ULUSLARARASI İLİŞKİLERDE SİBER GÜVENLİK VE SİBER HUKUK

2023
YÜKSEK LİSANS TEZİ
ULUSLARARASI İLİŞKİLER

Mithat BAŞTUĞ

Tez Danışmanı
Dr. Öğr. Üyesi Muhammed Ali YETGİN

ULUSLARARASI İLİŞKİLERDE SİBER GÜVENLİK VE SİBER HUKUK

Mithat BAŞTUĞ

Tez Danışmanı
Dr. Öğr. Üyesi Muhammed Ali YETGİN

T.C.
Karabük Üniversitesi
Lisansüstü Eğitim Enstitüsü
Uluslararası İlişkiler Anabilim Dalında
Yüksek Lisans Tezi
Olarak Hazırlanmıştır.

KARABÜK
Haziran 2023

İÇİNDEKİLER

TEZ ONAY SAYFASI

Mithat BAŞTUĞ tarafından hazırlanan "ULUSLARARASI İLİŞKİLERDE SİBER GÜVENLİK VE SİBER HUKUK" başlıklı bu tezin Yüksek Lisans Tezi olarak uygun olduğunu onaylarım.

Dr. Öğr. Üyesi Muhammed Ali YETGİN .....

Tez Danışmanı, Büro Hizmetleri ve Sekreterlik

Bu çalışma, jürimiz tarafından Oy Birliği ile Uluslararası İlişkiler Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir. 21/06/2023

Ünvanı, Adı SOYADI (Kurumu) İmzası

Başkan: Doç. Dr. Ersin MÜEZZİNOĞLU (KBÜ) .....

Üye : Doç. Dr. Yavuz GÜLOĞLU (KÜ) .....

Üye : Dr. Öğr. Üyesi Muhammed Ali YETGİN (KBÜ) .....

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 olarak sunduğum bu çalışmayı bilimsel ahlak ve geleneklere aykırı herhangi bir yola tevessül etmeden yazdığımı, araştırmamı yaparken hangi tür alıntıların intihal kusuru sayılacağını bildiğimi, intihal kusuru sayılabilecek herhangi bir bölüme araştırmamda yer vermediğimi, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu ve bu eserlere metin içerisinde uygun şekilde atıf yapıldığını beyan ederim.

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

Adı Soyadı: Mithat BAŞTUĞ

İmza :

ÖNSÖZ

Bilişim çağı içerisinde olmamız nedeniyle siber alanın halen önem verilen bir alan olmaması sebebiyle bu tez çalışması ortaya çıkmıştır. Tez çalışmamız temelde literatür ve ulusal ve uluslararası belgeler ışığında yeni gelişmelerle harmanlanarak temel sorulara cevaplar aranarak ortaya çıkmıştır. Bu süreçte maddi ve manevi desteklerini esirgemeyen başta danışmanım Muhammed Ali YETGİN ve sevgili aileme teşekkürlerimi bir borç bilirim.

ÖZ

Güvenlik kavramı, uluslararası ilişkiler disiplini gibi farklı disiplinler içerisinde de değerlendirilmiş ve çeşitli yaklaşımlar geliştirilmiştir. Soğuk Savaş ile başlayan uzay yarışı, uluslararası dengeleri değiştirdiği gibi güvenlik kavramının da değişmesine neden olduğu gibi siber alanın doğmasına ve internetin ortaya çıkmasına da neden olmuştur. İnternetin hızla tabana yayılmasıyla birlikte siber alan genişlemiş ve yeni güvenlik açıklarının ortaya çıkmasına neden olmuştur. Bu güvenlik açıkları arasında siber güvenlik büyük bir sorun olarak bireyleri, şirketleri, devletleri ve uluslararası örgütleri derinden tehdit ettiği gibi büyük maddi ve manevi kayıpların ortaya çıkmasına neden olmuştur. Günümüzde siber güvenlik temel sorun olarak güvenlik meselesinin tam merkezinde dururken gelişen teknolojilerle birlikte her geçen gün çeşitlenmeye devam etmesi bireylerden devletlere kadar herkesi derinden endişe içerisine sürüklemektedir. Oluşan endişe ve korkunun giderilmesi adına bireyler, devletlerin çizdiği politikalar ekseninde kendi politikalarını belirlerken, devletlerde vatandaşlarını ve devletin varlığını korumak adına çeşitli adımlar atmaktadır. Fakat devletler siber alandan gelecek olan tehditleri bertaraf etmek veyahut engellemek adına çeşitli girişimlerde bulunsa da hedef belirlenen devletlere veyahut şirketlere yönelik siber alanı kullanarak saldırılar gerçekleştirmektedirler. Devletler veya devlet dışı aktörler, siber alanı kendi çıkarları ekseninde kullanması sebebiyle siber alanın denetimi için oluşturdukları veya oluşturmak istedikleri uluslararası çalışmalarda ikili davranarak hem ikili ilişkilerin engellenmesine hem de uluslararası güvenliğin tahsis edilmesine dolaylı yönden engel olmaktadırlar.

Anahtar Kelimeler: Siber Güvenlik, Uluslararası İlişkiler, Güvenlik, Siber Hukuk

ABSTRACT

The concept of security has been evaluated in different disciplines such as the discipline of international relations and various approaches have been developed. The space race, which started with the Cold War, not only changed the international balance, but also caused the concept of security to change, it also led to the emergence of the cyber space and the emergence of the internet. With the rapid spread of the Internet, the cyber space has expanded and has led to the emergence of new security vulnerabilities. Among these security vulnerabilities, cyber security has seriously threatened individuals, companies, states and international organizations as a major problem and has caused great material and moral losses. Today, while cyber security stands at the center of the security issue as the main problem, its continuing to diversify day by day with the developing technologies causes everyone from individuals to states to be deeply concerned. In order to eliminate the resulting anxiety and fear, individuals take various steps to protect their citizens and the existence of the state in the states, while determining their own policies in line with the policies drawn by the states. However, although states make various attempts to eliminate or prevent threats from cyberspace, they carry out attacks against targeted states or companies by using cyberspace. States or non-state actors indirectly prevent both the prevention of bilateral relations and the allocation of international security by acting bilaterally in the international studies they have created or want to create for the control of the cyber space, since they use the cyber space for their own interests.

Keywords: Cyber Security, International Relations, Security, Cyber Law

ARŞİV KAYIT BİLGİLERİ

Tezin Adı	Uluslararası İlişkilerde Siber Güvenlik ve Siber Hukuk
Tezin Yazarı	Mithat BAŞTUĞ
Tezin Danışmanı	Dr. Öğr. Üyesi Muhammed Ali YETGİN
Tezin Derecesi	Yüksek Lisans
Tezin Tarihi	21/06/2023
Tezin Alanı	Uluslararası İlişkiler Anabilim Dalı
Tezin Yeri	KBÜ/LEE
Tezin Sayfa Sayısı	135
Anahtar Kelimeler	Siber Güvenlik, Uluslararası İlişkiler, Güvenlik, Siber Hukuk

ARCHIVE REGISTRATION INFORMATION

Name of the Thesis	Cyber Security and Cyber Law in International Relations
Author of the Thesis	Mithat BAŞTUĞ
Advisor of the Thesis	Assist. Prof. Muhammed Ali YETGİN
Status of the Thesis	Master Degree
Date of the Thesis	21/06/2023
Field of the Thesis	Department of International Relations
Place of the Thesis	UNIKA/IGP
Total Page Number	135
Keywords	Cyber Security, International Relations, Security, Cyber Law

KISALTMALAR

ABD : Amerika Birleşik Devletleri

API : Uygulama Programlama Arabirimi

APWG : Kimlik Avı Önleme Çalışma Grubu

ARPA : Gelişmiş Savunma Araştırmaları Projeleri Birimi

ARPANET : Gelişmiş Araştırma Projeleri Dairesi Ağı

BM : Birleşmiş Milletler

BTK : Bilgi Teknolojileri ve İletim Kurumu

CCDCOE : NATO Müşterek Siber Savunma Mükemmeliyet Merkezi

CMCA : Bilgiyi Kötüye Kullanımı ve Siber Güvenlik Yasası

ÇKP : Çin Komünist Partisi

DARPA : Savunma Gelişmiş Araştırma Projeleri Ajansı

DDOS : Dağıtık Hizmet Reddi Saldırıları

ENIGMA : Almanya Kripto Cihazı

IWS : Internet World Stats

NATO : Kuzey Atlantik Antlaşması Teşkilatı

ODTÜ : Orta Doğu Teknik Üniversitesi

PDK : Politbüro Daimî Komitesi

TBMM : Türkiye Büyük Millet Meclisi

TCK : Türk Ceza Kanunu

TMK : Terörle Mücadele Kavramı

TR-BOME : Türkiye Bilgisayar Olayları Müdahale Ekibi

TUBİTAK : Türkiye Bilimsel ve Teknik Araştırma Kurumu

UNESCO : Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütü

ARAŞTIRMANIN KONUSU

Araştırmamız, uluslararası ilişkiler disipliniyle özdeşleşen ve diğer disiplinler içerisinde de yer alan güvenlik kavramının, siber alana entegre edilmesiyle birlikte var olan güvenlik sorunlarının siber alanda nasıl sorunlar ortaya çıkardığı ve klasik güvenlik anlayışı ile siber güvenlik anlayışı arasındaki tehlike boyutu karşılaştırılmış ve siber alandaki güvenlik çeşitliliği anlatılmıştır.

ARAŞTIRMANIN AMACI VE ÖNEMİ

Araştırmamızın amacı, sayısal veriler ve alanında uzman yazarların bilgelerini sentezleyerek fiziki dünya ile siber alanın doğrudan ve dolaylı ilişkisini birleştirerek geçmişten günümüze olan sürecin anlatılması ve gelecekte olması kuvvetle muhtemel vakaların ve kararların yorumlanmasını hedeflemektir. Araştırmamızın önemi ise siber alanın denetlenmesi için devletlerin ve uluslararası örgütlerin siber alanın kontrol edilmesi ve denetlenmesi için oluşturdukları hukuki metinlerin gelecek çalışmalar için bir rehber niteliğinde olması sebebiyle önem taşımaktadır.

Araştırmamız kapsamında yöneltilen sorular ışığında, gelecekte hem devletler hem de uluslararası örgütler düzeyinde oluşturulacak siber güvenlik politikalarına ve hukuki metinlere katkı sağlayacaktır. Özellikle araştırma kapsamında detaylı olarak anlatılan siber saldırı araçları ve vakaları, hukuki metinlerin tekrardan yenilenmesinde öncü olacaktır.

ARAŞTIRMANIN YÖNTEMİ

Araştırmamız, Doküman Analiz Yöntemi ile oluşturulmuştur. Bu bağlamda çalışmamızda sayısal veriler ışığında fiziki dünya ile siber alanda gerçekleşen etkileşim ve teknoloji transferleri bilimsel verilerle desteklenerek açıklanmıştır.

ARAŞTIRMA HİPOTEZLERİ / PROBLEM

Araştırmamızın temel problemi insanlık tarihiyle birlikte paralel şekilde gelişen güvenlik kavramının, son çeyrek asırda kökten değişmesi ve bu değişime bağlı olarak

var olan güvenlik sorunlarının yanı sıra yeni güvenlik sorunlarının ortaya çıkması ve yeni ortaya çıkan güvenlik açıklarının bireyden devlete kadar uzanan etkilerinin neler olduğu üzerine kurulmuştur. Ana problemin altında ise bireylere, şirketlere, devletlere ve uluslararası örgütlere çeşitli sorular yöneltilerek cevap aranmıştır.

KAPSAM VE SINIRLILIKLAR/KARŞILAŞILAN GÜÇLÜKLER

Bilgi ve iletişim çağında yer almamızdan kaynakla hayatımızın büyük bir kısmı siber alanda gerçekleşmektedir. Siber alanın aktif olarak kullanmak, bireyleri, şirketleri ve devletleri büyük iş yükünden kurtardığı gibi siber alanın her geçen gün katbekat artarak genişlemesi sınırlarının ve kapasitesinin belirli olmamasına neden olmaktadır. Çalışmamızda karşılaştığımız güçlükler arasında siber alanın anonim olması ve sınırlarının nereye doğru genişlediğinin bilinememesinden kaynaklanmıştır. Bahsettiğimiz zorlukların aşılması için çalışmamızda bireylerin, şirketlerin ve devletlerin ne tür adımlar atması gerektiği ve halihazırda atılan adımlarla birlikte siber alanın nasıl kontrol altında tutulacağı anlatılmıştır.

GİRİŞ

İnsanlık tarihiyle birlikte gelişen güvenlik kavramı, günümüze kadarki olan süreçte çeşitli algı değişiklikleri yaşadığı gibi yapısal olarak da büyük değişiklikler geçirerek günümüze kadar gelmiştir. İlk insanla başlayan avcı toplayıcı toplumlarda yiyecek ve barınmanın korunmasıyla ortaya çıkan güvenlik, daha sonrasında toplulukların can ve mal güvenliklerinin korunmasına evrilmiş ve bu evrilme beraberinde şehir devletlerin kurulmasına yardımcı olmuştur. Toplulukların ortak bir karar almasıyla yetkilerini belirli bir insan topluluğuna veya bir zümreye emanet etmesindeki temel motto, anarşizm ile birlikte oluşan güvenlik sorununun ortadan kaldırılması amacıyla oluşmuştur. Daha sonraki süreçlerde farklı faktörlerinde ortaya çıkması, güvenlik kavramının geri planda kalmasına ve toplumları tehlikeli bir noktaya sürüklemesi sebebiyle 1648 Westphalia Anlaşmasının imzalanmasına ve ulus devletlerin ortaya çıkmasına neden olmuştur. Ulus devletlerin oluşması, güvenlik kavramının pekişmesinde önemli bir konumda olduğu gibi güvenlik kavramının sancılı bir dönem içerisine girmesine de neden olmuştur.

Coğrafyanın geniş alanları kapsaması, bir topluluğun farklı bölgelerde varlığını devam ettirmesi ve bu topluluklarının tekrardan şehir devletçikleri oluşturmasına zemin hazırladığı gibi imparatorlukların parçalanmasında da büyük bir güç olarak karşımıza çıkmıştır. Açıklamak gerekirse, ulus devletleri devlet yapan üç unsur vardır. Bunlar; ülke, millet ve egemenliktir. Öncelikle ülkenin varlığı içinde yaşayan bir milletin var olması gerekmektedir. Ülke ve milletin var olması, egemenlik kavramının doğal olarak ortaya çıkmasına neden olmaktadır. Bir ülkeyi yöneten yönetici kadrolarının öncelikli hedefleri arasında egemenliğinin sağlanması ve bunun içinse güvenliğin tahsis edilmesi öncelikli hedefleri olmuştur. 1800'lü yıllara kadarki olan süreçte güvenlik kavramı sınırların güvenliğinin sağlanması üzerine kuruluyken, sanayi devriminin gerçekleşmesiyle birlikte güvenlik kavramında da ekonomik etkinin artmaya başlamasına neden olmuştur. Özellikle dünyanın küreselleşmeye başlamasıyla birlikte güvenlik kavramının çeşitlilik göstermesine neden olmuş ve devletlerin birden fazla alanda güvenliklerini sağlamaya çalışması öncelikli bir konu olmuştur.

20.yy'ın başlarında teknolojinin gelişmesiyle birlikte devletlerin sömürgecilik faaliyetleri kapsamında elde ettikleri ve kontrol ettikleri ülkelerde toplulukları kontrol etmek ve ulus ayaklanmalarını bastırmak için İnsansız Hava Araçlarını (İHA)

kullanmaya başlamışlar -Britanya kontrolünde olan Mısır'da gerçekleştirilen ayaklanmalarda İngilizler, ayaklanmaları bastırmak ve kontrol altına almak adına tarihteki ilk İHA örneklerini kullanmışlardır- ve bu durum güvenlik kavramının kapsamlı olarak değişmesinin ilk aşaması olmuştur (Satia, 2014). Bu durumun ortaya çıkması güvenlik algısında teknolojik hamlelerin etkisinin büyüklüğünü ortaya koymuştur.

II. Dünya Savaşından sonra ortaya çıkan ve Sovyet Rusya'nın yıkılışına kadarki olan süreçte etkili olan Soğuk Savaş'ın ortaya çıkması güvenlik algılarının tamamen değişmesine neden olmuştur. Uluslararası ilişkilerde yeni bir boyut olan siber alanın oluşması, Soğuk Savaş ile başlamış ve günümüze kadarki olan süreçte kapasitesini katbekat artırmıştır. Siber alanın ilk çalışma alanı askeri faaliyetlerle başladığı zaman sınırlı bir alan içerisinde faaliyet gösterirken 1991'de internet kullanımın tabana yayılmasıyla birlikte sınırları ve kapasitesi belirlenemeyen bir alanın doğmasına neden olmuştur. Sınırlarının belirlenememesi beraberinde fiziki adi suçların siber alanda işlenmesine, istihbarat ve casusluk faaliyetlerinin siber alanda işlenmesine, fiziki savaşların boyut değiştirerek siber saldırılara evrilmesine ve toplumsal olarak psikolojik olarak büyük yıkımların ortaya çıkmasına neden olmuştur. Yukarıda kısaca bahsedilen konular haricinde siber alanın yeteneklerinin, yeni teknolojik gelişmelerle birlikte farklı alanların doğmasına neden olduğu gibi güvenlik açığının da ortaya çıkmasına neden olmaktadır. Yüzyıl önce ulus devletlerin güvenlik parametreleri temelde siyasi, askeri ve ekonomik eksenliyken, bugün ulus devletlerin güvenlik parametrelerine teknolojik gelişmelerde eklenmiştir. Tek bir parametre olarak karşımıza çıksa da teknolojik gelişmeler, siyasi, sosyal, ekonomik, askeri ve toplumsal güvenlik konularında bugün en önemli aktör konumundadır.

Teknolojinin gelişmesiyle birlikte internet ve bilgisayar teknolojileri gelişerek, internetin tabana yayılmasına neden olduğu gibi dünyanın küçük bir köy konumuna gelmesine neden olmuştur. Bu durum büyük yeniliklerin ve fikri genişliklerin ortaya çıkmasına neden olduğu gibi toplumsal ayrışmanın, doğru ve yanlışın ayrımının yapılamamasını, siber savaşların ve siber suçların artmasına neden olmuş ve bu durum bireylere, şirketlere ve devletlere büyük bir maddi ve manevi büyük kayıpların ortaya çıkmasına neden olmuştur.

Dünya barışının sağlanması için devletler çeşitli uluslararası örgütlere üye olmuş ve ortak bir karar almış olmalarına rağmen siber alanın kapasitesinin belirlenememesi ve yeni teknolojik gelişmelerin hızlı entegre edilmesiyle yeni güvenlik sorunlarının doğması sebebiyle siber alanda ortak bir bildiri veyahut karar mekanizması oluşturamamışlardır. Hukuki olarak uluslararası sistem içerisinde siber alanda gerçekleştirilen eylemler ve faaliyetlerin engellenmesi veyahut denetlenmesi için bazı devletler çağrıda bulunmuş olsalar da bu çağrı karşılıksız kalmıştır. Bu çağrının karşılıksız kalmasında en önemli etken ise her devletin siber alanda farklı politikalar yürütmesinden kaynaklanmaktadır. Her devletin siber alanda gerçekleştirdiği eylemlerin farklı olması beraberinde meşru kavramının da çeşitlenmesine neden olduğu gibi için hukuki herhangi bir metnin ortaya çıkmasına engel olmaktadır. Uluslararası arenada ortak bir hukuki metin veyahut düzenleme yapılamazken devletler tamamen alanın boş bırakılmasını engellemek ve vatandaşlarıyla birlikte ülke içerisinde faaliyet gösteren şirketlerin ve kendi varlıklarının güvenliğini sağlamak adına ulusal çapta hukuki düzenlemeler gerçekleştirmektedir.

Bu sebepten dolayı tez çalışmamızın birinci bölümünde, uluslararası ilişkilerde güvenlik kavramının tarihsel olarak incelenerek gelişmeleri ele alınmış ve siber güvenliğe dönüştürülmesi durumunda yapısal ve fikri olarak değişimlerinin nasıl olacağı ele alınmış ve siber alanın tanımlanması ve beraberinde getirdiği güvenlik sorunları detaylıca tanımlanmıştır. İkinci bölümde siber alanda faaliyetlerde bulunan uluslararası örgütlerin ve devletlerin siber güvenliğinin sağlanması adına attıkları adımlar anlatılmıştır. Tezimizin son bölümünde ise siber güvenliğinin önemini ve ciddiyetinin algılanması adına gerçekleşen ulusal ve uluslararası vakalar anlatılmış ve analiz edilmiş ve sonuç kısmında genel bilgiler ve bulgular birlikte değerlendirilerek sonuca bağlanmıştır.

1. KAVRAMSAL OLARAK GÜVENLİK VE SİBER GÜVENLİK

1.1. Uluslararası İlişkilerde Güvenlik Anlayışı

1.1.1. Güvenlik Kavramının Tarihsel Gelişimi

İlk insanın varoluşundan günümüze kadar uzanan insanlığın en önemli problemi güvenlik ve güvenliğin sağlanması konusu olmuştur. İlk insanlarla güvenlik, yırtıcı hayvanlardan korunmak, barınma ihtiyacı ve avcı toplayıcı toplulukların yiyeceklerinin muhafazası üzerine kuruluyken insanlığın gelişimiyle birlikte insan hayatına giren bazı parametreler (mal, değerli madenler, para vb.) güvenlik algısının da çok yönlü olarak düşünülmesine neden olmuştur.

İnsanoğlunun tarihsel serüveninde içerisinde maddi unsurlarda güvenliğin sağlanması için çeşitli faaliyetler yürüttüğü gibi en değerli birikim olan bilginin de güvenliği içinde çeşitli yöntemler geliştirmişlerdir. Antik çağda iletilerinin güvenliğini sağlamak için kölenin saçının kesilip iletinin kafa derisine yazılmasıyla saçlarının uzaması yöntemi kullanılırken, zamanın ve çağın ilerlemesiyle birlikte alıcının iletiyi ısıtmasıyla görünür hale gelen görünmez mürekkepler ortaya çıkmış ve günümüzde de sıkça kullanılan bir iletinin içerisine gizlenen metinler olan stegonagrafi yöntemi kullanılmaktadır. (Beutelspacher, 2021). Bu kelimenin etimolojik incelemesine geçmeden önce özetlemek gerekirse, güvenlik en dar anlamıyla koruma ve savunma, en geniş anlamıyla tehlikeden sakınma ve tehlikeyi önlemeye yönelik tedbirler olarak tanımlanabilir.

Etimolojik olarak Latince se (olmaksızın) ve cura (endişe) kelimelerinin birleşmesinden meydana gelmiş olan (Arends, 2009), ve İngilizcede ‘tasasız, kedersiz’ olarak Latince securitas kelimesinden türemiştir (Kardaş, 2014). Güvenlik kavramı ilk insanların varlığından beri var olduğu için bu süre zarfında kendi içerisinde dönemlere ayrılmıştır. Arends, bu dönemleri Atinalılar dönemi, Romalılar dönemi ve modern ulus devletin kuruluş belgesi olan 1648 Westphalia Anlaşmasıyla başlayan yeni güvenlik anlayışı olarak açıklamıştır (Arends, 2009). Thomas Hobbes’un devlet tanımına baktığımızda, insanları yabancıların saldırılarından ve birbirlerine zarar vermelerinden engelleyebilecek, mutluluk içinde yaşayabilmelerine olanak sağlayacak ve bu düzeni sağlayabilmek adına bütün gücün tek bir kişide olmaksızın bir delegasyona

devredilmesiyle sağlanacağını ifade etmiştir (Hobbes, 2016). Hobbes, burada süper güçlerle donatılmış ve temel hedefi güvenliği sağlaması ve aynı çatı altında barış ve huzurla yaşamayı sağlamak için bir topluluğun kurulması gerekliliğine değinmiştir.

Kaynak: (https://www.britannica.com/event/Peace-of-Westphalia)(E.T. 06.01.2023).

Şekil 1: Gerard Terborc Tarafından Resmedilen Vestfalya Barışı'nın Çözümünü Tasvir Eden Yağlı Boya Eserleri

1648 Westphalia Anlaşması ile modern ulus devletlerin kurulmasıyla birlikte, güvenlik konusu güç, diplomasi, taktik ve strateji gibi konuları içeren geniş bir yelpaze haline geldi. Güç unsuru uluslararası ilişkiler alanında öne çıkan temalardan biri olmasına rağmen güvenlik unsuru ile ele alındığında iki kavramın birbirini tamamladığı görülmektedir. Güç kavramı, uluslararası ilişkiler kuramında birden farklı şekilde tanımlanmış, araç mı amaç mı olduğu sorusu disiplini meşgul etmesine rağmen gücün ortaya çıkmasının temelinde güvenlik konusu yer almıştır. Modern hukukun kurucu babası olarak bilinen ve doğal hukuk öğretisiyle ün kazanmış olan Hugo Grotius, Savaş ve Barış Hukuku kitabında, kişi can güvenliğini sağlamak ve korumak için gücün en etkili unsuru olan savaş unsurunu kullanabileceği ve bu kullanımın temel dayanağı olarak kişinin kendini savunma hakkının doğrudan doğanın herkesi kendisini korumakla görevlendirdiğini belirterek açıklamıştır (Grotius, 2011).

Güç unsurunu elinde ister birey, elinde tutsun, kendini güvenli bir düzeye kadar savunmuştur. Gücün elinde bulunması güvenliğe yaklaşımın da değişmesine neden olduğu gibi uluslararası ilişkilerdeki temek kuramların ortaya çıkmasına ve her birinin farklı yorumlanmasına da neden olmuştur. Öyle ki günümüzde devletler ve hatta

bireyler, 20 yılı aşkın bir süredir hayatımızda önemli bir yer işgal eden yumuşak güç kavramını bilerek veya bilmeyerek, kendi veya çevrenin çevresinin güvenliğini sağlamak ve korumak amacıyla kullanmaktadır. Basitçe anlatacak olursak yumuşak güç; askeri faktörleri içermeyen fakat siyasi, sosyal, ekonomik ve kültürel unsurları etkileyen bir güç olarak tanımlanabilir (Vuving, 2009).

Uluslararası toplumu yakından ilgilendiren güvenlik kavramı, 1789 Fransız Devrimi'nden sonra Yurttaş Hakları Bildirgesinde güvenliğin temel insan hakkı olduğunu belirtmesiyle girmiş daha sonrasında güvenlik kavramı Milletler Cemiyeti ve Birleşmiş Milletler şartında da yer alarak hukuki statüsünü tamamlamıştır (Kardaş, 2014). I. ve II. Dünya Savaşı arasındaki ve sonrasındaki uluslararası ilişkilere ilişkin ana tartışmalar, güvenlik konusuna çokça kafa yormuştur. Uluslararası ilişkiler disiplininde ise kuramsal açıdan ilk kez kullanılması ise 1952 yılında Arnold Wolfers'in National Security as an Ambiguous Symbol isimli makalesinde güvenliğin objektif ve sübjektif durumlarını ele almıştır. Wolfers'in kavramsallaştırmasına göre güvenlik kazanılmış olan değerlere karşı bir tehdidin oluşmaması (Tanrısever, 2011) hali olduğu gibi Wolfers makalesinde Fransa'nın I. Dünya Savaşındaki tutumundan örnek vererek kimilerinin algıladıkları tehdide karşı mütevazı ve daha yumuşak tepki verirken kimileri ise algıladıkları tehdide karşı sert ve doğrusal olmayan şekilde tepki vermektedir (Wolfers, 1952). Artık günümüz devletlerin ve bireylerin güvenlik yaklaşımı Soğuk Savaş dönemi öncesi gibi tek bir tehdit unsuru olmamakla birlikte günümüzde farklılık ve çeşitlilik göstermektedir (Köker, 2021). Şu an devlet ekosisteminde güvenlik algısının nasıl algılandığını anlayabilmek için uluslararası ilişkilerin temel tartışmalarında güvenlik konusuna bakmamız önemli olacaktır.

1.2. Güvenliğe İlişkin Temel Yaklaşımlar

1.2.1. Realist Güvenlik Anlayışı ve Siber Güvenlik Alanında İncelenmesi

Realizm, uluslararası ilişkiler alanında bilgiye bilimsel ve pozitivist bir bakış açısıyla bakmayı savunan ve uluslararası ilişkiler disiplininin en temel teoridir (Balcı ve Kardaş, 2014). Realizmin temel argümanı ise siyasi düzen ve güvenlik arasındaki bağlantıyı açıklamak üzerine kuruludur (Wolforth, 2009). I. Dünya Savaşı gibi yıkıcı bir savaşın tekrar ortaya çıkmasına engellemek ve dünya barışını korumak için yeni fikirler

ortaya atmış ve bu fikirleriyle idealist düşünce yapısına bir eleştiri getirerek uluslararası ilişkiler disiplininde yer almıştır. (Baştuğ, 2022).

Uluslararası İlişkiler disiplinin ortaya çıktığı I. Dünya Savaşı zamanında ve savaş sonrasında dünya siyasetini en çok ilgilendiren mesele güvenlik konusu olmuştur. Siyasal gerçekçiliğin güvenlik anlayışını ele aldığımızda, bu alanda çalışan akademisyenler temelde güvenlik sorununa bilimsel bir çözüm önerisi getirmek isteseler de daha çok I. Dünya Savaşından sonra ortaya çıkan güvenlik sorunlarının nasıl çözüleceği üzerine çalışmışlardır (Tanrısever, 2011).

Klasik realist kuramda güvenlik kavramı temel belirleyici faktör olduğu gibi devletin gücü, güvenliği sağlama kapasitesiyle birlikte değerlendirildiği gibi birbirini tamamlayan faktörlerdir (Darıcılı, 2017). Realist düşünceye göre güç kavramı kısa caddeli ve uzun vadeli olmak üzere ikiye ayrılmaktadır. Uzun vadeli güç, GSYİH (Gayri Safi Yurt İçi Hasıla), nüfus, toprak, coğrafya ve doğal kaynaklar olarak sıralanırken kısa vadeli güç unsurunda askeri, ekonomik güç, diplomatik beceriler ve ahlaki meşruiyet olarak sıralanabilmektedir (Goldstein ve Pevehouse, 2015). Realistlerin güç kavramına gereğinden fazla önem vermesinin arkasında uluslararası sistemin anarşik bir yapı içerisinde olmasından dolayı hayatta kalmak için gücün bir araç olarak kullanılması gerektiğine inanırlar. Bu bağlamda realistler bir devletin gücüne karşı yine diğer başka devletlerin gücüyle karşı koyulabileceğini savunurlar (Goldstein ve Pevehouse, 2015). Bu bağlamda, uluslararası örgütlerin kurulması ve güçler birliğinin oluşturularak ortak çıkarlar ekseninde diğer güç unsurlarına müdahale etme kabiliyeti veya gözdağı verme kabileyi kazandırılmıştır (Goldstein ve Pevehouse, 2015).

Realist kuram ile siber alan doğası gereği birbirine çok benzemektedir. Realist kuram uluslararası sistemin anarşik yapısından bahsederken, 1990'da internetin ortaya çıkmasıyla birlikte sürekli büyün ve gelişen siber alanda anarşik yapıya sahip olmuş ve kontrol edilemez bir güç unsuru olarak bugün denklemlerde yerini almaktadır. Siber alanda faaliyet gösteren bir devlet, askeri güç unsurunu koruyarak askeri güç ile elde edemeyeceği sonuçları alabileceğini keşfettiğinde siber alan büyük bir cazibe merkezi olarak görmeye başlamıştır. Bir örnek ile açıklamak gerekirse, 2010 yılında İran'ın nükleer çalışmalarını sekteye uğratmak için gerçekleştirilen Stuxnet saldırısı, İran'ın nükleer santrallerine büyük zarar vermiştir. İran'ın iddiasına göre saldırının arkasında büyük ve küçük şeytan olarak adlandırdığı ABD ve İsrail bulunduğunu iddia ederken

taraflar bu iddiayı asılsız olarak ilan etmişlerdir. Sonuç olarak askeri güç kapsamında gerçekleştirilmesi çok güç olan hareket siber alanda kısa sürede ve etkili şekilde gerçekleştirilmiştir. Bu durumdan kaynaklı siber alan yeni bir güç alanı konumuna gelmiştir.

Siber alanda gerçekleştirilen saldırılar sonrasında devletler, güç dengesini koruyabilmek için ulusal olarak bir dizi önlem alma girişiminde bulunmuş olsalar da uluslararası manada tek bir hukuki metin oluşturamamışlardır. Uluslararası arenada siber alanın kontrol edilmesine yönelik girişimler olmuş olsa da soğuk savaştan kalma kutuplaşma nedeniyle devletler temkinli yaklaşmaktadırlar. Örneğin, Brezilya 2009'da BM Genel Kurulu nezdinde siber savaşlarda bilgi ve telekomünikasyon silahlarının kullanılmasında davranış kanunun oluşturulması için öneri sunarken daimî üyelerden ABD, İngiltere ve Fransa bu duruma karşı çıkarken Rusya ve Çin uygun görmüştür (Türkay, 2013). ABD ve İngiltere'nin karşı çıkmasındaki olay siber uzayın denetlenmesinin engellenmesi ve kendi çıkarlarını engelleyecek bir durum olarak görmelerinden kaynaklanırken Fransa, ulusal hedeflerine ulaşabilmek için siber savaşın meşru olduğunu kabul etmektedir (Hildreth, 2001).

1.2.2. Liberal Güvenlik Anlayışı ve Siber Güvenlik Alanında İncelenmesi

Liberal kelimesi etimolojik olarak doğuştan özgür insana uygun olan liberalis kelimesinden gelmektedir (Zenginkuzucu, 2020). Liberalizm düşüncesi daha çok siyasi ve ekonomik düşünce açısından 18 ve 19.yy. arasında etkili olan düşünce, kendisini bulmak için ABD ve İngiltere doğal yayılma sahası olmuştur (Yorulmaz, 2020). Liberalizmin temelinde bireyin güvenliğinin, özgürlüğünün sağlanması ve korunması, mülkiyet hakkı ve eşitlik gibi temel kavramlar oluştururken bu kavramların korunmasını ve denetlenmesini sağlayacak olan temel aktör olarak devleti görmektedir (Yorulmaz, 2020; Sandıklı ve Emeklier, 2012). Hakların korunması ve güvenliğin sağlanması adına yetkili tek organı devlet olarak gördüğü gibi devlet dışı aktörlerin de (uluslararası kurumlar, çokuluslu şirketler, sivil toplum kuruluşları, bireyler, vd.) bu süreçte analiz birimi olarak incelenmesi gerekliliğini savunmaktadır (Sandıklı ve Emeklier, 2012).

Liberal görüş, uluslararası ilişkilerde güç kullanımından ziyade karşılıklı ilişkilere, küresel etkileşimlerin genişlemesine ve karmaşıklaşmaları üzerine eğilirler ve bu eğilim güvenlik ile özgürlüğün dengeli şekilde ilerlemesini sağlamaktır (Zenginkuzucu, 2020). Bu bağlamda liberal düşüncenin temeli olan karşılıklı bağımlılık olması durumunda devletler arasında iki yönlü siyasal ve ekonomik bağımlılık savaşların engellenmesi için önemli olduğu gibi güvenliğin sağlanmasında da önemli bir faktör olacaktır (Goldstein ve Pevehouse, 2015). Liberal görüş, temel hak ve hürriyetlerin korunması, hürriyetin korunması ve mülkiyet haklarının korunması ile devletlerle birlikte geliştirilecek siyasal ve ticari faaliyetler ile savaşlar engellenebilir ve uluslararası güvenliğin sağlanabileceğini belirtmiştir.

Siber güvenliğinde tam olarak sağlanması için gerekli olan siyasal ve ekonomik ilişkilerin sağlam temeller üzerinde kurulması ve karşılıklı bağımlılık ile oluşabileceğidir. Ancak liberal görüşte ifade edilen özgürlük kavramı siber alanda karşılığı net olarak belirlenememektedir. Kullanıcılar siber alanı iradeleri doğrultusunda kullanabildikleri gibi bazı devletler siber alanın kullanılmasını kısıtlayacak eylemlerde de bulunabilmektedirler. Siber güvenliği liberal düşünce ekseninde inceleyip genel bir çözüm yolu üretecek olursak eğer, mevcut uluslararası güvenliği koruyan BM bünyesinde siber alanın denetimini her devlete eşit oy hakkı vererek gerçekleştirilebileceği gibi ayrıca bireylerin özgürlüklerini garantiye alan ve bununla birlikte uluslararası şirketlerinde güvenliklerini siber alanda garantiye alan bütün devletlerin ortak katılımıyla uluslararası bir anlaşma yapılması gerektiği sonucuna varılabilir.

1.2.3. İngiliz Ekolü Güvenlik Anlayışı ve Siber Güvenlik Alanında İncelenmesi

İngiliz okulu uluslararası ilişkiler disiplininde realizm, akılcılık ve devrimcilik gibi birden fazla kuramı bünyesinde barındırmasından kaynaklı olarak çok zengin bir temele dayanmakta ve bu üç farklı kuramı tek bir çatı altında birleştirmesinden kaynaklı çok zengin bir birikime sahiptir (Devlen ve Özdamar, 2010). 1950 ve 1970 yılları arasında İngiltere'de aralarında Herbert Butterfield, Martin Wight, Hedley Bull ve Adam Watson gibi bir grup akademisyen tarafından uluslararası ilişkilerdeki radikalizm ve realizm düşüncelerine bağlı olarak gelişmemiş ve yeni bir kavram olan uluslararası

toplum kavramını geliştirmişler bu kavram ile düşüncelerini açıklamışlardır (Ağkaya, 2016). Uluslararası toplum kavramı ile İngiliz Ekolü, realist bakış açısında bulunan katı uluslararası anarşi fikrini reddederek, uluslararası ilişkilerin ontolojisinin uluslararası sistemin ötesinde bir uluslararası toplumu oluşturmasını savunmaktadır (Devlen ve Özdamar, 2010; Ağkaya, 2016).

İngiliz ekolünün temel amacı, devletlerin bağımsızlıklarını ve toplumun temel değerlerini korumaktır (Bilgiç, 2011). İngiliz ekolü yaklaşımında güvenlik kavramını da net bir şekilde tanımlanmıştır. Özellikle I. Dünya Savaşından sonra kurulan ve II. Dünya Savaşı'nın başlamasıyla başarısızlığı kabul edilen Milletler Cemiyeti'nin ortadan kalkması ve II. Dünya Savaşı sonrası kurulan Birleşmiş Milletler'in yapısal sıkıntılarından sonra İngiliz Ekolü de güvenlik kavramının tam mana ile oluşabilmesi için öncelikli olarak düzenin oluşturulması ve bu düzenin oluşabilmesi için de devletlerin ortak değerler ve prensipler üzerine çalışmaları gerektiğini savunmaktadır (Bilgiç, 2011).

İngiliz ekolünün uluslararası ilişkiler disiplini açısından bakıldığı zaman sağlam üç temel üzerinden şekillendiği görülmektedir. Oluşturulan ortak değerlerin oluşturulması, savaşların engellenmesi için ortak alanların oluşturulması ve devletlerin egemenlik haklarına yönelik saldırıların engellenmesi gibi önlemler üzerine çalışmaları, İngiliz ekolü mantığının siber alana entegrasyonunun gerçekleşmesi halinde büyük değişimlerin olması kuvvetle muhtemeldir. Siber alan ile uluslararası ilişkiler disiplinlerinin ortak noktalarının olmasından dolayı uluslararası ilişkiler disiplinde kullanılan kuramların siber alana entegre edilme fikri de siber alanın anarşik yapısının kontrol edilebilmesi ve egemenliklerine yönelik saldırıların engellenmesi adına önemli bir entegrasyon olacaktır. Bu bağlamda yapılması gereken öncelikli olarak internetin BM kurumu bünyesinde -Güvenlik Konseyi'nin tekelinde olmamak kaydıyla- denetlenmesini sağlayacak bir yapının oluşturulması gerekmektedir. Oluşturulacak olan bu yapı siber alanın diğer devletlere karşı bireysel veya topyekûn saldırıları engellemek ve uluslararası denetimin sağlanması açısından faydalı olacaktır.

1.2.4. Kopenhag Ekolü Güvenlik Anlayışı ve Siber Güvenlik Alanında İncelenmesi

II. Dünya Savaşı'nın sona ermesiyle birlikte güvenlik kavramı yapısal bir değişime uğramaya başlamıştır. Kavramın yapısal değişikliğe uğramasında Soğuk Savaş'ın iki kutuplu bir dünya yaratması etkili olmuştur. Soğuk Savaş döneminde kutup devletleri arasında artan nükleer tehdit krizi sebebiyle askeri odaklı bir güvenlik çalışmaları yaygınken yine Soğuk Savaş döneminin ürünü olan siber uzayın oluşturulması gibi Soğuk Savaş sonrası güvenlik paradigmaları salt asgari çalışmaların dışına çıkarak askeri olmayan çalışmalar -kimlik, kadın, çevre, yoksulluk, ekonomik istikrarsızlık, salgın hastalıkla ve en önemlisi siber alan- da dahil edilmeye başlanmıştır (Baran ve Macar, 2017). Dar bir güvenlik algısından çok küreselleşme ile kavramı etkileyecek olan farklı konuları da kavram içerisine koymaları iki kutup arasındaki gerilimin azalmaya başlaması sonrası dile getirilmeye başlandığı gibi daha sonrasından Soğuk Savaşın sona ermesi ile konular çeşitlenerek güvenlik kavramına dahil edilmişlerdir (Akgül Açıkmeşe, 2011).

Salt askeri eksende şekillenen güvenlik kavramının Soğuk Savaş sonrası Kopenhag Ekolünün varlığıyla çeşitliliği artmış ve askeri faaliyetlerden hariç farklı konular da güvenlik kavramını şekillendirmeye başlamıştır. Kopenhag okulunun temelleri 1985'te Kopenhag Üniversitesi içerisinde Barış ve Çatışma Araştırma Merkezi'nin Avrupa Güvenliğinin Askeri-Olmayan Boyutları başlıklı projesinin hayata geçirilmesiyle birlikte, başta Barry Buzan ve Ole Wæver gibi güçlü bir grup akademisyenlerin bir araya gelmesiyle temelleri atılmıştır (Akgül Açıkmeşe, 2011). Kopenhag ekolünün ortaya çıkması mevcut konjonktüre bir üçüncü yol olarak ortaya çıkmıştır. Güvenlik kavramı şekillenirken ekseriyetle kuvvet kullanımı veya kullanım tehdidi ekseninde şekillenirken Kopenhag Ekolü devlet dışı aktörlerin de eklenmesi gerekliliğini vurgulamış ve geleneksel kalıpların dışına çıkmıştır. Kopenhag Ekolünün bir güvenlik projesi olarak ortaya çıkmasında Avrupa'yı güvenlik ekseninde birleştirmek ve askeri yöntemlere başvurmadan da barışın korunabileceği ve olası saldırganların da caydırılabileceği fikrini anlatmak için ortaya çıkmıştır (Bilgin, 2010). Bunun yanı sıra barışın korunabilmesi adına yeni güvenlik sistemi inşasında güvenliğin özünü inceleyecek bir süreç analiz çerçevesi oluşturmuştur (Schroeder, vd., 2009).

Kopenhag Ekolü ile literatüre giren güvenlikleştirme modeli, referans alınan konuya yönelik doğuştan gelen tehdit gibi her şeyi ele almak ve bu tehditler ile başa çıkmak adına acil ve istisnai önlemlerin alınarak siyasal topluluklar içerisinde yeni bir anlayışın inşası olarak kavramsallaşmış (Aydındağ, 2021), referans konunun güvenlikleştirme sürecini betimleme sürecinde ise siyasallaştırılmış, siyasallaştırılmamış ve güvenlikleştirilmiş olarak üç ana kategoride değerlendirilir (Schroeder, vd., 2009). Genel olarak güvenlikleştirmeyi anlatmak gerekirse, geleneksel realist bakış açısında var olan söylemsel yaklaşımlara ve aşırı dar görüşlere karşı çıkarak güvenliği genel ve daha geniş bakış açısıyla her yönüyle incelenmesi gerektiğini savunmaktadır (Nissenbaum, 2005). Bu sebepten dolayı siber alanın yapısı ve düşünüldüğünde realist temeller ekseninde siber güvenliğin sağlanması mümkün olmayacağı için Kopenhag Ekolünün yaklaşımı daha uygun olmaktadır.

