INJOCMER International Journal of Communication and Media Research
Uluslararası İletişim ve Medya Araştırmaları Dergisi

CİLT/VOLUME: 5 MART/MARCH 2025 SAYI/ISSUE: 1

Atıf Bilgisi: Özkan, S. ve Yetgin, M. A. (2025). Siber Uzay İletişimi Bağlamında Çok Uluslu Şirketler ve Ulus Devletler**,** *Injocmer*, 5(1), 65-86.

Makale Geliş Tarihi:
20 Aralık 2024

Makale Kabul Tarihi:
31 Ocak 2025

ARAŞTIRMA MAKALESİ

SİBER UZAY İLETİŞİMİ BAĞLAMINDA ÇOK ULUSLU ŞİRKETLER VE ULUS DEVLETLER*

Sevcan ÖZKAN[1]

Muhammed Ali YETGİN**[2]

ÖZ

Gelişen bilimsel bilgi ve teknolojik gelişmeler, uluslararası ilişkileri derinden etkilemiş ve küresel ilişkilere daha birbirine bağlı ve veri odaklı bir yaklaşım sağlamıştır. Bu yaklaşım sonucunda küreselleşen günümüz dünyasında çok uluslu şirketlerin ve ulus devletlerin rekabeti, geleneksel maddi ürünlerin ve fiziksel alanların ötesine geçerek siber uzaya taşınmaktadır. Bu makalenin konusu, çok uluslu şirketlerin ve ulus devletlerin siber uzaydaki etkisini, rekabetini ve stratejilerini araştırmaktır. Küresel etkileşimler için önemli bir alan haline gelen siber uzayda, şirketlerin ve devletlerin çok yönlü etkisini anlamak için araştırmada, çok uluslu şirketlerde finans, otomotiv, enerji ve telekomünikasyon sektörleri ve ulus devletlerde ABD, Çin, Rusya, İran'a odaklanılmıştır. Çalışma, çok uluslu şirketlerin ve ulus devletlerin siber uzayda oynadıkları önemli role ışık tutmaya çalışarak, küresel ilişkilerin birbirine bağlılığını ve dijital çağda rekabetin gelişen doğasını vurgulamaktadır. Araştırmada nitel araştırma yöntemi olarak içerik analiz yöntemi uygulanmıştır. Araştırmadaki bulguların daha açıklayıcı bir şekilde ortaya konulması için Tematik Analiz yönteminden yararlanılarak SWOT Analizi uygulanmıştır. Çok uluslu şirketler, istihdam yaratma, vergi gelirleri ve yabancı yatırım yoluyla ülke ekonomilerine katkıda bulunarak küresel ekonomide önemli bir rol oynamakta ve teknolojik ilerlemelerin temelinde yer almaktadır. Siber uzayda çok uluslu şirketler, işlerini küresel olarak yürütmek için dijital platformları ve teknolojileri kullanarak ulusal sınırları aşmaktadır. Bu ekonomik etki, çok uluslu şirketler ve ulus devletler arasındaki ilişkide temel bir faktördür. Ulus devleler de en son teknolojilere erişimin yanı sıra kendi ekonomilerinde yeniliği teşvik etmek için genellikle çok uluslu şirketlere bağımlıdır. Siber güvenlik, yapay zeka, veri analitiği gibi alanlarda çok uluslu şirketler ve ulus devletler arasındaki işbirlikçi girişimler, siber uzayda karşılıklı faydalarla ilerlemelere yol açmaktadır. Siber

* Bu makale Sevcan Özkan'a ait "Çok uluslu şirketlerin ve ulus devletlerin siber uzayda etkisi" başlık tez çalışmasından üretilmiştir.

** Sorumlu Yazar
[1] Uluslararası İlişkiler Bilim Uzmanı, sevcan.ozkan@outlook.com.tr, ORCID: 0000-0002-8459-6176
[2] Karabük Üniversitesi, Safranbolu Türker İnanoğlu İletişim Fakültesi, m.ali.yetgin@karabuk.edu.tr, ORCID: 0000-0002-8120-4704

uzayın ortaya çıkışı, çok uluslu şirketler ve ulus devletler için yeni sınırlar açarak küresel etkileşimlerle devrim yaratmıştır.

Anahtar Kelimeler: Siber Uzay İletişimi, İletişim, Çok Uluslu Şirketler

MULTINATIONAL COMPANIES AND NATION-STATES IN THE CONTEXT OF CYBERSPACE COMMUNICATION

ABSTRACT

Advances in scientific knowledge and technological advances have profoundly affected international relations and have led to a more interconnected and data-driven approach to global relations. As a result of this approach, in today's globalized world, the competition of multinational corporations and nation-states is moving beyond traditional material goods and physical spaces to cyberspace. The subject of this article is to explore the influence, competition, and strategies of multinational corporations and nation-states in cyberspace. To understand the multifaceted impact of companies and states in cyberspace, which has become an important space for global interactions, the research focuses on the financial, automotive, energy, and telecommunications sectors in multinational companies and the US, China, Russia, and Iran in nation-states. The study sheds light on the important role that MNCs and nation-states play in cyberspace, highlighting the interconnectedness of global relations and the evolving nature of competition in the digital age. Multinational corporations play an important role in the global economy, contributing to national economies through job creation, tax revenues, and foreign investment, and are at the heart of technological advances. In cyberspace, multinational corporations transcend national borders using digital platforms and technologies to conduct their business globally. This economic impact is a key factor in the relationship between MNCs and nation-states. Nation-states, in turn, are often dependent on MNCs for access to the latest technologies, as well as for fostering innovation in their economies. Collaborative initiatives between MNCs and nation-states in cybersecurity, artificial intelligence, data analytics, etc. are leading to mutually beneficial advances in cyberspace. The emergence of cyberspace has revolutionized global interactions by opening new frontiers for multinational corporations and nation-states. Content Analysis method was applied in the research. To present the findings of the research more descriptively, the Thematic Analysis method was utilized and analyzed with SWOT Analysis.

