



İSTANBUL MEDENİYET ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI

**Siber Uzay Ve Uluslararası Hukuk: Devlet Kaynaklı
Yeni Nesil Tehditlere Karşı Hukuki Çözümler**

Yüksek Lisans Tezi

Huri Uysal

Nisan 2025



İSTANBUL MEDENİYET ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI

**Siber Uzay Ve Uluslararası Hukuk: Devlet Kaynaklı
Yeni Nesil Tehditlere Karşı Hukuki Çözümler**

Yüksek Lisans Tezi

Huri Uysal

Danışman

Dr.Öğr. Üyesi Özlem Yücel

Nisan 2025

TEZ JÜRİSİ ONAYI

Huri Uysal tarafından hazırlanan "Siber Uzay ve Uluslararası Hukuk: Devlet Kaynaklı Yeni Nesil Tehditlere Karşı Hukuki Çözümler" başlıklı bu Yüksel Lisans Tezi, Uluslararası İlişkiler Anabilim Dalı'nda hazırlanmış ve jürimiz tarafından kabul edilmiştir.

JÜRİ ÜYELERİ

İMZA

Tez Danışmanı:

Dr. Öğr.Üyesi Özlem Yücel
İMÜ SBF Uluslararası İlişkiler

Üyeler:

Doç.Dr. Abdülkadir Akıl
İstanbul Ticaret Üniversitesi

Prof.Dr. Ahmet Nohutçu
İMÜ SBF Siyaset Bilimi ve Kamu Yönetimi

Tez Savunma Tarihi: 28/ Nisan / 2025

BEYANLAR

Yazım ve Kaynak Gösterme Beyanı

Danışmanlığımda yazılan bu tezin APA yazım ve kaynak gösterme klavuzunda belirtilen kurallara uygun olarak yapılandırıldığı ve bu klavuzun metin içi kaynak gösterme standartlarının bu tezde tutarlı olarak uygulandığı tarafımdan teyit edilmiştir.

İmza

Dr. Öğr. Üyesi Özlem Yücel

Etik İlkeler Sadakat Beyanı

Hazırladığım bu tezin tamamen kendi çalışmam olduğunu, akademik ve etik kuralları gözeterek çalıştığımı ve her alıntıya kaynak gösterdiğimi beyan ederim.

İmza

Huri Uysal

ÖNSÖZ

Siber uzay kavramı, 20. Yüzyılda internetin bulunması ve bilgisayarların birbirine ağlarla bağlanması neticesinde hayatımıza girmiş, 21. Yüzyılda teknolojik gelişmelerin, internete bağlı cihaz sayısının artması ve nesnelerin interneti, yapay zeka gibi kavramların ortaya çıkması ile birlikte uluslararası alanda devletler açısından yeni bir hakimiyet alanının oluşmasını beraberinde getirmiştir. Bu yeni alan ve beraberinde getirdiği tehditlerin uluslararası hukukta nasıl karşılık bulduğu ise son zamanlarda merak konusu olmuştur.

Bu çalışmada uluslararası hukukun, devletlere karşı yönelen bu yeni nesil tehdit türü karşısındaki durumu incelenmiştir.

Başta tezimin konusunu, başlığını belirlememde ve bu çalışmanın her aşamasında beni en doğrusunu bulmaya yönlendiren, beni çalışmanın her aşamasında cesaretlendiren ve sabırla en iyisini yapacağım konusunda yüreklendiren danışmanım Dr. Öğr. Üyesi Özlem Yücel hocama teşekkürü bir borç bilirim.

Ayrıca beni her zaman ve her koşulda destekleyen, bu çalışma sürecinde hayal kırıklığına uğradığımda, yorulduğumda pes etmeden devam etmem için yüreklendiren sevgili annem Ayşe Uysal ve babam Mustafa Uysal'a teşekkür ederim.

Son olarak yüksek lisans öğrenciliğim sürecinde Uluslararası Hukuk dersini bana sevdiren ve benden desteğini esirgemeyen çok kıymetli hocam Prof. Dr. Berdal Aral'a çok teşekkür ederim.

Özet

SİBER UZAY VE ULUSLARARASI HUKUK: DEVLET KAYNAKLI YENİ NESİL TEHDİTLERE KARŞI HUKUKİ ÇÖZÜMLER

Uysal, Huri

Yüksek Lisans Tezi, Uluslararası İlişkiler Ana Bilim Dalı

Danışman: Dr.Öğr.Üyesi Özlem Yücel

Nisan,2025

Güvenlik olgusu ve güvende hissetme arzusu insanlar için olduğu kadar devletler için de en önemli ihtiyaçtır. İmparatorlukların kurulup yıkıldığı daha sonrasında devletlerin arenaya çıktığı uluslararası alanda değişmeyen tek şey güvenlik ihtiyacı olmuştur. Güvende hissetme ihtiyacı ise her zaman savunma ve saldırı taktiklerinin geliştirilmesi çabasını beraberinde getirmiştir. Asırlar boyunca savunma ve saldırı araçlarında yöntemler, saldırı araçları değişmiş ve her yeni bulunan teknoloji neredeyse ilk önce askeri alanda kullanılan saldırı ve savunma araçlarının yenilenmesi ve dönüştürülmesinde kullanılmıştır. Buharlı makinelerin icadı ile buharlı gemilerin geliştirilmesi ve neticede savaş gemilerinin büyüklüğünün artması, metalin işlenmesi neticesinde silah yapımı ve ateşli silahların, tüfeklerin ve neticede otomatik makineli tüfeklerin ortaya çıkması, içten yanmalı motorların üretilmesi neticesinde iki dünya savaşına da damgasını vuran savaş uçaklarının geliştirilmesi buna sadece birkaç örnektir. Üçüncü endüstri devriminin beraberinde getirdiği bilgi devrimi ve nihayetinde dördüncü endüstri devriminin ortaya çıkardığı teknolojik devrim de etkisini gene ilk önce askeri alanda göstermiştir. Öyle ki internetin bulunması askeri bir kurum olan DARPA tarafından savunma faaliyetlerinin geliştirilmesi amacıyla olmuştur. Bilgisayarların ve internetin gelişimi, adına siber uzay denilen, uluslararası alanda daha önce benzeri görülmemiş, insan yapımı bir alanın ortaya çıkmasına neden olmuştur. Bu yeni ve bilinmeyen alan yeni nesil tehditleri, yeni saldırı yöntemlerini de beraberinde getirmiştir. Ancak bu yeni nesil saldırı yöntemleri günümüze kadar uygulanmış olan uluslararası hukuk kurallarının da sorgulanmasına neden olmuştur. Bu çalışmada bu sorgulamanın nedenleri, nasıl oluştuğu ve sorunun çözümü için

yapılabilecekler siber uzay kavramının ortaya çıkışından itibaren aşama aşama günümüze kadar sürecin incelenmesi, en bilinen siber saldırılar ve bu yeni nesil tehdit karşısında uluslararası hukukun mevcut durumu ele alınarak incelenmeye çalışılmıştır.

Anahtar Kelimeler : Güvenlik ihtiyacı, Savunma ve saldırı, Teknolojik devrim, Yeni nesil tehdit, Siber uzay, Uluslararası hukuk

Abstract

CYBERSPACE AND INTERNATIONAL LAW: LEGAL SOLUTIONS AGAINST STATE-BASED NEW GENERATION THREATS

Uysal, Huri

Master Thesis, Department of International Relations

Supervisor: Assistant Professor Özlem Yücel

Nisan, 2025

The concept of security and the desire to feel safe are the most important needs for states as well as people. In the international arena where empires was established and collapsed and later states entered the arena, the only constant has been the need for security. The need to feel safe has always brought with it the effort to develop defense and attack tactics. Over the centuries, methods and means of defense and attack have changed, and almost every newly found technology has been used first in the renewal and transformation of attack and defense tools used in the military field. The invention of steam engines and the development of steamships and the resulting increase in the size of warships, the production of weapons as a result of metal processing and the emergence of firearms, rifles and eventually automatic machine guns, the development of fighter planes that left their mark on both world wars as a result of the production of internal combustion engines are just a few examples of this. The information revolution brought about by the Third Industrial Revolution and ultimately the technological revolution brought about by the Fourth Industrial Revolution also showed its effect first in the military field. In fact, the invention of the internet was made by DARPA, a military institution, for the purpose of developing defense activities. The development of computers and the internet has led to the emergence of an unprecedented and man-made area called cyberspace in the international arena. This new and unknown area has brought new generation threats and new attack methods. However, these new generation attack methods have also caused the international law rules that have been applied to date to be questioned. In this study, the reasons for this questioning, how it was formed and what can be done to solve the problem are examined step by step from the emergence of the concept of cyberspace to the present

day, the most known cyber attacks and the current status of international law in the face of this new generation threat are examined.

Keywords : Need for security, Defence and attack, Technological revolution, New generation threat, Cyber space, International law

İÇİNDEKİLER

ÖNSÖZ	iv
Özet	v
Abstract.....	vii
İÇİNDEKİLER	ix
KISALTMALAR.....	xii
Giriş.....	1
Tezin Amacı	2
Tez'in Kapsamı ve Yöntemi	3
Tez'in Özgün Yanı	5
1.BÖLÜM	6
Siber Uzay'ın Tanımı ve Özellikleri	6
1.1.Bilgisayarların ve İnternetin Gelişimi.....	6
1.2.Siber Uzay Kavramının Ortaya Çıkışı ve Siber Uzayın Tanımı ve Özellikleri8	
1.3. Siber Uzayın Getirdiği Yenilikler ve Tehditler	10
1.3.1. Nesnelerin İnterneti.....	12
1.3.2. Yapay Zeka.....	15
1.3.3. Endüstriyel Robotlar	17
1.3.4.Akıllı Şehirler	21
2.BÖLÜM	25
Siber Uzayda Devlet Kaynaklı Tehditler ve Kullanılan Yöntemler	25
2.1.Devletlerin Değişen Tehdit ve Güvenlik Algısı	25
2.2.Siber Orduların Kurulma Süreci	26
2.3.Devlet Kaynaklı Yeni Nesil Saldırı Yöntemleri	28
2.3.1.Virüsler	30
2.3.2.Worm (Solucan).....	30
2.3.4. DoS ve DDoS Atakları.....	31
2.3.5. Siber Casusluk	32
2.3.6. APT (Advanced Persistent Threat - Gelişmiş Kalıcı Tehdit).....	32
2.3.7. Mantık Bombası Virüsü.....	32
3.BÖLÜM	34
Siber Saldırı Örnekleri.....	34

3.1.Geçmişte Yaşanan Siber Saldırıları	34
3.1.1. 1982 Sibiry Mantık Bombası Saldırısı.....	34
3.1.2. Moonlight Maze Saldırısı (Ayışığı Labirenti saldırısı)	35
3.1.3.Titan Rain Saldırısı	35
3.1.4. 2007 Estonya Siber Saldırısı.....	36
3.1.5. 2008 Gürcistan Siber Saldırısı	37
3.1.6. 2010 İran Stuxnet Saldırısı	38
3.1.7. 2012 Suudi ARAMCO Siber Saldırısı	39
3.1.8. İsrail'in Lübnan'da Gerçekleştirdiği Siber Saldırı.....	40
4. BÖLÜM	43
Saldırı Suçu ile İlgili Temel Uluslararası Hukuk İlkelerinin Siber Saldırlara Uygulanabilirliği ve Tallinn Rehberi.....	43
4.1. Saldırı Suçu İle İlgili Temel İlkelerin Siber Saldırlara Uygulanması	43
4.2.Tallinn Rehberi ve Siber Saldırıları Konusundaki Önerileri	49
5.BÖLÜM	53
Uluslararası Örgütlerin Siber Uzay ve Siber Güvenlik ile ilgili Çalışmaları	53
5.1. BM, AB Ve NATO'nun Siber Uzay Ve Siber Güvenlik İle İlgili Çalışmaları	53
5.1.1. Birleşmiş Milletlerin Siber Uzay ve Siber Güvenlik ile İlgili Çalışmaları...	53
5.1.2. AB'nin Siber Uzay ve Siber Güvenlik İle İlgili Çalışmaları	55
5.1.3.NATO'nun Siber Uzay ve Siber Güvenlik ile İlgili Çalışmaları	57
5.1.4. NATO ve AB 'nin Siber Uzay ve Siber Güvenlik ile İlgili birlikte yaptıkları çalışmalar	59
5.2. Avrupa Konseyi, Afrika Birliği ve OECD'nin Siber Güvenlik İle İlgili Çalışmaları	60
5.2.1. Avrupa Konseyi'nin Siber Uzay ve Siber Güvenlik ile ilgili Çalışmaları.....	60
5.2.2. Afrika Birliğinin Siber Uzay ve Siber Güvenlik ile ilgili Çalışmaları.....	61
5.2.3. Ekonomik İşbirliği ve Kalkınma Örgütü'nün (OECD) Siber Uzay ve Siber Güvenlik Hususundaki Çalışmaları	63
5.3. Diğer Uluslararası Örgütlerin Siber Güvenlik Çalışmaları.....	65
5.3.1.Uluslararası Telekomünikasyon Birliği'nin (ITU) Siber Güvenlik İle İlgili Çalışmaları	65
5.3.2. Dünya Ticaret Örgütü'nün (WTO) Siber Güvenlik İle İlgili Çalışmaları	66
5.3.3. Uluslararası Para Fonu'nun (IMF) Siber Güvenlik İle İlgili Çalışmaları.....	66
6.Bölüm	68
Uluslararası Hukukta Siber Saldırıları Hususunda Karşılaşılan Sorunlar	68
6.1. Siber Saldırıları Atfedilebilirlik Sorunu	68
6.1.1. Devlet Tarafından Yapılan Siber Saldırıların Atfedilmesi Hususu	73

6.1.2. Devlet Eliyle Yaptırılan Siber Saldırıların Atfedilmesi Hususu	75
6.2. Hukuki Süreçlerdeki Diğer Mevcut Engeller	78
6.3. Emsal Kabul Edilen Davaların Siber Saldırlara Uygulanması Konusunda Yaşanan Karışıklıklar	82
6.3.1. 1949 Korfu Boğazı Davası Kararının Siber Saldırlara Uygulanması.....	82
6.3.2. 1986 Nikaragua Davası Kararının Siber Saldırlara Uygulanması	83
6.3.3.Eski Yugoslavya Uluslararası Ceza Mahkemesinin Tadiç Davası Kararının Siber Saldırlara Uygulanması	85
7.Bölüm	86
Siber Saldırıları ile İlgili Geleceğe Yönelik Öngörüler	86
7.1. Siber Tehditlerin Gelecekteki Evrimi ve Tehdidin Boyutlarının Anlaşılması	86
7.2.Siber Saldırıları İle İlgili Mevcut Durum ve Alınması Gereken Önlemler.....	88
7.3. Devletlerin ve Uluslararası Örgütlerin Konuyla ilgili Sorumlulukları	90
SONUÇ	96
KAYNAKÇA	100
ÖZGEÇMİŞ	118

KISALTMALAR

AB	Avrupa Birliđi
ABD	Amerika Birleşik Devletleri
AIVD	Hollanda Genel İstihbarat ve Güvenlik Servisi
APT	Gelişmiş Kalıcı Tehdit
ARAMCO	Arap - Amerikan Petrol Şirketi
ARPANET	İleri Araştırma Projeleri Ajansı Ađı
ARPA	İleri Araştırma Projeleri Ajansı
ARSIWA	Devletlerin Uluslararası Haksız Eylemlerden Dolayı Sorumluluđu
AUS	Akıllı Ulaşım Sistemleri
BAC	İşletme Yönetimi ve Hizmetleri
BBC	İngiliz Yayın Kurumu
BİT	Bilgi ve İletişim Teknolojileri
BM	Birleşmiş Milletler
BMGK	Birleşmiş Milletler Genel Kurulu
BİT /ICT	Bilgi Teknolojileri
CCDCOE	NATO İşbirlikçi Siber Savunma Mükemmeliyet Merkezi
CDMA	Siber Savunma Yönetim Otoritesi
CERT-EU	Avrupa Bilgisayar Güvenlik Olaylarına Müdahale Ekibi
CEPOL	Avrupa Birliđi Kolluk Kuvvetleri Ajansı
CIA	Merkezi İstihbarat Ajansı
DARPA	Savunma İleri Araştırmaları Ajansı
DoS	Hizmet Reddi
DDoS	Dağıtılmış Hizmet Reddi
DNS	Alan Adı Sistemi
GATT	Gümrük Tarifeleri Ve Ticaret Genel Anlaşması
GDPR	Genel Data Güvenliđi Direktifi
GGE	Hükümet Uzmanları Grubu
G.Kore	Güney Kore
HTML	Zengin Metin İşaret Dili

HTTP	Hiper Metin Transfer Protokolü
ECOSOC	Ekonomik ve Sosyal Konsey
ENISA	Avrupa Siber Güvenlik Ajansı
IBM	Uluslararası İş Makineleri
ITU	Uluslararası Telekomünikasyon Birliği
IMF	Uluslararası Para Fonu
ICJ	Uluslararası Adalet Divanı
ICCP	Bilgi Bilgisayar Ve İletişim Politikaları Komitesi
ICOM	Şirketleşmiş Malzeme Departmanı
IoT	Nesnelerin İnterneti
IIoT	Endüstriyel Nesnelerin İnterneti
LOAC	Silahlı Çatışma Hukuku
MIT	Massachusetts Teknoloji Enstitüsü
M2M	Makineden Makineye
NASA	Ulusal Havacılık ve Uzay Dairesi
NATO	Kuzey Atlantik Antlaşması Örgütü
NCIRC	NATO Bilgisayar Olaylarına Müdahale Yeteneği
NCIA	NATO İletişim ve Bilgi Ajansı
NSA	Amerikan Ulusal Güvenlik Dairesi
NIS	Ağ ve Bilgi Güvenliği Direktifi
UAD	Uluslararası Adalet Divanı
OAU	Afrika Birliği Örgütü
OECD	Uluslararası Ekonomik İşbirliği Örgütü
OEWG	Açık Uçlu Çalışma Grubu
OGSP	Ortak Güvenlik Ve Savunma Politikası
PC	Kişisel Bilgisayar
PCIJ	Daimi Uluslararası Adalet Divanı
PIC	Çevresel Ünite Denetleme Arabirimi
PLC	Programlanabilir Mantık Kontrolörü
SAP	Alman Çokuluslu Yazılım Şirketi
SCADA	Merkezi Denetim Ve Veri Toplama Sistemi
SOME	Siber Olaylara Müdahale Ekibi

SSCB	Sovyet Sosyalist Cumhuriyetler Birliđi
RAT	Rastgele Eriřim Tehdidi
RF	Rusya Federasyonu
UAD	Uluslararası Adalet Divanı
TCP/IP	İletiřim Kontrol Protokolü/ İnternet Protokolü
USB	Evrensel Seri Yolu
USOM	Ulusal Siber Olaylara Müdahale Merkezi
UNIDIR	BM Silahsızlanma Arařtırmaları Enstitüsü
vb	Ve benzeri
yy	Yüzyıl
YFC	Yugoslavya Federal Cumhuriyeti
WSN	Kablosuz Ağ Bađlantısı
WSIS	Dünya Bilgi Toplumu Zirvesi
WTO	Dünya Ticaret Örgütü

Giriş

Bilgisayarların hayatımıza girişı 1950'lerde olmuştur. 1958 yılında dönemin ABD başkanı Dwight D. Eisenhower askeri uygulamalarda teknolojinin geliştirilmesi, yeni teknolojik gelişmelerin takip edilerek askeri alana uygulanması amacıyla ARPA (İleri Araştırma Projeleri Ajansı - Advanced Research Project Agency) kurulmasına öncülük etmiş daha sonra bu ajans DARPA (Savunma İleri Düzey Araştırma Projeleri Ajansı - Defence Advanced Project Agency) adını almıştır (Dennis, 2024). İnternet'in tarihi ise, 1960'larda DARPA tarafından bilgisayar ve askeri araştırma projelerini desteklemek için geliştirilen ARPANET'e dayanır. ARPANET zamanla farklı kuruluşların da katkıları ile geliştirilmiştir (Bıçakcı,2014:101-130). 1983'te ise, ARPANET kullanıcıları iletişim kontrol protokolü /internet protokolü (TCP/IP) diye bilinen protokole geçmişlerdir (Güreşçi, 2019:85-97). Zamanla ARPANET kullanımdan kaldırılrsa da TCP/IP altyapısı ve protokolü kullanılmaya devam etti ve geliştirildi. Bilgisayar ve iletişim dünyası internetin bulunması neticesinde görülmemiş bir şekilde değışti. Dünya çapında yayın yapabilme, bilgilerin paylaşımı ve coğrafi sınırlamanın olmaması interneti insanlar için vazgeçilmez hale getirdi. Zamanla daha çok geliştirilen internet ağları ve e-mail gibi uygulamaların ortaya çıkması neticesinde internet kullanımı yaygınlaşmış ve kurumların kendi internet ağları oluşmaya başlamıştır. 1989'da Tim Barners Lee tarafından geliştirilen World Wide Web (Dünya Çapında Ağ) hayatımıza girdiğinde internet üzerinden bilgi paylaşımı mümkün hale gelmiştir. Çünkü Lee, World Wide Web ile HTML (Hyper Text Markup Language/ zengin metin işaret dili) formundaki içeriklere HTTP (Hyper Text Transfer Protocol/ Hiper Metin Transfer Protokolü) yolu ile ulaşım olanağı sağlamıştır (Lee, 1989:1-16). Tüm bu gelişmeler sayesinde dünyanın her yerinden insanlar istedikleri bilgiye erişebilme imkanı bulmuşlardır. İşte bu veri akışının ardında, içerisinde binlerce bilgisayarın, bilgisayar ekipmanlarının, sunucuların, internet sağlayıcı araçların, fiber optik kabloların bulunduğu siber uzay denilen alan yer alır. Bilgi akışının sağlanması amacıyla insan eliyle oluşturulan bu alan sayesinde dünyanın her neresinde olursak olalım bilgiye erişim sadece bir bilgisayar tuşu kadar uzağımızdadır. Bu yeni alan sayesinde devlet kurumlarının işleyişı kolaylaşmış, akıllı şehirler, akıllı ulaşım araçları hem devletin gelişmişliğinin işaretleri olmuş hem de insanların yaşamı daha konforlu hale gelmiştir. Yapay zeka teknolojileri sayesinde bilgiye erişimin, bankacılık işlemlerinin

kolaylaşması ile özellikle devlet dairelerinin iş yükü azalmış, endüstriyel robotlar ise, hem üretim süreçlerini hızlandırmış hem de üretimde kalitenin artırılmasını sağlamıştır. Tüm bu teknolojik yenilikler hayatımıza hemen hemen her alanda daha önce görülmemiş kolaylıklar getirmiştir. Tabii tüm bu kolaylıklar beraberinde güvenlik ihlallerini de getirmiştir. Özellikle devlet kurumlarının ağlarına illegal yollardan girilerek kurumlara ait gizli bilgilere ulaşılması neticesinde olayın tehlikeli boyutlara ulaşabileceği ve devletlerin gizli bilgilerine başka bir devlet tarafından ya da o devletin bir çalışanı tarafından erişilebileceği, bir zararlı yazılımın bankacılık sistemlerine bulaştırılması sonucunda milyarlarca dolar zarara yol açabileceği ve yahut da havaalanları, barajlar, akıllı trenler gibi internet ve bilgisayar sistemleri aracılığıyla kontrol edilen sistemlerin bir zararlı yazılım aracılığıyla işlemez hale getirilebileceği anlaşılmıştır. Dolayısıyla Siber uzay'ın tehlikeli yönü, bu alanda saldırmanın savunmaktan çok daha kolay ve ucuz oluşu hem devletlerin ilgisini çekmiş hem de tedirginlik yaşamalarına neden olmuştur. Pek çok devlet bu alandan gelebilecek tehlikelere engel olmak ve caydırıcılık elde etmek için artık siber ordular kurmaya başlamış bu da savaşın ve saldırının boyutlarının değişmesine neden olmuştur. İşte saldırının değişen bu boyutu yani siber uzay kaynaklı tehditler hem uluslararası hukuk hem de devletler için yeni bir boyuttur ve bu alandan gelmesi muhtemel saldırılar yeni nesil tehditler olarak algılanmaktadır.

Bu çalışmada uluslararası hukukta devletler arasında barışın korunabilmesi için bu yeni nesil tehditlere karşı etkin ve caydırıcı çözümler mevcut mu, yoksa bu yeni operasyon alanı ve bu alanda yaşanan devlet kaynaklı yeni nesil tehditler için yeni bir uluslararası örgüt gerekli mi, bu tartışılacaktır.

Tezin Amacı

1950'lerde Bilgisayarın icadı ve sonrasında 1969'da İnternetin ARPANET ile adım adım hayatımıza girişi ve önce sadece askeri alanda kullanılmaya başlayan internetin zamanla üniversiteler kamu kurumları gibi devlet dairelerinde kullanılmaya başlanması, 1990'larda bilgisayarların giderek küçülüp işlevlerinin artmaya başlaması ve kişiselleşmeye başlaması ardından World Wide Web ile internetin bireylerin hayatına girmesi, giderek karmaşıklaşan ağ donanımlarının coğrafi sınırları ortadan kaldırması, bir uygulama ile markete gitmeden alışveriş yapabilme imkanı sunan bilgisayar ve internet

ağları, tüm bu teknolojinin altyapısını sağlayan ve okyanus tabanlarında bile mevcut bulunan fiber optik kablolar siber uzay dediğimiz alanı oluşturan yapıdır.

Bilgisayarların ve internetin baş döndüren gelişimi ve siber uzay dediğimiz bu alanın hayatımıza kattığı pek çok yeniliğin ve artının yanında bir de güvenlik sorunları gibi dezavantajları vardır. Çünkü artık saldırının boyutları ve türleri çok değişmiş, çeşitlenmiş ve karmaşık hale gelmiştir. Bu güvenlik sorunları özellikle uluslararası alanda kendini hissettirmektedir.

Çalışmanın amacı, siber uzay dediğimiz alanın karmaşık yapısı ve güvenlik sorunları oluşturmaları, bu alanda devletler arasında meydana gelen saldırıların gün geçtikçe ve teknoloji ilerlemeye devam ettikçe daha tehlikeli boyutlara gelmeye başlaması neticesinde mevcut hukuki yöntemlerin, uluslararası hukukta bu konuda alınan kararların ve uluslararası örgütlerin bu konudaki girişimlerinin tek başına bu tehlikeleri önleyememesi nedeniyle siber uzay dediğimiz alanda ortaya çıkan ve çıkabilecek güvenlik eksikliklerinin giderilebilmesi için yeni uluslararası hukuk kuralları mı konulmalı, yoksa sadece bu alanı ve bu alandan gelecek saldırıları hedef alan, sadece siber uzayda hukuki düzeni ve güvenliği sağlamayı hedefleyen bir Uluslararası Siber Uzay Örgütü mü kurulmalı sorusunun cevabını aramaktır.

Tez'in Kapsamı ve Yöntemi

Siber uzay olarak tabir ettiğimiz alan yeni nesil saldırı yöntemlerinin geliştirilip uygulandığı, karmaşıklığı, dinamik yapısı ve anonim özelliği ile bilinen bir alandır. Bu alanda saldırmak savunmaktan çok daha ucuz ve daha kolaydır. Siber uzayda tehdit ve saldırılar çok çeşitli olduğu gibi bu saldırıları yapanlar da çok çeşitlidir. Ancak bu çalışmanın kapsamı siber uzay olarak tabir edilen alanda devlet kaynaklı yeni nesil saldırı yöntemlerini ve bu yöntemlerin uluslararası hukuk kapsamındaki karşılığı, gelişmeye ve tehlikeli hale gelmeye devam eden siber uzay kaynaklı saldırılara karşı uluslararası alanda daha etkili bir yöntem olabilir mi, belki de yeni bir uluslararası örgütün kurulması gerekir mi, bu konuları içeriyor.

Yedi bölüm halinde ele alınan bu konuda ilk bölümde önce Bilgisayarın ve internetin ortaya çıkışı ve gelişimi, internetin günden güne hayatımızın her alanına nasıl girdiği açıklayıcı bir dille anlatılacak, daha sonrasında siber uzay dediğimiz kavramın ortaya

çıkışı, tanımı, teknolojinin çok hızlı bir şekilde gelişmesi sonucunda beraberinde getirdiği yenilikler, yeni teknolojik gelişmeler, bunların oluşturduğu dezavantajlar ve güvenlik tehditleri, özellikle devletler arasındaki tehdit anlayışına getirdiği yenilikler açıklayıcı ve kavramsallaştırıcı yöntemle ifade edilecek.

Üç bölüm ve alt başlıklardan oluşan İkinci bölümde öncelikle devletlerin değişen tehdit ve güvenlik algısı ve buna bağlı olarak siber orduların kurulması süreci anlatılacaktır. Daha sonra siber uzayda devletler tarafından kullanılan yeni nesil saldırı yöntemlerine değinilecektir.

Gene üç bölüm ve alt başlıklardan oluşan üçüncü bölümde geçmişte yaşanan siber saldırı örnekleri ayrı başlıklar altında ayrıntılı bir şekilde incelenecektir. Dördüncü bölümde ise, saldırı suçu ile ilgili mevcut temel uluslararası hukuk ilkelerinin siber saldırılara uygulanabilirliği ve Tallinn Rehberi ayrıntılarıyla ele alınacaktır. Beşinci bölümün ilk ve ikinci kısmında BM ve AB gibi uluslararası örgütlerin ve uluslararası askeri bir ittifak olan NATO'nun ve ayrıca bu konuda önemli çalışmalar yapmış olan diğer uluslararası örgütlerin siber uzay konusunda yaptıkları çalışmaların ve aldıkları önlemlerin değerlendirilmesi yapılacaktır.

Uluslararası hukukta siber saldırılar hususunda karşılaşılan sorunların ele alınacağı altıncı bölümde ise, ilk olarak siber saldırılarda atfedilebilirlik konusu iki başlık halinde ele alınıp incelenecek, ikinci bölümde hukuki süreçlerdeki diğer mevcut engellere değinilecek ve altıncı bölümün son kısmında ise uluslararası hukukta silahlı saldırı konusunda emsal kabul edilen davaların siber saldırılara nasıl uygulanabileceği tartışılacaktır.

Yedinci bölümde ise, siber tehditlerin gelecekteki evrimi ve tehdidin gerçek boyutlarının anlaşılması konusu işlenecek, ardından siber saldırılar hususunda uluslararası alanda alınması gereken önlemler tartışılacak son olarak da devletlerin, BM, AB, NATO ve diğer uluslararası örgütlerin konu ile ilgili sorumluluklarına değinilecektir.

Tezin sonuç kısmında ise, öncelikle konu hakkında elde edilen bulgular paylaşılacak, bu yeni nesil saldırı yöntemlerine karşı alınabilecek farklı önlemler olabilir mi, uluslararası hukukta bu konu ile ilgili yeni çalışmalar yapılarak sorun çözülebilir mi veya sadece bu

alanda güvenliğini sağlamayı amaç edinecek yeni bir uluslararası örgüt mü kurulmalı, sorusu yanıtlanmaya çalışılacaktır.

Tez'in Özgün Yanı

21. Yüzyıl'ın yeni operasyon alanı olarak tabir edilen siber uzay pek çok araştırmaya da konu olmuştur. İnsanlar bu hem avantajlar, akıl almaz gelişmeler hem de tehlikeler ve tehditlerle dolu yeni alanı merak edip incelemeye almış ve bu yeni alan hakkında araştırmalar yapmıştır. Siber uzay konusunda ve siber uzayda güvenliğini sağlama konusunda, bu alandan gelen saldırılar konusunda yazılmış tezler mevcuttur. Ancak çoğu tezde bu alandan gelen saldırılar hem devlet hem birey hem de uluslararası şirketler bazında incelenmiş, bazıları bu saldırıları e-ticaret şirketleri nezdinde bazıları da tek bir ülke bazında o ülke içerisindeki bir şirket / şirketler veya okullar ya da akıllı şehirler bazında incelemiştir.

Bu çalışmada ise, yeni nesil saldırı ve tehdit yöntemleri yalnızca devlet bazında ve devletler tarafından gerçekleştirilen siber saldırıların, uluslararası alanda oluşturduğu güvensizlik kapsamında incelenecektir.

Genel olarak bu konu hakkında yazılmış diğer tezlerde mevcut hukuki yolların, uygulamaların, mevcut yasaların bu yeni nesil tehditlere uygulanabileceği; ancak gerektiği kadar tehlikeleri önlemediğinden bahsedilmiştir.

Bu çalışmayı, bu konuda yazılmış diğer tezlerden ayıran ise, ilgili konuda sadece mevcut uluslararası hukuk kuralları ekseninde değil, siber uzay dediğimiz alanda ortaya çıkan ve çıkabilecek güvenlik eksikliklerinin giderilebilmesi için yeni uluslararası hukuk kuralları mı konulmalı, yoksa sadece siber uzayı hedef alan, sadece bu alanda adaleti, güvenliğini ve barışı sağlamayı amaç edinen bir uluslararası örgüt kurulması gerekir mi, bu mümkün mü, sorularına cevap bulma amacı ile yola çıkılmış olmasıdır.

1.BÖLÜM

Siber Uzayın Tanımı ve Özellikleri

1.1.Bilgisayarların ve İnternetin Gelişimi

İkinci Dünya Savaşı sırasında Almanlar tarafından, Alman birlikleri arasında iletişim ve haberleşmenin kurulması amacıyla geliştirilen Enigma isimli şifreli aygıtın şifrelerinin çözülebilmesi için İngilizler tarafından bir teknik grup kurulmuştur. Daha sonra bu gruba dahil edilen ve o dönem doktora öğrencisi olan Alan Turing isimli genç, Clossus isimli bir cihaz oluşturdu. Bu cihaz çok hızlı bir şekilde şifreli mesajların içerisinden anlamlı olan kelime ve cümleleri ayırt edebiliyor ve tek seferde 25000 sözcüğü tarayabiliyordu. Bugünkü bilgisayarların atası sayılan bu cihaz günümüzdeki bilgisayarların gelişimine de ilham vermiştir (Orak, 2022:215).

1950'lerde gerçek anlamda bilgisayarların hayatımıza girmesi ile teknoloji farklı bir boyut kazandı. İlk kişisel bilgisayarların üretimi 1947 yılında önce transistörün¹ daha sonra da silikon yongaların² keşfedilmesi ile olmuştur. Bilgisayarların kapasitesi artarken ebatları da küçülmeye başlamıştır. Zamanla bilgisayar teknolojisinin, yazılım ve donanımın gelişimi ile bilgisayarlar daha çok gelişmiş ve değişmiş boyutları küçülürken işlemcileri güçlenerek işlevleri artırılmış, dolayısıyla ilk zamanlara kıyasla çok daha rahat taşınabilir bilgisayarlar hayatımıza girmiştir (Ekiz, Vatansever, Zengin ve Demir, 2000:73-81).

Bunun sonucunda 1975'te Altair 8800 ile kişisel bilgisayar terimi ilk kez ortaya çıkmış ve evlerde yerini almaya başlamıştır. Daha sonra ise, IBM 5100 ile kişisel bilgisayar kullanıcılarının sayısı artmıştır (Bıçakçı, 2014: 101-130). Gerçek manada ilk diz üstü bilgisayar ise, IBM (Uluslararası İş Makineleri- International Business Machine) tarafından IBM PC Convertible ismiyle 1986 yılında üretilip piyasaya sunulmuştur (Rahman, Khan ve Zaman, 2024: 821).

¹ Transistör: Küçük bir değerdeki gerilim veya akımla büyük miktarda akımı veya gerilimi kontrol etme amacı ile kullanılan yarı iletken bir devre elemanıdır. Aydınlatma Portalı , Mert Öztoprak , <https://www.aydinlatma.org/transistor-nedir-ne-ise-yarar.html> 20.08.2024

² Silikon Yonga: Yüksek saflıkta silikondan yapılan yarı iletken cihazların malzemesidir. Aydınlatma Portalı , Mert Öztoprak , <https://www.aydinlatma.org/transistor-nedir-ne-ise-yarar.html> 20.08.2024

İnternetin bulunması ise SSCB'nin 1957 de Sputnik isimli ilk yapay uyduyu uzaya göndermesi sonrasında ABD'nin kendisini teknoloji yarışında öne çıkaracak bir adım atmak için, ABD savunma bakanlığı bünyesinde oluşturulan DARPA tarafından savunma sistemleri için geliştirilmesi planlanan bilgisayar, teknoloji ve araştırma vb. projeleri desteklemek amacıyla bir paket anahtarlama sistemi üzerinde çalışmalara başlaması neticesinde olmuştur. Birbirinden bağımsız farklı bilgisayarları birbirine bağlayıp bilgi alışverişinde bulunmalarını sağlayacak bu ağ sistemi daha sonra ARPANET ismini almıştır. İnternetin temelini oluşturan bu sistemde ilk bilgi aktarımı 1960'ların sonlarında olmuştur (Bıçakçı, 2014:104).

ARPANET başlangıçta güvenlik ve askeri amaçlar için geliştirilse de daha sonra devlet kurumları, üniversiteler, okullar, bankalar gibi kamu kurumlarının kullanımına açılmış ardından bireylerin günlük yaşamlarında hızla yerini almıştır. Küba Krizi ile birlikte olası bir nükleer savaş halinde ARPANET'in saldırılardan etkilenmemesi için bazı çalışmalar yapılmıştır. Bu çalışmaların sonucunda ARPANET bünyesinde bulunan birimlerin olası bir nükleer saldırıdan önce ya da sonra birbirleri ile elektrik bağlantısında bulunarak iletişimi devam ettirebilmeleri için yeni bir ağ oluşturulmuştur. Daha sonra bu ağ ilk olarak İngiltere'de bulunan Ulusal Fizik Laboratuvarındaki bir ticari ağa sonra da Fransa'da bulunan bir bilimsel ağa bağlanmıştır. Böylece internetin uluslararası boyuttaki ilk altyapısı oluşturulmuştur (Bıçakçı,2014).

Tüm bu çalışmaların haricinde internetin gelişiminde Tim Berners Lee tarafından geliştirilen World Wide Web bir dönüm noktası olmuş, bilgiye erişim ve bilginin dünya çapında dolaşımı kolaylaşmış, bilgisayar ve bilişim teknolojileri önü alınamaz bir şekilde hayatımızın bir parçası olmuştur. Çünkü Tim Barners Lee World Wide Web ile HTML yani zengin metin işaret dili formundaki içeriklere HTTP hiper metin transfer protokolü yoluyla erişme olanağı sunmuştur (Lee, 1989,1990:1-16). Bu gelişmeler sonrasında insanların bilgiye ulaşması için coğrafi sınırların bir önemi kalmamış, kişiler ya da devlet kurumları tek bir tuşla ya da tek bir internet adresi ile dünyanın öbür ucunda yazılan bir kitaba, bir bilgiye bir videoya erişim imkanı bulmuşlardır.

Birçok bilgisayarın birbirine görünmez ağlarla bağlanarak bilgiye ulaşmayı kolaylaştırması ve dünyanın öbür ucundaki bir bilgisayarı kullanan kişi ya da kişilerle iletişimi mümkün kılması, gittikçe gelişen teknoloji ve siber ağlar sayesinde evimizde otururken banka kartımızla ya da kredi kartımızla marketten alışveriş yapabilme imkanı

bulmamız, telefonumuza indirdiğimiz bir uygulama ile şehir içerisinde arabamızı parkedebileceğimiz uygun bir park yeri bulmamız ya da benzer bir uygulama sayesinde hastaneden randevu alabiliyor olmamız veya üretim süreçlerimizde endüstriyel robotlar sayesinde hızlı, güvenli ve kaliteli üretim imkanını bulabilmemiz internet dediğimiz birbirinden bağımsız ve sınırsız sayıdaki karmaşık ağların geliştirilmesi neticesinde olmuştur.

Siber uzay olarak tabir ettiğimiz bu alan güvenlik açıklarını ve gizlilik ihlallerini de beraberinde getirmiştir. Özellikle devletlerin gizli bilgilerinin yer aldığı bilgisayar ortamlarına bu siber ağlar vasıtası ile sızılması neticesinde devletler açısından hayati öneme sahip bilgilere erişilmesi ve sonu savaşa varabilecek güvenlik ihlallerinin yaşanabilir olması, akıllı şehirlerde veya endüstriyel robotların yoğun olarak bulunduğu üretim süreçlerinde sisteme bulaştırılabilecek bir zararlı yazılım nedeniyle ülkede büyük bir kaos ortamının oluşması muhtemeldir.

1.2.Siber Uzay Kavramının Ortaya Çıkışı ve Siber Uzayın Tanımı ve Özellikleri

Dünya 18. Yüzyıl 'dan günümüze dört büyük endüstriyel devrimden geçmiştir. Bu devrimler küreselleşmeyi hızlandıran teknolojik gelişimleri tetiklemiştir.

İlk endüstriyel devrim endüstri 1.0, 18. yy'da su ve buhar enerjili mekanik üretim tesisleri ile başlamıştır. (dokuma tezgahları). Endüstri 2.0 1870'lerde Cincinnati Mezbahalarında ilk üretim hattı ile başlayan, iş bölümüne dayalı elektrik enerjili kitlesel üretimin devreye alınması ile başlamıştır. Endüstri 3.0 1969'da ilk programlanabilir mantıksal denetleyici ile imalatın otomasyonunu ileri aşamalara götürmeyi başaran elektronik ve bilgi teknolojilerinin hayata geçirilmesi ile başlamıştır. Endüstri 4.0 ise Siber teknolojilerin ve Siber uzayın çağıdır (Kılıç ,2023: 276-291).

İşte bilgisayarların, internetin ve bu teknoloji ile birlikte hayatımıza giren siber uzay kavramının oluşumu endüstri 3.0 ve endüstri 4.0 evreleri sırasında olmuştur. Teknolojinin yıllar içindeki bu hızlı gelişimi, hem bilgisayarların hem de internetin dünya çapında yayılımını hızlandırmıştır.

