VEKÂLET SAVAŞLARI VE SİBER GÜVENLİK

2023
YÜKSEK LİSANS TEZİ
BÖLGE ÇALIŞMALARI

Mümin TEKİN

Tez Danışman
Prof. Dr. Ali ASKER

VEKÂLET SAVAŞLARI VE SİBER GÜVENLİK

Mümin TEKİN

Tez Danışmanı
Prof. Dr. Ali ASKER

T.C.
Karabük Üniversitesi
Lisansüstü Eğitim Enstitüsü
Bölge Çalışmaları Anabilim Dalı
Yüksek Lisans Tezi
Olarak Hazırlanmıştır

KARABÜK
Nisan 2023

İÇİNDEKİLER

TEZ ONAY SAYSASI

Mümin TEKİN tarafından hazırlanan "VEKÂLET SAVAŞLARI VE SİBER GÜVENLİK" başlıklı bu tezin Yüksek Lisans Tezi olarak uygun olduğunu onaylarım.

Prof. Dr. Ali ASKER .....

Tez Danışmanı: Karabük Üniversitesi, İktisadi ve İdari Bilimler Fakültesi

Bu çalışma, jürimiz tarafından Oy Birliği ile Bölge Çalışmaları Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir. 26/04/2023

Ünvanı, Adı SOYADI (Kurumu) İmzası

Başkan : Prof. Dr. Ali ASKER (KBÜ) .....

Üye : Dr. Öğr. Üyesi Osman KURTER (KBÜ) .....

Üye : Dr. Öğr. Üyesi Ali Samir MERDAN (ÇKÜ) .....

KBÜ Lisansüstü Eğitim Enstitüsü Yönetim Kurulu, bu tez ile, Yüksek Lisans derecesini onamıştır.

Prof. Dr. Müslüm KUZU .....

Lisansüstü Eğitim Enstitüsü Müdürü

DOĞRULUK BEYANI

Yüksek lisans tezi olarak sunduğum, bu çalışmayı, bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu ve bu eserleri her kullanışımda alıntı yaparak yararlandığımı belirtir; bunu onurumla doğrularım.

Enstitü tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

Adı Soyadı : Mümin TEKİN

İmza :

ÖNSÖZ

Bu tez çalışmasının oluşumunda ve fikri gelişimimde bana ışık kaynağı olan değerli hocam Prof. Dr. Ali ASKER'e ve yönlendirmeleriyle destek olan değerli hocalarım Dr. Öğr. Üyesi Osman KURTER'e ve Dr. Öğr. Üyesi Ali Samir MERDAN'a sonsuz teşekkürlerimi sunarım.

Kişisel gelişimimi sağlama noktasında ve eğitim hayatımın iyi bir şekilde idame ettirilmesinde büyük payı olan aileme minnettarım.

ÖZ

Uluslararası ortamın anarşik yapısı tarafların birbirleri ile olan ilişkilerinde güç kullanımı veya güce sahip olmayı ya da sahip olunan gücü arttırmayı zorunluluk haline getirmiştir. Çünkü uluslararası ilişkilerde taraflar arasında, genel kabul görmüş kesin kararların alınması çıkar çatışmalarından dolayı imkânsız olarak karşımıza çıkmaktadır. Bu durum uluslararası ilişkilerde tarafların karşı taraf veya tarafları etkilemek ve çıkarları doğrultusunda hareket etmelerini sağlamak için bir baskı veya caydırıcılık aracı olarak kullanılması gerekliliğini ön plana çıkarmaktadır.

Vekâlet savaşları uluslararası alanda, çıkar çatışmalarında tarafların askeri güç kullanımının meydana getirebileceği sonuçlardan korunmak için uluslararası kuralların dışında kalan argümanları kendi çıkarları için kullanmaları neticesinde ortaya çıkmıştır.

Vekâlet savaşlarının; özel askeri birlikler, paralı askerler, terör grupları, sivil toplum kuruluşları, yerel güçler gibi argümanların varlığının yanında, günümüzde özellikle teknolojik gelişmeler neticesinde bilgiye ulaşım ve bilginin yayılım hızının artması sonucunda oluşturulabilen toplumsal baskı ortamı siber saldırıların kapsamının genişliği ve diğer argümanlara göre daha düşük maliyet ve yüksek etkisi kullanışlılığını tercih edilmesini arttırmaktadır.

Taraflar arasında siber saldırı, siber suç, siber uzay argümanlarının sıkça tercih edilmesi beraberinde, bilgi güvenliği ve doğruluğunun sağlanması ayrıca karşı harekât kabiliyetinin sağlanması için siber güvenlik kavramının ortaya çıkmasına ve gelişmesine neden olmuştur. Çalışma kapsamında vekâlet savaşlarının ortayı çıkışı ve kullanılışı, bununla birlikte siber saldırı, siber suç ve siber uzay kavramların ile birlikte gelişen siber güvenlik kavramının önemi üzerinde durularak kavramlarla ilgili genel bir bakış açısı oluşturulmaya çalışılmıştır.

Anahtar Kelimeler: Vekâlet Savaşları; Siber Saldırı; Siber Suç; Siber Uzay; Siber Güvenlik.

ABSTRACT

The anarchic structure of the international environment has made it a necessity to use force or to have poweror to increase the power in the in the relations of the parties with each other. Because in international relations, it is impossible to take generally accepted final decisions between the parties due to conflicts of interest. This situation highlights the necessity of using the parties as a pressure or deterrent tool in international relations to influence the other party or parties and to enable them to actin line with their interests.

In the histarical pracess; The armed force (army), which was accepted as the first means of pressure, was importand in the resolution of conflicts between countries. The hing population rate, the large number of the army and the superiority of the weapons used were used as a serious deterrent.

However, i recent history and today, convectional armies hav lost theirpriority in conflicts of interest between the parties due to technological developments, the excess of destructive power of convectional weapons, teh increase in social pressure, the establishmend of supranational organizations and institutions. Instead, less costly non-governmental organizations, private military companies, mercenaries, terrorist organizations, cyber attacks … etc. Methods have beea used. With the use of these arguments, a new concept called Proxy Wars has taken its place in the concept called Proxy Wars has taken its plac in the concept of power and theliteratüre on the use of power.

Proxy wars have emerged inthe international arena as a resultof the parties' use of arguments outside the international rules for their own interrests in order to protecet themselves foram the consequences of the use of militaray forc in conflicts f intererst.

Rroxy Wars; In additionto the existence of arguments such as Private Militaray Units, Mercenaries, Terrorit groups, Non-Güvernmental Organizations, Local Powers, the social pressure environment that can be created as a result of the increase in the speed of information Access and dissemination, especially as a result of technological

developments, the wide scope of cyber attacks and lower cost and cost compared to other argüments. Its high effect increases is usefulness.

The frequent preference of cyber attack, cyber crime and cyber space arguments among the parties has led to the emergence and development of the concept of Cyber Security in orderto ensure information security and accuracy, as well as to provide counter-action capability. Within the scope of the study, the emergence and use of Proxy Wars, as well as the importance of the concept of Cyber Security, which develops together with the concepts of cyber attack, cyber crime and cyber space, will be tried to create a general perspective on the concepts.

Keywords: Proxy Wars; Cyber Attacak; Cyber Crime; Cyber Spac; Cyber Security.

ARŞİV KAYIT BİLGİLERİ

Tezin Adı	Vekalet Savaşları ve Siber Güvenlik
Tezin Yazarı	Mümin TEKİN
Tezin Danışmanı	Prof. Dr. Ali ASKER
Tezin Derecesi	Yüksek Lisans Tezi
Tezin Tarihi	26/04/2023
Tezin Alanı	Bölge Çalışmaları Anabilim Dalı
Tezin Yeri	KBÜ/LEE
Tezin Sayfa Sayısı	114
Anahtar Kelimeler	Vekalet Savaşları; Siber Saldırı; Siber Suç; Siber Uzay; Siber Güvenlik

ARCHIVE RECORD INFORMATION

Name of the Thesis	Proxy Wars and Cyber Security
Author of the Thesis	Mümin TEKİN
Advisor of the Thesis	Prof. Dr. Ali ASKER
Status of the Thesis	Master Thesis
Date of the Thesis	26/04/2023
Field of the Thesis	Department of Regional Studies
Place of the Thesis	UNIKA/IGP
Total Page Number	114
Keywords	Proxy Wars; Cyber Attacak; Cyber Crime; Cyber Spac; Cyber Security

KISALTMALAR

AB : Avrupa Birliği

ABD : Amerika Birleşik Devletleri

APT : Gelişmiş Sürekli Tehdit (Devlet Destekli Özel Siber Saldırı Birimleri)

BGD : Bilgi Güvenliği Derneği

BIS : Departmentfor Business, Innovation and Skills (İş, Yenileşim ve Beceriler Bakanlığı

BM : Birleşmiş Milletler

BTK : Bilgi Teknolojileri Kurumu

CAATSA : Amerika'nın Hasımlarıyla Yaptırımlar Yoluyla Karşı Koyma Yasası

CCDCOE : NATO Kooperatif Siber Savunma Merkezi

CCS : Cyber Criminal Section (Siber Suç Bölümü)

CDMA : NATO Siber Savunma Yönetimi Otoritesi

CEO : Chief Executive Officer (En üst düzey yönetici)

CESG : Communications-Electronics Security Group(İletişim-Eletronik Güvenlik Grubu)

CNSS : Cyber National Security Section (Siber Ulusal Güvenlik Bölümü)

CPNI : Centre for the Protection of National Infrastructure (Ulusal Altyapıları Koruma Merkezi)

CSJ : Ashiyane Security Group, Cutting Sword of Justice

DDOS : Distributed Denial of Service (Dağıtık Hizmet Engelleme)

DEAŞ : Irak Şam İslam Devleti

DNS : Domain Name System (Alan İsimlendirme Sistemi)

EUROPOL: Avrupa Birliği Polis Teşkilatı

FATA : Siber Polis

FBI/CIA : Merkezi İstihbarat Teşkilatı (FBI İç Güvenlik / CIA Dış Güvenlik)

GCHQ : Government Communications-Electronics Security Group Savunma Bakanlığı İletişim Karargâhı)

GDPR : AB Genel Veri Koruma Regülasyonu (AB Vatandaşları Veri Gizliliği Kanunu)

ICS-CERT : Industrial Control System Computer Readiness Team (Sanayi Kontrol Sistemleri Bilgisayar Acil Müdahale Hazır Ekibi)

IDF : İsrail Savunma Kuvvetleri

IHS : Ira Hackers Sabotage

IP : İnternet Protocol Address (İnternet Site Adresleri)

İŞİD : Irak Şam İslam Devleti

JANGAL : DMO Elektronik Harp ve Siber Savunma Örgütü

JCC : Joint Cyber Center (Birleşik Siber Merkezi

KBÜ-LEE : Karabük Üniversitesi-Lisansüstü Eğitim Enstitüsü

MAHER : Siber Olaylara Müdahale Timi

MI6 : Gizli İstihbarat Servisi

MID : Rusya Federasyonu Dışişleri Bakanlığı

MOIS : Besic Siber Örgütü, İstihbarat ve Güvenlik Bakanlığı

NATO : Kuzey Atlantik Antlaşması Örgütü

NCF : Ulusal Siber Güç

NCIRC : NATO Bilgisayar Olaylarına Müdahale Birimi

NFC : Near Field Communication (Yakın Alan İletişim Teknolojisi)

NICIC : National Cybersecurity and Communications Integration Center (Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi)

NISA : Ulusal Bilgi Güvenliği Merci

NPV : Standing Committee of the National People's Congress (Cin Siber Güvenlik Grubu)

NSA : Ulusal Güvenlik Dairesi

OCS : Cyber Security Operations Centre (Siber Güvenlik Ofisi)

OCSIA : The Office of Cyber Security and Information Assurance (Siber Güvenlik ve Bilgi Güvencesi Ofisi)

PKK/PYD : Partiya Yekitiye Demokrat/Demokratik Birlik Partisi (PYD Suriye Yapılanması)

PTT : Posta Telefon Telgraf

QCF : Qassam Cyber Fighters

SDSR : Strategic Defence and Security Review (Stratejik Savunma ve Güvenlik Gözden Geçirmesi)

SILG : Devlet Bilişim Öncü Grubu

SNISCSG : Devlet Ağı ve bilgi Güvenliği Koordinasyon Küçük Grubu

SOME : Siber Olaylara Müdahale Ekipleri

SQL : Structured Query Language (Yapılandırılmış Sorgu Dili)

SSCB : Sovyet Sosyalist Cumhuriyet Birliği

SSTEK : Savunma Sanayi Teknolojileri AŞ

TCK : Türk Ceza Kanunu

TİB : Telekomünikasyon İletişim Başkanlığı

TSK : Türk Silahlı Kuvvetleri

TÜBİTAK : Türkiye Bilimsel ve Teknik Araştırma Kurulu

UEKAE : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

USCERT : Computer Emergency Readiness (Bilgisayar Acil Müdahale Hazır Ekibi)

USOM : Ulusal Siber Olaylara Müdahale Birimi

vb. : ve benzeri

WSIS : Dünya Bilgi Topluluğu Zirvesi

yy : Yüzyıl

s : Sayfa

ss : Sayfalar

ARAŞTIRMANIN KONUSU

Bilindiği üzere tarih boyunca ülkeler arasında çıkan anlaşmazlıkların çözümünde, ilk baskı aracı olarak kabul edilen silahlı güç (ordu) önem arz etmektedir. Nüfus oranının fazlalığı, ordunun kalabalık ve kullanılan silahların üstünlüğü ciddi bir caydırıcılık aracı olarak kullanılmıştır. Fakat yakın tarihte ve günümüzde, teknolojik gelişmeler, konvansiyonel silahların yıkım gücünün fazlalığı, toplumsal baskının artması, ulusüstü örgüt ve kuruluşların kurulması ile taraflar arasındaki çıkar çatışmalarında konvansiyonel ordular öncelik sıralaması yitirmiştir. Bunun yerine daha az maliyetli, sivil toplum örgütleri, özel askeri şirketler, paralı askerler, terör örgütleri, siber saldırılar vs. yöntemler almıştır. Bu argümanların kullanımı ile güç kavramında ve gücün kullanım literatürüne Vekâlet Savaşları olarak isimlendirilen yeni bir kavram yerini almıştır. Bunun yanı sıra Siber Güvenlik kavramı da bu bağlamda son derece önemlidir. Tez çalışmasının konusu Vekâlet Savaşları ve Siber Güvenlik kavramları üzerinedir.

ARAŞTIRMANIN AMACI VE ÖNEMİ

Uluslararası sistemde vekâlet savaşları kapsamında en önemli ve kullanışlı saldırılardan biri siber saldırılardır. Bu anlamda araştırmanın konusu ve amacı güncel olması bakımından büyük önem taşımaktadır. Tez çalışmasının bu önemine binaen Türkçe literatüre katkı yapacağı kanaatindeyiz.

ARAŞTIRMANIN YÖNTEMİ

Bu araştırmada Vekâlet Savaşları başlığı altında genel tanımlamalar ile yorumlara yer verilmiş olmakla birlikte, uluslararası literatürde yer alan bir takım çalışmalar (kitaplar, akademik makaleler, haber siteleri) araştırılarak tarama-inceleme yöntemiyle yapılmıştır. İkinci bölüm olan Siber Saldırı kısmında ise uluslararası ve bölgesel güç durumunda bulunan ülkeler ve toplulukların siber alanında yapmış oldukları düzenlemeler, uygulanan sistemler üzerinden değerlendirmeler yapılarak siber uzay, siber saldırı, siber suç, gibi kavramlar arasında bağ kurulmaya çalışılmıştır,

ARAŞTIRMA PROBLEMİ VE HİPOTEZLERİ

Bu çalışma uluslararası alanda eskiden beri kullanılmakta olan Vekâlet Savaşları kavramının, gelişen teknoloji ile birlikte küçülen dünyada ülkelerin kendi çıkarları doğrultusunda etki yapmak istedikleri topluluklar veya ülkelere karşı kullanımında uluslararası yaptırımlar ve toplum tepkisinden kaçınmak amacıyla tercih ettikleri en kullanışlı ve yaygın bir yöntemdir.

ARAŞTIRMANIN SINIRLILIKLARI/GÜÇLÜKLER

Çalışmada Vekâlet Savaşlarında kullanılan Siber Saldırılar üzerinde durulmuştur. Çalışma sırasında vekâlet savaşlarının karmaşıklığı ve Siber Saldırı gibi teknolojinin gelişmesi durumuna göre değişiklik gösterebilen, gerçekleştirilmiş olmasına rağmen taraf ve uygulayıcıların tespitinin zor olmasından dolayı yapılan eylemlerin sadece bir söylem olarak kaldığı, herhangi bir somut delil ile yapılan eylemlerin desteklenememesi gibi sorunsallarla karşılaşılmıştır.

1. VEKÂLET SAVAŞLARI

1.1. Vekâlet Savaşının Tarihsel Gelişimi

1.1.1. Genel Hatlarıyla Vekâlet Savaşları

Dünya üzerinde insanoğlu sürekli çıkar çatışmaları yaşamıştır. Her çatışmasından kendi istediği doğrultuda menfaat sağlamak insanoğlunun doğasının bir gereksinimidir. İnsan tek başına yaşamayı başaramayan, sosyal bir yapı arayışı içinde varlığını sürdürmeye çalıştığı için zaman içerisinde aileler, topluluklar, derebeylikler, devletler ve devlet üstü kuruluşlar olmak üzere pek çok sosyal yapı içerisinde bulunmuşlardır. İnsanların bireysel yapıdan ayrılarak, toplum olarak yaşamaya başlaması ve ihtiyaçlarını bu şekilde karşılama isteği, dünya üzerinde sınırların oluşmasına ortak tarih ve coğrafyaya sahip insanların bir araya gelerek kendi içlerinde bir düzen kurmaları, kendileri dışında kalan topluluklarla çıkarları doğrultusunda iletişim kurmaları uluslararası ilişkiler ortamını doğurmuştur. İnsanoğlu, bu ortamda çıkarlarını korumak için sahip olduğu gücü karşısındakiler üzerinde bir etki aracı olarak kullanmıştır. Ekonomik, nüfus, coğrafya, ordu vb. güçlerini her zaman karşı taraf için bir baskı aracı olarak görmüş ve her çıkar çatışmasında bunları kullanmaktan çekinmemiştir. Tarih boyunca uluslararası ilişkilerde sahip olunan nüfus, silah ve ordular önemli bir caydırıcılık olarak görülmüştür. Güçlü olanın zayıf olan üstünde istediği etkiyi bırakabildiği, çıkarlar söz konusu olduğunda ise savaşın hiç tereddütsüz tercih nedeni olarak kullanıldığı görülmektedir.[1] Yüz yüze yapılan cephe savaşlarının, zaman içerisinde teknolojik gelişmeler, toplum baskısı ve uluslararası alanlarda oluşturulan ulusüstü örgütlerin etkisi ile kısıtlamalar yaşaması, uluslararası alanda savaş tercihini ilk sıralarından almıştır. Fakat savaş tercihi her zaman uluslararası ilişkilerde güçlü bir tercih olarak kalmaktadır.

Birinci Dünya Savaş'ının yarattığı yıkımın tekrarlanmaması için oluşturulan Milletler Cemiyeti'nin çabaları İkinci Dünya Savaşı'nı engelleyememiştir. İkinci Dünya Savaşı teknoloji nedeniyle yıkım gücü artan silahların kullanılması daha büyük bir yıkama neden olmuştur. Yıkımın telafisi, ülkelerin bir birleri ile giriştikleri güç

[1] Haluk Özdemir, "Uluslar Arası İlişkilerde Güç: Çok Boyutlu Bir Değerlendirme," *Ankara Üniversitesi SBF Dergisi* 63/3, 2008, (ss. 113-144).

mücadelelerinde sahip olmak istedikleri silahların mali yükünün artması, karşılıklı iki ülkenin giriştiği bir savaştan bölge ülkeleri başta olmak üzere pek çok ülkenin etkilenmesi, ekonomik açıdan yaşanan çöküşler ülkeleri dış politikada yaşadıkları sıkıntıların çözümünde silahlı kuvvet çözümüne başvurmaları, kamuoyu desteğini kaybetmelerine neden olacağı için ülkeler çıkarları uğruna alternatif çözüm arayışlarına girmişlerdir.

Vekâlet savaşları, günümüzde Orta Doğu genelinde ve özellikle Suriye'de sıkça kullanılsa da kökleri çok eskilere dayanmaktadır. Ülkelerin birbirleri ile olan ilişkilerinde avantaj sağlamak için perde arkasında gerçekleştirdikleri eylemler tarih boyunca kendisini sürekli olarak göstermiştir. Örneğin; Osmanlı Devletinin 16. yüzyılda da Avrupa'da meydana gelen mezhep savaşlarında, kendisi için tehdit olarak görmüş olduğu Katolikliği yıpratmak için Protestan yapıları desteklemesi.[2] Çarlık Rusya'nın 19. yüzyılda da Osmanlı tebaasında bulunan kendisinin sıcak denizlere inme stratejisine uygun olduğunu düşündüğü Balkanlarda bulunan mezheplerin milliyetçilik yönünden desteklemesi[3] bunun yanında, İtilaf devletlerinin Osmanlı hükümeti içerisinde başlayan Kurtuluş Savaşı'na karşı doğrudan savaşa girmeyerek Yunanlıları ve zararlı cemiyetleri destekleyerek gerçekleştirdikleri[4] davranışlar vekâlet savaşları tarihine birer örnektir. Vekâlet savaşları, özellikle Soğuk Savaş dönemi olarak kabul edilen dönemde, ABD ile SSCB ülkelerinin doğrudan savaşa girmekten çekinmeleri neticesinde, taraf ülkeler tarafından farklı zamanlarda başvurulan bir yöntem olarak kendisini göstermektedir. Örneğin Süveyş Krizi, Küba Krizi, SSCB'nin Afganistan'ı işgali ve ABD'nin yerel güçlere yapmış olduğu destekler[5] Soğuk Savaş döneminde Vekâlet Savaşlarına örnek olarak gösterilebilmektedir. İki ülkenin doğrudan savaş tehdidinden çekinmelerindeki temel nedenleri, uluslararası sistemin etkisi, coğrafi mesafe ve nükleer

[2] Ömer Cona, "Suriye Krizinde Uluslararası Güç Mücadelesi: Vekalet Savaşları," (Ankara Hacı Bayram Veli Üniversitesi Türkiye ve Orta Doğu Amme İdaresi Enstitüsü, Yayınlanmış Yüksek Lisans Tezi), Ankara 2018, s.25.

.[3] Mithat Aydın, "19-20 Yüzyılda Osmanlı Balkanlarda Rusya'nın Casusluk Faaliyetleri," *Tarih Araştırmaları Dergisi*, 32/53, 2013, (ss. 17-54). s.37

[4] Mehmet Kayıran-M. Yahya METİNTAŞ, "Türk_Yunan İlişkileri (1878-1952," *Eskişehir Osmangazi Üniversitesi Türk Dünyası Uygulamaları ve Araştırma Merkezi Yakın Tarih Dergisi 2018,* (ss. 33-73). s.53

[5] Mustafa Aydın, "Vekalet Savaşları Nedir?- trguvenlikportali.com - e-güvenlik dersi-Modül 2-Güvenliğin Temel Kavramları," https://trguvenlikportali.com/ders-11-proxy-savaslar/, (Erişim tarihi: 01.01.2023).

silahlar olmuştur. Tüm bu etkileşimlere rağmen, ülkelerin birbirleri ile güç mücadelesini devam ettirmeye çalışmaları ve uluslararası arenada söz sahibi olma istekleri, onları, üçüncü bir ülke ve farklı coğrafyalarda farklı yöntemler ile güç mücadelesine girmeye itmiştir. Bu mücadele de günümüzdeki Vekâlet Savaşları kavramını veya her türlü imkânın kullanıldığı hibrit savaşları ortaya çıkarmıştır.[6] Oluşan yeni ortamda taraflar arasındaki kriz ve çatışmaların çözümünde, devletlere ait düzenli ordulara nazaran özel sektör tarafından yönlendirilen kuvvetler önem kazanmış ve çatışmalarda daha belirgin bir şekilde görülmüştür.

Vekâlet Savaşları; iki farklı gücün kendilerine vekil olarak seçmiş oldukları güçleri dışarıdan desteklemekte, doğrudan çatışmanın dışında kalmaya önem vermektedir. Bunun yanında vekillerin yetersiz olması veya zayıflaması gibi durumlarda ise dış aktör durumundaki ülke doğrudan savaşa müdahale edebilir. Bu gibi durumlar vekâlet savaşları kavramını değiştirmez ve konvansiyonel savaş kavramını ortaya çıkartmaz. Bu süreç anlık bir durum ve müdahaleden ibarettir. Bu duruma verilebilecek en iyi örnek, Yemen'de 26 Mart 2015 yılında ilerleyişini sürdüren Husi militanlarına karşı gerçekleştirilen, Suudi Arabistan'ın öncülüğünde yapılan, "Kararlılık Fırtınası" operasyonudur.[7]

Vekâlet Savaşlarındaki, artışın nedenleri arasında, terörizme karşı verilen mücadele, özel askeri birliklerin kullanılmasıyla çatışma maliyetini azaltması ve daha hızlı müdahale etme imkânı, teknolojik alandaki gelişmeler ve uluslararası arenada varlık göstermeye başlayan yeni güçlerin çatışması sıralanabilir.[8]

1.1.2. Terörizme Karşı Verilen Mücadele

Ülkelerin terörizme karşı vermiş oldukları mücadelede kendi sınırları dışında müdahale etmelerini gerekli görmeleri halinde, terörün merkezi olarak gördükleri yerlerde müttefikler edinerek sadece bu müttefikleri sıcak çatışmalara sokmaları, kendi askeri güçlerinin çatışma dışında tutmaları oluşabilecek kamuoyu tepkisini

[6] Ömer Cona, s.12.

[7] Yemen'de 'Kararlılık Fırtınası' Operasyonu, Anadolu Ajansı, https://www.aa.com.tr/tr/dunya/yemende-kararlilik-firtinasi-operasyonu/63227, (Erişim tarihi: 01.01.2023).

[8] Ömer Cona, s.55.

uzaklaştırmanın yanında, uluslararası arenadaki tepkilerden de kurtulmayı sağlamaktadır. Vekil devletin dışarıdan bu çatışmaya sadece müttefiklerine silah, mühimmat, istihbarat gibi yardımlarda bulunması olarak tanımlanabilir. El-Kaide'ye karşı ABD'nin Afganistan'da yerel güçleri kullanması[9]bu duruma en bariz örnek olarak gösterilebilmektedir.

1.1.3. Özel Askeri Birlikler

Özel askeri birlik; ülke dışında gerçekleştirilecek herhangi bir müdahalede maliyeti düşürmek ve müdahale hızını arttırmak için önem arz etmektedirler. Ülkeler kendilerine ait askeri birlikleri başka ülkelere göndererek çatışma ortamına girmeleri hem kamuoyu baskısı hem de mali yük oluşturmaktadır. Bunun için ülkeler asker gibi hareket edebilen, fakat ülkeler acısında girişilecek hareketleri konvansiyonel bir savaşın dışında tutabilecek güçlere yönelmişlerdir. Rusya'da Shchit, Wagner askerlikten ayrılmış fakat asker gibi hareket edebilen özel askeri yapılar bulunmaktadır.[10] ABD'nin de aynı şekilde kurulmuş en bilinen askeri yapısı Blackwater'dir.[11] Özel askeri birlikler, ülkelerin daha az maliyetle ve daha hızlı müdahil olmalarını sağlamıştır. Bu durum vekil devlet ve yerel güçler arasındaki ortaklık sayesinde her iki tarafın maliyetini düşürme çabası olarak gösterilmektedir. Maliyet odaklı olarak bakıldığında özel askeri birlikler, konvansiyonel bir savaşa kıyasla maliyeti düşük, hızlı bir müdahale yöntemidir. Fakat tarafların her ikisi de maliyet üzerinden değerlendirildiğinde, vekil devlet tek başına üstesinden gelemeyeceği işlemlerde, dış destek beklerken, dış destek sağlayan devletinde daha az maliyet olanaklarını göz önüne alacağı değerlendirildiğinde her iki tarafında beklediği etkiyi yaratıp yaratmayacağı muallaktır.[12]

---

[9] Giray Saynur Derman, Babur Haya, "11 Eylül Sonrası Afganistan'daki Güvenlik Sistemi," *Akademik Bakış Dergisi* 41, 2014, (ss.30-44) s.39

[10] Çağatay Cebe, *Rusya'nın Dış Politikadaki Gayrinizami Unsurları: Özel Askeri Şirketler*, Acta Fabula Çalışma Grubu, İstanbul 2020.

[11] Cebe, s.3.

[12] Deniz Alca, "Kim: Yeni Savaşlarda Asil Vekil Sorunu", *Savunma Bilimleri Dergisi*, Mayıs 2020, Sayı:37, (ss.25-48), s.37,38

1.1.4. Teknolojik Alanda Meydana Gelen Gelişmeler

Teknolojik alanda meydana gelen gelişmeler, insanlar tarafından teknolojinin daha etkin kullanımı sonucunda meydana gelen çatışma ortamını teknolojik ortama taşımıştır. Konvansiyonel savaşın maliyetli yapısı, askeri birliklerin savaş alanına sevki ve savaş sürecinde ihtiyaçlarının karşılanmasının sürekliliği, kullanılacak silahların maliyet yükü, bunların yanında devletlerin yapacakları eylemlerde uluslararası alanda karşılaşacakları yaptırımlardan kurtulmak için küçük donanımlı oluşturulmuş gruplar ile teknolojik imkânlar dâhilinde hedef alınan yapıların stratejik noktalarına gerçekleştirilecek anlık saldırıların maliyet, hız ve etki denkleminde siber saldırıların tercih nedeni olmasına zemin hatırlamıştır. Devletlerin temel yapılarını oluşturan kurum ve kuruluşlara yönelik gerçekleştirilen siber saldırılar ve bu saldırılar sonucunda meydana gelen kayıpları engellemek için ülkeler ve ulus üstü kuruluşlar bütçelerinden hatırı sayılır miktarlarda payları siber savunma ve siber saldırı birimlerinin kurulması ve bu birimlerin geliştirilmesine harcamaktadırlar. Özellikle NATO bünyesinde siber savunma ve siber saldırı birimleri oluşturulması için ayrıca bütçeler oluşturulmakta ve kararlar alınmaktadır.[13]

1.1.5. Uluslararası Arenada Varlık Göstermeye Başlayan Yeni Güçler

Uluslararası arenada güç kazanan ülkeler mevcut güç dengesine sahip ülkeler tarafından daima bir tehdit olarak algılanmışlardır. Ülkeler, taraf oldukları uluslararası anlaşmalar ve kabul etmiş oldukları sözleşmeler nedeniyle, yeni güç kazanan ülkelere karşı askeri bir güç yapısı kullanamayacaklarından yeni güç kazanan ülkeleri etki altına almak veya kendi istekleri açısından yönlendirmek için farklı yöntemler kullanmış, bu da vekâlet savaşlarındaki artışın temel nedenini oluşturmuştur.

Yukarıda belirtilen özellikler dikkate alındığında, vekâlet savaşlarının tarihsel gelişimi üzerinde şu şekilde bir yorum yapmak uygun olacaktır: Vekâlet Savaşları, tarih boyunca kullanışlı bir argüman olmuştur. Soğuk Savaş döneminde ABD ve SSCB'nin doğrudan bir cephe savaşına girememesi, karşılıklı rakip güç olmaları ve rakibi güçsüzleştirme, kendi alanını genişletme ve üçüncü bir ülke üzerinde birbirlerine karşı

[13] Doğan Şafak Polat, "NATO'nun Yeni Operasyon Alanı: Siber Uzay," *Güvenlik Bilimleri Dergisi*, UGK Özel Sayısı, 2020, (ss. 135-158), s.145.

etkin olma çabası, Soğuk Savaş sonrası dönemde ise kendi çıkarları doğrultusunda üçüncü bir ülke üzerinde veya düşman/rakibe karşı etkin olmak için yerel güçlerle yapılan işbirliği olarak kabul edilebilir. Vekâlet savaşının var olabilmesi için bazı argümanların bir arada bulunmasının gerekli olduğunu görülmektedir. Bunlar; üçüncü bir ülke, dış aktör, yerel güç, yerel güç ile dış aktör arasında ortak bir çıkar için kurulmuş iş birliğidir.

1.2. Güç Kavramı

Güç; sosyal bilimler içerisinde pek çok konuda olduğu gibi üzerinde tam bir fikir birliğine varılamamış bir olgudur. Bazılarına göre etki, bazılarına göre kapasite, bazılarına göre dış politikanın amacı, bazılarına göre de politikalara ulaşmak için kullanılan bir araçtır. En genel tanım olarak güç kavramı Jeffrey Pfeffer tarafından, "*davranışları ve olayların akışını değiştirebilme, direnme, üstesinden gelebilme, insanları normalde yapmayacakları hareketleri yapmaya ikna etme yeteneği*"[14] olarak tanımlanmaktadır. Uluslararası ilişkilerde ise A devletin B devletine karşı uyguladığı politikalar ile normal şartlarda hiçbir şekilde yapmayacağı bir şeyi yaptırması olarak bahsedilebilir. Güç, insanlar arasında olduğu gibi kurum ve devletler için de farklı yöntemlerle ifade edilmektedir. Devletler sahip oldukları güçle kendi istek ve çıkarları doğrultusunda diğer devletlerin veya grupların hareketlerini yönlendirmeye çalışmaktadır. Bazen de aslında o kadar güçlü olmamakla birlikte az güçlü devletler veya insanlar bir araya gelerek kendilerinden daha güçlü insanları veya devletleri etkilemeye çalışmaktadırlar.[15] Bu etkilemeye çalışmanın temelinde, güçlü devlete veya kişilere karşı kendilerini koruma güdüsü ile daha güçlü olanları etkileyerek kendi çıkarları doğrultusunda hareket etmelerini sağlamak yatmaktadır.

İnsanlar bu güç olgusuna karşı kendilerini korumak için kolektif bir yapı içerisinde hayatlarını idame etmeye başlamışlardır. Özellikle Vestfalya Barış Antlaşması ile insanlar arasında yaşanan dinsel çatışmalara son verilmiş, insanların

[14] Yönetim ve Organizasyon, 2 Ocak 2018 Blog Sayfası, "Örgüt İçi Güç Mücadeleleri, Politika" yazısı, Yönetim ve Organizasyon: Örgüt İçi Güç Mücadeleleri, Politika (canergenel.blogspot.com) URL uzantılı internet sayfası, (Erişim Tarihi:27.07.2023).

[15] Serhat Düvenci, "Devletin Köken Teorileri Açısından Devleti Doğuran Etmenler: Çeşitli Uygarlıklar ve Topluluklar Üzerinden Bir Değerlendirme," *Uluslararası Yönetim Akademisi Dergisi* 2, 2018, (ss. 66-93), s.84.

topraksal ve laik bir şekilde yaşamaya başlamalarının ilk adımı olarak görülmüştür.[16] Bu sayede insanların bulundukları toprağı bir vatan olarak kabullenmeleri ve bu vatanın güvenliğinin sağlanmasıyla da kendi güvenliklerinin sağlanacağı düşüncesi yerleşmiştir. Sömürgeciliğin artması, merkez devlet olarak anılan devletlerin çevre devletlerin imkânlarını kendi çıkarları ve menfaatleri için kullanmak istemesi, ulus-devlet anlayışının güçlenmesine yol açmıştır. Bu durum sınırsız özgürlüğün mutlak bir güvenlik sağlayamadığı düşüncesine neden olmuştur. Ulus güvenliğinin sağlanması için gerektiğinde bazı özgürlüklerden vazgeçilmesi düşüncesi ortaya çıkmıştır.[17] Bu düşünce zaman içerisinde gelişmiştir.

İlk başlarda gücün kaynağı hanedan ve onun ailesinin olması düşüncesi zaman içinde değişmiş ve gücün kaynağı olarak halk iradesi ön plana çıkmaya başlamıştır. Güvenlik ise devletin karasal sınırları dışından kaynaklı, varoluşlarına karşı tehlike arz eden durumlara karşı muafiyet sağlanması ile diğer devletler tarafından egemenliğinin tanınmasıdır. Geçmişte, devletin egemenliğine karşı oluşabilecek tehlikeler karşısında en yaygın kullanılan yöntemler askeri kabiliyetini arttırmak ve kullanışlı hale getirmektir. Bu durum gerçekleştirilemiyor ise müttefiklik ilişkileri kapsamında birleşmeler yaparak tehditler karşısında müttefiklikler kurarak güvenliği sağlamak yer almaktaydı. İkinci Dünya Savaşı sonrası Soğuk Savaş olarak isimlendirilen dönemde devletlerin güvenlik anlayışları caydırıcılık üzerine kurulmuştur. Gücünü arttıran bir devlet tehdit olarak algılanmış ve bu tehdide karşı önlem alınmıştır. Alınan önlemlerin başında da oluşan güç dengesizliğini dengelemek için güç birlikleri oluşturulması düşüncesi yaygınlaşmıştır. Bu düşünce zamanında güvenliğin sıfır toplamlı bir oyun olduğu düşüncesi ile bakılmış ve güvenliğin bölünebilirliğine inanılmıştır.[18]

---

[16] Merve Suna Özel Özcan, "Westphalian Devletler Sistemi ve Modernleşmenin Geleneksel Dünyanın Büyük Güçleri Olan İmparatorluklara Etkisi", *dergipark.org.tr sitesi,* https://dergipark.org.tr/tr/download/article-file/843945 URL uzantılı internet sitesi (Erişim tarihi 17.08.2023) (ss 49-62), s54.