Keywords: Cyberspace Communication, Communication, Multinational Companies

1. GİRİŞ

ABD Savunma Bakanlığı Askeri ve İlgili Terimler Sözlüğüne göre siber uzay "*internet, telekomünikasyon ağları, bilgisayar sistemleri, gömülü işlemciler ve denetleyiciler dahil olmak üzere birbirine bağlı bilgi teknolojisi (BT) altyapıları ağından ve yerleşik verilerden oluşan bilgi ortamında küresel bir etki alanı*" olarak tanımlanmıştır (U.S. Department of Defence [DOD], 2010, s. 58). Aynı zamanda siber uzay; siber strateji, siber güvenlik, siber savunma, siber suçlar, siber zorbalık, siber istihbarat, siber terörizm ve siber savaş gibi faaliyetleri barındıran dört geleneksel kara, deniz, hava ve uzay alanına eşit olarak beşinci savaş alanını temsil etmektedir (Quadri & Rasaq, 2020, s. 105).

Günümüzde, siber uzay teknolojileri dünya çapındaki hükümetler, kuruluşlar, işletmeler ve paydaşları tarafından, iş süreçlerini daha verimli hale getirmek, üretkenliği artırmak ve karlılığı optimize ederek ekonomik büyümeyi desteklemek için daha fazla benimsenmektedir. Dolayısıyla ekonomik büyümeyi, toplumsal refahı, etkileşimi ve küresel iş birliğini mümkün kılması yönünde yeni araçlar sağlayarak günümüz dünyasını olağanüstü şekillerde dönüştürmektedir (Mbanaso & Dandaura, 2015, s. 17).

Gelişmiş ve gelişmekte olan ulus devletler, terör ağları, bireyler, yatırımcılar, üniversiteler, şirketler ve diğer paydaşlar siber uzayın kullanımına öncelik vermektedir (Quadri

& Rasaq, 2020, s. 98). Siber uzay teknolojileri, yenilikler, girişimler, sosyal ağlar için yeni bir odak noktası haline gelirken aynı zamanda siber güvenlik konuları da önem kazanmaya başlamıştır. Siber uzayın kullanımı artıkça, ulusal kritik altyapılara, veri tabanlarına, endüstriyel operasyonlarına, komuta ve kontrol sistemlerine yönelik tehditler ve endüstriyel casusluk faaliyetleri de artmaktadır (Argaman & Siboni, 2014, s. 44). Bilgi teknolojisine toplumsal olarak artan bağımlılık, siber suçlar içinde yeni bir odak noktası haline gelmesine neden olmuş ve bu durum, yenilik fırsatları sunarken güvenlik stratejilerinin de değişmesine sebep olmuştur.

Siber uzayın fırsatları ve yenilikleri, tehditleri ve riskleri, çatışmaları ve savaşı, güvenlik açıklarını, hızla gelişen siber komploları, gelişmiş ve gelişmekte olan ülkeler arasındaki dijital eşitsizlik faktörlerini barındırması ülkelerin, şirketlerin ve bireylerin siber güvenlik algısını yeniden şekillendirmektedir. Dolayısıyla siber uzay, insanlığa büyük faydalar vaat eden, aynı zamanda bilgi alanı içinde ulusların üstünlük ve hakimiyet arayışından kaynaklanan tehlikeleri de içeren yeni bir dünya sahnesi sunmaktadır (Mbanaso & Dandaura, 2015, s. 18).

Makalenin temel amacı, giderek önem kazanan siber uzayda çok uluslu şirketlerin ve ulus devletlerin oynadığı rolü, bu aktörler arasındaki iletişimi, rekabeti ve uyguladıkları stratejileri derinlemesine incelemektir. Özellikle, siber uzayın küresel ilişkiler üzerindeki etkilerini ve bu alandaki gelişmelerin geleneksel rekabet anlayışını nasıl dönüştürdüğünü ortaya koymayı hedeflemektedir. Siber uzayın küresel ilişkilerdeki merkeziyetinin arttığı bir dönemde bu çalışmanın, güncel bir konuya ışık tutması büyük önem taşımaktadır.

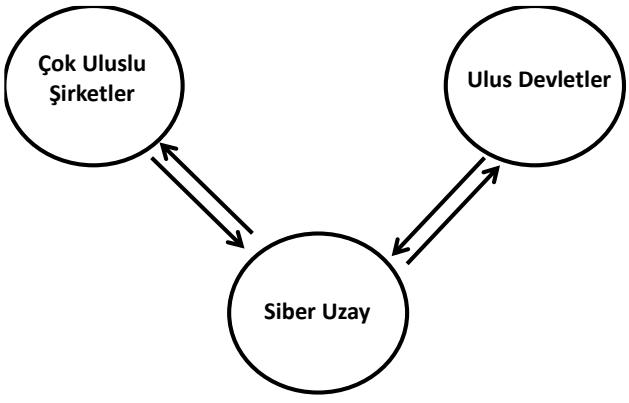
2. YÖNTEM

Araştırmanın ana problemleri aşağıdaki gibidir:

P_1: *Çok uluslu şirketlerin siber uzayda etkisi hangi düzeydedir?*

P_2*: Ulus devletlerin siber uzayda etkisi hangi düzeydedir?*

Çok uluslu şirketlerin ve ulus devletlerin siber uzayda "bilgi, güç, hız, güvenlik" temalarıyla etkisi söz konusudur. Araştırmanın problemleri doğrultusunda oluşturulan modeli aşağıda görülmektedir. Bkz. Şekil 1.



Şekil 1. Araştırmanın Modeli
Kaynak: Şekil yazar tarafından oluşturulmuştur.

