FIRAT ÜNİVERSİTESİ
SOSYAL BİLİMLER DERGİSİ
Journal of Social Sciences
p-ISSN:1300-9702 e-ISSN: 2149-3243

ULUSLARARASI POLİTİKADA BİR ETKİ ARACI OLARAK SİBER GÜVENLİK VE TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKASI UYGULAMASI: ULUSAL SİBER OLAYLARA MÜDAHALE MERKEZİ (USOM)

Cyber Security as an Influencer in International Politics and Türkiye's Cyber Security Policy Implementation: National Cyber Incident Response Center (TR-CERT)

Serkan GÜNDOĞDU[1]

[1]*Dr. Öğr. Üyesi, Munzur Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Siyaset Bilimi ve Uluslararası İlişkiler Bölümü, Tunceli, sgundogdu@munzur.edu.tr*, orcid.org/ 0000-0001-7597-879X

Araştırma Makalesi/Research Article

Makale Bilgisi
Geliş/Received: 07.03.2023
Kabul/Accepted: 11.09.2023

DOI:
10.18069/firatsbed.1261707

Anahtar Kelimeler
Uluslararası Politika, Siber Güvenlik, Siber Güvenlik Politikası, Ulusal Siber Olaylara Müdahale Merkezi

ÖZ

Teknolojik gelişmelere bağlı olarak internetin kullanımı gündelik hayatın her alanında etkin bir şekilde yer almaya başlamıştır. Bu süreç insanların hayatını birçok alanda kolaylaştırdığı gibi bazı sorunları da beraberinde getirmiştir. Bu sorunlardan önemli bir tanesi de güvenlik olmuştur. Uluslararası politika bakımından da yeni güvenlik önemlerine ihtiyaç duyulmuş, uluslararası ilişkiler disiplininde güvenlik kavramının önemli bir kavramı haline gelen siber güvenlik sorunun ortaya çıktığı görülmüştür. Bu çerçevede siber tehditlere karşı koyabilmek için savunma sistemlerini içeren siber güvenlik politikaları oluşturulmaya başlanmıştır. Çalışma kapsamında Türkiye'nin siber uzaydaki varlığı ve bu alanda kamu hizmetlerinin nasıl sağlandığı, siber güvenlik politikalarına ilişkin çalışmalarını nasıl planladığı incelenmiştir. Türkiye'nin siber güvenliği sağlama adına yapmış olduğu; politika, strateji ve eylem planları ile araştırma konusu sınırlandırılmıştır. Siber tehditleri azaltmak ve bertaraf etmek amacıyla, Türkiye'nin ulusal siber güvenlik stratejisi açısından önemli olan yapılar çalışma kapsamında verilmiştir. Bu bağlamda Ulusal Siber Olaylara Müdahale Merkezi'nin siber güvenlik stratejisine ve uluslararası politikada bir etki aracı olması noktasında ne denli bir etkiye sahip olduğu üzerinde durulmuştur.

Keywords
International Politics, Cyber Security, Cyber Security Policies, National Cyber Incident Response Center

ABSTRACT

Depending on the technological developments, the use of the internet has started to take place effectively in every aspect of daily life. This process has made people's lives easier in many areas and has brought some problems with it. One of the most important of these problems has been security. New security measures were also needed in terms of international politics, and it was seen that the problem of cyber security, which has become an important concept of security in the discipline of international relations, has emerged. In this context, cyber security policies including defense systems have been started to be created in order to counter cyber threats. Within the scope of the study, Turkey's presence in cyberspace, how public services are provided in this area, and how it plans its studies on cyber security policies are examined. What Turkey has done on behalf of providing cyber security; policy, strategy and action plans and the research subject are limited. In order to reduce and eliminate cyber threats, structures that are important for Turkey's national cyber security strategy are given within the scope of the study. In this context, it has been emphasized how the National Cyber Incidents Response Center has an impact on cyber security strategy and being an instrument of influence in international politics.

Atıf/Citation: Gündoğdu, S. (2023). Uluslararası Politikada Bir Etki Aracı Olarak Siber Güvenlik ve Türkiye'nin Siber Güvenlik Politikası Uygulaması: Ulusal Siber Olaylara Müdahale Merkezi (USOM). *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 33, 3, 1325-1337.

Sorumlu yazar/Corresponding author: Serkan GÜNDOĞDU, sgundogdu@munzur.edu.tr

1. Giriş

Bilişim ve teknolojik gelişmelerle ile birlikte pek çok alanda kullanılan tanımamalar süreç içinde tekrar gözden geçirilmektedir. Özellikle klasik anlamda (fiili/ somut ortamda) var olan savaş, düşman, güvenlik gibi çalışma konusuna dahil olan kavramların kullanım alanlarında değişiklikler görülmektedir. Bu yeni alanlardan biri olan siber uzay; ağlar, bilgi kaynakları ve veri sistemlerinin bir araya gelmesiyle yeni bir harekat ortamı oluşmuş ve NATO tarafından diğer harekat alanları kadar etkili biçimde savunması gereken bir operasyon alanı olarak kabul edilmiştir.

Bu yeni harekat sahası; çatışmalar, tehditler, kötü niyetli yazılımlar, suçların meydana geldiği ve klasik savaşa benzer özellikler gösterebilen soyut bir savaş/ üstünlük alanı olarak ortaya çıkabilmektedir. Siber uzayda gerçekleşen saldırının fiziksel saldırıya göre, farklı devlet ideolojileri nedeniyle oluşabilecek çatışmalar gibi, çok daha çeşitli ve güçlü tarafların karşı karşıya gelmesine sebep olabileceği görülmektedir. Gerçekleşen veya gerçekleşme ihtimali bulunan saldırıların siber silahlar ile siber uzayda vuku bulması, ulusal güvenliğe karşı siber saldırıları önleme ve caydırma stratejilerinden oluşan bir güvenlik yöntemine ihtiyacı beraberinde getirmektedir. Bu bakımdan siber uzayın tüm yönleriyle olmasa da belli yönlerinde ulus ve ulus üstü yapılar nezdinde anlaşmaya gidilmesi gerekliliğini meydana getirmektedir.

Siber güvenlik konusunda saldırıların uluslararası alanda tanılanması ve nelerin saldırı aracı olup nelerin savunma adına kullanılması gerektiğinin belirlenmesi bu bakımdan önemlidir. Birleşmiş Milletler, Avrupa Konseyi, G8 Ülkeleri ve NATO gibi uluslararası kuruluşlar siber güvenlik alanında kendilerine özgü stratejiler belirlemiştir. Bu aktörlerin siber güvenliğe yüklediği anlam; siber uzayın okyanuslar gibi sınır tanımlamasının olmaması, bilişim teknolojilerinin kullanımının yaygınlığı, ulusal ve uluslararası güvenliğin örtüşmesi, politik ve askeri çatışmaların siber boyutu tarzında çeşitli gerekçeler siber güvenliği uluslararası politikada etkili bir araç haline getirmiştir. Bu bakımdan siber alanda istikrarın korunması ulusun siyasi coğrafyasını korumaktan daha mühim hale gelebilmektedir. Bu alanda ulus nezdinde daha kapsamlı bir mücadele için farklı politikalar belirlemek ve çalışmalar yürütmek, devletin asli görevlerindendir. Çalışma yöntemi olarak literatür taraması yapılmış, alanda yapılmış çalışmalar incelenmiş, kurum içerikleri ve resmi yayınların incelenmesiyle oluşturulmuştur. Çalışmanın ilk kısmında kavramsal bilgilere yer verilmiş, tarihsel serüveni ve gelişimi aktarılmıştır. Siber güvenlik çalışmalarının genel hatlarına değinilerek Türkiye'nin siber güvenlik politikaları hakkında bilgiler sunulmuştur. Siber güvenlik politikasının uluslararası politikada bir etki aracı olup olmadığı sorusuna cevap aranmıştır.

2. Siber Güvenlik Kavramının Ortaya Çıkışı

Güvenlik kavramı, ulus devletin ortaya çıkmasıyla birlikte hızlı bir değişim içine girmiştir. Günümüzde bilim ve teknik alanında yaşanan ilerlemeler ve bunların küreselleşme ile etkilerinin dünya geneline yayılımı pek çok alan tanımlamalarını da değişime uğratmıştır. Özellikle Soğuk Savaş sürecinde düşman ve tehditlerin belli olduğu "klasik düşman" tanımlaması yerini çok daha karmaşık, öngörülemez ve değişken "tehdit" tanımlamasına bırakmıştır. Askeri tehdit/ riskler çok daha karmaşık ve çok boyutlu bir güvenlik tanımlamasına doğru evrilmiştir. Bilgi ve iletişim teknolojileri ile birlikte bilgisayar ve internet kullanımının yaygınlaşması, devlet kurum/ kuruluşlarının altyapısı ve sistem kontrolünün dijital aygıtlarla yapılması gibi birçok husus devletlerden bireylere kadar geniş bir yelpazenin siber tehditlerle etkileşime girebileceğini göstermektedir (Çelik, 2021: 1-2).