[17] Salim Işık, "J. J. Rousseau ve Egemenlik Anlayışı Üzerine," *İnönü Üniversitesi Hukuk Fakültesi Dergisi* 8/2, 2017, (ss. 79-98), s.87-88.

[18] H. Tarık Oğuzlu, "Dünya Düzenleri ve Güvenlik: Ulus-Devlet Güvenlik Anlayışı Aşılıyor mu?," *Güvenlik Stratejileri Dergisi* 3/6, 2007, (ss. 7-43), s.7.

Günümüzde bu yaklaşıma en uygun örnek olarak Birleşmiş Milletler Örgütü verilebilmektedir. Birleşmiş Milletler ulusal güvenlik ve barış ortamının sağlanması için kurulmuş bir örgüt olmak ile birlikte, devletlerin içişlerine karışılmasını yasaklamıştır.

1.3. Vekâlet Savaşları Tanımı ve Ortaya Çıkışı

Tarih boyunca ülkelerin uluslararası alanda karşılaştıkları sorunları çözmeye yönelik kullandıkları en etkili silah savaşlar olmuştur. Ancak günümüzde devletlerin birbirlerine karşı bağımlı hale gelmeleri, savaşın yarattığı yıkım, oluşturduğu ekonomik maliyetlerin fazlalığı ve Birleşmiş Milletler gibi uluslararası barışın sağlanması ve korunmasına hizmet etmek için kurulan uluslararası örgütleri kabul etme, sorunların barışçıl bir çatı altında çözüme kavuşturma düşüncesi savaşın uluslararası sorunların çözümünde ilk tercih olmaktan çıkarmıştır.

Ekonomik açıdan bakıldığında uluslararası bağımlığın artması ve ticaretin gelişmesi neticesinde iki ulus devletin savaşması halinde savaş ortamında tedarik imkânlarında meydana gelen aksamalar ve savaşta gelişen teknoloji nedeniyle tahrip gücü yüksek silahların kullanılması, sonucunda artan can kayıplarının açıklanması toplumun tepkisi nedeniyle savaşları uluslararası arenada ilk tercih olmaktan çıkarmıştır. Örneğin Ukrayna-Rusya Savaşı sebebiyle herkes tarafından dillendirilen şey, dünyada bir gıda krizinin yaşanacağı gerçeğidir. Bunun neticesinde devletler doğrudan bir savaşı göze almak yerine örtülü bir şekilde mücadele etmeyi tercih etmektedirler. Bu durum da karşımıza vekâlet savaşları kavramını çıkarmaktadır.

Vekâlet savaşları, devletlerin kendilerine doğrudan bağlı bir unsur olan orduları yerine, dışarıdan destekledikleri devlet dışı aktörler eliyle çıkarlarına ulaşmasına sağlayan, çok yönlü bir güç mücadelesini olarak tanımlanmıştır.[19]

Vekâlet savaşları savaşın simetrik boyutu yerine asimetrik boyutunun ön plana çıktığı devletler yerine uluslararası ortamda yeni katılmış olan, özel askeri şirketler, terör örgütleri, yabancı savaşçılar, sivil toplum kuruluşları ve siber korsanlar olarak karşımıza çıkmaktadır. Bu devlet dışı aktörler sayesinde, devletler uluslararası hukuktan kaynaklı durumlardan azledilmiş bir şekilde, hareket serbestisi bulunan aktörleri çıkarları

[19]Ömer Cona, s.2.

doğrultusunda kullanmaktadır. Bu sayede uluslararası alanda oluşabilecek bir yaptırıma maruz kalmamakla birlikte iç siyasette de oluşabilecek bir baskıdan kurtulmuş olmaktadırlar.

Vekâlet savaşlarının ortak bir tanımı bulunmamaktadır. Bununla birlikte farklı akademisyenler farklı tanımlamalarda bulunmuşlardır. Rusçuklu; güçlü bir ulusun, kendi çıkarları için üçüncü tarafı, paralı askerleri, terör gruplarını, başka bir ülkeyi kullanması olarak tanımlamıştır. Sandıklı'ya göre; özellikle bölgesel ve küresel güçlerin kendi çıkarlarını elde etmek ve nüfus alanlarını genişletmek maksadı ile kendi askeri unsurları yerine, müttefiklerini, edilgen ülkeleri, hedef ülkeleri parçalamış yapıları veya yandaşlarına cepheye sürerek kullanmaları durumu olarak tanımlamaktadır.[20] Bu tanımlamalardan özetle, taşeron örgütlerin güçlü devletler adına silahlı veya silahsız eylemler gerçekleştirmesi olarak tanımlanabilir.

Kavramsal olarak ise uluslararası veya bölgesel güç durumunda bulunan devletlerin, stratejik çıkarları ve teolojik hedefleri kapsamında, hedef ülkesinin psikolojik, sosyolojik, ekonomik, siyasi istikrarsızlık vb. enstrümanlar ile toplumu yaşanacak gelişmelere hazırlayarak daha sonraki süreç için kurgulanan, devletlerin fiilen karşılıklı olarak konvansiyonel ordularla çatışmadığı, Silahlı Çatışma Hukukuna tabi olmayan bir ortamda ilan edilmemiş ve fiili savaş halinin olmadığı, bununla birlikte etnik veya dini temelli muhalif grupların yabancı savaşçılarla destelenerek, dolaylı ve de örtülü olarak finanse edildiği, askeri, lojistik ve eğitim açısından desteklendiği örtük savaş hali olarak tanımlanmaktadır.[21]

Vekâlet savaşlarını tarih boyunca en etkin bir şekilde kullanan millet İngilizlerdir. Birleşik Krallık, bir bölgeyi veya devleti himaye altına almak veya işgal etmek istediği zaman sırası ile psikolog, sosyolog ve tarihçiler tarafından ülke üzerinde bölgesel araştırmalar yaptırır. Yapılan araştırmalar sonucunda hazırlanan raporlar İngiliz Devleti'ne sunulurdu. Rapordan sonra bölgeye haritacılar olarak tabir edilen kişileri gönderirler ve hazırlanan rapor doğrultusunda haritacılar tarafından ülkede bölücü haritalar hazırlanırdı. Hazırlanan haritalardan sonra ülkeye kışkırtıcı İngiliz ajanları

[20] Cemal Çoban, "Yeni Dünya Düzeni Bağlamında Terör, Vekalet Savaşları ve Türkiye," (Gaziantep Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi), Gaziantep 2018, s.122.

[21] Hasan Ateş, *Vekalet Savaşları Stratejik Eksende Gizli Kuvvet İstihbarat*, Detay Yayınları, Ankara 2017, s.7.

gönderilerek ülkede isyan ve kargaşa çıkartılarak güvensizlik ortamının oluşması sağlanırdı. Güvensizlik ortamlarında İngiliz ordusu devreye girer; ülke içerisinde çatışan gruplardan birini veya birkaçını destekleyerek, ülke üzerinde hâkimiyet kurması sağlanırdı. Desteklenen grupların ülke üzerinde hâkimiyet kurmasından sonra sıra ülkeyi kendi istekleri doğrultusunda yönlendirecek kişilerin eğitiminin gerçekleştirilmesi gerekirdi. Bu eğitim için İngiliz eğiticiler hâkimiyet kurulan ülkelere gönderilirdi. İngilizler tarafından seçilmiş hâkimiyet kurulan ülke yönetimine getirilecek kişilerin eğitimleri, İngilizlerin kurmuş olduğu eğitim kurumlarında eğiticiler tarafında gerçekleştirilirdi. İngilizler tarafından eğitilmiş olan ve onların her söylediğini yerine getirmeye hazır olan yerel unsurlar, İngilizler ülkeden çıktıktan sonra onların çıkarları doğrultusunda ülkeyi yönetirlerdi.[22]

Vekâlet savaşları için farklı isimlendirmeler de mevcuttur. Bu isimlendirmelerden biri beşinci kol faaliyetleridir. Beşinci kol; her muhite giren, her şeyi duyan ve gören, bir memleketi örümcek ağı gibi ören ve elinde her türlü vasıtası bulunan gizli bir ordudur. Bu ordu, her türlü meslek ve ihtisas erbabından kurulmuştur. Yani şimdiye kadar bilinen gizli teşkilatın çok büyütülmüş ve geliştirilmiş bir şeklidir.[23] Beşinci kol faaliyetleri savaş esnasında kullanılabildiği gibi savaştan öncede kullanılabilmektedir. Bir bölgeye müdahale edilecek veya orada bir grup veya topluluk desteklenecek ise öncelikle orada sorun algısı oluşturulmalı mevcut idare zayıflatılmalı veya etkisiz hale getirilmelidir.

Beşinci kolun barış ortamındaki faaliyetleri Sebahattin Ertürk tarafından şu şekilde sıralanmıştır.[24]

1- Gençliğin mefkûresini, karakterini ve ahlakını bozmak
2- Yabancı fikirlerin inkişafına yardım etmek ve milli mefkûreyi çürütmek,

[22] Mustafa Güldağı, *Coğrafi ve Zihinsel İşgalin Arka Planı Kuşatma*, Lopus Yayınları, Ankara 2019, s.63-64.

[23] TDK sözlüğüne göre "bir ülkede düşman için çalışan örgüt" anlamı taşır. Beşinci kol olarak adlandırma ilk kez 1936-1939 yıllarında İspanya iç savaşında kullanılmıştır. General Franco birlikleriyle dört koldan Madrid'e saldırırken, Madrid içinde Franco'ya çalışan istihbaratçılar, beşinci kol faaliyeti ile casusluk ve sabotaj yoluyla şehirde bir ayaklanma çıkartarak şehrin düşmesine yardımcı olmuşlardır.

[24] Sebahattin Ertürk, *Propaganda ve Beşinci Kolun İkinci Dünya Harbinde Oynadığı Roller*, Genelkurmay Başkanlığı Yayınları, Ankara 1951, s.84-85.

3- Bir kısım muharrirleri ve matbuattan birkaç paçavrayı satın alarak bazı cereyanları, belli etmeden, alevlendirmek,
4- Paranın ehemmiyetini belirtmek, muhitte kolayca para kazanmak ve zengin olmak hırsını yaratmak,
5- Gayrimemnunları, bilhassa başka ırktan olanları aramak, bulmak ve onları ajan olarak kullanmak,
6- Devlete ve hükümete küskün insanlar marifetiyle enerjik ve muktedir adamların aleyhine matbuatta yazılar yazdırmak,
7- İç emniyet ve düzenin manen ve maddeten bozmak,
8- İktisadi bakımdan alınan tedbirlerden faydalanılarak halkın maneviyatını bozucu ve hükümetin otoritesini sarsıcı yalan haberler yaymak,
9- Kadınları aile hayatından soğutarak lüks ve havailiğe teşvik etmek iyi anne ve zevce olmaktan uzaklaştırmak,
10- Fuhşu, kumarı ve içki taşkınlığını arttırmak,
11- Zührevi ve ırk sündürücü hastalıkları hususi teşkilat vasıtasıyla yaymak,
12- Çocuk düşürme lehinde cereyan uyandırmak ve buna ait ilaçları dağıtmak,
13- Öğrenciler arasında ahlaksızlığın inkişafı için gizli kitaplar, müstehcen resimler ve mecmualar dolaştırmak,
14- Ordu arasına zararlı fikirlerin ve zayıflatıcı cereyanların girmesini ve inkişafını temin etmek,
15- Ordu arasında disiplini gevşetici mahiyette neşriyat yapmak,
16- Harekât bakımından önemli olan askeri tesislerin, yol ve köprülerin durumunu incelemek ve tespit etmek "sabotaj ve hava bombardımanlarına hedef için"
17- Rejimi yıkıcı başka ideolojiler için müsait muhit yaratmak ve gizli cemiyetler kurmak.

Vekâlet savaşlarının asıl aktörleri hiçbir zaman ön tarafta görünmemektedir. Arka tarafta durarak belirlenen strateji çerçevede hareket etmekte, olayların gidiş hattına göre kullanılan aktörü yönlendirmekte ve kullanmaktadır. Beşinci kol faaliyetlerine en iyi örnek olarak Almanların gizli örgütü Gestapo aracılığı ile gerçekleştirmiş oldukları eylemler gösterilebilir. Almanlar gerçekleştirmiş oldukları bu faaliyetler sayesinde İkinci Dünya Savaşı'nda özellikle sınırlarına yakın olan Polonya, Hollanda, Norveç Danimarka gibi yerlerin işgali esnasında zorlanmamışlardır. "Beşinci Kol Faaliyetleri" ismi ilk kez İspanyol iç savaşında General Franco tarafından Madrid kuşatmasında

kullanılmamıştır. Buna göre General Madrid'i dört taraftan kuşatmıştır. Bu esnada beşinci kol olarak tabir ettiği ve kuşatma öncesinde Madrid'e gönderilen ajanlar sayesinde Madrid içerisinde yönetime karşı ayaklanmalar çıkartılarak iç karışıklık yaratılmıştır. Bu duruma beşinci kol faaliyeti, Truva atı, kaleyi içten fethetme gibi tabirlerde kullanılmıştır. Günümüzde ise bu duruma; Asimetrik Savaş, Hibrit Savaş Dördüncü Nesil Savaşlar gibi isimler verilmektedir.[25]

Vekâlet savaşları açısından bakıldığında beşinci kol harekâtları; hasım olunan gücün var olan güçlerini zayıflatma, zedeleme aktif hareket edememe veya ortadan kaldırma, savaşma ve direnç kabiliyetlerini zayıflatma veya ortadan kaldırma, silahlı güçlerini zayıflatma veya savaşma yetenek ve isteklerini ellerinden almak için girişilen faaliyetlerin bütünü olarak anlamlandırılabilir. Bu işlemlerin gerçekleştirilmesinde ise başat silah olarak basın olarak görülmektedir. Bunun yanında gelişen teknoloji ile birlikte yeni nesil özellikle sosyal medya ve dijital ortamda kendilerine sunulan şiddet içerikli ve asimile edici oyunlarla etki altına alınmaya çalışılmakta ve istenen şekilde yönlendirilmeye açık hale getirilmektedir.

Gelişen teknoloji ve haberleşme ağındaki gelişmelerden dolayı uluslararası literatürde; sorunların çözümü aşamasında ilk olarak tercih edilen güç kavramları da değişime uğramıştır. Küreselleşme ve teknolojik gelişmeler sayesinde bilgiye erişim kolaylaşmıştır. Haberler ve olaylar teknolojik imkânlar ile daha fazla kitlelere ulaşmayı sağlamış ve bunun neticesinde de toplumsal tepkilerin oluşması kolaylaşmıştır. Bu nedenle güç kelimesi klasik tanımının dışına çıkarak, yumuşak, akıllı güç olarak literatüre girmiştir. Günümüzde uluslararası kuruluşların artması, sivil toplum kuruluşlarının etkinliğinin artması, devlet dışı aktörlerin ortaya çıkması ve gelişen uluslararası medya yumuşak güç kavramını ortaya çıkarmıştır. Ülkelerin sadece ekonomik ve askeri güçleri ile diğerlerini etkileme çabalarının yanı sıra oluşturulacak uluslararası kamuoyu ile de diğer devletleri baskı altına alabilmesi durumu ortaya çıkmıştır. Sovyet lider İosif Stalin'in *"Eğer Amerikan sinema dünyasını kontrol edebilseydim, bütün dünyaya komünizmi yaymak için başka bir silaha ihtiyacım olmazdı"*[26] şeklindeki söylemi toplum üzerinde görsel ve işitsel etkisi bulunan

[25] Sebahattin Ertürk, s.10

[26] Mustafa Güldağı, s.246.

teknolojilerin uluslararası ilişkilerde ne kadar önem arz ettiğini göstermektedir. Sonuç olarak gelişen ve değişen teknoloji sayesinde klasik savaş taktik ve yöntemlerinde değişmeler meydana gelmiştir. Ülkeler arasında gerçekleşen savaşlarda tercih edilen sert güç kavramlarında da değişmeler olmuştur. Burada özellikle yumuşak güç kavramı karşımıza çıkmaktadır. Bu kavram *"Bir ülkenin çıkarları doğrultusunda çevresine, yeni süreçler yaratarak şekil verebilmesi"* olarak ifade edilmektedir.[27] "*Eğer benim istediğimi istemesini sağlayabilirsem, o zaman yapmak istediğim şeyi yapması için onu zorlamama gerek kalmaz*"[28] felsefesinin bir sonucudur. Etki etmek istediğiniz ülke üzerinde askeri ve ekonomik güçler ile baskı kurmak yerine kendisinin örnek alınması gereken bir yapısının olduğu bilincinin oluşturulması yeterli olacağı değerlendirme üzerine kurulmuştur. Ülke kendisinin diğer devletler tarafından etkileyici bir yapıya sahip olduğu hissini uyandırır ve kendisinde bir hayranlık oluşturursa, uluslararası alanda kendisinin takip edilmesini sağlar. İsteklerinin doğru olduğu kanaati ile takip edilmesi desteklenmesi duygusunu oluşmasına sağlamaktadır. Özellikle Amerika Birleşik Devletleri (ABD) yumuşak gücü dünya üzerinde Hollywood sayesinde etkin bir şekilde kullanmıştır.[29] ABD demokratik siyasi sistemi, özgür yaşam tarzı, serbest ticaret imkânları, insan hakları konusundaki ilerici düşünceleri, teknoloji ve iletişim alanındaki yenilikçi yapısı, sinema sektörü, popüler müzik, yeme içme imkânları ve moda sektöründeki etkinliği sayesinde hayranlık uyandıran ikna edici bir yapıya sahiptir.[30] Günümüzdeki teknolojik gelişmeler sayesinde özellikle sosyal medya alanındaki imkânları etkin kullanması sayesinde ABD yumuşak güç imkânlarından sonuna kadar faydalanmaktadır. Propaganda alanında Rusya Federasyonu da teknolojik imkânların sağladığı avantajlardan yararlanmaktadır. Özellikle ABD dünya üzerinde kullanılan bütün sosyal medya ağlarını yönetebilecek şekilde bir teknolojik yapı oluşturmuştur.

20. yüzyılda meydana gelen savaşların yarattığı yıkımlar, ayrıca savaşa katılan ülkelerde meydana gelen ekonomik durumlardan dolayı ülkeler konvansiyonel savaşlardan kaçınmak istemektedir. Bu durum bölgesel iş birliği teşkilatlarını, birleşen

[27] Latif Pınar, "Amerika Birleşik Devletleri'nin Yumuşak Gücü ve Hollywood," *İnsan ve Toplum Bilimleri Araştırmaları Dergisi* 6/1, 2017, (ss. 253-274), s.257.

[28] Mustafa Güldağı, s.246.

[29] Latif Pınar, s. 262.

[30] Latif Pınar, s.263.

ulusüstü yapılar ile silahsızlanmayı, güç kullanımı kısıtlamalarına taraf olmayı ve uluslararası alanda hukukun bağlayıcılığı gibi nedenler devletleri güç kullanmadan kaçınmaya itmiştir. Günümüz dünyasında savaş hukuku kurallarına bağlı kalarak uluslararası ortamda sonuç almak için mücadele etmek etkili bir yöntem olmaktan çıkmıştır.

Vekâlet savaşların en fazla görüldüğü dönemin Soğuk Savaş olarak anılan iki kutuplu dünya düzeninin olduğu dönem olduğu söylenebilir. ABD ile Rusya'nın kendi çıkarları için müttefik veya uydu devlet olarak kullandığı ülkeler bulunmaktadır. Kore Savaşı, Küba Krizi, Vietnam Savaşı, Angola Bağımsızlık Savaşı, Nikaragua Devrimi, Granada İşgali, Şili Darbesi ve Afganistan İşgali vekâlet savaşları için iyi birer örnektir. 2000 yıllara gelindiğinde görülmeye başlayan Orta Doğu'daki "Renkli Devrimlerin" vekâlet savaşları sonucunda ortaya çıktığı bir gerçektir.

1.4. Vekâlet Savaşlarının Nedenleri

Günümüzde devletler amaçlarına ulaşmak için maliyeti yüksek, sonuçları öngörülemez konvansiyonel savaşlar yerine alternatif yöntemler denemektedirler. Bu yöntem doğrudan birçok gücün (ekonomik, toplumsal baskı, sosyal medya, siber saldırılar) bir arada kullanıldığı hibrit bir savaş ortamı durumundadır. Konvansiyonel savaşın maliyetini bilen ve bu maliyete katlanmak istemeyen büyük güçler, rakiplerini zayıflatmak için alternatif yolara başvurmaktadırlar.

Günümüzde vekâlet savaşları, kirli, öngörülemez, karanlık savaş olarak anılmaktadır. Öngörülemeyen, karanlık ve belirsizliklerin olduğu ortamlar vekâlet savaşları için vazgeçilmeyen bir ortamdır. Vekâlet savaşlarının nedenlerini yedi başlık altında toplanabilmektedir. Ekonomik nedenler, savaşta kaybedilen asker sayısının etkisi, ülkelerdeki muhalif yapılar, özel askeri şirketler, terör örgütleri, siber teknolojiler, uluslararası yaptırım tehlikesidir.

1.4.1. Ekonomik Nedenler

Ülkelerin sonuçlarını kestiremedikleri konvansiyonel savaşların getirdiği ekonomik yükümlülükler, ayrıca konvansiyonel savaşta kullanılacak argümanların temini ve bunların kullanımı için sahip olunması gereken insan gücünün sürekli olarak

desteklenmesinin maliyetinin sürekliliği nedeniyle ülkeler etki etmek istedikleri ülkelere karşı vekâlet savaşı argümanlarını kullanmayı tercih etmektedirler. Savaşların ekonomik boyutların incelerken sadece kullanılan silahlara harcanan maddi değerler üzerinden gidilemez, savaşta yaralanan sakat kalan kişilerin bakımı, savaş sonrası oluşan toplumsal bozulmanın tekrar inşası da ekonomiyi olumsuz etkiler. Çünkü bunların ekonomik etkilerinin de ekonomiye maliyetinin hesaplanması gerekmektedir. Rakamsal olarak örneklendirmek gerekirse, Birinci Dünya Savaşı 500 Milyar dolar, İkinci Dünya Savaşı 1,5 trilyon dolar olarak hesaplanmıştır. Ülkeler bazında bakındığında ise bu maliyetin %21 ABD, %20 İngiltere, %18 Almanya ve %13 SSCB harcadığı[31] görülmektedir. Bu rakamlar ülkeler bazında değerlendirilmiş olsa da tüm dünya tarafından hissedilmiştir. Sonucu belirsiz olan bir savaş için katlanılacak maliyetin fazlalığı nedeniyle ülkeler açısından vekâlet savaşı tercihi öne çıkmaktadır.

1.4.2. Savaşta Kaybedilen Asker Sayısının Etkisi

Konvansiyonel savaşlarda teknolojik imkânlar ve kullanılan silahların önemi kadar asıl olan bir şey varsa insan gücü yani askerdir. Savaşta kaybedilen kişi sayısının yanında ülkelerin savaş öncesi yapılarına dönmeleri için gerekli iş gücünün de kaybı meydana gelmektedir. Bunun yanında yakınları yaralanan veya ölen insanların yaşadığı trajediler nedeniyle mutsuz bir toplum oluşur. Toplum yapısının değişmesi için uzun yıllar geçmesi gerekmektedir. Birinci Dünya Savaşı'nda 39 milyon, ikinci dünya savaşında ise 64-84 milyon insanın öldüğü[32] varsayıldığında ülkeler bazında kaybedilen asker sayıları, savaş sonrası tekrar üretim ve yeniden ayağa kalkma açısından ciddi bir sorun durumundadır.

Teknolojik imkânların artması; nükleer ve kimyasal silahların yaygınlaşması, neticesinde muhtemel bir konvansiyonel savaşta öngörülemeyen can kayıpları ve yıkımlar, ayrıca güç kullanımın sonucunda istenilen sonucun elde edilemeyecek olmasının getirdiği riskler bulunmaktadır. Bunlara karşılık vekâlet savaşlarında bayrak

[31] Mustafa Pamukoğlu, "Savaşların Maliyetleri," *Aydınlık Dijital Gazetesi*, Son Güncelleme; 06 Mart 2016, https://www.aydinlik.com.tr/koseyazisi/savaslarin-maliyeti-17640, (Erişim tarihi: 01.01.2023).

[32] Selçuk Bulut, "Tarihte En Çok İnsan Öldüğü 5 Savaş," *Milliyet Gazetesi*, https://www.milliyet.com.tr/molatik/tarih/tarihte-en-cok-insanin-oldugu-5-savas-90465, (Erişim tarihi: 01.01.2023).

göstermeme, düşük maliyet ve toplumsal bir baskının oluşmama durumu vekâlet savaşlarının tercih nedenleri arasındadır.

Diplomasinin taraflar arasında uzun soluklu ve yıpratıcı bir durum olması, sorunların çözümünde konvansiyonel savaş yöntemlerinin yukarıda sayılan nedenlerden dolayı tercih edilememesi nedeniyle devletlerin sorunların çözümlenmesinde alternatif çözümler aramaları, topyekûn savaşlarda araçların ve silahların kullanıldığı geniş çaplı ordular yerine küçük çaplı ama donanımlı grupların tercih edilmesi vekâlet savaşlarının nedenleri arasındadır.

1.4.3. Ülkelerdeki Muhalif Yapılar

Muhalefet; karşı gelmek, zıtlaşmak, kabul etmemek veya düşmanlık etmek kelimelerini içermektedir.[33] Zamanla bu kavram siyasi hayatta veya seçim yapılacak kuruluşlarda rakip olan tarafların birbirleri için yapmış oldukları söylemler olarak genişlemiştir.[34] Muhalefet kelimesinin birden çok kullanım alanı vardır. Vekâlet savaşlarındaki kullanım amacı ise, hedef alanın ülke içerisinde mevcut yönetimi istemeyen, mevcut yönetimin her yaptığına karşı çıkan veya mevcut yönetimi zayıflatmak için elindeki her türlü argümanı kullanmaya hazır gruplar olarak ifade edilebilir. Sivil toplum kuruluşları, muhalefet yapıları, milliyetçi yapılar bu tür gruplara örnek olarak verilebilmektedir. Bu yapıların yakın tarihte Arap Baharı olarak isimlendirilen isyan hareketleri çok güzel bir örnektir. İlk başlarda barışçı bir şekilde başlayan protestolar zaman içerisinde dış destekçilerin katkıları ve yardımları sayesinde bir halk ayaklanmasına dönüşmüş, daha sonra ise bu ayaklanmalar iç savaşları ve yönetimde değişmeler kadar gitmiştir. Bu uygulamalar özellikle soğuk savaş döneminde iki kutuplu dünya düzeni üzerinde sıkça kullanılmıştır. Örneğin: Sovyet-Afgan Savaşı'nda ABD Afganistan'daki yapılara destekleyerek Rusya'nın zafer kazanmasının önüne geçmiştir. Bunun yanında Rusya Federasyonu halen Yakın Çevre Doktrini

[33] Develioğlu, Ferit. *Lügat*, 1960, https://ia800603.us.archive.org/20/items/Osmanlca-TTrkreAnsiklopedikLkgat/0811-Osmanlica_Lughat-Eshanlam_Sozluk-Ferid_Develioghlu-Latin-Ebced-1960-1570s.pdf,(Erişim tarihi: 16.01.2023).

[34] A. Filiz Yavuz, "Muhalif olmak ve Muhalefet Yapmak," *Türk Yurdu Dergisi* 323, 2014. https://www.turkyurdu.com.tr/yazar-yazi.php?id=282, (Erişim tarihi: 16.01.2023).

kapsamında eski SSCB ülkelerindeki mevcut iktidarları muhalif kesimleri destekleyerek zayıflatmakta ve batı yanlısı hükümetlerin yıkılarak yerine kendisine yakın hükümetlerin kurulması için yoğun bir çaba zarf etmektedir.[35]

Genel bir tanımlama yapacak olursak, ülke içerisindeki yönetim sistemini beğenmeyen, yönetimi yıkmak, zayıflatmak ve yerine kendisinin yönetimini koymak isteyen grup veya kuruluşlara muhalif yapılar olarak belirtilebilmektedir. Vekâlet savaşlarında ise dış güçler muhalif yapıları uzun vadeye yayılan bir şekilde finansman, lojistik ve politik olarak desteklemektedirler.

1.4.4. Özel Askeri Şirketler

Özel Askeri Şirketler/Kontratçı Firmalar olarak ifade edilen kuruluşlar, askeri kuvvet için lojistik, insan gücü ve diğer hizmetleri sağlayan şirketler olarak ifade edilebilir.[36] Özel Askeri Şirketler ile paralı askerler birbirlerine karıştırılmaktadır. Fakat bu iki kavram birbirinden farklıdır. Paralı askerlerin herhangi bir resmi yapısı bulunmazken, özel askeri şirketlerin en azından kendi ülkelerinde kayıtlı bir şirketleri/resmi yapıları vardır. Müşterileri ile kontrat imzalayarak hizmet sunmaktadırlar. Dış ülkelerde gerçekleştirecekleri işlemlerde ise kanunlar kapsamında hareket etmektedirler.[37] Özel askeri şirketler kendilerine özel güvenlik şirketi de demektedir. Bu durumda özel askeri şirketleri yasal zemin üzerine oturtmakta yardımcı olmaktadır. Özel askeri şirketleri gruplandırmak mümkündür.

1- Savaşan veya operasyonel destek sağlayan şirketler
2- İstihbarat toplayan ve suç önleyen şirketler
3- Lojistik destek veren
4- Askeri eğitim ve malumat veren
5- Silah tedarik eden
6- Güvenlik sağlayan

[35] Süreyya Yiğit, Gökhan Gülbiten, "Rusya'nın Yakın Çevre Dış Politikası ve Azerbaycan," *Barış Araştırmaları ve Çatışma Çözümleri Dergisi* 5/1, 2017, (ss. 54-70), s.60-61.

[36] Sait Yılmaz, "21'inci Yüzyılda Güvenlik Alanının Yeni Sivil Aktörleri: Özel Askeri Şirketler ve Kontratçı Firmalar," *Güvenlik Stratejileri Dergisi* 3/6, 2007, (ss. 43-70). s.44.

[37] Sait Yılmaz, s.44.

7- Coğrafi saha ve risk analizi yapan şeklinde gruplandırabiliriz.[38]

Devletler çatışma ortamında, asker kayıplarının azaltmak, hızlı ve sonuç odaklı operasyonlar yürütmek ve konvansiyonel savaşın maddi yükünden sakınmak için özel askeri birlikleri tercih ederler. Özel askeri şirketler, çatışma alanında veya başka bir şekilde hayatına kaybetmesi durumunda, askerî açıdan bir can kaybı söz konusu değildir. Sadece şirket çalışanını kaybetmiştir. Ülke yönetimde olan iktidara karşı gerçekleşebilecek toplum baskısını ortadan kaldırmaktadır.[39] Aynı zamanda kamusal denetime ve uluslararası alanda gözleme kapalı olmaları da hareket kabiliyetlerini güçlendirmektedir. Devletlerin savaş alanında bile uyması gereken zorunluluklar mevcuttur fakat özel askeri şirketler devletin uyması gereken kurullardan muaftır. Bu da hareket serbestisi sağlamaktadır. Aynı zamanda gerçekleştirilecek eylemler üzerinde denetimi zorlaştırmaktadır.[40] Özel askeri şirketlere özel ordularda denilmektedir. ABD dünya üzerinde en çok özel askeri şirketi bünyesinde kullanan ülkedir. Kolombiya gibi ülkelerde özel askeri şirketler aracılığı ile operasyonlar yapmaktadır. Özel askeri şirketlere örnek verilecek olursa; ABD'nin Blackwater şirketi, Rusya'nın Wagner şirketi, Türkiye'de ise SADAT bulunmaktadır. Özel askeri şirketleri özellikle uluslararası alanda faaliyet gösteren şirketler tercih etmektedir. Özellikle enerji şirketleri askeri yapıda hareket edebilen gruplar ile güvenlik anlaşmaları yapmaktadırlar. [41]

1.4.5. Terör Örgütleri

Bu kısımda karşımıza iki kavram çıkmaktadır. Bunlar Terör ve Terörizmdir. Bu kavramlar aynı gibi görünseler de aslında birbirlerinden farklı kavramlardır. Kontrolsüz kitlelerin gerçekleştirdikleri aşırı şiddet ve katliamlara terör, terörün iradi bir yapı altında

[38] Duhan Kalkan, "Devletin Güç Kullanması Tekeli ve Özel Askeri Şirketler," *Bölgesel Araştırmalar Dergisi* 6/1, 2022, (ss. 148-173), s.158.

[39] Nurullah Çatal, "Vekâlet Savaşlarının Bir Aracı Olarak Özel Askeri Şirketler", *Assam Uluslararası Hakemli Dergisi*,2021, (ss.1-8), s.2.

[40] Duhan Kalkan, s.159-160.

[41] Filiz Çulha-Zabcı, "Yeni Savaşların Gizli Yüzü: Özel Askeri Şirketler," *Mülkiye Dergisi* 28/243, 2004, (ss.21-49), s.24.

kullanılmasına da terörizm denebilmektedir.[42] Terör üzerine yapılmış birçok tanım olsa da genel kabul gören bir tanımı yoktur. Siyasal amaç ile bombalama, öldürme ve adam kaçırma gibi güç kullanılma. Önceden belirlenen hedeflere ulaşmak için şiddet kullanma, şiddete başvuran bir grubun veya partinin kullandığı metot gibi tanımları mevcuttur. Hukuki yönden; Alarm, koku, dehşet, düşman veya tehdit eden bir olay veya tezahürden ötürü zarar geleceği hususunda endişe olarak tanımlanmaktadır.[43]

Ansiklopedik Zabıta Sözlüğünde; "*Sürekli korku altında tutmak amacıyla şiddet hareketleri, kaçırmalar ve cinayetler işleme eylemleri, sistemli şiddet hareketleri ve cinayetlere başvurma eylemi olarak da tanımlanmıştır*."[44] Bu tanımlamaların ortak noktaları, korku - panik yaratmaları ve toplum üzerinde baskı oluşturacak şekilde şiddet eylemleri olarak görülmektedir.

Vekâlet savaşları bağlamında terör örgütlerine bakılacak olursa, hedef alınmış olan ülkede faaliyet gösteren veya bu ülke sınırları içerisinde eylem yapma yeterliğine sahip uluslararası terör gruplarının başat ülke tarafından çeşitli argümanlar altında desteklenmesi ile gerçekleşen eylemler bütünüdür. Burada amaç hedef alınan ülkenin mevcut yönetimini zayıflatmak, halkta korku ve panik yaratarak yönetime karşı olan güveni sarsmanın yanı sıra, olası bir konvansiyonel savaş anında gerçekleşebilecek kendi ülke vatandaşlarının kaybını engelleyerek kendisine karşı oluşabilecek tepkilerden kurtulmaktır. Bu duruma en iyi örnek, halen devam etmekte olan Suriye iç krizidir. ABD, Suriye topraklarında faaliyet gösteren PKK/PYD terör örgütünü lojistik ve askeri alanda desteklemekte ve buralarda DEAŞ terör örgütüne karşı bu terör grubunun savaştığını öne sürmektedir.[45]

---

[42] *Türkiye ve Terörizm*, Türkiye Barolar Birliği Yayınları, Ankara 2006, s.3.

[43] *Türkiye ve Terörizm*, s.5.

[44] Yılmaz Altuğ, "Terörizm Sorunu," *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası* 51/1-4, 1987, (ss. 47-99), s.54.

[45] İsmail Sevinç, Veysel Babahanoğlu, "Küresel Güvenliğin Değişken Yapısı ve Terör Örgütleri Üzerine Etkisi: DEAŞ Terör Örgütü Örneği," *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Dergisi* 24/4, 2019, (ss. 969-987), s.982.

1.4.6. Siber Teknolojiler

Siber kelimesi Cyber kelimesinden türemiştir. Siber teknolojide; Bilgisayar ağlarına ait olan, internete ait olan, sanan gerçeklik olarak ifade edilebilir. Siber teknoloji sadece bilgisayar, yazılım ve üretilen teknolojik diğer ürünler olarak değerlendirilmemelidir. Burada teknoloji ile birlikte gelişim gösteren ve vekâlet savaşlarında güçlü bir silah olan propaganda imkânı teknolojik gelişmeler ile değişen iletişim ve bilginin yönetilmesi de güçlü bir silah durumundadır. Bunun yanında teknoloji kullanıcılarının eğilim ve isteklerini bilmek de elde edilebilecek güçlü silahlardan biridir. "*Hiçbir şey bedava verilenden daha pahalı değildir*."[46]

Bu atasözü günümüz teknolojisini çok iyi ifade eden bir sistemdir. Sanal alemde kullanılan birçok hizmetin neden ücretsiz olduğu sorusunun cevabı karşımıza çıkmaktadır. İnternet ortamında kullanılan birçok uygulama ücretsiz olarak sunulmakla birlikte uygulama kullanımı açısından, istenen sadece size özgü bazı kişisel verilerinize ulaşmaktır. Konum, beğeniler, mesajlar vs. gibi size özel olan verilerinize erişim izni isteyecektir. Bu izinlerin verilmesi ile istenen uygulama kullanıma açılacaktır. İzinlerin verilmemesi halinde ise uygulama kullanılamayacaktır. Bu durumda kişisel verilerinizin bir yerlerde birileri veya bir şeyler tarafından toplandığı daha sonra analiz edilerek yararlı bilgilerin çıkartıldığı bir süzgeçten geçirilerek bu bilgilerin üçüncü kişi veya kuruluşları sunulduğudur.[47] Google, Facebook, Twitter gibi firmalar bu sistemi en iyi kullanan bilinen firmalardır. Bunlardan herhangi birini ben kullanmıyorum deseniz de yine bu uygulamaların sizleri takip etmesini engelleme şansınız yok denecek kadar azdır. Çünkü bu firmaların ortağı veya sahibi olduğu yan kuruluşlar ile irtibatınız mevcut ise bu kuruluşlar sizi yine de izleme altına alabilirler.[48]

Doğru bilginin her şey olduğu düşünülen günümüzde, yapılmak istenen bir propaganda ile ilgili olarak, yapılan veri toplama işlemleri ile kamu oyu araştırmaları, yüz yüze oy toplama teknikleri, kitle iletişim araçları, parti toplantıları, mitingler, broşürler ve pankartlar gibi uygulamalar toplanan veriler ile tespit edilen yerlere farklı

[46] İrfan Atasoy, Okan Ormanlı, "Teknoloji ve Siber Güvenlik: Dijital Toplumun Geleceği," *İstanbul Aydın Üniversitesi Dergisi* 11/4, 2019, (ss. 399-409), s.403.

