Uluslararası Yönetim Akademisi Dergisi
Yıl: 2023, Cilt: 6, Sayı: 1, ss.173-188

https://doi.org/10.33712/mana.1254015

Bombalardan Baytlara: Siber Güvenliğin Ulusal Güvenlikteki Rolü ve Yapay Zekânın Siber Güvenlikteki Önemi

From Bombs to Bytes: Role of Cyber Security in National Security and Importance of Artificial Intelligence in Cyber Security

Hasan Alpay KARASOY
Prof. Dr., Selçuk Üniversitesi, İİBF,
Siyaset Bilimi ve Kamu Yönetimi Bölümü,
dr.alpaykarasoy@gmail.com
https://orcid.org/0000-0002-3813-2960

Hikmet Salahaddin GEZİCİ
Dr. Öğr. Üyesi, Selçuk Üniversitesi, İİBF,
Siyaset Bilimi ve Kamu Yönetimi Bölümü,
hsgezici@gmail.com
https://orcid.org/0000-0003-1573-2864

Makale Başvuru Tarihi: 21.02.2023
Makale Kabul Tarihi: 20.03.2023
Makale Türü: Araştırma Makalesi

ÖZET

Bu çalışma, devletin siber ortamda depoladığı veri miktarının artması ve kamu hizmetlerinin giderek daha fazla siber ortam aracılığıyla sunulması nedeniyle siber güvenliğe; siber güvenliğin sağlanmasında ise gerekli hız, çeviklik ve esnekliği sağlayan bir araç olarak görülen yapan zekâya odaklanmaktadır. Çalışmanın amacı ise siber güvenliğin neden bir ulusal güvenlik bileşeni olduğunun ve yapay zekânın siber güvenlikteki öneminin araştırılması, siber güvenlik alanında ülke uygulamalarından örnekler sunarak bunlardan çıkarımlar yapılmasıdır. Literatür taraması yapılarak hazırlanan bu çalışma sonucunda kamu sektörünün (devletin) siber saldırılardan en çok etkilenen alan olduğu; siber saldırıların askeri gücün operasyon sahasına yansıtılmasını etkileyebileceği; siber saldırıların ve siber ortama artan bağımlılığın toplum ve devleti bir arada tutan "güven" duygusunu baltalayabileceği; günümüzde siber saldırılarda yapay zekâ kullanımının kısıtlı olduğu ancak gelecekte kullanımının artacağı öngörüsü nedeniyle geleceğin siber güvenliğinin yapay zekâ odaklı hale geleceği gibi hususların önem taşıdığı görülmüştür. Buradan hareketle siber saldırıların ulusal güvenliği tehdit edebilecek potansiyelinin bulunduğu ve siber güvenliğin bir ulusal güvenlik bileşeni olduğu anlaşılmaktadır. Çalışmanın sonuç bölümünde de ülkelerin siber güvenlik uygulamalarından hareketle siber güvenliğin sağlanmasına yönelik önerilere yer verilmiştir.

Anahtar Kelimeler:

Siber Ortam,

Siber Güvenlik,

Ulusal Güenlik,

Yapay Zekâ,

ABSTRACT

This study focuses on cybersecurity and artificial intelligence, which are considered essential tools for ensuring the necessary speed, agility, and flexibility in cybersecurity due to the increasing amount of data stored by governments in the cyber environment and the growing dependence on cyber infrastructure for public services. The aim of this study is to investigate why cybersecurity is a component of national security and the importance of artificial intelligence in cybersecurity, while also providing examples from country practices in the field of cybersecurity. The study, prepared through a literature review, revealed that the public sector (government) is the most affected by cyber-attacks, which can impact a country's military power and damage the trust between government and society. It also highlighted that cyber-attacks and increasing dependence on the cyber environment can sabotage the "trust" emotion that holds together government and community. Although the use of artificial intelligence in cyber-attacks is currently limited, it is expected to increase in the future, leading to an artificial intelligence-focused approach to cybersecurity. As a result, it is understood that cyber-attacks pose a potential threat to national security, making cybersecurity a crucial component. The study concludes by proposing measures to enhance cybersecurity based on country practices.

Keywords:

Cyber Environment,

Cyber Security,

National Security,

Artificial Intelligence,

Önerilen Alıntı (Suggested Citation): KARASOY, Hasan Alpay ve GEZİCİ, Hikmet Salahaddin (2023), "*Bombalardan Baytlara: Siber Güvenliğin Ulusal Güvenlikteki Rolü ve Yapay Zekânın Siber Güvenlikteki Önemi*", **Uluslararası Yönetim Akademisi Dergisi**, S.6(1), ss.173-188, Doi: https://doi.org/10.33712/mana.1254015

1. GİRİŞ

1990'lı yıllardan itibaren siber ortam (siber uzay-internet), ekonomileri, toplumları ve insanları giderek artan bir şekilde birbirine bağlamıştır. Günümüzde ise siber ortam vatandaşların adli, sağlık ve kimlik bilgileri gibi önemli verilerinin saklandığı; sağlık, bankacılık, eğitim, dijitalleşen ve birbirine bağlı hale gelen enerji altyapıları (kritik altyapılar) gibi devletin sunduğu ve toplumun düzen ve huzurunun devamı için gerekli olan birçok kamu hizmetinin gerçekleştirildiği bir ortam haline gelmiştir. Dolayısıyla günümüzde devletin siber ortama taşındığı söylenebilir. Siber ortama artan bu bağlılık devlet (ve tabi ki özel sektör) için kaynak israfının azalması ve hizmet performanslarının artması gibi bir takım avantajlar getirirken, siber ortamdaki verilerin ve siber ortam aracılığıyla faaliyette bulunan kritik altyapıların güvenliğini de ön plana çıkarmıştır. Çünkü siber ortamın tasarlanma amacı bilgiyi korumak değil, bilgiyi depolamak ve paylaşmaktır (Eggers, 2016:153).

Siber ortamdaki varlığının artması, başka bir ifadeyle siber ortama taşınması nedeniyle devletin siber güvenliğini sağlamak günümüzün en önemli önceliklerinden ve aynı zamanda zorluklarından bir tanesidir (Ardielli ve Ardielli, 2017). Bu öncelik ve zorluğun bir nedeni olarak kamu sektörünün özel sektörden daha fazla veri depolaması ve bu verileri özel sektöre göre daha zayıf bir şekilde koruduğuna yönelik yaygın kanaattir (Eggers, 2016). Öte yandan devletler açısından siber saldırıların maliyeti, özel sektöre göre çok daha fazla olmaktadır. Örneğin bireyler siber güvenlik alanında genelde maddi kayıplardan ve verilerinin kötüye kullanımından endişe duysa da (Ardielli ve Ardielli, 2017) devletin siber uzaydaki varlılarına (ve faaliyetlerine) yapılacak bir siber saldırı geniş çaplı elektrik kesintilerine, akaryakıt sevkiyatının aksamasına; yaşanan enerji kesintileri hastanelerin, okulların, fabrikaların ve bankacılık sisteminin sekteye uğramasına; seçimlerin manipülasyonuna ve halkın demokratik işleyişe ve yönetime duyduğu güvenin azalmasına neden olabilir.

Siber saldırıların bu potansiyel etkileri nedeniyle Amerika Birleşik Devletleri (ABD) eski Savunma Bakanı Panetta, yıkıcı siber saldırıların ABD için siber Pearl Harbor ve siber 11 Eylül etkisinden daha fazlasını meydana getirebileceğini ifade etmiştir. Siber saldırıların, ABD'yi İkinci Dünya Savaşı'na girmeye zorlayan Pearl Harbor baskını (7 Haziran 1941) ve 21.yüzyıl için güvenlik anlayışını biçimlendiren 11 Eylül 2001'deki saldırıların meydana getirdiği etki ile kıyaslanması, siber ortamın güvenliği demek olan siber güvenliğin ulusal güvenliğin bir parçası olduğuna işaret etmektedir. Dolayısıyla günümüzde bitler ve baytlar (*bilgisayarlarda kullanılan verileri ifade eden kavramlar*) mermiler ve bombalar kadar ulusal güvenlik açısından bir tehdit haline gelmiştir (Lynn, 2011).

Siber güvenliği tehdit eden siber saldırılarla başa çıkabilmek için ise dinamik bir yaklaşım gerekli olup artan veri miktarı, verilerin daha hızlı analiz edilmesini zorunlu kılmaktadır. Günümüzde siber saldırılara verilen yanıtların çoğunluğu ise önceden belirlenmiş, kalıplaşmış (eski, bilindik) tepkilere dayalı, aceleci ve bazı durumlarda saldırının kendisinden daha çok zarara neden olabilecek ani tepkilere dayanmaktadır (Booker ve Musman, 2020:1). İşte bu nedenle siber güvenlik alanında hızlı ve esnek hareket etmeye olanak tanıyan ve bu yönüyle siber güvenlik ile adeta yapışık siyam ikizi görünümü veren bir yardımcı ön plana çıkmaktadır: *Yapay zekâ*.

Yukarıda bahsedilen önemine binaen, kamu hizmetlerinin sunumu ve toplumun nizam ve intizam içerisinde işleyebilmesi adına önemi gün geçtikçe artan siber ortamın güvenliği anlamına gelen "*siber güvenlik*" ve siber güvenliğin sağlanması açısından ise geniş bir potansiyel barındıran "*yapay zekâ*" bu çalışmanın temel konularını oluşturmaktadır. Çalışmanın amacı da siber güvenliğin ulusal güvenlik açısından önemi ve oynadığı rolü araştırmak; yapay zekânın siber güvenlikteki yerini incelemek ve siber güvenlik alanındaki ülke uygulamalarından hareketle kamu sektörü için siber güvenliğin sağlanmasına yönelik çıkarımlarda bulunmaktır.

Siber güvenlik ve yapay zekâ konularında Türkçe literatürde yer alan çalışmaların geneli bilgisayar bilimine özgü jargon kullanımı fazla olan ve soyut yazılar olduğundan bir sosyal bilimci açısından anlaşılmasının güç olduğu düşünülmektedir. Siber güvenlik ve ulusal güvenliği birlikte konu edinen çalışmalar, siber güvenlik stratejilerinde insan haklarının nasıl işlediğini konu alan (Ünver, 2017); kritik altyapı ve siber alanın dirençliliğinin ulusal güvenlik üzerindeki yansımalarını konu edinen (Can, 2022); Fransa'nın ulusal siber güvenlik stratejisini inceleyen (Köker, 2022) gibi çalışmalardır. Bu çalışmanın ise ulusal güvenlik açısından siber güvenliğin neden önemli olduğunu detaylı bir şekilde ve somut örneklerle ele alması, siber güvenlik alanında ülke uygulamalarından dersler sunması ve bunlardan çıkarımlar yapması yönüyle siber güvenliğin daha iyi anlaşılmasına katkıda bulunacağı düşünülmektedir.

Konu ile ilgili literatür taranarak hazırlanan bu çalışma iki bölümden oluşmaktadır. İlk bölümde siber güvenlik kavramı, siber güvenliğin ulusal güvenlik açısından taşıdığı önem ve yapay zekânın siber güvenlikteki yeri incelenecektir. İkinci bölümde ise siber güvenlik alanındaki ülke uygulamalarından bahsedilecek ve bundan hareketle sonuç bölümünde bazı önerilere yer verilecektir.

2. SİBER GÜVENLİK KAVRAMI VE ULUSAL GÜVENLİK AÇISINDAN ÖNEMİ

Günümüzde ulusal güvenlik açısından siber güvenliğin önemine geçmeden önce, siber güvenlik kavramını ana hatlarıyla tanımak yararlı olacaktır.