Özellikle endüstri 4.0 kavramını hayatımıza getiren 21. yy teknolojik gelişmelerin altın çağının yaşandığı dönem olmuştur.

Bu gelişmelerle birlikte bilgisayarların yazılım ve donanımlarının değişmesi, bilgisayarların boyutlarını giderek küçültüp daha rahat taşınabilir hale getirirken kapasitelerini ve işlevlerini artırmış, internet ise, başta askeri amaçlar için kullanılmak üzere çıktığı yolculuğunda tüm dünya için bilgiye ulaşmada vazgeçilmez bir araç haline gelmiştir.

Dünya çapında bilgisayar ve internet kullanımı çok büyük bir hızla artarken ilk olarak 1999 yılında MIT’de çalışan bir İngiliz girişimci olan Kevin Ashton tarafından Protector & Gamble’a yapılan bir sunumda Nesnelerin İnterneti (Internet of Things) kavramından bahsedilmiştir (Çakır, Yiğit ve Küçük, 2019:691-702). Daha sonra 2011 yılında Almanya’da nesnelerin interneti kavramı yeniden ortaya atılmıştır.

Siber Uzay’ın Getirdiği Yenilikler kısmında özellikle üzerinde duracağımız Nesnelerin interneti teknolojisi (IoT), SAP-German Multinational Software Company tarafından *"Fiziksel nesnelerin kolaylıkla bilgi ağlarına bağlanarak bilgi üretmelerini, iş süreçlerine aktif olarak katılmalarını ve katkıda bulunmalarını sağlayan genel ağ sistemi"* olarak tanımlanmıştır.³

İşte tüm bu internete bağlı nesnelerin, bilgisayarların donanım ve ekipmanları, işlemcileri, internet kabloları, fiber optik ağlardan oluşan akıl almaz karmaşıklıkta alan ve dünya çapında bu alanı kullanan kişiler uluslararası ilişkilerde siber uzay kavramını hayatımıza kazandırmıştır.

Siber uzay kavramının ana bileşenlerinden siber terimi bilgisayarlarla ilgili olan dahil olan anlamına gelmektedir ve ilk olarak Norbert Wiener isimli bir matematikçi tarafından 1948 yılında yayınlamış olduğu ve Sibernetik kavramını açıkladığı kitabında kullanılmıştır (Çahmutoğlu, 2020:4).

Sibernetik biliminin kurucusu ise El-Cezeri isimli İslam alimidir. (1136-1206) yılları arasında yaşamış olan bilgin matematik, sibernetik ve robotik alanlarında çalışmalar yapmıştır hatta ilk robotu yapıp çalıştırdığı kabul edilmektedir. Sibernetik bilimi canlılardaki sinir sistemini makinalara/bilgisayarlara uyarlamaya çalışan bilim dalı olarak bilinmektedir (<https://www.robotakademi.org/sibernetik-nedir/> 29.09.2024).

³ Ayrıca benzer bir tabir Çelteç, S. Say, H ve Hacıbeyoğlu, B. nin (2015) yazmış olduğu Nesnelerin internetine doğru: Güncel Konular ve Gelecekteki Eğilimler başlıklı makalede de geçmektedir. ss.640-644 http://openaccess.izmirakademi.org/confpaper/6/2015/103_20.09.2024

Siber uzay kavramı ise ilk olarak William Gibson'un 1982 yılında yayınlamış olduğu Burning Chrome isimli kısa hikayede daha sonra da gene aynı yazar tarafından yayınlanan Neuromancer isimli bilim kurgu kitabında dile getirilmiştir (Bıçakçı,2014:101-130). William Gibson kitabında siber uzayı tanımlarken "*Bilgisayar ağlarının ardındaki gizemli dünya* " tabirini kullanmıştır (Fırat, 2021:1-121).

Bilgisayar, internet ve bu alanda yaşanan hızlı gelişmelerin, çığır açan teknolojik yeniliklerin beraberinde getirdiği bu siber uzay kavramının tanımını yapmak için benzer pek çok fikir ortaya konmuş olsa da bunlar arasında en çok genel kabul gören, siber uzayın tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan sınırsız ve karmaşık ağlardan, fiber optik kablolardan, internete bağlı nesnelerden oluşan ortam olduğu yönündeki tabirdir (Çahmutoglu,2020:4).

Bilgisayarlardan, bilgisayarların donanım ve işletim sistemlerinden, karmaşık internet ağlarından, internet sağlayıcı aygıtlardan, fiber optik kablolardan, internete bağlı olarak çalışan tüm nesnelerden oluşan siber uzay esasen farklı katmanlardan oluşmaktadır.

Bu katmanların ilki Coğrafi katman olarak da tabir edilebilen fiziksel katmandır (Bıçakçı,2014:101-130). Bu katmanda siber uzay dediğimiz alanın fiziksel altyapısını oluşturan kablolar, ağ bağlantıları ve bu ağ bağlantılarının birbirine bağladığı cihazlar bulunur (Şafak,2024:184-201).

İkinci katman, Mantık katmanıdır. Bu katman veri alışverişinin sağlandığı veri akışının yapıldığı katmandır. Burada kişilerin e-mail adresleri, Ip numaraları vb. bilgiler ve bu katmanı kullanarak veri girişini sağlayan kişiler yer alır (Bıçakçı,2014).

Son katman ise, tüm bu katmanların oluşumunu sağlayan insan katmanıdır. Çünkü nihayetinde siber uzay dediğimiz alan insan eliyle oluşturulan bir alandır ve tüm bu teknolojinin işleyişinde insan unsurunun varlığı mecburidir (Bıçakçı,2014).

1.3. Siber Uzayın Getirdiği Yenilikler ve Tehditler

Siber uzayın bir parçası olan bilgisayarlar, karmaşık internet ağları, fiber optik kablolar, akıllı telefonlar ve akıllı cihazlar hayatımıza daha önce benzeri görülmemiş yenilikleri de beraberinde getirmiştir. İş ve işlemlerimizi internet aracılığıyla yapmak, bankada saatlerce beklemek yerine banka uygulaması ile bankacılık işlemlerimizi internet

üzerinden birkaç dakika içerisinde halletmek, acıktığımızda yemeği internetten sipariş etmek ya da ev için mutfak vb. tüm alışverişi internet mağazalarından online yapabilmek, bilgiye erişimin akıl almaz bir şekilde kolaylaşması neticesinde tek tuşla binlerce kilometre ötedeki yerler, insanlar hakkında bilgi edinebilmek, uzaktan online eğitimler aracılığıyla yeni bir meslek edinebilmek, hibrit çalışma imkanı ile işini evden online yapmak, hatta Google meet, Zoom uygulamaları gibi uygulamalar sayesinde internette, online ortamda toplantılar gerçekleştirebilmek bu yeniliklerden sadece birkaç tanesidir.

Akıllı ev aletleri, tabletler, akıllı telefonlar ve akıllı robotlar bireylerin evdeki ihtiyaçlarını giderip işlerini kolaylaştırırken akıllı trenler, metrolar, havaalanlarında kullanılan akıllı sistemler ve tüm bunları içerisinde barındıran akıllı şehirler, e-devlet sistemleri gibi devlet ve kamu dairelerindeki işlemleri kolaylaştıran sistemler, devletlere vatandaşlarına konfor ve kolaylık sağlama konusunda inanılmaz imkanlar sunmuştur.

Bu şekilde devlet dairelerinin yükü azalırken zamandan tasarruf imkanı da sağlanmıştır. Sadece bunlar da değil barajlar, nükleer santraller vb. devasa yapıların ve sistemlerin kontrollerinin bilgisayarlar ve internet aracılığıyla yapılabilmesi, savunma sanayiinde yeni nesil olarak tabir edilen insansız hava araçları, dron vb. kameralı keşif cihazları, yeni nesil silah sistemleri devletlere güç ve caydırıcılık açısından avantajlar sağlamıştır.

Ancak tüm bu pozitif yönlerinin yanında siber uzayın getirdiği tehlikeler de yadsınamayacak kadar büyüktür hatta devletler açısından bu tehlikenin boyutları daha derin ve daha fazladır. Çünkü devletler varlığını sürdürebilmek adına bu yeni alanda var olmak, teknolojik gelişmişliğini artırmak durumundadır. Ancak teknolojik gelişmişliğini artırırken eş zamanlı olarak bu yeni sistemleri olası saldırılardan korumak için savunma gücünü de aynı ölçüde geliştirmek zorundadır.

Çünkü artık tehdit ve saldırı sadece konvansiyonel sistemlerle, silahlarla tanklarla, uçaklarla değil yazılım teknolojisi tarafından geliştirilen bir virüs, bir trojan veya bir worm (solucan) vasıtasıyla da yapılabilmekte ve tıpkı konvansiyonel silahlarla verilen zarar kadar hatta belki daha fazla zarar oluşturabilmektedir.

Devletin bankacılık sistemlerine bulaştırılabilecek zararlı bir yazılım milyarlarca dolarlık ekonomik zararlara sebep olabilir, akıllı trenlerin, metro istasyonlarının, havaalanlarının işletim ve kontrol sistemlerine yapılacak bir siber saldırı sistemlerin çalışma şeklini bozup ölümle sonuçlanan kazalara neden olabilir, barajlar, nükleer santraller, doğalgaz boru hatları, altyapı sistemleri gibi kritik öneme sahip sistemlerin işleyişi yanlış bir yazılım yüklenmesi ya da siber saldırı yoluyla virüs bulaştırılması neticesinde devreden çıkarılarak devletlere altından kalkamayacakları zararlar verilebilir.

İşte tüm bu tehlikelerden dolayı devletler bir yandan teknolojik açıdan gelişirken bir yandan da bu gelişmenin neticesinde varlıklarını sürdürebilmek için bu yeni nesil tehdit türlerine karşı yeterli ve etkin savunmayı geliştirmek mecburiyetindedir. Çünkü bu yeni nesil tehditler devletlerin eskiden beri süregelen güvenlik ve tehdit algılarını tamamıyla değiştirmiştir.

Bu nedenle siber uzay "NATO tarafından 2016 yılında gerçekleştirilen Varşova zirvesinde tıpkı kara, hava, deniz ve uzay gibi bir hareket sahası olarak tanımlanmıştır" (Polat,2020:149).

Üstelik bilgisayarların, internetin ve neticede tüm bunları kapsayan siber uzay kavramının hayatımıza getirdiği farklı yeni kavramlar, teknolojiler ve korunması gereken yeni alanlar da ortaya çıkmıştır. Bunlardan devletler tarafından en çok kullanılanlar Nesnelerin interneti, yapay zeka ve bunlar aracılığıyla geliştirilen endüstriyel robotlar ve akıllı şehir uygulamalarıdır.

1.3.1. Nesnelerin İnterneti

Bilgisayarların icadı, internetin bulunması ve en nihayetinde siber uzay dediğimiz insan yapımı alanın hayatımıza kattığı yeniliklerden biri de Nesnelerin interneti kavramıdır.

İlk olarak 1999 yılında MIT’ de çalışan bir ingiliz girişimci olan Kevin Ashton tarafından Protector & Gamble’a yapılan bir sunumda bu kavramdan bahsedilmiştir (Çakır, Yiğit ve Küçük, 2019:691-702). Ashton kavramı “*fiziksel dünyadaki nesnelerin sensörler aracılığıyla internete bağlanabileceği bir sistem*” olarak tarif etmiştir (<https://www.internetsociety.org/> 2015:1-53).

Nesnelerin interneti kavramının daha sonra da pek çok tanımı yapılmıştır. Ancak bunlardan en çok tercih edileni belki de “Fiziksel ve sanal özelliklere sahip nesnelerin,

bilgi ağlarına kolaylıkla bağlanarak akıllı içerikler üretmesini sağlayan teknoloji” ifadesidir (Çakır, Yiğit ve Küçük, 2019).

Bu yeni teknoloji ile ilgili resmi tanım ise İstanbul Teknik Üniversitesi tarafından “*Her yerden, Her zaman ve Herşey için Bağlanabilirlik*” şeklinde yapılmıştır (Çakır, Yiğit ve Küçük, 2019).

Nesnelerin interneti yani Internet of Thins (IoT) nesnelere internet bağlantısı aracılığıyla kazandırılan verileri algılama ve bu verileri işleme yeteneğidir. Nesnelere kazandırılan bu yetenek sayesinde nesneler hem çevredeki değişiklikleri anlayabilir hem de bu değişikliklere hızlı yanıt verebilir hale gelmiştir (Chui, Löffler ve Roberts, 2010:1-10). Örneğin Japonya’da yol kenarlarında bulunan reklam panoları yoldan geçenlerin profillerini tüketici profilleri ile karşılaştırarak değerlendirme yapabilmekte ve bu değerlendirme neticesinde panodaki reklamı değiştirebilmektedir (Chui, Löffler ve Roberts, 2010).

Nesnelerin interneti teknolojisi her zaman, her yerden her şeyin birbirine bağlanarak bilgi üretebilmesi ile bilgi ve iletişimde yeni bir boyutun açılmasını sağlamıştır (Koçak, Alan, Kabadayı, Tümer. ve Cavdar, 2018: 294-320). Bu konuda ilk amatör çalışma İngiltere’de yapılmıştır. 1991 yılında İngiltere’de Cambridge Üniversitesi çalışanları üst katta bulunan kahve makinasının dolu mu, boş mu olduğunu anlamak amacıyla bir yazılım geliştirmişler ve kahve makinasına bu yazılımı entegre ederek makinanın dolu olduğunda aşağı kata sinyal göndermesini sağlamışlardır (Görkem ve Bozuklu, 2016: 47-68).

Böylece akıllı cihaz ya da nesnelerin interneti uygulamasının temelleri daha kavram ortaya atılmadan önce yapılmıştır. Günümüzde giyilebilir cihazlar, evlerde kullanılan akıllı cihazlar, artık gittikçe sayısı artan akıllı şehir uygulamaları gibi pek çok nesnelerin interneti uygulaması mevcuttur. Üstelik bu teknolojinin uygulama alanları ve bu teknoloji ile çalışan cihaz sayısı her geçen gün artmaktadır.

Nesnelerin interneti teknolojisinin devletler tarafından en çok kullanıldığı alanlar ise, savunma sanayisi ve akıllı şehir uygulamaları, hastanelerde tanı ve tedavi amaçlı kullanılan robotlar ve fabrikalarda kullanılan endüstriyel robotlardır. Bu cihazlar aynı

zamanda daha sonraki bölümde bahsedeceğimiz yapay zeka ile geliştirilen ve internet bağlantısı sağlanarak veri işleme kabiliyeti kazandırılan akıllı cihazlardır.

Günümüzde devletler askeri kabiliyetlerini artırmak, güç ve caydırıcılık elde etmek amacıyla envanterlerine akıllı sistemlerle donatılmış füzeler, insansız hava araçları vb. cihazlar eklemektedirler. İlerleyen bölümde de ayrıntılı olarak değineceğimiz Akıllı şehir uygulamaları ise, artık tüm devletler tarafından vatandaşlarının günlük hayatlarını kolaylaştırmak, şehir içerisindeki işleyişi, trafik akışını kontrol etmek, şehrin altyapı sistemlerinin işleyişini kontrol altında tutmak vb. nedenlerle pek çok şehirde uygulanmaya başlamıştır.

Bir sonraki bölümde daha ayrıntılı bir şekilde üzerinde duracağımız endüstriyel robotlar, fabrikalarda üretimin hızını ve kalitesini artırırken, hastanelerde tanı ve tedavi amaçlı kullanılan robotlar hastalıkların tanı sürelerini azaltarak hastaların yaşam sürelerini ve hayat kalitelerini artırmaktadır.

Ancak tüm bu teknoloji sağladığı kolaylıkların yanında siber saldırıya uğrama riskini de beraberinde getirmektedir. Çünkü internete bağlı olarak çalışan her cihaz internet ve bilgisayar aracılığıyla yapılan siber saldırılara da açık olacaktır. Üstelik devletler için sürekli gelişen bu teknolojiye ayak uydurmamak gibi bir tercih de yoktur ve artık bu yeni teknolojiler geri döndürülemez bir biçimde ve büyük bir hızla ilerlemeye devam etmektedir.

Bu nedenle içinde bulunduğumuz bu yeni çağ özellikle devletler açısından gerisinde durulacak bir çağ değildir (Kuvancı ve Akın, 2020: ss.24-45). Devletlerin, sahip oldukları teknolojik gelişmişlik ölçüsünde bu cihazları, akıllı şehir uygulamalarını, savunma ve saldırı sistemlerini ve internete bağlı çalışan, veri analizi yapan, bilgi üreten her cihazı (devlet bazında) siber saldırılardan koruma yetkinliğine de sahip olmaları eşit ölçüde zorunludur. Üstelik bu alanda çoğu zaman savunmak, saldırmaktan daha pahalıya mal olacağı için devletin ekonomik açıdan da oldukça gelişmiş olması gerekmektedir.

Ayrıca nesnelerin interneti teknolojisine bağlı olarak çalışan cihazların siber saldırıya uğraması durumunda bu cihazların geri dönülemez bir biçimde hasar görmesi, işletim sistemlerinin bozulması durumu söz konusu olacağından bu da devletler için ek bir

maliyet ve fiziki hasar ortaya çıkaracaktır. Uluslararası hukukta bu tür bir mağduriyetin karşılığı elbette olacaktır. Fakat bunun ne şekilde ve ne kadar sürede olacağı sorusu cevabının araştırılması gereken bir sorudur.

1.3.2. Yapay Zeka

Beynin yapısı ve zeka kavramı çok eski zamanlardan beri insanlar için hep cezbedici olmuş ve insanlar her zaman insan beynine benzer ve onun gibi çalışan cihazlar geliştirmek için uğraşmışlardır. Bakıldığı zaman bugüne kadar yapılmış çoğu icadın ardındaki sebebin insan beyninin yapısına ve çalışma şekline duyulan bu meraktan kaynaklandığı görülmektedir (Öztemel, 2020 : 75-91).

İnsan beyninin yapısına ve işleyişine karşı duyulan bu merak bilgisayarların ve internetin ve tüm bu cihazları birbirine bağlayan karmaşık ağ yapısının oluşturduğu siber uzay dediğimiz kavramın ortaya çıkmasına neden olmuştur.

Yapay zekâ ise nesnelerin interneti gibi siber uzay kavramı ile hayatımıza giren bir diğer kavramdır. Esasında yapay zeka ile ilgili çalışmalar ilk olarak 1936 yılında Alan Turing tarafından başlatılmıştır. Turing 1936 yılında yazdığı ve Türkçe isimleri ile “Hesaplanabilir Sayılar Üzerine ” ve 1950 yılında yazdığı “Bir makine düşünebilir mi?” olarak bilinen makaleleri ile bu alandaki ilk çalışmaları yapmıştır.

Ancak Alan Turing’in yapay zeka konusundaki en önemli katkısı 1950 yılında ortaya attığı Turing Testi ile olmuştur (Tugay ve Tugay, 2019: 376-384). Bu test bir kişinin, bir bilgisayar veya başka biri ile bir teletip aracılığıyla iletişim kurması üzerine kurgulanmıştır. Buna göre, eğer kişi iletişim kurduğu kişinin bilgisayar olduğunu farkedemezse bilgisayarların insan gibi düşünebildiği ve cevap verebildiği kabul edilecekti (Tugay ve Tugay, 2019).

Yapay zekanın bir terim olarak ilk kez ifade edilmesi ise 1956 yılında Dartmouth Kolejinde yapılan Dartmouth Konferansına dayanır. Yapay zeka üzerine Dartmouth Yaz Araştırma Projesi için bir teklif (A proposal for the Dartmouth Summer Research Project on Artificial Intelligence) isimli konferansın baş konuşmacılarından John McCarthy konuşmasının başlangıcında “*Bu konferans yalnızca geçmişi onurlandırmakla ve mevcut başarıları değerlendirmekle kalmayıp aynı zamanda gelecekteki yapay zeka*

arařtırmaları için fikir üretmeye de yardımcı oldu” ifadesini kullanmıř ve ardından “Bir makinenin insan beyninin düşünme işlevini ve zekanın işleyişini simüle edebileceğini düşünmek” şeklinde bir ifade kullanmıřtır (McCarthy, Minsky, Rochester ve Shannon, 1956).

Ardından 1962 yılında John McCarthy’nin desteęiyle IBM tarafından ilk kez satranç oynayan bilgisayar yazılımı üretildi (Güllü, 2022: 19-30). 1987 yılında bilim olarak kabul edilen yapay zeka’nın tanımı ise “insan tarafından yapıldığında zeki olarak adlandırılan davranışların makine tarafından yapılmasıdır” şeklinde ifade edilmiştir (Prim, 2006: 81-93). Bir dięer anlamda yapay zeka düşünme, anlama, faaliyete geçirmeyi sağlayacak bilgi işleme çalışmasının bilgisayarlar ya da akıllı cihazlar tarafından yerine getirilmesidir (Prim, 2006:81-93).

“Yapay zekâ, bilimsel bir ifade ile tanımlanırsa; tecrübelerden öğrenebilen, öğrendiklerini muhakeme edebilen, şekilleri, görüntü ve örüntüleri tanıyabilen, karmařık problemlere çözümler üretebilen, lisanı anlayarak kelimeler ile işlem yapabilen ve biliřim dünyasına farklı bir bakıř açısı kazandıran bir bilim dalıdır denilebilir” (Öztemel, 2020 :75-91).

Bu açıdan bakıldığında hayatımızda kullandığımız pek çok cihazın yapay zeka sayesinde düşünme, anlama ve faaliyete geçirme becerisi kazanarak hayatımızı kolaylaştırması oldukça cezbedicidir. Özellikle işten eve gelmeden yapay zeka ile üretilmiş temizlik robotları sayesinde evimizi telefonumuzda kullandığımız bir uygulama ile uzaktan temizleme imkanı bulabilmemiz, evin ısısını, sıcaklığını veya serinliğini daha eve gelmeden ayarlayabilmemiz, yapay zeka ile üretilmiş buzdolabımızın telefonumuza göndereceęi bir mesaj ile dolaptaki eksikleri bildirmesi neticesinde zamandan tasarruf etme imkanımızın olması ve daha akla gelebilecek pek çok kolaylık yapay zeka uygulamalarının hayatımıza kattığı artılardır.

Ancak günümüzde yapay zeka uygulamaları bireylerden daha çok devletler tarafından kullanılmaktadır. Yoęun bir şekilde savunma ve askeri sistemlerde kullanılmasının dışında özellikle şehirlerde kritik altyapı sistemlerinin kontrolünde, kamusal alanda, fabrikalarda, havaalanlarında, bankalarda, hastanelerde kısacası hayatın her alanında yapay zeka teknolojisi ile donatılmış bilgisayarlar, cihazlar, robotlar günlük hayatın

işleyişini kolaylaştırmak ve kamunun iş yükünü azaltmak amacıyla yoğun olarak kullanılmaktadır.

İlk bakışta devletin teknolojik gelişmişliğinin ve konfor düzeyinin göstergesi olan bu sistemler internete bağlı olarak çalışmaları nedeniyle siber saldırılara da açık olduğundan gerektiği gibi korunmadığı takdirde çok tehlikeli hale gelebilir ve bu sistemlere yapılacak bir siber saldırı; zararlı bir yazılım yüklenmesi veya DoS ve DDoS atakları aracılığıyla çalışamaz hale getirilmeleri çok ciddi kazaların, kayıpların yaşanmasına neden olabilir.

Üstelik oluşacak milyarlarca dolarlık ekonomik hasar bu zararın yalnızca başlangıcı niteliğinde olacaktır ki; yalnızca meydana gelen ekonomik zarar bile saldırı fiilinin işlendiğine kanıt niteliğindedir.

Bunun dışında hava kontrol sistemlerine yapılacak bir siber saldırı kontrol sisteminin bozulmasına, devreden çıkmasına ve hava trafiğinin düzenlenemez hale gelmesi neticesinde kazaların yaşanmasına neden olabileceği gibi aynı sorun şehir içerisindeki trafik kontrol sistemleri için de geçerlidir. Hastanelerde, hastalıkların tanı ve tedavisinde kullanılan yapay zeka temelli cihazların benzer bir saldırıya maruz kalması durumunda hastalıklara yanlış tanı konulması ya da gerekli tedavinin yapılamaması gibi hayati sonuçlar doğurabilecek hatalar meydana gelebilir.

Bu nedenle yapay zeka uygulamalarının yüksek siber güvenlik sistemleri ile korunması, bu sistemlerin günlük hayatta kullanılması kadar hayatidir. Fakat bu tür yüksek maliyetli sistemlere yönelik tehditler karşısında devletlerin Uluslararası hukuk nezdinde korunması konusu da ayrıca önem arz etmektedir.

1.3.3. Endüstriyel Robotlar

Siber uzay kavramını hayatımıza katan Endüstri 3.0 ve Endüstri 4.0 devrimleri olmuştur. Özellikle Endüstri 4.0 Almanya'da 2011 yılında düzenlenen Hannover Sanayi Fuarı'nda duyurulduktan sonra başdöndürücü bir şekilde hayatımızı ve dünyayı yeniden şekillendirerek teknolojiyi, bilgisayarları, interneti ve internet teknolojisi ile birlikte gelen siber uzay kavramını hayatımızın merkezine koymuştur (Gönen, Yılmaz, Şanoğlu, Karacayılmaz ve Özbirinci, 2021: 1142-1158).

Siber uzay kavramı ise hayatımıza nesnelerin interneti ve yapay zeka teknolojilerini getirmiştir. Nesnelerin interneti ve yapay zeka teknolojileri de bugün dünyanın neredeyse her yerinde fabrikalarda, endüstride, üretim süreçlerinin belkemiğini oluşturan endüstriyel robot teknolojisinin ortaya çıkmasını sağlamıştır.

Endüstriyel robotlar bugün tüm dünyada otomotiv sektörü, havacılık, savunma sanayi, sağlık vb. sektörlerde ve endüstriyel üretim süreçlerinde tekrarlayan iş süreçlerinin daha seri yapılması, üretim süreçlerinin daha verimli ve kaliteli hale getirilmesi, savunma sanayiinde ülkenin savunma kapasitesinin artırılması gibi amaçlarla ve sağlık sektöründe tanı ve tedavi yöntemlerinin geliştirilmesi gibi amaçlarla kullanılmaktadır (Uçan, Karacığan ve Eskicumalı, 2022:1-260).

Özellikle artan işçilik maliyetlerini düşüren endüstriyel robotlar, her türlü üretim faaliyetini standart bir operatörden daha hızlı gerçekleştirebilmektedir (Dilibal ve Şahin, 2018 :86-95). Ayrıca üretim sektörünün rekabet ortamında özellikle vazgeçilmez olan iki unsur, kaliteli ve ucuza imalat yapmaktır. Endüstride kullanılan robotlar işte tam da bu ihtiyacı karşılamak için yoğun bir şekilde kullanılmaktadır (Çengelci ve Çimen, 2005: 69-78).

Endüstriyel robotların kullanımının yaygınlaşmasının nedenlerinden bir diğeri de insanlar için tehlikeli olabilecek işlerin bu robotlar tarafından daha kolay ve hasarsız bir şekilde yapılmasıdır (Uçan, Karacığan ve Eskicumalı, 2022).

Robotlar, mekanik yapılardan, sensörlerden, aktüatörlerin ve bu cihazları yöneten ve kontrol eden bilgisayar yazılımlarının bir kombinasyonundan oluşurlar (Morantes, Victores ve Balaguer, 2015:1-4). Bu cihazlar, Nesnelerin İnterneti (IoT) teknolojisinin bu tür cihazlarda kullanılması amacıyla geliştirilen Endüstriyel Nesnelerin İnterneti (IIoT) uygulamaları ile çalışmaktadır. Bu sayede endüstriyel robotlar ağ üzerinden birbirleri ile otomatik iletişim kurarak üretimi kontrol etmekte ve operatör katkısını en az düzeye indirmektedir (Gönen, Yılmaz, Şanoğlu, Karacayılmaz ve Özbirinci, 2021).

Robotların kontrolü ve yönlendirilmesi süreçlerinde ise SCADA sistemlerine benzer şekilde PLC (Programlanabilir Mantık Kontrol Ünitesi) adı verilen bilgisayar benzeri sistemler ve PIC⁴ veya üretici firmaların kendilerine ait robotları kontrol etmek amacıyla imal ettikleri kontrol üniteleri kullanılmaktadır.

⁴ Peripheral Interface Controller (çevresel ünite denetleme arabirimi) giriş - çıkış (input - output I/O) işlemlerini çok hızlı gerçekleştirebilecek şekilde tasarlanmış bir chip 'tir. http://www.robotiksistem.com/pic_mikrodenetleyiciler.html 15.11.2024

PLC' ler sinyal giriş - çıkışlarının sınırlı olmasından dolayı basit yapıli robotlarda kullanılabilirler ama karmaşık yapıli robotlarda PLC' ler yeterli gelmediğı için robot üreten firmalar kendi kontrol ünitelerini de beraberinde üretmektedir (Çengelci ve Çimen, 2005: 69-78).

Ayrıca Robot üreten her firma, bu robotların gerçekleştireceğı iş ve işlemlerin belirlendiğı bir arayüz programını da geliştirir. Bu arayüz programı sayesinde robotun işlevleri programlanır ve robota yüklenir. Robotun hızı, çalışma şekli vb. işlemler de gene bu arayüz aracılığıyla kontrol edilir (Çengelci ve Çimen, 2005: 69-78).

Endüstriyel robotlar bugün dünyanın her yerinde, özellikle de gelişmiş ülkelerde endüstriyel üretimde hızı ve verimliliğı artırmak amacıyla yoğun bir şekilde kullanılmaktadır. Hatta imalat sanayiinde en çok robotun kullanıldığı dört ülkenin sırasıyla Japonya, G. Kore, Almanya ve ABD olduğu belirtilmiştir (Yılmaz, 2018: 109-120). Bunun dışında Endüstriyel robotların en yoğun kullanıldığı ülkeler Avrupa Birliğı üyesi ülkeler arasında yer almaktadır (Fırat ve Fırat, 2017:211-223).

Bu robotlar endüstriyel üretimin daha seri, daha pratik ve daha az maliyetle gerçekleştirilmesini ve daha kaliteli ürünler ortaya çıkmasını sağlasa da siber uzay ile etkileşim içerisinde olan ve birbiriyle bağlantılı olan cihaz sayısı arttıkça siber saldırı riski de aynı ölçüde artmaktadır (Gönen, Yılmaz, Şanoğlu, Karacayılmaz ve Özbirinci, 2021). Çünkü dijitalleşme ile birlikte üretimin siber-fiziksel sistemlerle yürütölmeye başlaması, üretim süreçlerinde pek çok yeniliğın ve fırsatın kapılarını açarken siber saldırılara da bir o kadar ortam hazırlamıştır (Güdek, 2023: 1129–1142).

Bu cihazların kontrol ya da programlama sistemlerine yapılacak olası bir siber saldırı ya da yetkisiz bir erişimin yanlış komutu neticesinde cihazın başta programlandığı görevin dışında ya da tamamen aksi yönde hareket etmesi veya kontrolden çıkması etraftaki insanların yaralanmasına ve hatta ölmesine neden olabilecek çok ciddi kazaların meydana gelmesine neden olabilir (Uçan, Karacığın ve Eskicumalı, 2022). Çünkü robotların hareket etmelerini, nesneleri kavramalarını ve kaldırmalarını sağlayan tutucular, motorlar ve dişliler bir siber saldırı olması durumunda kötüye kullanılarak çok ciddi zararlara ve can kayıplarına sebep olabilirler (Bhardwaj, Goundar ve Avasthi, 2019: 13-19).

Örneğın bir Endüstriyel robot tarafından ilk cinayet, 1981 yılında Japonya'da Kawasaki fabrikasında yapay zekâ ile kontrol edilen bir robot tarafından işlenmiştir. Robotu yöneten

yapay zekâ, hatalı bir şekilde bir çalışanı üretim engeli olarak algıladığı için onu yok etmesi gerektiğini düşünüp devasa kollarıyla çalışanı tutup yakınındaki öğütme makinesine atmıştır (Özkan, 2019:65).

Gene 2015 yılının Mayıs ayında Cincinnati'de bir araba fabrikasında robotik platforma kötü amaçlı yazılım bulaşması neticesinde, montaj robotlarındaki römork yükleme komut dizisinin bozulması sebebiyle sistem beklenmedik bir şekilde yeniden başlatılmış bu da bir işçinin kafatasının ezilmesi sonucunda ölmesine neden olmuştur (Bhardwaj, Goundar ve Avasthi, 2019).

Hindistan'da 2015 yılının Ağustos ayında Maruser'de bulunan Maruty fabrikasında Endüstriyel robotun kablolarının yetkisiz kişiler tarafından kurcalanması neticesinde, montaj hattındaki robotik kol bir işçiyi yakalayarak ölümüne neden olmuştur (Bhardwaj, Goundar ve Avasthi, 2019).

Bir diğer ölümlü kaza da 2016 yılının Nisan ayında ABD askeri üssünde meydana gelmiştir. Sisteme bulaştırılan kötü amaçlı yazılım sonucunda robotik sistem arızalanmış bu da robot havan topunun çalışma düzeneğinin bozulmasına neden olmuştur. Neticede dokuz ABD askeri eğitim tatbikatı sırasında havan topunun yanlış ateşlenmesi sonucu ölmüştür (Bhardwaj, Goundar ve Avasthi, 2019).

Bu kazaların yaşanmasına sebep olan siber saldırılar bir devlet tarafından gerçekleştirilmemiş olsa da bu sistemlerin siber saldırılara karşı zafiyetini göstermeleri ve bu cihazların gerektiği gibi çalışmamları durumunda ortaya çıkacak potansiyel tehlikeyi ortaya koymaları açısından oldukça önemlidir.

Görüldüğü üzere bünyesinde pek çok avantajı ve yeniliği barındıran bu sistemler aynı zamanda çok ciddi potansiyel tehditleri de içermektedir. Daha önce de belirttiğimiz gibi internete bağlı olarak çalışan ve bir şekilde bilgisayarlar tarafından yönlendirilen ve birbirleri ile BIT aracılığı ile bağlantılı olan her cihaz ya da sistem siber saldırılara karşı büyük ölçüde savunmasızdır. Çok yıkıcı sonuçları olabilecek böyle bir saldırı, bu tür cihazların siber saldırılar yoluyla kontrol edilerek rakip olarak görülen ya da düşman olarak belirlenen devlete ciddi zararlar vermek için kullanabilecek olmaları bakımından caydırıcı bir güç olarak devletlerin oldukça dikkatini çekmektedir.

Bu ciddi tehdit karşısında ülkelerin kendi içlerinde bu robotların siber saldırılardan korunması konusunda almaları gereken güvenlik önlemleri dışında Uluslararası hukuk çerçevesinde bu tür yıkıcı saldırıların meydana gelmesi durumunda hangi önlemler alınıyor ve daha fazla ne yapılabilir sorularının cevabı tartışılmalıdır.

1.3.4.Akıllı Şehirler

Dünya hızla teknolojik ilerleme ve dijitalleşme süreçlerini yaşarken, şehirlerde yaşayan nüfus oranı da tıpkı baş döndürücü teknolojik gelişmeler gibi hızla artmaktadır. Öyle ki, BM tarafından 2018 yılında yayınlanmış olan verilerde dünya nüfusunun yarısından fazlasının şehirlerde yaşadığı belirtilmiş ve 2030 yılına kadar bu rakamın %60'ların üzerine çıkabileceği söylenmiştir (Özcan, Yıldırım, 2023: 295-310). 2050'ye kadar ise bu oranın %70' lere çıkacağı tahmin edilmektedir (Varshney, Khan, Khan ve Verma , 2021: 1-11).

Şehirlerdeki bu hızlı nüfus artışı, kentsel altyapıların kullanımında, kaynak tüketiminde ve hizmet taleplerinde artışı da beraberinde getirecektir. Bu da kentlerin dönüştürülmesinde ve bu yeni duruma hazır hale getirilmelerinde bilgi teknolojileri gibi üst nesil teknolojilerin kullanılmasını zorunlu hale getirmektedir (Tozkoparan, 2019: 417-427).

İşte burada Akıllı şehir kavramı karşımıza çıkmaktadır. Akıllı şehir kavramı da tıpkı nesnelerin interneti, yapay zeka ve endüstriyel robot teknolojileri gibi siber uzay kavramı ile hayatımıza giren kavramlardan biridir.

Akıllı şehirler, bilgi ve iletişim teknolojilerinin, mevcut ve gelecek nesiller için ekonomik, sosyal, çevresel şartların sürdürülebilir hale getirildiği, yaşam kalitesinin artırıldığı, kentsel hizmetlerin ve altyapı hizmetlerinin verimliliğinin artırıldığı şehirler oluşturmak amacıyla kullanıldığı şehirlerdir (Özcan, Yıldırım, 2023: 295-310). Teknoloji ve kentsel süreçlerin birlikteliğini kapsayan bu sistemde amaç şehrin içerisindeki toplu taşıma sistemleri, hastaneler, işletmeler, ticaret, enerji üretimi, su tedarik ağları, atık sistemleri gibi tüm bileşenlerde, nesnelerin interneti ve yapay zeka teknolojileri kullanılarak şehirde yaşayan halkın refah düzeyini artırmak ve mevcut kaynakların sürdürülebilirliğini sağlamaktır (Düger, 2023: 1-15).

Akıllı güvenlik ve izleme sistemleri, risk yönetimi ve afet sistemleri, akıllı belediyeçilik hizmetleri, akıllı ulaşım sistemleri, akıllı hastane randevu ve sağlık sistemleri, akıllı

altyapı sistemleri akıllı şehirlerin bileşenlerinden sadece birkaç tanesidir (Özcan, Yıldırım, 2023 : 295-310). Ancak online bankacılık sistemleri, online eğitim ve online alışveriş hizmetleri de akıllı şehirlerin önemli bileşenleridir (Tozkoparan, 2019: 417-427).

Akıllı şehirlerin oluşum süreçlerinde akıllı telefon uygulamaları, açık data ve türkçeye makineden makineye olarak çevirilebilecek M2M (machine to machine) uygulamaları çok önemli bir yere sahiptir (Cerrudo, 2015:1-22).

Mobil uygulamalar, akıllı şehirler içerisinde vatandaşların bu uygulamalar sayesinde şehirle olan aktivasyonunu ve şehirdeki aktif katılımını artırırken, açık data uygulamaları ise hükümetler tarafından paylaşılan ve vatandaşları da aktif katılıma ve uygulama geliştirmeye teşvik eden uygulamalardır.

M2M olarak bilinen uygulamalar ise akıllı şehirlerin oluşumunda olmazsa olmaz olan akıllı cihazların birbirleri ile etkileşim ve iletişim halinde olmalarını sağlayan teknolojidir (Cerrudo, 2015). Bu teknolojiye makineler ve cihazlar herhangi bir insan müdahalesi olmadan birbirleri ile bilgi ve veri paylaşımında bulunarak eş zamanlı olarak çalışabilmektedir (<https://multitech.com/iot-wiki/machine-to-machine-m2m/> 25.11.2024).

Makineler arasında yapılan bu bilgi paylaşımı Kablosuz Sensör Ağları (WSN-Wireless Sensor Network) aracılığıyla gerçekleşmektedir. WSN (Kablosuz Sensör Ağları) küçük cihazlar, sensörler, baz istasyonları ve veri iletim sistemlerinden oluşan ağlardır ve şehir içerisinde daha çok akıllı ulaşım sistemlerinin desteklenmesi amacıyla kullanılmaktadır (Alshambri, Al Zain, Soh, Masud ve Al-Amri, 2020: 579-584).

AUS (Akıllı ulaşım sistemleri) olarak bilinen bu sistemde, bilgi ve iletişim teknolojileri, şehir içerisindeki ulaşımın kolaylaştırılması ve geliştirilmesi için ulaşım sistemlerine entegre edilmektedir. Bu sistemler tramvaylar, otobüsler, deniz taşımacılığı, trafik akış ve kontrol sistemleri, metrolar, havayolları gibi şehir içerisinde ulaşım ile ilgili tüm alanları kapsamaktadır (Avcı, 2023: 194-208).

Daha çok megakentlerde, şehirde yaşanan yoğun trafik akışını düzene sokmak, akıllı trafik lambaları aracılığıyla trafiğin, hem araç sürücüleri hem de yayalar açısından düzenli ve güvenli bir şekilde akışını sağlamak, metrolar ve tramvay hatları aracılığıyla ya da deniz taşımacılığı yoluyla şehir sakinlerinin ulaşım sorunlarını en aza indirmek,

havayoluyla seyahat edecek kişiler için süreçlerin kolaylaştırılması ve hava trafiğinin daha hızlı ve düzgün bir şekilde işlemesi gibi kolaylıklar sağlamaktadır.

Akıllı hastane randevu ve sağlık sistemleri, akıllı altyapı sistemleri ve afet yönetim sistemleri de akıllı şehirlerde, şehrin işleyişini düzenleyen ve şehirde yaşayanların hayatını kolaylaştıran diğer önemli akıllı sistemlerdir.

Tüm bu akıllı sistemler düzgün ve sorunsuz çalıştıkları takdirde, şehir içerisinde ulaşım sistemlerinin aksamadan çalışması, sağlık sistemlerine erişim ve tedavi süreçlerinin kolaylaştırılması, şehirdeki atıkların geri dönüşümü ve altyapı sistemlerinin düzgün bir şekilde işlemesi akıllı şehirlerin en büyük avantajları haline gelmektedir. Ancak bu sistemlerin birbirlerine bağlı olarak ve kablosuz ağlar aracılığıyla haberleşerek çalışması sisteme bulaştırılacak zararlı bir yazılımın ya da büyük çaplı bir DoS/DDos saldırısının tüm bu birbiriyle bağlantılı sistemleri felç edebileceği anlamına da gelmektedir.