Bilgisayarların tarihsel anlamda ortaya çıkışı, askeri alanda teknolojik gelişmelere duyulan ihtiyaçtan ve süper güçler arasında üstünlük sağlama hedefinden kaynaklı olduğu söylenebilir. Alan Turing, İkinci Dünya Savaşı sırasında geliştirmiş olduğu Turing makinesi ile algoritma ve hesaplamalar kullanabilen basit bir hesaplama cihazı geliştirmiştir. Bu bakımdan modern anlamda kullanılan bilgisayarların bir öncüsü olarak kabul edilmektedir (Gams, 2013: 9-11). Aynı dönemde ABD, olumsuz hava koşullarına bağlı savaş malzemelerinin hedef belirleyememesi üzerine silahların doğru hedefe yönelmesini sağlayacak bir teknoloji geliştirmeyi amaçlamıştır. 1943 yılında John Mauchly ve Presper Eckert ilk dijital bilgisayar kabul edilen Elektronik Sayısal Bütünleştirici ve Bilgisayar (ENIAC) isimli cihaz 1946 yılında icat edilmiştir (Shelburne, 2017: 26-28).

1950'lere gelindiğinde birçok devlet kurumu ve özel şirket büro işlemleri için elektronik bilgi işlem departmanları kurmaya başlamıştır. 1969 yılında kurulan ARPANET (Gelişmiş Araştırmalar Projeleri Dairesi Ağı) isimli bir ağın sonucu olarak bugün kullanılan internetin oluştuğu bilinmektedir. Bu ağ, üniversiteler ile

devlet kurumları arasında bağlantı kurulmasını sağlamıştır. 1990'larda ise "World Wide Web" in kurulması ile akademik alanın dışında pek çok kullanıcının birbiriyle bağlantı kurması sağlanmıştır. Bu gelişimler beraberinde bilginin her bir bireyin bilgisayarından erişebilir olması fikrini beraberinde getirmiştir. Böylece bilgisayar teknolojilerinde gerçekleşen teknik ve teorik ilerlemeler neticesinde bilgisayar kullanımı askeriyeden hükümetlere, özel şirketlerden bireylere kadar yayılım sağlamıştır (Campbell-Kelly, Garcia-Swartz, 2013: 18-19). Böylece günümüz dünyasında bilgi ve iletişim teknolojileri (BİT) her bir ülkenin merkez gündeminde yer almıştır.

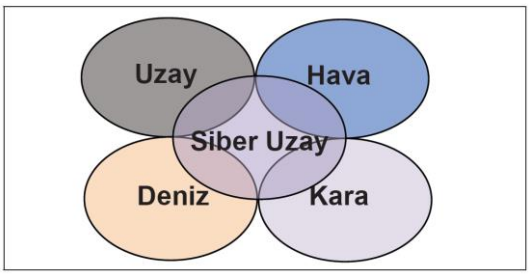
Bu gelişmelerin yanında "World Wide Web" in kurulmasından önce 2 Kasım 1988 tarihinde solucan adı verilen ilk kötü niyetli program MIT'deki bir bilgisayar vasıtasıyla yayılmıştır. O dönemin şartlarında aktif olarak kullanılan bilgisayarların yüzde 10'una bu solucan bulaşmıştır. Kötü niyetli program, askeri araştırma tesisleri ve üniversitelerin bilgisayarlarının temel işlemlerini büyük ölçüde yavaşlatıştır (Denning, 1989: 126). Bütün bu gelişmeler çok kısa zamanda internet kullanıcılarının sayısını önemli ölçüde arttırmasının yanında bilgi ve iletişim teknolojilerinin bu hızla gelişmesi/ genişlemesi beraberinde tehditleri de getirmiştir. Geçtiğimiz yıllarda siber saldırıların kapsamlı etkileri çok daha görünür hale gelmiştir. 2013 yılında Yahoo!'ya yapılan saldırıda üç milyara yakın kullanıcının verilerinin ihlal edildiği görülmüştür. 2017 yılında 150 farklı ülkede dijital cihaz kullanıcılarını dolandıran WannaCry fidye yazılımı saldırısı gerçekleşmiştir (Kaspersky, 2023). Görüldüğü üzere siber saldırıların bireylere, şirket ve devletlere oluşturduğu zararların maliyeti son derece dikkat edilmesi gereken düzeydedir.

Bütün bu gelişmeler göz önüne alındığında; siber güvenlikle ilgili modern güvenlik anlayışına yönelik konuların gündemde kalması ve anlaşılması sağlanmalıdır. Çalışma kapsamında konunun anlaşılması bakımdan siber güvenlik alanındaki temel kavramlar alt başlıklarda açıklanmıştır.

2.1. Beşinci Harekat Alanı Olarak Siber Uzay

Güvenlik, her dönemde üzerinde durulan ciddi bir konu olmuştur. Günümüzde modern teknolojilerinin ilerlemesi ile devletler ulusal savunma programlarını bu doğrultuda ilerletmiştir. Diğer bir değişle tehditlere karşı güvenli bir ortam oluşturulması bakımından etkili koruma yöntemine ihtiyaç duyulmuştur. Güvenlik alanında yaşanan bu değişimler ile kavram, siber uzay kavramını kapsayıcı bir anlamda kullanılmaya başlanmıştır. Hatta teknolojinin bu şekilde yaygınlaşması bireylerin, şirket, kurum ve devletlerin dijital cihazlar ile birbirine ağlarla bu derece bağlılığı siber uzayı çok daha dikkat edilmesi gereken bir alan olmaya doğru ilerletmiştir.

William Gibson tarafından 1984 yılında tanımlanan siber uzay, iletişim yöntemlerinin geliştirilmesi ve basitleştirilmesi üzerine gerçekleştirilen çeşitli yenilikler ve fikirlerin bir sonucu olarak kullanılan bir kavramdır. Bu bakımdan sadece donanım, yazılım ve veri olarak internet kullanımı olarak sınırlı tutulmayan kavram; sosyal hayat, bilgi ile temellenmiş fiziksel ve mantıksal yapılar eşliğinde ortaya çıkmaktadır (Sağıroğlu ve Alkan, 2018: 87). NATO, 2016 yılında Varşova Zirvesi'nde "Varşova'da NATO'nun savunma yetkisini yeniden teyit ediyoruz ve siber uzayı NATO'nun kendisini havada, karada ve denizde olduğu kadar etkili bir şekilde savunması gereken bir operasyon alanı olarak kabul ediyoruz" şeklinde ifadesiyle "siber uzayı" yeni bir savunma alanı olarak kabul ettiğini belirtmiştir (NATO, 2016; Şekil 1). Bu bakımdan siber uzay; ağları, bilgi kaynaklarını ve veri sistemlerini bir araya getiren yeni bir harekat ortamı oluşturmuştur.



Şekil 1. Beşinci Harekat Alanı Olarak Siber Uzay (Çiftçi, 2017:7)

Görüldüğü üzere siber uzay, dünya ve uzay dahil olmak üzere birbirine bağlı ağlardan oluşan veya bağımsız bilgisayarlar, cihazlar gibi bilgi sistemlerinin altyapılarıyla ve bu cihazlar tarafından depolanan veri ve uygulamalardan oluşan bütün yazılım ve donanımı barındıran sayısal ortamdır (Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016: 7). Böylece siber uzay, dünya- uzay ilişkisinin dahil olduğu bir alanda yer alan insan yapımı bilgisayarlar ve iletişim araçlarından oluşan, sayısal verilere dayalı somut bir alan olduğu söylenebilir. Bunun yanında siber uzayın günümüz koşullarında bir gerçeklik haline gelmesi beraberinde siber güvelik konusunun önemini göstermiştir. Devletler uzay, hava, deniz ve kara alanlarında olduğu gibi siber uzayda da hakimiyet alanlarını koruma edimine gitmiştir. Ülkeler ulusal güvenliklerine yönelik siber uzay ihlalleri konusunda anlaşmazlıklarla karşılaştıkları görülmektedir. Gün geçtikçe ilerleyen ve genişleyen siber uzayın etkisi nedeniyle internet kullanımı ve siber güvenlik yaklaşımı dikkatle ele alınması gereken konular haline gelmektedir.

