17 olarak tespit edilmiştir. Çevrim içi tacizlerin gerçekleştirildiği sosyal medya platformlarına bakıldığında ülkeden ülkeye popülerlik seviyelerine göre farklılık gösterdiği görülmektedir. Bununla birlikte genele bakıldığında en çok bahsi geçen sosyal medya platformunun Facebook olduğu görülmektedir. Facebook'u takip eden diğer platformlar Instagram, Whatsapp ve Twitter şeklindedir. Söz konusu siber

tacizlerin önlenmesine yönelik özellikle de yukarıda belirtildiği üzere bu siber tacizlere maruz kalan kadın ve çocukların siber şiddete karşı korunmasına yönelik olarak uluslararası alanda çeşitli insan hakları bildirge ve anlaşmaları bulunmaktadır. Bunlar arasında Kadınlara Karşı Her Türlü Ayrımcılığın Önlenmesi Sözleşme (CEDAW), Kadına Yönelik Şiddetin Ortadan Kaldırılmasına Dair Bildirge (DEVAW), the Beijing Declaration and Platform for Action (Pekin Deklarasyonu) örnek olarak gösterilebilir. Ayrıca, uluslararası insan hakları hukukunda "CyberVawg"ı tanıyan çeşitli Birleşmiş Milletler kararları da bulunmaktadır (University of Ljubljana Faculty, 2017).

Bu başlık altında incelenen bir diğer terim olan "siber zorbalık" için ise en eski tanımlardan birisi Bill Belsey tarafından sunulmuştur. Belsey'in yaptığı tanıma göre siber zorbalık "*bir birey veya grup tarafından kasıtlı, tekrarlanan ve düşmanca davranışları desteklemek için bilgi ve iletişim teknolojilerinin kullanılması*" şeklinde nitelenmiştir. Bu tanımdan da görüleceği üzere siber zorbalıkta söz konusu fiil tesadüfi olarak işlenememektedir (Haava, 2017). Avrupa Konseyi Siber Suçlar Sözleşmesi Komitesi tarafından yapılan tanımda siber zorbalık "*bilgisayar sistemlerinin, bireylere karşı zararla sonuçlanan veya sonuçlanması muhtemel olan şiddete neden olmak, şiddeti kolaylaştırmak veya şiddetle tehdit etmek için kişinin içinde bulunduğu koşulların, kişinin zayıflıklarının istismarına yol açacak şekilde kötüye kullanılması*" şeklinde tanımlanmıştır. Bu tanımda ana odak noktası siber zorbalık olmakla beraber hukuki olarak bağlayıcılığı olmayan bir tanımdır (Navarra ve diğer., 2021). Siber zorbalık genel mahiyeti itibariyle gençlere karşı yoğun olarak kullanılan yöntemleri bünyesinde barındırmaktadır. Bu yöntemlerin ilki yazılı ve sözlü davranışlardır. Öyle ki söz konusu davranışlar telefon görüşmeleri, metin mesajları, e-posta, blog, web siteleri ve sosyal medya platformları aracılığıyla yapılabilmektedir. İkinci olarak bu yöntemler görsel davranışlar ve dokümanlar şeklinde ortaya çıkabilmektedir. İnternet ortamında yayımlanan resim ve video görüntüleri buna örnektir. Bir kişiye karşı yapılan ve o kişiyi belirli bir gruptan kasıtlı olarak dışlama fiili ile de siber zorbalık yapılabilir. Başka kişilerin adlarını ve hesap bilgilerini kullanarak kişisel bilgilerini ele geçirmek ve ifşa etmekle birlikte ortaya çıkan kimliğe bürünme fiili de yine siber zorbalığın ortaya çıkmasında ana kategorilerden biri olarak sayılabilir (Schultze-Krumbholz ve diğer., 2012).

Siber Suç

Siber suç kavramı gelişen ve sürekli değişen teknolojik gelişmelerle yeni dinamikleri de beraberinde getirmektedir. Siber uzayın zamandan ve mekândan bağımsız yapısının yanı sıra bağlamının genişliği ve faillerin kendisini saklayabildiği anonim özelliği dolayısıyla siber suç failleri için avantajlı bir konum oluşmaktadır (Payne, 2020). Siber suçlar yoluyla bilişim sistemlerinin gizlilik, bütünlük ve erişilebilirliği hedef alınmakta siber uzay bağlamında farklı seviyelerdeki tehdit odaklarından gelen eylemlerle ülkelerin kendi mevzuatlarında suç kabul edilen eylemler işlenmektedir (Bilgi Teknolojileri ve İletişim Kurumu, 2022). Siber suçlar için yapılan tanımlara bakıldığında "*bilgisayar veya bilgisayar ağları ve donanımları kullanılarak işlenen suç*" şeklindeki tanımın ön plana çıktığı görülmektedir (Gordon ve Ford, 2006). Ekonomik Kalkınma ve İş Birliği Örgütü (OECD) tarafından yapılan siber suç tanımı "*otomatik işleme tabi tutulan verilere karşı veya verileri nakil etme işlemlerinde yasaya, ahlaki değerlere aykırı veya yetkisiz bir şekilde gerçekleştirilen her türlü eylemler*" şeklindedir (Çolak, 2016). Avrupa Konseyi Siber Suçlar Sözleşmesi'nde (Sanal Ortamda İşlenen Suçlar Sözleşmesi-Budapeşte Sözleşmesi) siber suçlar "*bilgisayar veri ve sistemlerinin gizlilik, bütünlük ve erişilebilirliğine dolandırıcılık ve sahteciliğe, çocuk pornografisine, telif ve benzeri haklara yönelik bilgisayarla ilgili her türlü kötü niyetli eylemler*" olarak nitelendirilmiştir (Budapeşte Sözleşmesi, 2001). Siber suç farklı kaynaklarda karşımıza eş kullanımları ile de çıkabilmektedir. ABD'de hukuk terimleri sözlüklerinden biri olan Black's Law siber suça ilişkin tanımını "*elektronik olarak depolanan verilerin çalınması ve sabote edilmesi gibi bilgisayar kullanımını gerektiren bir suç*" olarak yapmıştır (Black's Law Dictionary, 2009). Buradan görüleceği üzere farklı tanımlamalarda karşımıza çıkabilecek olan bilgisayar suçu kavramı siber suçla eş anlamda kullanılmıştır. Yine Avustralya'da kullanılan Australian Law Dictionary'e göre internet suçu siber suçla eş anlamda kullanılmaktadır. Bu sözlüğe göre siber suç "*internet, telefon ve kablosuz teknolojileri kapsayan iletişim teknolojileri alanında ortaya çıkan kriminal bir aktivite*" olarak tanımlanmıştır (Australian Law Dictionary, 2010).

Ülkemizde genişletilmiş bir tanım 2020-2023 Ulusal Siber Güvenlik Strateji ve Eylem Planı'nda kendisine yer bulmuştur. Söz konusu tanım "*bir bilişim sisteminin güvenliğini ve/veya buna bağlı verileri ve/veya kullanıcısını hedef alan ve bilişim sistemi kullanılarak işlenen suçlar*" şeklindedir. Strateji ve Eylem Planında 2023 yılı vizyonu için

belirlenen ana hedeflerden birisi de siber suçların asgari seviyeye indirilerek siber güvenlikle kapsamında suçlara karşı caydırıcılığın artırılmasıdır. Siber suçlarla mücadele, söz konusu dokümanda stratejik amaçlar arasında yer almaktadır. Planda, siber suçlarla mücadele için hem ulusal hem de uluslararası alanda iş birliği ve koordinasyona önem verilmesi gerektiği belirtilmiştir. Siber uzayın siber suçlar için geniş ve rahat bir ortam sağlamasından dolayı ülkelerin ulusal mülki sınırlarının ötesinde söz konusu suçların ortaya çıkabileceği değerlendirilmektedir. Bu çerçeveden bakıldığında dünyanın farklı coğrafyalarından fiziki sınırlar aşılarak internet ve ağ ortamında siber saldırılar gerçekleşmektedir. Bu da uluslararası iş birliğinin ne denli önem arz ettiğini ortaya koymaktadır (Ulaştırma ve Altyapı Bakanlığı, 2020). Bununla birlikte 2024-2028 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında da bir önceki stratejiye uygun olarak siber suçlarla mücadele hususuna vurgu yapılmış, siber saldırılar sonrasında kamu ve özel sektörü kapsayan zarara ilişkin yıllık maliyetin küresel olarak 9,5 trilyon dolar seviyelerine çıkacağı tahmininde bulunulmuştur. Yine bu belgede "Siber suçlarla mücadeleye yönelik kazanımların artırılması" başlıklı ulusal siber güvenlik hedefi ortaya konulmuştur (Ulaştırma ve Altyapı Bakanlığı, 2024). Siber suçlar kapsamında Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı bünyesinde yürütülen "Siber Ay" projesi çerçevesinde yapılan tanıma göre siber suç; "*bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzay kaynaklı olarak çeşitli tehdit odaklarından gelen ve kanunlara göre suç kabul edilen eylemler*" şeklindedir.

Diğer taraftan siber suçlar doğaları gereği mekândan ve zamandan bağımsız bir yapıda olduğu için suçun soruşturulmasında problemler yaşanmaktadır. Bu soruşturmanın yapılabilmesi teknik bilgiye sahip insan kaynağını ve yine teknik donanımı gerektirmektedir. İnternet servis sağlayıcılardan suç teşkil eden delillerin ve bilgi/belgelerin talep edilmesiyle söz konusu delilleri kullanacak kurum, kuruluş, kolluk ve yargı mensuplarına intikal etmesi arasında geçen süreler de uygulamada siber suçluların yakalanmasını zorlaştıran unsurlar arasındadır. Öyle ki süreyle yarışılan siber uzayda faillerin bulunması her geçen dakika hatta saniye zorlaşmaktadır. Bunun yanı sıra elektronik deliller üzerinde siber güvenlik açıkları dolayısıyla veriler taşınabilmekte, üzerinde değişiklik yapılabilmekte ve yok edilebilmektedir. Yine bu deliller üzerinde kolluk tarafından yapılan müdahaleler sonucunda deliller bozulabilmekte yahut usule ilişkin yanlışlıklar dolayısıyla hukuka aykırı delil

konumuna düşürülebilmektedir. Siber suç böyle bir bağlamda değerlendirildiğinde failler için uygun bir ortam oluşturmaktadır.

Bununla birlikte siber suç tabiri yerine bilgisayar suçu ve bilişim suçu kavramları da kullanılmaktadır. Siber uzay içerisinde yer alan tüm cihaz ve sistemler kullanılarak işlenen veya bu sistemlere karşı gerçekleştirilen siber saldırılar dolayısıyla bilişim suçları kavramı bilgisayar suçu kavramına göre ülkemizde daha çok tercih edilmektedir. Siber suç için kullanılan bir diğer ikame tabir ise "internet ortamında işlenen suç" şeklindedir. Öyle ki niteliği itibariyle siber suçlar çoğunlukla internet üzerinde ve ağ sistemine karşı işlenen suçlardır. Uluslararası literatürde de siber suçlar yerine kullanılan birçok farklı terim bulunmaktadır. Bunlara örnek vermek gerekirse; "digital", "virtual", "online", "high tech" ve ilgililik sıfatına göre "computer related", "internet related", "telecommunication related" ve "computer assisted" şeklinde kullanımların mevcut olduğu görülmektedir (Urbas ve diğer., 2004). Söz konusu terimler ülkelerin siber suçlara yaklaşım politikalarına göre farklılık arz etmektedir. BM kapsamında yürütülen siber suçlarla ilgili sözleşme çalışmaları temel alınarak sibere bağımlı (cyber dependant) ve siberle ilgili (cyber related) şeklinde ikili bir sınıflandırma yapıldığında bazı ülkeler siber suçların bilişim sistemleri vasıtasıyla işlenmesini temel alarak dar bir sınıflandırma yapmasına rağmen, diğer ülkeler siberin aracı kullanılarak işlendiği daha fazla suçu siber suçlar kapsamına almaktadır. Örneğin bilişim sistemleri vasıtasıyla hırsızlık, dolandırıcılık, internet ortamında çocuğun cinsel istismarı suçu da bu ülkelere göre "siberle ilgili suç" olarak kabul edilip siber suçlar kapsamına alınmaktadır. Son zamanlarda uluslararası sözleşmelerde tartışılan bir diğer alan da "siberle kolaylaşan (cyber enabled)" siber suçlar ifadesidir. Birçok suç türü siber araçlar vasıtasıyla kolaylıkla işlenebilmekte ve bu yorumla siberle kolaylaşan suçlar gündeme gelmektedir.

Uluslararası literatürde yukarıda yer verilen tanımların oluşturulmasında kullanılabilecek farklı yöntemler bulunmaktadır. Bu yöntemlerden biri aktör ve niyet tanımlama modelidir. Bu modelin sağladığı metodik süreç tanımlara farklı bir yaklaşım getirmektedir. Buradaki aktörden kasıt suç işleyen fail ya da varlıktır. Niyet ise oluşturulmak istenen zarar amacının ne olduğudur. Yani failin fiilini gerçekleştirme amacı ve güdüsü olarak nitelenebilecek bu terimin hukuk literatüründeki karşılığı saik olarak ifade edilebilir. Aktörün devlet olması durumunda niyetin sonucunun savaş veya türevleri olduğu sonucuna varılması ferdi saldırılara kıyasla daha muhtemeldir. Buna karşılık saldırının aktörü terörist

bir grup ise niyetin terörizm olduğu daha da belirginleşir. Ancak burada aktörlerin türüne göre niyetin kesin olarak belirlenemeyeceğini de bilmek gerekir. Yani yapılacak bu sınıflandırmada bir kesinlik bulunmamaktadır. Siber savaşa ilişkin nitelendirme yapılacak olursa saldırının aktörü olarak devletin kabulü durumunda ve askeri bir hedefe ulaşma gayesi varsa yapılan siber saldırı siber savaş olarak ortaya çıkar. Bunun tersine bir kişinin diğer bir kişiye psikolojik baskı amacıyla siber saldırıda bulunması siber zorbalık olarak nitelendirilebilir. Bir sonraki bölümde ayrıntılı olarak incelenecek siber saldırının aktör ve niyet tanımlama modelinde tanımı siber uzayda makul olarak zarara yol açması beklenebilecek eylem şeklinde yapılabilecektir. Bahse konu zarar ekonomik, psikolojik, itibari, stratejik ve benzeri alanlarda ortaya çıkabilecektir (Robinson ve diğer., 2015).

Dünya üzerinde gerçekleşen siber saldırıların suçun atfedilebilirliği kapsamında kim tarafından yapıldığı muğlaklık içerirken aynı zamanda finansörlüğün kimler veya hangi devletler tarafından karşılandığı da bir başka bilinmezlik ortamı oluşturmaktadır. Söz konusu tespitin yapılamaması siber terörizm ve siber suçlarla mücadelede en büyük engel konumundadır (Ulaştırma ve Altyapı Bakanlığı, 2013). Diğer taraftan uluslararası literatürde kabul edilmiş ortak bir siber suç tanımının olmamasından dolayı devletlerin mevzuatlarında siber suça yönelik müşterek bir kanuni düzenlemenin olmamasından dolayı siber suçluların soruşturulması, kovuşturulması ve bunun sonucunda cezai yaptırıma tabi tutulması mümkün olmamaktadır. Siber terörizmle mücadelede iş birliği büyük önem arz etmekle beraber ortak bir anlayışın olmaması siber saldırganların siber uzayda rahatlıkla hareket edebilmesine olanak tanımaktadır. Siber suçlara ilişkin ortak bir tanımın yapılması ve uluslararası alanda devletlerin kabul edeceği müşterek bir sözleşmenin imzalanması bu alandaki muğlaklığın giderilmesi açısından gerekli olmaktadır. Bu kapsamda siber suçlara karşı 2001 yılında imzalanan ve ülkemizin 2014 yılında tarafı olduğu Avrupa Konseyi Siber Suçlar Sözleşmesi (Budapeşte Sözleşmesi) ve Birleşmiş Milletler tarafından 74/247 sayılı kararla Bilgi ve İletişim Teknolojilerinin Suç Amaçlı Kullanımının Önlenmesine İlişkin Kapsamlı Uluslararası Sözleşme büyük önem arz etmektedir.

Kritik Altyapı

Devletlerin siyasi, stratejik ve ekonomik faaliyetleri için gerekli olan fiziksel ve sibere dayalı kritik sistem ve varlıklar kritik altyapı olarak nitelendirilmektedir. Birbirine bağlı ve bağımlı yapıda olan söz konusu alt yapıların birinde meydana gelen hasar veya

tahribat diğer altyapıları da etkilemektedir. Bu bağlamda devletlere yönelik siber saldırılar dolayısıyla bırakılan etki gittikçe yıkıcı bir hale dönüşmektedir. Özellikle son yıllarda teknolojinin gelişmesiyle birlikte kritik altyapılara ait fiziki sistemler bilgi ve iletişim teknolojilerine ilişkin altyapılara daha çok bağımlı hale gelmiştir. Bu sebeple söz konusu altyapıların ağ ve bilgi güvenliği kapsamında korunması gerekliliği artmıştır. Dolayısıyla kritik altyapılar siber uzam bağlamında gerçekleştirilen siber saldırıların açık hedefi konumuna gelmiştir. Endüstriyel kontrol sistemleri üzerinde gerçekleştirilen ve bilişim sistemlerini etkileyen siber saldırılar büyük tahribata ve bu vasıtayla toplumsal, ekonomik ve siyasi krizlere neden olabilmekte, siber terörizmin bir parçası olarak kullanılabilmektedir. Devletler arasında kullanılan bu yöntem, siber saldırı yapılan devletin askeri ve milli savunmasına dair dirençsizliğini tüm dünyaya ifşa eden operasyonlara dönüştürmektedir (European Commission, 2009). Kritik altyapılara yönelik siber saldırılarla devletlerin ulusal güvenliği, kamu güvenliği ve kamu düzeni olumsuz etkilenerek vatandaşların maddi ve manevi olarak hak kayıplarına ve menfaat ihlallerine maruz kalmasına yol açılabilmektedir. Kritik altyapılar bir yandan terörist faaliyetlerin hedefi konumuna gelirken, diğer taraftan siber saldırılar dolayısıyla kritik altyapılarda yıkıcı bir etki doğurarak toplumsal yaşamı olumsuz şekilde etkileyebilmektedir. Özellikle enerji, su yönetimi, sağlık, finans, elektronik haberleşme ve iletişim, bilgi teknolojileri, dijital altyapılar, nükleer, savunma sanayi ve devlet tesisleri gibi kritik altyapı sektörleri söz konusu siber saldırıların hedefi konumunda bulunmaktadır. Bu saldırılarda devletlerin vatandaşlarına verdiği hizmetler kesintiye uğrayabilmekte, büyük ekonomik kayıplar yaşanabilmekte, iletişim altyapıları tahribata uğratılarak ülkenin haberleşme ağı çökertilebilmekte, hastanelerdeki kayıt sistemlerine erişim sağlanarak sistemlerin kitlenmesine yol açılabilmektedir. Diğer taraftan su şebekelerine yönelik siber saldırılarda endüstriyel kontrol sistemleri ele geçirilerek zararlı maddelerin şebeke hattına dağıtılması ve vatandaşların sağlık problemleri karşılaşmasına yol açılabilmektedir. Kanalizasyon sistemlerine yönelik saldırılarda ise atık suların şebekeye normal dışı dağıtımına neden olunarak altyapıların zarara uğratılması, vatandaşların sağlık problemleri karşılaşması ve çeşitli diğer problemler ortaya çıkabilmektedir. Bankacılık sistemlerine yönelik siber saldırılarda vatandaşların maddi kayıpları söz konusu olmakta, nükleer tesislere yönelik saldırılarda ise büyük nükleer sızıntılar yaşanabilmektedir. Dijital altyapılara yapılan siber saldırılar genellikle ağ ve bağlantı kopması gibi problemleri doğurmakta elektronik devlet hizmetleri, kritik kamu hizmetleri ve kamu altyapıları zarar görmektedir. Savunma sanayine ilişkin saldırılarda devletlerin askeri sistemleri, deniz ve

hava seyrüsefer sistemleri, radar ve savunma sistemleri tahribata uğratılarak söz konusu saldırılarda verilen zararlar konvansiyonel savaşlarda destek unsuru olarak ön plana çıkmaktadır.

Birleşmiş Milletler tarafından yapılan kritik altyapı tanımı terörizm bağlamında şekillenmiş ve kritik altyapıları oluşturan tesislerin fiziki olarak ve internet yoluyla terör saldırılarına maruz kalmasının önlenmesinin büyük önem arz ettiği ifade edilmiştir. Bahse konu tanımda kritik altyapılar "*su gibi yaşamsal ürünlerin tedariklerinin sağlanması, enerji, ulaşım hizmetleri*" olarak sıralanmıştır (CTED, 2017). 2004 yılında Avrupa Birliği (AB) nezdinde Avrupa Komisyonu'nun yayımladığı "Terörizmle Mücadelede Kritik Altyapıların Korunmasına İlişkin Tebliğ"de kritik altyapılar "*kesintiye uğraması veya yok edilmesi durumunda vatandaşların sağlığı, emniyeti, güvenliği veya ekonomik refahı veya Üye Devletlerdeki hükümetlerin etkin işleyişi üzerinde ciddi bir etkiye sahip olan fiziksel ve bilgi teknolojisi tesisleri, ağları, hizmetleri ve varlıkları*" olarak tanımlanmıştır (European Commission, 2004) ABD'de milli standartların belirlenerek bu alanda çeşitli teknolojik faaliyetlerin yürütüldüğü NIST tarafından yapılan kritik altyapı tanımı ise "*fiziksel veya sanal olarak, ABD için hayati önem taşıyan sistem ve varlıklar*" olarak düzenlenmiştir (NIST, 2023b).

Ülkemizde söz konusu alanda yapılmış en önemli tanımlardan birisine Ulusal Siber Güvenlik Stratejisi 2013-2014 Eylem Planında (Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2013) yer verilmiştir. Ulaştırma ve Altyapı Bakanlığı tarafından yayımlanan 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında kritik altyapılara ilişkin tanım "*İşlediği bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar*" şeklindedir (Ulaştırma ve Altyapı Bakanlığı, 2020). Türkiye Bilimsel ve Teknik Araştırma Kurumu (TÜBİTAK) tarafından yayımlanan Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanında kritik altyapı tanımı "*işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim veya endüstriyel kontrol sistemlerini barındıran sistemler*" şeklindedir (TÜBİTAK, 2024)

Bilgi savaşı

Bilgi savaşı terimini tarihte ilk kullanan 1976 yılında Thomas Rhona olmuştur. Rhona'nın yaptığı tanım "*barış, kriz, krizin tırmanması, çatışma, savaş, savaşın sona erdirilmesi ve yeniden yapılanma/restorasyon spektrumundaki stratejik, operasyonel ve taktik düzeydeki rekabetler, rakipler, düşmanlar veya bunlar arasında hedeflerine ulaşmak için bilgi araçlarını kullanma*" şeklindedir (Libicki, 1995). Birleşmiş Milletler tarafından yayımlanan terimler sözlüğünde bilgi savaşı, siber savaş terimi ile aynı anlamda kullanılmıştır. Yapılan tanıma göre bilgi savaşı "*bilgisayar sistemlerinin düşman sistemlerine zarar vermek veya yok etmek maksadıyla kullanıldığı savaş tipi*" şeklindedir (Yayla, 2013a). ABD tarafından 1998 yılında yayımlanan Joint Doctrine for Information Operations isimli belgede bilgi savaşı tanımı "*bilginin yer aldığı ortamların ve bilginin kendisinin, düşman harp gücünü azaltmak ve yok etmek maksadıyla hedef alınması veya kendi lehte kullanılması faaliyetlerini içeren bir harekât türü*" olarak yapılmıştır (US Joint Chiefs of Staff, 1998). 1997 yılında John Arquilla ve David Ronfeldt isimli yazarlar tarafından "*ağ savaşları ve siber savaş*" olarak tanımlanan bilgi savaşı terimi, ağlarla ilgili bütünleşik yapıyı kapsamaktadır. Öyle ki buradaki tanımda yer verilen ağ savaşları, uluslararası düzeyde bilgiye ilişkin çatışma olarak nitelendirilmiş ve savaş açan fiilde bulunan tarafın özellikleri hakkında kamuoyunca bilinen gerçeklerin dezenformasyona uğratılması, bilgilerin manipüle edilerek gerçeklikten uzaklaştırılması ve bilginin değiştirilmesi gibi faaliyetleri de içine almaktadır. Bu terim sadece konvansiyonel askeri operasyon şeklinde değil, aynı zamanda politik, ekonomik ve toplumsal yönleriyle ortaya çıkmaktadır (Nocella ve Best, 2004).

Martin Libicki ise Rhona'nın tanımını uzun ve ayrıntılı bularak böyle bir tanımla bilgi savaşını nitelemek yerine, bu terimin daha anlaşılır olması adına bölümlere ayırma önerisini geliştirmiştir. Libicki bu öneride komuta ve kontrol, istihbarata dayanıklılık, elektronik, psikolojik, bilgisayar korsanlığı, ekonomik ve siber formları kullanmıştır.

Söz konusu formlar ve bunlara ilişkin tanımlamalara aşağıda yer alan Tablo 1'de yer verilmektedir.

Tablo 1. Libicki'nin Bilgi Savaşı Biçimlerine İlişkin Yedili Kategorizasyonu (Robinson ve diğer., 2015)

FORM	TANIM
Komuta ve Kontrol	Komuta etkinliğini bozmak için komuta merkezlerine veya komutanların kendilerine yapılan saldırılar
İstihbarata Dayanma	Rakibin farkındalığını azaltırken kendi durumsal farkındalığınızı artırmak
Elektronik	Kriptografi kullanımı ve bilgi aktarımı için fiziksel temelin bozulması (ör. radar karıştırma)
Psikolojik	Bilginin insan aklına karşı kullanılması (Askerlerin moralini bozmak veya sivil nüfusu etkilemek için propaganda yapılması)
Bilgisayar Korsanı	Bilgisayar sistemlerine saldırmak için virüslerin, mantık bombalarının ve Truva atlarının kötüye kullanılması
Ekonomik Bilgi	Bilgiye sahip olmak ve kontrol altında olmak güce götürür
Siber	Bilgi terörizmi, semantik saldırı, simülasyon savaşı, Gibson savaşı

Libicki'nin bu tabloda yer verdiği unsurlara bakıldığında terimi geniş anlamıyla analiz ettiği ve hassas içerikli mesajların gizliliği, konvansiyonel yollarla yapılan bilgisayar korsanlığı, bilgi terörizmi, semantik saldırı, simülasyon savaş ve istihbarata ilişkin hususları kapsama dahil ettiği görülmektedir. Bunların yanı sıra psikolojik boyutuyla da bilgi savaşı konusunu ele almıştır. Bu tablo bilginin insan aklına karşı kullanılması gibi uygulamalarla beraber askerlerin moralini bozmak veya sivil nüfusu etkilemek için propaganda yapılması ve yayılmasını da kapsamaktadır (Robinson ve diğer., 2015).

Denning (1999) ise bilgi savaşı teriminin ilk tanımı yapanlar arasında olmakla birlikte Rhona'nın yaptığı tanıma ikame bir tanım ileri sürmüştür. Bu tanım "*kazan-kaybet niteliğindeki bilgi kaynaklarına karşı saldırı ve savunma operasyonlarından oluşan doğrudan rekabet halinde olan saldırganlar ve savunucular arasında oynanan bir oyun*" şeklindedir. Denning önceki tanımlara kıyasla daha geniş bir tanım yapmıştır. Söz konusu alanın kapsamı dahilinde siber suçlar, kişilik haklarına ilişkin ihlaller ve kamu güvenliği gibi alanlarda yapılan saldırıların bulunabileceği belirtilmiştir. Tanımda adı geçen savunucular, bilgi savaşına konu olan bilgi ve verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini muhafaza etmek için savunma faaliyeti içerisinde hareket ederken, saldırganlar korunan bu alana girip zarar vermek saiki ile saldırı faaliyetleri yürütmektedir (Denning, 1999).

Bilgi savaşına dair yapılan bir diğer tanım ise "*düşmana karşı büyük avantaj, zafer, hedef elde etmek için bilgi kaynaklarını yok etmek, kullanmak veya tahrip etmek*" şeklindedir. Bu tanımın içeriğine bakıldığında bilgi savaşının kapsadığı eylemler tahdidi şekilde sayılmıştır. Geniş olarak bakıldığında ise somut olarak bu kapsama giren araçlar düşman hareketlerinin incelenmesi için kullanılan gözetleme sistemleri, son dönemde gelişen siber uzayda adını sıklıkla duyduğumuz casus uydular ve devletlerin istihbari olarak kullandıkları beşerî sistemlerdir. Diğer taraftan toplum üzerinde psikolojik olarak etki gücü ve potansiyeli olan argümanlar kullanılarak dezenformasyona yol açan faaliyetlerin yürütülmesi bilgi savaşının diğer yüzünü oluşturmaktadır (Shackelford, 2013).

Kopp, bilgi savaşının amacının: "*kişinin kendi bilgilerinin gizliliğini, bütünlüğünü ve kullanılabilirliğini korurken düşmanın bilgi sistemlerini ve süreçlerini bozmak, zarara uğratmak, istismar etmek ve kullanmak*" olduğunu belirtmiştir (Kopp, 2000). Bu tanım çerçevesinde bilgi savaşının siber uzayı da kapsadığı ve bununla birlikte siber savaşta tarafların sistemlerine ilişkin birçok yıkıcı faaliyeti içermesinden dolayı geniş olarak yorumlandığı görülmektedir. Diğer taraftan bilgi savaşının siber savaşı kapsamına alıp almadığı yani siber savaşın bir bilgi savaşı çeşidi olup olmadığı tartışmalıdır. Bu nedenle siber savaş kavramının da açıklanması önem arz etmektedir (Denning, 1999).

Siber Savaş - Siber Kullanılan Savaş

Teknolojinin gelişmesiyle son dönemlerde ortaya çıkan ve siber uzay olarak nitelendirilen sanal alem askeri konvansiyonel savaş tiplerinin ardından gelen yeni bir savaş alanı şeklinde literatüre girmiştir. Bilgi ve verilerin siber ortam bünyesinde bulunduğu, verilerin bu ortamda işlendiği, orduya ait silah ve teçhizatın siber uzayda yönlendirildiği, insansız hava araçlarının siber ortamda keşif, gözetleme ve silahlı araçlar vasıtasıyla hedefleri imha etme gibi yönlerinin de bulunduğu göz önüne alındığında kara, deniz, hava ve uzaydan sonra beşinci savaş alanın siber uzay olduğu söylenebilecektir. Yeni gelişen bu ortama göre devletlerin savaş stratejileri de farklılaşıp gelişmektedir. Siber savaşın tanımlanmasında en büyük problem yaratan nokta, uluslararası hukukun uygulandığı silah kullanımına dayalı suçlara ilişkin normların siber savaşa uygulanıp uygulanamayacağı meselesidir (Yayla, 2013a). Bu minvalde Alford (2001) tarafından yapılan siber savaş tanımı "*bir rakip sistemdeki yazılım kontrol süreçlerine karşı yürütülen ve karşı tarafı milli iradelerini yerine getirmeye zorlamaya yönelik her türlü hareket*" şeklindedir (Alford, 2001). Söz konusu tanıma bakıldığında buradaki amacın devletlerin kendi iç gündemlerini belirlemek amacıyla girişimde bulundukları argüman olarak nitelendirildiği görülmektedir. Ancak ulusal gündemle ilgisi olmayan dinsel inanışlar ve ideolojik düşünceler de siber savaşın konusunu oluşturabilmektedir. Bu yönüyle bakıldığında ulusal gündemi belirlemenin tek bir bakış açısıyla ve sadece bu saikle tanımlanması tartışma konusu olmuştur (Robinson ve diğer., 2015). Jeffrey Carr (2012) ise siber savaşı "*savaşmadan savaşma sanatı ve bilimidir; bir rakibi kanını dökmeden yenmek*" olarak tanımlamıştır (Carr, 2012). Bu tanımın siber savaşa sebep olan saldırganların saldırı motivasyonlarına dair herhangi bir ifade içermemesi eleştirilmiştir. Yine tanımda tartışılan bir diğer nokta ise kan dökülmeden siber savaş olup olamayacağı meselesidir. Örneğin enerji kritik altyapıları veya elektrik şebekelerine yapılan siber saldırı sonucunda can kaybının yaşanması muhtemeldir. Hal böyle iken kan dökmeden siber savaşın yapılabileceği argümanı sekteye uğramaktadır (Robinson ve diğer., 2015). Colarik ve Janczewski (2011) bu konuda kan dökülmeden siber savaşın olamayacağını savunmuştur (Colarik ve Janczewski, 2011). Parks ve Duggan'ın (2011) sunduğu tanıma göre bu terim *"bilgisayar ağı saldırı ve savunma ile özel teknik operasyonların bir birleşimi"* şeklinde tanımlanmalıdır. Söz konusu tanım geniş şekilde oluşturulmasının yanı sıra tanımda geçen "özel teknik operasyon" ifadesinin kapsamı

muğlaklık içermektedir. Ancak bu terimi tanımlayan kişiler ABD Savunma Bakanlığı belgelerine atıfta bulunarak söz konusu nitelemeyi yapmıştır (Parks ve Duggan, 2011).

Taddeo (2022) tarafından yapılan tanıma göre siber savaş "*bir devlet tarafından onaylanan ve düşman kaynaklarının derhal kesilmesini veya kontrolünü amaçlayan, hem fiziksel hem de fiziksel olmayan alanlarda değişen ajanlar ve hedeflerle yürütülen, şiddet düzeyi koşullara göre değişebilen bir saldırı veya savunma askeri stratejisi dahilinde, BİT'in belirli kullanımlarına dayanan savaş*" şeklinde nitelendirilmiştir. Bu tanıma bakıldığında derhal kesilme ibaresine ilişkin kısım eleştirilmiştir. Öyle ki bazı saldırı tipleri anlık değil etkisi sonradan çıkan gecikmeli sonuçları oluşturabilmektedir. Bunun yanı sıra hedef olarak nitelenen odakların fiziki olan ve olmayan şekilde ayrıştırılabileceği önermesi siber savaşa ilişkin yapılan diğer tanımlardan bu tanımı ayıran noktadır. Öyle ki siber savaşın kinetik etki yaratma olasılığı da bu tanımda kendisine yer bulmuştur (Taddeo, 2012).

Hukuki boyutuyla siber savaş incelendiğinde bazı yazarlara göre siber saldırı kullanılarak yapılan saldırıların savaş sebebi olamayacağı, devletin politikası kapsamında uygulanan siber saldırının tahribat oluşturma, casusluk veya sabotajda bulunmak için kullanılabileceği değerlendirilmektedir. Diğer taraftan siber saldırılara ilişkin bu zamana kadar karşılaşılan dünya örneklerine bakıldığında uluslararası hukuk bakımından BM Şartı 51. maddesinin gündeme gelmesi söz konusu olmaktadır. Söz konusu maddede haksız saldırılara karşı devletlerin meşru müdafaa hakkı düzenlenmektedir. Bazı görüşlere göre bu madde kapsamında meşru müdafaa şartları oluştuğu takdirde somut olaylara uygulanabileceği değerlendirilmektedir. Yine burada silahlı çatışma hukuku kapsamında değerlendirme yapıldığında saldırıya uğrayan devletçe siber saldırıya karşı meşru müdafaa hakkının gündeme geleceği düşünülmektedir (Yayla, 2013a).

Diğer taraftan **"**siber savaş" ile bu terimle sıklıkla karşılaştırılan "siber kullanılan savaş" kavramı arasında küçük farklılıklar bulunmaktadır. Bu farklılığın temelinde siberin amaç veya araç olarak kullanılma düşüncesi yatmaktadır. Küresel siber literatüründeki kullanımı ile "cyber warfare" siber saldırıların savaş benzeri bir niyetle kullanılmasıdır. Bu terim, savaş durumunda stratejik hedeflere ulaşmak amacıyla konvansiyonel araç ve silahların kullanılmasının yanı sıra siber saldırıların da kullanılması durumunu anlatır. Buna karşılık yine küresel siber literatüründeki kullanımı "cyber war" olan terim ise bir devletin

karşı tarafa savaş ilan etmesi halinde bu savaşta sadece siber savaş unsurlarının kullanıldığı durumları nitelemektedir. Bu farklılığı bir örnekle açıklamak gerekirse bir ülkenin diğer bir ülkeye karşı açıkça savaş ilan ettiği ve siber saldırıları da koordineli şekilde kullandığı bir durumda saldırıya uğrayan ülkenin elektrik kaynaklarının kesintiye uğratıldığını varsayalım. Saldıran ülke elektrik kesintisinden faydalanmış ve bir hava harekâtı düzenleyerek karşı tarafın askeri üslerini bombalamaktadır. Bu senaryoda hava saldırısının da yapılmasıyla kinetik bir saldırı kullanılmış olacaktır. Yani bu savaş türünde siber savaş tek bir savaş türü olarak kullanılmadığı için doğrudan siber savaş terimi burada kullanılmaz. Bunun yerine hem kinetik hem de siber savaşın kullanıldığı savaş olarak tanımlanabilir. Bir diğer örnekte ise bir ülke bir başka ülkeden gelen siber saldırılara maruz kalmaktadır. Amacı saldırılan ülkedeki ticari bilgileri o ülkenin ticaret bakanlığından çalmaktır. Siber saldırıların devlet destekli ya da devlete ait olduğuna dair kanıt olmamakla birlikte yazılımsal kodlar o ülkenin sorumlu olabileceğine delil başlangıcı kabul edilebilir. Burada elde edilmek istenen finansal bilgiler suç benzeri amaç olarak kabul edilebilir ve devletlerarası ticari ilişkilerde haksız rekabete yol açabilecek uygulamalara neden olabilir. Burada devletlerin gizli bilgilerini elde etmek aynı zamanda siber casusluk olarak da nitelenebilir. Niyet ve aktörle ilgili bilgiler arttıkça sonuç kesin bir hal alacak ve ayrım daha net şekilde yapılabilecektir (Robinson ve diğer., 2015).

Devletler bünyelerinde barındırdıkları kritik ve hassas verileri siber alanlarında muhafaza etmektedir. Söz konusu verilerin bu alanlarda muhafaza edilmesi devletler arasında yaşanabilecek savaş durumlarında söz konusu verilerin açık hedef konumuna düşmesine yol açmaktadır. Bu sebeple geleneksel savaş yöntemlerinin yanı sıra siber alanın savunulması da yeni bir savaş cephesinin savunulması gibi gerekli olmaktadır. Bu savunma için en önemli gereklilik ise siber alandaki yeteneklerin artırılarak siber savunma sistemlerinin hayata geçirilmesidir (Yayla, 2013a). Bu alandaki tehdit unsurları devletleri kritik bilişim sistemlerini korumak üzere konuşlandırılmış organik yapıları kurmaya yöneltmiştir. Siber savaşa yönelik tarih ABD-Irak arasında yaşanan Körfez Savaşındaki hava yolu ile yapılan saldırılara kadar gitmektedir (Yayla, 2013a; Conway, 2014). Söz konusu savaş sonrasında ABD tarafından askeri sistem içerisine entegre edilen Bilgi Savaşı Merkezi (Info War Center) hayata geçirilmiştir. Bu merkeze ek olarak ABD Ulusal Savunma Üniversitesi kapsamında siber savaşlarda görevlendirilecek askeri personelleri yetiştirecek okullar hayata geçirilmiştir (Yayla, 2013a). Sonraki dönemlerde ABD'de siber alanın ulusal

kapsamda hangi kurum veya kuruluş tarafından koordine edileceği konusu gündeme gelmiştir. Söz konusu alandaki boşluk ABD Uzay Komutanlığı'nın (Space Command), Stratejik Komutanlığa (Strategic Command-STRATCOM) çevrilmesiyle birlikte dolmuştur. STRATCOM tarafından siber savaş durumlarında operasyonların yönetilmesi ve koordinasyonu görevi tanımlanmıştır. STRATCOM bünyesinde 2010 yılında Siber Komutanlık (CYBERCOM) kurulmuştur (Yayla, 2013a; Foltz, 2004). Bu komutanlık siber saldırılara karşı devletin siber savunma güvenlik mekanizmasını yöneterek gerekli durumlarda karşı misilleme çerçevesinde siber saldırıda bulunmak görevlerine haizdir. Siber alanda ABD'nin en büyük rakiplerinden olan Çin ve Rusya da siber saldırılara karşı savunma araçlarını geliştirerek söz konusu alanda ABD'nin tek başına bir güç olmadığını fiilleri ve oluşturdukları savunma sistemleri ile ortaya koymaktadırlar. Çin tarafından kurulan Milli Özgürlük Ordusu konvansiyonel savaş ortamındaki (kara, deniz, hava) savunma önlemlerini siber uzaya da taşıyarak muhtemel siber saldırılara karşı stratejiler geliştirmiştir. Rusya tarafından söz konusu alanda saldırı ve savunmaya yönelik olarak yazılımlar geliştirilmiş aynı zamanda siber saldırılarla karşı devletlerin kritik altyapı ve sistemlerine sızacak zararlı virüsler halihazırda geliştirilmektedir. Son zamanlarda kapalı kutu olarak değerlendirilen ancak tüm dünyayı elindeki potansiyel güçlerle korkutan Kuzey Kore'ye bakıldığında "Unit 121" isimli kuruluş dikkat çekmektedir. Bu kuruluş da siber saldırılara karşı oluşturulmuş bir üs konumunda bulunmaktadır. Bu üste stratejik ve uygulamaya yönelik programlar hazırlanarak siber saldırı ortamına hazırlık yapılmaktadır (Aldoori, 2020).

Siber savaşların tarihine bakıldığında Çin ve Tayvan arasındaki savaş siber savaşın ilk örneklerinden biri olarak gösterilmektedir. Bu devletler arasında meydana gelen siyasi anlaşmazlık kendisini siber alana taşıyarak Çin tarafından yapılan siber saldırılarda Tayvan'a ait bilişim sistemleri hedef alınmıştır. Bunun gibi 2008 yılında meydana gelen Rusya ve Gürcistan çatışması, siber alanda meydana getirilen dezenformasyon çalışmaları ile alevlendirilmiştir. Öyle ki Rusya tarafından Gürcistan'a ait web siteleri hedef alınarak siber saldırılar vasıtasıyla söz konusu sitelerde yer alan haberlerin içerikleri değiştirilmiştir. Bu da Gürcistan halkının hem kendi devletine hem de var olan savaşa bakış açısını değiştirmiştir (Aldoori, 2020). Yine 2003 yılında meydana gelen ABD-Irak savaşında Pentagon tarafından Irak Savunma Bakanlığı'nın kendi ağlarına sızılarak Irak askerlerine savaşı bırakarak teslim olmalarına yol açan mesajların iletilmesi sağlanmıştır (Attrill, 2015).

Diğer taraftan siber suçların faili herkes olabilmektedir ve hedef kitlesinde ekonomik kazanç veya başka kişisel menfaatler elde edilebilecek bireyler bulunmaktadır. Bunun gibi siber terörü işleyen kişiler de devlet dışı süjeler olabilmektedir. Devletlere karşı yapılan ve siber teröre yol açan fiiller devletlerin kritik alt yapılarını kullanılamaz hale getirmektedir. Siber terörün amaçları arasında devletlere yönelik olarak siyasi ve ideolojik saikler olabilmektedir. Bununla birlikte siber terör vatandaşların devletlerine olan güvenini zedeleyecek sosyal amaçlı saldırılara da konu olabilmektedir. Bu saldırılarda vatandaşları korkutmak ve belirli davranışlara zorlamak üzerine planlar inşa edilmektedir. Ancak bunlardan farklı olarak siber savaşa yol açan fiiller sadece devletler veya devlet destekli süjeler arasında siyasi olarak saldırı ve savunma amaçlı gerçekleşmektedir (Aldoori, 2020; University of Ljubljana Faculty, 2017). Hukuki anlamda siber suçlar düzenlemede bulunulan yerli hukuk kurallarına göre cezalandırılmaktadır. Siber terör eylemleri ulusal olabileceği gibi uluslararası boyutlara ulaştığında milletlerarası hukuk kurallarına tabi olabilmektedir. Siber savaşa ilişkin hususlar ise sadece milletlerarası hukukun konusuna girmektedir. Bunların ortak bileşeni ise her birinde siber saldırı üzerinden karşı tarafa zarar verilmesi ve suçun işleniş biçiminin bilişim sistemleri olmasıdır.

Siber uzay içerisinde devletlere yönelik saldırıların iki farklı hedef alanı bulunmaktadır. Bunların ilki devletlerin günlük kamusal işlemlerini yürüttüğü ticari internet olarak nitelendirilen alandır. Bu alanı hedefine alan kitle, genel olarak devlet dışı aktörlerdir. Söz konusu alandaki siber kırılganlık Estonya ve Gürcistan saldırılarında kendisini göstermiştir. İkincisi ise askeri sistemlerin hedef olarak alındığı devletler arası siber savaşların kendisini gösterdiği alandır. Bu alan içerisinde siber saldırılara karşı korunma yeteneğini geliştiren askeri ağlar ön plana çıkmaktadır. Bu ağlar vasıtasıyla siber saldırı anında meydana gelen zarar önemli ölçüde azaltılmış olmakla birlikte bu ağların varlığı siber saldırılara ilişkin siber hassasiyetin artmasına neden olmaktadır. Söz konusu ağlar diğer devletlerin açık hedefi konumunda ortaya çıkmaktadır. Bu saldırılara ilişkin doğru savunma politikalarının oluşturulması ise siber tehditlere yönelik analizlerin ayrıntılı şekilde ele alınması ile gerçekleşmektedir. Öyle ki siber alanda gün geçtikçe gelişen farklı teknolojiler ve teknik kapasitenin artması bu analizlerin üzerine daha çok düşülmesini gerekli kılmıştır (Conway, 2014; Denning, 2006; Yener, 2013).

Konvansiyonel savaşların yerini alan siber savaşlarda bilişim sistemlerine yönelik yapılan saldırıların yanı sıra söz konusu saldırıların devletlerin kritik alt yapılarını ve fiziksel sistemlerini de etkileyebildiği bir ortam oluşmuştur. Söz konusu saldırılar neticesinde devletlerin sahip olduğu enerji tesislerine yönelik fiziki tahribatta bulunulabilmektedir. Öyle ki bir nükleer santralin bilişim sistemine yönelik yapılan siber saldırı sonrasında, söz konusu tesisin radyoaktif maddeleri kullanan nükleer reaktörlerinin teknik ayarlarında değişiklik oluşturularak üretilen elektrik enerjisi miktarı bundan etkilenebilmektedir. Bunun gibi vatandaşların temel ihtiyaçlarını etkileyecek şekilde elektrik, su, doğal gaz gibi temel ihtiyaca yönelik tesisleri etkileyen saldırı durumunda da olumsuz etkiler ortaya çıkmaktadır. Söz konusu alanlarda devletlerin bünyesinde bulundurduğu kritik tesisler siber saldırıların etkisi ile işlemez hale gelerek vatandaşların bu hizmetlere erişimi engellenebilir. Kısa süreli bu olaylarda vatandaşların devlete olan güveni azalacağı gibi uzun süreli olaylarda da sosyal krizlerin yaşanması kaçınılmazdır. Diğer taraftan söz konusu tesisler sadece amaç olarak değil araç olarak da kullanılabilmektedir. Örneğin siber saldırılarla bir doğalgaz santralinin basınç derecesi yükseltilerek patlayıcı bir güç oluşturulabilmektedir. Bunun yanı sıra su kritik alt yapılarına yapılan saldırı durumları özellikle de barajlara yapılan saldırı durumlarında sisteme erişim sağlanarak suyun kontrolü durdurulamaz şekilde etkilenebilir. Bu durumda baraj sularının taşarak su basması riskleri ile karşı karşıya kalınacaktır. Yine bunun gibi elektrik santrallerinde oluşturulabilecek sistem arızaları vasıtasıyla yüksek gerilim oluşturularak üretim tesislerini de etkileyecek geniş çaplı saldırılar gerçekleştirilebilir. Haberleşme alt yapısına yönelik saldırılarla tüm iletişim kesilmesine kadar ulaşabilecek riskler oluşabilmektedir (Yayla, 2013a). Söz konusu kritik altyapılara yönelen siber saldırılar dolayısıyla vatandaşlar olumsuz etkilenerek maddi ve manevi hak kayıplarına uğrayabilmektedir. Bununla beraber siber terörizme vücut veren ve ölümle sonuçlanan saldırılarla birlikte mal varlığı değerlerinin azalmasına sebep olan saldırılar da gerçekleşebilmektedir.

Siber Güvenlik

Güvenlik terimi köken olarak securitas" kelimesinden gelmektedir. Söz konusu terim "*kazanılmış değerlere yönelik tehdidin bulunmaması ve bu değerlere saldırılacağına dair korkunun bulunmaması*" olarak nitelendirilmiştir (Baldwin, 2003). Ülkemizde yapılan tanım ise "*toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet*" şeklindedir (TDK, 2022). Farklı bağlamlarda değişik

anlamlar kazanabilen bu kavram "*uluslararası sistemin bütününün ya da bütüne yakınının güvenliği", "coğrafi ya da işlevsel alt sistemlerin, bölgelerin güvenliği", "devletin güvenliği", "toplumun güvenliği", "toplumsal alt grupların güvenliği", "bireylerin güvenliği"* şeklinde alt kategorilerde sınıflandırılabilmektedir. Söz konusu sınıflandırmada güvenliğin gelişen teknoloji ile şekillenmesi ve dünya üzerinde yaşanan toplumsal olaylar etkili olmuştur.

İlk kez 1940'lı yıllarda ortaya çıkarılan bilgisayar virüslerine yönelik güvenlik önlemlerinin alınması gerekliliği 1970'li yıllarda mümkün hale gelmiştir. 1968 yılında Amerika Birleşik Devletleri Hava Kuvvetleri için geliştirilen bilgisayar ağı "Advanced Research Projects Agency Network (ARPANET)", siber güvenliğe dair ilk somut adım olarak atılmıştır. Bob Thomas tarafından bahse konu ARPANET geliştirilerek ağa bağlı bilgisayarlar kullanılmış ve makineler arası program geçişi sağlanmıştır. Bu sayede ilk kez solucan kötü amaçlı yazılımı siber güvenlik literatüründe kendisine yer bulmuştur. Yine bu dönemde ağ bağlantılı posta mesajlaşma sistemini geliştiren Ray Tomlinson tarafından "Creeper" isimli solucan keşfedilmiştir. Söz konusu solucanın bulaşı sağlanan cihazdan silinmesi amacıyla "Reaper" isimli program geliştirilmiştir (Bhadwal, 2023).

1986 yılında Lawrence Berkeley Ulusal Laboratuvarı doktoru Cliff Stoll tarafından ARPANET'in bağlı olduğu bilgisayarda ağ aracılığıyla gerçekleşen toplama işlemin hatası tespit edilerek bir siber güvenlik zafiyeti olarak nitelendirilmiştir. Söz konusu güvenlik zafiyeti Stoll tarafından kaleme alınan "The Cuckoo's Egg" adlı kitapta yayımlanmıştır. Bu kitapta yer verilen güvenlik zafiyetine ilişkin sistemsel müdahalelerin bilgisayar ağları vasıtasıyla gerçekleştirilebileceği tespiti yapılmıştır (QT Worldtel Inc., 2003). 1987 yılında ilk kez ticari antivirüs programları olan "Anti4us" ve "Flushot Plus" piyasaya sürülmüş ve toplumun siber güvenlik algısı oluşturulmaya başlanmıştır. Bu antivirüs programlarına karşılık siber saldırganlar tarafından çeşitli yeni yöntemler kullanılarak programlar etkisiz hale getirilmeye çalışılmıştır. Bunun akabinde 1994 senesinde Netscape tarafından Güvenli Hiper Metin Transfer Protokolünün (HTTPS) temelini oluşturan Güvenli Yuva Katmanı (SSL) protokolü geliştirilerek gizlilik ve güvenlik artırıcı sunucu-istemci modelinde şifreli iletişim kuran yapı ortaya çıkarılmıştır (Bhadwal, 2023).

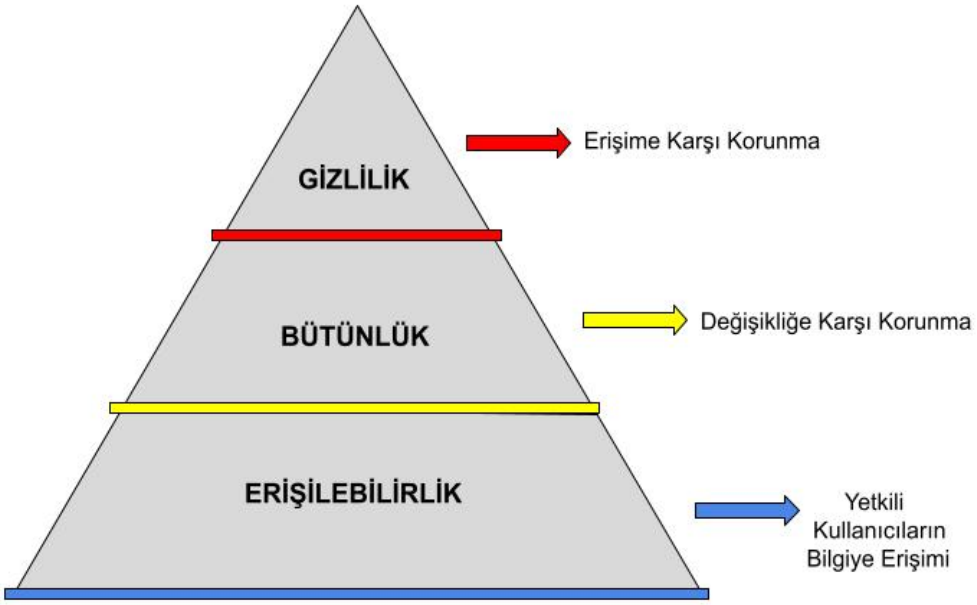
Uluslararası alanda yapılan siber güvenlik tanımları çeşitlilik barındırmakla beraber bu tanımların genelinde siber uzay bağlamında gerçekleşen siber saldırılara karşı alınan siber savunma önlemlerinin geçtiği görülmektedir. Uluslararası Telekomünikasyon Birliği (ITU) tarafından yapılan siber güvenlik tanımı "*siber ortamı, kuruluşları ve kullanıcıların varlıklarını korumak için kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitimler, en iyi uygulamalar, güvence ve teknolojiler bütünü*" şeklindedir (International Telecommunication Union, 2020). NIST ise siber güvenliği "*siber uzay kullanımını siber saldırılardan koruma veya savunma yeteneği" olarak tanımlamıştır* (NIST, 2019). ABD Savunma Bakanlığı tarafından yapılan bir diğer tanım ise "*platform bilgi teknolojisi de dahil olmak üzere diğer bilgi teknolojileri, elektronik iletişim sistemleri ve bilgisayarların içerdiği bilgilerin kullanılabilirliğini, bütünlüğünü, kimlik doğrulamasını, gizlilik ve reddedilme özelliklerini koruyan, yetkisiz erişimleri önlemek için erişim, kullanım veya bilgisayarlara zarar vermeyi önleme gibi siber alanda yapılan işlemler*" şeklindedir (U.S. Department Of Defense, 2020). Ulusal siber güvenlik kaynaklarımıza bakıldığında ise siber güvenlikle ilgili tanıma 2020-2023 Ulusal Siber Güvenlik Strateji ve Eylem Planı'nda yer verildiği görülmektedir. Söz konusu tanım "*siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin/verinin gizliliği, bütünlüğü ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber olayların tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber olay öncesi durumlarına geri döndürülmesini kapsayan faaliyetler bütünü*" şeklindedir.

Bilgi Güvenliği

Siber güvenliğin unsuru ve bir alt kümesi şeklinde nitelendirilebilecek bilgi güvenliği bazı yönleriyle siber güvenlikten farklılaşmaktadır. Siber güvenliğin ana amaçlarından birisi de bilgi ve veri güvenliğinin sağlanmasıdır. Bilgi güvenliğinden farklılaşan yönü ise kompleks bir yapıda siber saldırılara karşı siber savunma yöntemlerini içermesidir. NIST tarafından yapılan bilgi güvenliği tanımı "*gizlilik, bütünlük ve kullanılabilirlik sağlamak için bilgi ve bilgi sistemlerinin yetkisiz erişime karşı korunması*" şeklindedir (NIST, 2019). Bununla beraber "*gizliliği, bütünlüğü ve kullanılabilirliği sağlamak amacıyla bilgi ve bilgi sistemlerinin yetkisiz erişime, kullanıma, ifşa edilmeye, bozulmaya, değiştirilmeye veya yok edilmeye karşı korunması*" tanımı da NIST belgelerinde geçen bir diğer tanımdır (NIST,

2017). Ulusal literatüre bakıldığında 2020-2023 Ulusal Siber Güvenlik Strateji ve Eylem Planı'nda bilgi güvenliği tanımının yapıldığı görülmektedir. Söz konusu tanım "*bilişim sistemlerinin ve bilgilerin izinsiz kullanımını, yetkisiz kişilerce erişilmesini ve ifşa edilmesini, silinmesini, değiştirilmesini ve zarar görmesini engellemek, bu sistem ve bilgilere yetkili kişiler ve işlemlerin ihtiyaç duyulan zamanda ve kalitede erişebilmesini sağlamak için yürütülen faaliyetler bütünü*" şeklindedir (Ulaştırma ve Altyapı Bakanlığı, 2020).

Bilgi güvenliği politikası; üçlü sacayağı olarak nitelendirilen gizlilik, bütünlük ve erişilebilirlik unsurlarının korunması maksadıyla uygulanan güvenlik stratejisi ve yöntemleridir. Bahse konu üç temel unsura aşağıdaki Şekil 1'de yer verilmektedir:



Şekil 1. Bilgi Güvenliği Politikası Unsurları

Bilgi güvenliği kapsamında ilk temel unsur olarak ön plana çıkan gizlilik, yalnızca bilgiye erişim yetkisine sahip olan kullanıcı ve işlemlerin bilgiye ve veriye erişimi olarak nitelendirilmektedir. Söz konusu bilgi ve veri üzerinde değişiklik yalnızca yetki tanınmış kişilerce yapılabilmektedir (Fruhlinger, 2020). 13/07/2014 tarihli ve 29059 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Elektronik Haberleşme Sektöründe Şebeke ve Bilgi

Güvenliği Yönetmeliğinde yapılan gizlilik tanımı "*bilginin yetkisiz kişiler, varlıklar ya da süreçler tarafından erişilememesini, kullanılamamasını, değiştirilmemesini, depolanmamasını, başka bir ortama kaydedilmemesini veya ifşa edilmemesini*" şeklindedir (Elektronik Haberleşme Sektöründe Şebeke Ve Bilgi Güvenliği Yönetmeliği, 2014). Bu unsur kapsamında kişilere ait kritik ve hassas veriler yetkisiz erişime karşı korunmaktadır. Bu unsurun sağlanmasında yetkilendirme denetimi, genel anahtar şifrelemesi, kimlik doğrulama, biyometrik uygulamalar ve şifrelemede kriptografik anahtarlar kullanılan araçlardır (Fruhlinger, 2020).

Bilgi güvenliği kapsamında sağlanması gereken ikinci temel unsur bütünlüktür. Söz konusu unsur bilgi ve verilerin tahrifata uğramayacak şekilde tutulması, korunması ve değişiklik yapılmaması anlamına gelmektedir (Fruhlinger, 2020). Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliğinde yapılan bütünlük tanımı "*varlıkların doğruluğunu ve tamlığını koruma özelliği*" şeklindedir (Elektronik Haberleşme Sektöründe Şebeke Ve Bilgi Güvenliği Yönetmeliği, 2014). Hem yazılımsal hem de donanımsal anlamda bilgi ve verilerin saklandığı merkezi yapıların korunması amacıyla bütünlük unsurunun uygulanması gerekmektedir. Fiziksel bütünlük kadar verilerin sanal bütünlüğünün sağlanması da bütünlük unsuru kapsamında ele alınmaktadır (Fruhlinger, 2020).

Bilgi güvenliğinin üçlü sacayağının son unsuru erişilebilirliktir. Bu unsur çerçevesinde bilgi ve veriye erişim yetkisine sahip kullanıcıların istedikleri zaman erişim sağlayabilmesi sağlanmaktadır (Fruhlinger, 2020). Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliğinde yapılan erişilebilirlik tanımı "*yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliği*" şeklindedir (Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği, 2014). Siber saldırı türleri arasında yer alan hizmet engelleme saldırıları vasıtasıyla bilgisayar ve sistemlerin hizmet veremeyecek duruma gelmesine yol açılmaktadır. Söz konusu unsur bakımından bilgi ve verileri muhafaza eden sistemlerin sürekli olarak çalışır durumda ve muhtemel ağ yüklerini karşılayabilecek seviyede olması önem arz etmektedir. Erişilebilirlik kapsamında mevcut sistem ve donanımların güncelliği, hizmeti kaldırabilecek seviyede bant genişliği ve bilişim sistemlerinin devre dışı kalması durumunda yük devri ve kurtarma

kapasitesi gibi unsurlar değerlendirilmekte ve denetime tabi tutulmaktadır (Fruhlinger, 2020).

NIST tarafından oluşturulan bilgi güvenliği politikası kapsamında üç temel strateji bulunmaktadır. İlk politika grubunu program politikası olarak bilgi güvenliğinin hayata geçirilmesi oluşturmaktadır. Söz konusu politika grubunda kuruluşların uluslararası standartlar çerçevesinde bilgi güvenliği programına yönelik hedefleri belirlenmekte ve uyumlaştırma çalışmalarına yönelik kılavuz faaliyetleri yürütülmektedir. İkinci politika grubunu oluşturan "soruna özel politika" kuruluşlara yönelik güvenlik problemlerine karşı rehberlik hizmeti sağlanmasıdır. NIST tarafından ifade edilen son politika grubu ise "sisteme özel politika"dır. Bu politika grubu sistemlere ait erişim kontrolleri ve eylem izinlerini de kapsamına alan güvenlik yapılandırma ve yöntemleri belirlemektedir (NIST, 2017).

Bilgi güvenliği kapsamında ön risk değerlendirmesi önemli bir yer tutmaktadır. Karşılaşılan siber saldırılar ve güvenlik riskleri bağlamında kuruluşların sahip olduğu kritik varlıkların tanımlanması, karşılaşılan güvenlik açıklıklarının belirlenmesi ve tespiti, kuruluşa ait risk önceliklendirilmesi yapılması söz konusu değerlendirmede büyük önem arz etmektedir. Bilgi güvenliği standartlarına uyum sağlanması, kuruluşa ait stratejik unsurların ortaya konulması ve amaçlara dair sınırların çizilmesi bilgi teknolojileri stratejilerinin hangi standartlar ve politikalar doğrultusunda uygulanacağını belirlemede ön plana çıkmaktadır. Bu kapsamda yetkilendirilmiş kişilerin güvenlik sorumluluk alanlarının belirlenmesi ve denetime tabi tutulması da zorunlu unsurlar arasındadır. Özellikle siber saldırı ve kriz anlarında yetkili kişi ve kritik varlıklara dair tespitler bilgi güvenliği çerçevesinde ele alınmalıdır. Bilgi güvenliği politikalarının oluşturulmasında kullanılan lafzın ve dilin çalışan herkes için anlaşılır olması, politika uygulayıcılar için kolaylık sağlamaktadır. Bu sebeple açık ve anlaşılır bir politika dili oluşturulması gerekmektedir. Kuruluşların gereksinimleri ve kritik varlıklarının değişkenlik gösterebileceği düşünüldüğünde uyumlaştırma yapılan bilgi güvenliği standartlarının kuruluşa özel şartlarla tanımlanması önem arz etmektedir. Bu kapsamda kuruluşa özel ihtiyaçların belirlenerek bu çerçevede bilgi güvenliği politikası oluşturulması gereklidir. Siber güvenliğin bir alt kırılımını oluşturan bilgi güvenliği kapsamında yeni siber saldırılara karşı popüler pasif caydırıcılık yöntemleri takip edilerek somut olay özelinde politikalar geliştirilmelidir. Bilgi güvenliği politikalarının kuruluşlarda geçerlilik kazanması ise yönetim politikalarının alt kademeden üst yönetime kadar fiili

şekilde uygulanması ile mümkün olmaktadır. Bu sebeple standartlar çerçevesinde hazırlanan bilgi güvenliği politikaları belirli periyotlarda güncellenmeli, çalışan personele eğitim verilerek kuruluştaki herkesin bu politikalara uyması sağlanmalıdır (Fruhlinger, 2020).

Siber Saldırı (Siber Eylem)

Siber saldırı kavramı "*bilgisayar sistemlerinin, teknolojiye bağımlı işletmelerin ve ağların kasıtlı bir şekilde istismar edilmesi*" şeklinde tanımlanmaktadır (Blank, 2008). Bu tanıma benzer olarak ülkemizde daha ayrıntılı olarak "*siber uzaydaki bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler*" şeklindeki tanıma 2020-2023 Ulusal Siber Güvenlik Strateji ve Eylem Planında yer verilmiştir (Ulaştırma ve Altyapı Bakanlığı, 2020). Söz konusu tanımlara bakıldığında saldırıların hedefinde bilgisayar ve bilişim sistemleri, işletmeler ve ağların olduğu görülmektedir. Bununla birlikte bilgi güvenliği unsurlarının da tehlike altında olduğu ve saldırılara yol açan fiillerin kasıtlı olarak işlendiği ifade edilmektedir.

Siber saldırılar üç farklı sınıfta kategorize edilebilmektedir. Bunların ilkini gizliliğe yönelik siber saldırılar oluşturmakta ve bu gruptaki saldırılar genellikle siber saldırganlarca dinleme ve yetkisiz erişim sağlama gibi fiilleri içermektedir. İkinci sınıfta yer alan siber saldırılar bütünlüğe yönelik siber saldırılar olmakla birlikte bilgi ve veri üzerinde gerçekleştirilen manipülatif faaliyetleri kapsamına almaktadır. Son sınıfta ise kullanılabilirlik veya erişilebilirliğe ilişkin siber saldırılar yer almakta ve hizmet engelleme saldırıları ve dağıtık hizmeti engelleme saldırıları gibi siber saldırı türleriyle sistemlerin istemcilere yanıt veremez hatta çalışamaz hale gelmesine yol açılabilmektedir (Kabano, 2023)

Bu minvalde siber saldırılar sistem ve ağ tabanlı saldırılar olması dolayısıyla hem donanım hem de yazılımsal olarak bilgi ve verinin silinmesi, yok edilmesi, tahrifata uğratılması ve değiştirilmesi gibi etkileri ortaya çıkarmaktadır. Bilgi ve iletişim teknolojilerinin gün geçtikçe ilerlemesi ve gelişimi ile birlikte siber saldırılar da çeşitlilik kazanmaktadır. Bu saldırılar siber suçların işlenme türleri veya yöntemleri şeklinde ifade edilmektedir. Bahse konu siber saldırı türleri bir sonraki bölümde ayrıntılı şekilde ele

alınmıştır. Siber saldırılara ilişkin dünya üzerinde çeşitli teknik standartlar yayımlanmakta, birçok strateji ve eylem planında öncül düzenlemeler hayata geçirilmektedir. Ülkemizde de belirli periyotlarda yayımlanan strateji ve eylem planları kapsamında siber saldırılarla etkin mücadelede bulunulmasına yönelik eylem maddeleri yer almaktadır. Ancak siber saldırıların sürekli değişen dinamik yapısı dolayısıyla bu alanda teknik donanıma sahip kişilerin devlet tarafından istihdam edilmesi gerekmektedir. Söz konusu teknik personelin yerli ve milli yazılımlarla yeni nesil aktif ve pasif caydırıcılık içeren siber savunma yöntemlerini hayata geçirmesi bu minvalde büyük önem arz etmektedir. Siber güvenlik önlemlerinin alınması ve bu kapsamda bilgi güvenliği unsurlarının kamu ve özel sektöre yaygınlaştırılarak geniş şekilde ele alınması gerekmektedir.

2. SİBER SALDIRI TÜRLERİ

Siber saldırı araçları, siber uzay bağlamında tekil olarak kullanılabildiği gibi siber saldırganlar tarafından daha güçlü etki bırakacak çeşitli saldırı tiplerini barındıran gruplar halinde de bir araya getirilebilmektedir. Siber saldırıların teknoloji ile birlikte çeşitlilik kazanması siber saldırganların yakalanmasını zorlaştırmaktadır. Bu doğrultuda siber suçun faillerine yönelik soruşturma ve kovuşturma faaliyetleri yargı mercileri tarafından yerine getirilemez hale gelmektedir. Özellikle bilgisayar korsanlığı, kötücül yazılım saldırıları, hizmeti engelleme ve dağıtık hizmeti engelleme saldırıları, fidye amaçlı yazılımlar, veri ihlali saldırıları, köle bilgisayar ağları, gelişmiş kalıcı tehdit saldırıları, sıfırıncı gün saldırıları ve ortadaki adam saldırıları son yıllarda ortaya çıkan en belirgin siber saldırılar olarak dikkat çekmektedir. Siber saldırılar farklılık arz etmekte bu yüzden de belirli bir sınıflandırma yapmak zor olmaktadır. Ancak literatür kapsamında söz konusu saldırı türleri aşağıda yer verilen Tablo 2'deki haliyle dört farklı kategoride incelenebilecektir:

Tablo 2. Siber Saldırı Türlerinin Sınıflandırılması



2.1. Kötü Amaçlı Yazılım İçeren Siber Saldırılar

Kötücül yazılım saldırıları (malware attacks) bir siber saldırı grubunun genel ismi olarak nitelenebilir. Söz konusu saldırı türleri kendi içlerinde farklı özellikleri dolayısıyla ayrılmaktadır. CISCO tarafından yapılan sınıflandırmaya bakıldığında bahse konu saldırı tipleri bilgisayar virüsleri, solucanlar, fidye yazılımlar, klavye kaydediciler ve casus

yazılımları olarak sıralanabilir (FIRAT, 2022). Bununla birlikte Truva atları, oltalama saldırıları, köle bilgisayarlar, tuzak veya arka kapılar ve spamlar da kötücül yazılım saldırıları şeklinde nitelenmektedir (Bettany ve Halsey, 2017). Bu saldırı türünde bilişim sistemlerine, bilgisayarlara ve ağlara erişim sağlanarak çeşitli yazılım ve donanım sorunlarına yol açılabilmekte, kullanıcıların erişimi kısıtlanabilmekte, kriptografik siber faaliyetler yoluyla erişim engellenebilmektedir (Kirwan ve Power, 2013). Kötücül yazılım saldırıları için yapılan bir tanım tüm bu hususların etrafında "*bilgisayarlara sızılarak sistemlerde zayiat yaratmak amacıyla oluşturulan bilgisayara yönelik programlar*" şeklinde oluşturulmuştur (Nandal, 2017). Kötücül yazılım saldırı çeşitleri aşağıda ayrıntılı şekilde incelenmiştir:

Bilgisayar Virüsleri (Computer Viruses)

Bilgisayar virüsleri, bilgisayarlara kullanıcı istemi dışında bulaşarak sistem içerisindeki verilerin, bilgilerin ve yazılımların deformasyona uğratılmasına yol açan yapay şekilde oluşturulmuş kötü amaçlı yazılım türleridir (Study.com, 2023). Virüsler, bilgisayar kodlama dili kullanılarak çeşitli yöntemlerle ağ üzerinden ya da harici depolama birimleri (ör:USB bellek) aracı kullanılarak bilgisayarlara gizlice sızan programlardır. Virüsler tarafından yayılan viral kodlar, belirlenen sisteme tutunarak bilgisayar üzerinde çeşitli olumsuz etkiler oluşturmaktadır. Özellikle ".exe" uzantılı dosyalar bilgisayarlara virüs bulaştırma açısından en sık kullanılan dosya uzantıları konumundadır. Öyle ki ".exe" uzantılı dosya çalıştırıldığında sisteme yayılarak çoğalmaktadır. Söz konusu çoğalma işlemi e-posta, program indirme, link bağlantısına tıklama, oyun veya videolarla bulaşmaktadır (BTK, 2022).