Örneğin akıllı ulaşım sistemlerinde meydana gelebilecek bir aksama ya da akıllı trafik kontrol sistemlerinin gerektiği gibi çalışmaması trafiğin akışının bozulmasına ve kaos oluşmasına bununla birlikte ölümlü kazaların da yaşanmasına neden olabilir. Ya da havayolu sistemlerinde sisteme bulaşan bir virüs, büyük bir kaos ve karmaşa ortamının yaşanmasına neden olabileceği gibi hava trafik kontrol sistemlerinde virüs vb. zararlı bir yazılım nedeniyle oluşabilecek bir sorun da çok ciddi ekonomik ve fiziksel kayıpların yaşanmasına hatta yüzlerce kişinin ölümüne neden olabilir.

Üstelik tüm bu sistemlerin birbirleriyle bağlantılı olarak çalıştığı düşünüldüğünde tek bir sisteme bulaşan bir virüsün hızla yayılarak diğer akıllı sistemleri de etkisi altına alıp şehirdeki akıllı sistemlerin işleyişini aksatması hatta tamamen durdurması çok da uzak bir olasılık değildir.

Ayrıca şehirdeki enerji sistemlerine yönelik bir siber saldırıda, evlerdeki akıllı cihazlardan tutun da hastanelerde tanı ve tedavi amaçlı kullanılan tüm tıbbi cihazlara kadar tüm enerji ile çalışan sistemler kısa süreli ya da tamamen devreden çıkabilir veya daha da kötüsü cihazların devrelerinin yanması sonucunda büyük fiziksel hasarlar oluşabilir (Alibasic, Al Juraibi, Aung, Woon ve Omar, 2017: 1-10).

Görüldüğü üzere akıllı sistemler olarak tabir edilen tüm bu sistemler şehir hayatına kattıkları pek çok olumlu özelliğin ve getirdikleri faydanın yanında ihtiva ettikleri

güvenlik açıkları nedeniyle önemli riskleri de bünyesinde barındırmaktadırlar. Özellikle sistemlerin birbirleriyle bağlantılı olarak çalışması, güvenlik açıkları ve zayıf şifreleme nedeniyle olası bir siber saldırıda çok büyük fiziksel hasarların, ölümlü kazaların ve bir devletin altından kalkamayacağı ekonomik kayıpların meydana gelmesi çok uzak bir ihtimal değildir.

Çünkü artık bu çağda devletlerin saldırmak için tercih ettikleri silah, bombalar değil; akıllı şebekelerin işleyişini bozmak, akıllı trafik sistemlerini devreden çıkarmak veya kontrolünü ele geçirmek, akıllı hastane randevu sistemlerini kitleyerek kaos yaratmak vb. amaçlar için tasarlanmış kötü amaçlı yazılımlardır (Alibasic, Al Juraibi, Aung, Woon ve Omar, 2017: 1-10).

Bu nedenle teknolojik açıdan yüksek gelişmişlik düzeyine sahip devletler aslında aynı ölçüde bu tür tehditlere karşı savunmasızdır ya da daha dezavantajlıdır. Çünkü kaybedecek şeyi daha çoktur.

Bu tür yüksek teknoloji içeren akıllı sistemler ancak her sistem için özel ve karmaşık şifreleme yöntemleri geliştirilirse ya da çok büyük maliyetlerle etkili siber güvenlik duvarları kurulursa siber saldırılardan bir noktaya kadar korunabilir. Fakat birbirlerine bağlı olarak ve birbirleriyle haberleşerek çalışan bu tür akıllı sistemlerde küçük bir sorun bile çok büyük sonuçları doğurabilecek kapasiteye sahip olduğu için zararlı bir yazılımın sisteme bulaşması durumunda bunun hızla diğer sistemlere de yayılabileceği gözardı edilmemelidir. Bunun dışında yoğun bir DoS/DDoS saldırısının tüm sistemi felç edebilme ihtimali de oldukça kuvvetlidir.

Hal böyleyken devletler, hem çağın gerektirdiği bu teknolojik gelişmelerin gerisinde kalmadan hem de bu teknolojik gelişmelere ayak uydurması halinde tüm bu sistemleri siber saldırılardan gerektiği gibi koruyamaması durumunda nasıl bir yol izleyecekler ya da uluslararası hukukta bu mağduriyetin nasıl giderileceği konusu özellikle 2024 yılında İsrail tarafından yapılan katliam gibi siber saldırı sonrasında önemini daha da artırmıştır.

İsrailin yaptığı siber saldırıda patlayan cihazlar küçük çağrı cihazları olsa da o tür düzeneklerin evlerde bulunan akıllı cihazlara da konulabilmesi ihtimali oldukça ürkütücüdür. Belki de Uluslararası Hukuk tarafından İsrail'e bu katliam ile ilgili uygulanacak yaptırım ya da verilecek karar, devletlere böyle bir durumda haklarını nasıl arayacakları konusunda yardımcı olabilir.

2.BÖLÜM

Siber Uzayda Devlet Kaynaklı Tehditler ve Kullanılan Yöntemler

2.1.Devletlerin Değişen Tehdit ve Güvenlik Algısı

Tehdit algısı ve güvende hissetme olgusu çağlar boyunca imparatorluklar ve devletler için var olma ve varlığını sürdürme konusunda iki önemli unsur olmuştur. Çağlar boyunca imparatorluklar arasında yaşanan savaşların, çatışmaların çoğu tehdit algılama ve güvende hissetme olgusu sebebiyle çıkmıştır.

1648 Vestfalya Barışı sonrasında devletlerin, devlet/ulus kavramının ortaya çıkması ile uluslararası ilişkiler bir bilim dalı olarak ortaya çıkmış ve uluslararası alanda rekabeti de beraberinde getirmiştir. Devletler arasındaki güçlü olma, var olma ve varlığını sürdürme mücadelesi tehdit algısının ve güvende olma isteğinin de baş sebebi olmuştur. Çünkü bir devletin uluslararası alanda varlığını devam ettirebilmesi için güçlü olması gerekmektedir. Güç ise, diğer devletler için tehdit unsurudur. Kendi varlığını tehdit altında hisseden devlet, güvende hissedebilmek için ya saldırmak veyahut da savunmasını geliştirmek mecburiyetindedir. Bu nedenle devletler çağlar boyunca saldırı tekniklerini değiştirip geliştirmişler, savunma kapasitelerini güçlendirmek için gerekli olan aletlerin yapımı için bütçe ayırmışlardır.

Saldırı silahları ise her yüzyılda yaşanan gelişmelerle paralel olarak değişim ve gelişim göstermiştir. Birinci sanayi devrimi neticesinde geliştirilen buhar makineleri sayesinde askeri alanda çok önemli gelişmeler kaydedilmiştir. Buharlı gemilerin yelkenlilerin yerini alarak savaş gemilerinin büyüklüğünü ve yük taşıma kapasitesini birkaç kat birden artırması devletlerin caydırıcı gücünü artırmış ayrıca telgraf ve haberleşme araçları sayesinde orduların birbirleri ile irtibat kurması kolaylaşmıştır.

1800’lü yıllarda metalin işlenmesi hususundaki ustalık ateşin gücü ile birleşince silah ve tüfek yapımında peş peşe gelen yenilikler ve en son olarak 1800’ lerin sonlarına doğru

otomatik makineli tüfeğin yapılması orduların saldırı kabiliyetini ve etkisini on katına çıkarmıştır.

Birinci Dünya savaşında kendisini gösteren hava kuvvetleri gene 1800'lerin sonlarında içten yanmalı motorların üretilmesi neticesinde havacılık endüstrisinin hız kazanması ile mümkün olmuştur.

19.yy sonlarında ilk denizaltı üretilmiş, İkinci Dünya savaşı sürecinde geliştirilen ve saldırı kabiliyetleri artırılan savaş uçakları devletlerin caydırıcılık etkisini daha da artırmıştır.

20. yy başlarında meydana gelen üçüncü sanayi devrimi ise bilgi devrimini beraberinde getirmiş teknolojik gelişmeler özellikle de elektronik ile ilgili gelişmeler askeri alanda lazerli savaş araçlarının geliştirilmesini sağlamış böylece mesafe ölçülmeden de hedeflerin tam isabetle vurulabilmesini mümkün kılmıştır.

21. yy ise siber uzay ve siber güç olgusunun, siber saldırı araçlarının ortaya çıktığı, bilgisayarların ve internetin hatta internet aracılığı ile çalıştırılan nesnelerin bile, virüsler, truva atları vb. zararlı yazılımlar aracılığı ile silah olarak kullanılabildiği bir çağ olmuştur.

Dolayısıyla çağlar içerisinde devletler için tehdit algısı tamamen değişmiş, konvansiyonel saldırı araçlarının yerini yeni nesil olarak tabir edilen saldırı araçları almıştır. Tehdit algısının değiştiği uluslararası ortamda güvenlik algısı ve gereksinimleri de doğal olarak değişmiş, devletleri bu yeni nesil saldırı araçlarına karşı etkili önlemler alma yoluna itmiştir.

2.2.Siber Orduların Kurulma Süreci

Hızla gelişen teknoloji ve beraberinde getirdiği yeniliklerin kendisini en çok hissettirdiği alanlardan biri devletlerin tehdit algısı ve güvenlik ihtiyacı çerçevesinde askeri alan olmuştur. İnternet ile ilgili çalışmalar bile ilk olarak askeri alanda DARPA ile başlamıştır.

Dolayısıyla devletler açısından askeri harcamalar, savunma ve saldırı sanayisini geliştirme ihtiyacı, Maslow'un⁵ ihtiyaçlar hiyerarşisi (Maslow,1943: 370-396) piramidi devletler açısından göz önüne alındığında hep en başta yerini almıştır. Çünkü devletler

⁵ Abraham Maslow : 1908-1970 yılları arasında yaşamış Rus göçmen bir ailenin oğludur. Eğitimini Psikoloji bilimi üzerine alan Maslow çok iyi bir antropolog ve psikoloji uzmanıdır. Özellikle insan motivasyonu üzerine geliştirdiği ihtiyaçlar hiyerarşisi ile psikoloji alanında adını zirveye taşımıştır.

<https://www.economist.com/news/2008/10/10/abraham-maslow> 20.09.2024

açısından varlığını sürdürme kaygısı , gücünü ve egemenliğini sürdürme isteği tıpkı insanlardaki en temel ihtiyaç olan güvende hissetme hissi gibi ihtiyaçlar hiyerarşisinin en temelinde yer almaktadır. Bu nedenle çağlar boyunca devletler savaş veyahut saldırı söz konusu olduğunda ülke topraklarını ve halkını koruması için düzenli ordular kurma ve bu orduları eğitime ihtiyacı hissetmişlerdir.

Çünkü daima savaşa hazır bir ordu, dışarıdan gelebilecek savaş tehdidi, saldırı gibi durumlarda devletin varlığını, ülke topraklarının bütünlüğünü, halkın güvenliğini koruma görevini üstlenen ve bu amaç çerçevesinde üst düzey eğitimlerden geçen kişilerden oluşması sebebiyle devletin güvenlik ihtiyacı açısından çok önemli bir yere sahiptir. O sebeple, devletler için saldırı ve savunma kapasitesini artıracak silahlar, savaş uçakları, savaş gemileri vb. askeri teçhizat kadar tüm bunları etkili bir şekilde kullanacak yetişmiş bir ordu da hayati öneme sahiptir.

Benzer şekilde sürekli gelişen teknolojinin beraberinde getirdiği tehlikelerden korunmak ve olası siber saldırılara karşı etkili bir güvenlik duvarı oluşturabilmek için de siber orduların yetiştirilmesi gerekliliği bir yana, konvansiyonel anlamda kullanılan silahların, saldırı araçlarının, üretim sanayiinde kullanılan endüstriyel robotların, şehir içerisinde kullanılan akıllı sistemlerin tamamının bilgisayar ve internet aracılığıyla kontrol edilebilen sistemlerle donatılması sebebiyle teknik açıdan bilgisayar yazılım ve donanımlarını iyi bilen uzman kişilerin ordu içerisindeki ve hatta kurumsal yönetim sistemleri içerisindeki varlığı zorunlu hale gelmiştir.

Bunun yanında bir de bilgisayarların, internetin zararlı yazılımlar aracılığı ile silah olarak kullanılıp saldırı yapılabildiği bir ortamda siber orduların kurulması devletler açısından artık hayati bir öneme sahiptir. Pek çok devlet bu zorunluluğun farkına vararak uzun süredir siber ordular kurmaya, askeri okullarda bu alan üzerine bölümler açarak öğrenci ve uzmanlar yetiştirmeye başlamışlardır.

Bazıları bu siber orduları siber ordu komutanlığı ismi altında ve askeri kurumlar içerisinde bulundurmakta bazıları ise kurmuş olduğu siber orduya resmi bir görünüm vermeden kamu kurumlarının içerisinde dağınık halde bulundurmaktadır. Örneğin ABD, Çin, Hindistan ve İsrail siber ordu komutanlıkları kurmuş ve siber ordularını da resmi bir statü ile bu kuruluş altında bulundurmaktadır.

Rusya ve Türkiye ise, siber ordularına resmi bir statü vermeden kamu kurumları içerisinde dağınık halde bulundurmaktadır (Aslay, 2017:24-28). Örneğin 2018 yılında dönemin Ulaştırma Denizcilik ve Haberleşme Bakanı olan Ahmet Aslan, o dönemde Türkiye’de çeşitli kamu kurumları bankalar, dev şirketler, enerji tesisleri vb. kritik kuruluşlar içerisinde konuşlandırılmış 13 bin beyaz şapkalı hacker bulunduğunu belirtmiştir (Gökkoyun ve Şengül, 2019). Bu sayıya daha sonradan USOM bünyesinde oluşturulan siber olaylar müdahale ekibinde bulunan 3000’e yakın siber güvenlik uzmanı da eklenmiştir (<https://www.aa.com.tr/tr/bilim-teknoloji/siber-alemin-muhafizlari-beyaz-sapkali-hackerlar/1417719> 17.06.2024).

Genel olarak pek çok ülkede asker sayısı ile kurulan siber ordular içerisindeki yazılımcı sayısı birbirine paraleldir. Ancak bazı ülkeler coğrafi açıdan etraflarındaki ülkelere tehdit hissetmedikleri için asker sayılarını azaltırken gelişen teknoloji ve beraberinde getirdiği tehditler nedeniyle siber ordularının sayısını artırmaktadır (Aslay, 2017) .

2.3.Devlet Kaynaklı Yeni Nesil Saldırı Yöntemleri

20. yy da yaşadığımız bilgi devrimi ardından da 21. yy ve beraberinde getirdiği teknolojik yenilikler hayatımıza getirdikleri pek çok olumlu özelliğin yanında daha önce hiç karşılaşmadığımız tehdit türlerini de beraberinde getirmiştir. Günlük hayatta kişilerin maruz kaldığı tehditlerin yanı sıra belki de en büyük tehdit devletlere yöneltilen ya da yöneltilmesi muhtemel olan siber saldırılardır. Çünkü devletler açısından bu alanda saldırmak savunmaktan daha az maliyetlidir ve etkili bir kötü amaçlı yazılım konvansiyonel bir saldırının verebileceği hasarı hatta belki daha fazlasını çok daha ucuza ve kimlik gizlenerek verebilir.

Sessiz orduların ve hayalet silahların alanı olarak tabir edilen bu yeni nesil saldırı türü devletler tarafından daha çok diplomatik ve politik meselelerde karşı tarafa istediğini yaptırma, ekonomik ve psikolojik açıdan çöküntüye uğratarak istediğini alma ve/veya iç işlerine müdahale etme amacıyla kullanılmaktadır (Aydın, 2008:1-216).

Bu tarz saldırılarda silah olarak kullanılan teknolojik cihazların, kötü amaçlı yazılımların yeni nesil teknoloji olarak tabir edilmesi sebebiyle bu cihazlar ve kötü amaçlı yazılımlar aracılığıyla yapılan saldırılar da yeni nesil tehditler olarak tabir edilmektedir. Aslında

daha çok bilgisayar kullanılarak geliştirilen kötü amaçlı yazılımların internet aracılığıyla saldırı amaçlı kullanılması neticesinde ortaya çıkan yeni nesil saldırı yöntemleri, nesnelerin interneti ve yapay zeka kavramları ile farklı bir boyuta da evrilmiş, artık internetle çalışan pek çok cihaz bir saldırı aracı olarak kullanılabilir hale gelmiştir.

Kullanılan cihazlar değişiklik gösterse de devletler tarafından yapılan ya da yapılması muhtemel siber saldırılar genellikle Virüsler, Worm olarak da tabir edilen solucanlar, Truva atları (Trojan), RAT'lar, DoS ve DDoS atakları ve Siber casusluk yoluyla yapılmaktadır. Bu zararlı yazılımlar alt başlıklarda ayrı ayrı açıklanacaktır. Ancak bundan önce siber saldırı türlerine değinmek gerekmektedir.

Siber saldırılar Sentaktik, Semantik ve Karışık saldırılar olmak üzere üç gruba ayrılmaktadır (Polat, 2020: 135-158). Sentaktik saldırılarda hedef , bilgisayarların işletim sistemleridir. Zararlı kodlar, zararlı yazılımlar, DoS ve DDoS atakları bu tür siber saldırılara örnek gösterilebilir.

Semantik saldırılarda hedef, kullanıcının ulaştığı bilginin doğruluğudur. Sistem doğru çalışır ancak elde edilen bilgi yanlıştır. Bu tip siber saldırılar daha çok resmi internet siteleri, kritik altyapı sistemleri, nükleer santraller ve havaalanlarında kullanılan hava trafik kontrol sistemleri gibi kritik öneme sahip sistemlere yöneltilmektedir.

Bir de bu iki saldırı türünün aynı zamanda kullanıldığı Karışık saldırılar vardır. Burada hedef hem işletim sisteminin devreden çıkarılması hem de kritik sistemlere hatalı bilgi iletilmesidir (Polat, 2020).

2007 yılında Estonya'ya ve 2008'de Gürcistan'a yapılan siber saldırılar Sentaktik saldırı türüne girerken, İran Nükleer tesisine yapılan Stuxnet virüsü Karışık saldırı türüne girmektedir. Çünkü saldırıda hem zararlı bir yazılım türü olan virüs kullanılmış hem de nükleer tesisin SCADA sistemleri, yanlış bilgi gönderilerek yanıltılmıştır.

Aşağıda sentaktik, semantik ve karışık saldırı türlerine giren siber saldırı türleri açıklanmıştır. Siber uzayda saldırı amacıyla kullanılan yöntemlere geçmeden önce belirtmek gerekir ki, hangi saldırı türü olursa olsun, saldırı fiili başlı başına uluslararası hukuka aykırı bir eylemdir ve tüm bu saldırı türleri başka bir devletin iç işlerine müdahale

edilmemesi ve zarar vermeme ilkesini ihlal etmeleri nedeniyle uluslararası hukuka aykırılık teşkil etmektedir.

2.3.1. Virüsler

Siber Saldırılarda en çok kullanılan zararlı yazılım türlerindendir. Virüsler kendilerini kopyalamak için başka bir programa ve yayılabilmek için de bir ana programa bağlanmaya ihtiyaç duyarlar yani bulaşmak ve yayılmak için insan etkileşimine ihtiyaç duyarlar (Bozkurt, 2022: 26). Bir program veya USB (Universal Serial Bus ya da Türkçe ismiyle Evrensel Seri Yolu)⁶ bellek aracılığıyla bilgisayara veya sisteme entegre edilen virüs bulaşıp yayılabileceği ana programı bulduğunda bilgisayardaki ya da sistemdeki çalışma düzenini, dosyaları çalışamaz duruma getirir ya da çalışma düzenini tamamen bozar. Çalışma düzeni bozulan sistem ve/veya bilgisayar işlevini yerine getiremez hale gelir ve bu da bozulan sistemler ya da bilgisayarlar aracılığıyla kontrol edilen sistemlerin çalışamaz duruma gelmesine, bozulmasına ya da yanlış çalışarak daha büyük zararların meydana gelmesine neden olur.

Şu ana kadar geliştirilmiş en tehlikeli virüsün İran'ın Natanz Nükleer tesisine yapılan siber saldırıda kullanılan Stuxnet isimli virüs olduğu bilinmektedir. Özelliklerine ve vermiş olduğu fiziksel hasara Stuxnet siber saldırısı bölümünde de değineceğimiz Stuxnet virüsü nükleer santralin sistemine bir USB bellek aracılığıyla entegre edilmiş ve sebep olduğu fiziksel ve ekonomik hasarın yanı sıra İran'ın nükleer çalışmalarında 2 yıl gecikme yaşanmasına sebep olmuştur.

2.3.2. Worm (Solucan)

Virüslerin aksine kendi kendilerini kopyalamak için başka bir programa ihtiyaç duymayan ve insan etkileşimine ihtiyaç duymadan yayılabilen kötü amaçlı yazılımlardır (Bozkurt, 2022: 26). Çalışma sisteminin aksine bilgisayarlar ve sistemler üzerinde virüslerinkine benzer etkiler bırakırlar. Örneğin bilgisayarlarda donma, sistemin çökmesi, hata vermesi, bilgisayarlardaki dosyaların bozulması veya kaybolması vb. hatalar sisteme solucan (worm) bulaşmış olduğunu gösterir.

⁶ Aygıtlar arasında bağlantı ve veri akışını sağlayan cihazlardır.
<https://dictionary.cambridge.org/tr/sözlük/ingilizce/usb> 20.09.2024

2.3.3. Truva Atları (Trojan) ve RAT'lar

Truva atları görünürde meşru olan ancak onaylandığında bilgisayarlarda bilinmeyen (etkisini zamanla gösteren) ve istenmeyen zararlara sebep olan kötü amaçlı yazılımlardır (Bozkurt, 2022: 26). Bir internet bağlantısı, indirilen ya da üzerine tıklanan herhangi bir fotoğraf, resim, reklam veya indirilen bir müzik aracılığıyla sisteme bulaşan ve etkisini uzun süre içerisinde gösteren Truva atları, sistemdeki açıklardan yararlanarak kişisel bilgilerin ve hesap bilgilerinin çalınması için kullanılır.

Truva atlarının uzaktan yazılım yüklenebilmesini mümkün kılan türleri de vardır. Bunlara RAT (Remote Access Control-Uzaktan Erişim Kontrolü) (<https://www.techtarget.com/searchsecurity/definition/RAT-remote-access-Trojan> 19.12.2024) ismi verilir RAT'lar, Trojanların aksine bulaştıkları sistemlerde uzaktan bağlantı yoluyla merkeze bağlanarak farklı zararlı yazılımların da yüklenmesine sebep olabilecek kapasiteye sahiptirler.

2.3.4. DoS ve DDoS Atakları

DoS (Denial of Services- Hizmet reddi) atakları bir kaynaktan (bilgisayar) belirli bir servise, bir siteye yöneltilen ve sistemin çökmesine neden olan, sistemin hizmet vermesini ve kullanıcıların sisteme erişmesini engelleyen saldırı türüdür (Hathaway, 2011:1-72). Her sitenin ve her sistemin kaldırabileceği ağ yoğunluğu farklıdır. Bu tarz saldırılarda sisteme kaldırabileceğinden fazla ağ bağlantısı yüklenerek sistemin hizmet vermesi kullanıcıların sisteme erişmesi engellenir ve sistem çökmesi sorunu yaşanır.

DDoS (Distributed Denial of Services - Dağıtılmış Hizmet Reddi Atakları) ise aynı saldırı türünün birden fazla kaynaktan (bilgisayardan) daha yoğun biçimde yapılan türüdür (Hathaway, 2011:1-72). Bu tür saldırılarda sistem geçici olarak değil tamamen çöker ve hizmet veremez hale gelir. Örneğin geçmişte yaşanan siber saldırılar kısmında üzerinde ayrıntılı bir şekilde duracağımız 2007 Estonya ve 2008 Gürcistan siber saldırıları bu tür siber saldırılara örnek teşkil etmektedir.

2.3.5. Siber Casusluk

Siber uzayda sistemde bulunan güvenlik açıklarından yararlanılarak bilgi sistemlerine sızmak suretiyle gerçekleştirilen ve bilgi toplamak amacıyla yapılan illegal faaliyetlerdir. Çoğu zaman devletler tarafından birbirlerinin askeri ve teknik alandaki ve devlete ait gizli kalması gereken bilgileri sızdırmak ve teknik anlamda öne geçmek amacıyla gerçekleştirilen siber saldırı türüdür (Kara, 2013: 1-85).

2.3.6. APT (Advanced Persistent Threat - Gelişmiş Kalıcı Tehdit)

Genel olarak devletlerin kritik altyapı sistemlerini hedef almak amacıyla kullandıkları ve siber saldırı yapmak için özel olarak geliştirilen, ileri düzeyde ve uzun vadeli zarar verme özelliğine sahip zararlı yazılımlardır. APT'ler bulaştırıldıkları sistemlerde güvenlik duvarlarını kolayca aşabilen, uzun süre fark edilmeden sistem içerisinde çalışmaya devam eden ve geliştirilmesi için özel laboratuvarlar, teknik imkanlar ve profesyonel bir ekip gerektiren kötü amaçlı yazılımlardır (Kara, 2013: 1-85). Bulaştırıldıkları sistemi çökertmek üzerine programlanmışlardır.

Ayrıca bu tür virüsler devlet bütçesi ve imkanları olmadan geliştirilmesi neredeyse imkansız olan, büyük maliyetler gerektiren virüslerdir (Kara, 2013). Örneğin İran Natanz nükleer santraline yapılan siber saldırıda kullanılan Stuxnet virüsü APT tarzı bir virüstür.

Devletler bazen bu tür yeni nesil saldırı yöntemlerini ordu içerisinde istihdam ettikleri siber uzmanlar aracılığıyla bazen de finansal destek, eğitim ve ekipman sağladıkları terörist gruplar aracılığıyla veya devlet adına yetki ve imkan sağlanan hackerlar aracılığıyla hatta bazen de hedef devlet içerisinde satın aldıkları ajanlar aracılığıyla yaptırmaktadırlar.

Bu alanın anonim yapısını, daha yıkıcı ve caydırıcı sonuçları daha kolay ve daha az maliyetle elde edebildiklerini keşfeden devletler gün geçtikçe ve teknolojik imkanlar arttıkça bu tür yeni nesil saldırı yöntemlerine daha çok bütçe ve imkan tahsis etmeye başlamışlardır.

2.3.7. Mantık Bombası Virüsü

Bu virüs işletim sistemlerine, ağılara ya da programlara saldıran ve belirli koşullar gerçekleştiğinde (tarih veya saat) aktifleşen bir virüstür (<https://www.malwarebytes.com/logic-bomb> 17.09.2024). Çalıştığında ise bulaştığı sistemi, ağı ya da programı çökertir ve çalıştığı süre içerisinde stuxnet virüsüne benzer şekilde sistemin veya ağın çalışma düzenindeki aksamanın farkedilmesine engel olur. Ayrıca virüsün bulaştığı noktadaki işi bittiğinde kanıtları yok edebilir.

Bu virüs ile ilgili en bilinen saldırı 1982 yılında gerçekleşen ve Sibirya'da doğalgaz borularının patlamasına neden olan Sibirya mantık bombası saldırısıdır. Bu saldırının ayrıntılarına bir sonraki bölümde değinilecektir.

3.BÖLÜM

Siber Saldırı Örnekleri

3.1.Geçmişte Yaşanan Siber Saldırıları

Teknolojik gelişmişlik devletler açısından pek çok avantajı ve tehlikeyi beraberinde getirmektedir. Esasen teknolojik gelişmişlik seviyesi arttıkça devletler açısından tehdit ve saldırıya uğrama olasılığı da aynı ölçüde artmaktadır. Bunun nedeni artık pek çok şeyin internete bağlı olarak çalışması, bilgisayarlarla kontrol edilmesindendir. Kamu kurumlarında ve bankalarda tüm iş ve işlemlerin bilgisayarlar ve internet aracılığıyla yapılması, havaalanlarının, kritik altyapı sistemlerinin, barajların, hastanelerin, akıllı tren, metro vb. taşıma araçlarının internet bağlantılı sistemler aracılığıyla kontrol edilmesi ve askeri araçlarda kullanılan radar sistemlerinin, insansız hava araçlarının, akıllı füze sistemlerinin, savaş gemilerinin tüm sistemlerinin bilgisayarlar ve internet aracılığıyla kontrol ediliyor olması bir devlet açısından hem büyük bir avantaj, ekonomik açıdan gelişmişlik ve güç işareti hem de siber uzaydan gelebilecek yeni nesil tehdit türlerine karşı tehlike altında olduğunun göstergesidir.

Üstelik yakın geçmişte bu tür yeni nesil saldırı yöntemleri bazı devletler tarafından caydırma amacıyla ve çoğu zamanda siyasi saiklerle başka bir devlete karşı silah olarak kullanılmıştır. Bu saldırılardan ekonomik ve fiziksel anlamda en çok hasar verenler aşağıda açıklanmıştır.

3.1.1. 1982 Sibirya Mantık Bombası Saldırısı

SSCB'nin Kanada'dan siber casusluk yoluyla doğalgaz hatlarının kontrolünde kullanılan yazılım programının bilgilerini çaldığını farkedene CIA yazılım programının içerisine mantık bombası virüsü yerleştirmiştir. Virüslü yazılımı doğalgaz boru hatlarının kontrolünde kullanan SSCB, Sibirya doğalgaz boru hatlarının adeta atom bombası gibi patlaması neticesinde çok büyük ekonomik zarara uğramıştır.

Mantık bombası virüsü boru hatlarının çalışma düzenini bozarak borulara aşırı gaz yüklenmesine neden olmuş bu da borularda atom bombası gücünde bir patlamanın

gerçekleşmesine sebep olmuştur (Bayrak, 2020:27). Üstelik virüs boruların çalışma düzenindeki aksamının ve bozulmanın farkedilmesine de engel olmuştur (Darıcılı, 2017:69-72).

CIA tarafından hazırlanan bu virüslü yazılımı Sibiry gaz boru hatlarının kontrol sistemine angaje eden ise Albay Vladimir Vetrov isimli bir ajandır. Vetrov'un olay sonrasında casusluk suçundan dolayı SSCB tarafından idam edildiği bilinmektedir (Darıcılı, 2017).

3.1.2. Moonlight Maze Saldırısı (Ayışığı Labirenti saldırısı)

ABD'ye ait askeri bilgiler, uzay çalışmaları (NASA) ve kritik altyapı sistemlerine ait bilgilerin 1996 - 1998 yılları arasında siber casusluk yöntemi ile sistemli olarak çalınması olayıdır. Saldırıda ABD'ye ait askeri tesislerin haritaları, kritik altyapı sistemlerine ait bilgiler, askeri açıdan geleceğe yönelik projelerin bilgileri ve daha pek çok devlete ait gizli belge çalınmıştır . ABD bu saldırının izini sürmüş ve saldırının Rusya tarafından gerçekleştirildiği sonucuna varılmıştır (Özkan, 2019: 121-122) .

Saldırı neticesinde tüm çalışmaları (askeri haritalar ,kritik altyapı sistemlerine ait bilgiler, uzay çalışmaları ve devletin gizli belgeleri) yenilemek ve baştan düzenlemek mecburiyetinde kalan ABD milyarlarca dolarlık zarara uğramıştır (Özkan, 2019).

3.1.3.Titan Rain Saldırısı

2003-2007 yılları arasında ABD hükümetinin ve ABD'ye ait askeri sistemlerin kritik altyapı sistemlerinin, uzay çalışmalarının ve devlete ait gizli kalması gereken belgelerin çalınması amacıyla başlatılan ve terabaytlarca bilginin çalınması ile sonuçlanan siber saldırılardır (Özkan, 2019:126-127). 1998 yılında yapılan Moonlight Maze saldırısı ile benzer özellikler gösteren Titan Rain saldırısının izleri ABD'li uzmanlar tarafından takip edilmiş ve saldırının arkasında Çin'in olduğu tespit edilmiştir.

Özellikle ABD'ye ait askeri kuruluşların gizli bilgileri, askeriye ait lojistik faaliyetlerine dair gizli kalması gereken bilgi ve belgeler çalınmıştır (Özkan, 2019).

Saldırı sonucunda tüm bilgi ve belgelerin revize edilmesi ve casus virüsün bulaştırıldığı sistemlerin virüsten arındırılabilmesi çok büyük maliyetli harcamalar yapılarak mümkün olmuştur. Bu da devlet açısından büyük bir ekonomik kayıp anlamına gelmektedir.

3.1.4. 2007 Estonya Siber Saldırısı

SSCB, İkinci Dünya Savaşı sürecinde Nazi işgalinden kurtardığı Estonya'ya bu kurtuluşun nişanesi olarak başkent Tallinn'e koyulmak üzere bir bronz kızıl ordu heykeli göndermiştir. 1989'da SSCB yıkılmış Estonya bağımsızlığına kavuşmuştur. Estonya'da Sovyetler döneminin izlerinin silinmeye çalışıldığı süreçte 2007 yılında bronz heykelin başkent Tallinn'den taşınması gündeme gelmiş hatta halk tarafından da bu durum desteklenmiştir (Dilek, Talih ve Bensghir Kaya, 2023: 332-347).

Heykelin taşınması sürecinde ülkede yaşayan Estonyalılar ve Ruslar arasında bronz heykelin taşınması nedeniyle karşılıklı çatışmalar çıkmış aynı süreçte de Estonya devlet kuruluşlarına, bankalara, üniversitelere, kritik sistemlere, ulusal sistemlere, gazetelerin online sayfalarına, e-ticaret sitelerine yoğun DoS (Hizmet Reddi - Denial of Services) ve DDoS (Dağıtılmış Hizmet Reddi - Distributed Denial of Services) atakları yapılmış, internet siteleri çökme noktasına gelmiş, ülkenin en büyük bankası işlemlerini yapamaz hale gelmiş, kritik sistemler , üniversiteler , devlet kurumları çalışamaz hale gelmiştir (Dilek, Talih ve Bensghir Kaya, 2023).

DoS veya DDoS saldırı türlerinde hedef sisteme doğrudan saldırılmaz bunun yerine saldırı DNS'e (Alan Adı Sistemi) yönlendirilir. Bu sayede IP belirlenemediği için internet sitelerinin açılması ve hizmet vermesi imkansız hale gelir (Şafak, 2019:127-160). Bu nedenle yirmi sekiz gün boyunca süren bu saldırılarda Estonya işleyemez hale gelen bankalar, kamu kurum ve kuruluşları, üniversiteler, e-ticaret siteleri ve saldırıdan etkilenen diğer önemli sistemler nedeniyle milyarlarca dolar zarara uğramıştır (Herzog, 2011: 49-60).

Estonya siber saldırısının Rusya kaynaklı olduğunu vurgulamıştır. Her ne kadar Rusya saldırıyı inkar etse de saldırıda kullanılan alfabenin Rus alfabesi olması ve botnet⁷'lerin

⁷ Botnet'ler : DoS ve DDoS atakları gibi hizmet reddi saldırılarını gerçekleştirmek amacıyla kullanılan, ana bilgisayardan bağlanılarak virüsler aracılığıyla zombi haline getirilip hedef sisteme saldırmak için kullanılan bilgisayarlardır. Çelik, Ş.(2013) Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet

bağlandığı ana bilgisayarlar takip edildiğinde ana bilgisayarların merkezinin Rusya olması saldırının Rusya tarafından gerçekleştirildiğini göstermektedir (Şafak, 2019).

Estonya bu siber saldırılar nedeniyle NATO'dan yardım istemiş ve NATO'da Tallinn'e durumu incelemek üzere uzman bir ekip göndermiştir.

Estonya 28 gün süren ve tüm devlet dairelerinde, kamu kurum ve kuruluşlarında, bankalarda, günlük hayatta işlerin durmasına ve dolayısıyla milyarlarca dolarlık zarara sebep olan bu saldırılar sebebiyle uzun süre mali sorunlar yaşamıştır (Herzog, 2011: 49-60).

3.1.5. 2008 Gürcistan Siber Saldırısı

SSCB'nin çöküşü sonrasında 1991' de bağımsızlığını kazanan Gürcistan iki sene sonra Abhazya ve Güney Osetya'nın hakimiyetini Rusya tarafından mali destek ve koruma sağlanan milislere kaptırmıştır (Kara, 2013: 1-85). 2008 yılında Güney Osetya'daki milisler Gürcü köylerine karşı saldırı başlatınca Güney Osetya'nın başşehri de Gürcistan tarafından saldırıya uğramıştır. Ancak eş zamanlı olarak Rusya siber saldırılar başlatarak Gürcistan'ın dış dünya ile bağlantılarını kesmek için Gürcistan devlet kurumlarına, medya organlarına , para akışı ve mali kaynaklarını kesmek için de bankalara yoğun DDoS saldırıları gerçekleştirmiştir (Kara, 2013: 1-85).

Gürcistan'ın internet bağlantısı Türkiye ve Rusya aracılığıyla sağlandığı için Gürcistan saldırıları engellemek amacıyla, Rusya ile olan veri akışını (ağ bağlantısını) kesmiştir (Kara, 2013). Bunun üzerine Rusya siber saldırılarına gene botnet'ler aracılığıyla Çin üzerinden devam etmiştir.

Sonuçta Gürcü bankaları ve devlet sistemleri işleyemez hale gelmiş, kredi kartları ve cep telefonları çalışamaz duruma gelmiş hatta Gürcistan'daki bazı devlete ait bilgisayarlar botnet olarak kullanılıp dünyadaki pek çok bankaya siber saldırı düzenlenmiştir (Kara, 2013). Neticede bu bankalar Gürcistan ile olan iş ve işlemlerini sonlandırma ve

Kullanmaktan Kaçınma ilkesi Çerçevesinde bir Değerlendirme. Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Cilt: 15, Sayı: 1, 2013, s.137-175 (Basım Yılı: 2014)

bağlantılarını koparma kararı almışlar ve Estonya saldırısında olduğu gibi Gürcistan'da da milyarlarca dolarlık hasar ve ekonomik kayıp oluşmuştur (Özkan, 2019: 1-185).

3.1.6. 2010 İran Stuxnet Saldırısı

İran Natanz nükleer tesisi, İsfahan'da 100.000 metrekare alan içerisinde 8 metre uzunluğunda ve 2,5 metre kalınlığında iki duvarla korunan devasa bir Uranyum zenginleştirme tesisidir. Tesiste 7000 adet santrifüj bulunmaktadır ve bu santrifüjlerin 5000 tanesi uranyum zenginleştirme faaliyetleri kapsamında aktif durumdadır. Bu devasa tesis Alman Siemens firması tarafından SCADA isimli sistemle geliştirilmiştir (Çelik, 2014: 137-175).

Denetimli kontrol ve veri toplama sistemi olarak bilinen SCADA sistemleri büyük bir alandaki cihazların tek bir merkezden gözlemlenmesi, verilerin toplanıp işlenmesi, kaydedilmesi ve önceden planlanan iş ve işleyiş planlarının gözleminin yapılabilmesi için kullanılan bilgisayar temelli sistemlerdir. Bu sistemde bilgisayar görevini PLC (Programable Logic Controller - Programlanabilir Mantık Denetleyicisi) ismi verilen bir çeşit bilgisayar yapar. PLC'ler bilgisayarlar gibi kendilerine verilen komutları işleyip SCADA birimlerine iletirler (Çelik, 2014:147-148).

2010 yılında bu devasa tesisin SCADA sistemlerine iki farklı tarihte Stuxnet adı verilen virüs ile siber saldırı gerçekleştirilmiştir. Stuxnet virüsü burada SCADA isimli sistemi devre dışı bırakarak santrifüjleri besleyen elektrik akımının frekansını sürekli yükseltip alçaltarak santrifüjlerin en az 1000 tanesinin devreden çıkmasına ve santrifüjlerin yanarak ve eriyerek çalışamaz hale gelmesine neden olmuştur. Santrifüjlerin çalışma şeklinin değişmesi bilgisayarlar tarafından algılanamamıştır. Çünkü Stuxnet virüsü bulaştırıldığı sisteme 'ortadaki adam' yazılımını yerleştirmek suretiyle makineler ile onları kontrol eden bilgisayarlar arasındaki iletişimi keserek bilgisayarların, makinelerin doğru bir şekilde çalışıp çalışmadığını görmesini engeller ve bu şekilde sistemde meydana gelen hatanın bilgisayarlar tarafından algılanmasına engel olur (Şafak, 2020: 127-160).

Natanz Nükleer tesisine yapılan Stuxnet saldırısı da nükleer tesisteki santrifüjlerin aşırı ısınıp soğumasına neden olarak santrifüjlerin erimesine neden olmuş ancak sistemde

yaşanan bu büyük sorun ana bilgisayarlar tarafından algılanamamıştır. Bu nedenle tesisdeki binlerce santrifüj ile birlikte sisteme bağlı olarak çalışan ve sistemi kontrol eden 30 bine yakın bilgisayar da kullanılamaz hale gelmiştir. Bu da İran'ın Nükleer geliştirme programında en az iki yıl geriye gitmesine ve milyarlarca dolarlık ekonomik zarara sebep olmuştur (Çelik, 2014:147-148).

Stuxnet siber saldırısı ilk kez bir devlete karşı başka bir devlet tarafından gerçekleştirilen ve milyarlarca dolarlık zararın yanısıra fiziksel olarak da hasar veren bir siber saldırı olma özelliğine sahiptir (Collins ve McCombie, 2012:80-91). Ayrıca Stuxnet virüsü, tarihte ilk kez sabotaj amacıyla geliştirilmiş bir virüs olması açısından da çok önemlidir (Holat, 2021:115).

Bu nedenle Stuxnet saldırısı meydana gelebilecek yıkıcı hasarları gözönüne sermesi ve siber saldırı araçlarının devletler tarafından sabotaj için özel olarak geliştirilebileceğini göstermesi açısından çok önemli bir olaydır.