2.1. Siber Güvenlik Kavramı

Siber güvenlik kavramı siber ortamın, bu ortamda faaliyet gösteren örgütlerin ve bu örgütlerin çalışanlarının (siber ortamdaki) varlıklarını korumak ve bu varlıkların güvenliğini sağlamak için kullanılan bir kavramdır (Singar ve Akhiles, 2020:251). Siber ortam (siber uzay olarak da ifade edilebilir) bilgileri depolamak, değiştirmek ve iletmek için kullanılan sanal bir ağdır (Hajoary ve Akhilesh, 2020:79). Siber ortamın misyonu insanların, mal ve hizmetlerin, sermayenin ve fikirlerin özgürce dolaşımına dayalı küresel bir ekonomi oluşturmak şeklinde ifade edilebilir (Ilves, 2013). Siber ortam ise bu misyonunu ancak güvenli olduğu zaman, başka bir ifadeyle siber güvenlik sağlandığı zaman yerine getirebilir. Günümüz itibarıyla bakıldığında gerek kamu sektöründe gerekse özel sektörde olsun bir örgüte ait bilgiler ve varlıklar siber ortamda muhafaza edilmekte ve işlenmektedir. Siber güvenlik, siber ortamdaki saldırılara karşı bu bilgilerin ve varlıkların güvenliğini sağlamaktır (Singar ve Akhiles, 2020:251-252).

Siber saldırı kavramından bahsetmeden önce siber güvenlik hakkında yapılmış bazı tanımlara yer vermek gerekirse "*siber güvenlik, bilgisayarların, ağların, verilerin ve programların izinsiz erişime karşı korunmasıyla ilgili bilgi güvenliğinin bir parçasıdır*" (Accenture, 2022a); "*siber güvenlik, ağları, cihazları ve verileri suç amaçlı kullanımdan ve yasa dışı erişimden koruma sanatı, [siber ortamdaki] bilgilerin bütünlüğünü, gizliliğini ve kullanılabilirliğini garanti etme uygulamasıdır*" (CISA, 2021). Bu tanımlara benzer bir tanım yapan Hajoary ve Akhiles (2020:79) de siber güvenliği "*bilgisayarların, ağların, verilerin ve programların bütünlüğünü kötüye kullanım amaçlı yetkisiz erişimlerden, hasarlardan ve saldırılardan korumaya yönelik bir savunma tekniği*" şeklinde tanımlamışlardır.

Siber güvenliği tehdit eden siber saldırı kavramı ise Patterson (2022)'un aktardığına göre, "*yetkisiz erişim yoluyla bilgisayar sistemlerindeki bilgileri ele geçirmeye, değiştirmeye, ifşa etmeye veya yok etmeye yönelik istenmeyen girişimler*" şeklinde tanımlanmaktadır. Siber saldırılar mesafe tanımamaktadır ve okyanuslar siber saldırılar için bir koruma sağlamaz. Siber saldırıların ayrıca etkileşim hızı yüksektir (roketlerden çok daha hızlı); maliyeti düşüktür; failini belirlemek zordur ve kolaylıkla inkâr edilebilir (Nye, 2021). Ayrıca siber saldırılar asimetrik bir tehdit özelliği taşımaktadır. Şöyle ki örneğin konvansiyonel (geleneksel) bir savaşta ABD gibi güçlü bir orduya saldırmak için uçak gemileri, gelişmiş füzeler ve son teknoloji savaş uçaklarına ihtiyaç duyulmaktadır. Ancak siber saldırılar için böylesi gelişmiş araçlara ihtiyaç yoktur. Birkaç kararlı bilgisayar programcısı bir siber güvenlik açığı buldukları zaman ABD'nin askeri operasyon planlarını ele geçirebilir veya istihbarat yeteneklerini zaafa uğratabilir (Lynn, 2010).

Yine siber tehditlerin özellikleri kapsamında siber ortamda her zaman hücumun üstün olduğu belirtilmektedir. Bu nedenle bir ülke, siber güvenliğini sağlayabilmek için belirli bir siperin veya duvarın arkasına çekilmez, aksi halde istila edilme riskiyle karşı karşıya kalabilir. Tıpkı manevra savaşında olduğu gibi siber ortamda hız ve çeviklik önemlidir ve siber saldırganlardan bir adım önde olmak isteyen bir ülke, savunmasını sürekli olarak geliştirmelidir. Bunlara ek olarak, yukarıda da belirtildiği gibi, siber saldırılarda faili bulmak zordur ve failin devlet dışı bir aktör olması (örneğin terörist grup) durumunda ise bir devletin misillemede bulunabilecek hiçbir hedef olmayabilir. Son olarak bir ülkenin sahip olduğu caydırıcılık yeteneğinin siber uzaydaki uygulanmasının zor ve zaman alıcı olduğunu bilmek önemlidir. Soğuk Savaş yıllarında ülkelerin ellerinde bulunan nükleer silahlar önemli bir misilleme ve caydırıcılık unsuru idi. Ancak siber ortamda misilleme yoluyla bedel ödetmekten çok, saldırı yapanların bu saldırı sonucunda bir fayda elde etmesini engellemek ön plana çıkmaktadır (Lynn, 2010). Siber saldırıların yapıldığı alanlar ve amaçları ise çok çeşitlidir. Örneğin, tren sinyallerini veya trafik ışıklarını manipüle etmek, nükleer santralleri veya elektrik şebekelerini bozmak, bir ülkenin önemli bilgilerini veya bir şirketin teknolojik verilerini ele geçirmek gibi siber saldırıların amacı çok çeşitlidir (Koch vd., 2020:275-276). Siber güvenliğin tarihi süreç içerisinde yaşadığı dönüşümü görmek, kavramın anlaşmasını daha da kolaylaştıracaktır.

Tablo 1. Siber Güvenliğin Dönüşümü

Büyük/Ana Bilgisayarların Kullanıldığı Dönem (Mainframes)	**İstemci/Sunucu (Client/Server)**	**İnternet**	**E-Ticaret**	**Dijital**
1970'ler	1980'ler	1990'lar	2000'ler	Yakın Dönem
• Doğal Tehlikeler • Tahliye ve ilk yardım gibi (olay) yerinde yapılan fiziki müdahale önlemleri	• Az sayıda bir takım yeni teknolojilere bağımlılık • Sistem arızalarına temel afet müdahalesi • Virüs koruması geliştirildi	• Kurumsal çapta risk yönetimi tanıtıldı • Ortak mevzuata uyma politikası • Odaklanılan nokta işin sürekliliğini sağlamak	• Bilgide yenilik • Çevrimiçine geçiş • Bulut gibi dış kaynak kullanımı • Bağlı cihazlar	• Küresel şoklar (terör, iklim değişikliği, politik) • Dayanıklılık • Nesnelerin interneti • Kritik Altyapı • Devlet destekli siber saldırı, siber savaş

Kaynak: Hajoary ve Akhilesh, 2020:82.

Tablo 1'de ifade edildiği gibi 1970'li yıllarda olay yerinde fiziki müdahale şeklinde gerçekleşen bilgisayar sistemlerinin güvenliği (siber güvenlik), günümüz itibarıyla kritik altyapıların güvenliğindeki asli unsur olma, devlet destekli siber saldırıların ve siber savaşın yürütüldüğü bir mecra olma gibi ulusal güvenlik açısından çok önemli işlevlere sahip bir alan haline gelmiştir. Siber güvenliğin böylesine önemli bir alan haline gelmesinde günümüzde iletişim, ulaşım, alışveriş, enerji ve sağlık sektörü gibi birçok alanın internet ve bilgisayar sistemlerine bağlı olarak faaliyet yürütmesi önemli rol oynamaktadır (CISA, 2021).

Günümüzde kamu düzeninin gerçekleşmesi için hayati önem arz eden altyapılar (*adliye sistemi, sağlık sistemi, askeri teknolojiler, akıllı kent uygulamaları kapsamındaki girişimler vb.*) siber ortamda depolanır ve siber ortam aracılığıyla yürütülür hale gelmiş, özellikle Covid-19 pandemisi döneminde hem kamu sektörünün hem de özel sektörün dijital dönüşümü (*faaliyetlerini siber ortama taşıma*) hız kazanmıştır (Işık, vd., 2022). İşte gündelik hayatın daha fazla siber ortam odaklı hale geldiği günümüzde siber güvenlik, siber ortamdaki tehditlerin tanımlanmasına, değerlendirilmesine, siber ortamdaki risklerin azaltılmasına; siber ortamda bulunan verilerin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin güçlendirilmesine yönelik tehdit oluşturan siber saldırıların etkilerinin ortadan kaldırılmasına yardımcı olmaktadır (Ardielli ve Ardielli, 2017).

Siber güvenliği sağlamak, siber saldırıların tamamen ortadan kaldırılması ve bir örgütün hiçbir siber saldırıya maruz kalmaması şeklinde anlaşılmamalıdır. Bir örgütün hiçbir siber saldırıya maruz kalmaması ancak, zamanın geri alınması ve örgütün bütün faaliyetlerini kağıt-kalemle, daktiloyla ve internetle hiçbir bağlantısı olmayan araçlar kullanmasıyla mümkün olabilmektedir (Ilves, 2013). Günümüz itibarıyla böyle bir durum söz konusu olamayacağına göre siber saldırılardan da kurtulmak mümkün olmayacaktır. Bu durumu eski FBI direktörü Robert S. Mueller şu şekilde belirtmiştir: "*Önemli olan bir örgüte siber saldırının olup olmayacağı değil, örgütün ne zaman hackleneceği sorunudur*" (Işık, vd., 2022).

Siber güvenliğin rolünü bir benzetmeyle ifade etmek gerekirse, nasıl ki bir soyguncu alarm sistemlerine sahip bir eve girebilir, ancak tek hamlede bütün bir mahalleyi soyamazsa, siber güvenlikte de amaç bu girilen evdeki alarm sayesinde bütün mahallenin haberdar olması, soyguncunun işe yarar bir materyal ele geçirmesinin engellenmesi ve bu olaydan ders alınarak mevcut güvenlik açıklarının kapatılmasıdır (Chang, 2014).

Engellenmesinin mümkün olmadığı ancak etkisinin azaltılabilmesinin mümkün olduğu siber saldırıların türlerine bakılacak olursa, Avrupa Birliği Siber Güvenlik Ajansı'nın hazırladığı "*Tehdit Manzarası 2022*" adlı rapora göre siber güvenliğe yönelik 8 ana tehdit grubu vardır. Bu tehdit grupları ve açıklaması aşağıdaki tabloda ifade edilmiştir.