Bilgisayar virüsleri, sistem üzerinde ve sistemler arasındaki farklı programlara yayılarak çoğalmakta ve sistemler üzerinde bozucu, silici, işletim sistemi sorunları doğurucu ve veri kayıplarına yol açıcı problemler ortaya çıkarmaktadır. Çalışma metodolojisi, virüslerin ana bilgisayar dosyaları vasıtasıyla sisteme sızarak aktif hale getirilmesi ve bu ana dosyanın açılmasıyla viral kodların diğer dosyalara bulaşması şeklinde açıklanabilecektir. Bahse konu viral kodlar ağ üzerinden tüm sisteme yayılabileceği gibi, dosya paylaşım programları, sürücü faaliyetleri, maillere gelen bağlantı ve eklerin açılması suretiyle tek bir aygıt sistemi üzerinde yayılım sağlayabilmektedir (Study.com, 2023). Virüslü bilgisayarlar iletişim halinde oldukları diğer bilgisayarlara söz konusu virüsü bulaştırarak hedef

bilgisayarda bulunan veri ve bilgilerin bütünlüğünü bozmaktadır. Bununla birlikte virüs faaliyetleri ile kişilere ait hassas içerikler ifşa edilerek kişisel verilerin ihlali gündeme gelmektedir. Virüslerin sisteme sızma ve yayılmasına ilişkin süreci özetlersek; ilk aşamada virüslerin sistemde türemesi, ikinci aşamada viral kodlarla yazılmış programların aktif hale getirilmesi ve son aşamada virüslerin siber saldırganlar tarafından hedeflenen amaca uygun şekilde kullanılması yer almaktadır (Samet, 2018).

Dünya üzerindeki ilk örneklerine bakıldığında 1999 yılında keşfedilen Melissa virüsü ön plana çıkmaktadır. Söz konusu kötücül yazılım virüsü, Microsoft Word ve Outlook sistemlerine yönelmiş, kritik kurum ve kuruluşlar ile kullanıcılara istenmeyen e-postalar gönderilmiştir. Bu e-posta eklerini açmak suretiyle virüs, bilgisayar ve sistemlere bulaşı sağlamıştır. FBI, söz konusu saldırı neticesinde siber suçlar çerçevesinde ilk kez bir ulusal siber strateji planı oluşturmuştur. Melissa virüsü kurumsal posta sunucularını devre dışı bırakarak ABD Deniz Piyadeleri ve Microsoft ağlarına zarar vermiştir. Söz konusu zararın maddi boyutuyla 80 milyon dolar olduğu tahmin edilmektedir. FBI yetkilerinin açıklamalarında maddi zararın yanı sıra 300'den fazla şirket ve kurumun e-posta sunucuları aşırı yüklenme nedeniyle kapanmıştır. Virüs bulaşan bilgisayarlar da e-posta yoluyla diğer bilgisayarlardaki kullanıcı e-posta hesaplarındaki elli kişiye söz konusu ekleri iletmiş ve onların da saldırıdan etkilenmesine sebep olmuştur (TechTarget, 2023).

2000 yılında “I Love You” başlığıyla bilinen bilgisayar virüsü e-posta yoluyla mağdurlardan birisinin listesindeki bağlantılara aşk mektubu göndermiş ve bu mektup diğer bilgisayarlara da yayılım sağlamıştır. Dönemine göre bahse konu bilgisayar virüsü bu zamana kadarki en büyük maddi zarara sebep olan kötü amaçlı yazılım şeklinde değerlendirilmiştir. Saldırının gerçekleştirildiği 10 gün içinde tahmini 45 milyon kullanıcıya ulaşmış ve 10 milyar dolarlık hasara neden olmuştur (Study.com, 2023).

Bir diğer örnekte ise Equation Group'un özel olarak kullandığı kötü amaçlı yazılım platformları, saldırganların yıllarca virüslü sistemlerin tam kontrolünü ele geçirmelerini sağlamıştır. Saldırganlar tespit edilmekten kaçınmak için karmaşık şifreleme şemaları ve diğer yöntemler kullanırken, bu sistem verileri elde etmelerine ve etkinlikleri izlemelerine olanak tanımıştır. Equation Group'un sunduğu en modern ve gelişmiş kötü amaçlı yazılım implantı GrayFish'tir. Tasarım gereği GrayFish Windows işletim sistemi içinde gizli bir

kalıcılık mekanizması, depolama ve kötü amaçlı komut yürütme sağlar. Aynı zamanda oldukça gelişmiş bir önyükleme seti (bootkit) içerir. GrayFish, kodunu önyükleme kaydına enjekte ederek işletim sistemi yükleme mekanizmalarını ele geçirir ve böylece her aşamada Windows'un başlatılmasını kontrol etmeye olanak tanır. Bilgisayara virüs bulaştıktan sonra, GrayFish her adımı kontrol ederek gerekli değişiklikleri yapar. Windows açıldıktan sonra, ortamda kod yürütmeyi sağlamak için dört ila beş aşamalı şifre çözme başlatır. Aşamalar, yalnızca tüm seviyelerin başarılı bir şekilde yürütülmesi durumunda devam etmektedir. Başlatma sırasında herhangi bir hata oluşursa tüm GrayFish platformu kendi kendini imha etmektedir (Industrial Cybersecurity Pulse, 2022).

Bilgisayar Solucanları (Computer Worms)

Kötücül bir yazılım çeşidi olan bilgisayar solucanlarına bazı kaynaklarda virüslerin bir alt kolu olarak yer verilmektedir (BTK, 2022). Bilgisayar solucanları siber güvenlik ve bilişim literatüründe "kurtçuk" olarak da anılmaktadır. Söz konusu kötücül yazılımın ilk fonksiyonu, virüslerin bulaştığı sistemler üzerinde aktif şekilde çoğalarak üzerinde taşıdığı kötü amaçlı yazılım aracılığıyla sistemler üzerinde yıkıcı etki bırakmaktır. Kendisini sistemde kopyalama özelliği dolayısıyla bilgisayar solucanları sistemin otomatik olarak işlediği ve sistem kullanıcısının farkında olamayacağı bölümlere yayılarak kendisini rahatlıkla gizleyebilmektedir. Kötücül yazılım taşıyan solucanların kullanıcı tarafından fark edilebildiği zaman, solucanların sistemde kontrole imkân tanımayacak şekilde çoğalıp yayıldığı, sistemin kritik kaynaklarını ele geçirerek sistem üzerinde yavaşlatıcı, durdurucu veya diğer olumsuz etkiler yarattığı son evre olmaktadır (Techtarget, 2022).

Kötücül yazılım taşıyan solucanlar sistem sunucuları üzerinde gerçekleştirdikleri ele geçirme, yavaşlatma ya da işlevsiz hale getirme fonksiyonları dolayısıyla maddi kayıplara yol açabilmekte, kurumların ve özel şirketlerin önemli verilerini ele geçirerek değiştirebilmekte, kişisel bilgileri ifşa edebilmektedir. Solucanlar sızdığı sistemler üzerinde yapısal değişime uğrayarak kopyalayarak oluşturdukları klonlarını ağ üzerinden diğer sistemlere de bulaştırmaktadır (BTK, 2022). Bu yolla kopyalanan tüm sistemlerde yayılım yönetim ve denetim yetkisi kullanıcının iradesi dışında ele geçirilmekte, sistemin belleği ve bant genişlikleri üzerinde çeşitli zayiatlara neden olunmaktadır (Malwarebytes, 2024).

Solucanların bulaşarak yayılması belirli başlı yöntemlerle sağlanmaktadır. Bu yöntemlerden birisi de e-postaların eklerinde iletilen dosyalardır. Diğer bir yöntem web üzerinden ya da kullanıcıların veri paylaşımı yapabildiği eşler arası bağlantı (peer to peer-P2P) veya dosya transfer protokolü (FTP) ile kaynak bağlantısı kullanılarak yayılmadır (USOM, 2014). Dosya transfer protokolü, dosyaların bir ağ üzerinden cihazlar arasında aktarımını içeren işlemi ifade eder. Süreç, bir taraf diğerinin internet üzerinden dosya göndermesine veya almasına izin verdiğinde çalışır (Investopedia, 2024a). Solucanların yayılması, "I Seek You (ICQ)" gibi anlık mesajlaşma programları veya Internet Relay Chat (IRC) mesajlarıyla gönderilen linkler yoluyla da gerçekleşebilmektedir (Collins Dictionary, 2024a; Collins Dictionary, 2024b; USOM, 2014). P2P'nin çalışma sisteminde merkezi sunucu ya da sisteme bağlantı olması şartı yoktur. Dağıtık sistem içeren protokoller vasıtasıyla kullanıcılar doğrudan bağlantı sağlamaktadır. Söz konusu sistem son zamanlarda yaygınlaşan blok zincir teknolojisinde de gündeme gelmiştir. Öyle ki blok zincir sistemi içerisinde sistemde yer alan tüm süjeler eş işlem kaydı içeren dağıtılmış deftere haizdir. Tek bir süjenin defterinde meydana gelen veri bozulması veya siber saldırı yoluyla verinin değiştirilmesi diğer defterler tarafından kontrol edilerek denetleme şansı olduğu için bu sistem güvenilir olarak değerlendirilmektedir. Bu yolla değişiklik fark eden kullanıcılar değişikliği reddedebilecektir (Bilgi Platformu, 2024). Bunlar dışında ağ paketleri şeklinde yayılan solucanlar, bilgisayar belleklerine doğrudan nüfuz ederek sistemde zayiata yol açan kodları aktifleştirebilmektedir (USOM, 2014). Diğer taraftan birtakım solucanlar ise "ağ paketleri" şeklinde yayılım sağlamaktadır. Solucanlar tarafından belleklere doğrudan sızılarak yazılımsal kodlar etkin hale getirilmektedir. Bu şekilde yayılım sağlayan solucanlar ağlar ya da "bölgesel alan ağı/geniş alan ağı (LAN/WAN)" şeklinde kurumsal ağlar temelinde türeyebileceği gibi web veya intranet temelli de çoğalabilmektedir. Bu tip solucanlar ağ solucanları (network worms) olarak nitelendirilmektedir.

Dünya üzerinde bu zamana kadar ismi duyulan solucanlar Blaster, Morris Worm, Nimda, SQL Slammer, Stuxnet ve Love Bug olarak sıralanabilir. Blaster solucanı bilişim dünyasında MSBlast, Lovsan veya Lovesan şeklinde de isimlendirilmiştir. Söz konusu saldırılar o tarihte kullanılan Windows 2000 ve Windows XP işletim sistemleri kullanılan bilgisayarlarda büyük bir zarara yol açmıştır (Malwarebytes, 2024). Bunların yanı sıra Windows 2003 işletim sistemi ve Windows NT çalıştıran cihazlarda da olumsuz etkilere yol açmıştır. Bu solucan internete bağlı sistemlere yayılmak için bir "Dağıtılmış Bileşen Nesne

Modeli (DCOM)" güvenlik açığından yararlanmıştır. Bu güvenlik açığı, Windows'un "Uzaktan Prosedür Çağrısı (RPC)" protokolü kullanılarak gönderilen mesajları işleyen bir ara yüz bileşenidir. Blaster tarafından yeniden başlatma, devamlı olarak açılıp kapanma, internete erişimde sıkıntılar gibi durumlarla karşılaşılmıştır (HYPR, 2024). Diğer taraftan tuğlalama (bricking) denilen ve genellikle başarısız bir yazılımsal hata veya güncelleme kaynaklı oluşan ve sistemin kullanılamaz hale gelmesine yol açan belirtiler de yine bu saldırı sonrasında görülmüştür. Bunun sonucunda çalışır durumda olan cihazlar tamamen donmakta ya da durmaktadır. Bu terime tuğlalama denilmesinin sebebi de zaten kullanılamaz hale gelen cihazların bir kâğıt ağırlığı veya tuğladan farkının kalmamasıdır (Techterms, 2020). Blaster solucanı yaptığı saldırıda bilgisayarları zombileştirerek onları kullanılmaz hale getirmiştir. Zombileşen bilgisayarlar ağ üzerinde yayılım göstermeye başlamıştır. Windows işletim sistemi çalıştıran makineleri etkileyen solucan, Microsoft Corporation'a karşı Dağıtılmış Hizmet Reddi (DDoS) saldırıları gerçekleştiren bir botnet oluşturmuştur. Blaster saldırısının başarılı olup kolayca yayılmasında en büyük etken insan hatası kaynaklı olmasıdır. Söz konusu saldırı konusunda hem bireysel hem de kurumsal olarak uyarılarda bulunulmuş ancak ofislerdeki ve evlerdeki sistemlere yama uygulayarak eksikliklerin giderilmemesi Blaster'ın başarısına yol açmıştır. Blaster tarafından solucanın bulaştığı bilgisayarlarda yayınlanan iki mesajın ilki "Sadece seni seviyorum demek istiyorum SAN (I just want to say LOVE YOU SAN!!)" iken Blaster'ın Lovesan olarak bilinmesinin sebebi de bu mesajdır. İkinci mesaj ise doğrudan Bill Gates'e yönelerek "billygates bunu neden mümkün kılıyorsun? Para kazanmayı bırakın ve yazılımınızı düzeltin (billy gates why do you make this possible? Stop making money and fix your software!!)" şeklindedir (HYPR, 2024). Bahse konu solucanlardan dünya çapında adından söz ettirmiş bir diğeri olan Nimda'nın neredeyse 3 milyar dolar zarara neden olduğu ortaya çıkmıştır. Lovebug adlı solucan ise Nimad'dan daha büyük bir ekonomik yıkıma neden olarak 10 milyar dolar zayiat yaratmıştır (CNNBusiness, 2020).

Dünya üzerinde devletlerin siber güvenlik önlemlerini gözden geçirmesine ve siber uzayda güç elde etme ihtiyacına sebep olan "Stuxnet" saldırısı 2010 yılında İran'a ait nükleer tesislere yönelik gerçekleştirilen, zaman geçtikçe mutasyona uğrayarak sanayi ve enerji tesislerine de etki eden yıkıcı solucan saldırısı olarak literatüre geçmiştir. Bu saldırının İran'ın İsfahan eyaletinde bir şehir olan Natanz'da yer alan uranyum tesisindeki sayıca çok fazla santrifüjün infilak etmesine neden olduğu bildirilmiştir. Mutasyon virüs, su arıtma

tesisleri, enerji üretim merkezleri ve gaz boruları gibi altyapıları etkileyecek seviyeye gelmiştir. Stuxnet aslında ilk haliyle makineye ait faaliyetleri otomatikleştirmek amacıyla kullanılan PLC'yi hedef alan kötü niyetli yazılımsal bir saldırıdır. USB bellekler aracılığıyla bulaşan virüs, kendisine kurban olarak bir PLC bilgisayarı bulduktan sonra kodunu internet ortamında yenileyerek bilgisayarın himayesi altında tuttuğu elektromekanik aygıtlara zarar veren yönergeler iletmeye başlar. Aynı zamanda, virüs ana denetleyiciye hatalı geri bildirim göndererek ekipmanı izleyen kişinin, ekipman kendi kendini imha etmeye başlayana kadar herhangi bir sorun belirtisi görememiş olmasını sağlar (Trellix, 2023). Stuxnet, windows işletim sistemleri vasıtasıyla fabrikalar, enerji hatları, baraj gibi sanayiye yönelik aygıtların yönetimini ele geçirmek amacıyla kullanılan bir solucandır. Bu solucana ait kod bileşenleri dünyanın birçok ülkesine etki etmiştir. Etkiyi ciddi şekilde hisseden ülkeler arasında Çin, Hindistan ve Endonezya da bulunmaktadır (Imperva, 2023a). Bu virüsün ana ve ayırıcı özelliği, donanımsal özellikleri bozabileceği bilinen ilk virüs türü olmasıdır. Söz konusu solucanın dış politikalar da göz önüne alındığında İran'a karşı ABD Ulusal Güvenlik Ajansı (NSA), CIA ve Mossad tarafından yapay şekilde oluşturulduğu iddia edilmektedir (Trellix, 2023). Söz konusu saldırı sanılanın aksine kapalı devre sistemlerinin dahi siber saldırılar dolayısıyla zarar görebileceğini ortaya çıkarmıştır.

Bunların yanı sıra "Sapphire/Slammer" isimli solucan 2003'te kaydedilen verilere göre internet üzerinden saldırıda bulunarak %90 oranında bulaşıya ulaşmış ve bu oranı sadece 10 dakika gibi kısa bir süre içerisinde yakalamıştır (Caida, 2024). Bu istatistik göz önüne alındığında solucanların yayılma hızının çok ileri seviyelerde olduğu ve söz konusu yayılımı kısa sürede tamamlayarak ağ üzerinde bağlı cihazlara bulaşı sağladığı görülmektedir. Bant genişliği ile sınırlı şekilde etki doğuran Sapphire solucanı söz konusu yöntemle bilgisayar ve ağların paketleri iletebildiği hız oranında tarama yaparak saldırıyı gerçekleştirmiştir.

Truva atı yazılımı (Trojan Malware)

Truva atı yazılımının tarihsel ve etimolojik kökenine bakıldığında Antik Yunan'a kadar dayandığı görülmektedir. Odysseus tarafından "Truva Atı" olarak nitelendirilen hikâyede dönemin şehrine ait surların aşılarak şehrin işgal edilmesi amacıyla kullanılan tahtadan maket ajan, söz konusu kötücül yazılım saldırı tipini oluşturan model olarak bilişim

dünyasında örneklendirilmektedir (Wikipedia, 2023; Britannica, 2023). Tarihteki ilk truva atı yazılımı 1974 yılında geliştirilen ve "Animal" adı verilen yazılımdır. İsminden de anlaşılacağı üzere söz konusu yazılım programı hayvanların bilinmesi üzerine kurulu olan bir bilmece oyunu şeklinde inşa edilmiş ve sorulan soruların arasına sıkıştırılan farklı türde soruların oyun süresince cevaplanması istenmiştir. Söz konusu sürede oyun içerisine gizlenen programa kötücül yazılım yüklenerek kullanıcının sistemine rıza dışı erişim sağlanmıştır (Solomon, 2014). 1980'li yıllarda truva atı yazılımları bilişim sektöründe görülmeye başlanmış ve ilk kez teori şeklinde açıklanmıştır. Bu yazılım 1990'lı yıllarda geliştirilerek daha yıkıcı şekilde kötücül yazılım teknolojisi şeklinde ortaya çıkmıştır (Britannica, 2023).

Truva atı yazılımları yapısı itibariyle bilgisayar ve bilişim sistemlerine gizlice sızmakta ve internet üzerinden veya e-posta vasıtasıyla kullanıcılardan habersiz şekilde dışarıya veri iletmektedir (BTK, 2022). Bilgisayar içerisinde meşru bir kod olarak görünen ancak gerçekte kötücül yazılım taşıyan truva atı sistem verileri üzerinde tahrifat, verileri silme ve değiştirme gibi işlemleri de gerçekleştirebilmektedir (Wikipedia, 2023). Diğer taraftan sabit sürücü üzerinde izleme, kişisel şifre ve hesap bilgilerine erişim ve bu bilgileri ifşalama, yayma, klavye kaydedici fonksiyonu ile işlem geçmişini öğrenme gibi çeşitli zararlı faaliyetlerde de bulunabilmektedir (Britannica, 2023). Bu kötü amaçlı yazılım genellikle uygulama, oyun, crack program yamaları ve paket olarak indirilen dosyaların içerisine ustaca gizlenmektedir. Truva atı yazılımı ile beraber gerçekleştirilen siber saldırının etkisinin artırılması amacıyla sosyal mühendislik, kimlik avı ve sahtekarlığı gibi diğer saldırı türlerinden faydalanılmaktadır (Wikipedia, 2023). Yine dolandırıcılık, şantaj ve kurumsal casusluk gibi diğer suçlarda da söz konusu saldırı tipinde yardımcı suç aracı olarak kullanılabilmektedir (Britannica, 2023). Son yıllarda ürünler pazara sunulmadan ve henüz üretim aşamasında iken bu yazılımların cihazlara yüklenerek kullanıcılara bu şekilde satış yapıldığı örneklerle karşılaşılmaktadır. Kullanıcılar satın alıp ürünü kullanmaya başladıktan sonra uzaktan komut yöntemiyle yazılım aktif hale getirilerek kötücül kodlar etkinleştirilmektedir. Özellikle USB cihazlar ya da harici bellekler söz konusu kötücül yazılımların yayılmasında araç olarak kullanılabilmektedir (Bolat, 2020).

Truva atı yazılımları yapıları itibariyle iki temel unsur üzerine inşa edilmektedir. Bunların ilki istemci (client) bir diğeri ise sunucudur (server). İstemci kısmı hedef olarak

belirlenen bilgisayarda, sunucu ise siber saldırganın uzaktan kontrol (remote control) faaliyetlerinde bulunduğu bilgisayarda aynı anda çalışmaktadır (Alioğlu, 2019). Söz konusu saldırılar istemci-sunucu modeli üzerinde gerçekleştirilmektedir. Bu saldırılarla bilgisayar sisteminin iç yapısını ele geçirerek internet trafiğini yönetmek ve arka kapı (back door) erişim noktaları vasıtasıyla çeşitli zararlı faaliyetler yürütmek amaçlanmaktadır. Bunlardan birisi de karanlık ağ (dark web) üzerinden hassas ve kritik bilgilerin satılması işlemidir (Baker, 2022). İnternetten indirilen uygulama ve dosyaların arkasında gizlenen bu yazılım girdiği bilgisayarda kullanıcı tarafından fark edilemez (BTK, 2022). Söz konusu arka kapı sisteminin bilgisayarda aktif hale gelmesiyle beraber saldırıya uğrayan bilgisayarlar köle ve zombi bilgisayar şeklinde mutasyona uğrar (Britannica, 2024). Bilgisayar sistemi üzerindeki tüm açıklık ve zafiyetlerden faydalanan bu yazılım siber saldırganın kodlaması doğrultusunda hareket etmektedir. Diğer taraftan sadece bir casus olarak kullanılmamakta sistemlerde meydana gelen hataların giderilmesi amacıyla sistem yöneticileri ve mühendisler tarafından arızaların tespiti ve çözümlenmesi de sağlanmaktadır. Diğer virüslerden ayrılan noktaları yapıları gereği dış etki olmadan üreme veya çoğalma kabiliyetlerinin olmaması ve zararsız görünmeleridir (BTK, 2022).

Bilgisayar ve bilişim sistemlerine daha önce gerçekleştirilen truva yazılımları göz önüne alınarak yapılan tasnife bakıldığında yaklaşık on farklı truva atı yazılım saldırı tipi olduğu söylenebilmektedir. Bunların ilki “Exploit Trojan” olarak isimlendirilmekle birlikte isminden de çıkarım yapılabileceği üzere sömürü üzerine kurulu bir sisteme sahiptir. Bu saldırı tipinde uygulamalardaki güvenlik açıklıkları ve zafiyetlerin kötüye kullanılması yöntemi uygulanmaktadır. Bir diğer tür olan “Downloader Trojan” ise virüslü aygıtlar hedef alınarak zararlı yazılım içeren programın son sürümü aygıta yüklenmektedir. “Backdoor Trojan” saldırı tipinde network üzerinden erişim bağlantısı kurmak amaçlanmaktadır. Fidye yazılım saldırıları türevinde olan “Ransom Trojan” saldırısı da aynı mantıkla virüslü sistemdeki bilgilerin geri verilmesi için fidye isteminde bulunur. DDoS saldırılarının türevi olan “Distributed Denial of Service (DDoS) Attack” Truva atına gelindiğinde DDoS saldırısı oluşturmak için kullanılan öncül bir araç olduğu söylenebilir. Kablosuz yönlendiricilere (wireless router) erişim sağlamak amacıyla botnet veya zombi bilgisayarlar sayıca çok fazla bilgisayara bulaşı sağlar. “FakeAV Trojan” ise virüslere karşı koruma ve caydırıcılık sağladığı süsü verilen sahte programlardır. “Rootkit Trojan”, virüslerin sistemlerde etkin şekilde çalışma sürelerini artırmak amacıyla kullanılan ve sistem içerisinde virüslü

uygulamaları saklayan yazılımdır. ”SMS Trojan” ise söz konusu yazılımlar içerisinde mobil cihazlarda kullanılan tek yöntem olarak ön plana çıkmaktadır. Bu yolla mobil cihazlara gönderilen SMS’ler ekonomik kazanç elde etmek amaçlı araç olarak kullanılmaktadır. Son tip olan “Trojan GameThief”, son yıllarda gelişen ve popülerleşen sanal ortam oyuncularını hedefleyerek oyunlardaki kritik ve hassas bilgileri elde etme amacı taşımaktadır. Bu sayede elde edilen kişisel veriler yine diğer türlerde olduğu gibi karanlık ağ (dark web) üzerinden satışa sunulmaktadır. Söz konusu bilgilerin siber suçlular tarafından ifşa edilmesi sonucu maddi kayıplarla beraber manevi yıkım yaşatılarak itibar kayıplarına da yol açılmaktadır (Baker, 2022).

Dünya üzerinde büyük yıkıma yol açan truva atı saldırılara bakıldığında 2004 yılında Titan Rain (Titan Yağmuru) isimli siber saldırı ön plana çıkmaktadır. Bu saldırıda, ABD ve Birleşik Krallık’a ait kritik kurumların bilgisayar ve bilişim sistemlerine erişim sağlanmış ve iddia edilene göre Çin hükümetine söz konusu veri ve bilgiler sızdırılmıştır. ABD yetkililerince yapılan açıklamalarda bahse konu truva atı saldırılarının 2003 yılından 2005’e kadar düzenli ve sürekli olarak devam ettiği bulgusunu tespit ettikleri ifade edilmiştir. Birleşik Krallık tarafından yapılan siber saldırı açıklamasında ise söz konusu saldırının sona erdiği tarihin 2007 olduğu aktarılmıştır. Titan Rain Truva atı saldırısının siyasi ve askeri yönünün olması, İç Güvenlik, Dışişleri, Enerji gibi birçok bakanlığın verilerinin siber uzamda ele geçirilmesi konvansiyonel savaşlarda bahse konu siber saldırıların ve siber casusluğun ne denli etkili olduğunun göstergesi olmuştur (Counsil on Foreign Relations, 2005).

2007 yılında ortaya çıkan ve 2011 yılında birçok çeşidi türeyen Zeus/Zbot isimli bir diğer truva atı saldırısında kullanılan yazılım paketi, istemci-sunucu modelindeki bulut sunucularının “Zeus Komuta ve Kontrol (C&C) Merkezi” şeklinde isimlendirilen alana geri çağırma (callback) tekniği ve Zeus sunucusuna bilgi ve veri aktarımı ile süreci yönetmesine dayanmaktadır. Söz konusu yazılım Windows işletim sistemi üzerinde etkili olmuş ve söz konusu sistemlerin kullanıldığı cihazlara sızarak kişilere ait bilgilerin, kredi kartı ve banka hesaplarına ilişkin mali bilgilerin ele geçirilmesini sağlamıştır. ABD’nin hedef olarak belirlendiği bu saldırıda NASA, Amerikan Bankası ve ABD Ulaştırma Bakanlığı olumsuz etkilenmiş ve kritik kamu kurumlarının cihazları Zeus/Zbot truva atı yazılım paketi ile ele geçirilmiştir. Saldırı neticesinde 3.6 milyon civarında etkilenen cihaz olduğu paylaşılarak

sayının süreç boyunca arttığı görülmüştür (Imperva, 2023b). Zeus/Zbot truva atının çalışma metodolojisi köle bilgisayarların söz konusu siber saldırıda aracı kullanılarak bilgisayar ve sistemlerde irade dışı çalışma, URL erişim engelleme, bazı URL ile tanımlanmış internet sayfalarına sahte şekilde oluşturulan Hiper Metin İşaretleme Dili (HTML) yükleme, mevcut dosyalarda kullanıcının izni dışında yetkisiz erişimle istenmeyen davranışlarda bulunma ve dijital sertifikaların çalınması şeklinde görünüm kazanmaktadır (ENİSA, 2023a).

2007 yılında İsrail-Suriye savaşı kapsamında "Operation Orchard" harekâtı Suriye devletinin hava sahasında gerçekleştirilen İsrail saldırıları ile devam etmiştir. Söz konusu klasik savaş unsurlarını barındıran harekât İsrail tarafından Suriye hava savunma radar sistemlerine gerçekleştirilen truva atı saldırısı ile siber uzay sahasına da taşınmıştır. Bahse konu saldırıda Suriye'nin Deir Alzour şehri yakınlarındaki Al-Kibar isimli nükleer silah tesisi hedef alınmış ve söz konusu truva atı, enerji salınım sürecini kontrol eden nükleer reaktörü olumsuz şekilde etkilemiştir. Söz konusu truva atı nükleer tesiste çalışan Suriyeli bir personelin kişisel bilgisayarına İsrail istihbarat servisi (Mossad) ajanları tarafından gizlice sızdırılmıştır. Erişilen verilere bakıldığında Al-Kibar nükleer tesisinin kritik konumda kabul ettiği bölümlere ait fotoğraflar ortaya çıkmıştır. Bu saldırının önem arz eden bir diğer tarafı ise konvansiyonel ve siber savaş unsurlarının entegre edildiği hibrit savaş modelinin örneklerinden olmasıdır. Saldırının etkileri komşu sınır hattı bölgelerine tesir ederek Türkiye sınırında yer alan Tel Abyad'daki hava savunma radar sahasına taşmıştır. Bu saldırı neticesinde hassas güdümlü füze kullanımı ile karşı tarafta fiziki tahribat oluşturulmuştur. Böylelikle hava sahasının gardı düşerek İsrail kuvvetleri tarafından Suriye hava sahasına gizlice sızılmıştır. Yine saldırı neticesinde Suriye hava savunma radar sistemleri etkisizleştirilerek savaşta büyük bir avantaj sağlanmıştır. İsrail hava kuvvetleri tarafından Suriye havası kullanılarak El-Kibar nükleer tesisine 17 ton bomba atılmıştır. Bu saldırıyı gerçekleştiren devlet veya devlet destekli gruba dair isnat konusunda uzun bir müddet belirsizlik oluşmuştur. Ancak 2018 yılında İsrail Savunma Bakanı tarafından yapılan açıklamalar bahse konu siber operasyonun İsrail devleti tarafından gerçekleştirildiğini doğrulamıştır (Cyberlaw, 2021c).

2009 yılında ilk örneklerine rastlanan ve iki yıl boyunca süregelen Rusya menşeli truva atı yazılımı saldırısında Apple'ın tarayıcısı Safari'ye yetkisiz erişim sağlanmıştır. Söz konusu siber saldırı ile mobil bankacılık sektörü hedeflenmiş ve kişisel hesaplar üzerinde

yazılım vasıtasıyla rıza dışı işlemler planlanmıştır. Yetkisiz erişim sağlanan banka hesaplarından nakdi çıkışlar gerçekleştirilmiş ve siber saldırganların hesaplarına para aktarımı olmuştur (Malpedia, 2023). Rusya'da siber uzamdaki faaliyetleri ile bilinen Panin, SpyEye virüsünü geliştirmiş ve karanlık ağ üzerinden dağıtımını sağlayarak gelişmiş virüs bileşenlerini internet ortamında pazarlamak amacıyla farklı metotlara başvurmuştur. Söz konusu yöntemler arasında en bilineni finansal kurum ve kuruluşları etkileyen güncellenmiş versiyonların siber saldırganlarla paylaşımıdır (U.S. Department Of Justice, 2014).

2015 yılında tüm dünyayı siyasi, ekonomik ve toplumsal olarak etkileyen Rusya-Ukrayna savaşı sırasında Luhansk ve Donetsk bölgelerinde gerçekleşen askeri çatışmalarda Ukrayna'daki üç elektrik dağıtım şirketinin SCADA sistemlerine uzaktan erişim gerçekleştirilmiştir. Söz konusu siber olayda saldırganlar tarafından kritik enerji tesisleri kontrol altına alınmış ve komuta sistemleri ele geçirilmiştir. Bununla birlikte Ukrayna'nın başkenti Kiev'de ve batısında yer alan Ivano-Frankivsk bölgesinde elektrik dağıtımı yapan otuz trafoda kesinti gerçekleşmiştir. Söz konusu kesinti dolayısıyla 200.000 civarında kullanıcının elektrik enerjisinden mahrum kalmıştır. Saldırılar bununla sınırlı kalmamış ve 2016 yılında başkent Kiev'in kuzeyindeki akımı etkileyen elektrik iletim trafosunda da büyük bir siber saldırı yaşanmıştır. Bu saldırıya ilişkin Ukrayna ve ABD tarafının müşterek açıklamalarında, siber saldırının Rusya-Ukrayna arasındaki klasik savaşa binaen Rusya kanadından gerçekleştirildiği ve etkili bir hibrit savaş unsuru olduğu ifade edilmiştir. Öyle ki siber saldırı neticesinde gerçekleştirilen zafiyet taramalarında "BlackEnergy3" truva atı tespit edilmiştir. Endüstriyel kontrol sistemleri ve SCADA'lar üzerinde etkisi olan söz konusu kötücül yazılımın bu saldırıda Ukrayna'ya ait kritik altyapıları hedeflediği belirlenmiştir (JSİS University of Washington, 2017). BlackEnergy3 truva atı vasıtasıyla 2014 yılında yaşanan olayda kritik altyapılara yönelik bir saldırı düzenlenmiş ve sistemleri kontrol eden SCADA'lara kötücül yazılım içeren eklentiler gönderilerek DDoS siber saldırısı gerçekleştirilmiştir. Söz konusu olaydan dolayı siber dünyada bilinen ve BlackEnergy3 truva atını kullanan bilgisayar korsanlığı grubunun emareleri kendisini bu olayda da göstermiştir. Bu olayın gerçekleşmesinde dezenformasyona yol açan çeşitli manipülatif söylemlerle beraber Ukrayna parlamentosu yetkilerinin ağzından yazılmış gibi gösterilen bir mail iletisi ile karşı tarafın güveni kazanılmıştır. Söz konusu olayla arasında birkaç yıl bulunması Rusya'nın bu saldırıyı da yaptığına dair kanıtları güçlendirmiştir (ICP, 2021ç). Ukrayna'ya yönelik siber saldırılar neticesinde gerçekleştirilen kapsamlı analizde

devlete ait kritik altyapıların sabote edilmesinin hedeflendiği, kritik kamu hizmetlerinin kesintisine sebep olunmaya çalışıldığı ve devlete olan güvenin yıkılmasına uğraşıldığı tespit edilmiştir (JSİS University of Washington, 2017).

2016 yılında ortaya çıkan "Trickbot" isimli truva atı ise Birleşik Krallık başta olmak üzere diğer bazı Avrupa ülkeleri hedeflenerek bankacılık ve finans sektörüne darbe vurmak amaçlı geliştirilmiş kötücül yazılımdır (Malwarebytes, 2023b). Söz konusu siber saldırı Personally İdentifiable İnformation (PII) diğer bir deyişle kişisel bilgilere erişmek amacıyla banka ve internet ortamındaki hesapların çalınması olarak nitelendirilmektedir. Sahte kimlik dolandırıcılığı şeklinde uygulanan PII saldırıları entegre şekilde gerçekleştirilen saldırılarda kötücül yazılım saldırıları için siber saldırının ağırlığını artırıcı bir konumdadır. Öyle ki bu yöntemle saldırı için bir veri kümesi elde edilerek öncül bir saldırı argümanı ortaya konulmaktadır. Trickbot truva atı, gerçekmiş süsü verilen ancak sahte olan hesaplar aracılığıyla hedef olarak belirlenen yerlere ek ve bağlantı içeren mailler göndererek hibrit saldırılar gerçekleştirilmektedir (NCSC, 2020a).

2017'de ortaya çıkan bir diğer saldırı "Triton Kötü Amaçlı Yazılım Saldırısı"dır. Söz konusu saldırı endüstriyel kontrol sistemlerine yönelik son on yılda gerçekleşen en tehlikeli truva atı siber saldırılarından biri şeklinde gösterilmektedir. Suudi Arabistan'daki bir petrokimya tesisinde Schneider Electric şirketinin triconex isimli endüstriyel otomasyon güvenlik teknolojisi hedef alınarak yapılan siber saldırıda zehirli hidrojen sülfit gazının salınımına ve tesisin patlamasına yol açılarak çevre yerleşim yerlerinde yaşayan insanlara zarar vermek hedeflenmiştir. Saldırıda truva atı ile birlikte asli olarak bilgisayar korsanlığı yöntemi kullanılmış ve petrokimya tesisinin güvenlik sistemleri ele geçirilmiştir. Siber saldırganlar sistemlere "Arabellek Aşımı (Buffer Overflow)" yöntemiyle Uzaktan Erişim Truva Atı (RAT) yüklemişlerdir. Bu saldırının oluşumunda yazılımlar arası veri iletim hizmeti sunan arabelleğe gereğinden fazla kapasiteyi aşan miktarda veri yüklemişlerdir. RAT arabelleğe fazlaca yüklendiğinde, triconex endüstriyel güvenlik teknolojisine ait yazılımda sıfır gün ayrıcalık yükseltme güvenlik açığı ortaya çıkmış ve kötücül yazılım kodu yükseltilmiştir. Saldırıyı planlayan kişiler, sistem bileşenlerinin hızını değiştirmek ve daha büyük bir patlamaya sebep olmak amacıyla gereğinden daha fazla kodu enjekte etmeyi planlamışlardır. Fakat siber saldırganın yazılımsal olarak girdiği kodlar arasındaki tesadüfi

bir hata neticesinde can kaybı oluşmamış, yalnızca bahse konu petrokimya tesis hizmetleri kısa bir süreliğine hizmet verememiştir (Dover Mıcrosystems, 2017).

2019 yılında TrickBot truva atına ait yazılımı geliştiren hackerlar minimal değişiklikler sayesinde "webinject" özellikli saldırılar kurgulamaya başlamışlardır. Söz konusu özellik ABD merkezli Sprint, Verizon Wireless ve T-Mobile mobil operatörlerinin çalışma yöntemlerinde değişikliğe neden olmuştur. Saldırılar sonrasında elektronik haberleşme sektöründe marka ve itibar kaybı ile mali zararlar meydana gelmiştir (Malwarebytes, 2023b). Sistem kullanıcıları bahse konu mobil operatörlere ait internet sitelerine girdiklerinde TrickBot'a ait resmi sunucudan gelen yanıt yakalanmış ve tehdit aktörleri tarafından C&C sunucusuna iletilerek siber saldırı başlatılmıştır. Bu işlem sonrasında HTML ve JavaScript gibi komut dosyaları C&C sunucusu tarafından internet tarayıcısına enjekte edilmiş ve web sayfası oluşturulmadan sistem değiştirilmiştir (Malwarebytes, 2019).

2020 yılının ortalarında küresel çapta pandemiye yol açan Covid-19 virüsü, dezenformasyon faaliyetleri ile insanları korku ve panik ortamına sürüklemiştir. Söz konusu dezenformasyon çalışmaları kötücül yazılım saldırıları ile entegre şekilde büyük bir siber saldırı aracı olarak kullanılmıştır. Öyle ki 2020 yılının sonlarına gelindiğinde McAfee tarafından yapılan araştırmalara göre 3 milyonun üzerinde mobil cihaza gönderilen kötücül yazılım bulunmuştur. Bir önceki yılın tam iki katı oranında bir büyüklükle ortaya çıkan yeni kötücül yazılım saldırıları bu uygun ortamda başarıya ulaşmıştır. Özellikle de Covid-19 pandemisi süresince aşı tedariki ve uygulamaları ile ilgili kaotik ortamdan yararlanan siber saldırganlar saldırılarının büyük bir kısmını bu konuda gerçekleştirmiştir. Tüm saldırılar içerisinde truva atı saldırılarının oranı ise %90'ın üzerindedir. Mobil cihazlara gönderilen truva atı yazılımları ile dünyanın dört bir yanındaki kişilerin verilerine ulaşılmış ve kullandıkları cihazların yönetimi ele geçirilmiştir (Safeatlast, 2023).

Bukalemun Saldırısı (The Chameleon Attack)

Bukalemun saldırısı, internet kullanıcılarının hesaplarına ait giriş bilgisi ve şifre giriş iletilerini taklit eden meşru bir kod gibi görünen ve truva atlarını andıran yazılımlardır. Saldırının hazırlık aşamasında siber saldırganlarca, kullanıcı tarafından girilen bilgilerin hatalı olduğuna dair kısa süreli hizmet kesintisi uyarısı içeren mesaj karşı tarafa

iletilmektedir (BTK, 2022). Söz konusu uyarıyı içeren iletiye yer tutucu da denilmektedir (Aslay, 2017). Programcı siber saldırgan sisteme erişerek kullanıcılara ait sistem giriş bilgilerini içeren bukalemunun kaydettiği dosyaları ele geçirmektedir (Alioğlu, 2019).

Son zamanlarda çeşitli şekillerde görülen bukalemun yazılımlarının en popüler örneklerinden birisi "eFast Browser" adı verilen yazılımdır. Söz konusu yazılım Google Chrome web tarayıcısını pasif hale getirerek bu tarayıcının yerini kendisi almıştır. Eski tarayıcının yerini geçen yeni tarayıcı ticari amaçlı reklamlar, site yönlendirmeleri, klavye kaydetme gibi çeşitli işlemlere neden olmuştur. Söz konusu yazılımın başarılı olmasındaki en önemli faktör ise Chrome tarayıcısının haklarına sahip olan şirket tarafından geliştirilebilmesi amacıyla açık kaynak "Chromium" kodunu kullanmasıdır (Kozan, 2015).

Klavye İşlemlerini Kaydeden Program (Keylogger)

Klavye işlemlerini kaydeden program, siber saldırganların casus yazılımlar vasıtası ile kullanıcılara ait klavye tuşlamalarını kaydederek saldırı üssü olarak belirledikleri önceden kodlanmış adreslere kritik ve hassas verileri göndermelerini içeren siber saldırı türüdür (BTK, 2022). Bu saldırı türünün bilişim dünyasındaki karşılığı olan "keylogger" terimi Türkçe'ye "tuş vurucu kaydedici" olarak çevrilen "keystroke logger" teriminin kısaltması şeklinde kullanılmaktadır (Fruhlinger, 2022b).

Klavye işlemlerini kaydeden programlar saldırıları yazılım dışında donanımsal olarak da gerçekleştirilebilen casus yazılım türüdür. Bu yöntemde klavyelere fiziksel olarak yerleştirilen cihazlar aracılığıyla kullanıcının tuş vuruşları kaydedilmektedir. Söz konusu yöntem banka ATM'lerinde de uygulanmakta ve bu yolla kullanıcıların hesap bilgilerine erişim sağlanmaktadır. Dolaylı olarak özel hayatın gizliliğinin ihlaline vücut veren bu saldırılarda kişisel verilere saldırganlarca erişim sağlanabilmektedir. Bu saldırılara karşı özel sektörde faaliyet gösteren şirketler çeşitli siber güvenlik önlemleri alma ihtiyacı duymuştur. Öyle ki şirketler, verilerin korunması için güvenli ödeme sistemleri, SMS'le kullanıcıya tek seferlik şifre gönderimi, iki faktörlü kimlik doğrulama gibi yöntemlerle kullanıcıların sisteme olan güvenini artırmayı amaçlamaktadır (BTK, 2022).

Keylogger yönteminin çeşitli tipleri bulunmakla birlikte yalnızca tuş vuruşlarını kaydetmeyip kullanıcı hareketlerini izleme fonksiyonlarını da yerine getirmektedir. Keylogger sistemleri tarafından gerçekleştirilebilen diğer faaliyetler şöyledir:

- Belgelerden kopyalanan pano metni ve giriş yapılan kayıt verilerine erişim,
- Dosyaları, belgeleri ve aplikasyonlara ulaşarak içerik girişi yapabilme,
- Farklı zamanlara ayarlanmış ekran görüntüleri ve resimleri ele geçirme,
- Şifrelere ulaşmak amaçlı fayda sağlayacak olan ekran kontrollerine yönelik faaliyetler yürütmek.

Bazı keylogger türleri zararlı olmaktan çok fayda sağlamaktadır. Siber saldırı amacıyla kullanımı dışında söz konusu yöntem kullanıcılar, kamu kurum ve kuruluşları ile özel şirketler açısından fayda sağlamaktadır. Bunların başında, çocuklarının çevrimiçi etkinliklerini izlemek isteyen ebeveynlere ticari şirketlerce pazarlanan program ve sistemler gelmektedir. Bu programlar, izlenen bilgisayarların ebeveynlere ait olması durumunda yasal kabul edilmektedir. Öyle ki güvenli internet uygulamaları kapsamında aileler, söz konusu sistemleri yaygın şekilde kullanmaktadır. Bu şekilde aileler zararlı içerik barındıran siteleri tespit ederek çocuklarının psikolojilerini kötü etkileyebilecek uygulamalardan ve oyunlardan onları uzak tutabilmektedir. Bunun yanı sıra yine iş yerlerinde de bahse konu sistem ve programlar sıklıkla kullanılmaktadır. Özellikle ABD'deki yargılama mercileri, söz konusu programlar bilinçli ve rızaya dayalı olarak kullanıldığında bunları yasal olarak kabul etmektedir. Örneğin bir işyerinde yönetici konumundaki kişiler şirket bilgisayarları üzerinde izinsiz faaliyette bulunan bir personeli tespit ederse bilgisayarda kurulu olan klavye kaydediciden toplanan veriler ABD yasalarına göre kanıt olarak kullanabilecektir. Yine aynı yasalara göre işyerinde dahi olsa bilgisayardan internet bankacılığı gibi özel bir iş için kişisel verilerin aktarılacağı bir siteye girildiğinde bu bilgilerin yöneticiler tarafından rıza dışı ele geçirilmesi suç teşkil edecektir. Kuzey Karolina Elektronik Gözetim Yasası kapsamında federal yasa ile paralel olarak sözlü veya elektronik iletişimlerin dinlenmesi yasaklanmıştır. Dinlenmenin iletimle eş zamanlı olması yasanın tuş kaydedicilere yönelik uygulanmasında problemleri ortaya çıkarmaktadır. 2011 yılında Indiana'da bir işçi, işvereninin e-postalarına erişmek amacıyla yazılım tabanlı bir tuş kaydedici kullandığı gerekçesiyle yerel mahkemede dava açmıştır. Davacı işçi, işvereninin tuş vuruşlarını engellediği, e-posta, banka hesabı oturum açma bilgileri ve diğer kişisel içeriğe erişim sağladığı iddiası ile savunmada bulunmuştur. Yetkili ve görevli mahkeme engellemenin iletimle eş zamanlı olması

gerekliliğine odaklanarak bu davada işçinin hassas bilgilerinin iletimle eş zamanlı olarak kaydedildiğini kanıtlayamadığı yönünde karara varmıştır (Rosen Law Firm, 2024).

Klavye kaydedicilerin tarihine bakıldığında kronolojik olarak en eskileri bilgisayar çağına girilmeden önceki zamanlara rastlamaktadır. 1970'li yıllara gelindiğinde Sovyetler Birliği'ne ait istihbarat servisi, elektrikli daktilonun içerisine konuşlandırılan ve klavyeye girilen tuşlamaları radyo sinyalleriyle aktaran yeni bir teknoloji üretmiştir (Wikipedia, 2024). Söz konusu cihazlar Moskova ve Leningrad şehirlerinde ABD'ye ait büyükelçiliklerde kullanılarak buradaki daktilolara yerleştirilmiştir (CSO, 2024). Bahse konu olayda keylogger 16 adet daktiloda tespit edilmiş ve "selectic bug" olarak isimlendirilmiştir. Yine bu kaydedici sistem yazıcının hareketlerinden ortama saçılan manyetik bölgeyi hesaba katarak yazıcıya ait hareketleri izlemiş ve belleğine almıştır (Bilgi Güvende, 2022a).

1983'te Perry Kivolowitz isimli araştırmacı tarafından kavramsal kanıt şeklinde ilk bilgisayar keyloggerı üretilmiştir (CSO, 2024) Keylogger kullanımı 90'lı yıllarda giderek artmış ve bu dönem boyunca kötü amaçlı keylogger yazılımları oluşturulmuştur. Böylece söz konusu yazılımlar gün geçtikçe donanımların yerini almaya başlamıştır. Sektör hane halklarını hedeflediği kadar kimlik avı maksatlı saldırılarla sanayileşmiş ülkelerin önemli şirketleri üzerinde de etki etmeye başlamıştır (Bilgi Güvende, 2022a). 2015 yılında "Grand Theft Auto V" adlı oyunda farklı oyun eklenti modları içerisine gizlenmiş şekilde keyloggerlar tespit edilmiştir (PCMAG, 2015). 2017 yılına gelindiğinde Hewlett Packard (HP) dizüstü bilgisayar modelinin fabrika çıkışlı olarak topluca keylogger yüklü olarak gönderildiği tespit edilmiştir. HP tarafından yapılan açıklamada söz konusu durumun siber saldırı olarak nitelendirilmesinin yanlış olduğu, bunun sadece söz konusu modellerin dağıtıma çıkmasından önce klavye performansını teşhis etmeye yönelik araç olarak kullanılan ve silinmesi gereken uygulamalar şeklinde yorumlanması gerektiği söylenmiştir. Yani bu keyloggerların HP yaması olarak yazılımsal hata tespit vasıtası şeklinde kullanıldığı anlatılmaya çalışılmıştır (CSO, 2024b).

2020'li yıllarda ortaya çıkan ve geniş kitlelere yayılan keyloggerlara bakıldığında, kötü amaçlı yazılım programları olarak "snake keylogger" ve kökeni eskiye dayanan ancak yenilenen şekliyle "phoenix" göze çarpmaktadır (CSO, 2022). Snake KeyloggerZ veri

kaydedicisi ".NET" üzerinden kötü amaçlı olarak üretilen bir yazılımdır. Saldırıda bulunulan cihazdan kayıtlı halde kimlik bilgileri, daha önce girilen tuş vuruşları, sitelere ait ekran görüntüleri ve pano verilerini de içeren kritik ve kişisel bilgileri ele geçirmek hedeflenmiştir (Fortinet, 2021). Phoenix'e bakıldığında ise yine diğer keylogger gibi kötü amaçlı bir yazılım çeşidi olduğu ve neredeyse yirmi tane tarayıcı, dört tane posta istemcisi, çok sayıda FTP ve sohbet istemcisinden bilgi ve veri ele geçirdiği tespit edilmiştir. Phoenix yazılımı, bilgileri ele geçirme becerisi ile birlikte seksenin üzerinde güvenlikle ilgili değişik donanım ve analiz aygıtının faaliyetlerini yok etmeye çalışan Anti-AV modülünü içermektedir. Bununla birlikte söz konusu yazılım araştırıcı, tespit edici savunma ve korunma araçlarına haizdir. Phoenix başta Kuzey Amerika, Birleşik Krallık, Fransa ve Almanya olmak üzere Avrupa'nın muhtelif yerleri ile Orta Doğu'daki kişileri hedef tahtasına koymaktadır. Ortak şekilde basit posta aktarım protokolü (SMTP) ve FTP sızdırma protokolleri içermekle birlikte "Telegram" uygulaması kullanılarak veri aktarımı sağlamaktadır. Küresel çapta bir uygulama olan Telegram, yasal olması ve uçtan uca şifreleme şeklinde güvenlik formatı içermesi sebebiyle saldırganlarca tercih sebebi olmaktadır. Phoenix, Telegram'ın mesajlaşma yapay zekası üzerine Hiper Metin Transfer Protokolü (HTTP) talebi iletmektedir. Bu talep, Telegram'ın API anahtarını ve mesajlaşmaya ait kimliğini barındırmakla beraber buradan ele geçirilen veriler, URL kodlamasındaki metin parametresinden süzgece sokulmaktadır. Burada ortaya çıkan sonuç ise, Phoenix'in Telegram APİ'sini yasal olmayan şekilde kötü niyetli kullandığı ve veri sızdırdığı gerçeğidir. Yine bunun gibi "Masad Stealer" ve türevleri şeklinde oluşturulan kötü niyetli yazılımlar bahse konu metotları kullanarak veri hırsızlığı yapılmaktadır (Cybereason, 2024).

Casus Programlar (Spyware)

Casus programlar, bilgisayar ve sistemlere rıza dışı şekilde erişim sağlayarak internet kullanıcılarının kişisel bilgi ve verilerini çalan, ifşa eden ya da değiştirebilen yazılımlardır. Söz konusu programlar genellikle "adware attack" olarak nitelendirilen ve ticari amaçlarla kâr amaçlı olarak reklam şirketlerine satılan verileri hedeflemektedir (Fortinet, 2024b). Büyük verilere ihtiyaç duyan şirketler tüketicilerin ürüne olan bağlılığı, tercihleri ve yönelimleri çerçevesinde söz konusu verileri ticari hedefleri doğrultusunda satın almaktadır. Bu çerçevede şirketlerin veri havuzlarında kişilerin girdikleri web siteleri, internetten indirdikleri dosyalar gibi kişisel alanı ihlal eden veriler bulunmaktadır (Doğan, 2021).

Casus programlar ile kullanıcıların mikrofonlarını araç olarak kullanıp sesleri kaydedilebilmekte, sistem ve bilgisayardan ekran görüntüleri alınabilmekte, uzaktan kontrol fonksiyonu gerçekleştirebilmekte ve over-the-top medya servisleri (OTT), mesaj ve mail içerikleri görüntülenebilmektedir (Güngör, 2021). Ele geçirilen veriler ve bilgiler kredi kartı dolandırıcılığı, kimlik sahteciliği, bilgi hırsızlığı gibi çeşitli suçlarda araç olarak kullanılabilmektedir. Bu yöntemle şirketlere ait cihaz, sistem ve ağlar siber saldırılara karşı savunmasız hale getirilmekte ve sistem performansı etki altına alınarak internete erişim yavaşlatılmaktadır (Fortinet, 2023). Söz konusu veriler sadece ticari şirketlere değil aynı zamanda terör örgütleri ile de paylaşılabilmekte, bu da devletlerin milli güvenliğine ilişkin sorunları beraberinde getirmektedir.

Bu tür programlar, sistemlere erişim sağladıktan sonra gizli şekilde sistemde kalarak doğru zamanda verileri ele geçirme amacıyla üretilen yazılımsal kodlamalar olarak tezahür etmektedir. Söz konusu programlar kötücül yazılımların irade dışı indirilmesi (drive-by download) yöntemi, sahte açılır pencere yöntemi veya truva atlarının meşru kod şeklinde programa sızması ile de siber saldırıda araç olarak kullanılabilmektedir (Doğan, 2021).

Casus yazılım türlerine bakıldığında reklam yazılımları ön plana çıkmaktadır. Bu yazılımlar kullanıcı verilerinin reklamcılara satılmasını veya kötü niyetli reklamlarda kullanılmasını sağlamaktadır. “İnfostealer” denilen casus yazılım türü sistemlerden bilgi toplayarak bu bilgileri “instant messaging” denilen sistemlerde taramaktadır. Kökkitler (rootkit) sistemlerin zafiyetlerinden faydalanarak veya sistemlerin teknik kısımlarında yönetici yetkisiyle oturum açıp aygıtlara erişebilmektedir. Kökkitlerin sistem içerisinde belirlenmesi ve tespit edilmesi neredeyse imkansızdır. Diğer taraftan “RedShell” adı verilen casus yazılım türü, bilgisayar oyunları henüz cihaza kurulum aşamasındayken sisteme sızarak internet ortamındaki davranışları takip etmeye başlamaktadır. Bilgisayar oyunları ve konsol oyun pazarının büyük bir pazar payına sahip olduğu düşünüldüğünde oyun firmalarının bunu kötüye kullanması kaçınılmazdır. Sistem izleyicileri, keylogger mantığıyla çalışan ve özellikle sosyal medya hareketlerini izleyen casus yazılım türüdür. İzleme tanımlama bilgileri, yine aynı amaçla kullanılan ve çevrim içi hareketlerin izlendiği casus yazılım türüdür (Fortinet, 2024b).

Bir diğer casus yazılım türü olan “cookies” yani çerezler internette erişilen site bilgileridir. Bu siteler kullanıcıların cihazlarında gizlice saklanmaktadır. Çerez uygulamalarında asıl amaç internet kullanıcılarının web siteleri üzerindeki kullanım kolaylığını geliştirmek olduğu halde kötü niyetli siber saldırganlar tarafından kullanıcılara ait hareketlerin takip edilmesine (tracking cookie) de hizmet etmektedir (Güngör, 2021). Sabit disk içerisinde yer almakla birlikte hangi amaçla kullanılacağı saldırganların hedef aldıkları ortama ve kurbanlara göre farklılaşmaktadır. Özellikle de tüketicilere ait hareketlerin şirketler tarafından izlenebilmesi amacıyla kullanılmaktadır. Arama motorlarındaki tuşlama hareketleri, girilen anahtar sözcüklerin tespiti gibi durum analizleri ve internet alışveriş sitelerinin kullanılma sıklığı, girilen sitelerin tıklanma sayıları gibi çeşitli sayısal verilerin elde edilmesi yine çerezler aracılığıyla sağlanmaktadır. İnternet sitelerine girerken karşılaşılan matbu sözleşmeler kullanıcıların onayına sunulmakta ve bu vasıtayla çerezler kayda alınmaktadır. Fakat çerezlerin kabul edildiği bağlama göre kullanıcılar hakkında özel hayatın gizliliği ve kişisel verilerin ihlalini içerecek şantaj suçuna dahi sebebiyet verebilecek faaliyetlerde bulunulabilmektedir. Kişisel ve mahrem bilgilerin internet ortamında yayımlanması da yine karşılaşılabilen durumlardandır. Burada ayırt edilmesi gereken nokta internette e-ticaret yapan şirketler için kişisel verilerden çıkarılarak anonimleştirilmiş veri ve bilgilerin kullanılmasının yasal olduğudur. Bu veriler kullanıcıların ürünlere olan ilgisi, kullanım alışkanlıkları ve hobileri gibi kişisel bilgileri hakkında fikir vererek şirketlerin ticari satış politikalarını şekillendirmesine yardımcı olmaktadır (Güngör, 2015).

Bunların yanı sıra casus yazılımların olumsuz etkileri çarpıcı düzeye ulaşabilmektedir. Öyle ki işlemci kapasitesi, sabit-harici belleklerin kullanımı veya ağ trafiğini enterferansa uğratarak bilgisayarların tamamen çalışamaz hale gelmesine sebep olunabilmektedir. Yine sistemde donmaların yaşanması, ön yükleme (booting) başarısızlığı ve internet hızının düşmesi de sık yaşanan problemler arasında yer almaktadır. Casus yazılımlar kendilerine karşı üretilen başka yazılımları önleyerek sistemden silinmesinin önündeki engelleri ortadan kaldırabilmektedir. Bu tip yazılımlarla internet ortamındaki çerezler öğrenilerek dinamik link kütüphaneleri (DLL) değişikliğe uğratılabilir. Değişiklikle güvenliğe ilişkin problemler oluşabileceği gibi bağlantı hataları da gündeme gelebilir. Casus yazılımların varlığının göstergesi olarak kullanıcıların bilgisayarlarında istenmeyen e-postalar veya arama motorlarında çıkan reklamlar ile yönlendirmeye sebep olan pop-uplar

bulunabilir. Bu saldırılardan korunma yöntemi olarak uç noktada dış faktörlere karşı engelleyici bir katman oluşturulması bilinen ve uygulanan en sık yöntemdir. Öyle ki bu korumayı modern dönemde virüsten korunma programları sağlamaktadır. Bununla birlikte ağ güvenliği sağlayan önlemlerin alınması, pop-up önleme programları ve rıza dışı dosya indirmeye ilişkin "network inspection" denilen denetim sistemleri saldırılara karşı caydırıcılık ve korunma sağlanmasında kritik öneme sahiptir (Doğan, 2021).

Casus yazılımlar arasında "CoolWebSearch" ve "Cydoor" en çok bilinen yazılım saldırılarıdır. CoolWebSearch, tarayıcılar üzerinde etki eden casus yazılım ailesine aittir. Bu yazılım web tarayıcısını ele geçirmektedir. Yazılım, tarayıcıların şüpheli olarak addedilen farklı sitelere pop-up reklam ve linkler aracılığıyla yönlendirilmesine sebep olan kötücül kodlar indirebilmektedir. Tarayıcı üzerindeki ayarları değiştirerek siteler üzerinde arama yapılan sorgulamalar, erişim sağlanan linkler, IP adreslerini de içeren ve "digital footprint" veya "digital shadow" olarak nitelendirilen tüm hareketleri takip etmektedir. CoolWebSearch çalışma metodolojisine bakıldığında hackerlar web sayfalarının zafiyetlerinden faydalanarak tarayıcılara ait ana sayfa ve internet üzerindeki aramaları öğrenmek için farklı HTML kodlarını yayar. CoolWebSearch yazılımı varsayılan tarayıcıyı CoolWebSearch.com adresi ile değiştirmektedir. Söz konusu yazılım, Internet Explorer başta olmak üzere sonraki süreçte Google Chrome ve Mozilla Firefox gibi tarayıcılara yönelik saldırılar da gerçekleştirmiştir. Bunların yanı sıra söz konusu yazılım "pay per click" sistemiyle meşru olmayan şekillerde ekonomik kazanç da amaçlamaktadır. Diğer kötücül yazılımlarla bilgisayara başka bir yazılımla birlikte yüklenen programlar (PUP) şeklinde bilgisayarlara ve sistemlere bulaşarak potansiyel olarak tehdit oluşturmaktadır (Internet Security, 2024).

Şirketlerin yasal olarak KVKK metinlerini de kullanıcıların onayına sunarak çerezleri (cookies) kullanıcıların rızasına sunması ile casus yazılımlar arasında küçük bir farklılık bulunur. Özellikle bu konuda yaşanan ve yargıya taşınan davalarda genellikle şirketler meşru olarak bu uygulamaları kullanıcıların kullanıma sundukları savunmasını yapmakta ve casus yazılım kullanmadıklarını iddia etmektedir. Bu nüansın yargı mercilerince doğru şekilde değerlendirilerek tarafların haksız uygulamalarla karşılaşmasının

önlenmesi için bu konuda teknik personellerin ve bilişimci beyaz hackerların desteğinin alınması önemlidir.

Fidye Amaçlı Yazılımlar (Ransomware)

Fidye amaçlı yazılım, sistemlerde ve bilgisayarlarda depolanan veri ya da bilgilere kullanıcıların erişimini engelleyen kötücül yazılım türüdür. Bu yazılım aracılığıyla sistem ve bilgisayarların yönetimi ele geçirilerek verilerin yok edilmesi, şifrelenmesi, silinmesi, erişilemez hale getirilmesi gibi tehditlerle karşı taraf mağdur edilmektedir. Mağdurlara iletilen ve belirli bir meblağ karşılığında sisteme geri erişim sağlanabileceği mesajı bu saldırıların ana unsuru görünümündedir (NCSC, 2020b). Bu tür siber saldırı yazılımları kötücül yazılım kategorisinin en yıkıcı etki doğuran sınıfında yer almaktadır. Öyle ki yaklaşık 70 mb yer kaplayan 1000 adet dosyadan oluşan bir klasör 16 dakikalık bir sürede siber saldırganlar tarafından şifreleme sistemi ile kilitlenebilmektedir (Badejo, 2019). Tarihsel olarak bu saldırı tipinin ilk örneği The AIDS (AIDS Info Disk) Trojan (PC Cyborg Trojan) şeklinde isimlendirilen ve 1989'da Dr. Joseph Popp tarafından üretilen siber saldırı aracıdır. Bu siber saldırılarda ortalama 160 kilobayt saklama alanına sahip floppy diskler kullanılmıştır. Fidye amaçlı yazılımda kullanılan virüse karşı siber saldırganlar tarafından istenilen bedel ise 189 USD olarak belirlenmiş ve Panama'da yer alan postane hesabına yatırılması talep edilmiştir (Mohurle ve Patil, 2017).

Fidye amaçlı yazılımlar kategorize edildiğinde üçlü bir sınıflandırma ortaya çıkmaktadır. İlk sınıfta "korkutma fidye yazılımı (scareware)" olarak adlandırılan ve ele geçirilen dosyaların güvenilir şekilde korunduğu ancak saldırganlar tarafından istenen meblağın ödenmesine kadar pop-up olarak isimlendirilen çerezlerin sıklıkla görüldüğü fidye amaçlı yazılımlar bulunmaktadır. İkinci sınıfta bulunan "ekran kilitleme fidye yazılımları" ise işletim sistemlerini ele geçirerek kullanıcının erişimine kapatmaktadır. Sistem veya bilgisayar tekrar başlatıldığında siber saldırganlar tarafından kullanıcı ekranına yansıtılan örgüt logoları, terörist unsurlar ya da kullanıcının suç işlediğine dair uyarılarla mağdur konumunda bulunan kişiler tehdit edilmektedir. Söz konusu tehdidin sonlandırılmasının özellikle kripto para cinsinden belirli bir meblağın saldırganın paylaştığı banka hesabına yatırılması ile mümkün olabileceği belirtilerek karşı taraf zor durumda bırakılmaktadır. Üçüncü sınıfta ise "şifreleme fidye yazılımı (encoding ransomware)" bulunmakta ve bu

yazılım kullanılarak şifreleme anahtarı siber saldırgan tarafından mağdura sunularak silinen veya ele geçirilen belgelerin iade edileceği ya da kurtarılabileceği mesajı karşı tarafa iletilmektedir. Bu sınıfta yer alan fidye yazılımlar siber saldırganların son zamanlarda sıklıkla kullandığı etkin saldırılar kapsamında yer almaktadır (Mehra ve diğer., 2019).

Fidye amaçlı yazılımdan farklı olarak silici kötü amaçlı yazılım, genellikle yok etmeyi veya kalıcı kayba neden olmayı amaçlamaktadır. Otoritelere göre bu yöntemin kullanılma sebebi bir ağdan bilgi sızdırdıktan sonra bu fiile yönelik izleri gizlemek veya doğrudan kesintiye neden olmaktır (CSA Singapore, 2023). Bu saldırı türünde kullanıcının dosyalarına tekrardan erişim sağlayabilmesi fırsatı sunularak para aracı olarak fidye istenmektedir. Siber saldırganlar bunun yanı sıra verilerin ve fikri mülkiyet hakkı içeren unsurların sanal ortamda paylaşılmasını veya parayla satılmasını engellemek amacıyla fidye yani ödeme talep edebilmektedir (Australian Cyber Security Center, 2024). Saldırı sonrasında ödeme yaparak eski bilgilere erişim sağlanması amacıyla çoğunlukla bilinmeyen bir mail adresi vasıtasıyla siber saldırı gerçekleştirilmektedir. Mağdur kişilerle iletişim kurularak bilinmeyen ve yönlendirilmiş bir internet sayfasındaki yönergelerin takip edilmesi talep edilebilmektedir. Bu saldırılarda da şifrelenen sistemlere tekrar erişim amacıyla genellikle kripto para birimi cinsinden fidye istenmektedir. Fakat istenen fidye miktarı karşılansa dahi bilgisayarlara veya içerisindeki dosyalara erişebileceği konusunda kesinlik bulunmamaktadır. Bu yöntem literatürde "silici kötü amaçlı yazılım (wiper malware) olarak bilinmektedir. Değinilen nedenlerden ötürü, internet olmadan da çalışan dosya yedekleme sistemlerinin kullanılması kritik öneme sahiptir (NCSC, 2024).

Bir diğer fidye yazılımı olan "hizmet olarak fidye yazılım (RaaS)" siber saldırganların herhangi bir emek vermeden ve eğitim almadan ücretli üyelik modeli şeklinde ulaşabildiği intikam amacıyla kullanılan yazılım türüdür. RaaS paketleri ve üyelikler, kötü niyetli saldırılarda kullanılmak üzere, internette karanlık ağ (dark web) olarak isimlendirilen ve gizli olarak erişim sağlanan internet sitelerine dair platformlarda ücretli olarak sunulmaktadır (Mehra ve diğer., 2019). Hizmet olarak fidye yazılım saldırılarında kullanılan metotlar çoğunlukla kimlik avı e-postaları ve istismar kitlerinden oluşmaktadır. RaaS paketleri imtiyaz hakkı (franchising) şeklinde satış veya kiralama usulü ile saldırı gerçekleştirmek isteyen kişilere verilmektedir. Söz konusu paketleri satan siber saldırganlar paketleri satın alan kişilere kılavuzluk hizmeti de sunmaktadır. Söz konusu paketlere

herkesin ulaşabilmesi ve bilgisi olmadan dahi saldırıların gerçekleştirilebilmesi siber saldırıların artmasında büyük bir etki oluşturmaktadır. Siber saldırıların başarıya ulaşması sonucunda mağdurlardan haksız şekilde elde edilen fidye gelirleri servis sağlayıcılar, yazılımcılar ve siber saldırganlar arasında paylaşılmaktadır (Tripwire, 2018).