2.1. Kavramsal Çerçeve

Araştırmanın modelinde ön görülen problemlere dair değişkenleri arası ilişkiler açıklanmıştır.

2.1.1 Siber Uzay & Çok Uluslu Şirketler

Siber uzay, çok uluslu şirketler için büyük bir bilgi kaynağıdır. Şirketler, siber uzay aracılığıyla pazarlar, müşteriler ve rakip şirketler hakkında büyük miktarda veri toplayabilir, analiz edebilir. Bu, şirketlerin bilinçli iş kararları almalarını, değişen trendlere uyum sağlayabilmelerini ve yenilikçi iş stratejilerini geliştirmeleri sağlar. Ayrıca çok uluslu şirketler genellikle çevrimiçi bilgi paylaşım platformları kurarak küresel işgücü arasında iş birliği ve bilgi alışverişinde bulunabilirler.

Siber uzay, çok uluslu şirketlere güçlü bir rekabet avantajı sunmaktadır. Şirketler, dijital pazarlama, e-ticaret, müşteri ilişkileri yönetimi gibi alanlarda siber uzayı kullanarak küresel çapta varlık göstermektedir. Geniş kaynakları ve küresel erişimleri, çevrimiçi pazarlara hakim olmalarını ve dijital ekosistemleri şekillendirmelerini sağlamaktadır. Çok uluslu şirketler, çıkarlarını savunarak ve dijital ortamı şekillendirerek siber uzayla ilgili düzenlemeleri, standartları ve politikaları etkileyebilir. Ekonomik nüfuzları sayesinde, hükümetlerle müzakere etme ve çeşitli ülkelerdeki dijital altyapının gelişimini etkileme gücü elde etmektedirler.

Siber uzay, çok uluslu şirketlerin güvenliği için hem fırsatlar hem de zorluklar yaratmaktadır. Siber saldırılar, veri ihlalleri, bilgisayar korsanlığı ve fikri mülkiyet hırsızlığı gibi siber tehditler için yeni yollar sağlar. Bu doğrultuda çok uluslu şirketler, değerli varlıklarını korumak ve verilerinin bütünlüğünü, gizliliğini sağlamak için güçlü siber güvenlik önlemleri almak zorundadır. Sunduğu fırsatlar arasında ise çok uluslu şirketler, şifreli iletişim, güvenli ağlar ve gelişmiş kimlik doğrulama sistemleri dahil birçok gelişmiş güvenlik önlemleri için siber uzayı kullanmaktadır.

Siber uzay, çok uluslu şirketlerin benzeri görülmemiş bir hızda çalışmasını sağlayarak iletişimi, karar vermeyi ve işlemsel süreçleri kolaylaştırır. İnternet ve dijital teknolojiler ile çok uluslu şirketler, ticari operasyonlarını sınırlar ötesinde anında yürütebilir. Bu hız, tedarik zinciri yönetimini geliştirir, e-ticaret ve diğer platformlar aracılığıyla ürün ve hizmetlerin küresel ölçekte hızla sunulmasını sağlar.

2.1.2 Siber Uzay & Ulus Devletler

Ulus devletler dijital alanda bilginin büyümesine katkıda bulunan Ar-Ge, eğitim ve teknolojik gelişmelere yatırım yapmaktadır. Hükümetler genellikle yeni teknolojilerin geliştirilmesine ve siber uzayda bilgi paylaşımına yol açan inovasyon ve siber güvenlik araştırmalarını teşvik eden girişimleri finanse eder.

Ulus devletler, uluslararası ilişkilerde güç ve etki uygulamalar için siber uzayda faaliyet göstermektedir. Hakimiyetlerini savunmak veya stratejik hedeflerini takip etmek için casusluk, gözetleme ve siber saldırılar gibi çeşitli faaliyetlerde bulunmaktadırlar. Siber yetenekler, kritik altyapıyı hedef alabildikleri, iletişim ağlarını bozabildikleri veya hassas bilgileri çalabildikleri için ulus devletlere güçlerini yansıtmak için araçlar sağlamaktadır. Ayrıca ulus devletler, dijital dünyayı yöneten kuralları, normları ve yönetişim yapılarını şekillendirmeye çalışmaktadır. Bu etki mücadelesi, uluslararasındaki güç için daha geniş rekabeti yansıtır ve internet özgürlüğü, veri gizliliği ve devletler arasındaki güç dengesi gibi konular üzerinde etkileri vardır.