Tablo 2. Avrupa Birliği Siber Güvenlik Ajansına Göre Siber Güvenlik Tehdit Grupları ve Açıklaması

Tehdit Türü	Açıklaması
Fidye Yazılımı	Hackerlerin bir kişinin (veya işletmenin, devletin) verilerinin kontrolünü ele geçirmesi ve ardından bu verileri geri vermek için fidye talep etmesi. 2021 itibarıyla küresel fidye yazılımı saldırılarının verdiği hasar miktarının 18 milyar Euro'ya çıktığı düşünülüyor- 2015'teki değerin tam 57 katı.
Kötü Amaçlı Yazılım	Bir sisteme zarar veren yazılım (virüsler, solucanlar, casus yazılımlar)
Sosyal Mühendislik Tehditleri	Bilgi veya hizmetlere erişim sağlamak için insan hatasından yararlanma. Kullanıcıyı kandırarak kötü amaçlı belgeleri, e-postaları ve web sitelerini ziyaret etmelerini sağlamak ve böylece sistemlere veya hizmetlere yetkisiz erişimin sağlanması.
Verilere Yönelik Tehditler	Veri kaynaklarının yetkisiz erişim ve ifşa için hedef alınması. Verilere yönelik tehditler veri ihlalleri (siber saldırganların yaptığı kasıtlı saldırılar) ve veri sızıntıları (verilerin kasıtsız olarak yayımlanması) şeklinde ikiye ayrılmaktadır.
Hizmet Reddi Saldırıları	Ağ altyapısını aşırı yüklemek suretiyle kullanıcıların veri ve hizmetlere erişimini engellemeye yönelik saldırılar.
İnternetin Kullanılabilirliğine (Mevcut Olmasına) Yönelik Tehditler	İnternet altyapısının fiziki olarak ele geçirilmesi ve imha edilmesi (Ukrayna'nın 2022'deki işgalinde de görüldüğü gibi) ve sosyal medya web siteleri ile haberlerin etkin bir şekilde sansürlenmesini içerir
Dezenformasyon-Yanıltıcı Bilgilerin Yayılması	Korku ve belirsizlik yaymak için internet ortamında dezenformasyon içeren ve yanlış bilgilerin yayılması. 2022 Ukrayna saldırısında Rusya bu teknolojiyi Ukraynalıların savaş algılarını etkilemek için kullandı.[1]
Tedarik Zinciri Saldırıları	Örgütler ve tedarikçileri arasındaki ilişkiyi hedefler.

Kaynak: European Parliament, 2023.

Tablo 2'de ifade edildiği üzere siber güvenlik tehditleri, örneğin bir ülkenin siber ortamdaki verilerinin ele geçirilip ardından fidye istenmesi, ülke halkını korku ve paniğe sürükleyebilmesi ve devletin siber ortama bağlı sunduğu hizmetleri kesintiye uğratabilmesi yönüyle ulusal güvenlik açısından birçok tehdit unsurunu bünyesinde barındırmaktadır. Bu nedenle aşağıda, ulusal güvenlik açısından siber güvenliğin oynadığı rol üzerinde durulacaktır.

2.2. Ulusal Güvenlik Açısından Siber Güvenliğin Rolü

En genel anlamıyla ulusal güvenlik, "*bir ülkenin kendi topraklarını ve vatandaşlarını koruması ve savunması*" şeklinde tanımlanabilir (Longley, 2021). Toplumun işleyişini, huzurunu, sükûnetini bozan ve kamu hizmetlerinin sunumu aksatan geniş ölçekli tehditler birer "*ulusal güvenlik tehdidi*" olarak görülebilir. Günümüzde bu tür tehditlerin sadece askeri alanlardan gelmediği (*örneğin Covid-19 pandemisi bu tür bir tehditti*) dikkate alınarak ulusal güvenlik, sadece askeri boyutu olan bir kavram değil siyasi, sosyal, ekonomik, çevre ve insan haklarına ilişkin yönleri de bulunan bir kavram olarak görülmeye başlanmıştır (Küçükşahin, 2006:10).

Enerji altyapıları, sağlık, ulaşım ve bankacılık gibi alanların her geçen gün biraz daha fazla siber ortama bağımlı hale geldiği günümüz dijital dünyasında, askeri güçlere saldırmadan bir ülkenin ulusal güvenliğini tehlikeye atmak olanaklı hale gelmiştir. Siber ortama artan bağımlılık nedeniyle siber ortamda hiçbir ülke bir ada değildir ve bütün ülkeler siber tehditlere (Tablo 2'de bahsedilen) maruz kalabilir (Ilves, 2013). Siber saldırılar haiz olduğu bu önem nedeniyle 2021 Dünya Ekonomik Forumu toplantısında bulaşıcı hastalıklar, geçim sıkıntısı ve aşırı hava olaylarının ardından en büyük dördüncü küresel güvenlik riski olarak kabul edilmiştir (Işık vd., 2022).

Kamu hizmetlerinin ve kamu düzeninin aksaksız bir şekilde idame ettirilebilmesi için günümüzde yolların, sokakların ve binaların güvenli olması gerektiği kadar siber ortamın da güvenli olması gerekmektedir. Çünkü günümüzde kamu hizmetlerinin sunumuna aracılık eden ve siber ortam vasıtasıyla faaliyetlerini yürüten sistemlerde meydana gelebilecek bir arıza, problemin nedeni bulununcaya ve giderilinceye kadar ilgili kamu hizmetinin durmasına neden olacaktır (Rainer vd., 2020:18). Örneğin 2022 yılının Ağustos ayında Karadağ'ın dijital altyapısına, hükümet yetkililerinin ifadesiyle "*benzeri görülmemiş*" bir siber saldırı yapılması neticesinde, güvenlik nedeniyle belirli hizmetler geçici olarak durdurulmuştur (Reuters, 2022). Bir diğer örnek olarak ABD'nin en büyük petrol hattı sistemi olan Colonial Pipeline'a 2021 yılında yapılan siber saldırı verilebilir. ABD için kritik bir ulusal altyapı sistemi olan bu boru hattına yapılan saldırı neticesinde hat, 6 günlüğüne

1 Benzeri bilgiler için Bkz.: Karasoy, 2022.

kapatılmış ve 17 eyalete yakıt tedariki kesintiye uğramıştır. Bunun neticesinde ise etkilenen bölgelerde binlerce okul, işletme ve hastanenin faaliyetleri aksamıştır (Bansemer, 2021). Siber güvenliğin sağlanması özel sektöre nazaran kamu sektörü için daha zordur. Çünkü kamu sektörü genelde özel sektörden daha fazla veri depolamakta ve bu verileri daha savunmasız sistemlerde muhafaza etmektedir. Kamu kurumları, sadece maddi kazanç peşinde koşan hackerler tarafından değil, ulus-devletlerin finanse ettiği ve eğittiği ekipler tarafından da düzenli olarak hedef alınmaktadır (Eggers, 2016:140). Bu nedenledir ki siber güvenlik alanında en iyi kaynaklara sahip kuruluşlar bile kötü niyetli aktörlere karşı savunmasızdır (Bansemer, 2021).

Siber ortama bağımlı olan kamu kurumları içerisinde askeri kurumlar üst sıralarda yer almaktadır. Bu konuda ABD ordusundan bir örnek veren Flournoy ve Sulmeyer (2018), ABD ordusunun komuta-kontrol, ikmal veya iletişim ağlarına yapılacak bir siber saldırının, ordunun gücünü denizaşırı ülkelere yansıtma kabiliyetini baltalayabileceğini ve askeri kuvvetleri bağlantısız ve savunmasız bırakabileceğini ifade etmektedirler. Siber güvenlik konusunda kamu sektörü özel sektörden daha fazla endişelidir. Çünkü, siber güvenlik alanında yaşanacak bir aksaklık, vatandaşların devlete olan güvenini etkilemesinin yanı sıra bir ulusal güvenlik tehdidi de oluşturabilir (Işık vd., 2022).

Devletler siber tehditlerin en büyük hedefidir ve kamu sektörü, özel sektörden daha fazla (siber) güvenlik olayı ve veri ihlaliyle karşı karşıyadır (Eggers, 2016:142). Bu durum Avrupa Parlamentosu tarafından 2021 ve 2022 yıllarında hazırlanan raporlarda da görülmektedir. Avrupa Birliği Siber Güvenlik Ajansı (ENISA)'na göre Nisan 2020 ile Temmuz 2021 arasında siber güvenlik tehditlerinden en çok etkilenen ilk 5 sektör; kamu yönetimi/devlet (198 vaka bildirildi), dijital hizmet sağlayıcıları (152 vaka), halk (151 vaka), sağlık hizmetleri (143 vaka) ve bankacılık/finans (97 vaka) şeklinde sıralanmıştır. Haziran 2021 ile Temmuz 2022 arasında siber saldırılardan en çok etkilenen sektörlerin başında da kamu yönetimi/devlet (rapor edilen olayların %24'ü) gelmekte olup, kamu yönetimini dijital servis sağlayıcılar (%13), halk (12), hizmetler (%12), finans/bankacılık (%9) ve sağlık (%7) takip etmektedir (European Parliament, 2023). Buradan da anlaşılmaktadır ki siber güvenlik tehditlerinden en çok etkilenen sektör kamu sektörü (devlet) olup, ENISA'nın sıraladığı diğer sektörler de (örneğin sağlık sektörü, finans/bankacılık) sektörleri de kamu düzeninin ve huzurunun devamı için önemli kamu hizmetleri arasında yer aldığından, siber güvenlik tehditlerinin aslında dar anlamda kamu güvenliğine, geniş anlamda da ulusal güvenliğe yönelik bir tehdit olduğu söylenebilir.

Kamu hizmetleri giderek daha fazla dijitalleşip birbirine bağlı hale geldikçe, birbirine bağlı enerji altyapılarının güvenliğini sağlamak "*kritik*" önem kazanmıştır. Avrupa Birliği, ABD ve Çin gibi ülkelerin karbon nötr olma taahhüdü gereğince elektrik kullanımına ağırlık verilmesi, iklim değişikliği ve çevre kirliliği gibi tehditlerle mücadele için önemli bir adımdır. Öte yandan örneğin ulaşım sektörünün elektrifikasyonu, yıkıcı siber saldırılara da kapı aralayabilecektir. Örneğin, bir siber saldırganın elektrikli araç şarj noktalarını en yüksek kapasiteye ayarlaması elektrik şebekelerinde aşırı yüklenmeye, elektik kesintilerine, sistemin arızalanmasına ve elektrikle bağlantılı olan diğer enerji sistemlerinin hasar görmesine neden olabilir (Accenture, 2022b). Bu nedenledir ki günümüzde elektrik altyapısı başta olmak üzere kamu düzeninin ve huzurunun tesisi için önem arz eden birçok altyapı "*kritik*" sıfatıyla ifade edilir olmuştur ve "*kritik altyapı*" adıyla bilinmektedir.

Kritik altyapı, modern toplumsal hayatın idamesi için hayati önem taşıyan fiziki ve sanal sistemlerin genel adıdır (Darıcılı ve Çelik, 2022:260). Kritik altyapılar, hasar görmesi halinde vatandaşların güvenlik ve esenliklerine yönelik bir tehdit unsuru olabilecek fiziksel ve bilgi teknolojisi tesislerini, şebekelerini, hizmetlerini ve varlıklarını ifade etmektedir. Enerji tesisleri ve şebekeler, finans ve sağlık sistemleri, iletişim ve ulaşım altyapıları, baraj ve sulama sistemleri gibi sistemler kritik altyapı kapsamında değerlendirilmektedir (Küpeli, 2019:98-99). Bahsi geçen bu sistemlerin işleyişinde yaşanabilecek bir işlev bozukluğu toplumsal hayatın işleyişine büyük bir sekte vurabileceği için bu sistemler "*kritik*" olarak adlandırılmaktadır (Koch vd., 2020:275). Kritik altyapıların etkin ve güvenli yönetimi, bir devletin sosyal refah ve ekonomik gelişmişliğini göstermektedir. Haiz olduğu bu önem neticesinde kritik altyapıların güvenliğini sağlamak, modern devletlerin ulusal güvenlik stratejilerinin önemli bir bileşeni haline gelmiştir (Darıcılı ve Çelik, 2022:260).

Kritik altyapıların güvenliğine yönelik tehditler çeşitlidir: Deprem, tsunami, sel, fırtına veya insan hatasından kaynaklı tehditler bunlardan bazılarıdır. Bu tür fiziki çevreden gelebilecek tehditlerin yanı sıra kritik altyapıların komuta-kontrolüne olanak tanıyan dijital kontrol sistemleri, siber tehditler karşısında daha da savunmasızdır (Koch vd., 2020:275-276). Kamu hizmetlerinin sunulmasında ve dolayısıyla toplumsal hayatın sağlıklı bir şekilde idamesinde müstesna bir yeri bulunan kritik altyapılar büyük ölçüde ağ teknolojilerine dayalı olarak faaliyet gösterdiği için, bir devletin kritik altyapılarının siber güvenliğini sağlamak ulusal güvenlikle eş anlamlı hale gelmiştir (Darıcılı ve Çelik, 2022:260).