3.1.7. 2012 Suudi ARAMCO Siber Saldırısı

Dünyanın dev şirketlerinden biri olan Suudi ARAMCO 2012 yılında siber saldırıya uğramıştır. Saldırıda kullanılan Shamoon Virüsü şirketteki 30.000 den fazla bilgisayarın hard diskine geri dönülemez bir şekilde zarar vermiş, hard disklerdeki tüm bilgilerin silinmesine, şirket içi haberleşme uygulamalarının kullanılamaz hale gelmesine neden olmuştur (Gümüşbaş, 2018: 181-194).

Günlük cirosu milyarlarca doları bulan şirkette saldırı nedeniyle iki hafta boyunca hiçbir işlem yapılamaz hale gelmiş, virüsten etkilenen tüm bilgisayarların ve sistemin tamamen yenilenmesi gerekmiştir. Saldırı, meydana gelen fiziki hasarın yanı sıra hem hasar gören tüm sistemin yenilenmesi hem de şirket işleyişindeki iki haftayı bulan aksama nedeniyle milyarlarca dolarlık ekonomik kayba da neden olmuştur.

Bu saldırı ticari bir şirkete yapılan en büyük siber saldırı olma özelliğine sahiptir (Gümüşbaş, 2018). Ayrıca Stuxnet saldırısından sonra bir ülkenin kritik altyapı sistemlerine yapılmış en büyük siber saldırı olma özelliğine de sahiptir ([Varlık, E. \(2015\) https://siberbulten.com/siber-saldirilar-2/aramco-saldirisi/ 15.01.2025](https://siberbulten.com/siber-saldirilar-2/aramco-saldirisi/ 15.01.2025)).

Saldırının kimler tarafından gerçekleştirildiği konusunda da hem hata veren sistemlerde gösterilen yanan Amerikan bayrağı simgesi hem de saldırıyı üstlenen Cutting Sword of Justice (Adaletin Keskin Kılıcı) isimli grubun kendilerine Şii inancında Hz. Ali'nin lakabı olan Allah'ın Keskin Kılıcı'na ithafen bu ismi vermeleri ve o dönemde Suudi Arabistan tarafından izlenen politikanın İran'ın menfaatleri ile çatışıyor olması saldırının İran tarafından yapıldığı yönündeki şüpheleri kuvvetlendirmiştir (Varlık, E. (2015) <https://siberbulten.com/siber-saldirilar-2/aramco-saldirisi/ 15.01.2025>).

Nitekim Suudi Aramco'ya yapılan siber saldırı sonrasında ABD tarafından İran'a yönelik siber saldırı gerçekleştirilmiştir.

3.1.8. İsrail'in Lübnan'da Gerçekleştirdiği Siber Saldırı

Bugüne kadar yapılmış olan siber saldırılar içerisinde fiziksel manada hasar veren ilk siber saldırı 2010 yılında İran'ın Natanz Nükleer Tesisine yapılan Stuxnet siber saldırısıdır. Saldırı sonucunda oluşan fiziksel hasar bakımından değerlendirildiğinde daha önce benzeri görülmemiş bir hasar bırakan Stuxnet saldırısı bir devlet tarafından başka bir devlete karşı gerçekleştirilen ve fiziki olarak hasar veren ilk siber saldırı olarak bilinmektedir.

2012 yılında Suudi ARAMCO petrol şirketine karşı gerçekleştirilen ve 30.000 adet şirket bilgisayarının kullanılamaz hale gelmesine ve bir günlük cirosu bile milyar dolarları bulan şirketin günlerce işlem yapamaması nedeniyle çok ciddi ekonomik kayba uğramasına sebep olan Shamoon virüsü saldırısı ise siber saldırıların fiziksel hasarlara yol açabileceğini kanıtlayan ikinci önemli siber saldırıdır.

Ancak İsrail tarafından 18 Eylül 2024' de Lübnan'daki Hizbullah üyelerine karşı gerçekleştirilen ve en kanlı siber saldırı olarak tarihe geçen saldırıda İsrail, Hizbullah üyelerinin haberleşme amacıyla kullandıkları çağrı cihazlarına uzaktan sinyal göndermek sureti ile cihazların bir bomba gibi patlamasına neden olarak olay anında içlerinde çocukların da olduğu 9 kişinin ölmesine ve 2000 den fazla kişinin yaralanmasına sebep olmuştur (<https://www.youtube.com/watch?app=desktop&v=KLvYTCcmqEA>)

[17.10.2024](#)). Daha sonrasında ise patlamalar nedeniyle ölenlerin sayısının 37' ye yükseldiği belirtilmiştir.

Şu ana kadar gerçekleşen en güncel ve en kanlı siber saldırı olan bu olay siber katliamın artık olası olduğunu da ispatlamış bulunmaktadır (<https://www.youtube.com/watch?app=desktop&v=KLvYTCcmqEA> 17.10.2024).

BBC News'in haberine göre, çağrı cihazlarına nasıl sızıldığı ve cihazların nasıl patlatıldığı konusu henüz net olarak bilinmemekle birlikte uzmanlar bu büyüklükte bir hasarın oluşabilmesi için cihazların içerisine daha önceden patlayıcı yerleştirilmiş olması ihtimalinin çok güçlü olduğunu belirtmişlerdir (<https://www.bbc.com/turkce/articles/czj978p0w39o> 17.10.2024).

Gene aynı habere göre patlayan çağrı cihazlarının üzerinde Tayvan menşeli olan Gold Apollo'nun logosu bulunmaktadır. Ancak Tayvanlı şirket ile yapılan görüşmede şirket yetkilisi, uzun süre önce BAC Danışmanlık isimli ve Macar asıllı bir şirkete Gold Apollo markasının ismini kullanma hakkı verdiklerini belirtmiştir. İlgili şirket araştırıldığında ise şirketin aslında İsrail istihbaratının paravan şirketi olduğu yani İsrail ajanlarının kimliklerinin gizlenmesi amacıyla kurulan şirketlerden birisi olduğu belirlenmiştir (<https://www.nytimes.com/2024/09/18/world/middleeast/israel-hezbollah-pager-attacks-history.html?searchResultPosition=1> 17.10.2024)

Çağrı cihazlarının infilak etmesini sağlayan etken ise, cihazların imal edilmesi sürecinde içlerine yerleştirilmiş olan küçük patlayıcıların 18 Eylül 2024'te saat 15.30'da cihazlara gönderilen ve Hizbullahın lider kadrosundan gelmiş gibi görünen mesajlar ile aktif edilmesidir. Zira mesajlar geldikten saniyeler sonra patlamalar gerçekleşmiştir (<https://www.bbc.com/turkce/articles/czj978p0w39o> 18.10.2024).

Gene BBC News'in haberine göre, ikinci saldırıda hedef alınan çağrı cihazlarının menşeinin daha karışık olduğu zira infilak eden cihazlardan bazılarının Japon ICOM Şirketi tarafından üretilen IC-V82 model cihazlar olduğu görülmüş, şirketle iletişime geçildiğinde ise şirketin bu model çağrı cihazı üretmeyi 2014 yılında bıraktığı belirtilmiştir. Şirketin ABD'de bulunan bayisinden bir yetkili, patlayan çağrı cihazlarının sahte olduğunu ve bu modelin sahtesinin internette kolayca bulunabileceğini belirtmiştir (<https://www.bbc.com/turkce/articles/czj978p0w39o> 18.10.2024).

Siyaset, Ekonomi ve Toplum Arařtırmaları Vakfında Dıř Politika Arařtırmaları Direktörlüğü yapmakta olan Murat Yeřiltař TRT1'de yayınlanan Enine Boyuna programında *"İsrail'in yapmıř olduđu bu siber saldırının 3 ayrı saldırının bir parçası olduđunu, saldırıda uzaktan patlatılan çağrı cihazlarının MOSSAD'ın teknoloji istihbaratı birimi olan 8200 tarafından Macaristan'daki řirket aracılıđıyla ele geçirilip içlerine 10 mg ağırlığında çok küçük çaplı patlayıcılar yerleřtirilerek bu cihazların atılan bir mesaj aracılıđıyla patlamasını sağladıklarını ve bu řekilde pek çok insanın ellerini ve gözlerini kaybetmelerine hatta cihazı bel bölgelerinde taşıyanların karın bölgelerinde çok ciddi yaralanmaların meydana gelmesine neden olduđunu"* belirtmiřtir (<https://www.setav.org/israilin-lubnanda-gerceklestirdigi-saldiri-nasil-organize-edildi> 25.01.2025).

Bu saldırı, sürekli geliřen teknolojiyle birlikte tartıřmalara neden olan siber saldırıların ölümcül sonuçlara yol açıp açmayacağı sorusunun cevabını kesin bir řekilde vermiř bulunmaktadır. Hatta daha önce belirtildiđi gibi artık siber katliamın mümkün hale geldiđi de açıkça görölmüřtür.

Bu saldırıda, saldırı suçunu işleyen devlet ve işlenen suç açıkça bellidir. İsrail bu olayda sivillerin yaralanmasına ve hatta içinde çocukların da bulunduđu pek çok sivilin ölmesine neden olarak açıkça insanlıđa karřı suç ve savař suçu işlemiřtir.

İsrail'in işlediđi bu suçların neticesinde Uluslararası Hukuk açısından nasıl bir yaptırım uygulanacağı henüz belli deđildir. Ancak bu saldırının kim tarafından yapıldığı açıkça bilindiđinden, siber saldırılarla ilgili en büyük sorun olan atıf problemi bu saldırı için ortadan kalkmıř durumdadır. řimdi merak edilen İsrail'in işlediđi bu suçlar neticesinde nasıl bir yaptırımla karřılařacağı hususudur.

4. BÖLÜM

Saldırı Suçu ile İlgili Temel Uluslararası Hukuk İlkelerinin Siber Saldırılarına Uygulanabilirliği ve Tallinn Rehberi

4.1. Saldırı Suçu İle İlgili Temel İlkelerin Siber Saldırılarına Uygulanması

1648 Vestfalya Barışı ile ulusal devlet egemenliği ilkesinin temel hak olarak tanınması uluslararası alanda devletleri temel aktörler haline getirmiştir. Egemenliğini koruma ve sürdürme kaygısı ise devletleri uluslararası alanda diğer devletlere karşı savunmasız bir duruma düşmemek için güçlü olmak zorunda bırakmıştır. Bir devletin elde ettiği gücün bir başka devlet için güvenlik kaygısı anlamına geldiği bu durumda devletler arasındaki çatışma riski daima kriz ortamını ve savaş riskini canlı tutmuştur.

Özellikle güç mücadelesi ve egemenlik alanını genişletme kaygısı ile patlak veren Birinci ve İkinci Dünya Savaşları gibi tüm dünyayı etkileyen ve büyük yıkımlara, çok büyük kayıplara sebep olan savaşlar uluslararası alanda barışı ve huzuru hakim kılacak, devletler arasındaki ilişkileri düzenleyecek, krizleri savaşa varmadan çözüme kavuşturacak ve devletler arasındaki anlaşmazlıklarda adil çözüm yollarının bulunmasını sağlayacak hukuk kurallarının oluşturulmasını zorunlu kılmıştır. İşte bu ihtiyaç neticesinde ortaya çıkan Uluslararası hukuk, devletler arasındaki ve uluslararası toplum üyeleri arasındaki ilişkileri düzenlemek, uluslararası alanı güvenli, barışçıl ve huzurlu bir alan haline getirmek için yapılan antlaşmalar, koyulan kurallar bütünüdür.

Uluslararası alanda devletler arasında barışı ve güvenliği sağlama ve ortaya çıkabilecek sorunları barışçıl yollarla çözüme kavuşturma amacıyla kurulmuş olan ilk uluslararası örgüt ise 1920 yılında İsviçre’de kurulan Milletler Cemiyetidir (Polat,2020:1950-1967). Daha sonra 1922 yılında Milletler Cemiyeti sözleşmesi çerçevesinde PCIJ (Daimi Uluslararası Adalet Divanı) kurulmuştur. Uluslararası alanda genel yargı yetkisine sahip olan ilk mahkeme olma özelliğine sahip olan PCIJ, Uluslararası Adalet Divanının öncülü olma özelliğine de sahiptir.

Ancak Milletler Cemiyeti girişiminin başarısız olması ve kuruluş anlaşmasında devletler arasında çıkabilecek bir sorunda savaş seçeneğinin yasaklanmamış olması nedeniyle devletler arasında çıkabilecek sorunları savaş seçeneği olmadan çözüme kavuşturacak bir anlaşma yapılması zorunluluğu doğmuştur. Neticede Birinci Dünya savaşından sonra 1928 yılında imzalanan Briand Kellog Paktı devletler arasındaki ilişkilerde savaşı bir seçenek olmaktan çıkarsa da bazı ülkelerin antlaşmaya çekince koyması ve antlaşma hükümlerinin bir teamül hukuku olarak görülmemiş olması devletlerin istediklerini elde etmek için savaşmak ve saldırmaktan geri durmayacağını göstermiştir. Nitekim 1939 yılında patlak veren ve ilkinden çok daha büyük yıkımlara ve kayıplara neden olan İkinci Dünya savaşı da bunu kanıtlamıştır.

Savaş sonrasında devletleri uluslararası alanda yaşadıkları anlaşmazlıkları savaşa varmadan çözüme kavuşturmaya zorlayacak, bir devleti diğer bir devlete saldırmaktan, uluslararası alanda sağlanan barış ve huzur ortamını bozmaktan alıkoyacak caydırıcı önlemlerin alınması ve bağlayıcı hukuk kurallarının oluşturulması zorunluluk haline gelmiştir. Bu nedenle öncelikle uluslararası alanda barışı ve huzur ortamını tesis edip koruyacak uluslararası bir örgüt kurulması kararlaştırılmıştır. Birleşmiş Milletler örgütünün kurulması da bu ihtiyaç neticesinde olmuştur.

Örgütün kurucu antlaşması 1945 yılında San Francisco’da imzalanarak yürürlüğe girmiştir. Antlaşmanın özellikle 2/1. ve 2/4. Maddeleri zamanla öncelikle Yapılageliş kuralı (Teamül hukuk kuralı) olarak daha sonra ise, uluslararası hukukta jus cogens olarak tabir edilen emredici kural olarak kabul edilmeleri sebebiyle birliğe üye olmayan devletler için de bağlayıcı hale gelmiştir.

İlgili maddelerde bulunan hükümler şu şekildedir. BM kurucu antlaşması 2/1. Madde: “*Örgüt, üyelerinin egemen eşitliği ilkesine dayanmaktadır*” şeklindedir (Öztürk, 2017:37-53). BM 2/4. madde ise : “ *Tüm üyeler uluslararası ilişkilerinde herhangi bir devletin siyasi bağımsızlığına veya toprak bütünlüğüne karşı Birleşmiş Milletlerin amaçlarıyla bağdaşmayan herhangi bir şekilde kuvvet kullanımı tehdidinden veya kuvvet kullanımından kaçınacaklardır*” şeklinde ifade edilmiştir (BM Antlaşması, 1948: madde 2/4).

Gene 1945 yılında BM'ye bağlı olarak, devletler arasındaki anlaşmazlıkların hukuki yollardan çözülmesi ve uluslararası alanda usulsüz davranışlarda bulunan devletlerin hukuk karşısında yargılanması amacıyla Uluslararası Adalet Divanı Kurulmuştur. Divan 1946 yılında çalışmaya başlamıştır.

Ardından 2/4. maddedeki kuvvet kullanımı ifadesini ve BM antlaşmasının 51.maddesinde bahsi geçen silahlı saldırı ifadesinden neyin kastedildiğini, hangi saldırı türünün silahlı saldırı ve kuvvet kullanımı olarak değerlendirileceğini açıklığa kavuşturmak amacıyla 1974 yılında BM Genel Kurulu tarafından kabul edilen 3314 sayılı saldırının (Tecavüzün) tanımı isimli karar yürürlüğe girmiştir. İlgili kararda silahlı saldırının tanımı madde 2'de ve özellikle madde 3'te ayrıntılı olarak yapılmıştır. Kararın 2.Maddesinde: " *Bir devletin BM Antlaşmasına aykırı şekilde ilk kez silahlı kuvvet kullanması bir saldırı fiilinin prima facie kanıtı⁸ teşkil etmektedir. Ancak Güvenlik Konseyi, BM Antlaşmasına uygun şekilde bir saldırı fiilinin işlenmiş olduğu konusundaki bir tespitin, söz konusu fiillerin veya sonuçlarının yeterli ağırlıkta olmaması da dahil olmak üzere diğer ilgili şartlar ışığında haklı olamayacağı sonucuna varabilir*" ifadesi geçmektedir (BM Genel Kurulu 3314 sayılı karar, 1974: madde 2 https://inhak.adalet.gov.tr/Resimler/Dokuman/2312020095336bm_31.pdf 18.01.2025).

Kararın 3.maddesinde ve alt maddelerinde : Silahlı saldırının tanımı, "*Savaş ilan edilmiş olsa da olmasa da aşağıdaki fiillerin herhangi birisi 2'inci madde hükümlerine tabi ve ona uygun şekilde bir saldırı fiili niteliği taşır. a) Bir devletin silahlı kuvvetlerinin başka bir devleti istila etmesi veya ona hücum etmesi veya böyle bir istiladan veya hücumdan ileri gelen herhangi bir işgal ya da kuvvet yoluyla başka bir devletin ülkesinin veya bir bölümünün ilhakı b) Bir devletin silahlı kuvvetlerinin, başka bir devletin ülkesini bombardıman etmesi veya bir devletin başka bir devletin ülkesine karşı herhangi bir şekilde silah kullanması c) Bir devletin liman veya kıyılarının başka bir devletin silahlı kuvvetleri tarafından abluka altına alınması d) Bir Devletin silahlı kuvvetleriyle başka bir Devletin kara, deniz veya hava kuvvetlerine veya deniz veya hava filolarına saldırması*

⁸ Prima facie kanıt: Olayın ilk gerçekleştiği anda elde edilen delillerin değerlendirilmesi, hakimin bu ilk delillere göre karar vermesi anlamına gelmektedir. Keser, L. (2001) İlk Görünüş İspatı. Dokuz Eylül Üniversitesi Hukuk Fakültesi, İzmir. 1.Basım. ss.231-252 <https://hukuk.deu.edu.tr/wp-content/uploads/2020/01/L.Keser-13.pdf> 18.01.2025

e) Bir devletin başka bir devletle son yaptığı anlaşmaya göre o ülkede bulunan silahlı kuvvetlerinin anlaşmaya aykırı olacak şekilde ya da anlaşma süresi dolduktan sonra da varlığını sürdürmesi f) Ülkesini başka bir devletin emrine veren bir devletin, ülkesinin o devlet tarafından üçüncü bir devlete karşı saldırı amacıyla kullanılmasına izin vermesi g) Bir devlet tarafından ya da o devlet adına yukarıda sayılan fiillere varan veya bu ölçekte olan silahlı kuvvet fiillerini icra eden gayri nizami askerlerin veya paralı askerlerin, silahlı çetelerin veya grupların gönderilmesi" şeklinde yapılmıştır (BM Genel Kurulu 3314 sayılı karar, 1974: madde 3 https://inhak.adalet.gov.tr/Resimler/Dokuman/2312020095336bm_31.pdf 18.01.2025).

Bununla birlikte aynı kararın 4.maddesinde: "İlgili hükümlerin tüketici olmadığı ve Güvenlik Konseyi, BM Antlaşması hükümlerine göre başka fiillerin de saldırı olarak kabul edilebileceğini belirtir" ifadesi bulunmaktadır. Böylece silahlı saldırı tanımı yapılırken keskin bir çerçeve çizilmemiş silahlı saldırı niteliğinde olabilecek başka fiillerin de bu minvalde değerlendirilebileceğine ilişkin beyanda bulunulmuştur.

Esasında yukarıda bahsedilen 3.maddedin b bendinde de "Bir devletin başka bir devletin ülkesine karşı herhangi bir şekilde silah kullanması" ifadesine yer verilmiştir. Görüldüğü gibi burada da silahın türü belirtilmemiştir.

Saldırı ile ilgili bir başka hüküm de Uluslararası Ceza Mahkemesi Roma Statüsü⁹ Madde 8/4'te Saldırı suçu (Crime of Aggression) başlığı altında bulunmaktadır. Buradaki hükümde, BM Genel kurulunun 1974 tarihli ve 3314 sayılı kararındaki silahlı saldırı tanımına atıfta bulunulmuştur. Başlangıçta Mahkemenin yetki alanına giren suçlar yalnızca Soykırım Suçu, İnsanlığa Karşı Suçlar ve Savaş Suçlarıdır. Saldırı suçu ise statünün 5.maddesinde belirtildiği üzere statünün yürürlüğe girmesinden 7 yıl sonra, ilgili suçun tanımının yapılması ve bu tanımın BM Şartında belirtilen tanımla uyumlu

⁹ UCM Roma Statüsü : Uluslararası ceza mahkemesinin kurulması talebi insanlığa karşı suçların ve barışa karşı işlenen suçların incelenmesi amacıyla BM Genel Kurulu tarafından Uluslararası Hukuk Komisyonuna iletilmiştir. Daha sonrasında uygun görülen bu teklif üzerine kurulması planlanan Uluslararası Ceza Mahkemesinin kuruluş antlaşması olan Roma Statüsü yazılıp onaya sunulurken 17 Temmuz 1998 yılında imzaya açılmış. Roma statüsünün 60. Onay belgesinin imzalanmasını müteakiben 60 gün sonra 2002 yılında statü yürürlüğe girmiş ve neticede Uluslararası Ceza Mahkemesi 11 Temmuz 2002'de faaliyete geçmiştir. https://diabgm.adalet.gov.tr/Home/SayfaDetay/uluslararasi-ceza-mahkemesi-ucm28022020101834_19.01.2025

olması şartı ile mahkemenin yetki alanına girmiştir https://diabgm.adalet.gov.tr/Home/SayfaDetay/uluslararasi-ceza-mahkemesi-ucm28022020101834_19.01.2025). Ancak sonradan yetkilendirilmiş olsa da Roma Statüsünde Saldırı suçu ile ilgili atıf yapılmış olması oldukça önemlidir.

Saldırı suçu ile ilgili bu antlaşma hükümlerinin yanısıra, Uluslararası Hukuk Komisyonu tarafından 2001 yılında yapılan 53. oturumuda düzenlenerek BM Genel Kuruluna taslak metin olarak sunulan Devletlerin Uluslararası Hukuka Aykırı Fillerinden Doğan Sorumlulukları (ARSIWA)¹⁰ isimli belgede de saldırı suçu ile ilgili benzer ifadeler vardır. Burada uluslararası hukuka aykırı davranışlardan kastedilen de barışa karşı işlenen suçlardır (Topal, 2015:481-508). Bu belge henüz yürürlüğe girmemiş taslak bir metin olsa da devletlerin haksız fiillerinden dolayı sorumlulukları ile ilgili düzenlenen bir belge de saldırı suçu ve 6.bölümde değinilecek olan atıf konusunun ele alınmış olması, bu konularda fikir vermesi açısından önemlidir.

Bağlayıcı olmasa da bu belgede de değinildiği gibi bir devletin bir başka devlete karşı giriştiği bir silahlı saldırı neticesinde uluslararası alanda tesis edilen barış ve huzur ortamı bozulacağından saldırgan devlet uluslararası alanda barışı ve huzuru tesis etmek amacıyla koyulan kuralları çiğnemiş olacaktır. Bu da devletin haksız fiilinden dolayı sorumluluklarını doğurur.

Bu kuralların tümü uluslararası alanda barışın ve huzurun tesis edilmesi ve korunması için silahlı saldırıları ya da kuvvet kullanımını engellemek amacıyla koyulmuş kurallardır. Ancak bu kuralların siber uzay ve siber saldırılar hususunda nasıl uygulanacağı ile ilgili pek çok soru işareti mevcuttur ve halen bunların hepsi yanıtlanabilmiş değildir.

Bunlardan en basiti siber saldırılarda kullanılan zararlı yazılımların ya da geliştirilmiş özel bir virüsün veyahut da DoS ve DdoS atakları ile bir devletin bankacılık sistemine saldırıp sistemi işlemez hale getirmenin BM Şartı 2/4.maddede bahsedilen kuvvet

¹⁰ ARSIWA: Devletlerin Uluslararası Hukuka Aykırı Fillerinden Doğan Sorumluluğu. Birleşmiş Milletler Genel Kurulu A/RES/56/83, 28 Ocak 2002 (Altıncı Komite raporu üzerine (A/56/589 and Corr.1)) https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf 18.01.2025

kullanımı kapsamına girip girmediği ya da gene BM Şartı. 51. Maddede bahsi geçen silahlı saldırı ifadesindeki saldırı silahı olarak nitelendirilip nitelendirilemeyeceğidir.

Bir diğer soru da hangi ölçekte bir siber saldırının silahlı saldırı olarak nitelendirileceği hususudur. Bu tartışmalar neredeyse siber uzay kavramının ortaya çıkışından beri devam etmektedir. Bazı uzmanlar ilgili hükümlerde bahsi geçen silahlı saldırı ifadesinin yalnızca konvansiyonel anlamda yapılacak bir saldırı için geçerli olduğunu ifade etse de artık pek çok uzman 21.yy'ın teknolojik gelişmeleri neticesinde bilgisayarlar ve yazılım programları aracılığıyla üretilen zararlı yazılımların bir silah gibi kullanıldığını ve neticede silahlı saldırı ve kuvvet kullanımı ile ilgili hükümlerin bu yolla yapılan saldırıları da kapsayacağını ifade etmektedir (Temel,2021: 122-158).

Özellikle 18 Eylül 2024 tarihinde, İsrail tarafından Lübnan'da gerçekleştirilen ve aralarında çocukların da olduğu 37 kişinin ölümüne ve 2500 kişinin yaralanmasına sebep olan katliam gibi siber saldırı, siber saldırıların silahlı saldırı olarak görülüp görülmeyeceği ve siber saldırıların şiddetinin, konvansiyonel yöntemlerle yapılan saldırılara eşit olup olmayacağı konusundaki tüm sorulara bir cevap niteliğindedir esasen.

Kaldı ki, yapılan siber saldırının şiddeti bu boyutta olmasa bile, esas sorun kuvvet kullanımı ve neticesinde barış ve huzur ortamının bozulması ise bu bir devletin başka bir devletin kritik altyapı sistemlerine, bankacılık sistemlerine, hava kontrol ve takip sistemlerine, akıllı trafik kontrol sistemlerine, ulaşım sistemlerinin kontrol ünitelerine, evlerimizde kullandığımız akıllı cihazlara ya da İran örneğinde olduğu gibi nükleer tesislerin kontrol ünitelerine (SCADA sistemlerine) zararlı yazılımların ve virüslerin bir silah gibi kullanılarak saldırılması neticesinde de gerçekleşebilir.

Ya da 2007 yılında yapılan Estonya siber saldırısında olduğu gibi bir ay boyunca ülkenin tüm kamu dairelerini, bankacılık sistemlerini, hastane randevu sistemlerini DDoS saldırılarına maruz bırakarak halk arasında kaos oluşmasına, çok büyük maddi zararlara ve hatta kamunun zarar görmesine sebep olan bir saldırı da bir devletin bir başka devlete karşı kuvvet kullanımı olarak değerlendirilebilir (Değdaş, 2018:21-40). Üstelik örnek gösterilen tüm bu siber saldırılar sadece kuvvet kullanımı kuralını değil egemenliğe müdahale etmeme ilkesini ve zarar vermeme ilkesini de çiğnemiştir.

Bir başka soru işareti hatta üzerinde en çok tartışılan konulardan biri de henüz siber uzay ve siber saldırı kavramları ortaya çıkmadan çok önceleri hazırlanmış olan bu hükümlerin siber uzay ve siber saldırılar konusunda uygulanabilir olup olmadığıdır ve uygulanabilir ise nasıl uygulanacaktır.

4.2.Tallinn Rehberi ve Siber Saldırıları Konusundaki Önerileri

2007 yılında Estonya'nın maruz kaldığı siber saldırılar sonrasında, saldırı fiili ile ilgili mevcut uluslararası hukuk kurallarının Estonya'ya karşı gerçekleştirilen saldırıya uygulanıp uygulanamayacağı ya da nasıl uygulanabileceği konusunda tartışmalar yaşanmıştır. Daha sonra Estonya'nın başkenti Tallinn'de NATO tarafından kurulmuş olan NATO Siber Savunma Mükemmeliyet Merkezi (CCD COE) tarafından siber uzay ve siber saldırılar konusunda başvurulabilecek yol gösterici bir kaynak oluşturulması amacıyla farklı üniversitelerden bağımsız Uluslararası Hukuk Uzmanları merkezde bir araya getirilmiştir. İlgili uzmanların uzun süren çalışmaları neticesinde Tallinn Rehberi 1.0, 2013 yılında Uluslararası Hukuk Kurallarının Siber Saldırıları Uygulanması başlığı altında yayınlanmıştır.

Bu rehber, hukuki olarak bağlayıcı olmasa da UAD tarafından yardımcı kaynak olarak başvuru bir rehber olması açısından oldukça önemlidir. Daha sonra ilk yayınlanan rehber üzerinde yapılan bazı revize ve eklemeler neticesinde 2017 yılında Tallinn Rehberi 2.0 gene aynı uzman grubu tarafından hazırlanmış ve gene Cambridge Üniversitesi Yayınları tarafından yayınlanmıştır.

İlgili rehberde Uluslararası Hukuk Kurallarının siber uzay ve siber saldırılar konusunda nasıl uygulanabileceği, konuyla ilgili eksikliklerin nasıl giderilebileceği, Uluslararası hukukta bu konuyla ilgili hangi düzenlemelerin yapılabileceği gibi konular yer almaktadır.

Örneğin Tallinn Rehberi Bölüm 2'de UAD tarafından *“BM Şartı 2/4.madde ve 51. Maddede bahsi geçen kuvvet kullanımı /silahlı saldırı kavramlarına vurgu yapılmış ve*

kullanılan silah farketmeksizin kuvvet kullanımı yasaklanmıştır” ifadesine yer verilmiştir (Schmit vd.2013:1-215).

Bölüm 2 Kural 1/1’de: *“Hiçbir devlet siber uzay üzerinde egemenlik iddiasında bulunamaz ancak her devlet kendi ülkesi içerisinde bulunan siber altyapılar ve bunlarla ilgili faaliyetler üzerinde hakimiyet sahibidir”* ilkesi yer almaktadır (Schmit vd.2013:1-215).

Kural 1/3 ‘de: *“Bir devlete kendi toprakları üzerindeki siber altyapıyı ve siber faaliyetleri kontrol etme hakkını veren toprakları üzerinde sahip olduğu egemenlik hakkıdır”* ifadesi bulunur (Schmit vd. 2013: 1-215).

Gene Tallinn Rehberi Bölüm 2/1, Kural 10’da: *“Herhangi bir devletin toprak bütünlüğüne veya siyasi bağımsızlığına karşı tehdit oluşturan veya herhangi bir şekilde BM’nin amaçlarıyla bağdaşmayan bir siber operasyon yasa dışıdır”* ifadesi yer almaktadır (Lale,2020:10-23).

Kural 10/4’te *“Güç kullanımı olarak nitelendirilen bir eylemin muhakkak bir devletin silahlı kuvvetleri tarafından gerçekleştirilmesi gerekmez”* ifadesi yer almaktadır. (Schmit vd. 2013: 1-215). Yani bir devletin istihbarat teşkilatı veya siber olaylardan sorumlu ekibi ya da bilgisayar uzmanları gibi devlet tarafından yetki verilen kişilerce ilgili maddenin ihlal edilmesi neticesinde de bu fiil kuvvet kullanımı olarak nitelendirilir ve devlete atfedilir.

Kural 10/6 da geçen ifadede ise: *“Siber saldırı kuvvet kullanımı ölçüsüne ulaşmasa da müdahale etmeme yasağını çiğnemiş olabilir”* ifadesi yer almaktadır .

BM Genel Kurul kararları içerisinde en önemlilerden biri olan Devletler Arasında Dostça ilişkiler ve İşbirliğine İlişkin Uluslararası Hukuk İlkeleri konusundaki bildiride de müdahale etmeme ilkesine vurgu yapılmıştır. Kararda: *“Devletlerin uluslararası ilişkilerinde herhangi bir devletin siyasi bağımsızlığına karşı ya da ülke bütünlüğü aleyhine askeri, siyasi, ekonomik yada başka bir zorlamadan uzak durulması görevini anımsayarak”* ifadesi yer almaktadır (BMGK,1970:https://inhak.adalet.gov.tr/Resimler/Dokuman/2312020094506bm_17.pdf 02.02.2025).

Uluslararası adalet divanı da müdahale etmeme ilkesini Uluslararası Teamül hukukunun vazgeçilmez bir ilkesi olarak tanımlamıştır.

Tallinn Rehberi Bölüm 2/ 1 Kural 11’de ise : “*BM şartı bir eylemin ne zaman güç kullanımı anlamına gelenceğini belirlemek için bir ölçü belirlememiştir. Bu nedenle güç kullanımı ile ilgili uygun eşik değer bulma hususunda Uzmanlar grubu UAD’ın Nikaragua kararını dikkate almıştır. Bu kararda UAD bir eylemin silahlı saldırı olarak görülüp görülmeyeceğini belirlerken saldırının ‘ölçü ve etkilerinin’ dikkate alınması gerektiğini belirtmiştir*” ifadesi yer almaktadır (Yılmaz ve Irk, 2015 ve Beyoğlu, 2016). Yani eğer siber saldırı ölçü ve etkileri bakımından bir silahlı saldırının verdiği zararı vermişse bu saldırı da silahlı saldırı olarak değerlendirilecek ve mağdur devlete meşru müdafaa hakkı tanıyacaktır.

Bölüm 2 Kural 5/2’de: “*Egemen eşitlik ilkesi gereği tüm devletlerin diğer devletlerin toprak egemenliğine saygı duyma yükümlülüğü vardır*” ifadesi yer almaktadır (Schmit vd. 2013: 1-215). Adalet Divanının Nikaragua kararında belirtildiği gibi ‘*bağımsız devletler arasında bölgesel egemenliğe saygı, uluslararası ilişkilerin temel bir ilkesidir*’ ifadesi bulunur (Bilge,1955:228-242).

Kural 5/3’te: Uluslararası Adalet Divanının Korfu Kanalı davasında vermiş olduğu kararda belirtildiği gibi “*Başka bir devletin egemenliğine saygı duyma yükümlülüğü bir devletin kendi topraklarını diğer devletlerin haklarına aykırı eylemler için kullanılmasına bilerek izin vermeyeceği anlamına gelir*” ifadesi yer almaktadır (Yılmaz ve Irk, 2015 ; Beyoğlu 2016).

Kural 11/8 içerisinde geçen ifade de ise: “*Kişilerin yaralanmasına ya da ölümüne sebep olan veya nesnelere zarar veren onları yok eden eylemler açıkça güç kullanımıdır*” denilmiştir (Schmit vd. 2013: 1-215).

Rehberde ayrıca bir siber saldırının sorumlusunun belirlenmesinde Alan adının oldukça görünür bir belirteç olduğu, her devletin belli bir alan adı olduğu ve eğer detaylı bir inceleme ve iyi bir araştırma yapılırsa saldırının failinin tespit edilebileceği ifadesine yer verilmiştir (Schmit vd. 2013: 1-215).

Domain olarak da bilinen alan adı bir web sitesinin internet sitesi üzerindeki adı ve adresidir. Örneğin google.com veya youtube.com gibi. Bu adresler aynı zamanda

rakamlardan oluşan "216.58.216.164" benzeri bir IP adresine denk gelirler. Ancak internete girerken bu kadar uzun rakamlar serisinden oluşan bir adres yerine buna eşdeğer gelen alan adını ezberlemek çok daha basittir (<https://www.natro.com/blog/yeni-baslayanlar-icin-domain-nedir/09.10.2024>).

Ülkelerin domainleri ise Ülke Kodu Üst Düzey Alan Adı (Country Code Top Level Domain) olarak adlandırılan bir sistemle belirlenir. Bu sistemde her ülkenin domaini iki harfle temsil edilmektedir. Örneğin com.tr, com.de veya com.us gibi (burada -de Almanya'nın , -us Amerika'nın, -tr de Türkiye'nin alan kodudur) (https://www.atakdomain.com/blog/ulke-domain-uzantilari_09.10.2024).

Tallinn Rehberini hazırlayan uzmanlar grubu, bu konuda iyi bir araştırma yapılması durumunda saldırının gerçekleştirildiği IP adresine ulaşılabilirliğini ve dolayısıyla saldırının nereden kaynaklandığının bulunabilirliğini öne sürmüşlerdir.

Görüldüğü gibi, Tallinn rehberi siber saldırılar hususunda Uluslararası hukukta var olan mevcut ilkelerin siber saldırılara nasıl uygulanabileceği ile ilgili yol gösterici nitelikte ve tavsiyeler içeren bir kaynaktır. Ancak hukuki açıdan bağlayıcı nitelikte olmaması siber saldırılar konusunda ayrıca bağlayıcı hukuki önlemler alınmasını zorunlu kılmaktadır.

5.BÖLÜM

Uluslararası Örgütlerin Siber Uzay ve Siber Güvenlik ile ilgili Çalışmaları

5.1. BM, AB ve NATO'nun Siber uzay ve siber güvenlik ile ilgili çalışmaları

5.1.1. Birleşmiş Milletlerin Siber Uzay ve Siber Güvenlik ile İlgili Çalışmaları

Siber güvenlik konusu Birleşmiş Milletler ajandasına ilk olarak Rusya tarafından 1998’ de sunulan taslak metin sonrasında girmiştir (<https://disarmament.unoda.org/ict-security/> 10.07.2024). BM Siber Güvenlik hususundaki ilk çalışmalarını 1998 yılında yapmaya başlamış ve BM Genel Kurulu bu konudaki ilk kararını da gene aynı yıl (A/RES/53/70) sayılı karar ile almıştır (Akdağ, 2020). Alınan bu kararın temelinde de 1996 yılında Afrika’da yapılmış olan Bilgi Toplumu ve Gelişimi konusunda yapılan toplantı ve gene aynı yıl içerisinde Paris’te gerçekleştirilen terörizm konulu konferans vardır.

BM Paris Toplantısı sonrasında birliğe üye olan ülkeleri bilgi sistemlerinin güvenliği konusunda dikkatli olmaları ve önlem almaları yönünde uyarmıştır. BM, 1998 yılı itibarıyla her sene siber güvenlik konusunda düzenli olarak toplantı ve konferanslar düzenleyerek üye ülkeleri bu konu hakkında gerekli tedbirleri almaları hususunda uyarmıştır.

BM Tarafından 2018 yılında Ortak Geleceğimizin Güvenliği için Silahsızlanma başlığı altında 30. ve 31. maddeler oluşturulmuştur (Akdağ, 2020). Bunlar Siber alanın güvenli hale getirilmesi, üye devletlerin konu ile ilgili alınan kararları etkin bir şekilde uygulayarak siber alanın güvenliğine katkıda bulunması ile ilgilidir.

Birleşmiş Milletler 2000’ li yıllarla birlikte siber uzayın ve bu alandan kaynaklanan saldırıların insanlık için tehlikeli boyutlara ulaşabileceğini görmüş, hem kuruluş içerisinde hem de üye ülkelerin kendi orduları içerisinde siber güvenlik konusunda yapılanmaya gidilmesi gerektiğini vurgulamıştır. Daha sonrasında uluslararası güvenliğin sağlanması için devletlerin siber uzaydaki davranışlarını denetleyecek ve düzenleyecek

bir uzmanlar grubu olan Hükümet Uzmanları Grubu (Group of Governmental Expert) kurulmasına karar verilmiştir (<https://disarmament.unoda.org/ict-security/> 30.08.2024). Yirmi beş uzmandan oluşan bu grup ilk toplantısını 2019 yılında yapmış , siber güvenlik ile ilgili ilk raporunu da 2021 yılında yayınlamıştır.

BM bünyesi içerisinde kurulan bir diğer grup da OEWG' dir. (2018) Üye ülkelerin iş çevrelerini, hükümet dışı kuruluşlarını siber tehditler konusunda bilgilendirmek amacıyla kurulan bu grup (Open-Ended Working Group-Açık Uçlu Çalışma Grubu), GGE ile birlikte UNIDIR¹¹ çatısı altında bulunmaktadır. Siber Güvenlik ile ilgili kuruluşların UNIDIR çatısı altında kurulmasının nedeni kötü amaçlı yazılımların bir silah/saldırı aracı olarak kullanılmasının önüne geçmektir.

2020 yılında OEWG' nin çalışma tanımı ve konusu genişletilmiş görev süresi ise beş yıla çıkarılmıştır. Ayrıca 2020 Aralık ayında Siber Güvenlik ve Yeni Teknolojilere ilişkin Küresel Terörizm ile Mücadele Programı oluşturulmuştur. Programın amacı üye ülkelerin, Uluslararası ve bölgesel kuruluşların ve BM kuruluşlarının teröristler tarafından gerçekleştirilen siber tehditler konusundaki bilincini artırma ve ilgili tehditler hususundaki teknik kapasitelerini geliştirmektir. Genel Kurul tarafından 2021, 2022 ve 2023 yıllarında sırasıyla A/RES/76/19, A/RES/77/36 ve 77/37 ve A/RES/78/237 Sayılı kararlar yayınlanmıştır. Bu kararlar genel olarak bilgi ve telekomünikasyon alanındaki gelişmelerin uluslararası güvenlik açısından değerlendirilmesi ve bunlarla ilgili eylem alınması yönündedir (<https://disarmament.unoda.org/ict-security/> 24.01.2025).