[47] İrfan Atasoy, Okan Ormanlı, s.403.

[48] İrfan Atasoy, Okan Ormanlı, s.404.

metotlar ile uygulanarak hedef alınmış olan toplumun veya grubun yönü, amacı veya tutumunda değişiklikler sağlanabilmektedir.[49] İletişim veya etkileşim kişilerin kanaatleri üzerinde değişiklik yapmalarını sağlamaktadır. İnsan gördükleri, işittikleri veya okudukları şeyler üzerine fikirlerinde değişmeler yaşanmaktadır. Bu da yapılan konuşma ve izlenen gösterinin en fazla kişiye ulaşmasının sağlanması ile mümkün olmaktadır. Burada devreye teknoloji girmektedir. İnternet ortamında sosyal medya ağları üzerinden yapılan yayınlar sayesinde bireysel olarak ulaşılması mümkün olmayacak kadar fazla kişiye ulaşılmakta ve kişiler üzerinde etkiler oluşturulmaktadır.[50] We Are Social Digital'in 2022 yılında açıkladığı istatistikte internet kullanımının %59,72 mobil telefonlardan, %37,98 bilgisayarlardan, %2,27 laptoplardan, %0,03 de oyun konsollarından bağlanarak kullanılmıştır. Haber almak için kullanılan ortamlar rakamlarında ise %82 internetten, %61 televizyondan, %57 sosyal medyadan, %23 yazılı basından araştırılmaktadır.[51] Burada gelişen teknoloji ve insanların haber almak ve etkileşin hızının ne kadar gelişim ve değişim gösterdiğinin bir kanıtı durumundadır.

Bunların yanında ülkeler ve insanlar için hayati öneme sahip olan; kritik alt yapılar olarak isimlendirilebilen, enerji sektörü, ulaşım sektörü, haberleşme sektörü, silah sektörü, finans sektörü gibi yerlerin gelişen teknoloji ile her an adresi ve kuvvesi belli olmayan saldırılara maruz kalması ve bu saldırılar sonucundan geri döndürülmesi mümkün olmayacak şekilde zararlara açık olması riski de her zaman mevcuttur.

1.4.7. Uluslararası Yaptırım Tehlikesi

Güçlü bir aktörün daha güçsüz bir aktöre karşı yapmakta olduğu bir eylemi durdurması ya da yaptığı bir yanlışı düzeltmesi amacıyla uygulamaya koyduğu eylemler bütünü yaptırım olarak tanımlanabilir. Bunun yanında yaptırım, hukuka uymama durumunda cezalandırılma tehdidi, gerekli olduğunda cezalandırılması ve davranış

[49] Haluk Ölçekçi, "Vekalet Savaşlarının Bir Aracı Olarak Medya ve 15 Temmuz Sürecinde FETÖ'nün Medya Faaliyetleri," *Uluslararası 15 Temmuz ve Darbeler Sempozyumu*, Kartepe Zirvesi, 2018, (ss. 225-247), s.236.

[50] İrfan Atasoy, Okan Ormanlı, s.406.

[51] Seda Başpınar, "We Are Social Temmuz 2022 Raporu: İnternetle Aramızda Güven Sorunu Var," *Marketing Türkiye Haber Sitesi*, Son Güncelleme Tarihi: 26 Temmuz 2022, https://www.marketingturkiye.com.tr/haberler/we-are-social-internet/ (Erişim tarihi: 01.03.2023).

değişikliği yaratan zorlayıcı tedbirlerdir.[52] Uluslararası yaptırımların uygulanmasında dikkat edilmesi gereken en temel özellik, yaptırım uygulanan ülke veya kuruluşun uluslararası haklarının ihlal edilmemesidir.[53] Uluslararası ilişkiler açısından bakıldığından iki farkı unsur karşımıza çıkmaktadır. Devletler ve Uluslararası kuruluşlardır. Devletler uluslararası ilişkilerin en önemli aktörüdür. Bunun yanında uluslararası kuruluşlarda vardır. Bunlar AB, NATO, İslam İş Birliği Örgütü, Şanghay İşbirliği Örgütü gibi yapılardır.

Yaptırımlar; kınama, tanımama gibi yöntemlerin yanında ekonomik şekillerde de olabilmektedir. Bunu uluslararası alanda en fazla kullanan ülke ABD'dir. 2017 yılında çıkartılan Amerika'nın Hasımlarıyla Yaptırımlar Yoluyla Karşı Koyma Yasası (CAATSA) ile ABD tarafından hasım olarak belirlenen bir ülke veya uluslararası kuruluşa, ABD başkanı tarafından 12 farklı yaptırım tercihlerinden beş tanesinin uygulanması öngörmektedir.[54]

Uluslararası kuruluşlar açısından bakılacak olursa örgüte üye ülkeler, her bir katılım esnasında örgütün kurallarına bağlı kalacağını beyan eder. Bu da üye ülkelerin yapmış oldukları veya yapmaları gerektiği halde yapmadıkları eylemler sonrasında bazı yaptırımlar ile karşı karşıya kalmalarına sebep olabilmektedir.

BM tarafından uygulanabilecek yaptırımlar; Diplomatik olarak o ülke ile bağların kaldırılması, ekonomik olarak; tarım, silah, tıp vb ekonomik sektörlerin ticaretinin yasaklanması, askeri müdahaleler, çevresel olarak çevrenin korunması ve doğal kaynakların korunması, spor; belirli bir ulusun uluslararası etkinliklerden menedilmesidir.[55]

Yaptırımlar ülkeler bazında uygulanırken ülke vatandaşları açısından da bazı yaptırımlar uygulanabilir. Yaptırım uygulanmakta olan ülkenin vatandaşlarının veya

---

[52] Behnam Alipourvaghaslou, "Uluslararası Hukukta Yaptırım Rejiminin Genel İlkeleri ve Özellikleri," *Van Yüzüncü Yıl Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* Van YYÜ 40. Yıl Özel Sayısı, 2022, (ss. 157-186), s.159.

[53]Bilal Karabulut, "Uluslararası Yaptırımların Hukuksal Bir Analizi", *Uluslararası Hukuk ve Politika,* No: 12, Yıl: 2007, (ss.15-40), s.27.

[54] Uluslararası Hukukta Yaptırımlar: ABD Örneği, *Hukukçular Derneği*, https://hukukcular.org.tr/uluslararasi-hukukta-yaptirimlar-abd-ornegi/ (Erişim tarihi: 20.01.2023).

[55] Birleşmiş Milletler Yaptırım Listesi, 2022, https://blog.codevist.com/birlesmis-milletler-yaptirim-listesi-be863d6c80be (Erişim tarihi: 20.01.2023).

kuruluşların belirli yerlerde veya sektörlerde yatırım veya ticaret yapmalarının yasaklanması, vatandaşlarının belli ülkeler veya yerlere gitmelerinin engellenmesi gibi yaptırımlarda söz konusu olabilir.[56]

BM tarafından yaptırım uygulananlar: Afganistan, Orta Afrika, Kongo Demokratik Cumhuriyeti, Kore Demokratik Halk Cumhuriyeti, İran, İŞİD ve El Kaide, Libya, Mali, Somali, Sudan ve Yemendir.[57]

Ülkeler genel olarak bu tür ekonomik veya diğer yaptırımlara maruz kalmamak için hedef aldıkları ülke veya topluluk üzerinde baskı kurmak ve onları kendi ekseni etrafında toplamak için vekâlet savaşı yöntemlerine başvurmaktadırlar.

1.5. Vekâlet Savaşlarının Yöntemleri

Günümüzde savaşların sadece ordular arasında gerçekleşen açık cephe savaşı konseptinde anılması imkânsız bir durum haline gelmiştir. Gelişen teknoloji ve etkileri nedeniyle artık birçok aktörün kullanıldığı hibrit savaşlar gündemdedir. Değişen dünya ve gelişen yapı içerisinde bakıldığında ordular önemini kaybetmekte ve operasyonel özellikleri olan birlikler, özel askeri oluşumlar, sivil toplum kuruluşları, rakip görülen devletler içerisinde bulunan muhalif yapılar, terör örgütleri, ekonomik, sosyal ve finansal bağlantılar hibrit savaşlarda ön plana çıkmaktadır.

Vekâlet savaşının temelinde hedef alınan ülkede karışıklık çıkartmak, güven ortamını zedelemek, direnç gösterebilecek grup, kuruluş veya askeri yapıları zedelemek vb. gibi her alanda saldırı oluşturabilecek yapıların kullanılması durumu söz konusudur.

1.5.1. Ayaklanma ve Toplumsal Kargaşa Çıkartma veya Bastırma

Hedef olarak seçilen devlettin dış ilişkilerdeki önem ve dikkatini dağıtmak, dışarıda oluşan olaylara karşı ilgisi azaltmak ve direncini kırmak için ülke içerisinde bulunan muhalif grupların desteklenmesi, aşırı örgütlerin yönlendirilmesi, iktidarın yönetim gücünü zedelemek için ülke içerisinde yapay çatışmalar ve toplumsal eylemler

[56] Behnam Alipourvaghaslou, s.160-162.

[57]Behnam Alipourvaghaslou, s.160-161

çıkartarak yönetim gücünü zayıflatmak amaçlı eylemler bütünü veya taraf olunun bir hükümetin sürekliliğini sağlamak için ülke içerisinde bulunan muhalif ve zayıflatıcı eylemlerin son bulması için yardım sağlamak olarak ifade edilebilir. Bu durum özellikle soğuk savaş döneminde ABD ve Sovyetler Birliği arasında sürekli gerçekleşmiştir. Sovyetlerin Afganistan'ı işgalinden sonra Sovyet kontrolünde oluşturduğu kukla yönetim ile halk arasında meydana gelen çatışma ortamında muhalif güçlerin ABD tarafından desteklenmesi buna bir örnektir. Yakın zamanda Türkiye'de meydana gelen "Gezi Parkı Eylemleri" yabancı basını haklı bir eylem gibi göstererek desteklemesi ve yönetim gücünü zayıflatmaya çalışması bu duruma bir örnek olarak gösterilebilir. Gezi Parkı Eylemleri, devletlerin karşılıklı olarak savaşmadıkları, maliyeti düşük, rakip devleti yıpratma amacı güden bir vekalet savaşı şekli olarak görülmektedir.

1.5.2. Terör ve Terörizm Üzerinden Tehdit ve Gözdağı Verme

Terör halka korku ve panik yaratmadır. Terörün asıl amacı ölenlerin sayısı değil, gerçekleştirilen eylem neticesinde halkta meydana getirdiği korku olmasıdır.[58] Terör tanımında da herhangi bir amaca ulaşmak için sivillerin veya güvenlik güçlerinin ses getirici bir şekilde öldürülmesi olarak tanımlanmaktadır. Terörizm temelinde oluşturulan korku neticesinde istenilen amaçlar doğrultusunda toplumda bilinçsel ve duygusal bir yönelmek sağlanmasıdır. Bu amaçla gerçekleştirilen eylemlerin sansasyonel bir şekilde olması daha sonrasındaki korku ve panik ortamını arttıracağı için hedefler güvenlik ve sivil bile olsa amaç eylem sonrasındaki oluşacak korkunun etkisidir. Buda gerçekleştirilen eylemin güncel tutularak sürekli olarak görsel tutulması ile mümkün olmaktadır. Basın yayın organlarının terör eylemlerini haber yapış şekilleri, gelişen teknoloji sayesinde habere ve bilgiye ulaşma imkanlarının artması ve kontrolünün zorlaşması terör eylemlerinin kontrolsüz gösterimini arttırmaktadır. Bu da terör eylemlerinin amacı olan korku ve panik yaratma ortamına zemin hazırlayan kullanışlı bir araç durumuna gelmektedir. Terör örgütleri tarafından bu yöntem sürekli olarak kullanılmaktadır. Hatta bazen terör örgütleri gerçekleştirecekleri eylemlerin

[58] Yusuf Şen, "Terörün Toplumlar Üzerindeki Sosyo-Ekonomik Etkilerine Bakış: PKK Terörü ve Ağrı Gerçeği," *Ağrı İbrahim Çeçen Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* 1/2, 2015, (ss. 17-70).s.24

görüntü alınması ve yayınlanması için basın mensuplarını eylem yerine götürmektedir.[59] Bazı ülkeler tarafından diplomatik yönden çatışmalar çıkmaza girildiğinde terör eylemleri ile hedef ülkeler tehdit edilmektedir. Terör örgülerinin devletler tarafından desteklenmesi gerçekleştirilen eylemlerin basit, düşük maliyetli ve tarafsız bir durum oluşturması nedeniyle günümüzde tercih edilen bir vekâlet savaşı durumuna gelmiştir. Gerçekleştirilecek her eylem mevcut otorite üzerinde bir baskı aracı olması açısından önemlidir. Ayrıca terörün bir milleti ayrımı olmaması nedeniyle dünya genelinde geçerliği olan bir araçtır. Özellikle günümüzde eylem açısından küreselleşmenin etkisi ile sınır kavramlarının azalması herhangi bir zaman diliminde herhangi bir yerde gerçekleştirilebilecek eylemler olmasından dolayı kullanışlı bir alternatif vekâlet savaşı taktiğidir. Toplumsal alanlarda da eylem gerçekleştirebilecek olması ve sürekli saldırılara maruz kalınması halkın devlet veya hükümete olan güvenini sarsacak iç güvenlik açısından güvensiz bir ortam oluşturacaktır. Bunun yanında hükümetin dışarıda kendisinden istendiği bir şekilde hareket etmemesi sonucunda terör saldırısına maruz kalacağı düşüncesi de uluslararası alanda devletlerin veya hükümetlerin yönlendirilmesinde terör ve terörizmi kullanılacak bir silah durumuna getirmektedir. Uluslararası ilişkilerde, iyi kavramı uluslararası anlaşmalar veya ittifaklarda belirtildiği gibi değil, daha çok gücü temsil eden devlet veya devletlerin menfaatlerine ne kadar uygun olduğu ile belirlenmektedir.[60]

1.5.3. Etnik ve Mezhep Kimliğine Dayalı Çatışmalar Çıkartarak Güçsüzleştirme

Çok uluslu devletlerin dağılması, yıkılması veya devrim ile aynı çatı altında yaşamını devam ettiren grupların ayrılarak ulus devlet yapısına girmeleri, bünyeleri içerisinde bulunan farklı etnik yapılara mensup kişiler ile ortak bir çıkar ve hedef doğrultusunda birleşememeleri sonucunda etnik ve mezhep kimliğine dayalı ortaya çıkan bir çatışma şeklidir. Uluslararası arenada hedef veya rakip olarak seçilen ülke içerisinde bulunan etnik yapıların yönlendirilerek aralarında bir çatışma ve güvensizlik

[59] Osman Vedüd Eşidir, Gökhan Bak, "Şiddet Unsuru Olarak Terör Olaylarının Medyada Haberleştirilmesi", *Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi (ASEAD)*, 2018, (ss13-32),s.19

[60] Ahmet Kavlak, "Terör ve Meşru Terör", *Doğu Batı Dergisi 43, 2007* (ss,221-229) s.229

ortamı kazandırılması ile oluşturulan bir vekâlet savaşı yöntemidir. Etnik ve mezhep farklılıkları kullanılarak sosyal ve ekonomik yönden desteklemek veya ülke bünyesinde bulunan etnik ve mezhep olarak farklı kişilerin haklarının ihlal edildiğini ileri sürerek hedef ülkenin içişlerine karışılması olarak tanımlanmaktadır. Bunun yanında etnik milliyetçiliği kullanarak bulunduğu ülkede, referandum, ayrılma, halk oylaması gibi siyasal eylemlerde gerçekleştirilebilmektedir. Bu sayede hedef alınan ülke baskı altında tutulmakta ve istenen doğrultuda kararlar alması sağlanmaya çalışılmaktadır. Örneğin Rusya Federasyonu'nun Gürcistan üzerinde hakimiyet kurmak, sıcak denizlere inme ve Kafkasya politikalarını desteklemek için, Sovyet Rusya'nın dağılmasından sonra oluşan ortamda Gürcistan ile aralarında sorun yaşadıkları Abhazya ve Güney Osetya çatışmalarında Rusya Federasyonu'nun Abhazya ve Güney Osetya'yı desteklemesidir.[61] Rusya Federasyonu'nun desteği ile bölgede çatışmalar artarak devam etmiştir. Rusya Federasyonu barış çalışmalarında da bulunmuştur. Buradaki amacı ile bölgede barış ortamının sağlanması değil, sağlanan siyasi otoritenin kim tarafından sağlandığının ortaya konmasıdır. Rusya'nın buradaki en önemli politikasının, Abhazya ve Güney Osetya'nın Gürcistan'dan ayrılmasına sağlamaktır. Bu durumda sadece etnik farklılıkların kullanılması ile sağlanmıştır.[62]

1.5.4. Asimetrik Saldırılar ve Düşük Yoğunluklu Çatışma Yöntemleri

Asimetrik savaş; sıcak savaş öncesi veya çatışma esnasında kendisinden üstün durumda olan düşmana karşı, pozisyonunun güçlendirmek adına diğer tarafın düşünce, eylem ve teşkilatlanma olarak zaman ve mekân acısından farklı eylemler geliştirmesiyle icra etmeye çalıştığı bir harekât tarzı olarak tanımlanmaktadır.[63]

Asimetrik savaşın temelinde yatan olgu, kendisinden daha üstün bir güç ile doğrudan karşı karşıya geldiği zaman yok olacak olan bir gücün rakip gücün doğrudan karşısına çıkmak yerine onun farklı güç merkezlerini hedef aldığı savaş yöntemleridir. Uluslararası savaş hukukunda hedef olarak alınamayacak yerlerin asimetrik savaşta

[61] Barış Komar, Nihat Yılmaz, "Gürcistan'daki Etnik Çatışmalarda Rusya'nın Rolü", *İktisadi ve İdari Araştırmalar Dergisi"*, 2022, (ss.34-51), s44

[62] Barış Komar, Nihat Yılmaz, s,45

[63] Sercan Semih Atutay, Davut Ateş, "Türkiye'nin Sınır Ötesi Operasyonlarının Hukuki Çerçevesi," *Gazi Üniversitesi Hukuk Fakültesi Dergisi* 17/3, 2013, (ss. 109-146), s.118.

hedef olarak alınabilmesi, maliyet olarak düşük olması da bu yöntemin tercih edilme nedenlerinden biridir. Hedef ülkede bulunan, ulaştırma altyapısı, petrol ve doğalgaz depolama tesisleri, içme suyu tesisleri, acil durum karşısında hizmet verecek olan yerler, bankalar ve finans kuruluşları gibi hedeflerin alındığı asimetrik savaş yöntemidir. Asimetrik savaşta birliklerin önceden plan yapması imkansızdır. Çünkü karşı tarafın nerede ve ne zaman saldıracağı belirsizdir.[64] Asimetrik savaşta istihbarat ve istihbarata karşı koyma çok önemlidir. Karşı tarafın nerede ve nasıl saldıracağını bilmek tedbir almak ve saldırıya hazır olma imkânı sağlamaktadır.[65]

Düşük yoğunluklu çatışmalar ise hedef veya hasım devletin kaynaklarının sürekli olarak boşa harcamasını sağlayacak şekilde oluşturulan çatışma ortamlarıdır. Bu sayede hedef ülke kaynaklarını sürekli olarak boşa harcayarak yapması gereken yatırımları yapamayacak ve bir noktaya odaklandığı için uluslararası arenada etkinlik gösteremeyecektir. Düşük yoğunluklu çatışmalarda özellikle enformasyon akışı önemlidir. Düşük yoğunluklu çatışmaların yaşandığı yerler genellikle, enformasyonun zayıf olduğu ve dezenformasyonun arttığı yerlerdir. Ukrayna'nın Donbas ve Kırım bölgelerinde Rusya'nın yürüttüğü dezenformasyon faaliyetleri, bu durumu göstermektedir. Bu kapsamda Türkiye Cumhuriyeti'nin 1980'lerin ortalarından beri PKK terör örgütüne karşı sürdürmüş olduğu yöntem düşük yoğunluklu çatışma yöntemidir.

1.5.5. Siber Saldırı Örgütleri ile Zarar Verme

Teknolojinin ilerlemesi ve bilginin önemi tartışmasız en üst seviyelerdedir. Teknolojik gelişmelerde insanların günlük yaşamları içerisinde bulunan ulaşım, iletişim, enerji, sağlık, güvenlik vb pek çok alanda insan hayatının bir parçası olmaktadır. Teknolojinin insan hayatını kolaylaştıran yanı olduğu kadar insanları daha kolay hedef haline getiren yanları da vardır. Terör örgütleri tarafından teknolojinin kötü amaçla kullanılması insan yaşamını etkilemektedir. Terörün odak noktasının korku ve panik yaratmak, maddi ve manevi zarar vermek olduğu düşünüldüğünde siber ortamda istenen

[64] Talat Şafak, "Asimetrik Savaş Örneği Olarak 2006 İsrail-Lübnan Savaşı Hizbullah ve Çıkarımlar", *Aşiyan Kültür-Sanat ve Edebiyat Dergisi, 2013,* (ss 19-25), s.24

[65] Talat Şafak, s.24

etkiyi sağlayabilmektedir. Ülke içerisinde ulaşım, enerji dağıtımı, iletişim, finans gibi pek çok unsur teknoloji sayesinde kontrol edilmektedir. Bu durum hedef alının ülkeler acısında diğer ülkeler tarafından saldırı yeri olarak seçilmektedir. Konvansiyonel saldırılar veya terör eylemlerine göre gizlilik sağlaması bu yöntemin kullanılmasında tercih edilme nedenidir. Fakat bir intihar saldırıcısının yaratmış olduğu etkiyi sağlayamaması nedeniyle daha düşük bir etki yaratmaktadır. Siber saldırı; internet bağı kullanılarak siber ortamda örgütlerin, devletlerin veya bireylerin diğer devlet, örgüt veya bireylere karşı gerçekleştirdikleri bilgi çalmak, istihbarat toplamak ve diğer kişilerin elektronik alt yapısına zarar vermek amaçlı gerçekleştirdikleri saldırılardır.[66] Bu saldırıların devletler arasında olması durumu da siber savaş olarak isimlendirilmektedir. Devletlerarası ilişkilerde ise siber saldırılar daha ziyade gözdağı verme aracı olarak kullanılmaktadır. Örneğin ABD tarafından İran nükleer santraline gerçekleştirilen Stuxnet saldırısı İran'ın nükleer çalışmalarını yok etmeye yönelik bir saldırı olarak görülmektedir. Her ne kadar İran'ın yaptığı çalışmaları yok etmeyi başaramamış olsa da gerçekleşen etki neticesinde İran nükleer araştırmalarını en az iki yıl geriye döndüğü bir gerçektir. ABD tarafından kabul edilmemesi ve İran tarafından da ispatlanamaması nedeniyle bu saldırının gizlilik durumu halen devam etmektedir. Bu nedenden dolayı saldırılar sonrasında sağlamış olduğu anonimlik nedeniyle siber saldırılar vekâlet savaşlarında en çok tercih edilen saldırı yöntemlerinden biridir. Rusya'nın Estonya'ya karşı gerçekleştirmiş olduğu siber saldırılarda bu duruma örnek olarak verilebilir. Rusya'nın kabul etmemesi ve Estonya'nın da maddi deliller ile destekleyememesi neticesinde saldırı anonim olarak kalmıştır. Bilinen sadece saldırı esnasında çok sayıda Rusya'ya ait sunucular kullanılmış olmasıdır.[67]

1.5.6. Diğer Taktik ve Stratejiler

Vekâlet savaşları içerisinde, beşinci kol faaliyetleri olarak anılan faaliyetlerde bulunmaktadır. Bunların başında toplumsal psikolojik etki içerisinde çökertmek gelmektedir. Gelişen teknoloji ve sosyal medya ağları, iletişim araçlarındaki gelişmeler ve bu ağların saldırıya açık ve dezenformasyon durumunun bulunmasından dolayı

[66] Orhan Kurudal, "Bilişim Çağımda Siber Saldırılar ve Yeniden Bloklaşma", *Dünya İnsan Bilimleri Dergisi*, 2020-2, (ss. 132-158), s134

[67] Orhan Kurudal, s.147

buralarda istenen etkiler oluşturulabilmektedir. İnternet ortamında özellikle bilginin doğruluğunun zor olması veya imkânsızlığı, yayılımının kolay ve ulaşımının basit olması ile toplumsal psikolojik durumlar yaratmak kolaylaşmıştır. İnternet ortamında herhangi bir resim veya haber üzerinde gerçekleştirilecek bir manipülasyon sonucunda toplumda psikolojik baskılar oluşturulmaktadır. Diğer faaliyetlerden olan psikolojik harekât ise kitlelerin zihin duygu tutum ve davranışlarını etkilemek için bilimsel teknik ürünler ile varılmak istenen amaca yönelik propaganda yapılarak düşüncelerin ve algıların değişmesini sağlamak olarak tanımlanır.[68]

Hedef ülkeye yönelik ekonomik ve finansal etkilemelerde bir vekâlet savaşı olarak kabul edilebilir. Günümüzde hegemonik güçler uluslararası finans gücünü yön vermektedir. Bir ülkenin kredi notu çoğunlukla, politik ve ekonomik risklerin bir bileşeninden oluşmaktadır. Uluslararası yatırımcılar da yatırım yapmak istedikleri bir ekonomide bu notlara bakmaktadırlar.[69] Uluslararası kredilendirme şirketlerini bünyesinde bulundurmaları ve uluslararası şirketlerin bu finans kuruluşlarının kredilendirme notuna göre yatırım yapmaları ülkelere yapılan yatırımların durdurulması veya arttırılması için önem arz etmektedir. Kredilendirme şirketlerinin bir ülkenin kredi notunu değiştirmesi veya kredi notunu değiştirmemek ile birlikte ülkenin durumunu kötüleyici bir açıklama yapması bile hedef ülke için zor durumda kalacağını gösterir bir durumdur.

Bunların dışında BM ve NATO gibi ulusüstü örgütlerinde vekâlet savaşlarında kullanıldığı durumlar bulunmaktadır. Buna en iyi örnek olarak Irak ve Afganistan işgallerinde Barış Gücü, İnsani Yardım gibi kavramları kullanmaları ve bu sayede ulusüstü kuruluşların desteğini alarak operasyon gerçekleştirmiş olmalarıdır. Başta ABD, İngiltere ve Fransa olmak üzere ülkeler etki altında bulundurdukları ülkelere gerçekleştirdikleri operasyonları yasal ve toplumsal bir destek görünümü altında göstermek için NATO ve BM gibi örgütleri bir vekil yapı olarak kullanmaktadırlar.

[68] Hasan Ateş, *Vekâlet Savaşı Stratejisi Ekseninde Gizli Kuvvet İstihbarat*, Detay Yayınları, Ankara 2017, s.17-19

[69] Bilal Kargı, "Uluslararası Kredi Derecelendirme Kuruluşları ve Türkiye'nin Kredi Notu Üzerine Bir İnceleme", *International Journal of Social Sciences* 2014, (ss 351-370), s.353

ABD'nin Çöl Fırtınası harekâtı, resmen bir NATO harekatı olmamakla birlikte, NATO'nun koordinasyonu için gerekli NATO üyesi ülkeyi bir araya getirmiştir.[70]

1.6. Vekalet Savaşlarının Siber Güvenlik Bağlamı

Yukarıda sayılan nedenlerden dolayı, ülkelerin kendi güvenlikleri ve çalışmaları için bilinçlenmesi ve güvenliklerini sağlamak için bazı düzenlemeler yapmaları gerekliğini oluşmaktadır. Uluslararası alanda güç kullanımı açısında siber saldırılar her gün daha fazla bir şekilde kullanılmaktadır. Bunun en başta gelen nedenlerinde birinin ulusüstü kuruluşların bildirilerini ve ülkeler açısında nefsi müdafaa durumu dışında diğer ülkelerin toprak bütünlüğüne saygı göstermek mecburiyetlerinin bulunmasıdır.

Ulusal ve uluslararası alanda kurumlar ve ülkeler kendi çıkarlarını korumak için farklı yöntemler denemektedir. Günümüzde teknolojik açıdan meydana gelen gelişmeler teknolojinin zorunluluk haline gelmesi doğrultusunda, uluslararası ve ulusal alanlarda siber saldırılar öncelikli tercih yöntemi olarak kullanılmaktadır. Siber saldırılar sonucunda karşı tarafa verilen zararlar, psikolojik etkiler ve yapılan hızlı propagandalar ile istenen etki az maliyetli ve çabuk bir şekilde elde edilmektedir. Siber uzay kavramı fiziksel ve sanal alanın karışımı bir alandır. Sanal alanda meydana gelen bir eylem fiziksel alanda etki göstermektedir. Sanal alanda gerçekleşen eylemlerin fiziksel alanda etki oluşturması siber güvenlik kavramını ortaya çıkarmaktadır. Bu yüzden siber güvenlik alanında alınan tedbirler ulusal güvenlik kavramını ortaya çıkarmaktadır.[71] Bu duruma karşı kişiler, ülkeler ve ulusüstü örgütler tarafından bazı güvenlik önlemleri alınması bir gereklilik haline gelmiştir.

Günümüzde teknoloji kullanımı bir tercih olmaktan çıkarak, bir zorunluluk durumuna gelmiştir. Teknolojik imkanların gelişmesi, oluşan sanal ortamlar kişileri bulundukları gerçek ortamlardan uzaklaştırarak daha çok sanal ortamda vakit geçirmeye yöneltmektedir. Bu durumda vekâlet savaşları için kolay ulaşım ve etkileşim yapmak için kullanılan bir yöntem haline getirmektedir. Vekâlet savaşlarının temelinde hedef alınan toplum veya ülke içerisinde bulunan kişiler üzerinde belirli bir algı oluşturmak ve

[70] Sanem Özer, Ceren Uysal Oğuz, Senem Atvur, "NATO ve AB'nin Değişen Güvenlik Stratejilerinin Afganistan Örneğinde Değerlendirilmesi", *Akdeniz İ.İ.B.F. Dergisi*\ 2010, (ss 257-285) s.265

[71] Sahil Bıçakcı, "Siber Güvenlik ve Savunma", *Güvenlik Yazıları Portalı*, Kasım 2019, (ss. 1-8), s.1

tebaası bulunulan toplumun kendisi için olumsuz olduğu, kendisini veya etnik yapısını önemsemediği bilincinin oluşturulması gerekmektedir. Kişilerin algısını değiştirmek için onlar ile iletişim içerisinde olmak ve onların fikirlerine dokunmak gerekmektedir. Bu aşamada teknoloji devreye girmektedir. Vekâlet savaşlarının temelinde en az maliyet ile en fazla etki gerçekleştirmek olmasından dolayı teknolojinin sağlamış olduğu sanal ortamdaki etkileşim çok etkili bir iletim ortamı sağlamaktadır. Aşağıda teknolojinin insanlara etkileşimi üzerine bir istatistik verilmektedir.

50 Milyon kullanıcıya ulaşma süresi

1- Radyo: 38 yıl
2- Televizyon: 13 yıl
3- İnternet: 4 yıl
4- Facebook'un 100 milyon kullanıcıya ulaşma süresi: 9 ay

(İnsanlar tarafından kullanılan teknolojilerin etkileşim hızları ve iletişim süreleri gösterilmektedir.)[72]

Bu istatistikten de anlaşılacağı gibi örgütler ve devletler hedeflerindeki toplumun bireylerine ulaşmak ve bireyler üzerinde etki sağlamak için teknolojik imkanları kullanmakta ve yüz yüze belki ulaşmayacağı kadar kişiye ulaşarak etki oluşturmaktadır. Teknoloji sadece saldırı amaçlı değil propaganda, manipülasyon, ajitasyon ve kıyaslama aracı olarak da kullanılmaktadır.

[72] Yetişkinler için Siberay Farkındalık Slaytı, Siber Suçlarla Mücadele Daire Başkanlığı, https://www.siberay.com/sunumlar, (Erişim tarihi: 01.03.2023), s. 26.

2. SİBER GÜVENLİK

2.1. Siber Güvenlik Konusuna Genel Yaklaşım

Teknolojideki hızlı gelişme, buna bağlı olarak küçülen dünya ve sadece çizgisel bir anlam olarak görünmeye başlayan sınırlar ülkelerin ve ulus üstü örgütlenmelerin fiziki tedbirler yanında internet (sanal ortam, siber uzay, sanal alem vs.) gibi yerlerde de tedbirler almaya zorlamıştır. Günlük yaşantımızın bir parçası olmaktan çıkarak bir zorunluluğu haline gelen internet sınırsız bir bilgi havuzu içermekle birlikte sınırsız bir tehlike bataklığı durumuna gelmiştir. Günümüz dünyasında, gelişen teknolojiyle insanların birbirleri ile iletişiminin hızlanması ile orantılı olarak insanların birbirlerine karşı gerçekleştirebilecekleri saldırılarda aynı oranda ve hızda artmaktadır. Bu saldırı ve savunma durumları devletler, ulus-uluslararası şirketler ve ulusüstü birliklerinde hedef alındığı bir durum ortaya çıkarmıştır. Esasen internet, ilk bulunduğunda sadece bilgi paylaşımı ve sınırsız bir iletişim aracı olarak kurulduğu için herhangi bir saldırıya karşı tedbir alma gereksinimi duyulmamıştır. Fakat daha sonra kötü niyetli kişilerini aracı ve arka kapısı durumuna gelmesi, hayatın idamesinde zorunlu hale gelen ülkeler için milli güvenlik açısından önemi bulunan alt yapılar olan; barajlar, su arıtma tesisleri, petrol tesisleri, enerji sistemleri, telekomünikasyon, e-Devlet sistemleri, ulaşım sistemleri, finansal sistemler gibi yerlerin hedef alınması sonucunda internet ortamında da önlemler ve savunmacı tedbirler alınması bir zorunluluk haline gelmiştir.

Siber güvenlik konusunda karşılaşılan en büyük problemlerden biri, özgürlük ile güvenlik dengelenmesidir.[73] Siber ortamda güvenlik sağlamaya çalışırken, asıl amaç olan bilginin özgürce dolaşımı olan internetin amacı dışına çıkmamak gerekmektedir. Güvenlik gerekçeleri ile hükümetler, kişilerin özel bilgilerini, internet ve telefon iletişim bilgilerini takip ettiği ortaya çıkaran gelişmeler olduktan sonra internet kullanıcıları arasında ciddi kaygılar oluşmuştur.[74] İnternet altyapısına gelebilecek fiziki zararlar

[73] Mehmet Nesip Öğün, Adem Kaya, "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler," *Güvenlik Stratejileri Dergisi,* (ss. 145-181), s.151.

[74] Mehmet Nesip Öğün, Adem Kaya, s.151

kullanıcılara yönelik tehditler oluşturmaktadır. Aynı şekilde zararlı yazılımlar ve kodlarda internet kullanımını kısıtlamaktadır.[75]

Bir taraftan da siber suçlar her gün artmakta ve bu suçlar ülke ve dünya ekonomisi için ciddi tehlikeler oluşturmaktadır. Bu amaçladır ki; Avrupa Birliği Göç, İçişleri ve Vatandaşlıktan Sorumlu Komisyon Üyesi Dmitris Avramopoulos, Avrupa Birliği Polis Teşkilatı (Europol) tarafından hazırlanan 2019 internetten işlenen değerlendirmesi raporu için "*Siber suçlara karşı bir arada hareket etmeliyiz. Çünkü bu sadece devletlerin değil, herkesin sorumluluk sahibi olduğu bir alan*" ifadelerini kullanmıştır.[76] Ayrıca aynı raporda çocuk istismarı suçunun internetten hızlı yaygınlaştığına değinilmiştir. Bunun yanı sıra siber suçların diğer konvansiyonel suçlarla birlikte işlenerek daha büyük tehditler oluşturabileceği belirtilmiştir.