Fidye yazılım saldırılarına bakıldığında 2012 yılında Orta Doğu'da ortaya çıkan "Shamoon" fidye yazılımı dikkat çekmektedir. Öyle ki söz konusu yazılım vasıtasıyla Suudi Arabistan'nın sahip olduğu en büyük ulusal petrol şirketlerinden Saudi Aramco'ya siber saldırı gerçekleştirilmiştir. Yapılan açıklamalarda ayrıcalıklı erişim yetkisine sahip bir şirketin Saudi Aramco ağında kötü niyetli olarak bahse konu fidye yazılımını harekete geçirdiği ifade edilmiştir. Söz konusu saldırının sistemlere bulaşan virüsle birlikte sabit disk verilerini sildiği ve sistem ara yüzlerindeki verileri alevli ABD bayrağı şeklinde görselleştirdiği tespit edilmiştir. Söz konusu kötücül yazılım, 30.000'den fazla sistem ve bilgisayara bulaşı sağlamış ve söz konusu cihazların kullanılamaz hale gelmesine yol açmıştır. Saudi Aramco şirketi saldırıya karşılık virüsün yayılmasını engellemek amacıyla kurumsal ağını dışarıya kapatmıştır (CSA, 2022).

Rusya-Ukrayna arasında 2014 yılında başlayan savaşın etkileri halen devam ederken savaşın konvansiyonelden sibere dönüşü de geçen on yıl içerisinde daha belirgin hale gelmiştir. Öyle ki ABD ve İngiltere'nin de içerisinde bulunduğu Batı bloğu fidye yazılım saldırıları için Rus hackerların ciddi faaliyetlerinin olduğunu aktarmışlardır. Batı tarafından, Ukrayna'nın ilhakı nedeniyle Rusya'ya uygulanan ambargolar çerçevesinde Rus vatandaşı yedi kişinin Rusya'nın en ünlü siber suç örgütlerinden Trickbot örgütü üyesi olması nedeniyle iadesi talep edilmiştir. Bu suçlulara ilişkin iade prosedürünü işletmeyen Rusya olaya sessiz kalmıştır. Söz konusu örgüt üyeleri Covid-19 pandemisi döneminde ABD ve İngiltere'deki sağlık kuruluşları ile hastanelere siber saldırı gerçekleştirmiştir. Bunun yanı sıra kritik altyapıları etkileyen ciddi tahribatları da planlayarak icraate geçtikleri ifade edilmiştir. 2022 yılında International Business Machines (IBM) tarafından Ukrayna'ya yönelik siber savaşın ana komuta merkezi olarak Trickbot siber suç örgütü gösterilmiştir. 2023 Şubat ayı başlarında yine Birleşik Krallık tarafından yayınlanan açıklamalarda "birinci seviye ulusal güvenlik tehdidi" alarmı verilmesine sebep olan yaklaşık olarak 150 adet fidye amaçlı yazılım saldırısının belirlendiği ve bunlara karşı önlem alındığı aktarılmıştır (Politico, 2023).

2019 senesinde gerçekleşen bir diğer fidye yazılım saldırısı sonucunda Norveç merkezli Norsk Hydro şirketi faaliyetine son vermek durumunda kalmıştır. Söz konusu şirketin bölgedeki 900.000 civarında eve enerji sağladığı düşünüldüğünde vatandaşların ve devlet ekonomisinin büyük bir zarar uğradığı görülmektedir. Söz konusu ekonomik kayıp yaklaşık 51 milyon dolar olup bununla birlikte şirkete ait 3.000'den fazla sunucu saldırıdan olumsuz etkilenmiştir. Yine bu Norsk Hydro şirketi de dahil olmak üzere birçok firma ve vatandaşın bilgisayarından meydana gelen küresel ağın büyük ve önemli alanları kriptografik yazılımlarla şifrelenmiştir (TIME, 2021). Saldırının büyüklüğüne ilişkin değerlendirme yapıldığında Norsk Hydro şirketinin dünyanın en büyük alüminyum üretim tesislerinden birisine sahip olup 40 farklı ülkede 35.000 çalışanı olan izabe tesis ve fabrikaları olması söz konusu siber saldırının etki derecesini göstermektedir. Söz konusu saldırı Norsk Hydro şirketini küresel üretim miktarlarını etkilemiş ve Avrupa ile ABD'de yer alan üretim tesisleri tedarik zinciri süreçleri bakımından zarar görmüştür. Bununla beraber üretim tesislerine ait otomasyonlu endüstriyel kontrol sistemleri devre dışı kalmış, üretimin ve operasyonların devamlılığını için SCADA sistemlerinin komuta ve kontrolü otomatik olmayan klasik şekilde yönetilmiştir. Diğer taraftan siber saldırılarda en önemli unsurlardan birisinin insan unsuru olduğu bu örnekte bir kez daha pekişmiştir. Bahse konu fidye yazılımı saldırısı, Norsk Hydro şirketine ait tesis çalışanının şirketin müşterisinden gönderilen virüslü bir maili açması sonucu gerçekleşmiştir. Söz konusu personel hatası bilgisayar korsanlarının kötü niyetli amaçlarına hedef olmuş ve sistem altyapılarına erişim sağlanmıştır. Bu yetkisiz erişimle birlikte siber saldırganlarca kötücül yazılım içeren virüs sisteme sızdırılmıştır. Diğer taraftan söz konusu fidye yazılım saldırısı gelişmiş kalıcı tehdit (APT) siber saldırısı ile güçlendirilerek saldırının etki derecesi artırılmıştır (CyberBrokers, 2020).

2020 yılında ABD Washington DC Polis Departmanına yönelik gerçekleştirilen SolarWinds siber saldırısı ABD'ye ait kurum ve kuruluşları olumsuz etkileyerek servis sağlayıcısı kritik altyapılarının siber güvenlik zafiyetlerini ortaya çıkarmıştır. Söz konusu saldırı kritik altyapıların yanı sıra tedarik zincirini de olumsuz şekilde etkilemiş ve bilgi teknolojileri sektörü ve diğer bağlantılı sektörlerin üretiminin durmasına sebep olmuştur. FBI yetkililerine göre söz konusu siber saldırı Rusya tarafından kasıtlı olarak gerçekleştirilmiştir. Öyle ki SolarWinds saldırısının arkasında Rusya devletinin desteklediği bir siber suç çetesinin bulunduğu, söz konusu çetenin "Darkside" olduğunun teyit edildiği

ifade edilmiştir. Saldırının gerçekleştirilmesi sonrası karanlık ağ üzerinden saldırı gelirlerinin paylaşılması neticesinde hizmet olarak fidye yazılımı (RaaS) varyantının SolarWinds kapsamında uygulandığı belirlenmiştir. Kullanılan yönteme bakıldığında 100 gb civarında Colonial verisinin ele geçirilmesi ve rehin alınması söz konusu olmuştur. Bu verilerin siber saldırganlar tarafından kamuoyuna sunulması ile ABD kuruluşları tehdit edilmiştir (ICP, 2021b). Gelişmiş kalıcı tehdit saldırısını gerçekleştiren kişilerin arka kapı sokarak SolarWinds şirketinin tedarik zincirine eriştikleri ve şirket müşterilerinin SolarWinds tarafından sunulan truva atı kurulum paketlerini indirmeleri sırasında SolarWinds ürünlerini çalıştıran sistemlere ait verilerin ele geçirildiği belirtilmiştir (CIS, 2021). Bu saldırı neticesinde fidye yazılımına vücut veren veriler karşılığında mağdur konumundaki kişi ve şirketten yüksek miktarlı tekrar erişim ve veri iadesi ücreti talep edilerek kurbanlar zor duruma sokulmuştur. Burada umulan bir diğer amaç ise ABD'nin konvansiyonel anlamda güçlü bir devlet olduğu tüm dünyada kabul görmüş iken aslında siber saldırılarla bu konvansiyonel gücünü dahi kullanamayacağını gözler önüne sermek olmuştur (ICP, 2021b). SolarWinds saldırısı ile birlikte kontrol ve komuta sistemlerinin devre dışı kalması ve tedarik zinciri boyutuyla zincirleme bir etki bırakması bu şekilde yapılan bir saldırının küresel ve birçok sektöre tesir eden potansiyelini göstermiştir. Söz konusu sektörler arasında özellikle üretim, enerji, sağlık, ulaşım, ekonomi ve kamu hizmetleri sektörlerinin gelmesi söz konusu potansiyel tehlikeyi ortaya koymaktadır. Öyle ki üretimin aksaması durumunda devlet için kritik varlıklar ve savunma sistemleri etkilenebilmekte, sağlık kuruluşları hastalarına hizmet veremeyecek duruma gelebilmekte, ulaşımda yaşanan sıkıntılar tedarik zincirini etkileyebilmekte ve devletlerin kamu hizmetleri sekteye uğrayabilmektedir.

ABD yetkilileri tarafından yapılan açıklamalarda ABD'nin Colonial Pipeline, Kaseya ve JBS gibi yüksek profilli siber saldırılara maruz kaldığını bunun yanı sıra halihazırda devam eden Rusya-Ukrayna savaşında da siber saldırılarla karşılaşılması dolayısıyla siber güvenliği güçlendirmenin ulusal bir öncelik haline geldiği aktarılmıştır (ICP, 2022). 2021 yılında adından söz ettiren Colonial Pipeline fidye yazılımı saldırısı küresel çapta etkisi olan bir diğer saldırıdır. Bu saldırı ile ABD'de yer alan en büyük rafine ürün boru hattı kullanılamaz hale gelmiştir. Öyle ki söz konusu boru hattı, ABD'nin batısından doğu kıyılarına kadar mazot, benzin, ev ısıtma yağı, askeri yakıt ile uçak ve jet yakıtlarının büyük bölümünü karşılamaktadır. Colonial Pipeline saldırısı neticesinde rafine

ürünlerin ABD Körfezi kıyısından ABD Atlantik kıyısına taşınması ve iletimi kesilmiştir. Söz konusu boru hattı Texas'taki Gulf Coast'tan Linden, New Jersey'e kadar uzanmakla birlikte ABD ordusuna ikmali de içeren günde 100 milyon galon ve 2,5 milyon varil yakıtı 8.500 millik boru hattıyla taşıdığı göz önünde bulundurulduğunda söz konusu saldırının önemi ortaya çıkmaktadır. Yakıt iletimindeki sıkıntılar dolayısıyla ABD'nin güneydoğusunda yer alan benzin istasyonlarına yakıt ikmali sağlanamamış ve petrol kıtlığı dolayısıyla istasyonlarda araç kuyrukları oluşmuştur (ICP, 2021b). Söz konusu saldırı neticesinde yakıt iletim ve dağıtımına ilişkin kesinti yaşanması sebebiyle üç gün sonra ABD'nin Alabama, Florida, Georgia, Kuzey ve Güney Carolina eyaletlerinde yakıt tüketimi %100'e ulaşmıştır (CNN Politics, 2021). Bununla beraber Charlotte eyaletinde benzin istasyonlarında mevcut yakıt miktarı %29'a gerilemiş, Washington DC'deki petrol istasyonlarında ise % 13 seviyesinde tüketilebilecek yakıt kalmıştır (WBTV, 2021); Bloomberg, 2021). Yetkililer tarafından fidye yazılım saldırısı neticesinde saldırıya uğrayan şirketin siber saldırganlara şifre çözme aracı karşılığında 75 Bitcoin (5 milyon dolar) civarında bir meblağ ödediği aktarılmıştır (The New York Times, 2021a). Yine ABD'de faaliyet gösteren kamu kurum ve kuruluşları ile bakanlıklar bu saldırıdan olumsuz şekilde etkilenmiştir. Bu kurumlar Pentagon, Siber Güvenlik ve Altyapı Güvenliği Dairesi ve ABD Hastalık Kontrol ve Önleme Merkezi olarak ön plana çıkmaktadır (The New York Times, 2021b). Bununla beraber Colonial Pipeline siber saldırısı uçakların uçuş rotalarında, hava koridorlarında ve güzergâhlarda değişikliklere sebep olmuştur. Söz konusu değişiklikler arasında Charlotte Douglas Uluslararası Havalimanı'nda boru hattının devre dışı kalması dolayısıyla meydana gelen yakıt kıtlığı kapsamında American Airlines hava yolu şirketinin uçuş saat ve tarihlerini değiştirmesi de yer almaktadır (Reuters, 2021). Söz konusu uçuşlardan Honolulu ve Londra gibi farklı rotalarda dört günlük süreçte uçuş programlarına yakıt ikmaline fırsat veren istasyonlar ve uçaklar eklenmiştir. Buna örnek olarak Hartsfield-Jackson Atlanta Uluslararası Havaalanı'nın tedarikçiler tarafından kullanması verilebilecektir (CNBC, 2021).

2021 senesinde gerçekleşen olayda Brezilya'da faaliyet gösteren dünyanın en büyük et işleyicisi JBS'e yönelik fidye yazılım saldırısında bulunulmuştur. Bu olayın sonrasında CISA ve FBI yetkilileri tarafından yapılan açıklamalarda söz konusu siber saldırının arkasında Rusya'nın bulunduğu değerlendirilmiştir. Rusya destekli hacker grubunun hizmet olarak fidye yazılımı yöntemini uyguladığı tespit edilmiştir. Saldırı neticesinde ABD'de

faaliyette bulunan dokuz büyük et paketleme tesisi işlemez hale gelmiş ve gıda sektöründe tedarik zinciri olumsuz şekilde etkilenmiştir. Bu döneme denk gelen Covid-19 pandemisi nedeniyle halihazırda üretimde yaşanan sıkıntılara söz konusu gıda krizi de eklenmiştir. Bu nedenle söz konusu şirket ve dağıtım ağındaki diğer gıda şirketleri iflas etme tehlikesiyle karşılaşmıştır. CISA yetkililerinin açıklamalarında gıda ve tarımın kritik altyapı sektörü olması nedeniyle bu sektörde gerçekleşecek siber saldırıların yıkıcı etkisi olduğu ifade edilmiştir. Bununla beraber fiziksel ve sanal varlıklar ile kritik sistem ve ağların ABD için önemine değinilerek bunların yok olması halinde ulusal güvenlik, ekonomi ve halk sağlığı üzerinde vatandaşlara yönelik olumsuz durumlar oluşacağı aktarılmıştır (ICP, 2021c).

2022 yılındaki bir diğer fidye yazılım saldırısı ABD'de faaliyet gösteren ve Heritage Provider Network'ün CA merkezli bağlı kuruluşu olan San Bernardino Regal Medical Group'a yönelik olarak gerçekleştirilmiştir. Bu saldırı sonrasında hastalara ait kritik ve hassas verilerine erişim kesilmiştir. Veri ihlali ile birlikte kişisel bilgilerin çalınmasına yol açan bu saldırı sonucunda yaklaşık 3.3 milyon hasta etkilenmiştir. Güneydoğu Colorado Hastane Bölgesi tarafından yapılan açıklamada saldırıdan etkilenen hastalara 3 Şubat 2023 itibariyle tebligat yazılarının iletildiği ve kişisel bilgileri yayınlanan hastalara ücretsiz olarak kimlik hırsızlığına karşı koruma hizmetlerinin verileceği aktarılmıştır (The HIPAA Journal, 2023). Son zamanlarda sağlık kuruluşlarına yönelik gerçekleştirilen siber saldırılardaki artış çeşitli araştırmaları beraberinde getirmiştir. Check Point Research'e göre küresel çapta sağlık kuruluşlarına yönelik siber saldırılar 2022'de %74 artmıştır. 2021 yılında yapılan araştırmada ise gerçekleştirilen ankette hastanelerin dörtte birinde fidye yazılımı saldırısı neticesinde gerçekleşen ölüm oranlarında yüksek seviyede artış olduğu gözlemlenmiştir. CyberPeace Enstitüsü tarafından yapılan araştırmada sağlık kritik altyapılarına yönelik gerçekleşen siber saldırılar sonucunda ortalama hasta bakım sürelerinde 19 günlük uzama meydana geldiği aktarılmıştır (IEC, 2023a).

Bu bağlamda 2009-2022 yılları arasında HIPAA Journal Sağlık Hizmeti Veri İhlali Raporuna göre veri ihlali bildirim sayıları aşağıdaki Şekil 2'de gösterilmektedir:



Şekil 2. Yıllık Sağlık Hizmetleri Veri İhlalleri (The HIPAA Journal, 2023b).

Bu rapordaki verilere bakıldığında 2009 yılından bu zamana kadar yıllık olarak veri ihlallerinin sürekli arttığı görülmektedir. Söz konusu grafik bahse konu artışın ciddi oranlara çıktığını somut olarak göstermektedir. HIPAA Journal Sağlık Hizmeti Veri İhlali Raporuna göre 2022 yılında 1 milyondan fazla kayıttan oluşan 11 sağlık hizmeti veri ihlali ve 500.000'den fazla kayıttan oluşan 14 veri ihlali rapor edilmiştir. Bu veri ihlallerine vücut veren siber saldırılar içerisinde fidye yazılımı ve bilgisayar korsanlığı saldırıları en büyük paya sahiptir (The HIPAA Journal, 2023b).

2022 yılında tekrar başlayan Rusya-Ukrayna savaşı sürecinde “Shamoon” fidye yazılımı siber saldırganların kullandığı gelişmiş bir siber saldırı yöntemi şeklinde tekerrür etmiştir. 2022 yılının başlarından bu zaman kadar siber güvenlik araştırmacıları yeni silici kötücül yazılım ve bunların gelişmiş türevlerinde önemli bir artış tespit etmiştir. Şubat 2022'de ABD’de faaliyet gösteren uydu iletişim sağlayıcısı Viasat'ın KA-SAT ağına yönelik yapılan siber saldırı neticesinde çok sayıda modem, AcidRain isimli silecek kötücül yazılımı vasıtasıyla çalışmaz hale getirilmiştir. Söz konusu saldırı ile Ukrayna başta olmak üzere Avrupa'da hizmet veren on binlerce Viasat müşterisi olumsuz etkilenmiştir. Öyle ki kullanıcıların internet bağlantıları kesilmiş ve haberleşme ağlarında problemler ortaya çıkmıştır. Almanya'da kinetik enerjiyi elektrik enerjisine çeviren 5.800 adet rüzgar türbini kontrol ve komuta eden SCADA’lar etkisiz hale getirilmiştir. Ukrayna hükümeti adına çalışan güvenlik personelleri, siber saldıranlarca devlete ait kurum ve kuruluşlar, banka ve

finans merkezleri ile kamu şirketlerini de içeren hedeflerin sekiz çeşit silici kötücül yazılım vasıtasıyla etkisiz bırakıldığı ifade edilmiştir. Söz konusu sekiz yazılım sırasıyla AcidRain, WhisperGate, WhisperKill, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero ve Industroyer2'dir. Rusya-Ukrayna savaşı süresince yeni silici kötücül yazılım güncellemeleri ve gelişmiş tür varyantlarının artışı küresel olarak potansiyel bir siber tehdit unsuru olarak ortaya çıkmıştır (CSA, 2022).

2023 yılında sağlık kritik altyapı sektörüne yönelik ABD'de gerçekleştirilen fidye yazılım saldırıları kapsamında ABD'de altı eyalette faaliyet gösteren ve yaklaşık otuz hastaneyi işleten Ardent Health Services yetkililerince yapılan açıklamada, bahse konu fidye yazılım saldırılarının Şükran Günü'nde proaktif olarak sağlık altyapısı ağlarının devre dışı kalmasına sebep olduğu ifade edilmiştir. Siber saldırıdan olumsuz şekilde etkilenen hastane ve sağlık kuruluşlarının günlük işlemlerine ve faaliyetlerine uzun bir süre dönemediği aktarılmıştır. Öyle ki bu süreçte çoğu hastanenin kayıt sistemi çevrim dışı kalmış ve bu sebeple hastalar bölgedeki diğer hastanelere nakledilmiştir (AXIOS, 2023). Wall Street Journal'a göre Sağlık ve İnsani Hizmetler Bakanlığı (HHS), 2023 yılı başından Eylül ayına değin fidye yazılım içeren siber saldırılarda 61 milyondan fazla kişinin tıbbi verilerinin sızdırıldığı ifade edilmiştir (WSJ.COM, 2023). Emsisoft'a göre ise 2023 Eylül ayına kadar hastane ve sağlık kuruluşlarına yönelik en az 128 fidye yazılımı saldırısı meydana gelmiştir (AXIOS, 2023).

2023 yılında meydana gelen bir diğer siber saldırıda Kuzey Amerika menşeili Dole şirketine yönelik fidye yazılımı saldırısı gerçekleştirilmiştir. Bu saldırı neticesinde 3000 çalışanı bulunan ve seri üretim yapan fabrika kapatılmıştır. Dole fidye yazılım saldırısı dolayısıyla küresel ölçekte gıda üretimi sekteye uğramış ve geçici gıda kıtlığı meydana gelmiştir (CyberCrimeMagazine, 2023). Bu saldırı neticesinde ortaya çıkan gıda kıtlığı, sektörü de olumsuz etkilemiş ve Dole şirketine ait ürünlerin bir haftadan uzun bir süre piyasaya arz edilememesine sebep olmuştur. ABD Menkul Kıymetler ve Borsa Komisyonu'na (SEC) sunulan yıllık raporda söz konusu saldırının Dole şirketine etkisinin sınırlı olarak operasyonel bazda olduğu ifade edilmiştir. Bu saldırının Dole şirketinin yaklaşık 10,5 milyon dolarına mâl olduğu ve bu miktarın 4,8 milyon dolarının halihazırda süren operasyonlara ilişkin olduğu aktarılmıştır. Bununla birlikte Legacy Dole sunucularının yarısını etkileyen bahse konu saldırının kullanıcılara ait bilgisayarlara olumsuz etkide

bulunduğu ve son kullanıcıların %25'inin bundan etkilendiği ifade edilmiştir (The Record, 2023).

Federal Soruşturma Bürosu İnternet Suçları Şikâyet Merkezi tarafından yayımlanan istatistiklere göre 2022'de gerçekleşen siber saldırılar neticesinde ABD'de siber suçlara ilişkin 800.944 şikâyetin kolluk ve diğer adli mercilere ulaştığı aktarılmıştır. 2016'daki istatistiklerle kıyaslandığında geçen altı yıl içerisinde bahse konu sayının yüzde yüz altmış sekiz (%168) oranında arttığı görülmüştür. 2022 yılında suça vücut veren siber saldırılar neticesinde maddi kayba uğrayanların yaklaşık yedi kat artarak 10,3 milyar dolara çıktığı tespit edilmiştir. ABD'nin New York şehrinde yaşanan siber saldırılarda %53 artış gerçekleşmiş ve söz konusu saldırılar sonucunda maddi zarar 106,2 milyon dolardan 775 milyon dolar seviyelerine yükselmiştir. Burada dikkat çekilmesi gereken nokta ise artışa etki eden en büyük siber saldırı türü payını fidye yazılım saldırılarının oluşturuyor olmasıdır. Söz konusu siber saldırılarda kritik altyapı sektörlerinden özellikle sağlık ve kamu sağlığı, finans, ticari ve devlet tesislerinin bulunduğu ifade edilmektedir (Dinapoli, 2023).

Söz konusu saldırılara karşı alınabilecek başlıca önlemler ise düzenli çevrim dışı ve site haricinde yedeklemeler yaparak sistemde oluşan aksaklıkların hızlı bir şekilde tespit edilmesini sağlamak, ihlal olması durumunda yaygın hasarı önlemek için ağ izleme ve gözden geçirme sistem günlüklerini uygulamaktır (CSA Singapore, 2023). Bunların yanı sıra güvenilir güvenlik paketleri ve kötü niyetli saldırılardan korunma amaçlı yazılımlar siber güvenlik önlemleri arasındadır. Aynı zamanda bu yazılımların güncel tutulması da büyük önem arz etmektedir. Tabi ki söz konusu saldırılarda yaygın şekilde kullanılan şüpheli bağlantı linki ve bu bağlantılara entegre eklerden mümkün olduğunca uzak durularak şüphe ile yaklaşılması kritik öneme haizdir (Fortra, 2018).

Arka Kapılar (Back/Trap Door)

Gizli veya arka kapı olarak adlandırılan siber saldırılar bilişim sistemlerine ait yazılımlarda veri alışverişi istasyonları dışında güvenlik zafiyeti olan ve açıkta bırakılan noktaları nitelemektedir (Ehliz, 2019). Bu siber saldırı türünde işletim sistemi programlarını kodlayan siber saldırganlar, ileride parola değiştirmeyi mümkün kılan sistem giriş yöntemlerine ait kodları hedefteki cihaza veya sisteme gömerek gizlemektedir (BTK, 2022).

Siber saldırganlar tarafından kullanıcılara ait giriş bilgileri atlanarak arka kapılar vasıtasıyla uzaktan erişim sağlanmaktadır. Bu vasıtayla daha zor şekilde girilebilecek sistemlere kolaylıkla giriş yapılabilmektedir.

Arka kapılara vücut veren sisteme giriş boşlukları siber saldırganlar tarafından isteyerek oluşturulabildiği gibi istenmeyen şekilde oluşan arka kapılar da ortaya çıkabilmektedir. İki durumda da siber saldırganların erişim sağladığı sistemler dolayısıyla yasa dışı işlemler gerçekleştirilebilmektedir. Söz konusu arka kapılardan sistemlere ait kritik verilere erişim sağlanarak altyapılara yönelik siber saldırılar düzenlenebilmektedir. Hedef olarak seçilen bilgisayar ve sistemlerdeki açık portlar tespit edilerek şifre kırma, ağ üzerindeki hareketleri ve işlemleri izleme, hesap oturumlarına erişme, DoS ve DDoS gibi tehlikeli siber saldırı atakları gerçekleştirilebilmektedir (BTK, 2022).

Arka kapı metotlarına bakıldığında bunlar arasında en sık kullanılan yöntemin dinleme ajanı yerleştirilmiş portların açık tutulması olduğu söylenebilecektir. Truva atlarından farklı olarak herhangi bir perdeleme olmadan açıkça görünmesi ve sistem üzerinden gizlice erişim sağlamaya yarayan yazılımlar olmasıdır. Truva atlarına benzer tarafı ise uzaktan erişim yöntemi şeklinde kullanılabilmesidir. Yine istenen amaca ulaşılabilmesi için virüs ve solucanların kötü niyetli kullanımına da açık konumdadır. Yani arka kapılar bu yazılımların aracı olarak da kötü niyetli faaliyetlerde ve siber saldırılarda kullanılabilir (Sağıroğlu ve Alkan, 2018). Arka kapı saldırılarının en bilinen örneklerinden biri Amerikan Ulusal Güvenlik Ajansı (NSA) hedef alınarak Microsoft'un Windows işletim sistemlerinde bıraktıkları gizli girişleri içeren siber saldırılardır. Bu olayın ortaya çıkışı ise 2016'da FBI tarafından Apple'dan talep edilen tuzak kapı isteğidir. Facebook ve Google ise meydana gelebilecek güvenlik açıklarına yönelik saldırıları göz önüne alarak Apple'a destek olmuşlardır. Buna karşılık Microsoft'un kurucusu olan Bill Gates söz konusu istekte bir beis görmediğini ifade etmiştir. Linux için de söz konusu talebin gönderildiği söylenmişse de bu yazılımın açık kaynak kod yapısına sahip olmasından ötürü söz konusu durumun oluşması pek olası olmamıştır (Güngör, 2021).

Yaşanmış arka kapı saldırılarından biri olan FinFisher (FinSpy) bir diğer ismiyle WingBird yazılımı, web kameraları ve mikrofonlar vasıtasıyla kullanıcılara ait kişisel bilgileri, gizli dosyaları, canlı yayın verilerini ele geçirebilmektedir (Kaspersky, 2021). Söz

konusu zararlı yazılım, normalde ücretli olan programların yama şeklinde ücretsiz olarak sunulmasıyla gerçekleştirilmektedir. Bu yama dosyaları bazı zarar verici sitelerde seri numaraları ile paylaşılarak yayılmaktadır (Alioğlu, 2019). Arka kapı uygulamalarına karşı açık kaynak kodlu yazılımların geliştirilmesi başlıca siber güvenlik önlemi olarak görünmektedir.

Korsan Amaçlı Yazılımlar/Kökkitleri (Rootkit)

Korsan amaçlı yazılımlar İngilizcede kök ve yazılım araç paketi manasına gelen kelimelerin bir araya gelmesinden meydana gelmiştir (Malwarebytes, 2023a). Kök kitler de denilen bu yazılımların kök tarafı Unix ve Linux işletim sistemlerinde sistem yöneticisi hesabı, kit tarafı ise uygulayıcı yazılımsal araçlar için kullanılmaktadır. Korsan amaçlı yazılımlar bilgisayar ve diğer sistemlerde gizlenerek istemsiz erişim sağlayan programlardır. Bilgisayar ve ağ üzerinden yönetici seviyesinde erişime olanak tanıyan kök kitleri sistemde saklanabilen kötücül yazılımlarla entegre şekilde siber saldırılarda kullanılmaktadır (Veracode, 2023). Sistem ön yüklemesinde çalıştırılan araçlar kök kitler aracılığıyla kendisini gizlemektedir. Bu kapsamda kayıt defteri anahtarları ve kullanıcılara ait hesaplar saklanmaktadır (ENİSA, 2024b). Kök kitleri, sistem içerisinde yüksek düzeyde imtiyaz veren yapıya sahiptir. Söz konusu yapılar cihazlardaki varlıkları gizlemek amacıyla programlanmaları nedeniyle tehlike oluşturmaktadır. Özellikle uzaktan kontrol yetkisi dolayısıyla sistemleri olumsuz şekilde etkilemektedir. Söz konusu özellik kimlik avı mailleri aracılığıyla etkinleştirilmektedir. Bu yazılımlar erişime kök seviyede olanak tanıdıklarından dolayı antivirüs programlarını engellemek, kullanıcılara ait hareketleri izlemek, kişilere ve kurumlara ait verileri ele geçirmek ya da diğer kötü amaçlı yazılımları etkinleştirmek gibi faaliyetlere neden olabilmektedir (Malwarebytes, 2023a).

Korsan amaçlı yazılımların virüslerden farkı, bilgisayar ve sistem üzerinde yayılmayı ve sistemi yavaşlatmayı hedef almamasıdır. Bu yazılımların temel amacı bahse konu sistemlerde gizlenerek yönetici seviyesinde kontrol sağlamaktır. Söz konusu yazılımların sisteme gizlice yerleşmesini sağlayan ise, güvenli kaynak niteliğindeki programların kökkit şeklinde kontrol merkezi (kernel) yapısında yüksek yetkiyle donatılmasıdır. Kökkitler kontrol merkezine farklı modüller atayarak sistem içerisinde yayılmaktadır. Aynı zamanda kullanıcılara ait hareketleri kayıt altına alan söz konusu yazılımlar güvenlik zafiyetlerinden

faydalanarak sistemlerde tahribat yaratmaktadır. Bununla amaçlanan yetki artırımı saldırılarında olduğu gibi üst yönetici olarak yetki gerektiren işlemlerin kolaylıkla yerine getirilebilmesidir. Bu yazılımlar genellikle windows işletim sistemlerini etkilemekte ve gizlilik sağlamaktadır. Gizliliğin sağlanması gerçekleştirilen sistem sorgulamalarına süreklilik arz edecek şekilde yanıltıcı cevapların gönderilmesi ile mümkün olmaktadır. Kökkitler farklı tarama yöntemleri sayesinde tespit edilebilmekte ve kritik altyapılara yönelik siber saldırılar ve dolandırıcılık faaliyetleri önceden engellenebilmektedir. Ancak kökkitler kernel üzerine ve sistem çekirdeğine entegre olan antivirüs programları dolayısıyla tespit edilememektedir. Bu sebeple daha gelişmiş saldırı tespit ve önleme sistemlerinin kullanılması ve kökten çözüm içinse mevcut işletim sistemi yenilenmesi gerekir (Doğan, 2021).

Tek olarak kökkitler zayiat noktasında büyük yıkımlara yol açamazken virüs, truva atı ve solucanlarla entegre şekilde çalıştıklarında yıkıcılık özellikleri yüksek oranda artmaktadır. Yapılarına göre kökkitler farklı isimlerle nitelendirilmektedir (Samet, 2018). Bunların ilki "kernel rootkit"dir. Bu tür kökkitler çekirdek üzerindeki rootkit işletim sistemlerine etki etmektedir. Sistem değişikliklerine yol açılarak gizleme faaliyetlerinde bulunulmaktadır. Bununla beraber donanımsal ve hıza ilişkin özellikleriyle ön plana çıkmaktadırlar (Yıldız, 2022). Diğer bir tür ise "Hypervisor (Virtualized) Rootkit" olarak isimlendirilmektedir. Bu tip kökkitler donanımların sanal hale getirilmesinden faydalanarak donanımla çekirdek arasına yerleşir. Bu vasıtayla işletim sisteminden donanımlara gönderilen talepleri tespit eder (ENİSA, 2024b). Hiper yöneticilerin himayesi altında tutulan sanal donanımlar sorunsuz çalışıyormuş izlenimi yaratmaktadır. Bu sebeple de Rootkit tarafından yapılan kötücül hareketler gün yüzüne çıkmamaktadır (Yıldız, 2022). Üçüncü tür rootkit "firmware/hardware rootkits" olarak adlandırılır. Bu türün ana özelliği yazılımın küçük olması ve çok sık değişikliğe uğratılmasa dahi güncellenebilmesidir (ENİSA, 2024b). Firmware rootkit sabit yazılım içerisine gömülü haldeki kodlamalardan yararlanmaktadır (Yıldız, 2022). Bir diğer kökkit olan "Application Rootkit" kullanıcı modunda faaliyet gerçekleştirmektedir. Sistem hizmetlerine etki ederek değişikliğe sebep olan bu yazılımlar ağ bağlantılarını da değiştirir. Diğer kökkitlerden farklı olarak bu kökkitler antivirüs programları tarafından tespit edilebilmektedir (ENİSA, 2024b). Donanımsal erişime ihtiyaç duyulmayan ve özel sürücüsü bulunmayan kökkitlerdir. İleri seviyede programlama diline haiz olan yazılımlar içeren bu kökkitler sistem API'lerinden faydalanırlar. Sıklıkla

karşılaşan bir tür olan “Memory Rootkit”, kalıcı sistem depolama cihazına girerek uzun bir süre burada konuşlanmaktadır. Bellek veya RAM bu kökkitlerin içerisine yüklendiği konumlarda hareket etmektedir. Son tür olarak “Bootloader Rootkit” ise sabit sürücülere ait MBR üzerinde yayılarak boot komutuna zarar verir. Böylece bu işlemden sonraki aşamada sistem kontrolünü elinde tutar. Sonuç olarak “full disk encryption” olarak nitelendirilen sistemlere saldıracak konuma gelmektedir (Yıldız, 2022).

Gelişmiş Kalıcı Tehdit Saldırıları (Advanced Persistent Threat-APT)

Gelişmiş kalıcı tehdit saldırıları, yetkisiz ağ erişimlerinin ardından erişim sağlanan ağda uzun süre konuşlanan saldırı türüne denmektedir. Söz konusu saldırılarda özellikle devletlere ait milli savunma sistemleri, merkez bankaları ve kritik altyapılar temel hedefler arasında yer almaktadır. Devletler arası kutuplaşmış yapılar dolayısıyla konvansiyonel ortamda gerçekleşen askeri yardımlaşmalar siber uzayda da kolektif olarak kendisini göstermektedir. Özellikle siber casusluk faaliyetleri kapsamında söz konusu saldırılar ön plana çıkmaktadır (Ping ve diğer., 2014). Bu kapsamda devletlere ait büyük projeler ve askeri istihbarata yönelik gizli bilgiler gelişmiş kalıcı tehdit saldırıları sayesinde ele geçirilebilmektedir (Alioğlu, 2019). Bu saldırı türü diğer saldırı türlerinden farklı şekilde tekrar eden ve karmaşık yöntemlerle yapılmaktadır.

Saldırganın kimliğinin gizlenmesini içeren söz konusu modele sahip saldırıların ilk evresini sisteme sızma aşaması oluşturmaktadır. Bundan sonraki evrede hedefteki ağlar tespit edilerek güvenlik zafiyetleri üzerinden siber saldırı gerçekleştirilmektedir. Gelişmiş kalıcı tehdit saldırısı daha önceden belirlenmiş bir senaryo çerçevesinde düzenlenmektedir. Önemli özelliklerinden bir diğeri de sistem içerisinde öğrenme, türeme ve kritik verileri çalma gibi faaliyetlerle beraber bir ağa bağlı olmadan dahi hedef sistemlerin kontrolünü ele geçirerek hakimiyet kurabilmesidir (Bolat, 2020).

2010 yılında gerçekleştirilen ve ABD ile İsrail tarafından İran’ın nükleer tesislerine yönelik SCADA sisteminin güvenlik zafiyetlerinden faydalanılarak yapılan Stuxnet saldırısı da bu kategoride değerlendirilmektedir. Söz konusu saldırı uzun bir süre kimliğini gizleyen gelişmiş kalıcı tehdit modeli sunmaktadır. Yine 2013’te Çin hükümetinin ABD’ye ait F-35 savaş uçaklarının teknik bilgilerini içeren dokümanları ele geçirmesine yol açan saldırı APT

saldırısı olarak değerlendirilmektedir. Söz konusu saldırılardan korunmak amacıyla hedef konumda bulunan kurumların bilgi güvenliğine ilişkin tedbirleri almaları kritik önem taşımaktadır. Yine sistemlerin risk analizi ve "outside in and inside out" ağ trafiğinin takip edilmesi alınabilecek önlemler arasında yer almaktadır. Virüs engelleme programları bu tip saldırıları önleyebilecek etkiye sahip olmadığından sistemlere sızan siber suçluların dış ortamla iletişiminin kesilmesi gerekmektedir. Bu kapsamda bilinmeyen IP adresleri dikkatle incelenerek isteklere yönelik öncül bir yol haritası belirlenmesi gerekir. APT saldırılarına yönelik güvenlik duvarlarının ve mail adreslerinin kontrolü, ağ erişimi kontrolü (NAC), veri sızıntısı önleme sistemlerinin (DLP) yaygınlaştırılması, virüs engelleme programlarının kullanılması, uygulama güvenliği ve yük dengeleme (WAF), ağ tarama ve takip faaliyetleri ile log sistemlerini içeren siber güvenlik yapılarının inşası diğer önlemler arasındadır. Kritik altyapılara yönelik bu saldırılar tek bir kurum veya kuruluşun savunma tekeline bırakılamayacak kadar önemli olduğundan genellikle siber güvenliğe ilişkin genel bir yöntemi olan ülkelerde Siber Olaylara Müdahale Ekipleri (SOME) vasıtasıyla iş birliği ve koordinasyon sağlanarak söz konusu saldırılara karşı öncül ve ardıl tedbirler alınmaktadır (Tnetworks, 2024).

Küresel çapta etki yaratabilir düzeyde olan ABD'de kurularak ağını genişleten ve dünyanın en gelişmiş siber saldırı gruplarından biri olan Equation Group'un gerçekleştirdiği saldırılar adından söz ettirir hale gelmiştir. Kaspersky Lab tarafından 2015 yılında yapılan açıklamalarda, bu gruba ait kötü amaçlı yazılımların sabit disk ürün yazılımını yeniden programladığı ve on yıldan fazla radarın altına saklanıp özel bilgileri çalabildiği aktarılmıştır. Gelişmiş kalıcı tehdit olarak nitelenen bu grubun destekleyicisi olan devlet veya örgütün mahiyeti bilinmezken Equation Group saldırılarının yapıca karmaşık olması ve araç olarak kullanılan imza türleri dolayısıyla perde arkasındaki gücün NSA'ya ait Tailored Access Operations (TAO) birimi olduğu varsayımını güçlendiren argümanlar bulunmaktadır (ICP, 2022; TechTarget, 2014).

2.2. Ağ ve Sistem Hedefli Siber Saldırılar

Hizmeti Engelleme (DoS) ve Dağıtık Hizmeti Engelleme (DDoS) Saldırısı

Hizmetin engellenmesi saldırısı (Denial of Service-DoS) dağıtık hizmeti engelleme saldırısına (Distributed Denial of Service-DDoS) kıyasla daha sade şekilde gerçekleştirilen, hedef sistem ve bilgisayarlara sızarak bunların hizmet vermelerine engel olan yazılımlardan oluşmaktadır (Cole, 2001) DDoS saldırısı ise tek bir bilgisayar kaynağı yerine birden fazla kaynaktan gelen siber saldırılar şeklinde gerçekleşmektedir (Güngör, 2021). DDoS saldırılarının çalışma metodolojisi hedefteki web sitelerine iletilen ve bu sitelerden cevap bekleyen sahte paketlerle sistemi meşgul etmek üzerine inşa edilmektedir. Birden çok köle bilgisayardan yoğun bir şekilde sunucuya yükleme yapılarak bant genişlikleri daraltılmaktadır. Özellikle saldırıların kaynakları DoS ve DDoS saldırılarında gizlenmekte ve siber saldırganların soruşturulması ve kovuşturulması zorlaşmaktadır. Söz konusu saldırılara karşı bant genişliğinin artırılması ve sunucunun kapasitesinin siber saldırı kapasitesinin üzerine çıkarılması önem arz etmektedir (Karakuzu, 2015).

DoS saldırılarının altı farklı türde yapıldığı söylenebilir. Bunların ilki "Arabellek Aşımı" saldırılarıdır. Bu saldırı web sitesine veri akışı amacıyla programlanan veya planlanandan çok daha fazla sayıda ve arabellek değerinin kapasitesini aşan trafik akışı ile oluşturulmaktadır. Diğer bir saldırı türü olan "SYN Attacks" saldırıları internet ortamında kullanılmayan IP'lerin (Internet Protocol) paket halinde kurban olarak belirlenen cihaza iletilmesiyle oluşmaktadır. Her pakete kaynak tahsis edilirken onay paketleri SYN paket kaynağına gönderilir. Hedefteki cihaz cevap alamadığı IP adreslerine SYN-ACK paket gönderimi işlemini tekrarlar. Bu şekilde devam eden kısır döngü sonrasında hedefteki cihaz daha fazla dayanamayarak bağlantı problemi yaşayacaktır. "Teardrop Attacks" türündeki saldırılarda paket kapsamındaki verilerin kategorize edilmesi aşamasında cihaz üzerinde ekstra yük oluşacağı için sistem bu yüklemeye dayanamamaktadır. "Smurf Attacks" türünde siber suçlular kurban olarak seçtikleri bilgisayardan ağ aracı (ping) talep eder. Sahte şekilde hazırlanan ping paketi saldırılan bilgisayarın IP adresinden gönderilmiş gibi gösterildiği için ağ ortamındaki tüm aracı cihazlar ping yollar. Söz konusu trafik hedef cihaza ağır gelerek bağlantının çökmesine yol açar. Diğer bir tür olan "Servislere Aşırı Yüklenme"de siber suçlular özel portlara çok sayıda İnternet Denetim İleti Protokolü (ICMP) paketi

gönderilerek aynı sonuçlara ulaşılmaya çalışılır. Son tür olarak nitelendirilen "Message Flooding" saldırılarında sistemin mevcut çalışırlığına dokunmadan paketler iletilerek hedef bilgisayar kullanıcılarında söz konusu paketlerin normal olduğu kanısı yaratılır. Bu şekilde siber suçlular saldırdıkları kullanıcının davranışları üzerine etki ederek yönetimi ele geçirmektedir (İTÜBİDB, 2023).

DDoS saldırıları, köle, zombi veya bot olarak adlandırılan "Botnet" bilgisayarlar tarafından sistem ve sunucu üzerinde yavaşlatıcı veya durdurucu etki yaratması hedeflenen siber saldırılardır (BTK, 2022). Siber saldırganlar bu saldırı türünde gerçek kimliklerini gizlemekte ve botnetler vasıtasıyla çok sayıda diğer köle bilgisayara bulaşmaktadır. Söz konusu yöntemle hedef sunucu köle bilgisayarların isteklerine cevap veremeyerek kullanılamaz hale gelmektedir (Jia ve Zhou, 2005). Hedef olarak belirlenen sunucu bilgisayarın IP'sine normal seviyenin üzerinde eş zamanlı olarak iletilen istekler hedef sistemi devre dışı bırakmaktadır. Botnet yazılımlar pasif halde bekletilmek üzere yüklendikleri sistemlerde hazırlık aşaması biterek icrai hareket aşamasına sıra geldiğinde aktifleştirilmektedir. Bununla birlikte kullanıcılar tarafından "ping" bağlantı çıkış isteklerinin görmezden gelinmesi DDoS saldırılarının başarıya ulaşmasında büyük bir etki yaratmaktadır (BTK, 2022).

Söz konusu saldırılar sonucunda saldırıya uğrayan taraflar ekonomik kayıpların yanı sıra itibar yönünden de zayıflamaktadır. Bu saldırılar neticesinde internet bant genişliği olumsuz etkilenerek merkezi işlem birimi (CPU) ve rastgele erişim belleği (RAM) kapasitesi daralmaktadır. Trafik türlerine göre saldırının çeşitliliği değişmektedir. Öyle ki birim tabanlı saldırılar sahte trafik hatları kullanılarak uygulanan yöntemlerdir. Bu yöntemde sn/bit(bps) türünden ölçüm kullanılmaktadır. Diğer taraftan protokol ve ağ katmanı yoluyla yapılan saldırılar, saldırılan ağ altyapısına sayıca çok fazla paketin iletilmesi yoluyla yapılır. Bu saldırı tipinde ise SYN Flood'lar ve Smurf DDoS kullanılmakla beraber iletilen paket PPS türüyle ölçülür. Son yöntem olan uygulama katmanı saldırısında aplikasyonların kötü niyetli isteklerle meşgul olmasına sebep olunmaktadır. Boyutların ölçülmesinde kullanılan birim ise RPS'tir (Fruhlinger, 2024b).

Kullanılan teknik bakımından değerlendirildiğinde IP paketlerinin sahte şekilde oluşturulan paketlerle taklit edildiği ve başlık bilgilerine ilişkin değişiklik yapılarak bu

metodun kullanıldığı görülmektedir. Yani kaynak bilgisi gerçeklikten uzak şekilde karşıya yansıtılmakta veya bu bilgi hiç verilmemektedir (Fruhlinger, 2024b). Farklı bir bilgisayar kullanıcısının IP adresi kaynak gösterilerek saldırıyı gerçekleştiren gerçek suçlular perdeleme yapmaktadır (Sağıroğlu ve Alkan, 2018). Bu metoda "kimlik sahtekarlığı" da denilmektedir. DDoS saldırılarının ana amacı zaten saldırının geldiği gerçek kaynağı gizlemektir. Yine "yansıma yöntemi" olarak kullanılan ve sahte IP oluşturularak saldırının yapıldığı bilgisayardan gönderilmiş gibi görünen paketin dışarıdan üçüncü bir kişice cevaplandığı süsü verilerek dolandırıcılık planlanabilmektedir. Bu durumda hedef bilgisayar siber saldırının ne şekilde ve kimler tarafından yapıldığını bilememektedir. Bir başka yöntem olarak değerlendirilen "amplifikasyon" ise çevrim içi şekilde hizmet veren site veya uygulamaların paket kümelerine yanıt vermesi için yanıltılması ile ortaya çıkmaktadır (Fruhlinger, 2024b)

Bu saldırı yöntemlerine karşı koymanın en iyi yollarından biri bireysel veya kurumsal sitelere gelen HTTP taleplerinin önüne geçilmesidir. Ancak bu şekilde siteye girişler engelleneceği için siber suçlular amaçlarına ulaşamamış olacaktır. Diğer bir yol ise DDoS trafiğinin meşru şekilde var olan trafikten ayrık tutulmasıdır. Bu şekilde saldırının dozajı azaltılarak etki alanı daraltılacaktır. Saldırının geldiği yer veya bölgenin bilinmesi durumunda IP adreslerinin engellenmesi işe yarayacaktır. Yine bu doğrultuda uygulama katmanına yönelik siber saldırıların engellenmesi amacıyla herkesin kullanımına açık olan siteler kapatılmalıdır. Söz konusu durumda çözüm amacıyla kullanılacak ilk yol defansif faaliyetlerde bulunmak iken diğer yol ise altyapının dayanıklılık seviyesinin artırılması olacaktır. Ağ altyapısının güçlendirilmesi ve yüksek miktarda trafiği aynı anda kaldırabilecek kapasitenin sağlanması için içerik dağıtım ağı (CDN) kullanımı desteklenmelidir (Fruhlinger, 2024b) Bu sistem dağıtılmış sunucuların web site içeriğinin dağıtımını içerik sağlayıcıların veya kullanıcıların oldukları bölgeye yakınlaştırarak kullanım hızını artırır. Öyle ki sistemde kopyalanan dosyalar geçici şekilde proxy sunucularında önbelleğe alınarak yakın sunucular vasıtasıyla içeriğe erişim hızlanır (Akamai, 2024)

Kanada'nın Montreal şehrinde "mafiaboy" isimli yazılımsal kod sayesinde henüz reşitlik kazanmamış bir çocuk küresel çapta etkisi olan büyük şirketlere DoS siber saldırılarında bulunarak neredeyse 1 milyar USD ekonomik kayba yol açmıştır (Geers,

2011). Söz konusu saldırı 2001 yılında gerçekleşmiş ve o zamanın teknolojisi için olağanüstü bir olay olarak tarihe geçmiştir (Harrison, 2000). Bu zamana kadar geçen 20 yıllık süreçte söz konusu saldırılar her gün herkesin karşılaşabileceği sıradan siber saldırılar olarak bilinmektedir.

Küresel çapta etki doğuran olaylara bakıldığında ilk akla gelen örnek 2007 yılında meydana gelmiştir. Bu olayda, 1947 yılında dikilen ve Sovyet Rusya döneminden kalma heykelin Estonya'nın Tallinn şehrine nakledilmesi dolayısıyla Rusya devleti Estonya'ya karşı intikam amaçlı siber saldırı gerçekleştirmiştir. Klasik devlet anlayışını bırakan ilk devletlerden olan Estonya kamuya ilişkin hizmetlerde dijital ortama bağlı yapısıyla "e-stonia" ismiyle nitelendirilmiştir. İnternet ortamında gerçekleştirilen kamusal hizmetler dolayısıyla siber saldırıların hedefinde olan Estonya yirmi iki günlük bir siber saldırı atağına maruz kalmıştır. Gerçekleştirilen siber saldırılarda dağıtık hizmeti engelleme yöntemleri uygulanmış ve bu kapsamda kamuoyuna açık olan internet siteleri hedeflenmiştir. Diğer taraftan e-postalar da söz konusu saldırıda bir diğer hedef olarak belirlenmiş ve özellikle online bankacılık ve alan adlarına yönelik kötüye kullanma faaliyetlerinde kullanılmıştır. Bu saldırılar sonucunda devletin kritik sistemleri devre dışı kalmış ve önemli bakanlıklara ait internet siteleri ele geçirilmiştir. Söz konusu siber saldırılarda ping'lerin otomatik olmayan şekilde klasik yöntemlerle başlatılması da dahil olmak üzere köle bilgisayar ağlarının kullanıldığı DDoS saldırılarına sebep olan yönlendirici yazılımdaki güvenlik zafiyetlerinden yararlanan faaliyetler gerçekleştirildiği belirlenmiştir. Rusya'nın enformasyon doktrini kapsamında Estonya'ya karşı gerçekleştirdiği siber saldırılarda bilgi operasyonu ve dezenformasyon metoduyla kamuoyu üzerinde manipülatif eylemler planladığı görülmüştür (NATO CCDCOE, 2007).

2008 yılında Güney Osetya Savaşı sırasında Rusya-Gürcistan arasındaki gerilim konvansiyonel savaşın siber savaşa dönüşmesiyle devam etmiştir. Söz konusu savaşta Rusya tarafından Gürcistan'a yönelik siber saldırılarda SQL güvenlik zafiyetlerinden yararlanılmıştır. Öyle ki bu saldırıda kötü amaçlı MS toplu komut dosyaları dağıtılmış ve hizmet engelleme saldırıları aktif şekilde uygulanmıştır. Web sitesi tahrifatı (defacement) olarak adlandırılan siber saldırılar entegre şekilde mailleri hedef alan spamlar ile birlikte kullanılmıştır. Gürcistan'a ait önemli ve kritik kurumlar ile parlamento, bakanlık ve Abhazya yerel yönetimi de söz konusu saldırıda ana hedefler olarak belirlenmiştir. Diğer taraftan

banka ve finans kuruluşları da bu saldırılardan olumsuz etkilenmiştir. Saldırılarla birlikte haberleşme ve iletişim hatları Rusya'dan geçen Gürcistan'ın birincil iletişim operasyonları devre dışı kalmıştır. Diğer taraftan ortaya çıkan internet kesintileri dolayısıyla Gürcistan'a yardımcı olmaya çalışan devletlere ait acil durum müdahale ekipleri (CERT) teknik yardım sağlamıştır (Buresh, 2021). Söz konusu DoS ve DDoS saldırıları kinetik askeri operasyonlarla birlikte gerçekleştirilen siber saldırıların en önemli örnekleri arasında yer almaktadır (Cyberlaw, 2021b). Söz konusu olay ABD ve diğer Avrupa ülkelerinde çeşitli siber güvenlik önlemlerini beraberinde getirmiş NATO tarafından ise Bükreş Zirvesinde NATO Siber Savunma Yönetimi Otoritesi (Cyber Defence Management Authority-CDMA) ve Estonya'nın Tallinn şehrinde NATO Siber Savunma İş Birliği Mükemmeliyet Merkezinin (Cooperative Cyber Defence Centre of Excellence-CCDCOE) inşa edilmesi kararlaştırılmıştır (Hughes, 2009; NATO CCDCOE, 2023).

2016 yılında gerçekleştirilen Mirai Botnet siber saldırısı DDoS yönteminin kullanıldığı en önemli örnekler arasında yer almaktadır. Söz konusu saldırı IoT cihazlarının tablolar vasıtasıyla taranarak bulaşı sağlanan ve DDoS saldırılarında kullanılan internet sitelerini engellemiştir. Söz konusu internet sitelerinden en ünlüleri OVH ve Brian Krebbs'tir. Bununla beraber Mirai Botnet, bulut tabanlı Amazon, Netflix, PayPal, The New York Times, Twitter ve Verizon'un da dahil olduğu site performanslarını yöneten DNS servis sağlayıcısı Dyn isimli şirketi de olumsuz etkilemiş ve bahse konu internet sitelerine erişim engellenmiştir. Mirai Botnet kötü amaçlı yazılımı, virüsün bulaşı sağladığı cihazlar yeniden başlatıldığında ve varsayılan şifrenin hemen değiştirilmediği durumda çok kısa sürede tekrar bulaşı sağlaması dolayısıyla hedef cihazlar bir süre sonra çalışamaz hale gelmektedir (Mazebolt, 2022).

Son yıllarda oluşan bir istatistiğe göre DDoS saldırılarının kayıt edildiği sistemlere gelen verilere bakıldığında günde yaklaşık 20.000 DDoS türünde siber saldırı yapıldığı ve bu saldırıların muhatap olduğu ülkelerin başında ABD ve Çin'in geldiği tespit edilmiştir (Güven, 2022). Bu şekilde DDoS saldırıları vasıtasıyla devletler üzerinde bir karalama kampanyası oluşturularak halkın yönetime olan güveni azaltılmaya çalışılmaktadır. Söz konusu saldırıların en büyük muhataplarının dünyanın teknoloji devi iki ülke olması ve yine bu iki ülkenin teknoloji konusunda birbirlerine rakip oldukları göz önüne alındığında, ticari

olarak son zamanlarda konjonktürel ambargoların konulması siber ortamda da yine aynı rekabetin sürdüğünün kanıtıdır.

DoS ve DDoS, gerçekleştirilen siber saldırılarda araç olarak kullanılmakla beraber aktivist akımların sanal dünyada karşılık bulması için de uygulanmaktadır. Hizmet engelleme saldırıları devletler arası karşılıklı saldırılarda siber saldırıların temel unsuru olarak ön plana çıkmaktadır. Bu kapsamda dijital altyapılar, dijital sağlayıcılar ve finans kritik altyapılarına yönelik siber saldırılar devletlerin temel varlık ve tesisleri bakımından yıkıcı olabilmektedir. Bununla birlikte internet alan adları ve DNS'e ilişkin siber saldırılar maddi ve manevi kayıplara yol açmaktadır. Siber saldırılara karşı savunmada faaliyet gösteren siber güvenlik ve risk yönetim merkezleri ile kritik altyapılara ait endüstriyel kontrol sistemleri hizmet engelleme saldırıları dolayısıyla devre dışı kalmaktadır (Fruhlinger, 2022a).

DoS ve DDoS ataklarına karşı alınabilecek başlıca önlem somut durumların analizinin yapılarak kaynakların belirlenmesidir. İç veya dış kaynaklı olabilecek olan DoS saldırıları internet bağlanma hızı ve maillerin görüntülenmesinde yaşanan problemlerle gün yüzüne çıkabilmektedir. Yani bu problemler sorunun olduğuna dair birer emare statüsündedir. Söz konusu durumlarda çıkış noktaları dikkat edilmesi elzem olan noktalardır. HTTP Proxy çıkış noktalı sistemlerde taleplerin tek kaynak mı yoksa birden fazla kaynaktan mı geldiği tespiti önem arz etmektedir. Ağ geçidi çıkış noktalarında paketlere ilişkin sistemsel kontrollerin gerçekleştirilmesi bir diğer önemli noktadır (İTÜBİDB, 2023).

Köle Bilgisayar Ağları (Botnet)

Köle bilgisayar ağları diğer bir deyişle botnet İngilizcedeki robot ve ağ kelimelerinin bir araya gelmesinden oluşmaktadır. Kullanıcılar tarafından farkına varılmadan erişim sağlanan sistem ve cihazlar uzaktan kontrol edilerek hedeflenen amaç doğrultusunda kullanılmaktadır (Andress ve Winterfeld, 2011). Söz konusu köle ağlar, yazılımcıların oluşturdukları botlar arasında mantıksal bir bağlantı kurarak tek bir noktadan bu bilgisayarlara gönderilen kötücül yazılımlarda araç olarak kullanılmaktadır (ENİSA, 2023a). Botlar içerdikleri kötücül yazılım kodlarıyla güvenli olmayan bilgisayar ve sistemlerden bir ağ yapısı meydana getirmektedir (Andress ve Winterfeld, 2011). Söz konusu ağ yapısı içerisinde yer alan kötücül kodlar bilgisayar, cep telefonu, tablet, internete bağlı olan

uygulama ve sistemlere zarar vermektedir (Mazebolt, 2022). Robotlar uzaktan kumanda ve kontrol mekanizması (Command and Control Mechanism-C&C)) vasıtasıyla zombi bilgisayarlar olarak görünüm kazanmaktadır. Siber saldırganlarca güvenlik zafiyeti olan bilgisayar ve sistemler taranarak muhtemel hedefler tespit edilmektedir. Yapılan tespit sonrası hedeflere yönelik icrai hareketler gerçekleştirilmekte ve saldırıya geçilmektedir. Söz konusu saldırılarda kullanılan hizmet engelleme, trafik izleme, istenmeyen e-posta, kötücül yazılım gibi çeşitli yöntemler saldırının etki alanı nüfuzunu artırmaktadır (Samet, 2018).

Diğer taraftan kötücül yazılımlar arasında yer alan virüs ve solucan saldırıları köle bilgisayar ağları ile birlikte kullanılarak botların hedeflere ait işletim sistemleri üzerinde hakimiyet kurması sağlanmaktadır. Bu vasıtayla botlar tarafından bilgisayar ve sistemlerde kayıtlı dosyalar ele geçirilerek hedeflenen zararlı faaliyetler gerçekleştirilebilmektedir (ENİSA, 2023a). Söz konusu zararlı faaliyetler kullanıcıların rızası dışında bilgi ve verilerini ele geçirme, ifşalama, silme veya yok etme, hizmetin reddi, dolandırıcılık ve diğer suça sebebiyet veren hareketlerin nitelikli halleri şeklinde sıralanabilecektir (Mazebolt, 2022). Kullanıcılara ait cihazların ve sistemlerin tabir yerindeyse mutasyona uğratılarak köle bilgisayar veya zombi makine haline getirilmesi ile siber saldırılar, kritik altyapıların tahribatından vatandaşların maddi ve manevi hak kayıplarına kadar büyük ölçekli zararlar ile sonuçlanabilmektedir (Bolat, 2020). Açık kaynak yazılımlı sistemlere kötücül yazılımlar aracılığıyla sızılması ile uzaktan kontrol edilerek tek merkezden yönetilmektedir (Blank, 2008). Köle bilgisayarlar dağıtık sistemler olmalarının avantajı ile mali kazanç, yoğunlaştırılmış siber saldırı, DDoS atakları, oltalama, istenmeyen e-posta, yasa dışı yazılım dağıtımı, veri ihlalleri, kimlik avı hırsızlığı gibi suç amaçlı faaliyetlere de açık kapı bırakmaktadır. Yerel ağlar üzerinde etkili olan bu saldırılar çok katmanlı yönlendirme ve kontrol merkezlerinden meydana gelmesi dolayısıyla uzak bölgelerdeki bilgisayar ve sistemler ile farklı dildeki cihazlar üzerinde etki doğurabilmektedir. Bununla birlikte sistemlere sızan botnetler yönlendirme ve kontrol merkezi vasıtasıyla kendi kendine revize ve yönetim fonksiyonunu yerine getirebilmektedir (Kara ve Şişeci, 2011). Diğer taraftan kötücül yazılımlarla suç amaçlı kullanılan köle ağlar faydalı şekilde de kullanılabilmektedir. Örneğin İnternet Aktarmalı Sohbet (IRC) olarak nitelenen sistem faydalı bir köle bilgisayar ağıdır. Yine tarayıcı üzerinde internet sitelerinin dizinlere eklenmesi amacıyla kullanılan

“Google Spider” ve “GoogleBot” programları da faydalı bot örneklerindendir (Güngör, 2021).

Çatal Bomba (Fork Bomb)

Çatal bomba ya da diğer bir deyişle tavşanlar Unix ve Linux işletim sistemlerinde kullanılan ve işlem çoğaltma kabiliyetine sahip ögeleri alt öğelere ayrıştıran sistemsel çağrılar olarak nitelendirilmektedir. Bu saldırı tipi için çatal ve tavşan terimleri çoğalma ve dallandırma yeteneği dolayısıyla kullanılmaktadır (Imperva, 2023a). Söz konusu siber saldırı türü ilk olarak 1974’te üretilen Fork yazılımı olarak görünüm kazanmıştır (Infocarnivore, 2010).

Çalışma metodolojisine bakıldığında sistem kaynaklarının art arda aldıkları “fork bomb” çağrısı sonrası aşırı yüklenme dolayısıyla yeni komutlara karşı duyarsız kalması söz konusu olmaktadır. Bu kapsamda çatal bombalar DDoS saldırıları mantığında hareket etmektedir (Imperva, 2023a). Çatal bomba saldırısının temel özelliği olan hızlı şekilde türeme ve koloni oluşturma fonksiyonları dolayısıyla hedefteki sistemler yavaşlamakta veya işlevsiz hale gelmektedir (BTK, 2022). Saldırı çerçevesinde ortaya çıkan çatal etkisi sayesinde sistemlere ve bilgisayarlara ait çekirdekler ile bellekler sömürüldüğü için sisteme ilişkin optimal azami sınıra ulaşılmadan sistem kaynakları kullanılamaz duruma gelmektedir. Bu süreç sonunda oluşan duruma ise çekirdek paniği (kernel panic) ismi verilmektedir. Söz konusu süreç ve sürekli olarak gerçekleşen döngü sonucunda veri kayıpları ortaya çıkmaktadır (Imperva, 2023a).

Diğer taraftan çatal bombaya dair yazılımsal kodların basit ve sade yapıları dolayısıyla siber saldırganlara büyük bir kolaylık sağladığı değerlendirilmektedir. Hatalı oluşturulan kod kümeleri genellikle istem dışı tavşan yazılım şeklinde ortaya çıkabilmektedir. Kodlanarak oluşturulan söz konusu yazılımlar dolayısıyla kopya sayısı çok yüksek miktarlara ulaşabilmektedir (Kaspersky, 2023a). Siber saldırganlarca üretilen tavşan yazılımlar özellikle DoS ve DDoS saldırılarında yardımcı olacak şekilde kullanılarak hizmet engellemeleri yapılabilmektedir (Güngör, 2021).

Sıfırıncı Gün/İlk Gün Açıklığı Saldırıları (Zero-Day Exploit)

Sıfırıncı gün saldırıları, yazılım geliştiricileri ya da üreticilerinin güvenlik zafiyetleri kaynaklı problemleri tespit edip çözemeyecekleri süreler içerisinde bilgisayar korsanları tarafından söz konusu açıklıklardan faydalanılarak gerçekleştirilen siber saldırılardır (Kaspersky, 2023b). İlk gün açıklığı da denilen bu saldırı, programları üreten ve geliştiren yazılımcılar ile ilgili pazarda satan kişi veya şirketlerin söz konusu yazılım ve ürün piyasaya sürülmeden önce farkına varılamayan güvenlik zafiyetlerini içermektedir (Walker, 2014). Bu saldırı türü, programların piyasaya sürülmesinin ardından satıcı ve geliştiricilerin bilgisayar korsanlarınca ortaya çıkarılan güvenlik zafiyetinin kamuoyuyla paylaşılması ile eş zamanlı olarak öğrenmelerini ve bu sorunu çözmek için gerekli zamana sahip olmamaları şeklinde özetlenebilecektir. Geliştiriciler güvenlik açığını fark ettikleri anda düzeltme fonksiyonlu yamalar yaparak ortaya çıkan sorunlara yönelik çözüm bulmaya çalışmaktadır. Söz konusu yama çalışması ise saldırganların hedefledikleri başarıya ulaşma olasılığını yükseltmektedir. Yazılımcılar, satıcılar veya üreticiler tarafından saldırıya vücut veren güvenlik zafiyetlerinin tespit edilmesi durumunda ise siber saldırganlarca yararlanma kodu (exploit code) yazılarak siber saldırı faaliyetleri gerçekleştirilmektedir (Zer0-Day, 2024). Bu saldırılarla beraber en sık kullanılan saldırı yöntemleri arasında kimlik hırsızlığı ve sahte oluşturulan spamlar bulunmaktadır. Söz konusu saldırılar neticesinde saldırganlar tarafından elde edilen bilgiler karanlık ağ (dark web) olarak nitelendirilen ve kimliklerin gizlenerek özel tarayıcıların kullanıldığı platformlar üzerinden satışa çıkarılmaktadır. Satış amaçları arasında mali kazanç elde edilmesi, siyasi veya sosyal mesajların iletimi, itibar kayıplarına yol açma, terörist faaliyetler ve devletler arası savaşlarda siber silahların kullanımı gibi hususlar ön plana çıkmaktadır

Son on yılda sıfırıncı gün saldırıları popülerlik kazanarak büyük bir artış göstermiştir. 2011'de Nevada Creech Hava Kuvvetleri Üssü'nde meydana gelen olayda Predator ve Reaper insansız hava araçlarına yönelik bir sıfırıncı gün açığı saldırısı gerçekleştirilmiştir. Bu saldırıda droneların kokpitlerine ve yer birimlerine yerleşmiş virüsler üssün yetkilileri tarafından saklanmıştır. Söz konusu hava sahası üssündeki ağ uzmanları bu virüsü Danger Room'dan okuyarak öğrenmişlerdir. Sıfırıncı gün saldırısı ile keylogger saldırılarının entegre edilmiş hali olarak görünen virüs; insansız hava araçlarının Afganistan, Pakistan,

Yemen gibi savaş bölgelerindeki görevleri esnasında uzaktan bu araçları yöneten pilotların tuş vuruşlarını kayıt altına almıştır (Wired, 2011).

Yine söz konusu saldırılarda bilgisayar kod satırları yazılım ve programlarını oluşturan küçük parçalar (Lines of Computer Code-LOC) saldırı kodlarını içeren satırlarda olasılık olarak 1/1000 oranında sıfırıncı gün güvenlik zafiyetine sebep verebilecek 20'ye kadar hatalı kod satırı (bug) ortaya çıkarabilmektedir (Goodman, 2015). Söz konusu açıklıklardan faydalanan siber saldırganlar saldırıların etkisini artırarak büyük zafiyetler ortaya çıkarmaktadır (Ablon ve Bogart, 2017). Buna örnek olarak 2017 yılı Nisan ayında meydana gelen olayda Shadow Brokers isimli bilgisayar korsanlığı çetesi Windows işletim sistemi üzerinde bir güvenlik zafiyeti tespit etmiş ve sıfırıncı gün saldırısında bulunarak NSA'ya ait kritik belgeleri ele geçirmiştir (Danfeng, 2018).

Fransa menşeili Vupen isimli şirketin iştiraki Zerodium, 2019 Eylül ayında iPhone cihazları hedef alan tek tıkla İOS sıfırıncı gün istismarı için güvenlik açığına yönelik ödül olarak 1 milyon USD ödeyeceğini bildirmiştir. Söz konusu saldırı bubi tuzağı mantığında girilen sitelerde Iphone cihazları doğrudan ağına düşürmektedir. Yine aynı şirket tarafından yayınlanan haberde sıfır tıklamalı bütünsel zincirle android cihazları etkileyen yazılıma ilişkin ödül olarak ise 2.5 milyon USD belirlendiği belirtilmiştir. Aynı saldırı türüyle İOS özellikli cihazlarda güvenlik açığından faydalanılması durumunda ise ödül 2 milyon USD olarak belirlenmiştir. Yine söz konusu şirket tarafından Whatsapp ve iMessage için belirlenen sıfırıncı gün güvenlik açığı faydalanma ödül miktarı ise 1.5 milyon USD olarak güncellenmiştir (Forbes, 2019). Vupen CEO'su tarafından yapılan açıklamada erişim kısıtının kaldırıldığı sistemlerle (jailbreak) ilgili açıklıklar için Iphone'da 2 milyon USD, android için 2.5 milyon USD ödül koyulmuştur (Perlroth, 2021). Yine 2021 yılında Google Chrome hedef alınarak yapılan sıfırıncı gün açığı saldırısında web tarayıcısındaki "V8 Javascript motoru hatası" nedeniyle güvenlik zafiyeti oluşmuştur. Bu saldırı sonucunda Chrome güvenlik açıklıklarına karşı güncellemeler getirmiştir (Kaspersky, 2024b).

Ortadaki Adam Saldırısı (Man-İn-The-Middle)

Ortadaki adam saldırısı tarafların güvenli iletişim kurması esnasında saldırganların söz konusu iletişime dahil olması ve hedeflenen mesajların iletilmesidir. Siber saldırganlar

bahse konu saldırılarla birlikte mesajları takip etmekte ve bu mesajları yapısal değişikliğe uğratmaktadır (ENİSA, 2023b). CISCO, ortadaki adam saldırısına ilişkin tanımda "*iki taraf arasındaki bağlantıya yetkisiz müdahale veya kulak misafiri olmak*" şeklinde bir nitelemede bulunulmuştur (CİSCO, 2023). Söz konusu saldırı ile amaçlanan husus yetkisiz satın alma işlemleri, kimlik hırsızlığı ve bilgisayar korsanlığı için öncül bir saldırı yaratmaktır. Bununla birlikte iletişimin taraflarının kurduğu hattın gizlice dinlenmesi ile birlikte web sitesi dolandırıcılığı saldırısı gerçekleştirilebilmekte ve kimlik sahteciliği yöntemiyle siber saldırının seyri değiştirilebilmektedir (Strongdm, 2023).