Bir yandan bu raporlar düzenli olarak yayınlanırken bir yandan da BM bünyesinde Bilgi ve İletişim Teknolojilerinin Suç Amaçlı Kullanımına Karşı Kapsamlı Bir Uluslararası Sözleşme Hazırlanması için bir Ad Hoc Komitesi kurulmuştur. Bu komite ayrıca Genel Kurul tarafından, Taraf Devletler Konferansı için taslak usul kurallarını hazırlamak ve Sözleşmeye ek olarak, gerektiğinde ek suçları da ele alan bir taslak protokol müzakere etmek üzere oturumlar düzenlemekle görevlendirilmiştir. Sonuç olarak beş yıllık bir çalışmanın neticesinde 2024 yılında BM Üye Devletleri tarafından görevlendirilen sivil

¹¹ UNIDIR : BM Silahsızlanma Araştırmaları Enstitüsü. 1980 Yılında BM bünyesinde kurulmuş olan örgütün merkezi İsviçre'dedir. Daha barışçıl ve daha güvenli bir dünya için silahsızlanma çalışmalarını yürütmek üzerine kurulmuştur. <https://www.ungeneva.org/en/about/organizations/unidir> 06.12.2024

toplum kuruluşlarının, bilgi güvenliği uzmanlarının, akademisyenlerin ve özel sektörün ortak katkılarıyla Siber Suç Sözleşmesi oluşturulmuştur(<https://news.un.org/en/story/2024/12/1158521> 24.01.2025). Sözleşmede, bilgi ve iletişim teknolojilerinin (BİT) kötüye kullanılması, bu yolla işlenen insan ticareti, uyuşturucu kaçakçılığı ve çevrimiçi mali suçlar gibi suçların benzeri görülmemiş bir ölçekte, hızda ve kapsamda artması ve bunun neticesinde oluşan riskler ele alınarak bu risklerin Devletlerin, işletmelerin, bireylerin ve toplumun refahı üzerinde yaratabileceği olumsuz etkileri vurgulanmıştır ve bu tür suçlara karşı uygulanması gereken yaptırımlar ele alınmıştır. Siber Suç Sözleşmesi'nin 2025'de Vietnam'da imzaya açılması kararlaştırılmıştır. Sözleşmenin Uluslararası hukuk kuralı olarak kabul edilmesinin ise 40 üye devletin sözleşmeyi imzalamasının ardından geçen 90 günün sonunda olacağı belirtilmektedir(<https://news.un.org/en/story/2024/12/1158521> 24.01.2025).

Uluslararası alanda bağlayıcılığı olabilecek böyle bir siber suç sözleşmesinin Birleşmiş Milletler tarafından düzenlenmiş olması önemli bir gelişmedir. Ancak sözleşmenin çerçevesinin devletler tarafından gerçekleştirilen siber saldırıları kapsamaması önemli bir eksikliktir.

Genel olarak siber güvenlik ile ilgili çalışmalarını terörizm ve bilgi teknolojilerinin teröristler tarafından ideolojilerini yayma amacıyla kullanılmasını önlemek üzerine yoğunlaştıran Birleşmiş Milletlerin siber uzay konusundaki çalışmalarının en büyük eksikliği tehlikenin boyutlarını tam olarak anlaşılmamış olması ve daha çok teröristlere ve terörizme odaklanmış olmalarıdır.

5.1.2. AB'nin Siber Uzay ve Siber Güvenlik İle İlgili Çalışmaları

Avrupa Birliği'nin siber güvenlik konusundaki girişimleri 1994 yılında yayınlamış olduğu Bengemann Raporu ile başlamıştır (Köksoy, 2020:635-674). Bu rapor AB'nin siber güvenlik politikası açısından önemli bir belgedir. Raporda ele alınan hususlar arasında internet Korsanlığı ile mücadele ve Avrupa Birliği'nin sosyal ve ekonomik gelişim sürecinde BTK'nın önemi gibi maddeler bulunmaktadır.

Siber uzay ve siber saldırıların ilk kez ayrıntılı olarak ele alındığı, bu konuda gerekli önlemlerin alınması ve güvenliğin artırılması için somut çözümler ortaya koyan, ağ ve

bilgi güvenliği konusunda net tanımlamalar yapan İnternetin Yasal Olmayan ve Zararlı İçeriğine İlişkin Belgeyi ise 1996’ da yayınlamıştır.

Daha sonra 2001 yılında NIS Proposal (Ağ ve Bilgi Güvenliği ile İlgili Öneri) 2002 yılında Elektronik Haberleşme Sektöründe Gizliliğin Korunması Direktifini yayınlamış 2004 yılında ise AB için siber güvenlik konularında çok önemli bir birim olan ENISA’yı (Avrupa Birliği Siber Güvenlik Ajansı) kurmuştur (Köksoy, 2020).

2005 yılında AB üye ülkelerine karşı gerçekleştirilen ya da gerçekleştirilmesi planlanan siber saldırıların önlenmesi ve bu saldırılara karşı cezaların artırılması hususunda bir çerçeve karar yayınlamıştır (Köker, 2022:48-77). 2006’da Verilerin Saklanması Direktifi ve Güvenli Bilgi Toplumu için Strateji Belgesi yayınlanmış, 2012’de ise AB Bilgisayar Acil Müdahale Ekibi kurulmuştur.

2013 yılında hem Avrupa Siber Suç Merkezi kurulmuş hem de Siber Güvenlik Strateji Belgesi oluşturulmuştur. Belge de, OGSP (Ortak Güvenlik ve Savunma Politikası)¹² aracılığıyla Siber Savunma Politikasının ve Kapasitesinin Artırılması, Siber suçların azaltılması ve AB için etkili ve tutarlı bir siber güvenlik politikasının oluşturulması konularına değinilmiştir. 2016 yılında çıkarılan 2. NIS Direktifi ağ ve bilgi sistemlerini daha güvenli bir hale getirmeyi amaçlayan ve üye ülkeler arasında siber güvenlik konusundaki dayanışmayı artırmaya yönelik ilk yasal düzenlemedir (<https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new> 09.10.2024).

2019 yılında ise Siber Güvenlik Yasası çıkarılmıştır (<https://eur-lex.europa.eu/EN/legal-content/summary/the-eu-cybersecurity-act.html> 09.10.2024). Bu yasa AB içerisinde refahın ve gelişimin sürekli hale getirilebilmesi için bilgi güvenliğinin ve ağ sistemlerinin güvenliğinin mecburi olduğunu kesinleştirmiştir.

¹² OGSP : Ortak Güvenlik ve Savunma Politikası , Siber savunma ve siber güvenlik konusunda birlik içerisinde ortak hareket etmek için oluşturulmuştur. Köksoy, F. (2020) Avrupa Birliği’nin Siber Güvenlik Politikası: Kurumsalcılık mı Tutarlılık mı? Güv. Str. Derg. 2020, 16(35): 635-674

Avrupa Birliđi esasen tüm bunları üyeleri arasında oluřturmayı planladıđı Dijital Tek Pazar düşünceinin temelini sađlamlařtırmak ve AB vatandaşlarının refahını ve güvenliđini artırmak amacıyla yapmıřtır. Oluřturulması planlanan bu Dijital Tek Pazar, Avrupa Birliđi için üyeleri arasındaki ticaretin hızlandırılmasını ve geliřtirilmesini, ticaret hacminin artırılmasını sađlayacak bir yoldur. Ancak Dijital Pazar kurmanın bir geređi olarak üye ölkelerin ve AB'nin biliřim altyapısını siber saldırılardan korumak Avrupa Birliđi için bir zorunluluk haline gelmiřtir. O nedenle, Avrupa Birliđi siber uzay ve siber güvenlik konularında neredeyse her yıl bir düzenleme yapmıřtır. Fakat siber uzay ve siber güvenlik konularında yapılan bu anlařmalar ve kurulan birimler, duyurulan strateji belgeleri rehber olmaktan öteye gidememiř ve hedeflenen başarıya ulařamamıřtır (Köksoy, 2020 ve Köker, 2022).

Bunun nedenlerinden biri birlik içerisinde yeteri kadar kurumsallařmanın sađlanamamıř olmasıdır ki, esasen daha bařından, siber güvenlik terimi konusunda AB'ye üye ölkeler arasında net bir tanımın olmaması siber güvenlik konusunun çerçevesinin belirlenmesinde bir boşluk oluřturmuřtur (Köksoy, 2020: 635-674). Bir diğeri de birlik üyelerinin konu ile ilgili iřbirliđi yapmaya istekli olmamasıdır.

5.1.3.NATO'nun Siber Uzay ve Siber Güvenlik ile İlgili Çalışmaları

NATO esasen oldukça geliřmiř bir biliřim altyapısına sahiptir. Ancak 1998-1999 Kosova Savařı sürecinde Sırlar tarafından gerçekteřirilen siber saldırılar sebebiyle bu yeni nesil saldırı yöntemlerine karřı önlem alma ve bu konuda savunmasını etkin hale getirme zorunluluđu hissetmiřtir.

2002 yılında Prag'da gerçekteřirilen zirvenin -Yüksek Güvenlik Tehditleri Bölümünde Siber saldırılar, terörizm ve kitle imha silahları ile birlikte en yüksek güvenlik tehditleri arasında ele alınmıřtır (Polat,2020:144).

NATO, 2007 yılında müttefiki Estonya'ya karřı gerçekteřirilen ve neredeyse bir ay süren siber saldırılar neticesinde tehlikenin ciddiyetinin daha çok farkına varmıř ve daha ciddi önlemler alma ihtiyacı hissetmiřtir. Müttefikine gerektiđi gibi yardım edemeyen NATO saldırılar sonrasında benzer bir saldırının tekrar etmesi durumunda müřterek bir savunma

planı çerçevesinde hareket edilmesi için Brüksel’de CDMA’yı kurdu (Cyber Defence Management Authority - Siber Savunma Yönetimi Otoritesi) (Polat,2020:135-158).

Daha sonra da Estonya’nın başkenti Tallin’de siber uzay, siber güvenlik ve siber savunma ile ilgili kapasitesini artırmak ve siber güvenlik ve siber savunma konusunda yönetimi tek bir merkezde toplamak amacıyla NATO Müşterek Savunma Mükemmeliyet Merkezini (CCD COE) kurmuştur (Polat,2020:135-158).

NATO ülkeleri arasında bu merkez tarafından düzenlenen Locked Shields (Kilitli Kalkanlar) ismindeki devasa tatbikatlara tüm üye ülkelerden askeri uzmanlar, bilgisayar mühendisleri ve uzman yazılımcılar katılmaktadır (Polat, 2020).

Ayrıca 2013 yılında gene aynı merkez bünyesinde Uluslararası Hukuk Uzmanları tarafından Siber Uzay ve Siber Saldırıları konusunda yol gösterici hukuki düzenlemeleri içeren ve UAD tarafından ikincil kaynak olarak başvurulmuş Tallin Rehberi 1.0 oluşturulmuştur. Daha sonra 2017 yılında Tallin Rehberi 2.0 olarak güncellenip Cambridge Üniversitesi tarafından tekrar yayınlanmıştır.

Örgütün siber ağlarının güvenliğinin sağlanması için NATO tarafından Mons’da Shape karargahı içerisinde NATO Bilgisayar Olaylarına Müdahale Yeteneği Birimi oluşturulmuştur. Birim NATO’nun bilgi sistemlerini ve ağ yapısını 24 saat siber saldırılara karşı korumakla görevlendirilmiştir.

NATO’nun siber uzay ve siber savunma ile ilgili eğitimleri ise İtalya ve Almanya’da kurulan merkezlerde verilmektedir. Ayrıca 2018 yılında gerçekleştirilen Brüksel Zirvesinde 2023 yılında faaliyete geçirilmesi düşünülen Siber Operasyonlar Merkezinin kurulması kararlaştırılmıştır (Polat, 2020). NATO siber uzaydan kaynaklanan ve sürekli çeşitlenen tehditler karşısında hem birlik bünyesinde hem de üye ülkeler nezdinde saldırı ve savunma kapasitesini geliştirmeye ve güncel tutmaya büyük önem vermektedir. Ancak

NATO’nun siber güvenlik konusundaki tüm bu çabalarına rağmen üyeleri arasındaki dijital ve teknolojik gelişim farklılığı NATO’nun bir bütün halinde bu konuda hızlı bir şekilde ilerlemesine ve aksiyon almasına mani olmaktadır

5.1.4. NATO ve AB ‘nin Siber Uzay ve Siber Güvenlik ile İlgili birlikte yaptıkları çalışmalar

Ekonomik ve ticari amaçlarla kurulmuş olan Avrupa Birliği ve bir güvenlik örgütü olan NATO işleyiş ve kuruluş amaçları bakımından iki farklı kuruluştur. NATO askeri ve politik saiklerle kurulmuş bölgesel bir örgüttür ve buna göre dizayn edilmiştir. AB ise ekonomik ve ticari amaçlarla kurulmuş uluslararası bir örgüttür.

Esasen iki kuruluş arasındaki bu farklılıklar organize bir işbirliği neticesinde birbirlerini tamamlayıcı olarak kullanılabilecek olsa da söz konusu siber uzay ve siber güvenlik olunca iki örgütün de konuya farklı yaklaşması bu durumu zorlaştırmaktadır. Ancak 22 ortak üyeye sahip olmaları onları bu konularda da işbirliği yapmaya mecbur bırakmaktadır.

Özellikle 2007 yılında Estonya’ya karşı gerçekleştirilen siber saldırı iki örgüt için de siber tehditlerin boyutlarını ve konunun önemini anlamaları açısından oldukça etkili olmuştur (Kutlu,2023:25-41). Bu saldırı sonrasında her iki örgüt de kendi bünyeleri içerisinde siber güvenlik konusunda çalışmalar yürütmüş ve ilgili tehditlere müdahale etmeleri amacıyla bilgisayar uzmanlarından oluşan ekipler oluşturmuşlardır.

Bu ekiplerden özellikle NCIRC (NATO Bilgisayar Olaylarına Müdahale Yeteneği - NATO Computer Response Capability) ve CERT-EU (Avrupa Bilgisayar Güvenlik Olaylarına Müdahale Ekibi - Computer Security Incident Response Team of all the EU) siber güvenlik konusunda ortak çalışmalar yürütmektedirler (Kutlu,2023:25-41).

AB birlik bünyesinde görev yapan yazılım uzmanlarının ve bilgisayar uzmanlarının ,NATO tarafından düzenli olarak her yıl gerçekleştirilen siber güvenlik konusundaki tatbikatlara katılımını sağlamaktadır (Köksoy, 2020:635-674).

Ayrıca 2016 yılında NATO ve AB arasında siber güvenlik, siber savunma konularında işbirliğinin güçlendirilmesi, ortak eğitim ve tatbikatların sayısının artırılması yönünde yapılan görüşmeler sonrasında NATO tarafından dört rapor hazırlanmıştır. İlk olarak 2017 Haziran’da bir rapor yayınlanmıştır. Raporda siber uzay ve siber güvenlik konularında iki örgüt arasında yapılacak işbirliğinin ayrıntıları yedi farklı başlık altında ele alınmıştır.

İkinci rapor 2017 yılı Kasım ayında yayınlanmıştır. Raporda Avrupa’da bir siber savunma mükemmeliyet merkezi kurulması üzerinde durulmuş ve raporda bu fikrin ayrıntılarına yer verilmiştir.

Daha sonra 2018 Mayıs ayında ve son olarak 2019 yılının Haziran ayında iki rapor yayınlanmıştır. Son yayınlanan raporda konunun politik yönleri ve iki örgüt arasında siber güvenlik konusundaki politik müzakerelerin artırılmasına değinilmiştir (Kutlu,2023:25-41).

Ancak tüm bu çalışmalar başta da belirtildiği gibi iki örgüt arasındaki farklılıklar nedeniyle kesintiye uğramaktadır. Avrupa Birliği konuya yalnızca birlik üyesi vatandaşların ve birliğin ticari geleceğine dair planlanan Dijital Pazar’ın siber tehditlerden korunması yönünden yaklaşmaktadır (Köksoy,2020: 635-674). NATO ise konuya, örgüte üye ülkelerin siber güvenliğinin sağlanması, NATO’nun siber saldırılardan korunması ve NATO’nun siber uzay ve siber güvenlik konularında çalışmalarının artırılması açısından yaklaşmaktadır (Bıçakçı, 2014: 101-130).

Siber saldırılar ve siber güvenlik konusuna karşı bu farklı yaklaşım AB ve NATO’nun bu konularla ilgili işbirliği içerisinde çalışmasını zorlaştırmaktadır.

5.2. Avrupa Konseyi, Afrika Birliği ve OECD'nin Siber Güvenlik İle İlgili

Çalışmaları

5.2.1. Avrupa Konseyi'nin Siber Uzay ve Siber Güvenlik ile ilgili Çalışmaları

İkinci Dünya Savaşı sonrasında önemli maddi ve manevi kayıplar yaşamış olan Avrupa’da, Avrupalı halklar arasındaki çatışmaları ve kıtada devam eden gerginliği azaltıp, halkları ortak menfaatler etrafında toplamak amacıyla 1948 yılında hükümetleri temsilen bir istişare meclisi (Avrupa Konseyi Parleментар Meclisi) oluşturulmuştur. Daha sonra 1949 yılında Avrupa Komisyonunu kuran Londra Antlaşması 10 ülkenin katılımıyla imzalanmıştır (https://www.mfa.gov.tr/avrupa-konseyi_.tr.mfa 18.12.2024).

İnsan hakları konusunda Avrupa İnsan Hakları Sözleşmesi gibi çok önemli bir sözleşmeyi hazırlamış olan Avrupa Konseyi, siber güvenlik konusunda da çok önemli bir adım atarak

bu konuda yapılmış ilk sözleşmeyi 2001 yılında Budapeşte'de imzaya açmıştır. Budapeşte Sözleşmesi olarak da bilinen Avrupa Konseyi Siber Suçlar Sözleşmesi 2004 yılında yürürlüğe girmiştir (Ünver, Canbay ve Mirzaoglu, 2011:23). İnternet ve diğer bilgisayarlı araçlar aracılığıyla işlenen suçlara karşı uluslararası alanda atılan ilk ve en önemli adım olarak görülen bu sözleşmede daha çok Avrupa halklarının siber suçlara karşı korunması, internet aracılığıyla işlenen dolandırıcılık vb. faaliyetler ve internet aracılığıyla yapılan çocuk istismarı <https://www.bg.org.tr/Doc/AvrupaBirligiSiberSuclarSozlesmesi.doc> 18.09.2024) gibi konulara öncelik verilse de sözleşmenin içeriğinde bulunan, özellikle bilgisayar sistemlerine ve bu sistemlerde gizlenen verilere karşı girişilen yetkisiz erişim ve bilgisayarların ve internetin kötüye kullanılması konuları devletler tarafından gerçekleştirilen siber saldırılar hususunda da başvurulabilecek bir belge olması açısından önemlidir (Ünver, Canbay ve Mirzaoglu, 2011: 23-24).

Avrupa Konseyi Siber Suçlar Sözleşmesi, Avrupa Konseyi üyesi olmayan ülkelerin de katılımına açıktır. Ayrıca bu sözleşme, gerek özel sektörde gerekse kamu sektöründeki verilerin korunması bakımından kabul edilmiş olan Uluslararası hukukun ilk bağlayıcı sözleşmesi olma özelliğine de sahiptir (Ünver, Canbay ve Mirzaoglu, 2011:24).

5.2.2. Afrika Birliğinin Siber Uzay ve Siber Güvenlik ile ilgili Çalışmaları

Afrikanın sömürge olmaktan kurtulması sonrasında Afrika kıtasında bulunan devletler arasında bir birlik kurulması amacıyla Mayıs 1963'te 32 devlet yetkilisi, Afrikanın ilk kıtasal kurumu olan Afrika Birliği Örgütünü (OAU) kurmak üzere Etiyopya'nın başkenti Addis Ababa'da toplanmış ve birleşik, özgür ve kendi kaderini tayin eden bir Afrika için örgütü kuran tüzüğü imzalamışlardır (<https://au.int/en/overview> 20.01.2025).

Örgütün ana amacı Afrika halklarının özgürlük, eşitlik, adalet ve diğer meşru haklarının gerçekleştirilmesidir. Kökeninde ise Afrika'nın birliğine, kültürüne ve ortak mirasına odaklanan Pan Afrikanizm hayali vardır.

1999 yılında Afrika Birliği Örgütü devlet ve hükümet başkanları, örgütün rolünün artırılması, gelişen ve değişen koşullara daha hızlı uyum sağlanması, Afrika kıtasının küreselleşen dünyaya daha hızlı adapte olabilmesi ve kıtadaki diğer ülkelerin de birliğe

katılımının teşvik edilmesi amacıyla Afrika Birliğinin kurulmasına yönelik Sirte Bildirgesini yayınlamışlardır.

Resmi olarak 2002 yılında kurulan Afrika Birliği 1963 yılında kurulmuş olan Afrika Birliği Örgütünün halefi olarak görülmektedir. (<https://au.int/en/overview> 20.01.2025)

İnsan hakları ve diğer pek çok konuda yapmış olduğu çalışmaların yanısıra Siber güvenlik konusunda da önemli bir çalışma yapmış olan Afrika Birliği, ayrıca birlik içerisinde siber güvenlik ile ilgili bir sözleşmeyi yürürlüğe koymuştur. Malabo Sözleşmesi olarak da bilinen bu sözleşme 2011 yılında hazırlanıp, 2014 yılında kabul edilmiştir. Ancak yürürlüğe girmesi 2023 yılında Moritanya'nın onayı sonrasında olmuştur (<https://dig.watch/resource/african-union-convention-on-cyber-security-and-personal-data-protection-african-union> 21.02.2024). Henüz çok yeni olsa da Siber güvenlik ve kişisel dataların korunması üzerine yapılan bu sözleşme Afrika Birliği içerisindeki ülkelerle, alt bölgesel, bölgesel ve uluslararası seviyede bir bilgi toplumu oluşturmayı hedeflemesi, Afrika bilgi toplumunun hedeflerinin tanımlaması, yönelimin genişletilmesi, üye ülkelerin bilgi ve iletişim teknolojileri ve siber güvenlik konusunda ayrıca bilinçlendirilip var olan mevcut yasalarının da güçlendirilmesi açısından oldukça önemlidir.

Sözleşmede Siber güvenlik, iki ana husus üzerinde ele alınmıştır. Bunlar Siber güvenliğin sağlanması ve kişisel dataların gizliliğinin korunması hususlarıdır. Sözleşme içerisinde kritik altyapı sistemlerinin, halk sağlığı için önemli olan hayati servislerin siber saldırılardan korunmasının ulusal güvenliğin sağlanmasında özellikle önemli olduğu ayrıca vurgulanmıştır. Ayrıca siber saldırıların sonucunda dataların ve datalardaki bilgilerin gizliliğinin ve bütünlüğünün bozulması konusu da özellikle ele alınmıştır.

Sözleşmenin üçüncü bölümünde Siber güvenliğin teşvik edilmesi ve siber suçla mücadele özel olarak ele alınmış ve Kural 24' te Ulusal siber güvenlik çerçevesi altında tüm üye devletler için siber güvenlik ile ilgili ulusal boyutta oluşturulması gereken çerçeveler ve stratejiler ele alınmıştır.

Kural 25/4' de Kritik altyapıların siber saldırılardan korunması ile ilgili iç yasal düzenlemelerin yapılmasının zorunluluğundan bahsedilmiştir. Kural 28' de ise Siber

güvenlik konusunda uluslararası işbirliğinin yapılması gereğinden ve bu işbirliğinin siber güvenliğin sağlanması konusundaki öneminden bahsedilmiştir.

5.2.3. Ekonomik İşbirliği ve Kalkınma Örgütü'nün (OECD) Siber Uzay ve Siber Güvenlik Hususundaki Çalışmaları

İkinci Dünya Savaşı sonrasında ekonomik açıdan dağılmış durumda bulunan Batı Avrupa ülkelerinin ekonomilerinin yeniden canlandırılması ve bu ülkelerin yeniden imar edilmesi için bir plan oluşturulmuştur. Marshall planı olarak adlandırılan bu programda ABD ve Kanada öncülüğünde çok büyük bir yardım fonu toplanmış ve bu fonun dağıtılmasına yardımcı olması amacıyla da 1947 ve 1960 yılları arasında Avrupa Ekonomik İş Birliği Örgütü kurulmuştur. Daha sonra 1961 yılında bu örgütün işlevini tamamlaması nedeniyle onun görevlerini üstlenecek, yetki ve görev alanı daha geniş bir örgüt olan OECD kurulmuştur. Halihazırda 38 üyesi olan örgütün 20 adet kurucu üyesi bulunmaktadır ve Türkiye'de bu kurucu üyeler arasındadır.

OECD, üyeleri arasında ekonomik kalkınma, mali istikrar, yatırım, girişimcilik ve teknoloji gibi konularda gelişmenin ve istikrarın sağlanması için çalışmaktadır. Ayrıca bu konularda yıllık düzenli olarak Datalar paylaşmaktadır (<https://www.mfa.gov.tr/iktisadi-isbirligi-ve-gelisme-teskilati-oecd.tr.mfa> 14.12.2024).

Datalar ekonomi, toplum, eğitim, finans ve sağlık, teknoloji ve inovasyon gibi önemli konulara ait anlamlı bilgileri içeren sayısal ve elektronik verilerdir (<https://www.datamarket.com.tr/sozluk/data/> 15.12.2024). OECD tarafından düzenli olarak yayınlanan bu datalardan iş dünyası ve devlet birimleri ve akademik birimler tarafından faydalanılmaktadır.

Bugün dünya nüfusunun %18'ini, dünya GSYİH (Gayrisafi Yurt içi Hasıla) sinin yarından fazlasını ve dünya ticaretinin çoğunluğunu kapsayan OECD bu açıdan da uluslararası alanda çok önemli bir yere sahiptir (<https://www.state.gov/the-organization-for-economic-co-operation-and-development-oecd/> 14.12.2024). Bu nedenle siber güvenlik konularında yapmış olduğu çalışmalar uluslararası alanda önemli bir etkiye sahiptir. OECD içerisinde siber güvenlik konularında çalışmalar yapan asıl birim Bilim, Teknoloji ve Sanayi Direktörlüğüne bağlı olarak çalışmalar yürüten Bilgi, Bilgisayar ve İletişim

Politikaları Komitesidir. İngilizce kısaltması ICCP olan bu komite esasen Bilgi ve iletişim teknolojilerinin faydalarından mümkün olduğu kadar çok yararlanmayı amaç edinen çalışmalar yapmaktadır. Bu amaçla da üye ülkelerin BIT ve bu alandan kaynaklanan siber güvenlik sorunları konusunda ileriye dönük çalışmalar yapmaları için onlara yol haritaları düzenlemektedir (Ünver, Canbay ve Mirzaoglu,2011:14-19).

ICCP bünyesinde farklı konularda çalışmalar yapan gruplar bulunmaktadır. Bu gruplardan siber güvenlik konusunda çalışmalar yapan ve klavuzlar yayınlayan Bilgi Güvenliği ve Gizliliği Çalışma Grubudur. Bu grubun yayınlamış olduğu klavuzlardan biri Kişisel Verilerin Gizliliğinin Korunması ve Sınırlar Ötesine İletilmesine Dair Klavuzdur. Klavuz kişisel verilerin küresel şebekelerde yayınlanmasının sınırlarını düzenlemektedir ve uluslararası bir mutabakat metni olma özelliğine sahiptir (Ünver, Canbay ve Mirzaoglu ,2011:15).

Bir diğer önemli çalışma ise Bilgi Sistemleri ve Şebekelerinin Güvenliğine Dair Klavuzdur. Bu klavuzda siber terörizm, virüsler vb. bilgisayar ve internet kaynaklı tehditler ele alınmış ve bu tehditlerle mücadele konusunda oluşturulabilecek politikalar ve alınabilecek tedbirler ile ilgili önerilerde bulunulmuştur. Siber güvenlik konularında bir çeşit küresel güvenlik kültürü oluşturulması amaçlanmıştır. 11 Eylül saldırıları sonrasında revize edilmiş olan bu çalışma bugün "Bilgi Sistemleri ve Şebekelerinin Güvenliğine Dair Klavuz : Güvenlik Kültürüne Doğru" adıyla bilinmekte ve OECD'nin kritik bilgi altyapıları ve siber güvenlik konularında yaptığı en etkili çalışma olarak görülmektedir (Ünver, Canbay ve Mirzaoglu, 2011:18).

Ayrıca Bilgi Güvenliği ve Gizliliği Çalışma Grubu tarafından 2003 yılında Güvenlik Kültürü ismiyle bir internet sitesi kurulmuştur. Bir platform özelliği gösteren bu site sayesinde tüm üye ülkeler , hatta OECD benzeri diğer kuruluşlar ve onlara üye devletler de siber güvenlik konularında yapmış oldukları çalışmaları bu sitede birbirleri ile paylaşarak fikir alışverişinde bulunabilmektedir (Ünver, Canbay ve Mirzaoglu ,2011:19).

OECD'nin yapmış olduğu bu çalışmalar, uluslararası alanda böyle önemli ve söz sahibi olan bir örgütün siber güvenlik konularında bu kadar bilinçli adımlar atması ve soruna çok yönlü yaklaşması açısından oldukça önemli ve umut vericidir.

5.3. Diğer Uluslararası Örgütlerin Siber Güvenlik Çalışmaları

Bunların dışında ITU (Uluslararası Telekomünikasyon Birliği), WTO (Dünya Ticaret Örgütü ve IMF'in (Uluslararası Para Fonu) de siber güvenlik konusunda önemli çalışmaları mevcuttur. Ancak hem söz konusu çalışmaların henüz yalnızca rapor aşamasında olmaları hem de genel olarak siber saldırılar ve siber güvenlikle ilgili olsalar da içerik bakımından bu tezin konusu dışında kalmaları nedeniyle bu örgütlerin çalışmalarına kısa kısa değinilecektir.

5.3.1.Uluslararası Telekomünikasyon Birliği'nin (ITU) Siber Güvenlik İle İlgili Çalışmaları

ITU, BM'nin bilgi ve iletişim teknolojileri konusunda uzmanlaşmış kuruluşudur (<https://www.itu.int/en/about/Pages/default.aspx> 30.01.2025). 2001 yılında, ITU Konseyi, hükümetleri, uluslararası kurum ve kuruluşları, şirketleri ve sivil toplum örgütlerini, geleceğin bilgi toplumu için ortak bir vizyon belirlemek için bir araya getirmek amacıyla Dünya Bilgi Toplumu Zirvesi (World Summit on the Information Society - WSIS) adıyla ve Birleşmiş Milletler Genel Kurulunun 56/183 sayılı kararı ile uluslararası bir toplantı düzenlemeyi kararlaştırmıştır. ITU'nun siber güvenlik konusundaki faaliyetleri bu zirve sonrasında başlamıştır (Ünver, Canbay ve Mirzaoglu,2011:1-28).

ITU içerisinde oluşturulan dört farklı kurumun siber güvenlik konusunda çalışmaları mevcuttur. Ancak bu dört grup içerisinde özellikle ITU Genel Sekreterliğinin faaliyetleri ve ITU Telekomünikasyon Geliştirme Sektörünün Faaliyetleri ön plana çıkmaktadır. ITU Genel sekreterliği, küresel çapta siber güvenlik faaliyetlerinin oluşturulması, ulusal ve bölgesel düzeyde siber güvenlik önlemlerinin alınması, çocukların internet ortamında korunmasına yönelik düzenlemelerin yapılması (<https://www.un.org/en/global-issues/child-and-youth-safety-online> 30.01.2025), küresel düzeyde asgari güvenlik ölçütlerinin oluşturulması, yazılım ve donanım sistemlerinin akreditasyonunun yapılması gibi faaliyetler yürütmektedir. ITU Genel Sekreterliği bu faaliyetleri gerektiği gibi yürütebilmek için Siber güvenlik konularında uzman olan kişilerden oluşan Yüksek Seviyeli Uzmanlar Grubu adıyla bir danışma kurulu oluşturmuş ve bu uzmanların çizmiş olduğu yol haritasına göre hareket etmektedir.

Ayrıca ITU Genel Sekreterliği tarafından Siber Güvenlik Kapısı ismi ile bir platform oluşturulmuştur. Bu platforma kamu ve özel sektör kuruluşlarının, sivil toplum örgütlerinin, akademik çevrelerin, uluslararası ve bölgesel örgütlerin katılımı sağlanmaya çalışılmaktadır (Ünver, Canbay ve Mirzaoglu, 2011). I

TU Telekomünikasyon Geliştirme Sektörü ise Siber güvenlik konusundaki çalışmalarını bünyesinde kurulan BİT Uygulamaları ve Siber Güvenlik Birimi ile yürütmektedir. Bu birim ise siber güvenlik konusundaki çalışmalarında daha çok geliştirmekte olan ülkeler için siber güvenlik konusunda rehberler yayınlamak üzerine yoğunlaşmaktadır (Ünver, Canbay ve Mirzaoglu,2011).

5.3.2. Dünya Ticaret Örgütü'nün (WTO) Siber Güvenlik İle İlgili Çalışmaları

Uluslararası ticaretin serbestleştirilmesi amacıyla 1947 yılında Gümrük Tarifeleri ve Ticaret Genel Anlaşması (GATT) imzalanmıştır. Mal ticareti ile ilgili kuralların belirlendiği bu anlaşma sonrasında devam eden müzakereler neticesinde 1994 yılında Dünya Ticaret Örgütü kurulmuştur (Demirtaş, Yalaman,2023:32-41).

Dünya Ticaret Örgütü (WTO) ilkinin 2016 yılında yayınladığı Siber Hazırlık Enstitüsü (Cyber Readness Institute) kitapçığının sonuncusunu 2020 yılında yayınlamıştır.

Kitapçıkta örgütün, üye devletlere, iş dünyasına yönelik küçük ve büyük çaplı siber saldırılar ve bu saldırıların ekonomik sonuçları konusunda uyarıları ve üye devletler arasında siber güvenlik konusunda bilgi paylaşımının önemine dair önerileri bulunmaktadır(https://www.wto.org/english/tratop_e/msmesandtra_e/27_march_2019_cybersecurity.pdf 30.01.2025).

5.3.3. Uluslararası Para Fonu'nun (IMF) Siber Güvenlik İle İlgili Çalışmaları

1944 yılında imzalanan Bretton Woods Antlaşması ile kurulan IMF, dünyada global finansal sistemin Covid-19 salgını ile birlikte dijital bir dönüşüm geçirdiğini ve bu dönüşüm ile birlikte siber tehditlere de daha açık hale geldiğini düşünmektedir. Zira IMF'e göre, Covid 19 salgını ile başlayan dijital dönüşüm sonrasında şirketler, siber suçluların hedefi haline gelmiş ve milyarlarca dolar kayıp oluşmuştur (Mourer ve Nelson, 2021: 24-27).

Salgın ve beraberinde yaşanan dijital dönüşüm büyük şirketleri siber suçluların hedefi haline getirmiş ve bu şirketlere yapılan siber saldırılar neticesinde milyarlarca dolarlık hasar oluşturmuş ve bu durumun finansal istikrarı tehdit ettiğini belirtmiştir (<https://meetings.imf.org/en/IMF/Home/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability> 30.01.2025).

Ancak IMF'in raporunda devlet ve devlet destekli grupların da siber saldırılar gerçekleştirdiği ve bu saldırıların daha çok: bozma, yok etme, zarar verme ve siber casusluk gibi amaçlarla yapıldığı belirtilmiştir (Mourer ve Nelson, 2021).

Kasım 2020'de "Küresel Finans Sistemini Siber Tehditlere Karşı Daha İyi Korumak İçin Uluslararası Strateji" adıyla bir rapor yayınlanmıştır. Dünya Ekonomik Forumunun öncülüğü ile yayınlanan bu raporda küresel finans sisteminin siber tehditlerden etkili bir şekilde korunabilmesi için bir takım stratejiler belirlenmiştir. Bu stratejilerin temelinde ise hükümetlerin, iş dünyasının, sivil toplum kuruluşlarının birlikte hareket etmesi gerekliliği bulunur. Zira küresel sistemin birbirine bağımlı yapısı bu kollektif çalışmayı zorunlu hale getirmektedir (Mourer ve Nelson, 2021). IMF tarafından yayınlanan raporlarda, Finans sektöründe ve şirketlerde bu tür siber saldırılardan kaynaklı kayıpların yaşanmasının, piyasaya olan güvenin sarsılmasına neden olacağını belirtilmiştir (Natalucci, Qureshi ve Suntheim, 2024 <https://meetings.imf.org/en/IMF/Home/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability> 31.01.2025).

6.Bölüm

Uluslararası Hukukta Siber Saldırıların Hususunda Karşılaşılan

Sorunlar

6.1. Siber Saldırıların Atfedilebilirlik Sorunu

Uluslararası hukukta siber saldırıların karşılığında yaptırım uygulanabilmesinin önündeki en büyük engel atfetme sorunudur. Siber uzay karmaşık yapısı nedeniyle görünmez orduların ve sessiz silahların alanı olarak kabul edilmektedir (Aydın, 2008:1-216). O nedenle bu alanda yapılan saldırıların takip edilebilmesi ve sorumluların bulunması oldukça karmaşık ve zor bir durumdur. Devletin saldırıdan sorumlu tutulabilmesi ve uluslararası hukuk tarafından gerekli yaptırımın uygulanabilmesi için ise, saldırının söz konusu devlete kesin bir şekilde atfedilebilmesi şarttır.

Hukuk Komisyonu tarafından 2001 yılında hazırlanmış ve BM Genel Kuruluna sunulmuş olan Devletlerin Uluslararası Hukuka Aykırı Fiillerinden Doğan Sorumluluğu (A/RES/56/83) ile ilgili belgenin 2. bölümünde Devletin iki şartla uluslararası hukuka aykırı eylemden dolayı sorumlu tutulabileceği belirtilmiştir. Bu şartlardan ilki Uluslararası hukuka aykırı fiilin devlete atfedilebilmesi şartıdır. İkincisi ise, devletin Uluslararası hukuktan kaynaklanan sorumluluğunu ihlal etmiş olmasıdır.

Görüldüğü üzere atıf yani atfetme konusu bir devletin Uluslararası hukuka aykırı olan bir fiilden dolayı yargılanabilmesi için ilk koşuldur. Ancak siber saldırılarda bu işlem hiç de basit değildir. Siber uzay karmaşık, anonim ve dinamik yapısı gereği, saldırgan devlete, özellikle de devlet teknolojik anlamda avantajlı durumda ise, kendini gizlemek için pek çok fırsat sunan bir alandır. Devletler genelde bu alanda yapacakları saldırıyı terörist gruplar aracılığıyla yaparlar ya da DDoS atakları olarak bilinen ve bir bilgisayar tarafından binlerce bilgisayarı (botnetler) ele geçirerek gerçekleştirilen ve takip etmesi çok zor olan saldırı tipini tercih ederler. Ancak bazen de güç gösterisi yapmak ya da gözdağı vermek amacıyla bizzat istihdam ettikleri siber ordular tarafından özel olarak üretilen kötü amaçlı yazılımlar yoluyla saldırıyı tercih ederler. Her iki durumda da atıf konusu geçilmesi gereken en büyük engeldir. Ancak geçilmez değildir.

Atfetme işlemi farklı teknikler gerektirir ve kendi içerisinde farklı boyutları vardır ve atıf işlemi ile ilgili çalışma yapılırken tüm boyutlar birbirleri ile bağlantılı şekilde ele alınmalıdır. Söz konusu bu boyutlar taktik, operatif ve stratejik olmak üzere 3'e ayrılmaktadır (Bolat, 2020:93-94). Her bir boyutun kendine has cevaplandırılması gereken soru türleri vardır. Bir boyuttan diğerine geçerken bir öncekinde sorulan sorulara verilen cevaplar diğer boyut ile ilgili çalışmalara eklenmelidir.

Taktik boyutta saldırının teknik özellikleri, yazılımın türü, bilgisayar ve/veya sisteme verdiği hasar incelenir ve bu minvalde sorular sorulup teknik konular aydınlatılmaya çalışılır. Operatif düzey, taktik düzeyde sorulan sorulara verilen cevapların, farklı kaynaklardan edinilen bilgilerle birleştirildiği düzeydir. Bu düzeyde alınan cevaplar, Stratejik düzeyde sorulan ve saldırının politik yönünü araştıran soruların cevaplarına eklenir ve saldırıyı hangi devletin yaptığı sorusuna net bir cevap bulunmaya çalışılır (Bolat, 2020:93-94). Burada atfetme işlemi en çok zorlayan durum tüm sorulara net şekilde cevap verilmesinin ve atfın derecesinin yüksek olmasının gerekliliğidir. Saldırganın kendisini çok rahat gizleyebildiği bu alanda tüm sorulara net cevaplar verebilmek ise oldukça zor, uzun ve uzmanlık gerektiren bir süreçtir (Bolat, 2020).

Ancak bu sürece geçmeden önce yapılan siber saldırının kuvvet kullanımı ya da silahlı saldırı kategorisine girip girmediği konusu netleştirilmelidir. Esasen devletler bu tür yeni nesil saldırıları çoğu zaman siyasi amaçlarını gerçekleştirebilmek, hedef olarak gördükleri devleti siyasi ve ekonomik açıdan yıpratmak ve hedef devlete politik anlamda istediklerini yaptırabilmek amacıyla yapmaktadırlar. Bu saiklerle yapılan bir siber saldırı kuvvet kullanımı ya da silahlı saldırı kategorisine girmese bile BM Şartı 2/1. Maddesinde bahsi geçen devletlerin egemen eşitliği ilkesine ve iç işlerine müdahale etmeme ilkesine ters düşmekte ve sadece bu haliyle bile BM Şartı kurucu hükümlerini ihlal etmektedir.