2.2. Siber Çatışmaların Genel Hatları

Siber saldırı, siber uzay alanında gerçekleşen çatışmalar, tehditler ve suçlarla ilişkili bir kavramdır. Bu bakımdan siber çatışma, klasik savaşa benzer özellikler gösterebilmektedir. Özellikle farklı devlet ideolojileri nedeniyle oluşabilecek çatışmalar, siber uzay ortamında da çok çeşitli ve güçlü tarafların karşı karşıya gelmesine sebep olabilecektir. Bu nedenle belirli saldırıların tahmin edilmesi veya koruma alanın fiziksel anlamda tespiti siber uzayda şuanın teknik bilgileriyle mümkün değildir. Bu durum siber uzayda gerçekleşen saldırının fiziksel saldırıya göre daha ani olmasına sebebiyet vermektedir. Bütün bu gelişmeler göz önünde bulundurularak, siber güvenlik konusunda saldırıların uluslararası alanda tanılanması ve nelerin saldırı aracı olup nelerin savunma adına kullanılması gerektiği belirlenmesi önemlidir (Stadnik, 2017: 138).

Siber çatışma olarak verilebilecek temel kavramlar sırası ile aşağıda verilmektedir:

a) Siber Tehdit: Siber uzayda ortaya çıkan bir açıklık sonucu bir bilginin kötü niyetliler tarafından ele geçirilmesi, işlevsiz hale getirilmesi veya tamamen kaldırılması anlamında kullanılmaktadır (Winther, Gran ve Dahll, 2005: 371). Devletlerin geçmişleri, milli güvenlik yaklaşımları gibi ibareler tehdit anlayışını tanımlamada farklılık göstermektedir.

b) Siber Suç: Bilişim sistemi güvenliği ve veri işlemlerini hedefleyen, bilgisayar ağı ile gerçekleştirilen kanun dışı eylemler olarak tanımlanmaktadır (Turhan, 2006: 30-31). Avrupa Konseyi Siber Suçlar Sözleşmesi ile, "Bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve kullanıma açık bulunmasına yönelik suçlar" içinde sisteme ve veriye yasadışı/ yetkisiz erişim, yasadışı müdahale, cihazların kötüye kullanımı; "Bilgisayarlara ilişkin suçlar"da bilişim sistemleri üzerinden gerçekleştirilen sahtecilik, dolandırıcılık fiilleri; "İçerikle ilgili suçlar" başlığında çocuk pornografisi; "Telif haklarının ve benzer hakların ihlaline ilişkin suçlar" alanında telif hakları ihlali ve benzer tarzında internetin yaygınlaşmasına bağlı gerçekleşen siber suçlar kategorize edilmektedir (Önok, 2013: 1243).

c) Siber Terörizm: Siyasi olarak güdülenmiş ulus atı toplulukların veya casusların halkı manipüle etmek ve güncel politikaları değiştirmek amacıyla bilgi bilişim teknolojilerini, yasalara aykırı olan biçimde, terör eylemlerine alet etmesi olarak tanımlanmaktadır (Andress ve Winterfeld, 2011: 198).

d) Siber Caydırıcılık: Olası taarruz ve risklere karşı güçlü savunma kapasitesi ve karşılık verebilme kabiliyetini içeren zaruri savunma önemlerinin alınması olarak ifade edilebilir (İduğ, Çalışkan ve Güler, 2013: 287).

e) Siber İstihbarat: Siber uzayda meydana gelen siber taarruz ve tehdit değerlendirmelerini gerçekleştirerek karşı taarruz ile bilgi temin edilmesidir (Keleştemur, 2015: 90).

f) Siber Casusluk: Bireyin, özel şirketlerin, devlet kurumlarının hayati derecede önemli bilgilerinin siber uzayda ilgililerin bilgisi olmadan temin edilmesidir (Yayla, 2014: 194).

g) Siber Taarruz: Bilişim teknolojileri vasıtasıyla gizlilik, erişim ve bilgi/ iletişim bütünlüğünün ortadan kaldırılması hedefiyle, siber uzayda yer alan kişi veya sistemlerin kasıtlı uyguladığı işlemler olarak tanımlanmaktadır (Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016: 7).

h) Siber Güvenlik: Bu kavram gerçekleşen saldırıların siber silahlar ile siber uzayda vuku bulması, manipüle yeteneği ve benzeri ulusal güvenliğe zarar veren saldırılar ile olumsuz/ istenmeyen etkilere karşı siber saldırıları önleme ve caydırma stratejilerinden oluşan bir güvenlik yöntemi olarak görülmektedir. Böylece ortaya çıkan sonuç, devletlerin sonsuz ihtimale dayanan siber saldırılara vereceği karşılık belirsiz koşullarda

gerçekleşmektedir. Böylece istikrarın korunması ulusun siyasi coğrafyasını korumaktan daha mühim hale gelebilmektedir (Calderaro ve Craig, 2020: 922).

Bahsi geçen maddelerden temel olanları alt başlıklarda detaylandırılmaktadır. Burada görülmesi gereken esas nokta; teknolojinin hızla gelişmesi ile günümüz dünyasının en önemli güvenlik sorunlarından biri haline gelen siber saldırı ihtimali ile en küçük bilginin bile çok büyük etkiler doğurmasına neden olabilmesidir. Hakimiyet kurma veya manipüle etme amaçları ağların kullanılabilmesi gibi en ciddi siber saldırıların devletler tarafından gerçekleştirilebildiği görülmektedir (Mareşi, 2020: 85). Örneğin Rusya ve ABD arasında gerçekleşen siber saldırılar, güç yarışı halinin modern teknolojik yapılara uyarlandığını görünür kılmaktadır. Özellikle siber uzayın anonimliği, dış uzay ve okyanuslar gibi sınır tanımlamasının olmaması, nedeniyle bölünmemiş/ fethedilmemiş olması saldırıların ele alınmasını zorlaştırmaktadır (Stadnik, 2017: 132). Bunun yanında siber saldırılar, asimetrik doğaları gereği saldırının nereden kaynaklandığına ilişkin sınırsız sayıda olasılık sunmaktadır. Bu nedenle siber saldırılarda oluşan zararlar tahminlerin ötesinde yıkıma neden olabilir ve saldırgan hiç bulunamayabilir. Başka bir değişle, siber uzayın düzenlenmesi ve ilgili tanımlamaların yeterince yapılmaması durumu bu alanının ivedilikle ele alınmasını gerekli kılmaktadır.

3. Uluslararası Politikada Etki Aracı Olarak Siber Güvenlik

Siber güvenliğin değişen dünyada devletlerarası ilişkilerde güvenlik sahası üzerinden tartışmaya konu olması, siber güvenliği uluslararası politikada ön plana çıkarmaktadır (Güntay, 2018: 80). Değişen dünyada özellikle teknolojideki ilerleme, siber güvenlikle doğrudan orantılı bir durumdur. Siber güvenliğin uluslararası ilişkilerde etkili bir araca dönüşmesi, siber güvenlik kavramının tarihsel süreçteki gelişimi ile paralellik göstermektedir. Siber güvenliğin tarihsel gelişimine bakıldığında, karşımızda şu şekilde bir tablo çıkmaktadır (Tablo 1).

Tablo 1. Siber Güvenlik Tarihsel Gelişimi

	İlk bilgisayar
1940	Virüslerle ilgili ilk teoriler
1950	Telefonda dolandırıcılık
	Bilgisayar korsanlığı
1960	İlk etik hackleme
	ARPANET
	Creeper
1970	Reaper
	İlk güvenlik projeleri
	İlk siber suçlular
	Yeni siber güvenlik terimler
	Turuncu Kitap
1980	Ticari antivirüsler
	Cascade
	Solucanlar
	DiskKiller
1990	ILOVEYOU virüsü
	Socket Layer (SSL)
	İlk hacker grubu
2000	DDoS saldırısı
	Yahoo saldırıları
	Devlet destekli saldırılar

Kaynak: (Nunes vd., 2019; 1607'den Akt. Öztunç, 2022: 28).