Söz konusu saldırılarda kullanılan metotlara bakıldığında, uç noktaların bulunduğu alanlardaki trafik yakalama ya da verilerin gözetim altında tutulduğu istasyonlardan geçip tekrar yönlendirme yapma işlemlerinin kullanıldığı görülmektedir. Uç nokta trafiğine yönelik işlemde tarafların iletişimde olduğu aygıtlara kötücül yazılımların yüklenmesi ya da kablolu ve kablosuz ağların dinlenmesi ile saldırı gerçekleştirilmektedir. Tekrar yönlendirme işlemi değişik seviyelerde oluşabilmekte ve yerel ağlar üzerinde IPv4 ARP sahteciliği, IPv6 yönlendirici reklamları ya da otomatik proxy tespiti gibi kötü amaçlı faaliyetlerde bulunulabilmektedir. DNS'e yönelik sahtecilik faaliyetleri ana bilgisayar adlarını sahte sunuculara yönlendirmek amacıyla kullanılmaktadır. İnternet üzerinden yapılan küresel çaplı veri yönlendirme saldırıları çoğunlukla Sınır Ağ Geçidi Protokolünün (BGP) yanlış şekilde yönlendirilmesi ile gerçekleştirilmektedir (ENİSA, 2024a). Bu protokol, yönlendirme yetkisi olan bir bilgisayar elemanıdır. Trafiğin kötücül şekilde yönlendirilmesi ve yasa dışı dinlemeler söz konusu protokol ile mümkün olmaktadır. Siber saldırganlar bu yöntemi kullanarak kişisel verilere, hesap bilgilerine ve daha birçok hassas veriye ulaşabilmektedir (Bishopfox, 2015).

Ortadaki adam tekniği kötücül saldırılar için bir araç olarak kullanılabildiği gibi yeri geldiğinde yararlı durumlar için de söz konusu olabilmektedir. Bilgilerin şifresiz şekilde incelenmeden bağlam dışına çıkışını engelleyen veri kaybı önleme (DLP) sistemleri buna örnek verilebilir. Söz konusu durumlarda iletişim hattındaki taraflar yasal koşullar hakkında açık şekilde süreç hakkında aydınlatılmaktadır (ENİSA, 2024a) Ortadaki adam metotları genel olarak sınıflandırılacak olursa sahtecilik yapılan IP, DNS ve HTTPS saldırı yöntemleri ile birlikte wifi dinleme, mail hesabını ele geçirme, SSL ve oturumun ele geçirilmesi şeklinde sıralanabilir (Strongdm, 2024).

IP sahtekarlığında (IP Spoofing) kullanıcıların güvenilir kaynağa bilgi verdiği izlenimi yaratılmaktadır. Bu sahtekarlık türünde internet yoluyla bağımsız bilgi paketleri iletimin ardından alıcılarda toplanmaktadır. Söz konusu paketler iki makine arasındaki alışveriş esnasında bu makinelerin IP adreslerine ait verileri barındırmaktadır. Bu alışveriş esnasında kaynak makineye ait IP çeşitli sızdırma araçlarıyla değiştirilerek sahte şekilde karşıya sunulmaktadır. Kör ve kör olmayan şeklinde sınıflandırılan IP Spoofing saldırılarında kör olan durumda karşı tarafa birkaç paket iletilir. Fiili gerçekleştiren kişiler yerel ağ yapısının dışında konumlanmaktadır. Kör olmayan ikinci türde ise hedef ve kaynak aynı alt ağda konumlanır. Paket sırası dizin bilgisi vasıtasıyla tespit edilir. Tespit sonrası güvenli olarak nitelenen makine bilgileri sahte şekilde sunularak kimlik doğrulama sistemi etkisiz hale getirilir (Timus, 2024). DNS sahtekarlığında spam göndericilerle sahte web siteleri üretilerek bu siteye yönlendirme yapılmaktadır. HTPPS sahtekarlığında ise güvenilirliği olmayan HTTP uzantılı internet sitelerine yönlendirme yapılarak siber saldırganların kullanıcı hareketlerini izlemesi sağlanır. Wifi dinleme (wifi eavesdropping), halka açık mekanlarda yaratılan sahte erişim noktaları vasıtasıyla izleme yapılan bir saldırı yöntemidir. SSL ele geçirme durumunda ise sunucularla HTPPS bağlantıları arasında dolaşan hassas verilerin hakimiyet altına alınması faaliyeti bulunmaktadır. Tarayıcı tanımlama bilgisi çalma olarak addedilen oturumu ele geçirme faaliyetleri, tarayıcılarda saklanan kaydedilmiş parolaları ele geçirmektedir. Bununla birlikte e-posta korsanlığı ve tarayıcıdaki adam (man in the browser) gibi ortadaki adam saldırı yöntemleri de bulunmaktadır (Secret Double Octopus, 2024).

2016 yılında Alibaba Group şirketine yönelik brute force saldırısında 100 milyona yakın kişinin bilgilerini içeren önceden ele geçirilmiş bir veri tabanı kullanılarak hedef hesapların %20'sine erişim sağlanmıştır. Söz konusu saldırıda daha önceden kullanılan parolalardan yola çıkılarak deneme yanılma yöntemini içeren sayısız varyasyon kullanılmıştır (Strongdm, 2024). Yine "CookieMonster Attack" olarak nitelenen ve yalnızca şifreli oturumlar kısmının doğru olarak ayarlanmadığı durumlarda iletişimin taraflarından farklı olarak araya giren parazit tarafın HTTPS çerez verilerini ele geçirdiği ortadaki adam saldırılarıdır. Bu saldırılardan küresel çaplı şirketlerin de etkilendiği belirtilerek özellikle Google hizmetleri, havayolu şirketleri ve bankalar gibi kritik sistemlerde başarıya ulaşıldığı ifade edilmiştir (Goodin, 2008).

17 Haziran 2011'de meydana gelen ve Hollanda menşeli sertifika sağlayıcı DigiNotar olayında söz konusu şirketin sertifika yetkilisi altyapılarına rıza dışı erişim saptanmıştır. Comodohacker isimli İranlı hackerın yaptığı iddia edilen saldırıda DigiNotar'ın harici Demilitarized Zone'daki sunucularına sızılarak söz konusu sunucular dosya alışverişi faaliyetlerinde kullanılmıştır. Saldırganın söz konusu saldırıyı yapma amacının 1995 yılı Srebrenica Soykırımını önleyemeyen Hollanda'ya karşı intikam alma güdüsü olduğu ifade edilmiştir. Saldırıyı gerçekleştiren hacker bütün günlük dosyaları silebildiği için sahte şekilde oluşturulan sertifika miktarı hesaplanamamıştır. Bu saldırılar sonucunda itibar yönünden olumsuz etkilenen şirket iflas ederek ticaret sicilinden silinmek zorunda bırakılmıştır (Cyberlaw, 2021a).

Yapılandırılmış Sorgu Dili Saldırısı (SQL Injection)

90'lı yıllardan beri gündemde olan yapılandırılmış sorgu dili (SQL Injection) saldırısı siber saldırganlar tarafından veri tabanlarındaki bilgileri çalması ve değiştirmesi amacıyla sorgulama dili içeren kodların kullanıldığı saldırı türüdür. Bu saldırı türünün gerçekleştirilmesi neticesinde çok fazla taleple sistemin kilitlenmesi, güvensiz sitelere yönlendirici reklamlar, pop-up şeklinde beliren mesajlar ile karşılaşılmaktadır. Yine bahse konu siber saldırılar aracılığıyla bilgi ve veriler açığa çıkarılabilmekte, bilgi güvenliği unsurlarına zarar verilebilmekte, kullanıcıların gizliliği tehlikeye sokulabilmekte ve saldırganlarca hedef sistemlere ait kontrol ve komuta yetkisine dair erişim sağlanabilmektedir (Kaspersky, 2023c). Diğer taraftan yanal hareket etkisi ile saldırganlarca veri tabanı sunucularına erişim sağlanması akabinde yetkili duruma getirilen kişiler izin yetkisi ile diğer sistemlere de erişim sağlayabilmektedir. Yapılandırılmış sorgu dili kodları yetki arıtımı ile yönetici yetkilerine, erişim ve kimlik doğrulama gibi hedeflere ulaşabilmektedir (Bright, 2022).

SQL enjeksiyon türlerine bakıldığında üç sınıfta incelemeye tabi tutulabilir. Bu sınıflandırma arka uç verilerine erişim ve zarar görme potansiyellerine göre kategorize edilmektedir. İlk tür olarak ifade edilen "Bant içi SQL" klasik olarak nitelendirilen enjeksiyon türüdür. Saldırı başlangıç ve bitişleri ortak iletişim aracı olarak kullanılmaktadır. Alt türlerinde ise "Hata tabanlı SQL" ve "Union tabanlı SQL" bulunmakla birlikte hata

tabanlı türde saldırgan tarafından üretilen hata iletileri aracılığıyla bilgi toplanmaya çalışılır. Union tabanlı türde ise tek HTTP yanıtı için veri tabanı üzerinden meydana getirilen Union türünden yararlanmaktadır. İkinci kategoride "Çıkarımsal SQL" olarak nitelendirilen ve sunucu üzerine yüklenen veriler aracılığıyla sunucu davranışlarının takip edildiği SQL türü bulunmaktadır. Söz konusu yönteme "Kör SQL" de denilmesinin sebebi verilerin internet sitesinin veri tabanlarından siber suçlulara iletilmemesidir. Bu şekilde anonimleşen yapıda bant içi saldırılar gözlemlenememektedir. Yürütmeye ilişkin hızları yavaş olan kör SQL'ler "Boolean SQL" ve "Zamana Dayalı SQL" olarak alt kategoriye ayrılabilir. Boolean SQL, veri tabanlarına iletilen SQL sorgusu ile bu sorguya bağlı olarak değişecek sonuca göre HTTP yanıtına dair bilgilerin değişime uğrayıp uğramayacağı belirtmektedir. Zamana dayalı olan türde ise veri tabanlarına iletilen SQL sorgusu saniye bazında beklemeye sebep olur. Bu süre esnasında sorgunun doğruluğu gözlemlenir. HTTP yanıtı bu süreç sonunda oluşturularak veri tabanındaki verilere bakılmadan iletinin doğruluğu tespit edilebilir. Son kategori olan "Bant dışı SQL" sadece web uygulamasında kullanılan veri tabanı sunucularındaki başlıca niteliklerin aktif hale getirilmesiyle uygulanabilmektedir. Diğer SQL yöntemlerinin alternatifi konumunda olan bu tür, bant içi SQL'in aksine saldırı başlangıç ve bitişindeki bilgileri toplamak amaçlı ortak kanalı kullanamamakta ya da sunucuların yavaş kalması halinde kullanılmaktadır (Imperva, 2024b).

SQL enjeksiyon saldırı örneklerine bakıldığında 2018 yılında meydana gelen "Cisco" ve 2019 yılında yaşanan "Fortnite" siber saldırıları ön plana çıkmaktadır. Cisco Prime License Manager sistemlerinde SQL enjeksiyon zafiyeti tespit edilerek ayrıcalıklı erişim konumunu hedef alan saldırganlar lisans yöneticilerinin hesaplarını ele geçirmiştir. Diğer taraftan Fortnite isimli online oyun dünya çapında ünlenerek yaklaşık 350 milyon kullanıcıya kapılarını açmıştır. Buradaki kaynağı fark eden saldırganlar SQL enjeksiyon zafiyeti tespit ederek kullanıcı hesaplarına erişim sağlamıştır (Kaspersky, 2024a).

Web Sitesi Tahrifatı (Defacement)

Web sitesi tahrifatı saldırıları kapsamında siber saldırganlar, internet sitelerindeki içerikleri hedefledikleri içeriklerle değiştirmektedir. Bu tahrifat çoğunlukla siyasi ya da dini bir mesajın iletilmesi, gizli ve hassaslık içeren görüntülerin ifşa edilmesi veya bazı bilgisayar korsanlarınca siber saldırıya uğranıldığına dair bildirim ile iletilmektedir. İnternet siteleri ve

web uygulamalarının içeriğindeki dosyalar üzerinde değişiklik yapılmasına güvenlik açıklığı bulunan durumlarda rastlanmaktadır. Diğer taraftan yetkisiz erişim, SQL enjeksiyonu, siteler arası komut dosyası çalıştırma (XSS), DNS ele geçirme ve kötü amaçlı yazılımlar web sitesi tahrifatlarının en önemli sebepleri olarak sıralanabilmektedir. Web sitesi tahrifatı neticesinde kurum ve şirketlerde mali zararlar, marka itibar kaybı, hizmet kesintileri ile manevi zararlar oluşabilmektedir. Bahse konu tahrifata karşı mücadelede güçlü kullanıcı kimlik doğrulaması, filtrelemeli güvenlik duvarları, izinsiz giriş ve saldırı tespit sistemleri (IDS), veri yedekleme, gelişmiş güvenlik protokolleri, güncel yazılımlar, hiper metin işaretleme dili girişlerinin temizlenmesi ve bot yönetimi önemli bir yer tutmaktadır (Ramotion, 2023).

Buna ilişkin örneklere bakıldığında 2018'de Birleşik Krallık'ta gerçekleşen web sitesi tahrifatı saldırısı öne çıkmaktadır. Ulusal Sağlık Servisi'nin (NHS) internet sayfasının bilgisayar korsanlarınca tahrifata uğratılması neticesinde sağlık kuruluşunda tedavi gören hastaların verileri çalınmıştır. Söz konusu internet sayfasında "AnoaGhost Tarafından Hacklendi" iletili mesaj birkaç saat sitede yayımlanmıştır. Söz konusu saldırının son yıllarda artan sağlık kritik altyapılarına ilişkin fidye yazılımı ve veri ihlali siber saldırılarına eklenmesi söz konusu alandaki siber güvenlik önlemlerinin artırılması ihtiyacını doğurmuştur (Imperva, 2023c).

Bununla birlikte 2019 yılında Gürcistan'a yönelik yapılan web sitesi tahrifatı olayında yaklaşık 15.000 internet sitesinin olumsuz etkilendiği ve çevrim dışı kaldığı ifade edilmiştir. Bu internet siteleri bağlı şekilde devlete ait kritik altyapıları da olumsuz etkilemiş ve saldırının niteliği bireysel zararlardan tüm kamuyu etkileyebilecek kapsamlı bir saldırıya dönüşmüştür. Öyle ki söz konusu siber saldırı sonucunda kamu hizmeti sunan internet siteleri, mali kuruluşlara ait internet siteleri ve ülke çapında yayın yapan kanalların internet siteleri zarar görmüştür (Imperva, 2023c).

Veri Sızıntısı/İhlâli Saldırıları (Data Breach Attack)

Veri ihlâli saldırıları, kişilere veya kurum ve kuruluşlara ait verilerin yetkisiz şekilde üçüncü taraflarla paylaşımı veya söz konusu verilere kötücül amaçlarla erişim sağlanması olarak nitelenmektedir. Bahse konu erişim irade dışı olabileceği gibi sistemlerdeki güvenlik açıklıklarından da kaynaklanabilmektedir (ASD, 2023). Veri sızıntısı yoluyla ele geçirilen

veriler üzerinde tahribat, tahrifat, ifşa, yayımlanma, karanlık ağ üzerinde satış ve diğer suçlarda araç olarak kullanma maksadıyla faaliyetlerde bulunulmaktadır. Söz konusu tehdit unsuru kritik altyapılara yönelik endüstriyel kontrol sistemleri ve kamu hizmetlerini hedefleyerek bireylerin devlete bağlılığını ve inancını zayıflatmaktadır. Bu kapsamda siyasi, sosyal, toplumsal ve ekonomik kriz durumları ortaya çıkabilmektedir (Fowler, 2016).

Veri ihlali saldırısı birbirine zincirleme şekilde bağlı olan üç aşamada meydana gelmektedir. Söz konusu aşamaların ilkini ön araştırma, ikincisini icrai hareket olan saldırı aşaması ve sonuncusunu ise ele geçirilen verilerin tehlike altında bulunduğunun mağdur konumdaki tarafa iletilmesi oluşturmaktadır. Birinci aşamada hedef olarak belirlenecek kişi ya da grup tespit edilerek güvenlik açıklıkları ortaya çıkarılmaktadır. Söz konusu güvenlik zafiyetlerini içeren ve hedeflenen ağa erişmek için olanak sağlayan kötücül yazılımlar karanlık ağda satışa sunulmaktadır. İkinci aşamada icrai olarak siber saldırı gerçekleştirilmekte ve son aşama öncesinde hareket tamamlanmaktadır. Kötücül yazılımlarla birlikte kimlik hırsızlığı, fidye yazılımları, sosyal mühendislik, SQL enjeksiyonu gibi siber saldırı yöntemleri kullanılmaktadır. IBM 2022 Veri İhlali Maliyet Raporunda yer verilen istatistiklerde veri ihlalleri saldırılarının %19'unu kimlik hırsızlığı saldırıları oluşturmaktadır (IBM, 2022a). Söz konusu saldırılarla beraber verilerin karanlık ağda satın alınması, fiziksel şiddetle birlikte gasp fiili ve sosyal mühendislik saldırıları aktif şekilde kullanılmaktadır. Bununla birlikte sosyal mühendislik saldırısına benzer olarak geliştirilen kimlik avı saldırıları bahse konu veri ihlallerinin %16'lık payını oluşturmaktadır. Kimlik avı ile birlikte sahte şekilde oluşturulan e-posta hesaplarından iletilen ek ve bağlantılar, kısa mesaj iletileri ve sosyal medya etkin şekilde uygulanmaktadır. Diğer taraftan kullanılan yöntemlerden biri olan fidye yazılımı ihlallerinin ortaya çıkarılması için 326 günlük bir sürenin geçtiği söz konusu raporda aktarılmıştır. Veri ihlaline ilişkin ortalama maliyet ise yine bu raporda 4.54 milyon USD olarak ifade edilmiştir. Bu miktarın kapsamına saldırganlarca talep edilen fidye miktarı dahil edilmemektedir. Bu miktarın da maliyet hesabında göz önünde bulundurulması durumunda siber saldırı maliyeti yükselmektedir. Söz konusu IBM raporunda "bulutta yanlış yapılandırma (cloud misconfiguration served)" hataları ise veri ihlallerinin %45'ini meydana getirmektedir (IBM, 2023). Bu saldırı kapsamında risk altındaki grupları küçük veya orta büyüklükteki şirketler, kurum ve kuruluşlar ile bireyler oluşturmaktadır (ASD, 2023).

Söz konusu veri ihlalleri içerisine sosyal güvenlik numaralarını, bankalara ait kişisel bilgileri, kişilerin hassas verilerini, fikri ve sınai mülkiyete ilişkin bilgileri ve sağlıkla ilgili bilgileri içermektedir. IBM tarafından yayımlanan veri ihlali maliyet raporlarına göre, 2022 yılında şirketlere veri ihlallerinin maliyeti yaklaşık 4.35 milyon USD tutmuştur. Kuruluşlarun %83'ü ise yıl içerisinde birden fazla sayıda veri ihlali yaşadıklarını bildirmişlerdir. Yine sağlık alanında yaşanan veri ihlalleri istatistiğine göre bunun maliyeti devletlere 10.10 milyon USD tutmaktadır. Söz konusu alandaki veri ihlali maliyeti tüm alanlara oranlandığında 2 kat fazla ihlal yaşandığı belirtilmektedir. Bu da siber saldırganların özellikle hastaların kişisel bilgilerini, hastanelerin ve sağlık kuruluşlarının güvenlik zafiyetlerinden yararlanarak sistem üzerinden ele geçirdiği anlamına gelmektedir. Bu raporda yayımlanan verilere göre veri ihlalleri sonucunda oluşan ve müşteri kitlesinin hesaba katılması sonrası ekonomik kayıp mağdurlara yaklaşık 1.42 milyon USD'ye mâl olmuştur. Söz konusu ihlallerin ortaya çıkarılması ve kontrol altında tutulması için harcanan para ise ortalama 1.44 milyon USD gerektirmektedir (IBM, 2024).

2017 yılında hackerlar tarafından kredi raporlama kuruluşu olan Equifax isimli şirket hedef alınarak veri ihlali saldırısı yapılmıştır. Bu saldırıda 143 milyonu aşkın ABD vatandaşının kişisel verilerinin ele geçirildiği ifade edilmiştir. Söz konusu saldırıda hackerlar, şirketin internet sitesinde yama yapılmamış bir zafiyetten faydalanarak sosyal güvenlik numaraları ve banka hesap bilgilerini de içeren birtakım bilgilere erişmek için yanal şekilde başka sunuculara geçmiştir. Söz konusu saldırının maliyeti toplamda 1.4 milyar USD'ye mâl olmuştur (IBM, 2024).

2022 yılında meydana gelen en çarpıcı örneklerden biri de Crypto.com veri ihlali saldırısıdır. 17 Ocak'ta gerçekleşen saldırıda 500 kişiye yakın kullanıcının kripto para cüzdanları ele geçirilmek istenmiştir. Yaklaşık olarak, Bitcoin hesaplarından 18 milyon USD, Ethereum hesaplarından 15 milyon USD ve diğer farklı miktarlarda elektronik para türlerinden yüksek meblağlar çalınmıştır. Saldırıların sebebi olarak 2FA sisteminin atlanarak hesap sahiplerinin bloke olması olarak gösterilmiştir. Saldırı sonrası yetkililer sistemler üzerinde denetim sağlandığı ve gerekli iyileştirmelerin yapıldığını ifade etmiştir. Söz konusu saldırı göstermiştir ki hem parola yöneticiliği hem de kritik verilerin şifrelenmesi büyük önem arz etmektedir (ERMProtect, 2022).

2022 Veri İhlali Maliyet Raporunda yer verilen veri ihlallerinin önlenmesi ve hafifletilmesi ile ilgili kısımda istikrarlı şekilde yapılan güvenlik zafiyetlerine ilişkin araştırma ve geliştirme çalışmaları, planlı olarak yapılan yedekleme uygulamaları, verilerin şifrelenmesi, veri tabanına yönelik iyileştirme ve düzeltmeler, yazılım ve donanım programlarının virüslere karşı korunması gibi tedbirler veri ihlallerinin önüne geçilmesi açısından kritiktir. Raporda bahsi geçen olay müdahale ekiplerine (Organization's Incident Response-IRP) sahip olan ve rutin şekilde olay müdahale planları denetlenen kuruluşlar ortalama 3.26 milyon USD maliyetle karşılaşmakla birlikte, bu yapılara sahip olmayan kuruluşlara göre veri ihlalinden doğan maliyetlere 2,66 milyon USD daha az maruz kalmaktadır. Yapay zeka (AI) ve otomasyon olarak nitelendirilen sistemleri kullanan kuruluşlar ise yine aynı rapora göre bu teknolojilerden faydalanmayan kuruluşlara göre %55.3 daha az veri ihlali maliyetine maruz kalmaktadır. Söz konusu teknolojiler SOAR (security orchestration, automation and response), UEBA (user and entity behavior analytics), EDR (endpoint detection and response) and XDR (extended detection and response) olarak sıralanabilir (IBM, 2022b). Bunların yanı sıra kimlik erişim yöntemleri (IAM); 2FA (İki Faktörlü Kimlik Doğrulama), MFA (Çok Faktörlü Kimlik Doğrulama) ve SSO (Çoklu Oturum Açma) hackerlara karşı bilgisayar savunma sistemlerinin başlıcaları olarak sıralanabilir. Bu sistemlerin kullanılması da veri ihlallerinin engellenmesi amacıyla büyük önem arz etmektedir. Sıfır güven yaklaşımı doğrultusunda sürekli kimlik doğrulama, yetkilendirme ve doğrulama, en düşük seviyede ayrıcalıklı erişim ve ağ etkinliklerinin takip edilmesi de yine bu alanda uygulanması gereken önlemlerdir (IBM, 2024).

2023 Ocak ayında T-Mobile şirketi tarafından yapılan açıklamada 37 milyon gibi yüksek sayıda müşterinin verilerinin çalındığı ifade edilmiştir. Söz konusu veriler içerisinde kişilerin adresleri, iletişim bilgileri, kimlik bilgileri de dahil hassas verilerinin de olduğu aktarılmıştır. Daha önce de 2021 Ağustos'unda aynı şirketin maruz kaldığı veri ihlallerine yönelik saldırılarda 80 milyon ABD vatandaşı ihlallerden etkilenmiştir. Bu olaylara yönelik açılan tazminat davalarında şirket mağdur konumunda bulunan kişilere karşı 350 milyon USD ödeme yapmakla yükümlendirilmiştir (NPR, 2023).

2.3. İnsan Hataları Kaynaklı Siber Saldırılar

Oltalama Saldırıları (Phishing Attacks)

Oltalama saldırıları "password" sözcüğünün ilk harfi ile balık avlamak manasında kullanılan "fishing" sözcüğünün birleşmesi ile ortaya çıkmıştır. Oltalama saldırıları literatürde "yemleme" ve "kimlik avı" şeklinde de anılmaktadır (Doğan, 2021). Bu saldırı tipinin genel mahiyeti, siber saldırganların kullanıcıları sahte web sitelerine yönlendirmesi ve bu sitelerde yer verdikleri gerçeğe yakın ara yüzler vasıtasıyla kullanıcılara ait şifre bilgileri ve kişisel bilgilerin ele geçirilmesi esasına dayanmaktadır (BTK, 2022).

Oltalama saldırıları günümüzde en sık rastlanan siber saldırılar arasında yer almaktadır. Bankacılık ve finans sektöründe gelişen teknoloji ile birlikte online ve mobil bankacılık işlemlerinde oltalama saldırıları kullanılarak insanlar mağdur edilebilmektedir. Söz konusu saldırılarda kurbanlar e-posta ile bağlantı linki paylaşımı vasıtasıyla oluşturulan sahte sitelere yönlendirilmektedir. Ara yüzleri benzer olan ancak ufak ayrıntılarla gerçeğinden ayırt edilebilen bu sitelerde kullanıcıların doldurması gereken formlar kullanılarak kişisel hassas bilgiler ele geçirebilmektedir. Bu bilgiler arasında kredi kartı bilgileri, oturum açma kimlik bilgileri ve hesap bilgileri de bulunmaktadır. Siber suçun failleri bu yöntemle mağdurlar üzerinden haksız ekonomik kazanç elde etmektedir (BTK, 2022)

Oltalama saldırıları türlerinden biri olarak nitelenen "Farmasötik Kimlik Avı (Pharming)" siber saldırılarında mağdurların çeşitli yöntemlerle kandırılmasına ek olarak, mağdurların kişisel hataları bulunmadan saldırıdan etkilenebildiği görülmektedir. Bu tür siber saldırılar mağdur kişinin elektronik cihazına yerleştirilen kötücül kodların harekete geçirilmesi ile gerçekleştirilebilmektedir (Güngör, 2021). Bunun gibi oltalama saldırıları farklı siber saldırı türlerini de içerecek şekilde kullanılabilmektedir. Kullanıcılar sanal bankacılık portalları, internet tabanlı alışveriş platformları veya sosyal medya ağları ve sahte web sitelerine yönlendirilebilmektedir. Oltalama saldırıları "Domain Name System (DNS)"e dayalı zafiyetlerden faydalanma ya da kullanıcılara ait ana bilgisayar dosyasını veya yerel ağdaki DNS yapılandırmasını farklı yöntemlerle değiştirmeyi hedefleyen "sunucu tabanlı" da işlenebilmektedir (Proofpoint, 2023). Bu yönlendirmeler sahte web sitelerine

yönlendirme tekniğinin yanı sıra sitelerin ağ adreslerinde (URL) yapılan harf değişiklikleri vasıtasıyla oluşturulan sahte sitelere yönlendirme şeklinde de sağlanabilmektedir.

Kimlik Hırsızlığı/Kimlik Avı Saldırısı

"Kimlik avı veya hırsızlığı" olarak nitelenen bir diğer oltalama saldırı türünde kullanıcılar kişisel bilgilerini kendi iradeleri ile karşı tarafa ileterek gerçeğe yakın ara yüzlere sahip olan web sitesi ve mail adresi görüntüleri ile kandırılmaktadır. Siber saldırganlar gerçek bir internet sitesi veya mail adresi görünümünü karşı tarafa sunup kendilerini ticari bir şirketin temsilcisi olarak tanıtmaktadır. Kullanıcılar ise gezinti yaptıkları internet sitelerinin gerçek olduğunu düşünerek çeşitli kişisel bilgilerini girmektedir. Aynı zamanda giriş parolaları ve kimlikleri de paylaşılan bilgiler arasında geniş yer tutmaktadır. Sahte şekilde oluşturulan mailler fidye yazılımı saldırıları ile entegre şekilde kullanılarak kullanıcıların sistemlerine erişimde aracı görevi üstlenmektedir. FBI verilerine göre 2021 yılında yayımlanan verilerde 323.972'nin üzerinde kimlik hırsızlığı yöntemiyle dolandırılan kişi olduğu ifade edilmiştir (Investopedia, 2024b). Bu saldırılarda kullanılan metotlar arasında; kişisel kartların çalınması, posta kutularından fiş, fatura ve belgelerin alınması, teknolojik aygıt depolama alanlarındaki dosyaların kopyalanması, sosyal mühendislik yöntemlerinin uygulanması, bilgisayar korsancılığı faaliyetlerinde bulunulması, virüs ve solucan yazılımlarının kullanılması, ısrarlı takip (stalking) denilen ve kişiler hakkında internet ortamında yayımlanan bilgilerin derlenerek kullanılmasına ilişkin yöntemler ve hedefteki kişilerin saldırganın kimliğini tanıyamayacak şekilde telefon ve diğer iletişim araçları vasıtasıyla yürütülen dolandırıcılık faaliyetleri bulunmaktadır (BTK, 2022).

Bunun yanı sıra kimlik avı saldırıları entegre saldırılar şeklinde Gelişmiş Kalıcı Tehdit (APT) saldırıları ile birlikte kullanılarak kamu kurum ve kuruluşları ile özel şirketlerin bilişim sistemlerine, kritik altyapılarına ve ağlarına yıkıcı etkiler bırakmaktadır. Bu saldırılar aracılığıyla söz konusu kurum, kuruluş ve şirketlerde çalışan personele yönelik kötü niyetli davranışlar gerçekleştirilerek yetkisiz erişimde bulunulmaktadır. Kapalı sistemlere yönelik kötü amaçlı yazılımlar aracılığıyla güvenlik sınırları aşılmaktadır. Söz konusu saldırılarda kurumsal itibar, küresel ticari şirketlerin pazar payları ve pazardaki hakimiyetleri, tüketicilerin şirkete duydukları güven ve diğer unsurlar olumsuz

etkilenmektedir. Buna ilişkin olarak sahte şekilde oluşturulan ve amacı bir üniversitedeki akademik çalışanlara gönderilerek üniversiteye ait kritik sistemlerin ele geçirilmesi olan bir olayda, sahte e-posta ve içerisindeki bağlantı linkinin bu konuda bilinçsiz olan çalışanlar tarafından açılması ve güvenlik açığının oluşması sonucu ile karşılaşılmıştır. Bu e-postada kullanıcının periyodik olarak değiştirmesi gereken parolasının kullanım süresinin dolmak üzere olduğu iletilmiştir. Söz konusu parola ile kullanıma devam edilebilmesi amacıyla 24 saat içinde şifre yenileme işlemi için ilgili adres talimatlarla yönlendirilen adres olarak gösterilmiştir (Imperva, 2024a).

Söz konusu kimlik avı saldırılarından korunmak amacıyla alınabilecek önlemlere gelinirse öncelikle "İki faktörlü kimlik doğrulama (2FA)" ön plana çıkmaktadır. Bunun dışında sıkı parola yöntemlerinin kurumsal olarak yaygınlaştırılması ve yerli uygulamalara yönelik koruyucu sistemlerin kurumların ve kurumsal şirketlerin bilgisayar sistemlerine kurulmasının sağlanması gerekmektedir. Düzenli aralıklarla sahte şekilde oluşturulan e-posta ve bağlantı linkleri kurum çalışanlarına iletilerek söz konusu oltalama testlerinin sonuçları personelin maillerine gönderilmesi ve farkındalık çalışmaları bu saldırılara karşı önemli tedbirler konumundadır.

Sosyal Mühendislik Saldırıları (Social Engineering)

Sosyal mühendislik saldırıları diğer bir deyişle "human hacking" siber saldırganlar tarafından çeşitli yöntemler kullanılarak hedef olarak belirlenen kişilerin kandırılması, ikna edilerek manipülasyona uğratılması ve zaaflarından yararlanılarak kişisel verilerinin ele geçirilmesidir (Mann, 2008). Bu tür siber saldırılar çoğunlukla mali kazanç elde etmek amacıyla gerçekleştirilmektedir. Kişiler farkında olmadan ancak iradeleri ile kredi kartı şifrelerini, banka hesaplarına ait parolalarını, şirketlerde çalışan yetkililer ise gizli kurumsal bilgileri siber saldırganlara vermektedir (Jacobson ve Idziorek, 2013).

Bu saldırılarda ele geçirilen bilgi ve veriler terör örgütlerine satılarak devletlerin milli güvenlik ve kamu düzeni yapıları olumsuz etkilenebilmektedir. Diğer taraftan kullanıcıların bilgisayar ve mobil cihazlarına zarar verilebilmekte ve sistemleri kullanıma kapatılabilmektedir. Sosyal mühendislik yöntemleri çeşitlilik arz etmekle beraber genellikle yemleme (phishing), spam mailler, telefonla ve mesajla kandırma gibi eylemleri

içermektedir (BTK, 2022). Siber saldırganlarca kullanıcılara ait e-posta veya sosyal medya hesapları sosyal mühendislik saldırısıyla eş zamanlı ele geçirilmekte, bu hesaplardaki diğer kullanıcılara toplu halde aynı içerikte metinler gönderilmektedir. Bu vasıtayla sahte olarak oluşturulan banka ödeme sayfalarına girilen finansal bilgiler saldırganlarca ele geçirilmektedir. Söz konusu sosyal mühendislik saldırılarının yaşam döngüsü sırasıyla hedefin tanımlanması, ortak bulunarak organize olunması, araç oluşturulması veya elde edilmesi, hedefin araştırılması, test edilmesi, yayılması, ilk ihlalin yapılması, giden bağlantı kabulünün kontrolü, erişimin genişletilmesi ve kimlik bilgilerinin elde edilmesi, bağlantı noktasının güçlendirilmesi, verilerin süzülmesi ve izlerin yok edilmesi şeklindedir (Doğan, 2021).

İstem Dışı Alınan E-Postalar (Spam)

İstem dışı alınan e-postalar, internet kullanıcılarının açık rızasına dayanmadan ticari veya farklı amaçlarla iletilen reklam veya propaganda içerikli mailler olarak nitelenebilecektir. Bu mail içerikleri kopyalanarak rızaları dışında diğer kullanıcılara da toplu şekilde gönderilebilmektedir. Söz konusu mailleri ileten saldırgan kişi veya kişi gruplarına da "spammer" adı verilmektedir. Mailler dolayısıyla sağlanan kişisel bilgiler siber saldırganların kendi veri tabanlarına aktarılmaktadır. Aktarılan veriler belirli meblağlar karşılığında ticari faaliyet gösteren ve kişiye özel reklam veren sektördeki ilgili şirketlere pazarlanmaktadır. Şirketler bu yöntemle kişilerin doğrudan ihtiyacı olan veya ilgisini çeken ürünlere yönelik reklam vererek satışlarını artırmaktadır. Söz konusu reklamlar, ticari amaçlı olduğu kadar pornografik öğeler içeren ürünlerin ve hizmetlerin küresel şekilde yayılması gibi etkileri de barındırmaktadır (BTK, 2022).

Çöpe Dalma/Artık Toplama Taktiği (Scavenging)

Çöpe dalma yöntemi, bilgisayarlar üzerinde gerçekleştirilen işlemler sonrası geride kalan kritik ve hassas bilgilerin siber saldırganlarca ele geçirilmesi olarak tanımlanmaktadır. Söz konusu yöntemde fiziksel çıktı şeklindeki belgeler ya da yazıcıda kalan bilgi ve verilere erişim sağlanması mümkün olmaktadır. Bununla beraber bilgisayar ve sistemlerde kullanıldıktan sonra silinen verilere farklı yollarla tekrar erişim sağlanması da artık toplama olarak nitelenmektedir (BTK, 2022).

Artık toplama yöntemi NIST tarafından yapılan tanımda "*veri elde etmek için nesne kalıntısında arama yapmak*" ifadesi ile kullanılarak süpürme (scavenging) şeklinde kısaltılmaktadır (NIST, 2023a). Bir başka tanımda bu terim "*bir sistemin veri kalıntısı üzerinden arama yaparak gizli veya değerli verileri arama süreci*" şeklinde özetlenmektedir (AttackSimulator, 2022). Verilerden geriye kalan artıklar kullanılarak gerçekleştirilen çöpe dalma yöntemi gibi, süpürme yönteminde de fiziksel çıktılı belgelerin taranması ve gelecekte kötü niyetli işlemlerde kullanılacak bilgilerin veri havuzunda depolanması sağlanmaktadır.

Gizlice Dinleme (Sniffing/ Eavesdropping)

Gizlice dinleme, sistemler ve ağlar üzerinden veri alışverişi gerçekleştirilirken siber saldırganlar tarafından araya girilerek ya da oluşan elektromanyetik dalgalar takip edilerek kontrol dışı kalan verilerin yeniden kapsama alınması olarak nitelenmektedir. Söz konusu saldırı, ağ üzerinden gerçekleştirilen veri alışverişi sırasında saldırganların yaptığı fiziki müdahaleler vasıtasıyla da rıza dışı dinlemeye vücut verebilmektedir (BTK, 2022). Bahse konu saldırılar ağ üzerindeki veri alışverişinin geliştirilen yazılımlarla gizlice dinlenilmesi (eavesdropping) ve elektromanyetik dalgalar aracılığıyla dinleme şeklinde de gerçekleştirilebilmektedir (Ehliz, 2019).

Bu kapsamda siber saldırganlar güvenlik açığı olan ve güvenilir olmayan ağlar üzerinden iletilen mesajları okumaktadır. Kurum ve kuruluşlar ile büyük şirketlerin fiziki altyapıları üzerine inşa edilen dinleme ve veri iletimi sağlayan cihazlar, zayıf güvenlik sistemleri ve dinleme gönderileri bu saldırılarda hedef konumunda bulunmaktadır. Kurumsal ve bireysel sistemler ile güvenli olmayan ağ yapıları üzerinden gerçekleştirilen dinleme faaliyetlerine karşı bilgi güvenliği ve siber güvenlik bakımından dayanıklılığının artırılması bu noktada alınması gereken başlıca önlemlerdir (Sangfor, 2022).

2.4. Diğer Siber Saldırı Yöntemleri

Mantık Bombası (Logic Bomb)

Mantık bombası; işletim sistemlerine, programlara ve ağlara yönelik gerçekleştirilen siber saldırılarda kullanılan ve sistemlere kötü amaçlı yük aktarımında bulunan yazılımsal

talimat kümeleridir. Söz konusu yazılım sabit disklere etki ederek içerisindeki dosyaların silinmesine, verilerin tahrifatına veya yok edilmesine neden olmaktadır. Bu yazılımlar aynı zamanda virüs ve solucan gibi kötücül yazılımlarla entegre şekilde kullanılarak siber saldırının yıkıcılığı artırılmaktadır. Mantık bombası, çoğunlukla hedeflenen sistem ve bilgisayara imtiyaz sahibi yetkililerce gizli şekilde yerleştirilmektedir (Zenarmor, 2023a). Bu yazılımların temel görevi sistem içerisine girdikten sonra virüs ve solucanlar için uyarıcı mekanizmaları pasiften aktife dönüştürmektir (Yener, 2013).

Söz konusu talimat kümelerinin çalışma yöntemi olumlu ya da olumsuz tetikleyicilere bağlı olarak gelişmektedir. Olumlu tetikleyicilerde ana unsur tanımlanmış koşullu emre dayalı mantık bombasını uyarmak ve patlatılmasını sağlamak iken olumsuz tetikleyicilerde tanımlanan koşulun gerçekleşmemesi neticesinde mantık bombasını harekete geçirmektedir. Burada olumlu ve olumsuz tetikleyicilerin bozucu koşul-geciktirici koşul mantığı ile mantık bombasına talimat verdiği görülmektedir (Zenarmor, 2023a).

İlk mantık bombası örneklerinden biri 1982 yılında "Trans Sibirya Boru Hattı olayı" olarak nitelenen olaydır (Hoffman, 2014). Bu olayın perde arkası ABD-Sovyetler Birliği arasında yaşanan Soğuk Savaş dönemi sonrasına dayanmaktadır. ABD Merkezî İstihbarat Teşkilatı (CIA) tarafından istihbarat servisinin kendilerine verdiği bilgide, Sovyetler Birliği Devlet Güvenlik Komitesi (KGB) tarafından Kanada menşeili bir şirketin yapımını üstlendiği Sibirya boru hattına casus program yerleştirildiği, boru hattına ait merkezi kontrol sisteminin teknik ve yazılımsal kılavuzlarının çalındığı aktarılmıştır (Zenarmor, 2023b). Söz konusu olay, doğal gaz boru hatları için Sovyetler Birliği'ne ait milli ve yerli yazılımının yeterli olmadığı gerekçesiyle ABD'nin kendi milli kodlarının Sovyet Rusya tarafından çalınması girişimi üzerine çıkmıştır. Bu girişimin ortaya çıkmasıyla ABD karşı atak yaparak Sovyetlerin çaldığı yazılımın içerisine mantık bombası yerleştirmiştir. Bu tuzağa düşen Sovyet Rusya ajanları yazılımı ülkelerine götürmüşlerdir. Zamanı geldiğinde pasif konumda olan mantık bombası aktif hale getirilerek söz konusu doğal gaz boru hattının patlaması ve infilak etmesi ile söz konusu olay neticelenmiştir (Fruhlinger, 2024a).

1998 yılının Haziran ayında Çernobil (CIH) Virüsünü içerisinde barındıran bir mantık bombası keşfedilmiştir. Çernobil Faciası yıl dönümlerinde pasif konumdaki mantık bombası aktifleşerek zarar verici bir konuma gelmektedir. Time bomb şeklinde çalışma

yöntemi izleyen bu mantık bombası FAT (Dosya Ulaşım Tablosu) ve BIOS devresini silmektedir (Microsoft, 2012).

Yakın dönemdeki olaylara bakıldığında ise 2019 yılında ortaya çıkan bir mantık bombası olayında Siemens Corporation şirketinde çalışan bir işçinin, şirket için çalıştırdığı programlara mantık bombası yerleştirdiği, elektronik tablo yazılımı konusunda oluşan yazılımsal hatalarda önceden programlanmış ve pasif halde bulunan yazılımın mantıksal şartlar oluştuğunda aktifleştirilerek mevcut yazılımsal hatayı düzeltmesi istenmiştir. Söz konusu plan iki yıl boyunca uygulanmış ancak saldırıda aracı olarak kullanılan personelin iş yerine gelmediği bir günde parolasını başka çalışanlara vermesi sonrasında siber saldırıya konu mantık bombası ortaya çıkmıştır (Zenarmor, 2023b).

Süper Darbe (Super Zapping)

Süper darbe, siber saldırganların sistemlerin ana unsurunu oluşturan kontrol ve güvenlik protokollerini aşarak geliştirilen çeşitli yazılımlarla kötücül faaliyetlerde bulunması olarak nitelenmektedir. Kurum ve kuruluşlar ile şirketler bahse konu süper darbe saldırılarında kullanılan "süper zap" adı verilen ve güvenlik duvarını aşan programlar vasıtasıyla tehdit altına girmekte, bilgi hırsızlığı kapsamında sistemsel güvenlik önlemleri alınmasını zorunlu kılmaktadır (BTK, 2022).

Süper darbe türündeki programlar kritik cihaz ve sistemler üzerinde olumsuz etkiler bırakmaktadır. Bunlar arasında en bilinen örneklerden olan, bankacılık ve finans sektörü üzerinde etkili olan ve hesap bakiyelerinin azaltılmasına neden olan siber saldırılardır. Bankacılık sektörü kritik altyapılar arasında bulunmakla birlikte bunlara gerçekleştirilen saldırılar küresel çapta krizlere neden olmaktadır. Bahse konu saldırılar çoğunlukla banka içerisinde çalışan personeller tarafından kişisel bilgisayarlar vasıtasıyla gerçekleştirilmektedir.

Salam Yöntemi (Salami Technique)

Salam yöntemi, siber saldırganlar tarafından uzun bir dönemde ölçek bakımından büyük parçalar yerine küçük parçaların hedefteki kişilerin fark edemeyeceği şekilde ekonomik kazanç elde etme amacı ile hesaplardan çekilmesidir. Bu yöntem çeşitli siber

saldırılarla entegre şekilde kullanılarak çevrim içi veri tabanları aracılığıyla mevcut saldırının etki düzeyi artırılmaktadır. Kişisel hesaplar yerine bankacılık sektörüne daha ağır şekilde darbe vuracak toplu hesapların yetkisiz ödeme ve kredilerle ele geçirilmesi aynı zamanda kamuyu ve devleti de büyük bir zarara uğratmaktadır. Bilişim sistemleri aracı kullanılarak zimmetine para geçiren banka görevlileri söz konusu yöntemi uygulamakta ve bulundukları konum ve sahip oldukları mesleğin avantajını kullanmak suretiyle mali kazanç elde edebilmektedir.

Salam yöntemine benzer olarak kullanılan ve yuvarlama yöntemi (penny shaving) de denilen bir diğer yöntemde, siber saldırganların bankaların sahip olduğu sistemlerdeki düşük miktarlı paraları kendi hesaplarına aktarması ve hedefteki kişilerin hesaplarındaki küçük meblağ hareketlerinin bu yöntemle fark edilmeyecek değerlere yaklaştırılması temel suç fiili olarak ön plana çıkmaktadır (Firmbee, 2023). Bununla birlikte banka hesaplarındaki kaynaklardan düşük meblağların transfer edilerek haksız kazanç sağlanmasında truva atları da aktif şekilde kullanılarak para transferleri gerçekleştirilmektedir (Ehliz, 2019).

Yetki Artırımı (Privilege Escalation)

Yetki artırımı saldırıları kurum, kuruluş ve küresel çaplı şirketlerin bilgisayar ve işletim sistemlerinde bulunan güvenlik zafiyetlerini tespit ederek açıklıklardan faydalanmak amacıyla yüksek seviyede yetkisi olan yönetici ya da personellerin yetkilerinin kötü amaçlı artırılmasıdır (Sans, 2017). Söz konusu saldırı "ayrıcalık yükseltme" ve "hesap devralma" şeklinde de ifade edilmektedir (Crowdstrike, 2022b). Siber saldırganlar hedeflerindeki sistemlere yönelik kontrol yetkisini ele geçirmek ve kritik verilere erişim sağlamak için bu saldırıları gerçekleştirmektedir. Sistemlere erişim yetkisi bulunan personelin giriş bilgileri ele geçirilerek hedef sistemlere gizlice sızılmaktadır (Sans, 2017). Yetki artırımı saldırılarında yetkisiz erişim elde eden siber saldırganlar dışarıdan kişiler olabileceği gibi, bu saldırılar hedef kuruluşlarda çalışan kişilerin çeşitli ikna yöntemleriyle operasyonel saldırı sürecine dahil edilmesi şeklinde de görünüm kazanabilmektedir (Crowdstrike, 2022b). Saldırganlar tarafından sisteme giriş yapıldıktan sonra yazılımsal kodlar kötü amaçlı değiştirilerek sistem içinde yer alan uygulama ve dosyalar tahrifata uğratılmaktadır. Bununla birlikte kuruluştaki yöneticilerin kendi sistemlerine alışılmış girişleri engellenebilmektedir. Parolalar değiştirilerek sistemsel bozulmalara neden olunmakta kritik sistemler cevap

veremez hale getirilebilmektedir (Sans, 2017). Yetki artırımı saldırılarında siber saldırganlar sistem açıklıklarını tespit ederek işletim sisteminde ve web uygulamalarında gerçekleşen hareketler, tasarıma ilişkin eksiklikler ve gözetim kusurlarını araç olarak kullanmaktadır. Bu tip yöntemler "yanal hareket" şeklinde ifade edilen ve siber saldırganların derin ağ (deep network) seviyesine indikleri saldırı metotları olarak ön plana çıkmaktadır. Söz konusu saldırı türü diğer saldırı yöntemleri ile birlikte kullanılarak sisteme sızılması ve zayiat verilmesi için kullanılmaktadır. Bu kapsamda özellikle fidye yazılımı ve oltalama saldırıları söz konusu entegre saldırılarda ön plana çıkmaktadır. Yetki artırımı ya da ayrıcalık yükseltme dikey ve yatay olmak üzere iki farklı şekilde gerçekleştirilmektedir. Yatay yetki artırımı düşük seviyedeki imtiyazlara sahip kullanıcı ve yöneticilerin hesaplarını ele geçirme şeklinde tezahür etmektedir. Söz konusu yöntemde kullanıcılara ait giriş bilgileri adı, parolalar, kişisel hesaplar, hassas bilgi içeren dosyalar veya uygulamalara erişim sağlanarak yetkili erişim sahiplerinin işlem izin alanları işgal edilmekte, imtiyazlı hakimiyet alanları yatay şekilde genişletilmektedir. Buna karşılık dikey yetki artırımı ise yatay yetki artırımına kıyasla sisteme girişte ve işlem yapabilmede daha yüksek yetkiye sahip personelin hesaplarına rıza dışı erişim hakkı sağlamaktadır. Üst yönetici erişimi (root access) yetkisi ele geçirilerek büyük bir imtiyaza sahip olunmakta ve diğer hesaplara da erişim sağlanarak işlem alanı genişletilmektedir (Crowdstrike, 2022b). 2019 yılında meydana gelen olayda Doğu Avrupa ülkelerinin kritik kurumlarına yönelik Microsoft Windows üzerinden bir dizi saldırı yapılmıştır. Söz konusu saldırı, ayrıcalık yükseltme yöntemiyle yapılmış olup belirsiz kod çalıştırma, güvenlik zafiyeti olan uygulamalar içerisindeki verileri izleme ve değiştirmeyi de içeren bir dizi ihlali ortaya çıkarmıştır.

Maskeleme/Kılık Değiştirme Saldırıları (Masquerading)

Maskeleme ya da diğer bir deyişle kılık değiştirme saldırısı, yetkisiz kişilerin görünüşte yetkiliymiş gibi gösterilerek perdeleme şeklinde sistemlere erişim sağlanmasıdır (NIST, 2023a) Söz konusu saldırıya maskeli balo da denilmesinin sebebi söz konusu yöntemde hedef olarak belirlenen sistemlerdeki güvenlik açıklıklarından yararlanılıp hesap bilgileri, hassas bilgiler ve parolalara kimlik gizlenerek ulaşılmasıdır. Maskeleme saldırısında kullanıcıya ait kimlik sorgulama kısmı aşılarak ayrıcalıklı erişim yetkisi sağlanmaktadır. Söz konusu ayrıcalıklı yetki hem içeriden hem de dışarıdan tehdit aktörleri tarafından gerçekleştirilebilmektedir (Cybertraining365, 2023). Maskleleme saldırılarıyla,

IP adreslerinde sahtecilik ve kimlik avı saldırıları sıkça kullanılmaktadır. Bu saldırılar neticesinde devletlerin ve şirketlerin kritik sistemleri tehlikeye girmektedir (SEON, 2023).

Maskeleme saldırılarında, siber savunma sistemlerinden kaçınmak amacıyla kullanılan dört sınıf yöntem bulunmaktadır. Bunların ilki “maskeli dosya uzantıları”dır. Söz konusu uzantılar zararsız gibi görünerek kullanıcıların kandırılmasına yol açmaktadır. Diğer bir sınıf ise “isim maskeleme”dir. Bu maskeleme türü "flash_en.exe" şeklinde yasal olan uygulama isimlerini araç olarak kullanmaktadır. Üçüncü sınıf maskeleme yöntemi “dosya konumlarını maskeleme”dir. Bu maskeleme türünde "C:\Windows\System32" gibi güvenli olarak nitelendirilen dizinler vasıtasıyla kötücül dosyalar gizlice sızdırılır. Son yöntem olan “dosya imzalarını maskeleme” ise siber suçlular tarafından program kodu imzalarının meta verilerle beraber kullanılmasıdır. “T1036.001 Geçersiz Kod İmzası” şeklindeki yazılımsal ifade söz konusu kötücül yazılımlar içerisinde kullanılan dosya imza maskeleme yöntemine örnek verilebilir (PICUS, 2022).

2010 yılında Pekin’de Halk Kurtuluş Ordusu olarak bilinen grupla ilişkisi olan “Elderwood Grubu” tarafından meydana getirilen Aurora Operasyonu olayında, ABD menşeili şirketlere yönelik kimlik avı yöntemi kullanılarak maskeleme siber saldırısı yapılmıştır. Bu saldırılarda 34 farklı şirket zarar görmüştür. Söz konusu şirketler arasında küresel çapta hizmet veren Google, Adobe ve Yahoo gibi şirketlerin de bulunması olayın vahametini göstermektedir. Bu saldırılar ile hedeflenen ana amaç şirketlerin piyasaya ait ticari sırları ile fikri ve sınai mülkiyete ilişkin unsurların ele geçirilmesi olmuştur. Bunlarla beraber saldırıların arkasındaki iddialardan birisi de Çinli bazı aktivistlerin Gmail hesaplarının ele geçirilmesi olmuştur. Söz konusu saldırılar küresel çapta etkiye yol açarak ekonomik kayıplara neden olmuştur. Bu saldırılardan korunmak amacıyla davranışsal analiz, parmak iziyle giriş yöntemi, uç nokta koruması, parola güvenliği ve çok faktörlü kimlik doğrulama (MFA) sistemlerinin kullanılması büyük önem arz etmektedir (SEON, 2024).

Diğer bir çarpıcı örneğe ise 2013 yılında yaşanan maskeleme saldırısında rastlanmıştır. Söz konusu saldırıda maskeleme ile yetkisiz erişim elde eden saldırganlar verileri ihlal etmiştir. Bu saldırı sonucunda Target adlı şirkete ait yaklaşık 70 milyon müşterinin verisi ele geçirilmiştir. Öyle ki Target'ın iklimlendirme cihazları yüklenicisi Fazio Mechanical Services de bu saldırıda etkilenmiş ve kritik bilgilerine erişim

sağlanmıştır. Karanlık ağ üzerinden erişim sağlanan bilgiler satılmış ve kişisel bilgiler ifşa edilmiştir. Diğer taraftan Target'in web uygulaması vasıtasıyla güvenlik zafiyetlerinden faydalanılarak sistem çökmesi ve hizmet devamlılığının yitirilmesi ile karşılaşılmıştır. Söz konusu saldırıda "Pass the Hash" adı verilen saldırı yöntemi aracılığıyla ayrıcalıklı yönetim hesabı "Etki Alanı Yöneticileri" grubuna dahil olunarak şirketin banka hesaplarını da içeren önemli ve hassas bilgilerine erişim sağlanmıştır (Cyware, 2019).

Bilgi ve Veri Aldatmacası (Data Diddling)

Bilgi ve veri aldatmacası İngilizcede dijital bilgi anlamına gelen "data" ve tahribat anlamına gelen "diddle" sözcüklerinin bir arada kullanılmasıyla oluşmuştur. Bu saldırı türü, sistemlere girilen verilerin ve sayısal ifadelerin kasti olarak hatalı işlenmesini kapsayan bilgisayar dolandırıcılığı şeklinde tanımlanabilir. Bu hatalı girişler, çoğunlukla gelir ve gider tabloları ile beyan esaslı mali unsurların kötüye kullanımını içermektedir. Bununla birlikte söz konusu saldırılarda bireylere, kurumlara ve şirketlere zarar vermek hedefiyle hareket edilmektedir. Bilgi ve veri aldatmacası donanım ve yazılımsal araçlarla yapılabilmekte, bu kapsamda uzaktan veya veri girişi yapan personel tarafından işlenebilmektedir (Computer Hope, 2021). Siber saldırıya neden olan fiiller kasıtlı şekilde sisteme hatalı girilen ifade ve verilerle oluşabileceği gibi söz konusu bilgi ve verilerin değişikliğe uğratılması veya istismar edilmesi şeklinde de vücut bulabilmektedir. Söz konusu siber yöntemle belgelerde tahrifat oluşturabilmenin yanı sıra gizli ve hassas veriler buna özel geliştirilen cihazlarla değiştirilebilmektedir (Ehliz, 2019).

Bilgi ve veri aldatmacası kapsamında oluşan veri dolandırıcılığı suçu çerçevesinde resmi ve özel belgede sahtecilik, sahte beyan, bilgisayar donanımlarının değiştirilmesi ve tahribatı, klavye kaydedici vasıtasıyla belgede tahrifat, verilerin hiç girilmemesi ve veri gözetim kontrol sistemlerinin kötüye kullanılması gibi durumlar ortaya çıkabilmektedir (The IT Law Wiki, 2023b). Bu kapsamda veri dolandırıcılığı ile mücadelede ağ, sistem ve cihazlar için yeni nesil bulut tabanlı antivirüs programları, eğitim ve farkındalık faaliyetleri, güvenli erişim yöntem protokolleri, yetki gerektiren işlemlerde çok faktörlü kimlik doğrulama gibi siber güvenlik önlemleri büyük önem arz etmektedir (NordVPN, 2023).

Eş Zamansız Saldırılar (Asynchronous Attacks)

Eşzamansız saldırılar, işletim sistemlerinin çalışma metodolojilerinde meydana gelen zafiyetlerden yararlanılarak söz konusu sistem komutlarının sıraya konulması sırasında henüz sırası gelmemiş olan komut içeriklerinin değiştirilmesi olarak ortaya çıkmaktadır. Söz konusu saldırılarda çıktı sırası düzeneği olarak gerçekleştirilen işlemlerde sıra bekleyen çıktılar, şekli ve içeriksel olarak tahrifata uğratılmaktadır. Bu saldırılar neticesinde resmi evrakların içerikleri değiştirilmekte, kurum ve kuruluşlarda kritik ve hassas bilgiler içeren belgeler tahrif edilmektedir. Güvenlik açıklıklarından faydalanılarak gerçekleştirilen söz konusu saldırılar sonucunda çok sayıda komuta yanıt veremeyen sistemlere rıza dışı giriş yapılarak içerik değiştirilmektedir (Avşar ve Öngören, 2010).

Donanımsal Saldırılar

Donanımsal saldırılar, siber saldırıların yalnızca ağ tabanlı yazılımlar vasıtasıyla değil aynı zamanda mikroçip gibi donanımlarla da yapılabileceğini göstermektedir. Yazılımlarla gerçekleştirilen siber saldırılar donanımsal saldırılara göre fazla olsa da donanımların avantajları da bulunmaktadır. Öyle ki birincil fonksiyonlarının dışında kullanıcılar tarafından tahmin edilemeyecek ikincil fonksiyonlar siber saldırganlarca kullanılmaktadır. Üretim aşamasında dahi elektronik cihazlara gömülen yazılımlar vasıtasıyla donanımsal saldırıların etki düzeyi artırılmaktadır. Öyle ki sıfır cihazlar genel olarak güvenli kabul edilip herhangi bir siber güvenlik endişesine yol açmamaktadır. Bu düşünceden hareketle özellikle son yıllarda küresel dijital cihaz ve bilgisayar donanımı üretimlerinde bahse konu saldırılar gerçekleştirilebilmektedir. Söz konusu donanımlar üretilirken arka kapı gibi çeşitli yazılımlar cihaza işlenerek sonradan kötücül faaliyetlerde kullanılmaktadır. Bu saldırı yöntemi aracılığıyla devlete ait kurum ve kuruluş cihazlarına yetkisiz şekilde erişim sağlanarak devletler arası siber casusluk ve istihbarat faaliyetleri gerçekleştirilmektedir (BTK, 2022).

Hukuka Aykırı İçerik Sunma

Hukuka aykırı içerik sunma saldırıları, hukuki sınırların aşılarak kişisel verilerin yayımlanma kurallarına aykırı şekilde ifşa edilmesi ve kanunen suç teşkil edecek içeriklerin internet ortamına arz edilmesi olarak nitelendirilebilir. Söz konusu içerikler, kişilik haklarını

ihlal edici nitelikte olduğu gibi aynı zamanda fikir ve sanat eserlerine ilişkin telif haklarının ihlali ve çocuk pornografisine özendirici faaliyetlerin yaygınlaşmasını sağlayan hususları da bünyesinde barındırmaktadır (BTK, 2022).

3. SİBER TERÖRİZM ve ULUSLARARASI HUKUK

Siber terörizmle mücadelede bilgisayar vasıtasıyla işlenen suçlara yönelik devletlerin ceza mevzuatlarının uyumlaştırılması ilişkin ilk çabalara 1983 yılında Ekonomik Kalkınma ve İş Birliği Örgütü bünyesinde başlanmıştır. "Computer Realted Crime: Analiysis of Legal Policy" isimli raporda bilgisayar suçlarına ilişkin olarak üye devletlerin cezai yaptırımlar bakımından mutabık kalacağı ortak bir öneri sunulmuştur. Ekonomik Kalkınma ve İş Birliği Örgütü tarafından 90'lı yıllarda kamu ve özel sektörün de katılımı ile bilgisayarlara yönelik sistem güvenliğinin sağlanması için stratejiler ve eylem planları yapılması yönünde teşvikler geliştirilmiştir (Oğuz ve diğer., 2006). Zaman geçtikçe söz konusu çalışmalara Birleşmiş Milletler ve NATO da dahil olmuş, Bileşmiş Milletler Sözleşmesi (BM Şartı) ve NATO Anlaşması kapsamında siber terörizme yol açan saldırı ve faaliyetlere karşı üye ülkelerin hukuki davranış prosedürleri ve fiziki müdahaleleri tartışılmaya başlanmıştır. Siber saldırılara ilişkin bu alanda literatürde herhangi bir özgü düzenlemenin ve bağlayıcı sözleşmenin bulunmaması uzun zaman siber alemdeki saldırıların cevapsız kalmasına yol açmıştır. Söz konusu alandaki boşluk fiziksel saldırılara karşı devletlerin verdiği cevaplara uygulanan uluslararası düzenlemelere kıyasen "hukuk a la carte" ilkesi doğrultusunda siber uzaydaki saldırı ve haksız fiillere de uygulanmıştır. Diğer taraftan uluslararası hukuktaki "due diligence" yani devletlerin kendi yetkileri altındaki sınırlarını diğer devletler aleyhinde kullandırtmama ilkesi de devletlerin ülke içi ve ülke dışı yetkileri doğrultusunda uygulanagelmiştir. Buna ek olarak sözleşmesel yükümlülüklere uyulması ile ilgili olan ahde vefa ilkesi ve zararın tazmin edilmesi gibi ilkeler siber uzamda uygulanabilecek genel ilkeler olarak ön plana çıkmıştır. Literatüre bakıldığında kimi yazarlar tarafından uluslararası hukukun siber uzam bağlamında işlenen fiillere de uygulanabileceği savunulmuştur. Buna ilişkin devletlerin söz konusu hukuk kurallarını uygulama yöntemlerine göre siber uzay hukukunun da gelişim kaydedeceği ifade edilmektedir. Karşıt görüşlü birtakım yazarlar ise siber uzayın kendine özgü yapısı gereği uluslararası hukuktan bağımsız olarak ele alınmasını ve yeni bir sözleşmenin imzalanması gerektiğini savunmaktadır. Ancak bu sözleşmenin devletler açısından bağlayıcı olup olmaması gerektiğine ilişkin literatürde ihtilaflar bulunmaktadır.

3.1. NATO Antlaşması Kapsamında Siber Saldırılarla Mücadele

Siber güvenlik alanında öncü uluslararası örgütlere bakıldığında NATO ön plana çıkmaktadır. NATO Anlaşması BM Şartı'nın bu anlaşmaya taraf devletlerce benimsenmesini ana ilke olarak ortaya koymuştur. NATO Anlaşması'nın 4. maddesinin siber saldırı durumlarında tarafları harekete geçirebileceği değerlendirilmektedir.

> *Madde 4- Taraflardan herhangi biri, Taraflardan birinin **toprak bütünlüğü, siyasi bağımsızlığı ya da güvenliği**nin tehdit edildiğini düşündüğü zaman, **tüm Taraflar birlikte danışmalarda** bulunacaklardır.*

Söz konusu maddede güvenlik, siyasi bağımsızlık ve toprak bütünlüğü hususlarında tehditlerin oluşması durumunda taraf devletlerin birbirlerine danışmada bulunması düzenleme altına alınmıştır (Euractiv, 2008). Diğer taraftan NATO Anlaşması'nın 5. maddesi, madde lafzında geçen bölgeler içindeki üye devletlere yönelecek herhangi bir saldırı durumunda diğer devletlerin bu saldırıyı kendilerine yönelmiş sayarak BM Şartı 51. maddesi ile birlikte karşı saldırı veya savunma hareketlerinde bulunacaklarını düzenlemektedir. Bu kapsam dahiline siber saldırıların girip girmeyeceği, saldırganın tespiti ve karşı koyma hususları uluslararası literatürde tartışma konusu olmaktadır (NATO, 1949).

> *Madde 5- Taraflar, Kuzey Amerika'da veya Avrupa'da içlerinden bir veya daha çoğuna yöneltilecek **silahlı bir saldırı**nın hepsine yöneltilmiş bir saldırı olarak değerlendirileceği ve eğer böyle bir saldın olursa BM Yasası'nın 51. Maddesinde tanınan **bireysel ya da toplu öz savunma hakkı**nı kullanarak, Kuzey Atlantik bölgesinde güvenliği sağlamak ve korumak için bireysel olarak ve diğerleri ile birlikte, **silahlı kuvvet kullanımı** da dahil olmak üzere gerekli görülen eylemlerde bulunarak saldırıya uğrayan Taraf ya da Taraflara yardımcı olacakları konusunda anlaşmışlardır. Böylesi herhangi bir saldırı ve bunun sonucu olarak alınan bütün önlemler derhal Güvenlik Konseyi'ne bildirilecektir. Güvenlik Konseyi, uluslararası barış ve güvenliği sağlamak ve korumak için gerekli önlemleri aldığı zaman, bu önlemlere son verilecektir.*

Söz konusu madde NATO üyesi ülkelerin silahlı bir saldırıya uğramaları durumunda kendi aralarında dayanışma esasına dayanan müşterek bir anlaşma olarak ön plana çıkmaktadır.

Bu madde uyarınca tekil veya çoğul olarak saldırı yapan tarafa karşı koyulacağı ve bunun BM Yasası 51. maddesi dayanak alınarak hayata geçirileceği ifade edilmektedir. Yine saldırıların silahlı olarak gerçekleştirilmesi de bu madde bağlamında kapsam dahilinde ele alınmış ve bildirim merci olarak Güvenlik Konseyi belirlenmiştir. Güvenlik Konseyi'nin harekete geçmesiyle beraber devletlerin aldığı önlemlere son verilmesi gerekliliği madde metninin son lafzında ifade edilmiştir.

3.2. BM Sözleşmesi Kapsamında Meşru Müdafaa ve Kuvvet Kullanımı

Uluslararası hukuk kuralları çerçevesinde saldırıya uğranılması durumunda devletlerin kendini savunma hakkı olarak nitelenen kuvvete başvurma hakkı (jus ad bellum) ve söz konusu hakkın kullanımında uyulması gereken kurallar dizininin (jus in bello) siber saldırılara karşı uygulanması konusu tartışmalıdır. Öyle ki bu alanda silahlı çatışma hukukuna ilişkin kurallar uygulanabilmekte ve saldırıların devletlere isnat edilmesine ilişkin olaylarla karşılaşılabilmektedir. Söz konusu tartışmalar çeşitli toplantı ve forumlarda ele alınmış ancak somut olarak bir neticeye erişilememiştir. Bununla birlikte ihtilafa konu husus uluslararası kuruluşlar tarafından yıllar içinde etraflıca ele alınmıştır. Siber güvenliğe ilişkin öncü uluslararası kuruluşlardan olan Birleşmiş Milletler bünyesinde de 1980 yılında siber güvenliğe yönelik çalışmalar yapılmaya başlanmıştır. Ancak bu zamana kadar siber alanda bir mevzuat eksikliği bulunmakla beraber konvansiyonel saldırılara uygulanan 1945 tarihli Birleşmiş Milletler Sözleşmesinde üye devletlerin kuvvet kullanma yasağı düzenleme altına alınmıştır. Öyle ki Sözleşmenin 2. maddesinin dördüncü fıkrasına göre uluslararası ilişkilerde hem toprak bütünlüğüne hem de siyasi bağımsızlıklara karşı saldırı durumlarında ulusal sınırlar haricinde kuvvet kullanılmasına başvurulamayacağı öngörülmektedir. Bu kapsamda istisnai haller dışında devletler, silahlı saldırı durumunda askeri güçlerini harekete geçirmeyeceklerine dair taahhütte bulunmuşlardır. Söz konusu istisnai haller ise Sözleşmenin 51. maddesinde düzenlenmiştir (United Nations, 1945):

> Madde 51- *Bu Antlaşmanın hiçbir hükmü¸ Birleşmiş Milletler üyelerinden birinin* ***silahlı bir saldırı****ya hedef olması halinde, Güvenlik Konseyi uluslararası barış ve güvenliğin korunması için gerekli önlemleri alıncaya dek, bu üyenin doğal olan* ***bireysel ya da ortak meşru savunma hakkı****na halel getirmez. Üyelerin bu meşru*

savunma hakkını kullanırken aldıkları önlemler hemen Güvenlik Konseyine bildirilir ve Konseyin işbu Antlaşma gereğince uluslararası barış ve güvenliğin korunması ya da yeniden kurulması için gerekli göreceği biçimde her an hareket etme yetki ve görevini hiçbir biçimde etkilemez.

Bu maddede üye devletlerden birisinin silahlı saldırıyla karşı karşıya kalması durumunda Güvenlik Konseyi tarafından önlemler alınıncaya kadar meşru müdafaa hakkının kullanılması yasaklanmamaktadır. Yani meşru müdafaa sınırı üye devletlerin saldırılara karşı kendisini savunmasında istisnai hallerin ilkini oluşturmaktadır. Diğer istisnai hal ise Sözleşmenin yedinci bölümünde düzenlenmiş olan Güvenlik Konseyi kararları kapsamında hayata geçirilmektedir. Bu kararlar siyasi bağımsızlık durumlarında yahut ülkelerin toprak bütünlüğüne karşı yapılan saldırı durumlarında hayata geçirilerek meşru müdafaaya vücut verebilmektedir (United Nations, 1945). Söz konusu saldırılar askeri saldırılar, nükleer saldırılar ve biyolojik saldırıları içine almaktadır. Bu kapsamda meşru müdafaa kapsamında devletler tarafından kuvvet kullanma amaçlı olarak siber saldırıların da kullanılabileceği değerlendirilmektedir. Bu durumda meşru müdafaanın gereklilik ve orantılılık şartları saldırılara karşı siber saldırılar ile cevap verilmesi kapsamında da uygulama alanı bulacaktır. Gerçekleştirilen saldırı halihazırda devam eden bir saldırı olmalı ve buna ilişkin yapılan siber savunma saldırı ile orantılı olmalıdır. Yine söz konusu yönteme son tahlilde herhangi bir barışçıl çözüme gidilemeyen durumlarda başvurulmalıdır.