Kritik altyapılar her ne kadar toplumsal hayatın idamesinde ve kamu hizmetlerinin sunumunda önemli rol oynuyor görünse de bu altyapılar esasında askeri stratejinin de temel direğidir (Siebold, 2022). Kritik altyapıların çoğu askeri operasyonları da destekler ve bu altyapılardaki olası bir aksaklık, ulusal güvenliği tehlikeye atabilir. Örneğin ABD sesli iletişim ve internet iletişiminin %90'ı, özel evlere ve ofislere hizmet veren aynı özel ağlar üzerinden gerçekleşmektedir. Amerikan ordusu, personelini ve bu personele ait yükü taşımak için sivil ulaşım sistemlerine, yakıt ihtiyacını karşılamak için ticari rafinerilere ve ödeme işlemlerini yapabilmek için finans ve bankacılık sistemine güvenmektedir (Lynn, 2011). Bu kapsamda değerlendirildiğinde kritik altyapılar, bir devletin siber saldırılar düzenleyebileceği sadece sivil birer hedef değil, aynı zamanda askeri birer hedeftir (Darıcılı ve Çelik, 2022) ve bu durum, günümüzde siber güvenliğin bir ülke açısından hava savunma sistemleri kadar önemli olduğuna işaret etmektedir (Siebold, 2022).

Siber ortama dayalı olarak faaliyet göstermeleri nedeniyle bir sektördeki kritik altyapıya yönelik yapılan siber saldırı, diğer sektörlerde de aksamalara neden olabilir. Örneğin bir ülkenin telekomünikasyon altyapısına yönelik bir siber saldırı, finans sistemini kesintiye uğratabilir (Fadia vd., 2020). Kritik altyapıların birbirine bağlı olması nedeniyle günümüzde askeri altyapı ve sivil altyapı arasındaki ayrımın ortadan kalktığı söylenebilir. Çünkü askeri bir çatışma durumunda sivil altyapılar doğrudan hedef alınabileceği ve bir ülkeye karşı pazarlık kozu olarak rehin tutulabileceği için, sivil altyapılar güvende değilse askeri altyapıları en iyi şekilde korumak için hazırlanmış planların bir önemi olmayacaktır (Lynn, 2010). Örneğin, bir ülkenin askeri üslerine giden elektriği kesmek amacıyla elektrik şebekesine düzenlenen bir siber saldırı, amaçlananın çok ötesine geçerek çevredeki sivil nüfusun elektrik kaynağını kesintiye uğratabilir, hastanelerin ve eğitim kurumlarının faaliyetlerini etkileyebilir (Flournoy ve Sulmeyer, 2018). Bu gibi örnekler günümüz savaş ortamında sivil ve askeri alan ayrımının giderek kaybolduğunu teyit etmektedir (Karasoy, 2021).

Siber güvenlik sadece bir ülkenin kritik altyapılarını hedef almasıyla değil aynı zamanda ülkenin siyasi istikrarını, ülke halkları arasındaki uyumu, demokratik kurumlara ve sürece olan inancı baltalaması yönüyle de ulusal güvenliği tehdit etmektedir. Siber güvenliğin bu sayılan boyutlarıyla ulusal güvenliği tehdit etmesindeki en müşahhas aktör Rusya'dır. ABD toplumunda kargaşa medyana getirmek ve demokratik sürece olan inancı aşındırarak ABD önderliğindeki liberal demokratik düzeni baltalamak amacıyla Rusya'nın 2016 ABD başkanlık seçimlerine müdahale etmesi, bizzat FBI (Federal Soruşturma Bürosu) eski direktörü James Comey'in ifadeleriyle teyit edilmiştir. 2014 yılında Ukrayna'daki seçimlere de müdahale eden Rusya, Ukrayna'daki oy sayma sistemlerini geçici olarak çalışamaz hale getirmiş ve oy sayımını saatlerce geciktiren bir siber saldırı düzenlemiştir. Bu saldırıların zamanına tespit edilmesi neticesiyle seçim sonucu değişmemiştir (Hennessey, 2017). Bu gibi örnekler, Rusya'nın (özellikle yeni doğan) demokrasilere zarar verebileceğini göstermektedir (Lee ve Talos, 2022).

ABD, siber güvenliğin bir kısmına yukarıda da değinilen önemi neticesinde kara, hava ve denizden sonra siber ortamı[2] yeni bir savaş alanı olarak sınıflandırmıştır (Eggers, 2016). Saldırı ve savunma amacıyla küresel internet altyapısının kullanılarak yapılan bilgisayar operasyonları "*siber savaş*" kavramıyla ifade edilmektedir (Filkenstein ve Govern, 2015:9-10). Günümüzde ulusal güvenliğe yönelik en büyük tehditlerden bir tanesi de devlet destekli siber savaştır. Seçimlere müdahale etmekten yerli inovasyon açığını kapamak için yabancı firmalara sanayi casusluğu yapmaya kadar devlet destekli siber saldırılar, dünya genelinde ülkeleri tehdit etmektedir (Fadia vd., 2020; Flournoy ve Sulmeyer, 2018). Siber saldırılar, modern silahlı çatışmaların da bir parçasıdır (Lee ve Talos, 2022).[3] Bu durum 2022 yılının Şubat ayında başlayan Rusya'nın Ukrayna'yı işgalinde de görülmüştür. Rusya, Ukrayna'daki hedeflerine ulaşmak için fiziksel ve siber saldırıları entegre bir biçimde kullanmıştır. Örneğin 2022'deki işgal girişiminin başlamasının ardından Rus askeri istihbarat teşkilatının bir parçası olan bilgisayar korsanları, yaklaşık 2 milyon yerliye elektrik sağlayan bir elektrik kuruluşuna siber saldırı düzenlemişler, ancak başarısız olmuşlardır (Pearson ve Bing, 2022). Savaşın başlamasının ardından on binlerce modemi devre dışı bırakan bir uydu internet ağına siber saldırıda bulunan Rusya, böylelikle Ukrayna komuta-kontrolünü bozmayı amaçlamış ve gerek Ukrayna gerekse bazı Avrupa Birliği ülkelerinde iletişim kesintilerine neden olmuştur (Pearson, 2022).

Seçimlere müdahale, kritik altyapılara hasar verme, silahlı çatışmalarla entegre biçimde kullanılma gibi tehditlerin yanı sıra, siber saldırıların ulusal güvenlik açısından tehdit ettiği bir unsur daha vardır: "*Güven*". Sosyal sermayenin temel bileşeni güvendir ve siyaset bilimci Robert Putnam'ın ifade ettiği gibi barışçıl ve

2 Bu çalışmada genelde "*siber ortam (cyber environment)*" kavramı kullanılmakla birlikte "*siber uzay (cyber space)*" kavramı da aynı duruma işaret etmektedir.

3 Devletler açısından silahlı kuvvetlerin yanında siber saldırıların da kullanılması, günümüz savaşlarının birer "*hibrit savaş*" olduğunu göstermektedir. Daha fazla bilgi için bkz.: Karasoy, 2021.

müreffeh toplumların altında yatan unsur, ortak paylaşılan normlar ve bu normlar ekseninde birbirine bağlı olan ağlardır (*toplumlun farklı kesimleri, sosyal ve siyasal örgütlenmeler vb.*) (Schneider, 2021). Farklı disiplinlerce yapılan sosyal sermaye tanımına göre, daha iyi bağlantılı aktörler (*gruplar, örgütler veya genel olarak toplumun tamamı vb.*) daha başarılı (*yani bu aktör bir işletme ise daha kârlı, bir ülke ise ekonomik açıdan gelişmiş, bir futbol takımı ise şampiyonluğa oynayan gibi*) olmaktadır. Bunun nedeni ise aktörlerin, daha iyi bağlantılı oldukları için daha fazla kaynak (*para, teknik bilgi, hammadde vb*.) paylaşımında bulunabilmesidir (Öztaş, 2014:163).

İnsanların, örgütlerin, devletlerin daha iyi bağlantılı olmaları nedeniyle fazla kaynak paylaşımında bulunabilmesi ve bu sayede daha başarılı olabilmesini ifade eden sosyal sermaye kavramının merkezinde "*güven*" yatmaktadır. Günümüzde insanların, toplumların, devletlerin ve orduların siber ortama gittikçe daha çok bağımlı hale gelmesi, "*güven*" unsurunu dünya genelinde daha çok ön plana çıkarmıştır. Bir başka ifadeyle, yapılan siber saldırıların bir hedefi de bütün toplumsal etkileşimleri gerçekleştirmek için ihtiyaç duyulan "*güven*" unsuru olmuştur. Örneğin günümüzde piyasalar çevrimiçi olarak birebirine bağlıdır ve piyasalara yönelik yapılan siber saldırıların hedeflerinden bir tanesi de sisteme yönelik bir güvensizlik meydana getirmektir. Öte yandan, hastanenin bilgisayar sistemlerindeki güvenlik açığından yararlanarak bir kalp pilinin hacklenmesi, hastada bir güvensizlik hissine neden olabilir. Siber saldırılar devletin tuttuğu ve vatandaşlarına ait olan bilgilerin bütünlüğüne ve doğruluğuna yönelik güvensizlik hissi meydana getirebilir, seçimlere yapılan müdahaleler demokratik sürece, işleyişe ve yöneticilere olan güveni baltalayabilir, ileri teknoloji üreten bir işletmenin fikri mülkiyetinin ele geçirilmesi şirketlerin ar-ge yatırımlarının düşmesine (*nasıl olsa bir başkası ele geçirecek düşüncesi nedeniyle*) neden olabilir (Schneider, 2021).

Kısacası hem toplumlar hem de devletler güvene yönelik saldırılar karşısında savunmasızdır. Günümüzde ise işletmeler, okullar, hastaneler, mahkemeler, kısaca kamu ve özel sektör kuruluşlarının neredeyse tamamı fidye yazılımı saldırısının (Tablo 1'de ifade edilen) hedefi haline gelmiş ve bu durum da hem devlet tarafından saklanan verilerin güvenliğine hem de demokratik kurumlarda güven inşa etme sürecine bir tehdit oluşturmuştur (Schneider, 2021).

İyi yönetilen toplumların dayanıklı toplumlar olduğu ifade edilmektedir (Coffey, 2019). Bu dayanıklılığa belki de en fazla, siber tehditler arasında yer alan dezenformasyon kampanyaları (Tablo 1'de ifade edilen) karşısında ihtiyaç duyulmaktadır. İyi yönetilen bir toplumda kurumlara ve yöneticilere olan güven de yüksek olacağı için, toplumda dezenformasyon kampanyalarının etkisi daha az olacaktır. Toplumu bütün halinde tutan bir "*harç*" mahiyetinde olan güven unsurunun ise siber saldırıların ana hedefi olduğu unutulmamalıdır.

Günümüzde internet (siber ortam) birçok yönden hayatı kolaylaştırsa da artan veri yığınıyla ve gün geçtikçe gelişen tehditlerle baş etmek giderek zorlaşmaktadır. Bu konuda yapay zekâ, siber güvenlik açısından önemli bir yardımcı olarak görülmeye başlanmıştır. Aşağıdaki başlıkta siber güvenlikte yapay zekânın önemi üzerinde durulacaktır.