Tabloya göre yıllar içinde teknolojideki gelişmeye koşut bir şekilde hem siber suçlarda artış meydana gelmiş hem de buna karşılık güvenlik önlemleri geliştirilmiştir. NASA'nın araştırmacı kitlesi ihtiyacına binaen oluşturulan İleri Araştırma Projeleri Ajansı Ağı (ARPANET) (Bıçakcı, 2014: 104), siber güvenliğin başlangıç projesi olmuştur (Öztunç, 2022: 31). Siber güvenliğin kaynaklandığı alan ise siber uzaydır. Siber uzayın kökleri

de internetin çıkış noktası olan ARPANET'in 1970'lere dayanan tasarımıdır (Kramer, Starr ve Wentz, 2008: 3). Bu bağlamda, 1970'li yıllar siber güvenlik için kritik bir eşiği temsil etmektedir. Temelleri Soğuk Savaş yıllarında atılan bir ağ sistemi olan internet (Bıçakcı, 2014: 104), 1992'de yalnızca bir milyon kişi tarafından kullanılırken bu sayı yıllar içinde milyar kullanıcıya ulaşmıştır (Kramer, Starr ve Wentz, 2008: 6). 1985 yılında ABD Savunma Bakanlığı tarafından geliştirilen Güvenilir Bilgisayar Değerlendirme Kriterleri Turuncu Kitap olarak adlandırılmıştır (Yang ve Wen, 2017: 6). Turuncu kitap olarak adlandırılan bu kılavuz, üretilen yazılımların dikkate alması gereken önlemlere yer vererek (Öztunç, 2022: 33), bir nevi siber güvenlik rehberi işlevini gören bir kılavuz olmuştur. Bu dönem, ABD ve SSCB arasında Soğuk Savaş yılları olarak da adlandırılmaktadır. Bunun yanında, Soğuk Savaş yıllarında devletlerarası casusluk çok yaygın bir durumdur. Devletlerarasındaki bu casusluk olayları, günümüzde siber uzayda gerçekleştirilen faaliyetler üzerinden devam etmektedir (Erendor ve Tamer, 2018: 59). Günümüzde hemen hemen her şeyin dijitalleştiği gerçeği göz önüne alındığında, casusluk faaliyetlerinin de bilişim sistemleri kullanılarak yapılıyor olması, siber güvenliğe duyulan ihtiyacı daha da artırmaktadır.

Teknolojinin tarihi süreç içerisindeki gelişimi, beraberinde siber suçların daha da etkin bir şekilde artmasını sağlamıştır. Özellikle 2000'den sonra devlet destekli bir görünüm kazanan siber suçlar, uluslararası ilişkilerde etkin bir araç konumuna gelmiştir. Siber tehditlerin devletler arasında bir kriz boyutuna ulaşmasının sonucunda, devletler siber alan üzerinde bir hakimiyet kurmak istemektedirler (Güngör ve Güney, 2017: 138). Bu hakimiyet mücadelesi, devletleri birtakım çalışmalar içerisine sokmaktadır. Siber tehditlerin bu kadar artması ve etkili bir hal alması, devletlerin siber güvenliğe dönük stratejiler geliştirmesini zorunlu kıldığı gibi, özel kuruluşların bile bünyelerinde bilişim teknolojileri uzmanlarına yer vermesine neden olmaktadır (Güleç ve Kişman, 2021: 133-134).

Uluslararası ilişkilerde tek aktör olarak sadece devletler yer almadığı gibi, siber güvenlik alanındaki faaliyetler de sadece devletler tarafından yürütülen faaliyetlerden ibaret değildir. Özellikle Avrupa Konseyi, G8, BM ve NATO gibi uluslararası kuruluşlar da siber güvenlik alanında çeşitli stratejiler benimsemektedirler (Güleç ve Kişman, 2021: 134). Devletlerin yanı sıra uluslararası aktörlerin de siber alanda bir çeşitlilik oluşturması, siber güvenliği uluslararası politikada etkili bir araç haline getirmektedir (Güntay, 2018: 80).

Siber güvenliği bu kadar değerli kılan esas nokta, sahip olunan siber güçtür. Siber gücün savaştan ticarete kadar birçok alanda etkili olması (Nye, 2010: 5), siber güvenliğin uluslararası ilişkiler bağlamında hem değerini hem de nasıl etkili bir araca dönüşebileceğini göstermektedir. Siber güvenliğin, ulusal ve uluslararası güvenlikle örtüşmesi (Çelik, 2018: 112) ve tüm politik ve askeri çatışmaların siber boyutunun da olması (Erendor ve Tamer 2018: 59), siber güvenliğin uluslararası alanda ekili bir araca dönüşmesinde önemli faktörlerdir.

Siber güvenliğin önemini kavrayabilmek için öncelikle siber uzayın neyi ifade ettiğinin bilinmesi gereklidir. Kavramsal çerçevede bahsedildiği üzere siber uzay, bütün bilişim sistemlerini ve kullanıcılarını kapsayan ve fiziksel olmayan evrene verilen isimdir (Bıçakcı, 2014: 106). Siber uzayın bu denli büyük bir alanı kapsıyor olması, bu alanda yer alan kullanıcıların her türlü siber suçu veya saldırıyı gerçekleştirebileceklerini göstermektedir. Bu suçların ya da saldırıların siber terörizm ve savaş boyutuna ulaşması dikkate alındığında, siber güvenliğin gerekliliği ve önemi daha da anlaşılmaktadır. Siber uzayın en büyük özelliği, siber uzayda eylem gerçekleştiren aktörlerin anonim kalabilmesini sağlamasıdır (Kotik, 2015: 36). Bu durum, gerçekleştirilen eylemlerin sonucunda, devletler arasında diplomatik gerilim ya da krizlerin doğmasına sebebiyet verebilmektedir. Devletler arasında bu tür olumsuzluklar olabileceği gibi, siber güvenlik noktasında uluslararası bir işbirliğinden de söz etmek mümkündür.

Teknolojideki ilerleme devletlerin sahip oldukları konvansiyonel silahları daha da etkili hale getirdiği gibi, bilişim alanındaki gelişmeler ile yazılım ve programların da silah olarak kullanılabileceğini göstermektedir (Çelik, 2013: 137). Siber uzayın konuşulduğu ve tartışıldığı günümüzde, siber müdahale araçları olarak siber saldırı silahları ve yöntemleri geliştirilmiştir (Güntay, 2018: 81).

3.1. Genel Olarak Siber Silahlar

Saldırı amaçlı siber kabiliyet edinmemin ilk yolu bir siber silah edinmekten geçmektedir (Peterson, 2013: 2). Bilişim sistemlerine zarar verebilecek genel yazılım ve programlar; Botnet, Dos Saldırısı, mantık bombası, solucan, Truva atı ve virüsler gibi vb. diğer zararlı yazılım ve programlar siber saldırı silahları olarak tanımlanabilmektedir (Çelik, 2013: 141).Siber güvenliği tehdit eden bu zararlı yazılım ve programları biraz

daha açarak incelemek, ne tür silahlar olduklarını görmek açsından önemlidir. Yıldız'a göre bazı siber silahları şu şekilde tanımlamak mümkündür (2014: 9-48);