Kopenhag Ekolünün temellerinin 1985'te ortaya atılması ve 1990'larda aktif şekilde çalışması elbette internetin tarihi ile paralel şekilde ilerlemesinden kaynaklı olarak güvenlik kavramı içerisine koymamız mümkün olacaktır. Bugün siber alan ve internet teknolojisi bir Soğuk Savaş ürünü ve ABD ekseninde askeri amaçla oluşturulmuş olsa da uluslar üstü ve bağımsız bir yapıya sahiptir. Siber alanda gerçekleştirilen kötü amaçlı faaliyetler bireyleri, şirketleri ve devletleri tehdit ettiği için siber güvenlik kavramının önemini bir kez daha hatırlatmaktadır. Kopenhag Ekolünün anlayışı bugün siber güvenliğin anlamlandırılmasında büyük etkiye sahiptir. Siber alanda gerçekleştirilen saldırıları ve savaşları sadece devletler başlatmamakla birlikte uluslararası şirketler kendi çıkar ve politikaları içinde gerçekleştirdiği gibi bir grup kullanıcı veyahut farklı düşüncede bulunan bir grup kullanıcı da devletlere veya şirketlere de saldırı başlatabilmektedir. Bu tarz saldırıların maliyetlerinin düşük olması ve riskinin az olmasından dolayı tercih edildiği gibi sonuçlarının çok büyük olması ve hedefe büyük miktarda ekonomik zarar vermelerinden dolayı da tercih edilmektedir.

Kopenhag Ekolünün güvenlik anlayışını siber güvenliğe entegre edecek olursak, öncelikli olarak siber alanda sadece devletleri bir aktör olarak görmekten vazgeçip devlet dışı aktörlerin de varlıklarını kabul etmemiz gerekmektedir. Nissenbaum'un da makalesinde bahsettiği gibi siber güvenliğe yönelik tehditler hükümet, özel sektör ve medya olarak üç ana kategoriden oluşmaktadır (Nissenbaum, 2005). Bu bağlamda siber alanın güvenlikleştirilmesi için öncelikle tehdidin kime yönelik (devlet, hükümet, şirketler, devlet dışı aktörler vd.) olduğunun belirlenmesi ve belirlenen kitleye yönelik

güçlü ve çeşitli araçlar kullanılarak ikna edilmesi gerekmektedir (Kassab, 2013). Fiziki dünyada gerçekleştirilen güvenlikleştirme faaliyetleri için çeşitli unsur ve araçlar kullanılırken siber alanın güvenlikleştirilmesi içinde benzer araçlar kullanılsa da bu araçlar ekseriyetle belirli olmayan ve gözle görülmeyen/hissedilmeyen unsurlar olmaktadır. Bu bağlamda kullanılan araçlar içerisinde en önemlileri ise internet, sosyal medya ve hacker grupları olmaktadır.

1.2.5. Küreselleşme ve Siber Güvenlik

Küresel kelimesi literatürde yaklaşık 400 yıldır kullanılmasına rağmen, küreselleşme kavramı 1960'larda literatürümüze girmiş ve 1980 itibariyle sıkça uluslararası ilişkiler disiplini de dâhil olmak üzere sıkça kullanılmaya başlanmıştır (İçli, 2001). Yeni bir kavram olmadığı gibi günümüze kadar uzanan süreçte küreselleşme, farklı topluluklar arasında üç dönem içerisinde gelişmiştir. Küreselleşme, 1800'lerden 1914'e kadar olan süreç birinci dönem, 1914'ten 1945 ile 1950'lere kadar olan süreç ikinci dönem ve son olarak 1945 ile 1950'den sonra günümüze kadar gelen dönem olarak sıralanmaktadır (Bayar, 2008). 1945'lerden günümüze kadar uzanan süreçte Marshall McLuhan'ın 1962'de The Gutenberg Galaxy: The Making of Typographic Man makalesinde bahsettiği Global Willage (Küresel Köy) kavramını ortaya atmasıyla küreselleşme kavramı bir bütünlük kazandığı gibi McLuhan literatürde "20.yüzyılın en büyük medya teorisyeni" veya "siber uzayın babası" olarak tanınmaya başlamıştır (Atalay, 2018).

Küreselleşme kavramı, bütün toplumları etkileyen büyük gelişmeler (teknolojik gelişmeler, savaşlar, uluslararası ticari ilişkiler, sosyolojik değişimler, vd.) gelişmesinde ve değişmesinde etkili olmuştur. Bayar'ın makalesinde bahsettiği küreselleşmenin dönemlerinde son dönemin tarihsel olarak büyük bir aralığı kapsaması, küreselleşmenin yeni bir dönemi daha olup olmadığı sorusunun sorulmasına neden olmaktadır. Bu noktada McLuhan'ın ortaya attığı küresel köy kavramı, yeni bir boyutun açılmasında etkili olabileceği muhtemeldir. Öyle ki McLuhan makalesini 1962'de yayınladığı sırada, internet teknolojisi daha askeri amaçlı ve soğuk savaş eseri olarak yeni yeni gelişirken bahsettiği konuların büyüklüğü 21.yy'ın ilk çeyreğine işaret etmektedir. Bu durumu örnekle açıklayacak olursak, McLuhan 1962'de internetin ve hatta işleyiş kapsamı

bakımından Facebook'un (yeni ismi ile Meta) kurulacağını öncesinden yazdığı makalede haberini vermiştir (Atalay, 2018).

21.yy. ile internet ve bilgisayar teknolojilerinin gelişerek temelde askeri amaçla başlayıp zamanla tabana yayılmasıyla birlikte kullanıcılar arasındaki ilişkiler daha çok geliştiği gibi dünyanın farklı noktalarında bulunan kullanıcılar arasındaki etkileşim oranı da artmaya başlamıştır. Bu durum siber uzayın oluşması ve sürekli olarak kendi kapasitesini katlayarak genişlemesine neden olmuştur. İnternetin yaygın kullanılması sonucunda toplumlar arasındaki kültürel etkileşim çok daha hızlı ve etkili olmaya başlamış ve bu durum beraberinde dünyanın küçük bir köy haline gelmesine neden olmuştur. Siber alanın oluşması, küreselleşmenin bir ürünü olarak ortaya çıkmasına neden olduğu gibi bugün siber alan küreselleşmenin daha farklı bir boyut kazanmasına da neden olmuştur.

İnternetin yaygınlaşması ve kullanıcı sayısının her geçen gün artmasıyla birlikte siber alanın kapasitesi genişlemiş ve dünya tek bir tık haline gelmiştir. Bu durum 21.yy'ın ilk çeyreğinden sonra nesnelere kadar ilerlemiş ve IoT teknolojisinin ortaya çıkmasına ve yeni ortaya çıkan teknolojik gelişmeyle evlerimizde bulunan diğer elektronik eşyalar da kendi aralarında aktif şekilde haberleşmesine neden olmuştur. Bu durum kullanıcıların sosyal ve kişisel hayatlarında olumlu bir gelişme olarak görülse de beraberinde siber suçların ortaya çıkmasına neden olduğu gibi siber alanda gerçekleştirilen kötü amaçlı eylemlere de kapı aralamaktadır.

Küreselleşmenin üçüncü döneminde yer alsak da 1991 küreselleşme için yeni bir boyut olarak değerlendirilebilir. İnternet her ne kadar askeri amaç için kullanılmak üzere tasarlanmış olsa da 1991'de www'in ortaya çıkması yeni bir dönem olarak yorumlanmaktadır. Www'in ortaya çıkması ve dünyanın her bir köşesini fiber optik kablolar ile fiziki şekilde bağlanması dünyanın küçük bir köy haline gelmesine neden olduğu gibi küreselleşmenin daha hızlı gerçekleşmesine neden olmuştur. 1991 öncesine bakacak olursak eğer küreselleşme ve kültürler arası etkileşim daha çok radyo, televizyon, telefon ve ticari ilişkiler üzerine kuruluyken 1991 sonrasında internetin askeri amaç doğrultusundan çıkıp tabana yayılmasına neden olmuştur. Tabana doğru bu yayılım internetin şirketlerin dünya genelinde ofis, üretim ve dağıtım sistemlerini birbirine bağlayan ve hızlı ve etkili iletişim kurmalarına olanak sağlayan özel bir ağ haline gelmesine neden olmuştur (Kitchin, 1998).

Küreselleşmenin bir ürünü olarak internet hızla gelişmekte olduğu gibi siber alanda kapasitesinin sınırsız olduğunu kanıtlamaktadır. Siber alanın kapasitesinin sınırlarının olmadığını bireyler metaverse dünyaları ile tekrardan hatırlamıştır. Temel olarak 1992'de edebi bir romanda fikir olarak atılan paralel evren 2020 itibariyle daha çok duyulur hale gelmiş ve 2021 itibariyle dünyaca ünlü sosyal medya, sağlık, eğitim, gayrimenkul ve teknoloji şirketleri meta verse dünyaları inşa etmek için siber alana yatırımlar yapmaya başlamıştır. Siber alanın kapasitesinin belirsizliğinin anlaşılması adına güzel bir örnek olan meta verse dünyaları, fiziki dünyanın kopyalanarak siber alanda yeni bir yaşam alanı inşa edilmesi olarak tanımlanabilir. Sanal alanda yenilikçi bir dünyanın oluşturulması ve bu dünya oluşturulurken temel mottonun fiziki dünyanın kopyası olarak tanıtılması siber alanın devasa boyutunu ve sınırlarının belirsizliğini bizlere kanıtlamaktadır.

Küreselleşme ile yeniliklerin ortaya çıkması, özelde kullanıcılara ve genelde devletlere, kurum ve kuruluşlara ve şirketlere büyük bir refah alanı sağladığı gibi ortaya çıkan sorunlarında büyük olmasına neden olmaktadır. Ortaya çıkan sorunlar, siber adi suçlar, siber istihbarat ve casusluk eylemleri ve siber zorbalık eylemleri olarak sıralanabilir. Ortaya konulan bu eylemler bütünüyle siber güvenliğin ana bileşenlerini oluşturmaktadır. Siber güvenlik kavramı temelde bireylerden başlayarak devletlere kadar uzanan geniş bir konu olarak gündemden düşmemektedir. Siber güvenliğin açık vermesinde eğitimsizlik ve farkındalığın olmamasından kaynaklı olduğu gibi siber alanın zayıf halkasının insan faktörü olmasından dolayı sıkça gündemde durmaktadır. Siber güvenlikte insan faktörünün zayıf halka olmasında ise üç ana tez öne sürülmektedir. İlk olarak siber alanda gerçekleştirilen iletişimin geleneksel iletişim biçimlerinden farklı olması ve yeni siber iletişimi kullanıcıların bir meydan okuma olarak görmesi, öne sürülen ikinci tezde ise sanal ortam ile reel ortam arasındaki ikiliklerden faydalanma ise ve son olarak öne sürülen üçüncü tezde ise siber alanın coğrafi alanlardan yoksun ve coğrafi alanların niteliklerinden yoksun yeni bir sosyal alan yaratmasından kaynaklanmaktadır (Kitchin, 1998). Bu sebeplerden dolayı insan faktörü siber güvenlikte her zaman için zayıf halka olarak bulunmaktadır.

Siber güvenliğin sağlanması için öncelikli olarak insan faktörünün donanımsal olarak yetiştirilmesi ve bilgilendirilmesi gerekmektedir. Bunun için öncelikli olarak eğitimin aileden başlaması gerekmektedir. Ailenin bilinçli hareketi yeni bireylerin gelişimini etkileyeceği gibi bu eğitim ve donanımsal yetiştirilmesi okullara zorunlu

olarak verilmeli ve siber güvenlik ders olarak anlatılması gerekmektedir. Bugün birçok devlet siber güvenlik politikalarını belirlerken devlet odaklı düşünmekten çok birey odaklı düşünerek bireylerin siber güvenlik alanında bilinçlenmesi üzerine politikaları yürütmektedir. Kısa bir örnek ile açıklayacak olursak Güneydoğu Asya ülkeleri arasında önemli bir konumda bulunan Singapur, küresel şehir devleti olmak adına siber güvenlik politikalarına ciddi önem göstermiş ve bu kapsamda dönemin başbakanı Lee Hsien Loong, Akıllı Ulus Girişiminde yaptığı konuşmayla devletlerinin üstüne düşeceği görevleri yapacakları gibi vatandaşlarının da bu alanda kendilerini geliştirmesi adına kamu kurum ve kuruluşlardan yardım almaları gerektiğini belirtmiş ve siber güvenlik alanında kalifiye elemanların yetiştirilmesi için yeni kurum ve kuruluşların varlığını tekrardan hatırlatmıştır (Baştuğ, 2022; Prime Minister's Office, 2014; Teh, vd., 2020).

Siber güvenliğin zayıf halkası olan insan faktörünün eksiklerinin giderilmesi siber suçların engellenmesi adına büyük bir girişim olduğu kadar diğer kamu kurum ve kuruluşlarıyla birlikte şirketlerinde yapısal değişikliklere giderek güvenliklerini yeni teknolojik gelişmeler ışığında değiştirmelidir. Günümüzde bu değişim kaçınılmaz bir durum olmasından dolayı devletler ve şirketler geç de olsa siber güvenlik alanında yapısal değişikliklere yönelmiştir. Devletlerin siber güvenlik alanında yapısal değişikliklere gitmesinde bazı önemli olaylar etkili olmuştur. Siber alanda devletler istihbarat ve casusluk faaliyetlerini maliyetsiz olmasından ve takip edilemez bir alan olmasından dolayı seçtikleri gibi siber savaşlardan da etkilenmemek adına yapısal değişiklikler yapmak kaçınılmaz olmuştur. Özellikle de 2007'de gerçekleştirilen Estonya saldırısı ve 2010'da İran'a yönelik gerçekleştirilen Stuxnet saldırısı siber güvenliğin önemini devletler için önemli bir parametre olarak görmektedirler.

1.3. Siber Uzay ve Siber Güvenlik

1.3.1. Siber Nedir?

Siber, bilgisayar ve bilgisayar ağlarını içeren ve bu kavramları içerisine alarak açıklamaya çalışan (Köker, 2021), Oxford sözlüğüne göre ise sanal gerçeklik, bilgi teknolojileri ve bilgisayarlarla ilgili anlamına gelmektedir (Akyeşilmen, 2018). Kısacası son çeyrek yüzyılda hayatımıza girmiş olan siber kelimesi, bilgisayar ve internet ile alakalı her şeyi açıklamak için kullanılan bir kelimedir. Siber kavramı yukarıda

bahsedildiği anlamlara gelmekle birlikte kavramı ilk olarak Norbert Wiener'in 1948'de yayınlanan cybernetics adlı romanıyla literatürümüze girmiştir. Wiener, cybernetics romanında kavramı hayvanda ve makinede kontrol ve iletişim olarak tanımlamıştır (Ottis ve Lorents, 2010).

İnsanların gelişen teknoloji içerisinde makineleri uzaktan kontrol etme isteği, insansız savunma ve sanayinin gelişmesi ve az maliyet fazla kâr hesaplamalarından dolayı siber kavramı ilk başlarda otomasyon üzerine kurulmuş olup daha sonrasında makinelerin insanlar gibi karar vermelerini sağlayabilmek için arayüz geliştirilmesiyle hızlı yükseliş evresine girmiştir. Bugün hayatımızda çok önemli bir kavram olan siber kelimesi literatüre bilimsel bir kavram olarak değil de edebiyat yoluyla bilim literatürüne girmiştir. Bu durum bazı tartışmaları beraberinde getirmiştir. Zamanın şartları ve teknolojik altyapının varlığı da göz önünde bulundurulacak olursa kavramın ütopik olması tartışmanın bir ucunu oluşturmaktadır. Fakat 21.yy. ile günümüzde siber kelimesi artık hayatımızın vazgeçilmez bir kelimesi olarak karşımıza çıkmasına rağmen tartışmalar şiddetini daha da artırmıştır. Fakat bu kez tartışmalar siber kelimesinin ütopik bulunmasından değil de kelime anlamının daha da genişletilmesi üzerine olmuştur.

1.3.2. Siber Uzay Nedir?

Siber uzay kavramı ilk defa William Gibson'ın 1984'te yazmış olduğu Neuromancer isimli bilimkurgu romanında kullanılmıştır (Kitchin, 1998). Etimolojik olarak Siberuzay -cyberspace- kavramını, siber ve uzay kavramlarının birleşmesiyle meydana gelmiştir (Türkay, 2013). Burada önemli bir kavram olarak siber kelimesinin yanına uzay kavramının eklenmesi aslında siber kelimesinin zaman içerisinde kalıbına sığmayan bir hareket sergilemesinden kaynaklanmıştır. Peki, neden siber kelimesinin yanına uzay kavramı eklendi? Uzay kavramı sonsuz olduğu düşünülen fakat sonsuz olduğu konusunda kesin bir kanıya varılamayan bir alan olmasından dolayı ve küreselleşmenin etkisiyle birlikte bilgisayarların hayatımızda daha fazla hissedilir olmasıyla birlikte siber kelimesinin de bahsedilen tanımlamaların içerisine koymak yetersiz ve kapasitesinin tam manasıyla bilinememesinden dolayı uzay kavramı eklenmiştir. Kelimenin özüne inecek olursak siber uzay, bilgilerin içeride çevrimiçi olarak saklandığı, paylaşıldığı ve gönderildiği ve arka planda kullanıcıların sanal hareketlerini gerçekleştirdikleri bir alan olarak tanımlamak doğru olacaktır (Singer ve

Friedman, 2018). Bu tanımda dikkat etmemiz gereken kelime ise uzay kelimesidir. Uzay kelimesinin tam anlamını sibere uygulamak manasız olmakla birlikte iletilmek istenen mesaj ise uzay kadar sonsuz ve sınırlarının belli olmamasından kaynaklanmaktadır.

Kaynak: (https://www.voltairenet.org/article207568.html)(E.T. 06.01.2023).

Şekil 2: Churchill'in 5 Mart 1946 'da ABD'nin Fulton Kasabasında Gerçekleştirdiği Konuşma

Siber uzay kavramı bilimsel bir kavram olarak hayatımıza girmiş olsa da kavramın doğup büyümesi bazı tarihsel olayların tetiklemesi sonucunda ortaya çıkmıştır. Winston Churchill'in 5 Mart 1946'da ABD'de de Fulton kasabasında gerçekleştirdiği konuşmasında Soğuk Savaş'ın ilanı olarak kabul edilen ünlü Demirperde konuşmasıyla (Ataç, 2019) birlikte uluslararası ilişkiler farklı bir boyuta evrildiği gibi Soğuk Savaş'ın teknolojik üstünlük sağlanmasında büyük tetikleyicisi olmuştur. Soğuk Savaş kavramı, ABD ve Sovyet Rusya ekseninde kutuplaşan ulus-devletlerin ideolojik, siyasi, sosyal, ekonomik ve teknolojik olarak bir yarış ve rekabet içerisinde olmalarına verilen isimdir. Özelde ABD ve Sovyet Rusya arasındaki rekabet, genelde ise Doğu ve Batı arasında gerçekleşen rekabet internetin temellerinin atılmasına neden olmuştur.

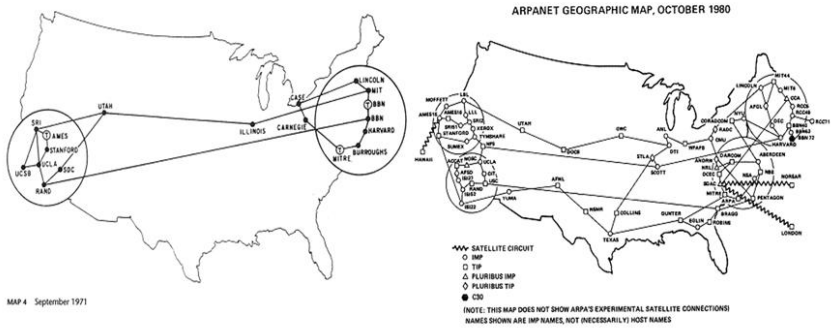
Soğuk Savaş sürecinde ABD'de başta Sovyet Rusya ve Doğu bloğunu çevrelemek ve dengelemek için Batılı devletlere askerî açıdan yerleşmeye ve ekonomi paketleri yayınlamaya başlamıştır. ABD'nin militarist davranışı karşısında Sovyet Rusya bütün silahları ve füzeleri etkisiz hale getirecek bir hamle yaparak 1957'de Sputnik-1 isimli uydusunu uzaya fırlatarak teknolojik üstünlüğü ele geçirmiş ve

kendisini koruyacağını bütün dünyaya duyurmuş olmuştur. Mozhaisky Askeri Uzay Akademisinde profesör olan Kuzhekin bu durumu uzay teknolojilerinin gelişmesi yeni bir cephe olarak uzayın seçilmesinde her şeyden önce siyasi, askeri ve diğer teknik faktörler ele alınarak belirlenmiştir (Ershov, 2011) ABD bu durumu gücüne ve prestijine bir darbe olarak yorumlamış, ABD'de çıkan Saturday Evening Post isimli dergide bu durum kaleme alınarak şüphesiz askeri füzeleri etkisiz hale getirecek ve bombardıman uçaklarını geçersiz kılacak bir teknolojik hamle olduğunu belirterek korkularını dile getirmiştir (Ershov, 2011).

ABD, bu durum karşısında kamuoyuna ve müttefik devletlere karşı Sovyet Rusya tarafından aşağılanma hissini unutturmak ve teknolojik yarıştan geri kalmamak adına Sputnik-1 uydusunun fırlatılmasından yaklaşık dört ay gibi kısa bir sürede ilk yapay uydusu olan Explorer-1'i 31 Ocak 1958'de uzaydaki yörüngesine göndermiştir (Akyeşilmen, 2018). Bu uydular telekomünikasyon ağı üzerinden çok büyük verilerin aktarımını ve iletişimini sağlamak adına büyük başarılar gerçekleştirmiş oldukları kadar yeni bir savaş arenasının doğmasına ve uzay savaşlarının başlamasına neden olmuştur.

Temelde siber uzay dört ana bileşenden meydana gelir. Bunlar; insan, bilgi, mantıksal çerçeve ve fiziksel altyapıdan meydana gelmektedirler (Akyeşilmen, 2018). Siber uzayın yapısının şekillenmesinde ve derinliğinin oluşmasında en önemli faktör insandır. İnsan, bilgi üreten, işleyen ve paylaşan bir yapısı olmasından kaynaklı olarak üretilen bilgilerin sunumu ve pazarlanması konusunda reel dünyanın dışında sanal dünyada yeni bir pazar alanı oluşmasında önemli bir aktör olmuştur. İnsandan sonra en önemli diğer bir bileşen ise bilgi ve mantıksal çerçevedir. Bilgi ve mantıksal çerçeve birbirinden farklı olduğu kadar birbirini tamamlayan olgulardır. Sanal katmanlar içerisinde tasarlanarak veyahut depolama amacıyla yerleştirilen yazılı ve görsel materyaller mantıksal çerçeve kapsamında geliştirilen kodlamalar ve komutlar sayesinde sanal dünyadan sistematik şekilde çekilmesine ve reel dünyada işlenmesine neden olmaktadır. Siber uzayın son bileşeni ise fiziksel altyapıdır. Fiziksel altyapı kullanıcıların isteği üzerine kurulan veyahut insanlığın teknolojik bütünleşmesi için kurulan bir alan olmadığından dolayı militarist bir yaklaşımın sonucu olarak ortaya çıkmıştır. Fiziksel altyapılar kapsamında kullanılan bilgisayarlar, kablolar, hizmet sağlayıcıları ve switchlerin gelişmesi çerçevesinde gerçekleşmiştir.

ABD yönetimi Sputnik-1'den sonraki süreçte Sovyet Rusya'ya karşı büyük bir teknolojik seferberlik başlatmıştır. Bu bağlamda ilk kurulan ve bugün hayatımızın her alanında olan internetinde doğmasına neden olacak Advanced Research Projects Agency (ARPA) yani Gelişmiş Araştırma Projeleri Ajansı kurulmuş ve bu ajansın başına ünlü psikolog ve bilgisayar bilimcisi olan J. C. R. Licklider getirilmiştir (Huaben, 2007). Hem bilgisayar bilimcisi hem de psikolog olmasının ARPA üzerinde büyük etkileri olduğu gibi Licklider'in geliştirdiği 'netizen' kavramını getirerek ARPA'ya galaksiler arası bilgi ağı vizyonun yerleşmesine yardımcı olmuştur (Hauben ve Hauben, 1998). Netizen kavramı internet ve vatandaş anlamına gelen "net" ve "citizen" sözcüklerinin birleşmesi ve onun yorumlanmasıyla meydana gelmiştir. (MacKinnon, 2012). Netizen kavramı kullanıldığı ilk dönemlerde kavramsal olarak anlaşılamamasına neden olduğu gibi bugün internetin yaygınlaşmasıyla birlikte günümüz toplumunu anlatan kilit bir kavram olmuştur. Öyle ki Licklider ne zaman ARPA'da ne zaman konuşma gerçekleştirse citizen'in sadece bilgisayarları birbirine bağlayan ulus üstü bir yapı olmaktan çıkararak siber uzayda diğer kullanıcıların da katılımıyla yeni bir dünya oluşmasından ve bu Dünya'da kullanıcıların siber uzayın geliştirilmesinde fayda olacağını anlatmıştır (Hauben & Hauben, 1998).



Kaynak: (https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html)

Şekil 3: 1970-1980 Yılları Arasında ARPANET Haritasının Değişimi

1960'ların sonuna doğru yeterli bütçenin ARPA'ya ayrılmasından sonra Licklider'in çizdiği yol üzerinden ARPANET kurulmuş ve çalışmalarına başlamıştır (Akyeşilmen, 2018). ARPANET'in kurulmasında ve geliştirilmesinde arkasında ABD hükümetinin mali desteğinin büyüklüğü etkili olduğu gibi diğer bir etken ise bilgisayarların kendi aralarında konuşma fikrini ütopik şekilde ortaya atan Ivan

Sutherland, Bob Taylor ve Lawrence Roberts'in DARPA'yı bilgisayarları devreler yerine siber uzayda paketlerle birbiriyle konuşmasını ikna etmeleri internetin şekillenmesine neden olmuştur (Leiner, ve diğerleri, 1997). Gerçekleştirilen bu adım neticesinde 1971'de Ray Temlinson tarafından 'Qwertyiop' yazılarak ilk mail atılmış, 1973'te ARPANET' ilk uluslararası bağlantı İngiltere'den University Collage of London ile Norveç'ten Royal Radar Establishment arasında gerçekleştirilmiş, 1974'te ARPANET'in ilk ticari versiyonu olan Telenet kurulmuş ve 1977'de artık mailler bilim çevrelerinde bir iletişim sistemi olarak kullanılmaya başlanmıştır (Yetgin ve Baştuğ, 2022). Fakat internet fikrinin tamamen hayatımıza girmesi ise World Wide Web (WWW) ile gerçekleşmiştir. 1989 yılında İngiliz bilim adamı Tim Berners-Lee tarafından bilgisayarların birbirine bağlanması ve herhangi bir olumsuzluk karşısında direnç gösterecek sistematik bir yapı kurulması amacıyla www icat edilmiş olup 1991'de tanıtılmıştır (SIU, 2016). Burada önemli olan husus ise internet ile www'in birbiri yerine kullanılmasına rağmen birbirinden farklı kavramlar olduğudur. İnternet, binlerce ağdan oluşan ve küresel çapta ağların birleşimini ifade eden bir kavramken www, internet üzerinden http aracılığıyla bilgi paylaşımını ve bilginin oluşturulmasını tanımlayan bir hizmettir (Akyeşilmen, 2018).

1990'lı yıllarda dijitalleşmenin başlaması, yeni bir çağın başamasına neden olduğu gibi siber uzayın tanımlanmasında sorun yaratmıştır. Bu bağlamda Beyaz Saray, 2003'te siber uzayı ABD'nin sinir ve kontrol sistemi olarak kabul ettiği Güvenli Siberuzay Ulusal Strateji Belgesi'ni yayınlamıştır (Kuehl, 2009). 2008'de yayınlanan Güvenli Siberuzay Ulusal Strateji Belgesine iki ek ile revize edilerek "…Siber uzay, bilgi teknolojisi altyapılarının birbirine bağlı ağı anlamına gelir ve internet, telekomünikasyon ağlarını, bilgisayar sistemleri ve kritik sektörlerdeki gömülü işlemcileri ve denetleyicileri içerir." Tanım daha kapsayıcı hale getirilmeye çalışılmıştır (Kuehl, 2009). Başkanlık imzasıyla yayınlanan belgede tanımlama bu şekilde verilirken Mayıs 2008'de dönemin ABD Savunma Bakan yardımcısı olan Gordon England'ın yayınlamış olduğu memorandumda siber alan; "…*İnternet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü işlemciler ve denetleyiciler de dâhil olmak üzere birbirine bağlı bilgi teknolojisi altyapıları ağı...*" olarak tanımlanmıştır (Kuehl, 2009).

Siber alanın ttanımı sürekli olarak yenilenmekte ve daha kapsayıcı hale getirilmeye çalışılmaktadır. Bu gelişmenin altında yatan temel etken, internet ve bilgisayar teknolojisindeki dikkat çekici gelişmedir. 2000 yılında dünya genelinde

internete ulaşan kişi sayısı 414 bin iken, bugün dünya üzerinde 5 milyardan fazla kullanıcı bulunmakta ve 1992 yılında kurulan internet sitesi sayısı 10 iken bugün kurulan internet sitesi sayısı 1,9 milyarın üzerindedir (Internet Live Stats, 2021). İnternet kullanıcı sayısının bu denli büyük bir sayıya ulaşması elbette beraberinde bireyler, şirketler ve devletler düzeyinde büyük güvenlik açığının oluşmasına neden olmuştur.

1.3.3. Siber Güvenlik Nedir?

Siber güvenlik kavramı ilk olarak 1970'lerde ABD'de duyulmuş, 1980'lerle birlikte bir ivme kazanmış ve 1990'dan sonra ise diğer ülkelere yayılmasıyla birlikte önem kazanmış ve üzerine düşünülen ve çözüm üretilmeye çalışılan bir kavram olmuştur (Cavelty, 2010). 2016-2019 Ulusal Siber Güvenlik Stratejisi belgesinde;

> "Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi..." (T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2016) olarak tanımlanmıştır.

Dönemin ABD başkanı Obama, siber güvenliği millet olarak karşı karşıya kalınan ve milli ve ekonomik güvenliği tehdit eden en ciddi mesele olarak tanımlamıştır (Çifci, 2017). Siber güvenliğin gelişmesi ve siber uzayın bir öncelik olarak belirlenmesinde öncülük eden Obama, siber güvenlik kavramının da tanımlanmasında önemli bir etken olmuştur.

Kaynak: (https://www.sibervatan.org/makale/enigma-sifreleme/17)(E.T. 05.01.2022)

Şekil 4: ENİGMA Genel Görünüm

Siber güvenlik kavramının net bir tanımı olmamakla birlikte genel ve geniş bir tanım vermek gerekirse, siber alanda bireylerin, kurum ve kuruluşların bilgi, belge, proje ve varlıklarını korumak amacıyla geliştirdikleri araçlar ve politikalar bütününe verilen isimdir. Fakat siber güvenliğin günümüzde bu kadar önem kazanmasının sebebi her ne kadar 1990 ile başlasa da asıl olarak temel nedeni II. Dünya Savaşı sırasında Almanya'nın bir grup matematikçiyi bir araya getirerek Yunanca gizem anlamına gelen ENİGMA'yı ortaya çıkarmalarıyla başlamıştır (Perendi ve Gope, 2021). ENİGMA'nın ilk örneği 1930'larda çıkmış olsa da rotar (dönence) sayısının az olması şifrelenen mesajların çözülmesin kolaylaşmasından dolayı rotar sayısı artırılmış ve son hali olan 26 ayara sahip ve içerisinde 3 ile 5 rotar barındıran son ENİGMA ortaya çıkmıştır (Beutelspacher, 2021).

ENİGMA'yı siber güvenlik için bu kadar önemli yapan husus ise dönemin ötesinde kullanılan teknoloji ve bu cihazın şifrelediği iletilerin çözülmesi adına verilen büyük çaba olmuştur. İngiltere, Almanların kripto silahına karşı kontra kriptocu gizli bir birim kurmuştur. Bletchley Parkı olarak tarihte yerini alan bölgede, İngiltere adına teorik bilgisayar bilimcisi olarak çalışan Alan Turing, yoğun çalışmalarıyla son teknoloji ürünü olan ENİGMA'nın şifrelerini çözmeyi başarmış ve Almanların füze saldırılarını ve nereleri hedeflediğini belirleyerek tarihin seyrini değiştirmiştir (Beutelspacher, 2021).

Bilginin korunması ve güvenli şekilde ulaştırılması kriptoloji biliminin kapsamında gelişmiştir. Yüzyıllardır ağır ağır gelişen bu bilim dalı siber uzayın keşfiyle farklı bir boyut kazanmıştır (Beutelspacher, 2021). Özellikle bilgisayarların kullanımın artması kriptoloji biliminin işinin hem kolaylaşmasına hem de zorlaşmasına neden olmuştur. Teknolojik atılımların fiziki hayatın ilerisinde davranması ve belirsizlikleri kendi lehine çevirmesiyle birlikte yeni teknolojik ürünlerin ve sistemlerin ortaya çıkmasına neden olmaktadır. Şifreli bilgilerin kırılması ve öğrenilmesi için geliştirilen teknikler teknolojik gelişimin de önünü açmıştır. Rötarlı cihazlardan bilgisayarlara, bilgisayarlardan da süper (kuantum) bilgisayarların ortaya çıkmasına neden olmuştur. Bu gelişmelerin ortaya çıkması ise siber güvenliğin doğmasına neden olmuştur.

Günümüzde siber güvenlik sadece ileti ve bilgilerin elde edilmesiyle olmamakla birlikte yeni gelişmeler sonucu ortaya çıkan kavramlar siber güvenliğin kapsamını ve alanını da geliştirmiştir. Özellikle Metaverse ve Second Life kavramlarının ortaya

çıkmasıyla birlikte siber güvenliğin kavram haritası genişlemeye başlamıştır. Kavram haritasının bu kadar genişlemesi tanımlama sorununu beraberinde getirmiştir.

Kavram haritasının gelişmesi ve kargaşanın ortaya çıkmasında devletlerinde büyük etkisi vardır. Devletlerin siber alanda aktif olarak faaliyet göstermesi ve çıkarlarının korunması adına gerçekleştirdikleri faaliyetler, siber güvenlik kavramının farklı tanım ve kapsamlarının ortaya çıkmasına neden olmuştur. Örneğin Almanya, siber güvenliği yalnızca internete bağlı bilgi ve iletişim teknolojisini dikkate aldığını belirtirken Hollanda'nın siber güvenliğe yaklaşımı bilgi ve iletişim teknolojilerini daha kapsamlı şekilde ele alarak kapsamını genişletmiştir (Baştuğ, 2022).

Siber güvenliği en etkin ve donanımlı şeklide kullanan devletler ise ABD ve Rusya'dır. Soğuk Savaş ürünü olarak ortaya çıkan siber uzay, her iki devletin çatışma alanı olmasına ve bu alanda üstünlük kurmalarından kaynaklı olarak üzerine düşülen bir kavram olmuştur. Özellikle Rusya'nın Sovyetler döneminden gelen bilgi ve birikimlerini bu alanda kullanması ve siber alanda hem siber güvenliğin hem de siber savaş kapasitesinin gelişmesine neden olmuştur (Baştuğ, 2022).

Siber güvenlik kavramının sıklıkla siber uzayla karıştırılması da siber güvenliğin anlamsal olarak anlaşılmamasına neden olmaktadır. Siber uzay kavramının, siber güvenlik kavramının anlaşılmasında ve resmi bir terminolojinin oluşmasında bir başlangıçtır (Althonayan ve Andronache, 2018). Tam olarak siber uzayın ne ifade ettiğinin belirsizliği ve bu belirsizliğin ortaya çıkardığı güvenlik kaygısından dolayı siber güvenliğin oluşmasında başlangıç seviyesini oluşturmaktadır. Soyut olarak karşımıza çıkan siber uzay kavramının somut bir yapıya bürünmesi siber güvenlikle olmuştur. Siber alanda gerçekleştirilen siber saldırılar, siber istihbarat faaliyetleri, siber espiyonaj faaliyetleri ve siber savaşların reel dünyada karşılıklarının olmasından dolayı siber güvenlik somut bir yapıya bürünmektedir.

Terminolojik olarak belirsizliklerin olması zaman içerisinde büyük sorunları meydana getireceği şüphesizdir. Bu kapsamda siber güvenliğin kapsamı, teknolojik yapısal değişikler ve yeniliklerin yakından takip edilmesiyle yenilenmeli ki hem siber uzayın her yapı birimine hâkim olmak hem de reel hayatta oluşacak zarar ve olumsuzluklarının engellenmesine yardımcı olacaktır. Daha açıklayıcı olmak gerekirse 1960'lı yıllarda bilgisayarlar, hassas verileri sızdırabilen yapıya sahip olabilir ve korunmasına yönelik adımlar atılması gerekliliği varken, 1970'lerde artık siber alandan

bilgisayarlara saldırılar gerçekleştirilebilir ve veriler çalınabilir durumuna, 1970 ve 1980'lerde ise bilgisayarların bir güç olarak kabul edilmesiyle birlikte askeri birimlere siber savaşlar için bilgisayarların kullanılması ve özel bölgelerin inşası algısı gelişmiş ve son olarak 1990'lardan sonra ise diğer aktörlerin de alınan önlemler ve hamleleri aynen karşı tarafa aktarabileceği algısı oluşmasına neden olmuştur (Warner, 2012).

2000'li yıllarda artık internete erişimin kolaylaşması yeni aktörlerin doğmasına neden olduğu gibi belirsizliğini koruyan siber alanda da yeni kapıların açılmasına neden olmuştur. Fiziki hayatta varlığını sürdüren terör ve terörizm faaliyetleri, istihbarat ve casusluk faaliyetleri, sosyal mühendislik, emlakçılık faaliyetleri, sigortacılık faaliyetleri ve siber borsacılık faaliyetleriyle siber güvenliğin alanı genişlemiştir. Siber güvenliğin klasik güvenlik anlayışı kadar önemli olduğu günümüzde, yeni kavramlar ve yeni pencereler açılmasına da neden olmuştur. Bu alanların içerisinde en önemlisi ise Metaverse dünyasının oluşmasıdır.

Kaynak: (https://www.cnbc.com/video/2022/12/08/a-brief-history-of-the-metaverse.html, tarih yok) (E.T. 06.01.2023)

Şekil 5: Temsili Meta Verse Evreni

Siber kelimesi gibi kurgu roman ile hayatımıza 1992'de Neal Stephenson tarafından yazılan Snow Crash romanıyla giren Metaverse kavramı, kullanıcıların dijital avatarlar aracılığıyla etkileşime girdiği, fiziksel dünyaya paralel devasa bir sanal ortam olarak tanımlanmaktadır (Lee, vd., 2021). Reid Hoffman'a göre ise metavers'in hayatımızın her anında var olduğunu fakat internet ve IoT (Internet of Things)

teknolojilerinin metaverse dünyasının oluşması için gerekli teknolojik altyapı ve birikime sahip olmadığını ve bu nedenle internetin, metaverse 'in yalnızca erken bir versiyonu olduğunu belirtmiştir (Markets Insider, 2021). Temelde yeni bir internet algısını oluşturmaya çalışan Hoffman bu düşüncesinde tek değildir. Xu ve arkadaşları da metaverse'i, katılımcıların dijital avatarlarının 3B ortamda diğer katılımcılarla ve yazılım uygulamalarıyla etkileşime girebildiği yeni nesil internet olarak tanımlamıştır (Xu, vd., 2021).

Teknolojinin her geçen gün gelişmesi ve teknolojinin siber alanla bağlantılı büyümesi oluşan güvenlik açığını artırdığı gibi siber alanın kapasitesinin belirsizliğini gözler önüne sermektedir. Bu belirsizlik içinde siber güvenliğe olan ihtiyaç artmaktadır. Siber güvenliğe gereği kadar değer verilmemesi durumunda bireyler, şirketler ve hatta devletler ağır sonuçlarla yüzleşmektedir. Örnek olarak verecek olursak 2001'de gerçekleştirilen 11 Eylül saldırıları her ne kadar terörist grubunun uçak kaçırarak yaptığı bir eylem olarak görülmüş olsa da arka planda siber terörizm bulunmaktadır. 11 Eylül saldırıdan sonra yapılan araştırmalar neticesinde teröristler saldırıyı internet üzerinden planladıklarını göstermiştir (Thomas, 2003). Bu bilginin dışında yine 16 Eylül 2002'de teröristler ABD içerisindeki uyuyan hücreleriyle haberleşmek için ise internet tabanlı telefon ile iletişim kurdukları ortaya çıkarıldı (Thomas, 2003).

Siber terörizm geleneksel terörizmden farklı olarak, terör faaliyetlerinde bilgisayar ve BİT'lerin kullanılmasıyla (Nomokonov & Tropino, 2012) ya da bilgisayar ağlarına saldırarak büyük çapta korku ve panik yaratan, devlet veya devlet dışı aktörlerin desteklediği donanımlı kişilerin yaptıkları eylemlerdir (Rai & Mandoria, 2019). Federal Acil Durum Yönetim Kurumu (Federal Emergency Management Agency-FEMA) ise siber terörizmi politik veya sosyal belli hedeflere ulaşmak için BİT ile halkı korkutmak, sindirmek ve zorla yaptırmak için sanal ortamda gerçekleşen yasadışı faaliyetler olarak tanımlamıştır (Terzi, 2019).

Bugün siber terörizm, bireyden başlayarak devletlere kadar uzanan geniş bir alana hâkimdir. Terör ve terörizm faaliyetleri bugün toplumlar ve devletler için büyük güvenlik sorunu olduğu gibi siber terörizm faaliyetleri de bir o kadar tehlikelidir ve korkutucudur. Siber alanın kapasitesinin ve ortaya çıkacak ekonomik, siyasi, sosyal ve kültürel zararların kapasitesinin belli olmamasından kaynaklı, devletlerin ve bireylerin siber güvenliğe daha çok önem vermesi gerekmektedir.

1.3.3.1. Siber Güvenliğin Klasik Güvenlik Anlayışından Farkı

Klasik güvenlik algısının şekillenmesinde çeşitli parametreler olmakla birlikte ekseriyetle devletlerin güvenlik politikaları sınır komşuları, ideoloji, terör, enerji, jeopolitik konum ve askeri faaliyetler etkili olmaktadır. Siber güvenlik için temelde siber suçlar, siber savaşlar, siber zorbalık, siber terörizm ve espiyonaj faaliyetleri sayılabilmektedir fakat siber alanın kapasitesinin belirsiz olması ve her geçen gün gelişen teknolojik yatırımlar, siber güvenliğin farklı parametrelerin ortaya çıkmasına neden olmaktadır. Son on sene içerisinde hayatımızda geniş yer kaplayan kripto paralar, sanal dünyalar ve IoT teknolojileri bu duruma örnek gösterilebilir.

Gelişen teknolojik gelişmeler sonucundan yeni kavramların ve güvenliği tehdit edecek yeni teknolojik gelişmeler güvenlik kavramının kavramsal haritasının yeniden güncellenmesine ve yeni anlamların yüklenmesine neden olmuştur. Bugün dijital teknolojilerin gelişmesi ve bireylerden, şirketlere ve hatta devletlere kadar geniş bir yelpazeye sahip olması ciddi kolaylıklar, özgürlük ve refah getirmiş olsa da siber saldırıları riskinin de artmasına ve dolayısıyla siber güvenliğin ulusal olmaktan çıkararak uluslararası öneme sahip olmasına neden olmuştur. Klasik güvenlik kavramında bireyler, şirketler ve devletler çıkar ve varlıklarının korunması ekseninde şekillenirken teknolojik gelişmeler sonucunda ortaya çıkan siber güvenlik ile beklentiler farklılaşmıştır.

Teknolojik gelişmeler ve diğer faktörlerin (salgın, ekonomik yapılanma vd.) birleşmesiyle birlikte insanlar evlerinden çalışmaya başlamaları, yapısal olarak ev internet ağının güvenliğinin düşük olması siber saldırıların artmasına ve ticari sırların saldırılara açık konumda olması sebebiyle ciddi güvenlik açığının ortaya çıkmasına neden olmuştur. İnsanların uzaktan çalışması fiziksel ve ruhsal olarak teknolojinin bir faydası olarak görülse de güvenlik farkındalığının azalmasına neden olmuştur (Korucu, 2021).

Siber alanın her geçen gün katbekat büyümesi siber güvenliğe olan ihtiyacı artırdığı gibi bireylerin, şirketlerin ve devletlerin siber güvenlikten beklentilerin artmasına neden olmaktadır. Fakat beklentiler her geçen gün arttığı gibi yeni ortaya çıkan kavramlarla da entegreli olması siber güvenlik kavramının bir kara deliğe dönüşmesine neden olmaktadır. Siber güvenliğin özellikle de uluslararası ilişkiler disiplini açısından incelendiğinde kara deliğe dönüşmesinde, siber alanda

gerçekleştirilen eylemlerde atfedilebilir olma konusunun belirsiz ve tespitini zor olması, hesap verme zorunluluğunun olmaması, nüfuz alanının geniş olması, fiziksellikten uzak ve klasik zaman anlayışını kırmasından dolayı kara deliğe dönüşmüştür (Çelik, 2018).