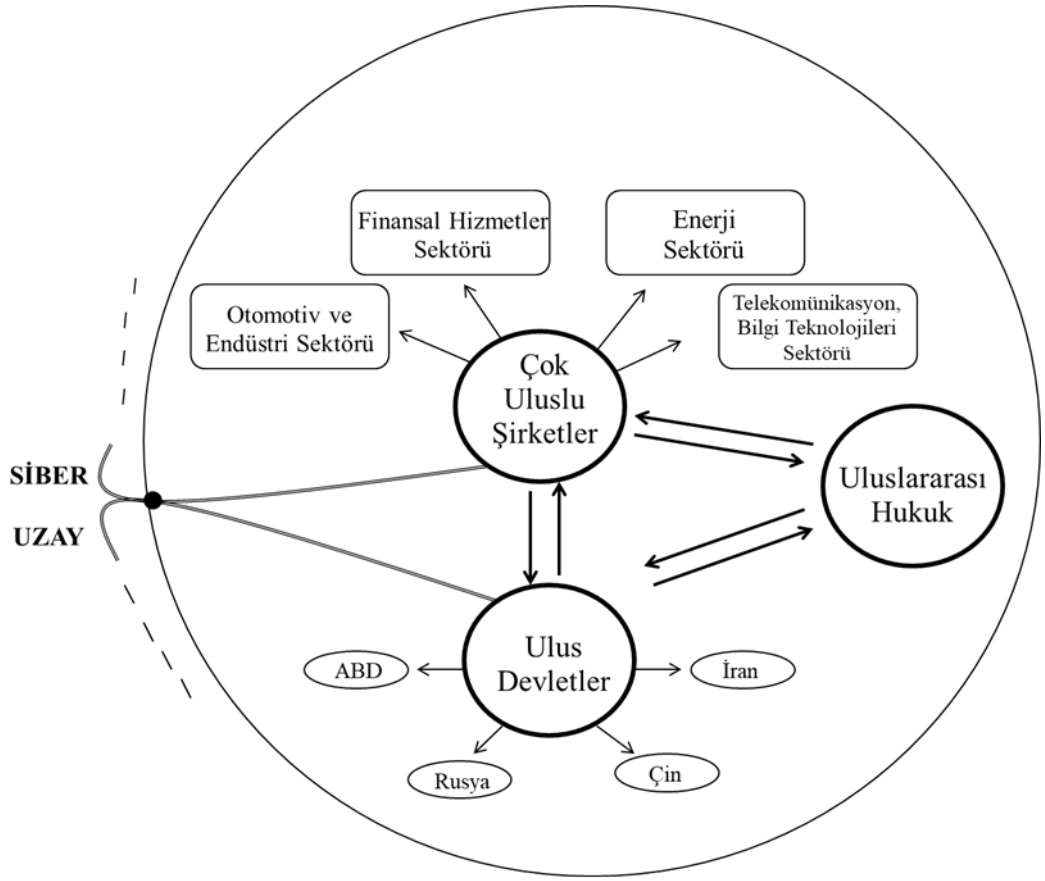
Ulus devletler, siber güvenliğin sağlanmasında ve siber tehditlere karşı savunmada çok önemli bir rol oynamaktadır. Hükümetler siber güvenlik stratejileri oluşturur, kaynakları tahsis eder ve ulusal siber uzayın korunmasında sorumlu kurumlar inşa eder. Bu doğrultuda kritik

altyapıyı korumakta, siber suçlarla mücadele etmekte ve güvenlik risklerini azaltmak için istihbarat operasyonları yürütmektedirler. Diğer yandan siber uzayın birbirine bağlı doğası, ulusal güvenliğe yeni zorluklar getirmektedir. Devlet destekli siber saldırılar, bilgisayar korsanlığı ve diğer suç faaliyetleri hükümetlerin ve vatandaşların mahremiyeti için önemli tehditler oluşturabilmektedir. Ulus devletler, güvenlik önlemlerini hem yurtiçinde hem de uluslararası siber tehdit ortamını ele alacak şekilde sürekli olarak uyarlamalıdır.

Siber uzay, ulus devletler için hızlı iletişim, iş birliği ve karar alma olanağı sağlar. Bilgiler anında paylaşılabilir ve ortaya çıkan zorluklara veya fırsatlara hızlı yanıt verilmesinde olanak tanır. Hükümetler, politikaları yaymak, vatandaşlarla etkileşim kurmak ve birden fazla kurum arasındaki faaliyetleri koordine etmek için siber uzayı kullanmaktadır. Ayrıca siber uzaydaki teknolojik gelişmelerin hızı, ulus devletler için hem fırsatlar hem de zorluklar sunmaktadır. Yapay zeka ve blok zinciri gibi gelişen teknolojiler, yönetişim, ekonomi ve güvenliğin çeşitli yönlerinde devrim yaratma potansiyeline sahiptir. Devletler, rekabetçi kalabilmek ve ortaya çıkan tehditleri etkili bir şekilde ele almak için teknolojik değişimin hızına uyum sağlamalıdır.

2.2 Araştırmanın Genişletilmiş Modeli

Siber uzayda çok uluslu şirketlerin ve ulus devletlerin etkilerinin yanı sıra çok uluslu şirketler ve ulus devletler arasında da siber uzayda karşılıklı bir ilişki söz konusudur. Araştırmanın problemlerinden; "P_1: *Çok uluslu şirketlerin siber uzayda etkisi hangi düzeydedir?"* ve "P_2*: Ulus devletlerin siber uzayda etkisi hangi düzeydedir?"* problemlerini tanımlayan model sektörel anlamda daha açıklayıcı olarak ifade edilmiştir. Genişletilmiş modelde; uluslararası hukuk açısından da etkileri açısından bir değişken tanımlanmıştır. Aynı şekilde uluslararası hukukun da siber uzayda etkisi söz konusudur. Araştırmanın genişletilmiş modeli için Bkz. Şekil 2