- **Sniffing:** Kelime anlamı koklamak olan sniffing, bir ağda yer alan bilgisayarlar arasındaki veri trafiğinin dinlenmesidir. Burada ki mantık bilgisayarlar arasındaki tüm verilerin yakalanarak saklanmasıdır. Korsanların yaygın bir şekilde kullandığı bu yöntemden korunmanın yolu, bilgisayarlar arasındaki bağlantıların şifreli hale getirilmesidir (Yıldız, 2014: 9-10).
- **Hizmet Dışı Bırakma:** DoS (Denial of Service), sunulan bir hizmetin aksaması ya da tamamen kesilmesi anlamını taşımaktadır. Bu yöntemde saldırgan kimliğini gizleyebildiği için tespiti zor bir hal almaktadır.
- **Arka Kapı (Backdoor):** Sadece saldırganın bildiği ve sistemdeki kimlik kontrol mekanizmasını devre dışı bırakarak karşıdaki sisteme uzaktan erişime imkan tanıyan bir kanaldır. Birçok virüs bulaştığı sistemde mutlaka arka kapı açmayı denemekte ve arka kapılar virüs yayıncısı için sisteme erişim imkanı sağlamaktadır.
- **Oltalama (Phishing):** Online dolandırıcılık olarak bilinen phishing yöntemindeki temel amaç, internet kullanıcısını kandırarak kredi kartı ve banka hesap bilgileri gibi gizili bilgilere erişim sağlamaktır.
- **Rootkitler (Kök Kullanıcı Takımı):** Bilgisayarda çalışan işlemleri veya sistem bilgilerini işletim sisteminden gizlemek suretiyle varlığını gizli bir şekilde devam ettiren zararlı programlara verilen isimdir.
- **Casus Yazılım (Spyware):** Bu programlar, internet ortamındaki kullanıcıların karşısına bedava şeklindeki reklamlar yoluyla çıkmaktadır. Kullanıcıların kendi bilgisayarlarına indirip kullandıkları bu programlar, kuruldukları bilgisayarlardaki bilgileri kendisini oluşturan kişiye göndermektedir.
- **Virüs:** Virüs, genellikle zararlı yazılımları kapsayan bir ifade olarak kullanılsa da bu yanlış bir tanımdır. Her zararlı yazılım virüs değildir. Virüs, kendi kendine çoğalabilen ve içinde gizlendiği program çalıştırıldığında sisteme yayılan bir zararlı yazılım türüdür.
- **Truva Atı (Trojen):** Faydalı bir işleve sahipmiş gibi görünen, fakat sistemdeki güvenlik mekanizmalarını aşabilecek fonksiyona sahip bir zararlı programdır.
- **Solucanlar (Worms):** Solucanlar da virüslerde olduğu gibi bir cihazdan diğerine kendisini kopyalayabilen yazılımlardır. Bilgisayarda dosya ya da veri transferi yapan fonksiyonların denetimini ele geçirip kendi kendilerine büyük miktarlarda çoğalabilmektedirler.
- **Zombi Ordular (Botnetler):** Zombi bilgisayarlar ya da botnetler, siber silahların en tehlikeli olanlarındandır. Burada dikkat çeken nokta, bilgisayar kullanıcısının haberi olmadan bilgisayarının işlenen suçlara alet edilmesidir. Bu tür bilgisayarlar robot veya bot olarak ifade edilmektedir. Botnetin bir paçası haline getirilen bilgisayarlar, örneğin bir web siteyi hizmet veremez bir hale getirebilmektedir
- **Klavye işlemlerini kaydeden programlar (Keyloggers):** Bu programlar, klavyede basılan her tuşu kaydetmekte ve programı kullanan kişiye bunları göndermektedir. Bankacılık işlemlerinde klavyeden şifre girilmesi ya da internette yapılan alışverişlerde kredi kartı bilgilerinin tuşlanması gibi vb. işlemlerde bu bilgileri kaydederek suçu işleyen ilgili kişiye göndermektedir.

Siber saldırı için kullanılan bu silahlar ve yöntemler gün geçtikçe daha da artmakta ve çeşitlenmektedir. Siber saldırılar, kullanıldıkları olaylara göre daha makro boyuta sahip sonuçlar doğurabilmektedirler. Örneğin 1992'de savaş başlamadan önce, ABD'nin Irak devletinin telekomünikasyon altyapısını çökerterek Iraklı askeri birlikler arasındaki bütün iletişimi tek tuşla kesmesi, siber saldırı gücünün ne boyutlara ulaşabileceğini göstermiştir.

3.2. Siber İstihbarat ve Casusluk

İstihbarat; dış politikayı şekillendiren ve ona göre uygulama yapılmasını sağlayan yabancı ülkelere ait bilgilerin toplanması ve işlenmesi adına yurt dışında gizli bir şekilde yürütülen faaliyetlerdir (Warner, 2002: 19). İstihbarat faaliyetlerine nitelik katan özellik gizliliktir. Casusluk da istihbaratı gizlilik içerisinde yapabilmenin kadim bir yoludur. Bütün bu faaliyetlerin temel çıkış noktası, devletlerin taşımış olduğu güvenlik kaygılarıdır. Bu güvenlik kaygısı siber alanı da kapsayan bir durumdur. Siber güvenliği sağlamak için de siber istihbarata ihtiyaç duyulmaktadır. Siber istihbarat, siber alandaki verilerden istihbarat oluşturma çalışmalarıdır (Karasoy,

2022: 233). Siber istihbaratta bilgiye erişim ve bilgiyi işlemek için iç ağlar, güvenlik cihazları ve sosyal medya platformları gibi vb. bütün networklardan yararlanılmaktadır (Mangır ve Küçükkırlı, 2019: 299).
Siber istihbarat, dijital cihazlara izinsiz bir erişim ile casusluk şeklinde yapılabileceği gibi, erişime açık kaynaklardan veri toplama şeklinde de yapılabilmektedir (Karasoy, 2022: 233). Bu bağlamda siber casusluk, yasadışı bir şekilde iletişim ağları ve bilgisayar sistemlerine erişerek, karşı grup ya da devlete ait gizli bilgilerin ele geçirilmesi eylemi olarak da nitelendirilebilir (Güntay, 2018: 89). Siber istihbaratın gerçekleşme şekli, bir ülkenin bilgisayar sistemlerine yönelik saldırı olabileceği gibi, ülkede enerji ve bankacılık gibi hizmet sunan kritik alanlara karşı yapılacak saldırılar da olabilir (Karasoy, 2022: 234). Bu durumda siber istihbarat faaliyetleri, siber saldırı silahları kullanılarak yapılmaktadır.

3.3. Siber Tehditler ve Savunma

Günümüzde internet sadece iletişim amaçlı kullanılan bir alandan ziyade, birçok dijital işlemin gerçekleştirilebildiği bir alan haline gelmiştir. Siber saldırı ve tehditlere karşı açık bir hedef olan internet, bu dönemde korunması gereken bir alana dönüşmüştür (Bıçakcı, 2014: 117). Koruması gereken ve kıymet verilen bir alanın doğal bir getirisi olarak, siber tehditlerin çeşitlenmesi ve artması da kaçınılmazdır. Bu bağlamda siber tehdit, bilişim teknolojileri kullanılarak bir toplumun iç ve dış düzenini muhafaza etme becerilerini kısmen veya tamamen yok etmek çabasıdır (Güntay, 2018: 92). Siber uzayın mesafe ve mekan gibi fiziki ortama bağlı değişkenlerden bağımsız olması durumu, siber tehditlerin hemen hemen her zaman ve her yerden gelebilmesine olanak tanımaktadır. Böyle bir durumda siber tehdit, sürekli olarak dikkat gerektiren ve buna karşılık siber savunma mekanizmalarının da sürekli devrede olması gereken bir ortamı zorunlu kılmaktadır.
Bilişim teknolojilerindeki ilerlemeyle beraber siber saldırı potansiyelinin artması, devletlerin bu alana dönük doktrinler üretmesine ve siber savunma kabiliyetlerini geliştirerek önlem almalarına sebep olmuştur (Yayla, 2014: 185). Bilişim teknolojilerinin kamusal alanda birçok özel ve kamusal hizmetin sunumun da bu denli etkin bir şekilde kullanılması, devletleri, siber güvenliği sağlamak adına caydırıcı tedbirler almaya yöneltmektedir. Siber tehditlere karşı siber savunma politikaları ve mekanizmaları geliştirmek, bu gerekliliğin bir sonucudur.