Siber alanda gerçekleştirilen eylemlerin kim/kimler tarafından, ne zaman ve nasıl yapıldığına dair somut verilere ulaşılamamasından dolayı siber güvenliğin belirsizliğini ortaya koymaktadır. Güncel bir örnekle açıklayacak olursak, 15 Temmuz 2022'de Arnavutluk'a yönelik gerçekleştirilen siber saldırı sonucunda Arnavutluk gümrük sistemlerini hedef almış ve gümrük sistemlerinin erişilemez hale gelmesine neden olmuş ve bu saldırı sonucunda Arnavutluk yönetimi İran'ı sorumlu tutmuş fakat İran resmi haber ajansı bu saldırının temelsiz olduğunu belirterek saldırının arkasında üçüncü taraflarında olabileceğini belirtmiştir (BBC News, 2022). Bir devletin diğer bir devlete karşı düşmanca saldırı gerçekleştirdiği iddia edilmekte fakat bu olayın siber alan vasıtasıyla gerçekleştirilmesi sebebiyle siber ayak izlerinin belirli olmaması ve yeterli kanıtların olmamasından kaynaklı olarak tarafların birbirlerine yönelttikleri ithamları havada kalmıştır.

Klasik güvenlik anlayışında bir devletin başka bir devlete karşı gerçekleştireceği eylem beraberinde bazı ağır sonuçları getirirken siber alanda gerçekleştirilen eylemler için sadece ithamlar ve ihtimaller üzerinden şekillendiği için -kaynağı belirlenen istisna saldırılar hariç- belirli bir düşman belirlenememektedir. Siber alanda gerçekleştirilen eylemler devletlerden hariç şirketleri ve bireyleri de derinden etkilemektedir. Şirketlere ve bireylere karşı gerçekleştirilen eylemler de siber güvenliğin bir parçası olmasından dolayı klasik güvenlik anlayışından farklı olarak siber güvenliğin eksikliği bireyleri ve şirketleri derinden etkilemekte ve sonuçlar hem fiziksel hem de mental olarak ağır olmaktadır. Sonuçlar her ne kadar devletler ve şirketler için ağır sonuçlar doğurma potansiyelinde olsa da dijitalleşen kamu kurum ve kuruluşlarıyla birlikte şirketler, siber alanın imkanlarını kullanarak uzun vadeli stratejiler geliştirebilme ve kullanıcı deneyimlerini göz önüne alarak yenilikçi imkanların oluşturularak bütün yapılanların güvence altında yapılmasına da imkân sağlamıştır (Akmeşe, 2020).

1.3.3.2. Güvenlik Kavramının Oksimoron İlişkisi

Küreselleşme hareketiyle birlikte başlayan teknolojik gelişmeler sonucu ortaya çıkan siber alan, dünyanın küçük bir köy olmasına ve bütün kullanıcıların birbiriyle

etkileşim içerisine girmesine neden olmuştur. Dünyanın küreselleşmesiyle birlikte iletişim yollarının çeşitlilik kazanmasına ve ihtiyaçların daha da artmasına neden olmuştur. Kullanıcıların, şirketlerin ve devletlerin ihtiyaçlarını karşılamak ve refah seviyelerini artırmak amacıyla siber alan daha da genişlemiş ve fiziki sınırlar ortadan kalkmaya başlamıştır. Kullanıcıların ihtiyaçları ve refah seviyelerinin artırılması amacıyla internet altyapıları ve kurum ve kuruluşların dijitalleşme süreci başlamış ve bu dijitalleşme süreci beraberinde büyük yararlar sağladığı gibi oluşan yeni alanlar beraberinde büyük problemlerin ve tehlikelerin de ortaya çıkmasına neden olmuştur. Ortaya çıkan bu tehlikeler ve güvenlik açıkları fiziki çeşitlilikler gösterdiği gibi ekseriyetle sanal ortamda veyahut siber alanda doğmaya başlamıştır.

İnternetin tabana yayıldığı 1990'lı yıllar birçok akademisyen için tehlikenin ve güvenlik açıklarının oluşmaya başladığı bir başlangıç tarihi olarak kabul edilse de güvenlik açığı asıl bilgisayar teknolojilerini gelişmeye başladığı 1970'li yıllarda ortaya konmaya başlamış ve dile getirilmeye başlanmıştır. Bu bağlamda tehlikenin anlatılmaya başlanması 1975'te Saltzer ve Schroder tarafından kaleme alınan ve psikolojik kabul edilebilirlik ilkesini tanımlayarak bilgisayar güvenliği ve erken tedbirler üzerine çalışma yapmalarına rağmen siber güvenlik farkındalığı 1990'lı yıllarda ciddi şekilde tartışılmaya başlanmıştır (Theofanos, 2020). Yeteri kadar ele alınmayan ve incelenmemesi sonucunda bugün internet ve bağlandığı makineler yazılım ve ağ protokollerindeki güvenlik açıklarından yararlanarak kolay hedef haline gelmesine neden olmuş ve bu durum büyük ekonomik kayıpların artmasına, politik ve ideolojik amaçlı saldırıların artmasın ve kişisel verilerin açık hale gelmesine neden olmuştur (Landwehr, 2009).

Klasik güvenlik algısının 1990'dan sonra internetin tabana yayılması ve hızlı şekilde gelişmesiyle birlikte siber alanda gerçekleştirilen eylemler, ulusal ve uluslararası güvenliği ciddi şekilde tehdit etmeye başlamıştır. Enformasyon teknolojileri ile başlayan güvenlik açıkları beraberinde klasik adi suçların siber alanda işlenmesine ve terör eylemlerine kadar ilerlemiştir. Terör eylemleri, fiziki dünyada gerçekleştiği gibi artık internetin tabana yayılmasıyla birlikte siber alanda da gerçekleşmeye başlamıştır. Bir örnek ile açıklayacak olursak 11 Eylül 2001'de El-Kaide'nin ABD'de bulunan ikiz kulelere gerçekleştirdiği saldırıda teröristler, ABD'de bulunan hücreleriyle haberleşmek için internet tabanlı telefonlarla gerçekleştirmelerinden dolayı fiziki terör saldırısı olduğu gibi siber terör faaliyeti olarak da kayıtlara geçmiştir (Yetgin ve Baştuğ, 2022).

Siber uzayın terör eylemlerinde ve adi suçların işlendiği bir merkez konumuna gelmesinde güvenlik algısında büyük değişimlerin yaşandığını ve güvenlik kavramının kavramsal olarak değişmesine neden olmuştur. Güvenlik algısı 20.yy'ın sonlarına kadar klasik bir anlayış içerisindeyken yenilikçi teknolojik hamlelerinin artmasıyla anlamsal değişikliklere gittiği gibi görünmez suçların sayısındaki artış nedeniyle sorgulanmaya da başlamıştır. Klasik güvenlik anlayışında kullanıcılar, şirketler ve devletler için tehdit unsurları fiziki olarak belirli olmasına rağmen siber alanda tehdit unsurlarının sayısı, şekli ve saldırı yöntemlerinin belirsiz olması ve bu saldırı formlarının yıllar içinde çok büyük değişimlere uğraması tam bir güvenlik sisteminin uygulanamamasına neden olmaktadır. Güvenlik ekseninde oluşan belirsizlik ve güvensizlik kavramsal olarak oksimoron durumuna düşmesine neden olmaktadır. Siber alanda gerçekleştirilen saldırıların kaynağının, sayısının, çeşidinin ve yapısının belirsiz olması güvenlik kavramının içinin boş bir yapıya dönüşmesine neden olduğu gibi güvenlik kavramından güvensizlik duyulmasına neden olmaktadır.

1.3.4. Siber Tehdit Araçları

Kriminolojinin günümüzde bilgisayar teknolojilerinin, yazılımların ve IoT teknolojilerinin gelişmesiyle birlikte siber suçlar önemli derecede arttığı gibi bu alana yapılan yatırımlar ve teknolojik ürünler ile yeni araçlar ortaya çıkmaya başlamıştır. Bu tehdit araçları; solucanlar, Truva atı, virüsler, yemleme, klavye takipçisi, DoS ve DDoS saldırıları, bot ve zombiler, fidye yazılımları, reklam yazılımları ve sosyal mühendislik faaliyetleri olarak karşımıza çıkmaktadır.

1.3.4.1. Solucanlar

Solucan yazılımlar, ana bilgisayardan hedef bilgisayara kendilerini otomatik olarak kopyalayan bir yazılımdır. Solucan yazılımlar diğer yazılımlardan farklı olarak hedef programlara yerleşip ilgili programların çalıştırılması sonucunda aktif olurken, solucanlar bilgisayarlarda hızla yayıldığı gibi internet hattında da dolaşımda olabilen ve bütün internet kullanan araçlara bulaşabilmektedir. Solucan yazılımlar hedeflenen sistemde ilk olarak dosya ve bilgi ileten sistemlerin içerisine yerleşerek ele geçirmek üzere programlanan ve sisteme girdikten sonra kendi başına ilerleyen ve çoğalabilen bir

yazılımdır (Siberay, 2022). Solucan yazılımların bilgisayar ve internet sistemlerine verdiği en büyük tehlikesi kontrol altına alınamamasından kaynaklanmaktadır. Bunun en önemli sebebi ise herhangi bir kontrol mekanizmasının emri olmadan kendi başına çoğalabilmesinden kaynaklanmaktadır.

Solucan yazılımlar internetin ve bilgisayarların yaygınlaşmasıyla birlikte büyük sorunların da gün yüzüne çıkmasına neden olmaktadır. Tarihte ilk solucanın üretilmesi ise bir test yazılım sonucu ortaya çıkmıştır. Kayıtlara geçen ilk solucan 2 Kasım 1988'de Bilgisayar bilimi alanında Cornell üniversitesinde lisansüstü öğrencisi olan Robert Tappan Morris tarafından kendi ifadesiyle internetin haritasını çıkarmak amacıyla oluşturulmuştur (Orman, 2003; Jajoo, 2021) Türünün ilk örneği olmasından kaynaklı olarak bu solucan bilgisayar bilimcilerin ilgisini çekmiştir. Bu süreçte oluşturulan Morris solucanı o dönemde kullanılan bilgisayarların %5-10 arasında etkilendiği ve zararın 98 milyon dolar olduğunu tahmin etmektedirler (Jajoo, 2021).

Morris solucanından sonraki süreçte bilgisayar bilimciler siber alana vuruluş büyük bir darbe olarak bu vakayı yorumlarken 2000 yılında "I Love You" veya "Love Bug" isimli bir solucanla tekrardan karşılaşmıştır. Love Bug solucanı, öncelikli olarak Microsoft Outlook kullanıcılarını hedeflemiş, e postadan içeri girmiş ve daha sonraki hedefi ise şifreleri ve görsel ve sesli materyallerin aktarılması ve silinmesini gerçekleştirmiş ve son olarak rehber listesine ulaşarak kendisini diğer kullanıcılara yaymakla kodlanmış bir yazılımdır (HSDL, 2000). Love Bug solucanın ortaya çıkmasıyla birlikte kurulan araştırma komisyonunda 55 milyondan fazla kişisel ve kurumsal bilgisayarın etkilenmiş olabileceğini düşündüğü gibi kim tarafından oluşturulduğu ve nasıl yerleştirildiği bugün de gizemini korumaktadır (HSDL, 2000).

1.3.4.2. Truva Atı

Truva atı yazılımları isminden de anlaşılacağı gibi faydalı bir program veyahut oyun gibi formlar içerisinde yer alan ve konak bilgisayarı hedef alıp zarar vermeye yönelik bir yazılım olduğu gibi (Çifci, 2017), ücretsiz programlar, e-posta ekleri ve anti virüs programlarının içerisine yerleşerek kendisini kamufle eden yazılımlardır (Akyeşilmen, 2018). Genellikle Truva atı yazılımları kullanıcıları cezbeden ve ilgilerini oluşturabilecek kelimeler, görsel materyalleri ve videoları paravan olarak kullanarak sisteme yerleşmektedir (Thimbleby, vd., 1998)

Siber güvenlik istatistiklerine baktığımızda üç büyük tür güvenlik olayının içerisinde yer alan Truva atını kötü niyetli kod sınıfında değerlendirilmektedir (Abuzaid, vd., 2013). Öyle ki Cincinnati üniversitesinde 1983-1984 arasında gerçekleştirilen deneysel araştırma da basit bir virüs yazılımının dahi basit bir bilgisayar sistemini tamamen ele geçirmesi birkaç saat alabildiğini göstermiştir (Denning, 1988). 1983-1984 yılları arasında bilgisayar kullanıcı sayısı ve teknolojik altyapı ve imkanlar göz önünde bulundurulursa kötü yazılımların diğer bilgisayarlara bulaşma süresi ve etkisinin çok dara ve kısıtlı olduğu anlaşılmaktadır. Günümüzde dijitalleşmenin her alanda etkili olması ve siber uzayda aktive olmuş bilgisayar ve internete bağlanan cihazların sayısını düşünecek olursak büyük sorunların ve beraberinde sosyo-ekonomik olarak büyük sorunlar doğurması kuvvetle muhtemel olacaktır.

Truva atı yazılımları virüsler gibi kendisini çoğaltamamakla birlikte virüsler kadar etkili olabilmektedirler. Truva atı yazılımları hedef bilgisayara yerleştikten sonra virüsler gibi aktif yıkıcı faaliyetler yerine proaktif bir saldırı yöntemi ile hackerler için sistem içerisinde bir giriş kapısı oluşturulmasında veyahut diğer faaliyetleri gerçekleştirebilmek amacıyla bir araç olarak kullanılmaktadır (Kara, 2015). Truva atı ile oluşturulan açık kapı ile hackerler, hedef bilgisayarları zombileştirmek, bilgisayarları botnet parçası haline getirmek, siber suçlar için bir araç olarak kullanmak ve bilgisayarda yapılanları izlemek amacıyla kullanmaktadır (Akyeşilmen, 2018) .

Bilgisayara solucanları anlatılırken verilen I Love You, sadece bir solucan olmamakla birlikte Truva atı özelliği de sergilemektedir. Çifci kitabında I Love You yazılımını Truva atı sınıflandırması içerisine koymasında aşk mesajı gibi görünüp kullanıcıyı kandırmaya odaklı olmasından dolayı bu yönüyle Truva atına benzetmekte olup hedef bilgisayara zarar vermesinden ve bilgisayar ağı içerisinde kendisini sürekli kopyalamasından kaynaklı olarak solucan olarak nitelendirmiştir (Çifci, 2017).

1.3.4.3. Virüsler

Bilgisayar teknolojilerinde virüs kavramı anlatılırken daha kolay anlaşılabilmesi için biyolojik yapıya zarar veren organizmalara benzetilerek anlatılmaktadır. Belirli bir konağın içerisine yerleşen canlı virüs, yerleştiği konağa yerleşir yavaş hareket eder gelişir ve ölümcül sonuçlar doğurmasına neden olabilmektedir. Bilgisayar virüsleri de canlı virüsler gibi hedef bilgisayara yerleşir, uyku modunda bekler, hedef bilgisayarın

ana bileşenlerini ele geçirir ve bu süreçte hedef bilgisayarın kontak kurduğu diğer bilgisayarlara geçer, etkinleştirildiğinde de öncelikli olarak hedef bilgisayar ile diğer bilgisayarların zarar verilmesinde veyahut yok edilmesi için tasarlanmış dijital varlıklardır (Thimbleby, vd., 1998).

Virüsler yapısı ve işlevi nedeniyle sürekli karıştırılan programlar olarak bilinmektedir. Genel bir tanımlama yapacak olursak virüsler, istemeden ve gizli şekilde bilgisayarlara giren, normal bilgisayar çalışma sistemini bozan ve verilere ve programlara büyük zararlar veren programlar olarak tanımlanmaktadır (Subramanya ve Lakshminarasimhan, 2001) Fakat hedef bilgisayarlara zarar veren her yazılım virüs olmamakla birlikte örnek verecek olursak solucanlar ve Truva atları virüs sınıfında yer almamaktadır (Subramanya ve Lakshminarasimhan, 2001; Çifci, 2017).

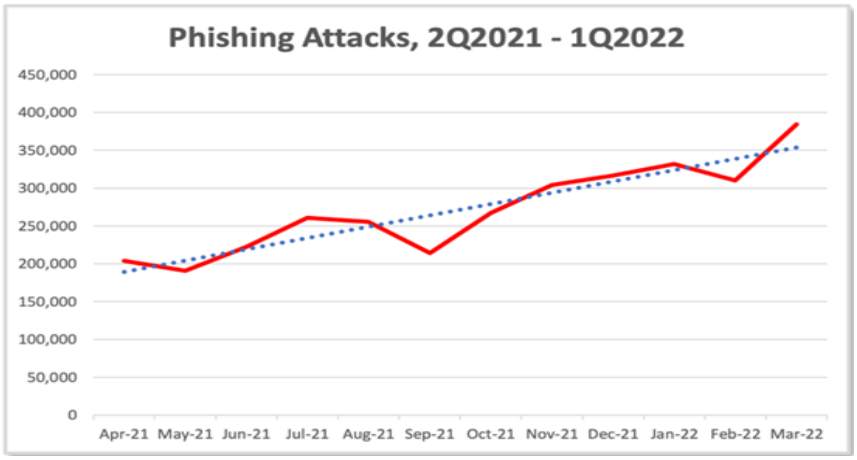
Virüslerin temel olarak işleyişi hedeflenen bilgisayara çeşitli yollar ile girmesi ve kendisini sistem dosyaları içerisinde gizlemesiyle başlar. Virüsün hedef bilgisayar içerisinde kendisini gizlemesi programlanmasıyla alakalı olabileceği gibi hedef bilgisayara virüsü yönlendiren kişinin saldırıyı geciktirerek hedef bilgisayarın yedekleme bantlarına yerleşme isteği sonucunda da planlı şekilde geciktirebilmekte ve bu gecikmeye terim olarak gecikme süresi olarak adlandırılır (Cohen, 1986). Hedef bilgisayara yerleşen ve gizlenen virüs, saldırıyı gerçekleştirecek olan kişinin belirlediği komutun aktif edilmesiyle harekete geçerek zarar vermeye başlar ve virüslü program her çalıştırılmasında aktif kaldığı süre boyunca hedef bilgisayara zarar vermeye devam eder (Cohen, 1986).

Virüsler, bilgisayar teknolojilerinin gelişmesi ve IoT teknolojilerinin yaygınlaşması sonucunda çağımızın en büyük sorunu olmaya devam etmektedir. Kendi kendini kopyalayan programlar 1960'larda John von Neumann'ın hücresel otomatlar üzerine yaptığı çalışmalardan beridir olmasına rağmen (Levy ve Crandall, 2020). 1990'larda internet ve bilgisayar teknolojilerinin gelişmesi dünyada bilgisayar, kod yazılımı ve internet kullanımını artırması zararlı yazılımların artmasına neden olmasına rağmen dünyada ilk bilgisayar virüs kavramını Leonard Adleman tarafından 3 Kasım 1983'te kullanmış ve ilk virüs olarak kabul edilmektedir (Cohen, 1986). Fakat Cohen'in aksine Miles, ilk bilgisayar virüsünün Rich Skrenta tarafından 1982'de Neumann'ın çalışmaları ışığında gerçekleştiği Elk Cloner olduğunu savunmaktadır (Miles, 2012). Cohen'in ilk virüs olarak Skrenta'nın geliştirdiği Elk Cloner'ı virüs sınıfına almamasını

Miles'ın makalesinde de bahsettiği üzere iyi huylu ve zararlı olmamasına dayandırabiliriz (Levy ve Crandall, 2020).

1.3.4.4. Yemleme/Oltalama

1996'da ilk kez ortaya çıkan yemleme/oltalama kavramı en genel tanımıyla siber alanda işlenen kimlik avcılığıdır (Huang, vd., 2009). Kimlik avcılığı için genel bir tanımlama yapacak olursak; güvenilir internet sitelerinin taklit edilmesiyle kullanıcıların kişisel bilgilerini, banka ve kredi kartı bilgilerini ve sosyal medya bilgilerini ele geçirmek üzere kurulan eski ve etkili bir yöntemdir (Basit, vd., 2021; Toğaçar, 2021). Eski ve etkili olan bu yöntemin büyüklüğünü anlamak için Gartner şirketinin 2007'de yapılan ankette, ABD'de yaşayan 3,6 milyon ABD'li doğrudan oltalama yöntemiyle 3,2 milyar dolar kaybettiğini açıklamıştır (Huang, vd., 2009).



Kaynak: (APWG, 2022)

Şekil 6: APWG Tarafından Nisan 2021- Mart 2022 Arasında Gerçekleştirilen Saldırı Grafiği

Gartner şirketinin 2007'de yapmış olduğu anket sonucunu değerlendirecek olursak dijitalleşmenin 2007'de belirli bir kitleyi kapsaması ve internet kullanımının günümüze oranın düşük olmasına rağmen 3,6 milyon insanın etkilenmesi büyük bir orandır. RSA siber güvenlik şirketinin 2016'da yayınladığı raporda dünya genelinden topladığı veriler ışığında 2016'da meydana gelen kimlik avı saldırıları sonucunda toplam 9 milyar dolara yakın bir zarar ortaya çıkmıştır (Basit, vd., 2021). Ayrıca Kimlik

Avı Önleme Çalışma Grubu'nun (Phishing Activity Trends Report-APWG) 2022'de yayınladığı raporda Nisan 2021-Mayıs 2022 arasında 400 bine yakın saldırı olmuş ve bu saldırılar içerisinde 700'ün üzerinde markalar hedef alınmıştır (APWG, 2022).

Kimlik avcılığı yöntemi, dijitalleşmenin toplumlar arasında yaygınlaşması ve internetten alışverişlerin artmasıyla birlikte artış göstermiştir. Bilgisayar kullanıcıların özellikle de alışverişlerinin internet üzerinden gerçekleştirmesi, e-posta yoluyla gelen kampanyaları sorgulamadan açması sonucunda yemleme yöntemine takılmaktadır. Yemleme tekniğinden toplumların korunması için bilinçli kullanıcılar olmaları gerekmektedir (Jakabsson, 2005). Kullanıcıların bilinçlenmesi yemleme saldırıların düşmesine neden olacağı gibi daha spesifik örneklerle karşılaşmaları ve yazılımların kompleks bir yapıya sahip olmalarına da neden olabilmektedir.

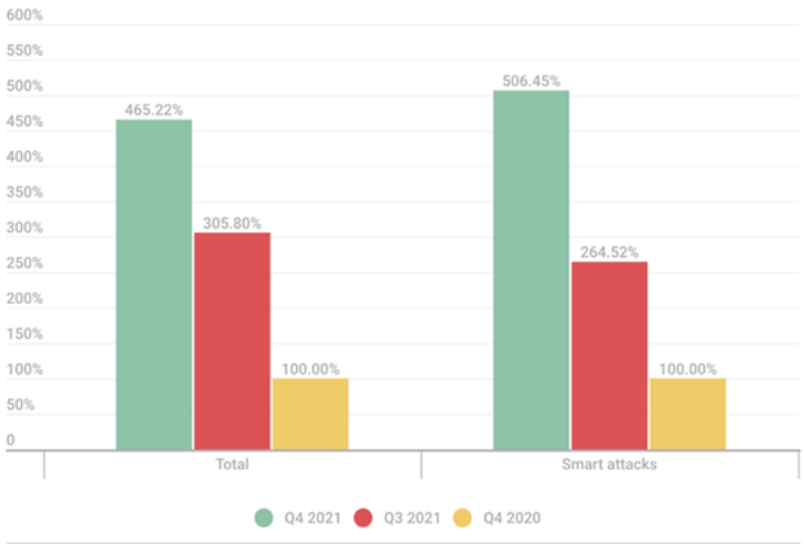
Kimlik avcılığı yöntemine başvuran saldırganlar yöntem olarak en çok sahte e-postalar ve sahte internet siteleri üzerinden gerçekleştirmektedir (Hong, 2012). Saldırganlar kimlik avcılığı yönteminde hedef belirledikleri kitleye yönelik e postalar hazırlamaktadırlar. Bir yönüyle sosyal mühendislik faaliyeti kapsamında da değerlendirmek mümkündür. Saldırganların e postalar ve sahte internet siteleri sonucunda ele geçirdikleri kişisel verileri para karşılığı satarak kar elde etmektedirler. Örnek olarak verecek olursak, çevrimiçi oyunlara giriş için gerekli olan kişisel verilerin ele geçirilmesi ve bu kişisel verilerin başka kullanıcılara satılması sonucunda oyun karakterlerinin satılmasıyla bir gelir elde etmektedirler (Hong, 2012).

1.3.4.5. Klavye Takipçisi

Hedef bilgisayara yerleştirilen program sayesinde kullanıcıların klavye hareketlerini, banka ve diğer alışveriş sitelerinin şifreleri ve diğer hareketlerin toplanarak aralıklarla hackerlere aktaran sistemdir (Akyeşilmen, 2018). Tehlikeli bir uygulama olduğu kadar kodlama aşamasında ucuz olmasından dolayı çokça tercih edilen bir uygulamadır (Tuli & Sahu, 2013). Klavye takipçisi yazılımının çalışması, kullanıcı ve çekirdek tabanlı olmak üzere iki farklı şekilde gerçekleşir. Kullanıcı düzeyindeki yazılımlar, tuş vuruşlarını izlemek için üst seviyede Uygulama Programlama Arayüzü (Application Programming Interface-API) kullanırken çekirdek tabanlı olan yöntemde ise bilgisayar, tablet ve telefonların işletim sistemi çekirdeğinin içinde çalışır ve klavyeden kaynaklanan tüm verileri kaydederek saldırgana iletir (Ladakis, vd., 2013).

1.3.4.6. DoS ve DDoS Saldırıları

DoS ve DDoS (Dağıtılmış Hizmet Reddi) saldırıları temel olarak hedef alınan servera kapasitesinin üzerinde giriş yapılması (Akyeşilmen, 2018) olarak genel bir tanımlama yapılabileceği gibi saldırganların verilen bir hizmetin yasal kullanımını engellemek için giriştikleri gayrimeşru yöntem olarak tanımlanabilir (Mirkovic ve Reiher, 2004). Bu atakların gerçekleşmesinde, ekonomik kazanç elde etme, ideolojik intikam ve siber savaş gibi faktörler etkili olmaktadır (Prasad, vd., 2014). DoS ve DDoS ataklarının gerçekleştirirken birden fazla yöntem kullanılırken sıklıkla başvurulan yöntem saldırganların hedef bilgisayara toplu paket akışı göndererek hedef bilgisayar içerisindeki önemli kaynakları tüketmesine neden olarak diğer kullanıcıların hizmete erişmesine engel olmak üzerine kuruludur (Mirkovic ve Reiher, 2004).



Kaynak: (https://securelist.com/ddos-attacks-in-q4-2021/105784/)

Şekil 7: Yıllara Göre DoS ve DDoS Saldırılarındaki Artış Oranı

DoS ve DDoS saldırıları zaman içerisinde istikrarlı şekilde artarak internet kullanıcılarını ve sistemleri zorlamaya devam etmektedir. Öyle ki 2010'da günlük 1300 DoS ve DDoS saldırısı bildirilirken 2017'de bu rakam günlük 28700 olarak bildirilmiş (Brooks, vd., 2021), 2021'in son çeyreğinde Kaspersky şirketinin DDoS Intelligence sistemine takılan sayıya göre günlük 86700 saldırı gerçekleşmiştir (Gutnikov, vd., 2022). İstikrarlı bir şekilde artış gösteren ataklar sistemlere ve hizmet sağlayıcılarına büyük zararlar verdiği gibi tarihsel gelişimi de çok farklı ilerlemiştir. İlk olarak saldırılar

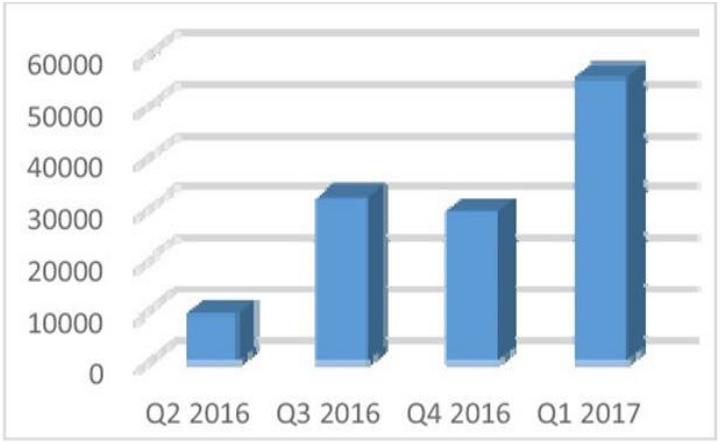
toplumsal olayların protesto edilmesiyle başlamış, daha sonrasında toplumsal olaylar yerini şaka amaçlı ve siber alanda mahlas bırakmak için gerçekleştirilmeye başlamış, bu saldırılar sonucunda para kazanılabileceğini keşfeden saldırganlar para amaçlı saldırılar yapmaya başlamışlar ve son olarak dijitalleşmenin devletler tarafından benimsenmeye başlaması sonucunda maliyetlerinin düşük olmasından ve etkinliğinin fazla olmasından kaynaklı olarak devletler bir saldırı yöntemi olarak DoS ve DDoS saldırılarını gerçekleştirmeye başlamışlardır (Brooks, vd., 2021).

DoS ve DDoS saldırılarından korunmak için birden fazla yöntem bulunmaktadır. Bu yöntem kullanıcılar ve servis sağlayıcılar olarak bir dizi önlemi kapsamaktadır. Kullanıcılar açısından inceleyecek olursak, kaynağı bilinmeyen e-postalar açılmamalı, bilgisayarın ve telefonların güvenlik paketleri her zaman son sürüm olmalı ve kaynağı güvenilir olmayan uygulamaların kullanılmaması gerekmektedir. Servis sağlayıcıları açısından ise internet trafiği içerisinde yer alan bağımsız bir yönlendirici kullanması saldırının erken tespiti ve saldırı esnasında hizmet reddine neden olacak sayıdaki girişlerin aşağı yönlü hareketi sağlayarak saldırının şiddetini azaltmalıdır (Feinstein, vd., 2003). Günümüzde siber alanın aktif kullanılmasından dolayı güvenlik şirketleri de büyük bir pazar haline gelen siber alanda da güvenlik filtrelerini oluşturmaktadırlar. Bu bağlamda servis sağlayıcıları öncelikli olarak gerçek kullanıcılar ile sahte kullanıcıları ayırabilmek adına ağa giren çıkan verileri süzebilecek bir filtre tercih etmeli, güvenlik duvarları oluşturmalı ve güvenlik protokollerini güncel teknolojik gelişmeler ışığında güncel tutmalıdır (Srivastava, vd., 2011).

1.3.4.7. Fidye Yazılımı

Fidye yazılımları, hedef bilgisayara yerleştikten sonra kişisel verilerin ve diğer yazılı ve görsel materyallere erişimi engelleyen kriptolu bir yazılım olmakla birlikte programda belirtilen veyahut saldırgan tarafından belirlenen para veyahut kripto para karşılığında verilerin geri bırakılmasını hedefleyen kötü amaçlı yazılımdır (Richardson ve North, 2017). Diğer kötü yazılımlarda da olduğu gibi siber alandaki faaliyetlerin artmasıyla birlikte kötü yazılımlarında sayısında ve saldırı miktarında da artışları olmuştur. Diğer zararlı yazılımlar gibi fidye yazılımı da yeni bir yazılım olmamakla birlikte yazılımın tarihi ve ilk ortaya çıkması 1980'lere kadar dayanmaktadır.

Fidye yazılımının ilk olarak ortaya çıkması, AIDS hastalığı hakkında uluslararası düzeyde bir konferansa katılan katılımcılara dağıtılan disketlerin içerisine yerleştirilen fidye yazılımı, katılımcıların disketi kullanmasıyla birlikte kişisel veriler kriptolu şekilde kilitlenmiş ve karşılığında Panama'daki bir postaneye 198 dolar ödemeleri karşılığında verilerin açılacağı bir pencere açılmış ve bu durum tarihe AIDS Truva Atı adıyla geliştirildiği için literatüre bu isimle anılmaktadır (Tandon ve Nayyar, 2019; Mohurle ve Patil, 2017).



Kaynak: Aidan, vd., 2017

Şekil 8: 2016 ve 2017'nin 1. Çeyreğinde Fidye Yazılım Saldırıları

Fidye yazılımları karmaşık bir kodlama ile hazırlandıklarından dolayı hedef alınan kurum kuruluş veya kişiler üzerinde büyük zararlara neden olmaktadır. Oluşan zararı yıllara göre açıklamak gerekecek olursak fidye yazılımları, 2016'nın 2.çeyreğinde 10 binin altında saldırılı yapılırken yine aynı yılın 4.çeyreğinde ulaşılan saldırı sayısı 33 bine yaklaşmıştır (Aidan, vd., 2017). Emsisoft'un 2020 için yaptığı tahminlerde de fidye yazılımları sonucunda verilen zararın maliyetinin 42 milyar dolar ile 170 milyar dolar arasında olduğunu belirtmektedir (BBC News, 2021).

Saldırı miktarındaki artışların her yıl katlanarak devam etmesi ve saldırının kurum, kuruluş ve bireysel kullanıcılara verdiği zararın büyük olması nedeniyle çok dikkat edilmesi gereken bir konu olduğu anlaşılmıştır. Fidye yazılımlarının ilk dönemlerinde bireysel kullanıcılar ve küçük gruplar hedef alınırken, zamanla hedef çeşitliliği artmış devlet kurumlarına, şirketlere ve hatta devletlere karşı bir siber saldırı aracı olarak kullanılmaya başlanmıştır. Kronolojik olarak vakalara bakacak olursak:

1989'da "AIDS Truva Atı" isimli yazılımla küçük bir grup hedef alınmış, 2005'de ilk modern fidye yazılımı olan "Trojan.Gpcoder" Rusya tarafından geliştirilmiş ve eski Sovyet devletlerini hedef alan sahte iş başvurusu formu şeklinde ortaya çıkmış, 2006'da artık fidye yazılımlarının karlı olarak görülmesiyle kriptolu fidye yazılımları ortaya çıkmaya başlamış ve ilk örneği olan "Trojan.Cryzip" ortaya çıkmış, 2007'de ilk başta Rusya'yı hedef alan ve daha sonrasında Avrupa ve ABD'ye yayılan ve kullanıcıların e postalarına cinsel içerikli mesajlar gönderen "Lucker" ortaya çıkmış, 2011'de ilk anonim ödeme hizmetiyle ortaya çıkan ve dönemin en büyük fidye yazılımı ortaya çıkmış, 2012'de "Citadel" ve 2013'de ilk kripto para ödemeli fidye yazılımlarının ortaya çıkmasına kadar süreç devam etmiştir (Richardson ve North, 2017).

Yıllar geçtikçe fidye yazılımları da kendisini geliştirmiş ve daha komplike bir yapıya sahip olmaya başlamıştır. Bu bağlamda küresel ölçekte değerlendirilecek 2017'de ilk küresel fidye yazılımı olan "WannaCry" ortaya çıkmıştır. WannaCry isimli fidye yazılımı sadece Microsoft Windows çalıştıran bilgisayarlar arasında yayılmaya başlamış ve kullanıcılardan fidye karşılığında 300 dolar değerinde Bitcoin talep etmesiyle gündeme gelmiş, bu saldırı sonucunda 150 ülkeden 230 bin bilgisayar etkilenmiş ve yaklaşık 4 milyar dolarlık bir kayba neden olmuştur (Kaspersky, 2022).

Günümüzde siber alanın genişlemesiyle birlikte diğer zararlı yazılımların arttığı gibi fidye yazılımlarının sayısı da verdiği zarar da artmaktadır. Öncelikli olarak fidye yazılımlarından korunmak için bilinçlenmek ve güncel gelişmeleri takip etmek, yeni saldırılardan etkilenmemek adına çok önemli olduğu gibi bunun yanında alınacak diğer önlemlerde kullanıcıları fidye yazılımın etkilerinden koruyacaktır. Alınacak önlemleri sıralayacak olursak eğer kullanılan anti virüs programlarınız her zaman lisanslı ve güncel olmalı, e posta kutunuza gelen spam mesajlar açılmamalı, verilerinizin herhangi bir kaybolma durumunda yedeklenmeli, Windows'un güvenlik duvarı açık tutulmalı ve güncel durumda olmalı ve güncel güvenlik sertifikalarına sahip güvenlik paketi kullanılmalıdır (Mohurle ve Patil, 2017). Bu önlemler sayesinde fidye yazılımları başta olmak üzere diğer zararlı yazılımların etkileri minimalize edildiği gibi tamamen engellenmesine de neden olacaktır. Fakat yukarıda bahsedilen önlemlerden hariç olarak öncelikli olarak siber güvenlik ve kötü amaçlı yazılımlar hakkında bilinçlenmek, güvenliğin yarısını oluşturmaktadır.

1.3.4.8. Sosyal Mühendislik

İnternet teknolojilerinin, altyapısının ve bilgisayar teknolojilerinin gelişmesiyle birlikte siber uzayın artan işlem hacmiyle birlikte dünyada bilginin korunması ve veri güvenliğinin sağlanması büyük bir sorun haline gelmiştir. Bilgilerin ve yazılı ve görsel materyallerin siber uzayda bulunması bazı bilgisayar korsanlarının kötü eylemlerine aracı olmakla birlikte bazı iyi niyetli uygulamaların da kötü amaçlarla kullanılmasına neden olmaktadır.

Dünyanın küreselleşmesiyle birlikte toplumlar zamanlarının çoğunu siber alanda bilgi ve veri paylaşarak geçirdiği gibi veri paylaşımlarını sosyalleşmek ve iletişim kurmak amacıyla sosyal medya uygulamaları üzerinden gerçekleştirmektedir. Bireylerin kişisel verilerinin hedef olduğu sosyal mühendislik faaliyetleri siber suçlar kapsamında ele alındığı gibi yapısal olarak siber suçlardan farklıdır. Sosyal mühendislik, anti virüs programlarından, şifreleme yöntemlerinden ve siber suçların ve kötü yazılımların engellenmesi için kullanılan bilgisayarların güvenlik duvarlarından bağımsız olarak gerçekleştirilen eylemler bütünü olmasından kaynaklı olarak farklılığını ortaya koymaktadır (Salahaddine ve Kaabounch, 2019). Bahsettiğimiz bu farklılıktan dolayı sosyal mühendisliğin hedefi kullanıcılar olduğu gibi araç olarak da sosyal medya uygulamalarını kullanmaktadır. Bu nedenle siber suçların gerçekleşmesinde zayıf halka bilgisayarlar olurken sosyal mühendislikte zayıf halka bireylerden oluşmaktadır. Bu bilgiler ışığında genel bir tanımlama yapacak olursak eğer sosyal mühendislik, birçok kullanıcının yeni arkadaşlar edinme, eski arkadaşlarını bulmak isteği ve yazılı ve görsel materyallerinin paylaşma isteğinden kaynaklı olarak sosyal ağları aktif olarak kullanmaktadır. Sosyal medyayı bu hedefler doğrultusunda kullanıldığı gibi sosyal medya uygulamaları da kullanıcıları diğer kullanıcılar ile eşleştirmek ve birbirini tanıma olasılığı hesaplama için kullanıcıların verilerini ve faaliyet hareketlerini toplayarak bir algoritmada işleyerek eşleştirmeye çalışmaktadır (Irani, vd., 2011). Sosyal medya uygulamalarının gerçekleştirdiği bu işlem sosyal mühendislik faaliyetlerinin en masum şekli olarak tanımlanmaktadır.

Sosyal mühendislik faaliyetinin açıklanması adına geliştirilen en büyük proje ise 2014'te veri uzmanı Aleksandr Kogan tarafından geliştirilen ve Global Science Research isimli şirketi kurarak, Meta üzerinden kullanıcılara sunulan "this is your digital life" uygulamasıdır (Berghel, 2018). Kogan tarafından tasarlanan uygulama

kullanıcılara kişilik testi yaptığını öne sürerek yaklaşık 50 milyon kişinin kişisel verilerini ve eğilimlerini toplayarak belirli algoritmik yazılımlarla işleyerek kişilerin siyasi, sosyal, ekonomik ve cinsel eğilimlerine yönelik reklamlar ve düşüncelerini etkileyecek sahte yazılı ve görsel mesajlar ileterek irade dışı eylemler gerçekleştirmelerini hedeflemişlerdir (Berghel, 2018). Global Science Research şirketi daha sonrasında Meta üzerinden kullanıcıları manipüle etmek ve 2016 ABD başkanlık seçimlerinde vatandaşların oy eğilimlerini değiştirmeye yönelik eylemler gerçekleştirdiği gerekçesiyle dava edilen Cambridge Analytica olarak varlığına devam etmektedir.

Kaynak:(https://www.socialsciencespace.com/2018/03/will-cambridge-analytica-hurt-legitimate-research/)

Şekil 9: Cambridge Analytica

Cambridge Analytica şirketi sosyal mühendislik faaliyetini dünya çağında gerçekleştiren bir şirket olmasından ve sosyal medyalardan elde ettiği bilgileri siyasi ekonomik ve kültürel olarak sınıflandıran ve dünyanın farklı ülkelerinde siyasi partilere hizmet veren şirkettir. Cambridge Analytica şirketinin ismi ilk olarak 29 Temmuz 2018'de Avam Kamarası Dijital, Kültür, Medya ve Spor Seçim Komitesinin yayınladığı sahte haberler hakkındaki raporda İngiltere'de yayınlanan Observer gazetesinde yayınlanan bir dizi haberler gösterilmiş ve Cambridge Analytica şirketince yönlendirilmiş olduklarının açıklanmasıyla ortaya çıkmıştır (Heawood, 2018). Observer gazetesinde çalışan Carole Cadwalladr, yaptığı çalışmalar neticesinde bulguları gazetesinde paylaşmış ve Cambridge Analytica'nın veya Cambridge Analytica ile bağlantılı diğer şirketlerin Meta uygulaması üzerinden yaklaşık 87 milyon kullanıcının ayrıntılı psikolojik profillerini oluşturduğunu ve 200 bin Meta üyesi kullanıcısının da kişisel verilerini izinsiz kullandığı ortaya çıkarmasıyla Cambridge Analytica skandalı ile

dünya tanışmış ve sosyal mühendisliğin nasıl bir boyuta geldiği somut şekilde ortaya konmuştur (Heawood, 2018; Gonzalez, vd., 2019).

Sosyal mühendislik faaliyetleri sadece kişisel verilerin elde edilmesiyle ilgilenmediği gibi espiyonaj, kontra espiyonaj, metaverse dünyalarının inşa edilmesi, siber suçların gerçekleştirilmesi ve casusluk faaliyetlerinde de aktif olarak kullanılmaktadır. Öyle ki 2015'te paylaşılan veriler ışığında Türkiye'de gerçekleştirilen sosyal mühendislik faaliyetleri kapsamında zararın 40 milyon olduğu tahmin edilmektedir (Yetgin ve Baştuğ, 2022). Cambridge Analytica şirketi üzerinden örneklendirecek olursak, kullanıcıların ve hatta uygulama geliştiricilerinin izni olmadan oluşturulan veri analiz uzmanlarınca toplanan veriler işlenerek kullanıcıların eğilimleri, yönelimleri, siyasi ve sosyal görüşleri sahte haberler ve reklamlar ile manipüle edilerek düşünceleri ve fikirlerinin değiştirilmesi hedeflenmiştir.

Dijitalleşen dünya ile sınırları belirlenemeyen siber uzay siber suçların işlendiği bir arena olduğu gibi istihbarat ve casusluk faaliyetlerinin de gerçekleştirildiği bir alan haline gelmiştir. Cambridge Analytica, Nijerya, Hindistan, Meksika, Kenya, Brezilya, Ukrayna, İtalya, Çekya ve Litvanya gibi birçok ülkede faaliyetlerde bulunmuştur (Digitalage, 2018). Modern sosyal mühendislik harikası olan şirket, vatandaşların diğer ülkelere olan yaklaşımlarını ve siyasi fikirlerini manipüle ederek faaliyetlerde bulunduğu gibi ulus devletlerin istihbarat servislerinden daha fazla veriyi ellerinde bulundurmuştur. Bir yönüyle şirket uluslararası istihbarat birimi olarak faaliyetler gerçekleştirmiştir.

Sosyal mühendislik faaliyetleri sonucunda kullanıcılar, şirketler, kamu kurum ve kuruluşlar ve hatta ulus devletler hakkında detaylı bilgiye sahip oldukları gibi bu bilgilerin önemli bir kısmı istihbarat seviyesinde de olmaktadır. Bu bilgi ve belgelerin elde edilmesinde ise birden fazla yol ve teknik tercih edilmektedir. Sosyal mühendislik faaliyetlerinde en sık kullanılan yöntem diğer siber suçlarda da aktif kullanılan kimlik avı e postaları ve Truva atı içerikli e postalar kullanılmaktadır (Applegate, 2009). Kaynağı bilinmeyen e postalar, reklam broşürleri veyahut programların aktif edilmesi sonucunda kullanıcının bilgisayarına veyahut akıllı telefonuna yerleştikten sonra bir dizi programları da kullanarak kullanıcıların kişisel verilerinin ele geçirilmesi sonucu işlenmesi olarak açıklanabilir. Diğer saldırı yöntemi ise gayri resmi olarak elde edilen verilerin işlenerek kullanıcıya ikna yoluyla kabul ettirilip rüşvet karşılığında geri

verilmesidir (Applegate, 2009). Bir diğer yöntem ise omuz sörfü olarak tanımlanmaktadır. Saldırıyı gerçekleştiren kişinin kullanıcı adını ve parolasını girerken şüphelenmeyen kullanıcının omzunun üstünden bakması sonucu elde ettiği kişisel veridir (Applegate, 2009).