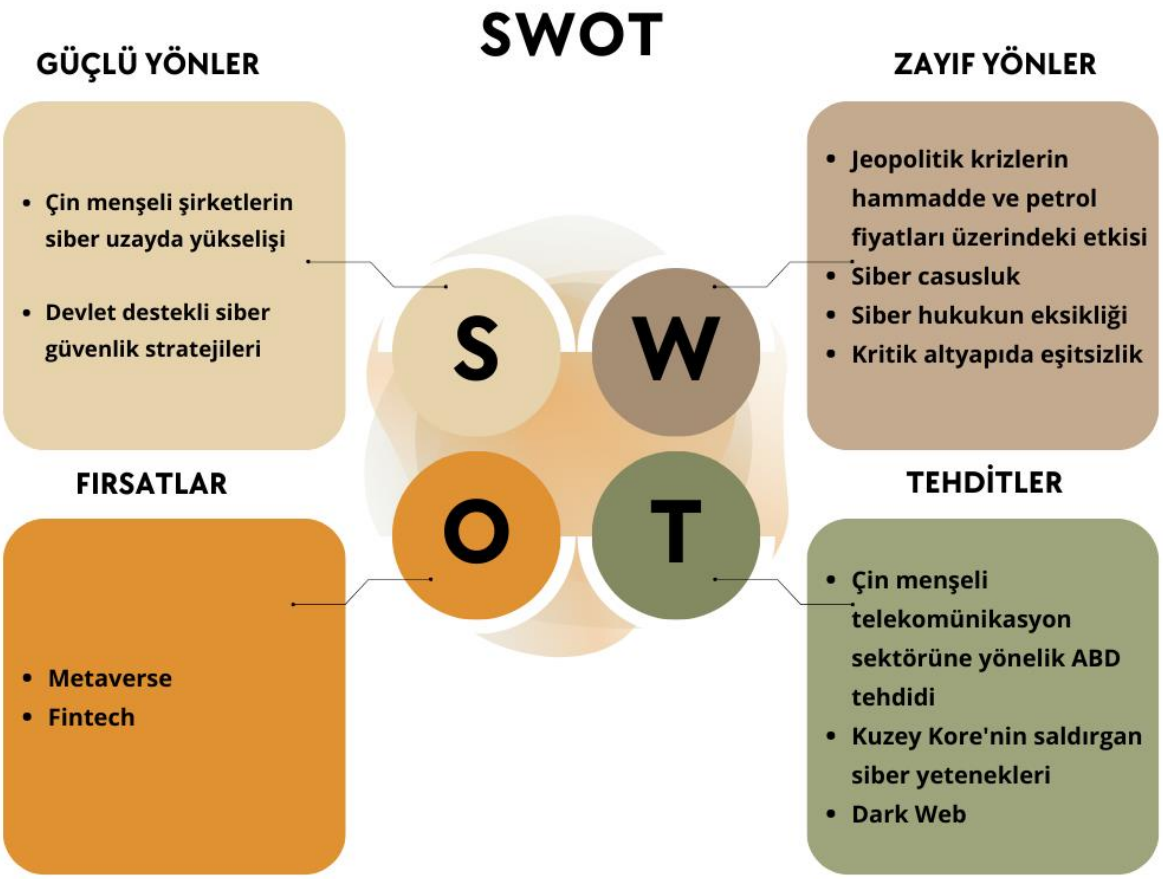
Şekil 2. Araştırmanın Genişletilmiş Modeli
Kaynak : Şekil yazar tarafından oluşturulmuştur

Uluslararası hukukun; çok uluslu şirketler ve ulus devletler açısından siber alandaki ilişkilerine yönelik anlaşılabilmesi önemlidir. Ancak siber hukuk diyebileceğimiz bu tartışma sahası hukuki anlamda uluslararası normlar çerçevesinde henüz yeterli bir düzeye ulaşamamıştır. Araştırmanın modeline hukuki yöne dair sorunsal da taşınmıştır. Böylelikle genişletilmiş bir model uygulanmıştır.

2.3 Ulus Devletler için SWOT Analizi

Aktan (2005)'a göre SWOT analizi, incelenen konunun güçlü ve zayıf yönlerini belirlemekte ve dış çevreden kaynaklanan fırsat ve tehditleri tespit etmektedir ve bilimsel anlamda durum analizi yapmaya imkân sağlayan tekniklerden birisi olarak kabul edilir (Çoban & Karakaya, 2010).

Şekil 3'te ulus devletler ile ilgili SWOT analizi şekli verilmiştir.



Şekil 3. Devletler SWOT Analizi
Kaynak : Şekil yazar tarafından oluşturulmuştur.

2.3.1 Güçlü Yönler

Çin Menşeli Şirketlerin Siber Uzayda Yükselişi; Dünya ekonomisi sadece ulus devletler tarafından değil, aynı zamanda çok uluslu şirketler tarafından da şekillenmektedir. Bu çok uluslu şirketler ticareti yönlendiren, gelir oluşturan, araştırma ve geliştirmeyi desteleyen ulusal ekonomik gücün kritik unsurlarıdır. Çin hükümeti de siber uzayda dijital güç olma hedefiyle çok uluslu şirketlere çeşitli sübvansiyonlar, teşvikler ve politikalar sağlayarak bilgi ve iletişim teknolojileri endüstrisini aktif olarak desteklemektedir.

Çin hükümetinin, teknolojik yeteneklerini geliştirmesine yönelik Huawei'ye araştırma ve geliştirme için verdiği maddi desteği, ABD'nin küresel teknoloji endüstrisindeki hakimiyetine bir meydan okuma olarak görülmektedir. 2022 verilerine göre ABD dışında 170 ülke ve bölgede faaliyet gösteren Huawei özellikle 5G endüstrisinde, Verizon ve Qualcomm gibi ABD menşeli şirketlere büyük bir rakip olarak görülmektedir (Huawei, tarih yok).

Xiaomi, Oppo ve Huawei gibi Çinli BİT şirketleri, Çin'deki düşük işçilik maliyetleri nedeniyle ürünleri daha düşük maliyetle üretip sattıkları ve benzer ürünleri daha rekabetçi bir fiyat noktasında sunabildikleri için küresel pazarda büyük bir avantaj elde etmiştir. Dünyanın en değerli ilk 20 teknoloji şirketi arasında yer alan 207,92 milyar dolar piyasa değerine sahip -dünyanın en büyük e-ticaret devlerinden biri- Alibaba ve 395,33 milyar dolar piyasa değerine sahip -en büyük oyun şirketlerinden biri- olan Tencent gibi Çinli BİT şirketleri de önemli

oranda iç pazara sahip olmakla birlikte teknolojik uzmanlıkları sayesinde küresel olarak genişleme fırsatını yakalamıştır (CompaniesMarketCap.com, 2023).