Bununla birlikte BM Şartı'nın 2. maddesinin dördüncü fıkrasında yer verilen kuvvet kullanma yasağının sadece üye devletleri bağlayıcılığı noktasında söz konusu madde fıkrasının kanun koyucular tarafından "opinio juris sive necessitatis" kuralına göre konulmuş olması dolayısıyla üye olmayan devletleri de bağlayıcı olduğu değerlendirilmektedir.

Madde 2-(4) Tüm üyeler, uluslararası ilişkilerinde gerek herhangi bir başka devletin ***toprak bütünlüğüne ya da siyasal bağımsızlığa*** *karşı, gerek Birleşmiş Milletlerin amaçları ile bağdaşmayacak herhangi bir biçimde* ***kuvvet kullanma*** *tehdidine ya da kuvvet kullanılmasına başvurmaktan kaçınırlar.*

Bahsi geçen hukuk kuralı, örf ve âdet şeklindeki yazısız kuralların da kanuni bir zorunluluk olduğuna dair fikir birliği içerisinde oluşturulmuş ve zamanla uygulanagelmiş

olması dolayısıyla sözleşmelere taraf olmayan devletleri de bağlaması esasına dayanmaktadır (Yayla, 2013b). Bu maddede devletlerin toprak bütünlüğü ve siyasal bağımsızlıkları kuvvet kullanma yasağı sınırının belirlenmesinde ana unsuru oluşturmuştur. Yine burada kuvvet kullanımına yol açan eylemler ve silahlı saldırılar devletlerin toprak bütünlüğü ve siyasal bağımsızlığına yönelik müdahale yasağının temelini oluşturmaktadır.

Diğer taraftan ABD yetkililerince hasmane niyet çerçevesinde askeri olarak ABD kuvvetlerine yönelmiş cana ve mala ilişkin saldırıların yakın güç kullanımı tehdidi oluşturduğu, bu sebeple de henüz saldırı fiziksel olarak gerçekleşmeden dahi "erken meşru müdafaa" kapsamında ele alınarak savunma amaçlı cevap verilebileceği ifade edilmektedir. Söz konusu husus, AB kapsamında daha dar şekilde ele alınmakta ve halihazırda gerçekleşmekte olan saldırılara karşı meşru müdafaada bulunulabileceği değerlendirilmektedir. Tallinn Manual uzmanlarının yorumlarında erken meşru müdafaanın siber saldırılara da uygulanabileceği, "son olası fırsat penceresi standardı" bağlamında siber saldırganların harekete geçmesiyle saldırılan devletin kendisini savunamayacak pozisyona düşebilecek olması halinde erken meşru müdafaa şartının yerine geleceği değerlendirilmektedir. Söz konusu meşru müdafaa siber saldırıların sona ermesine rağmen tekrarlama ihtimalinin yüksek olması durumunda da başvurulacak savunma yöntemi olarak ön plana çıkmaktadır. Diğer taraftan meşru müdafaanın kullanımı için öncelikle devlete isnat edilebilen mevcut bir saldırı olması ve uluslararası insancıl hukuk dahilinde hareket edilmesi gerektiği değerlendirilmektedir. Ancak devlet dışı aktörlerin de saldırılarına karşı belirli şartların gerçekleşmesi durumunda meşru müdafaa kullanılabilmektedir. Söz konusu devlete isnat hususu doğrudan veya dolaylı olarak gerçekleşebilmektedir. Öyle ki devlet adına işlem ve eylemde bulunan kişi ve organlar için doğrudan atfedilebilme kapsamında devletin sorumluluğu olabileceği, "gerekli özen ilkesi" çerçevesinde söz konusu işlem ve eylemlerin devletçe engellenememesi nedeniyle dolaylı devlet sorumluluğunun oluşabileceği ifade edilmektedir. Bu kapsamda gerekli savunma devlet tarafından "aktif" ve "pasif" şekilde gerçekleştirilebilmekte, verilen zararı azaltıcı nitelikte "hafifletici karşı saldırı" ve saldırganın cezalandırılmasına hizmet eden "denkleştirici karşı saldırı" ortaya çıkmaktadır. Ancak uluslararası hukuk bağlamında devletler için kendilerini savunmaya ilişkin tanınan yöntem yalnızca "hafifletici karşı saldırı"lardır (Kabano, 2023).

3.3. Devletlerin Uluslararası Sorumluluğu Kapsamında Siber Saldırılar

Uluslararası hukukta saldırılar söz konusu olduğunda devletlerin sorumluluğuna ilişkin belirli kuralların göz önünde bulundurulduğu görülmektedir. BM Uluslararası Hukuk Komisyonu tarafından 28 Ocak 2002 tarihinde yayımlanan A/RES/56/83 (Responsibility Of States For Internationally Wrongful Acts) isimli belge uluslararası alanda işledikleri haksız fiiller dolayısıyla devletlerin sorumluluğuna gidilen hükümler içermektedir. Bunun yanı sıra uluslararası örgütlerin de işledikleri haksız fiiller dolayısıyla bu belgede sorumluluk atfedilebilen kuruluşlar olarak yer aldığı görülmektedir (United Nations, 2002). Öyle ki bahse konu haksız fiillerin meydana gelmesi için belirli şartların oluşması gerekmektedir. Bu şartların en başında ihlale konu uluslararası yükümlülüklerin meri mevzuatta mevcut olan bir normun ihlalinden kaynaklanması gerekliliği gelmektedir. Bu alanda uluslararası antlaşmalar, örf ve âdet kuralları ve teamül hukuku kuralları ön plana çıkmaktadır. Söz konusu kurallara ilişkin yapılan ihlaller neticesinde devletlerin ve uluslararası örgütlerin sorumluluğuna gidilebilmektedir. Bunların yanı sıra isnat meselesinde zorunlu unsurlardan bir tanesi de haksız fiilin varlığı ve bu varlığın ispatı meselesidir. Söz konusu fiil, uluslararası normların ve yürürlükteki mevzuatın tanımladığı şekilde haksız fiil içermelidir. Bu kapsamda uluslararası yükümlülüklerin ihlaline yol açan davranışlar haksız fiil sonucunu doğurmaktadır. Aynı zamanda bu haksız fiil ispat edilmezse karşı tarafın söz konusu fiili dolayısıyla sorumluluğuna gidilememektedir. A/RES/56/83 belgesinde yukarıda bahsedilen kurallara ve hususlara yer verilmekte, bununla birlikte Uluslararası Daimî Adâlet Divanı (UDAD) ve Uluslararası Adâlet Divanı (UAD), A/RES/56/83'nin 1. maddesinde yer alan haksız fiile ilişkin hususlarda kararlar vermektedir (Erkiner, 2010). Bir Devletin uluslararası hukuka aykırı eylemlerinden sorumluluğu başlıklı söz konusu madde aşağıdaki şekilde çevrilebilecektir:

> *Madde 1- Bir Devletin her uluslararası hukuka aykırı eylemi, o Devletin uluslararası* ***sorumluluğunu*** *doğurur.*

Haksız fiilin unsurları ise aynı belgenin "Bir Devletin uluslararası hukuka aykırı eyleminin unsurları" başlıklı 2. maddesinde düzenlenmektedir.

Madde 2- Aşağıdaki eylem veya ihmallerden oluşan bir davranış söz konusu olduğunda, bir Devletin uluslararası hukuka aykırı eylemi söz konusudur:

*(a) Uluslararası hukuka göre **Devlete atfedilebilmesi**, ve*
*(b) Devletin uluslararası bir **yükümlülüğünün ihlalini** teşkil etmesi.*

Burada bahse konu fiilin devlete atfedilebilen icrai veya ihmali davranışla oluşabileceği ifade edilmektedir. Önemli olan bir diğer husus ise devlete isnat edilebilirlik unsurunun oluşmasıdır. Bu isnat doğrultusunda uluslararası hukukun bir yükümlülüğünün ihlal edilmesi gerekmektedir. Diğer taraftan siber saldırıların yapısı gereği atfedilebilirlik problemi oluşturduğu düşünüldüğünde kaynağı tespit edilemeyen saldırıların silahlı saldırı kabul edilse dahi devletler arası misillemeye ilişkin davranışların kime karşı kullanılacağı konusunda da belirsizlik bulunmaktadır (United Nations, 1945).

A/RES/56/83'in "Tazminat" başlıklı 31. maddesinde yer verilen ihlale ilişkin hususlarda devletin verdiği zararlara yönelik tazminat yükümlülüğü düzenlenmektedir. Söz konusu madde aşağıdaki gibidir:

Madde 31-
*1. Sorumlu Devlet, uluslararası hukuka aykırı eylemin neden olduğu zararı tam olarak **tazmin etme yükümlülüğü** altındadır.*
*2. Zarar, bir Devletin uluslararası hukuka aykırı eyleminin neden **olduğu maddi veya manevi** her türlü zararı içerir.*

Bu kapsamda söz konusu maddede ortaya çıkan zararın hem maddi hem de manevi boyutunun oluşabileceği ve tazminat yükümlülüğünün bu iki zarar türünü de kapsayıcı şekilde olabileceği düzenlenmektedir. Söz konusu madde hükmüne göre bir devlet verdiği zararlara ilişkin olarak tazmin yükümlülüğü ile karşılaşmaktadır. Çalışmanın ileriki bölümlerinde ayrıntılı olarak işlenecek devletin mali sorumluluğu çerçevesinde bu hükümler de göz önünde bulundurularak bir değerlendirme yapılacaktır.

A/RES/56/83'in "Bir Devletin organlarının yönetimi" başlıklı 4. maddesi kapsamında devlet organlarının fiillerinden ötürü devletin sorumluluğuna gidilebilmektedir. Bu doğrudan devlete isnat yapılabilecek bir yoldur.

> *Madde 4-*
> *1. Herhangi bir devlet organının davranışı; yasama, yürütme, yargı ya da diğer işlevleri yerine getirip getirmemesine, merkezi hükümetin ya da devletin bölgesel bir birimin organı olarak nitelendirilip nitelendirilmemesine ve devlet örgütlenmesindeki konumuna bakılmaksızın uluslararası hukuk uyarınca o* ***devletin bir eylemi olarak kabul*** *edilir.*
> *2. Organ, devletin iç hukuku uyarınca bu statüye sahip olan herhangi bir kişi veya kuruluşu kapsar.*

Bununla birlikte metnin "Devlet otoritesinin unsurlarını kullanan kişi veya kuruluşların davranışları" başlıklı 5. maddesi kapsamında kamu gücü yetkilerinin kullanımı sırasında devlet organı olmayan ancak bir kişi yahut birim tarafından uluslararası hukukun ihlali niteliği taşıyan davranışın meydana getirilmesi sonrası, söz konusu davranış bu kişi veya birime atfedilebiliyorsa fiilin devlet adına işlenmiş olduğu göz önünde tutularak isnat yine devlete yapılabilmektedir. Bahse konu 5. madde aşağıdaki gibidir:

> *Madde 5- Bu belgenin 4. maddesi kapsamında devletin bir organı olmayan ancak söz konusu devletin yasaları tarafından hükümet yetkisinin unsurlarını kullanma yetkisine sahip bir kişi veya kuruluşun davranışı, söz konusu kişi veya kuruluşun belirli bir olayda bu sıfatla hareket etmesi koşuluyla, uluslararası hukuk kapsamında devletin bir eylemi olarak kabul edilir.*

Devlete isnat edilebilen bir diğer noktayı ise devletin fiili olarak kabul edilen A/RES/56/83'in "Bir devlet tarafından başka bir devletin emrine verilen organların yürütülmesi" başlıklı 6. maddesinde düzenlenen bir devlet tarafından başka bir devletin emrinde görevlendirilen organların uluslararası hukuktaki ihlal davranışları oluşturmaktadır. Söz konusu maddenin işlerlik kazanması için görevlendirilen organ emri altındaki devletin kamu gücü yetkilerini kullanırken bu ihlal davranışının gerçekleştirilmesi gerekmektedir. Bahse konu madde aşağıdaki gibidir:

Madde 6- Bir devlet tarafından diğer bir devletin emrine verilen bir organın davranışı, organın emrine verildiği devletin hükümet yetkisinin unsurları kullanılırken hareket ediliyorsa, uluslararası hukuk uyarınca önceki devletin bir eylemi olarak kabul edilir.

Bunun yanı sıra A/RES/56/83'in 7, 8, 9 ve 10. maddeleri uluslararası hukuka göre devletin fiili olarak kabul edilen durumlarda devletin sorumluluğuna gidilebilen isnat unsurlarını içermektedir (United Nations, 2002). Bu minvalde kişi, kurum veya organ olarak emir altında görev yapanların yetki aşımı ya da talimatlara aykırı davranışları varsa, devletin denetimi altındayken söz konusu ihlaller oluşmuşsa, resmi otoritelerin yokluğu durumunda kamu gücü yetkisi ihlale mahal verecek şekilde kullanılmışsa veya A/RES/56/83'te verilen şartlar altında bir isyan hareketi veya benzeri davranışta bulunulmuşsa devletin fiili olarak kabul edilen bu davranışlar devletlerin sorumluluğuna gidilerek isnada konu olabilmektedir.

3.4. Siber Saldırıların Silahlı Saldırı Sayılması Tartışması

Bir siber saldırının silahlı saldırı sayılması onun BM Şartı 51. maddesi kapsamında meşru müdafaa için saldırı yapılan devlete meşru gerekçe kazandıracağı anlamına gelmektedir. Bu kapsamda önem arz eden Tallinn Manual'in 13. kuralı, silahlı saldırı eşiğini geçen bir siber saldırının meşru müdafaaya vücut vereceğini ve söz konusu saldırının silahlı saldırı olup olmadığının değerlendirilmesinde saldırı sonucunun etkisinin ve ölçeğinin belirleyici olduğunu aktarmaktadır (NATO CCDCOE, 2017). Söz konusu kılavuza ilişkin uzman yorumlarında UAD'nin davalarında ifade edilen ve özellikle kimyasal, biyolojik ve nükleer silahların kinetiklik özelliği bulunmasa dahi silahlı saldırıya vücut verdiği, siber saldırılarda kullanılan araçların da bu kapsamda değerlendirilmesi gerektiği ifade edilmektedir. Etki temeli kapsamında da söz konusu husus ele alınmakta, "can kaybına ve mülkiyete yönelik" araç kullanımının silahlı saldırı için yeterli olacağı aktarılmaktadır. Burada en önemli husus ise gerçekleştirilen saldırının insan hayatına yönelmesi veya mülkiyete ilişkin zarar doğurmasıdır. Bunun yanı sıra araç temelli yaklaşımın benimsenmesi durumunda kullanılan araç siber saldırının silahlı saldırı olmasını belirlemekte, hedef temelli yaklaşımda ise fiziksel hasara ilişkin değerlendirmeden bağımsız olarak siber saldırının

kritik altyapılara yönelmesi ve bu altyapıyı devre dışı bırakmak amacında olması silahlı saldırı sayılması için yeterli olmaktadır (Kabano, 2023).

Siber saldırıların silahlı saldırı olarak sayılması tartışmasında doktrinde üç farklı görüş yer almaktadır. Bu yaklaşımlar araç temelli, hedef temelli ve etki temelli olarak sıralanmaktadır. Araç temelli yaklaşım, BM Şartı lafzında geçen silahlı saldırının oluşması için askeri silah kullanımı olması gerektiği düşüncesi üzerinde yoğunlaşmaktadır. Ancak bu yorum yapıldığında BM Şartı kapsamında siber saldırıların kapsam dışı kaldığı söylenebilir. BM Uluslararası Adalet Divanı Nikaragua kararında yer verilen "sufficient gravity" kıstası söz konusu seviyeye erişildiğinde siber saldırının kapsam dahilinde olacağını açıklar niteliktedir. Ancak bunun olması için siberin araç olarak kullanıldığı ve konvansiyonel olarak da bilişim sistemi içeren komuta merkezi gibi fiziksel unsurların zarar gördüğü hibrit saldırıların olması gerekmektedir. İkinci yaklaşım türü olan hedef temelli yaklaşımda ise, siber saldırıların muhtemel zarar verme potansiyeli üzerinden hareket edilmektedir. Bu yaklaşımda meşru savunma için önem seviyesinin kritiklik gerektirmesi zorunludur. Devletlere yönelik yapılan kritik altyapı saldırıları bu yaklaşım vasıtasıyla gelen saldırılara karşı savunmanın meşruluğu için yeterli seviyededir. Literatürde yer alan son yaklaşıma bakıldığında etki temelli yaklaşım olduğu görülmektedir. Bahse konu yaklaşım, siber saldırıların karşı tarafta bıraktığı etki üzerinden bir anlayış geliştirmiştir. Burada karşılaşılabilecek problem etki ağırlığının hangi yöntemlerle ve nasıl ölçüleceğidir (Yayla, 2013b).

Tallinn Manual (Tallinn El Kitabı) kapsamında Tallinn modeli olarak ifade edilen yaklaşım söz konusu etkinin ölçülmesi bakımından önemli bir fikir sunmaktadır. 2013 yılında yazıya aktarılan söz konusu modele ait el kitabı siber saldırılar özelinde uluslararası hukukun uygulanabilirliğini incelemektedir. Bu kitap 2017 yılında güncellenmiş ve NATO tarafından da desteklenmiştir (NATO CCDCOE, 2017). Schmitt (1999) tarafından söz konusu yaklaşıma ilişkin olarak ortaya konulan modelde bazı kıstaslar ön plana çıkmaktadır. Bunlar sırasıyla; yıkıcılık, yakınlık, illiyet bağı, istilacılık, ölçülebilirlik, meşruluk beklentisidir. Yıkıcılıktan anlaşılması gereken husus oluşan zarara ilişkin büyüklüktür. Saldırı sonucunda oluşan etkinin yoğunluğu ve şiddeti burada belirleyici ölçüttür. Diğer taraftan olayın gerçekleştiği zaman da yıkıcılık için belirleyici unsur olmaktadır. Siber saldırılar söz konusu yoğunluk ve şiddette gerçekleştiğinde kuvvet kullanımı olarak

yorumlanmaktadır. Yakınlık kıstası ile saldırı sonrası zararın oluştuğu sürenin başlangıcı ifade edilmek istenmiştir. Burada sonucun kısa sürede oluşmuş olması kuvvet kullanımı kabulü için önemlidir. Bir siber saldırının ani şekilde karşı devletin kritik altyapılarına veya hayati önem taşıyan varlıklarına zarar vermesi, mantık bombası gibi zamanı belli olmayan veya gelişmiş kalıcı tehdit tipindeki uzun dönemli siber saldırılara göre kuvvet kullanımı değerlendirmesinde kolaylaştırıcı etken olmaktadır. İlliyet bağı, nedensellik olarak da bilinen ve karşı tarafa suçun atfedilebilirliğini sağlayan unsur olarak tanımlanabilir. Neden ve sonucun birbiriyle bağlantısının güçlü olduğu olaylarda kuvvet kullanımı yorumu daha kolay yapılmaktadır. Bir siber saldırı sonucunda karşı tarafta zayiat veya ölüm yaşanması buna örnek olarak verilebilir. İstilacılık, saldırıya uğrayan tarafın sınır ihlalinin derecesidir. Buradaki kıstas, güvenlik derecesi yüksek olan sistemlerin seviyesi düşük sistemlere göre ele geçirilmesinin istila düzeyini artırıcı özellikte olmasıdır. Ölçülebilirlik ise zarara ilişkin somut şekilde gerçekleştirilen tespitlerle açıklanabilir. Siber saldırılara ilişkin istatistiki verilerin ortaya konulabilir olması ve objektif olarak veriye ulaşılabilirlik kuvvet kullanımı nitelemesinde önem arz etmektedir. Son kıstas olan meşruluk beklentisi, siber saldırıların kapsam dahiline alınmasının istisnai hüküm şekilde değerlendirilmesinin bir gereğidir. Öyle ki burada kastedilen husus, yapısı gereği düzenlemeye tabi tutulmayan yasaklar dışındaki davranışların yasal olduğu beklentisidir. Uluslararası hukukta ve örf adet hukukunda yasaklanmamış davranışlar mefhumu muhalifi yorum yapıldığında meşru olarak kabul edilmektedir.

Siber saldırılara ilişkin yorum yapıldığında ise devletlerce kuvvet kullanma olarak yorumlanması pek muhtemel değildir. Ancak bu yorumun devletler tarafından kümülatif şekilde siber saldırının siyasi olarak sonuçlarına, belirli bir askeri operasyonun ayrılmaz parçası olup olmadığına, saldırıyı düzenleyen kişi veya kurumun yapısı ve niteliğine, hedef alınan unsurların kritiklik seviyesine bakılarak yapılması gerekmektedir. Bu yorumla birlikte kritiklik içeren bir sonuca ulaşılması durumunda kuvvet kullanımı değerlendirmesi yapılabilecektir. Askeri karakter ölçütü, bu noktada bir siber saldırının askeri bir harekatla ilgili ve onun bir parçası konumunda olması durumunda kuvvet kullanma yorumu için önemli bir etken olmaktadır. Devletin rolü kıstasında ise siber saldırının bir devlet tarafından yapılıp yapılmadığı ve saldırı ile olan yakın ilişkisi göz önünde bulundurulmaktadır. Söz konusu kıstaslara ek olarak meşru müdafaanın zorunlu unsurları konumunda bulunan gereklilik ve orantılılık ilkelerinin de BM Şartı 51. madde kapsamında örfi hukuk kuralları

olarak dikkate alınması gerekmektedir (Schmitt, 1999). Şunu da belirtmek gerekir ki söz konusu silahlı saldırılara karşı meşru müdafaada bulunma sınırı BM Şartında bahsi geçtiği üzere BM'nin kolektif olarak tedbir alıp saldırıların önüne geçmesine kadar olan sürede geçerlidir.

Devletler arası mücadelelerde bir devlet tarafından karşı tarafın aleyhine olacak şekilde ayaklanan isyancılara silah ve mühimmat sağlaması, finansal yardımda bulunulması, lojistik, eğitim ve bilgi desteği sağlanması BM Antlaşmasının kuvvet kullanma yasağı ve diğer devletlerin iç işlerine karışmama ilkesine aykırıdır. Diğer taraftan söz konusu yardımlar "silahlı saldırı" olarak değil kuvvet kullanma olarak kabul edilebilecektir. Öyle ki söz konusu eylemler dolayısıyla hak kaybı ve menfaat ihlali olan devletlerin, BM Antlaşması kapsamında devletlere sunulan meşru müdafaa ile kuvvet kullanma hakları ortadan kalkmaktadır. Tallinn Manual kapsamında silahlı saldırı seviyesine gelmeyen kuvvet kullanımına karşı cevap vermek isteyen devletler orantılı karşı tedbirleri devreye sokmak zorundadır (Schmitt, 1999).

Burada dikkat çekilmesi gereken nokta silahlı saldırıların kapsamına alacağı saldırıların çeşitleri ve düzeyleridir. Bu alanda muğlaklık olmakla birlikte siber güvenlik açısından değerlendirildiğinde siber saldırıların bu kapsamda değerlendirilip değerlendirilemeyeceği de tartışma konusudur. BM Şartı 51. madde kapsamında "silahlı saldırı" ifadesinin temel alınması nedeniyle sadece saldırı kapsamındaki fiillerin değil bunların nitelikli hali olarak kabul edilebilecek silahlı saldırıların da uygulamaya alınacağı belirtilmek istenmiştir. Fakat silahlı saldırı açık şekilde tanımlanmadığından bu ifadeden ne anlaşılması gerektiği belirsizlik içermektedir. Söz konusu ifade değerlendirmeye alınırken meşru müdafaanın zorunlu unsurları olarak kabul edilen gereklilik, aciliyet ve orantılılık ilkelerinin de göz önünde bulundurulması gerekmektedir. Saldırıdan farklı olarak silahlı saldırı ifadesi BM Şartına göre meşru savunma hakkı tanımaktadır. Günümüzde siber saldırıların etki düzeylerine bakıldığında sadece sanal ortamda kalmayarak fiziksel ortamı da etkilediği bir gerçektir. Devletlere ait önemli hizmet merkezlerinin, kritik altyapıların, tesislerin ve finans merkezlerinin hedeflenerek zarara uğratıldığı siber saldırılar sonucunda büyük yıkımlara yol açılmaktadır. Dahası bu saldırılar vasıtasıyla yaratılan etkiler neticesinde vatandaşların ölümü veya mal kayıpları söz konusu olabilmektedir. Söz konusu etkiler, devletleri siber saldırıların BM Şartı kapsamına alınmasına ilişkin açıklamalar

yapmaya itmiştir. Öyle ki bu bağlamda ABD'nin güvenlik birimine haiz devlet kanadından yapılan açıklamalarda BM Şartı'nın 2/4 maddesinin geniş yoruma tabi tutularak siber saldırıları da kapsaması gerektiği ifade edilmiştir (Bumiller ve Shanker, 2012).

Siber saldırıların bu etkilerine karşılık küresel olarak hukuk dünyasında oluşturulmuş, siber saldırıları önlemek ve caydırıcılık sağlamak amaçlı herhangi bir bağlayıcı mevzuat bulunmamaktadır. Söz konusu boşluğun bulunduğu bir ortamda mevcut silahlı saldırılara uygulanan uluslararası hukuk normlarının bu alana kıyasen uygulanması tartışılan bir konudur. Birtakım yazarlara göre savaş hukuku ve silahlı çatışma hukuku kapsamında inceleme yapıldığında siber saldırıların konvansiyonel saldırılarla aynı kapsamda yer alamayacağı ve bununla ilgili mevzuatın da kıyasen uygulanamayacağı belirtilmektedir. Bu fikrin karşıtlarına göre ise bilgi ve iletişim teknolojilerinin gelişmesiyle konvansiyonel savaş ortamının yerini sanal savaşlara bırakmasıyla söz konusu saldırılar kapsamında BM Şartı 51. maddesi çerçevesinde meşru savunma kurallarının uygulanabileceği ifade edilmektedir. Kuvvet kullanma hakkının (jus ad bellum) siber saldırılara karşı kullanımında savaş hukukuna ilişkin normların göz önünde bulundurulması gerekmektedir. Bilgi ve iletişim teknolojilerindeki gelişimle birlikte "silahlı kuvvet kullanma" ifadesi de farklı bir boyuta evrilmiştir. Buradaki silahtan anlaşılması gereken husus yine tartışma konusu olmaktadır. Siberin araç olarak kullanıldığı suçlarda, bu araçların silah olarak kabul edilmesi meselesi de yine aynı bağlamda gündeme gelmektedir (Yayla, 2013b).

1949 tarihli Cenevre Sözleşmesi ve Ek Protokol I kapsamında yapılan silahlı çatışma tabirinden devletler arasındaki bahse konu çatışmanın askeri bir özellik taşıdığı, askeri olarak öldürme, yaralama veya mülkiyete zarar unsurlarının anlaşıldığı ve ihtilaf halinde insancıl hukukun uygulama alanı bulacağı ifade edilmiştir. Sonuç odaklı yaklaşım doğrultusunda özellikle de devletlerin kritik altyapılarına yapılan siber saldırıların şiddetli neticeleri sebebiyle hasmane davranış olarak nitelendirilebileceği değerlendirilmektedir. Söz konusu saldırının belirli saldırı eşiğini geçmesi ve ciddi sonuçlara sebep vermesi dolayısıyla uluslararası insancıl hukuka tabi olması, Ek Protokol I'in 52. Maddesi doğrultusunda askeri hedeflerin etkisizleştirilmesine kıyasen uygulama alanı bulmaktadır. Diğer taraftan savaş hukuku veya silahlı çatışmalar hukuku bağlamında siber savaşların ele alınması hususu tartışmalıdır. Siber savaşların bilgi savaşını da içine alan bir yapıda silahlı çatışma hukuku kapsamında değerlendirilmesi için çatışmaya ilişkin yoğunluk unsurunun belirli bir seviyede

olması gerekmektedir. Yoğunluk unsurunun ilk ayağını oluşturan silahlı kuvvet sayılması, diğer kriteri sağlayabilmesi için de siber savaşın taraflarının niteliği önem arz etmektedir. Bu bağlamda savaş öncesi haklı gerekçeleri içeren uluslararası hukuk "jus ad bellum" ve savaş sırasında haklı gerekçeleri içeren uluslararası hukuk "jus in bello" söz konusu olduğunda siber savaşlar için uygulama alanı bulacağı değerlendirilmektedir (Kabano, 2023).

BM Uluslararası Adalet Divanı tarafından 2003 yılında karara bağlanan Petrol Platformları davası kapsamında "Olaylar Birikimi Teorisi (Nadelstichtaktik)" çerçevesinde belirli bir saldırının arkasından gerçekleştirilen ilave saldırıların silahlı saldırı olarak nitelendirilmesi olasılığı gündeme getirilmiştir. Söz konusu teori siber saldırılar bağlamında değerlendirildiğinde, ardışık saldırı kümesinin askeri alanda silahlı saldırıya vücut vermesinden yola çıkarak hukuka aykırı güç kullanımı içeren ardışık siber saldırıların da silahlı saldırı eşiğini yakalayabileceğinin göz önünde bulundurulabileceği görülmektedir (Kabano, 2023). Söz konusu saldırılara örnek olarak verilebilecek DDoS saldırıları ve botnet saldırıları tek başına olmasa da ardışık olarak işlenildiğinde silahlı saldırıya vücut verebilecektir. Bu kapsamda silahlı saldırıya cevaben saldırıya uğrayan devletler tarafından meşru müdafaa haklı gerekçeyle gerçekleştirilebilecektir.

3.5. Tallinn Manual ve Dava Örnekleri Kapsamında Siber Saldırılar

Siber güvenliğin sağlanmasında kutuplaşan siyasi dünyada devletlerin bir araya gelerek siber saldırı ve suçlara karşı çözüm üretmeyi amaçladığı, karşılıklı politikalara ilişkin görüşlerin bildirilerek stratejik amaçların ortaya konulduğu iki büyük organizasyon bulunmaktadır. Siber güvenliğin mevzuat kapsamında ve fiili olarak güçlendirilmesi ihtiyacını doğuran devletler arası siber savaşlarla ilgili BM Genel Kurulu nezdinde Silahsızlanma ve Uluslararası Güvenlik Komitesi bulunmaktadır. Bu Komite etrafında şekillenen alt gruplardan Silahsızlanma Araştırma Enstitüsü ve Terörle Mücadele Uygulama Görev Grubu söz konusu alanda siber güvenliğin sağlanmasına yönelik çeşitli faaliyetler yürütmektedir.

Diğer taraftan uluslararası düzenlemelerin müşterek bir siber ortamda hayata geçirilmesi amacıyla daha çok askeri alanda merkezileşen ancak sonrasında diğer alanlarda da çalışmalar yapan NATO, devletler arası bir yapıda alanında uzman kişilerden oluşan gruplar oluşturmuştur. 2007 yılında Estonya'ya yönelik saldırılar sonrasında siber ortamın bir savaş alanı olarak ortaya çıkışının akabinde 2008'de NATO tarafından Siber Savunma Mükemmeliyet Merkezi hayata geçirilerek siber güvenlik için önemli bir araştırma merkezi meydana getirilmiştir. 2012 yılında söz konusu faaliyetler kapsamında NATO tarafından stratejik ve politik hedeflerin ortaya konulması amacıyla Ulusal Siber Güvenlik Çerçeve Kılavuzu yayımlamıştır (NATO, 2012). NATO'nun siber güvenliğe ilişkin genel bakış açısı konvansiyonel savaşların yerini siber savaşlara bıraktığı ve silahlı çatışma hukuku normlarının siber uzayda meydana gelen siber saldırılara da uygulanması yönündedir. Söz konusu çalışma alanında NATO'da siber strateji ve politikalar üzerinde çalışıldığı görülmektedir. Bu çerçevede NATO tarafından oluşturulan Tallinn Manual söz konusu politikaların ortaya konulması açısından büyük bir önem arz etmektedir. Burada yer alan görüşler resmi görüşler olmamakla birlikte NATO tarafından desteklenen stratejilere söz konusu belgede yer verilmektedir. Siber Savunma Mükemmeliyet Merkezi de Tallinn Manual politikaları doğrultusunda destekleyici görüşler vermektedir. Bunun yanı sıra NATO ve ABD Siber Komutanlığı da yine bu kılavuzun faydalı olduğuna dair görüş belirtmiştir. Siber savaşların dünya üzerindeki kutuplaşmış siyasi yapı üzerinde de etkili olduğu düşünüldüğünde bu savaşlarda baş aktör konumunda olan ABD hükümeti Tallinn Manual'e paralel görüşlerini paylaşarak uluslararası alanda teamülen oluşan normların siber savaşlar için de geçerli olması gerektiğini ifade etmiştir (Bolat, 2020).

Tallinn Manual, hüküm ve anlaşmaların uygulanamadığı durumlarda siber saldırılara ilişkin uygulanması öngörülen teamül hukuku yani örf ve âdet hukuku olarak nitelenebilecek belirli müesseseleri içermektedir. Bunlardan bir tanesi de Martens Kaydı (Hükmü) olarak literatürde kendisine yer bulan ve 1899 yılında düzenlemeye geçirilen 2 nolu La Haye Sözleşmesinin giriş kısmındaki kurallar dizinidir. Söz konusu hükme göre savaş hukukuna ilişkin düzenlemeler hayata geçirilene kadar; teamülen uygulanan kurallar, yerleşik insani ilkeler ve toplumsal normların oluşturduğu kuralların uluslararası savaş hukuku çerçevesinde uygulama alanı bulacağı öngörülmektedir. Burada anlatılmak istenen husus, bir boşluk durumunda kamu vicdanı emirlerinin vücut bulacağıdır (ICRC, 2024).

Tallinn Manual 2.0 kapsamında söz konusu kılavuzdaki ana görüş devletlerin kendi topraklarında gerçekleşen siber saldırılardan sorumlu olduğu ve siber altyapıları üzerinde yasama, yargı, yürütme gibi temel idari fonksiyonları yerine getirebilecek egemenliğinin bulunduğu şeklindedir. Bununla birlikte diğer devletlerin egemenliğinin ihlaline yol açan siber saldırıların devletler tarafından gerçekleştirilmemesi gerektiği hususuna vurgu yapılmaktadır. Söz konusu husus "devletin egemenliğini ihlal etme yasağı" adı altında ele alınmaktadır. Diğer taraftan "gerekli özen ilkesi" kapsamında Tallinn Manual 2.0 devletlerin diğer devletlerin zararına yol açacak siber operasyonlara karşı gerekli özeni göstermesi ve kendi siber altyapılarını siber saldırganlara kullandırmaması gerektiğini kurala bağlanmıştır. Söz konusu ilkenin uygulanması bağlamında siber altyapılarını kullandırmaması gereken devletin saldırıyı bilmesi ve önleyebilecek kapasiteye sahip olmasına ilişkin hususlar burada gündeme gelmektedir. Devlet egemenliğini ihlal etme yasağı yalnızca devletler bağlamında değerlendirilirken gerekli özen ilkesi çerçevesinde devlet dışı aktörlerin de siber saldırılarına karşı siber altyapıları koruma ve kullandırmama yükümlülüğü oluşmaktadır (NATO CCDCOE, 2017). Devletin siber altyapıları üzerindeki yetkisinin kendi ülkesinde başlayan veya başka ülkede başlasa bile kendi ülkesinde neticelenen, etkisi bakımından yüksek siber saldırıları kapsadığı değerlendirilmektedir. Bu kapsamda Tallinn Manual'de belirtilen "önemli derecede etki" hususu rekabet hukukunda ortaya çıkan ve siber uzama da uygulanabilen "de minimis" yani buradaki anlamıyla etki derecesi bakımından kısıtlı saldırıları kapsamamaktadır. Bununla beraber Tallinn Manual kapsamında siber saldırıların kaynağının bir devlet siber altyapısı olarak tespit edilmesinin söz konusu saldırının o devlete isnadı için yeterli olmadığı da değerlendirilmiştir.

NATO, BM ve AB ile operasyonel ilişkilere sahip olan Uluslararası İnsancıl Hukuk Enstitüsü (IIHL) çerçevesinde oluşturulan Sanremo El Kitabı ise askeri operasyonlara kıyasen ele alınan siber uzam bağlamında ortaya konulan angajman kuralları arasında bilgisayarlarla işlenen fiiller yer almıştır. Öyle ki enformasyona ilişkin anlaşmaların siber saldırılar kapsamında ele alınması gerektiği, hasmane niyet kapsamında siber saldırıların ciddi sonuçlar doğurabildiği, kinetik olmayan siber saldırıların hasmane niyet olarak belirlenmesinde ciddilik, doğrudanlık ve aciliyet unsurlarının göz önünde bulundurulması gerektiği değerlendirilmektedir. Bu kapsamda uluslararası insancıl hukukla beraber askeri alanda kullanılan angajman kuralları askeri zorunluluk, askeri ve sivil ayrımı ile verilen zarar çerçevesinde orantılılık olarak belirlenmiştir. Söz konusu unsurlar doğrultusunda siber

uzayda gerçekleştirilen siber saldırılar için saldıran devletler tarafından diğer devletlerin bilgi teknolojileri altyapıları kullanılarak kritik altyapıların tahribata uğratılması tanımı yapılmıştır (Kabano, 2023).

Daha önceki bölümlerde siber saldırı örnekleri arasında yer verilen 2007 tarihli Estonya saldırısı siber saldırıların etkileri bakımından bir milat kabul edilmektedir. Bu saldırıya yönelik olarak uluslararası çatışma hukukunun uygulanmadığı görülmektedir. Öyle ki bu saldırı BM Sözleşmesi 2/4 bakımından silahlı saldırı olarak nitelendirilmemiştir. Ancak bu saldırıdan bir sene sonra Gürcistan'a yapılan siber saldırıya bakıldığında Rusya ile halihazırda sıcak çatışma ortamına yardımcı olması hususu göz önünde tutularak Gürcistan için BM 2/4 kapsamında meşru savunma hakkının mümkün olduğu savunulmuştur. Bu kapsamda silahlı çatışma hukuku devreye alınarak kuvvet kullanımı mümkün hale getirilmiştir (Bolat, 2020).

Diğer taraftan Birleşmiş Milletler Uluslararası Adalet Divanı tarafından teamül haline getirilmiş olan ve devletin finansör olarak kullanımı vasıtasıyla belirli gruplar tarafından gerçekleştirilen saldırılarda devletin fiiline karşılık kuvvet kullanımı meşru görülmemiştir. Buna örnek olarak askeri ve paramiliter saldırılar sonrası anlaşmazlık yaşanan ABD'ye karşı başvuruda bulunulan Nikaragua başvurusu ve kararı verilebilir. Nikaragua kararına konu olayda özetle, 1979 yılında Nikaragua'da karşıt gruplar arasında hükümete hâkim olma iç çatışması yaşanmış, ABD'nin hükümet karşıtı muhaliflere destek vermesi ve devletin iç işlerine karışması ile gruplar arasındaki ihtilaf daha da artmıştır. Bununla birlikte ABD tarafından Nikaragua Cumhuriyeti'nin ulusal limanlarına mayın döşenmiştir. Sovyet Sosyalist Cumhuriyetler Birliği (SSCB) ve Küba'nın da mevcut konumda iktidara sahip olan hükümete yakın destek vermesiyle iki taraf arasında gerginlik yükselmiştir. Bahse konu olayda BM Şartı 2. maddesinin dördüncü fıkrası kapsamında kuvvet kullanma yasağı gündeme gelmiştir. Yine BM kapsamında geniş yorumla değerlendirilen "sufficient gravity" kıstası çerçevesinde saldırının belirli seviyeye erişip erişmediği yani ciddi bir suç unsuru barındırıp barındırmadığı tartışılmıştır. Söz konusu kararda ABD'nin uluslararası örf ve âdet hukuku ile 1956 Sözleşmesi kapsamında tazminat yükümlülüğü altında olduğu sonucuna varılmıştır. Öyle ki Nikaragua tarafından açılan davanın en önemli savunma dayanağı iç işlerine müdahale yasağının ihlal edilmesi olmuştur (International Court of Justice, 2024a). Bu kapsamda siber saldırıların devletler tarafından finanse edilmesi de söz konusu olayda

olduğu gibi uluslararası çatışma hukuku kapsamında kuvvet kullanma olarak değerlendirilmemektedir. Ancak aynı kararda yer verilen ve devlet tarafından belirli grupların karşı tarafa saldırı yapmak üzere silahlandırılması ve eğitilmesi müdahale yasağı kapsamı dahilinde değerlendirilmiştir. Yani bu durumda siber saldırılar amacıyla devletler tarafından belirli kötücül yazılım yazan grupların eğitilmesi kuvvet kullanma olarak değerlendirilebilecektir. Bunun yanı sıra diğer türlü destek ve saldırılara karşı savunma sağlayan yapılar da yine kapsam dahilindedir (Bolat, 2020).

BM Sözleşmesi 2/1 kapsamında müdahale yasağının siber saldırılar açısından değerlendirilmesinde somut olay analizi önem taşımaktadır. Öyle ki bazı siber saldırıların kuvvet kullanımı için gereken seviyenin altında kalması durumunda bu saldırılar müdahale yasağı ihlali şeklinde yorumlanmayabilir. Söz konusu istisnai hallere girmeyen somut olaylarda müdahale yasağı delinmiş olmaktadır. Tallinn Manual uzmanlarının görüşüne göre zorlayıcılık hali olmayan siber olayların müdahale yasağına aykırı olmadığı değerlendirilmiştir. Söz konusu duruma örnek vermek gerekirse seçim dönemlerinde dezenformasyon çalışmaları ve manipülatif eylemler vasıtasıyla zorlayıcı siyasi müdahalelere karşı yapılan davranışlar müdahale yasağına ilişkin ihlal örneğini oluşturmaktadır. Bir diğer örnek de siber saldırılar aracılığıyla bir devletin kritik altyapılarına saldırı olması durumunda siber saldırıların etki derecesi bakımından müdahale yasağının ihlali sayılabileceği değerlendirilebilir. Öyle ki kuvvet kullanma sınırına yakın durumlarda bu yorum yapılabilmektedir. Bu sayılanlar gibi ekonomiye yönelen saldırılar da yine müdahale yasağının ihlali niteliği taşıyabilmektedir. Ancak tek başına ekonomik baskı oluşturulması kuvvet olarak nitelenemeyeceğinden burada bir kuvvet kullanımından da bahsedilemeyecektir. Nikaragua davasının yorumlanması da bu şekilde olmuş ve yalnızca saldırı birliklerinin finanse edilmesi hususu kuvvet kullanımına dahil edilmemiştir. Tallinn Manual kapsamında siber saldırıların silahlı saldırı olarak kabul edildiği durumlarda kuvvet kullanımı olarak nitelendirildiği görülmüştür (Bolat, 2020).

Öte yandan Uluslararası Adalet Divanı'nın Korfu Kanalı kararında özetle 1946 yılında iki İngiliz savaş gemisinin Korfu boğazından geçişi sırasında Arnavutluk tarafından döşenen mayınlara çarpması ve bununla birlikte iki devlet arasında uluslararası hukuk bağlamında kimin sorumlu olduğu hakkında ihtilafa düşülmesi söz konusu olmuştur. Bahse konu davada "divan coğrafi" kıstası temel alınarak Arnavutluk'un karasularına mayın

döşemesinin pasif fiille uluslararası sorumluluk doğurduğu, İngiltere'nin ise mayınları izinsiz toplamasının aktif fiille uluslararası sorumluluk doğurduğu ifade edilmiştir. Bu kapsamda Uluslararası Adalet Divanı Arnavutluk'un söz konusu olaylar neticesinde tazminat ödemesine karar vermiştir. Tarafların toprak bütünlüklerine saygı gösterilmesi gerekliliği doğrultusunda olaya ilişkin kararda yer verilen "devlet egemenliğine saygı gösterilmesi gerekliliği" hususu üzerinde bir sonuca varıldığı görülmektedir. Egemenliğe ilişkin koruyucu devlet politikası kapsamında söz konusu devlet tarafından hem kendi hem de karşı devletin egemenliğine saygı gösterilmesinin esas olduğu, bu yükümlülüğün karşı tarafa zarar verici fiillerde bulunmanın yanı sıra egemenlik altındaki bireylere ve somut unsurlara zarar veren veya zarar verme ihtimali yüksek olan ciddi fiiller için de geçerli olduğu sonucuna varılmıştır (International Court of Justice, 2024b).

Söz konusu ilkenin siber saldırılara uyarlanması durumunda siyasi olarak birden fazla devletin sınırlarını ihlal etme özelliği nedeniyle çeşitli problemlerin oluşabileceği düşünülebilecektir. Bir siber saldırı neticesinde saldırının gerçekleştiği ve neticenin oluştuğu yerdeki ağların devre dışı bırakılması durumunda devletler hem kendi ağlarını hem de diğer devletlerin ağlarını kullanılmaz hale getirebilir. Bu durumda devre dışı bırakma tedbirinin uygulanmasının gerekliliğine ilişkin muhtemel zararların rasyonel şekilde sorgulanması gerekmektedir. Söz konusu olayda uluslararası hukukun ve bahse konu ilkenin ihlali hem icrai olarak hem de ihmali davranışla gerçekleşebilmektedir. Siber saldırı altyapılarının yasa dışı örgütlere kullandırılması gibi yapılan saldırılara herhangi bir karşı koymada bulunmadan düşman devletlerin saldırıya maruz kalmasına yol açan ihmali eylemler de yine bu ilkenin ihlalini oluşturmaktadır. Bu ilke devletin hakimiyeti altındaki topraklarda veya münhasıran kontrolünde bulunan uluslararası alanlarda geçerlidir (Bolat, 2020).

2001 yılında imzalanan ve 2003 yılında yürürlüğe giren Budapeşte Sözleşmesi siber suça vücut veren saldırıları düzenleme altına almıştır. Sözleşmenin 2 ila 10. Maddeleri arasında bilgisayar sistemlerine yasa dışı erişim, yasa dışı araya girme, verilere müdahale, sisteme müdahale, cihazların kötüye kullanılması, bilgisayarla bağlantılı sahtecilik ve dolandırıcılık, çocuk pornografisiyle bağlantılı suçlar, telif hakkına ilişkin suçlar düzenlenmiştir. Bunun yanı sıra söz konusu suçlar bağlamında cezai soruşturma ve kovuşturmalar çerçevesinde usul hukukuna yer verilmiştir. 22. maddede yargılama yetkisi kapsamında suçun kendi ülkesi sınırlarında, ilgili taraf bayrağını taşıyan gemi veya kanuni

olarak kayıtlı uçakta işlenmesi durumunda o devletin yetki alanında bulunduğuna işaret edilmiştir. Ülkesel yetki tanınması bağlamında siber saldırılar çerçevesinde değerlendirildiğinde bu maddenin devletlere siber altyapıları üzerinde tam ülkesel yetki dayanağı teşkil ettiği değerlendirilmektedir. Yine Budapeşte Sözleşmesinin 32. maddesinde bilgisayar sistemi dahilinde veriyi ifşa etme yetkisine kanunen sahip olan kişinin rızasını alarak sunan devletin verilere erişilmesi ve verileri elde etmesi düzenlenmiştir (Budapeşte Sözleşmesi, 2001).

Diğer taraftan Birleşmiş Milletler bünyesinde 74/247 sayılı kararla Bilgi ve İletişim Teknolojilerinin Suç Amaçlı Kullanımının Önlenmesine İlişkin Kapsamlı Uluslararası Sözleşme Hazırlanması Ad Hoc Komitesi tarafından taslak sözleşme, 2024 yılında "*United Nations Convention Against Cybercrime: Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes*" başlığıyla kabul edilmiştir (United Nations Convention Against Cybercrime, 2024). Öyle ki bu sözleşmede öne çıkan hususlar siber suç kavramının hangi kapsamda ele alınacağı ve sibere bağımlı suçlar, siberin kolaylaştırdığı suçlar ve siberle alakalı suçlar kapsamındaki ayrım noktasında bilgi ve iletişim teknolojilerinin gelişmesiyle müşterek bir siber dilin belirlenmesidir. Siber saldırıların teknolojinin gelişmesiyle amaç olmaktan çıkarak araç konumuna gelmesi kapsamında siberin kolaylaştırdığı ve siberle alakalı suçlar artmış, konvansiyonel suçların daha kolay şekilde işlenmesine olanak sağlanmıştır. Bu da uluslararası hukukta oluşan siberle ilgili boşluğun giderilmesi amacıyla yeni bir sözleşme imzalanmasını gerekli kılmıştır. Söz konusu Sözleşmede siber suçların önlenmesi ve bu suçlarla mücadele edilmesi için daha verimli ve etkili tedbirlerin teşvik edilmesi ve güçlendirilmesi kararlaştırılmıştır. Bilişim sistemlerine yasa dışı erişim, yasa dışı dinleme, elektronik verilere müdahale, sistemlere müdahale, bilişim sistemleri ile ilgili sahtecilik, hırsızlık ve dolandırıcılık, çevrim içi çocuk istismarı veya çocuk cinsel istismarı materyali ile ilgili suçlar, mahrem görüntülerin rıza dışı yayılması ve suç gelirlerinin aklanması gibi siber suçlar sibere bağımlı ve siberle ilişkili suçlar çerçevesinde ele alınarak "ciddi suç" kavramı üzerinden hapis veya daha ağır bir ceza ile hürriyetten yoksun bırakılmaya dair cezai müeyyideler düzenleme altına alınmıştır (Yağcı, 2023). Ciddi suç bahse konu Sözleşmede "*en az dört yıl süreyle hürriyetinden yoksun bırakılma veya daha ağır bir ceza*" olarak belirli bir kıstas altında tanımlanmıştır (United Nations Convention Against

Cybercrime, 2024). Diğer taraftan usule ilişkin tedbirler ve kolluk kuvvetlerine ilişkin hususlar ile yargılama yetkisi yine bu Sözleşmede düzenlenmektedir. Sözleşmenin önemli kısımlarından birisini de uluslararası iş birliği kısmı oluşturmakta, kişisel verilerin korunması, suçluların iadesi prosedürü, hükümlülerin nakli, karşılıklı adli yardımlaşma, bilgi değişimi, önleyici tedbirler, teknik yardım ve kapasite geliştirme, ortak soruşturma, uygulama mekanizması ve uyuşmazlıkların çözümü gibi konularda detaylı bir düzenleme ortaya konulmuştur (Yağcı, 2023). Bahse konu Sözleşmenin 22. maddesi taraf devletlerin yargı yetkisini düzenlemekte ve ilk fıkrada Budapeşte Sözleşmesine benzer olarak suçun taraf devletin topraklarında işlenmesi veya taraf devletin bayrağını taşıyan gemi veya suçun işlenildiği zaman bahse konu devletin yasalarına göre tescil edilmiş olan hava taşıtında işlenmesi durumlarında o devlete gerekli tedbirleri alma hakkı tanınmıştır. Aynı maddenin ikinci fıkrasında Sözleşmenin 5. maddesine atıfla (egemenliğin korunması) taraf devletin vatandaşına karşı işlenmesi, taraf devletin vatandaşı tarafından veya ülkesinde mutat meskeni olan vatansız bir kişi tarafından işlenmesi, 17. maddede belirtilen bazı suçları kapsaması ve suçun taraf devlete karşı işlenmiş olması durumunda da bahse konu taraf devletin yargı yetkisine sahip olacağı düzenlenmiştir. Sözleşmenin 5. maddesinde belirtilen "egemenliğin korunması"nın ise devlet egemenliği ve toprak bütünlüğü ilkeleri doğrultusunda devletlerin iç işlerine karışmama ilkesinin uygulanmasına hizmet ettiği görülmektedir. 22. maddenin altıncı fıkrasında belirtilen husus ise genel uluslararası hukuk ilkeleri saklı kalmak üzere bu Sözleşmenin taraf devletlerin kendi iç hukuklarında tesis ettikleri cezai yargılama yetkilerine halel getirmeyecek olmasıdır. Sözleşmenin 6. maddesinde uluslararası hukuk ilkeleri kapsamında insan haklarına saygı gösterilmesi ve temel özgürlüklerin korunması gerekliliği aktarılarak bunların taraf devletler için yetki kullanımında bir yükümlülük olduğu belirtilmiştir.

2009 yılında Şangay İş Birliği Örgütü kapsamındaki çalışmalar neticesinde kabul edilen Yekaterinburg Sözleşmesi bilgi silahlarının geliştirilmesi ve kullanılması, bilgi savaşı, bilgi terörizmi ve siber suçlarla ilgili temel tehditlerden hareketle imzalanmıştır. Söz konusu sözleşmede bilgi savaşı; "*bilgi sistemlerine, süreçlerine ve kaynaklarına, kritik öneme sahip ve diğer yapılara zarar vermek, siyasi, ekonomik ve sosyal sistemleri baltalamak, toplumu ve devleti istikrarsızlaştırmak için nüfus kitlelerini psikolojik olarak manipüle etmek ve ayrıca devleti karşı tarafın çıkarına kararlar almaya zorlamak amacıyla bilgi alanında iki veya daha fazla devlet arasındaki çatışma*" olarak tanımlanmıştır. Bununla

birlikte siber suç kavramı, "*bilişim kaynaklarının kullanılması ve/veya bilişim alanında yasadışı amaçlarla etkilenmesi*" şeklinde ifade edilmiştir. Siber suçların bilgi kaynaklarına zarar vermek, fikri mülkiyet hakları ve mahremiyeti de içine alan vatandaşların yasal hak ve özgürlüklerinin ihlal edilmesi gibi amaçları olduğu vurgulanmıştır. Kritik altyapılara gerçekleştirilen siber saldırılarda bilgi silahlarının kullanıldığı, enformasyon savaşları doğrultusunda hava, balistik füze, askeri savunma tesisleri, ulaşım, iletişim ve komuta sistemlerini etkileyen saldırıların gerçekleştirildiği, bunların neticesinde devletlerin kendini savunma yeteneklerinin olumsuz etkilendiği, meşru müdafaa haklarının zedelendiği aktarılmıştır. Diğer taraftan bilgi terörizmi kapsamında terör örgütleri aracılığıyla bilgi kaynaklarına yönelik yasa dışı eylemlerde bulunulduğu ifade edilmiştir. Devletlere yönelen siber saldırılar sonucunda iş birliğinin yapılması, çatışmaların barışçıl yollarla çözümü, kuvvet kullanılmaması, iç işlerine karışmama ve insan haklarına saygı gösterilmesi ilkeleri doğrultusunda, 4.madde kapsamında yer verilen milli güvenlik ve kamu güvenliği gibi hususlarda devletlerin ülkesel yetkilerini kullanması gerekliği vurgulanmıştır (Şangay İş Birliği Örgütü, 2009).

Diğer taraftan 1928 tarihli Palmas Adası davası siber saldırılar bağlamında yetki kullanımında devletlerin egemenliği ilkesine saygı gösterilmesi için gündeme gelen dava örnekleri arasındadır. Dava soncunda çıkan kararda bahse konu egemenliğin siyasi bağımsızlığı simgelediği ve devletin işlevlerini yerine getirmesi hakkının bir diğer devletin müdahalesi olmaksızın kazanılmasının mümkün olduğu ifade edilmiştir (Raufoğlu, 2022). Devletin söz konusu egemenliğinin temelini kural koyma, uygulama ve yargılama yetkileri oluşturmaktadır. Siber uzam bağlamında söz konusu yetkiler siber ağlar ve siber altyapılar üzerinde kullanılan yetkileri içermektedir.

2000 yılında meydana gelen bir diğer olayda Mark Knobel isimli Yahudi kökenli Fransa vatandaşı, Yahoo isimli internet sitesinde Nazi propagandasına yol açan çeşitli eşyaların satın alınmak üzere bulundurulduğunu, söz konusu siteye Fransa'dan erişim sağlanabildiğini ve sitenin yer sağlayıcı (hosting) hizmetlerinin ABD tarafından sağlandığını tespit etmiştir. Bunun üzerine Yahoo kendisine gönderilen bahse konu yayınları kaldırma uyarısını dikkate almamış ve eşyalar sitede yayımlanmaya devam etmiştir. Sürecin devamında Knobel Fransa Mahkemesine başvurarak dava açmış, mahkeme tarafından ABD'de ilgili satışın meşru olduğu ancak Fransa ülke sınırlarına taşan söz konusu fiilin yasal

olmadığı ve etki doktrini kapsamında Fransa Mahkemesinin yetkili olduğu ifade edilmiştir (Raufoğlu, 2022).

Siber alandaki yetki hususunda ortaya çıkan bir diğer olay da ABD ve Microsoft arasında yaşanmıştır. Bu olay, ABD tarafından siber altyapılarına yönelik bir faaliyet için Microsoft şirketinden bilgi talep edilmesi üzerine, Microsoft'un İrlanda'da bulunan sunucuları üzerinde ABD'nin herhangi bir yetkisi olmadığı ve bu sebeple de istenilen bilgilerin kendileriyle paylaşılamayacağı cevabının verilmesi olarak özetlenebilir. Ancak Amerikan Mahkemesinin yetkili olduğu kararının Microsoft'a iletilmesi burada ülke dışı yetki ile hareket edilebileceğini göstermektedir. Buna benzer olarak Apple ve FBI arasında yaşanan bir diğer olay ABD'nin Kaliforniya eyaletine bağlı Sen-Bernardino'da gerçekleştirilen terör saldırısı faillerinin bulunması için, olayı aydınlatacak ilgili telefon kayıtlarının FBI tarafından istenilmesi ile filizlenmiştir. Söz konusu istemin neticesinde Apple özel hayatın gizliliği ve veri gizliliği doğrultusunda faillerin bilgilerini veremeyeceğini açıklamıştır. Bir başka örnekte ise Gutnick-Dow Jones davası olarak literatüre geçen olayda Joseph Gutnick isimli iş adamının vergi kaçakçılığı yaptığına dair haberler Dow Jones isimli şirketin sahibi olduğu New Jersey menşeili bir haber sitesinde yayımlanmıştır. Avustralya mahkemelerinin ülke dışında başlamış bir faaliyetin kendi ülkelerinde neticelenmiş ve sonuç doğurmuş olması gerekçesiyle kendilerine karşı yürütülen yetkisizlik iddiasının meşru olmadığı sonucuna varması ile dava sonuçlanmış ve şirketin tazminat ödemesine hükmedilmiştir (Raufoğlu, 2022). Söz konusu davalardaki olaylar "etki doktrini" kapsamında değerlendirmeye tabi tutulursa ülkesel yetkisi bulunmayan devletlerin dahi "ciddi sonuçlar kıstası" çerçevesinde ülke dışı yetki ile yetkili olduğu talebinde bulunabileceği ortaya çıkmaktadır. Burada devlet egemenliği ilkesi kapsamında genişletici bir yorumla ilgili sonuca da ulaşılabilmektedir. "Koruyucu yetki" içtihadına göre ise devletlerin ülke sınırları dışındaki ve kendi vatandaşlarına ait olmayan fiillerin milli güvenlik gerekçesiyle yetkileri dahilinde olduğu yorumu yapılabilecektir. Söz konusu husus Tallinn Manual kapsamında da savunulmuştur. Objektif ülkesellik ilkesi ve pasif vatandaşlık doktrini gibi temel görüşlerin de burada verilen kararlarda etkili olduğu görülmektedir.

4. İDARE HUKUKUNDA SORUMLULUK ve SİBER TERÖRİZM

İdare hukukunda siber terörizmin incelenmesi öncesinde devletlerin siber saldırılar kapsamında yetki alanları büyük önem arz etmektedir. Öyle ki devletin kural koyma, uygulama ve yargılama yetkileri bakımından siber uzamda gerçekleştirilen saldırılar kapsamında doktrinde tartışmalı görüşler ortaya çıkmıştır. Devletin ülkesel yetkisi bakımından sübjektif ve objektif yetki ile etki doktrini görüşleri ön plana çıkmaktadır. Bununla beraber ülke dışı kural koyma yetkisi bağlamında uyruğa tabi olma, bayrak devleti ilkesi, koruyucu yetki ve pasif yetki gibi farklı görüşler de bulunmaktadır. Teamül hukuku çerçevesinde de söz konusu yetkiler bakımından farklı görüşler ortaya atılmıştır. Diğer taraftan hukukun genel ilkeleri ve içtihadi uygulamalarla bu alandaki boşluk doldurulmaya çalışılmaktadır.

Öyle ki sübjektif yetki devletlerin kendi ülkeleri sınırlarında meydana gelen siber saldırıları, objektif yetki devletlerin sınırları dışında başlayan ancak kendi ülke sınırlarında neticelenen veya kendi ülkesinde bireylere ve objelere yönelik yapılan siber saldırıları, Tallinn Manual kapsamında ele alınan etki doktrini ise ülkesel sınırlardan bağımsız olarak o devlete ciddi derecede şiddet içeren ve etkide bulunan siber saldırıları kapsamaktadır. Ülke dışı yetki kapsamında bir devlet tarafından başka bir devlet üzerinde icrai siber yetkilerin kullanılması için, uluslararası hukuktan kaynaklanan özel yetkinin varlığı ve karşı devletin rıza şartlarının bulunması gerekmektedir (Raufoğlu, 2022).

Söz konusu alandaki tartışmalar eşliğinde devletlerin yargı yetkisine giren siber olaylar kapsamında iç hukukları nazara alınarak vatandaşların uğradığı zararların giderilmesi bakımından idare hukuku çerçevesinde düzenlemeler yapılması gerekliliği doğmaktadır. Bu bölümde idare hukuku bağlamında mevzuatımızdaki sorumluluk müessesini ortaya konulacak, siber terörizm dolayısıyla ortaya çıkabilecek maddi ve manevi zararların karşılanması bakımından ülkemizdeki kanun boşluğuna ve uygulanabilecek mevzuata ilişkin hususlar tartışılacaktır.

İdarenin sorumluluğuna girmeden önce sorumluluğun ne olduğu hususunun ortaya konulması gerekmektedir. Sorumluluk kavramı genel olarak tasarrufu altındaki olay ve durumların neticelerine ilişkin mesuliyet olarak nitelenmekle birlikte hukuki anlamda sorumluluk *"uyulması gereken bir kurala aykırı davranışın hesabını verme; tazminatla yükümlü tutulma; işlenmiş olunan bir suçun gerektiği cezayı çekme"* olarak tanımlanmaktadır (Yılmaz, 2004, sy. 1109). Söz konusu tanımdan yola çıkıldığında hukuki anlamda sorumluluk; bireylerin hukuki kurallara aykırı olarak çeşitli fiillerde bulunması neticesinde ortaya çıkan zararlardan yükümlü olunması olarak nitelenebilecektir. Söz konusu hukuki anlamda sorumluluk haksız fiilden ve sözleşmeden doğabileceği gibi cezai olarak da suç işlenmesi halinde söz konusu olabilmektedir. Bahse konu sorumluluğun ortaya çıkabilmesi için de zarar, kusur, illiyet bağı ve hukuka aykırılık unsurlarının oluşması gerekmektedir. İdare hukukunda sorumluluk kavramının ise sorumlunun idarenin faaliyetleri ve işlemleri doğrultusunda ortaya çıkması dolayısıyla fail bakımından özel hukuka göre farklılık arz ettiği görülmektedir.

4.1. İdarenin Sorumluluğu

Sorumluluğa ilişkin hususlar hukuki bağlamda "siyasi", "cezai" ve " hukuki (mali)" olarak sınıflandırılmaktadır. Bununla beraber idarenin özel hukuktan kaynaklanan sorumluluğu da bulunmaktadır. Söz konusu sorumluluk çeşitleri idare tarafından yerine getirilen görevler ve idari işlemler kapsamında hukuka aykırı hareketlerin oluşması ile ortaya çıkmaktadır. Söz konusu sorumluluk çeşitleri kusura dayalı olabileceği gibi kusursuz olarak da ortaya çıkabilmektedir. Aşağıda yer verilen idarenin sorumluluk çeşitleri kapsamında söz konusu hususlar detaylı olarak anlatılmıştır.

İdarenin Siyasi Sorumluluğu

Siyasi sorumluluk devleti yöneten kişilerin siyasi icraatları sebebiyle hesap verme ve gerekli yaptırımlara katlanmalarını da kapsayan görevlerine son verilmesi olarak nitelenmektedir (Kaboğlu, 2019, sy.127-128). Türk siyasi yapısına bakıldığında 2017 yılı itibariyle anayasa değişikliği sonrasında parlamenter sistemden cumhurbaşkanlığı hükümet sistemine geçilmesiyle yasama, yürütme ve yargı organları arasındaki ilişkilerde değişiklikler meydana gelmiştir. Öyle ki başbakan ve bakanlar kurulunun ortadan kalkması

ve cumhurbaşkanlığı yardımcılığı şeklinde yeni bir yapının ortaya çıkmasıyla idarenin siyasi sorumluluğu kavramında değişiklik meydana getirmiştir.

Anayasanın 104. maddesinin ilk fıkrasında geçen "Cumhurbaşkanı Devletin başıdır. Yürütme yetkisi Cumhurbaşkanına aittir." hükmü gereğince yeni sistemde yürütme yetkisinin Cumhurbaşkanı tarafından kullanılacağı ifade edilmiştir. Aynı maddenin sekizinci fıkrasında geçen "Cumhurbaşkanı yardımcıları ile bakanları atar ve görevlerine son verir." hükmü Cumhurbaşkanının yardımcıları ve bakanlar üzerindeki yetkisini göstermektedir.

Anayasanın 106. maddesinin beşinci fıkrasında yeni sistemle birlikte başbakan ve bakanların parlamentoya karşı sorumlulukları kalkarak cumhurbaşkanı yardımcısı ve bakanlar kurulu olmayan sistemdeki bakanların siyasi sorumluluğu düzenlenmiştir:

> *"Cumhurbaşkanı yardımcıları ve bakanlar, Cumhurbaşkanına karşı sorumludur. Cumhurbaşkanı yardımcıları ve bakanlar hakkında görevleriyle ilgili suç işledikleri iddiasıyla, Türkiye Büyük Millet Meclisi üye tam sayısının salt çoğunluğunun vereceği önergeyle soruşturma açılması istenebilir. Meclis, önergeyi en geç bir ay içinde görüşür ve üye tamsayısının beşte üçünün gizli oyuyla soruşturma açılmasına karar verebilir."*

Söz konusu değişiklikler değerlendirildiğinde siyasi sorumluluk hususunun değiştiği görülmektedir. Önceden siyasi sorumluluğun ikiye ayrılarak incelendiği "kolektif" ve "bireysel" sorumluluk ayrımı ortadan kalkarak sadece bireysel sorumluluğun ortaya çıktığı ve kuvvetler ayrılığı içeren bir sisteme geçildiği görülmektedir.

İdarenin Cezai Sorumluluğu

Cezai sorumluluk, adli yargı kapsamında bağımsız mahkemeler nezdinde verilen hükümler neticesinde oluşan ve adli para cezası ve hapis gibi cezai müeyyideleri içeren bir sorumluluk çeşididir. Bu sorumluluktaki en önemli ve belirgin özellik "suçta ve cezada şahsilik ilkesi" gereğince cezai müeyyideye katlanacak kişilerin gerçek kişi olması gerekliliğidir. Bu durumda özel hukuk ve kamu tüzel kişileri ile idarelerin söz konusu cezai sorumluluğu bulunmamaktadır. Ancak idarenin cezai sorumluluğunun bulunmaması idari

faaliyetleri yerine getiren gerçek kişilerin şahsi olarak cezai sorumluluklarını ortadan kaldırmamaktadır (Gözler, 2013, sy. 739).

İdarenin Hukuki (Mali) Sorumluluğu

İlk hali 1961 Anayasasında yer alan ve 1982 Anayasanın 125. maddesinde düzenleme altına alınan idarenin hukuki sorumluluğu "idare kendi eylem ve işlemlerinden doğan zararı ödemekle yükümlüdür" şeklinde ifade edilmektedir. Bu minvalde idarenin genel olarak özel ve kamu hukuku kapsamındaki sorumluluğu belirtilmiştir (Çağlayan, 2022, sy.642) Gözler'e (2013) göre malvarlığı sorumluluğu olarak da nitelenen bu sorumluluk çeşidinde genel olarak zarara sebebiyet veren kişilerin karşı tarafa yönelik zarar kapsamında tazminat yükümlülüğü bulunmaktadır. Bu yükümlülük kapsamında verilen zarar oranında karşı tarafın zararı kişisel mal varlığından iradi olarak karşılanmaktadır. Ancak söz konusu iradenin bulunmadığı durumlarda verilen zararın tazmini devlet tarafından cebri olarak yerine getirilerek zararı veren kişinin mal varlığından zarar oranında tazmin işlemi gerçekleştirilir. Söz konusu sorumluluğa tazmin şeklinde sorumluluk da denilmektedir. Bu tazmin işlemi aynen teslim şeklinde gerçekleşebileceği gibi tazminat olarak da yerine getirilebilmektedir (Gözler, 2013, sy. 739). Bununla birlikte bazı yazarlara göre şahıs varlığını ve mal varlığını beraber kapsayan bu sorumluluk türü genel olarak kişilerin mameleki üzerinde bir azalmayı veya önlenen artışın giderimini kapsamaktadır. Eren'e (1998) göre ise mali sorumluluk kısaca "edimini ifa etmeyen borçlunun mal varlığına devlet organları aracılığıyla alacaklının el koyması" şeklinde tanımlanmaktadır (Eren, 1998, sy. 80)

İdarenin hukuki sorumluluğu, Danıştay 10. Dairesinin birçok kararında idari sorumluluğun dayanağını oluşturan aşağıdaki gerekçelerle ortaya konmuştur (Danıştay 10. Daire 2007/3301 E.N, 2008/2939 K.N.):

> "*İdarenin hukuki sorumluluğu, kamusal faaliyetler sonucunda, idare ile yönetilenler arasında yönetilenler zararına bozulan ekonomik dengenin yeniden kurulmasını, idari etkinliklerden dolayı bireylerin uğradığı zararın idarece tazmin edilmesini sağlayan bir hukuksal kurumdur. Bu kurum, kamusal faaliyetler nedeniyle yönetilenlerin malvarlığında ortaya çıkan eksilmelerin ya da çoğalma olanağından yoksunluğun giderilebilmesi, karşılanabilmesi için aranılan koşulları, uygulanması*

gereken kural ve ilkeleri içine almaktadır. İdarenin hukuki sorumluluğu, kişilere lütuf ve atıfet duygularıyla belli miktarda para ödenmesini öngören bir prensip olmayıp; demokratik toplum düzeninde biçimlenen idare-birey ilişkisinin doğurduğu hukuki bir sonuçtur. İdari yargı da, bu anlayış doğrultusunda, idare hukukunun ilke ve kurallarını uygulamak suretiyle, idarenin hukuki sorumluluk alanını ve sebeplerini içtihadıyla saptamak zorundadır."