Sosyal mühendislik faaliyetlerinden etkilenmemek öncelikli olarak diğer siber saldırı araçlarında uygulanan güvenlik protokolleriyle benzerlik göstermektedir. Diğer siber saldırı türlerinden farklı olarak sosyal mühendislik faaliyetlerinden etkilenmemek için ekstra olarak sosyal medya uygulamalarını kullanırken kullanıcı profillerine detaylı bilgilerin yazılmaması ve yine uygulama üzerinden güvenlik açığı oluşturacak yazılı ve görsel materyallerin paylaşılması konusunda da hassas davranılmalıdır. Diğer saldırı türlerinde olduğu gibi sosyal mühendislik faaliyetlerinde de kullanıcıların bilinçlenmesi ve gerekli görülen seminerlere katılması faydalı olacaktır.

1.3.5. Siber Tehditlerle Mücadele Yöntemleri

Siber alanda gerçekleştirilen saldırılar ve kullanılan araçlar siber tehditler arasında gösterilmektedir. Siber tehditler teknolojik altyapının ve bilgisayar sistemlerinin gelişmesiyle kısa süre içerisinde artışa geçmiştir. Bugün siber tehdit unsurları olarak sayabileceğimiz, virüsler, solucanlar, fidye yazılımları, klavye takipçileri ve diğer araçlar gibi unsurlar tehditler sınıfında olduğu gibi bireysel saldırıların dışında devletlere ve uluslararası şirketlere gerçekleştirilen saldırılarda kullanılan DDoS saldırıları ve diğer türler de sayılmaktadır. Siber alanda gerçekleştirilen saldırı araçları ve bu araçlar ile bireysel saldırıların dışında uluslararası şirketlere ve örgütlere ve devletlere gerçekleştirilen saldırıların sonucunda siber güvenliğin önemi ortaya çıkmış ve bireyden devlete kadar olan yapıda siber güvenlik politikalarının ve yol haritalarının ortaya çıkmasına neden olmuştur.

Siber güvenlik politikaları belirlenirken kişi, kurum, kuruluş ve devletlerin farklı istek ve politikalarına göre şekillenmektedir. Örneğin ekseriyetle bireyler kendi siber güvenlik politikalarını oluştururken öncelikli olarak kişisel verilerin korunması, dijital mahremiyetin sağlanması ve parola güvenliğinin sağlanması üzerine dururken ulusal ve uluslararası şirketler, müşterilerinin kişisel verilerinin korunması, şirketlerinin ticari sırlarının ifşa edilmemesi ve şirketlerin gizli mahiyette bulunan ticari yönelim ve yatırımlarının ifşa edilmemesi üzerine siber güvenlik politikaları oluşturmaktadır.

Devletler ise hem bireylerin hem de bünyesinde barındırdığı ulusal şirketlerinin, ticari kazançlarını korumak ve kişisel verilerin güvenliğinin denetlenmesi üzerine siber güvenlik politikaları geliştirmektedir. Fakat devletler siber güvenlik politikalarını oluşturulurken bireylerden ve şirketlerden farklı olarak fiziki dünyada gerçekleştirilen istihbarat toplama, casusluk ve hatta savaşları da sanal ortama aktararak oluşturdukları bu alanı da siber güvenlik politikaları içerisine yerleştirerek yasal bir boyut oluşturmaktadırlar.

Siber güvenlik politikaları sadece siber suçların sayısı veya siber saldırıların sayısının artmasına karşılık geliştirilen bir politika olmamakla birlikte devletler düzeyinde inceleyecek olursak devletleri derinden etkileyen ve toplumsal hafızadan silinmesi zor olan olaylar sonucu da gerçekleştirilmektedir. Bu açıdan 11 Eylül saldırısı sonrasında ABD yönetiminin belirlediği siber politika ve 2007 Estonya saldırısı en iyi örnektir. Açıklamak gerekirse, 11 Eylül (9/11) 2001'de gerçekleştirilen saldırının hemen sonrasında ABD yönetimi Birleşmiş Milletler Genel Kurulu'nu toplamış ve 1368 sayılı kararı alarak terörün her türü ile mücadele etmek için gerekli olan tedbirleri almaya hazır olduklarını bildirdikleri gibi (Yetgin ve Baştuğ, 2022a). ABD'yi terörle mücadele konusunda desteklemeyecek olan ülkeleri de terörist olarak kategorize edileceğini bildirerek göz dağı vermiştir (Örnek, 2012). 9/11 saldırılarının klasik yöntemli bir terör saldırısı olmasına rağmen bu saldırıda da siber uzayın kullanışmış olması terörün siber uzay aracılığıyla da yapılabileceği anlaşılmıştır. Gerçekleşen terör saldırısı sonrasında dönemin ABD başkanı George W. Bush, 2002'de Ulusal Güvenlik Başkanlık Direktifi 16'yı imzalayarak hükümete düşmanlarına karşı siber saldırılar hazırlamak için yol gösterici politikalar hazırlamakla görevlendirmiştir (Türkay, 2013). 2003'te siber saldırılara ABD güvenlik topluluğunca karşılık verme koordinasyonunun geliştirilmesi amacıyla "Güvenli Siber uzay Ulusal Stratejisini ve askeri kapasitenin gelişen teknolojiyle uyumlu olması ve yine aynı yıl Savunma Bakanlığı Bilişim Operasyonları Yol Haritasında oluşan yeni fırsatları kullanarak yeni çıkan tehditlere ayak uydurması gerektiği vurgulanmıştır (Türkay, 2013). 2011 yılında Siber Uzay Stratejisi: Ağa Bağımlı Bir Dünyada Refah, Güvenlik ve Açıklık raporunu yayınlayarak uluslararası ticareti destekleyen ve açık ve güvenilir iletişim altyapısının teşvik edilmesi gerekliliği vurgulanmıştır (Selçuk, 2020), 2015'te yayınlanan Milli Güvenlik belgesinde siber güvenlik ve siber saldırılar yer almış ve yine 2015'te Savunma Bakanlığınca hazırlanan strateji belgesinde siber güvenlik hedefleri belirlenmiş ve 2018'de Ulusal Siber Strateji

yayınlanarak ABD başkanı vatandaşlarının ulusal güvenliği ve refahını kendine öncelik olarak kabul ettiğini beyan etmiştir (Selçuk, 2020).

Kaynak: (https://ccdcoe.org/)

Şekil 10: NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCOE)

Bir diğer vaka ise 2007'de Estonya'ya yönelik gerçekleştirilen siber saldırı da bir devleti çaresiz bıraktığı ve dünya ile bağlantılarının kesilerek çaresiz bırakılmasına örnek olduğu gibi NATO'nun siber güvenlik politikaları belirlemesinde önemli bir adım olmuştur. 2007'de Estonya'nın başkenti Tallinn'de bulunan Sovyetler döneminden kalan Bronz Asker Heykeli'nin Estonya hükümeti tarafından kaldırılması sonucu başlayan siber saldırılar sonucunda Estonya'nın bütün sistemleri ele geçirilerek iflas etme noktasına gelmiştir (Akyeşilmen, 2018). Estonya hükümeti saldırıların arkasında Rusya'nın olduğunu açıklamasına rağmen Rusya bu durumu inkâr etmiştir. NATO üyesi olan Estonya'ya yönelik yapılan geniş siber saldırı sonucunda NATO'nun siber kuvvet eksikliği de ortaya çıkmıştır. Buna bağlı olarak NATO, 2008 yılında Bükreş Zirve'sinde bu tarz saldırıların önlenmesi ve hangi adımların atılacağı kararlaştırılması adına Brüksel'de bir NATO Siber Savunma Yönetim Otoritesi'nin (Cyber Defense Management Authority- CDMA) kurulması kararlaştırılmış ve siber savunma kapasitesini tek bir merkezde toplamak için başkent Tallinn'de NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCOE) kurulmasına karar vermiştir (Ada ve Çakır, 2017; Baştuğ, 2022; Darıcılı, 2020).

Devletler ve uluslararası örgütler fiziki güvenliklerinin yanı sıra siber alanda da güvenliklerini sağlamak adına tedbirler aldıkları gibi bireyler de siber alanda gerçekleştirdikleri eylemler için de güvenliklerini sağlamaktadırlar. Bireylerin siber alandaki verilerinin ve siber alanda gerçekleştirdikleri eylemler hem devletler ekseninde

hem de bireysel olarak korunmaktadır. Her devlet vatandaşlarının siber alanda doğacak zararların engellenmesi hem de güvenliklerinin sağlanması adına kanun düzeyinde değişiklikler yapmaktadır. Fakat devletleri yapı taşı olan bireyler de siber güvenliklerinin sağlanması için bilinçlenmesi gerekmektedir. Bugün siber alanda gerçekleştirilen sosyal mühendislik faaliyetleri, DoS ve DDoS saldırıları, fidye yazılımlar ve diğer saldırı araçları öncelikli olarak bireyleri hedef alarak elde ettikleri veriler, büyük bir yapboz parçasının küçük bir kısmını oluşturmakta ve ulusal ve uluslararası güvenliği tehdit edebilecek bir açık oluşturmaktadır.

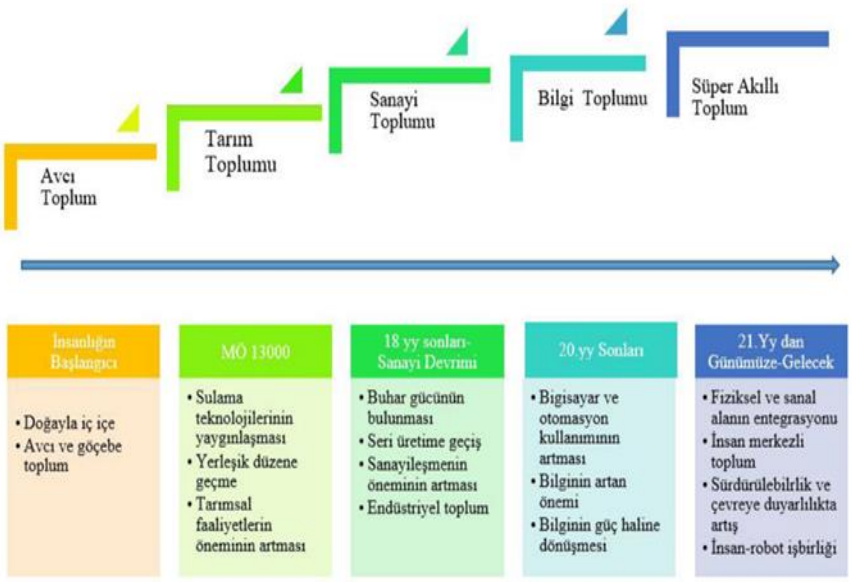
Siber alanda gerçekleştirilen saldırılarda ilk hedef olarak bireylerin alınmasında güvenliğin en zayıf halkasının bireyler olmasından dolayı öncelikli ilk hedef bireylerdir. Bireylerin zayıf halka olmaması için öncelikle siber alanın kapasitesini ve siber alanda yürütülen faaliyetlere ve saldırılara yönelik bilgi edinmesi gerekmektedir. Edinilecek olan bilgiler siber farkındalığın oluşmasına neden olacaktır. Siber farkındalığın oluşması için bireysel faaliyetlerin dışında okul, lise ve üniversite seviyelerinde düzenli ve yeni teknolojilerle gelişen eylemler siber güvenliğe entegre edilerek zorunlu olarak anlatılmalı ve ulusal bir güvenlik meselesi olarak algılanmasını sağlanmalıdır.

1.4. Toplumun ve Devletin Dijitalleşme Süreci

1.4.1. Toplum 5.0 ve Siber Güvenlik

Bilgi ve iletişim teknolojilerinin hızlı gelişimi toplumsal ve sektörel olarak büyük değişiklikleri de beraberinde getirmiştir. Dijital dönüşüm devletlerin ve şirketlerin dönüşmesini ve refah seviyesini artırdığı gibi toplumların da büyük oranda kültürel, siyasal, ekonomik ve manevi değerlerinde değişimlere neden olmuştur. İnternet ve bilgisayar teknolojilerinin yaygınlaşmaya başlamasıyla birlikte toplumlar da bilgiye açık, sorgulayan ve araştıran bir yapıya bürünmüştür. Toplum 5.0, akıllı toplum veyahut dijital toplum olarak adlandırılan yeni toplum modeli ilk olarak 1996'da Wired dergisinde yayınlanan Dijital Toplum İçin Manifesto ile dile getirilmiş ve internetin yaygınlaşması toplumun temelden değişeceğini belirttiği gibi bilginin sınırsız bir yapıya kavuşmasına olanak sağladığı için dolaylı yönden siber alanın kapasitesinin de belirsizliğini bizlere göstermiştir (Yetgin ve Baştuğ, 2022; Graham, 1998).

Tarihsel olarak insanlığı incelediğimizde her zaman yaşam standartlarının iyileşmesi ve refah seviyesinin artırılması için yeni yollara aramışlar ve dönemsel olarak dünyayı değiştirecek yeni buluşların bulunmasına yardımcı olmuşlardır. Örnekle açıklamak gerekirse sanayi devrimiyle bedenen çalışan toplumlar artık makinelerle tanışmış ve insan gücünü makinelere aktararak daha hızlı ve verimli işlemler gerçekleştirmeye başlamış, elektrik gücünün keşfedilmesiyle buharlı araçların çalışması için gereken enerji kaynaklarının çıkarılması için gerekli olan insan kaynağı da azalarak elektrikle çalışan aletlere dönüşmüşken dijital devrim olarak adlandıracağımız ilk bilgisayarların ortaya çıkmasıyla insanın yapması gereken işin bilgisayarlar tarafından hızlı, hata payı düşük ve etkili çalışma modeline geçilmiş ve son olarak üretim hattından fabrikaların satış planlamasına ve üretimde insan faktörünün azaltılarak robot ve makinelerin kullanılmasına kadar evrilmiştir (Saracel ve Aksoy, 2020).



Kaynak: (Duman, 2022).

Şekil 11: Tarihsel Süreç İçerisinde Toplam 5.0'a Geçiş

Toplum sürekli olarak yenilik ve refah üzerine çalışmalarını yürütürken devletlerde vatandaşlarının refahı için bazı adımlar atmaktadır. Bu bağlamda Toplum 5.0 kavramı, dönemin Japonya Başbakanı Shinzo Abe tarafından dünyada sanayi 4.0'ın etkisiyle birlikte gelişen dijital dönüşümün demografik, etnik, kültürel ve sosyolojik yönden değerlendirerek insanlar ile robotlar arasındaki iletişimi en etkili verimli şekilde

sağlanması olarak tanımlanan ve Japonya'da resmi olarak 22 Ocak 2016'da kabul edilen bir dönüşüm felsefesidir (Arı, 2021). Toplum 5.0'ın tanıtılması toplumsal bir vizyonun oluşması için gerekli bir adım olarak görülmektedir. Bu vizyon kapsamında Japonya, yeni teknolojileri bir araya getirerek hem ekonomik kalkınmayı hem de BM'nin belirlediği Sürdürülebilir Kalkınma Hedeflerine erişebilmek için dünyadaki sosyal sorunların çözülmesi için bir fırsat olarak görmektedir (Potocan, vd., 2020).

Toplum 5.0'ın sadece Japonya ile kalmayıp diğer devletlerinde benimsemesi teknolojik gelişmelerin insan merkezli olarak tekrardan yenilenmesi için büyük bir adım olacağı gibi insan ile makine arasında oluşacak olun sorunların giderilmesine yardım sağlayacaktır. Ayrıca Toplum 5.0 ile toplumların mevcut koşullarının tanımlanmasına insanların sorumlu bir birey olmalarına yardımcı olacaktır (Potocan, vd., 2020). Sorumlu insanın oluşması topluma büyük faydalar sağlayacağı gibi siber alanda insanın zayıf halka olmasının da önüne geçecektir.

1.4.2. Devlet Anlayışının Değişmesi: E-Devlet

Toplumda ve sanayide gerçekleşen devrimler ile toplum ve sanayi gibi devletlerin de siber alanda varlık göstermelerine neden olmuştur. Bugün devletler birçok eylemi siber alanda gerçekleştirmektedir. Devletler bugün gerçekleştirmek istedikleri eylemleri siber alanda gerçekleştirmek istemesinde bazı sebepler vardır. Bu sebepler toplumun refah seviyesini artırmak, kamuda israfın önüne geçilmesi ve bürokrasinin hızlanması amaçlı olduğu gibi devletin suç önleme, istihbarat ve casusluk faaliyetleri gibi eylemleri de siber alanda gerçekleştirmektedir. Devletler teknolojik gelişmeleri günümüzde dikkatlice takip ettiği gibi kamu hizmetlerine de entegre ederek vatandaşlarının hızlı ve etkin şekilde hizmet almalarını sağlamaktadır. Bu bağlamda devletler dijitalleşme yoluna gitmektedirler.

E-devlet veya elektronik devlet, devletlerin vatandaşlarına fiziki olarak sunduğu hizmet ve uygulamaların elektronik ortamda kesintisiz ve güvenli olarak yürütüldüğü (Efendioğlu ve Sezgin, 2017), vatandaşlarının yaşam kalitesini artırmak, bilgiyi yaymak, sosyal uyumu güçlendirmek ve kamu kurum ve kuruluşların küresel elektronik pazarda rekabetçi kalmasını sağlamak üzerine kurulu olan uygulamadır (Lambrinoudakis, vd., 2003). E-devlet sistemine geçmeyi hedefleyen bir devlet, gerekli kaynaklara sahip olsa da vatandaşların da bu sistemi kullanmak için belirli bir altyapı ve donanıma da sahip

olması gerektiği gibi bu durum bir ülkenin de gelişmişlik seviyesine bağlıdır (Naralan, 2018).

Dünyada birçok devlet (Türkiye, Estonya, ABD, Finlandiya, Singapur, vd.) dijitalleşme yoluna girmiş ve e-devlet uygulamasına geçiş yapmıştır. Fakat e-devlet sistemi de siber alanı aktif kullanmasından dolayı bazı problemleri de beraberinde getirmektedir. Bu problemlerden ise en önemlisi vatandaş ile uygulama arasındaki kopukluk ve e-devlet uygulamasının siber güvenliği. Dünyada gerçekleştirilen hizmet reddi saldırılarında devletlere yönelik ilk saldırı elektronik hizmetlerine yönelik olmaktadır. Örnek olarak 2007'de Estonya'ya yönelik gerçekleştirilen saldırılarda ilk hedefi iktidar ve diğer partilerin internet siteleriyle birlikte devlet kurumlarının ve Estonya parlamentosunun sayfaları erişime engellenmiş ve kullanıma kapatılmıştır (Darıcılı, 2020).

E-devlet uygulamasına yönelik gerçekleştirilen bu saldırılar vatandaşların devlet hizmetlerinden mahrum kalmasına neden olduğu gibi hizmet alan vatandaşların da kişisel verilerinin ele geçirilmesine de neden olmaktadır. Kişisel verilerin gizliliği devletler tarafından temel hak ve özgürlüklerinin korunması kapsamında korunduğundan dolayı e-devlet uygulaması içerisinde kişisel verilerin güvenliği için adım atılmaktadır. Bu bağlamda devletler fiziki hayatta olduğu gibi genel de siber alanda özelde ise e-devlet uygulaması içerisinde vatandaşlarının kişisel verilerini anayasal güvence altına alması, kişisel verilerin belirli ve temel ilkelere uygun olarak işlemesi, vatandaşlarının siber haklarının belirlenmesi ve hukuka uygun olup olmadığını denetleyecek mekanizmanın oluşturulması sağlamakla yükümlüdür (Bağcı, 2021).

1.5. Siber Uzayda Güç Kullanımı

1.5.1. Siber Güvenliğin Sağlanmasında Yumuşak Güç Unsuru ve Meşru Müdafaa

Uluslararası ilişkiler disiplinine 20.yy'ın başlarında realizm ile giren güç kavramı, bir devletin başka bir devlete karşı hedeflerinin gerçekleştirilmesi için uyguladığı baskı veya şiddet unsuru olarak tanımlanır (Yılmaz, 2011). Başka bir ifade ile açıklamak gerekecek olursak uluslararası ilişkilerde güç, başka bir aktör üzerinden etki yaratmaktır (Korhan, 2020). Devletler anarşik bir uluslararası sistem içerisinde

hayatta kalmak ve güvenliklerini sağlamak adına çeşitli yöntemler kullanmaktadırlar ve bu durum sıklıkla güç unsurunun aktif kullanılmasıyla oluşmaktadır. Küreselleşmenin yayılan dalgaları ile devletler sert güç unsurdan hariç yumuşak güç unsurunun da varlığını kabul etmişler ve uygulamaya başlamışlardır.

Yumuşak güç kavramı uluslararası ilişkiler literatürüne 1990 yılında Joseph S. Nye tarafından kaleme alınan "Liderliğe Zorunluluk: Amerikan Gücünün Değişen Doğası" adlı kitabında, bir ülkenin diğer ülkeye karşı zorla veya baskı altına almadan istediğini yapmaya ikna etme kabiliyeti olarak tanımlamıştır (Yılmaz, 2011; Yatağan, 2018). Soğuk Savaş ile gücün bileşenleri değişiklik göstermeye başlamış (nükleer, uydu, vd.) ve soğuk savaş sonrası yeni bileşenlerin doğmasına ve güç unsurunun yeniden tanımlanmasına neden olmuştur. Özellikle Soğuk Savaş ile başlayan rekabetçi uzay yarışı beraberinde internetin doğmasına neden olduğu gibi bir fiziki hayatta bir karadeliğin oluşmasına da neden olmuştur. Oluşan bu karadelik derin internet olarak anılırken yeni bir yumuşak güç unsuru olan siber gücün ortaya çıkmasına neden olmuştur.

Nye siber gücü, siber alanda gezen bilgilerin birbirine bağlanarak kullanılması yoluyla elde edilen bilgiler ışığında istenilen sonuca ulaşılması olarak tanımlarken (Korhan, 2020), Kuehl, tüm operasyonel alanlarda klasik güç araçlarına avantajlar yaratmak ve olayların gidişatını etkilemek için siber uzayı aktif olarak kullanmak olarak tanımlamıştır (Kuehl, 2009). Tanımları incelediğimiz zaman ortak noktanın bilgiden geçtiği ve sert gücün yerine bilgi gücünün öneminin ortaya çıktığı anlaşılmaktadır. Nye'a göre bilgiye bilgi kaynaklarının güç olarak kullanılması yeni bir olgu değilken siber güç yeni bir olgudur (Korhan, 2020). Siber alanın kendisini sürekli yenilemesi ve yeni teknolojik gelişmelerle birlikte sınırlarının belirsiz olması yumuşak güç unsuru olmaktan çıkıp kontrolsüz bir güç unsuru olarak da görülmesine neden olmaktadır. Siber alanın kapasitesinin ve etkisinin kesin olarak bilinememesi, gerçekleştirilecek eylemlerin etkilerinin de belirsiz olmasına neden olmakta ve bu durum beraberinde devletlerarası meşru müdafaanın oluşmasına neden olmaktadır.

Dijital çağ, beraberinde büyük yenilikler ve kolaylıklar getirdiği gibi adi suçların artmasına, saldırıların artmasına ve terör saldırılarının da siber alanda gerçekleştirilmesine neden olmuştur. Özellikle 9/11 saldırılarından sonra siber terörizm kavramı duyulmaya başlanmış ve bu durum beraberinde suçun önlenmesi ve saldırıya

uğrayan devletin kendisini savunması için gerekli olan meşru müdafaa yetkisini kendisinde bulmasına olanak sağlamıştır. Gerçekleştirilen saldırılara baktığımız zaman (9/11 terör saldırısı, Estonya saldırısı, İran'a yönelik gerçekleştirilen Stuxnet saldırısı, Arnavutluk saldırısı, vd.) meşru müdafaanın ortaya çıkmasına neden olmasına rağmen devletler tam olarak bu durumu yerine getirememektedir. Siber alanda gerçekleştirilen saldırıların kaynağının belirli olmaması, siber ayak izin takip edilememesi ve itham edilen devletlerin kabullenmemesi sonucunda meşru müdafaa kullanılamaz duruma gelmektedir. Siber saldırılar meşru müdafaa durumunu gündeme getirse de yetersiz bilgi ve kanıt nedeniyle meşru müdafaanın ölü doğmasına neden olmaktadır.

Her ne kadar meşru müdafaa siber alanda etkin olarak kullanılamasa da devletler siber alanda hedef gösterdikleri devletlere karşı yumuşak güç unsurlarını farklı alanlarda (ekonomik, sosyal, askeri, siyasi vd.) kullanmaktadırlar. Devletler yumuşak güç unsurlarını birbirlerine karşı sıkça kullandıkları gibi BM, AB ve NATO gibi uluslararası kuruluşlarda sıklıkla kullanmaktadırlar. Genellikle uluslararası kuruluşlar yumuşak gücü yaptırım yoluyla kullansalar da teşhir etme yoluna da başvurmaktadırlar. Bizzat BM tarafından açıklanmasa da Ekonomi ve Barış Enstitüsü tarafından ülke ve bölgelerin ne kadar barışçıl durumda olduğunu açıklayan bir liste oluşturulmakta ve bu liste BM Sekreterliği tarafından yayınlanmaktadır (Akkuş, 2020). Özellikle ülkeler bu endekste üst sıralara çıkmak için bir dizi önlemler aldıkları gibi sert gücü kullanmaktan da kaçınmaktadırlar. Ayrıca BM, Birleşmiş Milletler Bilim ve Kültür Kurumu (UNESCO), Uluslararası Adalet Divanı, BM Barış Gücü ve BM Mülteciler Yüksek Komiserliği gibi küresel organizasyonlar da küresel barışın sağlanması adına yumuşak güç unsurlarını kullanmaktadırlar.

1.6. Siber Uzayda Egemenlik

1.6.1. Dijital Vatandaşlık

Literatürde dijital vatandaşlık için farklı yorumlar ve tanımlamalar mevcuttur. Optus şirketi dijital vatandaşlığı, dijital araçların olanaklarından maksimum seviyede yararlanan ve oluşabilecek olan tehditleri de minimum seviyeye indiren kişi olarak tanımlamaktadır (Akyeşilmen, 2018).Vatandaşlık, bir ülkeye bağlı olan ve o ülkenin haklarından yararlanan kişiler için verilen bir isimken devletlerin dahi sanallaştığı bir

yüzyılda vatandaşlık kavramının da tanımı ve kapsamı değişmiştir. İlk olarak literatüre Mike Ribble ve Gerald Bailey tarafından 2004'te kazandırılan kavram, teknolojik gelişmeleri yakından takip eden ve teknolojik becerileri verimli kullanarak siber alanı sorumluluk sahibi olarak kurallarına uygun olarak kullanan kişiler için kullanmıştır (Aldemir ve Avşar, 2020). Günümüzde bir internet kullanıcısı birey, bulunduğu coğrafya veyahut ülkeden ayrılarak farklı bir coğrafyada veyahut ülkede eğitimlere, seminerlere ve ilişkilere başlayabilmektedir. Klasik devlet anlayışı ile sanallaşan devletler arasında ortadan kalkan sınırlar, vatandaşların siber alanda rahat ve kontrolsüz hareket etmelerine olanak sağlamakta ve vatandaşların özgürlük alanlarının genişlemesine neden olmaktadır.

Dijital vatandaşlık literatürümüze yeni ve gelişmekte olan bir kavram olarak girmesinden kaynaklı olarak doğal boşluklar bulunmaktadır. Yeni ve kısıtlı kaynaklardan elde edilen ve genel bir tanımlama çerçevesinde değerlendirdiğimiz dijital vatandaşlık kavramı, teknolojik gelişmeler ve siber alanın daha da genişlemesiyle birlikte netlik kazanmaya devam edecektir. Mike Ribble, dijital vatandaşlık kavramını 9 boyutta incelemeye çalışsa da dijital araçların kullanım yaşının her geçen sene daha da düşmesi ve yeni neslin doğar doğmaz dijital yerli olarak dünyaya gelmesi sebebiyle net bir bilgi vermenin zorluğundan bahsetmektedir (Çubukçu & Bayzan, 2013). Fakat genel bir inceleme yapacak olursak, eldeki veriler ışığında dijital vatandaşlığın unsurlarından bahsetmek gerekirse, ait olma, katılma ve koruma üzerine üç temel unsur üzerinde oluşmaktadır (Akyeşilmen, 2018). Siber alanda bireyler hangi din, dil, millet ve coğrafya fark etmeksizin siber alanda nereye ait olmak isterlerse oranın vatandaşı olabilmektedirler. Katılma unsuru, bireyler siber alanda gerçekleştirdikleri eylemler ve internet kullanımı için aktif katılım gerçekleştirdiklerinden dolayı katılım dijital vatandaşlığın olmazsa olmazı olarak gösterilebilir. Son unsur olan koruma unsuru diğerlerinden farklı bir noktadadır. Siber alana katılım sağlayan birey dijital varlıkları ve içerikleri tükettiği gibi siber alanda tüketiminin karşılığında içerik, uygulama ve yazılımda üreterek katkı sağlayarak mevcut yapının korunmasına ve sistemin işleyişine katkı sağlamaktadır (Akyeşilmen, 2018).

1.6.2. Siber Vatan

Son dönemde ortaya çıkan siber vatan kavramı dijital vatandaşlık kavramı gibi yeni bir kelime olmasından kaynaklı tanımsal boşlukları bulunmaktadır. Cumhurbaşkanı Recep Tayyip Erdoğan tarafından dile getirilen siber vatan kavramı, vatan savunmamızı, denizde mavi vatanı olduğu gibi, dijital dünyada siber vatanı da içine alacak şekilde genişletme şeklinde tanımlamıştır (Kanca ve Sağıroğlu). Söz öbeği olarak siber vatan kavramına bakacak olursak Türkiye'nin dijital araçlarını ve dijital kapasitesini oluşturan unsurların kritik altyapıları korumak üzerine oluşturulan doktrin olarak tanımlamakta mümkündür (Aydın, 2022). Siber alanda ülkelerin faaliyet göstermeleri bir nevi fiziki dünyadaki gibi devletlerin siber alanda da sınırlarını çizmişler ve bu sınırlarda egemenlik faaliyetlerini sürdürmektedirler. Fakat siber alanın sınırlarının bilinmemesi nedeniyle devletler dijital sınırlarını ve kırmızı çizgilerini siber alanda da oluşturmaktadır.

Devletler fiziki dünyada fiziki sınırlar içerisinde vatandaşlarının kişisel verilerini, haklarını, ulusal gizlilik seviyesindeki bilgi ve belgeleri korumakla yükümlü olduğu gibi dijital ortamda serbest dolaşan verilerin ve vatandaşlarının da bilgilerini korumakla yükümüdür. Bu koruma durumu vatanın da dijitalleşmesine neden olmaktadır. Siber vatan kavramı genç ve yeni bir kavram olmasından dolayı çok farklı yaklaşımlar bulunduğu gibi genel ve açıklayıcı bir tanımlama yapmak gerekirse, bir ülkenin iletişim altyapısının, kritik kurum ve kuruluşlara ait olan siber alanda yer alan bilgi ve belgelerin, vatandaşların temel hak hürriyetlerini engelleyecek ve tehlikeye atacak eylemlerin ve siber ortamda işlenen adi suçların, savaşların, istihbarat ve casusluk faaliyetlerinin engellenmesi adına siber alana çizilen sınır olarak tanımlamak mümkündür. Fakat siber güvenlik araştırmacısı Burak Bozkurtlara göre kıta sahanlığı gibi bir siber sınır çizmek pek mümkün olamayacağı gibi siber vatanı tanımlamak için çıkarılan kanunlara da kanun koruyucuların da zaman zaman uymaması vatandaşların devlete olan bağlılık ve inancında zayıflama olacağını savunmaktadır (Bozkurtlar).

Devletler, dijitalleşme ile işlemlerini siber alanda gerçekleştirdiklerinden dolayı fiziki varlıklarını tehdit eden unsurlara karşı hazırlıklı oldukları gibi siber alandan da gelecek olan tehdit ve saldırılara vatan savunması gibi tepki vermelidir. Bu bağlamda her devlet bünyesinde siber operasyon birimi oluşturmakta ve beyaz şapkalı olarak isimlendirilen hackerleri işe almaktadır. Göreve başlayan hackerler, kritik altyapı ve

iletişim sistemlerine gelecek olan siber saldırıların yanı sıra vatandaşların kişisel verilerinin ve eylemlerinin güvenli bir şekilde dolanmasını ve tehditlerin engellenmesine yönelik çalışmalar gerçekleştirmektedir. Fakat oluşan siber vatan kavramı tamamen savunma odaklı olmamakla birlikte ülkenin menfaat ve çıkarları konusunda da siber alanda faaliyette de bulunabilmektedirler.

2. SİBER ALANIN HUKUKİ BOYUTU

2.1. Siber Hukuk

2.1.1. Siber Hukuk Nedir ve Neden Gerekli?

İnternet ve bilgi teknolojilerinin gelişmesi, makineler ile insanlar arasındaki etkileşimin artması siber alanın çok yoğun kullanılmasına neden olduğu gibi siber alanının bir zorunluluk haline gelmesine neden olmuştur. Siber alanda milyarlarca kullanıcının anlık olarak birbiriyle etkileşim içerisinde olması büyük küreselleşme hareketlerini beraberinde getirmiş, olumlu ve yapıcı sonuçlar doğurduğu gibi beraberinde olumsuz sonuçlar doğurmasına da neden olmaktadır. Kullanıcıların farklı coğrafyalar ve farklı lisanda olmalarına rağmen siber alanda ortak bir payda da buluşup karşılıklı olarak veri paylaşımı içerisinde olabilmektedirler. Olumsuz yanı ise siber alanda milyarlarca kullanıcının milyarlarca veriyi ve bilgiyi bir denetim mekanizması olmaksızın paylaşması ulus devletlerin kendi halkları üzerinde kontrollerini kaybetme endişesini doğurmaktadır (Kiraz, 2021).

Son 20 yılda siber alanın kapasitesinin ve alanının genişlemesi, kontrolsüz bir güç unsuru olarak ortaya çıkmasına neden olmuştur. Siber alandan ilk olarak temel bilgi seviyesinin eksikliğinden kaynaklı olarak bireysel kullanıcılar etkilenmiş, daha sonrasında tüketim çılgınlığının artması ve küreselleşen artan rekabet ortamından kaynaklı olarak şirketlerin siber alandaki etkilenmiş ve en son olarak ulus devletler istihbarat, karşı istihbarat, casusluk, siber savaş ve siber saldırılara maruz kalmışlardır. İnternet ve bilgisayar teknolojilerinin ilk zamanlarında bu sorunlar fazla dile getirilmezken, 21.yy'ın ilk çeyreği ile kullanıcılar, şirketler ve devletler siber alanın üstünlüğünü kabul etmişler ve önlemler almaya başlamışlardır.

Hukuk, dinamik bir yapısı olmasından kaynaklı olarak sosyal, ekonomik, kültürel ve siyasal boyutları bulunmaktadır (Kiraz, 2021). Siber alan da tek başına siyasal, kültürel, sosyal ve ekonomik boyutları bünyesinde barındırmasından kaynaklı olarak hukuk kavramıyla birbirine benzediği gibi oluşturulacak olan siber hukuk da her ülkenin kendi örf ve kültürü, teknolojik gelişme düzeyi ve yaşam standartlarının farklı olmasından kaynaklı olarak oluşturdukları siber hukuk da birbirinden farklı olmaktadır (Kiraz, 2021). Kapsayıcı bir tanımlama yapmak gerekirse siber hukuk, siber alanda

kullanılan araçları (bilgisayarlar, yazılımlar, veri depolama cihazları, akıllı telefonlar, internet, vd.) kontrol eden, denetleyen ve yöneten düzenlemeler bütünü olarak tanımlanabilir (Cengiz, 2021). Her ülkenin farklı bir siber hukuk oluşturması uluslararası genel bir siber hukukun da oluşmasına engel olmaktadır. Hukuki olarak farklılığın oluşmasında en büyük etken ise ülkelerin siber alanı farklı şekillerde kullanması ve siber alanın anarşik yapısını aktif olarak kullanmalarından geçmektedir.

Bir ülkeye göre siber alanda gerçekleştirilen bir eylem kendi çıkar ve politikalarına uygun iken bir başka ülkeye göre ise bu durum yasaklanması gereken bir durum olarak algılanmaktadır. Örnek olarak verecek olursak, Brezilya'nın 2009'da BM'ye sunduğu tasarıda siber savaşlarda bilgi ve telekomünikasyon silahlarının kullanımında davranış kanunun oluşturulması isteğinde Rusya ve Çin uygun görürken ABD, İngiltere ve Fransa bu tasarıya karşı çıkmış, Fransa ise gerekçe olarak ulusal hedeflerine ulaşabilmek için siber savaşın meşruluğunu savunmaktadır (Türkay, 2013; Hildreth, 2001).

Siber hukukun oluşturulmasında ana sebep siber alanın anarşik yapasının düzenlenmesi ve bu anarşik yapı içerisinde işlenecek olan suçların engellenmesidir. Özellikle 21.yy. ile siber uzayda gerçekleştirilen saldırılar, devletlerin siber güvenlik politikaları oluşturmaya itmiş ve oluşturulan siber güvenlik politikalarını da hukuki bir zemine oturtturmak için bir araç olarak kullanmışlardır. Bu bağlamda oluşturulan en kapsamlı hukuki metin ise Avrupa Konseyi'nin (Council of Europe- CoE) 23 Ekim 2001'de imzaya açtığı Avrupa Konseyi Siber Suçlar Sözleşmesi olmuştur. Bahse konu olan sözleşmenin etkin ve kapsamlı olmasının asıl sebebi siber suçlara karşı ortak bilincin oluşturulması ve ortak bir cezalandırma sisteminin oluşturulmasından kaynaklıdır (Yılmaz ve Güllüpınar, 2020). Ayrıca yukarıda bahsedilen hususlardan hariç imza atan devletler kendi iç hukuk sistemlerinde düzenlemeler yaparak sözleşmeyle entegreli siber hukuk çalışmalarını yapmaları gerektiği vurgulanmış ve siber hukukun oluşması ve toplumun bilinçlenmesi için uluslararası iş birliğin teşvik edilmesi hedeflenmiştir (CoE 185 No'lu Anlaşma, 2001). Devletler tarafından oluşturulan siber güvenlik politikaları öncelikli olarak siber alanı daha etkin kullanmak ve devletin yapısını koruyabilmek adına oluşturdukları gibi vatandaşlarının da siber alanda özgür ve güvenli şekilde hareket etmelerini sağlamak için oluşturmaktadırlar. Bu yönüyle siber güvenlik politikaları ile siber hukuk aynı amaç için birbirini tamamlayan bir konumdadırlar.

Siber alanda gerçekleştirilen 2007 Estonya saldırısı, 2008 Gürcistan saldırısı ve 2010 İran'a yönelik gerçekleştirilen saldırı klasik Westfelya egemenlik anlayışının öneminin kaybetmesine neden olmuş, devletlere, şirketlere, kamu kurum ve kuruluşlarına ve bireylere yönelik gerçekleştirilen siber saldırılar hukuki düzenlemenin gerekliliğini ortaya koymuştur. Siber alan için yapılacak olan hukuki bir düzenleme siber alanın denetiminin sağlanmasında büyük bir etki yaratacağı gibi kişisel verilerin çalınmasına engel olacağı gibi siber alanda da insan haklarının korunmasına yardımcı olacaktır.

2.2. Siber Hukuka Ulusal Yaklaşımlar

2.2.1. Türkiye'nin Siber Hukuk Alanında Gerçekleştirdiği Faaliyetler

Türkiye'de diğer devletler gibi siber alanının düzenlenmesi ve suçun engellenmesi adına birtakım düzenlemeler gerçekleştirmiştir. Bu doğrultudaki ilk düzenleme 6 Haziran 1991 tarihli 3756 no'lu kanunun 20. Maddesine bilişim alanında suçlar başlığının eklenmesiyle başlamıştır (TBMM, 1991). Fakat her ne kadar adi suçların siber alanda işenmesini engellemek ve cezai yaptırımının oluşturulmasında büyük bir adım niteliği taşısa da siber güvenlik açısından zayıf kalmıştır. Türkiye'de kanuni düzenlemeler fiziki ve hukuki olarak ayırmak uygun olacaktır. Fiziki olarak Türkiye'nin internetle tanışması ve internetin potansiyelinin anlaşılması gerekmiştir. Bu bağlamda Türkiye'nin internet ile tanışması 1987'de Ege Üniversitesi'nin girişimleriyle Türkiye Üniversite ve Araştırma Kurumları Ağı'nın yurt dışı bağlantısını kurmasıyla başlayan ilk internetle tanışma, 1991'de TÜBİTAK ve ODTÜ ortaklığıyla oluşturulan TR-NET projesi geliştirilmiş ve 1993'te ODTÜ'de kiralık bağlantının kurulmasıyla Türkiye'nin farklı noktalarına internet sağlayan tek kaynağı olmuştur (Özdemir, 2021).

Türkiye, hukuki olarak siber alanı erken tanımış olsa da asıl farkındalık 2007'de NATO üyesi olan Estonya'ya yönelik gerçekleştirilen saldırı sonrasında siber güvenliğin ve hukuki düzenlemelerin önemini kavramış olsa da 2000 yılında çıkarılan yasalar, Devlet Planlama Teşkilatı (DPT) tarafından 2006'da hazırlanan 2006-2010 yıllarını kapsayan Bilgi Toplumu Stratejisi ve Eylem Planı ve 2010 yılı sonrası hazırlanan siber güvenlik strateji belgeleri ile siber alana yönelik ilgisini göstermiştir (Erendor, 2020: Töner Şen, 2021).

Türkiye, siber güvenlik politikalarını ve siber hukuk düzenlemelerini gerçekleştirirken ekseriyetle siber suçların ve siber saldırıların engellenmesi üzerine kurmuştur. Bu durum Ekim 2010'da Milli Güvenlik Kurulunun aldığı karar ile değişmiştir. Alınan karar doğrultusunda siber terör ve siber saldırıların küresel bir tehdit olarak kabul etmiş, saldırıların engellenmesi ve oluşturulan altyapıların denetimini ve güvenliğini sağlamak adına siber tatbikatların yapılmasına karar vermiştir (Erendor, 2020). 2012'de gerçekleştirilen Bakanlar Kurulu toplantısında Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna İlişkin Karar alınarak kamu kurum ve kuruluşlarında ulusal siber güvenliğin sağlanması ve bakanlıkça hazırlanan strateji ve eylem planına uyulması kararlaştırıldığı gibi kamu kurum ve kuruluşların siber güvenliğinin sağlanması adına milli çözümler oluşturulması ve maddi kaynak verilmesi de kararlaştırılmıştır (Resmî Gazete, 2012). Bu doğrultuda 2013 yılına kadar TÜBİTAK ve BTK ile 2008'de TR-BOME isimli siber tatbikat gerçekleştirmiş ve bu siber tatbikatlar sırasıyla 2011 ve 2013 yıllarında gerçekleştirilmiş, 2017'de dönemin Ulaştırma, Denizcilik ve Haberleşme Bakanı Ahmet Arslan tarafından gerçekleştirilen açıklama doğrultusunda devletin kritik kurum ve kuruluşları siber saldırılara karşı korumak adına 13 bin kişilik beyaz hackerlerden oluşan bir siber ordu kurduklarını açıklamıştır (Erendor, 2020; Sputnik, 2017).

Türkiye'de siber alanını düzenlenmesi ve denetlenmesi için gerçekleştirilen eylemler ekseriyetle siber güvenlik politikaları ile gerçekleşmiş ve bu bağlamda kritik kurumların kurulmasına da neden olmuştur. Bu bağlamda 19 Şubat 2014'te 5809 sayılı kanuna Ek Madde 1 eklenerek Siber Güvenlik Kurulu'nun kurulmasına karar verilmiş olup Siber Güvenlik Kurulunun başlıca amacı, oluşturulan siber güvenlik politikalarının, stratejilerinin ve eylemlerinin denetlenmesi ve onaylaması görevini üstlenmek olmuştur (Erendor, 2020)

Siber Güvenlik Kurulu'nun kurulmasıyla birlikte Türkiye'nin siber güvenlik politikalarının belirlenmesi konusunda somut bir adım olduğu gibi kurulun üyeleri Dışişleri, İçişleri, Milli Savunma, Ulaştırma ve Altyapı Bakanlığının müsteşarları, Millî İstihbarat Teşkilâtı Başkanı, BTK Başkanı, TÜBİTAK Başkanı ve MASAK Başkanı tarafından oluşmaktadır (Töner Şen, 2021). Eylül 2016'da 2016-2019 yıllarını kapsayan Ulusal Siber Güvenlik ve Eylem Planı'nı kabul etmiş ve 2016'nın mayıs ayında Siber Füzyon Merkezi kurulmuştur (Erendor, 2020; Töner Şen, 2021).