2.3. Siber Güvenlik ve Yapay Zekâ: Günümüzün Siyam İkizleri

Yapay zekâ, dijital teknolojinin insan zekâsının yapabileceği görevleri yerine getirebilecek sistemleri oluşturmak için kullanılması şeklinde tanımlanabilir (Şen ve Yurtoğlu, 2020:28). Ak (2021:122) ise yapay zekâyı, "*insan gibi akıl yürütebilen, anlam çıkarabilen, genelleme yapabilen, geçmiş tecrübelerden öğrenebilme yetisine kavuşabilen bir yazılım şekli veya makinenin modellenme halidir*" şeklinde tanımlamıştır. Yapay zeka, insan zekası gerektiren görevleri yapabilecek makinelerin beyni olarak görülebilir ve yapay zekada amaç, insan zekasını taklit eden makineler yapmaktır (Rainer vd., 2020:462).

İnsanoğlu hızla yapay zekâ ile hayat bulan otonom makinelerle ortak bir yaşam kurgusuna doğru ilerlemektedir. Yapay zekâ hâlihazırda günümüz yaşamının birçok alanına nüfuz etmekte olduğu bilinmektedir (Gezici, 2022:80). Yapay zekânın üretim yönetimi, iş süreçleri (Erdoğan, 2021:9), lojistik operasyonlar (Erdoğan, 2022:579), finansal risk yönetimi, ticari istihbarat, perakende satış, klinik çalışmalar ve ilaç keşfi, kamu hizmetleri (Gezici, 2022), hava ve uzay savunma, ses tanıma ve afet kurtarma gibi geniş bir kullanım yelpazesi vardır. Yapay zekânın kullanıldığı alanlardan bir tanesi de siber güvenliktir (Shabbir ve Anwer, 2015:8-9). Siber saldırıların hızına, çeşitliliğine ve siber ortamdaki olaylara ilişkin devasa veri hacmine ayak uydurmakta zorlanan siber güvenlik uzmanları için yapay zekâ, esnek ve uyarlanabilir olması nedeniyle bir yardımcı olarak görülmektedir (Leenen ve Meyer, 2019:46).

Siber tehditlerle başa çıkmak için birçok yapay zeka yöntemi (*örüntü tanıma, veri madenciliği, yapay bağışıklık sistemleri vb.*) kullanılsa da son zamanlarda siber tehditlerle mücadelede "*makine öğrenimi*" ve "*derin öğrenme*" en çok başarı kazanan yapay zeka teknikleridir (Truong vd., 2020:4). Yapay zekânın son evresi olarak nitelendirilen makine öğrenimi, "*bir problemi o probleme göre modelleyen bilgisayar algoritmalarının genel adıdır*" şeklinde tanımlamaktadır (Şen ve Yurtoğlu, 2020:27). Makine öğreniminin özel bir yöntemi olan derin öğrenme ise veriden öğrenme olarak açıklanabilir (Ak, 2021:125).

Siber güvenlikte uygulanan yapay zekâ tekniklerini somutlaştırmak adına aşağıdaki şekilde, yapay zekâ tekniklerini benimseyen siber güvenlik uygulamalarının başlıca dalları ifade edilmiştir.

Tablo 3. Yapay Zekâ Tekniklerini Benimseyen Siber Güvenlik Uygulamalarının Ana Dalları

YAPAY ZEKÂ TABANLI YÖNTEMLERİN SİBER GÜVENLİKTEKİ UYGULAMALARI			
Kötü Amaçlı Yazılım Tespiti	**Ağa İzinsiz Giriş Tespiti**	**Kimlik Avı/Spam Tespiti**	**Diğer**
• Virüsler, solucanlar ve Truva atları gibi zararlı yazılımlar genel olarak "*kötü amaçlı yazılım*" kavramıyla ifade edilmektedir. Siber ortamdaki varlıklar üzerinde kötü amaçlı yazılımların yıkıcı etkisi büyüktür. Bu nedenle kötü amaçlı yazılımları önlemek ve etkilerini hafifletmek için yapay zekâ teknikleri benimsenmektedir.	• Bir dijital sistemi güvenliği tehdit edici olası olaylardan, ihlallerden ve tehditlerden koruyan sisteme İzinsiz Giriş Tespit Sistemi (*instrusion detection system - IDS*) adı verilmektedir. IDS geliştirmek için yapay zekâ tabanlı teknikler esneklikleri, uyarlanabilirlikleri, hızlı hesaplamaları ve hızlı öğrenmeleri nedeniyle IDS geliştirmek için uygundur ve diğer teknikleri geride bırakmaktadır.	• Kimlik avı saldırısı, bir kullanıcının kimlik bilgilerini (bireysel, mali bilgiler, şifreler vb.) ele geçirmeye çalışan bir siber saldırıdır ve internetteki en tehditkâr saldırılardan bir tanesidir. Bu tür problemlerle başa çıkmak için yapay zekâ tabanlı uygulamalar kullanılmaktadır.	• Hassas verileri kötüye kullanmak için gelişmiş teknikler kullanan ve tespit edilmeden kalan karmaşık siber saldırılar "Gelişmiş Kalıcı Tehdit (Advanced Persistent Threat-APT) kavramıyla ifade edilmektedir. APT saldırılarına karşı koymak için de bilim insanları yapay zekâ tekniklerini önermektedir.

Kaynak: Truong vd., 2020:6-15'ten yararlanılarak hazırlanmıştır.

Tablo 3'te özetlendiği üzere yapay zekâ teknikleri siber güvenliği sağlamak için çeşitli amaçlarda kullanılmaktadır. Ancak bilinmektedir ki yapay zekâyı kullananlar sadece siber güvenlik uzmanları değil aynı zamanda siber saldırganlardır. Siber güvenlik için yapay zekânın oyunun kurallarını değiştirebilecek yetenekleri olsa da (Bansemer, 2021) yine yapay zekâ destekli yeni nesil siber saldırılar karşısında yetersiz kalabileceği de ifade edilmektedir. Dolayısıyla siber güvenlikte yapay zekâ hem saldırı hem de savunma amacıyla kullanılabilmektedir ve yapay zekâ gelecekte siber saldırılarda daha yoğun kullanılacağı için siber güvenliğin de daha fazla yapay zekâ odaklı hale geleceği ifade edilmektedir (Booker ve Musman, 2020:1). Siber saldırılarda yaşanan artış, yapay zekâ tabanlı siber güvenlik ürünleri pazarındaki büyümeyi hızlandırmıştır. Temmuz 2022 tarihli bir raporda, yapay zekâ tabanlı güvenlik ürünleri küresel pazarının 2021'de 14,9 milyar dolar olduğu ve bu rakamın 2030 yılına kadar 133,8 milyar dolara ulaşacağı tahmin edilmektedir (Violino, 2022).

Yapay zekânın insanlardan daha iyi siber saldırlar düzenlediği test edilmiştir (Dvorsky, 2017) ve zaten önemli bir ulusal güvenlik tehdidi olan siber tehditlere bir de yapay zekâ eklemek, güçlü bir tehdidi daha güçlü hale getirmektedir. Bu nedenle siber güvenlik uzmanları ve yapay zekâ geliştiricilerinin müşterek çalışması ve yapay zekâ destekli siber yetenekler tasarlaması önerilmektedir (Bansemer, 2021).

Yapay zekâ tekniklerinin siber saldırıların etkinliğini arttırmasına rağmen, günümüz siber saldırganlarının yapay zekâ tekniklerinden geniş ölçüde yararlanmaya başladıklarına dair sınırlı miktarda kanıt vardır. Siber saldırganların kullandığı mevcut saldırı tekniklerinin oldukça etkili olduğu, saldırılara yapay zekâ eklemenin saldırganlar için yeni güçlükler meydana getirebileceği ve siber saldırılara yapay zeka teknikleri entegre etmenin ek uzmanlık gerektirdiği durumları da göz önüne alınırsa, saldırganların yapay zeka tekniklerini neden yaygın kullanmadıkları şaşırtıcı olmayacaktır (Bansemer, 2021; Dvorsky, 2017). Dolayısıyla siber saldırganların yapay zekâyı kullanmamalarının (veya çok az kullanmalarının) ana nedeni, daha basit araçlarla amaçlarına ulaşabilmeleri nedeniyledir (Bansemer, 2021).

Günümüzde kullanımı sınırlı da olsa gelecekte siber saldırıları daha yıkıcı hale getirebilecek olan yapay zekâ teknikleri, siber güvenliğin sağlanması için de önemli bir potansiyele sahiptir. Yukarıda da ifade edilen bir yapay zekâ tekniği olan makine öğrenimi, öğrenmeyi hızlı bir şekilde otomatikleştirerek yeni saldırı davranışları da dâhil olmak üzere insanların farkında olmadıkları olayları (bilinmeyen bilinmeyenleri) aramada çok başarılıdır (Efe, 2021:152). Makine öğreniminin, izinsiz giriş tespit sistemlerine (Tablo 3'te belirtilen) uygulanması birçok siber güvenlik tehdidinin engellenmesine yardımcı olmuştur (Bansemer, 2021).

Siber güvenlik alanında yapay zekâ tekniklerinin yararlarına rağmen, günümüzde ne siber güvenlik uzmanları ne de yapay zekâ tek başına siber güvenliğin sağlanması için yeterli değildir (Chakraborty, 2020:152). Yapay zekâ teknikleri yararlı olmakla birlikte siber güvenlikle ilgili tüm görevlerde (tehdidi belirleme, tehdide yanıt verme, sistemi koruma ve kurtarma gibi) uygulanmasının zor olduğu kanıtlanmıştır. Bu nedenle yapay zekânın, izinsiz giriş tespiti gibi daha dar ve belirli görevlere uygulanmasının günümüz açısından daha yararlı olduğu ifade edilmektedir (Bansemer, 2021).

Siber tehditlerin (özellikle de devlet destekli olarak kullanılmasının) bir ulusal güvenlik tehdidi olduğu yukarıda izah edilmişti. Daha gelişmiş siber saldırılar yapmak isteyen devletlerin "*yapay zekâ silahlanma yarışına*" girmeleri, devletler açısından yeni ulusal güvenlik risklerine de kapı aralayabilecektir. Ülkelerin ulusal güvenliği için asıl tehlike, yapay zekâda rakiplerinin gerisinde kalması değil, yapay zekâ alanında oluşacak bir yarış algısının ülkeleri güvenli olmayan yapay zekâ sistemlerini konuşlandırmak için aceleye sevk etmesidir. Yapay zekâ yarışını kazanmak isteyen ülkeler rakiplerinin yanı sıra aslında kendilerini de tehlikeye atmaktadır (Scharre, 2019).

Ulusal güvenlik açısından siber güvenliğin oynadığı rolü ve yapay zekânın siber güvenlikteki yerinin izah edilmesinin ardından çalışmanın ikinci bölümünde siber güvenliğin sağlanmasına yönelik bu alanda başı çeken ülke uygulamalarından bazı derslere yer verilecektir.

3. SİBER GÜVENLİĞİN SAĞLANMASINA YÖNELİK ÜLKE UYGULAMALARINDAN ÖRNEKLER

Siber güvenlik konusunda dünyanın önde gelen ülkelerinin uygulamalarından belli başlı örnekler şu şekilde sıralanabilir (Bansemer, 2021; Işık vd., 2022; Lynn, 2010; Nye, 2021);

1. Birçok ülke ulusal güvenliğini sağlayabilmek için siber güvenliği öncelik listesinin başına koymaktadır ve siber güvenliğe proaktif (önleyici) bir yaklaşım sergilemektedir. Bunun anlamı, ilgili ülkenin henüz siber saldırılar olmadan önce harekete geçmesi ve siber saldırının yapılmasını önleyecek (*veya yapıldıktan sonra etkisini azaltacak*) tedbirlerin alınmasıdır. Bu nedenle kamu sektörünün siber güvenliğe tahsis edeceği kaynaklar (*maddi kaynak, insan kaynağı, bu alandaki eğitim-öğretim vb*.) büyük önem taşımaktadır.