Türkiye'de 2018 yılında gerçekleştirilen 5. Uluslararası Siber Suçlar Çalıştayı katılımcılarının konuşmalarında bu konuda pek çok önemli noktaya değinmişlerdir:

> Hollanda Yüksek Teknoloji Suçlarıyla Mücadele Birimi temsilcisi Sn. Roeland Van ZEIJST'in "Bilgisayar korsanlarının özellikle banka müdürlerini takip ettiklerini doğru zamanı beklediklerini ve Truva atı tabir edilen zararlı yazılımlar aracılığı ile banka bilgileri olan IBAN bilgilerini uzaktan erişim yolları ile ele geçirmeye çalıştıklarını, bunun yanında Dark web denen karanlık ağların kullanıldığı sanan ortamlarda çocuk istismar görüntüleri, çalıntı kredi kart bilgileri, sahta pasaport bilgileri ile uyuşturucu ve silah kaçakçılığında artış gözlemlendiğini beyan etmiştir."[77]
>
> Western Union temsilcisi Sn. Alan Perkins; "200 ülkede 550 bin acentelerinin bulunduğunu, suç tipleri üzerinden çalışın bir istihbarat birimlerinin olduğunu ve terörizmin finansmanı konusunun kendileri içinde büyük bir önem arz ettiğini, uyuşturucu satıcılarının küçük miktarlarda para transferleri yaparak dikkat çekmemeye çalıştıklarını, siber suçların özellikle uyuşturucu ticareti, insan ticareti, çocuk istismarı ve taklit ürünlerin satışında kilit rol oynadığını" beyan etmiştir.[78]
>
> ICAN temsilcisi Sn. Beher Esmat; "DNS de tıpkı diğer unsurların olduğu gibi toplum için yararlı olduğu kadar kötü amaçlı kullanıma da açık olabileceğini, çevirim için bankacılık aktivitesi yapıldığı esnada bir internet sitesinden DNS bağlantısının hacklenmesi sebebiyle kendinizi ummadığınız başka bir alanda bulabileceğinizi, DDOS ataklarının da çok popüler bir DNS saldırılarından biri olduğunu, DNS server Owner çökertmenin interneti çökertmeye

[75] Ecem İren, Özgü Can, "Bilgi Sistemlerinde Güncel Güvenlik Problemleri ve Önerilen Çözümler," *TUBAV Bilim Dergisi* 10/2, 2017, (ss. 27-42), s.40

[76]Selman Aksünger, "Siber Suçların Ekonomiye Verdiği Zararlarda Büyük Artış," *Anadolu Ajansı*, Son Güncelleme Tarihi: 10.10.2019, https://www.aa.com.tr/tr/dunya/siber-suclarin-ekonomiye-verdigi-zararda-buyuk-artis-/1608143, (Erişim tarihi: 01.03.2023).

[77] *5. Uluslararası Siber Suçlar Çalıştay Raporu*, Siber Suçlarla Mücadele Daire Başkanlığı, 10-13 Aralık 2018, s.23.

[78] *5. Uluslararası Siber Suçlar Çalıştay Raporu*, s.23

ve hatta çevirim için servileri çökertmeye yarayabileceğini bunun temelinde de çalınan domainlerin suç teşkil ede eylemlerde kullanılabileceğini" beyan etmiştir.[79]

Vodafone temsilcisi Sn. Gökhan Bozdoğan; "Teknolojinin gelişmesi ile birlikte siber saldırı kavramının çok değiştiğini, önceden sadece şirketlere, kurumlara ve devletlere gerçekleştirilen siber saldırıların bireysel olarak artık vatandaşlara da gerçekleştirilir bir hale geldiğini, bu nedenle güvenlik kavramının her birimiz tarafından dikkat edilmesi gerektiğini, siber saldırıların engellemesi kadar siber suçların engellemesinde güvenlik politikaları ve yaklaşımları olgusunun ortaya çıkmasında rol oynadığının; network güvenliği, uygulama güvenliği, mobil güvenlik, mobil güvenlik, data güvenliği gibi data güvenliğinin gibi huşuların bugün petrolden daha değerli olduğu, Google, Yahoo, Instagram gibi şirketlerin bu gün değerli olmasının tek nedeninin sahip oldukları içerik ve data olduğu, donanım alt yapısının sağlam olması kadar siber suçlar ve siber güvenliğe yaklaşımın milli bir güvenlik problemi olduğunun farkında olunmasının, bu doğrultuda kurulların kurulmasının ve kararların hızlı verilip anlık aksiyonların alındığı birikimli birimlerin çalışmasıyla sağlanabilecektir alt yapının kurulmasının önemini, siber saldırılara ve siber suçlara karşıda en etkin çözümün merkezi bir çözüm bulmak olduğunu"[80] vurgulamıştır.

Japan Cybercrime Ctrol Center (jc3) Birimi temsilcisi Sn. Sotoshi SHIMUZU; "Siber suç araştırmalarının kapasitesinin arttırılması gerektiğini, bunun yanında siber suçlara yaklaşımında önemli olduğunu, siber suçlara araştırmasını zorlaştıran temel dört nedenin olduğunu, bunların ilkinin herhangi bir sınırının bulunmaması ve gerçekleştirmenin daha az maliyetli olduğunu, siber suçun niteliğinin belirlemesinin çok zor olduğunu sırf bu nedenle bazı siber güvenlik sitelerinin bunları konuşmak için bloglar oluşturduğunu, bir diğer zorluğun kullanılan dil olduğunu, saldırganın dil değiştirme programları ile farklı dillerde suç işleyebileceğini bunun sonucunda soruşturmacının sorunlar yaşayacağını, dördüncü olarak da suç işleyen kişilerin IP bilgilerini kullandığı programlar veya GDPR gibi kanunlar sayesinde takibinin zorlaştığını, suçun mağduru ile failin farklı ülkelerde olmasının soruşturmayı zorlaştırdığını, ülkelerdeki kanunların farklı olmasında dolayı da problemler yaşandığını bunun önüne geçebilmek için standart bir uygulama üzerinde yoğunlaşılması gerektiğini"[81]beyan etmiştir.

Konuşmalardan da anlaşılacağı üzere, siber saldırı ve siber suçlar teknoloji ile paralel ve hatta daha hızlı bir şekilde gelişmektedir. Kullanışlı olması, maliyetinin düşüklüğü, sınır kavramının olmaması, takibinin zor olması vb. nedenlerden dolayı kullanım tercihinin başlıca nedenleridir. Yine konuşmacıların birleştiği ortak noktanın, siber saldırı ve siber suçlara karşı ortak mekanizmalar oluşturulması, merkezi yapıların oluşturularak bilgi paylaşımının arttırılması ile saldırı ve suçlara karşı ortak tepki verilebilecek yapıların oluşturulması, bunun yanı sıra sürekli olarak kendisini yenileyen donanımlı personellerin oluşturulması gerektiğine vurgu yapılmıştır. Tüm bu konular arasında asıl olan teknolojik gelişmeler karşısında bireysel farkındalığın oluşturulması ve kişisel güvenliklerin öneminin farkındalık yaratacak şekilde geliştirilmesidir.

[79] *5. Uluslararası Siber Suçlar Çalıştay Raporu*, s.24

[80] *5. Uluslararası Siber Suçlar Çalıştay Raporu*, s.25.

[81] *5. Uluslararası Siber Suçlar Çalıştay Raporu*, s.25-26.

2.2. Siber Güvenliğin Temel Kavramları ve Siber Güvenliği Tehdit Eden Araçlar

Siber Güvenliği oluşturan temel kavramlar; Siber Uzay, Siber Güvenlik, Siber Saldırı, Siber Savunma, Siber Terörizm, Siber Savaş ve Siber Silah olarak isimlendirilebilir. Siber Güvenliği tehdit eden araçlar ise; virüsler, Truva atları, kurtçuklar (Worms), Zombie ve botnetler, istem dışı elektronik postalar (spam), klavye işlemleri kaydeden yazılımlar, casus yazılımlar, servis dışı bırakmalar (DoS), aldatma (IP spoofing), şebeke trafiğinin dinlenmesi, yemleme ve propaganda olarak sayılabilir. Bu kavramlara kısaca değinmekte yarar vardır:

2.2.1. Siber Uzay

Bilgisayarların ve onu kullanan insanların internet ve benzeri ağlar içinde kurduğu iletişimden doğan sanal gerçeklik ortamını anlatan metaforik bir alandır. İnternet iletişim yöntemi acısında siber, yarattığı ortam acısında sanaldır. Siber uzay; *"Tüm dünya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunların birbirlerine bağlayan ağlardan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam olarak tanımlanmaktadır."*[82] Siber uzay devletlere yeni bir savaş ve mücadele alanı olarak seçilmiştir. ABD Savunma Bakanlığı tarafından; "*internet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü işlemci ve denetleyicileri de içeren, bilgi teknolojisi altyapılarının bağımsız ağlarından oluşan küresel etki alanı"* olarak ve 2001 yılında ABD Kongre Araştırma Servisi raporunda ise, *"insanların, bilgisayarlar ve telekomünikasyon aracılığıyla fiziksel coğrafya dikkate alınmadan tümden birbirine bağlı olması"*[83]şeklinde tanımlamıştır.

2.2.2. Siber Saldırı

Yönetim ve toplum üzerinde olumsuz etki oluşturabilecek farklı amaçları gerçekleştirmek için hedef seçilen şahıs veya kuruma bilişim sistemlerinin işleyişinin

[82] Siber Dünya Nedir?, Siber Suçlarla Mücadele Daire Başkanlığı, https://siberay.com/siber-dunya-nedir, (Erişim tarihi 01.03.2023).

[83] Siber Uzay ve Siber Güvenlik Kavramları, Türkiye Cumhuriyeti İçişleri Bakanlığı, İç Güvenlik Stratejileri Daire Başkanlığı, s. 9.

engellenmesi veya değiştirilmesi amacını güden planlı ve koordineli sanal eylemler bütünüdür. Siber Saldırılar kötü amaçlı yazılımların kullanıldığı bir sıralama ile gerçekleştirilen saldırılardır. Malware (kötü amaçlı) olarak isimlendirilen yazılımlar genellikle e-posta eki veya zararsız bir indirme yolu ile yayılan yazılımlardır. Siber Saldırı (Savaş); diğer ülkeler ile siyasal uyuşmazlık ve askeri çatışma durumlarında hasım ülkelere kısmi zararlar vermek (kısa süreli ekonomik zarar vermek, haberleşme ve ulaşım sistemlerini işlemez hale getirmek ve internet tabanlı hizmetleri aksatmak) kritik tesisleri sabote etmek veya siber casusluk maksadı ile kullanılmasıdır.[84] Türkiye Cumhuriyeti Ulaştırma Denizcilik ve Haberleşme Bakanlığı tarafından; "*Ulusal siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın her hangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler*[85] olarak tanımlanmıştır.

2.2.3. Siber Suç

Avrupa Toplulukları Komisyonu siber suçu elektronik iletişim ağları ve bilgi sistemleri kullanılarak veya bu tür ağ ve sistemlere karşı işlenen cezai fiiller olarak tanımlamaktadır. Siber Suçlarla Mücadele Daire Başkanlığı tarafından bilişim sistemleri kullanılmadan işlenemeyen suçlar olarak tanımlanmıştır. Siber suçlar tasnifi üç başlık altında incelenmektedir. Bunlar aşağıdakilerdir:[86]

Siber Destekli Suçlar: Birinci nesil siber suçlar olarak da anılan bu suçların işlenmesinde bilişim sistemlerinin çok az desteğinin olduğu suçlardır. Örneğin bir banka soygunu suçunun işlenmeden önce bankaya ait yerleşim krokisinin bilişim sistemleri kullanılarak elde edilmesi örnek olarak verilebilir.

Siber Nitelikli Suçlar: ikinci nesil suçlar olarak da ifade edilmektedir. Bu tür suçlar; geleneksel suçların işlenmesinde bilişim sistemlerinin kullanılması ile

[84] Covid 19 Pandemisi Döneminde Siber Suç Riskleri ve Güvenliğe Etkileri, Türkiye Cumhuriyeti İç İşleri Bakanlığı, İç Güvenlik Strateji Daire Başkanlığı, s. 58.

[85] *2016-2019 Ulusal Siber Güvenlik Stratejisi*, Türkiye Cumhuriyeti Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf, (Erişim tarihi: 19.12.2022).

[86] Siber Uzay ve Siber Güvenlik Kavramları, s.12-13.

gerçekleştirilen suçlar olarak tanımlanmaktadır. Örneğin, kimlik hırsızlığı, internet tabanlı kredi kartı dolandırıcılığı, oltalama gibi suçlardır.

Siber Ortama Özgü Suçlar: Siber bağımlılık suçları olarak da ifade edilmektedirler. Gerçekleştirilebilmeleri için internet tabanlı bilişim sistemlerinin kullanılmasının zorunlu olduğu suçlardır. Örnek olarak; Zararlı Yazılım Saldırıları, Bilgisayar Korsanlığı, Fidye yazılım saldırıları gibi saldırılardır.

2.3. Siber Güvenlik İlgili Kavramlar

2.3.1. Siber Güvenlik

Siber saldırıların engellenmesi veya hiç başlatılmaması için alınan tedbirlerin tümü siber güvenlik olarak adlandırılmaktadır. Her alanda kullanılan güvenlik teknolojileri siber güvenliğin araçları arasında yer alır. *Bilgi teknolojileri güvenliği* veya *elektronik bilgi güvenliği* olarak isim verilmektedir. Bilgisayarlar, mobil cihazlar, bilgisayar ağlarını ve elektronik verileri zararlı yazılımlara karşı korumak olarak da ifade edilebilmektedir. Geniş bir kavram olan siber güvenlik farklı kısımlardan oluşmaktadır. Bunlar; ağ güvenliği, bilgi güvenliği, operasyonel güvenlik, olağanüstü durum kurtarma ve iş sürekliliği, son kullanıcı eğitimi olarak isimlendirilebilir. Türkiye Cumhuriyeti Ulaştırma ve Denizcilik Haberleşme Bakanlığı tarafından; "*Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunması, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınması, saldırıların ve siber güvenlik olaylarının tespit edilmesi, bu tespitlere karşı tepki mekanizmalarının devreye alınması ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi"*[87] olarak tanımlamıştır.

2.3.2. Siber Savunma

Siber saldırılara karşı bireysel, kurumsal veya ülke olarak tehdit ve saldırıyı bertaraf etmek, meydana gelen saldırıyı sonlandırmak, geri çevirmek ve sonuçlarını

[87] *2016-2019 Ulusal Siber Güvenlik Stratejisi*, Türkiye Cumhuriyeti Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf, (Erişim tarihi: 19.12.2022).

minimize etmek için kaynakların koordineli bir şekilde kullanılması, mevcut yeteneklerin geliştirilmesi ve ulusal çapta bilinçlendirme sonucunda özellikle milli kampanyaların oluşturulmasına siber savunma denir.

2.3.3. Siber Savaş

Küreselleşmenin etkisiyle, fiziksel sınırların sadece çizgisel bir kavram haline gelmesi gerçek dünyadan ziyade sanal olan siber uzayın gerçekliğinin artması yaşamın bir parçası olmaktan çıkarak bir zorunluluk haline gelmesi ile oluşan ortamda gerçekleşen, siber saldırı, siber terörizm, siber suçlar gibi kötü amaçlı kullanımlar için geliştirilmiş kötü amaçlı yazılımların kullanılması sonucunda sanal ortamda maddi menfaat, siyasi çıkar, askeri tehdit vb. amaçlarla kullanılan her türlü çatışma ortamına siber savaş denilir. Bir ulus devletin başka bir ulus devlete ait bilgisayarlara veya bunlara bağlı ağlara, hasar vermek, aksatma amaçlı gerçekleştirdiği sanal saldırılar olarak tanımlanmaktadır. [88] Bu savaşın konvansiyonel savaştan ayrılan belirgin özellikleri arasında çok az sayıda kişi tarafından büyük kitleleri etkileyebilecek sonuçlar doğurduğu, düşük maliyetli olması ve izlerini kaybedebilmesinden dolayı hibrit savaşlarda yoğunluk olarak başvurulan bir yöntemdir.

2.3.4. Siber Silah

Gerçek dünyadaki silah kavramı ile aynı düşünülebilmekle birlikte, hedef alınan bir ağ yapısını kontrol etmek veya buradan sürekli ve düzenli olarak bilgi çekmeye yarayacak özel olarak tasarlanmış virüs ve kod parçalarından oluşan Zararlı yazılımlara siber silah denilebilir.[89] Siber silahlar hedef alınan yapıya genellikle e-posta, zararsız görünen indirme işlemleri, SQL veri tabanlarına yerleştirilen kodlar (SQL aşılama) ile oluşturulan açıklıklardan giriş yapılmak sureti ile kullanılmaktadır. Bu durumda

[88] Serkan Yenal, Naci Akdemir, "Uluslararası İlişkilerde Yeni Bir Kuvvet Çarpanı: Siber Savaşlar Üzerine Bir Vaka Analizi," *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* 11/1, 2020, (ss. 414-450), s.419.

[89] Ersin Çahmutoğlu, "Siber Uzayda Güç ve Siber Silah Teknolojilerinin Küresel Etkisi," *Analitical Politic* 1/1, 2020, (ss. 63-79), s.69.

karşımıza özellikle siber güvenlik aşamalarından biri olan son kullanıcı eğitiminin önemini ortaya çıkarmaktadır.

2.3.5. Siber Terörizm

Gerçek hayatın içende bulunan terörizm kavramı ile aynı amaca yönelmektedir. Belirli bir amaca ulaşmak için bir sanal alemde siber silahların kullanılması ile bilgisayar ağlarının kurulum amaçlarının dışına çıkartılarak kendi amaçları doğrultusunda halkı baskı altında tutma, yıldırma politikalarının hepsine siber terörizm denilmektedir. Günümüz teknolojisi ile çok hızlı bir dağılım sağlayan sosyal ağlarda dezenformasyon yaratarak olmayan bir bilgiyi gerçekmiş gibi göstererek gerçekleştirilen eylemler bütünüdür.[90] Sanal ortamda bilgiye ulaşmak ne kadar kolaysa bir bilginin yayılması da o kadar kolaydır. Buna karşılık bilginin doğruluğunu araştırma zahmetine girmeden ilk okunanın doğru olduğu kanaatine varılması da bilinçsiz bir kullanıma örnek olarak verilebilir. Sanal ortamda karşılaşılan bilgilerinin hepsine makul şüphe ile yaklaşarak bilginin genel kabul görmüş güveniler ortamlardan en az üç farklı kaynaktan doğrulanması gerekmektedir.

2.4. Siber Güvenliği Tehdit Eden Unsurlar

Siber güvenliği tehdit eden unsurlar denildiğinde herkesin ortak bazı unsurlar üzerinde birleştiği görülmektedir. Bunlar virüsler, solucanlar, Truva atları olarak sayılabilmektedir. Fakat siber güvenliğin en büyük riski kuşkusuz ki insan unsurudur. Burada insan unsuru olarak belirtilmek istenen, bilinçsiz kullanıcı olarak tabir edilen kısımdır. Bilinçsiz bir kullanıcının, internette son derece ilgi çekici olarak hazırlanmış bir linke tıklaması ile kendi bilgisayarındaki bütün özel bilgilerin alınması, hatta bilgisayarının başka suçlarda kullanılmasına imkân vermesi anlamına gelmektedir.[91] Aynı şekilde bilinçsiz bir kullanıcının yaptığı bir hata ile aynı ağa bağlı birçok bilgisayar

[90] Hüseyin Kazan, "Terör-Medya İlişkisi ve Medyada Terör Haberciliği," *Güvenlik Stratejileri Dergisi* 24, 2012, (ss. 109-147), s.131.

[91] Şahin Bayzan, Gülbahar Aytekin, "Neden Bilinçli ve Güvenli İnternet," güvenliweb.org.tr blog, Son Güncelleme Tarihi: 23 Nisan 2017, https://www.guvenliweb.org.tr/blog-detay/neden-bilincli-ve-guvenli-internet, (Erişim tarihi 20.01.2023).

ve ağ sistemi zarar görmektedir. Hatta bu zararlar fiziki zararlara dönüşmekte kitlesel zararlar doğuracak durumlara gelebilmektedir. Bunu en iyi örneklerden biri olarak Stunex'i verebiliriz. Stunext, endüstiriyet kontrol sistemlerini ve dış dünyaya kapalı sistemleri hedef alabileceğini ve bilgisayar yazılımlarının fiziki bir hasar verebileceğini gösteren en iyi örnektir.[92]

Siber ortamı sadece bilgi ve kişisel verilerin çalınabileceği bir ortam olarak görmemek gerekmektedir. İnternet ortamının bilgi çarpıtma için uygun bir ortam olması ve erişim kolaylığı sayesinde bilgiler çarpıtılarak insanlar yanıltılmaktadır. Bu da propaganda aracı olarak kullanılmasına imkân sağlamaktadır.[93]

2.5. Siber Güvenliği Tehdit Eden Araçlar

2.5.1. Virüsler

Virüs genel olarak sanal alemdeki zararlı yazılımlar olarak bilinmektedir. Fakat bu bilgi yanlış bir bilgidir. Her zararlı yazılım bir virüs değildir. Bununla birlikte virüs diğer dosyalara bulaşarak yayılan özel bir zararlı yazılımdır. Bu genellemeden yola çıkarak, bilgisayar virüsü, belleğe yerleşen, çalıştırabilen kendini ekleyen, yerleştiği programların yapısını değiştiren ve kendi kendini çoğaltabilen kötü amaçlı programlardır.[94] Tanımdan da anlaşılacağı gibi her zararlı yazılım bir virüs olarak tanımlanamaz, virüslerin en belirgin özellikleri kendilerini temiz yazılımlara bağlayarak bilgisayar ağları içerisinde kendi kendilerine yayılan programlar olmalarıdır.

2.5.2. Truva Atları

Faydalı bir yazılım gibi görünen aslında içeriğinde gizli ve güvenlik mekanizmalarını aşabilecek özelliklere sahip kodlar bulunan belli şartlar oluştuğunda

---

[92] *Dünyadan Örneklerle Siber Güvenlik Stratejileri ve Siber Uzay*, Türkiye Cumhuriyeti İç İşleri Bakanlığı, İç Güvenlik Stratejileri Dairesi Başkanlığı, Ankara 2020, s. 25.

[93] Kerim Emre Karabacak, "Terör Örgütlerinin Siber Uzay Kullanımı: DEAŞ Örneği," *Erzincan Binali Yıldırım Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* 1, 2022, (ss. 51-64), s.56.

[94] Süleyman Sadi Seferoğlu, "Bilgisayar Virüsleri," online ders anlatısı-https://yunus.hacettepe.edu.tr/~sadi/dersler/ebb/ebb467-guz2000/hale-p.html, (Erişim tarihi: 02.03.2023).

aktifleşecek veya kullanıcının vermiş olduğu izni sabote edebilecek yapılardaki zararlı yazılımlardır.[95] Truva atlarının belirgin özelliği kendiliğinden bilgisayar ağlarına bulaşamamalarıdır. Bu yazılımlar kötü amaçlı kişiler tarafından kullanıcının kandırılması veya yanıltması sureti ile yararlı bir yazılım gibi gösterilerek indirme yöntemi ile bilgisayar veya bilgisayar ağlarına kurulur. Truva atları bilgisayar ağlarına yerleştiğinde uygun zaman veya beklenen bir kod talimatını beklerler. Kötü amaçlı yazılımcıların amaçları doğrultusunda bulundukları ağlarda açıklar oluşturarak bilgisayar ağlarının güvenliklerini etkisiz hale getirerek ağlara zarar verirler.

2.5.3. Kurtçuklar (Worms)

Virüslerde olduğu gibi kurtçuklarda zararlı birer yazılımdır. Kendilerini başka cihazlara ve programlara kopyalayarak yayılırlar ve truva atlarından ayrılan en büyük özellikleri truva atlarının güvenli bir yazılım görüntüsü altında bekleyerek belli şartlar sağlandığında veya belli programlar çalıştırıldığında ortaya çıkar. Fakat kurtçuklar kendilerini kopyalayarak veri akışı üzerinde yavaşlamalara hatta durmalara neden olabilirler. Kurtcuklar ortaya çıktığında henüz güvenlik yazılımları tarafından tanınmadığı için veri akışına ciddi zararlar verebilirler. Bu nedenden dolayı kurtçuklar truva atlarına göre daha tehlikeli bir zararlı yazılımdır. Kurtçuklar cihazların veri akış yerlerine yerleşirler buralardan gerçekleşen veri transferlerine kendilerini kopyalamak sureti ile çoğaltarak diğer cihazlara da erişim sağlar ve o cihazlara da bulaşırlar. Kurtçuklar taşıyıcı olarak herhangi bir programa gerek duymadıkları için sistemde deliklere yol açarak dağılım hızlarını arttırabilirler.[96] Kötü amaçlı kişiler tarafından veri açık yollarında yoğunluk oluşturularak verilen hizmetin aksamasına, siteye erişilememesine veya hedeften gerçekleştirilen işlemlerin gerçekleştirilememesine neden olabilir.

[95] Berqnet Blogu, "Truva atı (trojan) nedir? Nasıl bulaşır? Ne tür zararlara yol açabilir?," Son Güncelleme Tarihi: 25 Şubat 2021, https://berqnet.com/blog/truva-ati, (Erişim tarihi: 02.03.2023).

[96] Refik Samet, Ömer Aslan, *Kötü Amaçlı Yazılımlar ve Analizi*, Grafiker Yayınları, Ankara, 2018, (ss. 225-255), s.229.

2.5.4. Zombi Ordular (Botnetler)

Zombi bilgisayarlar zararlı yazılımların en tehlikeli ve kullanımı en kolay olanlarındandır. Bilgisayar sahibi olaydan habersizdir. Amaçlar doğrultusunda Truva atı gibi yazılımlarla gizli bir şekilde ele geçirilmiş olan bilgisayarlar. Uygun ortam ve şartlar oluştuktan sonra verilen bir komut ile hedef olarak belirlenen bir site veya ağa saldırıya yönlendirilirler. Aşırı yükleme ile karşılaşan site veya ağ ise hizmet veremez hale gelebilir. Bu tür saldırılar genellikle güvenlik duvarı zayıf olan bilgisayarlar kullanılarak gerçekleştirilmektedir. Botnet bilgisayarlar bir dosyanın görüntülenmesinde, bilgisayar içerisinde bulunan kişisel bilgilerin çalınmasında, çalınan bilgiler ile banka ve alışveriş sistemleri üzerinde alışveriş yapılması ve hatta propaganda aracı olarak kullanılmak gibi ciddi suçlarda kullanılabilmektedirler.[97] Botnetler işleyiş açısından bakıldığında birkaç zararlı yazılımın bir arada kullanılması sureti ile oluşmaktadır. Hedef zararsız gibi görünen bir veriyi indirmesi sonucunda ağına yüklenen bir Truva atı sayesinde oluşturulan açıklara gönderilen kodlar ile aktif hale getirilir. Aktif hale getirilen cihazlar kullanılmak sureti ile üçüncü hedeflere saldırı gerçekleştirilir. Hedef saptırmak ve saldırı sonrası kötü amaçlı kişinin gizlenmesini sağladığı için kurumsal saldırılarda tercih edilen yöntemlerdendir.

2.5.5. İstem Dışı Elektronik Postalar (SPAM)

İstenmeyen elektronik postalar isminden de anlaşılacağı üzerine, istenmediği halde bilgisayarımıza gelen postalardır. Bu postalar günümüzde internetin ciddi bir kısmını oluşturmaktadır. Bu postalar genellikle reklam ve tanıtım tarzı mesajlar oluşmaktadır. İlk başta zararsız gibi görünen bir postanın altında bulunan bir zararlı yazılım ile bilgisayarınız veya bilgisayar içerisinde bulunan kişisel bilgilerinin ele geçirilebilmektedir. Bu sistem genellikle posta yolu ile geldiği için zaman zaman gelmesini beklediğimiz önemli bazı postalarında gelmesini geciktirmekte veya gelmesini engellemektedir.[98] Son kullanıcının bir anlık dikkatsizliği sonucunda aslında

[97] Radhika Sarang, Dikkat: Zombi Lot Botnets, McAfee Blog. Son Güncelleme 06 Kasım 2018, https://www.mcafee.com/blogs/consumer/mobile-and-iot-security/zombie-iot-botnets/, (Erişim tarihi 02.03.2023).

[98] Şeref Sağıroğlu, *Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler*, Grafiker Yayınları, Ankara 2018, s. 20-45.

kendisine gelmesini beklediği bir mail, e-posta veya reklamın içeriğinde gizlenmiş bir veriyi kendi ağına eklemesi sonucunda oluşabilecek tehditlerdir.

2.5.6. Casus Yazılımlar (Spyware)

Bu tip yazılımlar klavye hareketlerini, şifreleri, banka hesap bilgilerini ve özel dosyaları takip edebilen yazılımlardır. Genellikle ücretsiz kullanım hakkı olan sistemler aracılığı ile taşınırlar ve kullanıcılar tarafından cihazlara yerleştirilirler. Piyasada genellikle çocuk takip veya eş takip programı gibi reklamlar ile satışı gerçekleştirilirler.[99] Casus yazılımlar sanal ortamda genellikle bedava olan ve kullanışlı programlar aracılığı ile bilgisayar ağlarına bulaşabilirler. Bu yazılımlar bulaştıkları ağlardaki kişilerin kişisel bilgilerini, şifrelerini, banka bilgilerini vb. verilerini ele geçirmek için kullanılan yazılımlardır. Yazılımların en önemli özelliği, hedef şahsın herhangi bir eylemden haberdar olmamasıdır. Casus yazılımlar bulaştığı ağlardaki klavye ve ekran akış verilerini takip ederek hedefin kullandığı verileri ele geçirir ve bu yöntemle hedefe zarar vermektedir. Casus yazılımların hedefe yerleştirildiğinde doğrudan bilgi akışı sağlamaya başlarlar.

2.5.7. Hizmet Dışı Bırakma (dDOS)

İsminden de anlaşılacağı gibi hizmet dışı bırakma bir sisteme gerçekleştirilen saldırı sonucunda sistemi hizmet veremez hale getirmektir. Basit bir örnekle anlatılmak istenirse; hedef olarak seçilen siteye gereksiz çok miktarda istek bildirimler gönderilir ve sitenin asıl görevi olan hizmetleri yerine getirememesi sağlanır. Bu saldırıların miktarındaki artış ile site üzerinde fiziki bir tahribat yaratarak sitenin hiçbir şekilde hizmet veremez hale gelmesi de sağlanabilir.[100] Bu saldırı hedeften bilgi almak veya onun verilerinin ele geçirmekten ziyade hedefin gerçekleştirdiği işlemleri gerçekleştiremez hale getirmeyi amaçlamaktadır. Ağ kapasitesinin üzerinde bir talep

[99] Tim Fisher, Jerry Leger, "12 Best Free Spyware Removal Tools (March 2023)," lifewire.com blog, Son Güncelleme 1 Mart 2023, https://www.lifewire.com/best-free-spyware-removal-4151293, (Erişim tarihi 02.03.2023).

[100] Ahsan Parwez, "WordPress DDos Saldırıları: Türleri ve Bu Saldırılara Karşı Korunma Konusunda Ayrıntılı Bir Kılavuz," Cloudways by Digital Ocean, Son Güncelleme: 19 Ağustos 2022, https://www.cloudways.com/blog/wordpress-ddos-attacks/, (Erişim tarihi: 02.03.2023)

veya bilgilendirme yönlendirmesi yapılarak ağ kapasitesinin dolması veya aşılması ile ağın kilitlenmesinin sağlanması amacı doğrultusunda gerçekleşen saldırılardır. Özellikle kontrol mekanizması gerektiren hizmet veren kuruluşlara yönelik gerçekleştirilen saldırılar olarak dikkat çekmektedir. Örneğin elektrik santralleri, PTT hizmetleri, su şebeke, bankacılık işlemleri, alışveriş siteleri gibi yerlere karşı gerçekleştirilen saldırılardır.

2.5.8. Şebeke Trafiğinin Dinlenmesi (Sniffing)

Bu yöntem iki bilgisayar arasındaki trafiğin ele geçirilerek dinlenmesi anlamına gelmektedir. Bir bilgisayardan çıkan verilerin hedef bilgisayara ulaşmadan önce ara bir bilgisayara alınarak incelenmesi ve daha sonra verilerin tekrardan bırakılması olarak tanımlanabilmektedir. Bu sistemin önüne geçmenin en iyi yolu uçtan uca şifreli mesajlaşma sistemlerinin kullanılmasıdır. Bu şifreleme verilerin ele geçirilmesini engellememekle birlikte ele geçirilen verilerin şifreli olmasından dolayı herhangi bir şey anlaşılamayacağı anlamına gelmektedir.[101] Günümüzde özellikle uluslararası ticaret gerçekleştiren küçük ölçekli işletmeler bu tür saldırılara maruz kalmaktadır. Kuruluşlar karşı taraftaki muhatabı ile iletişimini güvenliksiz bir şekilde mail hesabı üzerinden gerçekleştirmektedir. Maillerinin sniffing yöntemi ile üçüncü bir bilgisayara geldikten sonra gönderilmesinin sağlandığı ortamdır Taraflar arasındaki mail akışı üçüncü bir kişi tarafından düzenlenmektedir. Özellikle para gönderimi için gönderilen hesap bilgileri değiştirilerek taraflar arasında gerçekleşmesi gereken para transferlerinin üçüncü hesaplara aktarılarak ele geçirilmesi şeklinde kullanılmaktadır.

2.5.9. Yemleme (Phishing)

Bu kavram “oltalama” olarak da isimlendirilmektedir. Bu yöntem ile bir sitenin birebir kopyasının oluşturulur. Kullanıcıların oluşturulan sahte siteye bütün bilgileri ile giriş yapmalarının sağlanması gerekmektedir. Genellikle posta yolu ile veya bilgilerin güncellenmesi istemleri şeklinde gerçekleştirilmektedir. Hedef kişiler bilgilerini güncellediğini düşündükleri esnada aslında kendilerine ait olan özel bilgilerin

[101] Sniffing Nedir?, Cyber Security Blog, Son Güncelleme: 19 Temmuz 2017, https://karslanblog.wordpress.com/2017/07/19/sniffing-nedir/, (Erişim tarihi: 02.03.2023).

çalındığının farkında olmazlar. Bu yöntemden korunmanın en iyi yolu dikkatli olmak ve banka gibi kuruluşların bilgi güncellemesini posta yolu ile yapmayacağı gibi basit bilgilerin bilinmesinin gerekliliğidir.[102] Amacın bilgilerin ele geçirilmesi olan bu yöntemde, kişiler kendilerine ait bilgileri kendilerine gönderilen reklam linkleri, tanıtım mailleri üzerinden değil hizmet veren sitenin yasal sitesi üzerinden gerçekleştirmeleri halinde kendilerini bu saldırılardan koruyabilmektedirler.

2.5.10. Propaganda

Kuvvet ile yapılamayanın hile ile yapmak olarak tanımlanan beşinci kol faaliyetleridir.[103] Ucuz ve erişiminin kolay olması nedeniyle siber ortam propaganda aracı olarak kullanılmak için çok elverişlidir. Sadece birkaç tık ile herhangi bir Word veya PDF belgelere ulaşılabilmektedir. Bu kullanımlar genellikle çatışma ortamlarında veya terörizm temelli olabilmektedir. Örneğin Çeçenistan ve Irak savaşları bu tür propagandaya örnek olarak gösterilebilmektedir.

Yukarıda belirtilen saldırıların biri veya birkaçı kullanılarak şahısların, ülkenin veya ülkelerin herhangi bir yerinde bulunan herhangi bir yere saldırılar düzenlenebilmektedir. Sınır kavramının bulunmadığı sanal ortamda gerçekleşen saldırılar ışık hızındadır. Bu nedenle bu saldırılara en az saldırı hızında veya daha hızlı bir şekilde karşılık verilmesi gerekliliği doğmaktadır. Teknolojiyle birlikte artık hayati öneme sahip enerji kaynakları, ulaşım sistemleri, üretim yapılara bu tür saldırılara her zaman açık durumdadır. Bu nedenden dolayı bu kötü amaçlı saldırılara karşılık kişisel ve ulus olarak alınması gereken bazı basit gibi görünebilecek ama çok büyük önem arz edebilecek tedbirler söz konusudur.

[102] Mehmet Nesip Öğün, Adem Kaya, s.160

[103] Yakup Halit Bulut, *Büyük Dizayn Algı Savaşları*, Yeniyüzyıl Yayınları, İstanbul 2017, s.83.