2.2.2. ABD'nin Siber Hukuk Alanında Gerçekleştirdiği Faaliyetler

Soğuk Savaşın bir ürünü olarak ortaya çıkan internet ile bilgisayar teknolojilerinin entegreli şekilde çalışması, siber alanın yeni bir boyut olmasına neden olduğu gibi devletlerin güvenliklerini en fazla etkileyen faktör olmasına da neden olmuştur. II. Dünya Savaşı ile başlayan istihbarat savaşları Soğuk Savaş ile kriptolu iletilerin çözülmesi için hızlı ve etkili bir araç olan bilgisayarların kullanılmasına ve daha sonrasında askeri amaçlı önleme ve etkin saldırı için bilgisayarların bağımsız şekilde birbiriyle konuşması fikriyle gelişmiştir. Almanya'nın kripto cihazı ENİGMA'yı çözmek için geliştirilen SIGIBA ile başlayan süreç, DARPA ve ARPA kurumlarının kurulmasına öncülük etmiş ve bu kurumların projesi olarak ARPANET'in oluşmasına ve 2003 itibariyle siber alanın ABD'nin sinir sitemi olarak tanımlanmasına neden olan bir süreç ortaya çıkmıştır (Kuehl, 2009; Huaben, 2007; Akyeşilmen, 2018).

2003 yılında Beyaz Saray'da yayınlanan Güvenli Siberuzay Ulusal Strateji Belgesi ile siber alan ABD'nin sinir sistemi olarak kabul edilmesi birden oluşmamış birtakım saldırılar sonucunda belge yayınlanmıştır. 24 Nisan 2001'de Hainan adası yakınlarında Çin Hava Kuvvetleri uçağı ile ABD istihbarat uçağının çarpışması sonrasında Çinli pilotun ölmesi sonrasında başlayan siber saldırılar, 80 bin Çinli hackerin ABD'ye yönelik gerçekleştirdiği saldırılar sonrasında oluşan zararın ne kadar olduğu bilinmezken The New York Times gazetesi bu saldırıyı Birinci İnternet Savaşı (WWWW1-World Wide Web War I) olarak okuyucularına duyurmuştur (Sertçelik, 2015; Deibert, vd., 2009). Daha sonrasında 11 Eylül 2001'de gerçekleştirilen terör saldırısının arkasında siber alanın kullanılması ve son olarak Rusya kaynaklı olduğu düşünülen ve ABD sistemlerine ne zaman sızdığı belirlenemeyen ve 2011'de tespit edilen Moonlight Maze saldırısı, ABD tarihinin en uzun süreli siber saldırısı olarak kabul edilmiş olup bu saldırı sonucunda Pentagon ve NASA'da bulunan stratejik belgeler kopyalanmış, Enerji bakanlığı ve sivil üniversiteleri de hedef almıştır (Akyeşilmen, 2018). Bu saldırı haberlere düşmesi sonucunda kamuoyunda büyük tepki toplamış, siber güvenliğin ulusal manada büyük bir öneme sahip olduğuna yönelik kuvvetli bir destek oluşmuş ve dönemin Savunma bakanı Ash Carter, Amerikan ağlarının güvenliğinin sağlanması ve savunulmasını şiddetle savunmuştur (Buchanan ve Sulmeyer, 2016).

2003 yılında ABD yönetiminin Güvenli Siberuzay Ulusal Strateji Belgesi zaman içerisinde ek maddelerin eklenmesiyle kapsamı değişmiştir. Siber alanın tam kapasitesinin belirlenememesi ve sınırlarının olmamasından kaynaklı olarak yeni gelişen teknolojik hamlelerle yeni tehdit unsurlarının doğmasına da neden olmuştur. Bu bağlamda dönemin ABD başkanı Bush, 2003'te çıkan karara ek iki madde daha ekleyerek siber uzayın tanım kapsamını değiştirerek çeşitliliği artırmıştır (Kuehl, 2009). ABD yönetimi çeşitli yıllar içerisinde siber alanının kontrolü ve hukuki düzenlemelerin yapılması adına çeşitli adımlar atsa da en etkili adımlar dönemin başkanı Obama tarafından atılmıştır. Bu bağlamda Obama, ilk olarak 2009 'da siber güvenlik ve siber alanın kavramlarının önemine vurgu yaparak bu alanda ulusal ve uluslararası farkındalığın oluşturulması amacıyla rapor yayınlamıştır (Selçuk, 2020). 2011'de uluslararası ticarette açık, güvenli ve güvenilir bilgi ve iletişim altyapısının kurulmasını teşvik eden Siber Uzay Stratejisi: Ağa Bağımlı Bir Dünyada Refah, Güvenlik ve Açıklık isimli raporu yayınlamış, 2015'de ABD Milli Güvenlik belgesinde siber güvenlik ve siber saldırılara yer verilmiş ve yine aynı yılda ABD Savunma Bakanlığı ülkenin stratejik kurumlarının siber güvenlik alanında hedeflerini belirlemiş ve son olarak 2018'de ABD başkanının siber alanda Amerikan vatandaşlarının ulusal güvenliğini ve refahını kendine öncelik olarak kabul eden Ulusal Siber Strateji Belgesini yayınlamıştır (Selçuk, 2020).

2.2.3. Rusya'nın Siber Hukuk Alanında Gerçekleştirdiği Faaliyetler

Rusya siber güç olarak günümüzde siber alanı etkin kullanan ve siber alanı domino eden önemli bir devlettir. Tarih sahnesinde etkin ve etkili devlet olan SSCB'den kalan Rusya, SSCB dağıldıktan sonra da arda kalan teknolojiyi ve bilgi birikimini de bünyesine katmasından dolayı siber alanda bu kadar etkin bir konumunda olmuştur. Soğuk Savaş döneminde ABD ile girilen teknoloji yarışı sonucunda elde edilen bilgi birikimi bugünkü Rusya'ya devredilmiştir. Teknolojik birikim Rusya için geleneksel bir yöntem olmasından kaynaklı olarak her zaman öncelikli olmuştur (Darıcılı, 2017). Miras bırakılan bilgi birikiminden hariç Rusya içerisinde gerçekleştirilen bazı eylemler ve olaylar da Rusya'nın siber güvenliğe ve siber alana yöneliminin artmasına neden olmuştur. Sovyetlerin döneminde yaşanan 1979-1989 arasında Afganistan'ın işgali sırasında ve Sovyetlerden sonra kurulan Rusya döneminde 1994-1996 Çeçen Savaşında

askeri birlikleriyle yaşanan iletişim problemleri ve bilişim teknolojilerinde kalınan gecikmelerden büyük zarar görmüş ve siber kapasitesinin artırılmasına karar vermiştir (Darıcılı & Özdal, 2017).

Rusya için büyük sorun olan bu problemlerin giderilmesi ve tekrarlanmaması adına büyük ve kapsamlı adımlar atarak siber alanda varlığını artıran ve siber kapasitesini artıran adımlar atmıştır. Atılan adımlar içerisinde en önemlisi ise 9 Eylül 2000'de yayımlanan Rusya Enformasyon Güvenliği Doktrini olmuştur (Acar, 2020). Yayınlanan bu belgenin tamamen güvenlik odaklı olması Rusya'nın iç karışıklıklara ve dış müdahalelere karşı attığı büyük bir adım olarak yorumlanmaktadır. Yayımlanan güvenlik doktrini Rusya'nın enformasyon güvenliğine verdiği önemi gösterdiği gibi Sovyetlerin yıkılmasından sonra bağımsızlığını kazanan devletleri de kendi ekseninde tutmak amacıyla bir araç olarak kullanabilmesinin altyapısını oluşturduğu doğrultusunda iddiaları da gündeme getirmiştir (Çifci, 2017). Bu iddia için ise gösterilen veriler ise; 2007'de Estonya saldırısı, 2008 Gürcistan saldırısı, 2009'da Kırgızistan saldırısı ve 2015'te Ukrayna saldırısı örnek olarak gösterilebilir (Çifci, 2017).

Rusya'nın 2000'de yayımladığı belgede enformasyon ve bilgi güvenliği bahsedilirken ilk kez 2008'de siber kelimesini resmi olarak kullanması güvenlik kavramını farklı bir boyuta taşımıştır (Çifci, 2017). Bilgi teknolojilerinin geliştirilmesi ve siber alanda aktif olmak Rus Savunma birimlerince büyük önem taşımış ve bu düşünce doğrultusunda 2011'de Savunma Bakanlığı tarafından Bilgi Çağında Rus Silahlı Kuvvetleri'nin Faaliyetlerine İlişkin Kavramsal Görüşler isimli belge yayınlanmıştır (Acar, 2020). Keir Giles'e göre bu belge Rus ordusunun siber savaş doktrini olarak tanımlanmıştır (Darıcılı, 2017). 2013'te dönemin Rusya Genelkurmay Başkanı olan Valery Gerasimov, Öngörüde Bilimin Değeri başlıklı makalesi yayınlanmıştır. Gerasimov'un kaleme aldığı makale -daha sonrasında Gerasimov doktrini olarak anılacaktır- hibrit savaşların üzerine durmuş ve bu doğrultuda savaş ve barış dönemlerinde siber alanın kullanılmasının hayati öneme sahip olduğunu belirtmiştir (Töner Şen, 2021).

Teknolojinin gelişmesi siber alanın kapasitesinin gelişmesine ve farklı yöntemlere sahip saldırı yöntemlerinin ortaya çıkması mevcut yasaların da yenilenmesine neden olmuştur. Bu bağlamda 2000'de kabul edilen Enformasyon Güvenliği Doktrini, 2016'da yenilenerek dönemin şartlarına uygun hale getirilmiştir

(Acar, 2020). Rusya'nın aktif olarak hem yasal hem de siber uzayda varlığı dünya kamuoyunda da ses getirmiştir. 2017'de Sputnik Türkiye'de yayınlanan Rusya'nın silahlı kuvvetleri 2035'te böyle olacak isimli haberde Michael Kaufman, Rusya'nın siber kapasitesini geliştirme yeteneğinde Batı'dan geri kalmadığını belirtmiş ve siber alana hem hukuki hem de ekonomik olarak ciddi yatırımlar yaptığını belirtmiştir (Sputnik, 2017).

2.2.4. Çin'in Siber Hukuk Alanında Gerçekleştirdiği Faaliyetler

Çin Halk Cumhuriyeti kuruluşundan itibaren 1949-1978 yılları arasında egemenliğini sürdürmek ve ülkesine yönelik olan tehditleri engellemek ve önlem almak amacıyla geri planda durmuş ve dünya siyaseti içerisinde sağlam adımlar atmak için geri planda kalmıştır. Fakat geri planda kalırken teknolojik altyapıların kurulması ve siber alan üzerinde etkin olmak adına büyük yatırımlar yapmaya devam etmiştir. Doğulu bir devlet olmasından kaynaklı olarak Çin, doğulu bir devlet olmasından kaynaklı olarak her zaman siyaseten ve politik olarak kapalı kapılar ardında olduğundan dolayı Batılı devletlerden farklı olmuş ve politikaları her zaman farklı olmuştur.

Dünyanın en kalabalık nüfusuna ve en fazla ticari işlem hacmine sahip olan bir devleti elbette teknolojinin son imkanlarından fazlaca yararlanacağı gibi oluşturulan teknolojik altyapıyı ve stratejik kurumlarını da korumak için siber alana büyük bir önem vermektedir. Öyle ki 2017 verilerine göre 731 milyon internet kullanıcısına sahip olması siber alanın korunması ve denetlenmesi için yeterli olmaktadır (Millward, 2017). Geniş bir kullanıcı ağına sahip olması sebebiyle bölgesel olarak diğer devletleri etkilediği gibi ABD'ye ve diğer Batılı devletlere bir alternatif olma yolunda politikalar, kendilerine özgü literatür ve adımlar atmaktadır. Örnekle açıklamak gerekirse, Çin terminolojisinde siber güvenlik kavramı yerine genellikle bilgi veya ağ güvenliği olarak bahsetmekte, askeri ve akademik terminolojide siberin karşılığı ağ veya network kullanılmakta ve siber alanın karşılığı olarak ise ağ alanı veya ağ uzayı olarak isimlendirmektedir (Töner Şen, 2021). Batı ile ortak bir literatür kullanmak yerine kendi literatürünü oluşturması, bu alanda üstünlük kurmak istemesiyle alakalıdır.

Çin'de literatürün milli oluşturulma isteği ve siber güvenlik stratejilerinin tek bir merkezden çıkması daha hızlı kararların alınmasına neden olmaktadır. Çin'in siber güvenlik politikalarının belirlenmesinde Çin Komünist Partisi (ÇKP) belirleyici olduğu

gibi önemli kararlar alınırken devlet başkanı ve başbakanın da yer aldığı partinin önemli isimlerinden oluşan 7 kişiden oluşan Politbüro Daimî Komitesi (PDK) etkili olmaktadır (Pekcan, 2020). PDK genel olarak ülke genelinde önemli kararlar aldığı gibi siber güvenlik kararlarının alınmasında da etkili olduğu gibi siber güvenlik ile ilgili konulardan sorumlu farklı kurumlar da bulunmaktadır. 2008'de kurulan Sanayi ve Bilgi Teknolojileri Bakanlığı kurulmuş ve bu bakanlık altında -sivil toplum kuruluşu olan Çin Ulusal Bilgisayar Ağı Acil Müdahale Teknik Ekibi/Koordinasyon Merkezi, Kamu Güvenliği Bakanlığı ve Devlet Güveliği Bakanlığı gibi kurum ve kuruluşlar siber alanda gerçekleştirilen eylemlerde farklı uzmanlıklara sahiptir (Pekcan, 2020).

Çin, siber güvenliğin sağlanması ve siber alandaki varlığını artırmaya yönelik ilk adım 2003'te Belge 27'yi yayınlayarak kritik altyapıların korunması, şifreleme teknolojilerinin geliştirilmesi, yeni inovasyonları desteklemek, yatırımları artırmak ve e devlet politikalarının belirlenmesi için kapsamlı ve önemli bir belge konumunda olmuştur (Raud, 2016). Belge 27'nin yayınlanmasından sonra büyük bir atılım yapan Çin, siber alana büyük bir önem vermeye başlayarak siber alanda etkin bir aktör olma yolunda emin adımlarla ilerlemeye devam etmiştir. Bu bağlamda 2006'da Devlet Konseyi tarafından bilim ve teknoloji alanındaki gelişimini belirlemek için orta ve uzun vadeli 2006-2020 Milli Programı açıklamış, 2010'da Beyaz Kitap yayınlanmış, Çin toprakları içerisinde siber güvenliğin sağlanması adına siber espiyonaj faaliyetlerinin engellenmesi ve bağımsız olmak için siber alanın aktif kullanılması kararlaştırılmış, 2012'de Yeni Politika Düşüncesi isimli strateji yayınlanmış, 2014'de devlet başkanı Xi Jinping başkanlığında İnternet Güvenliği ve Bilgilendirme için Küçük Merkez Lider Grubu çalışmalarını gerçekleştirmiş ve sonuçları hükümet raporunda sunulmuş ve 2015'de Çin Askeri Strateji yayınlanarak siber krizleri ve siber operasyonları yeni tehdit olarak kabul edilmiştir (Töner Şen, 2021; Pekcan, 2020).

Devlet genelinde üst düzey kararlar alınırken 2009'da halkın güvenli internet kullanabilmesi ve kültürel yozlaşmadan kurtarmak için Yeşil Baraj Gençlik Koruması projesi hayata geçirilmiş ve bu proje kapsamında yurt içinden ve yurt dışından alınan tüm bilgisayarlara, okullarda kullanılan ve internet salonlarında kullanılan bilgisayarlar için proje kapsamında geliştirilen yazılımın yüklenmesi kararlaştırılmıştır (Çifci, 2017). Hükümet, proje kapsamında halkın güvenli internete erişmesi ve yasaklı sitelere girilmesini engellemek için geliştirilmiş bir proje olarak açıklama yapsa da engellenen siteler ve yasaklı kelimelerin %85'i politik kelimeler ve siteler oluşturmaktadır (Çifci,

2017). Ayrıca 2015'te ulusal kongrede halkın siber güvenlik üzerine düşüncelerini göz önüne alarak bir kamuoyu yoklaması yapılarak bir tasarı oluşturulmuş ve bu tasarı 2016'da kabul edilmiştir (Göçoğlu ve Aydın, 2019). Son olarak Çin, 2022'de Siber Alanda Ortak Geleceği Olan Bir Toplumu Birlikte İnşa Etmek isimli bir beyaz kitap yayınlayarak, insanlığın faydası için interneti iyi amaçla geliştirmeyi, kullanmayı ve yönetmeyi hedefledikleri gibi bütün insanlığın bu konuda üzerine düşenleri yapması gerektiğini vurgulanmış ve Çin'in kendi çıkar ve haklarının korunması adına önemli bir kaynak teşkil etmektedir (Çahmutoğlu, 2022).

2.2.5. İngiltere'nin Siber Hukuk Alanında Gerçekleştirdiği Faaliyetler

İngiltere'nin siber güvenlik politikalarının oluşturulması mevcut teknolojik gelişmeleri yakından takip etmesiyle ve İngiltere'ye yönelik gerçekleştirilen saldırılar sonucunda şekillenmektedir. İngiltere'yi doğrudan etkileyen siber olaylar (WannaCry fidye yazılımı, Wonga siber saldırısı, Three Mobile saldırısı, Tesco Bank saldırısı vd.) sonucunda büyük adımlar atmak durumunda kalmıştır (Eren, 2020). İngiltere'ye yönelik gerçekleştirilen saldırıların fazla olması İngiltere'nin Batı ülkeleri içerisinde yüksek teknolojik altyapıya sahip olması ve teknolojik gelişmeleri yakından takip etmesiyle doğru orantılıdır. Öyle ki İngiltere'de dijital sektör, üretimin %16'sını, istihdamın %10'unu ve ihracatın %24'ünü oluşturması sebebiyle hedef ülke konumunda olmasına neden olmaktadır (Chakravorti ve Chatuverdi, 2017).

İngiltere'nin yeni teknolojileri benimsemesi ve siber alanının verimliliğinden faydalanmak adına çeşitli entegrasyonlar yapması beraberinde oluşacak siber suçlarında önüne geçmek adına çeşitli hukuki girişimlerde bulunmasına da neden olmuştur. İlk olarak 1990'da bilgisayar suçları ile ilgili ilk yasal düzenlemeyi gerçekleştirerek, çağın gereksinimlerini önceden fark ederek siber alanın önemli bir boyut olduğunu göstermiştir (Eren, 2020). Özellikle İngiltere'nin siber alanda hukuki olarak erken adım atmasındaki amaç, dünyanın önde gelen dijital ülkelerinden biri olmak ve İngiltere'de çevrimiçi olarak yaşamak ve çalışmak adına dünyanın en güvenli yeri olma isteğidir (Carr ve Tanczer, 2018). Ayrıca İngiltere, dijital ülke olma yolunda ilerlediği gibi vatandaşlarının da fiziki dünyada olduğu gibi siber alanda da kendilerini güvende hissetmelerini devlet politikası olarak kabul etmektedir (Couzigou, 2018).

İngiltere'nin oluşturduğu amaç, siber alanın anarşik yapıda olması ve gün geçtikçe yeni gelişen teknolojilerin siber alanla entegreli şekilde çalışmasından kaynaklı olarak ulaşılması daha zor bir duruma neden olmaktadır. Yıllara göre gelişen teknolojiler ışığında İngiltere, hızlı reaksiyon vererek hukuki altyapısını kurarak güncel gelişmeleri yakından takip etmektedir. Bu bağlamda 1998'de Veri Koruma Yasası çıkarılmış ve bu yasa güncel gelişmeler ışığında 2016'da AB tarafından da eklemeler yapılarak Genel Veri Koruma Yasası olarak yenilenerek, özel şirketlerde ve kamu kurumlarında tutulan kişisel verilerin korunmasına ve bilgilerin sınırlandırılması hakkında ciddi düzenlemeler yapılmıştır (Eren, 2020).

İngiltere, kişisel verilerin korunmasına yönelik ciddi adımlar attığı gibi oluşturulan hedeflerinde devletin de siber alanda korunaklı olması adına 2009'da siber alandaki politikalarını diğer güvenlik politikalarından ayırarak ayrı bir kapsamda değerlendirerek Güvenlik Stratejisi Emniyet, Güvenlik ve Siber Uzayda Dayanıklılık isimli ilk stratejik belgesini, 2010'da Siber Suç Stratejisi belgesi yayınlanarak siber suçlar tanımlanmış ve 2009'da Siber Güvenlik Ofisinin yerine 2010'da Siber Güvenlik ve Bilgi Güvencesi Ofisi kurulmuştur (Stoddart, 2016; Eren, 2020). 2011'de Ulusal Siber Güvenlik Stratejisi yayınlanmış ve 2011-2016 dönemi içinde siber güvenlik programı için 860 milyon sterlin kaynak ayırmıştır (Carr ve Tanczer, 2018). 2016'da hükümetin siber güvenlik politikasını şekillendirmek, kamu ve özel sektör, sivil toplum ve daha geniş tabana siber güvenlik politikalarının indirilmesi için Ulusal Güvenlik Stratejisi 2016-2021 belgesi yayınlanmış ve 2017'de Ulusal Siber Güvenlik Merkezi açılmıştır (HM Goverment, 2016). 2022'de yayınlanan Ulusal Güvenlik Strateji belgesinde İngiltere, 2030 yılına kadar siber alanda lider, sorumlu ve demokratik bir siber güç olma hedefi belirlemiş, hükümet, endüstri ve akademi üçgeni arasında güçlü ortaklıklar inşa edecekleri deklare etmişlerdir (HM Goverment, 2022).

2.2.6. Hindistan'ın Siber Hukuk Alanında Gerçekleştirdiği Faaliyetler

Dünyanın en kalabalık ikinci ülkesi olan Hindistan, doğal olarak internet kullanım oranının ve siber suçların da fazla olmasına neden olmaktadır. Örnekle açıklamak gerekirse 2012'den sonra Hindistan'da internet kullanımı büyük bir sıçrama gerçekleştirerek 6 kat artmış ve bu artış Hindistan'a dünyada en çok internet kullanan üçüncü ülke olma konumunu getirmiştir (Kesharwani, vd., 2019). İnternete kullanımının

çok fazla olması, doğal olarak siber alanda işlenen suç ve diğer faaliyetlerin de artmasına neden olmuştur. Symantec Corp'ın Hindistan için hazırladığı İnternet Güvenliği Tehdit Raporunda (Internet Security Threat Report- ISTR) kötü niyetli saldırılarda 4. sırada, Asya pasifik bölgesinde Japonya'dan sonra 2. sırada yer almaktadır (ISTR, 2017).

Hindistan yönetimi siber alanın farkındalığını geç kavramış olsalar da ilk adım 1999'da çalışmalarına başlanan ve 2000'de kabul edilen Bilgi Teknoloji Yasası olmuş ve teknolojik gelişmelerin yasada boşluk oluşmaması adına değişiklikler de gerçekleşmiş ve en önemli değişiklik olarak bilgisayar korsanlığı ve siber suçlar tanımlanmıştır (Drishtiias, 2021).

Hindistan'da gerçekleştirilen siber saldırıların sayısının fazla olması elbette Hindistan yönetiminin caydırıcı bir politika belirleyememesinden kaynaklı olmuştur. Siber güvenlik alanında önemli adımla 2013'ten sonra atılmaya başlamıştır. 2 Temmuz 2013'te ülkenin ilk Ulusal Siber Güvenlik Politikası yayınlanmış ve ardından Ulusal Teknik Araştırma Kurumu tarafından kritik bilgilerin korunması kritik kurumlara yönelik gerçekleştirilecek olan saldırıların engellenmesi için Ulusal Kritik Bilgi Altyapısının korunmasına yönelik tedbirler yayınlanmıştır (Dilipraj, 2013). Ayrıca Hindistan yönetimi, kendi siber ekosisteminin oluşturmak ve oluşturmayı hedeflediği ekosistem içerisinde kanunen güçlü ve denetleyici tedbirler alınması adına Ulusal Siber Güvenlik Politikası geliştirilmesi için Ar-Ge çalışmaları için kaynak ayırmıştır (Dilipraj, 2013).

2.2.7. Singapur'un Siber Hukuk Alanında Gerçekleştirdiği Faaliyetler

Güneydoğu Asya'da bir şehir devleti olan Singapur, bölgenin finans merkezi olması sebebiyle dijitalleşmeye ve siber güvenliğin sağlanmasına ciddi önem vermektedir (Alaca, 2020). Dönemin ve Singapur'un ilk dışişleri bakanı olan Sinnathamby Rajaratham, Singapur'un kısıtlı imkanları içerisinde bölgesel ve hatta küresel bir devlet olma yolunda ilerleyebilmesi için dijitalleşmenin gerekliliğini dile getirmiş ve Singapur'un uluslararası sistem içerisinde varlığını devam ettirebilmek için Küresel Şehir olması için büyük adımlar atmış (Heng, 2013), bu bağlamda 1980-1990 yılı başları arasında bilgisayar kullanımının sivil boyuta indirilmesiyle yazılım alanında bölgesel bir merkez olma hedeflerine ulaşmak için çalışmalara başlamışlardır (Alaca, 2020). Hedefleri doğrultusunda 1990 sonrası yaygınlaşan bilgisayar kullanımı

beraberinde internetin de yaygınlaşmaya başlamasıyla farklı bir boyut kazanmış ve internet altyapısına yoğunluk verilerek ülkenin internet altyapısı oluşturulmuş ve 2010 yılında dünyanın en hızlı internet altyapısına sahip olma unvanını kazanmış ve internete bağlı sanallaşma hareketi olan e-devlet projesini üç yıllık periyotlar halinde 2000-2006 yılları arasında gerçekleştirmiştir (Alaca, 2020).

24 Kasım 2014'te dönemin Singapur başbakanı Lee Hsien Loong, Akıllı Ulus Girişimi'nde yapmış olduğu konuşmada, ülkesinin sahip olduğu teknolojiyi, kapsamlı ve sistematik şekilde kullanarak dünyanın önde gelen şehirleri arasında yer almayı ve diğer ülkelerden yatırımcı çekerek bölgesel olmaktan çıkıp küresel olma yolunda ilerlemenin vatandaşlarına yönelik bir borç olduğunu ifade ederek, teknolojiyi ve interneti birleştirerek akıllı sistemler ve akıllı toplumlar inşa etme vizyonunu açıklamıştır (Prime Minister's Office Singapore, 2014).

Singapur'un bilişim alanında öncü olma isteği ve internet kullanımın çok fazla olması beraberinde büyük siber saldırıların gerçekleşmesine neden olmuştur. Öyle ki 2019'da gerçekleşen siber saldırı oranı 2018'e göre %51,7 artıştır (Alaca, 2020) Singapur'un karşılaştığı en büyük siber saldırı, 2018'de medikal istihbarat amaçlı gerçekleştirilen ve ülkenin tüm sağlık sistemine kayıtlı kişilerin verilerini çalan devlet destekli istihbarat grubu olan Whitefly tarafından çalınan verilerde aralarında başbakanın da bulunduğu 1,5 milyon kişinin verileri çalınmıştır (Alaca, 2020). Dijitalleşmeyi devlet politikası haline getiren Singapur için bu çapta büyük bir saldırı devlet imajına ve sistemlerine zarar vereceğini düşünerek bazı adımlar atmasına neden olmuştur. İlk olarak yenilikçi teknolojileri araştırmak, nitelikli eleman ihtiyacının karşılanması ve daha güvenilir bir ortam için Singapur Ulusal Üniversitesinde Güvenilir Yazılım Sistemleri kürsüsü, Singapur Yönetim Üniversitesinde Mobil Sistem Güvenliği ve Singapur Teknoloji Üniversitesinde Güvenli Kritik Altyapı ve Tasarım kürsüleri kurularak eğitimlerin verilmesini ve kalifiye elemanların yetişmesi amaçlanmıştır (Teh, vd., 2020).

Singapur, nitelik sahibi eleman yetiştirmesi siber güvenlik alanının teknik boyutunu oluşturduğu gibi hukuki kısmında da büyük adımlar atmıştır. 2013'te Ulusal Siber Güvenlik Master Planı kabul edilmiş (Alaca, 2020). 2014'te Bilgisayarın Kötüye Kullanımı ve Siber Güvenlik Yasası (CMCA) kabul edilmiştir (Craig, vd., 2015). Singapur, diğer devletlerden farklı olarak uygulamaya koyduğu yasaları çok katı şekilde

denetleyerek daha saldırgan bir politika yürüterek kendilerine yükledikleri misyona ulaşmak ve dünyada en güvenilir ülke olma yolunda adım atmaktadırlar. Bu bağlamda 2014'te Ulusal Siber Güvenlik Merkezini açarak gerçekleştirilen siber saldırıların arka planının araştırılıp suçluların ortaya çıkarılması ve ülkelerine yönelik gerçekleştirilecek olan saldırıların engellenmesi için çalışmaktadırlar (Craig, vd., 2015).

2.3. Siber Hukuka Uluslararası Yaklaşım

2.3.1. Birleşmiş Milletlerin Siber Hukuk Alanında Gerçekleştirdiği Faaliyetler

Siber alanın varlığı bilgisayar teknolojileri ile başlamış ve internetin yaygınlaşmasıyla birlikte geniş bir kitleye ulaştığından dolayı, uluslararası örgütler siber alanı her zaman bilgi güvenliği ve kişisel verilerin korunması üzerine şekillendirmiş ve zaman içerisinde değişimler ile mevcut yasa ve tekliflerini yenilemişler ve ihtiyaçlar doğrultusunda yeni kurumların kurulmasına öncülük etmişlerdir. Dünya barışının sağlanması amacıyla kurulan Birleşmiş Milletler (BM) de zaman içerisinde yapısal değişikliklere giderek siber alanın tehlikeli boyutlarını görerek çatışma riskinin ortadan kaldırılması veya çatışmaya uygun ortamların oluşmasını engellemek için çalışmalar gerçekleştirmiştir.

BM'nin siber alanı düzenleme ve genel bir kanun oluşturma isteği kuruluş felsefesinde bulunan uluslararası çatışmaların ve kuvvet kullanımın engellenmesiyle doğrudan bağlantılıdır. Günümüzde güçsüz ve zayıf devletler çatışma alanını fiziki olmaktan çıkararak daha ucuz ve etkili bir saldırı yöntemi olan siber alana kaydırması ve güçlü devletlerin de halihazırda bu alanda sıkça faaliyet göstermeleri nedeniyle BM şartının 2/4 maddesi olan kuvvet kullanmaktan kaçınma ilkesini siber alanı da kapsayacak şekilde güncellenmesini gündeme getirmiştir (Töner Şen, 2021).

İlk olarak BM, 1980'lerin sonlarında siber güvenlik, bilgi altyapısı güvenliğinin korunması üzerine tartışmalar yapmasıyla başlamış ve bu tartışmalar neticesinde 1990'da 45/121 sayılı Suçların Önlenmesi ve Suçluların Değerlendirilmesi kararı alınarak üye devletlerin bilgisayarlarda gerçekleştirilen istismar suçlarının engellenmesi adına etkin mücadele yapmaları gerekliliğine dikkat çekişmiştir (Ebrem ve Kurut, 2020). Üye devletler de BM çatısı altında taslak sunarak siber alanın düzenlenmesi için adımlar

atarak BM'nin siber alana yaklaşımını desteklemişlerdir. Bu bağlamda Rusya, Çeçen Savaşı sırasında yaşadığı olumsuzlukları not alarak 1998'de BM'ye taslak sunmuş ve bu taslak 2000'de BM'nin 55. Oturumu ve 63 sayılı kararının ortaya çıkmasına zemin hazırlayarak, bilgi teknolojilerinin suç amaçlı kullanımı ile mücadele edilmesini ele almıştır (Ebrem ve Kurut, 2020). Rusya sunduğu taslakla birlikte bilgi güvenliği alanında oluşabilecek suçların ve tehditlerin belirlenmesi ve değerlendirilmesi için 15 devlet uzmanından oluşan hükümet uzmanları grubunun kurulmasını istemiş ve bu öneri kabul edilerek 2004–2005, 2009–2010, 2012–2013, 2014–2015 ve 2016–2017 yıllarında toplam beş uzman grubu kurulmuştur (Eldem, 2021).

2002'de BM 57.oturum ve 239 sayılı kararında küresel siber kültürünün oluşturulması adına çalışmalar yapılması gerekliliği kararı alınmış ve bu karar doğrultusunda 23 Aralık 2003 BM Genel Kurul kurulunda alınan 58/199 sayılı karar ile Küresel Siber güvenlik Kültürü ve Kritik Bilgi Altyapılarının Korunması kararı alınmıştır (Türkay, 2013; Ebrem ve Kurut, 2020). Genel olarak bilgi teknoloji altyapılarının korunması ve siber güvenlik farkındalığı üzerine yoğunlaşan BM, 2017'de 2341 sayılı kararında kritik altyapı kaynaklarının terörist saldırılarından korunması için gerekli eylem planlarının hazırlanması ve Küresel Terörle Mücadele Stratejisinin uygulanması konusunda iş birliği çağrısında bulunmuştur (United Nations, 2017). 2023'te BM Genel Kurulu IŞİD'in uluslararası barış ve güvenliğe yönelik oluşturduğu tehdide ve tehdide karşı koymada üye devletleri desteklemek için 16. Raporu yayınlamış ve raporun 62.maddesinde kritik altyapıların terör saldırılarından korunmasına yönelik çabalara BM sistemi içinde öncelik verilmesi kararlaştırılmış BM Küresel Terörle Mücadele Koordinasyon Sözleşmesinde ortaya çıkan tehditler revize edilerek güncellenmiştir (United Nation, 2023).

BM kurulunda alınan bu kararlardan hariç BM'nin de katkı sağladığı birtakım toplantılar, sözleşmeler ve zirveler de gerçekleşmiştir. 2001'de Budapeşte'de imzalanan ve imzalandığı yerden ismini alan Budapeşte Sözleşmesi Avrupa Konseyi çatısı altında ve ABD'nin de katkılarıyla imzalanmış ve imzalayan devletlerin hepsinin BM üyesi olması sebebiyle BM'nin siber güvenlik politikalarında önemli bir rolü olmuştur (Ebrem ve Kurut, 2020). 2003'te Cenevre'de 175 ülke ve sivil toplum kuruluşların katılımıyla ilk zirve gerçekleştirilmiş ve ikinci zirve 2005'te Tunus'ta gerçekleştirilmiştir (Ebrem ve Kurut, 2020).

2.3.2. Avrupa Birliği'nin Siber Hukuk Alanında Gerçekleştirdiği Faaliyetler

Siyasi ve ekonomik temelde kurulan Avrupa Birliği (AB), siber güvenlik ekseninde ilk politikalarını gelişen teknolojilerle birlikte bilgi teknolojilerinin takip edilebilmesi 1990'lı yıllarda atmıştır. Bu süreçte AB ilk olarak Avrupa Suç Sorunları Komitesinin 1996'da siber suçların belirlenmesi ve siber suçlarla ilgilenecek olan Uzmanlar Komitesinin kurulmasını kararlaştırarak atmıştır (Töner Şen, 2021). AB, uzun yıllar siber güvenlik tanımı yapamamış ve strateji geliştirememiştir. Bunun nedeni ise AB'nin siber güvenliğe bütüncül ve kolektif bir vizyon içeren bir tanım yapamamasından kaynaklı olarak 2013'te yayınlanan Avrupa Birliği'nin Siber Güvenlik Strateji belgesine kadar daha çok bilgi güvenliği, ağ güvenliği ve siber suçların önlenmesi üzerine durmuştur (Köksoy, 2020).

AB üye ülkeler arasında siber güvenlik konusunda iletişim kanallarının kapanmaması ve iş birliğinin geliştirilmesi adına 13 Mart 2004'te Avrupa Birliği Siber Güvenlik Ajansını kurmuş ve bu ajans 1 Eylül 2005'te aktif hale gelmiştir. 2007'de Avrupa Polis Ofisi (EUROPOL), siber suçların artmasına bağlı olarak 'Web'i Kontrol Et' programını başlatmış, 2010'da ise AB Bakanları, siber güç ajansına yeterli destek verilmesi için Komisyona çağrıda bulunmuştur (Yılmaz, 2017). Çağın gereksinimlerine ve bilgisayar teknolojilerinin gelişmesiyle birlikte artan siber suçların engellenmesi için kayıtsız kalamayan AB, 7 Şubat 2013'te siber güvenlik alanında ilk somut adımını atarak 'Avrupa Birliği'nin Siber Güvenlik Stratejisi' belgesini yayınlamış ve 6 Temmuz 2016'da üye devletler arasında siber güvenlik alanında iş birliğinin artırılması ve ağ ve bilgi sistemlerinin güvenliğini artırmak için NIS Direktifi isimli ilk yasal düzenlemeyi kabul etmiştir (Köksoy, 2020). 2013'te atılan bu adım beraberinde Siber Güvenlik Yasasının oluşturulması adına büyük bir adım olmuş ve 2017'de çalışmalar başlatılmış ve 11 Mart 2019'da Avrupa Parlamentosu tarafından onaylanarak yürürlüğe girmiştir (Nezgitli ve Benzer, 2020).

2016'de NIS isimli ortaya çıkan ilk yasal düzenleme zamanın şartları ve gereksinimleri doğrultusunda tekrardan 27 Aralık 2022'de Direktif 2022/2555 veya NIS2 adıyla düzenlenerek, gerekli siber kriz yönetim yapısının oluşturulması, AB nezdinde çıkarılmış olan rapor ve stratejilerin tamamına uyulması üye devletlerin yeni

gelişmelere uygun olacak şekilde siber güvenlik stratejilerini oluşturmaları hedeflenmiştir.

2.3.3. NATO'nun Siber Hukuk Alanında Gerçekleştirdiği Faaliyetler

Soğuk Savaş sonrası 1949'da güvenlik örgütü olarak kurulan NATO, birçok uluslararası görevde faaliyet göstermiş ve halen varlığını devam ettirmektedir. Kuruluş itibariyle güvenlik endeksli olan NATO, uluslararası sistemin ve küreselleşme hareketleriyle mecburi bir değişim içerisine girmiştir. Bu bağlamda NATO, içerisinde 4 belirgin döneme ayrılmıştır. Bu dönemler, i) Soğuk Savaş dönemi (1949-1991), ii) Soğuk Savaş sonrası olan ilk on sene (1991-2001), iii) 11 Eylül saldırısından sonraki dönem ve son olarak NATO'nun Lizbon Zirvesi Deklarasyonunu kabul edildiği dönem olarak ayrılmaktadır (Töner Şen, 2021).

NATO, siber alanın farkındalığına 1990'da fark etmiş ve çeşitli adımlar atmış olsa da asıl farkındalığın oluşmasına neden olan 2 kırılma noktası olan 11 Eylül saldırısı ve 2007 Estonya saldırısı olmuştur. Kronolojik olarak NATO'nun değişimini incelemek gerekirse ilk adım 1990'da Londra Zirvesinde NATO, alan dışı kavramını ortaya atarak tehdit alanını ve içeriğini genişletmiş, 7-8 Kasım 1991 Roma Zirvesinde de Yeni Stratejik Konsepti kabul ederek NATO bölgesi harici olan bölgelerde de tehditlerle mücadele edileceğini bildirmiştir. Bu tehditler arasında ilk örneklerinden olan bilgi savaşı da siber alanın aktif olarak kullanılması olmuştur. Özellikle de 1994'te Rusya, Çeçen direnişçileri bastırmak için Çeçenistan'ın başkenti Grozni'ye girmesiyle başlamış ve bu süreçte harekatın planlanan gibi gitmemesi ve Çeçen direnişçilerin ölü Rus askerlerinin görüntülerini internet ortamına aktarmasıyla bastırma hareketi farklı bir boyut kazanmış ve NATO'nun bilgi savaşının ilk örneklerinden birisiyle karşılaşmasına neden olmuştur (Bıçakçı, 2012).

O dönemde gerçekleşen bu olay, siber alanın korunması ve denetlenmesi gereken bir alan olarak görülmesine neden olmuştur. NATO, halihazırda 1991'de Siber Savunma ve Yönetim Kurulu (Cyber Defence and Management Board-CDMB) ve Askeri Otoriteler ve Muhabere ve Bilgi Sistmeleri Ajansı (Military Authorities and Communications and Information Agency- MACIA) gibi kurumları kurarak hazırlıklara erkenden başlamış ve üye ülkelerin askeri ağ yapılarını ve yeteneklerinin farklı olmasından kaynaklı olarak tek bir sistem kurmak adına NATO Ağ ile Etkinleştirilmiş

Güç Programı (Network-Enabled Capability- NNEC) ve Ağ Merkezli Savaş (Network Centred War- NCW) için bilişim altyapılarının oluşturulmasını sağlamıştır (Töner Şen, 2021).

NATO genelinde siber alan ve ağ güvenliği üzerine çeşitli adımlar atılsa da ilk kırılma 11 Eylül saldırısı sonrasında olmuştur. 11 Eylül'de gerçekleştirilen saldırı sonrasında yapılan teknik takipte yetkililer teröristlerin saldırıyı internet üzerinden planladıklarını ortaya çıkarmış ve yapılan baskın ve soruşturma sonucunda 16 Eylül 2002'de teröristlerin ABD içerisinde uyuyan hücreleriyle haberleşmek için internet tabanlı telefonlarla iletişim kurduklarını ortaya çıkarmıştır (Thomas, 2003). Terör saldırısında siber alanın kullanılması terör faaliyetlerinin artık farklı bir boyuta taşınmasına ve güvenlik algılarının da tamamen değişmesine neden olmuştur. 11 Eylül saldırısı sonrasında gergin olan uluslararası sistem de yeni bir güvenlik meselesi tartışılmaya başlanmıştır. Tartışılan bu mesele ise 'Dijital Felaket' veya 'Dijital 11 Eylül' olarak adlandırılmıştır (Bıçakçı, 2012). Bu güvenlik senaryosunda üye devletlerin herhangi birisine yönelik gerçekleştirilecek olan siber saldırı sonrasında kritik altyapıların etkisiz hale getirilmesi ve ülke güvenliğinin savunmasız bir duruma düşmesi durumunda yapılacak ele alınmış ve bu kapsamda 21 Ekim 2002'de düzenlenen Prag Zirvesinde gündeme gelmiş ve Zirve'de siber saldırılara karşı savunmanın güçlendirilmesi kararlaştırılmıştır (Bıçakçı, 2012).

NATO için bir diğer kırılma ise 2004'te NATO'ya üye olan Estonya'nın 2007'de ağır bir siber saldırıya uğraması sonrasında oluşan güvenlik meselesi olmuştur. Estonya'nın gerçekleştirilen siber saldırı sonrasında çok fazla zarar görmesinin altında yatan nedenler incelendiğinde Estonya'nın internet kullanımın en yüksek ülkeler arasında olması, her vatandaşının devlet kurumlarına ve bankalara erişmesinin sağlayan dijital kimliğe sahip olması ve 355 devlet kuruluşunun siber alanda olmasından kaynaklı olarak saldırı büyük bir yıkıma sebep olmuştur (Bıçakçı, 2014). Yaklaşık 3 hafta süren saldırılar sonucunda ülke teknik olarak kapanmış ve her türlü işlem yapılamaz hale gelmiştir. Estonya, gerçekleştirilen siber saldırıların arkasında Rusya ve Rusya İstihbarat Servislerinin olduğunu iddia etmiş ve NATO üyesi olarak NATO'dan resmi olarak yardım talep etmiş fakat NATO'nun ilgili birimlerinin bu konuda yetersiz olmalarından kaynaklı olarak zamanında destek sağlayamamışlardır (Darıcılı, 2020).

Bu saldırı sonrasında NATO, siber alanda gerçekleştirilen saldırıların etkisini görmüş ve bu bağlamda 2008 Bükreş Zirvesinde siber güvenlik konusunu kapsamlı olarak ele almış, siber savunma çalışmalarının tek bir merkezde toplanması amacıyla Siber Savunma Yönetim Otoritesi (Cyber Defense Management Authority- CDMA) ve eğitim faaliyetlerinin organize edilebilmesi, araştırılması ve kavramsal üretim gerçekleştirmek amacıyla saldırının merkezi olan Tallinn merkezli NATO Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defence Centre of Excellence-CCDCOE) kurulmuştur ve NATO'nun ilk siber güvenlik politikası kabul edilmiştir (Darıcılı, 2020; Baykara, 2020).