4. Türkiye'nin Siber Güvenlik Politika Uygulaması USOM

Siber uzay, bireysel olarak hem kullanıcıların hem de devlet bazında ulus devletlerin siber güvenliğe yönelik önlem almaları gereken bir alandır. Bu konuda en çok sorumlu olan taraf ise, ulus devletlerin kendisidir. Bu sorumluluğun bir gereği olarak, devletler siber güvenlik için birtakım politikalar üretmekte ve bu doğrultuda da çalışmalar yürütmektedirler. Söz konusu durum Türkiye için de geçerlidir. Nitekim bu doğrultuda siber suçlar ilk kez 6 Haziran 1991 tarihinde çıkarılan 3756 sayılı Türk Ceza Kanunu'nun Bazı Maddelerinin Değiştirilmesine Dair Kanun'da yer almıştır. Böylelikle siber faaliyetler, ceza kanununda suç unsuru hüviyetini kazanmıştır. Yapılan şeyin hukuk aleminde suç sayılması ve yaptırımlara tabi olabilmesi için kanunda suç olarak yer alması zorunluluğu, yasadışı siber faaliyetlerin ceza kanununda yer almasını sağlamıştır. Bu doğrultuda devlet, siber uzayın suç teşkil edecek faaliyetler için kullanılması hususuna odaklanmıştır (Bıçakcı vd., 2015: 4). Hukuk devleti olmanın bir gereği olarak, siber suçlar için gerekli düzenlemeler ile hukuki alt yapı oluşturulmaya başlanmıştır. 2004 Tarihli 5237 sayılı Türk Ceza kanunu ile siber suç tanımı genişletilmiş ve 2006'da yapılan değişiklik ile siber suçlar 3713 sayılı Terörle Mücadele Kanunu'na dahil edilmiştir (Bıçakçı vd., 2015: 4).
Siber güvenliği sağlama adına sadece hukuki düzenlemeler yeterli olmamaktadır. Siber uzayın fiziki sınırlarının olmaması ve bilişim teknolojilerinin hayatın her alanında yer alamsı, siber suçlara karşı daha kapsamlı bir mücadeleyi mecbur kılmaktadır. Daha kapsamlı bir mücadele için farklı politikalar belirlemek ve çalışmalar yürütmek, devletin asli görevlerindendir. Siber suçlara karşı daha kapsamlı bir mücadele için kamu kurumları, Türkiye'nin siber uzaydaki varlığı ve bu alanda kamu hizmetlerinin nasıl sağlanacağı konusunda aktif politikalar üretmeye başlamışlardır (Bıçakcı vd., 2015: 5). Bu bağlamda Devlet Planlama Teşkilatı'nın yayımladığı bazı politika belgeleri şunlardır; "e-Türkiye Girişimi Eylem Planı-2022", "e-Dönüşüm Türkiye Projesi Kısa Vadeli Eylem Planı (2003-2004)", "e-Dönüşüm Türkiye Projesi Eylem 2005 Planı", "Bilgi Toplumu Stratejisi (2006-2010)" ve "Bilgi Toplumu Stratejisi Eylem Planı (2006-2010)" (Şentürk vd., 2012: 116). 2006-2010 dönemini kapayan eylem planı; siber güvenliğe yönelik tehditlerin takibi, bu konuda uyarılar

yayınlaması ve alınacak önlemler kapsamında bilgilendirme ve koordinasyonu sağlaması için Bilgisayar Olaylarına Acil Müdahale Merkezinin kurulacağını belirtmiştir (Bıçakcı vd., 2015: 5). Bütün bu politika belgeleri, Türkiye'nin siber güvenlik konusundaki çalışmalarını nasıl planladığını ifade eden önemli göstergelerdir. Bu konuda planlama yaparak bilgilendirme ve koordinasyon merkezi oluşturmak, Türkiye'nin devlet nezdinde siber güvenliğe verdiği önemi de göstermektedir.

Siber güvenliği sağlayacak politikalar kadar bu politikaları uygulayacak olan kurumsal yapı da bir o kadar önem arz etmektedir. Türkiye'de siber güvenliği tesis edecek ve sürdürecek olan kurumsal yapılar, döneme ve izlenen politikaya göre farklılık göstermektedir. Türkiye'de siber güvenlik çalışmaları 2012 yılına kadar Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) tarafından yürütülmüştür. Bakanlar Kurulu'nun 11/6/2012 tarihli ve 3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Kararı" sonucunda, o dönemdeki adıyla Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na devredilerek bu alanda Siber Güvenlik Kurulu oluşturulmuştur (Yılmaz ve Sağıroğlu, 2013: 329). Kurulun amacı; siber güvenliğe ilişkin alınacak önlemleri belirlemek, hazırlanan plan, program, usul, esaslar ve standartları onaylayarak bunların uygulanması ve koordinasyonunu sağlamaktır (3842 Sayılı Karar, 4. madde). Kurul; Ulaştırma, Denizcilik ve Haberleşme Bakanının (UDHB) başkanlığında Dışişleri, İçişleri Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme Bakanlıkları Müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, Milli istihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muharebe Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı, Mali Suçlar Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ve UHDB Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşmaktadır (3842 Sayılı Bakanlar Kurulu Kararı, 4. madde). Siber Güvenlik Kurulu, ulusal çapta siber güvenliğin sağlanmasının sadece bir kamu kurumu tarafından değil, bütün kamu kurumlarının katılımıyla sağlanabileceğini göstermektedir (Kurnaz ve Önen, 2019: 87).

3842 Sayılı kararın yanı sıra, 20/10/2012 tarihindeki bir diğer Bakanlar Kurulu Kararı olan 28744 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" ve 5809 sayılı Elektronik Haberleşme Kanunu gereğince ulusal siber güvenliğin sağlanmasına yönelik politika, strateji ve eylem planlarını hazırlamak ve koordinasyonu sağlamakla yetkili kurum, Ulaştırma Denizcilik ve Haberleşme Bakanlığıdır (UAB, 2016: 5). 2018 yılında Cumhurbaşkanlığı Hükümet Sistemi'ne geçişle birlikte UDHB, Ulaştırma ve Altyapı Bakanlığı (UAB) olarak yeniden düzenlenmiş ve siber güvenlik kurulu başkanlığı devam etmiştir. 2012 Tarihindeki bu çalışmaları takip eden diğer çalışmalar; Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ve 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'dır.

Türkiye'nin ulusal siber stratejisi açısından önemli olan bir diğer yapı, Ulusal Siber Olaylara Müdahale Merkezi'dir. Bu yapı, siber alanda ortaya çıkacak tehditlere karşı siber güvenliği sağlamak adına faaliyet yürütmektedir. Oluşum sürecine bakıldığında, 2013/4890 sayılı Bakanlar Kurulu Kararı ile "2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" kapsamında, Türkiye'de siber güvenliğine karşı siber ortamda ortaya çıkan tehditlerin belirlenmesi, muhtemel siber saldırıların etkilerinin azaltılması veya ortadan kaldırılması için önlemlerin geliştirilmesi ve ilgili aktörlerle paylaşılması amacıyla Bilgi Teknolojileri ve İletişim Kurumu bünyesinde 27/05/2013 tarihinde Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) oluşturulmuştur (USOM, 2023). USOM'un yanı sıra, 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı kamu kurum ve kuruluşları bünyesinde Siber Olaylara Müdahale Ekipleri (Kurumsal SOME, Sektörel SOME) oluşturulmasını sağlamıştır (USOM, 2023). USOM ve SOME'ler siber olayları bertaraf etmede, oluşması muhtemel zararları önlemede ve siber olayların yönetim koordinasyonun ulusal düzeyde ve işbirliği içerisinde gerçekleştirilmesinde hayati öneme sahip yapılar olarak ulusal siber güvenliğimize önemli bir katkı sağlamaktadır (USOM, 2023).

Siber tehditleri azaltmak ve bertaraf etmek amacıyla, 5809 sayılı Elektronik Haberleşme Kanununun verdiği yetkiler çerçevesinde Ulusal Siber Olaylara Müdahale Merkezi şu görevleri yerine getirmektedir (USOM, 2023);

- Türkiye'deki siber olaylara müdahale hususunda ulusal ve uluslararası koordinasyon çalışmalarını 7/24 çalışma biçimine göre yürütmek.

- Tespit edilen siber tehditlere karşın ilgili tarafları veya ülke çapında uyarı ve duyurular yaparak, yaşanması muhtemel olayların etkilerinin azaltılması ya da tamamen ortan kaldırılmasına yönelik önlemler geliştirmek.
- Siber saldırılara maruz kalan bilişim sistemleri için koruyucu tedbirler alma hususunda faaliyette bulunmak.
- Yapılan çalışmalar esnasında konusu suç teşkil eden bulgulara ulaşılması halinde, adli makamlar ve kolluk kuvvetleriyle koordineli bir şekilde çalışmak.
- USOM tarafından hazırlanan yerli ve milli SOME İletişim Portalı (SİP) üzerinden Türiye'nin siber güvenlik organizasyonunda yer alan Sektörel ve Kurumsal SOME'lere gerekli bildirimler, duyurular. Alarmlar, mesajlar ve ihbarlar gönderilir.
- USOM'a gelen ihbarlar incelenip değerlendirilerek gerekli aksiyonlar alınır veya aldırılır.
- Oltalama, zararlı yazılım ve port taraması gibi zararlı olduğu tespit edilen internet sitelerine erişim engellemesi yapılarak, etkilerinin azaltılması ve ortadan kaldırılması sağlanmaktadır.