3. SİBER GÜVENLİK STRATEJİLERİ

3.1. ABD'nin Siber Güvenlik Stratejileri

İnternet dünya üzerinde başlarda sadece askeri amaçla kullanılan bir araç olarak karşımıza çıkmaktadır. Özellikle ABD ve Sovyet Rusya arasında gecen Soğuk Savaş döneminde askeri alt yapı ve gizli haberleşmelerde sıkça kullanılmıştır. 1990 sonrası Sovyetler Birliği'nin dağılması ile hegemonik güç haline gelen ABD interneti sivilleştirmiştir. Burada internetin sivilleşmesi, ticarileşmesi ve küresel çapta yaygınlaşması, küresel hegemonyanın devamlılığı için önem arz etmektedir. 2000 yıllarına kadar rakipsiz bir şekilde geldiği siber uzay ortamında, özellikle 2000 yılından sonra Sovyet Rusya'nın mirasçısı konumunda bulunan Rusya Federasyonu askerî açıdan gelişme kaydetmesi ve siber uzay ortamını yeni bir güç ortamı olarak kabul etmesi ile yapmış olduğu gelişmelerin yanında, Çin kaynaklı tehditlerinde artması üzerine ABD siber güvenlik konusunda askeri ve istihbarı (beşinci kol faaliyetleri) kapsamında tedbirler alarak bir bizi direktif yayınlanmıştır.[104]

Temmuz 1995 yılında yayımlanan "13010 Nolu Başkanlık Direktifi" belgesi, ABD'nin siber güvenlik alanına yönelik hazırlanan ilk resmî belgesi olması açısından önemlidir. Mayıs 1997 tarihli "63 Nolu Başkanlık direktife (presidential directive-63) belgesi, ABD'nin kritik alt yapılarını belirten ilk resmî belgeye göre göre ABD'nin kritik alt yapıları olarak; "enformasyon, iletişim, enerji, bankacılık ve finans, ulaşım sektörleri ile içme suyu ve acil müdahale altyapısı, kamu sağlığı" olarak belirtilmiştir.[105]

Şubat 2003 tarihinde "The National Strategy to Securi Cyberpace" Siber Uzay'ın korunmasına yönelik ulusal strateji ABD'nin siber uzay kavramını tanımlayan, bu alandaki hedef ve planları ortaya koyan, ulusal siber uzayın nasıl korunacağına yönelik planları ortaya koyan, siber uzay tehditlerini ortaya koyan ilk resmi belgedir. "Cyberspace Policy Review" (Siber Uzay Politika Revizyonu) 2009 yılında başkan Obama tarafından yayınlanan belgede, ABD siber güvenlik sisteminde faaliyette bulunan kurum ve kuruluşların çok başlılığına dikkat çekilmiştir. Çok başlılığın

[104] Bkz: Ali Burak Darıcılı, "Demokrat Parti Hack Skandalı Bağlamında ABD ve RF'nin Siber Güvenlik Stratejilerinin Analizi," *Ulise: Uluslararası Çalışmalar Dergisi* 1/1, 2017, (ss. 1-24), s.5-7.

[105] Ali Burak Darıcılı, s. 6.

giderilmesi için tedbirler alınmış ve siber güvenlik sistematiğinin sadece bu kurumların birlikte ve eş güdümlü bir şekilde hareket etmesi ile sağlanabileceği belirtilmiştir.[106]

"International Strategy for Cyberspace: Prosperity, Security, and Openness In a Networked Word" (Siber Uzay İçin Uluslararası strateji: Ağlanmış Bir Dünya'da Refah, Güvenlik ve Açıklık), Obama tarafından ABD tarafından Dünya'ya bildirilen ABD'nin uluslararası düzeyde ülkenin siber uzay alanındaki amaç ve hedeflerini belirtildiği bir belge niteliğindedir. "National Security Strategy" (Ulusal Güvenlik Stratejisi), 2015 yılında yayımlanan bildirinin önemi ise ilk kez siber güvenlik kapsamının bildirilmiş olmasıdır. Burada tehdit algısı olarak Rusya Federasyonu'nun artan siber saldırı gücü ile Çin Halk Cumhuriyeti'nin gerçekleştirmiş olduğu, siber casusluk eylemleri gösterilmektedir. Bunun yanında müttefik ülkelere yönelik gerçekleştirilecek saldırılarda ABD'nin ülkelere destek vereceği bildirilmiştir. "The Departmant of Defence Cyber Strategy" (ABD Savunma Bakanlığı Siber Strateji Belgesi), belge ile ABD silahlı kuvvetlerine, ABD ağ teknoloji ve sistemleri ile gizli siber bilgilerini savunma, siber ataklara karşı ABD çıkarlarını koruma, askeri ve gizli siber operasyonları planlama ve bu tür operasyonlara rehberlik etme görevleri verilmiştir. Bu bildiri ile ABD kendisinin siber saldırı açısından da geliştirdiğini ve kendisine tehdit oluşturan unsurların gelişimlerini takip ederek gerekli olması halinde karşı tedbirleri alabileceğini bildirmiştir. Aynı şekilde kendisi ile müttefik olan ülkelere karşı gerçekleştirilen saldırılar karşısında da yönlendirici olarak hareket edebileceğini göstermiştir. 2009 tarihinde çıkartılan Cyberspace Policy review" (Siber Uzay Politika Revizyonu) bildirgesi ile ABD bünyesinde faaliyet gösteren ABD Savunma Bakanlığı (United States Depatment of Defense), ABD İç Güvenlik Bakanlığı (The Department of Homeland Security) ve ABD Gizli Servisi (FBI/CIA) bünyesinde birimler oluşturulmuştur. Bunların dışında görev verilen bazı kurumlar kendi yapılarını oluşturmuşlar ve federal yapının bir parçası olan eyalet yönetimleri de kendi siber ağ yapılarını oluşturma yetkisine kavuşmuşlardır.[107] ABD Savunma Bakanlığı siber güvenlik alanında en yetkili kurum olarak görünmektedir. Savunma bakanlığının bünyesinde bulunan STRATCOM bünyesinde kurulan CYBERCOM tarafından yürütülmektedir. Bu birim siber kaynaklar üzerinde tarama yaparak raporlarını askeri bilgisayarlara uygun hale getirmekle

[106] Ali Burak Darıcılı, s. 6.

[107] Ali Burak Darıcılı, s. 7.

görevlidir. Bu birim dahilinde "24 Hava Kuvvetleri, Ordu Siber Savaş Birimi, Donanma Siber Savaş Birimi, Deniz kuvvetleri Siber Savaş Birimi"[108] bulunmaktadır. Bu birimlerin yanı sıra ABD'de NSA bünyesinde, şifre kırma, kriptolama ve gizli haberleşme takip etmek için kurulan Ulusal Güvenlik Ajansı (National Security Agency/NSA), Savunma Bakanlığı bünyesinde, Kara, Deniz ve Hava Kuvvetleri bünyesinde her biri kendi sorumluluk alanında çalışan Birleşik Siber Merkezi (Joint Cyber Center/JCC).

ABD İç Güvenlik Bakanlığı (özellikle 11 Eylül terör saldırısından sonra kurulmuş ve terör ve terörizm olaylarını takip etmekle görevli bir kurumdur) kritik alt yapıları korumak, alt yapılarının verimliğini arttırmak, hükümetin iletişim ve operasyonel gücünün devamlılığına sağlamak, ulusal siber güvenlik şartlarını ilerletmekle görevlidir. ABD'ye yönelik siber saldırıların faillerinin yakalanması ve hukuki sürecin takibi içinde ABD Adalet Bakanlığı bünyesinde United States Deportment of Justice departmanı kurulmuştur. Burada gerçekleşen siber saldırıların kayıtlarının yapılması ile analiz sistemleri kullanılarak gelecekte gerçekleştirilebilecek saldırılara karşıda hazırlıklı olmanın yanında faillerin belirlenmesi ve belirlenen faillerin yargılanması usullerinin de takip edildiği görülmektedir.[109]

ABD istihbarat yapısı içerisinde de Başkanlık beyannameleri kapsamında kurulmuş örgütlenmeler vardır. Bunların en önemlisi ise Federal Araştırma Bürosu (FBI) bünyesinde oluşturulmuştur. FBI ABD'nin iç istihbarat ihtiyacını karşılamak ve diğer devletlerin ABD içerisinde gerçekleştirecekleri casusluk faaliyetlerini takip için kurulmuş bir örgüttür. Bu örgütün bünyesinde Siber Güvenlik kapsamında Siber Ulusal Güvenlik Bölümü (Cyber National Security Section/CNSS) ve Siber Suç Bölümü (Cyber Criminal Section/CCS) kurulmuştur.[110]

2000 yılların başında güç kazanan Rusya Federasyonu ve Çin Halk Cumhuriyeti'ni kendisi için bir tehdit olarak algılayarak özellikle bu iki ülkenin faaliyetlerine karşı kendisini ve müttefiklerini korumak için yatırımlar yapmıştır. Siber güvenlik alanlarında sadece kamu gücü ile yetinmeyerek özel sektör girişimleriyle

[108] Ali Burak Darıcılı, s. 8.

[109] Ali Burak Darıcılı, s. 9-10.

[110] Ali Burak Darıcılı, s.10.

birlikte hareket etmiş ve gelişmeler doğrultusunda yeni önlem ve tedbirler alarak karşı hamleler yapmak istemiştir. ABD Siber Güvenlik yapılanmasında sadece savunma tarafında kalmayarak siber uzay ortamının sağladığı imkânlar dahilinde karşı hamle, propaganda gibi silahları da kendi çıkarları doğrultusunda kullanmaktan çekinmemiştir.[111]

3.2. Rusya'nın Siber Güvenlik Stratejileri

Rusya Federasyonu; Soğuk Savaş sonrası SSCB'nin varisi olmasından dolayı siber alanda selefi olduğu bütün alt yapılara ve bilgi birikimini kendi bünyesinde tutmayı başarmıştır. Bu birikim neticesinde siber alanda hızlı bir ilerleme göstermiştir. Özellikle Sovyet Rusya sonrasında yaşadıkları uluslararası ortamda gerçekleşen olayların sonucu olarak hızlı ve kesin çözüm aramaları ve yıpranan otoritesini tekrar sağlamak için atılımlar yapmıştır. Özellikle Çeçenistan çatışmalarında Çeçenlerin kullandıkları haberleşme kanalları ile uluslararası alanda ciddi bir olumsuzluklar yaşamıştır.

Rusya Federasyonu özellikle 2000 yılı ile siber alana ciddi yatırımlar yapmaya başlamıştır. Bu yılda yayınlanan ve yürürlüğü giren doktrinler ile hızlı bir ilerleme kat etmiştir. 24 Ocak 2000 yılında Rusya Federasyonu Ulusal Güvenlik Konsepti, 9 Eylül 2000 yılında Rusya Federasyonu Enformasyon Güvenliği Doktrini, 12 Mayıs 2009 yılında Rusya Ulusal Güvenlik Stratejisi, 2011'de Bilgi Çağında Rus Silahlı Kuvvetleri'nin Faaliyetlerine İlişkin Kavramsal Görüşler, 27 Şubat 2013 tarihinde Valery Gerasimov tarafından yayınlanan Öngörüde Bilimin Değeri makalesi, Tchekinov ve Bogdanov tarafından yayınlanan Yeni Nesil Savaşın Doğası ve İçeriği[112] makalesi Rusya Federasyonu'nda siber alanda meydana gelen gelişmeleri yönlendiren doktrin ve makalelerdir.

Rusya Federasyonu Ulusal Güvenlik Konsepti'ne göre, Rusya Federasyonu ilk kez sanal uzay ortamının varlığının farkında olduğunu göstermektedir. Bu belge içerik olarak herhangi bir düzenleme içermemekle birlikte özellikle bilgi güvenliğinin Rusya Federasyonu tarafından önemini belirtmektedir. Belge içerik olarak;

[111] Ali Burak Darıcılı, s.10.

[112] Servet Habip Topçu, "Rusya Federasyonu'nun Siber Güvenlik Stratejisi: Kırım Örneği," *Uluslararası İlişkiler Çalışmaları Dergisi* 2/1, 2022, (ss. 19-35), s.22-25.

1) Ekonomik, politik, teknolojik, çevresel ve enformasyon faktörlerinin uluslararası alanda giderek daha fazla rol oynadığı,
2) Enformasyon güvenliği alanındaki gelişmelerin, Rusya'nın ulusal çıkarlarını oluşturan bir bütünün parçası olduğu;
3) Rusya'nın enformasyon alanındaki çıkarlarının, modern iletişim teknolojilerinin gelişiminde ve devletin enformasyon kaynaklarına izinsiz erişiminin engellenmesinde yattığını;
4) Enformasyon alanında, bilgi ve telekomünikasyon araçlarının normal işleyişinin bozulması, veri güvenliğinin sağlanamaması ve bu verilere izinsiz erişim gibi, Rus ulusal güvenliğine yönelik artan bir tehdidin var olduğu vurgulanmaktadır (Rusya Federasyonu Dışişleri Bakanlığı (MID) (2000)).[113]

Ülkeler, uluslararası alanda sahip oldukları güçleri doğrultusunda diğer ülkeleri kendi çıkarları ekseninde hareket ettirebilmektedirler. Yumuşak güç vekâlet savaşları kavramlarının temelinde elde edilen bilgilerin etki edilmek istenen mesaj kapsamı içerisinde yoğrularak hedef ülke grup veya topluluğa en hızlı şekilde ulaştırılmasıdır. Mesaj ulaştırıldıktan sonra bu mesajın kabul edilmesi için tekrarlanarak kabul görmesi sağlamalıdır. Günümüzde siber uzayın mesajın oluşturulması, hedefe ulaştırılması ve kabul görmesi için tekrarlanması aşamalarında kullanılışlı bir silah olduğu göz ardı edilemeyecek kadar net bir şekilde ortadadır. Rusya Federasyonu da bu önemi 24 Ocak 2000 yılında farkına varmış, alınabilecek tedbirler konusunda net bir çizgi belirtmese de Rusya Federasyonu Ulusal Güvenlik Konsepti belgesi ile bu alanın ne kadar önemli olduğunu belirterek, bunu bir ülke politikası haline getirmiştir. Belge bu yönü ile önem taşımaktadır.

9 Eylül 2000 yılında Rusya Federasyonu Enformasyon Güvenliği Doktrini; bu doktrin Rusya Federasyonu'nun güvenlik konusundaki yol haritasını, amaçlarını, konu hakkındaki resmi görüşleri ve prensiplerini içermektedir.[114] Keir Giles'e göre " *doktrin tamamen savunma amaçlıdır. Saldırıdan söz edilemez. Bilgilere bütüncül bir yaklaşım getiriyor gibi görünse de güvenlik, batılı güvenlik yaklaşımlarından farklı olarak birkaç kavramı listeler. En önemli farklılık, medyaya yönelik liberal olmayan bir tutumdur. Ne*

[113] Servet Habip Topçu, s.23

[114] Sergei A. Medvedev, "Offence-Defence Theory Analysis of Russian Cyber Capability," (Naval Post-Graduate School, Master Thesis), Monterey, California, 2015.

olursa olsun bir medya kuruluş özel veya devlete ait ise doktrin bunun kabul edilebilir olduğunu belirtir ve hükümetin Rusya yanlısı mesajlar vermesini şarttır."[115]

Doktrin uluslararası alanda artan enformasyon silahlanmasına dikkat çekmekte ve bu silahlanmamın önlenebilmesi için uluslararası toplumun enformasyon güvenliğini arttıracak bir yapıda hareket etmesi gerektiğini belirtmektedir. Doktrin genel olarak saldırgan bir yapıdan ziyade savunma amaçlı bir yapı oluşturmaktadır. İstihbarat ve elektronik haberleşme alanından bilgi, propaganda ve psikolojik operasyonlara karşı koyma yöntemlerinin ve araçlarının iyileştirilmesine yönelik görevleri öncelikli olarak belirtmemiştir. 12 Mayıs 2009 yılında "*Russia's National security Strategy to 2020*" (2020'ye Doğru Rusya Ulusal Güvenlik Stratejisi) doktrin hazırlanması, güvenlik konseyinin doğrudan gözetimi altında gerçekleştirilmiştir.[116] Güvenlik Konseyi personeli yanında Güvenlik Konseyine Bağlı bakanlıklar arasında bir çalışma gurubu oluşturuldu.[117] Çeşitli kollarının temsilcileri, hükümet personeli, cumhurbaşkanlığı personeli, Federal Bölgelerdeki başkanlıkların tam yetkili temsilcilerinin personelleri, Rusya Bilimler Akademisi'nin uzman toplulukları ve büyük işletmelerin temsilcilerinin katılımı ile oluşturulan bir çalışma grubu tarafından hazırlanmıştır.

Belge içeriğinde bilgi güvenliği (Siber Güvenlik) üzerine metinler şu şekildedir:

1) Sibernetik ve yüksek teknoloji alanında yaşadı faaliyetlerin gelişmesi, Rus ulusal güvenliği üzerinde olumsuz bir etkiye sahiptir.
2) Küresel enformasyon mücadelesinin artması, ülkelerin istikrarına, ekonomilerine, sosyal şartlarına ve kurumlarına yönelik tehditleri arttıracaktır.
3) Bilişim ve telekomünikasyon alanlarında teknolojik geri kalmışlığın giderilmesi; hükümet askeri yönetim sistemleri ve kilit öneme sahip sistemlere yönelik bilgi güvenliği teknolojilerinin geliştirilmesi ve ulusal enformasyon alt yapısının küresel bilgi ağlarıyla uyumlu hale getirilmesi gerekmektedir.
4) Kritik öneme sahip alt yapı ve yüksek riskli tesislerin bilgi ve telekomünikasyon güvenliğe ile kurumsal e bireysel enformasyon güvenliği düzeyini artırarak ve

[115] Keir Giles, *Russia's National Security Strategy to 2020,* NATO Defense College College e Defense de 1'OTAN- June 2009.

[116] Keir Giles, *Russia's National Security Strategy to 2020,* NATO Defense College College e Defense de 1'OTAN- June 2009.

[117] Servet Habip Topçu, s.24.

ulusal güvenlik sistemini için birleşik bilgi telekomünikasyon sistemi oluşturarak ulusal güvenliğe yönelik enformasyon tehditler önlenir.[118]

Belgenin hazırlanmasında geniş çaplı bir çalışma grubu oluşturulmuş olmasına rağmen içerik olarak bakıldığında dar kapsamlı bir belge olduğu görülmektedir. Bunun yanında küresel enformasyonun öneminin ve kritik öneme sahip tesislerin korunmasına yönelik olarak hazırlanmış bir doktrin olma özeliğini de göstermektedir. 2011 Yılında yayınlanan Bilgi Çağında Rus Silahlı Kuvvetleri'nin Faaliyetlerine İlişkin Kavramsal Görüşler; bildirinin özellik açısından bakıldığında ilk kez Rusya Federasyonu Silahlı Kuvvetlerinin siber uzay alınanda oluşan tehditler ve alınması gereken tedbirler konusunda söz hakkı olduğunu bildirmesi nedeniyle önemlidir.[119]

27 Şubat 2013 tarihinde Valery Gerasimov tarafından yayınlanan Öngörüde Bilimin Değeri; Rusya Genelkurmay Başkanlığı yapmış olan Valery Gerasimov'un yazdığı makale Rusya Federasyonu'nun yeni askeri yaklaşımlarını ortaya koymaktadır. Bu yaklaşıma göre;[120] Makale genelinde Rusya Federasyonu'nun bu zamana kadar yayınladığı belgelere nazaran daha saldırgan bir yapıda olması söz konusudur. Günümüz teknoloji ile konvansiyonel savaşta kullanılan unsurlardan ziyade siber uzayda kullanılan silahların daha etkili olduğu, özellikle enformasyon silahının etkin bir şeklide çatışmanın ilk başlarında veya çatışma başlamadan önce kullanılması gerektiği, bu silahın etkilerinden sonra ise askeri imkanların barışı ve düzeni sağlamak amacı ile gerçekleştirildiği kisvesi altında gerçekleştirilmesi gerektiği belirtilmiştir.

Ukrayna'da 2010 seçimleri ile iktidara gelen Yanukoviç'in uygulamış olduğu politikalar ekseninden Ukrayna yönünü Doğu'ya çevirmiştir. Batı yanlısı grupların Yanukoviç'in AB anlaşmasını imzalamayacağını açıklaması ile Kiev Meydanı'nda gerçekleştirdikleri barışçıl protestolar zaman içerisinde yasa dışı bir durum haline gelmiştir. Bu iktidarsız ortamda Rusya Federasyonu, Ukrayna'ya karı DDOS saldırıları

[118] Servet Habip Topçu, s.24-25.

[119] Russian Federation Armed Forces' Information Space Activities Concept, *Ministry of Defence of the Russian Federation*, https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle,(Erişim tarihi: 09.01.2023).

[120]Russian Federation Armed Forces' Information Space Activities Concept, *Ministry of Defence of the Russian Federation*, https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle,(Erişim tarihi: 09.01.2023)

gerçekleştirerek haberleşme altı yapısını ve Ukrayna kamu hizmetlerini kullanılamaz hale getirmiş veya hizmetleri yavaşlatmıştır.[121] Bir yandan da Kırımın ilhakını haklı çıkarmak için dezenformasyon çalışmaları gerçekleştirilmiştir. Uluslararası alanda ve haber portallarında "Kırım aslında Rus toprağıdır" "Kırım'daki Rus Nüfus tehdit altındadır" "Ukrayna Hükümeti ABD uydusu" gibi dezenformasyon çalışmaları ile işgale uygun zemin hazırlanmıştır. Bu çalışmaların sonucunda da Ukrayna da bir türlü oluşturulamayan siyasi otorite boşluğundan faydalanarak 16 Mart 2014 tarihinde yeşil adamların ablukası altında bulunan Kırım parlamentosunun kararı ile Rusya tarafından ilhak edilmiştir.[122]

3.3. Çin'in Siber Güvenlik Stratejileri

İnternet kullanıma açısından en fazla kullanıcısına sahip mobil hizmetler, ödeme sistemleri acısından dünyanın en büyük dijital pazarı olan Çin siber güvenliğini arttırmak istemektedir. İnternet kullanımı artış oranlarına bakıldığında 2010 yılında internet kullanıcısı sayısının 457 milyona, 2017 yılında 731 milyona ulaşmıştır.[123] Artan internet kullanımı ile paralel olarak internet ortamında işlenen suçlarda da ciddi oranda bir artış yaşanmıştır. Bu saldırılardan 350000 insanın etkilenmiştir.[124] Bu etkileşim sonucunda Çin siber güvenlik konusuna öncelik vermiştir.

Çin devleti olarak siber güvenlikteki öncelikli konular diğer uluslararası arenadaki güçlerle aynı kapsamda ele alınmıştır. Bunlar kritik altyapı fonksiyonlarının zarara uğratılması, internetin, bilginin ve her türlü sanan dosyanın toplum düzenine, ekonomik gelişmeye, mülkiyet hakkına, askeri yapıya zarar vermek amaçlı kullanımının önlenmesidir. Çin siber güvenlik politikasını daha çok ulusal çapta uluslararası alana

[121] Servet Hatip Topçu, s.29

[122] Mustafa Kemal Öztopal, "Önde Gelen Uluslararası Örgütlerin Kırım'ın Yasadışı İlhakına Tepkileri," *Uluslararası Suçlar ve Tarihi Dergisi* 19, 2018, (ss. 105-135), s.111.

[123]Steven Millward, "China Now has 731 million internet users, 95% Access from their pones-Techinasia," Access From Their Phones-techinasia.com Haber Bloğu, Son Güncelleme: 23 Ocak 2017, Https://www.techinasia.com/china-731-million-internet-users-end-2016, (Erişim tarihi: 03.03.2023).

[124] Volkan Göçoğlu, Mehmet Devrim Aydın, "Siber Güvenlik Politikası: ABD, Rusya ve Çin Üzerine Karşılaştırmalı Bir Analiz," *Güvenlik Bilimleri Dergisi* 2, 2019, (ss. 229-252), s.243.

kapalı bir şekilde yönlendirmektedir.[125] 1980 yıllar internetin ve ticarileşmenin gelişme gösterdiği dönemlerdir. Çin ilk resmî siber güvenlik belgesi olarak isimlendirilecek belgesi de 1986 yılında "Devlet Ekonomik Bilgi Yönetimi Lider Küçük Grup" yapıyla başlamıştır. Bunu 1999-2001 yılında "Devlet Bilişim Öncü Grubu" (SILG) kurulmuş, 2003 yılında bu grup alt grubu olarak "Devlet Ağı ve Bilgi Güvenliği Koordinasyon Küçük Grubu (SNISCSG)" faaliyete geçirilmiştir.[126] Daha sonra SNISCSG tarafından 2003 yılında "Belge 27" açıklandı. Bu belge aktif savuma stratejisine göre hazırlanmıştır.[127] Kapsam olarak bilgi teknolojileri alanında yerel teknolojiler geliştirilmesi, bu alanda çalışan veya hizmet verin kurumlar arasında koordinasyonunu sağlanması, sektörün bütçesinin arttırılarak desteklenmesi gerekliliği vurgulanmıştır.[128] Yapılan yatırımlarla birlikte istenen hedeflere ulaşılması akabinde kurum 2008 yılında tasfiye edilmiştir. Çin Danıştay Kurulu tarafından 2006-2020 yıllarını kapsayacak şekilde "Orta ve Uzun Vadede Bilim ve Teknolojinin Geliştirilmesi Ulusal Programı: 2006-2020"ın temel noktası bilişim sektörünün desteklenmesi, enerji kaynaklarının arttırılması, çevre teknolojilerinin geliştirilmesi, fikri hakların korunarak geliştirilmesi ile Çin'in rekabetçi yapısının desteklenmesidir. Buradan da anlaşılacağı üzerine Çin'in siber güvenlik alanında gerçekleştirmek istediği, başarıların milli ve yerli güç yazılım donanımla sağlanabileceği, üretin süreci boyunca ve geliştirilmesinde de devlet desteğinin gerekliğini stratejisi geliştirildiği söylenebilir. Çin kendi bilişim teknolojisini üreterek sektörde hegemonik durumda bulunan ülkelerin etkilerinden kurtulmak ve ulusal bağımsızlığını burada da sağlamak istemektedir. İnternet teknolojisinin olmadan siber güvenliğinin de sağlanamayacağı yönünde bir siyaset izlemektedir.[129]

---

[125] Volkan Göçoğlu, Mehmet Devrim Aydın, s.244.

[126] Ali Burak Darıcılı, Barış Özdal, "Çin Halk Cumhuriyeti'nin Siber Güvenlik Stratejilerinin Analizi," *Güvenlik Stratejileri Dergisi* 28, 2018, (ss. 1-35). s.3.

[127] Steven Millward, "China Now has 731 million internet users, 95% Access from their pones-TeArasınchinasia," Access From Their Phones-techinasia.com Haber Bloğu, Son Güncelleme: 23 Ocak 2017, https://www.techinasia.com/china-731-million-internet-users-end-2016, (Erişim tarihi: 03.03.2023).

[128]Özge Özdemir, "Siber Krizin Tarihçesi (ABD ve Çin Arasındaki Siber Mücadelenin Kilit Tarihleri", https://businessht.bloomberght.com/piyasalar/haber/1099882-siber-krizin-tarihcesi url uzantılı haber portalı, (görüntülenme tarihi 03.03.2023).

[129]Özge Özdemir, "Siber Krizin Tarihçesi (ABD ve Çin Arasındaki Siber Mücadelenin Kilit Tarihleri", https://businessht.bloomberght.com/piyasalar/haber/1099882-siber-krizin-tarihcesi url uzantılı haber portalı, (görüntülenme tarihi 03.03.2023).

2014 yılında "İnternet Güvenliği ve Bilişim için Merkezi Lider Küçük Grup" adıyla oluşturulan grubun amacı ise devlet kurumlara arasında internet kullanıcılı ve bilişim sektörlerinin geliştirilmesi amacıyla gerekli koordinasyonun ve ortak siyasi yapının oluşturulmasıdır. Bu grubun Çin başkanlığına bağlı olarak faaliyet göstermesi Çin tarafından siber güvenliğe verilen öneminde ayrıca bir göstergesidir. Çin başkanlığına bağlı olarak hareket etmesindeki temel amaç ise alınacak kararlar ve uygulanacak işlemlerden bürokratik engellerin üstesinden hızla gelinmesini amaçlamaktır.

26 Mayıs 2015 tarihinde ise Çin Savunma Bakanlığı tarafından Çin askeri stratejisi açıklanmıştır. Bilgi toplumunun hızlı gelişimi, bu yeni koşullara senkronize olacak yeni planlar oluşturulması gerekliğini, enformasyonun önemine değinilmiştir. Yerel yapıların bile bu değişimde önemli olduğu, savaş sistemleri, komuta yapısı, tüm askeri unsurların ağ yapısına entegre olduğu, siber operasyon veya saldırılara karşı tehdit altında oldukları belirtilerek gerekli önlemlerin alınarak her zaman hazır durumda bulunulması gerekliliği belirtilmiştir.[130]

Çin Siber Uzay İdaresi tarafından 27 Aralık 2016 tarihinde "Ulusal Siber Güvenlik Stratejisi" yayınlanmıştır. Bu belge özet olarak siber uzayın ülke güvenliği için yeni tehditler oluşturduğunu, bu alandan kaynaklanacak her türlü tehlikenin bertaraf edilmesi için Çin tarafından teknik, hukuki, bilimsel ve askeri tedbirlerin alınacağı, iç güvenliği tehdit eden her türlü casusluk ve müdahalelerin her ne suretle olursa olsun durdurulacağı ülkenin kritik olarak adlandırılan alt yapılarının korunması için gerekli önlemlerin alınacağı, Çin'in şeffaf açık rekabetçi bir ekonomiyi desteklediği yerel şirketlerin bilişim ve teknoloji sektörlerinin desteklenmesi gerekliğini bildirilmiştir.[131]

Uluslararası alanda iş birliği kapsamında ise Rusya Federasyonu ile aynı çizgide olduğu görülmekle birlikte kısaca; 1 Mart 2017 tarihinde Siber Uzay Belgesi ile siber uzay alanının askerileştirilmesine ve caydırıcılık olarak kullanılmasına karşı olduğu,

---

[130] Ali Burak Darıcılı, Barış Özdal, "Çin Halk Cumhuriyeti'nin Siber Güvenlik Stratejilerinin Analizi", *Güvenlik Stratejileri Dergisi,* 2014, (ss.1-35), s.15.

[131] Nurbane Keskin, "ABD-Çin Rekabetinin Siber Güvenlik Bağlamında Ortadoğu'ya Yayılması", Ufuk Üniversitesi Siyaset Bilimi ve Uluslararası İlişkiler Ana Bilim Dalı, Yüksek Lisans Tezi, Ankara 2022, s.56.

uluslararası güvenlik ve istikrarı zedeleyecek her türlü girişimlerin, siber uzay alanında devletler, kuruluşlar ve hatta bireyler tarafından oluşturulabileceğini, yönetimsel olarak denetlenmesi ve yönlendirilmesi gerektiğini, denetimin belirlenmesi için genel hukuk normlarının kabul edilmiş olan BM uygun bir dayanak olduğunu, uluslararası bilişim ve teknoloji şirketlerinin destekleneceğini, yabancı yatırımların destekleneceğine, kamu yararı ve ulusal güvenlik çerçevesinde yabancı yatırımcıların destekleneceğine tekelleşmenin engelleneceğine Çin'in çok taraflı bir yönetim şeklini benimsediği belirtilmiştir.[132] Burada çok taraflı bir yapı tarafından yönetilmesi Çin'in uzun zaman içerisinde gerçekleştirmek istediği ABD hegemonyasına karşı yapılan bir girişim olarak değerlendirilebilmektedir. Çin ile ABD arasında sürekli olarak karşılıklı güvensizlik üzerine kurulu ilişkiler görülmektedir. Bu çatışmacı ve fikir ayrılıkları ile süren ilişkiler siber uzay alanında da devam etmiştir. Çatışmaları ortandan kaldırmak veya en aza indirmek için iki ülke arasında 2013 yılında görüşmeler başlamıştır. Bu esnada ortaya çıkan Amerika Ulusal Güvenlik Ajansı çalışanı Edward Sanwden, Amerika Ulusal Güvenlik Ajansının Çin kuruluşları üzerinde faaliyetlerinin inanılmaz boyutları çıktığını ifşa etmiştir. Bunun üzerine Çin ABD'yi ikiyüzlülük ile suçlamıştır. Daha sonra görüşmeler 2014 yılında ABD'nin Çinli askerleri casusluk yapmak ile suçlaması ile görüşmeler sona ermiştir.[133]

ABD ile Çin arasında 25 Haziran 2015 yılında ise siber alanda düzenlenmesi gereken ahlak kurullarına yönelik görüşmeler yaptıklarını açıklamışlardır. ABD Dışişleri Bakanı John Kerry "ABD ve Çin, siber güvenlik alanında bir devletin nasıl tutum sergileyeceğine dair birlikte çalışmalı. Siber faaliyetler konusunda eylem kuralları oluşturmak adına Çin, birlikte çalışmayı kabul etti" açıklamasında bulunmuştur. Sonuç olarak ABD ve diğer ülkeler Çin'i teknolojik gelişmeleri neticesinde uluslararası bir güç ve tehlike olarak kabul etmişlerdir. Bunun yanı sıra Çin'de ABD'nin internet ve teknoloji alanında pazarın büyük çoğunluğunu elinde tutmasından dolayı ABD'nin siber güvenlik ortamında lehine bir ortamın varlığını ileri sürmektedir.[134]

[132]Nurbane Keskin, s.56.

[133] Özge Özdemir, "Siber Krizin Tarihçesi (ABD ve Çin Arasındaki Siber Mücadelenin Kilit Tarihleri", https://businessht.bloomberght.com/piyasalar/haber/1099882-siber-krizin-tarihcesi url uzantılı haber portalı, (görüntülenme tarihi 03.03.2023).

[134] Ali Burak Darıcılı, Barış Özdal, s.32.

3.4. İngiltere'nin Siber Güvenlik Stratejileri

Dünya genelinde siber uzaya bakış açısının ve bu alandan gelebilecek tehditlerin anlaşıldığı ve bir dönüm noktası olarak kabul edilebilecek 11 Eylül 2001 Terör Saldırıları sonucunda, birçok gelişmiş ülkede olduğu gibi İngiltere'de de Siber Uzayın önemi anlaşılmış ve bu alan üzerine yatırımlar başlamıştır. 7 Temmuz 2005 yılında geleneksel olarak kabul edilen savunma yöntemlerinin yanında siber uzay alanını da kapsayan gelişmeler yaşanmıştır.[135] Bu çalışmalar kapsamında 2010 yılı mayıs ayında "Stratejik Savunma ve Güvenlik Gözden Geçirmesi" (Strategic Defence and Security Review-SDSR) açıklanmıştır. Bu açıklamaların akabinde ise 2010 ekim ayı içerisinde "Belirsizlik Çağında Güçlü Britanya" isimli ulusal güvenlik stratejileri yayınlanmıştır.[136] Yayınlanan stratejilerden siber güvenlik riskleri ve siber savaş en öncelikli tehdit olarak algılanırken bunların yanında, terörizm, uluslararası askeri krizler, doğal afetler gibi tehditler göz önünde bulundurulmuştur. Siber güvenlik alanında gerçekleştirilecek tedbir ve önlemler için 2011 yılında Kasım ayında "Ulusal Siber Güvenlik Stratejisi yayınlanmıştır. Strateji 2012 ve 2015 yılları arasında İngiltere'nin siber güvenlik çerçevesinin oluşturmaktadır. İngiltere'de de diğer ülkelerde olduğu gibi siber güvenlik ve siber uzay alanında faaliyet göstermek ve bu alanlarda yapılan etkinlikleri düzenlemek amacı ile kurumlar oluşturulmuştur. Bu kurumlar 2009 yılında Siber Güvenlik Ofisi (The Office of Cyber Security) olarak kurulmuştur. Bu kuruluş daha sonra 2010 yılında Siber Güvenlik ve Bilgi Güvencesi Ofisi (The Office of Cyber Security and Information Assurance-OCSIA) olarak güncellenmiştir. Kurumun görev ve kapsamı ise İngiltere Güvenlik Bakanlığı ve Ulusal Güvenlik Konseyi'ne siber uzay ve siber ortamdaki politika öncelikleri hakkında yardımcı olmaktır. Başka bir ifade ile İngiltere'nin siber uzay ortamındaki bilgi güvenliği ve kapsamını oluşturmaktadır.[137]

Kurum bu faaliyetlerini yürütmek için Siber Güvenlik Ofisi (Cyber Security Operations Centre-OCS), İçişleri Bakanlığı (Home Office), Savunma Bakanlığı, İletişim Karargahı (Government Communications Headquarters-GCHQ), İletişim-Elektronik

[135] Murat Güngör, "Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma," (Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı, Yayınlanmamış Uzmanlık Tezi), Ankara 2015, s.88.

[136]Murat Güngör, s.88.

[137] Murat Güngör, s.90.

Güvenlik Grubu (Communications-Electronics Security Group-CESG), Ulusal Altyapıları Koruma Merkezi (Centre fort he protection of national Infrastructure-CPNI), İş, Yenileşim ve Beceriler Bakanlığı (Department for Business,Innovation and Skills-BIS)[138] gibi İngiltere devlet yönetimini doğrudan ilgilendiren diğer bakanlıklar ile iş birliği yaparak iletişim halinde bulunmaktadır.

İngiltere 2016 yılında Ulusal Siber Güvenlik Stratejilerini yayınlamıştır. Bununla birlikte bütçeden ayrılan 1,9 Milyar dolarlık ödenek ile hazırlanan yeni Ulusal Siber Güvenlik Merkezi ile siber alanda savunmada olduğu kadar saldırıda da aktif bir duruma gelmeyi amaçlamaktadır.[139]

2022 yılında açıklanan Siber Strateji belgesinde savunma stratejilerinin yanında, saldırgan operasyonel bir yapının hedeflendiği görülmektedir.[140] Bu kapsamda 2020 yılında tamamlanan Ulusal Siber Güç ile siber savunmanın yanında, siber saldırı ve operasyon gücüde artırılmıştır. Oluşturulan alt yapı çalışmaları sayesinde terörle mücadele, kritik alt yapıların korunması, endüstri-sanayi temsilcileriyle stratejik ortaklık, müttefik devletlerle işbirliği gibi geniş bir açılım gerçekleştirmiştir.