Devlet Destekli Siber Güvenlik Stratejileri; BİT alanındaki teknolojik gelişmelerin hızlı gelişimi, fırsatların yanı sıra yeni tehditleri de beraberinde getirmekte ve ulus devletler için siber altyapıya daha fazla bağımlı hale gelmesine neden olmaktadır. Dolayısıyla hükümetler toplumun ve ekonominin işleyişi için önemli varlıklar olarak nitelendirilen kritik altyapıların karşı karşıya olduğu siber güvenlik riskleriyle mücadele etmek için ulusal siber güvenlik ve savunma stratejileri geliştirmektedir. Bu doğrultuda siber tehdit ortamına göre uyarlanmış stratejiler; siber güvenlik teknolojilerine ve yeteneklerine yatırım yapılmasını, ülkelerin siber güvenlikle ilgili uluslararası kuruluşlar, özel sektör ve diğer ülkelerle iş birliği yapmasını, siber saldırıları caydırmak veya siber saldırılara karşı yanıt vermek için saldırgan siber yetenekler geliştirmesini içermektedir.

Her ülkenin kendi ulusal çıkarları, jeopolitik kaygıları ve iç politikaları tarafından yönlendirilen siber güvenlik stratejileri konusunda kendine özgü bir bakış açısı vardır. ABD'nin siber strateji belgelerinde genellikle hükümet ve özel sektör iş birliğine vurgu yapılmaktadır. Trump yönetimi döneminde, önleyici siber saldırılar yoluyla saldırgan siber operasyonları hızlandırma, siber caydırıcılık gücünü artırma ve siber misilleme yeteneğini geliştirme gibi stratejiler belirlenmiştir (Wolff, 2018). ABD'nin hayati çıkarlarını savunma amacıyla belirlenen siber stratejiler, siber saldırılara hızlı yanıt verme yeteneği için saldırıları izleme veya atfedebilme kapasitesine yatırım yapma, çevrimiçi pazarlar ve kripto para birimleri gibi araçların kullanımını engellemek için soruşturma araçlarını kullanma, ortak tehditlere karşı caydırıcılığı güçlendirmek ve uluslararası güvenliği korumak için uluslararası ittifaklar oluşturma gibi prensipler üzerine kurulmuştur.

Çin, en hızlı büyüyen dijital ekonomiye sahip olmasının yanı sıra, siber güvenlik stratejisinde temel olarak devlet desteğiyle yerli yüksek teknoloji endüstrilerini teşvik etme ve yerli yazılım-donanım üretimine öncelik verme yaklaşımını benimsemiştir. Bu stratejiyle, Çin hükümeti siber uzaydaki egemenliğini koruma, internetin rejimi tehdit edici veya ulusal güvenliğe zarar verici şekilde kullanılmasını engelleme, Çin'in sosyalist ideolojisini çevrimiçi platformlarda güçlendirmek, denetleyici mekanizmaları güçlendirme, yabancı web sitelerine erişimi kısıtlama ve politik olarak kabul edilmeyen içeriği filtreleme gibi stratejik hedeflere odaklanmıştır. Bu hedefler çerçevesinde Çin, Büyük Güvenlik Duvarı aracılığıyla siber uzayı kontrolü altında tutmaktadır (Chandel, Jingji, Yunnan, Jingyao, & Zhipeng, 2019). Ayrıca Çin'de faaliyet gösteren yabancı şirketlerin siber saldırılara karşı önlem almak için devletten sertifika alma, güvenli ve kontrol edilebilir bir şekilde faaliyet gösterme zorunluluğu bulunmaktadır.

İran'ın ulusal güvenlik stratejilerinin oluşturulmasında baskın liderler, güçlü bir askeri yapı ve güçlü kültürel kimlik baskın unsurlar olarak kabul edilmektedir. Dolayısıyla İran rejiminin siber uzay alanındaki temel amaçları ülke içindeki çevrimiçi faaliyetleri izleme ve kontrol etme, içerik filtreleme, rejime karşı çıkan muhalif unsurların örgütlenme ve iletişim kurma yeteneklerini engelleme, ulusal güvenliklerini korumak için saldırgan siber yeteneklerini geliştirmektir. Ayrıca vatandaşları küresel siber uzaydan ayıran, Şii Müslüman normlarına uygun, hükümetin ağ içeriklerini tamamen kontrol etmesini sağlayan ve yerli internet hizmetleri sunmayı amaçlayan proje çerçevesinde rejimle örtüşmeyen Batılı unsurların İran ağına sızmasını önleme, siber saldırı ve siber casusluğa karşı savunma yetenekleri oluşturmada kilit önemdedir (Çahmutoğlu, 2021, s. 7) (Sajedi & Ariani, 2014).

Rusya'nın siber strateji belgelerinde, bilgi güvenliğini sağlama, yerli bilgi altyapısını geliştirme, uluslararası işbirliği kurma, uluslararası hukuka uyum, siber tehditlerle mücadele ve dijital egemenlik çerçevesinde devletin kendi topraklarındaki internet üzerinde denetiminin genişletilmesi gibi hedefler önemsenmektedir. Ayrıca Rusya siber stratejilerinde stratejik hedeflere ulaşmak ve ulusal çıkarlarını korumak için siber yetenekler de dahil olmak üzere çeşitli araçların kullanımını vurgulamaktadır. Dolayısıyla Rus hükümeti, Gerasimov Doktrini çerçevesinde, rakip bir ulus devletlerin kritik altyapısını, iletişim ağlarını veya bunlardan yararlanabilecek asimetrik faaliyetler yürüterek savaşma potansiyelini zayıflatmak için geleneksel ve askeri olmayan araçlara izin veren bilgi alanının asimetrik doğasını kabul etmektedir (McKew, 2017) (Gerasimov, 2016, s. 24).