   Mayıs 2022 itibarıyla en son yayınlanan Küresel Siber Güvenlik İndeksinde 1. ve 2. sıralarda yer alan ABD ve İngiltere, siber saldırılara hazırlık konusunda sınıfının en iyisi kabul edilmektedir. Bu iki ülkenin de ortak özelliği, net ve iyi tanımlanmış bir siber güvenlik gündemi ve siber güvenlik stratejisi ile birlikte, siber güvenliği en önemli ulusal savunma önceliği haline getirmeye yönelik güçlü bir kararlılıktır. ABD Başkanı J. Biden, Amerikalıların siber güvenliğini iyileştirmek için Mayıs 2021'de bir başkanlık emri yayınlamış ve siber güvenliğe yönelik kaynak arttırma ihtiyacını vurgulamıştır. Birleşik Krallık ise 2016'da başlatılan Ulusal Siber Güvenlik Stratejisi'ni desteklemek için yaklaşık 2 milyar sterlinlik kaynak ayırmıştır. Ayrıca Birleşik Krallık'ta kurulan Ulusal Siber Güvenlik Merkezi, siber saldırılarla aktif olarak mücadele etmektedir ve 2020 yılında yaklaşık 1200 örgütün siber saldırılarla başa çıkmasına yardımcı olmuştur.

   Siber güvenlik konusuna önem veren ülkelerden bir tanesi de İsrail'dir. Bu ülke siber güvenlik için öncelikle insan kaynağı oluşturmaya odaklanmış ve bu konuya önemli miktarda zaman ve kaynak ayırmıştır. Siber güvenlik eğitimini ortaokulda başlatan İsrail, dünyada lise düzeyinde eğitimde siber güvenliği seçmeli ders olarak okutan tek ülkedir. Buna ek olarak dünya siber güvenlik alanında doktora derecesi alınabilen ilk ülke de İsrail'dir. Tüm bu yatırımlar İsrail'i bir siber güvenlik merkezi haline getirmiştir.

2. Devletler açısından etkili bir siber güvenlik hizmeti sunmanın en önemli başarı faktörü olarak, siber güvenlik stratejinin sadece siber güvenlik alanına odaklanmış özel bir kurum tarafından yürütülmesi gösterilmektedir. Küresel Siber Güvenlik İndeksi'ne göre 131 ülke böyle bir siber güvenlik kurumuna sahiptir. Bu kurum, kritik altyapıları veya diğer herhangi bir devlet kurumunu hedef alan bir siber güvenlik tehdidi durumunda liderliği ele almakta ve devlet içindeki tüm kuruluşlarla işbirliği yapmaktadır.

   Belirtilmesi gereken bir diğer nokta da iyi bir siber güvenliğe sahip devletlerde yukarıda (madde ii) bahsedilen siber güvenlikten sorumlu kurumun, ülkenin Başbakanı ve Cumhurbaşkanı ile doğrudan bir bağlantısının olduğudur. Bu durum, devlet içindeki bürokrasiyi azaltıp kurumun başındaki yöneticinin

doğrudan devletin icra birimine rapor vermesini sağlamakta, aynı zamanda da ilgili devletin siber güvenliğe verdiği önemi göstermektedir.

3. Devletler, artan siber tehditler karşısında kamu-özel sektör işbirliğinin en iyi strateji olduğunu kabul etmektedir. Siber güvenlik konusunda kamu ve özel sektör arasında karşılıklı bir bağımlılık vardır. Çünkü devletlerin ulusal siber güvenlik ajansları, siber saldırıları gönüllü olarak raporlaması için özel sektörün işbirliğine bağlıdır.

   Özel sektörün yenilikçi kapasitesinden yararlanmak, devletin siber güvenlik alanında yeni kaynaklar edinmesi konusunda önemli iyileştirmeler getirebilecektir. Kamu bürokrasisinin ağır işlemesine nazaran özel sektörün nispeten dinamik yapısından siber güvenlik alanında yararlanmak gerekmektedir. Örneğin ABD Savunma Bakanlığı Pentagon'un, ilk kez finanse edilmesinin ardından yeni bir bilgisayar sistemini işler hale getirmesi ortalama 81 ay sürmektedir. Günümüzün teknoloji devi iPhone ise 24 ayda geliştirilmiştir. Dolayısıyla özel sektörün teknolojideki hızı, bir kamu kurumunun söz konusu teknoloji için bütçe hazırlaması ve bunun için kongreden onay alması için geçen zamandan daha kısadır.

   Siber güvenlik alanında yetenek eksikliği bulunan Singapur, kamu ve özel sektör arasında başarılı bir ortaklık örneği sergileyerek bu eksikliğini gidermiştir. Kamudaki yükseköğretim kurumlarının kısa sürede yeterli insan gücünü yetiştiremediğinin bilincinde olan Singapur, özel sektörden siber güvenlik alanında bir eğitim programı talep etmiş ve sonuç olarak kamu sektörü kısa sürede yetenekli siber güvenlik uzmanları kazanmıştır.

4. Birleşik Krallık'ta bulunan Küresel Siber Güvenlik Kapasite Merkezi'nin ifadesiyle "*siber güvenlik konusunda devletlerin en önemli başarı faktörlerinden bir tanesi siber güvenliğin insan boyutuna (insanın yetenekleri, eğitimi, düşünce yapısı vb.) odaklanmaktır*". Bu kapsamda ABD Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA), ülke genelinde siber güvenlik alanında farkındalık oluşturmak için "*Siber Güvenlik Farkındalık Ayı*" kampanyaları düzenlemektedir. Bu kapsamda hazırlanan sosyal medya gönderileri, kısa videolar, blog gönderileri ve e-postalar siber güvenlik alanında farkındalığı arttırmayı hedeflemektedir.

5. ABD Savunma Bakanlığı'na bağlı bir kuruluş olan DARPA (*İleri Savunma Araştırma Projeleri Ajansı*)'nın Ocak 2016'da düzenlediği "*Cyber Grand Challenge*" adlı yarışma siber güvenlik açıklarının keşfedilmesi amacıyla düzenlenmiştir ve bu yarışmada keşfedilen güvenlik açıklarının iyileştirilmesine yardımcı olmuştur.

6. Devletlerin dikkat etmesi gereken önemli bir husus da devletlerarasında siber ortamda herhangi bir kural oluşturmanın ve bu kuralın uygulanıp uygulanmadığını bilmenin güç olduğudur. Siber ortamda oluşturulan kurallara destek verdiğini beyan eden devletler, aynı zamanda rakiplerine karşı da geniş ölçekli siber saldırlar düzenlemişlerdir. Örneğin 2015 yılının Aralık ayında Birleşmiş Milletler Genel Kurulu, 11 gönüllü üyenin onayıyla bağlayıcı olmayan uluslararası siber normları kabul etmiştir. Bu normların oluşturulmasına yardım eden ve daha sonra yayınlanmasını onaylayan Rusya, aynı ay Ukrayna'daki bir elektrik şebekesine siber saldırı düzenlemiş ve yaklaşık 225 bin kişiyi elektriksiz bırakmıştır. Bu itibarla uzmanlar, siber saldırıların hiç olmayacağını varsaymak yerine yapılan siber saldırılar sonucundaki hasarın miktarına odaklanmak gerektiğini vurgulamaktadır.

4. SONUÇ

Devletin siber ortama taşınmasıyla birlikte, toplumsal hayatın idamesi açısından önem arz eden birçok kamu hizmeti ve bu hizmetlerin altyapıları (elektrik şebekeleri, sağlık ve bankacılık, iletişim ve ulaşım, eğitim, oy verme ve sayım işlemleri, medya, adliye verileri vb.) da siber ortama taşınmıştır. Nasıl ki fiziki ortamda devletin kamu hizmetlerini gerektiği gibi sunabilmesi açısından güvenlik en önemli ihtiyaç ise, devletin sanal ortamda veya sanal ortam vasıtasıyla sunduğu kamu hizmetlerinin gerektiği gibi sunulabilmesi açısından da siber ortamın güvenliği en önemli ihtiyaçtır. Siber ortamın güvenliği ise kısaca "*siber güvenlik*" kavramıyla ifade edilmektedir.

Ulusal güvenliğin sağlanabilmesi noktasında siber güvenlik kritik bir rol oynamaktadır. Siber güvenlik uygulamalarının muhteviyatı teknolojik gelişmlerle uyumlu olarak hızla dönüşmektedir. Birçok yeni teknoloji gibi yapay zeka teknolojisi de siber güvenlik alanında yeni görevler üstlenmektedir. Devletlerin siber ortamda özel sektörden daha fazla veri depolamaları nedeniyle artan veri yığını ve bu veri yığının güvenliğinin sağlanmasında, günümüzün fenomeni olan yapay zekâ teknolojileri kritik bir bileşen haline dönüşmüştür.

Ulusal güvenliğin sağlanması ve kamu düzeninin, huzurunun temini için önemli rol oynayan birçok altyapı (*elektrik şebekeleri, sağlık ve bankacılık sistemi, barajlar, ulaşım, iletişim vb.*) dijitalleşip birbirine bağlandığı için bu altyapılar "*kritik altyapı*" olarak adlandırılmıştır. Kritik altyapıların komuta kontrol sistemleri siber ortama bağlıdır ve bu nedenle bir ülkenin kritik altyapılarının siber güvenliğinin sağlaması, sosyal ve ekonomik gelişmişliğinin bir göstergesi olduğu gibi, ulusal güvenlik stratejisinin de bir bileşeni haline gelmiştir. Kritik altyapılar gibi toplumsal işleyiş ve kamu hizmetlerinin sunumu açısından siber ortamın arz ettiği önemin farkında olan siber saldırganlar da bu nedenle en önemli hedef olarak kamu sektörünü ve halkı seçmektedirler. Nitekim Avrupa Parlamentosunun 2021 ve 2022 yılları için yaptığı değerlendirmede, siber tehditlerden etkilenen ilk 5 sektör arasında kamu sektörü ilk sırada yer almıştır.

Kritik altyapıların güvenliği aynı zamanda bir ülkenin askeri gücü ve askeri gücün sahaya yansıtması açısından da önemlidir. Kritik altyapıların dijital ortamda birbirine bağlı oluşu askeri ve sivil altyapı arasındaki ayrımı ortadan kaldırmıştır (*yukarıda ABD ordusunun faaliyetlerinin çoğunlukla sivil altyapıya dayanması örneğinde olduğu gibi*). Günümüzde askeri stratejilerin temel direği olan kritik altyapıların güvende olmaması, askeri gücün sahaya yansıtılmasını kısıtlayabilir ve olası bir çatışmada kritik altyapılar askeri bir hedef haline gelebilir. Siber saldırıların günümüz silahlı çatışmalarının bir parçası olduğu düşünüldüğünde (*Rusya'nın Ukrayna'ya yönelik saldırılarında olduğu gibi*) kritik altyapıların siber güvenliğini sağlamanın (*elbette ki fiziki güvenliğini sağlamakta olduğu gibi*) bir ülke açısından hava savunma sistemi kadar önem arz ettiği söylenebilir.