NCF (Ulusal Siber Güç) ile birlikte İngiltere gelişen İngiltere Silahlı Kuvvetleri ve İstihbarat Servisleri ile siber tehditleri belirleme ve tehditleri yok etme kabiliyetine kavuşmuştur. Bu kapsamda NCF hem dış istihbarat MI6 hem de GCHQ istihbarat karışımı bir yapıya sahip olmuştur. Bu kapsamda siber olaylara karşı gerçekleştirilecek savunma eylemlerinde Savunma Bakanlığı, saldırı eylemlerinde ise GCHQ yetkili kılınmıştır. 2022 yılında gerçekleştirilen güncellemeler ile birlikte NCF'nin kapsamı genişlemiştir.[141] Yeni tanımlanan siber güvenlik kavramları ile birlikte İngiltere

[138] Murat Güngör, s.89.

[139] Gordon Carrera, "İngiltere'de Siber Güvenlik Merkezi Açıldı," *BBCNEWS Türkçe*, Son Güncelleme: 14 Şubat 2017, https://www.bbc.com/turkce/haberler-dunya-38967467, (Erişim tarihi:11.01.2023).

[140] Ersin Çahmutoğlu, "ABD'deki USCYBERCOM muadili olarak görünen İngiltere'nin NCF birimi Türkiye İçin Model olabilir mi?," *Linkedin Haber Blogu*, Son Güncelleme: 22 Aralık 2021, https://tr.linkedin.com/pulse/abddeki-uscybercom-muadili-olarak-g%C3%B6r%C3%BClen-ingilterenin-ncf-birimi, (Erişim tarihi: 11.01.2023).

[141] Gordon Carrera, "İngiltere'de Siber Güvenlik Merkezi Açıldı," *BBCNEWS Türkçe*, Son Güncelleme: 14 Şubat 2017, https://www.bbc.com/turkce/haberler-dunya-38967467, (Erişim tarihi:11.01.2023).

Güvenlik ve Sınırlardan sorumlu devlet bakanı tarafından yapılan bir açıklama ile Rusya, Çin, İran ve Kuzey Kore'nin "düşman ülkeler"[142] olduğunu açıklamıştır.

3.5. İsrail'in Siber Güvenlik Stratejileri

İsrail bulunduğu coğrafya açısından bakıldığında belki de en riskli ülkeler arasında yer almaktadır. İsrail siber uzay alanında bu kadar gelişmiş ve gelişmenin yanında bu teknoloji ihraç etme kabiliyetine sahip ender ülkelerden biridir. Buna rağmen İsrail'de resmi herhangi bir siber güvenlik uygulamaları bulunmamaktadır. Buna rağmen İsrail bünyesinde bulunan 200'den fazla şirket ve araştırma geliştirme girişimleri ile ABD'den sonra en çok siber ürün ihraç eden ülkedir.[143] İsrail'in siber güvenlik alanındaki başarılarının sırrı kamu ve özel sektörün başarılı bir şekilde uyum sağlaması ve bu uyumun mühendislik bilgilerinin ülkenin girişimci ruhu ile desteklenmesinden gelmektedir.[144] Bu teoriye en iyi destekleyen cümle ise CyberArk'ın CEO'su Udi Mokady tarafından söylenmiştir. *"Herkes İsviçre saatlerini İsviçre'den, bilgi güvenliğini ise İsrail'den almanızı anlar."* İfadesinden şirketlerin kendilerine ne derece güvendiği ve dışardan da artan talebin doğruluğunu ifade etmeye çalışmıştır.

Siber güvenlik alanında elde edilen başarıda kamu özel sentezindeki uyumun yanında, bu uyumu destekleyen hükümetlerin cömert desteklerinin yanında askeri yapısının da siber güvenlik sektörü arasındaki iletişim ve bilgi paylaşımlarıdır. İsrail'in oluşturduğu bu kamu özel sentezinin başarısının, hükümetler ve askeri yapılar tarafından desteklenmesinin yanında aynı zamanda ülkenin sahip olduğu girişimcilik ruhu ile birleşmesi, siber güvenlik üzerine oluşan pazarda da ciddi söz sahibi olmalarını sağlamıştır. Özellikle siber güvenlik konusunda online sistemler üzerinde

[142] İngiltere Siber Düşmanlarını Açıkladı-Yeni Türkiye'nin Düşünce Merkezi, *Yeni Şafak Gazetesi,* Son Güncelleme: 28 Aralık 2021, https://www.sde.org.tr/dunya/ingiltere-siber-dusmanlarini-acikladi-haberi-25166, (Erişim tarihi: 11.01.2023).

[143] Siber Güvenlik Ulusu: İsrail Ağı Korumada Nasıl Dünya Lideri oldu, Cybersecuritycover Haber Blogu, https://itrade.gov.il/turkiye/siber-guvenlik-ulusu-israil-agi-korumada-nasil-dunya-lideri-oldu/, (Erişim tarihi: 11.01.2023).

[144] Engin Savçın, Devletlerin Siber Güvenlik Politikalarının Şekillendirilmesi Sürecinde Kamu –Özel Sektör İşbirliğinin Artan Önemi; İsrail ve Yeni Zelanda Örnekleri, (Yalova Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi), Yalova 2020, s.63.

yoğunlaşmaktadır. Mobil cihazların yaygınlaşması ve online sistemlerin kullanılması ile siber ihlal konusunda her bir birey doğrudan hedef durumuna düşebilecektir.[145]

İsrail Milli Eğitim Bakanlığı lise ve ortaokul çağındaki çocuklardan siber güvenlik konusunda eğitim görmek isteyenler için okul sonrası programlar düzenleyerek eğitimler vermektedir.[146] Bu eğitimler tamamen gönüllülük ve isteğe bağlı olarak gerçekleşmektedir. İsrail Savunma Kuvvetlerinde (IDF) 18 yaşında askerlik zorunluluğunun bulunması ve askere giden herkesin mühendis olmasının değerini idrak ediyor olması bu gönüllük ortamının desteklenmesine katkı sağlamaktadır.[147]

İsrail siber güvenliğini diğer güvenlik yapılarından ayıran en temel özelliklerinden biri de hackerlerin hatalarını ortaya çıkarma eğitimleri sayesinde, tüm kötü amaçlı hazırlanmış yazılımların %94 önceden tespit ederek öngörücü bir siber güvenlik sağlamaktadırlar.[148] Günümüzde büyük şirketlerin hemen hepsi internet ortamında hizmet vermektedirler. Bu anlık internet ortamında gerçekleştirilen işlemler için en tehlikeli olan ise siber saldırılardır. İşte bu saldırılar daha hazırlık aşamasında iken israilli güvenlik şirketleri CyberX, ThetaRay, Aorato, Reversing Labs ve Seculert gibi siber güvenlik firmaları sofistike gerçekleşecek saldırıları tespit etmek için anomali-algılama yazılımlarına sahiptirler.[149] Bunun yanında Votiro gibi firmalar ise şüpheli aktiviteleri otomatik olarak silerek sisteme zarar vermesini engeller veya en az zarar ile saldırının savuşturulmasına sağlamaktadır ki bu esnada Hexadite isimli yazılım, anlık olarak müşteriyi konu hakkında bilgilendirirken saldırıyı da incelemektedir.[150]

---

[145] Engin Savçın, s.63.

[146]Cybersecuritycover," Siber Güvenlik Ulusu: İsrail Ağı Korumada Nasıl Dünya Lideri oldu," https://itrade.gov.il/turkiye/siber-guvenlik-ulusu-israil-agi-korumada-nasil-dunya-lideri-oldu/ URL uzantılı sayfa (görüntüleme tarihi 11.01.2023)

[147] Yasemen Özfındık Kotik, "Uluslararası İlişkilerde Siber Güvenlik Algısı ve Ulus Devletin Değişim Stratejisi," (Çukurova Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi), Adana 2015, s.66.

[148] Yasemen ÖzfındıkKotik, s.9.

[149] Cybersecuritycover," Siber Güvenlik Ulusu: İsrail Ağı Korumada Nasıl Dünya Lideri oldu," https://itrade.gov.il/turkiye/siber-guvenlik-ulusu-israil-agi-korumada-nasil-dunya-lideri-oldu/ URL uzantılı sayfa (görüntüleme tarihi 11.01.2023).

[150] Cybersecuritycover," Siber Güvenlik Ulusu: İsrail Ağı Korumada Nasıl Dünya Lideri oldu," https://itrade.gov.il/turkiye/siber-guvenlik-ulusu-israil-agi-korumada-nasil-dunya-lideri-oldu/ URL uzantılı sayfa (görüntüleme tarihi 11.01.2023).

İsrail'de resmi bir siber güvenlik yasası veya eylem planı bulunmamakta birlikte, önceliğin veri ve bilgisayarların korunması olarak belirlenen bazı düzenleyici işlemlerde gerçekleştirilmiştir. Bunlar;1995 yılında çıkartılına "Bilgisayar Yasası" siber suç ile sivil mücadele etmenin alt yapısını oluşturmuştur.[151] 1998 yılında ise "Kamu Güvenliğini Sağlama Yasası" bilgisayarları ve alt yapı hizmetlerinin güvenliği için çıkarılmıştır. En kapsamlı plan ise 11 Aralık 2002 tarihinde hazırlanan "Ulusal Sivil Siber Savunma Planı"dır.[152] 2011 Mayıs ayında İsrail Ulusal Siber Girişimi yayınlanmıştır. Bu yayının amacı siber güvenlik ile ilgili AR-GE merkezleri kurmak, ulusal siber güvenlik ağ yapısını geliştirmek, yenilikleri takip ederek, acil durumlar ile başa çıkabilecek kabiliyete hazır olmaktır. Bunların yanında özel sektör, akademik yapılar ve ordunun birlikte çalışması için gerekli olan uyum ortamını hazırlamak, AR-GE çalışmalarını takip etmek ve AR-GE ürünlerinin ihracatını sağlayarak kontrol altında tutmaktır.[153] İsrail siber uzay alanını askeri ve ekonomik bir alan olarak görmektedir. Yerli yazılımlar geliştirerek, geliştirilen bu yazılımların ihracatı sayesinde ekonomik bir katkı sağlamaya çalışmaktadır. Özel sektör kamu sentezinde başarının, desteklenmesi ve girişimci yapının yönlendirmesi ile özel şirketlerin ürettikleri her ürünün ihracından aynı zamanda İsrail devleti ekonomik ve askeri hedeflerine ulaşmasına katkı sağlamaktadır.

3.6. İran'ın Siber Güvenlik Stratejileri

İran'da diğer ülkeler gibi siber uzay ve siber güvenlik alanında tedbirler alan ve düzenlemeler oluşturan, siber alanda söz sahibi ülkelerden birindir. Özellikle ABD ve İsrail merkezi siber saldırılara maruz kalmakta olması da kendisinin siber güvenlik alanında geliştirmek zorunda olduğunu bir göstergesidir. İran, ABD ve İsrail tarafından ortak hedef olarak gözetilen ve düşman ülke olarak tanımlanabilecek bir ülke durumundadır. Özellikle ülkenin kritik alt yapılarına yönelik siber saldırılar gerçekleştirilmektedir. Ülkenin Orta Doğu'da bölgesel bir güç olması ve nükleer gücü

[151] Oğuz Turhan, "Bilgisayar Ağları ile İlgili Suçlar (Siber Suçlar), Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Planlama Uzmanlığı Tezi, 2006, s.131.

[152]Yasemen Özfındık Kotik, s.65.

[153] Yasemen Özfındık Kotik, s.65.

sahip olmasının yanı sıra bu gücü geliştirme konusunda çalışmalarına devam etmesi de ülkenin ayrıca siber saldırılara hedef olmasının nedenleri arasındadır.[154]

İran'ın siber alanda kedisini geliştirme çabalarının dönüm noktası olarak, ABD ve İsrail'in ortak bir saldırısı olduğu değerlendirilen, İran'a ait Natanz Nükleer Tesisine karşı düzenlenmiş olan Stuxnet Operasyonu'dur. Bu operasyon 2005 yılına yapımına başlanan Natanz Nükleer santraline 2007yılında sızdırılan Stuxnet yazılımının 2010 yılında tespit edilmesi ile anlaşılabilmiştir. Yazılım bir USB bellek tarafından Hollandalı bir casus aracılığı ile santrale yüklenmiş ve yüklenme işleminden sonra kendisini santraldeki ağ yapısına gizleyerek çalışmasına başlamıştır. Tespiti için gecen üç yıllık süre içerisinde santral dahilinde sabotaj eylemlerine devam etmiştir. Bu saldırı ile İran'ın nükleer çalışmalarının 30 yıl geriye aksatıldığı değerlendirilmektedir.[155] İran, bu saldırıdan sonra siber güvenlik alanında çalışmalarına hızlandırmıştır. Bu kapsamda İran hem defansif hem de ofansif olarak kendisini siber alanda geliştirmiştir. Defansif olarak kurulan yapılar genellikle devlet yapısı içerisinde kurulmakla birlikte, ofansif olarak oluşturulan yapılar ise devlet destekli ve devlete bağlı faaliyet gösteren gruplar şeklinde oluşturulmuştur.[156] Oluşturulan yapılan kurumsal olarak incelendiklerinde, defansif olanlar; Siber Uzay Yüksek Konseyi, Ulusal Pasif Sivil Savunma Teşkilatı, Siber Savunma Komutanlığı, DMO Elektronik Harp ve Siber Savunma Örgütü (JANGAL), Besic Siber Örgütü, İstihbarat ve Güvenlik Bakanlığı (MOIS), Siber Polis (FATA), Siber Olaylara Müdahale Timi (MAHER)'dir. Ofansif olanlar ise; Ira Hackers Sabotage (IHS), Ashiyane Security Group, Cutting Sword of Justice (CSJ), Qassam Cyber Fighters (QCF), Ajax Security Team (Flying Kitten), Mabna, Rana ve Nars Enstitüleri, APT Grupları ve Diğer Aktörler[157] olarak bilinmektedirler. Siber Uzay Konsey 2012 yılında Hamenei'nin direktifi ile kurulmuştur. Konseyin görevi Cumhurbaşkanı başkanlığında ulusal siber güvenlik ve bilgi güvenliği alanlarında politikalar oluşturmak ve kurumlar arasında koordinasyonu sağlamak ile görevlidir. İran Silahlı Kuvvetleri bünyesinde kurulmuş olan bu teşkilatın görevi, İran'ın kritik öneme sahip alt yapılarını devlet veya devlet dışı saldırılara karşı korumaktır. Siber Savunma Komutanlığı Ulusal

[154] Ersin Çahmutoğlu, *İran'ın Siber Gücü*, İRAM Yayınları, Ankara 2021, s.13.

[155] Ersin Çahmutoğlu, s.4.

[156] Ersin Çahmutoğlu, s.8-11.

[157] Ersin Çahmutoğlu, s.14-28.

Pasif Sivil Savunma Teşkilatı altında kurulmuş bir yapıdır. İran'ın ulusal siber savunmasından sorumlu bir kuruluştur. 2010 yılında gerçekleşen Stuxnet saldırısı sonrasında pasif sivil savunma teşkilatının önerisi ile kurulmuştur. Kuruluş ulusal siber savunma kuruluşu olmakla birlikte gerek görülmesi halinde ofansif eylemlerde gerçekleştirebilecek ofansif altyapıya sahip bir kuruluştur. DMO Elektronik Harp ve Siber Savunma Örgütü (JANGAL) hakkında resmi olarak herhangi bir bilgi bulunmamakla birlikte, elektronik harp ve siber savunma örgütünün DMO bünyesinde harp kapsamında operasyonel faaliyetler yürüten bir örgüt olduğun değerlendirilmektedir. Besic Siber Örgütü DMO bünyesinde kurulduğu ve siber güvenlik örgütlerinden farklı olarak İnternet operasyonları tabanlı bir örgüttür. Bünyesinde oluşturduğu birimler sayesinde eğitim, dijital içerik, sosyal medya mühendisliği gibi alanlarda faaliyet yürüttüğü değerlendirilmektedir. İstihbarat ve Güvenlik Bakanlığı (MOIS) İran'ın resmî istihbarat bakanlığıdır. Dış istihbarat operasyonları, dezenformasyon ve propaganda faaliyetlerinden sorumludurlar. 2011 yılında kurulan Siber Polis, 2009 yılında başlayan "Yeşil Harekât" sonrasında kurulmuştur. Siber suçların takibi ile görevli olan siber polis siber uzay ortamında meydana gelen kimlik/veri hırsızlığı, siber zorbalık, bilgi operasyonları gibi suçların takibini yapmaktadır. Siber Olaylara Müdahale Timi (MAHER) siber alanında uzman akademik veya teknik uzmanlığı bulunan kişilerin kullanıldığı bir gruptur. Ulusal siber alanının 7/24 esasına göre takip ederek analizler yapmak olası operasyonları tespit ederek müdahale etmek devlet ve özel irtibatına sağlayarak eğitimler yaparak açıkların ve aksaklıkların tespiti için tatbikatların yapıldığı birimdir.[158]Siber olaylara karşı oluşturulan devlet destekli birimler ise genellikle hacker olarak tanımlanan aktivistlerden oluşmaktadır. Bunların yanı sıra İran haker Sabotaj Grubu (IHS), Aşiyan Güvenlik Grubu, hakkında pek fazla bir bulunmayan Cutting Sword of Jusice (CSJ), Qassam Syper Fights, Mabna, Rana ve Nasr Enstitüsüler, devlet içinde APT Grupları (Devlet içerisinde görev yapan personellerden veya bağımsız olarak devlet tarafından dolaylı yoldan desteklenen grupların genel adlarına kısaca APT denilmektedir) ve diğer aktörler yer almaktadır. 2011 yılından bu zamana kadar İran'ın en aktif siber saldırılar düzenlediği grubudur. Siber casusluktan, finansal yapılara, kritik alt yapılara yönelik

[158] Ersin Çahmutoğlu, s.14-17.

saldırılar düzenlemektedir.[159] İran destekli bütün APT grupları aynı Rusya ve Çin'de olduğu gibi tamamen devlet desteklidirler. Hedefleri arasında da çoğunlukla, ABD, İsrail, Suudi Arabistan ve Türkiye'ye ait kritik altyapılar, enerji santralleri, kamu kurumları, telekomünikasyon ve bankacılık kuruluşları bulunmaktadır.[160]

Bilgiler geneline bakıldığında İran ABD, İsrail ve Suudi Arabistan başta olmak üzeri pek çok ülke tarafından aktif bir şekilde ambargoya tabi tutulmaktadır. Buna karşılık kendi içinde milli imkanlar ile oluşturmuş olduğu teknolojiler ve yazılımlar sayesinde siber güvenlik alanında hem defansif hem de ofansif olarak iki taraflı hareket edebilme kabiliyetine sahiptir. Defansif tarafı tamamen devlet kurum ve kuruluşları tarafından gerçekleştirilirken, ofansif tarafında ise doğrudan devlet kurumlarının bulunmadığı fakat devlet veya kurumları tarafından desteklenen bağımsız kuruluşlar ve aktivist grupların kullanıldığı görülmektedir. Araştırmanın başında belirtiler vekâlet savaşları kavramına uygun bir hareket tarzını oluşturmaktadır.

3.7. NATO

İkinci Dünya Savaşı'ndan sonra Sovyetler Birliği devasa bir alanı ve kalabalık nüfusu himayesine alması[161] sonrasında, ABD tarafından SSCB'nin yayılmacı politikasını önlemek için bazı önlemler alınması sonucunda; ABD öncülüğünde 12 devletin bir araya gelerek 1949 yılında NATO (Kuzey Atlantik Anlaşması Örgütü) kurulmuştur.[162] Türkiye 1952 yılında NATO'ya Yunanistan ile birlikte üye olmuştur.[163] NATO şu anda dünya üzerinde 30 devletin üyesi olduğu ortak bir askeri savunma birliği olarak yer almaktadır.[164] NATO'nun politik ve askeri iki temel noktası vardır. Politik temel nokta; NATO demokratik değerleri destekleyerek, üyelerine sorunları çözmede

[159] Ersin Çahmutoğlu, s.19-20.

[160]APT nedir?, Infinitumit.com Haber Bloğu, Son Güncelleme: 8 Aralık 2022, https://www.infinitumit.com.tr/apt-nedir/#:- (Erişim tarihi: 12.01.2023).

[161] Özge Güleç, Zülfükar Aytaç Kişman, "Uluslararası İlişkiler Açısından Siber Güvenlik ve NATO'nun Siber Güvenlik Stratejileri," *Akademik Açı* 1/1, 2021, (ss. 127-154). s.138

[162] Fırat Purtaş, "Soğuk Savaş Sonrası NATO'nun Dönüşümü ve Genişlemesi Çerçevesinde Türk Amerikan Askeri İlişkileri," *Güvenlik Stratejileri Dergisi* 1/2, 2005 (ss. 7-31). s.8.

[163] Fırat Purtaş, s.11.

[164] NATO Nedir?, https://www.nato.int/nato-welcome/index_tr.html, (Erişim tarihi: 13.01.2023).

güven oluşturmak ve uzun vadede çatışmayı önlemek için savunma ve güvenlik ile ilgili danışma ve iş birliği sunmaktadır.[165]

Askeri temel nokta; NATO öncelikli olarak oluşan ihtilafları barışçı yöntemler ile çözmeyi kendisine görev olarak kabul etmiştir. Diplomatik yollarla yapılan barışçıl çözümlerin yeterli olmaması halinde ise, kriz yönetimi altında askeri operasyon yapma yeteneğine sahip bir topluluktur.[166] Bu operasyonlar NATO'nun kuruluş antlaşmasının 5. Maddesi dayanak olarak alınarak gerçekleştirilmektedir. "*Madde 5: Taraflar, Avrupa ve Kuzey Amerika'da bir veya daha fazlasına yönelik silahlı saldırının hepsine yönelik bir saldırı olarak kabul edileceğini kabul ederler ve sonuç olarak, böyle bir silahlı saldırı meydana gelirse, her birinin bireysel haklarını kullanarak veya Birleşmiş Milletler Şartı'nın '51. maddesi tarafından tanınan toplu meşru müdafaa, bu şekilde saldırıya uğrayan Tarafa veya Taraflara, silahlı kuvvet kullanımı da dahil olmak üzere gerekli gördüğü şekilde, bireysel olarak ve diğer Taraflarla uyum içinde derhal harekete geçerek yardımcı olacaktır. Kuzey Atlantik bölgesinin güvenliğini yeniden sağlamak ve sürdürmek için kuvvet Bu tür bir silahlı saldırı ve bunun sonucunda alınan tüm önlemler derhal Güvenlik Konseyi'ne bildirilecektir. Bu önlemler, Güvenlik Konseyi uluslararası barış ve güvenliği sağlamak ve korumak için gerekli önlemleri aldığında sona erecektir.''*[167]Madde 5 anlaşıldığı kadarı ile BM Madde 51 gereği saldırıya uğrayan ülkenin meşru müdafaa hakkını kullanmasındaki durumunun saldırıya uğrayan devlet tarafından bireysel veya birleşmiş milletler olarak gerçekleştirilebileceği ifade edilmiştir.

BM madde 51 *''Bu antlaşmanın hiçbir hükmü, Birleşmiş Milletler Üyelerinden birinin silahlı bir saldırıya hedef olması halinde, Güvenlik Konseyi uluslararası barış ve güvenliğin korunması için gerekli önlemleri alıncaya dek, bu üyenin doğal olan bireysel veya ortak müdafaa hakkına halel getirmez. Üyelerin bu meşru müdafaa hakkını kullanırken aldıkları önlemler derhal Güvenlik Konseyi'ne bildirilir ve Konsey'in iş bu Antlaşma gereğince uluslararası barış ve güvenliğin korunması yada yeniden kurulması*

[165] Özge Güleç, Zülfükar Aytaç Kişman, s.139.

[166] Özge Güleç, Zülfükar Aytaç Kişman, s.139.

[167] Kamuran Reçber, "NATO Kurucu Andlaşması 5. Maddesinin Saldırı Fiii Acısından Analizi",*The Journal of Diplomatic Research- Diploması Araştırmaları Derğisi,* 2020, s.1.

için gerekli göreceği biçimde her an hareket etme yetki ve görevini hiçbir biçimde etkilemez."[168]

NATO üye ülkeler ile her gün çeşitli seviyelerdeki tehditler ve sorunlar karşısında istişarelerde bulunmakta ve kararlar almaktadırlar. Bu kararlar oy birliği kuralı çerçevesinde 30 üye ülkenin oy birliği ile karar vermesi sonucunda alınmaktadır.[169] NATO üye ülkeler ile iş birliği ve paylaşım içerisinde olduğu kadar gerekli olması halinde üyesi olmayan ülkeler ile de iş birliği ve istişarelerde bulunabilmektedir.

NATO bir güvenlik koalisyonun olmasından dolayı üyelerinin güvenliğini sağlamak için farklı alanlarda görüşmeler yapmakta ve yapılan görüşmeler ve incelemeler sonucunda da gerek gördüğü güvenlik tedbirlerini almaktadır. Özellikle 1994 yılında Çeçenistan Rusya savaşında Çeçenistan tarafından internetin kullanılması ve bütün imkanlar ile kullanılması ilk bilgi savaşı olarak anılmaktadır. 1999 yılında Kosova'da meydana gelen güvenlik zafiyeti sonrasında Sırp Hacker gruplarının NATO savaş kabiliyetini zayıflatma çabaları sonrasındaki girişimleri NATO'nun siber alında tedbirler almaya zorlamıştır.[170] Bu saldırıların sonucunda, NATO "Siber Savunma Programı" açıklayarak uygulamaya koymuştur. Bunun akabinde de NATO'ya yönelik olabilecek saldırılara karşı, siber saldırıları tespit etmek, NATO ağlarının saldırılara karşı korunması, kullanıcılara bilgi ve yardım sağlanması için "NATO Bilgisayar Olaylarına Müdahale Birimi (NCIRC) kurulmuştur.

NATO'da özellikle 2008 yılında gerçekleştirilen Bükreş Zirvesi'nden sonra alınan kararlar siber alanda NATO'nun değişim sürecinin başlangıcı kabul edilebilir. Bu zirvede siber alan ile ilgili olarak aşağıdaki iki önemli karar alınmıştır;

1) Siber savunmayı koordine edebilmek adına, kabiliyetleri incelemek ve riskleri karşı uygun güvenlik sağlamak için NATO Siber Savunma Yönetimi Otoritesi'nin (CDMA) kurulmuştur.

---

[168] Ulaş Karadağ, "Birleşmiş Milletler Antlaşma'na Göre Meşru Müdafaa Hakkı," *İnönü Üniversitesi Hukuk Fakültesi Dergisi* 7/2, 2016, (ss. 171-186), s.175.

[169] Özge Güleç, Zülfükar Aytaç Kişman, s.140.

[170]Hakan Aksoy, "Siber Güvenlik Meselesinde Askeri Uzmanlaşma: NATO Örneği," *TUİÇ Akademi*, Son Güncelleme: 16 Mart 2021, https://www.tuicakademi.org/siber-guvenlik-meselesinde-askeri-uzmanlasma-nato-ornegi/, (Erişim tarihi: 16.01.2023).

2) NATO'nun birlikte çalışabilirliğini geliştirmek için, siber farkındalık, eğitim ve öğretim çabalarını geliştirmek gibi ana hedeflerle Kooperatif Siber Savunma Merkezi (CCD COE) oluşturulmuştur.[171]

2008 Bükreş zirvesi sonrasında 2010 yılında Lizbon zirvesinde NATO bilgisayar olaylarına müdahale birimleri tekrar revize edilmiştir. Siber savunma yeteneklerindeki boşluklar tespit edilmesi, diğer tehditler ile siber tehditlerin birlikte analiz edilmesi amacı ile NATO Uluslararası Personeli bünyesinde yeni güvenlik sorunları birimi oluşturulmuştur. 2014 yılında Savunma Politikası ve Planlaması Komitesi oluşturulmuş, komite siber savunma ve siyasi düzeyde rehberlik ve gözetim sağlamak için kurulmuştur. Aynı yıl Genişletilmiş NATO Siber Savunma Politikası ve Siber Savunma Eylem Planı kabul edilmiştir. Eylem planında siber alanındaki savunmanın topluluğun ortak savunması olduğu belirtilmiş ve siber saldırılar karşısında 5. Maddenin uygulanmasının istenebileceği belirtilmiştir. Siber savunma alanının bütün ortakların ağlarına yönelik genişletilmesi çalışmasında belki de ön önemli olan düzenleme, 2016 yılında Varşova Zirvesi'nde Siber Savunma Taahhüdünün devletler tarafından imzalanmasıdır. NATO aldığı tedbirler ile kara, deniz, hava ve uzay alanları dışında siber alanında güvenlik açısından önemini vurgulamıştır. Alınan tedbirlerle siber alanda askerileşme hız kazanmıştır.

Siber alanın sürekli olarak değişmesi ve farklılaşmasının yanında sınır kavramının bulunmamasından dolayı, NATO sürekli olarak kendisini güncellemekte ve üye ülkelere karşı gerçekleştirilen siber operasyonlar ve siber saldırıları analiz ederek siber savunma alanını geliştirerek güncellemektedir. Bunun yanında siber alada devlet yapılarının dışında bireysel ve kurumsal yapılarında tehdit ihtivası nedeniyle, NATO uluslararası alanda bilişim sektöründe kendisini kanıtlamış olan Microsoft, Google ve IBM, Uluslararası Standartlar Birliği, İnternet Mühendisliği birliği ile iş birliği kapsamında çalışmalar yürütmektedir.[172] NATO ülkelerinin katılım ile düzenlenen Uluslararası Siber İhtilaf Konferansları ve üçüncü olarak ise NATO üyesi ülkelerin tamamının katılımı ile düzenlenen siber alan tatbikatlarıdır.[173] Bunun yanında NATO

[171] Hakan Aksoy, 16 Mart 2021.

[172] Doğan Şafak Polat, s.145.

[173] Doğan Şafak Polat, s.146.

beşinci maddenin siber saldırılar kapsamında uygulanmasını da kabul etti, bu durum NATO üyesi herhangi bir ülkeye karşı gerçekleştirilecek siber saldırının NATO ülkelerine yapılmış olabileceğini kabul etmişlerdir.[174]

NATO 2011 yılında Gözden Geçirilmiş NATO Siber Savunma Politikasını kabul etmiştir. Bu politika kapsam olarak; NATO üyesi devletlerin koordinasyon temelli bir yaklaşım ile siber saldırılara karşılık verebilecek organizasyonlar geliştirmek için plan ve kapasite sağlamak, ayrıca tüm üye devletlerin güvenliğini sağlamak için siber politikalarını uyumlu hale getirmektir.[175] Bunun sonucunda NATO siber saldırılara karşı bir bütün halinde hareket edebilme kabiliyeti kazanmaktadır. Bu kapsam devamlılığın için 2012 yılında 58 milyon avroluk bir bütçe ayırmıştır. Ayrıca ortak istihbarat paylaşımı ve farkındalık yaratmak için bünyesi dahilinde siber tehdit farkındalık birimi oluşturulmuştur. 2014 yılında ise; her gün daha karmaşık ve yaygın bir hal alan siber saldırılara karşı, güçlendirilmiş siber savunma politikaları kabul edilmiştir. Politika kapsamında giderek karmaşıklaşan ve kendisini yenileyen saldırılara karşı ortaklar arasında diyalog ve koordinasyonun sürekli olarak en üst seviye bulundurulması gerekliği belirtilmiştir. Siber saldırılar alanında ortak bir hukuk kuralları bütünü olmadığı için üye ülkeler, kendi ülkelerindeki kurumların siber saldırılara karşı sürekli olarak desteklenmesinin ve güncellemelerin önemi belirtilmiştir. 2016 yılındaki zirvede ise kara, deniz, hava ve uzay alanları gibi alanların siber alanında bir alan olduğu tanımlanmıştır. Bu kapsamda yapılan düzenlemelerde ortak hukuk bağlamı olmadığı belirtilerek üyeler arasındaki koordinasyonun ve bilgi paylaşımının önemi belirtilmiş, ağ güvenliğinin sağlanması için ortak bir harekât ve koordinasyonun oluşturulması gerekliği vurgulanmıştır.2018 yılında Brüksel'deki zirvede müttefiklerin savunma kapasitesini geliştirmek için, Belçika'da bir Siber Operasyon Merkezi'nin kurulması kararlaştırılmış olup, merkezin 2023 yılında faaliyete geçeceği bildirilmiştir.[176]

Bu bilgiler genelinde bir değerlendirme yapmak gerekirse NATO siber güvenlik konusunda yaşanmışlıklardan kendisine ders çıkartarak gerekli adımları atmaktadır. Yapılan düzenlemelerin ortak noktası NATO'nun kuruluş amacı doğrultusunda

[174] "NATO Üyeleri Yeni Siber Savunma Politikasın Kabul Etti," Son Güncelleme: 16.06.2021, NATO üyeleri yeni siber savunma politikasını kabul etti (savunmatr.com), (Erişim tarihi: 16.01.2023).

[175] Doğan Şafak Polat, s.147.

[176] Doğan Şafak Polat, s. 144-149.

savunma odaklı olmakla birlikte ofansif yönünü de geliştirmektedir. Yapılacak operasyonların ve siber güvenlik tedbirlerini önündü bazı engellerde mevcuttur. En önemli olan engel, siber saldırı olaylarına karşı ortak bir hukuk düzeninin bulunmamasıdır. Bunun yanında üye ülkeler arasındaki görüş farklılıkları, alınan kararlara rağmen altyapılarını yeterli kadar hızlı bir şekilde geliştirilememesi, yeterli kadar maddi bütçenin sağlanamaması, üyelerin iç güvenlik tedirginlikleri nedeniyle bilgi paylaşımında tereddüt yaşamaları, üyelerin bir kısmın teknolojik olarak ileri seviyede olmaları ve bazı üyelerin teknoloji alanında geri kalmış olmaları ve teknolojik aktivitelerin sürekli olarak değişmesi gibi nedenlerde ile yeterli güvenlik sağlama konusunda sorunlar yaşanmaktadır. 5. Maddenin siber saldırılara karşı nasıl uygulanacağı konusunda netlik olmaması, siber saldırıların saldırı yerinin net olmaması bunun yanında ölçülülük ilkesinin sağlanmasındaki saldırının boyutu ve ölçülülük tanımının yapılamaz olması da NATO'nun siber alanda alacağı güvenlik politikalarında aksaklığa neden olmaktadır. Her ne kadar bünyesinde çok güçlü ülkeler olsa da siber alan gücünün en zayıf halkası kadar olacağı gerçeği de göz önündü bulundurularak hızlı bir şekilde adımlar atılmaya çalışmalar sürdürülmelidir.

3.8. Türkiye'nin Siber Güvenlik Stratejileri

Siber dünyada dDos saldırıları gibi saldırıları saymazsak gerçekleştirilen saldırılar genellikle hedef alınan ağın açık veya zayıf yanları tespit edilerek yapılmaktadır. Bu bağlamda savunmacı durumunda olan ülke veya grup saldırının tam olarak nereden ve nasıl geleceğini önceden kestirmek, hazırlık yapmak, karşılık vermek ve silahsızlandırmak için adete samanlıkta iğne arama tabirinin bizzat yaşanmasına benzer bir durum oluşturmaktadır. Bu durumda siber ortamda savunmada olmaktansa, saldırıda olmanın daha avantajlı bir yöntem olduğu kanaatini oluşturmaktadır.[177] Bu açıdan bakıldığında özellikle Türkiye'nin 2012 yılında gerçekleştirilen siber saldırılarda dünyada üçüncü sırada olduğu görülmektedir. Bu kavramların bu kadar net olmasına rağmen ulus devletler siber saldırılara karşı kendi imkanları dahilinde karşılık

[177] Salih Bıçakcı, F. Doruk Ergun, Mitat Çelikpala, "Türkiye'de Siber Güvenlik," Kadir Has Üniversitesi Uluslararası İlişkiler ve Sosyal Bilimler Yüksek Okulu-https://edam.org.tr/document/CyberNuclear/SiberKitapTR/edam_siber_guvenlik_b2.pdf, (Erişim tarihi: 20.01.2023).

verebilmekte ve o derecede güvenlik sağlayabilmektedirler. Bu durumda ülkelerdeki siber güvenlik anlayışının gelişmişliği o ülkedeki siber güvenlik önlemlerinin güvenilirliği ile aynı çizgide seyretmektedir.[178]

Türkiye'de siber alana yönelik ilk düzenlemeler iç hukuk kapsamında 6 Haziran 1991 yılında, 3756 Sayılı Türk Ceza Kanunu'nda yapılan değişiklik ile girmiştir. Bu değişiklik ile; kanunun 20 maddesine "Bilişim Alanında Suçlar" başlığı altında, bir bilgisayardan programların, verilerin veya diğer unsurların hukuku aykırı olarak ele geçirilmesi ve bu verilerin başkasına zarar verecek şekilde kullanılması, nakledilmesi veya çoğaltılması ile ceza unsuru haline gelmiştir.[179] Yapılan bu değişiklik ile Türkiye hukuk literatüründe ilk defa bilişim suçu olarak kabul edilen bir suç yazılı olarak girmiştir. Bu tarihten sonra 2003 yılı Dünya Bilgi Topluluğu Zirvesi (WSIS) takip edilmiştir. 2004 yılına gelindiğinde ise bilgi güvenliği için "Elektronik İmza Kanunu" ve sürekli artış gösteren bilişim suçlarının önüne geçmek için ise "Türk Ceza Kanunu" çıkartılmıştır.[180] 2004 yılında internetin mobil cihazlar aracılığı ile hizmete girmesi ve ulaşım kolaylığı kazanması bilinçsiz kullanım oranını da arttırmıştır. Bu kullanım ağının bir anda genişlemesi de bilgi güvenliğinin ön plana çıkarmıştır. Bilgi güvenliği konusunda kullanıcıları bilinçlendirmek ve bilinçli bir yapı oluşturmak için 2007 yılında "Bilgi Güvenliği Derneği" (BGD) kurulmuştur.[181]

Bilgi Güvenliği Derneği'nin, koordinesinde Bilgi Teknolojileri İletişim Kurumu ve TÜBİTAK tarafından eğitimler, konferanslar, çalıştaylar düzenlenmiştir. Bunun yanında TÜBİTAK bünyesinde 'Siber Güvenlik Enstitüsü' TSK bünyesinde 'Siber Savunma Merkezi' kurulmuştur. Bu kapsamda yapılan çalışmalar neticesinde siber alanın önemi anlaşılması üzerine de Ulaştırma Denizcilik ve Haberleşme Bakanlığı tarafından yapılan çalışmalarda, Bilgi Güvenliği Derneği'nin de katkıları ile 'Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin

[178] Noelle Kneel, "Siber Saldırıların Kaynaklandığı İlk 10 Ülke," Government Blog, Son Güncelleme: 23 Nisan 2013, https://www.govtech.com/security/hacking-top-ten.html, (Erişim tarihi: 20.01.2023).