Bir devlet tarafından başka bir egemen devlete karşı gerçekleştirilen siber saldırı eğer kuvvet kullanımı ve/veya silahlı saldırı kategorisine girerse bu durumda mağdur olan devlet açısından BM Şartının 51. maddesinde bahsi geçen meşru müdafaa hakkını doğurur. Ancak bununla ilgili pek çok koşulun gerçekleşmesi gerekmektedir. Bu koşullardan ilki saldırının barış zamanında gerçekleştirilmiş olmasıdır. Bunun dışında

yapılan siber saldırının silahlı saldırı kategorisine girip girmediği hususunda üç temel yaklaşım bulunmaktadır. Bunlar Araç Odaklı, Hedef Odaklı ve Etki Odaklı yaklaşımdır (Bolat, 2020:54-55).

Araç odaklı yaklaşımda baz alınan nokta saldırı için kullanılan aracın (siber uzayda bu zararlı yazılımlar ya da botnetler aracılığıyla yapılan DoS ve DDoS atakları) bir silah gibi kullanılarak hedef devlete zarar verilmesidir. Burada dikkat daha çok amacın anlaşılmasına yöneliktir. Yani eğer devletin amacı hedef olarak gördüğü diğer egemen devlete zarar vermekse ve bu zararı da siber saldırı araçlarını bir silah gibi kullanarak yapıyorsa bu durumda yapılan eylem silahlı saldırı kapsamına girmektedir ve fail olan devlet, kuvvet kullanımından kaçınma ilkesini ihlal etmiş olarak görülmektedir.

Hedef odaklı yaklaşım, adından da anlaşılacağı gibi saldırıda hedef alınan ve zarar gören sistemleri baz alır (Bolat, 2020:54-55). Örneğin saldırının hedefinin bir devletin kritik altyapı sistemleri olması durumunda devlete ait bilginin gizliliği, ulaşılabilirliği ve güvenliği tehlikeye girdiğinde devlet açısından çok önemli ve büyük kayıplara neden olabilecek hatta can kayıplarına sebep olabilecek sistemlerin çökmesi, gerektiği gibi çalışmaması ve hatta tamamen devre dışı kalması durumu söz konusu olabilir. Böyle bir durumda devlet, yalnızca milyar dolarlarla ifade edilecek ekonomik hasara değil, sivil halkın yaralanmasına, hatta can kayıplarına sebep olabilecek fiziki hasarlara da maruz kalmış olur. Ayrıca zarar verilen sistemin önemi dikkate alındığında bankacılık sistemleri ve/veya devlete ait kritik öneme sahip bilgi ve belgelerin kaydedildiği sistemlere yapılan bir siber saldırı da silahlı saldırı olarak değerlendirilecektir (Collins ve McCombie, 2012: 80-91).

Etki odaklı yaklaşımda ise saldırının hedef devlet üzerindeki etkisine bakılır. Eğer saldırının etkisi hedef devlet açısından yıkıcı sonuçlar meydana getirmişse ve konvansiyonel silahların verebileceği fiziksel ve ekonomik zararı vermişse bu saldırı da, silahlı saldırı olarak nitelendirilir (Bolat,2020:54-55).

Sonuçlarının değerlendirilebilmesi açısından, Tallinn Rehberini hazırlayan Uluslararası hukuk uzmanları tarafından en çok kabul gören etki odaklı yaklaşımdır. Ancak bir ülkenin kritik altyapı sistemlerini hedef alan bir siber saldırıda hedef odaklı yaklaşım da dikkate alınmak durumundadır. Zira kritik altyapı sistemlerinin zarar görmesi ve işlemez hale

gelmesi neticesinde ölümcül kazaların, ciddi yaralanmaların ve altından kalkılamayacak ekonomik hasarların meydana gelmesi mümkündür.

Siber saldırıların kuvvet kullanımı kapsamına girip girmediği konusunda baz alınan ölçütler sadece bunlar değildir. Tallinn Rehberi'nin oluşturulması sürecinde en yetkili isimlerden biri olan Michael Schmitt siber saldırıların, kuvvet kullanımı kapsamına girip girmeyeceği hususunda Ciddiyet, Aciliyet, Doğrudanlık, İstilacılık, Ölçülebilirlik, Varsayımsal Meşruiyet ve Sorumluluk olmak üzere yedi tane ölçüt belirlemiştir (Çelik, 2014:137-175). Ölçütlerin ayrıntılarına geçmeden önce belirtmek gerekir ki belirtilen bu ölçütler yalnızca saldırının ölçüsünün nasıl değerlendirileceği, bunun bir kuvvet kullanımı olup olmadığı konusunda bir fikir sunması mahiyetinde önem taşımaktadır. Bunun dışında bir bağlayıcılığı bulunmamaktadır.

Belirtilen ölçütlerden **Ciddiyet (Severity)**: Saldırının neticesinde ortaya çıkan zararın boyutu ve önemini, **Aciliyet (Urgency)**: Saldırıdan kaynaklı sorunların ortaya çıkma hızını, **Doğrudanlık (Directness)**: Saldırı ile netice arasındaki bağın kuvvetini, **İstilacılık (Invasiveness)**: saldırının hedef devletin topraklarına ve kritik altyapı sistemlerine hangi boyutta yayıldığını, **Ölçülebilirlik (Measurability)**: Saldırının etkilerinin/sonuçlarının ölçülebilirliğini (maddi zararın boyutu vb.), **Varsayımsal Meşruiyet (Hypothetical Legitimacy)**: Saldırının Uluslararası hukukta meşru olarak görülen ekonomik baskı ya da psikolojik savaş kapsamında olup olmadığını, **Sorumluluk (Responsibility)**: Fail olduğu düşünülen Devlet ile yapılan saldırı arasındaki bağın kuvvetini ölçmektedir.

Schmitt'e göre, bu yedi ölçüte büyük oranda cevap veren saldırılar silahlı saldırı/kuvvet kullanımı olarak nitelendirilmelidir (Çelik, 2014:137-175). Sonuç olarak Schmitt'in iddiasına göre, yapılan bir siber saldırı tüm bu ölçütleri karşılaması durumunda silahlı saldırı olarak nitelendirilebilir ve kuvvet kullanımı ilkesinin ihlal edilmesi sebebiyle mağdur devlet açısından meşru müdafaa hakkı doğurur. Ancak bu ölçütlerin ve Tallinn Rehberinin bağlayıcı bir özelliğinin bulunmaması ve ilgili rehberin, Uluslararası Adalet Divanı tarafından yalnızca yardımcı kaynak olarak kullanılıyor olması bu konuda soru işaretlerine neden olmaktadır.

Yapılan saldırının, her ne kadar bağlayıcı ölçütler olmasa da tüm bu ölçütleri karşıladığı bir durumda gene asıl sorun olan saldırının atfedilmesi meselesi ile karşı karşıya kalınacaktır. Ancak gün geçtikçe artan teknolojik gelişmeler, saldırgan devletlere daha rahat gizlenme imkanı sağlasa da aynı gelişmeler atıf konusunu da kolaylaştırmaktadır. Zira siber saldırılarda kullanılan zararlı yazılımların türü ve bu yazılımlarda sıkça kullanılan kodlar, ya da saldırının türü çoğu zaman saldırganı ele vermektedir. Örneğin DoS ve DDoS türü dağıtılmış hizmet reddi saldırıları çoğunlukla Rusya tarafından kullanılmaktadır. 2007 Estonya ve 2008 Gürcistan siber saldırıları buna örnek olarak gösterilebilir. Virüs ve zararlı yazılım türleri ise daha çok ABD tarafından kullanılmaktadır (Aykut,2021). Örneğin 1982 yılında virüslü yazılım sebebiyle Sibirya doğalgaz boru hattında oluşan patlama ve 2010 yılında İran Natanz nükleer tesisine yapılan Stuxnet siber saldırısı.

Özellikle Stuxnet virüsü APT (Gelişmiş Kalıcı Tehdit) olarak bilinen ve geliştirilmesi için özel laboratuvarlar ve milyarlarca doların gerekli olduğu daha önce görülmemiş türde bir virüstür. Öyle ki, David E. Sanger 2012 Haziran'ın da New York Times Gazetesi'nde yayınladığı raporda, Stuxnet'in ABD ve İsrail tarafından yapıldığı ve çok daha büyük bir planın parçası olduğunu iddia etmiştir. (Memiş, 2015:76).

Yine eski CIA ve NSA çalışanı Edward Snowden, 2013 yılında sızdırdığı belgelerde ve Der Spiegel'in kendisi ile yaptığı röportajda Amerikan istihbarat örgütlerinin siber uzayda gerçekleştirdiği diğer faaliyetlerden ve Stuxnet'i NSA ve İsrail'in beraber oluşturduğundan bahsetmiştir (Memiş, 2015:77).

Bunun dışında pek çok bilişim uzmanının da Stuxnet saldırısının arkasında ABD ve İsrail'in olduğu konusunda ısrarcı olduğu bilinmektedir (Holat, 2021:115). Stuxnet virüsünü inceleyen RF merkezli Karspersky Laboratuvarı da Stuxnet'in ulus-devlet desteği olmadan geliştirilemeyecek kadar karmaşık olduğunu belirtmiştir (Memiş, 2015:75).

Bunların haricinde elbette sadece yazılımın, kullanılan kodun, yapılan saldırının türü değil politik sebepler de bu araştırmalar sırasında göz önünde bulundurulmalıdır. Zira devletler siber saldırıları daha çok siyasi anlamda istediklerini yaptırabilmek amacıyla gerçekleştirmektedir. O nedenle devletler arasında yaşanan politik gerginlikler de bazen

saldırgan tarafı ele vermek açısından ipucu olmaktadır. Örneğin 2007 Estonya siber saldırısı öncesinde Tallinn şehrindeki Sovyetler döneminden kalma anıtın yerinin değiştirilmesi Rusya tarafından tepki çekmiş ve hemen akabinde Estonya'ya yönelik siber saldırılar başlatılmıştır. Rusya durumu inkar etse de saldırıların sinyalleri takip edildiğinde saldırının Rusya kaynaklı olduğu anlaşılmıştır. Benzer şekilde ABD'nin çok uzun bir süre İran'ın nükleer çalışmaları konusunda tehditler savurduğu, eğer İran nükleer çalışmalarına devam ederse kendisine yaptırım uygulamak ya da saldırmakla tehdit ettiği dünya kamuoyu tarafından bilinmektedir.

Atfetme hususunda devletin sahip olduğu istihbarat sisteminin gücü ve etkisi de çok önemlidir. Bunun en çarpıcı örneği, 1998 yılında ABD'ye yönelik yapılmış olan Moonlight Maze saldırısında ABD Dışişleri bakanlığı ve Savunma bakanlığının organize çalışmaları ve saldırı ile ilgili tüm ayrıntıların, şüpheli e-postaların ve e-posta hesaplarının, sinyallerin takip edilmesi neticesinde saldırının Rusya tarafından yapıldığının kanıtlanmış olmasıdır.

Görüldüğü üzere atıf konusu çok boyutlu bir işlemdir ve yapılan siber saldırı ile ilgili her şeyin, her teknik ayrıntının, politik gelişmelerin dikkatlice takip edilip analiz edilmesi, saldırı ile ilgili tüm istihbaratın titizlikle toplanıp işlenmesi ve diğer elde edilen bulgularla karşılaştırılması sonucunda elde edilen net ve somut bilgilerle hareket edilmesi çok önemlidir.

6.1.1. Devlet Tarafından Yapılan Siber Saldırıların Atfedilmesi Hususu

Devlet tarafından bizzat gerçekleştirilen siber saldırılar genel olarak devletin bir organı ya da bu konuda özel olarak istihdam edilmiş siber orduları tarafından yapılmaktadır. Devlet kurumları içerisinde istihdam edilen bilgisayar programlama ve yazılım konularında uzmanlaşmış kişiler tarafından özel olarak siber saldırı amacıyla belli bir hedefe yönelik geliştirilen zararlı yazılımlar aracılığıyla gerçekleştirilen siber saldırılarda daha çok SCADA sistemlerinin hedef alındığı gözlemlenmiştir (Loukas, 2015: 106-143).

Özellikle kritik altyapı sistemlerinde, metrolar, demiryolları, havaalanları ve barajlar gibi büyük tesislerde ve nükleer santrallerde sistemin işleyişinin kontrolünü sağlayan bu tür

sistemlere yönelik yapılan siber saldırılarda Stuxnet gibi, özel laboratuvarlarda büyük maliyetlerle geliştirilmiş zararlı yazılımlar kullanılmaktadır. Bu tür zararlı yazılımların üretilmesi de ancak bir devletin finansal olarak altından kalkabileceği bir iştir.

Ayrıca daha önce de bahsettiğimiz gibi her devletin siber saldırıda kullandığı saldırı yöntemi farklılık arz etmektedir. Örneğin DoS ve/veya DDoS tipi saldırılar da yapılmış olabilir. Burada yapılacak tek ve en önemli şey, saldırının fail olduğu düşünülen devlete atfedilmesi olduğu için öncelikle saldırının hangi yöntemle yapıldığının tespit edilmesi, yani atfetme işlemi için ilk adımların atılmasıdır. Bunun için önce saldırıya maruz kalan sisteme, kullanılan bilgisayarlara, saldırı öncesinde ve sonrasında atılmış olan e-postalara ayrıntılı olarak bakılması ve detaylı bir istihbarat incelemesinin yapılması gerekir. Saldırı taktik, operatif ve stratejik boyutlarıyla ele alınarak incelenmeli ve siber saldırı neticesinde ortaya çıkan hasar (fiziksel ve ekonomik) tam ve ayrıntılı bir şekilde incelenerek ayrıntılı bir rapor oluşturulmalıdır (Bolat, 2020:93-94).

Atıf işleminin kesin bilgilere dayanması gerekliliğinden dolayı tüm bunlar yapıldıktan sonra saldırıyı gerçekleştirdiği düşünülen devlet ile ilgili kuvvetli bir ipucu bulunması halinde mağdur devlet, ilgili devlet aleyhinde uluslararası yargıya başvuruda bulunabilir. Yargıya başvuru yapıldıktan sonra ise, öncelikle saldırının silahlı saldırı ölçüsünde olup olmadığı değerlendirilmektedir. Yapılan saldırı silahlı saldırı ölçeğine ulaşmamışsa mağdur olan devlete herhangi bir meşru müdafaa hakkı tanınmamaktadır. Ancak burada artık verilen ekonomik zararın da ölçü bakımından dikkate alınması gerekmektedir. Çünkü siber saldırı yoluyla verilen ekonomik hasar neticesinde mağdur devletin finansal açıdan çökme ihtimali de mevcuttur ve ekonomik güç çağımızda bir devletin egemenliğinin, bağımsızlığını ve varlığını sürdürmesinin en gerekli araçlarından biridir. Bu nedenle saldırı suçu değerlendirilirken mağdur devlete verilen ekonomik zarar da göz ardı edilmemelidir.

Ayrıca siyasi saiklerle yapılan siber saldırılarda hasar verilmemiş olsa bile bir devletin egemenliğine müdahale etmeme ilkesinin çiğnenmesi nedeniyle saldırgan devlete belirli bir yaptırım uygulanması devletler için bu tür müdahalelerde bulunmama konusunda caydırıcı olacaktır.

6.1.2. Devlet Eliyle Yaptırılan Siber Saldırıların Atfedilmesi Hususu

Devletler her zaman saldırıyı bizzat kendileri gerçekleştirmezler. Özellikle siber uzay gibi karmaşık ve dinamik yapıya sahip ve gizlenmenin bir o kadar kolay olduğu bu alanda bu karmaşık yapıdan faydalanmak ve kendilerini gizlemek amacıyla siber saldırıyı bizzat yapmak yerine terör örgütlerini ya da bir kişi veya bir grubu saldırıyı gerçekleştirmek için kullanabilirler. Bu kişi bazen hedef devlet içerisinde bir ajan da olabilir. Devletler bu kişilere yetki vererek, saldırıyı gerçekleştirmek için gerekli eğitim ve finansal desteği vererek bu kişileri adeta maşa olarak kullanırlar. Devletin bu yolla gerçekleştirdiği siber saldırılarda asıl sorun bu kişi, grup ya da teröristlerle olan illiyet bağının hangi ölçüde olduğunun bulunmasıdır. Bunun için de öncelikle saldırı fiilinin nereden ve kim tarafından gerçekleştirildiğinin tespit edilmesi gerekmektedir.

Zor bir süreç olsa da sürekli gelişen teknoloji gizlenmeyi kolaylaştırırken aynı zamanda saldırganın tespit edilmesini de kolaylaştırdığı için alan adı ve IP adresi olarak bilinen ve saldırının nereden yapıldığı, saldırının gerçekleştirildiği bilgisayarın kime ait olduğu gibi bilgilere ulaşılmasını sağlayan ve neredeyse kimlik numarası olarak görülebilecek belirli harf ve numaralardan oluşan adreslerin takip edilmesi neticesinde saldırganlara ulaşılması artık daha basit bir hale gelmiştir. Adres takip yöntemi DoS ve DDoS atakları gibi siber saldırı türlerinde saldırganın izinin bulunması hususunda biraz olsun yardımcı olsa da Stuxnet gibi USB türü cihazlarla SCADA sistemlerine bulaştırılan virüslerde aynı etkiyi göstermemektedir. Bunun nedeni virüsün bağlantısı takip edilebilecek bir ağ aracılığıyla bulaştırılmamış olmasıdır. Bu tür durumlarda saldırının detaylarının bulunması ve saldırıyı gerçekleştiren devlete atfedilebilmesi, virüsü içeriye taşıyan kişinin yakalanması ve fail olduğu düşünülen devlet ile olan illiyet bağının açığa çıkarılması ile mümkün olacaktır.

Örneğin, İran Natanz nükleer tesisine yapılan Stuxnet siber saldırısında Stuxnet isimli virüs, ABD ve İsrail tarafından özel laboratuvarlarda geliştirilmiş ve nükleer tesisin SCADA sistemlerine Hollanda istihbarat servisine bağlı olarak çalışan İran asıllı bir mühendis tarafından USB aracılığıyla bulaştırıldığı belirtilmiştir. Ayrıca olaydan birkaç yıl önce CIA ve Mossad'ın tesislere sızmak için Hollanda'dan yardım talebinde bulunduğu da bilinmektedir (<https://siberbulten.com/siber-guvenlik/stuxnet-hakkindaki-efsaneler-son-buldu-nasil-bulastirildigi-ortaya-cikti/> 16.07.2024).

Böyle bir durumda saldırı fiilinin hangi devlete atfedileceği hususu ile ilgili Uluslararası Hukuk Komisyonu tarafından hazırlanıp BM Genel Kuruluna sunulmuş olan “Devletlerin Uluslararası Hukuka Aykırı Fiillerinden Doğan Sorumlulukları” ile ilgili düzenlenen ARSIWA isimli belgeye başvurularak fikir sahibi olunabilir. Söz konusu belge incelendiğinde bu durumda nasıl bir yol izlenebileceği hususunda birkaç madde özellikle göze çarpmaktadır. Bunlardan ilki ; ARSIWA Kural 2/8' de : *“Bir devletin yönlendirdiği veya kontrol ettiği bir davranış, bir kişi ya da grubun davranışı, eğer o kişi ya da grup bir devletin talimatıyla veya o devletin kontrolü altında hareket ediyorsa o davranış uluslararası hukuka göre ilgili devletin eylemi olarak kabul edilir”* (BMGK, 2001: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

21.02.2025). Bu ifadeye göre eğer iddia edildiği gibi virüsü Natanz Nükleer tesisinin Scada sistemlerine USB aracılığıyla bulaştıran kişi Hollanda Genel İstihbarat ve Güvenlik Servisine (AIVD) bağlı bir ajan ise zaten Hollanda Devleti söz konusu eylem ile ilgili uluslararası hukuk açısından sorumlu bulunmaktadır. Zira ARSIWA Kural 2/4'te belirtildiği gibi *"Devlet içerisindeki konumu her ne olursa olsun eylem devletin bir organı tarafından ya da o organın bir üyesi tarafından gerçekleştirilmişse ve devlet bu eylemin uluslararası hukuka aykırı olduğunu biliyorsa o eylem ilgili devlete atfedilecektir"* (https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

21.02.2025) O sebeple burada Hollanda devleti işlenen eylemden uluslararası hukuk açısından sorumludur.

Ayrıca olayda sisteme yerleştirilen virüsün ABD ve İsrail tarafından geliştirilmiş olması ve sisteme sızmak için CIA ve Mossad'ın Hollanda'dan yardım talebinde bulunması ve en nihayetinde virüsün ilgili birimlerden elde edilip sisteme entegre edilmesi ARSIWA Kural 2/ 6'da belirtilen: *“Başka bir devlet tarafından bir devletin emrine verilen organlarının eylemleri, eğer organ emrine verildiği hükümet otoritesinin unsurlarını kullanarak eylemi gerçekleştiriyorsa önceki devletin eylemi olarak kabul edilir”* ifadesinden hareketle gene Hollanda devletinin uluslararası hukuka aykırı eylemde bulunduğu sonucuna varılabilir. Çünkü burada Hollanda devleti istihbarat ajansını ve ajansın bir üyesini ABD ve İsrail'in yetkisine vererek onlara bağlı hareket etmesine müsaade etmiştir.

Ayrıca yine ARSIWA Kural 4/16’da: “*Bir devletin başka bir devletin eylemiyle bağlantılı sorumluluğu*” ifadesi dikkate alındığında Uluslararası hukuka aykırı bir eylemin işlenmesinde yardım etmek ve destek vermek de ilgili devletin Uluslararası hukuk karşısında işlenen eylemden sorumlu tutulacağını gösterir. Ancak burada akıl karışıklığına sebep olan durum ABD ve İsrail ve bu devletlere bağlı gizli örgütlerin eylem ile bağlantısının hangi ölçüde olduğunun (Stuxnet virüsünün bu devletlerin gizli servisleri tarafından özel olarak hazırlanması dışında) bulunması ve eylemin ilgili devletlere de atfedilip atfedilemeyeceği durumudur.

Esasında eylemi planlayan ve Hollanda’dan sistemlere sızmak için yardım talebinde bulunan ABD ve İsrail’dir. Burada ARSIWA Kural 4/17’ye baktığımızda, belirtilen ifade :“ *Uluslararası hukuka aykırı bir eylemin işlenmesi üzerinde uygulanan yönlendirme ve kontrol durumunda yönlendirme ve kontrol işlemini yapan devlet ilgili eylemden sorumlu tutulacaktır*” şeklindedir BMGK,

2001:https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

21.02.2025) ABD ve İsrail’in Hollanda istihbarat servisine bağlı olarak çalışan ajana söz konusu virüsün bulunduğu USB’yi verip bunu nasıl sisteme bulaştıracak hususunda yönlendirmede bulundukları ve süreci takip ve işlemin gerçekleşip gerçekleşmediğini kontrol ettikleri kabul edilirse burada iki devletin de uluslararası hukuk açısından işlenen eylemden sorumlu olacakları aşikardır.

Ancak görüldüğü gibi bu süreç oldukça uzun ve meşakkatlidir. Kaldı ki, olayla ilgili üç devletin de eylemi inkar etme ihtimalleri mevcuttur. O nedenle işledikleri hukuksuz eylem neticesinde sorumluluktan kaçamamaları için daha somut, net ve inkar edilemez delillerle sonuca varılması gerekmektedir. Bu da belki ancak eylemi gerçekleştiren ajanın yakalanıp bağlantılarının bulunması ile mümkün olabilir ki gizli servis ajanlarının bağlantılarını itiraf etme ihtimali neredeyse sıfırdır veyahut da Stuxnet isimli virüsün ayrıntılı bir şekilde incelenmesi ile bir ipucu bulunabilir. Ancak buradan elde edilen bilgi ile net bir şekilde suç atfedilir mi bu da kesin değildir. Üstelik burada atıf konusunda başvuru belgenin de henüz taslak mahiyetinde olması durumu daha karmaşık hale getirmektedir.

Diğer yandan, bir devletin hukuksuz bir eylemde bulunduğu yönünde suçlanabilmesi ancak kesin kanıtlarla mümkün olabilmektedir. Yani İran burada yapılan saldırıyı fark ettiği anda meşru müdafaa hakkını kullanmak için başvurmak istese bile önce saldırıyı kimin gerçekleştirdiğini, saldırının hangi devlete atfedileceğini net bir şekilde belirlemek durumundadır. Örneğin İsrail'in Lübnan'da gerçekleştirdiği siber saldırı sonrasında Lübnan'ın bu saldırıdan İsraili sorumlu tutması oldukça basittir. Üstelik saldırıyı İsrail devleti değil, devlete bağlı istihbarat örgütünün bu tür saldırılardan sorumlu olan bir birimi gerçekleştirmiş olsa da saldırıyı gerçekleştiren birimin İsrail devleti ile illiyet bağı olduğundan saldırı direk ve kesin bir şekilde İsrail devletine atfedilebilecektir. Ancak İran Stuxnet siber saldırısında ve Suudi ARAMCO şirketine yapılan Shamoon virüsü saldırısında, İran'ın ve Suudi Arabistan hükümetinin böyle net bir şekilde ve kısa zamanda saldırganları tespit etme ve kesin bir atıfta bulunma şansları yoktu.

Görüldüğü gibi genel olarak siber uzay dediğimiz karmaşık dünyada atıf işlemi oldukça zor ve zaman alan bir süreçtir. Bu sebeplerden dolayı siber saldırılarda mağdur durumda olan devletin sorununu çözüme kavuşturacak mağduriyetini giderecek ve saldırgan devletlerin uluslararası hukuktan kaynaklanan sorumluluklarından kaçmalarını kesin bir şekilde önleyecek tedbirlerin alınması zorunludur. Ancak bu tedbirlerin neler olması gerektiği tartışılmalıdır.

6.2. Hukuki Süreçlerdeki Diğer Mevcut Engeller

Siber saldırılarda saldırgan devlete karşı yürütülecek hukuki mücadelede en büyük problem atfetme konusu olsa da tek sorun elbette bu değildir. Siber uzay ve bu alanda gerçekleştirilen saldırılar çok uzak bir geçmişe sahip olmadığı için siber uzay kavramının ortaya çıkışından çok önceleri oluşturulmuş olan uluslararası hukuk kuralları ve normları her ne kadar yorumlanarak ya da kıyaslanmaya çalışılarak bu yeni nesil saldırı yöntemlerine karşı hukuki çareler aranıyor olsa da uluslararası hukuk'ta halen bu konu ile ilgili doldurulması gereken pek çok boşluk ve aşılması gereken pek çok engel mevcuttur.

Bu sorunların en başında da bu tür saldırılarda başvurulabilecek hukuki yolları gösteren, devletlerin çekince koyamayacağı antlaşmaların ve bir devlet tarafından başka bir devlete karşı gerçekleştirilen ve fiziksel zarar oluşturan bir siber saldırı neticesinde alınmış emsal

bir kararın bulunmayışı gelmektedir. Emsal kararlar elbette bir kural değildir ve bunlar olmasa da farklı çözümler bulunabilir. Ancak bu gibi durumlarda fikir vermeleri açısından önemlidirler. Bu tür durumlarda başvurulabilecek tek ayrıntılı kaynak Tallinn Rehberidir. Ancak onun da sadece Uluslararası Adalet Divanı tarafından yardımcı kaynak olarak başvuru bir doktrin olması nedeniyle bağlayıcı niteliği yoktur. Bu nedenle, geleneksel savaş yöntemleri ile yapılan saldırıları önlemek için yazılan uluslararası hukuk kuralları ve oluşturulan antlaşmalarda bulunan maddeler bu alana uygulanmaya çalışılmakta, siber saldırılarla ilişkili olmayan emsal kararlardan bu konu ile ilgili olası davalarda nasıl bir yol izleneceğine dair çıkarımlar yapılmaya çalışılmaktadır. Bu durum da haliyle sıkıntılı ve zor süreçlerin yaşanmasına neden olmaktadır.

Bu konuda net ve bağlayıcı Uluslararası hukuk kurallarının ve normlarının şu ana kadar oluşturulamamış olmasının nedenlerinden biri uluslararası hukuk konusunda uzman olan isimlerin siber saldırıların etkileri ve potansiyel riskleri konusunda görüş ayrılığına düşmeleridir (Temel, 2021:122-158). Bir kısım uzmanlar siber saldırıların hiçbir zaman konvansiyonel yöntemlerle yapılan bir saldırı ile eşit ölçüde hasar veremeyeceğini ve bu alanda gerçekleştirilen saldırılar hususunda mevcut hukuk kurallarının uygulanmasının yeterli olacağını öne sürerken bir kısım uzman da siber uzayın yapı ve nitelik bakımından tamamen farklı bir alan olduğunu, siber saldırıları gerçekleştirmek için kullanılan zararlı yazılımların gitgide daha tehlikeli bir hale geldiğini ve daha önce yapılmış birkaç siber saldırıda özellikle de en son 2024'de İsrail'in Lübnan'da gerçekleştirdiği siber saldırıda görüldüğü gibi siber silahların konvansiyonel silahlarla eşit ölçüde hasar verme gücünün olduğunu bu sebeple siber uzay ve siber saldırılar hususunda net ve bağlayıcı kuralların konulması gerektiğini belirtmişlerdir (Temel, 2021). Uzmanlar arasında yaşanan bu görüş ayrılıkları durumun ciddiyetinin net olarak anlaşılmasını engellemektedir.

Bir diğer sorun da siyasi amaçları elde edebilmek için ekonomik ve politik baskı aracı olarak siber saldırıların kullanılmasının suç olarak nitelendirilmemesidir (Bolat, 2020: 62). Birleşmiş Milletler Şartı 2/1. maddesinde bahsi geçen devletlerin egemen eşitliği ilkesi gereği devletlerin, birbirlerinin işlerine müdahale etmeme ilkesine riayet etmeleri uluslararası teamül hukukunun bir gereğidir. Ancak siyasi amaçları gerçekleştirebilmek için ekonomik ve politik baskı aracı olarak kullanılan siber saldırılar, uluslararası

hukukun müdahale etmeme ilkesini açıkça ihlal etmektedir. Müdahale etmeme ilkesinin ihlali ise Uluslararası teamül hukukunun çiğnenmesi anlamına gelmektedir.

Başka bir sorun da konvansiyonel yöntemlerle yapılan saldırılar için yazılmış olan hukuk kurallarının siber uzay gibi çok yeni ve dinamik bir alanda yeni nesil saldırı yöntemleri ile gerçekleştirilen saldırılar için uygulanmaya çalışılmasıdır. Bu durum mevcut hukuk kurallarının yorumlanması yoluyla aşılmaya çalışılmaktadır. Bu da vakit ve dolayısıyla hak kaybına neden olmaktadır. Şöyle ki, büyük ekonomik ve maddi hasara sebep olmuş bir siber saldırı sonrasında ilk belirlenecek husus her saldırıda olduğu gibi öncelikle saldırının BM Şartı 2/4. Maddesinde net bir dille yasaklanan kuvvet kullanımından kaçınma ile ilgili cümlede bahsi geçen kuvvet kullanımı içerisinde sayılıp sayılmayacağıdır. Yani yapılan saldırının bir silahlı saldırı statüsünde olup olmadığına ya da kuvvet kullanımı kapsamına girip girmediğine bakılacaktır. Söz konusu madde ile ilgili yorum yapılırken de 1969 Viyana Antlaşmalar Hukuku Sözleşmesinin 31/1.” Maddesinde geçen: "Bir antlaşma hükümlerine, antlaşmanın bütünü içinde konu ve amacının ışığında, verilecek alelade manaya uygun şekilde iyi niyetle yorumlanır." ifadesi dikkate alınarak yorum yapılır (file:///Users/MelekAsli/Downloads/Viyana_Antlaşmalar_Hukuku_Sözleşmesi.pdf 11.12.2024). Bu durumda BM antlaşması 2/4. maddede bahsi geçen kuvvet kullanımından kaçınma ifadesi antlaşmanın bütünü içerisinde ve iyi niyetle yorumlandığında BM antlaşmasının amacı olan barışın korunması ilkesi gereği kuvvet kullanma aracı olarak neyin kullanıldığı değil kuvvet kullanımı neticesinde barışın tehlikeye girmesi söz konusu olduğundan antlaşmanın hükmü belirli bir silaha işaret etmemektedir. Yani silah olarak neyin kullanıldığı değil onun kuvvet kullanma aracı olarak kullanılmış olması ve sonucunda barışın ihlal edilmiş olması baz alınmaktadır. Hangi eylemin saldırı olarak kabul edileceği ise BM Genel Kurulunun 3314 sayılı (XXIX) 1974 tarihli kararının 1. maddesinde: "*Saldırı, bir devletin, diğer bir devletin egemenliğine, ülke bütünlüğüne veya siyasi bağımsızlığına karşı veya iş bu tanımda belirtildiği üzere BM Antlaşması ile bağdaşmayan diğer herhangi bir tarzda silahlı kuvvet kullanılmasıdır.*" şeklinde ifade edilmiştir. Bu tanıma göre, istihdam ettiği siber orduları aracılığı ile yapılacak yoğun bir DoS/DDoS saldırısı ya da özel olarak geliştirdiği bir virüsü, hedef devletin egemenliğine, ülke bütünlüğüne ve bağımsızlığına zarar verecek şekilde ekonomik açıdan yıpratma veya siyasi müdahale aracı olarak kullanmak da siber

araçları silah gibi kullanmak anlamına geleceğinden, saldırı eylemi gerçekleşmiş olacaktır. Üstelik bu durum barışın ihlali anlamına gelecektir.

Bundan başka hangi saldırı türünün silahlı saldırı kategorisine gireceği ise gene aynı kararın 3. maddesinin b bendinde daha net bir ifade ile belirtilmiştir. İlgili maddede silahlı saldırı: “*Bir devletin silahlı kuvvetlerinin başka bir devletin ülkesini bombardıman etmesi veya bir devletin ülkesine karşı herhangi bir şekilde silah kullanması*” şeklinde tanımlanmıştır (BMGK, 1974:

https://inhak.adalet.gov.tr/Resimler/Dokuman/2312020095336bm_31.pdf 13.01.2025 ve Albal, 2018). Bu tanıma göre değerlendirme yapıldığında ‘Bir devletin başka bir devletin ülkesine karşı herhangi bir şekilde silah kullanması’ ifadesinde de saldırının tanımı için kullanılan silahın türü belirtilmemiştir. Sadece herhangi bir şekilde silah kullanılması ifadesi bulunmaktadır.

Ayrıca gene 3314 sayılı 1974 tarihli kararın 4.maddesinde: “*İlgili hükümler tüketici değildir. Güvenlik Konseyi BM Antlaşması hükümlerine göre başka fiillerin de silahlı saldırı teşkil ettiği tespitini yapabilir*” ifadesi yer almaktadır. Buna göre 3.maddede silahlı saldırı kategorisine gireceği belirtilen saldırı türlerinin ya da saldırı silahlarının dışında farklı türde ve saldırı amacıyla kullanılan herhangi bir silahla yapılan eylemin de silahlı saldırı olarak kabul edilebileceği yönünde fikir vermektedir. Bu da günümüzde zararlı yazılımların bir silah olarak kullanılıp hedef devlete çok büyük maddi kayıplar hatta Stuxnet ve ARAMCO saldırılarındaki gibi fiziki hasarlar verilebileceği ve bunun Uluslararası hukuk nezdinde silahlı saldırı kategorisine girebileceği neticesini doğurur. Hatta 2024'de İsrail'in Lübnan'da gerçekleştirdiği ve pek çok kişinin ölmesine neden olan siber saldırı bu konuda artık şüpheye de yer bırakmamaktadır.

Ancak görüldüğü üzere bu sonuçlara da farklı kaynaklardan, farklı sözleşmelerden çıkarımlar ve yorumlar yapılarak varılmaktadır. Üstelik bu yorumlar da farklılık gösterebilir. O nedenle devletler tarafından gerçekleştirilen siber saldırılar ile ilgili net bir tanım, net bir çerçeve ve dolayısıyla da net hükümler henüz oluşturulmamıştır. Bu da kafa karışıklığı ve vakit kaybı yaşanmasına neden olmaktadır.

6.3. Emsal Kabul Edilen Davaların Siber Saldırlara Uygulanması Konusunda Yaşanan Karışıklıklar

Siber saldırılar hususunda bugüne kadar saldırıya uğrayan, zarar gören bir devlet tarafından saldırgan devlet aleyhine bir davanın açılmamış olması ve saldırgan devlete nasıl bir yaptırım uygulanacağı ile ilgili emsal bir kararın olmaması nedeniyle bu saldırılar meydana geldiğinde, siber saldırının bir kuvvet kullanımı mı, silahlı saldırı mı olduğu, saldırının hangi devlet tarafından gerçekleştirildiği, nasıl atıfta bulunulacağı, mağdur devletin uluslararası hukuk açısından hakkını nasıl koruyacağı ya da saldırgan devlete nasıl bir yaptırım uygulanacağı hususunda uluslararası alanda kuvvet kullanımı ve silahlı saldırı konularında emsal kabul edilen davalara ve bu davalarda verilen kararlara bakılmaktadır. Daha önce de belirtildiği gibi emsal kararlar bir kural niteliğinde değildir. Ancak bu gibi konularda fikir oluşmasına yardım etmeleri açısından önem arz etmektedirler.

6.3.1. 1949 Korfu Boğazı Davası Kararının Siber Saldırlara Uygulanması

1946 yılında iki adet İngiliz savaş gemisi Korfu Boğazından geçerken gemilerin daha önce boğaza döşenen mayınlar nedeniyle hasar görmesi sonucunda mürettebattan yaralanan ve ölenlerin olması nedeniyle İngiltere konuyu Uluslararası Adalet Divanına taşımış ve mayınların Arnavutluk tarafından döşendiğini bu nedenle Arnavutluk'un kendisine tazminat ödemesi gerektiğini öne sürmüştür (International Court of Justice.1949:<https://www.icj-cij.org/sites/default/files/case-related/1/001-19490409-JUD-01-00-EN.pdf> 22.02.2025 ve Yazıcı ve İnanç, 2018). Uluslararası Adalet Divanı verdiği kararda Korfu Boğazının uluslararası boğaz statüsünde olduğunu ve dolayısıyla İngilterenin serbest geçiş hakkına sahip olduğunu, Arnavutluk'un kendi karasularına mayın döşeme hakkına sahip olsa da karasularından geçecek olan gemileri uyarma yükümlülüğü olduğunu belirtmiş (Bilge, 1955: 228-242). Durumun Arnavutluk açısından uluslararası hukuki sorumluluk doğurduğuna karar vermiştir (<https://uluslararasıihukukcalismalari.wordpress.com/2017/04/07/korfu-bogazi-davasi-corfu-channel-case-united-kingdom-of-great-britain-and-northern-ireland-v-albania-judgment-of-4-april-1949/> 18.09.2024).

İngiltere ise olay sonrasında Arnavutluk karasularından mayınları temizlemesi nedeniyle Arnavutluk'a karşı müdahale etmeme ilkesini çiğnediği için hukuki açıdan sorumlu bulunmuştur (Bilge, 1955: 228-242).

Uluslararası hukukta ilk itiraz davası olması ve UAD tarafından bu davada verilmiş olan kararın emsal kabul edilmesi nedeniyle oldukça önem arzeden bu davanın neticesinde verilen kararın siber saldırılar hususunda nasıl uygulandığı ya da uygulanabileceği sorusu ise devletlerin bizzat yönetmiş olduğu siber saldırılarda, İngiltere hakkında verilmiş olan müdahale etmeme ilkesinin çiğnenmesi ile alakalı olabilir.

Bunun dışında, Arnavutluk için verilen kararı siber saldırılara uygulamaya çalışırsak; yani bir devletin kendi karasuları içerisinde gerçekleşmesi muhtemel bir siber saldırı ile ilgili başka bir devleti uyarabilmesi eğer saldırı bizzat devletin bir kurumu ya da devlet tarafından bu işle görevlendirilen bir kişi veya grup tarafından yapılacaksa mümkün olabilir. Ancak hiçbir devlet kendi kendisini ele vermeyeceğinden bu durum olası değildir. Eğer saldıran devletin kendisi (bir kurumu ya da devlet tarafından görevlendirilen biri) değilse devletin bir birey tarafından gerçekleştirilmesi muhtemel bir siber saldırıdan haberi olması siber uzay dediğimiz dünyanın karmaşık yapısı nedeniyle neredeyse imkansızdır.

Yani uluslararası alanda emsal olarak kabul edilen bu davanın ve neticesinde verilen kararın devletlerin bizzat yapmış olduğu ya da yapması muhtemel siber saldırılar neticesinde ortaya çıkan sorunlara cevap verebilmesi ancak tam ve kesin bir atıf yapılabilmesi durumunda ya da İngiltere aleyhine verilen kararda olduğu gibi müdahale yasağının çiğnenmesi ile ilgili olabilir.

6.3.2. 1986 Nikaragua Davası Kararının Siber Saldırılarına Uygulanması

Nikaragua'da 1979 yılında Sandinista devrimcilerinin girişimleri ile Samoza rejimi yıkılarak yeni bir hükümet kurulmuştur. Kurulan bu hükümetin SSCB ve Küba gibi Sosyalist rejimlere yakınlığı ABD'yi oldukça rahatsız etmiş bu durumdan duyduğu rahatsızlık nedeniyle ABD yeni rejime karşı muhalif olan silahlı eylemcilere askeri yardım, istihbarat ve ayrıca teknik ve taktik eğitim yardımında bulunmuştur (International Court of Justice, 1984 :<https://www.icj-cij.org/sites/default/files/case-related/70/070->

[19841126-JUD-01-00-EN.pdf](#) 22.02.2025 ve Yılmaz ve Irk, 2015). Nikaragua hükümeti bu yardımdan duyduğu rahatsızlık nedeniyle UAD'a başvurarak ABD'nin kendisine karşı uluslararası hukuktan doğan sorumluluklarını ihlal ettiğini, Nikaragua'nın iç işlerine müdahale ettiğini ve kendisine karşı kuvvet kullanımında bulunduğunu, bu nedenle Uluslararası hukuk kuralları gereğince cezalandırılması gerektiğini belirtmiştir (<https://uluslararasıihukukcalismalari.wordpress.com/2017/02/11/nikaraguada-askeri-ya-da-yari-askeri-faaliyetler-davasi-nikaragua-davasi-case-concerning-military-and-paramilitary-activities-in-and-against-nicaragua-nicaragua-v-united-states-of-amer/> 18.09.2024).