Siber saldırıların ulusal güvenlik açısından önem arz ettiği en önemli konulardan bir tanesi de toplumdaki "*güven*" unsuruna verdiği tahribattır. Siber saldırılar yoluyla ülkelerin seçim süreçlerine yapılan müdahaleler demokratik kurumlara ve sürece olan güveni baltalayabilecek; yapılan ar-ge faaliyetlerine siber saldırılar yoluyla izinsiz erişim, yeni keşif ve icatların sağladığı faydalara olan güveni sarsabilecek ve devlet tarafından depolanan verilerin sızdırılması veya siber saldırılar yoluyla ele geçirilmesi, vatandaşların devlete olan güvenini azaltabilecektir. Güven unsurunun ortadan kalkması ise hem devleti hem de toplumu daha zayıf hale getirebilmekte ve dezenformasyonlar karşısında daha savunmasız kılabilmektedir.

Siber güvenlik söz konusu olduğu zaman saldırılar karşısındaki hız ve çeviklik önem arz etmektedir. Günümüzde siber güvenlik personeline bu hız ve çevikliği kazandıracak bir yardımcı vardır: Yapay zekâ. Yapay zekâyı günümüz açısından siber güvenliğe yardımcı bir unsur olarak değerlendirmek en doğru tespit olacaktır. Çünkü siber güvenlik açısından tek başına siber güvenlik uzmanları veya yapay zekâ yeterli değildir. Siber saldırılarda her ne kadar günümüzde olmasa da (*çünkü günümüzde saldırganlar yapay zekâ olmadan da etkili saldırılar yapabilmektedir*) gelecekte yapay zekânın daha çok kullanılacak olması durumunda, siber güvenlikte de yapay zekânın daha yoğun kullanılacağı tahmin edilmektedir.

Siber saldırılar açısından vadettiği potansiyele binaen devletlerin güvenli olmayan bir yapay zekâ yarışına girmeleri ise, hem bu yarışa giren hem de diğer ülkeler açısından bir ulusal güvenlik riski anlamına gelecektir. Güvenlik ve işbirliği yapay zekâ teknolojilerindeki temel düstur olmalıdır çünkü bir güvenlik tehdidi olarak yapay zekâ konusunda yaşanacak bir yarış kimsenin kazanamayacağı bir yarıştır (Scharre, 2019).

Siber güvenlik alanında örnek olarak verilen ülke uygulamaları göz önüne alınarak siber güvenliğin sağlanması konusunda sıralanabilecek bazı öneriler ise şunlardır;

- "*Siber güvenlik söz konusu olduğunda hazırlık için en iyi zaman dündür*" (Alperovitch, 2022). Bu söz, siber güvenlik alanında kurumların sürekli olarak hazırlıklı olmak ve yeniliği teşvik etmek durumunda oldukları şeklinde yorumlanabilir. Kamu sektörü (devlet) ise genelde hantal işleyen yapısı nedeniyle eleştirilir. Bu açıdan kamu sektörü siber güvenlik alanında yeniliği teşvik etmek adına belirli aralıklarla yarışmalar düzenleyebilir (*yukarıda Cyber Grand Challenge örneğindeki gibi*). Kazananlara hatırı sayılır miktarda ödüllerin verileceği bu yarışmalar sayesinde kamu sektörü, siber güvenlik alanındaki açıkların bulunmasına ve güvenliği sağlayıcı yeni tekniklerin geliştirilmesine önayak olabilir (Bansemer, 2021).
- Devlet siber güvenlik alanında özel sektörün yenilikçi kapasitesinden yararlanması da önem taşımaktadır. Yukarıda Singapur örneğinde de bahsedildiği üzere kamu sektörü siber güvenlik alanında özel sektörden örneğin eğitim programları satın alabilir ve bunun karşılığında özel sektöre fon sağlayabilir (Işık vd., 2022).
- Devletin siber güvenlik yeteneğini geliştirmesinin bir yolu da eğitimden geçmektedir. Yukarıda bahsedildiği gibi İsrail, henüz ortaokul seviyesinden itibaren okullarda siber güvenlik eğitimi vermeye başlamıştır. Hindistan'da yapılan bir araştırmada kentlerde yaşayan çocukların %99'unun interneti zayıf şifrelerle kullandığı tespit edilmiştir (Hajoary ve Akhiles, 2020:82). Okul çağından itibaren verilen eğitim sayesinde öğrencilerin siber güvenlik alanındaki farkındalığı arttırabilecektir.

- Siber güvenlik alanındaki eğitim sadece okul çağındaki öğrencilerle sınırlı kalmamalı, toplumun her bir ferdini kapsamalıdır. Yukarıda "*Siber Güvenlik Farkındalık Ayı*" örneğinde de görüldüğü gibi kamu kurumları yılın belirli günlerinde toplumun her kesimine yönelik bilgilendirici faaliyetler (*sosyal medya paylaşımları, kentlerdeki reklam panolarına yapıştırılacak afişler vb*.) yapmalıdır. Örneğin belirli aralıklarla üniversitelerde halka açık ve ücretsiz siber güvenlik konferansları verilebilir ve toplumun her kesimi bu konuda bilinçlendirilebilir.
- Devletin siber güvenlik alanında yaşanacak bir krizle mücadele etmesi için gerçek bir kriz yaşaması beklenmemelidir. Bu noktada siber tatbikatlar öne çıkmaktadır. Nasıl ki bir yangın tatbikatı olası bir yangın durumunda bir kuruluşun hazırlık durumunu ve hızını ölçmekte ise siber tatbikatlar da aynı amaca hizmet etmektedir. Tatbikat kapsamında siber ortamı kullanan sistemlere (örneğin elektrik şebekesi) yapılacak bir siber saldırı ile saldırganların sisteme nasıl girdikleri, nasıl kontrol altına alınabilecekleri, verdikleri hasarın boyutu gibi konularda bir müdahale ve kurtarma planı geliştirilebilir.

Son olarak belirtilmelidir ki siber saldırıları durdurmanın olanağı yoktur. Siber güvenlikte de amaç zaten saldırıları durdurmak değil bu saldırılara dayanabilecek sistemler oluşturmaktır. Devletin de bütün siber saldırılara karşı etkin bir savunma yapması gerçekçi bir yaklaşım değildir. Bu nedenle bazı siber güvenlik zafiyetleri yaşaması, devletin siber güvenlikte başarısız olduğu anlamına gelmemelidir. Burada önemli olan husus, günümüz dijital devletinin hazırlığı ve gerekli kaynakları zamanında tedarik etmesidir (Eggers, 2016:153). Böylelikle en sofistike siber saldırılarda dahi siber güvenlik korunabilecektir. Siber güvenliğin söz konusu kapasitesini artırmasında yapay zeka hızla en kritik bileşenlerden birisi haline gelmektedir.

KAYNAKÇA

ACCENTURE (2022a), "*What is Cybersecurity?*", **Accenture Corporate Web Page** (E-Article), (tarihsiz), https://www.accenture.com/au-en/insights/cyber-security-index (Erişim Tarihi: 10.12.2022).

ACCENTURE (2022b), "*Cybersecurity for Connected Energy Ecosystems*", **Accenture Corporate Web Page** (E-Article), (tarihsiz), https://www.accenture.com/be-en/insights/utilities/cybersecurity-connected-energy (Erişim Tarihi: 10.12.2022).

AK, Tarık (2021), "*Yapay Zekâ Teknolojileri, Güvenlik ve Kolluk Kuvvetlerinin Suç Önleme Faaliyetleri*", **SDE Akademi Dergisi**, S.1(1), ss.120-140.

ALPEROVITCH, Dimitri (2022), "*How Russia Has Turned Ukraine into a Cyber-Battlefield the Kremlin's Hackers Are Already Targeting Kyiv*", **Foreign Affairs** (E-Article), 28 Ocak 2022, https://www.foreignaffairs.com/articles/russia-fsu/2022-01-28/how-russia-has-turned-ukraine-cyber-battlefield (Erişim Tarihi: 28.12.2022).

ARDIELLI, Eva ve ARDIELLI, Jiří (2017), "*Cyber Security in Public Administration of Czech Republic*", **Socıálno-Ekonomıckά Revue**, S.15(4), ss.42-50.

BANSEMER, John (2021), "*Soon, the Hackers Won't be Human But AI Can Boost Cyber Defenses, too*", **Foreign Affairs** (E-Article), 10 Aralık 2022, https://www.foreignaffairs.com/articles/united-states/2021-12-10/soon-hackers-wont-be-human (Erişim Tarihi: 28.12.2022).

BOOKER, Lashon B. ve MUSMAN, Scott A. (2020), "*A Model-Based, Decision-Theoretic Perspective on Automated Cyber Response*", **The AAAI-20 Workshop on Artificial Intelligence for Cyber Security (AICS)**, 7-8 Şubat 2020 – New York (US), ss.1-10.

CAN, Aybike (2022), "*Ulusal Güvenlik Açısından Kritik Altyapı ve Siber Alan: Sivil Hazırlıklılık ve Dirençlilik Perspektifinden Kavramsal Bir İnceleme*", **Diplomasi ve Strateji Dergisi**, S.3(2), ss.279-311.

CHAKRABORTY, Anirban (2020), "*Technology to Combat Cyber Attacks by Artificial Intelligence*", **International Journal of Progressive Research in Science and Engineering**, S.1(3), ss.149-153.

CHANG, Kenneth (2014), "*Automating Cybersecurity*", **The New York Times**, 03 Haziran 2014, https://www.nytimes.com/2014/06/03/science/automating-cybersecurity.html?searchResultPosition=1 (Erişim Tarihi: 04.12.2014).

CISA (2021), "*Cybersecurıty Awareness Month 2021: Do Your Part*", **CISA Corporate Web Page** (E-Article), https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Awareness%20Month%202021%20-%20One%20Pager.pdf (Erişim Tarihi: 15.11.2021).

COFFEY, Luke (2019), "*How to Defeat Hybrid Warfare Before it Starts*", **Defence One**, 21 Ocak 2019, https://www.defenseone.com/ideas/2019/01/how-defeat-hybrid-warfare-it-starts/154296/ (Erişim Tarihi: 10.12.2019).

DARICILI, A. Burak ve ÇELİK, Soner (2022), "*National Security 2.0: The Cyber Security of Critical Infrastructure*", **PERCEPTIONS: Journal of International Affairs**, S.26(2), ss.259-276.

DVORSKY, George (2017), "*Hackers Have Already Started to Weaponize Artificial Intelligence*", **Gizmoda Corporate Web Page**, 17 Eylül 2017, https://gizmodo.com/hackers-have-already-started-to-weaponize-artificial-in-1797688425 (Erişim Tarihi: 14.12.2022).

EFE, Ahmet (2021), "*Yapay Zekâ Odaklı Siber Risk ve Güvenlik Yönetimi*", **Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi**, S.5(2), ss.144-165.

EGGERS, William D. (2016), "*Government's Cyber Challenge*", **Deloitte Review**, S.16, ss.138-155.

ERDOĞAN, Uğur (2021), "*Dijital Dönüşüm Çağında Dijital Girişimcilik ve Dijital İnovasyon*", **Girişimcilik ve İnovasyon Araştırmaları: Yeni Trendler ve Dijital Dönüşüm** (Ed. Zekeriya MIZIRAK, Ali KAHRAMAN, Birol MERCAN, Fatih KALECİ), Necmettin Erbakan Üniversitesi Yayınları, Konya, ss.1-26.

ERDOĞAN, Uğur (2022), "*Lojistikte Dijital Dönüşüm: Akıllı Lojistik*", **Dijital Dünyanın Kapılarını Aralamak Farklı Bakış Açılarından Dijitalleşme Üzerine Güncel Yazılar** (Ed. Özlem AKGÜN, Meltem DİKTAŞ), Nobel Akademik Yayınları, Ankara, ss.577-603.

EUROPEAN PARLIAMENT (2023), "*Cybersecurity: Main and Emerging Threats*", **News European Parliament**,https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats (Erişim Tarihi: 02.02.2023).