USOM'u sadece belirtmiş olduğumuz bu görevler çerçevesinde değerlendirmek, siber güvenlik konusunda üstlenmiş olduğu rol itibariyle dar kapsamlı bir tanımlamaya sebebiyet verecektir. USOM, Türkiye'deki bütün kamu kurumları, özel sektör kuruluşları, internet servis sağlayıcıları ve diğer internet aktörleri ile çalışma yapma; Sektörel ve Kurumsal SOME'lere, üniversitelere ve siber güvenlik topluluklarına yönelik siber güvenlik eğitimi faaliyetinde bulunma; ulusal ve uluslararası sivil, askeri siber güvenlik tatbikatlarına, NATO tatbikatlarına ve konferanslar ve çalıştaylara katılma yetkilerine de sahiptir (USOM, 2023). USOM'un siber güvenliğe yönelik uluslararası tatbikat ve organizasyonlarda bulunabilmesi, bu yapının, Türkiye'nin siber güvenlik stratejisi için ne denli kritik bir rol üstlendiğini göstermektedir. USOM'un NATO'nun siber güvenlik tatbikatlarında bulunabilmesi, kıymetli kabiliyete sahip bir yapı olduğunun göstergesidir.

USOM, Bilgi Teknolojileri ve İletişim Kurumu bünyesinde 27/05/2013 tarihinde oluşturularak faaliyete başlamış, fakat resmi açılışı 10/02/2020 tarihinde Cumhurbaşkanı Recep Tayyip Erdoğan tarafından yapılmıştır. USOM'un siber saldırılara karşı kullanmış olduğu yazılımlar ise, tamamen yerli ve milli olan AVCI, AZAD, KASIRGA gibi yazılımlardır (USOM, 2023). Siber güvenliği sağlamada kullanılan yazılımların yerli ve milli olması, hem USOM'u daha etkin kılmakta hem de Türkiye'nin uluslararası alandaki imajını ve gücünü artırmaktadır. USOM, CNA (CVE Numbering Authorities) kabul sürecini başarılı bir şekilde tamamlayarak, CVE (Common Vulnerabilities and Exposure) Programı tarafından CVE Topluluğuna kabul edilmiştir (USOM, 2023). CVE Programı, siber güvenlik için ortak tanımlayıcılar sağlayan güvenlik zafiyetlerinin yer aldığı listedir. CVE tanımlayıcıları veya CVE numaraları, sistemleri saldırılara karşı korumak amacıyla kullanılan güvenlik açığı bilgilerinin hızlı bir şekilde keşfedilmesine imkan tanımaktadır (USOM, 2023). Böylece Türkiye'de üretilen yazılımlarda, donanımlarda veya ürünlerde tespit edilen güvenlik açıkları USOM tarafından üretici firmalara bildirilmekte ve yapılan koordinasyonların sonucunda da gerekli aksiyonlar alınarak giderilmektedir (USOM, 2023).

Türkiye, Global Siber Güvenlik Endeksine göre, siber güvenlik alanında Avrupa'da 6'ncı, dünyada ise 11'incisırada yer almaktadır (USOM, 2023). Bu bilgiler, Türkiye'nin siber uzayda nasıl bir konumda olduğunu göstermekle beraber, bu alanda erişmiş olduğu gücü de ifade etmektedir. USOM'un, siber güvenlik alanında ülkeye kazandırmış olduğu bu kabiliyet, Türkiye'nin uluslararası politikada pazarlayabileceği bir yetenektir. Türkiye'nin siber güvenlik alanındaki bu yeteneği, devletlerarası ilişkilerde de kullanılabilecek etkin bir araçtır.

5. Sonuç

Günümüz dijitalleşen dünyasında birçok kamusal hizmetin siber alana taşınması, bu alanın korunmasına yönelik devletlere kritik bir misyon yüklemektedir. Bu misyonundaki önemli bir nokta ise, bu alan üzerinden sunulan hizmetlerin bir süreklilik arz etme zorunluluğudur. Hizmetlerde bir aksama olmaması ve süreklilik sağlanması adına siber alanı korumak için siber güvenliğe ihtiyaç duyulmaktadır. Teknolojideki gelişmelerin sadece kamusal hizmetlerin sunumunda değil, ayrıca askeri alanda da kullanılması siber güvenliğin önemini daha da artırmaktadır. Siber güvenliği sağlanabilmesi ise, siber uzay denilen alemde sahip olunun güce bağlıdır. Siber uzayın fiziki sınırlarının olmaması, siber güvenliğe tehdit oluşturabilecek her türlü siber saldırının her yerden gelebilme ihtimalini yükseltmektedir. Bu saldırılar basit siber suçlar olabileceği gibi siber terörizm ya da siber savaş gibi makro boyutlara da sahip olabilir. Farklı ölçütlere sahip bu siber saldırılar birçok siber silah

ve yöntemle gerçekleştirilmektedir. Bunlardan öne çıkan bazı silah ve yöntemler virüsler, casus yazılımlar, truva atları, tuş dinleyiciler, solucanlar ve botnetler gibi benzerleridir. Bu durumda siber güvenliği sağlamak, kapsamlı politikalar üretmek ve bu politikaları uygulamaktan geçmektedir.

Siber uzayın sınırının olmaması ve siber saldırıların her yerden gelebilmesi, söz konusu ülke güvenliği olduğunda uluslararası krizlere de sebebiyet verebilmektedir. Böyle bir durumda kendi siber güvenliğini sağlayabilmek önemli bir kabiliyettir. Bu kabiliyet, aynı zamanda uluslararası ilişkilerde politik bir güçte sağlamaktadır. Siber güvenliği uluslararası politika da etkili bir araç yapan tek faktör sadece zarar verme amaçlı saldırılar değildir. Siber saldırılar ile Siber istihbarat ve casusluk faaliyetlerinde bulunmak da siber güvenliği etkili bir araç yapmaktadır. Siber güvenliğin uluslararası bir etki aracı olması, Türkiye'nin bu alanda gerekli çalışmaları hızlı bir şekilde yapması için itici bir etken olmuştur.

Türkiye'de siber güvenliğe ilişkin ilk çalışmalar hukuki altyapı oluşturularak başlanmıştır. Siber suçlar ilk kez 6 Haziran 1991 tarihinde çıkarılan 3756 sayılı Türk Ceza Kanunu'nda yer almıştır. Akabinde 2004 Tarihli 5237 sayılı Türk Ceza kanunu ile siber suç tanımı genişletilmiş ve 2006'da siber suçlar 3713 sayılı Terörle Mücadele Kanunu kapsamına alınmıştır. Hukuki çalışmaların yanı sıra, 2012 yılına kadar TÜBİTAK'ın görev alanı olarak belirlenen siber güvenlik çalışmaları, bu tarihten sonra Bakanlar Kurulu kararları ve 5809 sayılı Elektronik Haberleşme Kanunu gereğince Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na devredilmiştir. Bakanlı bünyesinde kurulan Siber Güvenlik Kurulu; içerisinde birçok bakanlık müsteşarı, kurum ve kuruluş ile siber güvenlik konusunda bütüncül bir yapı özelliği sergilemiştir. Siber Güvenlik Kurulu'nun ilk ve ikinci toplantısı arasındaki altı aylık süreçte USOM kurulmuş ve 2013 tarihinde faaliyete başlamıştır. USOM, üstlenmiş olduğu görevler itibariyle siber güvenliği sağlama hususunda Türkiye'deki en etkili yapıdır. USOM'un siber güvenliğe yönelik uluslararası koordinasyon görevini de icra ediyor olması, sadece ulusal bazda değil uluslararası alanda da etkin bir yapı olduğunu göstermektedir. USOM'un NATO gibi güçlü bir askeri ittifakın siber güvenlik tatbikatlarında yer alacak kapasitede olması, USOM'un ne kadar etkili bir aktör olduğunu göstermektedir. Bu durum, Türkiye'nin uluslararası politikada siber güvenlik gibi güçlü bir araca sahip olduğu gerçeğini yansıtmaktadır. Bu gerçeği kanıtlar nitelikte olan bir diğer önemli bilgi ise, Global Siber Güvenlik Endeksi verileridir. Endekse göre, Türkiye siber güvenlik alanında Avrupa'da 6'ncı dünyada ise 11'inci sırada yer almaktadır. Bu veriler, aynı zamanda siber güvenliğin uluslararası politika da nasıl etkili bir araç olduğunu göstermekle beraber, USOM'un alanında ne kadar güçlü bir yapı olduğunu da göstermektedir.

Kaynaklar

Andress, J. and Winterfeld, S. (2011). *Cyber warfare: Techniques, tactics and tools for security practitioners.* ABD: Elsevier.

Bıçakcı, S. (2014). NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik. *Uluslararası İlişkiler Akademik Dergi, 10*(40), 101-130.

Bıçakcı, S., Çelikpala, M. ve Ergun, D. (2015). Türkiye'de Siber Güvenlik, EDAM Siber Güvenlik Kağıtları Serisi. Sayı: 1, 1-35. https://edam.org.tr/wp-content/uploads/2015/12/EDAM_TR_Siber_Guv_1.pdf.