2.3.2 Zayıf Yönler

Jeopolitik Krizlerin Hammadde ve Petrol Fiyatları Üzerindeki Etkisi; Jeopolitik krizlerin siber uzayda oluşturduğu zayıflık ise hammadde ve petrol fiyatları üzerindeki etkisini, muhtemelen bu ürünlerin üretimi ve dağıtımında yer alan kritik altyapı ve ulaşım sistemlerine yönelik siber saldırı riskini, siber casusluk, piyasa manipülasyonu içermektedir. Son 5 yıldır yaşanan jeopolitik krizler sırasında hammadde ve petrol arzını etkileyebilecek bazı önemli riskler ve kırılganlıklar arasında; askeri çatışmalar, ticari anlaşmazlıklar, bölgesel yaptırımlar ve siyasi istikrarsızlar sayılabilir. Bu zorluklar arz ve talep üzerindeki etkileri nedeniyle yaşanan hammadde kıtlığı ve petrol fiyatlarındaki yükselme hem işletmeler hem de tüketiciler üzerinde önemli etkiler yaratabilmektedir. Latin Amerika, Afrika ve Orta Doğu gibi büyük madencilik ve hammadde üretiminin olduğu ülkelerinde yaşanan herhangi bir siyasi kriz, birçok hammaddenin arzının kesintiye uğramasına ve arzın azalmasını etkileyerek endüstrilerdeki üretimi etkileyebilmektedir. Örneğin 2020'de İran'da Kasım Süleymani suikastı, petrol piyasalarına duyarlılığı artırmış ve jeopolitik konuları yeniden gündeme getirmiştir (Kumar, 2020).

2022'de Rusya'nın Ukrayna'yı işgali ve ardından Rusya'ya yönelik ekonomik yaptırımlar petrol, gaz ve bazı tarım ürünlerinin fiyatlarının artmasına, Rusya'da üretilen bazı endüstriyel uygulamalarda kullanılan (inşaat, elektronik cihaz, uzay araçları, nükleer reaktörler, gıda, uçak ve diğer taşıtlar vb.) önemli metaller arasında yer alan alüminyum, nikel, paladyum gibi hammaddelerin ticaretinin ve küresel piyasaların ciddi bir şekilde etkilenmesine neden olmuştur. Ayrıca Rusya ve Ukrayna, otomobil parçaları ve çip endüstrisi için gerekli olan önemli neon, paladyum, platin, nikel, helyum, kripton gibi birçok gazın ve değerli metalin büyük ve önemli üreticileridir. Çatışma sebebiyle, değerli metal fiyatları %10 ile %30 oranında artış göstermiş ve bu oran araç fiyatlarına da yansımıştır. Özellikle Ukrayna, dünyanın neon gazı arzının çoğundan sorumlu olduğu için çiplerin geliştirilmesinde önemli rol oynamakta ve küresel çip krizini etkilemektedir (Financial Times, 2022).

Rusya-Ukrayna Savaşı ve ABD-Çin arasındaki ticaret savaşları örnekleriyle yaşanan jeopolitik krizlerin yanı sıra, Covid-19 salgını, artan hammadde fiyatları, çeşitli elektronik ve diğer endüstrilerde kullanılan iletken çip krizine sebep olmuştur.

Siber Casusluk; Son 30 yılda, devlet destekli ve devlete bağlı olmayan siber tehdit aktörlerinin aktif olarak siber casusluk faaliyetlerini kullanması, siber uzayda büyüyen ve önemli bir tehdit oluşturmaktadır. Siber casusluk yapan ulus devlet destekli siber tehdit aktörleri, siyasi, ekonomik ve askeri amaçlarla motive olmaktadır. Askeri planlar, hükümet sırları veya kritik altyapı gibi hassas bilgileri hedef alan ulus devlet destekli siber tehdit aktörleri, önemli kaynaklara ve gelişmiş siber araçlara sahiptir ve bu durum onları güçlü bir tehdit haline getirmektedir. Siber casusluk faaliyetleri yürüten ulus devletler genellikle, kritik

altyapıya, hükümetin resmi ağlarına ve rakip ulus devlet menşeli çok uluslu şirketlere karşı büyük ölçekli ve hedefli siber saldırılar gerçekleştirmelerine izin veren, gelişmiş teknolojik yeteneklere ve önemli kaynaklara sahiptir. Siber casusluk faaliyetlerinin atfedildiği ve devlete bağlı siber tehdit aktörlerinin bulunduğu ulus devletlerden bazıları Çin, Rusya, Kuzey Kore ve İran'dır.

1996-1997 yılları arasında gerçekleşen Moonlight Maze saldırısı, Rus hükümetine veya Rus devlet destekli siber tehdit aktörlerine atfedilen ve ABD'yi hedef alan devlet destekli ilk büyük çaplı siber casusluk operasyonlarından biri olarak bilinmektedir. Siber saldırıda NASA, Pentagon, üniversitedeki sistemler, silah laboratuvarları, ABD Enerji Bakanlığı ve birkaç Amerikan devlet kurumu hedeflenmiştir. Gizli bilgilerin veri ihlaline yönelik iki yıllık bir süre boyunca gerçekleştirilen saldırıda, silah yönlendirme sistemleri, deniz istihbarat kodları, teknik araştırmalar, askeri haritalar, askeri donanım tasarımları, şifreleme teknikleri ve Pentagon'un savaş planlamasıyla ilgili veriler çalınmıştır (Westby, 2020). Infrastructure Defence'nin baş yöneticisi James Adams, "*çalınan bu bilgilerin değeri on milyonlarca- belki de yüz milyonlarca- dolardır. Bilgiler, en yüksek teklifi verene satılmak üzere internet üzerinden Moskova'ya gönderildi*" ifadelerinde bulunmuştur (FAS, 2000). Saldırılarda Rus hükümeti sorumlu tutulmuş, ancak Moskova'daki bir IP adresi dışında ABD suçlamalarını destekleyen çok az somut kanıt elde edilmiştir. Bu büyük siber casusluk operasyonunun önemi ve çalınan bilgilerin hassas doğası nedeniyle kanıtlar gizli tutulmuştur.