Nikaragua hükümeti ayrıca ABD tarafından kendisinin egemenliğine, toprak bütünlüğüne ve siyasi bağımsızlığına karşı askeri veya yarı askeri faaliyetler sürdürüldüğünü ileri sürmüştür. Yani silahlı saldırıya uğradığı yönünde beyanda bulunmuştur.

UAD dava ile ilgili kararını 1986 yılında vermiş ve kararında ABD'nin Nikaragua hükümetine karşı silahlı gruplara eğitim, silah, finans ve teknik destek vermesinden dolayı ABD'nin uluslararası hukuktan doğan sorumluluklarını ihlal ettiğini, Nikaragua Devletine karşı müdahale etmeme yasağını ve kuvvet kullanma yasağını çiğnediğini belirtmiştir (Beyoğlu, 2016:1-125).

Ancak Divan silahlı saldırıda bulunulduğu konusundaki iddia ile ilgili verdiği kararda silahlı grupları yalnızca eğitmenin ve onlara silah sağlamanın silahlı saldırı eşiğini aştığını, ABD söz konusu silahlı gruplar ile birlikte bizzat eylemlere katılmış ve eylemi yönetmiş olsaydı eğer, bu durumda yapılan işlemin silahlı saldırı eşiğini aşmış olacağı belirtilmiştir (Yılmaz ve Irk, 2015). Neticede mahkeme ABD'yi Nikaragua hükümetine karşı kuvvet kullanma yasağını ve müdahale etmeme yasağını ihlal etmesi nedeniyle Nikaragua'ya tazminat ödemekle yükümlü kılmıştır (Beyoğlu, 2016).

Uluslararası hukukta emsal niteliğinde olan bu kararın siber saldırılar ile ilgili olası bir davaya nasıl ışık tutacağı ise dava sonucunda verilen kararda belirtilen bir devletin başka bir devlete karşı gerçekleştirilen siber saldırıda, saldırganlara konu ile ilgili eğitim, finans ve gerekli ekipmanın sağlanması yoluyla kuvvet kullanımı ve müdahale yasağını çiğnemiş olacağı ihtimali ile ilgilidir. Bu kararın devletlerin bizzat kendi organları aracılığıyla gerçekleştirdikleri siber saldırılarda uygulanması ise gene müdahale yasağının çiğnenmesi ve kuvvet kullanımı üzerine yoğunlaşacaktır. Ancak bu sefer devlet

saldırı sürecini bizzat yönetmiş ve saldırı sürecine katılmış olacağı için bu durum silahlı saldırı olarak nitelendirilebilir.

6.3.3.Eski Yugoslavya Uluslararası Ceza Mahkemesinin Tadić Davası Kararının Siber Saldırlara Uygulanması

Bosna’da 1992-1995 yılları arasında yaşanan soykırım sonrasında karara bağlanan ilk dava Dusko Tadić davasıdır (Demiray, 2024: 93-116). Dusko Tadić Bosna savaşı sürecinde oluşturduğu Tecavüz kampları ve işlediği savaş suçları nedeniyle Eski Yugoslavya Uluslararası Ceza Mahkemesi tarafından yargılanmış ve insanlığa karşı işlenen suçlardan 6 kez ve savaş hukukunu ihlal etme suçlarından 5 kez olmak üzere 11 farklı suçtan hüküm giymiştir. (<https://www.icty.org/en/press/tadic-case-verdict>, 22.02.2025 ve Demiray, 2024).

Mahkeme Eski Yugoslavya Federal Cumhuriyeti’nin sırlara savaş süresince vermiş olduğu askeri ve mali yardım nedeniyle devletin işlenmiş olan soykırım suçundaki sorumluluğunun bulunup bulunmadığını tespit etmek amacıyla genel kontrol testi uygulamıştır (<https://uluslararasıhukukcalismalari.wordpress.com/2016/12/31/soykirim-davasi-case-concerning-the-application-of-the-convention-on-the-prevention-and-punishment-of-crime-of-genocide-bosnia-and-herzegovina-v-serbia-and-montenegro-26-february-2007/> 18.09.2024).

Buna göre eğer YFC, (Yugoslavya Federal Cumhuriyeti Ordusu) soykırım suçunu işleyen sırlara yalnızca askeri ve mali yardım yapmakla kalmayıp, askeri operasyonların planlamasında ve koordinasyonunda da bizzat yer almışsa bu durumda devletin grup üzerinde genel kontrolü olduğuna ve devletin sorumluluğuna hükmedilecektir. Nitekim daha sonra UAD tarafından yapılan yargılamada YFC’nin Sırlara yalnızca askeri ve mali yardım yapmakla kalmayıp sırların yaptıkları katliama iştirak ettiklerine hükmetmiştir (Değer, 2009: 61-95).

Uluslararası alanda emsal olarak kabul edilen bu davanın ve özellikle uygulanan genel kontrol testinin siber saldırılar ile ilgili davalarda uygulanabilmesi ise ; Devlet eliyle X kişiye ya da gruba veyahut da bir terörist grubuna yetki verilerek, teknik ve mali yardımda bulunularak ve bizzat saldırının planlamasını yaparak siber saldırı gerçekleştirilmesi durumunda söz konusu olabilir. Saldırıda devletin sorumluluğunun hangi ölçüde olduğu, devletin saldırı sürecine ne kadar dahil olduğu konusunda genel kontrol testi uygulanarak sonuca ulaşılabilir.

7.Bölüm

Siber Saldırıları ile İlgili Geleceğe Yönelik Öngörüler

7.1. Siber Tehditlerin Gelecekteki Evrimi ve Tehdidin Boyutlarının Anlaşılması

Siber uzay oldukça karmaşık ve dinamik bir yapıya sahiptir. Onu dinamik yapan da artık neredeyse her gün gelişen teknoloji ile birlikte hayatımıza giren teknolojik ve akıllı cihazlardır. Her yeni üretilen teknolojik ve akıllı cihaz internet bağlantısı ile bu alana dahil olmakta ve siber uzay olarak tabir edilen büyük, karmaşık yapıda yerini almaktadır. Hayatımıza pek çok yenilik ve kolaylık getiren bu akıllı cihazlar özellikle kamusal alanda işlemlerin daha kolay yapılmasını sağlayarak iş yükünü ve zaman tasarrufunu artırmıştır. Ayrıca internet bağlantısı ile çalışan akıllı cihazlar sadece kamusal alanda değil, özellikle bankacılık sistemleri, fabrikalar, havaalanları, hastaneler, metrolar, hızlı trenler, barajlar, nükleer santraller, kritik altyapı sistemlerinin işleyişinde ve savunma sanayiinde sürecin yönetiminden tutun da kullanılan silah ve füze sistemlerine kadar her aşamada yer almaktadır.

Özellikle devletler için güç kavramının ayrılmaz bir parçası haline gelen teknolojik gelişmişlik düzeyi, sağladığı avantajların ve kolaylıkların yanında sebep olabileceği dezavantajlarla devletler için hem geliştirilmesi hem de savunmada kalınması gereken bir alan haline almıştır. Esasen teknolojinin saldırı kapasitesine kattığı güç ilk olarak Körfez Savaşı'nda kendini göstermiştir. Füzelerin istenilen noktayı vurması ta o zaman bile teknolojinin gücünün zamanla bunun çok daha ötesine geçeceğini göstermişti (Bıçakçı, 2012:205-226). O zamandan bugüne teknolojinin sürekli gelişimi, saldırının ve saldırmak için kullanılan silahların türünü değiştirmiş, siber uzayda kullanılan sessiz silahların konvansiyonel yöntemlerle verilebilecek hasarlara eşdeğer ölçüde hasar verebileceği 2007'de Estonya siber saldırısı, 2008'de Gürcistan siber saldırısı, 2010'da İran Natanz Nükleer tesisine yapılan Stuxnet siber saldırısı ve 2012'de Suudi ARAMCO şirketine yapılan siber saldırı neticesinde net bir şekilde görülmüştür.

Üstelik en son 18 Eylül 2024 tarihinde İsrail'in Lübnan'da gerçekleştirdiği siber saldırıda meydana gelen ölüm ve yaralanmalar siber saldırıların artık katliama yol açabileceğini de açıkça göstermiştir. Bu yüzden teknolojik açıdan ne kadar gelişmiş olursa uluslararası

alandaki o denli güçlü sayılan devletler arasında aynı ölçüde de tehlike altındadır. Çünkü internete bağlı olarak çalışan tüm sistemler siber saldırıların hedefi olabilecek potansiyele sahiptir. Üstelik teknoloji gelişmeye devam ettikçe tehdidin boyutları da artmaktadır. Bankacılık sistemlerine ya da borsaya yapılacak ve çözümü günler sürebilecek bir siber saldırı bir devlet için altından kalkamayacağı ekonomik kayıplara sebep olabilir. Ya da havaalanı, metro veya hızlı tren gibi ulaşım hizmeti verilen alanlarda veya trafik kontrol sistemlerinde tüm sistemin kontrolünü sağlayan cihazlarda siber saldırı nedeniyle yaşanacak bir arıza çok büyük kazaların yaşanmasına, yaralanmalara ve hatta pek çok kişinin ölmesine neden olabilir.

Bunun yanı sıra nükleer tesislerin, barajların kontrol sistemlerine bulaştırılacak Stuxnet benzeri bir virüs sistemin çalışma düzeninin bozulmasına ve baraj kapaklarının kontrolsüz bir şekilde açılıp sel felaketi yaşanmasına ya da daha tehlikelisi bir nükleer sızıntı tehdidine yol açabilir.

Günümüzde pek çok fabrikada işleyişin ve üretimin hızlandırılması amacıyla endüstriyel robotlar kullanılmaktadır. Bu robotların çalışma sisteminde siber saldırı nedeniyle meydana gelecek bir arıza fabrika içerisinde kazaların ve ölümlerin yaşanmasına sebep olabilir. Savunma sanayiinde kullanılan insansız hava araçlarının, akıllı füze sistemlerinin çalışması sırasında siber saldırı nedeniyle meydana gelebilecek bir programlama hatası çok ciddi tehlikelerin vuku bulmasına sebep olabilir. Siber casusluk yoluyla bu tür cihazlara ait bilgilerin ve/veya devlete ait çok kritik bilgilerin çalınması o devlet için milyarlarca dolarlık kayıplara ve devlete ait çok önemli sırların bir başka devletin eline geçmesine neden olabilir.

Siber uzay kavramı ve beraberinde getirdiği yeni nesil tehdit türleri günümüzde bile bu denli tehlike barındırırken teknolojik gelişim bu hızla devam ettikçe bu yeni nesil saldırı türünün daha etkili ve tehlikeli boyutlara evrilmesi çok da uzak bir gelecekte olmayacaktır. Bu nedenle tehdidin boyutlarının iyi anlaşılması ve bu tehditlere karşı etkili önlemlerin alınması tüm devletler için zorunluluk arz etmektedir.

7.2.Siber Saldırılar İle İlgili Mevcut Durum ve Alınması Gereken Önlemler

Üçüncü ve Dördüncü endüstri devirleri ile başlayan ve günümüzde artık Beşinci endüstri devrimine doğru evrilen baş döndürücü teknolojik gelişmelerin hayatımızı getirdiği nokta ne ondan kaçabildiğimiz ne de kendimizi güvende hissedebildiğimiz bir dünya haline gelmiştir. İnsan eliyle oluşturulan bu yeni dünya, siber uzay dediğimiz alanın hayatımızı yeniden ve geri dönülemez bir biçimde şekillendirdiği, fırsatların ve yeni nesil tehdit türlerinin etrafımızı çevrelediği bir alandır. Bu durum belki de bireylerden çok devletleri etkilemektedir. Baş döndürücü teknolojik ilerlemelere ayak uyduramayan bir devletin var olması, egemenliğini sürdürmesi, güçlü bir devlet olması günümüzde artık imkansız hale gelmiştir. Ancak teknolojik gelişmişlik seviyesi çok yüksek olan devletlerin de hem bu seviyeyi sürekli devam ettirme zorunluluğu vardır. Hem de bu alanda güvenliğini en yüksek seviyede tutmaya mecburdur. Aksi takdirde uluslararası alanda varlığını devam ettirme ya da egemen bir devlet statüsünde kalabilme ihtimali yok denilecek kadar azdır.

Uluslararası alanda getirdiği fırsatların, güç algısına yaptığı katkıların yanında bir virüs ya da günler süren bir DoS ve/veya DDoS saldırısı ile milyarlarca dolarlık kayıp yaşama riski, kritik altyapı sistemlerine veya savunma sistemlerine yapılabilecek bir siber saldırı neticesinde oluşabilecek fiziki hasarların bir devlete altından kalkamayacağı ekonomik ve maddi kayıplar verebilme ihtimali azımsanmayacak kadar büyük bir tehlikedir. Üstelik bu tehlikenin boyutları günümüzde bile bu denli fazlayken ve teknolojinin gelişimi bu denli hızlıyken çok da uzak olmayan bir gelecekte bu tehlikenin hangi boyutlara ulaşabileceği 2024 yılında İsrail'in, Lübnan'da yapmış olduğu katliam gibi siber saldırı neticesinde artık aşikar olmuş ve tehdidin boyutlarının ciddiyeti net bir şekilde anlaşılmıştır.

Şu ana kadar yapılmış olan siber saldırılar neticesinde meydana gelen fiziki hasarların ya da ortaya çıkan milyarlarca dolarlık ekonomik kayıpların sonucunda henüz bu saldırıları yapan devletlerin uluslararası hukuk nezdinde caydırıcı bir ceza almamış olması, saldırıya maruz kalan devletin mağduriyetinin giderilmemiş olması ya da daha da önemlisi saldırının meydana gelmesi halinde bu saldırının nasıl tanımlanacağı, saldırıyı yapan devlete ne tür bir yaptırımın uygulanacağı ile ilgili net hükümlerin olmayışı, bu tür saldırılar neticesinde nasıl karar alınması gerektiği hususunda siber saldırılar ile ilgili hiçbir emsal kararın bulunmayışı bu konuda çok ciddi kafa karışıklıklarının ve

belirsizliklerin yaşanmasına neden olmaktadır. Bunun başlıca nedenlerinden biri saldırıya uğrayan devletin uluslararası alanda zayıf bir görünüm vermemek amacıyla saldırıya uğradığını gizlemesidir. Bu durum zaten bu tür saldırılar ile ilgili gerekli önlemlerin alınmasının önündeki en önemli engellerden biridir.

Bir başka önemli neden de siber uzay kavramı ortaya çıkmadan çok çok önceleri oluşturulmuş uluslararası hukuk kurallarının bu alanda yapılan saldırılarda ne yapılması, nasıl bir yol takip edilmesi gerektiği yönünde tam olarak yanıt veremiyor olmasıdır. Daha önceki bölümlerde de görüldüğü üzere mevcut uluslararası hukuk kuralları ancak yorumlanarak bu yeni nesil saldırıların sonucunda nasıl bir yol izlenmesi gerektiği bulunmaya çalışılmaktadır. Bu da hem fazla vakit kaybına sebep olmakta hem de net bir sonuca varılamamaktadır. Bu sorunun aşılabilmesi için öncelikle, saldırıya uğrayan devletin bunu bir zayıflık olarak görmeyip açıkça saldırıya uğradığını ve saldırının neticesinde ortaya çıkan maddi ve fiziki hasarı belirtmesi gerekmektedir. Böylece bu tür durumlarda uygulanabilecek gerekli hukuki düzenlemenin yapılabilmesi ve benzer bir mağduriyetin yaşanması durumunda nasıl bir yol takip edileceğinin bulunması mümkün hale gelecektir.

Ancak yapılacak düzenlemenin net kurallar koyması önem arz etmektedir. Yorumla açık bir düzenleme yapılması tekrar kafa karışıklığı yaşanmasına neden olacaktır. Örneğin: BM Şartı 2/4.maddesinde bahsi geçen kuvvet kullanma tehdidi ve kuvvet kullanma yasağından antlaşmanın başka bir yerinde bahsedilmemiştir. Hangi tür saldırının kuvvet kullanma kapsamına gireceği ya da siber saldırıların kuvvet kullanımı olarak değerlendirilip değerlendirilmeyeceği, eğer kuvvet kullanımı olarak değerlendirilecekse hangi ölçekte bir siber saldırının kuvvet kullanımı olarak nitelendirileceği konusu muallaktır. Ayrıca BM antlaşması 51.maddede bahsi geçen silahlı saldırı ifadesinde hangi tür silahla saldırmanın meşru müdafaa hakkını doğuracağı konusunda da net bir ifade yoktur. Ancak BM Genel Kurulu 1974 tarihli ve 3314 sayılı kararının 4. maddesinde geçen“ *Güvenlik Konseyi, başka fiillerin (de) saldırı teşkil ettiği tespitini yapabilir*” (BMGK, 1974

https://inhak.adalet.gov.tr/Resimler/Dokuman/2312020095336bm_31.pdf 11.12.2024) ifadesine dayanarak siber saldırılarda kullanılan yöntemlerin de silah olarak kabul edilebileceği sonucuna varılabilmektedir. Görüldüğü gibi bu konu ile ilgili net

tanımlamaların ve net kuralların olmayışı sorunu net bir şekilde belirlemeyi ve çözüme kavuşturmayı zorlaştırmaktadır. Üstelik bugüne kadar yapılmış en tehlikeli siber saldırıların bizzat BM Güvenlik Konseyi üyeleri tarafından yapıldığı düşünüldüğünde böyle bir kararı vermenin bu devletlere bırakılmasının ne kadar doğru olduğu da tartışılır.

Esasen bu tür saldırılarda yoruma yer bırakmayacak şekilde ve hem mağdur olan devletin hakkının korunmasını hem de saldırgan devlete gerekli yaptırımın uygulanmasını sağlayacak, özellikle siber saldırılar ile ilgili bağlayıcı hukuki düzenlemelerin yapılması neredeyse zorunluluk haline gelmiştir. Uluslararası hukuk uzmanlarının ve Birleşmiş Milletlerin bu tehdit karşısında yeni kurallar, yeni ve net hükümler içeren yasalar oluşturmaları, durum daha da karmaşık hale gelmeden bu alanda kafa karışıklıklarına sebep olan sorunların çözümü için yeni ve etkili yollar bulmaları aciliyet arz etmektedir. Hatta sürekli gelişen ve gittikçe baş döndürücü hale gelen teknolojik ilerlemeler siber uzay ve siber saldırılar konusunda yeni hukuki düzenlemelerin de ötesinde yeni oluşumlara gidilmesini de zorunlu kılabilir. Çünkü net olarak anlaşılan bir durum vardır ki yeni nesil tehdit türlerine eski hükümlerle çare bulunamamaktadır.

7.3. Devletlerin ve Uluslararası Örgütlerin Konuyla ilgili Sorumlulukları

Teknolojik gelişmeler dünyada küreselleşme sürecini hızlandırırken bu gelişmelerin beraberinde getirdiği yeni nesil tehdit türlerine karşı alınacak önlemleri tek bir devlet nazarında ya da sadece devletler nazarında ele alıp sorunun çözümü için çerçeveyi daraltmak bu konuda sadece geçici ve etkili olmayan çözümler üretilmesine neden olacaktır. Belki devletler, Rusya'nın yaptığı gibi global DNS¹³ ağı ile bağlantılarını kesip kendi milli DNS sunucularını oluşturarak siber saldırılara karşı devlet bazında önlem alabilirler.

Rusya 11 Mart 2022'de Global DNS ağı ile bağlantısını keserek uzun süredir üzerinde çalıştığı ve RuNet ismini verdiği kendi milli DNS (Etki Alan Adı Sunucusu- Domain Name System)¹⁴ ağına bağlanmış ve böylece küresel DNS ağına bağlıyken maruz

¹³ Küresel DNS (Alan Adı Sistemi) ad sunucusu ağı, alan adlarını IP adreslerine çevirmek için birlikte çalışan bir sunucu sistemidir. Bu devasa ağ küresel olarak yayılmıştır ve web trafiğini amaçlanan hedefine yönlendirerek internetin omurgasını oluşturur. <https://dnsmadeeasy.com/post/global-dns-network-benefits> 15.12.2024

¹⁴ TCP/IP ağları için kullanılan global bir isim çözümleme protokolüdür. DNS sunucuları, URL (Uniform Resource Locator-Tekbiçimli Kaynak Konumlayıcı) veya FQDN (Fully Qualified Domain Name-Tam Etki Alanı Adı)

kalabileceği siber saldırılardan korunmak için bir aşamaya kadar etkili olan bir yol bulmuştur (<https://www.webtekno.com/rusya-kuresel-internet-agiyla-baglantisini-kesti-h82374.html> 15.12.2024).

Böyle bir çözüm devletler için olası bir siber saldırıda küresel ağ ile bağlantısını kesip kendilerini bu saldırılardan koruyabilmeleri açısından umut vericidir. Ancak bu çözümün SCADA sistemleri gibi kapalı devre sistemlere yapılan siber saldırıları nasıl engelleyeceği bilinmemektedir.

Devletler bu şekilde kendi bireysel önlemlerini bir dereceye kadar alabilecek olsalar da artık tüm devletler ve uluslararası örgütler için problem haline gelen ve uluslararası alanda barışın sürdürülebilirliğini tehdit eden siber saldırıların ve siber tehditlerin çözümü için küresel çapta da önlemler alınmalıdır. Çünkü siber uzay hem her devletin kendi sınırları içerisinde bulunan siber alanın hakimiyeti ve getirdiği sorumluluklar açısından hem de küresel anlamda oluşturduğu tehlike açısından çok yönlü ve tüm ülkelerin, uluslararası örgütlerin, askeri ve ekonomik kuruluşların birlikte çalışmasını gerektiren, küresel çözümlerin oluşturulması gereken bir alandır. Bu nedenle siber uzay ve bu alanda saldırı amacıyla kullanılan ve yeni nesil tehdit türleri olarak tabir edilen silahlar konusunda devletlerin, uluslararası alanda bu konunun çözüme kavuşturulması ve birbirleri arasında barışı ihlal edecek tehditlerin oluşturulmaması ile ilgili birbirlerine karşı ve uluslararası hukuk karşısında sorumlulukları olduğu gibi pek çok devletin bir araya gelerek oluşturmuş olduğu uluslararası örgütlerin de bünyesinde barındırdığı, haklarını korumakla yükümlü olduğu devletlere karşı ve uluslararası alanda barışın devamını sağlamak hususunda önemli görevleri mevcuttur.

Bu nedenle hem devletler hem de uluslararası örgütler siber uzay kavramının ortaya çıktığı ilk zamanlardan bugüne bu alanda güvenliği sağlamak için kendi açılarından pek çok önlem almışlardır. Ancak daha önceki bölümlerde de değindiğimiz gibi bu önlemlerin hemen hepsi ya devletlerin kendi kişisel siber alanlarını korumak ve bu alanda saldırı gücünü geliştirmek amacıyla almış olduğu önlemlerdir ya da uluslararası örgütlerin kendi

adreslerini IP'lere çözümleyerek, hatırlanması zor olan IP adresleri yerine daha kolay olan sunucu (host) isimlerinin kullanılmasına olanak verir [https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/dns-\(domain-name-system---etki-alani-ad-sunucusu\)](https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/dns-(domain-name-system---etki-alani-ad-sunucusu)) 15.12.2024

bünyelerinde ve örgütün amacı çerçevesinde almış olduğu sınırlı önlemlerdir. Örneğin Birleşmiş Milletler siber uzay ve siber saldırılar konusunda ilk çalışmayı yapan örgüttür. BM siber uzay ve siber saldırılar ile ilgili ilk çalışmasını 1998 yılında yapmıştır (Akdağ, 2020:523-526). Bu tarihten sonra BM her yıl siber uzay konusunda düzenli olarak çalışma yapmış ve raporlar yayınlamıştır. Ancak bu çalışmaların ve raporların %98 gibi çok büyük bir kısmı teröristler ve teröristlerin yapmış olduğu siber saldırılar üzerine yoğunlaşmış ve devlet kaynaklı siber saldırılar çoğunlukla gözardı edilmiştir.

Birleşmiş Milletler tarafından 2024 yılında imzalanmış olan Siber Suçlar Sözleşmesi ise uluslararası nitelikte olmasına rağmen hem devletlerin birbirlerine karşı yapabilecekleri siber saldırıları kapsamamaktadır hem de henüz yürürlüğe girmemiştir.

Benzer şekilde Avrupa Birliği siber uzay konusunda pek çok çalışma yapmış olsa da bu çalışmalar bireysel bazda (Avrupa birliği vatandaşlarının siber alanda güvenliğinin sağlanması) ve oluşturulması düşünülen Dijital Tek Pazar'ın siber güvenliğinin sağlanması konuları çerçevesinde sınırlı kalmıştır ve ayrıca AB içerisinde siber saldırılar konusunda gelişmiş bir güvenliğe sahip olan bazı devletlerin iş birliği hususunda isteksiz olması AB'nin bu konuda etkin çalışmalar yapmasını ve etkili önlemler almasını zorlaştırmaktadır.

Bu uluslararası kuruluşların içerisinde bugüne kadar siber uzay ile ilgili en kapsamlı çalışmaları yapan, askeri amaçlarla kurulmuş bir savunma örgütü olan NATO'dur (Polat, 2020:135-158). Ancak NATO'da bu konuda üyeleri arasındaki teknolojik gelişmişlik farkı nedeniyle sorun yaşamaktadır. ABD, İngiltere, Almanya, Kanada gibi teknolojik açıdan son derece gelişmiş üyelerin yanı sıra Romanya, Letonya, Karadağ gibi teknolojik açıdan daha geride kalmış ülkeler NATO içerisinde Siber uzay ve siber saldırılar konusunda yapılan çalışmalara, tatbikatlara eşit ölçüde ve gerektiği gibi katılım göstermemektedir. Bu da NATO'nun bir bütün halinde siber savunma konusuna entegre olup bu konuda daha hızlı gelişme kaydetmesine engel olmaktadır.

Öncelikle Birleşmiş Milletler ve AB uluslarüstü iki örgüt olarak konunun öneminin ve barındırdığı potansiyel tehlikenin farkına vararak konuyu tek yönlü değil bütün yönleriyle ele almalı (özellikle devletlerin gerçekleştirdiği siber saldırılar hususunda) ve tüm üye devletleri, hem kendi siber güvenliklerini, siber savunmalarını geliştirme hem de

uluslararası alanda barışı ihlal edecek saldırılardan kaçınma konusunda sık sık bilinçlendirmeli ve örgüt içerisinde uluslararası alanda barışı ihlal edici saldırıda bulunan devlete karşı belirli bir yaptırım uygulamalıdır. Kaldı ki, Endüstriyel Robotların en yüksek oranda kullanıldığı ülkeler Avrupa Birliği içerisinde yer almaktadır (Fırat ve Fırat, 2017:211-223). AB belki de kuruluş amacı gereği konuyu daha çok ekonomik açıdan ve AB vatandaşları özelinde ele almayı tercih edebilir. Ancak endüstriyel robotların, birlik içerisinde anlaşmazlık yaşayan iki devletten biri tarafından siber saldırının hedefi olmasının konuyu ekonomik açıdan çok farklı boyutlara taşıyacağını hesap etmeli ve bununla ilgili önlemleri almalıdır.

Birleşmiş Milletler ise özellikle 2024 yılında İsrail'in Lübnan'da yapmış olduğu siber saldırının ardından artık siber uzay ve siber saldırılar hususunda konuya kısıtlı bir açıdan bakma ve siber saldırıları yalnızca terör ve terörist gruplar çerçevesinde değerlendirme hakkına sahip değildir. Zira siber saldırıyı terörist bir grup gerçekleştirmiş olsa bile bu örgütün arkasında saldırıyı finanse eden, örgüte gerekli ekipman desteğini sağlayan hatta süreci yöneten güç çoğu zaman bir devlettir. Burada aslolan bu şekilde, siber uzayın karmaşık yapısından faydalanarak saldırı suçu işleyen ve bu suçu örtmeye çalışan devletin tespit edilerek uluslararası hukuktan kaynaklanan sorumluluklarından kaçmasını önlemektir. Zira BM'nin kuruluş amacı uluslararası alanda barışın tesis edilmesini sağlamaktır. Hal böyleyken örgüt içerisinde bir devletin siber uzayın karmaşık yapısından faydalanıp kendisini gizleyerek uluslararası hukuk kurallarını ve barışı ihlal etmesi neticesinde gerekli yaptırımı almaması ve bu durumun diğer devletlere bu minvalde cesaret vermesi, BM'nin kuruluş amacına uygun hareket etmediği, uluslararası alanda güvenliği sağlayamadığı neticesini doğuracaktır.

Benzer şekilde NATO'nun da siber güvenlik ve siber savunma konularında yetkinliklerini artırması gerekmektedir ve bunu da siber güvenlik konusunda en zayıf olan üye devletin seviyesini dikkate alarak yapmalıdır. Elbette burada tüm üye devletlerin bu konuda istekli olması ve işbirliği içerisinde hareket etmesi gerekmektedir.

AB ve NATO'nun konuyla ilgili örgüt olarak bireysel sorumlulukları olduğu gibi siber saldırılar ve siber güvenlik konularında birlikte yerine getirmeleri gereken sorumlulukları da mevcuttur. Zira 22 ortak üyeye sahip bu iki örgütün siber güvenlik ve siber saldırılar

gibi artık çağımızın kaçınılmaz bir problemi haline gelen bir konuda ortak çözümler üretmeleri zorunluluk haline gelmiştir. Özellikle Avrupa Birliği'nin konuyu yalnızca AB vatandaşları nezdinde ya da sadece ekonomik meseleler bazında ele almaktan vazgeçerek devlet eliyle yapılan siber saldırılar hususunda da NATO ile çalışmaya ve çözüm üretmeye istekli olması gerekmektedir. Burada AB'ye üye devletlerin de bu konudaki sorunlara çözüm üretmek için çalışmalara katılmaları zorunlu hale getirilmelidir. Zira siber uzay ve bu alandan kaynaklanan yeni nesil tehdit türleri en çok devletler açısından tehlikeli hale gelmiştir. Çünkü bir vatandaşın bireysel açıdan teknolojiye ayak uydurma zorunluluğu yoktur. Ancak bir devletin mevcut teknolojiye ayak uydurma zorunluluğu vardır. Yani devlet teknolojinin, yeni gelişmelerin dışında ya da uzağında duramaz. Bu yüzden hem gelişen ve yenilenen teknolojiye ayak uydurmalı hem de sahip olduğu teknolojik gücü korumalıdır. Bunu yapmak için de işbirliğine ihtiyacı vardır.

Siber güvenlik konusundaki çalışmaları henüz rapor aşamasında olan ITU, WTO ve IMF'in siber güvenlik konusunu ciddiye alarak, çözüm üretmeye çalışmaları oldukça ümit vericidir ancak çalışmaların çerçevesinin genişletilmesi gerekmektedir.

Avrupa Konseyi, Afrika Birliği ve OECD gibi örgütlerin siber güvenlik çalışmalarına gelince, bu örgütler arasında konuya en geniş açıdan yaklaşan OECD'dir. Geliştirilmesi gereken yönleri olmakla birlikte OECD gibi önemli bir uluslararası ekonomik işbirliği örgütünün siber tehditlerin ciddiyetini anlamış ve konuyu küresel boyutta ele almış olması oldukça önemlidir. Avrupa Konseyinin siber güvenlik konusunda yapmış olduğu çalışma ise bu konuda yapılan ilk sözleşme olması dolayısıyla önemli bir yere sahip olsa da sözleşmenin çerçevesi tehdidin boyutları açısından çok sınırlı kalmaktadır. Sözleşmenin çerçevesinin genişletilmesi ve revize edilmesi gerekmektedir.

Afrika Birliği'nin siber güvenlik çalışmaları ise bölgesel bir örgütün bu konuyu ciddiye alarak çalışmalar yapmış olması açısından oldukça umut vericidir. Çünkü bölgesel bir örgüt olsa da insan hakları alanında yapmış olduğu önemli çalışmalarla öne çıkmış böyle etkili bir örgütün siber güvenlik konularında da etkili çalışmalar yürüteceği ve bölgesini aşan bir farkındalık uyandıracığı umudunu artırmaktadır. Ancak elbette tüm bu çalışmalar sürekli gelişen teknoloji ile birlikte revize edilmeye de muhtaçtır.

Diğer yandan uluslararası alanda siber uzay ve siber saldırı kavramları ortaya çıkmadan çok daha önceleri oluşturulmuş olan uluslararası hukuk kurallarının bu yeni tehdit türlerine gerektiği gibi cevap veremediği de artık kabul edilmelidir. Günümüzde özellikle siber uzay ve siber saldırılar hususunda düzenlenen iki belge vardır. Bunlardan biri Tallinn Rehberidir. Ancak o da hukuki açıdan bağlayıcı özelliğe sahip değildir. Yalnızca UAD tarafından yardımcı olarak başvuru bir doktrindir. Diğer de Avrupa Konseyi bünyesinde 1997 yılında oluşturulan siber uzay suçları uzman komitesi tarafından hazırlanıp 2001 yılında Budapeşte de imzalanan Avrupa Konseyi Siber Suçlar Sözleşmesi diğer adıyla Budapeşte Sözleşmesi'dir (Önok, 2013: 1229-1270). Ancak bu sözleşme de az önce de bahsedildiği gibi yalnızca bilgisayar ağları üzerinden işlenen hak ihlalleri, çocuk pornografisi, bilgisayarlarla ilgili dolandırıcılık ve ağ güvenliği ihlallerini konu edinmektedir (<https://www.coe.int/tr/web/impact-convention-human-rights/convention-on-cybercrime> - / 02.02.2025 ve [https://afyonluoglu.org/PublicWebFiles/cyber/legislation/2001-Avrupa Birlięi Siber Suęlar Sözleşmesi-TR.pdf](https://afyonluoglu.org/PublicWebFiles/cyber/legislation/2001-Avrupa_Birlięi_Siber_Suęlar_Sözleşmesi-TR.pdf) 02.02.2025). Daha çok üye devletlerin iç hukuk yollarında vatandaşların bilgisayar kaynaklı saldırılardan korunması amacıyla yapılmış bu sözleşme, devletler tarafından uluslararası alanda gerçekleştirilen siber saldırıları kapsamamaktadır.

Bu nedenle teknoloji bu denli başdöndürücü bir hızla ilerlerken ve beraberinde getirdiği tehlike her gün biraz daha büyürken bu yeni nesil tehditlere eskiden görülmüş ve konuyla ilgili olmayan dava kararlarının yorumlanması ve eski hukuk kuralları ile ya da soruna direk çözüm üretemeyecek sözleşmeler aracılığıyla çözüm bulmaya çalışmak sorunları içinden çıkılmaz hale getirmektedir. Bu yüzden devletler arasında siber saldırıyı caydırıcı hale getirecek, olası bir saldırıda çözüme kısa yollardan gitmeyi ve etkili sonuçlar almayı kolaylaştıracak yolların bir an önce bulunması ve uygulanması artık zorunluluk halini almıştır.

SONUÇ

Küreselleşme olgusunun ve bu olguyu hızlandıran, artıran teknolojik ilerlemelerin hayatımıza getirdiği artıların mı eksilerin mi daha çok olduğu konusu ayrıntılı olarak tartışılması gereken bir konudur. Ancak konuyu devletler açısından ele aldığımızda tehdidin boyutunun çok daha büyük olduğu görülmektedir. Öncelikle eski çağlardan beri süregelen devletlerin güvenlik kaygısı hususunda, daha önceleri ortaya çıkan güvenlik tehditlerine benzemeyen ve tehdidin kaynağının tam olarak bilinemediği, silahı tutan elin görülemediği yeni bir tehdit alanı ve türü ortaya çıkmıştır. Siber uzay olarak tanımlanan bu alan insan eliyle oluşturulmuş yapay bir alandır ve dinamik yapısı gereği teknolojik yenilikler ve internete bağlı olarak çalışan cihaz sayısı arttıkça genişlemeye devam etmektedir. Bu alanda saldırı aracı olarak kullanılan silahlar ise konvansiyonel silahlara benzemeyen, kodlama ve yazılım araçlarıyla yapılan ancak konvansiyonel silahların verdiği hasara eşit ölçüde hatta belki daha fazla hasar verebilen zararlı yazılımlardır.

Günümüzde neredeyse herşeyin internete bağlı olarak çalıştığı, teknolojik gelişmelerin hayatımızı çepeçevre kuşattığı bu sanal dünyada, teknolojik yeniliklere ayak uyduramayan devletlerin uluslararası alanda ayakta kalma, ekonomik bağımsızlığını devam ettirme olasılığı neredeyse sıfırken benzer durum teknolojik açıdan son derece gelişmiş ülkeler için de geçerli olmaya başlamıştır. Devletin teknolojik gelişmişlik seviyesi ne kadar yüksek ise bu seviyeyi koruma ve bu alandan gelebilecek tehditlere karşı hazırlıklı olup bunları bertaraf etme gücü de aynı oranda yüksek olmalıdır. Aksi takdirde sahip olunan akıllı silah sistemleri, akıllı şehirler, işleyişi SCADA sistemleri ile takip edilen barajlar, kritik altyapı sistemleri, nükleer tesisler, akıllı tren sistemleri, metrolar, havaalanları, fabrikalar, yollarda trafiği düzenleme amacıyla kullanılan akıllı trafik sistemleri, kamuda işleyişi hızlandırmak için kullanılan sistemler, hastanelerde kullanılan akıllı sistemler ve robotlar, borsa sistemleri, zararlı bir yazılım ya da günler hatta haftalar sürebilecek bir DoS veya DDoS saldırısı neticesinde işlemez hale gelebilir ve hatta sistemin tamamen çökmesi sorunu yaşanabilir, milyarlarca dolarlık ekonomik kayıplar hatta ölümle sonuçlanan kazalar meydana gelebilir ki, çok yakın bir tarihte İsrail'in Lübnan'da gerçekleştirmiş olduğu siber saldırı, siber katliamın da artık mümkün olduğunu gözler önüne sermiştir.

Siber saldırılarda, saldırının uluslararası hukuk açısından kuvvet kullanma ya da silahlı saldırı kategorisine girip girmediği ve çoğu zaman bu tür saldırıların kim tarafından gerçekleştirildiğinin tespit edilmesi ve saldırıyı yapan devlete atfedilmesi süreci ise çok zor ve çok uzun bir süreç gerektirmektedir. Bu nedenle mağdur olan devletlerin kendilerini tehdit altında hissettikleri ve güvenlik endişesi yaşadıkları bir uluslararası ortam oluşmaktadır. Böyle bir ortamda da barışın ve huzurun tesis edilmesi neredeyse imkansızdır. Bunun nedeni de siber uzay kavramının ortaya çıkmaya başladığı zamandan günümüze kadar uluslararası hukukta siber güvenlik konusunda yapılmış yalnızca iki tane bağlayıcı mutabakat metni olmasıdır. Bunlardan ilki Avrupa Konseyi tarafından hazırlanmış olan Avrupa Konseyi Siber Suçlar Sözleşmesidir. İkincisi ise OECD tarafından hazırlanmış olan Kişisel Verilerin Gizliliğinin Korunması ve Sınırlar Ötesine İletilmesine Dair Klavuzdur. Ancak her iki sözleşmenin de bağlayıcılığının kapsamı kişisel verilerin gizliliği ve korunması çerçevesi ile sınırlıdır.

Günümüzde devletler tarafından gerçekleştirilen ya da gerçekleştirilecek siber saldırılar ile ilgili konularda başvurulabilecek tek ciddi çalışma ise, UAD tarafından yardımcı kaynak olarak kullanılan ancak hukuki açıdan bağlayıcılığı olmayan Tallin Rehberi' dir. Devletler arasındaki saldırılar hususunda hukuki açıdan bağlayıcı olan uluslararası hukuk kurallarının tamamı siber uzay ve siber saldırılar kavramları ortaya çıkmadan çok önceleri geleneksel saldırı sistemlerine karşı koyulmuş kurallardır. Endüstri 5.0 devrimine doğru hızla evrilen teknolojik ilerleme sürecinde bu hızlı teknolojik ilerlemenin beraberinde getirdiği yeni nesil tehdit türlerine 1940'lı yıllarda daha internet kavramı ortaya çıkmadan önce konvansiyonel yöntemlerle yapılan saldırıları önlemek için oluşturulan hukuk kuralları ile çare bulunamayacağı artık net olarak anlaşılmalıdır. Mevcut Uluslararası hukuk kuralları konvansiyonel yöntemlerle gerçekleştirilen saldırılarda bile saldırgan devlete caydırıcı bir yaptırım uygulama ve mağdur devletin mağduriyetinin giderilmesi noktasında çok meşakkatli, uğraştırıcı ve zaman alıcı bir süreç iken, aynı hukuk kurallarının gerçek dünyadan tamamen farklı özelliklere sahip, dinamik ve insan eliyle oluşturulan siber uzay'da ihtiyaçlara cevap vermesini beklemek, ancak etkili çözümlerin bulunmasını geciktirecektir.

Günümüze kadar meydana gelen ve mağdur devlete çok büyük ekonomik kayıplar veren, fiziksel hasarların meydana gelmesine neden olan siber saldırılar sonucunda ne

yapılabileceği, nasıl bir karar alınabileceği şu ana kadar konuyla ilgisi olmayan mahkeme kararlarının yorumlanması yoluyla bulunmaya çalışılmıştır. İsrail'in yapmış olduğu siber katliam sonrasında İsrail Başbakanı Benjamin Netanyahu uluslararası hukuk nezdinde yargılanıyor olsa da nasıl bir yaptırım uygulanacağı henüz bilinmemektedir. Sonuç olarak mağdur olan devletin mağduriyetinin giderilmediği ve saldıran tarafın da bu karışıklıkta kendini gizleme şansı bulup cesaretlendiği ve uluslararası hukuktan kaynaklanan sorumluluklarından kaçtığı bir durum meydana gelmektedir.