[179] 765 Sayılı Türk Ceza Kanunu'nun Bazı Maddelerini Değiştirilmesine Dair Kanun (TCK), *Resmi Gazete* 20901 (14 Haziran 1991), Kanun No. 3756.

[180] Mustafa Ünver, "Türkiye'de Siber Güvenlik," Academia.edu, https://www.academia.edu/24842186/T%C3%BCrkiyede_Siber_G%C3%BCvenlik , (Erişim tarihi 21.01.2023).

[181] Şeref Sağıroğlu, Mustafa Alkan, "Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık", Grafiker Yayınları, Aralık 2018, s.9.

Bakanlar Kurulu Kararı' 2012 yılında Cumhurbaşkanı Abdullah Gül'ün onayı ile Resmî Gazete'de yayınlanmıştır.[182] Bu yönetmeliğin amacı; *"kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda yer alan sistemlerin güvenliğinin sağlanmasına ve gizliliğinin korunmasına yönelik tedbirlerin alınması ve bilgi ve iletişim teknolojilerine ilişkin kritik altyapıların işletiminde yer alan gerçek ve tüzel kişilerce uyulması gerekli usu ve esasları düzenlemektedir."*[183] Siber Güvenlik konusunda çıkartılan ilk hukuki bir belge olması açısından önemlidir. Ulaştırma ve Denizcilik Bakanlığı'nın altına siber güvenlik olaylarını takip etmesi için "Siber Güvenlik Dairesi" BTK –TİB bünyesinde de Ulusal Siber Olaylara Müdahale Birimi olan (USOM) kurulmuştur. 2013 yılı içerisinde ayrıca *"Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"* yayınlanmıştır.[184] Bu eylem planı ile;

1. Kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin sağlanmasına,
2. Kamu ya da özel sektör tarafında işletilen kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanmasına,
3. Siber güvenlik eylemlerinin sonuçların en düşük düzeyde kalmasına, olayların ardından sistemlerin en kısa sürede normal çalışmalarına dönmesine yönelik stratejik siber güvenlik eylemlerinin belirlenmesine ve oluşan suçun adli makam ve kullukça daha etkin araştırılmasının ve soruşturulmasının sağlanması amaçlanmıştır.[185]

Bu amaçtan da anlaşıldığı üzerine bu yönetmeliğin temel kapsamı ise kamu bilişim sistemlerini ve kamu yada özel sektör tarafından işletilen kritik altyapıların bilişim alt yapısını kapsadığı görülmektedir.

[182] Bakanlar Kurulu Kararı (BKK), *Resmi Gazete* 28447 (20 Ekim 2012), Kanun No. 3842.

[183] Salih Bıçakcı, F. Doruk Ergun, Mitat Çelikpala, s. 257.

[184] Resmi Gazete- https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf URL uzantılı internet sitesi (Görüntüleme tarihi 23.01.2023).

[185] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, Ocak 2013, s.10.

USOM kapsamında; kritik alt yapıları işleten, kamu veya özel sektör kuruluşlarının siber saldırılara karşı korumak için Siber Olaylara Müdahale Birimleri (SOME) kurulması için 2013 yılında bir yönetmelik yayınlamıştır. SOME'ler bakanlıklar bünyesinde, hizmet gereklerine göre, bakanlık birimleri, bağlı, ilgili ve ilişkili kurumları kapsayacak şekilde kapsayıcı bir şekilde kurulurlar. Bakanlık dışında kalan kurumlarda kendi bünyelerinde SOME kurabilirler, kurumsal SOME'lerin eşgüdümü ulaştırma denizcilik haberleşme bakanlığı tarafından sağlanır, sektörel SOME'lerin kurulduğu kamu kurumları dışında kalan aynı sektörde faaliyet gösteren özel şirketlerde SOME kurabilirler.[186] SOME'lerin görevleri aşağıdaki gibidir;

1) Kurumlara doğrudan veya dolaylı yoldan gelen veya gelecek siber saldırılara karşı önlem alınmasına sağlamak, bu tür olaylara karşı müdahale edebilecek ve kayıt altına alabilecek mekanizmaya kurmak veya kurdurmak, kurumları bilgi güvenliği konularında çalışmalar yapmak veya yaptırmak,
2) Kurumlara yönelik siber saldırılara yönelik olarak kurumların bilişim sistemlerinin kurulması, işletilmesi ve geliştirilmesinde kuruluşlara öneride bulunmak,
3) Hizmet verdiği sektörde siber olayların önlenmesi veya sonuçlarının azaltılmasına yönelik yürüttüğü eylemleri hizmet SOME'si ile birlikte yürütmek ve durumun gecikmeksizin USOM'a bildirilmesini sağlamak,
4) SOME hizmet verdiği kuruma yönelik bir siber saldırı gerçeklemesi halinde bunu gecikmeksizin bağlı olduğu SOME ve USOM'a bildirmek ve öncelikli olarak saldırıyı kendi imkanları ile bertaraf etmeye çalışacak, yeterli olmaması halinde ise hizmet sektör SOME'si veya USOM'dan yardım isteyecektir,
5) Kurumsal SOME'ler siber saldırılar esnasında suç işlendiğine yönelik bir değerlendirmede bulunurlarsa gerekli inceleme için gecikmeksizin durumu kanuni makamlara bildireceklerdir,[187]

---

[186] Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ (SBOT), *Resmi Gazete* 28818 (11 Kasım 2013), Kanun No. 3842.

[187] Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkındaki Tebliğ, https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=19004&mevzuatTur=Teblig&mevzuatTertip=5#:~:text=Sekt%C3%B6rel%20SOME'lerin%20g%C3%B6rev%20ve,USOM'la%20koordineli%20%C5%9Fekilde%20y%C3%BCr%C3%BCt%C3%BCrler.&text=(2)%20Sekt%C3%B6rel%20SOME'ler,olaylar%C4%B1%20gecikmeksizin%20USOM'a%20bildirirler. Url Uzantılı Sayfa (Görüntüleme Tarihi 05.08.2023).

6) SOME'ler kurumlarına yönelik saldırıları hemen hizmet SOME'sine ve USOM'a bildireceklerdir,
7) Hizmet SOME'si yada USOM tarafından bildiriler siber olaylara müdahale edeceklerdir.
8) Kurumsa SOME'ler iletişim bilgilerini belirleyerek her daim ulaşılabilir bir şekilde hizmet SOME'sine ve USOM'a bildirmesi gerekmektedir.

Bu görevleri yerine getirirken SOME'ler doğrudan USOM'lar ile irtibatlı bir şekilde faaliyet gösterirler. Bunun yanında USOM ile SOME'ler arasındaki irtibat hizmet sektöründe faaliyet gösteren SOME tarafından sağlanır. Kurumsal SOME'lerin USOM'a doğduran irtibatı mevcut değildir.

Dünyada siber alanda güvenlik sağlamaya çalışan bütün devletlerin yapmış oluğu gibi Türkiye Cumhuriyeti'nde de bazı kanunu düzenlemeler yapılmıştır. Bu düzenlemeler başlık olarak şöyledir.

1) 2813 sayılı Bilgi Teknolojileri ve İletişim Kurumunun Kuruluşuna yönelik kanun,
2) 5809 Sayılı Elektronik Haberleşme Kanunu,
3) 5070 Sayılı Elektronik İmza Kanunu,
4) 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve bu yayınlar yoluyla işlenen suçların mücadele edilmesi hakkında kanun,
5) 6475 Sayılı Posta Hizmetleri Kanunu'nun 655 Sayılı Ulaştırma Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde kararname,
6) 6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun,
7) 6362 sayılı Sermaye Piyasası Kanunu 115. madde,
8) 5271 sayılı Ceza Muhakemesi Kanunu 5. Bölüm,
9) 6102 sayılı Türk Ticaret Kanunun 1525 inci maddesi[188] gibi maddeler yayınlanmıştır.

Bunların yanında siber suçlar ile ilgimi olarak TCK;

1) Bilişim sistemlerine girme sucu (TCK 243),

[188] Serkan Yenal, Naci Akdemir, "Uluslararası İlişkilerde Yeni Bir Kuvvet Çarpanı; Siber Savaşlar Üzerine Bir vaka Analizi", *ÇAKÜ Sosyal Bilimler Enstitüsü Dergisi*, (ss414-450), s. 427

2) Sistemleri engelleme, bozma, erişilmez kılma, verileri yok etme veya değiştirme suçu (TCK 244),
3) Banka ve kredi kartlarının kötüye kullanılması (TCK 245),
4) Yasak cihaz veya program kullanma suçu (TCK 245/a)[189]

Çıkartılan kanunlar, yapılan düzenlemeler ve yaptırımlara rağmen maalesef ki siber alanda eylemler durmamakta her gün kendisini güncelleyerek yenilenmektedir. Bu kapsamda, güncellemelerin ağ yapısına mümkün olan en az zararı vermesi amacı ile Savunma Sanayi Başkanlığı tarafından denetlenen, SSTEK-Savunma Sanayi Teknolojileri AŞ tarafından, Türkiye Siber Güvenlik Kümelenmesi projesi takip edilmektedir. Bu proje ile ulaşılmak istenen amaçlar;

1) Türkiye'deki siber güvenlik firmalarının sayısını arttırarak siber güvenlik alanından kalifiyeli, özel sektör temelli yapıyı genişletmek,
2) Siber güvenlik ekosistemini sağlayarak, üyelerin teknik idari ve finansman açısından desteklenmesini sağlamak,
3) Üyelerin markalaşmalarını destekleyerek, uluslararası alanda rekabet gücü kazandırmak,
4) Siber alanda en zayıf halka olan insan üzerinde siber güvenlik kavramını geliştirmek ve nitelikli gelişmiş insan kaynağını sağlamaktır.[190]

Bu ve benzeri projelerin hazırlanması ve geliştirilmesindeki temel nokta, siber alanda gereklilik olan teknolojik yazılımın geliştirilmesi, yerlilik ve dışa bağımlılıktan kurtulma çabasıdır. Her ne kadar ağlar ve bu ağların kurulu olduğu alanlar diğer yerlerden bağımsız olsalar da ağlarda kullanılan yazılımlar üzerinde bağımsızlık sağlanamaması halinde sürekli olarak güvenlik konusunda dışa bağımlılık devam edecektir.

Ülkeler ve NATO kapsamında bir genelleme gereksiniminde, ülkeler gelen olarak kendi çıkarları ve güvenlikleri doğrultusunda hareket etmeye önem vermektedirler. Bunu için kendi iç hukuklarında gerekli hukuki düzenlemeler yapmakta ve düzenlemeleri uygulamaya sokmaktadırlar. Bunun yanında ABD ve İsrail kendileri için düşman olarak belirledikleri ülkeler üzerinde etki kurmak istemekte veya bu

[189] Serkan Yenal, Naci Akdemir, s.428.

[190] Serkan Yenal, Naci Akdemir, s.428-429.

ülkelerin her zaman bir kontrol ağının içerişinde tutmak istemektedirler. Bunun için ara ara siber operasyonlar gerçekleştirmektedirler. Bunun yanında enformasyonu birinci tehdit olarak gören Rusya Federasyonu ve Çin Halk Cumhuriyeti tarafından bu alan bilgi ve istihbarat ağı olarak kullanılmaktadır. İngiltere özellikle bu alanın tehlikelerini terörizm üzerinden görmekte iken diğer ülkeler ise kendileri için tehdit oluşturacak ülkeler bazında bakmaktadırlar. Batılı ülkeler tarafından sürekli olarak ambargo altında tutulan İran ise adeta *"kötü komşu insanı ev sahibi yapar"* (anonim) cümlesi misali kendisinin zor durumda bırakılmak istendiğini fark ederek kendisini geliştirmekte ve bünyesinde oluşturmuş olduğu özel yapılar veya özel sektörde kurulmuş olan şahısların desteklenmesi ile siber alanda varlığını hissettirmektedir. Türkiye ise bu alanda sayılı diğer ülkelere göre biraz daha geç kalmakla birlikte geride değildir. Diğer ülkelerin geldikleri noktanın, geçmiş 20 yıllık sürece bağlı olduğu göz önüne alındığında Türkiye'nin yapılacak atılım ile siber alandaki yerini almasının önünde herhangi bir engel görünmemektedir.

Ülkelerin, birbirlerinden ayrışan bu yapılarına rağmen ortak noktaları da mevcuttur. Ülkeler Siber alanın sınırsız bir alan olmasından dolayı ortak bir yapı tarafından denetlenmesinin gerekliğini belirtmektedirler. Fakat bu durum yakın zamanda gerçekleşme ihtimali düşük bir yapı olarak görünmektedir. Çünkü uluslararası alanın ortak bir devlet düzeninin bulunmaması bu düzenlemenin önündeki en belirgin engeldir. Ülkeler kendi çıkarları için diğer ülkelerin açıklarını kullanmaktan veya etkilemekten çekinmemektedirler. Terörizme karşı ortak hareket etme ve siber alanın askerileştirilmemesi gibi orta tutumlarda bulunmakla birlikte güvensizlik ortamının hâkim olması siber alanın askerileştirilmesinin önündeki en büyük engel olmakta, vekalet savaşlarının bir gereği olan ülke içerisinde terör gruplarının kullanışlı birer argüman olması da diğer birliktelikleri engellemektedir. Girişimci bir yapı ile siber güvenlik alanını bir kazanç kapısı haline getirmiş olan ABD ve İsrail ise ürün pazarlamasının yapılması için uluslararası alanda bir birlik ve bütünlük oluşumunun önünde en büyük engellerden biridir. Zira siber alanda satış yapabilmek için risklerin varlığı önemlidir. Risklerin bulunmadığı bir ortamda, güvenlik önlemlerinin de herhangi bir önemi kalmayacaktır.

3.9. Siber Güvenliğin Milli Güvenlik Ekseninde Yorumlanması

Siber Güvenlik, aslında var olmayan ve sanal bir ortamda meydana gelen işlemler hakkında güvenlik olarak görünmektedir. Fakat günümüzde sanal ortamda kişiler, kurumlar ve ülkeler için hayati öneme sahip bilgiler ve veriler bulunmaktadır. Bu bilgilerin güvenliği ve korunması açısından bakıldığında üçüncü kişilerin eline geçmesi halinde telafisi mümkün olmayan sonuçlar doğurabilmektedir. Sanal ortamda saldırıları dört farklı şekilde ilişkilendirilebilir. Siber Savaş ve Ekonomik casusluk daha çok devletler ile ilişkilerde görülen bir tehdit iken siber suç ve siber terörizm gibi kavramlar daha çok devlet dışı aktörler tarafından yönetilen bir ilişkilendirmedir.

Milli güvenlik ekseninde siber güvenliğin sağlanabilmesi için, bütün yasal düzenlemelerin gerçekleştirilmiş ve uygulanmakta olduğu varsayıldığında; siber güvenliğin sağlanması için teknik ve operasyonel işlemlerin gerçekleştirilebildiği fiziki imkanları uygun bir merkez üzerinden, ulusal ve uluslar arası alanda stratejik planlamaların geliştirildiği, yönetildiği, değişen durumlar karşısında uygun yasal düzenlemelerin araştırıldığı, endüstri ve uluslar arası alan ile iyi ilişkilerin bulunduğu, uluslararası alanda ilişkilerin ve bilgi alışverişinin bulunduğu, uygulamaya yönelik kararların sunulabildiği idari bir yapı olarak tanımlanabilir.

Karşımıza siber güvenlik ile ilgili olarak siber güvenlik unsurları çıkmaktadır. Bu unsurlar, Gizlilik, Bütünlük, Kimlik Doğrulama ve inkâr edememedir.[191]

3.9.1. Gizlilik

Kelime anlamı olarak, herkes tarafından bilinmeyen açıklanmasının kişinin kişisel hak ve çıkarlarını zarar verme hali[192] olarak tanımlanmaktadır. Gerçek hayattaki anlamına yakın bir anlamda siber uzaydaki anlamı mevcuttur. Buna göre *"verilere sadece yetkisi olan kişiler tarafından erişiminin sağlanması, yetkisi olmayan kişiler tarafından erişiminin engellenmesidir."*[193] Buradaki asıl amaç verilerin herkes

[191] Şerif Sağıroğlu, Mustafa Alkan, *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*, Grafiker Yayınları, Ankara 2019, s. 302-305.

[192] Türk Dil Kurumu (TDK), "Gizlilik," https://sozluk.gov.tr/, (Erişim tarihi: 24.01.2023).

[193] Şerif Sağıroğlu, Mustafa Alkan, s.41.

tarafından erişilebilir olmasının önüne geçerek sadece yetkili kişilerin erişiminin sağlanmasıdır.

3.9.2. Bütünlük

Bütünlük, kelime anlamı olarak, eksiksiz, değiştirilmemiş anlamlarına gelmektedir. Siber alanda ise bu terim; *"verilerin işlenme şeklinin ve içeriğinin değiştirilmediğinden emin olunmasıdır."*[194] Verilerin bir ortamdan başka bir ortama gönderilmesi esnasında verilerin içeriğinde değişikliğe imkân verilmemesi, verinin ilk hali ile diğer ortamlarda da kullanılmasının sağlanabilmesidir.

3.9.3. Kimlik Doğrulama

Veriyi kullanan kişinin kim olduğu ve kişinin bu kullanımda yetkili kişi olduğunun tespit edilmesine imkân sağlayacak önlemler demektir.[195] Örnek; E-İmza (elektronik imza) sistemleri buna örnek olarak verilebilirler.

3.9.4. İnkâr Edememe

Veriyi gönderen kişinin tespitine imkân sağlanması, olası bir durumda veriyi gönderen-alan veya veriyi kullanan kişinin tespitine imkân sağlayan sistemleri bütün olarak ifade edilebilir.[196] Bu unsur açık anahtar alt yapısı veya zaman damgası ile sağlanır (Loğ kayıtlarının düzenli olarak tutulması).

3.9.5. Erişilebilirlik

Yetkili kullanıcılar tarafından veriye gerek görüldüğü zaman ulaşılabilmesi, veriye ulaşım imkanlarının sürekli olarak aktif halde olması anlamına gelmektedir.[197]

[194] Şerif Sağıroğlu, Mustafa Alkan, s.41.

[195] Şerif Sağıroğlu, Mustafa Alkan, s.41.

[196] Şerif Sağıroğlu, Mustafa Alkan, s.42.

[197] Şerif Sağıroğlu, Mustafa Alkan, s.42.

Yetkili kişilerin veriye ulaşmasının önünde herhangi bir engelin bulunmaması, yetki kimlik doğrulamasını gerçekleştirdiği esnada her an veriye ulaşılması olarak ifade edilmesidir. Veriye ulaşım üzerinde yetkili kişinin erişiminin engellenmemesi veya kısıtlamalar ile karşılaşmamasıdır.

3.10. Siber Güvenlik için Alınması Gereken Tedbirler

İnsan ve silah kullanımın az olması, maliyetinin düşüklüğü ile izinin sürdürülebilirliğin zor olması gibi etkenlerden dolayı siber saldırılar tercih nedenleridir. Siber güvenlik konusunda yetişmiş yeterli personel ve imkanların azlığı da bir etkendir. Bunların yanında ülkelerin güvenliklerini sağlamak için oluşturdukları kanunların yetersizliği, saldırılarından sınır kavramlarının olmaması, özel, kamu veya kurumsal olarak saldırıların yapılabilecek olması uluslararası alanda tam bir iletişim ve paylaşım yapısının bulunmaması da bu tür saldırıların seçilmesinde önemli bir etkendir.

Siber alanda kurum ve kuruluşlar, şahıs ve devletlere yönelik tehdit, güvenlik zafiyetleri arttıkça siber güvenlik hakkında bilinç ve gelişmelerde değişiklik göstermektedir. Siber tehdit alanlarındaki sınırların bulunmaması ise uluslar arası alandaki tedbirlerin önemi ortaya çıkartmakta ve uluslar arası ilişkilerdeki iletişimin önemini arttırmaktadır.

Devletler acısında bakıldığında; siber alında meydana gelen bir saldırıya karşılık olarak konvansiyonel bir karşılık verilmesi gerektiğini savunan bir düşünce yapısının bulunması yanında, aynı yöntem ve silahlar ile karşılık verilmesinin gerektiği düşüncesinin de varlığı görülmektedir. Bu da uluslararası alanda güç kullanımında orantılık ilkesinin önemini göstermektedir. Fakat siber alanda gerçekleşen saldırıların tam yerinin veya kim tarafından gerçekleştirildiğinin tespit edilmesinin mümkün olmaması da bu durum için bir handikap doğurmaktadır.

Özellikle ekonomik açıdan güçlü devletler bu tür saldırı ve tehditlere karşı ciddi manada önlem almaya çalışmaktadırlar. Fakat bu alanda gerçekleştirilen bütün yatırımlara rağmen her şeyin bir bütün veya başarı sağlama olasılığı da bulunmaktadır. Çünkü teknoloji gündelik yaşamımızda bir ilgi alanını olmaktan ziyade hayatı idamede bir zorunluluk haline gelmiştir. Her yeni gelişme de yanında yeni açıklar ve sorunlar doğurmaktadır.

Örneğin terörizme karşı olarak görünmekle birlikte, siber ortamda çeşitli imkanlar ile rakip firma veya ülkeler üzerinde baskı kurmak veya onları kendi çıkarları doğrultusunda hareket etmek zorunda bırakmak için kurum ve ülkeler bazında siber ortam propaganda aracı olarak kullanılmaktadır. Bu sayede hem terörizme karşılık durumu ortaya çıkmakta hem de izlerinin takip edilememesinden dolayı istenen baskının sağlanması mümkün olmaktadır.

Türkiye açısından Siber Güvenlik çalışmalarına bakıldığında ise son dönemlerde başta ülke olarak maruz kalınan siber saldırılardaki artış bu saldırıların önlenmesi ve karşılık verilmesi gerekliliğini ortaya çıkartmıştır. Bu açıdan geliştirilen bazı faaliyetler olarak; Siber Güvenlik Eylem Planları, Ulusal Bilgi Güvenliği Programı, Yasal Çalışmalar, Ulusal Bilgi Güvenliği Kapanı, Siber Güvenlik Müdahale Ekipleri ve Birimleri, Siber Güvenlik Tatbikatları, Konferanslar, Çalıştaylar ile Askeriye bünyesinde geliştirilen teşkilatlanmalar olarak söz edilebilmektedir.[198]

Bu çalışmalar kapsamında Siber alanda işlenen suçlara karşı TCK'ya 243 ve 244 maddeler olarak girilmiş olan 'Bilişim Alanında İşlenen Suçlar' maddeleri eklenmiş, kişisel verilerin korunması için 5651 sayılı 'İnternet ortamında Yapılan Yayınların Düzenlenmesi ve bu Yayınları Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun' ile 5070 sayılı Elektronik İmza Kanunu yer almaktadır.

Bunlara ek olarak TSK bünyesinde, TÜBİTAK ve UEKAE ile birlikte Bilişim Sistemleri Güvenliği bölümü kurulmuş ve bu birim ilk başka TSK bünyesinde faaliyet göstermeye başlamıştır. Buna ek olarak 2012 yılında TSK Siber Savunma Merkezi Başkanlığı kurulmuştur.

Ülke genelinde meydana gelebilecek saldırıların önlenmesi, muhtemel saldırı ve eylemlerin tespit edilmesi saldırıların etkinliğinin azaltılması veya tamamen yok edilmesi, oluşabilecek zararların en kısa zamanda telafisi için Bilgi Teknolojileri ve İletişim Kurumu bünyesinde 'Ulusal Siber Olaylara Müdahale Merkezi' (USOM, TR-CERT) 27 Mayıs 2013 tarihinde oluşturulmuştur. Başkanlık bünyesinde kurulan USOM ulusal ve uluslararası alanda siber ortamda oluşabilecek bir tehditler ile ilgili olarak yapılan ihbarları ilk değerlendirme birimi olarak çalışmakta, kurumlar arası iletişimi

[198] USOM Hakkında, Ulusal Siber Olaylara Müdahale Merkezi, https://www.usom.gov.tr/hakkimizda, (Erişim tarihi 03.03.2023).

sağlamakta ve tehdidin ortadan kaldırılması sırasındaki aşamaları takip ve koordinesini sağlamaktadır. Bunun yanında ulusal ve uluslararası alanda siber saldırılara karşı tatbikatlar gerçekleştirerek kurum ve kuruluşları siber saldırılara karşı bilinçlendirmekte ve halihazırda bulunan durumlarını test etmektedir.[199] Siber Güvenlik Kurulu toplantıları sonucunda kamu kurum ve kuruluşların kendi bünyeleri kapsamında siber saldırıları karşı Siber Olaylara Müdahale Ekipleri (SOME) oluşturulması kararlaştırılmıştır.

Etkin bir siber savunma sistemi için yapılması gereken bazı hazırlıklar vardır. Bu hazırlıklardan en son kısmı reaksiyon göstererek karşılık verilmesidir. Bunlardan önce yapılması gereken bazı tedbirler mevcuttur;

1) Yapılan saldırıları önlemek için saldırıları tespit ve koruma sistemi yaklaşımı gereklidir. Olası saldırı yerlerinin ve saldırganların tespiti, hedef ve hasar sonuç ilişkilerinin kurulmuş olduğu bir sistem oluşturulmalıdır,
2) Tehdidin tespiti için ağlar üzerinde veya donanımlarda kurulmuş vaziyette bir savunma sistemi kurulmalıdır,
3) Yapılan saldırıların, ne zaman, kim ve ne araçları ile yapıldığına yönelik yapılan tespitlerin ve saldırı şeklinin kayıt altına alınarak analiz edilmesini sağlayacak bir kayıt sisteminin oluşturulması gereklidir,
4) Son aşama olarak, saldırılara karşı koyma (tepki verme), yukarıda belirtilen sistemler kapsamında tespit edilen saldırılarını önleme, meydana gelen saldırı hasarlarının giderilerek sistemin en hızlı şekilde ve eksiksiz olarak tekrar eski haline getirilmesi aşamasıdır.[200]

Siber Güvenlik için gerekli adımlar kontrol edildiğinde genel olarak bilinen tepki verme eyleminin aslında sistemin en son aşaması olduğu görülmektedir. Anlık saldırılara tek başına yapılabilecek müdahalelerin geçici ve eksik bir tedbir olmasının yayında, her saldırı bir sonraki saldırının bir ön hazırlığı veya araştırması olduğu yaklaşımı unutmamalıdır. Bu nedenle siber güvenlik sistemleri oluşturulurken, gerçekleşmiş saldırıların kaydedilmesi ve analiz imkanlarının sağlanması, olası saldırıların tespitinin yapılmasında ve önlenmesinde hayatı bir öneme sahip olmaktadır.

[199] Ulusal Siber Olaylara Müdahale Merkezi (USOM), https://www.usom.gov.tr/hakkimizda URL Uzantılı Sayfa (Görüntülenme tarihi 05.08.2023).

[200] Sağıroğlu, Alkan, s. 41.

Hiçbir savunma yoktur ki saldırı öncesi tespit edilerek yapılan hazırlık ile başlamadan önünün kesilmesi kadar iyi bir savunmak değildir. Gerçekleşen her saldırı ağ ve veriler üzerinde etki bırakabilmektedir. Gerçekleşen bir saldırıdan sonra hasarın geri getirilmesindense, saldırı gerçekleşmeden önce önünün kesilmesi daha önemli bir aşamadır. Saldırıya mümkün olduğu kadar maruz kalınmamasını ön gören savunma stratejilerinin kurulması gerekmektedir.

Etkin bir siber güvenlik ağı kurulabilmesi için dikkat edilmesi gerekli olan hususlar vardır. Bu hususlar ise aşağıdaki özetlenebilir;

1) Kurulan ağlar için bir güvenlik politikasının oluşturulması ve oluşturulan politikaların uygulanması gereklidir.
2) Ağın veya verinin korunması için gerekli olan güvenlik tedbirlerinin alınması gereklidir. Bir ağın güvenliği için yeterli koruma prensibi kullanılmalıdır.
3) İyi bir risk analizi ve yönetim sisteminin kurulması gerekmektedir. Analizlerden çıkan sonuçların sürekli olarak güncellenmesi gereklidir. Bu sisteminde kontrolü için yönetim tarafından eksiklikler giderilmelidir.
4) Kurulan sistemde mevcut eksikliklerin tespiti için uzman kişi veya kuruluşlar ile anlaşılarak gerekli sızma testlerinin yapılması ve analizler sonucunda çıkan eksikliklerin hızla giderilmesi gereklidir.
5) Sistemi kullanan kişilerin mümkün olduğu kadar az yetki ile donatılması politikası güdülmelidir. Sistemde ne kadar az yetki dağıtımı yapılır ve yetkili kişiler tarafından kullanılırsa eksiz ve hataların önüne geçilmede başarı imkanları sağlanmış olacaktır.
6) Ulusal ve uluslararası alanda kabul görmüş siber güvenlik standartları takip edilmeli ve uygulanmalıdır. Bunun yanında standartların kabul etmiş olduğu sistemlerin dışındaki uygulamalarda takip edilmelidir. Kurulan sisteme yönelik tespit edilen bir aksaklık olması halinde giderilmesi için gerekli çalışmalar yapılmalıdır.
7) Ağın güvenliğinin sınırsız saldırılara açık olabileceği değerlendirilerek, ağ üzerinde işlenen verilerin anlık kaydının yapılması ve verinin yedeklenmesinin sağlanmasına imkân sağlayan yapılar oluşturulmalıdır.
8) Güvenlik ağlarının kurulum, kullanım ve kontrollerinde sürekli olarak güncellemeler gerçekleştiği için ağlardan sorumlu güvenlik uzmanlarının sayılarının arttırılması, fikir alışverişi ortamının sağlanarak sürekli olarak

sistemlerin güvenliğinin sağlanmasına yönelik yeterli miktarda yetişmiş insan kaynağının sağlanması için tedbirler alınmalı ağın genel güvenliği için uzmanlar kadar kullanıcılarında dikkat etmesi gereken hususlar konusunda eğitimler verilerek bilinçli kullanıcılar kazanılmalıdır. Tek bir kişi tarafından sağlanan güvenliğin tek düze bir güvenlik olacağı unutulmamalıdır.[201]

[201] Şerif Sağıroğlu, Mustafa Alkan, s,44.

SONUÇ

Güç, etki altına alma, himaye etme gibi kavramlar insanlığın varoluşundan bugüne kadar gelen kavramlardır. Farklı zaman ve durumlarda insanlar güç ve etki altında bulundurmaya farklı araçlar ile sağlamışlardır. Dünya savaşları sonrasında dünya üzerinde kurulan ulus üstü kuruluşlar, bu kuruluşların yayınladığı bildiriler ve dünya üzerinde bulunan pek çok ülkenin bu bildirileri kabul ederek yaptırımlarını kabul etmeleri, dünya üzerinde her ülkenin diğer ülkenin sınırlarını kabul etmesi ve dokunulmazlığına saygı göstermesi gerekliliğini doğurmuştur.

İnsanoğlunun doğasından gelen güce sahip olma ve hükmetme içgüdüsü, giderek artan insan ihtiyaçları ve kısıtlı kaynaklara sahip olmak istenmesi nedeniyle ülkeler kabul etmiş oldukları bildirilerin sınırlarını aşmadan güç kullanma ve etki yaratma çabası içerisine girmişlerdir. Bu durum karşımıza vekalet savaşlarını çıkarmaktadır.

Ülkeler, taraf oldukları antlaşmaları aşmadan, kendi çıkarları doğrultusunda diğer ülkeleri etkilemek ve şekillendirmek için güç kullanmayı farklılaştırmışlar. Bu durum vekâlet savaşlarının kullanımında bir artış sağlamıştır. Vekâlet savaşları çıkarlar doğrultusunda üçüncü ülke veya bağımsız gruplar aracılığı ile yönlendirilen güç mücadelelerinde, teknoloji en önde kullanılan bir silah olarak görünmektedir.

Teknolojik gelişmeler kapsamında iletişimin sınırsız bir şekilde ulaşılabilir olması, bilgiye erişim ve kullanım konusunda ışık hızının sağlanması ile aynı imkanların artık hayatın bir zorunluluğu haline girmesi teknolojinin vekalet savaşlarında kullanılan en önemli güç unsuru haline getirmiştir. Düşük maliyet ve izlerinin gizlenmesinin sağladığı avantajları güç kullanımında istenen bir ortam yaratmaktadır.

Zaman içerisinde kişiler, kurumlar ve ülkeler gerçekleştirilen siber saldırının etki ve sonuçlarından kendilerini korumak için siber güvenlik gereksinimi yaşamışlardır. Bu gereksinimin karşılanması içinde özel birimler, kanunlar çıkartılmıştır. Fakat siber saldırı ve tehditlere karşı ulusal çapta gerçekleştirilen çabalar yetersiz kalmaktadır. Bu nedenle uluslararası kuruluşlar ile olan iş birliğinin arttırılması gerekmektedir. Bunun yanında uluslararası ortam anarşik bir ortamdır. Ülkelerin karşılıklı yaşadıkları çıkar çatışmaları ve teknolojik olarak farklı gelişmişlikte olmaları, birbirleri üzerinde güç gösterisi yaparak etki yaratmaya çalışmaları onların birbirleri ile siber güvenlik alt yapısı konusunda paylaşım yapmalarının önünde engel teşkil etmektedir.

Her şeye rağmen siber güvenliğin temelinde insan unsuru bulunmaktadır. Siber saldırıların etkilerinin en aza indirilmesi veya etkilerinin en kısa zamanda en az maliyetle giderilmesi için öncelikli yapılması gereken bilinçli bir eğitim sisteminin organize edilmesidir. Kurumlarda çalışan personelleri son teknoloji güvenlik tedbirleri hakkında eğitmek artık bir zorunluluk haline gelmiştir. Bir personelin yaptığı bir hata yüzünden sahip olunan bütün ağ zarar görmekte ve hatta yok olmaktadır. Kurumsal olarak siber saldırı risklerine göre analizler yapılmalı ve bu analizler doğrultusunda planlar oluşturularak gerekli tedbirler alınmalıdır. Bununla yetinmeyerek olası bir saldırı durumunda uygulamaya konulabilecek yedek planlar bulunmalıdır. Siber güvenlikte en güçlü halka ile en zayıf halkanın insan unsuru olduğu unutulmamalıdır. Dolayısıyla, günümüz teknolojisinde, eğitim çok büyük bir öneme sahiptir. Devlet ve özel sektör karışımı yapılar ile ilköğretim çağındaki çocuklar, eğitim kurumlarında gözlemlenmelidir. Konusunda uzman kişi veya gruplar tarafından yapılan incelemelerde, yeteneği olan çocuklar tespit edilmelidir. Tespit edilen bu çocuklar siber ve teknolojik açıdan özel eğitimlere tabi tutulmalı veya gerekli yönlendirmeler yapılarak sadece günümüz değil gelecek nesiller için de siber güvenlik ve teknoloji uzmanları olarak yetişmelidirler. Bu tespitlerin yanında, ilköğretim aşamasından başlayarak gelecek nesillere siber uzay, siber saldırı ve siber güvenlik alanlarında bilinçlendirme eğitim ve kursları sürekli olarak güncellenerek verilmelidir.