2007 saldırısı NATO için bir milat olarak kabul gördükten sonra siber güvenliğe ciddi önem verilerek, 2009'da gerçekleştirilen Strasburg/Kehl Zirvesinde güvenlik raporu hazırlanması kararlaştırılmış ve 2010'da sunulan raporda öncelikli saldırılar arasında siber saldırı eklenmiş, 2012'de Siber Tehdit Farkındalık Birimi oluşturulmuş, 2013'de Tallinn El Kitabı hazırlanmı,2014 Galler Zirvesinde güçlendirilmiş siber savunma politikası kabul edilmiş ve siber saldırıların NATO'nun 5.maddesini gündeme getirebileceği ilk defa dile getirilmiş, 2016 Varşova Zirvesinde siber alanın başlı başına askeri operasyon sahası olarak tanımlamış, 2017'de Tallinn El Kitabı güncellenmiş, 2019 Londra Zirvesinde NATO'nun 5G teknolojisi başta olmak üzere iletişim sistemlerini korumak ve kapasitelerinin artırılmasına daha fazla önem verilmesine karar vermiştir (NATO, 2023). Ayrıca Haziran 2022 Madrid zirvesinde müttefikler, NATO'nun yol gösterici rehberi olan yeni bir Stratejik Kavram Konsepti üzerinde uzlaşı sağlayarak Rusya'yı güvenliğe yönelik en önemli ve doğrudan tehdit olarak tanımlamasının haricinde ilk kez Çin Halk Cumhuriyeti'ne hitaben terörizm ve siber tehdit gibi unsurlarla nasıl tepki verileceği ele alınmıştır (NATO, 2022).

2.3.4. Şanghay İş birliği Örgütü'nün Siber Hukuk Alanında Gerçekleştirdiği Faaliyetler

Bölgesel ayrılıkçı hareketlerin ve terör faaliyetlerinin engellenmesi üzerine kurulan Şanghay İşbirliği Örgütü (ŞİÖ), 11 Eylül saldırısından sonra hedef ve kapsamını genişleterek bölgesel ekonomik bir güç unsuru olma yolunda ilerlemektedir (Yardımcıoğlu ve Koçarslan, 2012). ŞİÖ, anlaşmaya taraf olan üyeler arasında uyuşturucu kaçakçılığının önlenmesi, yasadışı göç ve diğer sınır güvenliğini etkileyecek

olan unsurların engellenmesi ve terörizm faaliyetlerinin istihbarat birimlerince bilgi alışverişi içerisinde bulunarak engellenmesi amacıyla varlığını sürdürerek uluslararası sistemin barış ve huzurunun sağlanmasına büyük katkılar sağlamaktadır (Akiner, 2010). 2001 sonrası bölgesel olmaktan çok ekonomik olarak da etkin ve etkili bir örgüt olma yolunda ilerlemeye çalışan örgüt ortak bir siber güvenlik politikası oluşturamamaktadır. Bunun ana sebebi ise, örgüt içerisinde bulunan Çin ve Rusya gibi baskın karakterde olan devletlerin kendi çıkar ve amaç politikalarının farklı olması ve bu farklılıktan kaynaklı olarak siber güvenlik politikaları devletlerin kendi politikalarına bırakılmıştır (Baştuğ, 2022).

ŞİÖ'nün, siber güvenlik alanında atmış olduğu en somut örnek ise 16 Haziran 2009'da gerçekleştirdiği Yekaterinburg Deklarasyonu'nda üye devletler arasında bilgi teknolojilerini genel olarak düzenleyerek bilgi güvenliğinin sağlanması ve siber suçların bilgi güvenliğini tehdit etmesinden kaynaklı olarak temel iş birliğinin vurgulanması gerekliliğini bildirmesi olmuştur (Töner Şen, 202; Hathaway, vd., 2012)

2.3.5. Afrika Birliği'nin Siber Hukuk Alanında Gerçekleştirdiği Faaliyetler

21.yy. ile küreselleşme bütün dünyayı etkisi altına aldığı gibi Afrika kıtasını da etkisi altına almıştır. Tarihsel süreçte açlık, yoksulluk ve sömürge ile anılan Afrika kıtası, teknolojik gelişmelerden birlikte büyük bir potansiyel oluşturmuştur. 2000 yılında kıtada internet kullanana kişi sayısı 4,5 milyon kişiyken 2017'de bu rakam 453 milyona yükselmiştir (Orji, 2018). Internet World Stats'in (IWS) hazırladığı veriler ışığında 2022'nin ikinci çeyreğinde ise kıtada internete erişim sağlayan kişi sayısı 600 milyonu geçmiş ve bu rakam 2000 yılından itibaren karşılaştırılacak olursa 22 sene içerisinde %14.362 artış olduğunu göstermektedir (IWS, 2022).

DÜNYA İNTERNET KULLANIMI VE NÜFUS İSTATİSTİKLERİ 2022 Yılı Tahminleri						
Dünya Bölgeleri	Nüfus (2022 Tahmini)	Dünya Nüfusu %'si	İnternet Kullanıcıları 30 Haziran 2022	Penetrasyon Oranı (% Pop.)	Büyüme 2000-2022	İnternet Dünyası %
Afrika	1.394.588.547	%17,6	652.865.628	%46,8	%14.362	%11.9
Asya	4.352.169.960	%54.9	2.934.186.678	%67.4	%2.467	%53,6
Avrupa	837.472.045	%10.6	750.045.495	%89,6	614 %	%13,7
Latin Amerika / Karib.	664.099.841	%8.4	543.396.621	%81,8	%2.907	%9.9
Kuzey Amerika	374.226.482	%4,7	349.572.583	%93.4	%223	%6.4
Orta Doğu	268.302.801	%3,4	211.796.760	%78.9	6.378 %	%3,9
Okyanusya / Avustralya	43.602.955	%0,5	31.191.971	%71,5	%309	%0,6
DÜNYA TOPLAM	7.934.462.631	%100.0	5.473.055.736	%69.0	%1.416	%100.0

Kaynak: (IWS, 2022)

Şekil 12: 2022'de Bölgelere Göre İnternet Kullanımı ve Büyüme Oranları

Afrika ülkeleri birlik olma yolunda bazı girişimlerde bulunmuşlardır. Bu girişimlerden ilki Afrika Birliği Örgütü olmuştur. 1957'de Gana ile başlayan bağımsızlık hareketi kısa bir zaman içerisinde bütün Afrika kıtasına yayılmış ve Afrikalı lider ve düşünürlerin tek bir çatı altında toplanması gerektiği söylemleri artmıştır ve 25 Mayıs 1963'te Etiyopya'nın başkenti Addis Ababa'da 30 devletin katılımıyla imzalanmıştır (İpek, 2012). Afrika devletlerinin ortak bir üyelik içerisinde yer alma çabalarının altında yatan en önemli etken, sömürgecilik faaliyetlerinin engellenmesi ve tam bağımsız bir devlet olmak için gerekli dayanışmanın kıta devletleriyle gerçekleştirilmesi olmuştur. Fakat örgüt, içerisinde yaşadığı bazı problemler ve sıkıntılar neticesinde istenilen performansı sergileyememiştir. Soğuk Savaşın ve Afrika devletlerinin aralarında gerçekleşen çatışmaların son bulması ve dünya siyasetinin ideolojilerden ayrılarak çıkar eksenli hareket etme isteği ve birlik kurma yolunda ilerlemesiyle birlikte ikinci girişim 2001'de Afrika Birliği kurulmuştur (Orji, 2018).

Afrika Birliğinin amaçlarına bakılacak olursa, Afrika ülkeleri ve Afrikalılar arasında büyük bir birlik ve dayanışma meydana getirmek, kıtanın sosyo-ekonomik ve siyasi entegrasyonun artırılması, Afrika devletlerinin menfaatlerini kıta içerisinde

korumak, barış, güvenlik ve istikrarın korunması amaçlanmıştır. Yukarıda bahsedilen amaçların dışında en önemlisi ise bilim ve teknolojik alanlarda araştırmaların artırılması, nitelikli eleman sayısının artırılması ve verilen desteğin artırılması hedeflenmiştir (İpek, 2012).

Bilim ve teknolojiye yatırımın artırılması ve altyapı tesislerinin yenilenmesi veyahut oluşturulması, çağın kaçınılmaz bir unsuru olmuştur. İstatistiksel olarak da baktığımızda birliğin aldığı bu karar internet penetrasyonundaki artışın nedenini de göstermektedir. 2000'li yıllarla başlayan teknolojiye ve internete erişimin artması dünyada köklü değişikliklerin yaşanmasına neden olduğu gibi Afrika devletlerinde telekomünikasyon piyasalarının liberalleşmesine, geniş bant kapasitesinin artmasına ve mobil telekomünikasyon teknolojilerinin de artmasına neden olmuştur (Orji, 2018). Gerçekleşen yenilikler her uluslararası örgütte olduğu gibi siber güvenliğin sağlanması için gerekli adımların atılmasına itmiş ve bu bağlamda Afrika devletleri de adımlarını atmış fakat her devlette aynı hızda ve kapasitede ilerlememiştir. Örnekle açıklamak gerekirse, 2005'te Güney Afrika Gelişim Topluluğu üyesi olan Güney Afrika, Zambiya, Zimbabwe, Mozambik ve Malawi, siber suçları kendi yasalarına uygun hale getirmek için girişimlerde bulunmuş ve hızlı bir süreç belirlemişlerken aynı çalışmayı başlatan Tanzanya, Kenya ve Uganda gibi devletlerde uyum süreci çok yavaş ilerlemiştir (Ünver, vd., 2011).

Devletler siber alanın düzenlenmesi için çeşitli girişimlerde bulunduğu gibi Afrika Birliği 'de üye devletlerle ortak karar almak için bir dizi karar alma çalışmaları gerçekleştirmiş fakat bu çalışmalar 2008 yılına kadar somut adımlar atamamıştır. İlk adım 2008'de siber güvenliğin teşvik edilmesi, siber suçların izlenmesi ve önlenmesi, siber alanda tüketicinin haklarının korunması, siber güvenlik politikalarının belirlenmesini deklare eden *Afrika'da Telekomünikasyon, Bilgi ve İletişim Teknolojileri Politikalarının ve Mevzuatın Uyumlaştırılmasına İlişkin Çalışma* adında rapor yayınlamıştır (African Union, 2008). 5 Kasım 2009'da İletişim ve Bilgi Teknolojilerinden Sorumlu Afrika Birliği üyesi bakanlar, Güney Afrika'nın Johannesburg'da Oliver Tambo Deklarasyonu'nu kabul etmişler ve bu deklarasyon kapsamında Afrika kıtasının ihtiyaçlarına yönelik siber güvenlik politikalarının belirlenmesi ve siber mevzuat sözleşmesinin geliştirilmesi için ortak karar almışlardır (Orji, 2018). Afrika Birliği üye devletleri siber güvenlik politikaları belirlemek için sık sık çeşitli görüşmeler ve çalışma grupları kurmuşlardır. 2011'de *Afrika'da Siber*

Güvenlik için Güvenilir Bir Yasal Çerçevenin Kurulmasına İlişkin Taslak Sözleşme belirlenerek birlik üyesi devletlerin güvenlik yönetişimi ve siber suçların kontrol edilmesine yönelik yasaların tasarlanması ve iç hukuk ile uyumlu hale getirilmesi amaçlanmıştır (African Union, 2011). Taslak görüşme 2012'de Afrika Birliği Siber Güvenlik Uzman Grubu tarafından incelenerek kabul edilmiş, imzalanmak için Ekim 2013'te Yürütme Konseyi'ne yönlendirilmiş fakat akademisyenlerin ve muhalefetin baskıları nedeniyle taslak metin Ocak 2014'te kabul edilmiştir (Orji, 2018).

27 Haziran 2014'te Afrika Birliğinin Malabo'da gerçekleştirilen 23. Olağan Oturumunda Afrika Birliği devlet başkanları tarafından Siber Güvenlik ve Kişisel Verilerin Korunmasına İlişkin Afrika Birliği Sözleşmesi kabul edilmiştir (Orji, 2018). Bahsi geçen sözleşmenin maddelerine kısaca bakmak gerekirse, madde 3'te elektronik ticaret ile birlikte doğan kullanıcıların haklarının korunması e kişisel verilerin güvenliği sağlanmış, madde 7'de elektronik işlemlerde kişisel verilerin korunması kararlaştırılmış, madde 9'da kişisel verilerin nasıl işleneceği ve kimlerin erişimine izin verileceği detaylıca anlatılmış, madde 11'de üye devletlerin her biri vatandaşlarının kişisel verilerinin korunması için gerekli kurumların kurulması kararlaştırılmış, madde 24'te ulusal siber güvenlik politikalarının ve stratejilerinin belirlenmesi kararlaştırılmış ve madde 25'te üye devletlerin siber suçlara karşı etkili mevzuat çalışmalarının yapılması kararlaştırılmış ve madde 26'da siber güvenlik kültürünün oluşturulması hedeflenmiştir (African Union, 2014).

2.4. Siber Uzayda İnsan Hakları

2.4.1. Bireyin Siber Hak Alanı

1990'lı yıllarda yaygınlaşmaya başlayan internet kullanımı, günümüzde hayatımızın ayrılmaz bir parçası olmuş ve hayatımızın bütün alanında vazgeçilmez bir noktaya gelmiştir. Bu vazgeçilmez durum beraberinde büyük kolaylıklar, zaman tasarrufu ve refah getirdiği gibi insan hakları ihlallerinin ortaya çıkmasına, fiziki zorbalıkların sanal zorbalığa dönüşmesiyle aratan depresyon ve intiharlara, özel hayatın gizliliğinin ortadan kalmasına ve hak ihlallerinin ortaya çıkmasına neden olmuştur. Dünya genelinde anlık 4,95 milyar insanın internet kullanımına ulaştığı ve sosyal medya kullanıcı sayısının Ocak 2022 itibariyle 4,62 milyar olduğunu göz önüne alacak olursak,

siber suçların ve siber hak ihlallerinin çok fazla olması kaçınılmaz bir durum olarak karşımıza çıkmaktadır (Kemp, 2022).

İnternet kullanımıyla birlikte artan siber alanın hacmi, bireylerin özgürleşmesi, etkileşim içerisinde kalması ve anonimlik sayesinde siber alanda hareketlerinin gelişmesine neden olmuşken oluşan bu hacim beraberinde hakların ihlal edildiği ve anonimlik maskesi ile suçluların siber alanda serbest şekilde faaliyetlerine devam etmesine neden olmaktadır. Birleşmiş Milletler İnsan Hakları Yüksek Komiserliği dijitalleşmeyi, dünya demokrasisinin gelişmesinde ve demokratik katılımın sağlanması adına önemli bir araç olduğunu belirtmektedir (Akyeşilmen, 2018). Teknolojik gelişmelerin oluşturduğu fırsatlar bireylerin refahına seslenmesinden kaynaklı olarak bir aldatmaca oluşturmakta ve oluşan güvenlik açıklarının ötelenmesine neden olmaktadır. Örnekle açıklamak gerekirse, etkili iletişim araçlarından olan sosyal medyalar, temelde haberleşme ve sosyal iletişim becerilerinin artmasına neden olduğu gibi görünmeyenin arkasında zorbalığın ortaya çıkmasına neden olmaktadır. Yapılan saha araştırmasına bakacak olursak 18-35 yaş aralığına 1933 kişinin katılımıyla gerçekleştirilmiş ve yöneltilen sorularda, katılımcıların %35,1'i siber zorbalığa kaldığını belirtmiştir (Ekinci ve Kayapalı Yıldırım, 2020). Rakamsal olarak düşük çıkmasının sebebi ise yine aynı katılımcıların siber zorbalık kavramının ne olduğunu bilenlerin oranı %47,5 iken bilmeyenlerin oranı ise %52,5 olarak aktarılmıştır (Ekinci ve Kayapalı Yıldırım, 2020).

Günümüzde internet kullanımın yaygınlaşması sanallaşan kavramların bilinmemesine veyahut kapsamlarının ve işleyişinin nasıl olduğunun bilinmemesi, bireylerin temel hak ve hürriyetlerinin fiziki hayatta olduğu gibi sanal dünyada da olduğunu bilmemesinden kaynaklı olarak sanal ortamda gerçekleştirilen eylemlerin farkında olmamaktadırlar. Bu durum dijital mahremiyetin ortadan kalmasına neden olmaktadır. Dijital mahremiyet, geleneksel mahremiyet anlayışı ile aynı anlam bütünlüğünde olsa da kullanılan araçlarda ve yöntemlerde farklılıklar vardır. Gelişen sosyal medya araçları ile kullanıcıların değişen yaşam şekillerinin birbiriyle sentezlenmesi sonucu dijital mahremiyet ortaya çıkmaktadır.

Sosyal medya araçlarının temel mottoları gizlilik olmasına rağmen programların yapısı gereği içerisinde tezatlıkları barındırmaktadır. Kullanıcılar sosyal medyalarda kendilerine bir dünya oluşturarak bir mahremiyet bölgesi oluşturmaktadır fakat sosyal medya araçlarında oluşturulan bu dünyalar, geleneksel mahremiyet alanı özelliklerini

taşımamaktadır. Bir örnekle açıklamak gerekirse, Meta, diğer platformlara göre daha fazla mahremiyet ve gizlilik sunmasına rağmen Meta'nın kurulmasındaki ana fikir göstermek ve etkileşime girmektir (Barkuş ve Koç, 2019). Bu durum kendi içerisinde paradoks oluşturduğu gibi kullanıcılara siber alanda da mahremiyet sadece fikir olarak pazarlanmaktadır.

Siber mahremiyet konusunda bir diğer paradoks ise kanuni düzenlemelerle kişisel verilerin korunmasına yönelik çeşitli çalışmalar yapılarak hukuki olarak kullanıcıların mahremiyeti sağlanmaya çalışılmaktadır. Fakat tam tersi olarak devletler birtakım sebeplerden dolayı (terör, istismar, vd.) sosyal medyaları denetlediği gibi takip etmektedir. Örnek ile açıklamak gerekirse, Nisan 2023'te İngiliz hükümeti tarafından sunulan Online Safety Bill isimli yasa tasarısı ile Whatsapp ve Signal gibi uygulamaların uçtan uca şifreleme özelliğini kaldırmasını istediği gibi diğer sosyal medya uygulamaları olan Meta, TikTok gibi uygulamaları da sıkı şekilde denetlemek istemektedir (Cankurt, 2023; Milmo, 2023; BBC News, 2021). Fikir olarak çıkarılmak istenilen yasa incelendiğinde vatandaşların mağdur olmaması ve siber alanda da güvenliklerinin sağlanması adına büyük bir adım olarak görülebilirken aynı yasa farklı yorumlamayla kişisel mahremiyetin ortadan kalkmasına da neden olabilmektedir. Bu sebepten dolayı bireyler temel hak ve özgürlüklerinin fiziki hayatta farkında oldukları gibi sanal dünyada da temel haklarının farkında olmaları gerekmektedir. Bu gereklilik bireylerin bilinçlenmesine ve sanal dünyada maruz kalacakları eylemlerin engellenmesine neden olacaktır.

2.4.2. Bilişim Hakları Nelerdir?

Yayınlanan tüm insan hakları belgeleri ışığında, dünya halklarının haklarının güvence altına alınması, mevcut hakların günümüz şartlarına göre geliştirilip korunması ve BM şartının 55.maddesinin yükümlülüklerinin yerine getirilmesi insan haklarının güvence altına alınması günümüz şartlarında önemlidir (Viyana Deklarasyon ve Eylem Programı, 1993). Genel bir açıklama yapacak olursak insan hakları yayınlanan tüm belgelerde vurgulandığı gibi evrensel, bölünmez ve birbiriyle bağlantılı olan kurallar bütünüdür. Bilişim teknolojilerinin gelişmesi ve siber alanın aktif kullanılmasıyla birlikte bilişim hakları gündeme gelmiş ve bugün vazgeçilmez bir unsur olarak karşımıza çıkmaktadır.

Bugün gelinen noktada bilişim sistemlerinin ve teknolojilerinin gelişmesi, ortaya çıkan yeni teknolojik uygulamaların ve ürünlerin kullanıcıların kişisel verilerine erişmesi ve işlemesi ve siber alanın kapasitesinin artması kişisel verilerin ihlal edilmesine neden olmaktadır. Bu bağlamda çeşitli önlemler alınırken genel kabul görmüş bir hukuki metin bulunmamakla birlikte ülkeler kendi hukuki sistemlerine uygun kanunlar ve yönetmelikler çıkarmaktadırlar. Burada ortaya çıkan hukuki ikilik sorunu kullanıcıları mağdur ettiği gibi devletlerin de ortak bir karar çıkaramamalarına neden olmaktadır. Devletlerin tek bir hukuki metin oluşturamaması ise siber alana ve siber alanda gerçekleştirilen faaliyetlerin, devletler düzeyinde farklı yorumlanmasından kaynaklanmaktadır. Örnek olarak verecek olursak Fransa için siber alan, ülke menfaatleri ve ulusal güvenliğin sağlanması açısından gereklilik olarak görülürken farklı bir ülkede cezai yaptırımların gerçekleştirilmesi gerektiği düşünülmesine neden olmaktadır.

Bireylerin siber alanda çok fazla zaman geçirmesindeki etken, siber alanda sınırsız bir özgürlük vadetmesi ve demokratik katılımın varlığından kaynaklı olarak çok fazla tercih edildiği gibi bunun yanında özgürce fikirlerin beyan edilmesi ve bu fikirler beyan edilirken anonimlik sağlaması cazip bir alan olmasına neden olmaktadır. Bireylerin siber alanda gerçekleştirdikleri zaman süresinde birden fazla kişisel veriler ağ tabanında tutulmakta ve siber alanda serbest şekilde dolaşmaktadır. Her ne kadar kullanılan uygulamalar ve internet sitelerin güvenlik önlemleri olsa da veriler elde edilemez değildir.

Ülkemiz açısından bireyin siber alandaki haklarını korumaya yönelik çeşitli kanuni eklemeler yapılmıştır. Ülkemizde bilişim suçlarına yönelik tek bir kanun bulunmamakla birlikte mevcut kanunlara bilişim suçlarının eklenmesiyle bir hukuki dayanak oluşturulmuştur (BTK, 2019). Buna göre, Türkiye'de ilk yasal metin 1991'de Türk Ceza Kanuna (TCK) eklenmiş ve en kapsamlı bilişim suçları ile ilgili düzenleme 5237 sayılı TCK'da yer almış ve ilgili kanunun onuncu bölümünde bilişim alanında suçlar başlığı altında bilişim sistemlerine girme, sistemleri bozma ve engelleme ve verilerin silinmesi konularına yönelik düzenlemeler gerçekleştirilmiştir (BTK, 2019).

3. SİBER GÜVENLİĞİN ÖNEMİNİ ORTAYA KOYAN SAHA ve VAKA ANALİZİ

3.1. Siber Alanda Gerçekleştirilen Savaşlar

Gelişen telekomünikasyon teknolojileri ile yenilikçi teknolojilerin ortaya çıkması kaçınılmaz bir durum olduğu gibi fiziki dünyada gerçekleştirilen eylemler de değişmeye başlamıştır. İnsan refahının sağlanması ve etkin zaman tasarrufu ile üretimin artırılması amacıyla başlayan yenilikçi teknolojik yaklaşımlar, büyük kolaylık sağladığı gibi beraberinde çağımızın en büyük sorunlarının da ortaya çıkmasına neden olmuştur. Bu sorunlara kısaca bakmak gerekirse dünya kamuoyunu ve uluslararası sistemi tehdit eden siber savaşlar, siber saldırılar, istihbarat ve casusluk faaliyetleri, siber zorbalık ve sosyal mühendislik olarak saymak mümkündür.

Teknolojinin dinamik ve durağan olmayan bir yapısı olmasından dolayı her geçen gün yeni problemlerin ortaya çıkmasına neden olmaktadır. Modern bilgisayarların ortaya çıkması beraberinde bilgisayarların birbiriyle konuşması fikrinin ortaya çıkmasına ve bu fikir neticesinde internetin temellerinin atılmasına neden olmuştur. Teknolojinin durağan olmaması yeni teknolojilerin ortaya çıkmasına neden olmuştur. Günümüzde internet teknolojisi ile farklı bir boyut kazanan bilgisayar teknolojileri siber alanın sınırlarının belirlenememesine neden olmuştur. Siber alanın belirsizliği ve yeni teknolojilere uygun yapıya sahip olması fiziki dünya yerine sanal dünyaların ortaya çıkmasına da neden olmuştur. Bu durum beraberinde büyük bir tehdit alanın oluşmasına neden olmuştur.

Oluşan bu tehdit alanında kullanıcılar, şirketler ve devletler kendi menfaatleri doğrultusunda eylemler gerçekleştirmeye başlamasına neden olmuştur. Özellikle devletler, sosyal mühendislik faaliyetlerini gerçekleştirerek kullanıcıların düşüncelerini manipüle ederek kitlesel hareketlere yön vermektedir. Devletler siber alanda sosyal mühendislik faaliyetleri gibi proaktif yöntemlere başvurduğu gibi aktif saldırı yöntemlerini de kullanmaktadırlar. Özellikle siber saldırıları aktif olarak kullanarak, gizli materyallerin elde edilmesi, dijital ambargoların ve yaptırımların uygulanması, siber istihbarat ve siber casusluk faaliyetlerinin siber alanda gerçekleştirilmesinde aktif olarak siber alanı kullanmaktadırlar.

Siber alanın devletler düzeyinde bu kadar aktif olarak kullanılmasının temelinde teknolojik kabiliyet alanının geniş olması ve gizlilik oluşturmaktadır. Teknolojik kabiliyet alanının genişliği, devletlerin vatandaşlarından veya şirketlerden daha fazla teknolojiye sahip olması, yeni teknoloji geliştirecek gücünün ve kapasitesinin olması veya satın alma gücünün olması, siber alana yönelimi artırdığı gibi fiziki saldırı veyahut fonlama yöntemlerinden daha ucuza ve etkili olması da siber alanın cazibesini artırmaktadır. Devletlerin siber alanı seçmesindeki bir diğer nedense siber alanda gerçekleştirilen eylemlerin kaynağının takip edilemez olması sebebiyle uluslararası toplumda gerçekleştirilen siber saldırılarda fail durumuna düşmemesine olanak sağlamasından kaynaklı tercih edilmektedir.

Genel algı içerisinde siber savaş ile siber saldırılar birbirinin yerine kullanılmaktadır. Fakat iki kavram birbirinden farklıdır. Siber saldırılarda amaç maddi gelir elde etmek üzerine kuruluyken siber savaşta amaç ise, gelir elde etmek yerine karşı tarafın büyük maddi kayıplar verdirerek kritik altyapılarının ve tesislerin kullanılamaz hale getirilmesi üzerine kuruludur (6. e-Safe Siber Güvenlik Zirvesi, 2022). Siber savaşa örnek olarak 2007 Estonya saldırısı ve İran'ın nükleer çalışmalarını sekteye uğratmak üzerine 2010'da gerçekleştirilen Stuxnet saldırısı gösterilebilir.

3.1.1. Savaş Hukuku

Hukukun zaman içerisinde etkili kalması ve caydırıcı bir unsur olarak varlığını devam ettirmesi gerekiyorsa yeni gelişmelere duyarlı olması gerekmektedir. Hukukun yeni gelişmelere duyarlı olması eski normları sileceği gibi güncel bir hal alacaktır. Hukukun güncel kalması içinse uluslararası örgütlerin, uluslararası mahkemelerin, seçmenlerin ve siyasi eylem gruplarının devletler arasındaki fikir birliğini sağlamasıyla olmaktadır (Schmitt, 2014). Hukuk yapısal olarak etkili kalabilmesi için yeni gelişmelere açık olsa da savaşın engellenmesi için tamamen etkili olamamakta olduğu gibi savaşın şiddetinin azaltılması veyahut sivil kaybın en aza indirgenmesi için savaş hukukunun ortaya çıkmasına yardımcı olmuştur. Savaş hukuku kavramı birden ortaya çıkmadığı gibi halihazırda var olan hukuki metinlerin savaş esnasında uygulanmasıyla oluşmaktadır. Kennedy, günümüzdeki savaşları birleşik küresel kurumlar tarafından değil de yoğun kurallar ağı ve ortak varsayımlar tarafından yani hukuk tarafından yönetilen bir alanda gerçekleştiğini savunmaktadır (Kennedy, 2006).

Savaş kavramının tanımlanmasında ve açıklanmasında net bir tanım bulunmamakla birlikte tanımlamamasında hukuksal bakış açısı farklılıkları kadar ideolojik, siyasal, ekonomik ve sosyal yaklaşımlarda tanımlanamamasında etkili olmaktadır (Aslan, 2008). Savaş hukuku iki temel üzerine kurulmuş ve silahlı kuvvet kullanımı da hukuksal olarak jus ad bellum ve jus in bello olmak üzere iki boyut içerisinde değerlendirilmektedir. I. Ve II. Dünya Savaşlarının getirdiği büyük yıkım ve istikrarsızlık, devletlerin savaşın önlenmesi veya önlenemez ise de savaşın kurallarının belirlenmesi için adım atmaya itmiştir. Bu bağlamda, BM Sözleşmesi ve Silahlı Çatışma Hukuku ile ele alınmıştır (Çifci, 2017). Savaş hukukunun oluşturulmasında temel amaç her zaman devletlerin herhangi bir uyuşmazlık içerisinde ilk olarak savaşa başvurmalarını engellemek ve bunun yerine uluslararası platformlarda savaş girişimini engellemek üzerine oluşturulmuştur (Aslan, 2008).

II. Dünya Savaşının başlaması uluslararası barışın tesis edilmesi için oluşturulan Milletler Cemiyetinin yetersiz kaldığını göstermiş ve II. Dünya Savaşı sonunda dünyanın tekrardan bir savaşa sahne olmaması adına güçlü bir yapıda olan BM kurulmuş ve BM Sözleşmesinin 2. maddesinin 4. bendinde üye devletlerin herhangi bir başka devletin toprak bütünlüğüne zarar verecek ya da siyasal bağımsızlığına karşı herhangi bir şekilde kuvvet kullanımından kaçınacağı gibi kuvvet kullanma tehdidinde de bulunulmayacağını belirtmiştir (BM Anlaşması, 1945). Yine aynı anlaşmanın 7. Bölüm 39. Maddesinde Güvenlik Konseyi, barışın tehdit edilmesi, tehdit edilmesi ya da saldırı eylemi olduğunu saptaması durumunda 41 ve 42. maddelerde yer alan silahlı kuvvet kullanımını içermeyen önlemlerin alınmasını kararlaştırmıştır. (Birleşmiş Milletler Anlaşması, 1945) Ayrıca barışın tesis edilmesine yönelik hemen her devletin kabul ettiği 1949 tarihli Cenevre sözleşmesinin 2. maddesine yönelik insancıl hukuk kurallarının silahlı çatışmalarda her iki devlete de eşit olarak uygulanacağı kararlaştırılmıştır (Aslan, 2008).

3.1.2. Siber Savaşlar Neden Bu Kadar Tercih Ediliyor

Soğuk Savaş ile başlayan teknolojik yarış sonucunda ortaya çıkan internet siber alanın genişlemesine neden olmuştur. Siber alanın aktif kullanılmasıyla birlikte siber alanın görünen kısmından hariç görünmeyen yüzünün keşfedilmesi bazı kesimlerin dikkatini çekmiştir. Özellikle ABD'nin siber alanı savaş alanı olarak ilan etmesi ve

akademi çevresinde siber savaşların tanımlarının yapılmasıyla ilgi siber alana kaymıştır (Arquilla, 2013). Siber savaşların dünya genelinde bu kadar fazla tercih edilmesinde öncelikli olarak saldıran kişinin kimliğinin tespitinin zor olmasından dolayı tercih edilmektedir. Bir diğer neden ise siber savaş sırasında hedef ülkenin ekonomik olarak büyük zararlara uğramasına neden olması etkili olmuştur.

Örnek ile açıklayacak olursak 2007 Estonya saldırısı sırasında ülke 3 haftalık uzun bir süre dijital dil ile off konumunda kalmış, bankalar, kamu kurum ve kuruluşları işleyişini gerçekleştirememiş ve vatandaşlar neredeyse özgürlüklerini kaybetmiştir. Estonya hükümeti saldırının Rusya tarafından yapıldığını açıklasa da kesin bir kanıt bulunamamıştır. Örneği inceleyecek olursak, fiziki şartlarda Rusya, Estonya'ya saldırmış olsa çok büyük askeri yığınak yapması lazım ve bununla birlikte mevcut yasaları çiğnemesinden kaynaklı olarak ağır bir ekonomik yaptırımla karşı karşıya kalması mümkün olacaktır. Ayrıca savaş esnasında insan ve askeri teçhizat kayıpları da Rusya hükümetine ciddi sonuçları olacaktır. Fakat aynı etkiyi bir grup insan ve yazılımlar ile ülke içerisinde güvenli şekilde yapıp hem sivil ve askeri kaybın önüne geçmiş olacak hem de fiziki savaştan daha etkili bir sonuç alarak ülkesini fail konumuna düşürecektir.

Devletler yukarıda saydığımız nedenlerden dolayı siber savaşları tercih ettiği gibi bir de bu durumun sosyolojik boyutu bulunmaktadır. Bir devletin başka bir devlete saldırması durumunda kazanan taraf olmak için büyük bir orduya ihtiyacı olduğu gibi kamuoyunda da geniş bir destekleyici kitlesi olması gerekmektedir. Modern popüler demokrasilerinde halklar, savaşların yıkıcılığını, adaletsizliğini ve insanlık dışı bir eylem olduklarına inandıkları için siber savaşlara yönelmektedir (Dunlap, 2012). Siber savaşların ortaya çıkmasıyla birlikte halk nezdinde konvansiyonel bir savaş gibi etki yaratmaması, siber savaşların önemsiz bir durum olarak görülmesine neden olmuştur. Bu durum siber savaşa özgü olan boşlukların olmasından kaynaklanmaktadır.

Siber unsurların günümüzde aktif olarak kullanılması, konvansiyonel savaşlarda elde edilmesi güç olan sosyolojik travma ve etkilerin siber alanda farklı araçlarla daha kolay olarak yaratılmasından dolayı da siber savaşlar etkin şekilde tercih edilmektedir. Örnek olarak açıklamak gerekirse, ABD halkında yerleşik olan Ortadoğu imajının oluşmasında her ne kadar konvansiyonel savaşlar etkili olmuş olsa da asıl toplumları şekillendiren ve manipüle eden sinema sektörü ve internet haberciliği olmuştur. 11 Eylül

saldırısından güvenlik algısı köklü olarak değiştiği gibi ABD sinema sektörü de köklü değişiklikler yaşayarak yeni bir tür olarak kara mizah Ortadoğu ortaya çıkmış ve ortaya çıkan filmlerde Ortadoğu halkı terörist olarak gösterilmekten kaçınılmamıştır (Boggs ve Pollard, 2006).

Kamuoyunda siber savaşların konvansiyonel savaşlara nazaran daha geri planda kalmasında siber savaşta kullanılan araçların etik ve akıllıca bir politikalarının olmaması ve kamusal veyahut siyasi tartışmamaların olmaması, kamuoyunun yeteri kadar bilgi sahibi olmamasından dolayı önemsiz olarak görmektedirler (Dipert, 2010). Bir diğer boşluk ise siber savaşlarda tarafların kimliklerinin belirleme sorunun olmasından kaynaklı olarak inkâr edebilme ortamının oluşmasıdır (Dipert, 2010).

3.2. Siber Güvenlik İçin Gerçekleştirilen Siber Savunma Faaliyetleri

3.2.1. Siber İstihbarat Faaliyetleri

Devletlerin, şirketlerin ve toplumların dijitalleşmesi, yeni bir alan olan siber alanın genişlemesine ve bu alanda aktif ve proaktif eylemlerin gerçekleştirilmesine neden olmuştur. Yüzyıllardır bireyler, şirketler ve devletler fiziki olarak rekabet içerisinde olduklarından dolayı dünyanın en eski mesleklerinden birisi olan istihbaratçılığı aktif olarak kullanmışlardır. İstihbarat kelime anlamı "*yeni öğrenilen bilgiler ve haberler*" olarak Arapçadan dilimize geçmiş bir sözcüktür (TDK, 2022). İstihbarat kavramına bugüne kadar farklı bakış açılarından birden fazla tanımlaması yapılmış olsa da genel bir tanımlama yapmak gerekirse, elde edilen bilgi, haber ve söylemlerin bir araya getirilerek değerlendirilip ayıklanması sonrasında gerekli analizlerin yapılıp yorumlanması sonucu salt bilginin gerekli kurum ve kuruluşlara verilmesi olarak tanımlanabilir.

20.yy'ın son çeyreğinden itibaren gerçekleşen teknolojik atılım hareketleri, bireylerin, şirketlerin ve devletlerin dijitalleşmesine olanak sağlamış ve yeni bir boyut olan siber alanın açılmasına ve aktif kullanılmasına neden olmuştur. Özellikle de son 20 sene içerisinde siber alanın kapasitesinin ve hareket alanının katlanarak büyümesi ve fiziki dünyada gerçekleştirilen eylemlerin siber alana taşınması, büyük kolaylıklar sağladığı gibi beraberinde de büyük sorunları getirmiştir. Özellikle de siber tehditlerin ve siber savaşların siyasi, sosyal, ekonomik ve kültürel olarak büyük yıkımlara neden

olması sebebiyle istihbarata olan ihtiyaç gün geçtikçe artmıştır. Siber alanda istihbaratın gerekliliğini anlamak için istihbaratın bileşenlerini anlamak gerekmektedir. Devletler ve şirketler varlıklarını devam ettirebilmek ve söz sahibi olmak adına istihbaratın coğrafi, ulaştırma, sosyal, ekonomik, teknolojik, siyasi ve askeri bileşenlerinden sıkça yararlanmaktadırlar (Çifci, 2017).

İstihbarat bileşenlerinin çok fazla çeşitlilik göstermesi, fiziki dünyada olduğu gibi siber alanda da istihbaratın önemli bir unsur olmasına neden olmuştur. Bilgi çağının gelişmesiyle birlikte geleneksel istihbarat yerini daha güvenli, iz bırakma oranı daha düşük olan siber istihbarata yöneltmiş ve beraberinde sinyal istihbaratı ve ölçüm ve iz istihbaratlarının gelişmesine de öncülük etmiştir (Bayraktar, 2014). Fakat siber istihbaratın ortaya çıkması ve etkili sonuçlar ortaya koymasında zayıf halka olan insan faktörünün etkisi çok büyük olmuştur. Siber alanı yapılan işin kalitesinin artırılması, daha verimli sonuçlar alınabilmesi ve sosyalleşme amacıyla aktif olarak kullanan kullanıcılar, arkalarında belirli bir siber ayak izi bırakmaktadırlar. Kullanıcıların beraberinde bıraktığı izlerin takip edilmesi sonucunda toplanan veriler işlenerek istihbarata konu olup olmamasına karar verilerek kullanılmaktadır (Fachkha ve Debbabi, 2016).

Devletler ve şirketler günümüzde aktif olarak siyasi ve ekonomik varlıklarını koruyabilmek ve etki alanlarını artırabilmek için siber alanın ürünlerinden aktif olarak faydalanmaktadır. Devletler ve şirketlerin ayrı siber güvenlik politikaları ve siber yaklaşımları olsa da devletler diğer devletlerin yetki alanında faaliyet gösteren kendi şirketlerini de korumakta ve şirketlerin çıkarlarına göre de politikalar belirlemektedir. Şirketler yeni pazarların oluşturulması adına siber alanı aktif kullandığı gibi uluslararası ticaret sisteminde tekel konumunda olmak veyahut öncü olmak için de siber alanı aktif kullanarak hedef şirketlere saldırılar gerçekleştirerek ticari sırları elde ederek siber alanda ticari istihbarat faaliyetlerinde bulunmaktadırlar.

Devletler de şirketler gibi ticari sırların elde edilmesi üzerine faaliyette bulundukları gibi ülkesel ekonomi politikalarının belirlenmesi, çıkarlarının korunması ve hedeflerinin gerçekleşmesi için siber istihbarata sıkça başvurmaktadırlar. Devletler toplanan verilerin işlenmesi ve tasnif edilmesi için çeşitli algoritmalar kullansa da klasik istihbarat unsuru olan insan kaynağına her zaman ihtiyaç duyulduğunu da belirtmek gerekmektedir. Klasik istihbarat ile siber istihbarat arasındaki fark ise klasik istihbaratta

belirli bir hedef ve kısıtlı bir bilgi elde edilirken, siber istihbaratta konu çeşitliliği fazla ve geniş bir alana hâkim olunmaktadır.

Bilgi çağının bir ürünü olarak ortaya çıkan internet ve siber alan, aktif olarak kullanılmaya başlanmasıyla birlikte saldırıların ve istihbarat faaliyetlerinin ilk örnekleri de ortaya çıkmaya başlamıştır. Cuckoo's Egg (Guguk Kuşu olayı) olarak kayıtlara geçen ilk vaka, 1986'da Rus istihbarat birimi KGB ajanı olan Markus Hess tarafından Lawrence Berkeley Ulusal Laboratuvarı'na yönelik gerçekleştirdiği bir dizi saldırı sonucu sistem içerisinden pek çok gizli belgeleri elde etmiştir (Jupillat, 2016). Cuckoo's Egg olayı siber istihbarat ve casusluk alanında ilk vaka olarak kayda geçtiği gibi bu olayı Jupillat makalesinde küresel gözetleme olarak ifade etmiştir (Jupillat, 2016).

Siber istihbaratta vaka örnekleri olduğu gibi çok uluslu projeler de bulunmaktadır. ABD ve İngiltere, öncülüğünde başlatılan ve daha sonrasında Kanada, Avustralya ve Yeni Zelanda'nın da katılımıyla oluşturulan Echelon projesi, hedef ülkelerin telefon görüşmelerinin ve telgraf yazışmaların dinlenmesi üzerine kurulmuştur (Abdurahmanlı, 2021). Resmi olarak ABD hükümeti bu projenin varlığını kabul etmediği gibi reddetmemiştir (Slaon, 2000). Fakat bu projeyi doğrulamaya en yakın açıklamaysa Merkezi İstihbarat Direktörü George Tenet'in sinyal istihbaratı üzerine yapmış olduğu konuşma kaynak olarak gösterilmektedir (Slaon, 2000).

3.2.2. Siber Terörizm Faaliyetleri

Terör kavramı, Fransızca kökenli olup Fransız Devrimi sırasında ortaya çıkan ve devrimcilerin içeride bulunan düşmanlara karşı gerçekleştirdikleri doğrudan veyahut dolaylı olarak ortaya koydukları eylemler olarak kullanılmıştır (Küçükcan, 2010). Etimolojik olarak kavram, Latince terrere kelimesinden gelerek anlamı korkutmak, ürkütmek veya sindirmek anlamına gelmektedir (Saraçlı, 2007). Terörle Mücadele Kanunu madde 1'de ise, baskı, cebir, şiddet veya yıldırma yoluyla yapılan; cumhuriyetin siyasi, sosyal ve ekonomik yapısını değiştirmeye yönelik yapılan eylemler olarak tanımlanmıştır (Terörle Mücadele Kanunu, 1991). Terör kavramı için genel ve kapsayıcı bir tanımlama yapmak gerekirse vatandaşların, şirketlerin ve hatta devletlerin kararlarını etkilemek ve değiştirmek için ortaya konan eylemler bütünü olarak tanımlanabilmektedir. Dünya genelinde her yerde görülebilen terör eylemleri vatandaşlar üzerinde ve devletin algı sisteminde büyük acılar bıraktığı gibi insanlığın

teknoloji ile tanışmasıyla birlikte farklı bir boyuta evrilmesine neden olmuştur (Yetkin ve Baştuğ, 2021b).

İnsanlığın ve teknolojinin zamanla değişmesi, devletlerinde terör ve terörizme karşı olan yaklaşımlarının değişmesine neden olmuştur. Uzun yıllar boyunca devletlerin ve kurumlarının üzerinde bir baskı ve korku unsuru olarak görülürken devletler ve devlet dışı aktörler, terörü diğer devletlere ve toplumlara karşı bir koz unsuru olarak kullanmaya başlamışlardır (Mannik, 2009). Devletlerin teröre karşı yaklaşımlarındaki değişimlerin ana sebebi dış politikalarının veyahut stratejilerinin kabul ettirmek için güç ve baskı unsuru olarak kullanmasından kaynaklanmaktadır. Teknolojinin gelişmesiyle birlikte terör de hem şekil değiştirmiş hem de fikir olarak kendisini değiştirerek yeni alanlar ve çağa uygun yeni yöntemler geliştirmiştir ve bu durum siber terörizmin ortaya çıkmasına neden olmuştur.