Öncelikle uluslararası hukuk uzmanları ve uluslararası örgütler siber uzay'ın çok ciddi tehditler barındıran, gizlenmenin çok kolay olduğu bir alan olduğunu ve bu alanda saldırı silahı olarak kullanılan zararlı yazılımların, DoS ve DDoS ataklarının verdiği zararın konvansiyonel yöntemlerle yapılan bir saldırı neticesinde verilen hasara eşit ölçüde ve belki de daha yıkıcı olabileceğini net olarak kabul etmelidir. Bu konuda uzmanlar arasında fikir ayrılığının olmaması konuya net bir bakış açısıyla yaklaşmayı kolaylaştıracaktır.

Daha sonrasında bu yeni nesil tehdit türlerine karşı caydırıcı ve etkili olabilecek ve tüm uluslararası alanda bağlayıcılığa sahip olacak hukuk kurallarının nasıl oluşturulabileceği ya da bu konuda başka türlü ve daha etkili bir çözüm bulunabilir mi, konusu tartışılmalıdır. BM, AB, NATO, Avrupa Konseyi, Afrika Birliği ve OECD gibi bünyesinde pek çok üye devleti barındıran ve uluslararası alanda etkin olan örgütlerin siber uzay ve siber saldırılar konusunda halihazırda almış oldukları önlemler kendi bünyeleri içerisinde artırılabilir. Hatta uluslararası alanda barışın ve huzur ortamının tesis edilmesi amacıyla kurulmuş olan Birleşmiş Milletlerin ve uluslararası hukuk uzmanlarının bu durumu ciddiye alarak özellikle siber uzay ve siber saldırılar hususunda devletler açısından bağlayıcı, net kavramlar içeren, net kurallar ve yasaklar getiren uluslararası hukuk kurallarının oluşturulmasını sağlaması gerekmektedir. Ancak bu uluslararası ve bölgesel örgütlerin kurulma amaçları farklı olduğu için ve halihazırda pek çok görevleri olduğu için görevi yalnızca siber uzay ve siber güvenlik konularını ele almak olan tamamen yeni bir uluslararası örgüt kurulması ihtimali ele alınabilir.

Kuruluş amacı bakımından Birleşmiş Milletler örgütüne benzeyen ve uluslararası alanda barışın ve huzurun tesisi için çalışacak ancak örgüt yapısı bakımından farklılıklar

gösteren bir Uluslararası Siber Güvenlik Örgütü kurulabilir. Uluslarüstü niteliğe sahip bu örgütün bünyesinde bir de son teknolojik gelişmeleri an be an takip edip raporlayarak bu raporları örgüte bağlı üye ülkelerin temsilcilerine gönderen Siber Teknoloji birimi bulunduran, her üye devletin eşit oranda söz sahibi olacağı ve koyulan kuralların, oluşturulan antlaşmaların her üye devlet tarafından çekincesiz ve eşit ölçüde uygulanacağı bu uluslarüstü örgüte bağlı olarak çalışacak UAD benzeri bir Uluslararası Siber Suçlar Yüksek Mahkemesi oluşturulabilir.

Üye devletlerin uluslararası hukuk uzmanlarının görev yapacağı ve aynı zamanda örgütün en yetkili organı olan bu yüksek mahkeme de kendi içerisinde iki alt birimi barındırır. Birincisi: Mahkemeye elektronik kanıtlar sunacak Siber Uzman Birimi, ikincisi ise, bir enstitü gibi çalışacak ve mahkemenin gelecek yapılanmasında görev alacak uluslararası siber uzay hukuku uzmanlarını yetiştirecek Siber Uzay Hukuku Enstitüsü.

Sürekli gelişen teknoloji karşısında kendisini sürekli geliştirecek, yalnızca siber uzay ve siber saldırılar hususunda görev yapacak, bu alanda yaşanan mağduriyetleri çözmek için bünyesinde uluslararası bir mahkeme de bulunduracak böyle bir örgütün kurulmasının sağlanması ve siber uzay hukuku kurallarının da bu örgüt bünyesinde istihdam edilecek uluslararası siber hukuk uzmanları tarafından oluşturulması siber uzayda mağdur devletin daha mağdur, saldırgan devletin de daha cesur olması ihtimalini ortadan kaldırıp daha adil ve barışçıl bir uluslararası alan oluşturulmasını sağlayabilir.

KAYNAKÇA

Ada, M. ve Çakır, H.(2017) Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi. Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 5 (2017) ss.632-656

Akdağ, İ.(2020) BM Tarafından Gerçekleştirilen Siber Güvenlik Çalışmaları . TASAM-Türk Asya Stratejik Araştırmalar Merkezi.
https://tasam.org/trTR/Icerik/61754/birlesmis_milletler_tarafindan_gerceklestirilen_siber_guvenlik_calismalari 20.08.2024

Albal, E.(2018) Uluslararası Hukukta Saldırı Suçu. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Ana Bilim Dalı, ss.1-200

Alcaraz,C. ve Zeadally, S.(2015) Critical Infrastructure Protection: Requirements and Challenges for the 21st Century. In International Journal of Critical Infrastructure Protection (IJCIP), vol. 8, Elsevier Science, ss. 53-66

Alibasic, A., Al Juraibi, R., Aung, Z., Woon, W.L. ve Omar, M.A. (2017) Cybersecurity For Smart Cities : A Brief Review. Conference Paper in Lecture Notes in Chapter Science. ss. 1-10

Alpyavuz, T. (2009). Soykırım Suçu. Journal of Naval Science and Engineering, Vol. 5, No.1, ss. 49-61

Alshambri, H., Al Zain, M.A., Soh, B., Masud, M. ve Al-Amri, J. (2020) Cybersecurity Attacks on Wireless Sensor Networks in Smart Cities: an Exposition. International Journal of Scientific and Technology Research , cilt :8 , sayı :1, ss.579-584

Altunkaya, Ş., (2022). *Siber Güvenlik ve Ulus-Devlet: Stuxnet Üzerine Bir İnceleme* . Dijitalleşen Dünyada Birey, Toplum, Siyaset Kongresi, İstanbul, Turkey

Arimatsu, L (2012) , A Treaty for Governing Cyber Weapons ; Potential Benefits and Practical Limitations. 2012 4th International Conference on Cyber Conflict, 2012 NATO CCD COE Publications, Tallinn. ss.91-109

Aslay, F.(2017) Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi. International Journal of Multidisciplinary Studies and Innovative Technologies. Vol 1, no: 1 ss. 24-28

Avcı, İ.(2023) Akıllı Ulaşım Sistemlerinde Siber Saldırıları Ve Önlemler. Akıllı Ulaşım Sistemleri ve Uygulamaları Dergisi Cilt:6 – Sayı:1, ss.194-208

Avrupa Konseyi (2001) Avrupa Birliği Siber Suçlar Sözleşmesi. Budapeşte 23.11.2001 Bilişim Güvenliği Ve Bilişim Suçlarına Karşı Mücadele Derneği
<https://www.bg.org.tr/Doc/AvrupaBirligiSiberSuclarSozlesmesi.doc> s.e.t. 18.09.2024

Bayrak, M.(2020) ABD ile Birleşik Krallıkın AB ve NATO Çerçevesinde Siber Alanlarının Tarihsel Analizi. Cyberpolitik Journal, Cilt :5 sayı:9, ss.22-51

Bhardwaj, A., Goundar, S., ve Avasthi, V. (2019) Cybersecurity Attacks on Robotic Platforms. Network Security, ss.13-19

Bıçakcı, S.(2014) “NATO’nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik”, *Uluslararası İlişkiler*, Cilt 10, Sayı 40, ss. 101-130.

Bilge, S.A.(1955) Milletlerarası Adalet Divanının Korfu Boğazı Davası (ilk İtiraz) Hakkında Verdiği 28 Mart 1948 Tarihli Karar. Ankara Üniversitesi SBF Dergisi Cilt: 10, Sayı:1, ss.228-242

Birleşmiş Milletler Genel Kurulu (1970) “Birleşmiş Milletler Antlaşması Doğrultusunda Devletler Arasında Dostça İlişkiler ve İşbirliğine İlişkin Uluslararası Hukuk İlkeleri Konusunda Bildirge” ss.1-11

https://inhak.adalet.gov.tr/Resimler/Dokuman/2312020094506bm_17.pdf 02.02.2025

Birleşmiş Milletler Genel Kurulu (2001) “Draft Articles on Responsibility of States for Internationally Wrongfull Acts with Commentaries”-ARSIWA. ss.1-114

https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

21.02.2025

Bolat, C. (2020) Siber Saldırlara Karşı Meşru Müdafaa Hakkının Uluslararası Hukuk Açısından İncelenmesi. İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalı, ss.1-201

Bozkurt,M.U.(2022) Siber Saldırıların BM Şartı’nda Yer Alan Silahlı Saldırı Kavramı Kapsamında Değerlendirilmesi. Çanakkale Araştırmaları Türk Yılığ, Sayı: 32 ss.21-45

Cerrudo, C. (2015) An Emerging Us (And World) Threat : Cities Wide Open To Cyber Attacks. IOActive Labs, report. ss.1-22

Collins, S. ve McCombie, S.(2012) Stuxnex: The Emergence of a New Cyber Weapon and Its Implications. Journal of Policing Intelligence and Counter Terrorism. 7 /1 , ss.80-91

Choucri, N., & Clark, D. D. (2013). Who controls cyberspace? Bulletin of the Atomic Scientists, 69(5), ss. 21–31

Çakır, Sönmez, F. Vd. (2018) Nesnelerin İnterneti ve Giyilebilir Teknolojiler. Sosyal Araştırmalar ve Davranış Bilimleri Dergisi, Cilt 4, Sayı. 5 , ss.84-95

Çakır, A.C. , Yiğit, H. ve Küçük, K. (2019) Nesnelerin İnterneti Tabanlı Akıllı Şehirler Üzerine Bir İnceleme. UMYOS’19 Sinop, 8. Uluslararası Meslek Yüksekokulları Sempozyumu, ss. 691-702

Çahmutoğlu, E. (2020) Siber Uzayda Güç ve Siber Silah Teknolojilerinin Küresel Etkisi. Analytical Politics. Cilt:1 Sayı:1, ss.1-17

Çelik, Ş. (2014) Stuxnet Saldırısı ve Abd'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Cilt: 15, Sayı: 1, 2013, ss. 137-175

Çelik, S.(2018) Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım. Academic Rewiev of Humanities and Social Sciences cilt.1/ sayı 2 ss. 110-119

Çelik, S. ve Gürkaynak, M.(2019) The New Front in Global Insecurity : Cyberspace. International Journal of Social Inquiry cilt.12, sayı.2 , ss.545-566

Çengelci, B. ve Çimen, H. (2005) Endüstriyel Robotlar. Makine Teknolojileri Elektronik Dergisi 2005 (2), ss. 69-78

D'Amato, A.(2012) International Law, Cybernetics and Cyberspace. International Law Studies cilt.76, ss.60-71

Datta, S.K. ve Bonnet, C. (2015) Internet of Things and M2M Communications as Enablers of Smart City Initiatives. International Conference on Next Generation Mobile Applications, Services and Technologies. Conferans bildirisi, ss.1-7

Dal, U.(2019) Uluslararası Sorumluluk Hukukunda Uluslararası Hukuka Aykırı Eylemin Devlete Atfedilmesi. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı, ss.5-205

Darıcı, A.B (2017) Amerika Birleşik Devletleri Ve Rusya Federasyonunun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi. Uludağ Üniversitesi Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalı, Doktora Tezi, ss.1-241

Darıcı, A.B.(2018) Askerileştirilen ve Silahlandırılan Siber Uzay. Sosyal ve Beşeri Bilimlere Dair Araştırma Örnekleri, ss.311-327

Darıcı, A.B. (2020) Devletlerin Siber Espiyonaj Faaliyetleri; Uluslararası Sistem ve Güvenlik. Contemporary Issues of International Relations: Problems of International

Community, Cyber Espionage Activities Of States: International System And Security, ss. 21-37, Cambridge Scholar Publishing, U.K.

Dartmouth College (1956) <https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth> 19.09.2024

Dennis, M.A. (2024) Defense Advanced Research Projects Agency (DARPA) . Britannica <https://www.britannica.com/topic/Defense-Advanced-Research-Projects-Agency> 29.09.2024

Değdaş,U.C.(2018) Uluslararası Hukukta Önleyici Meşru Müdafaa Hakkı. Hukuk Fakültesi Dergisi, cilt:1 ,sayı:6, ss.21-40

Değer, O.(2009) Soykırım Suçu ve Devletin Sorumluluğu: Uluslararası Adalet Divanı’nın Bosna-Hersek v. Sırbistan-Karadağ Kararı, Uluslararası İlişkiler, Cilt 6, Sayı 22 (Yaz 2009), s. 61-95.

Demiray, Ş.N.(2024) Eski Yugoslavya için Uluslararası Ceza Mahkemesinin Tadiç Kararı İncelemesi. Tokat Gaziosmanpaşa Üniversitesi Hukuk Fakültesi Dergisi. Cilt:2 Sayı:1 ss. 93-116

Demirtaş, Yalaman, M.(2023) Kuruluşundan Günümüze Dünya Ticaret Örgütünün Küresel Ticaretteki Rol ve İşlevi. İstanbul Ticaret Üniversitesi Dış Ticaret Dergisi. Cilt:1 Sayı:1. ss.32-41

Dilek, E., Talih, Ö. ve Bensghir Kaya, T. (2023) Estonya 2007 Siber Saldırılarının İncelenmesi ve Ülkelerin Ulusal Güvenlik Politikalarına Etkileri. Bilgi Yönetimi Dergisi Cilt :6, Sayı : 2 , ss. 332-347

Dilibal, S. ve Şahin, H. (2018) İşbirlikçi Endüstriyel Robotlar ve Dijital Endüstri. Uluslararası 3D Yazıcı Teknolojileri Ve Dijital Endüstri Dergisi. 2:1, ss.86-95

Dost, S.(2023) Yapay Zeka ve Uluslararası Hukukun Geleceđi. SDÜHFD Cilt: 13 Sayı:2 ss.1272-1313

Dudek, W. ve Szykiewicz, W. (2019) Cyber-security for Mobile Service Robots - Challenges for Cyber-physical System Safety. Journal of Telecommunications and Information Technology no: 2 ,ss.29-36

Düger, Y. (2023) Akıllı şehirleri bekleyen temel hak ve özgürlük ihlalleri, Urban 21 Journal, cilt: 1 sayı: 1, ss. 1-15

Ekiz, H. ,Vatansever, F., Zengin, A. ve Demir, Z. (2000) Hesaplamanın Tarihi ve Bilgisayarların Gelişimi. SAÜ Fen Bilimleri Enstitüsü Dergisi, 4.Cilt, 1. ve 2.sayı, ss.73-81

Erdem, Ö.ve Kara, M. (2015) Honey Thing: Nesnelerin İnterneti İçin Tuzak Sistem. Conference: 8th International Conference on Information Security and Cryptology ss.1-6

Erdem, T. (2020) 21. Yüzyılda Uluslararası İlişkilerde Yeni Güç Rekabet Sahası: Siber Uzay, T.C. Trakya Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Anabilim Dalı Doktora Tezi ss.1-404

Eren, V. ve Aydın, A. (2014) Sosyal Medyanın Kamuoyu Oluşturmadaki Rolü ve Muhtemel Riskler, KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi 16 (Özel Sayı I): ss.197-205

Eren, M.(2016) AB'nin Siber Güvenlik Politikası. Marmara Üniversitesi Avrupa Birliği Enstitüsü, Avrupa Birliği Siyaseti ve Uluslararası İlişkiler Ana Bilim Dalı ss.1-137

Erkiner, H.H. (2007). Devletin Haksız Fiilden Dolayı Uluslararası Sorumluluğunda Uluslararası Hukuk Komisyonu'nun Tespit Ettiđi İsnat Kuralları. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi , cilt.13, ss. 145-180

Erkiner, H.H. ve Tezel, A. (2022) Uluslararası Teamül Hukuku Kurallarının Varlığının ve Değişiminin Tespiti. Marmara Üniversitesi Hukuk Araştırmaları Dergisi, Cilt 28, Sayı 2, ss 662-693, Marmara Üniversitesi Hukuk Fakültesi'nin Kuruluşunun 40. Yılı Özel Sayısı

Farwell, J.P and Rohozinski, R.(2011) Stuxnet and the Future of Cyber War, Survival: Global Politics and Strategy, 53: 1, ss. 23-40

Fırat, O.Z. ve Fırat, S.Ü.(2017) Endüstri 4.0 Yolculuğunda Trendler ve Robotlar. İstanbul Üniversitesi İşletme Fakültesi Dergisi, cilt: 46, sayı:2, ss.211-223

Fırat, O.Z. ve Fırat, S.Ü.(2017) Dördüncü Sanayi Devriminde Riskler : Robotlar ve Yapay Zekanın Yönetişim Sorunları. Global Sanayici: Ekonomi ve İş Dünyası Dergisi, Yıl: 8 Sayı:81, ss.66-70

Fırat, T.(2021) Stratejik bir Belirsizlik Alanı Olan Siber Uzayda Norm Oluşturma Çabalarının İncelenmesi. Yalova Üniversitesi Lisansüstü Eğitim Enstitüsü, Uluslararası ilişkiler ana bilim dalı, ss 1-121

Foltz, By. A.C. (2012) Stuxnet, Schmitt Analysis and The Cyber “Use of Force” Debate. JFQ / sayı. 67, ss. 40-48

Ford.C.A.(2020) International Security in Cyberspace : New Models for Reducing Risk. Arms Control and International Security Papers cilt: 1/ sayı: 20, ss.1-8

Got, A. Technological Revolutions in War : From the Onset of the Industrial Age to the 21st Century. Askeri Tarih Araştırmaları Yıllık Raporu No: 23, ss. 75-83

Gökçer, O. ve Ercan, P.G.(2020) Siber Savaşlarda Jus ad Bellum ve Jus in Bello. Alternatif Politika, 12 (1): 172-203

Gökkoyun, S.C. ve Şengül, S.(2019) Siber Alemin Muhafızları : Beyaz Şapkalı Hackerlar
<https://www.aa.com.tr/tr/bilim-teknoloji/siber-alemin-muhafizlari-beyaz-sapkali-hackerlar/1417719> 17.06.2024

Gönen, S. , Yılmaz, E.N., Şanoğlu,S., Karacayılmaz, G. ve Özbirinci, Ö. (2021) Endüstri 4.0 Sürecinde Unutulan Bileşen : Siber Güvenlik. Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 9 , ss.1142-1158

Görkem, L. ve Bozuklu, M. (2016) Nesnelerin İnterneti : Yapılan Çalışmalar ve Ülkemizdeki Mevcut Durum. Gaziosmanpaşa Bilimsel Araştırma Dergisi, Sayı:13, ss.47-68

Gözcan, Z.(2019) Geleneksel Savaş Kavramı ve Siber Savaş : Siyasal ve Hukuksal Değerlendirmeler. Çanakkale Onsekiz Mart Üniversitesi Sosyal Bilimler Ens.Uluslararası İlişkiler Anabilim Dalı. ss. 1-106

Güçdemir, Y.(2012). Bilgisayar Ağları, İnternetin Gelişimi ve Bilgi Kirlenmesi. İstanbul Üniversitesi İletişim Fakültesi Dergisi / Istanbul University Faculty of Communication Journal (17). ss.371-379

Güdek, B. (2023) Endüstriyel Dönüşüm ve Endüstri 5.0. Ömer Halisdemir Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi Yıl: 2023 Cilt-Sayı: 16(4) ss: 1129–1142

Güldoğan, M.V.(2022) Siber Savaşta Mütakabiliyet. Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Gazetecilik Anabilim Dalı, Bilişim Bölümü ss.1-168

Güllü, O. (2022). Yapay Zekânın Yükselişi: İnsan Öğrenmesi Makine Öğrenmesi Oyun Karşılaşmaları. ISophos: Uluslararası Bilişim, Teknoloji ve Felsefe Dergisi, Cilt 3, Sayı 7, ss: 19-30.

Gültekin, O. (2022) Siber Saldırıları ve Uluslararası Güvenlik. Selçuk Üniversitesi Uluslararası İlişkiler Ana Bilim Dalı, Uluslararası İlişkiler Bölümü, ss. 1-91

Gümüşbaş, A. (2018) Siber Savaş Hukukunda Meşru Müdafaa Hakkı ve İsnat Edilebilirlik: Stuxnet ve Aramco Saldırıları. TASAM, ss.181-194

Güneş, A.(2019) Küresel Güçlerin Ulusal Siber Güvenlik Stratejileri, Cyberpolitic Journal, Cilt:4, Sayı: 8, ss.242-258

Güntay, V. (2019) 21.YY. Paradoksu Olarak Siber Uzay ve Uluslararası Hukuk. Journal of Politics and International Relations. cilt.1 / sayı: 2 , ss.87-109

Güreşçi, R. (2019) Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirmesi. Savunma Bilimleri Dergisi Mayıs 2019/ Cilt: 18/ Sayı: 1 ss.75-98

Hathaway, O. (2011) The Law of Cyber Attack. California Review Jenuary 2011 ss. 1-72

Helmbrecht, U. (2017) ENISA Overview of Cybersecurity and Related Terminology, Version 1, September 2017

Herzog.S.(2011) Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security , cilt. 4, sayı. 2, Strategic Security in the Cyber Age (Summer 2011), ss. 49-60

Holat, O. (2021) Yeni medya ve siber savaş kavramları bağlamında Stuxnet saldırısı örneğinin incelenmesi. Abant Kültürel Araştırmalar Dergisi, 6(11): 105-125

International Court of Justice Reports (1949) Corfu Channel Case, Judgement of April 9th 1949: I.C.J. Reports 1949, s.4 <https://www.icj-cij.org/sites/default/files/case-related/1/001-19490409-JUD-01-00-EN.pdf> 22.02.2025

International Court of Justice (1984) Case Concerning Military and Paramilitary Activities on and against Nicaragua, ss.392 , <https://www.icj-cij.org/sites/default/files/case-related/70/070-19841126-JUD-01-00-EN.pdf> 22.02.2025

İTÜBİDB <https://bidb.itu.edu.tr/sevir-defteri/blog/2013/09/07/internet%27in-tarihçesi>
20.09.2024

Kanat, S. ve Akoğuz, N. O. (2024) Uluslararası İlişkiler ve Yapay Zeka : Uluslararası Güvenlik Açısından Bir Değerlendirme. Sosyal Ve Beşeri Bilimler Araştırmaları Dergisi Cilt :25 Sayı:54, ss.60-73

Kara, M. (2013) Siber Saldırıları - Siber Savaşlar ve Etkileri. İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, ss. 1-85

Karadağ, U.(2016) Birleşmiş Milletler Antlaşmasına Göre Meşru Müdafaa Hakkı. İnönü Üniversitesi Hukuk Fakültesi Dergisi Cilt:7 Sayı:2, ss.171-185

Karadağ, Ş.(2019) Siber Uzayda Uluslararası Hukuk Mümkün Mü? International Social Sciences Studies Journal 5(36) ss.2827-2833

Karagül, S. ve Özkan. M.F (2015) Bilgi Teknolojileri Ve Uluslararası İlişkilerde Fırsat-Tehdit Paradoksu. Bilgi Ekonomisi ve Yönetimi Dergisi 2015 Cilt: X Sayı: I ss. 115-127

Karabacak, E.K.(2022) Terör Örgütlerinin Siber Uzay Kullanımı : DEAŞ Örneği. EBYÜ İİBF Dergisi, Haziran 2022, 4(1), ss. 51-64

Karakuş, G. ve Gönen, İ. (2022). Askeri Alanda Endüstri 4.0 Uygulamaları. *Avrupa Bilim ve Teknoloji Dergisi*, (43), ss.104-109.

Kasapoğlu, C.(2017) Hayaletlerin İzlerini Sürmek : Uluslararası Nitelikteki Siber Saldırıların Soruşturulması. EDAM, Siber Politikalar ve Dijital Demokrasi 2017/4 ss.1-14

Karasoy, H. A. ve Gezici, H.S. (2023) Bombalardan Baytlara: Siber Güvenliğin Ulusal Güvenlikteki Rolü ve Yapay Zekanın Siber Güvenlikteki Önemi. Uluslararası Yönetim ve Ekonomi Dergisi, Cilt :6 Sayı:1, ss.173-188

Keser, L. (2001) İlk Görünüş İspatı. Dokuz Eylül Üniversitesi Hukuk Fakültesi, İzmir. 1.Basım. ss.231-252

Kılıç, R.(2023) Sanayi Devrimlerinin Serüveni: Endüstr 1.0’dan Endüstri 5.0’a. Takvim-i Vekayi, Cilt: 11, No: 2, ss.276-291

Koçak, Alan, A.,Tümer, Kabadayı, E. ve Cavdar, N. (2018) Yeni nesil bağlantı ve yeni nesil iletişim : Nesnelerin interneti üzerine bir inceleme İşletme Araştırmaları Dergisi 10/1 ss.294-320

Koh, H. H.(2012) International Law in Cyberspace. Harward International Law Journal cilt.54 ss.1-12

Korhan, S.(2018) Siber Uzayda Uluslararası İlişkilerin Değişen Parametreleri, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Ana Bilim Dalı, Uluslararası İlişkiler Bölümü, ss.1-84

Korhan, S.(2024) Küresel Dijital Yönetişim Sorunu : Siber Hukuk Bağlamında İnternet Yönetişimi Forumu (IGF) Örneği. İstanbul Medeniyet Üniversitesi, Lisansüstü Eğitim Enstitüsü, Uluslararası İlişkiler Anabilim Dalı, ss. 1-412

Koşunalp, S. Ve Arucu, M.(2018) Nesnelerin İnterneti ve Akıllı Ulaşım. Akıllı Ulaşım Sistemleri ve Uygulamaları Dergisi. C.1 Sayı 1, ss.1-7

Köker. A(2022) Avrupa Birliğinin Gelişen ve Değişen Tehdit Algısı: Siber Güvenlik , EUROPolitika S.14, ss.48 – 77

Köksoy, F. (2020) Avrupa Birliği’nin Siber Güvenlik Politikası: Kurumsalcılık mı Tutarlılık mı? Güv. Str. Derg. 2020, 16(35): ss. 635-674

Kutup, N.(2016) Nesnelerin İnterneti; 4H Her yerden, Herkesle, Her zaman, Her nesne ile Bağlantı. İzmir Ekonomi Üniversitesi

Kumtepe, Kadioğlu, C.Ç (2022) Siber Uzayda Kuvvet Kullanma Yasağı ve Yasağın İstisnalarının Geçerliliğinin Tallinn Rehberi Kapsamında Değerlendirilmesi. The Turkish Yearbook of International Relations cilt: 53, ss.21-40

Kutlu, F. B. (2023). A New Field Between Two Old Allies: Cybersecurity Approaches of EU and NATO (2016 – 2020). Journal of Diplomatic Research, 5(1), ss. 25-41

Kuvancı, B. ve Akın, F.(2020) Dördüncü Sanayi Devriminin Bir Sonucu Olarak Siber Tehditler Ve Siber Güvenliğin Aile, Şirket Ve Devlet Bazında Önemi. Dergipark akademik / İş ve Hayat , Cilt:6, Sayı: 11, ss.24-45

<https://dergipark.org.tr/tr/pub/isvehayat/issue/57736/823535> s.e.t. 17.08.2024

Lee, T.B (1989) Information Management: A Proposal. CERN DD/OC (Mart 1989) ss.1-17.

Lin, H.S.(2010) Offensive Cyber Operations and The Use Of Force. Journal Of National Security Law And Policy. Cilt :4 Sayı:63. ss.63-86

Loukas, G. (2015) Cyber-Physical Attack : A Growing Invisible Threat. Butterworth - Heinemann is an Imprint of Elsevier. ss. 1-255

https://books.google.com.tr/books?id= OicBAAQBAJ&pg=PR7&hl=tr&source=gbs_selected_pages&cad=1 - v=onepage&q&f=false 15.11.2024

Maurer, T. ve Nelson, A. (2021) The Global Cyber Threat. Finance and Development. Mart 2021. ss.24-27

Memiş, U.(2015) Siber Caydırıcılık Kavramının Nükleer Caydırıcılık Olgusu İle Karşılaştırmalı Analizi. Uludağ Üniversitesi Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Ana Bilim Dalı. ss.1-151

Memiş, U.(2018) Bir Güvenlik Sorunu Olarak Siber Uzay. Türk Asya Araştırmaları Merkezi, TASAM.

[https://tasam.org/tr TR/Icerik/50249/bir_guvenlik_sorunu_olarak_siber_uzay](https://tasam.org/tr_TR/Icerik/50249/bir_guvenlik_sorunu_olarak_siber_uzay)
[20.09.2024](https://tasam.org/tr_TR/Icerik/50249/bir_guvenlik_sorunu_olarak_siber_uzay)

Malwarebytes sitesi <https://www.malwarebytes.com/logic-bomb> 17.09.2024

McCarthy, J., Minsky, M.L., Rochester, N. ve Shannon, C.E.(1956) A Proposal For The Dartmouth Summer Research Project On Artificial Intelligence, Dartmouth College
<https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth> 18.09.2024

Morantes, S., Victores, J.G. ve Balaguer C. (2015) Cryptorobotics : Why Robots Need Cyber Safety. Frontiers in Robotics and AI. makale 23, ss.1-4

Natalucci, F., Qureshi, M.S. VE Suntheim, F. (2024) Rising Cyber Threats Pose Serious Concerns for Financial Stability. IMF Blog
<https://meetings.imf.org/en/IMF/Home/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability> 31.01.2025

Orak, M. (2022) Siber Ordular ve Siber Savaşlar. KAYTEK Dergisi Yıl: 3 Sayı: 2
Tarih: 2021 ss: 214-226

Önal, M.A.(2021) Siber Uzay ve Güvenlik İlişkisi Bağlamında Siber Güvenliğin Boyutları. Hitit Ekonomi ve Politika Dergisi. Cilt:1 Sayı:2 ss.114-123

Önok, M. (2013) Avrupa Konseyi Siber Suçlar Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi Cilt: 19, Sayı :2 ,ss.1229-1270

Özcan, Yıldırım, K. (2023) Akıllı Şehir Bileşenleri- Akıllı Şehir Uygulamaları ve Akıllı Mekan Yönetimi. Mediterranean Journal of Humanities. mjh.akdeniz.edu.tr XIII, ss. 295-310

Özkan, İ. (2019) Siber Saldırıların Ekonomik Boyutu . Bilecik Şeyh Edebali Üniversitesi Sosyal Bilimler Enstitüsü İktisat Anabilim Dalı ss 1-185

Öztemel, E., (2020). Yapay Zekâ ve İnsanlığın Geleceği. *Bilişim Teknolojileri ve İletişim* , Ankara: Türkiye Bilimler Akademisi. ss.75-91

Polat, D.Ş.(2020) NATO'nun Yeni Operasyon Alanı : Siber Uzay. Güvenlik Bilimleri Dergisi, Şubat 2020 , UGK Özel Sayısı ss.135-158

Polat, D.Ş. (2020) Kuruluşundan Çöküşüne Milletler Cemiyeti Sistemi. Elektronik Sosyal Bilimler Dergisi, Ekim/October(2020) - Cilt:19 - Sayı:76 , ss.1950-1967

Prim, H. (2006) Yapay Zeka. Journal of Yaşar University, 1(1), ss.81-93

Poyraz, M. (2024)‘Silahlandırılmış Yapay Zekâ Otonom Silah Sistemleri ve Uluslararası Hukuk’, Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi 14(1), ss. 887-894

Published by the International Criminal Court (2021) Rome Statue of International Criminal Court of Justice ss.1-89

Rahman, T.N., Khan, N. ve Zaman, Z.I. (2024) Redefining Computing : Rise of Arm from Consumer to Cloud of Energy Efficiency. World Journal of Advanced Research and Reviews. 21(1), ss. 817-835

Sambur, B.(2016) By Nazlı Couchri Cyberpolitics in International Relations. Cambridge MIT Press (2012) Cyberpolitic Journal cilt.1 sayı.1
web page : www.cyberpoliticjournal.org 20.08.2024

Saldırı'nın (Tecavüzün) Tanımı : Birleşmiş Milletler Genel Kurulu'nun 3314 (XXIX) Sayılı ve 1974 Tarihli Kararı
http://inhak.adalet.gov.tr/Resimler/Dokuman/2312020095336bm_31.pdf 18.01.2025

Sarı, O. (2013) Uluslararası Hukuk ve Türk Ceza Hukuku Bağlamında Siber Güvenlik ve Bilişim Sistemlerine Yönelik Suçlar. Harp Akademileri Stratejik Araştırmalar Enstitüsü, Harp/Harekat Hukuku Anabilim Dalı Yüksek Lisans Tezi ss.1-246

Schmitt, M. N. vd. (2013) Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence ss.1-215

Schmitt, M.N. (2017) Grey Zones in the International Law of Cyberspace. The Yale Journal Of International Law , cilt. 42: 2 , ss. 1-21

Shen, Y.(2015) Cyber Sovereignty and the Governance of Global Cyberspace. Chin. Polit. Sci.Rev. 1. ss.81-93

Şafak, E.(2019) Uluslararası Hukukta Değişen Güvenlik Algısı ve Saldırı Suçu Bağlamında Siber Saldırıları”, SÜHFD., C. 28, S. 1, 2020, s. 127-160

Şafak, E.(2020) Uluslararası Hukuk Bağlamında Siber Savaş ve Savaş Hukuku Kurallarının Siber Savaşa Uygulanabilirliği Meselesi. New World Architecture Of Economy And Security ss.215-253

Tarhan, K. (2018) Uluslararası Güvenliğin Bir Bileşeni Olarak Siber Güvenlik. Selçuk Üniversitesi Uluslararası İlişkiler Anabilim dalı Uluslararası İlişkiler Bölümü, ss. 1-88

Temel, H. (2021) Kuvvet Kullanma Hukuku Kapsamında Siber Saldırı Kavramı. Milli Savunma Üniversitesi Yayınları , Yayın Numarası : 21/02 ss. 122-158

Terzi, M.(2018) 2016-2019 Ulusal Siber Güvenlik Strateji Belgesi Kapsamında Türkiye İncelemesi. Kara Harp Okulu Bilim Dergisi cilt: 28, sayı: 1, ss. 73-108

Tosun, F.(2009) “Uluslararası Hukuk’ta ‘Kuvvet Kullanma ve Karışma’ Kavramlarının Değişen Anlamı.” Güvenlik Stratejileri Dergisi. Cilt:5 sayı:9, ss.89-118

Tozkoparan, İ.B.(2019) Değişen Güvenlik Anlayışında Geleceğin Akıllı Kentleri. ASSAM Uluslararası Hakemli Dergi 13. Uluslararası Kamu Yönetimi Sempozyumu Bildirileri Özel Sayısı. ss.417-427

Tugay, B. ve Tugay, R. (2019). “Uluslararası Sistemin Geleceğini Yapay Zekâ Üzerinden Analiz Etmek”, Journal of Academic Value Studies, Cilt:5, Sayı:3; ss. 376-384

Turak, Y. (2015) Nesnelerin İnterneti ve Güvenliği ss.1-14

UNIDIR (2017) The United Nations, Cyberspace and International Peace and Security, Responding to Complexity in the 21st Century. UNIDIR Resources, ss.1-82

UN General Assembly (1974) Definition of Aggression, United Nations Audiovisual Library of International Law, ss 1-4

Uçan, R., Karacığan, A.O. ve ESKİCUMALI, E.(2022) Endüstriyel Robotlarda Güvenli Çalışmaya İlişkin Esaslar Ve Uygulamalar. İksad Yayınevi, ss.1-260

Ünal, A.N ve Yarman, B.S.B (2014) Milli Güç Unsurlarının Belirlenmesinde Siber Uzay Faktörü, 7th International Conference on Information Security and Criptology. ss.278-284

Ünver, M., Canbay, C. ve Mirzaoğlu, A.G. (2011) Uluslararası Kuruluşların Siber Güvenlik Faaliyetleri. 1. Basım. Bilgi Teknolojileri Ve İletişim Kurumu. ss.1-28

Varshney, H., Kahn, R.A., Khan, U. ve Verma,R. (2021) Approaches Of Artificial Intelligence And Machine Learning in Smart Cities : Critical Review. IOP Conference Series : Materials Science and Engineering, 1022. ss.1-11

Viyana Antlaşmalar Hukuku Sözleşmesi (22 Mayıs 1969) 31/1. madde. BM Enformasyon Merkezi UNIC Ankara [file:///Users/MelekAsli/Downloads/Viyana Antlaşmalar Hukuku Sözleşmesi.pdf](file:///Users/MelekAsli/Downloads/Viyana%20Antlaşmalar%20Hukuku%20Sözleşmesi.pdf) 11.12.2024

Yayla, M.(2013) Hukuki Bir Terim Olarak Siber Savaş . TBB Dergisi s.104 ss.177-202

Yayla, M.(2013) Uluslararası Hukukta Siber Saldırlara Karşı Kuvvet Kullanma. TBB Dergisi 2013/107 ss.199-220

Yazıcı, B. ve İnaç, H. (2018) Uluslararası Hukuk Açısından Korfu Boğazı Davası ve Sonuçları. Akademik Bakış Dergisi. Uluslararası Hakemli Sosyal Bilimler E-Dergisi Sayı: 70 ss. 148-165

Yenal, S. ve Akdemir, N. (2020) Uluslararası İlişkilerde Yeni Bir Kuvvet Çarpanı : Siber Savaşlar Üzerine Bir Vaka Analizi. Journal of Institue of Social Sciences, Cilt:11 Sayı: 1, ss.414-450 <https://dergipark.org.tr/en/pub/jiss/issue/54441> 30.08.2024

Yılmaz, B.A.(2020) Siber Terörizm ve Değişen İstihbarat Anlayışı. Anadolu Strateji Dergisi cilt: 1 sayı:1 ss.65-81

Yılmaz, D.H(2019) Birleşmiş Milletler Antlaşması, Kuzey Atlantik Antlaşması ve Uluslararası Hukuk Açısından Siber Saldırıların Tanımlanması Sorunu. Journal of Social and Humanities Sciences Research, 6(38), ss.1641-1655

Yılmaz, F.(2018) Robotlar Hayatımızda. FSM İlmî Araştırmalar İnsan ve Toplum Bilimleri Dergisi Sayı :12, ss. 109-120

Yılmaz, E.A. ve Irk, O. (2015) Nikaragua Divan Kararları Işığında Kuvvet Kullanma ve Meşru Müdafaa Sorunu. CBÜ Sosyal Bilimler Dergisi, Cilt:13, Sayı:2, Haziran 2015 ss. 151-166

Yiğit, T ve Akyıldız, M.(2014) Sızma Testleri için Bir Model Ağ Üzerinde Siber Saldırı Senaryolarının Değerlendirilmesi. Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi 4(1) ss. 14- 21

Zifcak, S.(2012) The Emergence of Wikileaks : Openness, Secrecy and Democracy. More or Less, Democracy and New Media ss.123-143

Welukar, J.N. ve Bajoria, G.P. (2021) Artificial Intelligence in Cyber Security- A Review. International Journal Of Scientific Resourch İn Science And Technology. cilt:8 sayı:6 ss.488-491

WU.J.X. Vd.(2018) Security for cyberspace: challenges and opportunities. Front Inform Technol Electron Eng 2018 19(12): ss.1459-1461

<https://smallseotools.com/tr/plagiarism-checker/> 25.07.2024

<https://www.state.gov/the-organization-for-economic-co-operation-and-development-oecd/> 14.12.2024

https://www.mfa.gov.tr/iktisadi-isbirligi_ve-gelisme-teskilati-oecd.tr.mfa 14.12.2024

<https://dnsmadeeasy.com/post/global-dns-network-benefits> 15.12.2024

[https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/dns-\(domain-name-system---etki-alani-ad-sunucusu\)](https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/dns-(domain-name-system---etki-alani-ad-sunucusu)) 15.12.2024

<https://uluslararasıhukukcalismalari.wordpress.com/2017/04/07/korfu-bogazi-davasi-corfu-channel-case-united-kingdom-of-great-britain-and-northern-ireland-v-albania-judgment-of-4-april-1949/> 18.09.2024

<https://www.icty.org/en/press/tadic-case-update-0> 22.02.2025

ÖZGEÇMİŞ

Adı: Huri
Soyadı: Uysal
Uyruğu: Türkiye Cumhuriyeti
Doğum Yeri ve Tarihi:
Tel:
E-posta:
Yazışma adresi:

Derece	Kurum	Alan	Mezuniyet Durumu
Lisans	Anadolu Üniversitesi	Uluslararası İlişkiler	2012-2016
Yüksek Lisans	İstanbul Medeniyet Üniversitesi	SBKY/ Yerel Yönetimler ve Şehircilik	2017-2018
Yüksek Lisans	İstanbul Medeniyet Üniversitesi	İktisat	2019- Ayrıldı
Yüksek Lisans	İstanbul Medeniyet Üniversitesi	Uluslararası İlişkiler	2022- Devam ediyor

Yıl	Kurum	Görev
2008-2010	TTNET	Üst Düzey Yönetici Asistanı
2013 - 2014	PGM - Proje Gözetim Mühendislik	Yönetici Asistanı
2018-2020	İDO	Tercümanlık
2021-2023	Doç.Dr.Hasan Emre Koçak Kliniği	Yönetici Asistanlığı - Tercümanlık
2023	ABD 'de bir Üniversite /Online	Veri Analisti

Yabancı Dil:
İngilizce - İleri seviye
Almanca - Temel seviye