Diğer taraftan sorumluluk türleri bakımından değerlendirildiğinde medeni sorumluluk ile idari sorumluluk arasında özel hukuk ve idare hukuku ayrımı görülmektedir. Öyle ki medeni sorumluluk özel hukuk bağlamında kişiler arası ilişkilerde verilen zararlara ilişkin ve uyuşmazlık halinde adli yargının görevli olduğu sorumluluk çeşididir (Çağlayan, 2022). Özel hukuk kapsamında kişiler arasındaki sözleşme ve haksız fiil kaynaklı borç ilişkisi sebebiyle ortaya çıkan anlaşmazlıklar sonucunda medeni sorumluluk alanı oluşmaktadır. Borç ilişkisinde edimini ifa etme borcunu yerine getirmeyen tarafın devlet eliyle cebren ifası sağlanmaktadır. Söz konusu cebri ifa sorumluluk olarak nitelenmektedir. Medeni sorumluluk bağlamında bu sorumluluğun muhatapları gerçek ve tüzel kişilerdir. Müeyyidesel bağlamda mal varlığının aynen teslim veya tazminat yoluyla yerine konulması mümkündür. Bununla birlikte medeni sorumluluk kapsamında zarar sözleşmenin ihlali ve haksız fiil dışında kanuni sebepler, tehlike ve fedakarlığın denkleştirilmesi sebebiyle de ortaya çıkabilmektedir (Gözler, 2013, sy. 740-741).

Hukuki sorumluluğun ikinci çeşidini oluşturan idari sorumluluk ise bu çalışma kapsamında asıl olarak incelenecek bölümü oluşturmaktadır. İdari sorumluluk idare hukuku bağlamında kişilerin değil de idarenin kamu hukukuna konu faaliyetleri dolayısıyla verdiği zarardan dolayı ortaya çıkan ve idarenin mal varlığından tazmin edilerek zarar gören kişinin mal varlığına aktarılan değerlere ilişkin cebri tazmini içeren sorumluluktur. İdari sorumluluğun muhatabı olarak kamu tüzel kişileri söylenebilecektir. Bununla birlikte ortaya çıkan zarar kusur, risk ve fedakarlığın denkleştirilmesi bağlamında değerlendirilmektedir. Söz konusu sorumluluk "akdi (sözleşmesel) sorumluluk" ve "akit dışı (sözleşme dışı) sorumluluk" olarak ikiye ayrılmaktadır.

İdare ile kişiler arasında yapılan sözleşmeler neticesinde idare tarafından sözleşmeye aykırı davranılması sebebiyle idare tarafından verilen zararın tazmin edilmesine akdi

(sözleşmesel) sorumluluk denilmektedir. Burada öne çıkan husus ise kamu tüzel kişisi ve özel hukuk kişisi arasında yapılan akitlerde akdi sorumluluk öncelikli olarak uygulama alanı bulacaktır. Bu kapsamda sözleşme dışı sorumluluk hükümlerinin bu süjeler arasında uygulanma olanağı bulunmamaktadır. Akit dışı sorumluluk ise isminden de anlaşılacağı üzere kişilerle idare arasında herhangi bir sözleşme bulunmayan durumlarda idare tarafından gerçekleştirilen tek yanlı işlem ve eylemlerle kişilere karşı verilen zararın tazmin yükümlülüğünü içeren sorumluluk çeşididir. Söz konusu sorumluluk çeşidi teamülen "idari sorumluluk" olarak da anılmaktadır. Bu kapsamda idarenin sorumluluğu kusura göre farklılık arz etmektedir (Gözler, 2013, sy. 740-741).

Kusur kavramı çerçevesinde idarenin kusur sorumluluğu; kusurlu işlem ve eylemler neticesinde oluşan ve kişilere verilen zararların tazminini içeren yükümlülük olmakla birlikte, Derdiman (2007) tarafından hizmetin işleyişine yönelik olan ve idare tarafından gerçekleştirilen kamu hizmetlerindeki kusurlu işlem ve eylemler neticesinde meydana gelen zararların giderilmesi olarak nitelenmektedir. Söz konusu husus içtihatlarla geliştirilen kamu hizmeti ilkelerindeki aksaklık olarak da ifade edilmiştir (Derdiman, 2007 sy.138). Hukuka aykırı olan idari işlemlere istisnalar dışında kusur da atfedilmektedir. Buradan kural olarak idarenin kusurlu sorumluluğunun bulunduğu çıkarımı yapılabilecektir. Yine bu kapsamda mefhumu muhalifinden değerlendirme yapıldığında hukuka aykırılığın bulunmadığı durumlarda kusurlu bir işlemden de bahsedilemeyecektir. İdare hukuku kapsamında "iddia eden iddiasını ispat etmekle yükümlüdür" kuralı uygulama alanı bulmaktadır. Bu kapsamda idarenin işlemleri ve eylemleri dolayısıyla zarar gördüğünü iddia eden taraflar bunu ispat etmek durumundadır. Bunun istisnası olarak kusur karineleri gösterilebilir ki bu karineler ispat yükünü tersine çevirmektedir. Bu durumda idareler, gerçekleştirdikleri işlem ve eylemler için kusursuz olduğunu ispat etmedikçe tazmin etme yükümlülüğü doğmaktadır (Gözler, 2013, sy. 741-751).

Bununla beraber İdari Yargılama Usulü Kanununun (İYUK) 20. maddesinde düzenleme altına alınan re'sen araştırma ilkesi kapsamında mahkeme kendiliğinden de herhangi bir şekilde elde ettiği bilgi ve belgelerle idarenin kusurlu olduğuna hükmedebilmektedir (İYUK, 1982). Kusur sorumluluğu idarenin birincil sorumluluğu kapsamında ele alınmaktadır. Öyle ki kusurlu sorumluluğa gidilebilen durumlarda kusursuz sorumluluğa gidilememektedir (Çağlayan, 2022, sy.649). Diğer taraftan idarenin kusurlu

sorumluluğuna gidilebilmesi için aranan kusur şartında kusurun belirli bir ağırlık derecesinde olması hususu faaliyetin yürütülmesindeki zorluklar bağlamında açıklanmaktadır. Öyle ki idare işlem ve faaliyetlerinde kusur işleme korkusuyla birçok görevini yerine getiremeyebilir. Bu durumda basit kusur-ağır kusur ayrımı dolayısıyla idarenin işlem ve eylemlerini rahatlıkla yerine getirebilmesine hizmet eden kusurun derecesi büyük önem arz etmektedir (Çağlayan, 2022, sy.657).

Kusur kavramı idare hukuku bağlamında idare tarafından gerçekleştirilen hizmetin kötü, geç veya hiç işlememesinin yanı sıra idare tarafından yerine getirilmesi gereken ödevdeki eksiklik olarak nitelenmektedir. Hizmet kusuru, kamu görevlilerinin görevlerini yerine getirmeleri sürecinden ayrı olarak düşünülemeyecek nitelikte, resmi sıfatıyla bağlantılı olarak kabul edilebilecek kusurları kapsamına almaktadır (Gözler, 2013, sy. 753-755). İdari faaliyetler sırasında zarar doğan zararlara kamu görevlisi veya memur tarafından sebep olunmasına rağmen, bahse konu personelin zararı gerçekleştirdiğinin tespitinin zor olması ve kusura ait bireyselleştirmenin yanlışlığı düşüncesiyle hizmet kusuru bakımından idarenin sorumluluğuna gidilmektedir (Düren, 1979, sy.287). Bu durumda sorumlu tutulan kişi ya da makam kamu görevlisi olmamakta, görevi nedeniyle temsil ettiği kamu tüzel kişisi olmaktadır. Kusur kavramı ifade edildiğinde idare hukuku bağlamında akla gelen kavram hizmet kusuru kavramı olmaktadır. Bu kusur türü asli ve anonim yani kişilere atfedilemeyen, genel ve esnek bir kusur türüdür (Çağlayan, 2022, sy.650). Hizmet kusuru Yayla (2009) tarafından nesnel ve anonimlik arz eden kamu hizmetlerinin yetersiz şekilde halka sunulması sebebiyle oluşan sorumluluk çeşidi olarak nitelenmektedir (Yayla, 2009, sy.361). Bu kusur çeşidinde idarenin yapması gereken hizmeti gereğine aykırı, geç veya hiç işletmemesi özel hukuktan esinlenerek oluşturulmuştur (Yıldırım, 2008).

Kişisel kusur ise kamu görevlilerinin görevlerini ifa etmesinden bağımsız olarak düşünülebilecek kusurlardır. Bu kusur çeşidi saf kişisel kusur olarak nitelendirilen ve görevde olmadığı sırada özel hayatla ilgili işlenen kusurları kapsamaktadır. Bununla beraber kamu görevlisinin görevi sırasında işlediği kişisel saikle işlenen kusurlar, aşırıya kaçan davranışlar ve mazur görülemeyecek hatalar gibi kusurlu işlem ve eylemler dolayısıyla "fevkalade ağır" kusur olarak nitelenmektedir. Kamu görevlilerinin görevi dışında ancak görev dolayısıyla ve hizmetin ifası vesilesiyle veya idarenin verdiği araçlar sayesinde işledikleri kusurlar da kişisel kusur kapsamında değerlendirilmektedir (Gözler, 2013, sy.

753-755). Fransız Danıştayı kararlarına da konu olan kişisel kusur kapsamında hizmet dışı kusurlar, salt kişisel kusurlar, suça vücut veren kusurlar, ağırlık derecesi yüksek olan kusurlar ve kasti olarak işlenen davranışlar bağlamındaki kusurlar kişisel kusur olarak kabul edilmektedir (Çağlayan, 2022, sy.662).

Türk yargı sisteminde kamu görevlilerin kişisel kusurları kapsamında kamu görevlisine karşı adli yargıda tazminat davası yerine idarenin sorumluluğu çerçevesinde idari yargı mercileri nezdinde tam yargı davası açılmaktadır. Söz konusu husus Anayasanın 129. maddesinin beşinci fıkrasında açıkça düzenleme altına alınmıştır:

> "*Memurlar ve diğer kamu görevlilerinin yetkilerini kullanırken işledikleri kusurlardan doğan tazminat davaları, kendilerine rücu edilmek kaydıyla ve kanunun gösterdiği şekil ve şartlara uygun olarak, ancak idare aleyhine açılabilir.*"

Anayasanın 40. maddesinde "Temel hak ve hürriyetlerin korunması" başlığı kapsamında devletin tazminat yükümlülüğü düzenlenerek resmi görevin ifası sırasındaki kişisel kusurlar aşağıdaki şekilde ifade edilmiştir:

> *"Kişinin, Resmî görevliler tarafından vaki haksız işlemler sonucu uğradığı zarar da, kanuna göre, Devletçe tazmin edilir. Devletin sorumlu olan ilgili görevliye rücu hakkı saklıdır."*

Söz konusu düzenlemelere ek olarak Devlet Memurları Kanunu'nun (DMK) 13. maddesinin birinci fıkrasında da benzer bir hükme yer verilmektedir (Devlet Memurları Kanunu, 1965):

> *"Kişiler kamu hukukuna tabi görevlerle ilgili olarak uğradıkları zararlardan dolayı bu görevleri yerine getiren personel aleyhine değil, ilgili kurum aleyhine dava açarlar. Ancak, Devlet dairelerine tevdi veya bu dairelerce tahsil veya muhafaza edilen para ve para hükmündeki değerli kağıtların ilgili personel tarafından zimmete geçirilmesi halinde, zimmete geçirilen miktar, cezai takibat sonucu beklenmeden Hazine tarafından hak sahibine ödenir. Kurumun, genel hükümlere göre sorumlu personele rücu hakkı saklıdır."*

Kural olarak idare hukukunda yer alan ve kamu görevlisinin kişisel kusurundan veya hizmet kusurundan dolayı kişileri uğrattığı zararlar dolayısıyla, idarenin sorumluluğu kapsamında kamu görevlisine değil de idareye karşı dava açılmasının istisnası şeklinde düzenlenen İYUK'un 28'inci maddesinin dördüncü fıkrasında kamu görevlisine karşı açılabilecek dava düzenlemesi 2014 yılında yapılan değişiklikle mülga olmuş ve yeni hükümde sadece idareye karşı açılabilecek davaya yer verilmiştir. İlgili kanun hükmü aşağıdaki gibidir (İdari Yargılama Usulü Kanunu, 1982):

> "*Mahkeme kararlarının süresi içinde kamu görevlilerince yerine getirilmemesi hâlinde tazminat davası ancak ilgili idare aleyhine açılabilir."*

Söz konusu hükmün değişiklikten önceki halinin Anayasanın 129. maddesinin dördüncü fıkrası ile çelişiyor olması bu hususta bir değişikliği zorunlu kılmaktaydı. Öyle ki Anayasanın bahse konu madde fıkrası memurların görevlerini ifa ettikleri sırada işledikleri kusurlardan dolayı sadece idareye dava açılabileceği ve gerekli hallerde ilgili memura rücuyu içerecek şekilde aşağıdaki düzenlemeyi gerekli kılmıştır:

> *"Memurlar ve diğer kamu görevlilerinin yetkilerini kullanırken işledikleri kusurlardan doğan tazminat davaları, kendilerine rücu edilmek kaydıyla ve kanunun gösterdiği şekil ve şartlara uygun olarak, ancak idare aleyhine açılabilir."*

Yukarıda anılan Devlet Memurları Kanunu'nun 13. maddesi ve Anayasanın 129/5. maddesinde açıkça belirtildiği üzere idarenin, kamu görevlisinin kusuru ile tazminata yol açan davranışları dolayısıyla rücu davası açıp ilgili memura zarar miktarı meblağı rücu etme hakkı saklıdır. Söz konusu davranışlar yalnızca kamu gücüne dayanmamakta aynı zamanda özel hukuktan kaynaklı işlemler de kapsam dahilindedir (Duran, 1974). Bu minvalde idare rücu hakkını cebri icra yetkisine dayanarak re'sen yerine getirememektedir. Bu hakkın kullanılabilmesi kamu görevlisi davalı olarak gösterilecek rücu davası ile mümkün olmaktadır. Burada davacı olarak her ne kadar idarenin bulunduğu bir durum söz konusu olsa da yargılamaya konu zararın tazmininin kamu görevlisine isnat edilecek olması ve Türk idare hukukundaki teamüllere göre rücu davasında görevli yargı yerinin idari yargı değil adli yargı mercileri olarak belirlenmesi önem arz eden noktalardır (Gözler, 2013, sy. 760-761).

Devletin sorumluluğu kapsamında kişisel kusurlara yönelik zararların tazmini daha önce de ifade edildiği gibi Anayasanın 40. maddesinin üçüncü fıkrasında haksız işlemler neticesinde uğranılan zararların Devlet tarafından tazmin edilmesi ve rücu hakkı aşağıdaki gibi düzenleme altına alınmıştır:

> *"Kişinin, Resmî görevliler tarafından vaki haksız işlemler sonucu uğradığı zarar da, kanuna göre, Devletçe tazmin edilir. Devletin sorumlu olan ilgili görevliye rücu hakkı saklıdır."*

4.2. İdarenin Kusursuz Sorumluluğu

Kusursuz sorumluluk, kusurlu sorumlulukta olduğu gibi içtihatlara dayalı olarak oluşan bir sorumluluk çeşididir (Çağlayan, 2022, sy.647). Söz konusu sorumluluk, idarenin hukuka uygun şekilde yerine getirdiği işlem ve eylemler kapsamında ortaya çıkan zararların tazmin edilmesi yükümlülüğü olarak nitelenebilecektir. Bu bağlamda herhangi bir kusur atfedilemeyen idare, kusursuz sorumluluk gereğince bu zararı tazmin eder. İdarenin sorumluluğu kural olarak kusurlu, istisnai olarak ise kusursuz sorumluluk şeklinde ifade edilebilecektir. Bu çerçevede dar yorumlama yapıldığında somut olay özelinde kusurlu sorumluluğa gidilememesi veya ortaya çıkan zararın başka şekilde tazmin edilmesi söz konusu olmazsa tamamlayıcı nitelikte olan kusursuz sorumluluğa başvurulmaktadır. Bu kapsamda kusursuz sorumluluğa ikincil (subsidiaire) sorumluluk da denilmektedir. Kusursuz sorumlulukta ispat hususu konusunda zarar gören kişiye yönelik bir kolaylık getirilmiştir. Öyle ki zarar gören kişi idarenin mevcut olay özelinde kusurunu ispat etmekle yükümlü değildir. İdarenin de kusursuzluğunu ispatı gibi bir durumu söz konusu olmaz. Bu kapsamda idare herhangi bir kusur aranmadan dahi sorumlu tutulacaktır (Gözler, 2013, sy. 761-762). Bu da kusursuz sorumlulukta kurtuluş kanıtı imkânı olmadığı anlamına gelmektedir. Söz konusu niteliği dolayısıyla kusursuz sorumluluğa tam hukuki sorumluluk da denilmektedir (Çağlayan, 2022, sy.667). Diğer taraftan Duran (1974) idari sorumluluğun idarenin işlem ve eylemleri dolayısıyla zarar gören kişilerin zararının tazmini bakımından ele alınması gerektiğini belirtmiştir. Söz konusu tazminat yükümlülüğünün kamu hukuku bağlamında imkân ve fırsat eşitliği esasına dayandığını belirtmiştir. Bu kapsamda devlet ve

idari organların zarara uğrayan kişilerin bozulan yaşam standartlarının yeniden sağlanması için idarenin tazminatla sorumlu olduğunu aktarmıştır (Duran, 1974).

Bununla birlikte bilgi ve iletişim teknolojilerinin gelişmesi ve idareler tarafından vatandaşa sunulan kamu hizmet ve işlemlerinin sanal ortama taşınması ile bu hizmetlere yönelik siber saldırılar artış göstermiştir. Söz konusu alanda bulunan boşluk dolayısıyla vatandaşların kamu hizmetleri nedenli uğradığı zararların tazmin edilmesi konusunda muğlaklık bulunmaktadır. Söz konusu muğlaklığın giderilmesi için kamuda veri işleme ve korunmasına yönelik riskleri içine alan mevzuat ve içtihatların hayata geçirilmesi önem taşımaktadır. Bu bağlamda ülkemizde henüz gelişme sağlanamamış söz konusu alandaki boşluk Fransız hukuku çerçevesinde kısmen tartışma ortamı bulmuştur. Bu tartışmalarda kusursuz sorumluluğun risk sorumluluğu çerçevesinde eşyalar, riskli yöntemler ve tehlikeli durumları kapsadığı, bilgisayar yoluyla meydana gelen sorumluluk türünün söz konusu kapsamın dışında olduğu ve idarenin kusursuz sorumluluk ilkeleri ile örtüşmediği, üretici kaynaklı sorunlar, verilerin tahrifatı veya yazılımsal problemler dolayısıyla ortaya çıkan zararlardan devletin sorumlu tutulmasının haksızlığa mahal vereceği, ancak devletin vatandaşlarına karşı yükümlülükleri doğrultusunda kusursuz sorumluluk ve idari denetime dayalı olarak tazminat yükümlülüğü bulunduğu değerlendirilmiştir. Söz konusu verilerin işlenmesine dayalı sorumluluk bağlamında devletin kusursuz sorumluluğu tartışılarak bu sorumluluğun kamu yükümlülüklerine ilişkin eşitlik kuralı ihlalini rastlantısal, özel ve olağan dışı hatalar ile doğurması şartı koşulmuştur (Chatillon, 2002).

Bununla ilgili 2000 yılında yaşanan “Milenyum Bug” virüsü olayı literatüre “Y2K hatası” olarak geçmiştir. Binyıl hatası olarak da bilinen siber saldırının çıkış noktası 1960'lardan 80'lere kadar yazılan bilgisayar programlarının iki basamaklı kodları kullanmasıdır. Sözgelimi 1970 tarihi yerine 70 yazılarak bilgisayarlarda veri depolama maliyetleri düşürülmeye çalışılmıştır. 2000 yılı ile birlikte bilgisayar programcıları bilgisayarların 00'ı 2000 olarak değil, 1900 olarak yorumlayabileceğini fark etmişlerdir. Bu kapsamda günlük veya yıllık olarak programlanan işlemlerde aksaklıkların ortaya çıkacağı sonucuna varılmıştır. 31 Aralık 1999 tarihinin ertesi günü 1 Ocak 2000'e tarihine geçildiğinde, bilgisayar ve sistemler 31 Aralık 1999'u yuvarlayarak 1 Ocak 1900 olarak tanımlamıştır. Söz konusu işlem sonrasında günlük faiz oranları etkilenmiş, hesaplama yapan finans şirketleri ve bankalar bir günlük faiz oranı yerine aradaki yüz yıllık süreden

dolayı yüksek bir faiz oranı hesaplaması yapmıştır. Diğer taraftan söz konusu siber saldırı kritik altyapıları da etkilemiş ve enerji santralleri, su basıncı ve radyasyon gibi güvenlik kontrollerine sahip tesisler tehdit altında kalmıştır. Bunun yanı sıra taşımacılık hizmetleri ve buna bağlı olarak tedarik zinciri de olumsuz etkilenmiş özellikle havayolları şirketlerine ait planlı uçuş kayıtlarının tutulduğu bilgisayarlar için risk ortamı doğmuştur (National Geographic, 2024). Söz konusu virüse ilişkin olaylar sonrasında karar veren mahkemeler idarelerin işlem yaptığı bilgisayarların üretim hataları dolayısıyla kusursuz olamayacağı sonucuna varmıştır. Geçerlilik süresinin son tarihi "2000" olan kredi kartlarının "00" şeklinde programlanması neticesinde bu tarihin "1900" olarak algılanmasının getirdiği sonuçlar görüldüğü üzere birden çok sektörde küresel bir etki yaratmıştır (Chatillon , 2002).

Bu sorumluluk türü idare hukuku bağlamında değerlendirildiğinde idarenin sorumluluğunu ortadan kaldıran ya da azaltan hallerden; "beklenmeyen hal" ve "üçüncü kişinin fiili" gibi durumlarda dahi ortadan kalkmamakta veya azalmamakta olduğu görülmektedir. Yalnızca "mücbir sebep" ve "mağdurun kusuru" durumlarında idarenin sorumluluğu azalabilmekte veya tamamen ortadan kalkmaktadır. Kusursuz sorumluluk niteliği gereği kamu düzenine ilişkin olmasından dolayı yargılamanın tüm aşamalarında öne sürülebilmektedir. Bununla birlikte kusursuz sorumluluğu ortaya koyan sebepler hâkim tarafından da re'sen göz önünde bulundurulmaktadır. Diğer taraftan kusursuz sorumluluk hem idare bakımından hem de zarar gören kişiler bakımından objektif sorumluluk unsuru taşımaktadır (Gözler, 2013, sy. 761-762). Kusursuz sorumluluk iki temel ilkeye dayanmaktadır. Bunları "fedakarlığın denkleştirilmesi ilkesi" ve "sosyal risk ilkesi" oluşturmaktadır.

"Kamu Külfetleri Karşısında Vatandaşların Eşitliği" ilkesi olarak da anılan fedakarlığın denkleştirilmesi ilkesi Anayasanın 10. maddesinde de yer verilen eşitlik ilkesi kapsamında idarenin topluma hizmet etmek amacıyla gerçekleştirdiği ve tehlike içermeyen işlem ve eylemler dolayısıyla ortaya çıkan külfetlerin toplumdaki belirli kişilerin üzerinde kalması neticesinde herhangi bir kusur aranmaksızın idare tarafından tazmin edilmesi olarak nitelenmektedir (Gözler, 2013, sy. 741). Söz konusu ilke Alman Hukuku literatüründe "fedakârlığın denkleştirilmesi ilkesi", Fransız Hukuku literatüründe ise "kamu yükümlülükleri karşısında eşitlik ilkesi" şeklinde kullanılmaktadır. Ayrıca bu ilke kusursuz sorumluluğun bir uzantısı olarak idare tarafından kusurlu bir işlem veya eylem, tehlikeli

faaliyet ya da tehlikeli araç kullanılmayan durumlarda toplumdaki diğer vatandaşlara kıyasen özel ve olağandışı bir zararla karşılaşması neticesinde idarenin söz konusu zararı tazminini temel almaktadır (Onar, 1968).

Devletin idari işlem ve eylemleri ile faaliyetleri dolayısıyla sorumlu olmasının yanı sıra idari nitelikte olmayan bazı faaliyetleri dolayısıyla da sorumluluğu söz konusu olabilmektedir. Devletin yasama ve yargı faaliyetleri ile yürütme organı tarafından yerine getirilerek idari nitelikte olmayan ve hükümet tasarrufu olarak adlandırılan bazı faaliyetleri kapsamında söz konusu sorumluluk veya sorumsuzluk ortaya çıkabilmektedir. Devletin yargı faaliyetleri kapsamında Danıştay ve Yargıtay içtihatlarında da yer aldığı üzere açık bir kanun hükmü bulunmadıkça sorumluluğun olmadığı teamülen bilinmektedir. Hükümet tasarrufları karşısında zarar görenlerin iptal ve tazminat davası açmasının mümkün olmaması ise devletin hükümet tasarrufları kapsamında sorumluluğunun bulunmadığı anlamına gelmektedir (Gözler, 2013, sy. 741).

Fedakârlığın denkleştirilmesi ilkesi kapsamında zararın tazmini için söz konusu zararın zarar gören kişiye doğrudan müdahale neticesinde oluşması gerekmektedir. Söz konusu husus fedakârlığın denkleştirilmesini tehlikelilik ilkesinden farklılaştırmaktadır (Düren, 1979). Bununla birlikte sosyal risk ilkesi kapsamında sorumluluğa gidilebilen durumlarda bu ilke kapsamında sorumluluğa gidilememektedir. Bu da söz konusu ilkenin risk ilkesine göre ikincil (subsidiaire) ve tamamlayıcı bir ilke olduğunu göstermektedir. Diğer taraftan kamu düzenine ilişkin olan fedakarlığın denkleştirilmesi ilkesine ilişkin sebepler bu nedenle yargılamanın tüm aşamalarında öne sürülebilmekte ve hâkim tarafından re'sen göz önüne alınmaktadır. Risk ilkesinde gerçekleşen kazalardan dolayı idarenin sorumluluğuna gidilebilirken fedakarlığın denkleştirilmesi ilkesi kapsamında kazalara ilişkin idarenin sorumluluğuna gidilememektedir. Fedakarlığın denkleştirilmesi ilkesi kapsamında uğranılan zararın özel ve anormal bir zarar olması gerekmektedir. Özel zarardan toplumun tümünün değil belirli kişi veya kesimlerin uğradığı zararlar, anormal zarardan ise belirli bir ağırlık derecesinin üzerinde olan zararlar anlaşılmalıdır. Söz konusu zararlar dört kategoride incelenmektedir. Bunları sırasıyla bayındırlık işlerinden kaynaklı daimî zararlar, hukuka uygun işlemler kaynaklı zararlar, kanunlardan doğan zararlar ve son olarak uluslararası anlaşmalardan doğan zararlar olarak sıralamak mümkündür (Gözler, 2013, sy. 771-774). Düren (1979), bahse konu bayındırlık eserleri veya bu alanda faaliyetlerin

yürütülmesi sebebiyle yakın bölgelerdeki taşınmazların maliklerinin karşı karşıya kaldığı özel ve olağandışı zararların tüm toplumca karşılanmasını fedakârlığın denkleştirilmesi olarak nitelemektedir. Söz konusu ilkenin özel hukuktaki "komşuluk zararları" müessesesinin idare hukuku bağlamındaki yansıması olduğunu ifade etmiştir (Düren, 1979). Çağlayan'a (2022) göre ise ticari zararlar, yol seviyesini değişmesi dolayısıyla ortaya çıkan zararlar, kullanım engeli ve değer kayıpları adı altındaki zararlar da bu ilke kapsamında sorumluluk oluşturmaktadır (Çağlayan, 2022, sy.686).

Diğer taraftan idarenin işlemleri bazı durumlarda hukuka aykırı nitelikte olabilmektedir. Bu durumu fark eden idare söz konusu işlemini hukuka uygunca geri alabilmektedir. Söz konusu geri alma işlemi dolayısıyla fedakarlığın denkleştirilmesi ilkesi kapsamında idarenin kusursuz sorumluluğuna gidilebilecek özel ve anormal zarar ortaya çıkabilmektedir. Ancak bazı görüşlere göre de hukuka aykırı bir işlem istisnalar dışında evleviyetle kusura da yol açacağından kusurlu sorumluluk kapsamında da idarenin sorumluluğuna gidilebileceği ifade edilmektedir. Danıştay kararlarına bakıldığında ise idari işlemin geri alınmasından doğan zararlar dolayısıyla kararların gerekçelerinde söz konusu hususlar belirtilmeden tazminata hükmedilmektedir (Çağlayan, 2022, sy.691).

Bununla beraber bazı özel durumlarda da idarenin sorumluluğu söz konusu olabilmektedir. İdarenin yasama faaliyetleri kapsamında ortaya çıkan zararların tazminine yönelik kanunda açık hükmün bulunmadığı hallerde idarenin sorumluluğuna dair yerleşik bir fikir birliği bulunmamaktadır. Söz konusu sorumluluğun bulunduğunu ifade eden görüşlere göre anayasal eşitlik, sosyal devlet ve hukuk devleti ilkelerine göre kanun kaynaklı zararların tazmini gerekmektedir. Bununla beraber uluslararası anlaşmalardan doğan zararlarda da mevcut sözleşmenin tazminatı yasaklamamış olması durumunda idarenin sorumluluğuna gidilebileceği ifade edilmektedir. Bunun yanı sıra özel ve anormal olma şartlarının da idarenin sorumluluğu için doğmuş olması gerekmektedir. Çağlayan (2022) tarafından uluslararası sözleşmelerde kanunlardan doğan zararlarda uygulanan tazminat usulünün uygulanabileceği ve fedakarlığın denkleştirilmesi ilkesi kapsamında idarenin kusursuz sorumluluğuna gidilebileceği belirtilmektedir. Diğer taraftan yargısal faaliyetler dolayısıyla hukuk sistemimizde devletin sorumluluğuna gidilemeyeceği kabul edilmektedir. Bu görüşe varılmasında ana faktörler özel hukuka ilişkin haksız fiil ve istihdam edene yönelik sorumluluk ilkelerinin idare hukuku bağlamında kullanılamaması, idare hukuku

ilkelerinin yargı faaliyetlerinde uygulanma olanağını bulunmaması ve kanuni olarak belirlenmiş tazminat hükümlerinin genelleştirilememesi olarak sıralanmaktadır. Çağlayan (2022) tarafından yapılan değerlendirmeye göre yargılama faaliyetleri dolayısıyla ortaya çıkan zararların fedakarlığın denkleştirilmesi ilkesi gereğince tazmin edilebileceği ifade edilmektedir. Bunun yanı sıra 5271 sayılı Ceza Muhakemeleri Kanunu kapsamında "koruma tedbirleri nedeniyle tazminat" hususu düzenleme altına alınmıştır. Bununla bağlantılı olarak zarar gören kişilerin tazminat talep edebilme hakkı bulunmaktadır. Yine bunun gibi 5237 sayılı Türk Ceza Kanunu'nun 257. maddesi bağlamında da görevini kötüye kullanan memura idare tarafından rücu edilebilen kusurlu sorumluluk hususu düzenlenmektedir (Çağlayan, 2022, sy.692-698).

4.3. Risk İlkesi Kapsamında İdarenin Sorumluluğu

Bu ilke idarenin gerçekleştirdiği tehlikeli faaliyetler ya da kullandığı tehlikeli araçlar sebebiyle risk sorumluluğu kapsamında idarenin zarar görenlerin zararını tazmin etme yükümlülüğü kapsamında değerlendirilmektedir. Fransız Danıştayı kararlarına da konu olan bu ilkeye "komşuluk riski" de denilmektedir (Çağlayan, 2022, sy.671) Risk ilkesi doğrultusunda idarenin sorumlu tutulabilmesi için belirli hususların bir araya gelmesi gerekmektedir. Bunların başında zararın olağanüstü ağırlıkta yani kamunun katlanması gereken olağan külfetleri aşan bir yapıda gerçekleşmiş olması gelmektedir. Bununla birlikte risk sorumluluğu kapsamında kastedilen risk sıradan veya adi bir risk değil, istisnai olarak kabul edilebilecek özel bir risktir. Diğer taraftan kusursuz sorumluluk daha önce de bahsedildiği üzere kusurun kanıtı gerekmeksizin idarenin sorumluluğuna gidilebilen yani idareye isnat edilebilen bir sorumluluk alanı oluşturmaktadır. Risk sorumluluğu kapsamında kusur karinesine imkân tanınmamakta, böylece kusursuzluğunu ispatla dahi ilgili idare sorumluluktan kurtulamamakta, zarar gören kişinin de idarenin kusurlu olduğunu ispat etmesi gerekmemektedir (Gözler, 2013, sy. 762-763).

Türk idare hukuku sisteminin Fransız hukukunu kaynak edinmesi ve teamüllerle gelişen bir hukuk alanı olmasından dolayı risk ilkesi kapsamında idarenin kusursuz sorumluluğu hallerinin Fransız Danıştayının kararlarından esinlenerek bir araya getirildiği değerlendirilmektedir. Gözler (2013) tarafından bahse konu risk ilkesinin tanımında da yer

alan tehlikeli şeyler bir liste halinde derlenmektedir. Bu kapsamda "tehlikeli şeyler": patlayıcı maddeler, tehlikeli alet ve ateşli silahlar, su, gaz ve elektrik gibi tehlikeli bayındırlık eserleri, idareye ait taşıtların verdiği zararlar ve kan ürünlerinin nakli olarak listelenmiştir. Diğer taraftan yine risk sorumluluğuna yol açan "tehlikeli yöntemler": genç suçluların eğitimleri, akıl hastalarının deneme çıkışları ve mahkumlara verilen çıkma izinleridir. Bunun yanı sıra "tehlikeli durumlar" kapsamında değerlendirilen hususlar da risk ilkesi kapsamında idarenin kusursuz sorumluluğuna vücut vermektedir. Kamu görevlilerinin görevlerini ifa ettikleri sırada "mesleki risk" olarak nitelenen iş kazaları ya da meslek hastalıkları gibi durumlarda da idare bu kapsamda sorumlu tutulmaktadır. Söz konusu mesleki riskler dolayısıyla oluşan tazminatlar memurlar ve işçilerin tabi oldukları sigorta kurum ve kuruluşları tarafından karşılanmaktadır. Bununla birlikte Danıştay tarafından verilen kararlarda söz konusu tazminatın idarenin sorumluluğu kapsamında hükmedilen tazminat miktarından veya sosyal haklardan düşülmesi uygulaması teamülen yerleşmiştir. Türk hukuk sistemi içerisinde meri mevzuatta yer alan özel yasal düzenlemeler de bu sorumluluk kapsamında tazminata hükmedilmesini sağlamaktadır (Gözler, 2013, sy. 766). Diğer taraftan idare hukukunda yer alan idari hasar kuramı kapsamında yalnızca tehlike arz eden kamu hizmetleri değil, sürekli gelişen teknoloji ile yeni gelişen kamu hizmetleri kapsamında da ele alınabileceği değerlendirilmektedir.

Eren (1998), idarenin risk ilkesi kapsamında sorumluluğunun idarenin eylem ve faaliyetleri ile bunlarda kullanılan araçların tehlikesi çerçevesinde bireylerin zarar görmesi durumunda faaliyeti yürüten kişilerin kusurlarına bakılmaksızın tazminat sorumluluğunun doğduğunu ifade etmektedir (Eren, 1998, sy. 14). Diğer taraftan kamu hizmetlerinin yerine getirilmesi için kamu personellerinin yanı sıra arızi işbirlikçi olarak nitelenen kişiler kısa süreliğine söz konusu hizmetler için kamu yararı amacıyla yardımcı olmaktadır. Bu kişilerin kamu hizmeti yerine getirilirken işledikleri kusurlar nedeniyle idareye isnatta bulunulamamaktadır. İdareye kusur atfedilemeyen bu durum için Fransız Danıştayı tarafından verilen kararlarda kusuru bulunmamasına rağmen idarenin söz konusu durumlarda da ortaya çıkan zararı tazmin etmesi gerektiği ifade edilmektedir (Gözler, 2013, sy. 767). Bunun yanı sıra bayındırlık eser ve işleri kaynaklı üçüncü kişilerin uğradığı zararlar kapsamında ülkemizde adli yargının görevli olduğu bilinmektedir. Öyle ki bayındırlık işlerinin ihale yoluyla özel kişilere yaptırılmayıp doğrudan idarece ifa edilmesi durumunda idare hukuku hükümleri uygulanabilecektir. Toplantı ve gösteri yürüyüşleri kapsamında oluşan zararların tazmin

edilmesi konusunda ülkemizin de idare hukukunda müktesebata vücut veren Fransız Danıştayı kararlarında devletin idare hukuku bağlamında sorumlu olduğu üzerinde kararlar verilmektedir. Öyle ki kusursuz sorumluluk çerçevesinde sosyal risk sorumluluğu kapsamında bu sorumluluk ortaya konulmaktadır. Ancak bazı Danıştay kararlarına bakıldığında sosyal olaylar dolayısıyla ilgisi olmadan zarara uğrayan kişiler için idarenin tazminat yükümlülüğü kapsamında kusursuz sorumluluğun yanı sıra, kusurlu sorumluluk ve idarenin sorumsuzluğu kararları verildiği görülmektedir (Çağlayan, 2022, sy. 679). Söz konusu kararlardaki tutarsızlık içtihatlara yönelik verilen bu olaylarda mahkemenin takdir yetkisi ile açıklanabilecektir.

Bu çalışmanın idare hukuku bağlamında asli konusunu oluşturan ve idarenin terörle mücadelesi kapsamında üçüncü kişilerin ortaya çıkan zararlarının tazmin edilmesine ilişkin temel kanun olan 5233 sayılı Terör ve Terörle Mücadeleden Doğan Zararların Karşılanması Hakkında Kanun çerçevesinde idarenin kusuru olmasa dahi idari sorumluluğu kapsamında tazminat ödemesi öngörülmektedir. Örnek vermek gerekirse terörle mücadele kapsamında teröristlerle çatışma esnasında atılan patlayıcı ve yanıcı maddeler dolayısıyla taşınmazları zarar gören kişilerin uğradıkları zarar kadar tazminatı idare tarafından karşılanmaktadır. Söz konusu Kanunun 2. maddesinde terör faaliyetleri dolayısıyla ortaya çıkan zararlardan mağdur olan özel hukuk gerçek ve tüzel kişilerinin idarenin sorumluluğu kapsamında tazmini düzenlenmektedir. Bahse konu Kanun bağlamında idarenin, üçüncü kişilerin maddi zararlarını sulhen karşılama yöntemi kullanılarak tazmin etmesi hususu düzenlenmiştir. Bu özel usul kullanılarak sulhen karşılanacak zararlar 5233 sayılı Kanunun 7. maddesinde açıkça belirtilmiştir. Bahse konu maddenin lafzı aşağıdaki gibidir (Terör ve Terörle Mücadeleden Doğan Zararların Karşılanması Hakkında Kanun, 2004) :

> ***Madde 7-*** *Bu Kanun hükümlerine göre sulh yoluyla karşılanabilecek zararlar şunlardır:*
> *a) Hayvanlara, ağaçlara, ürünlere ve diğer taşınır ve taşınmazlara verilen her türlü zararlar.*
> *b) Yaralanma, engelli hâle gelme ve ölüm hâllerinde uğranılan zararlar ile tedavi ve cenaze giderleri.*
> *c) Terörle mücadele kapsamında yürütülen faaliyetler nedeniyle kişilerin mal varlıklarına ulaşamamalarından kaynaklanan maddî zararlar.*

Terörle mücadele esnasında zarar gören kişiler, mirasçılar ya da yetkili temsilcileri bahse konu Kanunun 6. maddesinde düzenleme altına alınan başvuru süresi, şekli, incelenmesi ve sonuçlandırılması kapsamında başvurularını gerçekleştirmektedir. Bu Kanun maddesi aşağıdaki şekildedir (Terör ve Terörle Mücadeleden Doğan Zararların Karşılanması Hakkında Kanun, 2004):

> *"Zarar gören veya mirasçılarının veya yetkili temsilcilerinin zarar konusu olayın öğrenilmesinden itibaren altmış gün içinde, herhâlde olayın meydana gelmesinden itibaren bir yıl içinde zararın gerçekleştiği veya zarar konusu olayın meydana geldiği il valiliğine başvurmaları hâlinde gerekli işlemlere başlanır. Bu sürelerden sonra yapılacak başvurular kabul edilmez. Bu Kanun kapsamındaki yaralanma ve engelli hâle gelme durumlarında, yaralının hastaneye kabulünden hastaneden çıkışına kadar geçen süre, başvuru süresinin hesaplanmasında dikkate alınmaz."*

Terör olayları nedeniyle kişilerin uğradıkları zararlar üzerine bir başkan ve altı üyeden oluşan zarar tespit komisyonları zarar gören kişilerin valiliğe başvurusundan itibaren on gün içerisinde salt çoğunlukla toplanarak üye tam sayısının salt çoğunluğu ile karar verir. Burada dikkat çekilecek bir diğer nokta ise başvuruların dava açma süresince yapılması durumunda başvuruya ilişkin sonucun tebliğine kadar dava açma süreleri durmaktadır. Komisyon tarafından zarar tespiti ve ödenecek tutar tespiti yapılarak sulhname tasarısı hazırlanmaktadır. Zararın karşılanması bakımından sulhnamenin imzalanmasının ardından valinin onayı ile ifa türüne ilişkin Bakanlık bütçesinden söz konusu zararların karşılanması için ayrılan ödenek üç ay içerisinde zarar miktarı başvuru sahibine ödenmektedir. Sulhname tasarısının kabul edilmemesi halinde ya da komisyon tarafından ilgiliye gönderilen davet yazısına otuz gün içerisinde icabet edilerek imza edilmemesi ve bu sebeple de Kanunun 12. maddesi çerçevesinde sulhnamenin kabul edilmemiş sayılması halinde ise uyuşmazlık tutanağı düzenlenerek ilgililere tebliğ edilmektedir. Başvuru sahiplerinin sulhen çözüm bulunamayan durumlarda genel hükümlere göre idari yargı yoluna başvurması mümkündür. Söz konusu yargı yolunda açılacak tam yargı davası kapsamında idarenin kusursuz değil kusurlu sorumluluğu kapsamında yargılama yapılmaktadır (Terör ve Terörle Mücadeleden Doğan Zararların Karşılanması Hakkında Kanun, 2004).

1990 yılından önceki Danıştay kararlarında terör olaylarına yönelik olarak mahkeme tarafından hizmet kusuru yorumu yapılmaktaydı. 90'lı yıllardan sonra ise söz konusu olayların yorumunda idarenin kusursuz sorumluluğu üzerinden gidilmiştir. Terör faaliyetlerine karşılık idarenin yerine getirmekle yükümlü olduğu güvenlik önlemlerini yerine getirmemesi durumunda söz konusu olaylardan sorumluluk atfedilebiliyorsa kusurlu sorumluluk söz konusu olacaktır (Çağlayan, 2022, sy.680-681).

Risk ilkesi kapsamında idarelerin tazmin yükümlülüğü ile yaptırıma tabi tutulması için belirli başlı şartların oluşması gerekmektedir. Ancak bundan önce idarenin sorumluluğu için gerekli olan şartların ortaya konulması önem arz etmektedir. Bu kapsamda sorumluluk için fiilin mevcudiyeti, kusurlu idari fiil, zarar ve illiyet bağı gibi şartlar duruma göre farklılık arz etmektedir. Öncelikli şart olan fiilin mevcudiyeti idarenin kusurlu ve kusursuz sorumluluğu kapsamında icrai veya ihmali idari işlem ve eylemler şeklinde ortaya çıkmaktadır. Söz konusu idari işlem ve eylemlerin doğrudan idarenin tasarrufunda gerçekleşmesi gerekliyken, istisnai olarak idare ile iş birliği içerisinde idari faaliyetlerde bulunan kişilerin işledikleri kusurlu davranışlardan idare sorumlu olabilmektedir. Bunun yanı sıra idare ile imzalanan imtiyaz sözleşmesi sahipleri tarafından gerçekleştirilen eylem ve işlemler idareye isnat edilememekte, özel hukuk kişilerine karşı yönlendirilmektedir. Yalnızca imtiyaz sahiplerinin aczi durumunda idare de söz konusu tazminat dolayısıyla ikincil olarak sorumlu olabilmektedir (Gözler, 2013, sy. 780-785). Diğer taraftan idare ile bir özel hukuk kişisi arasında kamu hizmeti dolayısıyla iş gördürme usulü bulunuyorsa sorumluluk idareye yüklenebilecektir. Buna benzer olarak kamu idareleri arasında diğeri adına işlem ve eylemde bulunma durumunda yürütülen hizmetlerde hizmeti yürüten idarenin verdiği zarar nedeniyle hizmetin gerçek sahibi olan idareye sorumluluk atfedilebilecektir (Çağlayan, 2022, sy.700).

Fiilin mevcudiyeti ve bu fiilin kusurlu olmasının yanı sıra bir diğer şart olan zarar şartının da idarenin sorumluluğu kapsamında etki doğurabilmesi için belirli başlı şartlara sahip olması gerekmektedir. Öyle ki zarar unsurundan bahsedilebilmesi için zarar gören kişinin mal varlığı (mamelek) veya şahıs varlığından eksilmeye yol açacak bir zararın mevcudiyeti olmalıdır. Bununla beraber idari sorumluluğun tazmin edici özelliğinden dolayı zarar gerçekleşmiş olmalıdır. Bahse konu zarar kapsamında kusursuz sorumluluğa hükmedilebilmesi için zararın özel ve olağandışı olması gerekmekte, yani tüm toplumun

değil belirli bir kişi veya kesimin zarar görmesi ve belirli ağırlık derecesinde gerçekleşmiş olmalıdır (Duran, 1974). Bir diğer şart olan kesinlik şartı ise mevcut durumda veya olayın devamı niteliğinde ileride de gerçekleşecek kesin durumlara yönelik olan, doğması muhtemel zararları kapsamına almayan ancak ciddi şans kaybı olarak nitelenen bazı durumları içeren zorunlu unsurlardandır (Gözler, 2013, sy. 780-785). Danıştay kararlarında söz konusu durumların gerekçesinde "ihtimale dayalı, muhtemel ve tahakkuk etmemiş zarar" yorumu yapılmaktadır. Zarar için gerekli bir diğer şart ise zarara uğradığını iddia eden kişinin hakkının ihlal edilmesi veya bu kişinin hukuken korunan menfaatine ilişkin bir davranış sonucunda zararın oluşmasıdır. Zararın ön şartı olarak kabul edilebilecek olan bu şart zarar gören kişinin hukuka aykırı ve gayri meşru olarak nitelenebilecek bir durumda olmaması ve bu kapsamda hukuki sınırlar içerisinde korunan menfaatlere yönelik olmasını gerekli kılmaktadır (Çağlayan, 2022, sy.702-704). Ortaya çıkan zararın tazminata hükmedilebilmesi için para ile ölçülebilir mameleke yönelik bir zarar olması gerekmektedir.

Maddi zararlar niteliği itibariyle para karşılığı olan zararlardır. Maddi olarak malvarlığının aktifinde azalma veya pasifinde artma şeklinde ortaya çıkabilmektedir. Bununla beraber yoksun kalınan kar ve değer kayıpları da maddi zararlardan sayılabilecektir. Ancak şahıs varlığına yönelik olan manevi zararlar kural olarak para ile ölçülebilir kabul edilse dahi uygulamada belirli manevi zarara yol açan durumlarda tazminat oluşmaktadır. Söz konusu durumlara; manevi değerlere yönelik durumlar, yüzde kalıcı yara izine yol açan veya diğer uzuvlarda benzeri estetik zararlara yol açan durumlar, belirli sınırı aşan fiziksel acılar, yakınının vefat etmesi gibi olaylarda duyulan manevi acılar ve hayat şartlarındaki bozulmalar tadadi şekilde örnek verilebilir. Diğer taraftan sadece kusursuz sorumlulukta söz konusu olan, zararın özel ve anormal yani belirli ağırlığı aşan zararlar olması hususu burada da kusursuz sorumluluk bakımından gerçekleşmesi zorunlu olan hususlardır (Gözler, 2013, sy. 780-785). İdarenin sorumluluğuna ilişkin son zorunlu şart ise illiyet bağı yani nedensellik bağı şartıdır. Düren (1979) hayatın olağan akışı içerisinde idarenin sorumluluğuna neden olan zararın idarenin faaliyeti ile bağıntılı olması durumunda illiyet bağının oluştuğunu ifade etmektedir. İlliyet bağı, neden-sonuç ilişkisini ortaya koyan ve zararın sorumluluk makamı ile olan doğrudan bağını nitelemektedir. Söz konusu bağ idareye atfedilebilecek bir fiil kaynaklı ve idarenin doğrudan illiyet bağı kurulabilen fiilinden dolayı olmalıdır. İlliyet bağı hem kusurlu hem de kusursuz sorumluluk için geçerli olmakla birlikte bu bağ bazı durumlarda kısmen veya tümüyle kesilebilmektedir (Düren, 1979, sy. 329).

Diğer taraftan idarenin sorumluluğu zararla sorumlu makam arasında doğrudan bir bağ kurulmasını sağlayan illiyet bağı ile doğru orantılı olarak azalabilmekte hatta bazı durumlarda ortadan kalkabilmektedir. İlliyet bağını kesen sebepler mücbir sebep, beklenmeyen hal, zarar görenin davranışı ve üçüncü kişinin davranışıdır. Ancak Danıştay'ın bazı kararlarına göre söz konusu illiyet bağının aranmayacağına dair sonuçlar ortaya çıkmaktadır. Terör olayları kapsamında risk sorumluluğu söz konusu olduğunda sosyal riskler dolayısıyla idarenin sorumluluğuna gidilebilirken burada illiyet bağı şartı aranmayacaktır. Gözler (2013) tarafından yapılan değerlendirmede söz konusu Danıştay kararlarına göre kusursuz sorumluluğun nedensellik bağını kaldırması mümkün değildir. Gözler kusursuz sorumluluğun sadece kusur şartını ortadan kaldırdığını belirterek bu konuda verilen Danıştay kararlarını eleştirmektedir. İlliyet bağını kesen sebepler dolaylı olarak idarenin sorumluluğuna da ortadan kaldırmakta ya da söz konusu sorumluluğu azaltabilmektedir. Mücbir sebep, Gözübüyük (1977) tarafından "*sebep olduğu zarardan, makul bir suretle alınması gereken önleyici tedbirlerle kaçınılmayan, kaynağı teşebbüsün dışında olan olağanüstü bir hadise*" olarak nitelenmiştir (Gözübüyük, 1977). Mücbir sebepler idarenin kendi fiilinden kaynaklanmayan dışsal, öngörülemez, ağırlığı ve şiddeti itibariyle önlenemez nitelikte olan olayları ifade eder. Dışsallık idarenin faaliyetlerinin dışında kalan olayları, öngörülemezlik önceden tasavvur edilemeyecek nitelikteki olayları ve önlenemezlik ise idare tarafından söz konusu olayın gerçekleşmemesi için alınacak tedbirlere rağmen olayın gerçekleşmesinin önüne geçilememesini, ortaya çıkan zararın azaltılamaması veya ortadan kaldırılamamasını ifade etmektedir. Söz konusu önlenemezlik durumunun ortaya çıkıp çıkmadığının belirlenmesi için yargı yerinin işini kolaylaştıracak nitelikte bazı unsurlar bulunmaktadır. Bunlar arasında idare tarafından kamu hizmetinin ifası sırasında uygun bir yerin seçimi, uyarı ve gerekli düzenlemelerin yapılması ve etkin şekilde somut olaya göre araç ve gereçler ile tesislerin sağlanması sayılabilmektedir (Çağlayan, 2022, sy.710-712). Mücbir sebep durumunda idarenin sorumluluğu azalmamakta, kusurlu ve kusursuz olması fark etmeksizin sorumluluk doğrudan doğruya ortadan kalkmaktadır. Bu kapsamda idarenin sorumluluğuna gidilerek tazminat isteminde bulunulamamaktadır (Gözler, 2013, sy. 786-795). Ancak mücbir sebebe gidilebilecek olayda idarenin faaliyeti veya davranışı dolayısıyla neticenin daha da ağırlaşması durumunda idarenin kısmi sorumluluğu doğacaktır. Mücbir sebep olarak sayılan olayın hayatın olağan akışının dışında sıklıkla karşılaşılmayan bir durum oluşturması, olayın yer ve zaman olarak daha önceden

tahmin edilemeyen bir yapıda olması, olaya ilişkin yoğunluk derecesi, süre olarak uzunluğu ve olayın idarenin davranışının dışında doğal olarak gelişmesi mücbir sebebin taşıması gereken diğer niteliklerdir (Çağlayan, 2022, sy.710-712).

Beklenmeyen hal durumunda ise mücbir sebepten farklı olarak idarenin işlem ve eylemleri dolayısıyla yani dışarıdan herhangi bir fiil olmadan gerçekleşen olaylar söz konusudur. İçsellik olarak nitelenebilecek ve idarenin faaliyetleri sırasında gerçekleşen bir olay ortaya çıkmaktadır. Söz konusu beklenmeyen hale yol açan sebepler idarenin içinden kaynaklanmaktadır da denilebilir. Bahse konu içsellik önlenemez bir durumda ortaya çıkmalı ve idare bu olayı tüm tedbirleri alsa dahi kendi cebri gücüyle dahi engelleyemez konumda bulunmalıdır. Mücbir sebepte olduğu gibi öngörülemezlik ve önlenemezlik şartları burada da söz konusu olmaktadır. Beklenmeyen hallerde idareye kusur atfedilebilmekte ve idarenin sorumluluğu devam etmektedir. Beklenmeyen hal sadece kusuru ortadan kaldırdığı için kusurlu sorumluluğu tümüyle ortadan kaldırmakta ancak kusur şartı aranmayan kusursuz sorumluluk durumlarında idarenin sorumluluğu devam etmektedir (Onar, 1968, sy. 254).

Diğer taraftan zarar görenin davranışı dolayısıyla fiil doğrudan idareye atfedilemiyorsa yani nedensellik bağı kurulamıyorsa idarenin kusurlu ve kusursuz sorumluluğu ortadan kalkmaktadır. Bir diğer deyişle zarar gören mağdurun kendi hareketi dolayısıyla somut olay özelinde idareye atfedilebilme şartı ortadan kalkabilecek ve idarenin mesuliyeti söz konusu olmayabilecektir (Onar, 1968, sy.1721). Zarar görenin hukuk dışı konumu veya durumu dolayısıyla uğradığı zararın sorumluluğu kapsamında idareye isnatta bulunulamamaktadır. Bunun yanı sıra mağdur tarafından zarara yol açan risklerin önceden bilinerek üstlenilmesi durumunda idare söz konusu zarardan sorumlu tutulamamaktadır. Bununla birlikte zarar görenin kusuru ile idarenin kusuru birleşiyorsa yani her iki tarafın da kusurunun bulunduğu müterafik bir davranışta zarar görenin kusuru oranında tazminatta indirim yapılabilmektedir. Bu kapsamda orantısal olarak idarenin sorumluluğu azalmakta ve sorumluluk taraflara pay edilmektedir (Çağlayan, 2022, sy.719-720).

Buna benzer olarak üçüncü kişilerin kusurlu veya kusursuz davranışları dolayısıyla idarenin sadece kusurlu sorumluluğu azalabilmekte veya ortadan kalkabilmektedir. Atay (2006) kusursuz sorumluluk durumunda özellikle de risk ilkesi çerçevesinde üçüncü kişilerin fiillerinin idarenin sorumluluğunu azaltıcı veya ortadan kaldırıcı etkisi bulunmadığını ifade

etmiştir (Atay, 2006, sy.182). Bu durumda idari yargıda idareye karşı dava açılarak tazminat sorumluluğuna idare katlanacaktır. Söz konusu tazminat daha sonra idare tarafından üçüncü kişiye rücu edilebilmektedir (Çağlayan, 2022, 724-726). Zarar gören kişi zarar gördüğü olayın idarenin sorumluluğuna giren kısmı için idari yargıda tazminat talebinde bulunabilmektedir. Bu tazminatın geri kalan kısmı için üçüncü kişilere karşı adli yargı kapsamında dava açılması gerekmektedir. Yani tazminat isteminin tümü idareye karşı açılacak dava ile alınamamaktadır. Bu husus idare hukuku kapsamında müteselsil sorumluluğun bulunmamasından kaynaklanmaktadır. Sonuç olarak mücbir sebep ve beklenmeyen hal durumlarında idarenin sorumluluğu ortadan kalkarken, zarar görenin veya üçüncü kişinin davranışları dolayısıyla ortaya çıkan zarar durumlarında sorumluluk tamamen veya kısmen ortadan kalkabilmektedir. Bunun yanı sıra mücbir sebep ve zarar görenin davranışı sonucu oluşan zararlar hem kusurlu hem de kusursuz sorumluluk üzerinde etki doğururken, beklenmeyen hal ve üçüncü kişinin davranışları durumunda oluşan zararlar sadece kusurlu sorumluluk üzerinde etki doğurmaktadır (Gözler, 2013, sy. 786-795).

4.4. İdarenin Sorumluluğu Kapsamında Zararın Tazmini

Zarar kavramı kişilerin mamelekinde ya da şahıs varlığı değerlerinde meydana gelen ve iradesizce oluşan azalmalar olarak nitelenmektedir. Bunun yanı sıra tazminat ise söz konusu eksilmeler dolayısıyla sorumluluğuna gidilen kişi veya kuruma görevli yargı yeri tarafından yüklenen ödev şeklinde tanımlanmaktadır (Akyılmaz, 1998, sy.170). İdarenin sorumluluğu kapsamında zarar gören tarafından tazminatın istenilebileceği sorumlu kamu tüzel kişisinin veya devlet tüzel kişisinin belirlenmesi gerekmektedir. Devlet tüzel kişiliği bakımından kamu hizmetlerine ilişkin faaliyetlerin bakanlıklar tarafından yürütüldüğü düşünüldüğünde söz konusu bakanlıkların kendi faaliyetleri dolayısıyla sorumlulukları doğmaktadır. Cumhurbaşkanlığına bağlı olan devlet birimlerinin yürüttükleri kamu hizmeti, işlem ve eylemlerinden ise Cumhurbaşkanlığı makamı sorumlu olmaktadır. Yargısal faaliyetler kapsamındaki işlem ve fiillerden Adalet Bakanlığı sorumlu iken, yasama faaliyetleri ve milletlerarası sözleşmeler kapsamında gerçekleştirilen işlem ve eylemlerden ise faaliyetin isnat edilebildiği bakanlık sorumlu olmaktadır (Çağlayan, 2022, sy.728).

Diğer taraftan kamu görevlilerinin birden çok kurum, kuruluş ve kamu tüzel kişiliğinde görevlendirilmesi durumunda kamu hizmeti dolayısıyla oluşan zarar hangi kamu tüzel kişiliğinin görev alanına giriyorsa sorumluluk söz konusu kamu tüzel kişiliğine atfedilebilecektir. Geçici olarak idarelerin yardımlaşması kapsamında yürütülen kamu hizmetleri kapsamında yardım eden değil yardım isteyen yani hizmetin asıl sahibi olan idarenin sorumluluğu bulunmaktadır. Bunun yanı sıra idari vesayet denetimi ilişkisine tabi idarelerin yürüttükleri faaliyetlerden doğan zararlar söz konusu olduğunda bu zararlardan vesayet denetimine tabi olan idare sorumlu olmaktadır. Arızi işbirlikçilerin yardım etmek amaçlı idarenin faaliyetine iştirak etmesi dolayısıyla oluşan zararlardan ise idari işlem veya eylemin faaliyet ve görev alanına giren kamu tüzel kişisi sorumlu olmaktadır (Çağlayan, 2022, sy.728-729).

Bununla birlikte bazı zararlar birden çok kamu tüzel kişisinin sorumluluğu altında olabilir. Bu durumda ise zarara yol açma oranında kamu tüzel kişileri sorumluluğa katlanır. Söz konusu sorumlu kamu tüzel kişisine karşı idari yargı çerçevesinde açılacak tam yargı davası ile tazminat isteminde bulunulmaktadır. Söz konusu tam yargı davası idari işlemlerden, idari işlemlerin icrasından ve idari eylemlerden kaynaklı olarak açılabilmektedir. İYUK'un 2. maddesinin birinci fıkrasının b bendinde tam yargı davasının tanımı yapılmıştır. Söz konusu tanım "*idari eylem ve işlemlerden dolayı kişisel hakları doğrudan muhtel olanlar tarafından açılan tam yargı davaları*" şeklindedir. Bununla beraber tam yargı davasına ilişkin usuller İYUK'ta açıkça belirtilmektedir. İYUK'un "Üst makamlara başvurma" başlıklı 11.maddesi aşağıdaki şekildedir (İdari Yargılama Usulü Kanunu, 1982):

> *1. İlgililer tarafından idari dava açılmadan önce, idari işlemin kaldırılması, geri alınması, değiştirilmesi veya yeni bir işlem yapılması üst makamdan, üst makam yoksa işlemi yapmış olan makamdan, idari dava açma süresi içinde istenebilir. Bu başvurma, işlemeye başlamış olan idari dava açma süresini durdurur.*
> *2. Otuz gün içinde bir cevap verilmezse istek reddedilmiş sayılır.*
> *3. İsteğin reddedilmesi veya reddedilmiş sayılması halinde dava açma süresi yeniden işlemeye başlar ve başvurma tarihine kadar geçmiş süre de hesaba katılır.*

İdari işlemlerin icrası sebebiyle ortaya çıkan zararlar dolayısıyla İYUK'un 12. maddesi "İptal ve tam yargı davaları" başlığı ile düzenleme altına alınmıştır. Aşağıda söz konusu düzenlemeye yer verilmektedir (İdari Yargılama Usulü Kanunu, 1982):

> *İlgililer haklarını ihlal eden bir idari işlem dolayısıyla Danıştay'a ve idare ve vergi mahkemelerine doğrudan doğruya tam yargı davası veya iptal ve tam yargı davalarını birlikte açabilecekleri gibi ilk önce iptal davası açarak bu davanın karara bağlanması üzerine, bu hususstaki kararın veya kanun yollarına başvurulması halinde verilecek kararın tebliği veya bir işlemin icrası sebebiyle doğan zararlardan dolayı icra tarihinden itibaren dava süresi içinde tam yargı davası açabilirler. Bu halde de ilgililerin 11 nci madde uyarınca idareye başvurma hakları saklıdır.*

İdarenin eylemleri dolayısıyla zorunlu idari başvuruya ilişkin usuller ve ön karar alınmasına dair hususlar İYUK 13. maddesinde "Doğrudan doğruya tam yargı davası açılması" başlığı çerçevesinde düzenleme altına alınmıştır. Bu madde aşağıdaki gibidir (İdari Yargılama Usulü Kanunu, 1982):

> *1. İdari eylemlerden hakları ihlal edilmiş olanların idari dava açmadan önce, bu eylemleri yazılı bildirim üzerine veya başka suretle öğrendikleri tarihten itibaren bir yıl ve her halde eylem tarihinden itibaren beş yıl içinde ilgili idareye başvurarak haklarının yerine getirilmesini istemeleri gereklidir. Bu isteklerin kısmen veya tamamen reddi halinde, bu konudaki işlemin tebliğini izleyen günden itibaren veya istek hakkında otuz gün içinde cevap verilmediği takdirde bu sürenin bittiği tarihten itibaren, dava süresi içinde dava açılabilir.*
> *2. Görevli olmayan adli yargı mercilerine açılan tam yargı davasının görev yönünden reddi halinde sonradan idari yargı mercilerine açılacak davalarda, birinci fıkrada öngörülen idareye başvurma şartı aranmaz.*

Hakları ihlal edilen kişiler zorunlu idari başvuru yolu adı altında tam yargı davası açmadan önce hakkını ihlal ettiğini düşündüğü idari makama başvuru yapmaktadırlar. Bu zorunlu idari yol sonrasında idarenin kabul veya ret şeklinde verdiği karara da ön karar adı verilmektedir. Söz konusu ön karar tarihinden itibaren dava açma süresi içerisinde tam yargı davası açılabilmektedir.

4.5. İdarenin Tazminat Sorumluluğuna İlişkin Temel İlkeler

İdarenin sorumluluğuna ilişkin ilkeler nakden tazmin, sorumluluk nispetince tazmin, taleple bağlılık, tam tazmin ve denkleştirme ilkesi olarak sıralanabilecektir. Söz konusu ilkeler doğrultusunda tazminat isteyebilecek kişiler ise Danıştay'ın çeşitli kararlarında yer verildiği üzere zarar gören haricinde ölümle sonuçlanan idari olaylarda maktul ya da maktulenin annesi, babası, eşi, çocukları, kardeşleri, yetiştiren kişiler, birlikte yaşadığı kişi, nişanlısı ve duygusal bağ bulunan yakın akrabalarıdır. Bunun dışında bedensel zarar gören mağdurlar ve yakınları manevi tazminat talebinde bulunabilmektedir (Çağlayan, 2022, sy. 730-735). Nakden tazmin ilkesi ile kastedilen aynen tazmin yani fiili olarak tazmin değil, para karşılığı bir değerle mal varlığı değerinin aktifinde artışa yol açan nakden tazminat talebidir. Söz konusu nakden tazmin sermaye veya gelir yani geçici ya da ömür boyu irat şeklinde oluşabilmektedir. Bu ilkenin temeli yargı mercilerinin idareye emir ve talimat verememesi ile yakından ilişkilidir. Aynen tazminin mümkün olması durumunda yetkili yargı merciinin emri ile söz konusu idare "fiili yapma borcu" durumuna düşmektedir. Bu sebeple söz konusu nakden tazminat ilkesi idarenin sorumluluğunda tazminat için geçerli ilke konumundadır. Bunun yanı sıra idarenin verdiği zararla orantılı olarak nakdi bir tazminata hükmedilmesi gerekmektedir. Söz konusu ilkeye sorumluluk nispetince tazminat denilmektedir. İdare tarafından verilen zararın aşılarak zararın üstünde bir miktar kararlaştırılamaz.

Diğer taraftan hukuktaki genel ilkelerden olan "ultra petita karar verme yasağı" kapsamında davacının talebinden daha fazla nakdi miktara hükmedilememektedir. Söz konusu ilke taleple bağlılık ilkesi (ultra petita) olarak nitelenmektedir. Bu husus İYUK'un 3. maddesinin birinci fıkrasının d bendinde açıkça ifade edilmiştir. Söz konusu madde hükmünde tam yargı davaları açılırken dava dilekçesinde idarenin işlem ve faaliyetleri dolayısıyla ortaya çıkan zararın miktarının talep edilmesi gerekliliği ortaya konmuştur (İYUK, 1982). Taleple bağlılık ilkesi kapsamında mahkeme tarafından değerleme faizi adı altında faize hükmedilebilmesi için bahse konu faizin davacı tarafından maddi veya manevi tazminat talebiyle birlikte talep edilmesi gerekmektedir (Çağlayan, 2022, sy.738-741). İYUK'un 16. maddesinin dördüncü fıkrası kapsamında davacı tarafından talep edilen miktar, nihai karar verilinceye kadar herhangi bir usul ve süre şartına uyulmaksızın tek seferliğine artırılabilmektedir (İYUK, 1982). İdare hukuku kapsamında yer alan tam tazmin ilkesi

doğrultusunda idarenin verdiği zarar nedeniyle nakdi olarak zararın tam değerinde tazminata hükmedilmesi gerekmektedir. Söz konusu zararın tazmini neticesinde mağdurun malvarlığında fazlaca artma veya azalmaya neden olunmamalı, fakirleşme ya da zenginleşme durumu oluşmamalıdır.

Fransız Danıştayı içtihatlarına göre zararların hesaplanma tarihi mallara ve kişilere yönelik zararlara göre farklılık arz etmektedir. Öyle ki mallara yönelik zararların tazminatının hesaplanma tarihi zararın oluştuğu gün olarak belirlenirken, kişilere yönelik zararlarda hükmün verildiği günkü şartlar ve ekonomiye göre tazminat hesaplanmaktadır. Bunun yanı sıra feri tazminatlar adı altında açıkça talep edilmek şartıyla temerrüt faizlerine ve idarenin açık şekilde kötü niyetinden doğan telafi edici tazminatlara da mahkemenin takdir yetkisi doğrultusunda karar verilebilmektedir. Son olarak zararların öngörülememesi durumlarında ileriki zamanlarda ortaya çıkan zararlar ve zararların sonradan ağırlaşması durumlarında ilk tazminat kesin hüküm şeklinde verilse dahi yeni bir tazminat talebinde bulunulabilmektedir (Gözler, 2013, sy. 795-802). Çağlayan (2022) tarafından idarenin tazminine ilişkin temel ilkelerden denkleştirme ilkesi ise mağdurun uğradığı zarar neticesinde sosyal yardım ve sair kazançlar elde etmesi durumunda söz konusu kazanç miktarı tazminata hükmedilen miktardan düşülmelidir. Danıştay tarafından verilen kararlarda söz konusu kararlar doğrultusunda oluşan yerleşik içtihada göre 2030 sayılı Nakdi Tazminat ve Aylık Bağlanması Hakkında Kanun çerçevesinde mahkemece hükmedilen tazminat miktarlarında indirime gidileceği belirtilmektedir (Çağlayan, 2022, sy. 733).

Zararın tazminine ilişkin olarak İYUK'un 24. maddesinde mahkemeler tarafından verilen kararlarda açıkça tazminat miktarının belirtileceği ifade edilmektedir. Söz konusu tazminat sermaye şeklinde toptan ve defaten olabileceği gibi, mahkemenin takdirine bağlı olarak belirli bir süreçte ve sürekli olarak irat şeklinde de ödenebilmektedir (İYUK, 1982). Bununla beraber zararın tazmininde zararın meydana geldiği tarih, hesaplanacak tutarın belirlenmesinde temel tarih olarak esas alınmaktadır. Belirli bir sürece yayılan olaylarda Danıştay tarafından daha önce verilen kararlara bakıldığında olay başlangıç tarihinin temel alındığı görülmektedir. Çağlayan'a (2022) göre de maddi tazminata konu olaylarda mahkeme tarafından zararın tazmininin hesaplanmasında karar tarihi temel alınmalıdır. Söz konusu miktar belirlendikten sonra taleple bağlılık ilkesi gereğince talep sahibinin talep ettiği miktar zarar miktarından daha az ise söz konusu ilke doğrultusunda hareket edilmesi

gerektiği ifade edilmektedir. Çağlayan (2022) tarafından söz konusu talep miktarının mahkemenin hükmettiği tazminat miktarından az kalması durumunda dava yoluyla tamamlanması gerektiği değerlendirilmektedir. Bununla beraber manevi zararlar durumunda karar tarihi miktarın belirlenmesinde esas alınmaktadır (Çağlayan, 2022, sy.737).