FADIA, Ankit, NAYFEH, Mahir ve NOBLE, John (2020), "*Follow the Leaders: How Governments Can Combat Intensifying Cybersecurity Risks*", **McKinsey & Company** (E-Article), 16 Eylül 2020, https://www.mckinsey.com/industries/public-and-social-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks (Erişim Tarihi: 15.12.2022).

FILKENSTEIN, Claire Oakes ve GOVERN, Kevin H. (2015), "*Introduction: Cyber and the Changing Face of War*", **Faculty Scholarship at Penn Law**, https://scholarship.law.upenn.edu/faculty_scholarship/1566 (Erişim Tarihi: 30.11.2022).

FLOURNOY, Michele ve SULMEYER, Michael (2018), "*Battlefield Internet a Plan for Securing Cyberspace*", **Foreign Affairs**, 14 Ağustos 2018, https://www.foreignaffairs.com/articles/world/2018-08-14/battlefield-internet adresinden alındı (Erişim Tarihi: 25.11.2022).

GEZİCİ, Hikmet Salahaddin (2022), "*Yapay Zekâ*", **Kurumsal Bilgi Yönetimi Teknolojik Eğilimler** (Ed. Mustafa KOCAOĞLU, Sefa USTA), Eğitim Yayınevi, Konya, ss.79-99.

GEZİCİ, Hikmet Salahaddin (2022), "*Yapay Zekâ ve Vergi Yönetimi: Finlandiya Örneği*", **Vergi Raporu**, S.277, ss.46-66.

HAJOARY, Pinosh Kumar ve AKHILESH, K. B. (2020), "*Role of Government in Tackling Cyber Security Threat*", **Smart Technologies: Scope and Applications** (Eds. K. B. Akhilesh, D. P. Möller), Springer Publisher, Singapore, ss.79-96.

HENNESSEY, Susan (2017), "*Deterring Cyberattacks How to Reduce Vulnerability*", **Foreign Affairs**, https://www.foreignaffairs.com/reviews/review-essay/2017-10-16/deterring-cyberattacks (Erişim Tarihi: 25.11.2022).

ILVES, Toomas H. (2013), "*Cybersecurity: A View from the Front*", **The New York Times**, 11 Nisan 2013, https://www.nytimes.com/2013/04/12/opinion/global/cybersecurity-a-view-from-the-front.html?searchResultPosition=16 (Erişim Tarihi: 15.12.2022).

IŞIK, Öykü, JELASSI, Tawfik ve KELLER-BIRRER, Valerie (2022), "*Five Lessons of Cybersecurity the Public Sector Can Offer*", **The European Business Review**, 4 Mayıs 2022, https://www.europeanbusinessreview.com/five-lessons-of-cybersecurity-the-public-sector-can-offer/ (Erişim Tarihi: 05.12.2022).

KARASOY, Hasan Alpay (2021), **Kamu Güvenliğinde Yeni Paradigmalar: Hibrit Savaş, Asimetrik Savaş, Vekalet Savaşı, İstihbarat ve Terörle Mücadele**, Nobel Yayınları, Ankara.

KARASOY, Hasan Alpay (2022), "*Hibrit, Asimetrik ve Vekâlet Savaşları: 2022 Rusya Ukrayna Savaşını Üçlü Sacayağı Üzerinde Bir İnceleme*", **Medeniyet Araştırmaları Derrgisi**, S.7(2), ss.44-56.

KOCH, Tobias, MOLLER, Dietmar P. ve DEUTSCHMANN, Andreas (2020), "*Smart Technologies as a Thread for Critical Infrastructures*", **Smart Technologies: Scope and Applications** (Eds. K. B. Akhilesh, D. P. Möller), Springer Publisher, Singapore, ss.275-289.

KÖKER, Ahmet Emre (2022), "*Ulusal Siber Güvenlik Stratejisi: Fransa*", **UPA Strategic Affairs**, S.3(1), ss.42-78.

KÜÇÜKŞAHİN, Ahmet (2006), "*Güvenlik Bağlamında Risk ve Tehdit Kavramları Arasındaki Farklar Nelerdir ve Nasıl Belirlenmelidir?*", **Güvenlik Stratejileri Dergisi**, S.2(4), ss.7-41.

KÜPELİ, Hayrettin (2019), "*Kritik Altyapılar ve Terörizm Tehdidi*", **Genel Olarak İç Güvenlik Yönetimi** (Ed. T. Avaner, B. Övgün), Gazi Kitabevi Yayını, Ankara, ss.85-110.

LEE, Martin ve TALOS, Cisco (2022), "*Russia's War in Ukraine: 3 Cybersecurity Takeaways for Enterprises*", **Venturebeat** (E-Article), 13 Kasım 2022, https://venturebeat.com/security/russias-war-in-ukraine-3-cybersecurity-takeaways-for-enterprises/ (Erişim Tarihi: 05.12.2022).

LEENEN, Louise ve MEYER, Thomas (2019), "*Artificial Intelligence and Big Data Analytics in Support of Cyber Defense*", **Developments in Information Security and Cybernetic Wars** (Ed. M. Sarfaz), IGI Global Publisher, Pennsylvania (US), ss.42-63.

LONGLEY, Robert (2021), "*National Security Definition and Examples*", **Thoughtco** (E-Article), 24 Eylül 2021, https://www.thoughtco.com/national-security-definition-and-examples-5197450 (Erişim Tarihi: 25.11.2021).

LYNN, William J. (2010), "*Defending a New Domain the Pentagon's Cyberstrategy*", **Foreign Affairs**, 1 Eylül 2010, https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain (Erişim Tarihi: 02.12.2022).

LYNN, William J. (2011), "*The Pentagon's Cyberstrategy, One Year Later*", **Foreign Affairs**, 28 Eylül 2011, https://www.foreignaffairs.com/united-states/pentagons-cyberstrategy-one-year-later (Erişim Tarihi: 10.12.2022).

NYE, Joseph S. (2021), "*The End of Cyber-Anarchy? How to Build a New Digital Order*", **Foreign Affairs**, 14 Aralık 221, https://www.foreignaffairs.com/articles/russian-federation/2021-12-14/end-cyber-anarchy (Erişim Tarihi: 02.12.2022).

ÖZTAŞ, Nail (2014), **Örgüt: Örgüt ve Yönetim Kuramları II**, Otorite Yayınları, Ankara.

PATTERSON, Nicholas (2022), "*What is Cyber Security and Why is it Important?*", **Southern New Hampshire University**, 21 Temmuz 2022, https://www.snhu.edu/about-us/newsroom/stem/what-is-cyber-security (Erişim Tarihi: 04.12.2022).

PEARSON, James (2022), "*Russia Downed Satellite Internet in Ukraine -Western Officials*", **Reuters**, 10 Mayıs 2022, https://www.reuters.com/world/europe/russia-behind-cyberattack-against-satellite-internet-modems-ukraine-eu-2022-05-10/ (Erişim Tarihi: 30.11.2022).

PEARSON, James ve BING, Christopher (2022), "*The Cyber War between Ukraine and Russia: An Overview*", **Reuters**, 10 Mayıs 2022, https://www.reuters.com/world/europe/factbox-the-cyber-war-between-ukraine-russia-2022-05-10/ (Erişim Tarihi: 30.11.2022).

RAINER, R. Kelly, PRINCE, Brad, SPLETTSTOESSER-HOGETERP, Ingrid, SANCHEZ-RODRİGUEZ CRİSTOBAL, Ebrahimi Sepideh (2020), **Introduction to Information Systems Supporting and Transforming Business**, Wiley Publisher, Canadian, Fifth Canadian Edition.

REUTERS (2022), "*Montenegro's State Infrastructure Hit By Cyber Attack – Officials*", **Reuters**, 26 Ağustos 2022, https://www.reuters.com/world/europe/montenegros-state-infrastructure-hit-by-cyber-attack-officials-2022-08-26/ (Erişim Tarihi: 30.11.2022).

SCHARRE, Paul (2019), "*Killer Apps the Real Dangers of an AI Arms Race*", **Foreign Affairs**, 16 Nisan 2019, https://www.foreignaffairs.com/articles/2019-04-16/killer-apps (Erişim Tarihi: 04.12.2022).

SCHNEIDER, Jacquelyn (2021), "*A World Without Trust the Insidious Cyberthreat*", **Foreign Affairs**, 14 Aralık 2021, https://www.foreignaffairs.com/articles/world/2021-12-14/world-without-trust (Erişim Tarihi: 30.11.2022).

SHABBIR, Jahanzaib ve ANWER, Tarique (2015), "*Artificial Intelligence and its Role in Near Future*", **Journal of Latex Class Files**, S.14(8), ss.1-11.

SIEBOLD, Sabine (2022), "*Cyber as Important as Missile Defences - ex-NATO General*", **Reuters**, 21 Aralık 2022, https://www.reuters.com/world/cyber-important-missile-defences-ex-nato-general-2022-11-21/ (Erişim Tarihi: 10.12.2022).

SINGAR, Arjun V. ve AKHILESH, K. B. (2020), "Role of Cyber-Security in Higher Education", **Smart Technologies: Scope and Applications** (Eds. K. B. Akhilesh, D. P. Möller), Springer Publisher, Singapore, ss.249-264.

ŞEN, Y. Furkan ve YURTOĞLU, Doğanay (2020), "*Teknoloji ve Güvenlik İlişkisi Bağlamında Yapay Zekânın İstihbarat Analizindeki Önemi*", **Güvenlik Çalışmaları Dergisi**, S.22(1), ss.24-48.

TRUONG, Thanh Cong, DIEP, Quoc Bao ve ZELINKA, Ivan (2020), "*Artificial Intelligence in the Cyber Domain: Offense and Defense*", **Symmetry**, S.12(3), ss.1-24.

ÜNVER, Gül Nazik (2017), "*Ulusal Siber Güvenlik Strateji Belgelerinde İnsan Hakları*", **Cyberpolitik Journal**, S.2(4), ss.104-129.

VIOLINO, Bob (2022), "*Artificial Intelligence is Playing a Bigger Role in Cybersecurity, But the Bad Guys May Benefit the Most*", **CNBC**, 18 Eylül 2022, https://www.cnbc.com/2022/09/13/ai-has-bigger-role-in-cybersecurity-but-hackers-may-benefit-the-most.html (Erişim Tarihi: 05.12.2022).

YAZAR BEYANI / AUTHORS' DECLARATION:

Bu makale Araştırma ve Yayın Etiğine uygundur. Beyan edilecek herhangi bir çıkar çatışması yoktur. Araştırmanın ortaya konulmasında herhangi bir mali destek alınmamıştır. Yazar(lar), dergiye imzalı "*Telif Devir Formu*" belgesi göndermişlerdir. Mevcut çalışma için mevzuat gereği etik izni alınmaya ihtiyaç yoktur. Bu konuda yazarlar tarafından dergiye "*Etik İznine Gerek Olmadığına Dair Beyan Formu*" gönderilmiştir. / This paper complies with Research and Publication Ethics, has no conflict of interest to declare, and has received no financial support. The author(s) sent a signed "*Copyright Transfer Form*" to the journal. There is no need to obtain ethical permission for the current study as per the legislation. The "*Declaration Form Regarding No Ethics Permission Required*" was sent to the journal by the authors on this subject.

YAZAR KATKILARI / AUTHORS' CONTRIBUTIONS:

Kavramsallaştırma, orijinal taslak yazma, düzenleme, nihai onay ve sorumluluk – **Y1** ve **Y2**. / Conceptualization, writing-original draft, editing, final approval and accountability – **A1** and **A2**.