Dijital çağın gereksinimi olarak internet kullanımının yaygınlaşması, yeni dijital dönüşümlerin yaşanmasına neden olmuştur. Siber alanın her geçen gün katlanarak büyümesi, yatırımların bu alanda yoğunlaşması ve ciddi bir para trafiğinin gerçekleşmesi, devletlerin ve çokuluslu şirketlerin ilgisini çektiği gibi terör örgütlerinin de ilgisini çekmiştir. Günümüzde yazılı ve görsel materyallerin siber alanda serbest dolaşımda olması ve paraların sanallaşması sebebiyle terör örgütlerini cezbetmiş ve terörizm faaliyetleri için de yeni bir eylem alanı oluşmasına neden olmuştur. Siber ve terörizm kelimelerinin birleştirilerek oluşturulan siber terörizm kavramı ilk defa 1980'de Barry Collin tarafından kullanılmış ve temel amacı olarak, terör eylemlerinde internete bağlı kişisel bilgisayarları ele geçirmek, saldırılarda bilgisayar teknolojilerini kullanmak ve internet tabanlı saldırılar gerçekleştirerek kritik kurum ve kuruluşlara zarar vermek olduğu gibi örgütün para ihtiyacını karşılayabilmek ve propaganda yapmak olarak tanımlanmıştır (Yılmaz, 2020).

Siber terörizm faaliyetleri günümüzde sıkça kullanılmakta olsa da hâlâ devletler siber alanda hâkim konumda bulunmaktadır. Devletlerin siber alanda aldıkları önlemler fazla olsa da siber alan tamamıyla keşfedilememiş bir alan olduğu için hala açıklar mevcuttur. Var olan bu açıklar sayesinde eylemlerini gerçekleştiren terör örgütler anlık veyahut aynı açık kapıdan birkaç kez saldırı gerçekleştirirken devletler kurum ve kuruluş altyapılarına yönelik sistematik saldırılar gerçekleştirerek kendi güvenlik katmanlarını

denedikleri gibi açıkları da keşfederek siber terörizme fırsat vermemeye çalışmaktadırlar (Craig ve Valeriano, 2018).

İnternet teknolojilerinin gelişmesiyle kullanıcı ağının artması terör örgütlerinin dikkatini çektiği gibi yeni bir propaganda alanının oluşmasına ve saldırıların da çağın şartlarına uygun olarak sanallaşmasına neden olmuştur. Terör örgütlerinin siber alanda gerçekleştirdiği saldırıları incelemeden önce interneti kullanarak gerçekleştirdikleri propaganda araçlarını incelemekte fayda vardır. Örnek olarak IŞİD, hazırladığı yazılı ve görsel mesajları dünyanın farklı yerlerinde bulunan militanları ve sempatizanlarına iletmek, örgüte yeni sempatizan kazandırmak ve yayınlanan mesajlar ile dünyanın farklı ülkelerinde bulunan hücrelerini uyandırmak için bir araç olarak kullanmaktadır. Bunun ilk örneği, 5 Temmuz 2014'te ilk e-dergisi *Dabiq* yayın hayatına başlamıştır (Sönmez, 2019). İngilizce, Arapça, Almanca ve Fransızca yayınlanan dergi, reklam alanında eğitim almış, ve anadili İngilizce olan kişileri kullanarak dünyanın farklı kesimlerinde bulanan ve internet kullanan kişileri kazanmak adına çalışmalar gerçekleştirmeye başlamıştır (Türkoğlu, 2017). Ayrıca 2015'te IŞİD'e bağlı olan Cyber Caliphate isimli hacker grubu, ABD Merkez Komutanlığında çalışan personellerin Youtube ve Twitter hesaplarını ele geçirerek propaganda faaliyetlerinde bulunmuşlardır (Agazzi, 2020).

Bir diğer örnek ise 11 Eylül'de El-Kaide tarafından gerçekleştirilen fiziki terör saldırı sadece fiziki olarak kalmamış ve siber alanın da terör amaçlı kullanılabileceğini kanıtlamıştır ve ilk siber terör eylemleri arasında yer almıştır. 11 Eylül saldırısı ile İslam fobinin yaygınlaşması ve Müslümanların hedef olarak gösterilmesiyle başlayan süreçte El-Kaide, ABD hükümetine karşı tehdit mesajları yayınlamış ve birçok farklı web sitesine yönelik saldırılar gerçekleştirmiş ve ABD hükümeti saldırıları engellemek adına internet iletişimini kesintiye uğratarak saldırıları hafifletmek istemiştir (Halder, 2011). Bu durum beraberinde cihad kavramının sadece savaş veyahut propaganda yoluyla olmayacağı gibi siber cihad kavramının ortaya çıkmasına da neden olmuştur (Halder, 2011).

Son örnek olarak, PKK terör örgütünün siber alanda gerçekleştirdiği saldırı girişimleri incelenebilir. PKK terör örgütünün siber saldırı grubu olan PKK Hack Team, adını 2006'da devlet kurum ve kuruluşları ile diğer internet sitelerine gerçekleştirdiği 2307 adet saldırı ile isimlerini duyurmuştur (Bıçakçı, vd., 2015). Örgütün saldırı yapan

grupları sürekli olarak siberay ve emniyet istihbarat tarafından kontrol edildiği için önleme ve karşı saldırılar ile bertaraf edilmektedir.

Terör örgütleri siber alanı saldırıları ve propaganda aracı olarak kullandıkları gibi siber alanda devlet kurum ve kuruluşlarına yönelik saldırılar gerçekleştirdiği gibi saldırı yapılacak mesajını vererek kamuoyunda korku ve paniğe de yer vermektedirler. Oluşturulan bu korku ve panik havasında ekonomik durgunluğa sebep olacağı gibi olağanüstü güvenlik önlemleri hayatın doğal akşını da engellediği için sosyal hayatta da büyük panik ve korku oluşturmaktadır (Cho ve Woo, 2017). Çünkü saldırının siber terör olarak kabul edilebilmesi için vatandaşlar arasında hem ekonomik hem de insani faaliyetler konusunda ciddi korku ve endişe yaratması gerekmektedir (Heickerö, 2014).

3.2.3. Siber Casusluk Faaliyetleri

Bilgi ve iletişim çağında devletlerin ve şirketlerin güvenliklerine yönelik gerçekleştirilen en büyük saldırılar siber casusluk faaliyetleri olmuştur. Bilgisayar ve internet teknolojisinin önlenemez şekilde büyümesi, şirketler ve devletler düzeyinde büyük kolaylıklar yarattığı gibi bu kolaylıkların sağlandığı siber alan, şirketlere ve devletlere yönelik büyük bir savaş arenasının oluşmasına da neden olmuştur. Casusluk faaliyetlerini bir sanat olarak kabul edecek olursak eski tarihlerden itibaren sürekli olarak başvurulan bir faaliyetler bütünüdür.

Casus kelimesi etimolojik olarak Arapça kökenli kelime olarak literatürümüze girmiş, düşman menfaatine yönelik gözetleme faaliyetlerinde bulunarak gizli şeylerin elde edilmesi olarak tanımlanabileceği gibi, 1889 Lahey Antlaşması'nın 29. maddesinde kelime, gizli şekilde düşman saflarından bilgi elde etmeye veya elde eden kimse olarak tanımlanmış, 1907 Lahey Konferansı'nda ise kelime, gizli ve sahte bahanelerde bulunarak elde edilen bilgi ve belgeleri elde eden kimse olarak tanımlanmıştır (Yayla, 2014).

Casusluk bir sanat olarak tarih buyunca kendisine yer bulmuş ve tarihte yer bulmasında nüfuz alanı geniş insanların daha fazla bilgiye sahip olma isteği, şirketlerin diğer şirketlerin faaliyetlerinden haberdar olmak ya da piyasada tekel olma isteği ve devletlerin egemenlik ve güvenliklerinin tesis edilmesinde bir araç olarak casusları kullanması sebebiyle popülaritesi hiçbir zaman eksilmemiştir. Zaman içerisinde gelişen

bilgi ve iletişim teknolojilerinin gelişmesiyle birlikte casusların A noktasından elde ettiği gizli bilgi veya belgelerin B noktasına iletilmesinde büyük kolaylıklar yaşanmasına neden olmuştur. Teknolojini gelişmesi verilen toplanması konusunda devrimler yarattığı gibi günümüzde artık casuslukta insan faktörünün kullanımı yerini bilgisayarlara ve siber alana bırakmıştır. Eskiden casusluk faaliyetleri ekseriyetle askeri ve siyasi amaçlar için kullanılırken günümüzde ekonomik, kültürel, teknolojik, eğitim ve sosyal amaçlarla yani hayatımızın tüm alanıyla alakalı konularda aktif olarak kullanılmaktadır.

Casusluk faaliyetleri kapsamında siber alanda kullanılabilir çok fazla araç ve yöntem olduğu gibi bunlar içerisinde en çok tercih edilen DDoS saldırıları, kimlik avı, sosyal mühendislik faaliyetleri ve yazarlı yazılım ve virüsler olarak gösterilebilir. Elbette teknolojinin her geçen gün katlanarak gelişmesi yeni yöntemlerin oluşmasına ve casusluk faaliyetlerinin de gelişmesine olanak sağlayacaktır. İstihbarat ve casusluk bir devletin ayakta kalabilmesi ve politikalarının belirlenebilmesi için önemli bir faktördür. İnternetin gelişmesiyle birlikte asırlardır süren güvenlik ile özgürlük arasındaki gerilime de yeni bir yaklaşım getirmiş ve siber casusluk kavramının ortaya çıkmasına neden olmuştur (Banks, 2017). Siber casusluk, bir düşman tarafından belirlenen sistem ve ağlara sızarak veyahut yardımcı program ve yazılımlarla yerleşerek kasıtlı olarak bilgi ve belgelerin elde edilmesi veyahut yapılacak olan değişikliklerle ilgili sabotajların yapılması olarak tanımlanabilir (Banks, 2017).

Siber casusluk kavramına yönelik vereceğimiz örnekler (Moonlight Maze ve Titan Rain saldırıları, 2016 ABD seçimlerine müdahale, 2007 Estonya saldırısı, vs.) temelde siber güvenliğin farklı kollarıyla birlikte ortak örnek olarak gösterilmektedir. Siber alanda gerçekleşen bir vaka, siber saldırı, siber istihbarat, siber casusluk ve sosyal mühendislik faaliyetleri kapsamında değerlendirilmesi muhtemeldir. Bunun ana sebebi ise bilgi, belge ve siber ayak izinin siber alanda serbest şekilde dolaşımda olmasından kaynaklı, gerçekleştirilen eylem sonucunda elde edilen veriler birden farklı alan için kullanılmaktadır.

Örnekler üzerinden siber casusluğu inceleyecek olursak karşımıza ilk olarak Moonlight Maze ve Titan Rain vakaları çıkmaktadır. Moonlight Maze (Ay Işığı Labirenti) vakası, ABD'ye yönelik gerçekleştirilen en uzun süreli saldırı olmakla birlikte, ne zaman yerleştiği bilinmeyen ve 2011'de keşfedilmiş, Pentagon ve NASA'nın

sistemlerine yerleşerek belgelerin kopyalandığı bir saldırıdır (Akyeşilmen, 2018). ABD'ye yönelik gerçekleştirilen bu saldırıda virüsün ne zaman eklendiği ve ne kadar bilginin çıktığı bilinmemekle birlikte bu saldırı, dergilere kapak olacak kadar ABD kamuoyunda geniş yankı bulmuş ve 2015'te Ash Carter yaptığı açıklamada, saldırıların tekrar yaşanmaması ve ABD'nin kurum ve kuruluşların güvenliğinin sağlanması için Amerikan ağlarının korunması gerektiğini vurgulamıştır (Buchanan ve Sulmeyer, 2016; Akyeşilmen, 2018).

Titan Rain vakası, net olmamakla birlikte Çin kaynaklı olarak değerlendirilen ve 2003'te sistematik olarak düzenlenen saldırılar sonucunda ABD Füze Havacılık Ordu Komutanlığı'nın Merkezi'ne sızılarak, füze ve hava savunma sistemlerinin yazılımlarının ve askeri sırlar elde edilmiştir. ABD'li yetkililerin bu saldırıda Çin'i suçlamalarındaki neden saldırının Çin'in Guangdong eyaletine kadar takip edildiğini ve daha sonrasında kaybolduğunu iddia etmeleri olmuş olsa da net bir şekilde nereden kaynaklandığını belirtmemişlerdir. Casusluk faaliyetlerinde devletlerin devletlere karşı gerçekleştirdiği eylemler gibi şirketlerden şirketlere veyahut devletlerden şirketlere yönelikte saldırılar gerçekleşmektedir. ABD yönetimi ekonomik casusluk faaliyetlerinin engellenmesi için 1996'da Ekonomik Casusluk Yasası'nı çıkarmış ve bu yasa kapsamında ABD şirketlerine yönelik ekonomik siber casusluk yapan 5 Çinli askeri ekonomik casusluk yapmakla suçlamıştır (Skinner, 2014).

3.2.4. Siber Manipülasyonlar

Dünyanın dijitalleşme süreci içerisine girmesi bilginin de dijitalleşmesine ve siber alanda işlenmesine neden olmuştur. Kaçınılmaz bir durum olan bilginin dijitalleşmesi beraberinde yeni sorunların ortaya çıkmasına, sosyolojik açıdan toplumlarda derin yaraların oluşmasına ve yine toplumlar arasında güvensizlik ve istikrarsızlığın oluşmasına neden olmaktadır. Özellikle son dönemde artış gösteren sosyal medya kullanımı, bilginin kolayca ve hızlı şekilde yayılmasına neden olduğu gibi bir grup veya kesimin de hedef tahtasına konmasına neden olmaktadır. Sadece sosyal medyalarla gerçekleşmeyen bu durum televizyon yayınları, radyo yayınları ve ajanslar aracılığıyla da gerçekleşmektedir. Basın ve yayın organlarıyla birlikte sosyal medyalarda ortaya çıkan spekülatif ve manipüle edilmiş haberler dijital etik kavramının da önemini ortaya koymaktadır.

Etik, insan hakları, adalet, dünya barışı ve bireyin ve toplumun refahının sağlanması için ahlaki eylemler ve yargılar üzerine çalışmaktır (Özcan, 2021). Kapsam ve çalışma açısından incelendiğinde etik kavramı da dönemin şartlarına, siyasi, sosyal, ekonomik ve teknolojik gelişmelerle birlikte kapsamını değiştiren ve gelişen bir kavramdır. Toplumsal algılamanın ve değer yargılarının değişmesi etik kavramının yarım asır öncesi ahlaki değerler ile günümüzde ahlaki değerleri karşılaştırdığımızda etik kavramının da değiştiğini görmekteyiz. Sosyal kavramının günümüzde çeşitlenmesi ve nüfuz alanının bu kadar artması bazı kararların da değişmesine veyahut yenilenmesine neden olmaktadır. Etik kavramı dijitalleşerek dijital sahada da etiğin üst seviyede tutulması gerekliliğini ortaya koymaktadır. Bu bağlamda devletler, şirketler ve aileler dijital etik ilkelerini dikkate alarak siber güvenlik stratejilerini oluşturarak, bilgi ve bilginin üretimi, korunması, saklanması ve dağıtılmasını amaçlamaktadırlar (Tekke ve Aybala, 2021). Siber güvenlik içerisine etik kavramının yerleştirilmesiyle bireylerin şirketlerin ve devletlerin maruz kaldığı yanlış bilgi veyahut yanlış yönlendirilme gibi durumların engellenmesi için hayati önem taşımaktadır.

Etik kavramının siber alanda sürekli olarak dile getirilmesindeki en büyük etken, sosyal medyada gerçekleştirilen eylemler sonucu ortaya çıkan açık kapıların kalması ve bu açık kapıların sosyal mühendislik faaliyetleriyle işlenerek kötü amaçlı kullanılmasından kaynaklanmaktadır. Sosyal medyaların aktif olarak kullanılması sosyal mühendislik faaliyetlerinin kullanılması için açık kapı bıraktığı gibi bireysel gazetecilik kavramının da ortaya çıkmasına neden olmuştur (Özdemir, 2021). Geleneksel haber kaynakları olan gazete, televizyon ve radyo yayınları, tüzel kişilik adı altında faaliyetlerini gerçekleştirip kanunlar karşısında bir sorumluluğa sahipken sosyal medyada haber yayıncılığı adı altında faaliyet gösteren sayfa ve gruplar, kişisel siyasi görüşleri, önyargılı yaklaşımlar, taklit etme veyahut kaynağı belirli olmayan ve kaynaksız şekilde haber adı altında paylaşımlar gerçekleştirdiği gibi herhangi bir kanuni düzenlemeye tabii olmadığı gibi kanunlar karşısında da herhangi bir sorumluluğa sahip olmamaktadırlar (Özdemir, 2021). Sosyal medyalarda paylaşılan editoryal materyaller, siber alanda kullanıcıları acımasızlaştırmaya ve kutuplaşmaya itmektedir. Bu durumun ana sebebi ise günümüzde çoğu kullanıcı bilgileri elemek ve filtrelemek için sosyal medya aracını kullanmakta fakat sosyal medya ortamında paylaşılan bilgiler ekseriyetle kaynaktan mahrum olmasından kaynaklı kullanıcıları manipüle etmek konusunda büyük başarılar sağlamaktadır (Lin ve Kerr, 2017).

Çeşitli sosyal medyaları habercilik faaliyetleri kapsamında kullanan kişiler, yapılan istatistiksel verilerden faydalanarak sosyal medya uygulamalarının etkileşiminin en fazla olduğu saatleri özellikle tercih etmelerinde asıl amacın habercilik olduğunun sorgulanmasına neden olmaktadır. Öyle ki Facebook uygulaması için etkileşimin en yüksek olduğu saat 15.00 ve gün olarak çarşamba iken Instagram uygulaması için etkileşimin en fazla olduğu saatler sabah 08.00 ve akşam 17.00 ve gün olarak pazartesi ve perşembe günleri etkileşimin fazla olduğu gözlemlenmiştir (Er, 2022). Özellikle Instagram uygulamasının etkileşim saatlerine dikkat edecek olursak işe gidiş ve çıkış saatlerine denk gelmesi sebebiyle kısa süreli etkileşimin olmasına neden olmaktadır. Uygulama kullanıcıları işe gidiş ve çıkış saatlerinde yolculukları kapsamında Instagram üzerinden haber takibi gerçekleştirirken zamanın kısıtlı olmasından kaynaklı olarak haberin kaynağını sorgulamak yerine, haberle etkileşim içerisine girerek gördüğüne inanma potansiyelinde olmaktadır. Bu durum siber manipülasyonun gerçekleşmesi için büyük bir olanak sahası oluşturduğu gibi bilginin güvenirliliğini de tartışma konusu yapmaktadır (Lin ve Kerr, 2017).

Siber alanda paylaşılan yazılı veya görsel haberler gerçekliği yansıtmayabileceği gibi halkın kin ve nefrete sürüklenmesinde, halkın psikolojik olarak etkilenmesine ve kitlesel hareketlerin gerçekleşmesine neden olmaktadır. Bu durumun engellenmesi için öncelikle haber kaynaklarının araştırılması gerektiği gibi paylaşım gerçekleştirilmeden önce detaylı olarak sorgulanması ve araştırılması gerekmektedir. Gerçek dışı paylaşım yapan hesapların hukuki olarak suçlu olduğu gibi paylaşımın kullanıcılar tarafından da sorgusuz şekilde paylaşılması suç unsuru olarak kabul edilmektedir. Ayrıca siber alanda manipülatif hareketlerin ve paylaşımların engellenmesi için güçlü bir denetim mekanizmasının varlığı kaçınılmaz olmak zorundadır.

3.3. Araştırmanın Problemlerinin Değerlendirilmesi ve Analizi

P1. Afrika Birliğinin siber güvenlik politikalarının oluşmasında Çin Halk Cumhuriyeti'nin etkisi ne düzeydedir?

1970'lerde Çin'de başlatılan ekonomik reformlar sayesinde bugün dünyanın en büyük ikinci ekonomisi olarak dünya siyasetinde ve dünya ticaretinde yer almaktadır. 1949'da Mao önderliğinde kurulun Çin, uzun süren iç savaşlar ve siyasi istikrarsızlığın giderilmesi için büyük bir çaba harcamasına rağmen dünyanın en büyük ikinci

ekonomisi olmasının altında nüfusunun olumsuzluğunu iş gücüne çevirerek olumlu şekilde faydalanması ve teknolojik yenilikleri özümseyerek ilerlemesinden kaynaklanmıştır. Sadece dünya ekonomisinde en üst sıralarda olmadığı gibi siber alanda da listelerin üst sıralarındadır. Çin, kendi siber kapasitesini geliştirdiği gibi, dolaylı yönden de diğer devletlere de (Rusya, Kuzey Kore, İran, vd.) çeşitli destekler sağlayarak gelişmesine de destek vermektedir. Verilen bu destek, doğrudan olmakla birlikte dolaylı yönden de gerçekleşmektedir.

Teknolojik gelişmeleri yakından takip eden Çin, gelişen teknolojileri halihazırda var olan sistemlerine entegre etmesiyle birlikte büyük bir teknoloji üssü olma yolunda ilerlediği gibi var olan son teknolojik altyapısını korumak ve elde edilecek bilgilerle de daha da güçlendirmeyi temel hedef olarak belirlemiştir. Bu doğrultuda sistemlerin ve hizmet sektöründe faaliyet gösteren şirketlerinin hem ülke içinde hem de ülkeler arasında korumak adına siber istihbarat faaliyetleri gösterdiği gibi Çin'in ekonomik politikalarının da kuvvetlenmesi adına siber casusluk ve siber saldırılarda gerçekleştirmektedir. Çin, yukarda sayılan faaliyetleri gerçekleştirmek için siber gruplarını kullandığı gibi Çin istihbarat teşkilatını da aktif olarak kullanmaktadır. İnternet ve bilgisayar teknolojilerinin gelişmesiyle diğer devletlerin kritik kurum ve kuruluşlarına siber saldırılar gerçekleştirdiği gibi siber casusluk faaliyetleri de gerçekleştirmektedir. Ayrıca Çin istihbarat teşkilatı, Çin'in ulusal çıkarlarının korunması ve uluslararası ilişkilerde tartışmalı konu olan Tayvan meselesinde aktif olmak adına çeşitli ülkelerle stratejik iş birlikleri gerçekleştirmektedir. Örnek olarak açıklamak gerekirse, Gine Bissau, Gambiya, Senegal ve Nijer'de gerçekleştirdikleri stratejik iş birlikleri sayesinde Tayvan'ın faaliyetlerini izlemektedir (Yetgin, 2021).

Çin, ideolojik olarak Batılı devletlerden farklı olması ve kapalı bir kutu olarak tanımlanması sebebiyle çeşitli ambargolar ile karşı karşıya kalmaktadır. Bu sebepten dolayı Çin, özellikle Ortadoğu ve Afrika ülkeleri ile çeşitli stratejik iş birliği ilişkilerine girmektedir. Geliştirilen stratejik girişimler ekseriyetle, enerji ve teknolojik haberleşme ve altyapıların kurulması üzerine kurulmuştur. Çin'in Afrika'da gerçekleştirdiği stratejik yatırımlar ve krediler, Afrika devletlerini ekonomik olarak rahatlattığı gibi Çin'e bağımlı hale de getirmektedir. Afrika devletlerinin Çin'e bağımlı hale gelmesi ve çok fazla yatırım alanı açmalarının altında da tarihsel süreçte Batı devletlerinin Afrika kıtasında gerçekleştirdikleri faaliyetlere karşı bir tepki netliğinde olmasından kaynaklanmaktadır. Öyle ki Batılı devletler ardı ardına Çin devlet markası Huawei'nin

5G teknolojisinin ülkelerinde hassas bilgi ve belgelerin Çin istihbaratına gönderildiği bahanesiyle yasaklamış olmasına rağmen Afrika devletleri Huawei'nin 5G teknolojisine sahip olmak için çok sıcak yaklaşmışlar ve çeşitli anlaşmalar yapmışlardır. Tarihsel olarak gelen öfke ve bağımsızlık isteği netice olarak Afrikalı devletlerin Çin hegemonyasına girmesine neden olmuştur.

Siber alanın genişlemesi, devletlerin güvenlik problemlerinin ortaya çıkmasına neden olduğu için devletler özelde kendi hukuk sistemlerine uygun olan siber güvenlik politikaları belirlediği gibi uluslararası örgütlerin de kapsayıcı hukuki düzenlemeler yapmalarına izin vermişlerdir. İnternet kullanım oranı ve potansiyelinin fazla olduğu Afrika'da Afrika Birliği de kapsayıcı düzenlemeler gerçekleştirmiştir. Ekseriyetle siber güvenlik alanında gerçekleştirilen hukuki düzenlemeler Batı eksenli ortaya çıkması sebebiyle Afrika Birliği özgün bir çalışma ortaya koymak adına çok çalışmış ve bu çalışma ekseriyetle şirketlerin, kritik telekomünikasyon altyapılarının korunması ve devlet güvenliğinin sağlanması eksenli olması öncelikli olmuştur. Burada Çinli şirketlerin yapmış olduğu yatırımların var olması, Afrikalı ülkelerin siber güvenlik politikaları oluştururken doğrudan ve dolaylı yönden Çin eksenli düşünmelerine neden olmaktadır.

P2. Siber vatandaşlık, ikinci hayat ve siber vatan kavramlarının son dönemde ortaya çıkması yeni bir sistemin oluşturulması için atılan adım mıdır?

Hayatımızın siber odaklı hale gelmesi, bazı teamüllerin ortadan kalkmasına neden olduğundan dolayı yeni kavramların ortaya çıkmasına neden olmuştur. Yeni ortaya çıkan bu kavramların (siber vatandaşlık, siber vatan, siber hayat, siber ordu, vd.) bazıları tanımsal olarak büyük boşlukları da beraberinde barındırmaktadır. Tarihsel süreçte incelediğimizde vatandaşlık, ordu, vatan ve sınır gibi kavramlar fiziki olarak kapasitesi, alanı ve tanımı mevcutken 2000'li yıllardan sonra yaygınlaşan siber alan ile bu kavramlarda siber ön adını alarak tekrardan yenilenmiştir. Tarih sahnesinde uzun bir süre devam ve değişime uğramayan bu kavramlar nasıl oldu da çok kısa bir süre içerisinde değişime uğramıştır?

Hızlı değişimin altında yatan en büyük etken, siber alanın kullanıcılar tarafından hem duygusal hem de kolaylıkları açısından hızla benimsenmesinden kaynaklanmaktadır. Elbette bu kabullenmenin altında özümseme ve benimseme olduğu gibi dünya devletlerinin birbirlerine yönelik uyguladıkları siyasi ve ekonomik

politikaları da etkili olmuştur. Özellikle 11 Eylül saldırısından sonrasında ABD ve Batı medyası tarafından Asya ve Ortadoğu ülkelerinde bulunan Müslüman ülkelere yönelik atfedilen 'terörist' yaftasının yapıştırılması, sosyolojik olarak derin yaraların açılmasına neden olmuştur. Aynı şekilde yine ABD ve Batı medyası üzerinden başlatılan Rusya ve İran karşıtlığı da bu ülke vatandaşlarına bakışların değişmesine neden olmuştur. Bu noktada siber alan bütün kullanıcılara sınırsız bir özgürlük vererek dinsiz, devletsiz ve ideolojisiz bir dünya vatandaşlığı sunmasından dolayı çok hızlı büyümüştür. Ayrıca yine devletlerin vatandaşlarına yönelik uyguladığı sansür ve kısıtlamaların da siber alanda olmaması vatandaşlara büyük bir özgürlük alanının doğmasına neden olmuştur.

Yukarıda bahsettiğimiz nedenlerden dolayı kullanıcılar kalıplarının dışına çıkabilmek için siber alanı kullanmışlar ve bu durum yeni bir hayatın inşa edilmesi fikrinin ortaya çıkmasına neden olmuştur. 1990'lı yıllarda ütopik bir kavram olarak ortaya çıkan ikinci hayat/ meta evren veyahut popüler ismi ile metaverse, dinsiz, mezhepsiz, ideolojisiz ve devletsiz bir evrenin kurulmasına olanak sağlaması, kullanıcıların hepsinin eşit kabul edilmesiyle yeni bir vatandaşlık türünün doğmasına ve yeni bir devlet formunun ortaya çıkmasına neden olmuştur.

Toplumsal bir iç isyan ile başlayan bu süreç bugün engellenemez ve takip edilemez bir noktaya gelmiş ve hızla da gelişmektedir. Günümüzdeki teknolojik imkanlar giyilebilir teknolojik ürünlerini ortaya çıkarmış ve bu araçlar sayesinde yeni metaverse evrenleri kurulmaya başlamıştır. İlerleyen süreçlerde mevcut teknolojilerin gelişmesi ve yeni teknolojik olanakların ortaya çıkması ile bu süreç daha geniş bir tabana yayılması kuvvetle muhtemeldir.

P3. Terör, sosyoloji, kültürel ve siyasal kavramların siber alana entegre edilmesiyle ortaya çıkan güvenlik zafiyetlerinin uzunca bir süre devletlerin nezdinde kabul edilmemesindeki ana etken?

İnsanlığın varoluşundan itibaren insanlığın bir parçası olan kültürel etkileşim, siyasal etkileşim, terör ve terörizm kavramları, zamanın şartlarına ve gerekliliklerine uygun şekilde dönüşmüş ve yeniden şekil almıştır. Zaman içerisinde yaşanan teknolojik gelişmeler, toplumsal yapının değişmesine, sosyolojik açıdan köklü değişikliklere, siyasal söylemlerin değişmesine ve terör ve terörizm kavramlarının yeniden anlamlandırılmasına neden olmuştur. Sanayi devrimleriyle başlayan teknolojik gelişmeler toplumlara pozitif katkılar sağlayarak ilerlemiş ve günümüze kadar gelmiştir.

Yukarıda bahsettiğimiz kavramlar temelde toplum ile bağlantılı olup toplumların teknolojiyi ne kadar özümsemesi ile doğrudan bağlantılıdır. Bu sebepten dolayı teknolojik gelişmeler, toplumların içerisine ne kadar yerleşirse ortaya çıkan pozitif ve negatif sonuçlarda o kadar fazla olmuştur.

Soğuk Savaş sonrasında başlayan uzay yarışı, siber alanın oluşmasına ve bugün kullandığımız internetin doğmasına neden olmuştur. 1990'larda www'in toplumlar arasında yaygınlaşma başlaması yeni kültürel devrimlerin başlamasına neden olduğu gibi yeni tehditlerin de hızla büyümesine neden olmuştur. Toplumlar ekseriyetle teknolojik gelişmeleri öncelikle pozitif yönleriyle ele aldıklarından dolayı negatif yönleri her zaman arka plana atılmıştır. Örnek ile açıklamak gerekirse siber güvenlik kavramının popülaritesi 1990'larda başlamış olsa da toplumlar siber güvenliğin önemini 2000'li yıllardan sonra fark etmiş ve bilinçlenmeye başlamıştır. Fakat buradaki bilinçlenme uzun bir süre boyunca kişisel verilerin güvenliğinin sağlanması adına gerçekleşmiştir.

Siber güvenlik kavramı çok geniş bir literatürü bünyesinde barındırması ve bilgisayar ve internet teknolojilerinin sürekli olarak kapasitesini katlayarak devam etmesi nedeniyle yeni güvenlik açıklarının keşfedilmesine ve bazı açıkların hala bulunamamasına neden olmaktadır. Örnek olarak terör kavramını ele alacak olursak, toplumları ve devletleri fiziki olarak etkileyen terör, 11 Eylül saldırısı ile farklı bir boyut kazanmıştır. Saldırı sonrasında yapılan araştırmalar, teröristlerin uydu telefonlarını kullanarak gizlice haberleştiklerini ve bu şekilde koordine olduklarını göstererek terör kavramının da siberleşmesine neden olmuştur. Dünyada açık ve net bir örneğin olması sebebiyle devletler siber terör faaliyetlerinin engellenmesi için çeşitli girişimler yapmış olsa da yeteri kadar etkin olamamışlardır. Devletlerin, ortak veyahut bireysel olarak aldıkların yeteri kadar etkili olmamasının altında iki ana etken yatmaktadır. Birincisi, siber alanın kapasitesinin belirlenememesi ve durağan olmayan bir şekilde büyümesinden kaynaklı olarak alınan ortak veyahut bireysel kararların etkisi yetersiz kalmaktadır. İkinci etken ise siber alanın yeteri kadar önemsenmemesi ve siber alanın farklı şekillerde yorumlanmasından kaynaklıdır.

Siber alanın farklı yorumlanması temelde devletlerin çıkarları ve stratejilerine uygun davranmasından kaynaklıdır. Örnek olarak açıklamamız gerekirse Fransa'ya göre siber alanda gerçekleştirilen faaliyetleri ulusal çıkarları gereği uygun olurken

Brezilya'ya göre siber alanın denetlenmesi ve siber alanda gerçekleştirilen faaliyetlerin dünya barışının sağlanması adına elzem bir konu olarak görmektedir. Devletlerin bu politikaları, toplumlarında siber alana olan yaklaşımlarını da etkilemektedir. 2005 sonrası artan sosyal medya uygulamaları katlanarak devam etmesi, siber alanın kapasitesinin gelişmesine neden olduğu gibi devletlerin sosyal medya aracılığı ile istihbarat ve casusluk faaliyetlerini maliyetsiz ve risksiz olarak gerçekleştirmesine olanak sağladığı gibi devletlerin yine kendi politikalarını vatandaşlarına kabul ettirmek için sosyal medyaları kendi lehlerine yönelik kullanmalarına neden olmuştur.

Sonuç olarak internet kullanıcıları, siber alanın tehlikelerinden çok toplumların kolaylıklarına ve sosyalleşmelerine odaklanmaları sebebiyle siber alanda ciddi güvenlik açıklarının oluşmasına neden olmuşlardır. Oluşan bu açıkların giderilmesi için ise devletler, diğer politikalarına öncelik vermelerinden kaynaklı olarak siber güvenliğin ulus güvenliğinin bir parçası olmasını tam anlamamakla birlikte, uzun yıllar sadece kişisel verilerin korunması ve siber suçlara ilişkin düzenlemeler gerçekleştirerek siber güvenliğin sağlandığını vatandaşlarına kabul ettirmiştir. Fakat siber güvenliğin sağlanması sadece ceza kararlarının alınmasıyla değil, teknik altyapının güçlendirilmesi, milli güvenlik duvarlarının inşa edilmesi, nitelikli elemanların yetiştirilmesi, toplumsal siber güvenlik bilincinin yaygınlaştırılması, ağır cezai yaptırımların uygulanması ve uluslararası örgütlerde iş birliklerinin gerçekleştirilmesi ile sağlanabilmektedir.

P4. Kripto paraların ortaya çıkması devletlerin siber güvenlik politikalarını nasıl etkiledi?

2008'de Satoshi Namakoto isimli anonim bir kişi veyahut bir grubun yayınladığı makale ile başlayan kripto para serüveni büyük bir taleple karşılaşmasıyla birlikte çeşitli alt coinlerin ortaya çıkmasına ve küresel çapta ciddi miktarda bir para sirkülasyonunun oluşmasına neden olmuştur. Kripto paraların ortaya çıkmasındaki etkenlere bakacak olursak karşılıklı güven yerine teknolojik çağa uygun ve daha güvenli olan kriptografyanın olması, merkezi ve aidiyeti olmayan ve üçüncü tarafların olmadığı bir sistem oluşturulmak istenmesiyle ortaya çıkmış ve hatta teknolojik çağın zaruri bir sonucu olarak yorumlanabilir. 2009'da Bitcoin ile başlayan süreç 2022 yılında tarihin en büyük seviyesi olan 69 bin dolar seviyelerine ulaşması kripto paralara olan yatırımların çok fazla artmasına neden olduğu gibi beraberinde büyük problemlerin ortaya çıkmasına da neden olmuştur.

Ortaya çıkan problemler içerisinde en önemlisi devletlerin güvenliklerini tehdit ettiği gibi devletlerin merkez bankalarını da tedirgin etmiştir. Bu tedirginliğin oluşmasında devletler düzeyinde terörün finanse edilmesi ve kayıt dışı paranın denetimsiz olarak dolaşımda olması olarak görülürken merkez bankaları nezdinde ise basılı olmayan kayıt dışı paraların ülke içerisinde dolaşımda olması ve ulusal para politikalarının istikrarsız bir yapıya sürükleme endişesi oluşmasına neden olmuştur. Oluşan endişe ve tedirginliği biraz anlatmak gerekirse, terör örgütleri arasında gerçekleşen ödeme ve para göndermelerin teknik takibe takılmaması ve gizlilik konusunun ön planda olmasından kaynaklı aktif olarak kullanması, devletleri ve uluslararası barışı da doğrudan etkilemektedir. Terör örgütlerinin finansman edilmesinde aktif olarak kullanılan kripto paralar siber terörün de teşvik edilmesinden dolayı siber güvenliğin bileşenleri içerisinde değerlendirilmektedir.

Bitcoin ’in ortaya çıkmasıyla başlayan kripto paralara olan ilgi, istikrarlı bir şekilde artmış ve dünya ekonomisini derinden etkileyen Covid-19 pandemisiyle birlikte bir kazanç olarak görülmeye başlanmasıyla birlikte popülaritesi artmıştır. Artan popülarite ile yeni iş kollarının kurulmasına olanak sağladığı gibi yeni sektörlerin de ortaya çıkmasına neden olmuştur. Fakat ortaya çıkan yeni yapıları denetleyecek bir yapının olmaması ve çok sayıda olması, büyük bir ekonomik tehlikenin ortaya çıkmasına neden olmuştur. Bu durumun önüne geçmek adına devletler kripto paralara ve kripto borsalara yönelik tutumları katı ve yasaklayıcı olmuştur. Her ne kadar devletlerin tutumları katı olsa da kripto para piyasasına çok büyük etkileri olmamıştır.

P5. Devletlere yönelik gerçekleştirilen siber saldırılar da fiziki saldırılar gibi değerlendirilmeli midir?

Bilişim teknolojilerinin gelişmesiyle birlikte başlayan sanallaşma devletlerin de sanallaşmasına neden olduğu gibi saldırıların da sanallaşmasına neden olmuştur. Yaşanan sanallaşma siber alanın kapasitesinin gelişmesine neden olmuştur. Siber alanın kapasitesinin gelişmesi, beraberinde bir dizi cevapsız soruları da getirmiştir. Bu sorulardan en önemlisi, siber kapasitenin nelere olanak sağladığı ve bu olanakların kullanımıyla birlikte hedef şirket veyahut devletlere ne gibi etkileri olacağı soruları olmuştur. Siber alanın aktif kullanılmasıyla birlikte başlayan siber saldırı araçları zaman içerisinde çeşitlilik kazanmış ve bu çeşitliliğin artması beraberinde saldırılarında büyümesine neden olmuştur.

Bilgi ve iletişim teknolojilerinin gelişmesi, devletlerin siber alanda aktif olmalarına ve değişim içerisine girmelerine neden olmuştur. Devletlerin siber alana girmesiyle birlikte, devletlere yönelik siber saldırılar, siber istihbarat ve siber casusluk faaliyetleri de hız kazanarak artmıştır. Peki devletler neden klasik saldırı tiplerinden ve istihbarat faaliyetlerinden vazgeçerek siber alanda faaliyet göstermeye başlamışlardır? Bu sorunun cevabı oldukça basit şekilde zaman ve maliyet kazanımı olarak açıklanabilir. Devletler fiziki saldırıları zorunda kalmadıkça tercih etmemektedirler. Bunun nedeni ise oluşacak olan fiziki saldırılar neticesinde ekonomik ve sosyal dengenin bozulması ve siyasal desteğin kaybolması olarak açıklanabilir. Ekonomik ve siyasal kaygılardan hariç olarak fiziki saldırılarda insan gücünün de aktif olarak kullanılması savaş hukukunun da ihlal edilmesine neden olabilmektedir. Bu durumlardan dolayı devletler kısa vadede etkili sonuçlar alabilmek adına siber saldırıları ve siber savaşları kullanmaktadır. Bu durumu en iyi özetleyen örnek ise 2010 yılında İran'a yönelik gerçekleştirilen Stuxnet saldırısı gösterilebilir.

Stuxnet saldırısı İran'ın nükleer programını engellemek için gerçekleştirilen bir saldırı olmakla birlikte, İran'ın Ortadoğu'daki etkinlik ve nüfuzun da kırılması için gerçekleştirilmiş bir saldırıdır. Sonuç olarak hangi ülke tarafından tasarlandığı belli olmayan virüs, İran'ın nükleer reaktörlerinden bir kısmı zarar görmüş ve bazıları kullanılamaz hale gelmiştir. Buradaki önemli husus ise kim tarafından tasarlandığı belli olmayan bir kod İran'ın nükleer çalışmalarını sekteye uğramıştır. Yine aynı şekilde 2007'de NATO üyesi olan Estonya'ya yönelik gerçekleştirilen DoS/DDoS ataklarıyla yaklaşık 1 aylık büyük bir saldırıya uğrayarak devlet işleyişi kullanılamaz duruma gelmiştir.

Yukarıda verilen örnekler ışığında fiziki saldırılar gibi siber saldırılar ve siber savaşlar devletler ve devlet destekli gruplar tarafından aktif olarak kullanılmaktadır. Devletler siber saldırıları tercih etmelerinde ekonomik olması, kimlik bilgilerinin gizli ve saldırı kaynaklarının takip edilmesinin zor olması, insan faktörünün güvende olması sebebiyle aktif tercih etmektedirler. Aktif olarak siber saldırıları kullanmaları devletlerin bu konuda siber saldırıları fiziki saldırılar gibi değerlendirilip değerlendirilemeyeceği tartışmalarının yaşanmasına neden olmaktadır. Günümüz şartlarında bu tartışmalar sıkça yaşanacağı gibi net ve somut bir adım atılamayacağı kuvvetle muhtemeldir. Çünkü bir devlet diğer devleti siber saldırı ile suçlarken somut delillerin olmaması sebebiyle ithamlar havada kalmaktadır.

SONUÇ VE DEĞERLENDİRME

İnsanlık tarihiyle paralel şekilde ilerleyen güvenlik kavramı, zaman içerisinde ontolojik ve epistemolojik olarak büyük değişimler gerçekleştirerek, günümüzdeki formunu kazanmasına neden olmuştur. 1990'lı yıllarla birlikte hayatımıza giren siber kavramının klasik güvenlik anlayışının anlamsal ve kavramsal olarak değiştirttiği gibi dijital güvenlik kavramının da şekillenmesine ön ayak olmuştur. Siber alanın 1990'lı yıllarla hayatımızın her alanında yer alması, bireylerin, şirketlerin ve devletlerin sanallaşmasına olanak sağladığı gibi beraberinde yeni güvenlik açıklarının oluşmasına neden olmuştur. Siber alanın yaygınlaşmasıyla birlikte başlayan yeni güvenlik açıklarını sadece siber kavramına yüklememek gerekmektedir. Siber alanın oluşmasında temel faktörün insan olması, güvenlik açıklarının ortaya çıkmasına neden olmuştur.

İnsan faktörü yeni güvenlik paradigmasının oluşmasında olumlu etkileri olduğu gibi olumsuz yönlerinin de ortaya çıkmasında neden olmuştur. Bu nedenlere bakmak gerekirse eğer insan faktörünün eğitim ve teknoloji birikimi doğrudan etkili olduğunu görebiliriz. Temelde insanın teknolojik bilgi birikimine ve yeterli eğitime sahip olması, siber alanın güvenliğinin sağlanmasında büyük rol oynamaktadır. Fakat bahsettiğimiz bu parametreler de tek başına siber güvenliğin sağlanması konusunda yetersiz kalmaktadır. Siber alanın yeni teknolojik gelişmelerle entegre halde olması ve tabana yayılması, siber alanın kapasitesinin gelişmesine neden olmuştur. Oluşan bu kapasite genişlemesi kontrol edilemez gizemli bir alanın ortaya çıkmasına neden olmuştur.

Temelde siber alanın ortaya çıkması, yeni bir güvenlik açığının (uzay savaşlarının) kapatılması için oluşmuş olsa da kontrol edilemez şekilde büyümesi siber alanın önemini ortaya koymuştur. Günümüzde siber alanda gerçekleştirilen bireysel yazışmalar, bankacılık işlemleri, resmi görüşmeler ve evraklar, devlet yazışmaları, istihbarat ve casusluk faaliyetleri yeni risklerin ve güvenlik açıklarının ortaya çıkmasına neden olmuştur. Oluşan bu güvenlik açıkları ilk zamanlar kişisel bilgisayarlara yetkisiz erişim sağlanmasıyla başlamış daha sonrasında kişisel verilerin güvenliğinin sağlanamamasına evrilmiştir. Günümüzde ise teknolojik gelişmeler ve bilgisayar teknolojilerinin gelişmesiyle birlikte kötü amaçlı yazılan yazılımların ağlar üzerinden yayılması, hacker gruplarının gerçekleştirdiği saldırılar, şirketlerin ticari sırlarının deşifre edilmesi için gerçekleştirilen saldırılar, siber saldırılar ve siber savaşların ortaya çıkmasına neden olmuştur.