3713 sayılı Terörle Mücadele Kanunu ve 5233 sayılı Terör Ve Terörle Mücadeleden Doğan Zararların Karşılanması Hakkında Kanun

Terör ve terörizmle mücadele kavramları devletlerin kara, hava ve deniz alanlarında karşılaştığı örgütlü suçlar bağlamında ele alınmaktadır. Terör kavramının tanımı 3713 sayılı Terörle Mücadele Kanunu'nun 1.maddesinde aşağıda yer verildiği şekliyle düzenleme altına alınmıştır (Terörle Mücadele Kanunu, 1991):

> *"Terör; cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir."*

Söz konusu tanımdaki ifadelerde devletin güvenliği, kamu düzeni, temel haklar, Anayasa ve Cumhuriyete karşı işlenen ve suç oluşturan eylemlere yer verilmektedir. 5233 sayılı Terör Ve Terörle Mücadeleden Doğan Zararların Karşılanması Hakkında Kanunun "Kapsam" başlıklı 2. maddesinde söz konusu tanıma atıf yapılarak burada yer verilen eylemler dolayısıyla meydana gelen maddi zararların sulhen karşılanmasına ilişkin usul ve esaslar düzenlenmektedir. Bahse konu Kanunun 2. maddesi aşağıdaki gibidir (Terör Ve Terörle Mücadeleden Doğan Zararların Karşılanması Hakkında Kanun, 2004):

> *"Bu Kanun, 3713 sayılı Terörle Mücadele Kanunu'nun 1 inci, 3 üncü ve 4 üncü maddeleri kapsamına giren eylemler veya terörle mücadele kapsamında yürütülen faaliyetler nedeniyle zarar gören gerçek kişiler ile özel hukuk tüzel kişilerinin maddî*

zararlarının sulhen karşılanması hakkındaki esas ve usullere ilişkin hükümleri kapsar.

Aşağıda belirtilen zararlar bu Kanunun kapsamı dışındadır:

a) Devletçe arazi veya konut tahsisi suretiyle yahut başka bir şekilde karşılanan zararlar.

b) Bir mahkeme kararı gereğince veya 4353 sayılı Maliye Vekaleti Baş Hukuk Müşavirliğinin ve Muhakemat Umum Müdürlüğünün Vazifelerine, Devlet Davalarının Takibi Usullerine ve Merkez ve Vilayetler Kadrolarında Bazı Değişiklikler Yapılmasına Dair Kanunun 30 uncu ve 31 inci maddeleri gereğince karşılanan zararlar.

c) Avrupa İnsan Hakları Mahkemesince, İnsan Haklarını ve Ana Hürriyetleri Korumaya Dair Sözleşmenin veya eki protokollerin ihlâl edildiği gerekçesiyle Sözleşmenin 41 inci maddesine göre hükmedilen veya Sözleşme hükümleri uyarınca dostane çözüm yoluyla uzlaşılan tazminatın ödenmesi sonucunda karşılanan zararlar.

d) Terör dışındaki ekonomik ve sosyal sebeplerle uğranılan zararlar ile güvenlik kaygıları dışında kendi istekleriyle bulundukları yerleri terk edenlerin bu sebeple uğradıkları zararlar.

e) Kişilerin kendi kasıtları sonucunda oluşan zararlar.

f) 3713 sayılı Kanunun 1 inci, 3 üncü ve 4 üncü maddeleri kapsamındaki suçlar ile terör olaylarında yardım ve yataklık suçlarından mahkûm olanların bu fiillerinden dolayı uğradığı zararlar.

İkinci fıkranın (f) bendinde yazılı suçlardan dolayı ceza kovuşturması açılmış bulunanlar hakkında kovuşturma sonuçlanıncaya kadar bu Kanuna göre işlem yapılmaz."

Söz konusu madde hükmünde aynı zamanda 3713 sayılı Terörle Mücadele Kanunu'nun 3. ve 4. maddelerinde yer verilen terör suçları ve terör amacı ile işlenen suçlara atıf yapılarak bu suçların da 5233 sayılı Kanun kapsamında tazminat sorumluluğunu doğuracağı ifade edilmektedir. Terörle Mücadele Kanunu'nun "Terör suçları" başlıklı 3.maddesi aşağıdaki gibidir (Terörle Mücadele Kanunu, 1991):

"Madde 3 – *26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 302, 307, 309, 311, 312, 313, 314, 315 ve 320 nci maddeleri ile 310 uncu maddesinin birinci fıkrasında yazılı suçlar, terör suçlarıdır."*

Bu madde incelendiğinde ise terör suçu olarak değerlendirilen suçların 5237 sayılı Türk Ceza Kanununun (TCK) "Millete ve Devlete Karşı Suçlar ve Son Hükümler" başlıklı dördüncü kısmın "Devletin Güvenliğine Karşı Suçlar" başlıklı dördüncü bölümünde düzenlenen "Devletin birliğini ve ülke bütünlüğünü bozmak", "Askerî tesisleri tahrip ve düşman askerî hareketleri yararına anlaşma"; dördüncü kısmın "Anayasal Düzene ve Bu Düzenin İşleyişine Karşı Suçlar" başlıklı beşinci bölümünde düzenlenen "Anayasayı ihlal", "Cumhurbaşkanına suikast ve fiilî saldırı", "Yasama organına karşı suç", "Hükûmete karşı suç", "Türkiye Cumhuriyeti Hükûmetine karşı silâhlı isyan", "Silâhlı örgüt", "Silâh sağlama" ve dördüncü kısmın "Milli Savunmaya Karşı Suçlar" başlıklı altıncı bölümde düzenlenen "Yabancı hizmetine asker yazma, yazılma" suçlarını kapsadığı görülmektedir.

Bununla birlikte Terörle Mücadele Kanunu'nun "Terör amacı ile işlenen suçlar" başlıklı 4.maddesi aşağıdaki gibidir (Terörle Mücadele Kanunu, 1991):

Madde 4 – *Aşağıdaki suçlar 1 inci maddede belirtilen amaçlar doğrultusunda suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlendiği takdirde, terör suçu sayılır:*

a) Türk Ceza Kanunu'nun 79, 80, 81, 82, 84, 86, 87, 96, 106, 107, 108, 109, 112, 113, 114, 115, 116, 117, 118, 142, 148, 149, 151, 152, 170, 172, 173, 174, 185, 188, 199, 200, 202, 204, 210, 213, 214, 215, 223, 224, 243, 244, 265, 294, 300, 316, 317, 318 ve 319 uncu maddeleri ile 310 uncu maddesinin ikinci fıkrasında yer alan suçlar.

b) 10/7/1953 tarihli ve 6136 sayılı Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanunda tanımlanan suçlar.

c) 31/8/1956 tarihli ve 6831 sayılı Orman Kanunu'nun 110 uncu maddesinin dördüncü ve beşinci fıkralarında tanımlanan kasten orman yakma suçları.

ç) 10/7/2003 tarihli ve 4926 sayılı Kaçakçılıkla Mücadele Kanununda tanımlanan ve hapis cezasını gerektiren suçlar.

d) Anayasanın 120 nci maddesi gereğince olağanüstü hal ilan edilen bölgelerde, olağanüstü halin ilanına neden olan olaylara ilişkin suçlar.

e) 21/7/1983 tarihli ve 2863 sayılı Kültür ve Tabiat Varlıklarını Koruma Kanununun 68 inci maddesinde tanımlanan suç."

Söz konusu maddeye bakıldığında 5237 sayılı TCK'da düzenleme altına alınan çeşitli suç tiplerin bulunduğu, bununla beraber TCK'nın "Topluma Karşı Suçlar" başlıklı üçüncü kısmının "Bilişim Alanında Suçlar" başlıklı onuncu bölümünün 243. ve 244. maddeleri "Bilişim sistemlerine girme" ve "Sistemi engelleme, bozma, verileri yok etme veya değiştirme" başlıkları altında terör amacı ile işlenen suçlar arasında yer almaktadır.

Bu kapsamda değerlendirme yapıldığında, terör amacı ile işlenen suçlar arasında yer alan ve TCK'nın 243. ve 244. maddeleri çerçevesinde işlenen bilişim sistemlerine girme, sistemlerde kalarak engelleme, bozma, yok etme ve değiştirme gibi fiiller terör tanımına uygun şekilde terör örgütüne ait faaliyetler kapsamında işlenmesi durumunda terör suçu sayılmaktadır. Bahse konu maddeler kapsamında gerçekleştirilen fiiller siber uzam bağlamında değerlendirildiğinde devleti ve vatandaşları etkileyen siber saldırılara karşılık geldiği görülmektedir. Öyle ki bilgisayar korsanlığı, virüs, solucan, truva atı, mantık bombası, çatal bomba ve bukalemun saldırısı gibi kötücül yazılımlar, casus program ve yazılımlar, arka kapılar, korsan amaçlı yazılımlar, sıfırıncı gün saldırıları, veri ihlâli saldırıları, ortadaki adam ve SQL enjeksiyon saldırıları vasıtasıyla bilişim sistemlerine yetkisiz erişim sağlanabilmekte; dağıtık hizmeti engelleme, köle bilgisayar ağları, gelişmiş kalıcı tehdit, web sitesi tahrifatı ve veri aldatmacası saldırıları yoluyla da yetkisiz erişim sağlanan sistemlerdeki verilere yönelik bahse konu engelleme, bozma, yok etme ve değiştirme işlemleri gerçekleştirilebilmektedir.

Meri mevzuat kapsamında değerlendirme yapıldığında sürekli olarak değişen ve gelişen bilgi ve iletişim teknolojileri çerçevesinde siber saldırılar da devamlı şekilde değişime uğramaktadır. Özellikle yapay zekâ tabanlı olarak geliştirilen programlar, sistemler özelinde güvenlik zafiyetlerini tespit ederek etki gücü yüksek siber saldırılara neden olunmaktadır. Bu sebeple TCK'da bilişim suçları adı altında düzenleme altına alınan 243, 244 ve 245. maddelerin siber saldırganlarca sürekli olarak geliştirilen siber saldırılara karşı yetersiz kalacağı değerlendirilmektedir. Birleşmiş Milletler bünyesinde çalışmaları halihazırda devam eden bilgi ve iletişim teknolojilerinin suç amaçlı kullanımı hakkında uluslararası sözleşme kapsamında sibere bağımlı suçların yanı sıra siberle ilgili ve siberin

kolaylaştırdığı suç tipleri de tartışmaya açılarak detaylı şekilde ele alınmaktadır. Bu kapsamda yeni suç tiplerinin geliştiği ve klasik suçlara entegre şekilde işlenen siber suçların ortaya çıkacağı değerlendirilmektedir. Söz konusu alanda ülkemizde birincil seviyede siber suçlar kanunu ve siber güvenlik kanununun oluşturulması gerekliliği ortaya çıkmaktadır (Yağcı, 2023).

4.6. Siber Terörizm ile Tazminat Yükümlülüğü İlişkisi

Siber terörizm, idarenin sorumluluğu kapsamında değerlendirildiğinde devletin vatandaşlarına karşı tazmin yükümlülüğü gündeme gelmektedir. İdare tarafından gerçekleştirilen tehlikeli faaliyetler veya kullanılan tehlikeli araçlar sebebiyle sosyal risk ilkesi kapsamında risk sorumluluğu doğmakta ve idarenin zarar görenlerin zararını tazmin etme yükümlülüğü ortaya çıkmaktadır (Gözler, 2013, sy. 741). Değişen ve gelişen teknolojik ortamda siber saldırılar da farklılaşmakta ve vatandaşlara yönelik maddi ve manevi zararlarla karşılaşılmaktadır. Siber saldırılar neticesinde kişisel verilere erişim sağlanabilmekte, banka hesap bilgileri ele geçirilebilmekte, bu bilgiler karanlık ağda satılarak kazanç sağlanabilmekte ve terörist faaliyetlere yol açılarak devletlerin kritik altyapılarını da etkileyen yıkıcı faaliyetler yürütülebilmektedir. Bu vasıtayla vatandaşlar siber güvenlik önlemlerini yeterli seviyede almayan devletler nedeniyle temel ihtiyaçlarına kadar uzanan sosyal hizmetlerden mahrum kalabilmektedir.

İdarenin faaliyet alanına giren idari olay ve konularda önleme yükümlülüğü çerçevesinde siber güvenlik önlemlerinin alınmaması neticesinde gerçekleşen siber saldırılarla kişilere ait mal varlıkları zarar görebilmektedir. Maddi zararların yanı sıra söz konusu saldırılar sonucunda manevi zararlar da oluşabilmektedir. İdare hukukunda sosyal risk kavramı genellikle klasik terör olayları neticesinde vatandaşların gördüğü zararlara karşı idarenin sorumluluğuna gidildiği durumlarda söz konusu olmaktadır. Ancak siber saldırılar neticesinde de gerçekleşebilecek maddi ve manevi zararların idarenin sorumluluğu kapsamında tazmin edilmesi hususu gelişen teknolojilerle birlikte düzenleme altına alınması gereken bir görünüm kazanmıştır. Siber saldırılar yapıları gereği devletleri hedefleyerek siber terörizme yol açtığı kadar bireysel saldırılar şeklinde de ortaya çıkabilmektedir. Danıştay tarafından verilen kararlarda söz konusu bireysel terör saldırıları çerçevesinde de

idarenin sosyal risk ilkesi çerçevesinde sorumluluğuna gidilmiştir. Bu karar doğrultusunda anayasaya uygun olarak hakkaniyet esasına dayanılıp kişilerin uğradığı zararlar tazmin edilmektedir. Bahse konu hususa ilişkin Danıştay İdari Dava Daireleri Kurulunun ilgili E:2015/2652, K:2017/1271 sayılı kararında yer verilen gerekçe aşağıdaki gibidir (Danıştay İdari Dava Daireleri Kurulu, 2017):

> "*İdarenin hukuki sorumluluğu, kamusal faaliyetler sonucunda, idare ile bireyler arasında bireyler zararına bozulan ekonomik dengenin yeniden kurulmasını, idari etkinliklerden dolayı bireylerin uğradığı maddi zararlar yanında manevi zararların da idarece tazmin edilmesini sağlayan bir hukuksal kurumdur. Bu kurum, kamusal faaliyetler nedeniyle bireylerin malvarlığında ortaya çıkan eksilmelerin ya da çoğalma olanağından yoksunluğun giderilebilmesini, yine bu surette oluşan manevi zararların karşılanabilmesi için aranılan koşulları, uygulanması gereken kural ve ilkeleri içine almaktadır.''*

Söz konusu kararda yer verilen gerekçede idare tarafından kamusal faaliyetler yerine getirilirken bireylerin karşı karşıya kaldığı zararların sosyal risk ilkesi çerçevesinde tazmininin mümkün olduğu, idarenin bu tazminat sorumluluğuna hem maddi hem de manevi olarak katlanması gerektiği, mal varlığının pasifindeki artış ya da aktifindeki eksilmelerle birlikte yoksun kalınan kârdan dolayı da söz konusu yükümlülüğün ortaya çıkabileceği ifade edilmiştir.

Bununla birlikte Danıştay İdari Dava Daireleri Kurulunun söz konusu konuya dair verdiği bu kararın gerekçesinde sosyal risk ilkesinin tazminat yükümlülüğüne vücut veren terör suçlarında araç olarak kullanıldığı, nedensellik bağı bulunmayan durumlarda bahse konu ilkenin gündeme geleceği, nedensellik bağı yoksa ilk olarak hizmet kusuru o da yoksa kusursuz sorumluluk kapsamında olayın incelenmesi gerektiği ifade edilmektedir (Danıştay İdari Dava Daireleri Kurulu, 2015/2652 E.N, 2017/1271 K.N):

> *''Görüldüğü üzere; 5233 sayılı Yasa, yargısal ve bilimsel içtihatlarla kabul edilen "sosyal risk" ilkesinin yasalaşmış halidir. Bu nedenle, adı geçen Yasanın uygulama alanı yalnızca "sosyal risk ilkesi" uyarınca tazmini mümkün olan uyuşmazlıklarla sınırlı bulunmaktadır. Başka bir ifadeyle, zarar ile idari eylem arasında nedensellik*

bağının kurulabildiği hallerde sosyal risk ilkesinin uygulanmasına olanak bulunmadığından; bu gibi hallerde öncelikle, idare hukuku kuralları çerçevesinde hizmet kusurunun bulunup bulunmadığının araştırılması, hizmet kusuru yoksa kusursuz sorumluluk ilkesine göre zararın tazmin edilip edilemeyeceğinin belirlenmesi; dolayısıyla, idari eylemlerden doğan zararın, hizmet kusuru veya kusursuz sorumluluk ilkeleri uyarınca tazmini gereken davalarda, 2577 sayılı Yasanın 13. maddesinin uygulanması gerekmektedir." (Kaynakça: https://www.danistay.gov.tr/assets/pdf/yayinlar/dergi/15_05_2018_114253.pdf)

Diğer taraftan Danıştay İdari Dava Daireleri Kurulunun E:2013/4602, K:2014/1220 sayılı kararında yer verilen gerekçe aşağıdaki gibidir (Danıştay İdari Dava Daireleri Kurulu, 2013/4602 E.N, 2014/1220 K.N.):

"İdarenin hukuki sorumluluğu, kamusal faaliyetler sonucunda, idare ile bireyler arasında bireyler zararına bozulan ekonomik dengenin yeniden kurulmasını, idari etkinliklerden dolayı bireylerin uğradığı maddi zararlar yanında manevi zararların da idarece tazmin edilmesini sağlayan bir hukuksal kurumdur. Bu kurum, kamusal faaliyetler nedeniyle bireylerin malvarlığında ortaya çıkan eksilmelerin ya da çoğalma olanağından yoksunluğun giderilebilmesini, yine bu surette oluşan manevi zararların karşılanabilmesi için aranılan koşulları, uygulanması gereken kural ve ilkeleri içine almaktadır. İdare, Anayasamızın 125. maddesinde de belirtildiği üzere, kural olarak yürüttüğü kamu hizmetiyle nedensellik bağı kurulabilen zararları tazminle yükümlü olup; idari eylem ve/veya işlemlerden doğan zararlar idare hukuku kuralları çerçevesinde, hizmet kusuru veya kusursuz sorumluluk ilkeleri gereği tazmin edilmektedir. Bunun yanında, idarenin faaliyet alanıyla ilgili, önlemekle yükümlü olduğu halde önleyemediği birtakım zararları da nedensellik bağı aramadan tazmin etmesi gerekmektedir. İdarenin kusura dayalı ya da kusursuz sorumluluğu yanında, Anayasanın öngördüğü sosyal hukuk devleti anlayışına uygun olarak ve bu temel üzerinden, kolektif sorumluluk anlayışı çerçevesinde bilimsel ve yargısal içtihatlar ile geliştirilen sosyal risk ilkesi, Anayasanın yukarıda öngördüğü amaçların gerçekleştirilmesine yöneliktir."

Söz konusu gerekçede idarenin hukuki sorumluluğunun hem maddi hem de manevi tazminatları kapsadığı, idarenin eylemi ile illiyet bağı olan zararların hizmet kusuru ya da kusursuz sorumluluk kapsamında ele alınacağı ancak idare tarafından önlenmekle yükümlü olunmasına rağmen önlenemeyen zararlar kapsamında sosyal devlet ilkesi gözetilerek sosyal risk ilkesinin uygulanması gerekliliği ifade edilmiştir.

Terör olayları kapsamında yukarıda yer verilen karardaki bir diğer gerekçe de aşağıdaki gibi ifade edilmiştir (Danıştay İdari Dava Daireleri Kurulu, 2013/4602 E.N, 2014/1220 K.N.):

> *"Sosyal risk ilkesi ile toplumun içinde bulunduğu koşullardan kaynaklanan, idarenin faaliyet alanında meydana gelmekle birlikte, yürütülen kamu hizmetinin doğrudan sonucu olmayan, toplumsal nitelikli riskin gerçekleşmesi sonucu oluşan, salt toplumun bireyi olunması nedeniyle uğranılan özel ve olağandışı zararların da topluma pay edilerek giderilmesi amaçlanmıştır. Genel bir ifade ile "terör olayları" olarak nitelenen eylemlerin, Devlete yönelik olduğu, Anayasal düzeni yıkmayı amaçladığı, bu tür olaylarda zarar gören kişi ve kuruluşlara karşı kişisel husumetten kaynaklanmadığı bilinmekte ve gözlenmektedir. Sözü edilen olaylar nedeniyle zarara uğrayan kişiler, kendi kusur ve eylemleri sonucu değil, toplumun bir bireyi olmaları nedeniyle zarar görmektedirler. Belirtilen şekilde ortaya çıkan zararların ise, özel ve olağandışı nitelikleri dikkate alınıp, terör olaylarını önlemekle yükümlü olduğu halde önleyemeyen idarece, yukarıda açıklanan sosyal risk ilkesine göre, topluma pay edilmesi suretiyle tazmini hakkaniyet gereği olup, sosyal devlet ilkesine de uygun düşecektir."*

Söz konusu gerekçede terör faaliyetleri kapsamında Devlete yönelen veya Anayasal düzeni yıkma girişimini içeren çeşitli saldırılardan sadece o devletin vatandaşı olduğu için zarar gören kişilerin, somut olayda özel ve olağandışı koşulların sabit olması üzerine uğradıkları zararlar hakkaniyet gereği tazmin edilmektedir. Siber saldırılar neticesinde de bahse konu saldırıdan zarar gören kişiler devletlere ait kritik altyapılara yapılan siber saldırıdan olumsuz etkilenmesi durumunda maddi ve manevi olarak tazminat alma hakkına kavuşacaktır. Bu hakların elde edilmesi doğrultusunda hak kayıplarının büyük oranda azalacağı değerlendirilmektedir. Siber güvenlik önlemlerinin idare tarafından gereklerinin

yerine getirilmemesi, siber savunma araçlarının gerektiği gibi kullanılmaması, teknik ekipman ve insan kaynağı eksiği gibi hususlar da söz konusu tazminat yükümlülüğünün doğmasında etki doğurmaktadır. Söz konusu unsurların da somut olay özelinde ele alınması gerektiği düşünülmektedir. Sosyal risk ilkesi bağlamında siber terörizmin ele alınarak hakkaniyet ilkesi doğrultusunda sosyal devlet ilkesinin hayata geçirileceği ve vatandaşların menfaat ihlallerinin sona ereceği değerlendirilmektedir.

SONUÇ VE ÖNERİLER

Bu çalışmada devletlere ve topluma karşı siyasi, toplumsal, ekonomik ve diğer sebeplerle siber uzamda gerçekleştirilen siber saldırılar neticesinde oluşan siber terörizm ve idare hukuku bağlamında sosyal risk ilkesi kapsamında devletin tazminat sorumluluğu ele alınmıştır. Bununla birlikte bilgi ve iletişim teknolojilerinin gelişmesiyle sürekli bir devinim halinde olan siber saldırı türleri mercek altına alınarak siber güvenlik ve bilgi güvenliği kapsamındaki gereklilikler incelenmiştir. İdare hukukunda uygulanan meri mevzuat kapsamında terör faaliyetleri sonucunda toplumun uğradığı zararların devlet tarafından tazmin edilmesi yükümlülüğü ele alınarak siber saldırılar kapsamında söz konusu zararların giderilmesine ilişkin sonuçlar ortaya konulmuştur.

Çalışmanın ilk bölümünde incelenen siber ve terörizm kavramlarının tarihsel gelişimi çerçevesinde sürekli bir değişim içerisinde olduğu, söz konusu kavramların siber uzamda söz konusu değişim ve devinimle birlikte farklılıklar gösterdiği, bilgi ve iletişim teknolojilerinin gelişmesiyle konvansiyonel savaşların yerini hibrit savaşlara bıraktığı, siber terörizmin gerçekleştirilmesinde araç olarak kullanılan siber saldırı yöntemlerinin hacktivist faaliyetlerle birlikte hibrit savaş unsuru olarak da kullanıldığı, bununla birlikte devletlerin klasik savaş savunma sistemlerine ilaveten bilgi güvenliği ve siber güvenliğe ilişkin savunma yöntemlerini uygulamasının gerekli olduğu değerlendirilmektedir.

İkinci bölüm çerçevesinde siber saldırganlar tarafından yaygın şekilde kullanılan siber saldırı türleri incelenmiş, sürekli değişen teknoloji ve yazılımdaki gelişmelerle etki alanı genişlemiş farklı siber saldırı yöntemlerinin literatüre girdiği görülmüştür. Söz konusu siber saldırılar ile devletlere ait kritik altyapılar ve endüstriyel kontrol sistemleri etkisiz hale getirilerek siyasi, toplumsal, ekonomik ve çevresel krizlerin ortaya çıkarılabileceği değerlendirilmektedir. Bu bölümde incelenen siber saldırı türlerine bakıldığında bilgisayar korsanlığı, kötücül yazılım saldırıları, casus yazılımlar, DoS ve DDoS saldırıları, fidye yazılımı saldırıları, veri ihlali saldırıları, ortadaki adam saldırıları, sıfırıncı gün saldırıları, botnetler, gelişmiş kalıcı tehditler, arka kapılar ve oltalama saldırılarının etki bakımından öne çıktığı görülmektedir. Bahsi geçen siber saldırı yöntemlerinin, yeni geliştirilen saldırı teknikleri ile entegre şekilde kullanılarak etki düzeyi çok daha yüksek olan saldırılara yol açılabildiği görülmektedir. Diğer taraftan konvansiyonel savaş unsurlarına ek olarak siber

savaşlarda araç olarak kullanılan söz konusu yöntemlerle devletlerin siber uzamda tahakküm kurma yarışına girdiği görülmüştür. Bu vasıtayla kara, hava, deniz ve uzaydan sonra beşinci savaş sahası olarak nitelenen siber uzayın son yüzyılda öneminin arttığı değerlendirilmektedir.

Üçüncü bölüm kapsamında siber terörizmle mücadeleye değinilerek siber saldırılara karşı savunma ile ilgili uluslararası belge ve metinlere dayalı değerlendirmelerde bulunulmuştur. Uluslararası hukuk bağlamında Birleşmiş Milletler Şartının 51. maddesi kapsamında üye ülkelerin bireysel ve müşterek meşru müdafaa hakkı ile Güvenlik Konseyinin yetkileri saklı tutularak NATO Anlaşmasının 5. maddesi çerçevesinde müttefik devletlerden birisine yönelen silahlı saldırıya karşı diğer devletlerin meşru savunmaya yardım etmesine ilişkin hususlar bu bölümde ele alınmıştır. Söz konusu siber saldırıların silahlı saldırı eşiği ve kuvvet kullanma yasağının sınırlarına yönelik muğlak yönleri uluslararası literatür kapsamında tartışılmıştır.

Tezin dördüncü ve son bölümünde idare hukuku bağlamında sorumluluk kavramı ele alınarak kusurlu ve kusursuz sorumluluk kavramları çerçevesinde sosyal risk ilkesi incelenmiştir. Bununla birlikte idarenin sorumluluğuna ilişkin şartlar tartışılarak idarenin eylem ve faaliyetleri dolayısıyla vatandaşların uğradıkları zararların tazmin edilmesi hususu ele alınmıştır. Bu kapsamda 3713 sayılı Terörle Mücadele Kanunu ve 5233 sayılı Terör Ve Terörle Mücadeleden Doğan Zararların Karşılanması Hakkında Kanuna siber terörizm kapsamında değinilmiştir. Bununla birlikte siber terörizmin idare hukukunda sosyal risk ilkesi ile ilişkisi incelenmiş ve siber saldırılar sonucunda vatandaşların uğradıkları zararların idarenin tazminat yükümlülüğü kapsamında hangi yasal düzenlemeler bağlamında değerlendirileceği tartışılmıştır. Söz konusu alandaki boşluklar tespit edilerek öneriler kısmında bu boşluklara ilişkin çözüm önerilerine yer verilmiştir.

Bu çalışmada bahse konu sonuçlara binaen ortaya konulan çözüm önerileri aşağıdaki gibidir:

Kritik Altyapılara İlişkin Öneriler:

Ülkemizde kritik altyapı sektörleri, 20 Haziran 2013 tarihli ve 2 sayılı Siber Güvenlik Kurulu kararı gereğince Ulusal Siber Güvenlik Stratejisi 2013-2014 Eylem Planı'nın 5 nolu eylem maddesinde düzenlenmiştir. Söz konusu sektörler "Elektronik Haberleşme", "Enerji", "Finans", "Ulaştırma", "Su Yönetimi" ve "Kritik Kamu Hizmetleri" şeklinde altı ayrı başlık altında ele alınmış ve buna göre kurumsal yapı oluşturulmuştur. Bununla beraber gelişen bilgi ve iletişim teknolojileriyle beraber kritik altyapıların bilgi teknolojileri sektörüne bağlı ve bağımlı hale gelmesiyle bu sektöre ilişkin siber saldırılar büyük bir artış göstermiştir. Diğer taraftan küresel olarak kritik altyapı çeşitliliğinin artması ile söz konusu alanların kendi özelinde siber güvenlik önlemlerinin alınması ihtiyacı hasıl olmuştur. Bu bağlamda ülkemizle uluslararası düzenlemeler ve AB direktifleri arasında mevzuat uyumlaştırma çalışmaları yapılması gerektiği değerlendirilmektedir. Ülkemizin kritik altyapı sektörlerine ilişkin siber güvenlikle ilgili uluslararası metinler ve diğer devletlerin kanuni düzenlemeleri ile mevzuat bakımından uyumlaştırma çalışmaları gerçekleştirmesi büyük önem arz etmektedir. Öyle ki siber uzamda sınır aşan suçlarla mücadele kapsamında ortak bir literatüre sahip olmak, siber saldırganların yakalanması, soruşturulması ve kovuşturulması için devletlerin önceliği olarak ortaya çıkmaktadır.

Bu kapsamda ülkemizde halihazırda yukarıda bahsi geçen kritik altyapılara ilaveten gelişen ve değişen bulut bilişim, 5G, blok zincir, IoT, internet alan adları, veri merkezleri, internet yer sağlayıcılar gibi yeni nesil teknolojilere yönelik siber saldırılara karşı siber dayanıklılığın artırılması amacıyla BM, NATO ve AB Direktifleri ile uyum kapsamında "Bilgi Teknolojileri Sektörü"nün hayata geçirilmesi gerekmektedir. Bununla birlikte "Birlik Genelinde Yüksek Düzeyde Ortak Bir Siber Güvenlik Düzeyine Yönelik Önlemlere İlişkin Direktif (NIS2 Direktifi)" çerçevesinde sırasıyla yüksek kritik sektör başlığı altında düzenlenen "BİT Servis Yönetimi"nin, NIS2 Direktifi ve Kritik Kuruluşların Dayanıklılığı Direktifi (CER Direktifi)" kapsamında kritik altyapı olarak belirlenen "Dijital Altyapılar" sektörünün ve NIS2 Direktifi bağlamında diğer sektörler başlığı altında düzenleme altına

alınan “Dijital Sağlayıcılar” sektörünün ülkemizde kritik altyapı sektörü olarak belirlenmesi önerilmektedir.

Bununla birlikte ilerleyen teknolojilerle birlikte üretimdeki artış ve sanayileşmenin gerektirdiği tesis ve varlıkların siber güvenliğinin devletler bakımından önemi ve BM kapsamında gerçekleştirilen çalışmalar göz önünde bulundurulduğunda, “Sanayi” sektörünün ülkemizde kritik altyapı sektörü olarak belirlenmesi gerektiği değerlendirilmektedir. Yine sanayileşmenin getirdiği seri üretim dolayısıyla tedarik zinciri boyutu da bulunan ve NATO kapsamında kritik altyapı sektörü olarak belirlenen “Kritik Üretim” sektörünün de ülkemizde düzenleme altına alınması önerilmektedir. Söz konusu alanlarla bağlantılı olarak ABD’nin Siber Güvenlik ve Altyapı Güvenlik Ajansı (CISA) ile NATO kapsamında kritik altyapı sektörü olarak değerlendirilen “Ticari Tesisler” ve “Devlet Tesisleri”nin de ülkemizde hayat geçirilmesi önerilmektedir.

BM kapsamında belirlenen “Acil Durum Hizmetleri” ve Birleşik Krallık’ta düzenleme altına alınan “Acil Servisler” kritik altyapı sektörleri ülkemizde devlet tesislerinin yanı sıra kritik varlık ve tesislerin sürekliliğinin sağlanması bakımından hayata geçirilmelidir. AB ve ITU belgelerinde yer alan “e-ticaret” sektöründe özellikle son yıllarda kişisel banka ve hesap bilgilerinin ele geçirildiği, siber saldırılarda vatandaşların maddi ve manevi zararlara uğradığı görülmektedir. Bu sektörün de ülkemizde kritik altyapı sektörü olarak düzenlenmesi ve ilgili kuruluşların siber dayanışma içerisinde sektör paydaşı olarak yer aldığı bir yapı önerilmektedir. Diğer taraftan NIS2 Direktifinde düzenlenen, tedarik zinciri boyutuyla tüm sektörün lojistiğini, iletim ağlarını ve dağıtımı etkileyen “Posta ve Kargo” sektörü de ülkemizde kritik altyapı sektörü olarak hayata geçirilerek gerekli siber güvenlik yapılanması ve kurumsallaşma sağlanmalıdır.

Diğer taraftan siber uzamda askeri sistem, altyapı ve tesislere yönelik gerçekleştirilen siber saldırılar neticesinde askeri araç ve gereçler, mühimmat, savaş uçak ve gemilerinin radar ve navigasyon sistemleri, sinyal bozucu teknolojiler gibi askeri kritik varlıklar zarar görebilmekte konvansiyonel savaşların sonuçları siber savaş taktikleriyle etkilenebilmektedir. Bu minvalde, ülkemizde NATO kapsamında kritik altyapı olarak belirlenmiş olan “Savunma Sanayi” sektörünün ayrı bir kritik altyapı sektörü olarak belirlenmesinin uygun olacağı önerilmektedir. Devletlerin değişen siber savaş ve terörizmle

mücadele stratejilerinin kara, deniz ve hava gibi konvansiyonel savaş alanlarından uzay sahasına taşınması ile uzayda devletlere ait olan uydu, sistem, hava araçları, radar ve savunma sistemlerine ilişkin önlem alınması ihtiyacı hasıl olmuştur. Avrupa Güvenlik ve İş Birliği Teşkilatı (AGİT) kapsamında belirlenen "Havacılık ve Uzay" sektörü ile NIS2 ve CER Direktiflerinde düzenlenen "Uzay" sektörünün ülkemizdeki mevzuatla uyumlaştırılması gerektiği değerlendirilmektedir.

BM çalışmaları kapsamında düzenlenen "Nükleer" kritik altyapı sektörü, AB Direktiflerinde yer alan "Tehlikeli Madde Üretimi" ve "Kimyasal Endüstri" sektörü, NIS2 Direktifinde düzenleme altına alınan "Kimyasal" ve "Malzeme ve Atık" sektörleri ülkemizde uyumlaştırılması gereken diğer sektörlerdir. CISA tarafından "Nükleer Reaktörler" ismiyle düzenlenen bu sektör Birleşik Krallık kapsamında "Kimyasallar" ve "Sivil Nükleer" olarak addedilmiştir. Özellikle 2010 yılından sonra kurulmaya başlanmış Akkuyu, Sinop ve Trakya nükleer güç santralleri dolayısıyla nükleer enerji sektörünün ülkemizde kritik altyapı sektörü olarak kurumsallaşmış bir yapıda belirlenmesi gerekmektedir. Ülkemizde kurulan bahse konu nükleer tesislerin siber güvenliğinin sağlanması için, güçlü bir siber dayanıklılık yapılanması içerisinde "Nükleer" sektörün enerji sektöründen ayrıştırılarak sınıflandırılması önerilmektedir.

Söz konusu kritik sektörlere ek olarak son yıllarda gıda ve sağlık sektörlerindeki fidye yazılım saldırılarının artışı bu alanda da devletleri ve uluslararası kuruluşları kritik altyapılar bakımından önlemler almaya yöneltmiştir. ABD ve AB'de yer alan "Gıda ve Tarım" sektörü ile AB, BM ve NIS2 Direktifi kapsamında kritik altyapılar arasında yer alan "Sağlık" sektörü kapsamında ülkemizde gerekli çalışmalar gerçekleştirilerek bu adlar altında kritik altyapı sektörlerinin düzenleme altına alınması önerilmektedir. Söz konusu alanda gerçekleşecek siber saldırılar neticesinde vatandaşların uğradığı zararlar idarenin kusursuz sorumluluğu ve sosyal risk ilkesi çerçevesinde tazmin edilebilecektir. Yukarıda uluslararası düzenlemeler çerçevesinde yer verilen kritik altyapılara, uluslararası kuruluşlara ve ülkemizde halihazırda bulunmayan kritik altyapı sektörlerinde önerilen sorumlu kurum ve aşağıdaki Tablo 3'te yer verilmiştir:

Tablo 3. Kritik Altyapı Türlerine ve Sorumlu Kuruluşlara İlişkin Öneriler

Kritik Altyapı Türü	**Belirleyen ve Düzenleyen Uluslararası Kuruluş**	**Ülkemizde Önerilen Sorumlu Kuruluş**
Bilgi Teknolojileri	NATO / BM	Bilgi Teknolojileri ve İletişim Kurumu (BTK)
Savunma Sanayi	NATO	Millî Savunma Bakanlığı (MSB) / Savunma Sanayi Başkanlığı (SSB)
Acil Servis Sektörü	NATO / BM	AFAD
Nükleer	BM	Nükleer Düzenleme Kurumu / Enerji Piyasası Düzenleme Kurumu (EPDK)
Dijital Altyapılar	AB	BTK
Dijital Sağlayıcılar	AB	BTK
Uzay	AB / AGİT	Türkiye Uzay Ajansı
BİT Servis Yönetimi	AB	BTK
Malzemeler ve Atıklar	AB	Çevre, Şehircilik ve İklim Değişikliği Bakanlığı
Kimyasal Endüstri	AB	Makine ve Kimya Endüstrisi
Sanayi	BM	Sanayi ve Teknoloji Bakanlığı
E- Ticaret	ITU / AB	Ticaret Bakanlığı
Gıda ve Tarım	AB	Tarım ve Orman Bakanlığı
Posta ve Kargo	AB	Posta ve Telgraf Teşkilatı Genel Müdürlüğü / BTK
Sağlık	BM / AB	Sağlık Bakanlığı
Ticari ve Devlet Tesisleri	NATO	İç İşleri Bakanlığı / MSB

Diğer taraftan söz konusu kritik altyapıların kontrol ve komuta sistemleri olan endüstriyel kontrol sistemleri ve SCADA'lar kötücül yazılım saldırıları, casus programlar, fidye yazılım saldırıları, DoS ve DdoS saldırıları ile gelişmiş kalıcı tehdit saldırıları kullanılarak ele geçirilebilmektedir. Sürekli olarak değişen ve gelişen siber saldırılara karşı yazılım geliştirme yöntemi ve makine öğrenmesi ile yerli ve milli yapay zekâ uygulamaları kullanılarak siber güvenlik önlemleri alınması gerektiği değerlendirilmektedir. Bununla birlikte kritik altyapıların korunmasında deneyimlerin paylaşılması ve sektör paydaşları arasında adli ve teknik yardımlaşma önemli bir yer tutmaktadır. Bu kapsamda Birleşik Krallık nezdinde örnekleri bulunan "SCADA ve Kontrol Sistemi Bilgi Değişimi Programı", "Kritik Altyapı Koruması Referans, Uyarı ve Bilgi Ağı"nın ülkemize de uyarlanarak hayata geçirilmesi önerilmektedir. Bununla beraber AB mevzuatında yer alan "Ulusal Kritik Altyapıların Korunması Programı" ile benzer bir yapının ülkemizde oluşturulması önerilmektedir. Siber saldırılar neticesinde siber suçluların soruşturulması ve kovuşturulması için ulusal düzeyde "Siber Kriz İrtibat Örgütü Ağı" oluşturularak kritik altyapılara yönelik siber saldırılarla ilgili bilgi paylaşımı ve adli yardımlaşma ağlarının oluşturulması önerilmektedir. Enerji ve su kritik altyapı sektörlerinde 2019 yılında imzalanan protokolle ülkemizde hayata geçirilen ve siber güvenlik operasyon merkezini bünyesinde barındıran Ulusal Test Yatağı Merkezinin yanı sıra diğer kritik altyapılara ilişkin siber güvenlik, siber tehdit, siber olay tespiti ve tehdit analiz programlarının geliştirilmesi gerektiği değerlendirilmektedir. Bu kapsamda kritik altyapılarda "Endüstriyel Kontrol Sistemleri Siber Acil Durum Müdahale Ekibi" şeklinde sektöre özgü ekipler oluşturulması önerilmektedir. Diğer taraftan Çin'de örneği bulunan "Siber Uzay İdaresi (CAC)" gibi bir kuruluşun ülkemizde de hayata geçirilmesi ve buna bağlı olarak Birleşik Krallık'ta emsalleri bulunan "Ulusal Altyapıyı Koruma Merkezi (CPNI)" ve "Kritik Altyapı Güvenlik Operasyon Merkezi" yapılarının ulusal koruyucu güvenlik otoritesi altında ülkemizde hayata geçirilmesi önerilmektedir.

Siber Güvenlik Önlemlerine İlişkin Öneriler:

Siber güvenlik önlemleri bakımından kimlik avı ve sıfırıncı gün saldırılarına karşı "İçerik Silahsızlandırılması ve Yeniden Yapılanma (CDR)" koruyucu sistemleri, zararlı yazılımların tespit edilmesi amacıyla "Siber Güvenlik Açığı Değerlendirmesi (CVA)" uygulamalardaki siber tehditlerin tespiti ve ağ güvenliğinin iyileştirilmesinde kurumsal

yapıda kullanılmalıdır. Bununla beraber filtrelemeli güvenlik duvarları kullanılarak ağ trafiğine yönelik şüpheli hareketler izlenmelidir. Bu kapsamda İP, port, web ve içerik taramaları yapılarak kritik belgelere erişim yetkisi olan kişilere ilişkin "En Az Ayrıcalık İlkesi (POLP)" çerçevesinde sıfır güven modeli ve "tam zamanında yaklaşım" ilkesi benimsenmelidir. Güvenlik operasyon merkezleri (SOC) kapsamında tespit, raporlama, güvenlik bilgisi ve olay yönetimi (SIEM) sağlayan sistemler terk edilerek; ağ trafiği analizi (NTA), bulut teknolojisi, uç nokta tespiti ve yanıtı (EDR) ve bütüncül koruma sağlayan proaktif tehdit tespit ve yanıt yöntem sistemleri (XDR) kurumsal yapıda yaygınlaştırılmalıdır. Yine sistem tabanlı ve bulut teknolojisi kullanan, bilinemeyecek siber saldırıları yapay zekâ ve makine öğrenimini (ML) ile önceden algılayan yeni nesil antivirüs (NGAV) programları kullanılmalıdır. "User activity monitoring (UAM)" yazılımsal izleme uygulamaları ile kötü amaçlı etkinlikler tespit edilerek siber istihbarat ve casusluk faaliyetleri ortaya çıkarılmalıdır. Bal küpü (Honeypot) gibi aldatma teknolojileri (deception technology) ile hackerlara yönelik hedefler taklit edilerek yetkisiz ve izinsiz giriş faaliyetleri tespit edilmelidir. Bunun yanı sıra uygulamaya yönelik siber güvenlik tatbikatları ülkemizde yaygınlaştırılarak bu tatbikatların kritik altyapı sektörleri özelinde ulusal ve uluslararası çapta gerçekleştirilmesi önerilmektedir.

Siber saldırıların önceden gerçek zamanlı olarak analiz, tahmin ve optimizasyon işlemlerinin yapılabilmesi amacıyla "Dijital ikizler" çerçevesinde test ve inovasyon laboratuvarları kurularak potansiyel siber saldırıların sanal simülasyonuna ilişkin çalışmaların yürütülmesi önerilmektedir. Diğer taraftan CSA kapsamından yürütülen çalışmalar bağlamında siber güvenlik sertifikasyon çerçevesi ülkemizle uyumlaştırılarak yönetilen güvenlik hizmetleri, olay yönetimi, denetim, teknik destek ve penetrasyon testi gibi tedbirlerin alınmasında öncül bir kılavuz olarak rehber edinilmelidir. 2024 yılında getirilen değişiklikle söz konusu siber sertifikasyon şemaları siber güvenlik hizmet sağlayıcılarını daha güvenli hale getirecek ve ülkemizin ihraç ettiği dijital nitelikli ürünlerde Avrupa ile uyum sağlanılmasına fayda sağlayacaktır. Bununla birlikte Siber Dayanışma Yasası (Cyber Solidarity Act) kapsamında hayata geçirilen siber güvenlik uyarı sistemi ile yapay zekanın ve ileri veri analitiğinin kullanımı siber saldırılar öncesinde üye devletlerin siber dayanıklılık kapasitesini artırmakta ve sınır ötesi uyarılarla öncül tedbir alınmasını sağlamaktadır.

Uluslararası Siber Güvenlik Mevzuatına İlişkin Öneriler:

Siber uzay bağlamında gerçekleştirilen siber saldırıların zamandan ve mekândan bağımsız olması sebebiyle saldırganların tespit edilmesi, soruşturulması ve kovuşturulmasında problemlerle karşılaşılmaktadır. Ülkemizde siber suçları düzenleyen mevzuat hükümleri bulunmakla birlikte, özel olarak oluşturulmuş bir siber güvenlik kanunu bulunmamaktadır. Söz konusu boşluğun doldurulması adına Avrupa Konseyi Siber Suç Sözleşmesi (Budapeşte Sözleşmesi), Lanzarote Sözleşmesi ile BM tarafından uzmanlar seviyesinde görüşmeleri gerçekleştirilen ve "*United Nations Convention Against Cybercrime: Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes*" başlığıyla kabul edilen "Bilgi ve İletişim Teknolojilerinin Suç Amaçlı Kullanımının Önlenmesine İlişkin Kapsamlı Uluslararası Sözleşme" kapsamında ülkemizde birincil düzenleme seviyesinde "Siber Güvenlik Kanunu" veya "Siber Saldırıların Önlenmesine Dair Kanun" adı altında yasal düzenleme çalışması yapılması önerilmektedir. Özellikle bahse konu uluslararası sözleşme kapsamında ele alınan "Siberle İlişkili", "Siberle Kolaylaşan" ve "Siberin Araç Olarak Kullanıldığı" bazı suç kategorileri TCK'da yer almamaktadır. Bahse konu suç tiplerinin TCK'ya eklenmesi gerekmekte ve söz konusu hususlar da göz önünde bulundurularak ülkemizde siber casusluk ve siber terörizm faaliyetlerini yürüten suçluların cezalandırılması amacıyla TCK'dan bağımsız olarak bir "Siber Suçlar Yasası" çıkarılması önerilmektedir. Bunun yanı sıra ABD'de örneği bulunan "Siber Güvenlik Araştırma ve Geliştirme Yasası", "Siber Güvenlik İyileştirme Yasası" ve "Siber Olay Raporlama Yasası (CIRCIA)" kapsamında benzer kanuni düzenlemelerin ülkemizde de hayata geçirilmesi önerilmektedir. Diğer taraftan nesnelerin internetine yönelik siber saldırıların siber terörizm faaliyetlerinde sıklıkla kullanılmaya başlanması ile yeni nesil teknolojilerle yapılan saldırılara çözüm bulunması, uyum sağlanması ve teknik önlemlerin düzenlenmesi çerçevesinde ABD'de örneği bulunan "IOT Siber Güvenliği Geliştirme Yasası" adı altında bir düzenleme ülkemiz için de önerilmektedir.

Bunların yanı sıra AB mevzuatı kapsamında 2022 yılında yayımlanan ve ağa bağlanan dijital unsur içeren ürünler için siber güvenlik sertifikası ve standardizasyonunu öngören, ürünlerin yaşam döngüsü boyunca siber güvenlik gereksinimlerini ortaya çıkaran,

sektörde tek tutarlı bir çerçeve oluşturan, dijital ürünlerin tedarik zincirini doğrudan etkileyen, kritik ve çok kritik ürün gruplarıyla sertifikasyona kılavuzluk yapan, söz konusu ürünlerin piyasaya arzında ve kullanıcılar için pazara sunulmasında siber güvenlik önlemleri öngören "Siber Dayanıklılık Yasası (CRA)"nın ülkemizde uyumlaştırılması önerilmektedir. Bu kapsamda ürün güvenliğine yönelik siber güvenlik tedbirlerini içeren birincil bir düzenleme çıkarılması önerilmektedir. Yine bu düzenleme sayesinde AB ortak pazarında ağa bağlanabilen ürünlerin ihracatı kapsamında yerli üreticinin pazar hacminin ve rekabet gücünün artacağı öngörülmektedir. Söz konusu uyumlaştırma kapsamında IOT cihazlar üzerinden gerçekleştirilen ve siber terörizme sebebiyet veren saldırılara karşı caydırıcılık sağlanmasının mümkün olacağı değerlendirilmektedir. Diğer taraftan yüksek kritik ve diğer kritik altyapı sektörlerinin sınıflandırmaya tabi tutulduğu "Birlik Genelinde Yüksek Düzeyde Ortak Siber Güvenliğe Yönelik Önlemler Hakkındaki Direktifi (NIS2 Directive)"nin ülkemizdeki mevzuatla uyumlaştırılması gerektiği değerlendirilmektedir. 2023 yılında AB'de yürürlüğe giren NIS2 Direktifi ile temel ve önemli kuruluşların belirlenmesi çerçevesinde ülkemizde de belirlenecek sektörler bazında kurumsallaşma sağlanması önerilmektedir. Bu kapsamda ülkemizde siber saldırıların gerçekleştirildiği kuruluşlar nezdinde bilgi paylaşımı, denetim, Siber Olaylara Müdahale Ekiplerinin (SOME) belirlenmesi ve geliştirilmesi, tek irtibat noktası (POC) sağlanması, iş birliği ve siber kriz makamları arasında plan ve stratejilerin paylaşılmasının mümkün olacağı değerlendirilmektedir.

Bununla birlikte 2019 yılında yayımlanan "Siber Güvenlik Yasası (CSA)" ile siber güvenlik mevzuatımızın uyumlaştırılarak ürün, hizmet ve süreçlere yönelik sertifikasyon çalışmalarının yapılması gerektiği değerlendirilmektedir. Ülkemizde de yerel olarak oluşturulacak laboratuvar test ortamları ile CSA kapsamında yer alan "Ulusal Siber Güvenlik Sertifikasyon Otoritesi"nin temsilciliğinin bulundurulması önerilmektedir. 2023 yılında Avrupa Komisyonu değişiklik önerisi ile "yönetilen güven hizmetleri" için kabul edilen siber olaylara müdahale sızma testleri ve güvenlik denetimlerinin Avrupa Sertifikasyon Programı dâhilinde ülkemizde de hayata geçirilmesi önerilmektedir. Bu bağlamda AB'de 2023 yılında yürürlüğe giren CER Direktifi çerçevesinde ülkemizde faaliyet gösteren kritik kurum, kuruluş ve işletmelerin toplumsal ve ekonomik sürdürülebilirliğinin sağlanması için sahip oldukları kritik varlık ve tesislere yönelik siber dayanıklılığın artırılmasına dair teknik çalışmaların gerçekleştirilmesi önerilmektedir.

Ülkemizdeki Mevzuata İlişkin Öneriler:

Ülkemizde siber terörizmle mücadele kapsamında 3713 sayılı Terörle Mücadele Kanunu ve 5233 sayılı Terör Ve Terörle Mücadeleden Doğan Zararların Karşılanması Hakkında Kanunun yanı sıra siber saldırılar dolayısıyla vatandaşların karşılaşabileceği maddi ve manevi zararların tazminatına ve idarenin sorumluluğuna ilişkin özel bir düzenleme çıkarılması gerektiği düşünülmektedir. Öyle ki Tallinn Manual kapsamında siber saldırılara karşı uluslararası hukukun uygulanabilirliği, silahlı saldırı seviyesine gelmeyen kuvvet kullanımı kapsamında ülkemizde mevzuat çalışmaları yapılması önerilmektedir. Bununla birlikte BM Uluslararası Hukuk Komisyonu tarafından 28 Ocak 2002 tarihinde yayımlanan A/RES/56/83 belgesi, BM Şartının 51. maddesi ve NATO Anlaşması'nın 5. maddesi bağlamında uluslararası hukukun siber saldırılara uygulanması bakımından ülkemizde uyumlaştırma çalışmaları yapılması önerilmektedir. Bu çalışmalar çerçevesinde siber saldırılara karşı caydırıcılığın sağlanması ve söz konusu saldırılara karşı koyma amacına hizmet edecek hukuki zeminin sağlanması amacıyla birincil ve ikincil düzenleme çalışmalarının yapılması gerektiği değerlendirilmektedir. Öyle ki bu alanda bahse konu düzenlemelerin de göz önünde bulundurularak ülkemizde hayata geçirilecek "Siber Güvenlik Terörle Mücadele Yasası" söz konusu alandaki boşluğun giderilmesinde önemli bir rol oynayacaktır.

Bunun yanı sıra icrai olarak siber saldırılardan etkilenen vatandaşlarına karşı da yükümlülüğünün bulunması gerektiği hususu çalışmanın ana konularından birini oluşturmaktadır. 5233 sayılı Kanun kapsamında devletin siber terör faaliyetlerinden etkilenen gerçek ve özel hukuk tüzel kişilerin zararlarını karşılaması, belirli başlı hususları içermesi dolayısıyla mevzuat ve içtihatlarla şekillenen idare hukukundaki boşlukların tamamlanması gerekmektedir. Söz konusu siber terör faaliyetleri dolayısıyla devletin icrai olarak vatandaşlarını koruması gereken kişilik haklarının ihlali, özel hayatın gizliliği, kişisel verilerin ihlali, maddi ve manevi hak ihlalleri ile idarenin ihmali suretle gerekli siber güvenlik tedbirlerini almaması alanlarında uğranılan zararlara yönelik tazminatların düzenleme altına alınması gereklilik arz etmektedir. Bu kapsamda 5233 Sayılı Kanun kapsamının bu çalışmada yer verilen Danıştay kararlarında görüleceği üzere maddi zararlarla birlikte manevi zararları içine alacak şekilde genişletilmesi gerektiği değerlendirilmektedir. Ülkemizdeki mülkiyet tanımına bakıldığında ise 4721 sayılı Türk Medeni Kanunu'nun 683.

maddesinde "*Bir şeye malik olan kimse, hukuk düzeninin sınırları içinde, o şey üzerinde dilediği gibi kullanma, yararlanma ve tasarrufta bulunma yetkisine sahiptir…*" ifadesi geçmektedir. Söz konusu maliklik; taşınır ve taşınmaz malların yanı sıra Anayasa Mahkemesi kararlarında fikri mülkiyet hakları ve sınai mülkiyet hakları gibi hakları da kapsamaktadır. Bu kapsamda siber saldırılar neticesinde mülkiyet zararına yönelen fiiller devletin tazminat sorumluluğunu doğurabilecektir. Söz konusu mülkiyet hakları tazmininin temelini Tallinn Manual belgesinde yer verilen; saldırıların can kaybına veya mülkiyete yönelik olması ve belirli yoğunluğa ulaşması durumunda silahlı saldırı olarak değerlendirilebileceği kıstası oluşturmaktadır. Söz konusu kılavuz örnek alınarak ülkemizde bu alanda çıkarılacak yeni bir düzenleme ile siber saldırıların silahlı saldırı sayılmasına ilişkin kıstasların belirlenmesi, Tallinn Manual ve diğer uluslararası belgelere uyum sağlanması gerektiği değerlendirilmektedir.

3713 Sayılı Kanun'un 1.Maddesindeki "Terör" Tanımına "siber saldırı" ve "kritik altyapılara yönelik saldırılar" ifadelerinin eklenmesi gerekmektedir. Söz konusu ifadelerin eklenmesi ile siber terörizme ilişkin saldırılarda vatandaşların uğradığı zararlar tazmin edilebilecek ve uluslararası literatürde yer alan siber suç tanımlamalarıyla uyumlu hale gelecektir. Bununla birlikte 3713 Sayılı Kanun'un 4.Maddesindeki "Terör Suçu Sayılan Suçlar"a TCK'nın 245/A maddesinin eklenmesi gerekmektedir. Öyle ki söz konusu maddede yasak cihaz ve programlar vasıtasıyla siber saldırıların da gerçekleşebileceği değerlendirilmekte, BM bünyesinde yayımlanan "Bilgi ve İletişim Teknolojilerinin Suç Amaçlı Kullanımının Önlenmesine İlişkin Kapsamlı Uluslararası Sözleşme" kapsamında siberle ilgili, siberle kolaylaşan ve siberin araç olarak kullanıldığı suçlarla verilen zararların tazminine ilişkin söz konusu maddenin eklenmesinin dayanak teşkil edeceği değerlendirilmektedir.

İnternet ortamı, ağ ortamı ve bilgisayar ortamı üzerinde işlenen siber saldırılar ve sair faaliyetler dolayısıyla idarenin kusursuz sorumluluğuna gidilip gidilemeyeceği tartışılması gereken bir noktadadır. Öyle ki kusursuz sorumluluk kapsamında idare tarafından verilere erişim ve söz konusu verilerin işlenerek imha edilmesine yönelik politikalar, ulusal siber güvenlik tedbirleri, pasif caydırıcılık araçlarının kullanımı ve diğer yazılımsal ve donanımsal araçlardaki eksiklikler dolayısıyla ortaya çıkan teknolojik sorunlar kişilere yönelik tazminat taleplerinin nedenleri arasında sayılabilecektir. Burada idarenin sorumluluğuna gidilmemesi

hakkaniyet gereği isabetli olmayacaktır. Bilgi ve iletişim teknolojilerinin gelişmesi kapsamında bilişim alanındaki "zero trust" anlayışı gereğince dışsal tehditlerin yanı sıra içsel tehditler de ortaya çıkabilmektedir. Söz konusu alandaki güvenlik riskleri gereğince devletlerin kritik veri ve işletim sistemleri ulusal ve uluslararası terörist faaliyetlerin hedefi konumuna gelebilmektedir. Bu kapsamda idarenin kusurlu ve kusursuz sorumluluğunun gündeme gelmesi gerekmektedir. Bahse konu alandaki riskler elektronik risk olarak nitelenebileceği gibi veri işlemeden doğan riskler olarak da özelleştirilebilmektedir. Bu nedenle özelleşen bu alan için Türk hukuk sisteminde hem meri hukuk bağlamında hem de içtihatlarla geliştirilmesi gereken bir kanun boşluğu bulunduğu ortadadır. Söz konusu elektronik risk kapsamında ülkemizde mevzuat çalışmalarının gerçekleştirilerek yargı içtihatlarıyla bu alandaki boşluğun doldurulması önerilmektedir. Bununla birlikte söz konusu hukuki alanda arabuluculuk müessesesinin hayata geçirilmesi ve nizasız yargılama çerçevesinde yargılama hızının artırılmasının sağlanması gerektiği düşünülmektedir.

Uluslararası İş Birliği ve Siber Farkındalığa İlişkin Öneriler:

Türk idari yargısında e-idarenin ve e-işlemlerden kaynaklı idarenin sorumluluğuna gidilebilecek hususların kusursuz sorumluluk bağlamında mevzuatın yanı sıra içtihatlarla da desteklenmesi gerektiği düşünülmektedir. Siber terörizmin önlenmesi bağlamında uluslararası iş birliği ve koordinasyon büyük önem arz etmektedir. Bu kapsamda ülkemizde faaliyet gösteren kurum ve kuruluşların üye oldukları uluslararası birlik ve platformların yanı sıra ikili iş birlikleri ile devletler arası veri paylaşımına vücut veren teknik ve adli yardımlaşmaların yapılması gerektiği değerlendirilmektedir. Bu kapsamda dünya uygulamalarında örneği bulunan "Uluslararası Siber Suçlar Adli ve Teknik Yardımlaşma Ağı" gibi paylaşım platformlarına üye olunması önerilmektedir.

Yine söz konusu Siber Dayanışma Yasası kapsamında AB siber güvenlik rezervinin hayata geçirilmesi ile özel sektör ve kamu iş birliği geliştirilmiş, üye ve ilgili üçüncü ülkelerin yardım talebi doğrultusunda siber olay müdahalesi için söz konusu özel sektör rezervinin yardımda bulunacağı kararlaştırılmıştır. Bu rezerv siber güvenlik olay inceleme ve acil durum mekanizması işlevi görerek siber savunma hazırlık eylemlerini destekleme kapsamında siber dayanıklılığa ilişkin test çalışması yürütmektedir. Ülkemizin de bahse

konu sistem örnek alınarak bir mekanizma oluşturması ve siber alanda uluslararası iş birliği anlaşmalarına imza atması gerektiği değerlendirilmektedir.

Bilgi ve iletişim teknolojilerinin gelişmesiyle uluslararası uygulama ve mevzuatlarda olduğu ülkemizde de çağa ayak uydurmak üzere değişiklikler, iyileştirmeler ve modernizasyon çalışmaları yapılması gerekli olmaktadır. E-idare ve e-devlet hizmetlerinin gelişmesi sonrasında da kamusal dokümanların internet ortamına taşınması, vatandaşlara ait kişisel verilerin büyük veriyi de içine alacak şekilde veri merkezlerinde tutulması ve kamu hizmetlerine yönelik işlem ve eylemlerin dijital platformlar ve uygulamalar üzerinden yapılır hale gelmesi, ulusal ve uluslararası alanda siber saldırıların artmasında ve bu yolla işlenen siber suçların çeşitlenmesinde siber suçlulara büyük bir motivasyon kaynağı olmuştur. Çalışmanın önceki bölümlerinde yer verilen siber saldırı türleri gün geçtikçe çeşitlilik arz etmekte ve pasif caydırıcılık unsurlarının hem bireysel hem de devlet eliyle yürütülmesi gerekli olmaktadır. Siber saldırılara karşı savunmanın iç çekirdeğini ve en önemli halkasını oluşturan insan unsuru dolayısıyla bireylerin siber farkındalığının oluşturulması gerekmektedir. Bu kapsamda devletin yaş farkı gözetmeksizin vatandaşlar üzerinde olumlu etki bırakacak siber farkındalığa yönelik eğitim ve seminer çalışmaları yapması gerekmektedir.

KAYNAKLAR

ABCNEWS. (2000). 15-Year-Old admits hacking NASA computers. https://abcnews.go.com/Technology/story?id=119423&page=1. adresinden 15 Aralık 2023 tarihinde alınmıştır.

Ablon, L. ve Bogart, A. (2017). Zero Days, Thousands of nights:The life and times of zero-day vulnerabilities and their exploit. https://www.rand.org/pubs/research_reports/RR1751.html. adresinden 5 Nisan 2024 tarihinde alınmıştır.

AFCEA. (2012). The evolution Of U.S. CYBERPOWER, https://www.afcea.org/committees/cyber/documents/theevolutionofuscyberpower.pdf. adresinden 11 Aralık 2023 tarihinde alınmıştır.

Agustina, J. R. (2015). Understanding cyber victimization: digital architectures and the disinhibition effect. *International Journal of Cyber Criminology,* 9(1), 35-54. https://doi.org/10.5281/zenodo.22239.

Aithor. (2024). Burning chrome by William Gibson analysis & summary. https://aithor.com/essay-examples/burning-chrome-by-william-gibson-analysis-summary. adresinden 17 Mart 2024 tarihinde alınmıştır.

Akamai. (2024). What Is A Cdn (Content Delivery Network)?. https://www.akamai.com/our-thinking/cdn/what-is-a-cdn. adresinden 27 Haziran 2024 tarihinde alınmıştır.

Akman, M. (2023). Kadına yönelik siber şiddet. https://hukukvebilisim.org/kadina-yonelik-siber-siddet/. adresinden 12 Ocak 2024 tarihinde alınmıştır.

Aktaş, M. (2023) Unraveling the Moonlight Maze: The state-sponsored cyber espionage campaign that changed cybersecurity forever, https://medium.com/unraveling-the-moonlight-maze-the-statesponsored-cyber-espionage-campaign-thatchanged1a79e129b358. adresinden 6 Ekim 2023 tarihinde alınmıştır.

Akyılmaz, B. (1998). İdari yargıda tazminat şekilleri ve hesaplanması. *SÜHFD*, 6(1-2), 170.

Aldoori, A. (2020). *Uluslararası hukukta siber suçla mücadele* [Yüksek lisans tezi / İstanbul Üniversitesi]. http://nek.istanbul.edu.tr:4444/ekos/TEZ/ET002065.pdf

Alexander, D. C. (2014). Cyber threats against the North Atlantic Treaty Organization (NATO) and selected responses. *İGÜSBD,* 1(2), 3-4. https://dergipark.org.tr/tr/download/article-file/89251

Alford, L. (2001). Cyber warfare: A new doctrine and taxonomy. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5cb40ae255f5d92cb5bc9ee04181e28edfdec065. adresinden 11 Aralık 2023 tarihinde alınmıştır.

Alioğlu, S. D. (2019). *Siber saldırılar ve ülkelerin siber güvenlik politikaları* [Yüksek lisans tezi / İstanbul Bilgi Üniversitesi].

https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=k97efjw6jfyzKtSSzYBo7g&no=o1IMl4Xz1izj2L3TXCCSYQ

Alkhouri, L. (2019). Cyber jihadism: Today and tomorrow. Pektas, S. ve Leman J. (Ed.), Militant Jihadism: Today and tomorrow (1. Baskı, 83-100) içinde. Leuven University Press.

Alkhouri, L., Kassirer, L. A. ve Nixon, A. (2016). *Hacking for ISIS: The emergent cyber threat landscape*. Flashpoint Press. https://books.google.com.tr/books/about/Hacking_for_ISIS.html?id=6Lq3nQAACAAJ&redir_esc=y

Anderson, D. (2013). Shielding the compass: How to fight terrorism without defeating the law. *SSRN,* E. https://doi.org/10.2139/ssrn.2292950.

Andini, O. P. (2021). Cyber terrorism criminal acts in the perspective of transnational organized crime. *Unnes Law Journal*, 7(2), https://doi.org/10.15294/ulj.v7i1.38804

Andress J. ve Winterfeld S. (2011). *Cyber warfare: Techniques, tactics and tools for security practitioners* (1. Baskı). Syngress Press.

ASD. (2023). IBM data breach cost reports. https://www.cyber.gov.au/learn/threats/data-security. adresinden 17 Mart 2023 tarihinde alınmıştır.

Aslay, F. (2017, Kasım, 11). Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi. *International Journal of Multidisciplinary Studies and Innovative Tecnologies,* 1(1), 24-48. https://dergipark.org.tr/tr/pub/ijmsit/issue/32341/359378

Aslay, F. (2017). Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies,* 1(1), 24-28

Atay, E. (2006). *İdare hukuku* (1.Baskı). Turhan Kitabevi Yayınları.

AttackSimulator. (2022). Scavenging. https://attacksimulator.com/glossary/scavenging/. adresinden 8 Mart 2023 tarihinde alınmıştır.

Attrill, A. (2015). *Cyberpsychology*. Oxford University Press.

Australian Government Signals Directorate. (2024). Ransomware. https://www.cyber.gov.au/ransomware. adresinden 20 Şubat 2024 tarihinde alınmıştır.

Australian Law Dictionary. (2024). Cybercrime (internet crime) definition. http://www.oxfordreference.com/view/10.1093/acref/9780195557558.001.0001/acref-9780195557558-e-0921?rskey=eFEDr8&result=4. adresinden 6 Ocak 2023 tarihinde alınmıştır.

Avrupa Konseyi Siber Suçlar Sözleşmesi (Budapeşte Sözleşmesi), CETS no. 185, Budapeşte, 23.11.2001.

Avşar, Z. ve Öngören, G. (2010). *Bilişim Hukuku* (1. baskı). Türkiye Bankalar Birliği Yayınları.

AXIOS. (2023). Ransomware hits emergency rooms across U.S.. https://www.axios.com/2023/11/28/ransomware-hits-us-emergency-rooms. adresinden 15 Aralık 2023 tarihinde alınmıştır.

Backe, E. L. (2018). Networked individuals, gendered violence: A literature review of cyberviolence. *Violence and Gender.* 5(3). https://doi.org/10.1089/vio.2017.0056

Badejo, K. (2019). *How i survived a ransomware attack* (1. Baskı). Lulu Publishing.

Baker, K. (2022). What is a trojan horse? (Trojan malware). https://www.crowdstrike.com/cybersecurity-101/malware/trojans/#:~:text=A%20Trojan%20Horse%20(Trojan)%20is,the%20contents%20of%20the%20device. adresinden 3 Mart 2024 tarihinde alınmıştır.

Baldwin, D. A. (2003). Güvenlik kavramı. *Avrasya Dosyası*, 9(2), 5-35.

Bettany, A. ve Halsey, M. (2017). *Windows virus and malware troubleshooting* (1. Baskı). Apress Publishing.

Bhadwal, A. (2023). The history of cyber security: A detailed guide. https://www.knowledgehut.com/blog/security/history of-cyber-security. adresinden 8 Ekim 2023 tarihinde alınmıştır.

Bilgi Güvende. (2022). Keylogger saldırıları tarihi. https://bilgiguvende.com/keylogger-saldirilari-tarihi/. adresinden 22 Şubat 2023 tarihinde alınmıştır.

Bilgi Platformu. (2024). Peer to peer (P2P) nedir? P2P ağı nasıl çalışır?. https://www.btcturk.com/bilgi-platformu/peer-to-peer-nedir-p2p-agi-nasil-calisir/. adresinden 14 Haziran 2024 tarihinde alınmıştır.

Bilgi Teknolojileri ve İletişim Kurumu. (2014). USOM-Siber güvenliğe ilişkin temel bilgiler.https://dsy.usom.gov.tr/usom/19/02/190211082958_siber_guvenlige_giris_ve_temel_kavramlar.pdf. adresinden 25 Temmuz 2024 tarihinde alınmıştır.

Bilgi Teknolojileri ve İletişim Kurumu. (2022). Dijitalleşen dünyada bilişim suçları ve mücadele yöntemleri. https://www.btk.gov.tr/uploads/pages/arastirma-raporlari/dijitallesen-dunyada-bilisim-suclari-ve-mucadele-yontemleri-6218e2417eaea.pdf. adresinden 21 Eylül 2023 tarihinde alınmıştır.