Calderaro, A. and Craig, A. J. S. (2020). Transnational Governance of Cybersecurity: Policy Challenges and Global İnequalities in Cyber Capacity Building. *Third World Quarterly, 41*(6), 917–938. https://doi.org/10.1080/01436597.2020.1729729

Campbell-Kelly, M. and Garcia-Swartz, D. D. (2013). The History of the İnternet: The Missing Narratives. *Journal of Information Technology (Sage Publications Inc.), 28*(1), 18-33. https://doi.org/10.1057/jit.2013.4

Çelik, S. (2021). *Küreselleşme sürecinde değişen güvenlik algısı: Siber güvenlik örneği*. (Yayınlanmamış doktora tezi). Süleyman Demirel Üniversitesi Sosyal Bilimleri Enstitüsü Uluslararası İlişkiler Ana Bilim Dalı, Isparta.

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

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

Çiftci, H. (2017). *Her yönüyle siber savaş.* Ankara: TÜBİTAK Popüler Bilim Kitapları.

Dale, P. (2013). Offensive Cyber Weapons: Construction, Development and Employment. *The Journal of Strategic Studies, 36*(1), 120-124, https://indianstrategicknowledgeonline.com/web/Offensive%20Cyber%20Weapons.pdf.

Denning, P. J. (1989). The Science of Computing: The Internet Worm. *American Scientist, 77*(2), 126–128. from JSTOR: https://www.jstor.org/stable/27855650

Erendor, M. E. ve Tamer, G. (2018). The New Face of The War: Cyber Warfare. *Cyberpolitik Journal, 2*(4), 57-74.

Gams, M. (2013). Alan Turing, Turing Machines and Stronger. *Informatica* (03505596), *37*(1), 9–14.from: https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=e5h&AN=90449673&site=eds-live

Güleç, Ö. ve Kişman, Z. A. (2021). Uluslararası İlişkiler Açısından Siber Güvenlik ve NATO'nun Siber Güvenlik Stratejileri. *Akademik Açı, 1*(1), 127-154.

Güngör, U. ve Güney, O. (2017). Uluslararası İlişkilerde Güvenliğin Dönüşümü Çerçevesinde Bilgi Güvenliği ve Siber Savaş. *Karadeniz Araştırmaları, 14*(55), 131-146.

Güntay, V. (2018). Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler. *Güvenlik Stratejileri Dergisi, 14*(27), 79-111.

İduğ, Y., Çalışkan, F. ve Güler, T. (2013). Siber caydırıcılık ve Türkiye'nin siber imkân ve kabiliyeti. *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı* içinde (s.287-290). Ankara: Bilgi Güvenliği Derneği Bildiriler Kitabı.

Joseph S. Nye, Jr. (2010). Cyber power. https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf

Karasoy, H. A. (2022). Yeni Nesil Savaş ve Siber İstihbarat. *Güvenlik Bilimleri Dergisi, 11*(1), 223-240.

Kaspersky. (2023). What is wannacry ransomware?. (Erişim: 09.01.2023), https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

Keleştemur, A. (2015). *Siber İstihbarat.* (1. Baskı). İstanbul: Yazın Basın Yayınevi.

Kramer, F. D., Starr, S. H. and Wentz, L. K. (2008). Towards a (Preliminary) theory of cyberpower. https://apps.dtic.mil/sti/pdfs/ADA486839.pdf.

Kurnaz, S. ve Önen, S. M. (2019). Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Stratejileri. *International Journal of Politics and Security, 1*(2), 82-103.

Mangır, D. Ş. ve Küçükkırlı, S. N. (2019). Gelenekselden Dijitale Siber İstihbarat ve Rus Dış Politikası. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* (Prof. Dr. Fuat Sezgin Özel Sayısı), 296-308.

Mareşi, N. C. (2020). Information in Cyberspace - Actuality and Challenges. *Strategic Impact, 76*(3), 76-88. Retrieved November 1, 2021, from Central and Eastern European Online Library: https://www.ceeol.com/search/article-detail?id=913126

NATO. (2016). Warsaw summit communiqué. Press Release (2016) 100, Warsaw, 8-9 July 2016, from NATO: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

Nunes, R. C., Colomé, M., Barcelos, F. A., Garbin, M., Paulus, G. B. and Silva, L. A. D. L. (2019). A case-based reasoning approach for the cybersecurity incident recording and resolution. International Journal of Software Engineering and Knowledge Engineering, 29(11n12), 1607-1627'den Akt. Öztunç Yüsra Mizgin, 2022, ABD ve Türkiye'de Siber Güvenlik Politikalarının Karşılaştırmalı Analizi, Ufuk Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisan Tezi, Ankara.

Önok, M. (2013). Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 19*(2), 1229-1270.

Özfındık Kotik, Y. (2015). *Uluslararası ilişkilerde siber güvenlik algısı ve ulus devletin değişen stratejisi*. (Yayınlanmamış yüksek lisans tezi). Çukurova Üniversitesi Sosyal Bilimler Enstitüsü, Adana.

Sağıroğlu, Ş. ve Alkan, M. (2018). *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık.* Ankara: Grafiker Yayınları.

Shelburne, B. J. (2017). The ENIAC at 70. *Math Horizons, 24*(3), 26-29. https://doi.org/10.4169/mathhorizons.24.3.26

Stadnik, I. (2017). What İs An İnternational Cybersecurity Regime And How We Can Achieve İt?. *Masaryk University Journal of Law and Technology, 11*(1), 129-154. https://doi.org/10.5817/MUJLT2017-1-7

Şentürk, H., Çil, C. Z. and Sağıroğlu, Ş. (2012). Cyber Security Analysis of Turkey. *Internatıonal Journal of Informatıon Securıty Scıence, 1*(4), 112-125.

Turhan, O. (2006). Bilgisayar ağları ile ilgili suçlar (Siber Suçlar). Planlama Uzmanlığı Tezi, Ankara: Devlet Planlama Teşkilatı.

Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2016). Ulusal siber güvenlik stratejisi 2016-2019. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf

USOM (2023). https://www.usom.gov.tr/.

Warner, M. (2002). Wanted: A Defmition of Intelligence. *Studies in Intelligence, 46*(3), 15-22. https://apps.dtic.mil/sti/pdfs/ADA525816.pdf.

Winther, R., Gran, B. A. and Dahll, G. (2005). Computer safety, reliability, and security. *24th International Conference SAFECOMP*, Norveç: Fredrikstad.

Yang, S. C. and Wen, B. (2017). Toward a Cybersecurity Curriculum Model for Undergraduate Business Schools: A Survey of AACSB-Accredited İnstitutions in the United States. *Journal of Education for Business, 92*(1), 1-8.

Yayla, M. (2013). Hukuki Bir Terim Olarak Siber Savaş. *TBB Dergisi*, (104), 177-203. http://portal.ubap.org.tr/App_Themes/Dergi/2013-104-1247.pdf

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

Yıldız, M. (2014). *Siber sular ve kurum güvenliği*. Denizcilik Uzmanlık Tezi, Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (Erişim Tarihi: 20.12.2022). https://afyonluoglu.org/PublicWebFiles/Reports-TR/Akademi/Uzmanl%C4%B1k%20Tezi-2014%20Kas%C4%B1m-Avrupa%20Konseyi%20siber%20su%C3%A7lar%20s%C3%B6zle%C5%9Fmesi%20kapsam%C4%B1nda%20T%C3%BCrkiye%27nin%20g%C3%BCvenli%C4%9Fi.pdf

Yılmaz, S. ve Sağıroğlu, Ş. (2013). Siber saldırı hedefleri ve Türkiye'de siber güvenlik stratejisi. *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı* içinde (323-331).

3842 Sayılı Bakanlar Kurulu Kararı (2012). https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf. (Erişim Tarihi: 15.12.2022).

Etik, Beyan ve Açıklamalar

1. Etik Kurul izni ile ilgili;
☑ Bu çalışmanın yazar/yazarları, Etik Kurul İznine gerek olmadığını beyan etmektedir.

2. Bu çalışmanın yazar/yazarları, araştırma ve yayın etiği ilkelerine uyduklarını kabul etmektedir.

3. Bu çalışmanın yazar/yazarları kullanmış oldukları resim, şekil, fotoğraf ve benzeri belgelerin kullanımında tüm sorumlulukları kabul etmektedir.

4. Bu çalışmanın benzerlik raporu bulunmaktadır.