Gerçekleştirilen siber saldırıların etkilerinin büyük ve etkili olması, devletlerin ilgisini çekmiş ve siber savaşların ortaya çıkmasına neden olmuştur. Devletlerin siber savaşları tercih etmelerindeki nedenler ise anonimlik ve ekonomik olarak uygun maliyetli olmalarından kaynaklanmaktadır. Devletler klasik savaş unsurlarını kullanmak yerine siber savaş araçlarını kullanarak anonimlik sağladığı gibi uluslararası sisteme dahil olan diğer devletlerle kötü duruma düşmedikleri için ve klasik savaş unsurlarından çok daha ucuz ve insani kaybın olmaması sebebiyle siber savaşları benimsemişlerdir. Fakat siber savaşların devletlerce özümsenmesi beraberinde hukuki olarak eksikliklerin ortaya çıkmasına neden olmuştur. Günümüzde devletlere yönelik gerçekleştirilen siber saldırılan artması uluslararası arenada hukuki metinlerce denetlenmesi ve engellenmesi hedeflenmiştir fakat bu durum siber alanın anarşik bir yapıya sahip olmasından dolayı mümkün olmamaktadır.

Siber uzayda gerçekleştirilen faaliyetlerin denetlenmesi için devletler kendi hukuki metinlerinin oluşturulmasında büyük adımlar atmış olsalar da uluslararası bir bütünlük sağlayamamışlarıdır. Devletlerin siber alanı kendi çıkarları gereği kullanmalarından dolayı uluslararası bir bütünlük sağlamaları günümüz şartlarında pek mümkün görünmemektedir. Bu çıkarımın yapılmasında özellikle Birleşmiş Milletler 'in, Avrupa Birliği'nin ve diğer uluslararası örgütlerin aldıkları kararlar etkili olmaktadır. Tüm ülkelerce kabul edilen bir uluslararası metnin ortaya konması için öncelikli olarak ideolojik, jeopolitik, siyasi, sosyal ve dini olarak ayrımın ortadan kalması ve tek bir dünya vatandaşlığının ortaya konması gerekmektedir. Fakat kutuplaşmanın yoğun olduğu bir dünya sisteminde bu durumun gerçekleşmesi fantastik bir durum olarak görünmektedir.

Siber saldırılar ve siber savaşlar devletler tarafından gerçekleştirildiği gibi bir takım hacker grupları tarafından da gerçekleştirilmektedir. Devletlerden bağımsız hareket eden bu grupların saldırılarının engellenmesi ise yine devletlerin ortak hareket ederek hacker ordularının hareket alanlarının daraltılmasıyla olacağı gibi toplumun siber alanı kavraması ve bilgilendirilmesiyle de engellenebilmektedir. Toplumsal siber bilincin oluşturulması, siber ortamda gerçekleştirilen saldırıların azalmasına neden olacağı gibi sosyal mühendislik faaliyetlerinin azalmasına ve adi suçların engellenmesine de olanak sağlayacaktır. Toplumsal bilincin oluşması devletlerin siber alanda gerçekleştirdiği faaliyetlerin denetlenmesi için bir baskı unsuru olacağı gibi yeni

gelişen teknolojik gelişmelerde bilinçli şekilde yaklaşmamıza ve doğacak sorunların minimum seviyede kalmasına olanak sağlayacaktır.

Çalışmamızda toplumsal bilince yapılan vurgunun sürdürülmesinin temel nedeni, insan faktörünün teknolojik gelişmelere duyarsız kalması ve hazırlıksız yakalanmasındandır. Siber alandaki gelişmelere duyarsızlık yeni adi suçların ortaya çıkmasına ve siber manipülasyonun artmasına neden olmaktadır. Siber manipülasyonun içerisinde ise en aktif kullanılan yöntem telefon dolandırıcılığı yöntemidir. Dolandırıcılar, sosyal mühendislik faaliyetleri sonucunda hedefledikleri kişilerin, kişisel bilgilerini kullanarak sanal olarak manipüle ederek çeşitli haksız kazançlar elde etmektedir. Dolandırıcılar hedefledikleri kişilerden haksız kazanç elde ettikleri gibi hedef kişinin kişisel verilerini banka bilgilerini, pasaport bilgilerini, sosyal güvenlik numaralarını ve şifrelerini ele geçirerek siber alanda satma girişiminde de bulundukları gibi (Bayzıt, 2022) Tekkanat ve arkadaşlarının telefon dolandırıcılığının etkileri üzerine yapmış olduğu çalışma sonucunda kişisel verilerin internet ortamında saklanması ve saklanan bu verilerin güvenliğinin sağlanması konusunda büyük bir zafiyet doğurduğunu ortaya koymuştur (Tekkanat, vd., 2018).

Devletler ciddi şekilde telefon dolandırıcılığı ve bilişim suçlarının engellenmesi adına güçlü adımlar atmaktadırlar. Örnekle açıklamak gerekirse ABD, 2003-2018 yılları arasında 50 yasa ortaya çıkarmış ve dönemin şartlarına göre revize edilerek, kişisel verilerin izinsiz ele geçirilmesi ve saldırı şeklinde kullanılması durumunda kanunda nitelikli hal olarak belirterek isnad edilen suça ek olarak 2 yıl hapis cezası eklenmesi kararlaştırılmıştır (Bayzıt, 2022). Fransız hukuk sisteminde kimlik sahteciliği dolandırıcılık 2 yıl hapis ve 30 bin Euro para cezası, Alman hukuk sisteminde ise hükümler 2 bende ayrılmış olup bireysel işlenen bir suç olması durumunda 2 yıla kadar hapis cezası veyahut para cezası olduğu gibi çete olarak işlenen suç sayılması durumunda ise 3 aydan 5 yıla kadar hapis cezası öngörülmüştür (Bayzıt, 2022).

Türk hukuk sisteminde ise dolandırıcılık suçu bakımından TCK m. 158'e göre eylem bilişim sistemlerinin, banka veya kredi kurumlarını araç olarak kullanılmasıyla gerçekleşen durumlarda 3 yıldan 10 yıla kadar hapis cezası ve 5 bin güne kadar adli para cezası ile cezalandırılır, banka veya diğer kredi kurumlarınca tahsis edilmemesi gereken bir kredinin açılmasını sağlamak maksadıyla gerçekleşen

eylemlerde alt sınır olarak 4 yıl ve suç ile elde edilen paranın 2 katından az olmamak kaydıyla adli para cezasına hükmedilmiştir (Resmi Gazete, 2004).

Toplumsal bilincin gelişmesi, siber güvenliğin tamamen sağlanacağı anlamına gelmemelidir. Siber güvenliğin sağlanması için bireyin bilinçlenmesi gerektiği gibi devletlerinde siber güvenliğin sağlanması ve vatandaşlarının korunması için siber güvenlik politikaları belirlenmesi ve hukuki düzenlemelerin yapılması gerekmektedir. Devletler, siber güvenliğin sağlanması için siber alanı denetlemek ve vatandaşlarını korumak için hukuki altyapılar oluşturduğu gibi uluslararası düzeyde de hukuki altyapının oluşturulması çalışmalar gerçekleştirmektedirler.

KAYNAKÇA

Çelik, S. (2018). Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşim. *Academic Review of Humanities and Social Sciences, 1(2),* s. 110-119.

Çifci, H. (2017). *Her Yönüyle Siber Savaş, Ankara: Tübitak Popüler Bilim Kitapları.*

Çubukçu, A., & Bayzan, Ş. (2013, 5). Türkiye'de Dijital Vatandaşlık Algısı ve Bu Algıyı İnternetin Bilinçli, Güvenli ve Etkin Kullanımı ile Artırma Yöntemleri. *Middle Eastern & African Journal of Educational Research,* s. 148-174.

Özcan, N. (2021). Dijital Etik Üzerine Nitel Bir Araştırma. *Gençlik Araştırmaları Dergisi, 9(25),,* s. 89-105.

Özdemir, H. (2021). *Dijital Mahremiyet (2.Baskı).* İstanbul: İnsan ve Hayat Kitaplığı.

Abdurahmanlı, E. (2021, 8 3). Siber İstihbarat Kapsamında: Echelon İstihbarat Sistemi. *Akademik Tarih ve Düşünce Dergisi*, s. 1212-1234.

Abuzaid, A. M., Saudi, M. M., Taib, B. M., & Abdullah, Z. H. (2013). An efficient trojan horse classification (ETC). *International Journal of Computer Science Issues,* s. 96-104.

Acar, H. (2020). *Rusya'nın Siber Güvenlik Politikası.* Ankara: Nobel Akademik Yayıncılık.

Agazzi, A. E. (2020). Phishing and Spear Phishing: Examples in Cyber Espionage and Techniques to Protect Against Them. *arXiv preprint arXiv:2006.00577.*

Aidan, J. S., Verma, H. K., & Awasthi, L. K. (2017). Comprehensive Survey on Petya Ransomware Attack. *In 2017 International Conference on Next Generation Compiting and İnformation System*, s. 122-125.

Akgül Açıkmeşe, S. (2011). Algı mı, Söylem mi? Kopenhag Okulu ve Yeni Klasik Gerçekçilikte Güvenlik Tehditleri. *Uluslararası İlişkiler Dergisi, 8 (30),* s. 43-73.

Akiner, S. (2010). The Shanghai Cooperation Organisation: A Networking Organisation For a Networking World. *Global Strategy Forum,* s. 5-26.

Akmeşe, S. (2020). Kamuda Dijital Dönüşümün Siber Güvenlik ve Dijital Güvence Boyutları ve İç Denetimin Rolü. *Denetişim, (20),* s. 108-119.

Akyeşilmen, N. (2018). *Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik. Ankara: Orion Kitapevi.* Ankara: Orion Kitapevi.

Alaca, A. (2020). Singapur'un Siber Güvenlik Politikası. *Yeni Küresel Tehdit Siber Saldırılar Siber Güvenlik ve Politika Uygulamaları* (s. 283-298). içinde Ankara: Nobel Akademik Yayıncılık.

Althonayan, A., & Andronache, A. (2018). Shifting from information security towards a cybersecurity paradigm. *In Proceedings of the 2018 10th International Conference on Information Management and Engineering*, (s. 68-79).

Applegate, S. (2009). Social Engineering: Hacking the Wetware! *Information Security Journal: A Global Perspective, 18(1)*, s. 40-46.

APWG. (2022). *Phishing Activity Trends Report.* APWG Report: https://docs.apwg.org/reports/apwg_trends_report_q1_2022.pdf?_ga=2.255909067.1355406380.1663004628-1163617556.1663004628&_gl=1*42uqar*_ga*MTE2MzYxNzU1Ni4xNjYzMDA0NjI4*_ga_55RF0RHXSR*MTY2MzAwNDYyNy4xLjEuMTY2MzAwNDYzNy4wLjAuMA.., adresinden alındı

Arends, J. (2009). Homeros' dan Hobbes ve Ötesine:" Güvenlik" Kavramının Avrupa Geleneğindeki Boyutları. *Uluslararası İlişkiler Dergisi,6 (22)*, s. 3-33.

Arquilla, J. (2013). Twenty Years of Cyberwar. *Journal of Military Ethics, 12:1*, s. 80-87.

Aslan, M. Y. (2008). Savaş Hukukunun Temel Prensipleri. *TBB Dergisi, 79*, s. 235-274.

Ataç, K. K. (2019). Soğuk Savaş. *Güvenlik Yazıları, No 35*, s. 1-9.

Atalay, G. E. (2018). Dijital Çağda Marshall McLuhan'ı Yeniden Düşünmek: Bir Uzantı ve Ampütasyon Olarak Yeni Medya Teknolojileri. *Sosyal Araştırmalar ve Davranış Bilimleri Dergisi, 4(6)*, s. 27-48.

Aydın, E. (2022). Mavi Vatan, Gök Vatan ile Siber Vatan Söz Öbeklerinin Anlamları ve Oluşturulma Yöntemleri. *The Journal of Turkic Language and Literature Surveys (TULLIS), 7(3)*, s. 167-178.

Aydındağ, D. (2021). Copenhagen school and securitization of cyberspace in Turkey. *Propósitos y Representaciones, 9(1).*

Ağkaya, O. (2016). İngiliz Okulu ve Uluslararası Toplum Düşüncesi. *Ankara Üniversitesi SBF Dergisi, 71(4)*, s. 1059-1089.

Bıçakçı, S., Ergun, D., & Çelikpala, M. (2015). Türkiye'de Siber Güvenlik. *Ekonomi ve Dış Politika Araştırma Merkezi (EDAM) Siber Politika Kağıtları Serisi, 1*, s. 1-35.

Baştuğ, M. (2022). *Siber Güvenlik Açısından Asya Bölgesinin Güvenlik ve Çatışma Analizi.* Ankara: Detay Yayıncılık.

Baştuğ, M. (2022). *Siber Güvenlik Açısından Asya Bölgesinin Güvenlik ve Çatışma Analizi.* Ankara: Detay Yayıncılık.

Bakanlığı, U. D. (2016). *Ulusal Siber Güvenlik Stratejisi.* Ulaştırma ve Altyapı Bakanlığı: https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf adresinden alındı

Balcı, A., & Kardaş, T. (2014). *Realizm, Uluslararası İlişkilere Giriş.* İstanbul: Küre Yayınları.

Banks, W. C. (2017, 66). CYBER ESPIONAGE AND ELECTRONIC SURVEILLANCE: BEYOND THE MEDIA COVERAGE . *Beyond the media coverage*, s. 513-525.

Baran, T., & Macar, E. (2017). Değişen Güvelik Yaklaşımları Örneğinde Kopenhag Okulu'nun Toplumsal Güvenlik Yaklaşımı. *Uluslararası Sosyal Araştırmalar Dergisi, 10 (54)*, s. 251-258.

Barkuş, F., & Koç, M. (2019). Dijital Mahremiyet Kavramı ve İlgili Çalışmalar Üzerine Bir Derleme. *Bilim, Eğitim, Sanat ve Teknoloji Dergisi (BEST Dergi), 3(1)*, s. 35-44.

Bayar, F. (2008, 34 2). Küreselleşme Kavramı ve Küreselleşme Sürecinde Türkiye. *Uluslararası Ekonomik Sorunlar Dergisi*, s. 25-34.

Bayraktar, G. (2014). Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber istihbarat. *Güvenlik Stratejileri Dergisi, 10(20)*, s. 119-143.

Bayzıt, T. (2022). KİMLİK HIRSIZLIĞININ TÜRK CEZA HUKUKU VE KARŞILAŞTIRMALI HUKUK BAKIMINDAN DEĞERLENDİRİLMESİ. *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi,, 19*(2), s. 635-658.

Bağcı, C. (2021). *Dijital Milli Güvenlik Politikaları.* İstanbul: Motto Yayınları.

BBC News. (2021). *Fidye Yazılımlar: 2020'de 170 Milyar Dolar Hasara Neden Olan Yazılımlara Karşı Eylem Çağrısı*. BBC News Türkçe: https://www.bbc.com/turkce/haberler-dunya-56942123#:~:text=Siber%20güvenlik%20şirketi%20Emsisoft'un,170%20milyar%20dolar%20arasında%20oldu adresinden alındı

BBC News. (2022, 09 07). *Arnavutluk, 'siber saldırı' ile suçladığı İran'la diplomatik ilişkileri kesti*. BBC News: https://www.bbc.com/turkce/articles/cyjv82810xko adresinden alındı

Berghel, H. (2018). Malice Domestic: The Cambridge Analytica Dystopia. *Computer, 51(5)*, s. 84-89.

Beutelspacher, A. (2021). *Gizli Diller ve Kodlar*. İstanbul : Runik Kitap.

Bilgiç, A. (2011). Güvenlik İkilemi" ni Yeniden Düşünmek: Güvenlik Çalışmalarında Yeni Bir Perspektif. , 123-142. *Uluslararası İlişkiler Dergisi, 8(29)*, s. 123-142.

Bilgin, P. (2010). Güvenlik Çalışmalarında Yeni Açılımlar: Yeni Güvenlik Çalışmaları. *SAREM Stratejik Araştırmalar Dergisi, 8(14)*, s. 69-96.

Birleşmiş Milletler Anlaşması. (1945). https://inhak.adalet.gov.tr/Resimler/SayfaDokuman/2212020141836bm_01.pdf : https://inhak.adalet.gov.tr/Resimler/SayfaDokuman/2212020141836bm_01.pdf adresinden alındı

Boggs, C., & Pollard, T. (2006). Hollywood And The Spectacle Of Terrorism. *New Political Science, 28(3)*, s. 335-351.

Brooks, R. R., Yu, L., Ozçelik, I., Oakley, J., & Tusing, N. (2021). Distributed Denial of Service (DDoS): A History. *IEEE Annals of the History of Computing, 44(2)*, s. 44-54.

BTK. (2019). *Türkiye'de Bilişim Hukuku*. https://internet.btk.gov.tr/turkiye-de-bilisim-hukuku: https://internet.btk.gov.tr/turkiye-de-bilisim-hukuku adresinden alındı

Buchanan, B., & Sulmeyer, M. (2016). Russia and cyber operations: Challenges and Opportunities For The Next US Administration. *Carnegie Endowment for International Peace, 3*, s. 1-5.

Cairns, P., Thimbleby, H., & Anderson, S. (1998). A Framework for Modelling Trojans and Computer Virus Infection. *The Computer Journal, 41(7)*, s. 444-458.

Cankurt, A. H. (2023, 04 20). *İngiliz Hükümeti, WhatsApp ve Signal'in uçtan uca şifreleme özelliğini kaldırmasını istiyor*. Egirisim: https://egirisim.com/2023/04/20/ingiliz-hukumeti-whatsapp-ve-signalin-uctan-uca-sifreleme-ozelligini-kaldirmasini-istiyor/ adresinden alındı

Cavelty, M. D. (2010). Cyber-Security. In The Routledge Handbook of New Security Studies. *Routledge*, s. 166-174.

Chakravorti, B., & Chatuverdi, R. S. (2017). *Digital Planet 2017: How Competitiveness and Trust in Digital Economies Vary Across the World. Medford.* Massachusetts: The Fletcher School, Tufts University.

Cho, H. S., & Woo, T. H. (2017). Cyber Security in Nuclear Industry–Analytic Study From the Terror Incident in Nuclear Power Plants (NPPs). *Annals of Nuclear Energy, 99*, s. 47-53.

Cohen, F. (1986). *Computer Viruses.* California: University of Southern California, Published PhD Thesis.

Couzigou, I. (2018). Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations. *International Review of Law Computers & Technology, 32(1)*, s. 37-57.

Craig, A. J., & Valeriano, B. (2018). Realism and Cyber Conflict: Security in The Digital Age. *Realism in Practice, 85*.

Craig, A. N., Shackelford, S. J., & Hiller , J. S. (2015). Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis. *American Business Law Journal, 52(4)*, s. 721-787.

Darıcılı, A. B. (2017). *Siber Uzay ve Siber Güvenlik ABD ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi* . Bursa: Dora Yayıncılık.

Darıcılı, A. B. (2020). Estonya'nın Siber Güvenlik Politikası. *Yeni Küresel Tehdit Siber Saldırılar Siber Güvenlik ve Politika Uygulamaları* (s. 189-203). içinde Ankara: Nobel Akademik Yayıncılık.

Darıcılı, A. B., & Özdal, B. (2017). Enformasyon Savaşı Bağlamında Rusya Federasyonu-Türkiye İlişkilerinin Analizi. *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi, 4(1)*, s. 19-40.

Denning, P. J. (1988). *Computer Viruses.* RIACS Teknik Raporu (No. NASA-CR-184680).

Devlen, B., & Özdamar, Ö. (2010). Uluslararası İlişkilerde İngiliz Okulu Kuramı: Kökenleri. *Uluslararası İlişkiler Dergisi, 7(25)*, s. 43-68.

Dilipraj, E. (2013). India's Cyber Security 2013: A Review. *CAPS Issue Brief, 97 (14)*, s. 1-4.

Dipert, R. R. (2010). The Ethics of Cyberwarfare. *Journal of Military Ethics, 9(4)*, s. 384-410.

Duman, M. Ç. (2022). Toplum 5.0: İnsan Odaklı Dijital Dönüşüm. *Sosyal Siyaset Konferansları Dergisi*, s. 309-336.

Dunlap, C. J. (2012). The Intersection of Law and Ethics in Cyberwar: Some Reflections. *Air & Space Journal, 24*, s. 1-13.

Ebrem, İ. S., & Kurut, D. (2020). *Birleşmiş Milletler'in Siber Güvenlik Politikası.* Ankara: Nobel Akademik Yayıncılık.

Ekinci, O., & Kayapalı Yıldırım, S. (2020). *Siber Zorbalık.* Ankara: Nobel Bilimsel Eserler.

Eldem, T. (2021). Birleşmiş Milletler Sistemi ve Küresel Siberalan Güvenliği Regülasyonu. *Marmara Üniversitesi Siyasal Bilimler Dergisi, 9 (1)*, s. 17-45.

Eren, M. (2020). *İngiltere'nin Siber Güvenlik Politikası. Yeni Küresel Tehdit.* Ankara: Nobel Akademik Yayıncılık.

Ershov, N. V. (2011). Space Echo of Cold War. *Historical, Philosophical, Political and Legal Sciences, Cultural Studies and Art History. Theory and Practice Questions, 8(4)*, s. 62-65.

Fachkha, C., & Debbabi, M. (2016). Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization. *IEEE Communications Surveys & Tutorials, 18(2),*, s. 1197-1227.

Feinstein, L., Schnackenberg, D., Balupari, R., & Kindred, D. (2003, 1). Statistical Approaches to DDoS Attack Delection and Response. *Proceedings DARPA İnformation Survivability Conference and Exposition* , s. 303-314.

Göçoğlu, V., & Aydın, M. D. (2019). Siber Güvenlik Politikası: ABD, Rusya ve Çin Üzerine Karşılaştırılmalı Bir Analiz. *Güvenlik Bilimleri Dergisi, 8(2)*, s. 229-252.

Goldstein, J. S., & Pevehouse, J. C. (2015). *Uluslararası İlişkiler.* Ankara: BB101 Yayınları.

Gonzalez, F., Yu, Y., Fegueura, A., Lopez, C., & Aragon, C. (2019). Global Reactions to the Cambridge Analytica Scandal: A Cross-Language Social Media Study. *In Companion Proceedings of the 2019 world wide web conference*, s. 799-806.

Graham, S. (1998). The End of Geography or The Explosion of Place? Conceptualizing Space, Place and Information Technology. *Progress in Human Geography, 22(2)*, s. 165-185.

Grotius, H. (2011). *Savaş ve Barış Hukuku.* İstanbul: Say Yayınları.

Gutnikov, A., Kupreey, O., & Smeley, Y. (2022). *Securelist*. https://securelist.com/ddos-attacks-in-q4-2021/105784/: https://securelist.com/ddos-attacks-in-q4-2021/105784/ adresinden alındı

Halder, D. (2011). Information Technology Act and Cyber Terrorism. Sundaram, P. M. and Umarhathab, S. (Eds.), Cyber Crime and Digital Disorder. *India: Manonmaniam Sundaranar University.*, s. 75-89.

Hauben, M., & Hauben, R. (1998). The Net and Netizens: The Impact of the Net on People's Lives (Chapter 1). *First Monday, 3(7)*, s. 1-21.

Heawood, J. (2018). Pseudo-Public Political Speech: Democratic Implications of the Cambridge Analytica Scandal. *Information Polity, 23(4)*, s. 429-434.

Heickerö, R. (2014, 38). Cyber Terrorism: Electronic Jihad. *Strategic Analysis*, s. 554-565.

Heng, Y. K. (2013, 35 3). A Global City in an Age of Global Risks: Singapore's Evolving Discourse on Vulnerability. *Contemporary Southeast Asia*, s. 423-446.

Hildreth, S. A. (2001). Cyberwarfare. *Library of Congress Washington DC Congressional*, s. 1-17.

HM Goverment. (2016). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf adresinden alındı

HM Goverment. (2022). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf adresinden alındı

Hobbes, T. (2016). *Leviathan* . İstanbul: Yapı Kredi Yayınları.

Hong, J. (2012). The State of Phishing Attacks. *Communications of the ACM, 55(1)*, s. 74-81.

HSDL. (2000, 05 18). *I Love You' Computer Virus and Its Impact on U.S. Financial Services Industry: Hearing before the U.S. Senate, Committee on Banking, Subcommittee on Financial Institutions, One Hundred Sixth Congress, Second Session*. HSDL: https://www.hsdl.org/c/abstract/?docid=35679 adresinden alındı

https://ccdcoe.org/. (tarih yok). https://ccdcoe.org/ adresinden alındı

https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html. (tarih yok). https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html adresinden alındı

https://securelist.com/ddos-attacks-in-q4-2021/105784/. (tarih yok). https://securelist.com/ddos-attacks-in-q4-2021/105784/ adresinden alındı

https://www.britannica.com/event/Peace-of-Westphalia. (tarih yok). https://www.britannica.com/event/Peace-of-Westphalia adresinden alındı

https://www.cnbc.com/video/2022/12/08/a-brief-history-of-the-metaverse.html. (tarih yok). https://www.cnbc.com/video/2022/12/08/a-brief-history-of-the-metaverse.html adresinden alındı

https://www.sibervatan.org/makale/enigma-sifreleme/17. (tarih yok). https://www.sibervatan.org/makale/enigma-sifreleme/17 adresinden alındı

https://www.socialsciencespace.com/2018/03/will-cambridge-analytica-hurt-legitimate-research/. (tarih yok). https://www.socialsciencespace.com/2018/03/will-cambridge-analytica-hurt-legitimate-research/ adresinden alındı

https://www.voltairenet.org/article207568.html. (tarih yok). https://www.voltairenet.org/article207568.html adresinden alındı

Huaben, M. (2007). History of ARPANET. *Site de l'Instituto Superior de Engenharia do Porto, 17*.

Huangh, H., Tan, J., & Lin, L. (2009). Countermeasure Techniques For Deceptive Phishing Attack. *In 2009 International Conference on New Trends in Information and Service Science, IEEE.*, s. 636-641.

İçli, G. (2001). Küreselleşme ve Kültür. *CÜ Sosyal Bilimler Dergisi, 25(2)*, s. 163-172.

Internet Live Stats. (2021). https://www.internetlivestats.com/: https://www.internetlivestats.com/ adresinden alındı

Ünver, M., Canbay, C., & Mirzaoğlu, A. G. (2011). Siber Güvenliğin Sağlanması: Türkiye'deki Durum ve Alınması Gereken Tedbirler. *Ankara: Bilgi Teknolojileri ve İletişim Kurumu (BTK)*.

İpek, C. D. (2012, 1 3). Afrika Birliği Örgütü ve Kıtada İşbirliği Arayışları. *21. Yüzyılda Eğitim Ve Toplum Eğitim Bilimleri Ve Sosyal Araştırmalar Dergisi*, s. 111-130.

Irani, D., Balduzzi, M., Balzaroddi, D., Kirda , E., & Pu, C. (2011). Reverse Social Engineering Attacks in Online Social Networks. *n Detection of Intrusions and Malware, and Vulnerability Assessment: 8th International Conference; DIMVA 2011*, s. 55-74.

IWS. (2022). https://www.internetworldstats.com/stats.htm: https://www.internetworldstats.com/stats.htm adresinden alındı

Jajoo, A. (2021). A study on the Morris Worm. *ArXiv Preprint ArXiv:2112.07647*.

Jakabsson, M. (2005). Modeling and Preventing Phishing Attacks. *In Financial Cryptography, 5*, s. 1-19.

Jupillat, N. (2016). From the Cuckoo's Egg to Global Surveillance: Cyber Espionage That Becomes Prohibited Intervention. ,. *NCJ Int'l L., 42*, s. 934-987.

Köker, A. E. (2021). *Tehdit, Caydırıcılık, Güvenlik, Çatışma ve Savaş İkileminde Siber Dünya.* İstanbul: Urzeni Yayıncılık.

Köksoy, F. (2020). Avrupa Birliği'nin Siber Güvenlik Politikası: Kurumsalcılık mı Tutarlılık mı? *Güvenlik Stratejileri Dergisi, 16(35),* s. 635-674.

Kara, İ. (2015). Türkiye'de Zararlı Yazılımlarla Mücadelenin Uygulama Ve Hukuki Boyutunun Değerlendirilmesi. *Akademik Bakış Uluslararası Hakemli Sosyal Bilimler Dergisi ,(52),* s. 87-98.

Kardaş, T. (2014). *Güvenlik. Uluslararası İlişkilere Giriş içinde.* İstanbul: Küre Yayınları.

Kassab, H. S. (2013). In Search of Cyber Stability: International Relations, Mutually Assured Destruction and The Age of Cyber Warfare. *In Cyberspace and International Relations: Theory, Prospects and Challenges*, s. 59-76.

Kemp, S. (2022). *Digital 2022: Global Overview Report*. https://datareportal.com/reports/digital-2022-global-overview-report: https://datareportal.com/reports/digital-2022-global-overview-report adresinden alındı

Kennedy, D. (2006). Of War and Law. *United Kingdom: Princeton University Press*.

Kesharwani, S., Sarkar, M. P., & Oberoi, S. (2019). Cyber Security in India: Threats and Challenges. *Cybernomics, 1(2),* s. 32-34.

Kiraz, O. Z. (2021). Siber Güvenlik Bağlamında Yeni Tehdit Algılamalarının Türkiye'nin Güvenlik Politikalarına Etkileri. *Journal of Management Theory and Practices Research, 2(2),* s. 69-88.

Kitchin, R. M. (1998). Towards geographies of cyberspace. *Progress in human geography, 22(3),* s. 385-406.

Korhan, S. (2020). Uluslararası İlişkilerde Siber Güvenlik: Caydırıcılık, Güç ve Diplomasi. F. Köksoy içinde, *Yeni Küresel Tehdit: Siber Saldırılar* (s. 51-65). Ankara: Nobel Akademik Yayıncılık.

Korucu, O. (2021). Yeni Normal Dünya Düzeninin Siber Güvenlik ve Bilgi Güvenliğine Etkileri. *Yönetim Bilişim Sistemleri Dergisi, 7(1),* s. 44-60.

Kuehl, D. (2009). From Cyberspace to Cyberpower: Defining the Problem. *Universty of Nebraska Press.*, s. 24-42.

Lambrinoudakis, C., Gritzalis, S., Dridi, F., & Pernul, G. (2003). Security Requirements for E-Government Services: A Methodological Approach for Developing a Common PKI-Based Security Policy. *Computer communications, 26(16),* s. 1873-1883.

Landwehr, C. E. (2009). A National Goal for Cyberspace: Create an Open, Accountable Internet. *IEEE Security & Privacy, 7(3)*, s. 3-4.

Lee, L. H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., & Hui, P. (2021). All One Needs to Know About Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem and Research Agenda. *ArXiv Preprint ArXiv:2110.05352, 14(8)*, s. 1-47.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., . . . Wolff, S. S. (1997). The Past and Future History of The Internet. *Communications of the ACM, 40(2),*, s. 102-108.

Levy, S., & Crandall, J. R. (2020). The Program With a Personality: Analysis of Elk Cloner, The First Personal Computer Virus. *ArXiv Preprint ArXiv:2007.15759.*

Lin, H., & Kerr, J. (2017). On Cyber-Enabled Information/Influence Warfare and Manipulation. *Center for International Security and Cooperation, Stanford, SAD*, s. 4-22.

MacKinnon, R. (2012). The Netizen. *Development, 55*, s. 201-204.

Mannik, E. (2009). Terrorism: Its Past, Present and Future Prospects. *KVÜÕA toimetised, (12)*, s. 151-171.

Miles, C. (2012). Early History of the Computer Virus. *Prof. Dasgupta's History of Computer Science The Center for Advanced Computer Studies University of Louisiana*, s. 1-8.

Milmo, D. (2023, 01 17). *TechScape: Sonunda, İngiltere'nin çevrimiçi güvenlik yasası parlamentoda gününü alıyor - işte bilmeniz gerekenler*. The Guardian: https://www.theguardian.com/technology/2023/jan/17/online-safety-bill-meta-pinterest-snap-molly-russell adresinden alındı

Mirkovic, J., & Reiher, P. (2004). A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. *ACM SIGCOMM Computer Communication Review, 34(2)*, s. 39-53.

Mohurle, S., & Patil, M. (2017). A Brief Study of Wannacry Threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science, 8(5)*, s. 1938-1940.

NATO. (2022). *The Secretary General's Annual Report 2022.* NATO.

NATO. (2023, 04 13). *Cyber Defence*. NATO: https://www.nato.int/cps/en/natohq/topics_78170.htm adresinden alındı

Nezgitli, S., & Benzer, R. (2020). Avrupa Birliği Siber Güvenlik Kanunu. *Journal of Information Systems and Management Research, 2(1)*, s. 10-17.

Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology, 7*, s. 61-73.

Nomokonov, V. A., & Tropino, T. L. (2012). Cybercrima As a New Criminal Threat. *Criminology: Yesterday, Today, Tomorrow, 1(24)*, s. 45-55.

Orji, U. J. (2018). The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability? *Masaryk University Journal of Law and Technology, 12(2)*, s. 91-129.

Orman, H. (2003). The Morris Worm: A Fifteen-Year Perspective. *IEEE Security & Privacy, 1(5)*, s. 35-43.

Ottis, R., & Lorents, P. (2010). Cyberspace: Definition and Implications In International Conferencn Cyber Warfare and Security. *Academic Conferences International Limited*, s. 267-270.

Pekcan, C. (2020). *Çin Halk Cumhuriyeti'nin Siber Güvenlik Politikası.* Ankara: Nobel Akademik Yayıncılık.

Perendi, D. M., & Gope, P. (2021). The Language's Impact on the Enigma Machine. *Cryptology ePrint Archive*, s. 1-7.

PM Lee Hsien Loong at the Smart Nation Launch,. (2014). Prime Minister's Office Singapore: https://www.pmo.gov.sg/Newsroom/transcript-prime-minister-lee-hsien-loongs-speech-smart-nation-launch-24-november, adresinden alındı

Potocan, V., Mulej, M., & Nedelko, Z. (2020). Society 5.0: Balancing of Industry 4.0, Economic Advancement and Social Problems. *Kybernetes.*

Rai, M., & Mandoria, H. (2019). A Study on Cyber Crimes Cyber Criminals and Major Security Breaches. *Int. Res. J. Eng. Technol., 6(7)*, s. 233-240.

Resmi Gazete. (2004). *TÜRK CEZA KANUNU 5237 sayılı kanun.* 06 26, 2023 tarihinde mevzuat.gov.tr: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5 adresinden alındı

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, Mitigation and Prevention. *International Management Review, 13(1)*, s. 10-17.

Sönmez, G. (2019, 21 21). El-Kaide'den DEAŞ Sonrası Döneme: Küresel Militan Selefi Hareketin Dönüşümü ve Geleceği. *Güvenlik Çalışmaları Dergisi*, s. 134-148.

Salahaddine, F., & Kaabounch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet, 11(4)*, s. 89-106.

Sandıklı, A., & Emeklier, B. (2012). Teoriler Işığında Güvenlik, Savaş, Barış ve Çatışma Çözümleri, İsanbul: Bilsam Yayınları, 3(70). *Güvenlik Yaklaşımlarında Değişim ve Dönüşüm* (s. 3-59). içinde İstanbul: Bilsam Yayınları.

Saraçlı, M. (2007). Uluslararası Hukukta Terörizm. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, 11(1)*, s. 1049-1078.

Saracel, N., & Aksoy, I. (2020). Toplum 5.0: Süper Akıllı Toplum. *Social Sciences Research Journal, 9 (2)*, s. 26-34.

Satia, P. (2014, 5 1). Drones: A History from the British Middle East. *Humanity: An International Journal of Human Rights, Humanitarianism, and Development*, s. 1-31.

Schmitt, M. N. (2014). The Law of Cyber Warfare: Quo Vadis. *Stan. L. & Pol'y Rev., 25,*, s. 269-299.

Schroeder, M. N., Taufika, R., Elder, L., Simoni, F., Abil, S., & Pronk , M. (2009). Securitisation and the Copenhagen School. *International Studies Quarterly, 53,*, s. 1-4.

Scott Levy, J. R. (2020). The Program with a Personality: Analysis of Elk Cloner, the First Personal Computer Virus. *arXiv:2007.15759*, 1-8.

Selçuk, Z. (2020). Yeni Küresel Tehdit: Siber Saldırılar. F. Köksoy içinde, *Amerika Birleşik Devletleri'nin Siber Güvenlik Politikası.* Ankara: Nobel Akademik Yayıncılık.

Sertçelik, A. (2015). Siber Olaylarda Siber Aracılığıyla. *Medeniyet Araştırmaları Dergisi, 2 (3)*, s. 25-42.

Siberay. (2022). Zararlı Yazılımlar (Virüs, Truva Atı, Soluncan): https://www.siberay.com/zararli-yazilimlar-virus-truva-ati-solucan adresinden alındı

Singer, P. W., & Friedman, A. (2018). *Siber Güvenlik ve Siber Savaş (2. Baskı).* Ankara: Buzdağı Yayınevi.

SIU. (2016). A Brief History of IT. *IT Computer Technical Support Newsletter, 2(29)*, s. 1-6.

Skinner, C. P. (2014, 46 4). An International Law Response to Economic Cyber Espionage. *Connecticut Law Review*, s. 1165-1207.

Slaon, L. D. (2000). Echelon And The Legal Restraints On Signals Intelligence: A Need For Reevaluation. *Duke LJ, 50*, s. 1467-1510.

Sputnik. (2017). *Sputnik*. Türkiye, 13 Bin Hackerdan Oluşan 'Siber Ordu' Kurdu: https://sputniknews.com.tr/20170518/turkiye-13bin-hacker-siber-ordu-1028516923.html, (E.T. 08.11.2022) adresinden alındı

Srivastava, A., Gupta, B. B., Tyagi, A., Sharma, A., & Mishra, A. (2011). A Recent Survey on DDoS Attacks and Defense Mechanisms. *In International Conference on Parallel Distributed Computing Technologies and Applications*, s. 570-580.

Subramanya, S. R., & Lakshminarasimhan, N. (2001). Computer viruses. *IEEE potentials, 20(4)*, s. 16-19.

Töner Şen, S. (2021). *Siber Uzay ve Uluslararası Hukuk.* İstanbul: Onikilevha Yayıncılık.

Türkay, Ş. (2013). Siber Savaş Hukuku ve Uygulanma Sorunsalı. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 71(1)*, s. 1177-1227.

Türkiye, 13 bin hackerdan oluşan 'siber ordu' kurdu, https://sputniknews.com.tr/20170518/turkiye-13bin-hacker-siber-ordu-1028516923.html, (E.T. 08.11.2022). (tarih yok).

Türkoğlu, E. (2017, 5 1). KÜRESEL BİR TERÖR ÖRGÜTÜ OLARAK IŞİD'İN DİJİTAL DERGİ KULLANIMI: KONSTANTİNİYYE ÜZERİNE BİR İNCELEME. *Erciyes İletişim Dergisi "akademia"* , s. 162-180.

Tandon, A., & Nayyar, A. (2019). A Comprehensive Survey on Ransomware Attack: A Growing Havoc Cyberthreat. *Data Management, Analytics and Innovation*, s. 403-420.

Tanrısever, O. F. (2011). *Güvenlik, Devlet ve Ötesi Uluslararası İlişkilerde Temel Kavramlar.* İstanbul: İletişim Yayınları.

Teh, K., Suhendra, V., & Lim, S. C. (2020). Singapore's Cybersecurity Ecosystem. *Communications of the ACM, 63(4)*, s. 55-57.

Teh, K., Suhenra, V., Lim, S. C., & Roychoudhury, A. (2020). Singapore's Cybersecurity Ecosystem. *Communications of the ACM, 63(4)*, s. 55-57.

Tekkanat, E., Topaloğlu, M., & Yılmaz, O. (2018). Bilişim Suçları ve Psikolojik Etkileri Açısından Türkiye'de Telefon Dolandırıcılığının Etkin Analizi. *Ege Eğitim Teknolojileri Dergisi, 2*(2), s. 44-54.

Tekke, A., & Aybala, L. (2021). Sosyal Medyada Etik, Bilgi Manipülasyonu ve Siber Güvenlik. *Akademik İncelemeler Dergisi, 16(2),* s. 44-62.

Terörle Mücadele Kanunu. (1991). https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=3713&MevzuatTur=1&MevzuatTertip=5: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=3713&MevzuatTur=1&MevzuatTertip=5 adresinden alındı

Terzi, M. (2019). E-government and Cyber Terrorism: Conceptual Framework, Theoretical Discussions and Possible Solutions. *Tesam Akademi, 6(1)*, s. 213-247.

Theofanos, M. (2020). Is Usable Security an Oxymoron?. *Computer, 53(2)*, s. 71-74.

Thomas, T. L. (2003). Al Qaeda and the Internet: The Danger of'Cyberplanning'. *Foreign Military Studies Office (ARMY) Fort Leavenworth Ks*, s. 112-123.

Tuli, P., & Sahu, P. (2013, 2 3). System Monitoring and Security Using Keylogger. *International Journal of Computer Science and Mobile Computing*, s. 106-111.

UN Security Council. (2017). https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/241/71/PDF/N1724171.pdf?OpenElement: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/241/71/PDF/N1724171.pdf?OpenElement adresinden alındı

United Nation. (2023). *Sixteenth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat.* Office of Counter-Terrorism.

United Nations. (2017). *Resolution 2370 (2017) / adopted by the Security Council at its 8017th meeting, on 2 August 2017.* United Nations.

(1993). *Viyana Deklarasyon ve Eylem Programı.* Viyana: Vienna Declaration and Programme of Action,.

Vuving, A. (2009). How soft power works. *Asia-Pacific Center for Security Studies Honolulu United States*, s. 1-20.

Warner, M. (2012). Cybersecurity: A Pre-history. *Intelligence and National Security, 27(5)*, s. 781-799.

Wolfers, A. (1952). National security" as an ambiguous symbol. *Political science quarterly, 67(4)*, s. 481-502.

Wolforth, W. C. (2009). Realism and security studies. *In The Routledge Handbook of Security Studies,67 (4)*, s. 9-20.

Xu, M., Niyato, D., Kang, J., Xiong, Z., Miano, C., & Kim, D. I. (2021). Wireless Edge-Empowered Metaverse: A Learning-Based Incentive Mechanism for Virtual Reality. *ArXiv Preprint ArXiv:2111.03776.*

Yılmaz , B. A. (2020). Siber Terörizm ve Değişen İstihbarat Anlayışı. *Anadolu Strateji Dergisi, 2(1)*, s. 65-82.

Yılmaz, S. (2011). Yumuşak Güç ve Evrimi. *Turan-Sam, 3(12)*, s. 31-36.

Yardımcıoğlu, M., & Koçarslan, H. (2012). Çok Kutuplu Dünyaya Doğru: Şanghay İşbirliği Örgütü. *Kahramanmaraş Sütçü İmam Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 2(2)* , s. 163-174.

Yatağan, A. G. (2018). Sert Güç Unsurlarının Yumuşak Güç Aracı Olarak Etkileri. *Kara Harp Okulu Bilim Dergisi, 28(2)*, s. 69-94.

Yayla, M. (2014, 4 2). Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı. *Hacettepe Hukuk Fakültesi Dergisi*, s. 181-200.

Yetgin, M. A., & Baştuğ, M. (2022). *Metaverse ve Şirketlerde Dijital Dönüşüm. Ankara: Detay Yayıncılık.* Ankara: Detay Yayıncılık.

Yetkin, M. A. (2021). *Çin İstihbarat Örgütünün Stratejik Analizi.* Ankara: Gazi Kitabevi.

Yetkin, M. A., & Baştuğ, M. (2021b). Devlet Terörizmi Bağlamında Tarihsel Vakaların İç ve Dış Etkilerinin Analizi: BM Güvenlik Konseyi Üyeleri Örneği. *İstanbul Aydın Üniversitesi Sosyal Bilimler Dergisi, 13(4)*, s. 955-980.

Yorulmaz, M. (2020). Realizm ve Liberalizm Perspektifinde Arktik Bölge Güvenliği ve Süregelen Güvenlik İkilemi. *OPUS Uluslararası Toplum Araştırmaları Dergisi, 16 (32)*, s. 5250-5273.

Zenginkuzucu, D. M. (2020). *Güvenlik Çalışmaları (Cilt I) Kuramsal Yaklaşımlar.* İstanbul: Hiper Yayın.

6. e-Safe Siber Güvenlik Zirvesi. (16 Mart 2022). Siber Saldırı ve Siber Savaş Arasındaki Farklar [Video dosyası].https://www.youtube.com/watch?v=bOQVoIUnGCM&t=87s, (E.T. 10.12.2022).

ŞEKİLLER LİSTESİ

ÖZGEÇMİŞ

Eğitim hayatına 2014'te Selçuk Üniversitesi Uluslararası İlişkiler anabilim dalında başladı, hazırlık eğitimiyle birlikte 2019'da mezun oldu ve 2020'de Karabük Üniversitesi Uluslararası İlişkiler anabilim dalında Tezli Yüksek Lisans eğitimine başladı. Yazar, Haziran 2023 yılı itibariyle mezun olarak bu süreçte eğitim hayatına 2 kitap, 2 makale ve 1 kongreyle katkı sağladı. Halihazırda yayınlanmayı bekleyen 1 kitap ve 2 makalesi bulunmakta.