Girişimcilik ruhu ile teknolojik alanda geliştirilen ürünler uygun şartlarda dünya pazarlarına açılmalıdır. Teknolojik alanda gerçekleştirilecek ar-ge çalışmaları ve teknoloji üretimi maliyetli bir yapıya sahip gibi görünebilmektedir. İlk başlarda devlet veya devlet destekli kurumlar tarafından alt yapı yatırımları gerçekleştirilmelidir. Daha sonra oluşturulan bu alt yapılar sürekli olarak güncellenmeli ve ar-ge ortamları devlet kontrolünde özel sektör rahatlığında geliştirilmesi sağlanmalıdır. Geliştirilen teknolojiler ise yine devlet kontrolünde gerekli ortamlar oluştukça dünya pazarına sunulmalıdır. İsrail ve ABD örneklerinde olduğu gibi geliştirilen teknolojiler ekonomik bir gelir kapısı olarak kullanılmalıdır. Burada asıl önemli olan geliştirilen teknolojinin uygun ortamda dünya pazarına sunulmasını sağlayacak girişimci yapıların desteklenmesidir. Ülkemizden örnek olarak; Baykar Teknoloji firmasının Suudi Arabistan Askeri Sanayisi ile gerçekleştirmiş olduğu anlaşma örnek olarak verilebilir. Bu anlaşma iki ülke arasında imzalanan bir anlaşmadan ziyade, üretilen ve ihraç edilen teknolojinin üretim aşamasında ortak hareket edilen kuruluşların fazlalığı ile dikkat

çekmektedir. İki ülke arasındaki anlaşmada rakip firmaların ABD ve Çin gibi ülkeler olduğu değerlendirildiğinde, gerçekleştirilen kamu, özel sektör işbirliklerinin ne kadar önemli ve gerekli olduğu bir kez daha göz önüne gelmektedir. Örnekten de anlaşıldığı gibi rakiplerin ABD ve Çin gibi uluslararası arenada söz sahibi olan ülkelerdir. Bu ülkeler alanda hâkim güç kurmakla diğer ülkeleri etkilemeye çalışmaktadırlar. Bunun için kendilerine rakip olan ülkeleri küçük düşürmek ve etkisiz kılmak için siber saldırılar düzenlemektedirler. Üretilen teknolojik ürünlerin uygulama ve kullanılışlı olması gerekliliktir. Fakat bu özelliğin arka tarafında üretilen teknolojilere karşı gerçekleştirilen siber saldırı veya karalama çalışmalarına karşı güvenlik tedbirlerinin alınması gerekliğini oluşmaktadır. Bu da her geliştirilen teknoloji ile siber güvenlik kavramının da geliştirilmesi anlamına gelmektedir. Çünkü hayatımıza giren her yeni teknoloji aynı zamanda yeni saldırılara zemin hazırlayan birer araç durumundadır. Bu saldırıların temelinde ise hedef ülke hakkında sürekli bilgi akışı temelli bir istihbarat sağlanması, hedef ülkenin karalanması, küçük düşürülerek uluslararası arenada güvensiz bir ülke konumuna düşürülme çalışmaları bulunmaktadır.

Hedef ülkelerin küçük düşürülmesi, karalanması ve düzenli olarak istihbarat akışısın sağlanması için ülkede öncelikle güvensiz bir ortamın hâkim olduğu izlenimini oluşturmak gerekir. Burada da en fazla kişiye ulaşan dezenformasyon ve bilgi kirliği yaratma çabasıdır. Bir ülkede dezenformasyon ve bilgi kirliğinin önüne geçilememesi, bilginin doğruluğunun ve bütünlüğünün temin edilmemesi güvensizlik ortamının oluşmasını sağlamaktadır. Güvensizlik ortamının oluşturulması hedef ülkelerin etki altına alınmasına kolaylaştırmakta ve istenen doğrultuda kamu oyu baskısının oluşturulmasına sağlamaktadır. Bu durumdan ülkelerin kendisini koruyabilmesi için düzenli olarak bilginin doğruluğunun sağlanması için sanal ortamın takibi gereklidir. Tespit edilen dezenformasyon ve yanlış bilgiye hemen müdahale edilmeli ve gerekli kamuoyu bilgilendirmeleri yetkili kişi veya kuruluşlar ile yapılmalıdır. Bu noktada, özellikle Rusya Federasyonu tarafından Kırım'ın yasa dışı ilhakı esnasında kullanmış olduğu dezenformasyon ve propaganda çalışmaları incelenmelidir. Bu tür saldırı veya karalamalar önceden tespit ve karşı tedbirler alınabilecek alt yapılar oluşturulmalıdır.

Stratejik yerlerin (elektrik dağıtım ve bakım merkezleri, su ve kanalizasyon işletmeleri, bankalar, ekonomik değere haiz işletmeler, kamu kurum ve kuruluşları… vb) güvenliğinde özellikle sistemin işlemesi önemlidir. Herhangi bir saldırı anında sistemde meydana gelen aksaklıklara sistem işlevine devam ederken müdahale edilmesi

gerekmektedir. Bu nedenle özellikle stratejik öneme sahip olan yerlerin kurulum ve işleyiş sistemleri herhangi bir saldırı anında sistemi kapatmadan müdahale etmeye uygun bir şekilde tasarlanmalıdır. Bu tür yerlerin güvenliğinin sağlanmasında iyi eğitilmiş bilinçli insanların çalışması ve kullanılan yazılımlarının milli ve yerli olmasına önem verilmelidir. Böylelikle gerekli olduğunda işleyişe girebilecek zararlı yazılımlara karşı koruma sağlanırken olumsuz ön yargılardan da arınmak mümkün olacaktır.

Siber saldırılar sanal alemde gerçekleşmektedir. Sanal alem sınırsız bilgi ve imkân sağladığı içinde Siber Güvenlik konusunda; devlet ve kuruluşlar tarafından oluşturulan konferans ve çalıştaylar yeni bilginin tespiti açısında önem arz etmektedir. Bu noktada, tek başına özel sektör veya kamunun yeterli olmadığı göz önünde bulundurulmalıdır. Bu nedenle özel sektöre kamu (devlet) tarafından destek verilmeli ve koordineli bir şekilde bu tür etkinliklerin arttırılması sağlanmalıdır. Dünya üzerinde her gecen gün güncellenen bir bilgi takibi yapılmaktadır. Bilginin güncelliği ile birlikte siber güvenlik ve gerekli olması halinde saldırı için yenilenebilirlik sağlanmalıdır. Alanında uzman kişiler tespit edilerek, bu kişilerin kamu bünyesinde veya kamu bünyesi tarafından desteklenen özel kuruluşlarda istihdamı sağlanmalıdır. Albert Einstein'in söylediği gibi "Tecrübe okulunun öğrenim ücreti yüksektir; ama akılsızlara bir şeyler öretebilen, başka okul da yoktur." En maliyetli öğrenme şekli tecrübe ederek öğrenmektir. Edinilen tecrübelerden ders alınması ve yapılacak düzenlemeler ile uğranacak zararlar en aza indirilebilir. Sanal ortam her türlü saldırıya açık durumdadır. Siber Güvenliğin arttırılması ve geliştirilmesi için karşılaşılan siber saldırılara maruz kalan veri tabanlarının arşivlenmesi sağlanmalıdır. Arşivlenen veri tabanları üzerinde gerekli tetkik ve incelemeler gerçekleştirilerek saldırının özellikleri belirlenmelidir. Belirlenen özellikler veri tabanı güvenlik ağı analizine eklenmelidir. Bu sayede daha sonradan meydana gelebilecek benzer veya aynı saldırılara karşı hızlı hamle yapılabilecek şekilde tedbirler alınması gerekir. Yapılacak bu çalışmalar ile veri kayıpları en az seviyede veya hiç olmayacak şekilde yedekli bir akış şematiği oluşturulmalıdır.

Tüm bu sayılanlara bakıldığında siber uzayda saldırıların ve tedbirlerin fazlalığı, saldırıların hepsinin veya bir kısmının birlikte kullanılabileceği göz önünde bulundurulduğunda önceliğin bilinçli ve güvenli kullanım olduğunun unutulmaması gerekmektedir. Bilinçli ve güvenli kullanım için eğitim programlarının ilköğretim aşamasından başlayarak her yaş ve unvanda güncellenerek tekrarlanması gerekir. Siber

güvenliğin en üst seviyeye çıkartılabilmesi için saldırı fazlalığı ve çeşitliliği göz önüne alındığında; tek yapılı güvenlik tedbirlerinden ziyade, koordineli bir şekilde bilgi paylaşımı sağlanmış milli ve yerli yapıya sahip grup veya topluluk çalışmaları tercih edilmelidir. Alınan tedbirlerin güvenilirliğinin düzenli olarak kontrol edilmesi için oluşturulan sanal ortamlarda uzman kişi veya gruplar tarafından siber saldırı ve sızma işlemleri gerçekleştirilmelidir. Bu sayede siber güvenlik ağının güncel ve güvenilirliği test edilmelidir. Herhangi bir açık veya yetersizlik tespit edildiği takdirde ise gerekli güncellemeler yapılarak güvenlik en üst seviyede tutulmalıdır. Siber güvenlik sistemlerinin günümüz teknolojisinde istek olmaktan çıktığı ve zorunluluk olduğu göz önünde bulundurulmalıdır. Geliştirilen teknolojiler ile birlikte siber güvenlik teknolojileri de geliştirilmelidir. Bu çalışmaların maliyetli olduğu göz önüne alındığında girişimci ruh ile birlikte uygun ortamda kontrollü bir şekilde pazarlamasının yapılması ve oluşan maliyetlerini azaltılması mümkündür. Teknolojik gelişmeler kapsamında bakıldığında, bu teknolojilerin gereken istihdam ve ihracat çalışmaları ile maliyetin üstünde bir katkı sağlayacağı unutulmamalıdır.

KAYNAKÇA

Aksoy Hakan, "Siber Güvenlik Meselesinde Askeri Uzmanlaşma: NATO Örneği," *TUİÇ Akademi*, Son Güncelleme: 16 Mart 2021, https://www.tuicakademi.org/siber-guvenlik-meselesinde-askeri-uzmanlasma-nato-ornegi/, (Erişim tarihi: 16.01.2023).

Aksünger Selman, "Siber Suçların Ekonomiye Verdiği Zararlarda Büyük Artış," *Anadolu Ajansı*, Son Güncelleme Tarihi: 10.10.2019, https://www.aa.com.tr/tr/dunya/siber-suclarin-ekonomiye-verdigi-zararda-buyuk-artis-/1608143, (Erişim tarihi: 01.03.2023).

Alca, Deniz, "Kim: Yeni Savaşlarda Asil Vekil Sorunu", Savunma Bilimleri Dergisi, Mayıs 2020, Sayı:37, (ss. 26-48).

Alipourvaghaslou Behnam, "Uluslararası Hukukta Yaptırım Rejiminin Genel İlkeleri ve Özellikleri," *Van Yüzüncü Yıl Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* Van YYÜ 40. Yıl Özel Sayısı, 2022, (ss. 157-186).

Altuğ Yılmaz, "Terörizm Sorunu," *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası* 51/1-4, 1987, (ss. 47-99).

Yemen'de 'Kararlılık Fırtınası' Operasyonu, *Anadolu Ajansı*, https://www.aa.com.tr/tr/dunya/yemende-kararlilik-firtinasi-operasyonu/63227,(Erişim tarihi: 01.01.2023).

Atasoy İrfan, Ormanlı Okan. "Teknoloji ve Siber Güvenlik: Dijital Toplumun Geleceği," *İstanbul Aydın Üniversitesi Dergisi* 11/4, 2019, (ss. 399-409).

Ateş Hamza, Akpınar Aydın. "Üniversitelerdeki FETÖ Yapılanması: Türk Üniversitelerindeki İhraç Edilen Akademisyenler Üzerine Bir Araştırma," *Strategic Public Management Journal* 3/5, 2017, (ss. 1-30).

Atutay Sercan Semih, Ateş Davut. "Türkiye'nin Sınır Ötesi Operasyonlarının Hukuki Çerçevesi," *Gazi Üniversitesi Hukuk Fakültesi Dergisi* 17/3, 2013, (ss. 109-146).

Aydın Mithat, "19-20 Yüzyılda Osmanlı Balkanlarda Rusya'nın Casusluk Faaliyetleri," *Tarih Araştırmaları Dergisi*, 32/53, 2013, (ss. 17-54).

Aydın Mustafa, "Vekalet Savaşları Nedir?- trguvenlikportali.com - e-güvenlik dersi-Modül 2-Güvenliğin Temel Kavramları," https://trguvenlikportali.com/ders-11-proxy-savaslar/,(Erişim tarihi: 01.01.2023).

Baykar, “Baykar’ın Suudi Arabistan’a İhracatı ABD’de Yankı Buldu” başlıklı haberi, 11 Ağustos 2023, https://baykartech.com/tr/haberler/baykarin-suudi-arabistana-ihracati-abdde-yanki-buldu/ URL uzantılı internet sitesi (Erişim tarihi 17.08.2023)

Başpınar Seda, “We Are Social Temmuz 2022 Raporu: İnternetle Aramızda Güven Sorunu Var,” *Marketing Türkiye Haber Sitesi*, Son Güncelleme Tarihi: 26 Temmuz 2022, https://www.marketingturkiye.com.tr/haberler/we-are-social-internet/, (Erişim tarihi: 01.03.2023).

Bayzan Şahin, Aytekin, Gülbahar. “Neden Bilinçli ve Güvenli İnternet,” güvenliweb.org.tr blog, Son Güncelleme Tarihi: 23 Nisan 2017, https://www.guvenliweb.org.tr/blog-detay/neden-bilincli-ve-guvenli-internet, (Erişim tarihi 20.01.2023).

Berqnet Blogu, “Truva atı (trojan) nedir? Nasıl bulaşır? Ne tür zararlara yol açabilir?”, Son Güncelleme Tarihi: 25 Şubat 2021, https://berqnet.com/blog/truva-ati, (Erişim tarihi: 02.03.2023).

Bıçakcı Salih, Ergun, F. Doruk, Çelikpala, Mitat, “Türkiye’de Siber Güvenlik,” Kadir Has Üniversitesi Uluslararası İlişkiler ve Sosyal Bilimler Yüksek Okulu-https://edam.org.tr/document/CyberNuclear/SiberKitapTR/edam_siber_guvenlik_b2.pdf, (Erişim tarihi: 20.01.2023).

Bıçakcı, Sahil, “Siber Güvenlik ve Savunma”, *Güvenlik Yazıları Portalı Kasım 2019,* (ss1-8).

Enformasyon Nedir, https://bilgibilimi.net/enformasyon-nedir/,(Erişim tarihi: 09.01.2023).

BKK, Bakanlar Kurulu Kararı (Kanun No. 3842). *Resmi Gazete* 28447 (20 Ekim 2012), Erişim 28.01.2023. https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm.

BMA, Santransisko’da 26 Haziran 1945 Tarihinde Yapılmış ve İmzalanmış Olan Birleşmiş Milletler Andlaşması ile Milletlerarası Adalet Divanı Statüsünün Onanması Hakkında Kanun (Kanun No. 4801). *Resmi Gazete* 6902 (24 Ağustos 1945), Erişim 28 Şubat 2023. https://www.resmigazete.gov.tr/arsiv/6092.pdf.

Bulut Selçuk, “Tarihte En Çok İnsan Öldüğü 5 Savaş,” *Milliyet Gazetesi*, https://www.milliyet.com.tr/molatik/tarih/tarihte-en-cok-insanin-oldugu-5-savas-90465,(Erişim tarihi: 01.01.2023).

Bulut Yakup Halit, *Büyük Dizayn Algı Savaşları*, Yeniyüzyıl Yayınları, İstanbul 2017.

Cebe Çağatay. *Rusya’nın Dış Politikadaki Gayrinizami Unsurları: Özel Askeri Şirketler*, Acta Fabula Çalışma Grubu, İstanbul 2020.

Corera Gordon. “İngiltere’de Siber Güvenlik Merkezi Açıldı,” *BBCNEWS Türkçe*, Son Güncelleme: 14 Şubat 2017, https://www.bbc.com/turkce/haberler-dunya-38967467, (Erişim tarihi:11.01.2023).

Çapar, Bengü, ‘Bir İşletim Sistemi Olarak Bilgi Yönetimi:Teorik Bir Yakalaşım,’konferans sunumu https://strateji.deu.edu.tr/wp-content/uploads/2014/09/B%C4%B0R-%C4%B0LET%C4%B0%C5%9E%C4%B0M-S%C4%B0STEM%C4%B0-OLARAK-B%C4%B0LG%C4%B0-Y%C3%96NET%C4%B0M%C4%B0_TEOR%C4%B0K-B%C4%B0R-YAKLA%C5%9EIM.pdf, URL uzantılı sayfa (görüntüleme tarihi 04.08.2023)

Sniffing Nedir?, Cyber Security Blog, Son Güncelleme: 19 Temmuz 2017, https://karslanblog.wordpress.com/2017/07/19/sniffing-nedir/, (Erişim tarihi: 02.03.2023).

Siber Güvenlik Ulusu: İsrail Ağı Korumada Nasıl Dünya Lideri oldu, Cybersecuritycover Haber Blogu, https://itrade.gov.il/turkiye/siber-guvenlik-ulusu-israil-agi-korumada-nasil-dunya-lideri-oldu/,(Erişim tarihi: 11.01.2023).

Çahmutoğlu Ersin, “ABD’deki USCYBERCOM muadili olarak görünen İngiltere’nin NCF birimi Türkiye İçin Model olabilir mi?”, *Linkedin Haber Blogu*, Son Güncelleme: 22 Aralık 2021, https://tr.linkedin.com/pulse/abddeki-uscybercom-muadili-olarak-g%C3%B6r%C3%BClen-ingilterenin-ncf-birimi, (Erişim tarihi: 11.01.2023).

Çahmutoğlu Ersin, “Siber Uzayda Güç ve Siber Silah Teknolojilerinin Küresel Etkisi,” *Analitical Politic* 1/1, 2020, (ss. 63-79).

Çahmutoğlu Ersin, *İran’ın Siber Gücü*, İRAM Yayınları, Ankara 2021.

Çeliksoy Ergün, Ouma Smith, “Terör Örgütlerinin İnternet Kullanımı,” *Bilişim Hukuk Dergisi* 1/2, 2019, (ss. 243-267).

Çoban Cemal, “Yeni Dünya Düzeni Bağlamında Terör, Vekalet Savaşları ve Türkiye,” (Gaziantep Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi), Gaziantep 2018.

Cona, Ömer, “Suriye Krizinde Uluslararası Güç Mücadelesi: Vekalet Savaşları.” (Ankara Hacı Bayram Veli Üniversitesi Türkiye ve Orta Doğu Amme İdaresi Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi) (Ayrıntılı bilgi için Ankara 2018, (Suriye Krizinde Uluslararası Güç Mücadelesi: Vekalet Savaşları, Nobel Bilimsel Eserler Yayınları incelenebilir,)

Çulha-Zabcı Filiz, “Yeni Savaşların Gizli Yüzü: Özel Askeri Şirketler,” *Mülkiye Dergisi* 28/243, 2004, (ss.21-49).

Darıcılı Ali Burak, Özdal Barış. "Çin Halk Cumhuriyeti'nin Siber Güvenlik Stratejilerinin Analizi," *Güvenlik Stratejileri Dergisi*, 28, 2018, (ss. 1-35).

Darıcılı Ali Burak, "Demokrat Parti Hack Skandalı Bağlamında ABD ve RF'nin Siber Güvenlik Stratejilerinin Analizi," *Ulise: Uluslararası Çalışmalar Dergisi* 1/1, 2017, (ss. 1-24).

Derman, Giray Saynur, Haya Babur. "11 Eylül Sonrası Afganistan'daki Güvenlik Sistemi," *Akademik Bakış Dergisi* 41, 2014, (ss.30-44)

En Yüksek BM Kurulunda Bir Koltuk, Deutschland.de Dijital Haber Sitesi. https://www.deutschland.de/tr/topic/politika/almanya-birlesmis-milletler-guvenlik-konseyi-uyeligine-aday, (Erişim tarihi: 28.02.2023).

Develioğlu, Ferit. Lügat, 1960, https://ia800603.us.archive.org/20/items/Osmanlca-TTrkreAnsiklopedikLkgat/0811-Osmanlica_Lughat-Eshanlam_Sozluk-Ferid_Develioghlu-Latin-Ebced-1960-1570s.pdf adresinden indirilmiştir,(Erişim tarihi: 16.01.2023).

Siber Savaş Uygulanacak Hukuk Hakkında Tallinn El Kitabı, pdf Free Download (docplayer.biz.tr), (Erişim tarihi: (16.01.2023).

Talat Şafak, "Asimetrik Savaş Örneği Olarak 2006 İsrail-Lübnan Savaşı Hizbullah ve Çıkarımlar", *Aşiyan Kültür-Sanat ve Edebiyat Dergisi, 2013,* (ss 19-25).

Düvenci Serhat, "Devletin Köken Teorileri Açısından Devleti Doğuran Etmenler: Çeşitli Uygarlıklar ve Topluluklar Üzerinden Bir Değerlendirme," *Uluslararası Yönetim Akademisi Dergisi* 2, 2018, (ss. 66-93).

Ertürk Sebahattin, *Propaganda ve Beşinci Kolun İkinci Dünya Harbinde Oynadığı Roller*, Genelkurmay Başkanlığı Yayınları, Ankara 1951.

Eskier Uğur, "Birleşmiş Milletler (BM) Nedir? (Kuruluşu, Amacı, Yapısı)", makaleler.com sitesi, https://www.makaleler.com/birlesmis-milletler-nedir, (Erişim tarihi: 28.02.2023).

Eşidir,Osman Vedüd, Bak Gökhan, "Şiddet Unsuru Olarak Terör Olaylarının Medyada Haberleştirilmesi", *Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi (ASEAD)*, 2018, (ss13-32).

Fisher Tim, Leger, Jerry. "12 Best Free Spyware Removal Tools (March 2023)," lifewire.com blog, Son Güncelleme 1 Mart 2023, https://www.lifewire.com/best-free-spyware-removal-4151293,(Erişim tarihi 02.03.2023).

Giles Keir, *Russia's National Security Strategy to 2020*, NATO Defense College College e Defense de 1'OTAN- June 2009.

Göçoğlu Volkan, Aydın, Mehmet Devrim, "Siber Güvenlik Politikası: ABD, RUSYA ve Çin Üzerine Karşılaştırmalı Bir Analiz," *Güvenlik Bilimleri Dergisi* 2, 2019, (ss. 229-252).

Güldağı Mustafa, *Coğrafi ve Zihinsel İşgalin Arka Planı Kuşatma*, Lopus Yayınları, Ankara 2019.

Güleç Özge, Kişman Zülfükar Aytaç, "Uluslararası İlişkiler Açısından Siber Güvenlik ve NATO'nun Siber Güvenlik Stratejileri," *Akademik Açı,* 1/1, 2021, (ss. 127-154).

Güngör Murat, "Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma," (Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı, Yayınlanmamış Uzmanlık Tezi), Ankara 2015.

Hasan Ateş, *Vekalet Savaşları Stratejik Eksende Gizli Kuvvet İstihbarat,* Detay Yayınları, Ankara 2017.

Uluslararası Hukukta Yaptırımlar: ABD Örneği, Hukukçular Derneği, https://hukukcular.org.tr/uluslararasi-hukukta-yaptirimlar-abd-ornegi/, (Erişim tarihi: 20.01.2023).

Işık Salim, "J. J. Rousseau ve Egemenlik Anlayışı Üzerine," *İnönü Üniversitesi Hukuk Fakültesi Dergisi* 8/2, 2017, (ss. 79-98).

APT nedir?, Infinitumit.com, Haber Bloğu. Son Güncelleme: 8 Aralık 2022, https://www.infinitumit.com.tr/apt-nedir/#:-, (Erişim tarihi: 12.01.2023).

İren Ecem, Can Özgü. "Bilgi Sistemlerinde Güncel Güvenlik Problemleri ve Önerilen Çözümler," *TUBAV Bilim Dergisi* 10/2, 2017, (ss. 27-42).

Kalkan Duhan, "Devletin Güç Kullanması Tekeli ve Özel Askeri Şirketler," *Bölgesel Araştırmalar Dergisi* 6/1, 2022, (ss. 148-173).

Karabacak Kerim Emre, "Terör Örgütlerinin Siber Uzay Kullanımı: DEAŞ Örneği," *Erzincan Binali Yıldırım Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* 1, 2022, (ss. 51-64).

Karabulut Bilal, "Uluslararası Yaptırımların Hukuksal Bir Analizi", *Uluslararası Hukuk ve Politika,* No: 12, Yıl: 2007, (ss.15-40).

Karadağ Ulaş, "Birleşmiş Milletler Antlaşma'na Göre Meşru Müdafaa Hakkı," *İnönü Üniversitesi Hukuk Fakültesi Dergisi* 7/2, 2016, (ss. 171-186).

Kargı, Bilal, "Uluslararası Kredi Derecelendirme Kuruluşları ve Türkiye'nin Kredi Notu Üzerine Bir İnceleme", International Journal Of Social Sciencex 2014, (ss 351-370).

Kavlak, Ahmet, "Terör ve Meşru Terör", *Doğu Batı Dergisi 43, 2007* (ss,221-229)

Kayıran Mehmet, Metintaş M. Yahya. "TÜRK_YUNAN İLİŞKİLERİ (1878-1952), Eskişehir Üniversitesi Türk Dünyası Uygulama ve Araştırma Merkezi Yakın Tarih Dergisi 2018, (ss.33-73)

Kazan Hüseyin, "Terör-Medya İlişkisi ve Medyada Terör Haberciliği," *Güvenlik Stratejileri Dergisi* 24, 2012, (ss. 109-147).

Keskin, Nurbane, "ABD-Çin Rekabatinin Siber Güvenlik Bağlamında Ortadoğu'ya Yayılması", Ufuk Üniversitesi Siyaset Bilimi ve Uluslararası İlişkiler Ana Bilim Dalı, Yüksek Lisans Tezi, Ankara 2022.

Kılıç Mehmet, "Milli Mücadele Döneminin Siyasi ve Stratejik Açıdan Değerlendirilmesi," *Stratejik ve Sosyal Araştırmalar Dergisi* 3/1, 2019, (ss. 48-69).

Kırel Çiğdem, "Örgütsel Çatışma ve Güç İlişkisi," *Anadolu Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* 1, 1997, (ss. 477-492).

Kneel Noelle, "Siber Saldırıların Kaynaklandığı İlk 10 Ülke," Government Blog, Son Güncelleme: 23 Nisan 2013, https://www.govtech.com/security/hacking-top-ten.html, (Erişim tarihi: 20.01.2023).

Kurudal, Orhan, "Bilişim Çağımda Siber Saldırılar ve Yeniden Bloklaşma", *Dünya İnsan Bilimleri Dergisi,* 2020-2, (ss 132-158), s134

Komar, Barış, Yımaz,Nihat, "Gürcistan'daki Etnik Çatışmalarda Rusya'nın Rolü", *İktisadi ve İdari Araştırmalar Dergisi"*, 2022, (ss.34-51).

Radhika Sarang, Dikkat: Zombi Lot Botnets, McAfee Blog. Son Güncelleme 06 Kasım 2018, https://www.mcafee.com/blogs/consumer/mobile-and-iot-security/zombie-iot-botnets/, (Erişim tarihi 02.03.2023).

Medvedev Sergei A., "Offence-Defence Theory Analysis of Russian Cyber Capability," (Naval Post-Graduate School, Master Thesis), Monterey, Colifornia, 2015.

ABD'den İran'a "Siber Hırsızlık" Yaptırımı," Memleket Haber Ajansı, Son Güncelleme Tarihi: 23 Mart 2018, https://www.memleket.com.tr/abdden-irana-siber-hirsizlik-yaptirimi-1356889h.htm, (Erişim tarihi: 12.01.2023).

Millward, Steven, "China Now has 731 million internet users, 95% Access from their pones-Techinasia," Access From Their Phones-techinasia.com Haber Bloğu, Son Güncelleme: 23 Ocak 2017, Https://www.techinasia.com/china-731-million-internet-users-end-2016, (Erişim tarihi: 03.03.2023).

NATO Nedir?, https://www.nato.int/nato-welcome/index_tr.html,(Erişim tarihi: 13.01.2023).

Oğuzlu H. Tarık, "Dünya Düzenleri ve Güvenlik: Ulus-Devlet Güvenlik Anlayışı Aşılıyor Mu?," *Güvenlik Stratejileri Dergisi* 3/6, 2007, (ss. 7-43).

Ögün Mehmet Nesip, Kaya Adem, "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler," *Savunma Sanayi Dergisi* 9/18, 2013, (ss. 145-181).

Özel Özcan, Merve Suna, "Westphalian Devletler Sistemi ve Modernleşmenin Geleneksel Dünyanın Büyük Güçleri Olan İmparatorluklara Etkisi", *dergipark.org.tr sitesi*, https://dergipark.org.tr/tr/download/article-file/843945 URL uzantılı internet sitesi (Erişim tarihi 17.08.2023)

Ölçekçi Haluk, "Vekalet Savaşlarının Bir Aracı Olarak Medya ve 15 Temmuz Sürecinde FETÖ'nün Medya Faaliyetleri," *Uluslararası 15 Temmuz ve Darbeler Sempozyumu*, Kartepe Zirvesi, 2018, (ss. 225-247).

Özdemir Haluk. "Uluslar Arası İlişkilerde Güç: Çok Boyutlu Bir Değerlendirme," *Ankara Üniversitesi SBF Dergisi* 63/3, 2008, (ss. 113-144).

Özdemir Özge. "Siber Krizin Tarihçesi (ABD ve Çin Arasındaki Siber Mücadelenin Kilit Tarihleri)," *Bloomberg Dijital Haber Sitesi*, Son Güncelleme: 07.07.2015, https://businessht.bloomberght.com/piyasalar/haber/1099882-siber-krizin-tarihcesi, (Erişim tarihi: 10.01.2023).

Özer,Sanem, Oğuz,Ceren Uysal, Atyur, Senem, "NATO ve AB'nin Değişen Güvenlik Stratejilerinin Afganistan Örneğinde Değerlendirilmesi", *Akdeniz İ.İ.B.F. Dergisi 2010,(ss 257-285).*

Özfındık-Koik Yasemen, "Uluslararası İlişkilerde Siber Güvenlik Algısı ve Ulus Devletin Değişim Stratejisi," (Çukurova Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi), Adana 2015.

Öztopal Mustafa Kemal, "Önde Gelen Uluslararası Örgütlerin Kırım'ın Yasadışı İlhakına Tepkileri," *Uluslararası Suçlar ve Tarihi Dergisi* 19, 2018, (ss. 105-135).

Pamukoğlu Mustafa, "Savaşların Maliyetleri," *Aydınlık Dijital Gazetesi*, Son Güncelleme; 06 Mart 2016, https://www.aydinlik.com.tr/koseyazisi/savaslarin-maliyeti-17640, (Erişim tarihi: 01.01.2023).

Parwez Ahsan, "WordPress DDos Saldırıları: Türleri ve Bu Saldırılara Karşı Korunma Konusunda Ayrıntılı Bir Kılavuz", Cloudways by Digital Ocean, Son Güncelleme: 19 Ağustos 2022, https://www.cloudways.com/blog/wordpress-ddos-attacks/,(Erişim tarihi: 02.03.2023).

Pınar Latif, "Amerika Birleşik Devletleri'nin Yumuşak Gücü ve Hollywood," *İnsan ve Toplum Bilimleri Araştırmaları Dergisi* 6/1, 2017, (ss. 253-274).

Polat Doğan Şafak, "NATO'nun Yeni Operasyon Alanı: Siber Uzay," *Güvenlik Bilimleri Dergisi* UGK Özel Sayısı, 2020, (ss. 135-158).

Purtaş Fırat, "Soğuk Savaş Sonrası NATO'nun Dönüşümü ve Genişlemesi Çerçevesinde Türk Amerikan Askeri İlişkileri," *Güvenlik Stratejileri Dergisi* 1/2, 2005 (ss. 7-31).

Reçber, Kamuran. "NATO Kurucu Andlaşması 5. Maddesinin Saldırı Fiili Acısından Analizi",*The Journal of Diplomatic Research- Diploması Araştırmaları Derğisi, 2020*

Russian Federation Armed Forces' Information Space Activities Concept, *Ministry of Defence of the Russian Federation*, https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle, (Erişim tarihi: 09.01.2023).

Sağıroğlu Şeref. *Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler*, Grafiker Yayınları, Ankara 2018.

Sağıroğlu Şerif, Alkan, Mustafa. *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*, Grafiker Yayınları, Ankara 2019.

Samet Refik, Aslan Ömer, *Kötü Amaçlı Yazılımlar ve Analizi*, Grafiker Yayınları, Ankara 2018, (ss. 225-255).

Savçın, Engin. Devletlerin Siber Güvenlik Politikalarının Şekillendirilmesi Sürecinde Kamu –Özel Sektör İşbirliğinin Artan Önemi; İsrail ve Yeni Zelanda Örnekleri, (Yalova Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi), Yalova 2020,

NATO Üyeleri Yeni Siber Savunma Politikasın Kabul Etti, Son Güncelleme: 16.06.2021, NATO üyeleri yeni siber savunma politikasını kabul etti (savunmatr.com), (Erişim tarihi: 16.01.2023).

Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ (Kanun No. 3842), *Resmi Gazete* 28818 (11 Kasım 2013), Erişim 21.01.2023, https://www.resmigazete.gov.tr/eskiler/2013/11/20131111-6.htm.

Seferoğlu Süleyman Sadi, "Bilgisayar Virüsleri," online ders anlatısı-https://yunus.hacettepe.edu.tr/~sadi/dersler/ebb/ebb467-guz2000/hale-p.html, (Erişim tarihi: 02.03.2023).

Sevinç İsmail, Babahanoğlu Veysel. "Küresel Güvenliğin Değişken Yapısı ve Terör Örgütleri Üzerine Etkisi: DEAŞ Terör Örgütü Örneği," *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Dergisi* 24/4, 2019, (ss. 969-987).

Siber Suçlarla Mücadele Daire Başkanlığı, "Siber Dünya Nedir?," https://siberay.com/siber-dunya-nedir, (Erişim tarihi 01.03.2023)

5. Uluslararası Siber Suçlar Çalıştay Raporu, Siber Suçlarla Mücadele Daire Başkanlığı, 10-13 Aralık 2018.

Şen Yusuf, "Terörün Toplumlar Üzerindeki Sosyo-Ekonomik Etkilerine Bakış: PKK Terörü ve Ağrı Gerçeği," *Ağrı İbrahim Çeçen Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 1/2, 2015, (ss. 17-70).

TCK, 765 Sayılı Türk Ceza Kanunu'nun Bazı Maddelerini Değiştirilmesine Dair Kanun (Kanun No. 3756), *Resmi Gazete* 20901 (14 Haziran 1991), Erişim 28.01.2023. https://www.resmigazete.gov.tr/arsiv/20901.pdf.

Tokcan Hüseyin, "Bilginin Üretimi ve Kullanımı Açısından Bilgi Yönetimi: Üniversite'de Akademik Yöneticilerin Bilgi Yönetimi Algıları Üzerine Bir Uygulama," (Kırıkkale Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Doktora Tezi), Kırıkkale 2015.

Topçu Servet Habip, "Rusya Federasyonu'nun Siber Güvenlik Stratejisi: Kırım Örneği," *Uluslararası İlişkiler Çalışmaları Dergisi* 2/1, 2022, (ss. 19-35).

Türkiye ve Terörizm, Türkiye Barolar Birliği Yayınları, Ankara 2006.

Dünyadan Örneklerle Siber Güvenlik Stratejileri ve Siber Uzay, Türkiye Cumhuriyeti İç İşleri Bakanlığı. İç Güvenlik Stratejileri Dairesi Başkanlığı, Ankara 2020.

2016-2019 Ulusal Siber Güvenlik Stratejisi, Türkiye Cumhuriyeti Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf, (Erişim tarihi: 19.12.2022).

USOM Hakkında, Ulusal Siber Olaylara Müdahale Merkezi, https://www.usom.gov.tr/hakkimizda, (Erişim tarihi 03.03.2023).

Ünver Mustafa, "Türkiye'de Siber Güvenlik," Academia.edu, https://www.academia.edu/24842186/T%C3%BCrkiyede_Siber_G%C3%BCvenlik , (Erişim tarihi 21.01.2023).

Yavuz A. Filiz, "Muhalif olmak ve Muhalefet Yapmak," *Türk Yurdu Dergisi* 323, 2014. https://www.turkyurdu.com.tr/yazar-yazi.php?id=282, (Erişim tarihi: 16.01.2023).

Yenal Serkan, Akdemir Naci. "Uluslararası İlişkilerde Yeni Bir Kuvvet Çarpanı: Siber Savaşlar Üzerine Bir Vaka Analizi," *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* 11/1, 2020, (ss. 414-450).

İngiltere Siber Düşmanlarını Açıkladı-Yeni Türkiye'nin Düşünce Merkezi, *Yeni Şafak Gazetesi*, Son Güncelleme: 28 Aralık 2021,

https://www.sde.org.tr/dunya/ingiltere-siber-dusmanlarini-acikladi-haberi-25166,(Erişim tarihi: 11.01.2023).

Yılmaz Malik, 'Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi,' *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, 49,1 2009 (ss95-118)

Yılmaz Sait, "21'inci Yüzyılda Güvenlik Alanının Yeni Sivil Aktörleri: Özel Askeri Şirketler ve Kontratçı Firmalar," *Güvenlik Stratejileri Dergisi* 3/6, 2007, (ss. 43-70).

Yiğit Süreyya, Gülbiten Gökhan, "Rusya'nın Yakın Çevre Dış Politikası ve Azerbaycan," *Barış Araştırmaları ve Çatışma Çözümleri Dergisi* 5/1, 2017, (ss. 54-70).

ÖZGEÇMİŞ

Mümin TEKİN, İlk ve Orta Öğretimini Karaman ilinde tamamladıktan sonra, 2001-2003 yıllara arasında Akdeniz Üniversitesi'nde Bilgisayarlı Muhasebe eğitimini tamamladıktan sonra, 2003-2005 yılları arasında Adile Sadullah Polis Meslek Yüksek Okulunda polislik eğitimi alarak Emniyet Teşkilatında polis memuru olarak göreve başladı. 2005-2009 yılları arasında Anadolu Üniversitesi İşletme Fakültesini tamamladı. 2019 yılında Karabük Üniversitesi, Yüksek Lisans Enstitüsünde, Bölge Çalışmaları Ana Bilim Dalında yüksek lisansa başladı. Halen Karabük İl Emniyet Müdürlüğünde polis memuru olarak görev yapmakta ve yüksek lisansına devam etmektedir.