Bishopfox. (2015). An overview of BGP hijacking. https://bishopfox.com/blog/bgp-hijacking-overview. adresinden 2 Ocak 2024 tarihinde alınmıştır.

Black's Law Dictionary. (2024). Crime definition & legal meaning. https://thelawdictionary.org/crime/. adresinden 5 Ocak 2023 tarihinde alınmıştır.

Blank, S. (2008). WebWar I: Is Europe's first information war a new kind of war?. *Comparative Strategy Journal*, 27(3), 227-247. https://www.tandfonline.com/doi/full/10.1080/01495930802185312

Bloomberg. (2021). Gasoline pinch to grind on for weeks with truck shortage, https://www.bloomberg.com/news/articles/2021-05-13/gasoline-pinch-may-grind on-for-

week-or-more-amid-truck-shortage?embedded-checkout=true. adresinden 15 Kasım 2023 tarihinde alınmıştır.

Bolat, C. (2020). *Siber saldırılara karşı meşru müdafaa hakkının uluslararası hukuk açısından incelenmesi* [Doktora Tezi /İstanbul Üniversitesi]. http://nek.istanbul.edu.tr:4444/ekos/TEZ/ET001670.pdf

Bozdemir, M. (1981). What Is terror and terrorism?. *School of Political Sciences Press and Publication College*.

Bright. (2022). What is a SQL injection attack?. https://brightsec.com/blog/sql injection-attack/. adresinden 24 Mart 2023 tarihinde alınmıştır.

Britannica. (2023). Trojan. https://www.britannica.com/technology/trojan-computing. adresinden 3 Mart 2023 tarihinde alınmıştır.

Britannica. (2024). Trojan definition. https://www.britannica.com/technology/trojan-computing. adresinden 3 Mart 2024 tarihinde alınmıştır.

Broadcom. (2024). What is cyber espionage?. https://www.vmware.com/topics/cyber-espionage. adresinden 6 Mart 2024 tarihinde alınmıştır.

Buchan, R. (2019). *Cyber espionage and international law*, (1. Baskı). Bloomsbury Yayıncılık.

Bumiller, E. ve Shanker, T. (2012). Panetta warns of dire threat of cyberattack on US. http://www.nytimes.com/2012/1z0/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewan ted=all&_r=0. adresinden 14 Ocak 2024 tarihinde alınmıştır.

Buresh, D. L. (2021). Russian cyber-attacks on Estonia, Georgia, and Ukraine, including tactics, techniques, procedures and effects. *Journal of Advanced Forensic Sciences*, 1(2), 15-26. https://openaccesspub.org/advanced-forensic sciences/article/1686

CAIDA, (2024). The spread of the Sapphire/Slammer worm. https://www.caida.org/catalog/papers/2003_sapphire/. adresinden 17 Ağustos 2024 tarihinde alınmıştır.

Canadian Centre for Cyber Security. (2022). An introduction to the cyber threat environment. https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment. adresinden 07 Mayıs 2024 tarihinde alınmıştır.

Carr, J. (2011). *Inside cyber warfare* (2. Baskı). O'Reilly Media Inc.

Cassim, F. (2012). Addressing the spectre of cyber terrorism: a comparative perspective. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, 15(2). http://dx.doi.org/10.4314/pelj.v15i2.14

CertByLAB. (2018). Siber ortamla ilgili kullanılan kavramlar. https://www.certbylab.com/blog/siber-kavramlar/. adresinden 25 Aralık 2023 tarihinde alınmıştır.

Chen, P., Desmet, L. ve Huygens, C. (2014). A study on advanced persistent threats, *IFIP,* [Konferans Bildirisi]. 15th International Conference on Communications and Multimedia Security, Aveiro, Portekiz.

Choi, K. (2008). Computer crime victimisation and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, 2(1), 308–333. https://www.researchgate.net/publication/238621672_Computer_Crime_Victimization_and_Integrated_Theory_An_Empirical_Assessment

Choi, K., Scott, T. M. ve LeClair, D. P. (2016). Ransomware against police: diagnosis of risk factors via application of cyber-routine activities theory. *International Journal of Forensic Science & Pathology (IJFP)*, 4(7), 253–258. https://doi.org/10.19070/2332-287X-1600061.

CIS. (2021). The SolarWinds cyber-attack: What you need to know. https://www.cisecurity.org/solarwinds. adresinden 1 Ocak 2023 tarihinde alınmıştır.

CİSCO. (2023). Man-in-the-middle attack definition. https://learningnetwork.cisco.com/s/question/0D53i00000KsugaCAB/maninthemiddl e-attack-definition. adresinden 22 Mart 2023 tarihinde alınmıştır.

CNBC. (2021). Pipeline outage forces american airlines to add stops to some long-haul flights southwest flies in fuel. https://www.cnbc.com/2021/05/10/colonial-pipeline-shutdown-forces-airlines-toconsider-other-ways-to-get-fuel.html. adresinden 1 Ocak 2023 tarihinde alınmıştır.

CNNBusiness. (2020). 'I love you': How a badly-coded computer virus caused billions in damage and exposed vulnerabilities which remain 20 years on. https://edition.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html. adresinden 21 Ağustos 2024 tarihinde alınmıştır.

Colarik, A. ve Janczewski, L. (2011). Developing a grand strategy for cyber war. *IEEE*, [Bildiri sunumu]. 7th International Conference on Information Assurance and Security (IAS).

Coleman, K. G. (2008). Cyber espionage targets sensitive data. https://technews.tmcnet.com/sip-trunking/topics/security/articles/47927-cyber-espionage-targets-sensitive-data.htm. adresinden 24 Mart 2024 tarihinde alınmıştır.

Collins. (2024). Definition of 'ICQ'. https://www.collinsdictionary.com/dictionary/english/icq. adresinden 2 Şubat 2023 tarihinde alınmıştır.

Collins. (2024). Definition of 'IRC. https://www.collinsdictionary.com/dictionary/english/irc. adresinden 10 Şubat 2023 tarihinde alınmıştır.

Computer Hope. (2021). Data diddling. https://www.computerhope.com/jargon/d/data diddling.htm. adresinden 24 Mart 2023 tarihinde alınmıştır.

Conway, M. (2014). Reality check: assessing the (un)likelihood of cyberterrorism. *Springer New York,* 103-121. https://link.springer.com/chapter/10.1007/978-1-4939-0962-9_6

Corcoran, L., McGuckin, C. ve Prentice, G. (2015). Cyberbullying or cyberaggression?: A review of existing definitions of cyber-based peer-to-peer aggression. *Societies*, 5(2). 245-255.

Correia, J. V. (2022). An explorative study into the importance of defining and classifying cyber terrorism in the United Kingdom. *SN Computer Science*, 3(84) https://doi.org/10.1007/s42979-021-00962-5

Counsil on Foreign Relations. (2005). Titan rain. https://www.cfr.org/cyber operations/titan-rain. adresinden 6 Ekim 2023 tarihinde alınmıştır.

Crowdstrike, 2022b, What Is Privilege Escalation?, https://www.crowdstrike.com/cybersecurity-101/privilege-escalation/. adresinden 15 Mart 2023 tarihinde alınmıştır.

CSA. (2022). A closer look at wiper malware. https://www.csa.gov.sg/Tips Resource/publications/cybersense/2022/a-closer-look-at-wiper-malware. adresinden 20 Şubat 2023 tarihinde alınmıştır.

CSO. (2017). Keylogger found in keyboard driver of 475 HP notebook models. https://www.csoonline.com/article/3241237/keylogger-found-in-keyboard-driver-of-475-hp-notebook-models.html. adresinden 22 Şubat 2023 tarihinde alınmıştır.

CyberBrokers. (2020). Norsk Hydro–A ransomware case study. https://cyberbrokers.co.uk/norsk-hydro-a-ransomware-case-study/. adresinden 11 Ekim 2023 tarihinde alınmıştır.

CyberCrimeMagazine. (2023). Ransomware minute: Latest attacks and news. https://cybersecurityventures.com/ransomware-minute/. adresinden 1 Mart 2023 tarihinde alınmıştır.

Cybereason. (2024). Phoenix: The tale of the resurrected keylogger. https://www.cybereason.com/blog/research/phoenix-the-tale-of-the-resurrected-alpha-keylogger. adresinden 26 Şubat 2023 tarihinde alınmıştır.

Cyberlaw. (2021a). DigiNotar. https://cyberlaw.ccdcoe.org/wiki/DigiNotar_(2011). adresinden 14 Ocak 2024 tarihinde alınmıştır.

Cyberlaw. (2021b). Georgia-Russia conflict (2008). https://cyberlaw.ccdcoe.org/wiki/Georgia-Russia_conflict_(2008). adresinden 8 Ekim 2023 tarihinde alınmıştır.

Cyberlaw. (2021c). Operation orchard/outside the box (2007). https://cyberlaw.ccdcoe.org/wiki/Operation_Orchard/Outside_the_Box_(2007). adresinden 6 Ekim 2023 tarihinde alınmıştır.

Cybertraining365. (2023). Masquerade. https://www.cybertraining365.com/cybertraining/Topics/Masquerade. adresinden 19 Mart 2023 tarihinde alınmıştır.

Cyware. (2019). Masquerade attack: A wolf in sheep's clothing. https://cyware.com/news/masquerade-attack-a-wolf-in-sheeps-clothing-93393863. adresinden 21 Mart 2023 tarihinde alınmıştır.

Çakmak, H. ve Altunok, T. (2009). *Suç terör ve savaş üçgeninde siber dünya,* Platin Yayınları.

Çolak, H. (2016). Siber terörizmin önlenmesinde kurumsal yapılanma ve uluslararası adli yardımlaşma. *Türk Hukuk Araştırmaları Dergisi*, 1(1), 21-52. https://www.jurix.com.tr/article/4414?u=0&c=0

Danıştay 10. İdare Dairesi. 2007/3301 E.N, 2008/2939 K.N. https://www.kararara.com/danistay/10d/danistay5924.htm
Danıştay İdari Dava Daireleri Kurulu. 2013/4602 E.N, 2014/1220 K.N. https://www.danistay.gov.tr/assets/pdf/yayinlar/dergi/20_05_2019_042338.pdf
Danıştay İdari Dava Daireleri Kurulu. 2015/2652 E.N, 2017/1271 K.N. https://www.danistay.gov.tr/assets/pdf/yayinlar/dergi/15_05_2018_114253.pdf

Darıcılı, B. A. (2017). Demokrat parti hack skandalı bağlamında Amerika Birleşik Devletleri ve Rusya Federasyonu'nun siber güvenlik stratejilerinin analizi. *Yıldırım Beyazıt Üniversitesi Uluslararası Çalışmalar Dergisi,* 1(1), 1-24.

Defense Advanced Research Projects Agency. (2024). The sputnik surprise https://www.darpa.mil/about-us/timeline/creation-of-darpa. adresinden 12 Şubat 2024 tarihinde alınmıştır.

Denning, D. (1999). Information Warfare and Security, *I&S,* 113-115 https://procon.bg/system/files/04.08_Monitor_1.pdf.

Denning, D. (2000, Mayıs). Cyber terrorism. *Committee on Armed Services U.S. House of Representatives*. [Testimony before the Special Oversight Panel on Terrorism]. Washington DC, USA.

Denning, D. (2006). A view of cyberterrorism 5 years later. *Jones and Bartlett Publishers* 123-139. https://www.semanticscholar.org/paper/A-View-of-Cyberterrorism-Five-Years-Later-Denning/ab4959efc212996c2a6555df94a3d3d08756043a

Department Of Emergency And Military Affairs. (2024). Terrorism definitions. https://dema.az.gov/sites/default/files/Publications/AR-Terrorism%20Definitions-BORUNDA.pdf. adresinden 8 Haziran 2024 tarihinde alınmıştır.

Derdiman, C. (2007). *İdare hukuku* (1. Baskı). Alfa Aktüel Yayınları.

Dinapoli, T. P. (2023). Cyberattacks on New York's critical infrastructure. https://www.osc.ny.gov/files/reports/pdf/cyberattacks-on-new-yorks-critical infrastructure.pdf. adresinden 18 Aralık 2023 tarihinde alınmıştır.

Doğan, D. (2021). Siber güvenlik açısından siber saldırı senaryolarının incelenmesi. https://openaccess.maltepe.edu.tr/entities/publication/fe10deb2-5d0e-4cd0-b44e-5ec636e6f53b. adresinden 25 Mart 2024 tarihinde alınmıştır.

Doğrul, M., Aslan, A. ve Çelik E. (2011, Haziran, 7-11). Developing an international cooperation on cyber defense and deterrence against cyber terrorism. *IEEE*, [Bildiri sunumu]. 3. Uluslararası Siber Çatışma Konferansı, Tallinn, Estonya.

Dover Mıcrosystems. (2017). Why triton is one of the most dangerous pieces of malware ever. https://www.dovermicrosystems.com/case-study/triton-cyberattack/. adresinden 27 Eylül 2023 tarihinde alınmıştır.

Duggan, M., Rainie, L., Smith, A., Funk, C., Lenhart, A. ve Madden, M. (2014). Online harassment. https://www.pewresearch.org/wp-content/uploads/sites/9/2014/10/PI_OnlineHarassment_72815.pdf. adresinden 17 Ocak 2024 tarihinde alınmıştır.

Dunnigan, J. F. (2002). *The next war zone: Confronting the global threat of cyberterrorism*, Citadel Press.

Duran, L. (1974). *Türkiye idaresinin sorumluluğu*. Türkiye ve Orta Doğu Amme İdaresi Enstitüsü Yayınları.

Düren, A. (1979). *İdare hukuku dersleri*. Ankara Üniversitesi Hukuk Fakültesi Yayınları.

Ehliz, H. (2019). Bilişim suçlarının ulusal ve uluslararası düzeyde değişen güvenlik algısı üzerinde etkisi. [Yüksek lisans tezi, İstanbul Üniversitesi]. http://nek.istanbul.edu.tr:4444/ekos/TEZ/ET001167.pdf

Eldem, T. (2021). Uluslararası siber güvenlik normları ve sorumlu siber egemenlik. *İstanbul Hukuk Mecmuası,* 79(1), 347-378. https://dergipark.org.tr/tr/pub/ihm/issue/62018/928426

Elektronik Haberleşme Sektöründe Şebeke Ve Bilgi Güvenliği Yönetmeliği, R.G. T. 13/07/2014, S. 29059.

Elyashar, A., Uziel, S., Paradise, A. ve Puzis R. (2020). The chameleon attack: Manipulating content display in online social media. https://doi.org/10.48550/arXiv.2001.05668.

Enders, W. ve Sandler, T. (2012). The political economy of terrorism (2. Baskı). Cambridge University Press.

ENİSA. (2015). National cyber security centre of The Czech Republic for the periode from 2015 to 2020. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf. adresinden 7 Aralık 2023 tarihinde alınmıştır.

ENİSA. (2023a). Botnets. https://www.enisa.europa.eu/topics/incident response/glossary/botnets. adresinden 10 Mart 2023 tarihinde alınmıştır.

ENİSA. (2023b). ENİSA glossary man-in-the-middle. https://www.enisa.europa.eu/topics/incident-response/glossary/man-in-the-middle. adresinden 21 Mart 2023 tarihinde alınmıştır.

ENİSA. (2024a). Man-in-the-middle. https://www.enisa.europa.eu/topics/incident-response/glossary/man-in-the-middle. adresinden 29 Mart 2024 tarihinde alınmıştır.

ENİSA. (2024b). What is a rootkit. https://www.enisa.europa.eu/topics/incident-response/glossary/rootkits. adresinden 19 Haziran 2024 tarihinde alınmıştır.

Eren, F. (1998). *Borçlar hukuku-Genel hükümler* (1. Baskı). Beta Yayınları.

Ergil, D. (1992). Uluslararası terörizm, *Ankara Üniversitesi SBF Dergisi,* 47(3) https://dergipark.org.tr/tr/pub/ausbf/issue/3116/43234

Erkiner, H. H. (2010). *Devletin haksız fiilden kaynaklanan milletlerarası sorumluluğu* [Doktora Tezi /Marmara Üniversitesi]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=nRm2tRJp-X7LJDNI8CXulQ&no=cXaGWFdkHsiWI3tuDDL3sQ

ERMProtect. (2024). Top 10 data breaches so far in 2022. https://ermprotect.com/blog/top-10-data-breaches-so-far-in-2022/. adresinden 3 Nisan 2023 tarihinde alınmıştır.

Eshan, L. (2018). *Ethical hacking: A beginners guide to learning the world of ethical hacking* (1. Baskı). Shockwave Publishing via Publish Drive.

Eubank, W. L. ve Weinberg, L. B. (1994). Does democracy encourage terrorism?. *Terrorism and Political Violence*, 6, 417-435.

EurActiv. (2008). NATO agrees on common approach to cyber defence, http://www.euractiv.com/en/infosociety/nato-agrees-common-approachc-yber-defence/article-171377. adresinden 14 Ocak 2024 tarihinde alınmıştır.

European Commission. 2004. Critical infrastructure protection in the fight against terrorism, https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex%3A52004DC0702 . adresinden 9 Eylül 2023 tarihinde alınmıştır.

European Commission. (2009). Protecting Europe from large scale cyber-attacks and disruptions: Enhancing preparedness, security and resilience, https://eur lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52009DC0149. adresinden 11 Eylül 2023 tarihinde alınmıştır.

European Parliamentary. (2021). Combating gender-based violence: Cyber violence European added value assessment. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU(2021)662621_EN.pdf. adresinden 5 Ocak 2024 tarihinde alınmıştır.

European Union ve University of Ljubljana Faculty of Social Science. (2017). Cyber violence against women & girls report, https://wave-network.org/wp-content/uploads/WP2-Report-on-Cyber-VAWG.pdf. adresinden 12 Şubat 2024 tarihinde alınmıştır.

Fascendini, F., ve Fialová, K. (2012). Voices from digital spaces: Technology related violence against women. https://www.genderit.org/resources/voices-digital-spaces-technology-related-violence-against-women. adresinden 13 Mart 2024 tarihinde alınmıştır.

Federal Ministry of The Interior. (2011). Cyber security strategy for Germany, Berlin: Federal ministry of the interior https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Germany_2011_Cyber_Security_Strategy_for_Germany.pdf. adresinden 9 Aralık 2023 tarihinde alınmıştır.

Fernando, R. (2023). Computer virus list, types & examples. https://study.com/learn/lesson/computer-virus-types-examples.html. adresinden 11 Ocak 2024 tarihinde alınmıştır.

Fırat, H. (2022). *Siber terörizm - Yeni bir terör tehdidi ve riskler* (1. Baskı). TİAV Yayınları.

Firmbee. (2023). Salami tactics-the path-breaking project management method https://firmbee.com/salami-technique-project-management-method. adresinden 11 Nisan 2023 tarihinde alınmıştır.

First Line Practitioners. (2024). "Hacktivism": about the origins, meaning and history of online Activism. https://www.firstlinepractitioners.com/hacktivism. adresinden 21 Aralık 2023 tarihinde alınmıştır.

Flutter, A. (2018). '*Cyber' semantics: Why we should retire the latest buzzword in security studies*. Journal of Cyber Policy, 3(3), 1-16. DOI: 10.1080/23738871.2018.1514417

Foltz, B. C. (2004). Cyberterrorism, computer crime, and reality. *Information Management & Computer Security*, 12(2), 154–166. https://doi.org/10.1108/09685220410530799.

Forbes. (2019). Why zerodium will pay $2.5 million for anyone who can hack android but only $2 million for an iphone. https://www.forbes.com/sites/jeanbaptiste/2019/09/04/why-zerodium-will-pay-2-5-million-for-anyone-who-can-hack-android-but-only-2-million-for-an-iphone/?sh=76574948716b. adresinden 10 Şubat 2024 tarihinde alınmıştır.

Fortinet. (2021). Deep dive into a fresh variant of snake keylogger malware. https://www.fortinet.com/blog/threat-research/deep-dive-into-a-fresh-variant-of-snake-keylogger-malware. adresinden 24 Şubat 2023 tarihinde alınmıştır.

Fortinet. (2023). What is spyware?. https://www.fortinet.com/resources/cyberglossary/spyware. adresinden 11 Mart 2023 tarihinde alınmıştır.

Fortinet. (2024a). What is hacking?. https://www.fortinet.com/resources/cyberglossary/what-is-hacking. adresinden 18 Haziran 2024 tarihinde alınmıştır.

Fortinet. (2024b). What is spyware?. https://www.fortinet.com/resources/cyberglossary/spyware. adresinden 11 Mart 2024 tarihinde alınmıştır.

Fowler, K. (2016). *Data Breach Preparation and Response*. Syngress Press.

Fruhlinger, J. (2020) The CIA triad: Definition, components and examples. https://www.csoonline.com/article/568917/the-cia-triad-definitioncomponents-and-examples.htmladresinden 8 Ekim 2023 tarihinde alınmıştır.

Fruhlinger, J. (2022). Keyloggers explained: How attackers record computer inputs. https://www.csoonline.com/article/3326304/keyloggers-explained-how-attackers-record-computer-inputs.html. adresinden 15 Mayıs 2024 tarihinde alınmıştır.

Fruhlinger, J. (2022a). Ddos attacks: Definition, examples, And techniques, https://www.csoonline.com/article/571981/ddos-attacks-definition-examples-and techniques.html. adresinden 2 Mart 2023 tarihinde alınmıştır.

Fruhlinger, J. (2022b). Keyloggers explained: How attackers record computer inputs, https://www.csoonline.com/article/3326304/keyloggers-explained-how attackers-record-computer-inputs.html. adresinden 20 Şubat 2023 tarihinde alınmıştır.

Fruhlinger, J. (2024a). Logic bombs explained: Definition, examples, prevention. https://www.csoonline.com/article/2115905/logic-bomb.html. adresinden 4 Mart 2024 tarihinde alınmıştır.

Fruhlinger. J. (2024b). DDoS attacks: Definition, examples, and techniques. https://www.csoonline.com/article/3648530/ddos-attacks-definition-examples-and-techniques.html. adresinden 27 Şubat 2023 tarihinde alınmıştır.

Gardner, B. ve Thomas V. (2014). Building an ınformation security awareness program: Defending against social engineering and technical threats (1. Baskı). Syngress Press.

Geers, K. (2011). Strategic cyber security-NATO Cooperative Cyber Centre of Excellence (CCD COE) Publication. https://ccdcoe.org/uploads/2018/10/2011_Proceedings_0-1.pdf. adresinden 19 Haziran 2024 tarihinde alınmıştır.

Giantas, D. ve Stergiou, D. (2018). From terrorism to cyber terrorism: The case of ISIS. *SSNR.* http://dx.doi.org/10.2139/ssrn.3135927

Gibson, D. R. (2015). *Effective help desk specialist skills* (1. Baskı). Pearson Education.

Gibson, W. (1984). *Neuromancer* (1. Baskı). Ace Books Press.

Goodin, D. (2008). CookieMonster nabs user creds from secure sites. https://www.theregister.com/2008/09/11/cookiemonstor_rampage/. adresinden 11 Temmuz 2024 tarihinde alınmıştır.

Goodman, M., (2015). *Future crimes* (1. Baskı). Penguin Random House Publishing.

Gordon, S. ve Ford, R. (2002). Cyberterrorism?. *Computers & Security,* 21(7), 636-647. DOI:10.1016/S0167-4048(02)01116-1

Gordon, S. ve Ford, R. (2006). On the definition and classification of cybercrime, *Journal in Computer Virology*, 1, 14. https://www.semanticscholar.org/paper/On-the-definition-and-classification-of-cybercrime-Gordon-Ford/602ebdcf999983233d2534998a74d3d50b5101ad

Government of Belgium. (2012). Cyber security strategy: Securing cyberspace, Belgium: Government of Belgium. https://nsarchive.gwu.edu/themes/custom/nsarchive/templates/pdfjs/web/viewer.html?file=https%3A%2F%2Fnsarchive.gwu.edu%2Fsites%2Fdefault%2Ffiles%2Fdocuments%2F4378259%2FGovernment-of-Belgium-Cyber-Security-Strategy.pdf. adresinden 4 Ocak 2024 tarihinde alınmıştır.

Government of Canada. (2010). Canada's cyber security strategy. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-cbr-scrt-strtgy/archive-cbr-scrt-strtgy-eng.pdf. adresinden 15 Aralık 2023 tarihinde alınmıştır.

Gözübüyük A. P. (1970). *Alman, Fransız, İsviçre ve İtalyan ceza kanunlarıyla mukayeseli Türk Ceza Kanunu açıklaması* (3. Baskı). Kazancı Yayınevi.

Gözübüyük A. P. (1977). *Mücbir sebepler-Beklenmeyen haller* (1. Baskı). Kazancı Yayınevi.

GreyCampus. (2024). What is hacking?. https://www.greycampus.com/opencampus/ethical-hacking/what-is-hacking. adresinden 5 Ocak 2024 tarihinde alınmıştır.

Güngör, M. (2015). *Ulusal bilgi güvenliği strateji ve kurumsal yapılanma* [Uzmanlık tezi / T.C. Kalkınma Bakanlığı]. http://www.bilgitoplumu.gov.tr/wp-content/uploads/2015/11/Ulusal_Bilgi_Guvenligi_Strateji_ve_Kurumsal_Yapilanma.pdf

Güngör, M. B. (2021). *Türk hukukunda bilişim suçları ve bilişim yoluyla işlenen suçlar* [Yüksek Lisans Tezi / Yalova Üniversitesi].

Güven, F. (2022). *Siber saldırılar ve Türk kamu yönetiminin çözümleri* [Doktora Tezi / Süleyman Demirel Üniversitesi]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Haava, E. (2017). *Cyber Bullying Among Irish Primary School Pupils* [Masters Dissertation. Technological University Dublin]. doi:10.21427/H82Y-VE42

Harrison, A. (2000). Update: Mafiaboy not the big fish in DoS attacks. https://www.computerworld.com/article/2594513/update--mafiaboy-not-the-big-fish-in-dos-attacks.html. adresinden 14 Mart 2024 tarihinde alınmıştır.

Hatcher, J. (2014). *Hacking: Hacking for beginners and basic security: How to hack* (2. Baskı). Lulu Publishing.

Helvacıoğlu, A. D. (2004). Avrupa konseyi siber suç sözleşmesi-Temel hükümlerin incelenmesi. Atamer, Y. M. (Ed.) *İnternet ve hukuk*, İstanbul Bilgi Üniversitesi Yayınları.

Hoffman, C. P. (2014, Kasım, 6-9). Bombing to lose: reassessing the strategic logic of suicide terrorism, *Air Command and Staff College Maxwell AFB*, [Konferans sunumu]. 2014 Society for the History of Technology (SHOT) Annual Meeting, Michigan, ABD.

Holt, T. J. (2012). Exploring the intersections of technology, crime, and terror. *Terrorism and Political Violence*, 24(2), 337-354. https://doi.org/10.1080/09546553.2011.648350.

Hughes, R. B. (2009). NATO and cyber defence, mission accomplished?. https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/NATO%20and%20Cyber%20Defence%20-%20Mission%20Accomplished.pdf. adresinden 18 Kasım 2023 tarihinde alınmıştır.

Hypr. (2024). Blaster worm. https://www.hypr.com/security-encyclopedia/ms-blaster-worm. adresinden 13 Mart 2023 tarihinde alınmıştır.

IBM. (2022a). Cost of a data breach report 2022, https://www.key4biz.it/wp content/uploads/2022/07/Cost-of-a-Data-Breach-Full-Report-2022.pdf. adresinden 18 Mart 2023 tarihinde alınmıştır.

IBM. (2022b). Cost of a data breach report. https://www.key4biz.it/wp-content/uploads/2022/07/Cost-of-a-Data-Breach-Full-Report-2022.pdf. adresinden 2 Nisan 2024 tarihinde alınmıştır.

IBM. (2023). What is a data breach?. https://www.ibm.com/topics/data-breach. adresinden 17 Mart 2023 tarihinde alınmıştır.

IBM. (2024). What is a data breach?. https://www.ibm.com/topics/data-breach. adresinden 6 Mayıs 2024 tarihinde alınmıştır.

ICANNWiki. (2024). Arpanet. https://icannwiki.org/ARPANET. adresinden 7 Ocak 2024 tarihinde alınmıştır.

ICP. (2021a). Oldsmar water treatment facility attack is an example of rising cyber threat. https://www.industrialcybersecuritypulse.com/facilities/water-treatment-facility-targeted-by-hackers/. adresinden 18 Ocak 2024 tarihinde alınmıştır.

ICP. (2021b). Attacks on critical national infrastructure escalate with colonial pipeline hack. https://www.industrialcybersecuritypulse.com/facilities/attacks-oncritical-national infrastructure-escalate-with-colonial-pipeline-hack/. adresinden 1 Ocak 2023 tarihinde alınmıştır.

ICP. (2021c). JBS The worlds biggest meat supplier is hit with ransomware in another attack on critical infrastructure. https://www.industrialcybersecuritypulse.com/facilities/jbs-the-worlds-biggest-meatsupplier-is-hit-with-ransomware-in-another-attack-on-critical-infrastructure/. adresinden 2 Ocak 2023 tarihinde alınmıştır.

ICP. (2021ç). Throwback attack blackenergy attacks the Ukrainian power grid https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwbackattack-blackenergy-attacks-the-ukrainian-power-grid/. adresinden 11 Kasım 2023 tarihinde alınmıştır.

ICP. (2022). Throwback attack: The equation group, god of cyberespionage. https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-the-equation-group-god-of-cyberespionage/. adresinden 26 Nisan 2024 tarihinde alınmıştır.

ICRC. (2024). Convention (ıv) respecting the laws and customs of war on land and its annex: Regulations concerning the laws and customs of war on land the hague.

https://www.icrc.org/en/doc/resources/documents/article/other/57jnhy.htm. adresinden 20 Ağustos 2024 tarihinde alınmıştır.

Imperva. (2023a). Fork bomb attack (rabbit virus). https://www.imperva.com/learn/ddos/fork-bomb/#:~:text=A%20fork%20bomb%20. adresinden 5 Mart 2023 tarihinde alınmıştır.

Imperva. (2023b.) Trojans. https://www.imperva.com/learn/applicationsecurity/trojans/. adresinden 3 Mart 2023 tarihinde alınmıştır.

Imperva. (2023e). Website defacement attack. https://www.imperva.com/learn/application-security/website-defacement-attack/. adresinden 3 Ekim 2023 tarihinde alınmıştır.

Imperva. (2024a). Phishing attacks. (https://www.imperva.com/learn/application-security/phishing-attack-scam/. adresinden 14 Nisan 2024 tarihinde alınmıştır.

Imperva. (2024b). SQL (Structured query language) injection. https://www.imperva.com/learn/application-security/sql-injection-sqli/. adresinden 13 Şubat 2024 tarihinde alınmıştır.

Imperva. (2024c). What is a fork bomb?. https://www.imperva.com/learn/ddos/fork-bomb/#:~:text=A%20fork%20bomb%20. adresinden 4 Mart 2024 tarihinde alınmıştır.

International Court of Justice. (2024a). Military and paramilitary activities in and against Nicaragua (Nicar. v. U.S.). https://www.icj-cij.org/en/case/70. adresinden 21 Ağustos 2024 tarihinde alınmıştır.

International Court of Justice. (2024b). Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania). https://www.icj-cij.org/en/case/1. adresinden 21 Ağustos 2024 tarihinde alınmıştır.

International Organisation for Standardization/International Electrotechnical Commitee (ISO/IEC). (2023). ISO/IEC 27032, Information technology ıt security techniques guidelines for cybersecurity. https://www.iso.org/standard/76070.html. adresinden 2 Mayıs 2024 tarihinde alınmıştır.

International Telecommunication Union. (2020a). Definition of cybersecurity https://www.itu.int/en/ITU T/studygroups/com17/Pages/cybersecurity.aspx. adresinden 14 Ekim 2023 tarihinde alınmıştır.

Internet Security. (2020). CoolWebSearch nedir? Önleme ve koruyucu önlemler. https://www.internetsecurity.tips/what-is-coolwebsearch-prevention-and-protective-measures/. adresinden 12 Haziran 2024 tarihinde alınmıştır.

Investopedia. (2024a). File Transfer Protocol (FTP) meaning and uses. https://www.investopedia.com/terms/f/ftp-file-transfer-protocol.asp. adresinden 14 Haziran 2024 tarihinde alınmıştır.

Investopedia. (2024b). Phishing: What it is and how to protect yourself? https://www.investopedia.com/terms/p/phishing.asp#:~:text=What%20Is%20Phishing%3F

,to%20represent%20a%20legitimate%20firm. adresinden 14 Nisan 2024 tarihinde alınmıştır.

İçişleri Bakanlığı Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı. (2024). Siber Dünya Nedir?. https://www.siberay.com/siber-dunya-nedir. adresinden 14 Şubat 2024 tarihinde alınmıştır.

İçişleri Bakanlığı Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı. (2024). Siberay Sözlüğü. https://www.siberay.com/kurumlar/Siberay.com/SIBERAY-Sozluk.pdf. adresinden 16 Şubat 2024 tarihinde alınmıştır.

İçişleri Bakanlığı İç Güvenlik Stratejileri Dairesi Başkanlığı. (2021). Siber güvenlik kavramları ve terimleri sözlüğü.

İTÜBİDB. (2013). Denial of Service (DoS) saldırıları ve korunma yöntemleri. https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/denial-of-service-(dos)-sald%C4%B1r%C4%B1lar%C4%B1-ve-korunma-y%C3%B6ntemleri. adresinden 15 Nisan 2024 tarihinde alınmıştır.

Jacobson, D. ve Idziorek, J. (2013). *Computer security literacy: Staying safe in a digital world* (1. Baskı). Chapman and Hall Press.

Jaishankar, K. (2007). Establishing a theory of cyber crimes. *International Journal of Cyber Criminology,* 1(2), 7-9. https://doi.org/10.5281/ZENODO.18792.

Jalil, A. S. (2003). Countering cyber terrorism effectively:Are we ready to rumble?.https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154. adresinden 14 Ocak 2024 tarihinde alınmıştır.

Jeutner, V. (2019). The Digital Geneva Convention A Critical Appraisal of Microsoft's Proposal. *Journal of International Humanitarian Legal Studies*, 158-170.

Jonason, P. K. (2021). Cyber-dating abuse in young adult couples: Relations with sexist attitudes and violence justification, smartphone usage and impulsivity, https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0253180. adresinden 11 Nisan 2024 tarihinde alınmıştır.

JSİS University of Washington. (2017). Cyberattack on critical infrastructure: Russia and the Ukrainian power grid attacks, https://jsis.washington.edu/news/cyberattack critical-infrastructure-russia-ukrainian-power-grid-attacks/. adresinden 11 Kasım 2023 tarihinde alınmıştır.

Kabano, J. (2023). *Siber uzayda hasmane "davranı" ve "niyetin" belirlenmesi* (1. Baskı). Adalet Yayınevi.

Kara, M. ve Şişeci, N. (2011). Botnetlerle mücadelede dünyadaki ve Türkiye'deki durum. *TÜBİTAK-UEKAE*, [Bildiri sunumu]. XIII. Akademik Bilişim Konferansı 2011, Malatya, Türkiye.

Kara, O., Aydın, Ü. ve Oğuz, A. (2006, Kasım, 3-5). Ağ ekonomisinin karanlık yüzü: Siber terör. *Karabük Üniversitesi.* 5. Uluslararası Bilgi ve Yönetim Kongresi, Kocaeli, Türkiye.

Kaspersky. (2021). FinFisher spyware improves its arsenal with four levels of obfuscation, UEFI infection and more. https://www.kaspersky.com/about/press-releases/2021_finfisher-spyware-improves-its-arsenal-with-four-levels-of-obfuscation-uefi-infection-and-more. adresinden 14 Nisan 2024 tarihinde alınmıştır.

Kaspersky. (2023a). Fork bomb. https://encyclopedia.kaspersky.com/glossary/fork bomb/. adresinden 5 Mart 2023 tarihinde alınmıştır.

Kaspersky. (2023b). What is a zero-day attack?. https://www.kaspersky.com/resource center/definitions/zero-day-exploit. adresinden 15 Mart 2023 tarihinde alınmıştır.

Kaspersky. (2023c). What is Sql injection? Definition and explanation. https://www.kaspersky.com/resource-center/definitions/sql-injection. adresinden 22 Mart 2023 tarihinde alınmıştır.

Kaspersky. (2024a). What is SQL injection? Definition and explanation. https://www.kaspersky.com/resource-center/definitions/sql-injection. adresinden 13 Şubat 2024 tarihinde alınmıştır.

Kaspersky. (2024b). What is a Zero-day attack?-Definition and explanation. https://www.kaspersky.com/resource-center/definitions/zero-day-exploit. adresinden 9 Mart 2024 tarihinde alınmıştır.

Kirwan, G. ve Power, A. (2013). Cybercrime: The psychology of online offenders. *Cambridge University Press*, 80-82.

Kopp, C. (2000). Information warfare: A fundamental paradigm of infowar. *WSJ,* 46-55. https://www.ausairpower.net/OSR-0200.html.

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. Kramer, D. F., Starr, S. H. ve Wentz, L. K., Cyberpower and national security, (1. Baskı) içinde. National Defense University Press.

La Haye Kara Savaşı Kuralları Sözleşmesine Ek Yönetmelik (1907 IV Sayılı)

Lee, C. S., Choi, K., Shandler, R. ve Kayser, C. (2021). Mapping global cyberterror networks: an empirical study of Al-Qaeda and ISIS cyberterrorism events. *Journal of Contemporary Criminal Justice*, 37(3), 333-355. https://doi.org/10.1177/10439862211001606.

Lehto, M., Huhtinen, A. ve Jantunen, S. (2011). The open definition of cyber: Technology or a social construction?. *International Journal of Cyber Warfare and Terrorism*, 1(2), 1-9. https://www.igi-global.com/article/open-definition-cyber/64309

Libicki, M. (1995). What is information warfare?, *Small Wars Journal,* https://smallwarsjournal.com/documents/libicki.pdf.

Lockhart, A. (2007). *Network security hacks* (2. Baskı). O'Reilly Media.

Luiijf, E. (2014). Definitions of cyber terrorism. Akhgar, B., Staniforth, A. ve Bosco, F. (Ed.) *Cyber crime and cyber terrorism investigators handbook*, (1. Baskı) içinde. Singres Press.

Mala, C. C. ve Neethu, J. (2015). An overview of cyborg. *International Journal of Engineering Research & Technology.* [Bildiri sunumu]. NSRCL-2015 Conference Proceedings.

Malpedia. (2023). SpyEye. https://malpedia.caad.fkie.fraunhofer.de/details/win.spyeye. adresinden 4 Mart 2023 tarihinde alınmıştır.

Malwarebytes. (2019). Trickbot adds new trick to its arsenal: tampering with trusted texts. https://www.malwarebytes.com/blog/news/2019/09/trickbot-adds new-trick-to-its-arsenal-tampering-with-trusted-texts. adresinden 11 Ekim 2023 tarihinde alınmıştır.

Malwarebytes. (2023a). What is a rootkit?. https://www.malwarebytes.com/rootkit. adresinden 13 Mart 2023 tarihinde alınmıştır.

Malwarebytes. (2023b). What is TrickBot malware?. https://www.malwarebytes.com/trickbot. adresinden 11 Ekim 2023 tarihinde alınmıştır.

Malwarebytes. (2024). Computer worm. https://www.malwarebytes.com/computer-worm. adresinden 25 Şubat 2024 tarihinde alınmıştır.

Mann I. (2008). *Hacking the human: Social engineering techniques and security countermeasures* (1. Baskı). Gower Publishing.

Maras, M. H. (2012). *Computer Forensics: Cybercriminals, Laws, and Evidence* (2. Baskı). Jones & Bartlett Learning Press.

Maurer, T. (2011). Cyber norm emergence at the United Nations-An analysis of the UN's activities regarding cyber-security, https://www.belfercenter.org/publication/cyber-norm-emergence-united-nations-analysis-uns-activities-regarding-cyber-security. adresinden 16 Şubat 2024 tarihinde alınmıştır.

Mazebolt. (2022). Why are the Mirai Botnet attacks so famous?, https://blog.mazebolt.com/mirai-botnet-attacks-explained. adresinden 11 Mart 2023 tarihinde alınmıştır.

McQuade, S. C. (2006). *Understanding and managing cybercrime*. Prentice Hall (Pearson Education).

Mehra, C., Sharma, A. K. ve Sharma A. (2019). Elucidating ransomware attacks in cyber-security. *International Journal of Innovative Technology and Exploring Engineering*, 9(1). DOI: 10.35940/ijitee.A8106.119119

Melnitzky, A. (2012). Defending america against cyber espionage through the use of active defenses. *Cardozo Journal of International & Comparative Law*, 20(2), 537-566.

Menesini, E., Nocentini, A., Palladino, B., Frisen, A., Berne, S., Ortega-Ruiz, R., Calmaestra, J., Scheithauer, H., Schultze-Krumbholz, A. ve Luik, P. (2012). Cyberbullying

definition among adolescents: A comparison across six European countries. *Cyberpsychol Behavior and Social Networking*, 15, 455–462. doi: 10.1089/cyber.2012.0040.

Mıcrosoft. (2012). CIH (Çernobil) virüsü. https://answers.microsoft.com/tr-tr/windows/forum/all/cih-%C3%A7ernobil-vir%C3%BCs%C3%BC/a1de04f7-d8eb-4d94-9e70-60c5b775affb. adresinden 11 Ocak 2024 tarihinde alınmıştır.

Mohurle, S. ve Patil, M. (2017). A brief study of wannacry threat: ransomware attack. *International Journal of Advanced Research in Computer Science*, 8(5), 1938-1940. https://www.ijarcs.info/index.php/Ijarcs/article/view/4021

Nandal, P. (2017). *Malware detection* (1. Baskı). Anchor Academic Publishing.

Nasrat, Q. (2015). *Siber terörizmle mücadele ve uluslararası hukuk* [Yüksek lisans tezi / Atatürk üniversitesi]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

National Institute of Standards and Technology (NIST). (2015). NISTIR 8074 (2): Supplemental information for the interagency report on strategic u.s. government engagement in international standardization to achieve US objectives for cybersecurity. https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf. adresinden 5 Mayıs 2024 tarihinde alınmıştır.

National Institute of Standards and Technology (NIST). (2017). NIST special publication 800-12 revision 1 An introduction to information security. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf. adresinden 11 Ekim 2023 tarihinde alınmıştır.

National Institute of Standards and Technology (NIST). (2019). Glossary of key information security terms NISTIR 7298 revision 2. https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf. adresinden 1 Ocak 2023 tarihinde alınmıştır.

National Institute of Standards and Technology (NIST). (2023a). NIST glossary masquerading. https://csrc.nist.gov/glossary/term/masquerading. adresinden 19 Mart 2023 tarihinde alınmıştır.

National Institute of Standards and Technology (NIST). (2023b). NIST glossary critical infrastructure. https://csrc.nist.gov/glossary/term/critical_infrastructure. adresinden 9 Eylül 2023 tarihinde alınmıştır.

NATO. (1949). The North Atlantic Treaty https://www.nato.int/cps/fr/natohq/official_texts_17120.htm?selectedLocale=tr. adresinden 14 Ocak 2024 tarihinde alınmıştır.

NATO. (2012). CCDCOE National cyber security framework manual. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf. adresinden 11 Ağustos 2024 tarihinde alınmıştır.

NATO CCDCOE. (2007). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective.

https://www.ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf. adresinden 28 Aralık 2023 tarihinde alınmıştır.

NATO CCDCOE. (2017). (*Tallinn manual 2.0: On the international law applicable to cyber warfare* (1. Baskı). Cambridge University Press.

NATO CCDCOE. (2023). North atlantic treaty organisation. https://ccdcoe.org/organisations/nato/. adresinden 18 Kasım 2023 tarihinde alınmıştır.

NCSC. (2020a). Advisory: Trickbot. https://www.ncsc.gov.uk/news/trickbot-advisory. adresinden 4 Mart 2023 tarihinde alınmıştır.

NCSC. (2020b). Mitigating malware and ransomware attacks. https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks. adresinden 20 Şubat 2023 tarihinde alınmıştır.

Newsweek. (2016). U.S. military launches cyberattacks against ISIS. https://www.newsweek.com/us-military-launches-cyber-attacks-isis-432441. adresinden 21 Aralık 2023 tarihinde alınmıştır.

Nikfar, J. (2020). Globalisation and future of power relations in the Arabic Middle-East: a case study of Egypt and Libya. *Humanities and Social Sciences Communications*, 7, 134. https://doi.org/10.1057/s41599-020-00631-7.

Nocella, A. J. ve Best, S. (2004). *Terrorists or freedom fighters?: Reflections on the liberation of animals.* Lantern Books Press. https://books.google.com.tr/books?hl=tr&lr=&id=1juWE6y1C1QC&oi=fnd&pg=PA1&ots=MgUuA4VcKz&sig=tniAhjGnZv9IHi_pvbF9WC_pgRg&redir_esc=y#v=onepage&q&f=false

NordVPN. (2023). Data diddling, https://nordvpn.com/tr/cybersecurity/glossary/data diddling/. adresinden 22 Mart 2023 tarihinde alınmıştır.

NPR. (2023). T-Mobile says breach exposed personal data of 37 million customers. https://www.npr.org/2023/01/20/1150215382/t-mobile-data-37-million-customers-stolen#. adresinden 18 Nisan 2024 tarihinde alınmıştır.

NTNU. (2024). What is cybernetics?. https://www.ntnu.edu/itk/what-is adresinden 02 Ocak 2024 tarihinde alınmıştır.

O'Brien, C. (2021). What is cyber terrorism and is it a threat to US national security?. *Small Wars Journal*. https://smallwarsjournal.com/jrnl/art/what-cyber-terrorism-and-it-threat-us-national-security

O'Brien, M. ve Yar, M. (2008). *Criminology: the key concepts* (1.Baskı). Routledge Press.

Onar, S. S. (1968). *İdare hukukunun umumi esasları* (3.Baskı). İsmail Akgün Matbaası.

Oriyano, S. P. (2017). *Penetration testing essentials* (1. Baskı). Sybex Publishing.

Oxford University. (2015). Where does the word cyber come from?. https://blog.oup.com/2015/03/cyber-word-origins/. adresinden 7 Aralık 2023 tarihinde alınmıştır.

Parks, R. ve Duggan, D. (2011). Principles of cyberwarfare. *IEEE Security & Privacy*, 9(5) 30-35. https://www.scirp.org/reference/referencespapers?referenceid=3387464

Payne, B. K. (2020). Defining cybercrime. Holt T. J., Bossler A. M. ve Macmillan P. (Ed.) *The palgrave handbook of ınternational cybercrime and cyberdeviance*, (1. Baskı) içinde.Springer International Publishing.

Pazarcı, H. (2020). *Uluslararası hukuk dersleri* (4. Baskı). Turhan Kitabevi.

PCMag. (2015). Some GTA V modders hit with keylogger. https://www.pcmag.com/news/some-gta-v-modders-hit-with-keylogger. adresinden 18 Mart 2024 tarihinde alınmıştır.

Perlroth, N. (2021). This is how they tell me the world ends: The cyberweapons arms race. *Bloomsbury Publishing*, NY, 4(2), 272-274. DOI:10.5204/lthj.2658

Picus. (2022). Masquerading attacks explained-MITRE ATT&CK T1036 https://www.picussecurity.com/resource/masquerading. adresinden 13 Temmuz 2024 tarihinde alınmıştır.

Pitts, V. (2016). *Cyber crimes: History of world's worst cyber attacks* (1. Baskı). Alpha Editions.

Plotnek, J. J. ve Slay, J. (2021). Cyber terrorism: a homogenized taxonomy and definition. *Computers & Security*, 102 1-9. https://doi.org/10.1016/j.cose.2020.102145.

Politico. (2023). U.S., U.K. sanction Russian hackers in ransomware attacks. https://www.politico.com/news/2023/02/09/us-uk-sanction-russian-hackers-00082033. adresinden 1 Mart 2024 tarihinde alınmıştır.

Pollitt, M. M. (1998). Cyberterrorism-Fact or fancy?, https://www.sciencedirect.com/science/article/abs/pii/S1361372300870098?via%3Dihub. adresinden 2 Ocak 2024 tarihinde alınmıştır.

Porterfield, J. (2017). *White and black hat hackers* (1. Baskı). The Rosen Publishing.

Proofpoint. (2023). What is pharming?. https://www.proofpoint.com/us/threat reference/pharming. adresinden 16 Eylül 2023 tarihinde alınmıştır.

QT Worldtel Inc. (2003). Centralized out of band authentication system (C.O.B.A.S.). http://www.cybersecuritycooperation.org/documents/QT_COBAS_White_Paper.pdf. adresinden 4 Eylül 2023 tarihinde alınmıştır.

Raj, M. (2015). *Python penetration testing essentials* (1. Baskı). Packt Publishing.

Ramotion. (2023). Website defacement: Motivations, prevention and recovery. https://www.ramotion.com/blog/website-defacement/. adresinden 6 Ekim 2023 tarihinde alınmıştır.

Raufoğlu, T. (2022). *Hukuki yönleri ile siber alanda yetki sorunu* (1. Baskı). Adalet Yayınları.

Reuters. (2021). American airlines adds fuel stops to two flights after pipeline outage. https://www.reuters.com/business/energy/american-airlines-adds-fuel-stopstwo-flights-after-pipeline-outage-2021-05-11/#:~:text=American%20said%20its%20daily%20flight,in%20Boston%20for%20additional%20fuel. adresinden 1 Ocak 2023 tarihinde alınmıştır.

Risdata. (2000). Maroochy shire sewage spill, https://www.risidata.com/Database/Detail/maroochy-shire-sewage-spill. adresinden 11 Ekim 2023 tarihinde alınmıştır.

Robinson, M., Jones, K. ve Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security,* 49, 70-94. DOI:10.1016/j.cose.2014.11.007

Rosen Law Firm. (2024). North Carolina law. https://www.rosen.com/divorce/divorcearticles/keylogger-nc-divorce/. adresinden 21 Temmuz 2024 tarihinde alınmıştır.

Safeatlast. (2024). Malware statistics https://safeatlast.co/blog/malware-statistics/. adresinden 4 Mart 2024 tarihinde alınmıştır.

Sağıroğlu, Ş. ve Alkan, M. (2018). *BGD Siber güvenlik ve savunma farkındalık caydırıcılık* (1. Baskı). Grafiker Yayınları.

Samet, R. (2018). Kötü amaçlı yazılımlar ve analizi. Sağıroğlu, Ş. ve Alkan, M. (Ed.) *Siber güvenlik ve savunma farkındalık ve caydırıcılık* (1. baskı) içinde. Grafiker Yayınları.

Sandler, T. (2015). Terrorism and counterterrorism: an overview. *Oxford Economic Papers*, 67(1), 1-20. https://doi.org/10.1093/oep/gpu039

Sangfor. (2022). What is an eavesdropping attack and how does it work?. https://www.sangfor.com/glossary/cybersecurity/what-is-eavesdropping-attack-and how-does-it-work. adresinden 8 Mart 2023 tarihinde alınmıştır.

SANS. (2017). Attack and defend: Linux privilege escalation techniques of. https://www.sans.org/white-papers/37562/, (16.03.2023)

Schmitt, M. N. (1999). Computer network attack and the use of force in international law: Thoughts on a normative framework. *Columbia Journal of Transnational Law*, 37, 21-22.

Secret Double Octopus. (2024). Man in the middle attack. https://doubleoctopus.com/security-wiki/threats-and-tools/man-in-the-middle-attack/#security-wiki-content. adresinden 8 Mart 2024 tarihinde alınmıştır.

Sehrbrock, M. (2021). Hacktivism an overview

https://marlenecsblog.wordpress.com/2021/11/12/hacktivism-an-overview/. adresinden 19 Ocak 2024 tarihinde alınmıştır.

SEON. (2023). Masquerade attack, https://seon.io/resources/dictionary/masquerade attack/. adresinden 16 Mart 2023 tarihinde alınmıştır.

SEON. (2024). What Is a masquerade attack?. https://seon.io/resources/dictionary/masquerade-attack/. adresinden 15 Haziran 2024 tarihinde alınmıştır.

Shackelford, S. J. (2013). Toward cyberpeace: Managing cyberattacks through polycentric governance. *American University Law Review*, 62(5). 1301. https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1888&context=aulr

Simplicity. (2024). The A to Z of Cybersecurity Glossary https://www.simplicityvoip.net/hubfs/glossary.pdf. adresinden 14 Mart 2024 tarihinde alınmıştır.

Singapore CSA. (2023). Wiper malware. https://www.csa.gov.sg/singcert/Publications/a-closer-look-at-wiper-malware. adresinden 20 Şubat 2023 tarihinde alınmıştır.

Smith, J. (2015). *White hat hacking* (1. Baskı). Cavendish Square Publishing.

Smith, R. G., Grabosky, P. ve Urbas, G. (2004). Cyber criminal on trial. *Cambridge University Press,* 21. https://assets.cambridge.org/97805218/40477/frontmatter/9780521840477_frontmatter.pdf

Soesanto, S. (2020, 17 Nisan). Cyber Terrorism: Why it exists, why it doesn't, and why it will. https://www.realinstitutoelcano.org/en/analyses/cyber-terrorism-why-it-exists-why-it-doesnt-and-why-it-will/. adresinden 11 Ocak 2024 tarihinde alınmıştır.

Solomon, M. G. (2014). *Security strategies in windows platforms and applications* (1. baskı). Jones & Bartlett Publishers.

Stalans, L. J. ve Finn, M. A. (2016). Understanding how the internet facilitates crime and deviance. *Victims & Offenders,* 11(4), 501-508. https://doi.org/10.1080/15564886.2016.1211404.

Stark, R. (1999). Cyber terrorism: Rethinking new technology, department of defense and strategic studies, http://www.infowar.com/mil_c4i/stark/Cyber_Terrorism-Rethinking_New_Technology1.html. adresinden 14 Ocak 2024 tarihinde alınmıştır.

Staude-Müller, F., Hansen, B., ve Voss, M. (2012). How stressful is online victimization? Effects of victim's personality and properties of the incident. *European Journal of Developmental Psychology*, 9(2), 260-274.

Strongdm. (2024). Man-in-the-Middle (MITM) attack: Definition, examples & more. https://www.strongdm.com/blog/man-in-the-middle-attack. adresinden 24 Nisan 2024 tarihinde alınmıştır.

Study.com. (2023). Computer virus list, types & examples https://study.com/learn/lesson/computer-virus-types-examples.html. adresinden 23 Aralık 2023 tarihinde alınmıştır.

Suler, J. (2004). The online disinhibition effect. *Cyber Psychology & Behavior*. 7(3), 321-326. https://doi.org/10.1089/1094931041291295.

Şangay İşbirliği Örgütü. Yekaterinburg sözleşmesi. (2009). https://eng.sectsco.org/documents/?year=2009. adresinden 22 Aralık 2024 tarihinde alınmıştır.

Tabansky, L. (2011). Basic concepts in cyber warfare. *Military and Strategic Affairs*, 3(1), 75–92. https://scholar.google.com/citations?view_op=view_citation&hl=en&user=PnonZSkAAAAJ&citation_for_view=PnonZSkAAAAJ:KlAtU1dfN6UC

Taddeo, M. (2012). An analysis for a just cyber warfare, in: Cyber Conflict (CY-CON). https://ccdcoe.org/uploads/2012/01/3_5_Taddeo_AnAnalysisForAJustCyberWarfare.pdf. adresinden 12 Ocak 2024 tarihinde alınmıştır.

TDK. (2022). Güncel Türkçe sözlük. https://sozluk.gov.tr/. adresinden 28 Eylül 2023 tarihinde alınmıştır.

Techtarget. (2014), NSA TAO: What tailored access operations unit means for enterprises. https://www.techtarget.com/searchsecurity/tip/NSA-TAO-What-Tailored-Access-Operations-unit-means-for-enterprises. adresinden 28 Aralık 2023 tarihinde alınmıştır.

Techtarget. (2022). Computer worm, https://www.techtarget.com/searchsecurity/definition/worm. adresinden 6 Şubat 2023 tarihinde alınmıştır.

TechTarget. (2023). Melissa virus, https://www.techtarget.com/searchsecurity/definition/Melissavirus#:~:text=The%20Melissa%20virus%20was%20distributed,the%20infected%20user's%20address%20book. adresinden 15 Aralık 2023 tarihinde alınmıştır.

Techterms. (2020). Bricking. https://techterms.com/definition/bricking. adresinden 6 Nisan 2024 tarihinde alınmıştır.

Tereshchenko, N. (2013). US foreign policy challenges: Cyber terrorism & critical infrastructure, https://www.e-ir.info/pdf/39119. adresinden 11 Şubat 2024 tarihinde alınmıştır.

The Crown Prosecution Service. (2024). Terrorism. https://www.cps.gov.uk/crime-info/terrorism adresinden 11 Ocak 2024 tarihinde alınmıştır.

The HIPAA Journal. (2023). Regal Medical Group ransomware attack affects 3.3 million patients. https://www.hipaajournal.com/regal-medical-group-ransomware-attack-southeast-colorado-hospital-district-email-breach/. adresinden 14 Nisan 2023 tarihinde alınmıştır.

The HIPAA Journal. (2023b). 2022 healthcare data breach report, https://www.hipaajournal.com/2022-healthcare-data-breach-report/. adresinden 27 Eylül 2023 tarihinde alınmıştır.

The IT Law Wiki. (2023b). Data diddling. https://itlaw.fandom.com/wiki/Data_diddling#cite_note-2. adresinden 22 Mart 2023 tarihinde alınmıştır.

The New York Times. (2021a). Colonial pipeline paid 75 bitcoin or roughly $5 million to hackers. https://www.nytimes.com/2021/05/13/technology/colonialpipeline-ransom.html. adresinden 1 Ocak 2023 tarihinde alınmıştır.

The New York Times. (2021b). Scope of Russian hacking becomes clear:multiple U.S. agencies were hit, https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security pentagon.html. adresinden 10 Kasım 2023 tarihinde alınmıştır.

The Record. (2023). Dole, Pepsi bottler issue more info on recent cyberattacks. https://therecord.media/dole-pepsi-bottler-issue-more-info-on-recent-cyberattacks. adresinden 11 Ekim 2023 tarihinde alınmıştır.

The White House. (1997). Critical foundations: Protecting America's infrastructures. https://sgp.fas.org/library/pccip.pdf. adresinden 14 Ocak 2024 tarihinde alınmıştır.

ThreatDown. (2024). What is cyber espionage?. https://www.malwarebytes.com/cybersecurity/business/what-is-cyber-espionage. adresinden 17 Şubat 2024 tarihinde alınmıştır.

TIME. (2021). This company was hit with a devastating ransomware attack-but instead of giving in, it rebuilt everything. https://time.com/6080293/norsk-hydro ransomware-attack/. adresinden 27 Eylül 2023 tarihinde alınmıştır.

Timus. (2022). IP spoofing nedir? IP sahtekarlığı ne kadar tehlikelidir?. https://berqnet.com/blog/ip-spoofing. adresinden 12 Nisan 2024 tarihinde alınmıştır.

Tnetworks. (2024). İlerlemiş kalıcı tehdit saldırısı. http://www.tnetworks.com.tr/cozumler/advanced-persistent-threats-apt. adresinden 4 Mart 2024 tarihinde alınmıştır.

Tony Blair Institute for Global Change. (2020). Snapshot: how extremist groups are responding to COVID-19. adresinden 10 Şubat 2024 tarihinde alınmıştır. https://institute.global/sites/default/files/2020-05/Snapshot%203%20COVID19%20V02.pdf

Trellix. (2023). What is stuxnet?, https://www.trellix.com/en-us/security awareness/ransomware/what-is-stuxnet.html. adresinden 7 Şubat 2023 tarihinde alınmıştır.

Trend Micro, (2015). Hacktivism 101: A brief history and timeline of notable incidents. https://www.trendmicro.com/vinfo/es/security/news/cyber-attacks/hacktivism-101-a-brief-history-of-notable-incidents. adresinden 19 Ocak 2024 tarihinde alınmıştır.

Tripwire. (2018). Ransomware-as-a-Service (RaaS): How it works. (https://www.tripwire.com/state-of-security/ransomware-service-raas-works. adresinden 14 Mayıs 2024 tarihinde alınmıştır.

TÜBİTAK. (2024). Kritik bilgi sistem altyapıları için asgari güvenlik önlemleri dokümanı. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/kritik-bilgi-sistem-altyapilari-ic-in-asgari-gu-venlik-o-nlemleri-6445b90e-b2ad-4e5e-9c13-6ae19ba10e37.pdf. adresinden 16 Eylül 2023 tarihinde alınmıştır.

Ulaştırma ve Altyapı Bakanlığı. (2013). Ulusal siber güvenlik stratejisi ve 2013-2014 eylem planı. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/some-2013-2014-eylemplani.pdf. adresinden 10 Ağustos 2024 tarihinde alınmıştır.

Ulaştırma ve Altyapı Bakanlığı. (2020). 2020-2023 Ulusal Siber Güvenlik Strateji ve Eylem Planı.

Ulaştırma ve Altyapı Bakanlığı. (2024). 2024-2028 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı.

United Kingdom Government. (2006). UK Terrorism Act. https://www.legislation.gov.uk/ukpga/2006/11/contents

United Kingdom Government. (2008). UK Counter-Terrorism Act. https://www.legislation.gov.uk/ukpga/2008/28/contents. adresinden 11 Nisan 2024 tarihinde alınmıştır.

United Kingdom Government. (2011). UK Terrorism Prevention and Investigation Measures Act. https://www.legislation.gov.uk/ukpga/2011/23/contents. adresinden 11 Nisan 2024 tarihinde alınmıştır.

United Kingdom Government. (2015). UK Counter Terrorism and Security Act. https://www.legislation.gov.uk/ukpga/2015/6/contents/enacted. adresinden 11 Nisan 2024 tarihinde alınmıştır.

United Kingdom Government. (2019). UK Counter Terrorism and Border Security Act. https://www.legislation.gov.uk/ukpga/2019/3/contents. adresinden 11 Nisan 2024 tarihinde alınmıştır.

United Kingdom National Cyber Security Center. (2020). Mitigating malware and ransomware attacks. https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks. adresinden 20 Şubat 2024 tarihinde alınmıştır.

United Nations. (1945). The Charter of the United Nations. https://www.un.org/en/about-us/un-charter#:~:text=The%20Charter%20of%20the%20United,force%20on%2024%20October%201945. adresinden 14 Temmuz 2024 tarihinde alınmıştır.

United Nations. (2002). Responsibility of States for internationally wrongful acts A/RES/56/83. https://documents.un.org/doc/undoc/gen/n01/477/97/pdf/n0147797.pdf. adresinden 11 Mart 2024 tarihinde alınmıştır.

United Nations. (2024). Convention against cybercrime/strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes A/AC.291/L.15. https://documents.un.org/doc/undoc/gen/v24/055/06/pdf/v2405506.pdf. adresinden 24 Ağustos 2024 tarihinde alınmıştır.

United States General Accounting Office. (1997). Operation desert storm. https://www.gao.gov/assets/nsiad-97-134.pdf. adresinden 4 Nisan 2024 tarihinde alınmıştır.

United States Navy Defense Intelligence Agency. (1999). Cyberterror: Prospects and implications. https://apps.dtic.mil/sti/citations/ADA393147. adresinden 17 Ocak 2024 tarihinde alınmıştır.

US Army Training and Doctrine Command. (2005). *Cyber operations and cyber terrorism*, (1. Baskı), Government Printing Office.

US Canada Power System Outage Task Force. (2004). Final report on the August 14, 2003 blackout in the United States and Canada. https://www3.epa.gov/region1/npdes/merrimackstation/pdfs/ar/AR-1165.pdf. adresinden 24 Aralık 2023 tarihinde alınmıştır.

US Computer Security Resource Center. (2012). Guide for conducting risk assessments. https://csrc.nist.gov/pubs/sp/800/30/r1/final. adresinden 13 Şubat 2024 tarihinde alınmıştır.

US Computer Security Resource Center. (2024). Threat. https://csrc.nist.gov/glossary/term/threat adresinden 15 Mart 2024 tarihinde alınmıştır.

US Department Of Defense. (2020). DOD Dictionary of military and associated terms. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf. adresinden 14 Ekim 2023 tarihinde alınmıştır.

US Department Of Justice. (2014). Cyber criminal pleads guilty to developing and distributing notorious spyeye malware. https://www.justice.gov/opa/pr/cyber criminal-pleads-guilty-developing-and-distributing-notorious-spyeye-malware. adresinden 11 Ekim 2023 tarihinde alınmıştır.

US Government. (2001). Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act). https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.htm. adresinden 14 Mart 2024 tarihinde alınmıştır.

US Joint Chiefs of Staff. (1998). Joint doctrine for information operations (Joint Pub 3-13). https://www.c4i.org/jp3_13.pdf. adresinden 26 Nisan 2024 tarihinde alınmıştır.

Veracode. (2023). Rootkit: What is a rootkit?. https://www.veracode.com/security/rootkit. adresinden 13 Mart 2023 tarihinde alınmıştır.

Verywellfamily. (2024). The effects of slut shaming on teen girls. (https://www.verywellfamily.com/the-effects-of-slut-shaming-on-teen-girls-460586. adresinden 11 Aralık 2023 tarihinde alınmıştır.

Vitula, M. (2015). *Learning ANTI2 for android pentesting* (1. Baskı). Packt Publishing.

Walker, M. (2014). *CEH certified ethical hacker all-in-one exam guide* (1. Baskı). McGraw Hill Osborne Media

WBTV. (2021). GasBuddy reports 71% of gas stations without fuel in Charlotte metro amid colonial pipeline shutdown. https://www.wbtv.com/2021/05/11/long-lines charlotte-gas-supply-squeezed/. adresinden 15 Aralık 2023 tarihinde alınmıştır.

Weiner, N. (1948). *Cybernetics or control and communication in the animal and the machine* (2. Baskı). The MIT Press.

Weissbrodt, D. (2013). Cyber-conflict, cyber-crime, and cyber-espionage. *Minnesota Journal of International Law*, 22(347), https://scholarship.law.umn.edu/faculty_articles/223.

Wikipedia. (2023). Truva atı. https://tr.wikipedia.org/wiki/Truva_At%C4%B1#:~:text=Truva%20at%C4%B1%2C %20 Odysseus'un%20Truva,bir%20at%20yapma%20fikri%20gelir. adresinden 3 Mart 2023 tarihinde alınmıştır.

Wikipedia. (2024). IBM selectric typewriter. https://en.wikipedia.org/wiki/IBM_Selectric_typewriter. adresinden 20 Şubat 2023 tarihinde alınmıştır.

WİRED. (2011). Get hacked, don't tell: Drone base didn't report virus. https://www.wired.com/2011/10/drone-virus-kept-quiet/. adresinden 16 Mart 2023 tarihinde alınmıştır.

World Economic Forum (WEF). (2012). Risk and responsibility in a hyperconnected World: pathways to global cyber resilience. https://www.weforum.org/publications/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience/. adresinden 19 Nisan 2024 tarihinde alınmıştır.

Wortham, A.,(2012). Should cyber exploitation ever constitute a demonstration of hostile ıntent that may violate un charter provisions prohibiting the threat or use of force?. *Federal Communications Law Journal.* 64(3). https://www.repository.law.indiana.edu/fclj/vol64/iss3/8/

WSJ.COM. (2023). Surge in hospital hacks endangers patients cyber official says, https://www.wsj.com/articles/record-hacks-on-hospitals-endanger-patients-cyber official-says-25a7ad3b. adresinden 18 Aralık 2023 tarihinde alınmıştır.

Yağcı, B. (2023). Bilgi ve iletişim teknolojilerinin gelişmesiyle değişen siber suç tanımı ve yaklaşımlar. *Bilgi Teknolojilerinin ve İletişim Dergisi*, 1(1), 147-182.

Yao, D. D., Shu, X., Cheng, L. ve Stolfo, S. J. (2018). *Anomaly detection as a service: Challenges, advances, and opportunities* (1. Baskı). Morgan & Claypool Publishers.

Yayla, M. (2013a). Hukuki bir terim olarak "siber savaş". *Türkiye Barolar Birliği Dergisi,* 104*,* 177-202

Yayla, M. (2013b). Uluslararası hukukta siber saldırılara karşı kuvvet kullanma. *Türkiye Barolar Birliği Dergisi, 107,* 199-220.

Yener, S. (2013). *Siber uzay güvenliği: Ulusal güvenlik ve uluslararası güvenliğe etkileri* [Yüksek lisans tezi / Uludağ üniversitesi]. https://acikerisim.uludag.edu.tr/items/a4ee9139-8d0c-4a6f-9af7-b7de7ed1a817

Yıldız, D. (2022). Rootkit Nedir?. https://teknoloji.org/rootkit-nedir. adresinden 14 Mart 2024 tarihinde alınmıştır.

ZDNET. (2020a). Israel government tells water treatment companies to change passwords. https://www.zdnet.com/article/israel-says-hackers-are-targeting-its water-supply-and-treatment-utilities/. adresinden 27 Eylül 2023 tarihinde alınmıştır.

ZDNET. (2020b) Two more cyber-attacks hit Israel's water system, https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/. adresinden 27 Eylül 2023 tarihinde alınmıştır.

Zenarmor. (2023a). Logic bomb: Definition, examples, and prevention, https://www.sunnyvalley.io/docs/network-security-tutorials/what-is-logic-bomb. adresinden 4 Mart 2023 tarihinde alınmıştır.

Zenarmor. (2023b). Logic bomb: Definition, examples, and prevention. https://www.zenarmor.com/docs/network-security-tutorials/what-is-logic-bomb. adresinden 4 Mart 2024 tarihinde alınmıştır.

Zer0-Day. (2024). Zero-DAY vulnerability statistics. https://www.zero-day.cz/research/. adresinden 17 Temmuz 2024 tarihinde alınmıştır.

Zweig, J. M., Lachma, P., Yahner, J. ve Dank, M. (2014). Correlates of cyber dating abuse among teens. *J Youth Adolescence*, 43(8), 1306-1321. doi: 10.1007/s10964-013-0047-x.

657 sayılı Devlet Memurları Kanunu, R.G. T. 23/07/1965, S. 12056.

2577 sayılı İdari Yargılama Usulü Kanunu, R.G. T. 20/01/1982, S. 17580.

3713 sayılı Terörle Mücadele Kanunu, R.G. T. 12/04/1991, S. 20843.

5237 sayılı Türk Ceza Kanunu, R.G. T. 12/10/2004, S. 25611.

5233 sayılı Terör ve Terörle Mücadeleden Doğan Zararların Karşılanması Hakkında Kanun, R.G. T. 27/07/2004, S. 25535.

5271 sayılı Ceza Muhakemesi Kanunu, R.G. T. 17/12/2004, S. 25673.