Siber Hukukun Eksikliği; Siber uzayda uluslararası kabul görmüş hukuk kurallarının bulunmaması kötü niyetli siber aktörler tarafından istismar edilebilecek bir yasal boşluk oluşturmaktadır. Bu zayıflık siber saldırıların atfedilmesine yönelik zorlukları ortaya çıkarmakta, insan hakları ihlallerine yol açmakta, siber saldırı olasılığı artırmakta ve ulus devletler arasındaki güveni zedelemektedir.

Siber uzayda net yasal sınırların olmaması, siber tehdit aktörlerinin ulus devletlere, kritik altyapıya ve çok uluslu şirketlere yönelik siber saldırılar başlatmasını kolaylaştırmakta ve ulus devlet destekli aktörlerin veya diğer tehdit aktörlerinin siber saldırılar gerçekleştirmesi için cesaretlendirmektedir. Bu saldırılar ulusal güvenliğe, ekonomiye ve sosyal düzene önemli zararlar vermektedir. Siber hukukun ve açık kuralların yokluğunda, uluslar siber saldırılara karşı askeri çatışmaya dönüşebilecek misillemeyi tercih edebilir ve bu durum uluslararası sistemi istikrarsızlaştırabilir. Ayrıca siber saldırılar için net bir yasal standartlar oluşturulmadığından, siber saldırıların atfedilmesi zorlaşmaktadır. Bu durumda siber saldırıların belirli bir aktöre atfedilmesi daha zor hale gelir ve sorumlu tarafa karşı misilleme veya cezai önlemler almasını zorlaştırır.

2001 yılında imzaya açılan ve 2004 yılında yürürlüğe giren 48 maddelik Avrupa Konseyi Siber Suçlar Sözleşmesi (Budapeşte Sözleşmesi), 20 Kasım 2017 tarihli 14435 sayılı AB Konseyi kararı, 11 Nisan 2017 tarihli Siber Uzayda Sorumlu Devlet Davranışlarına İlişkin G7 Bildirgesi (Lucca Deklarasyonu), AGİT'in Daimî Konsey 1092. Genel Kurul toplantısında bilgi ve teknolojinin kullanımından kaynaklanan çatışma risklerini azaltmak için aldığı 1202 sayılı kararı 31 Ocak 2003 tarihli "*küresel bir siber güvenlik kültürünün oluşturulması*" amacıyla alınan 57/239 sayılı BM Genel Kurul kararı (UN General Assembly, 2003), NATO'nun Ocak 2020 tarihli "Siber Uzay Operasyonları İçin Müttefik Ortak Doktrini" (NATO, 2020, s. 21) gibi bilgi ve teknolojinin barışçıl kullanımı ve siber uzayda güvenliğin sağlanması için uluslararası işbirliğinin gerekliliğinin vurgulandığı, mevcut uluslararası hukukun özellikle BM Şartı'nın siber uzayda devlet davranışlarına uygulanabilirliğinin ve yasal zeminin oluşturulmasının vurgulandığı bir çok karar alınmıştır.

2009'da Estonya'nın başkenti Tallinn'de NATO Kooperatif Siber Savunma Mükemmeliyet Merkezi (CCDCOE), Uluslararası İnsancıl Hukuk kapsamında siber savaşın nasıl kapsamlı bir şekilde uygulanması gerektiğini tartışarak siber uzayı yöneten uluslararası hukukun ilk kapsamlı incelemesi sonucunda oluşturduğu Tallinn Manual 1.0 ve 2017'de Tallinn Manual 2.0 olarak ikinci baskısı sunulan el kitabı uluslararası hukukun siber alana uygulanmasına ilişkin analizler sunmaktadır (Schmitt, 2018; Tropeano, 2019). BM Güvenlik Konseyi'nin 2178 (2014) ve 2396 (2017) sayılı kararları da üye devletlerin, teröristlerin teknoloji ve iletişimi terör eylemleri için kullanmasını önlemek amacıyla ulusal önlemler alınırken aynı zamanda uluslararası iş birliği içinde hareket edilmesinin gerekliliğini vurgulamaktadır (UNCCT, tarih yok). İnsan hakların çerçevesinde ise BM İnsan Hakları Evrensel Beyannamesi ve Uluslararası Medeni ve Siyasi Haklar Sözleşmesi kapsamında güvence altına alınan, ifade özgürlüğü, mahremiyet hakkı, düşünce özgürlüğü ve örgütlenme özgürlüğü tüm insanların en temel hakları arasındadır. Ancak hükümetlerin uyguladığı siber güvenlik yasaları, insan hakları ve özgürlükleri üzerinde olumsuz bir etki yaratmakta ve doğrudan bir ihlal oluşturmaktadır.

Siber hukukun oluşturulamaması, insan haklarının daha geniş ölçekte ihlal edildiği durumlar yaratmaktadır. Bu ihlalde bireylerin mahremiyet haklarının korunamamasından daha kötü oluşacak senaryo, ulus devletlerin kritik altyapılarına yönelik gerçekleştirilen bir siber saldırıda bireylerin yaşam hakları ihlal edilebilir. Sağlık sistemleri, finansal hizmetler veya elektrik şebekeleri gibi kritik altyapıların zarar görmesi toplumda önemli kayıplara yol açmaktadır. Örneğin 2007'de ilk modern siber saldırı niteliği taşıyan Avrupa'nın en kablolu ülkesi olarak bilinen Estonya'ya karşı gerçekleştirilen saldırı sonucunda büyük bir mağduriyet yaşanmıştır (O'Connell, 2012). Devlet kurumları, finansal sistemler, ulaşım sistemleri çökmüş ve Avrupa ülkeleri Estonya'ya konvansiyonel savaş sonucundaki zararların iyileştirilmesi sürecinde yardım etmiştir. Ancak siber saldırı sonucunda yaşanan veri kayıplarının iyileştirilmesi için etkili bir süreç yürütülememiştir. Özellikle siber saldırılar sonucu veri kaybı yaşandığında, bu kayıpların hukuki süreçleri yetersiz kalmakta ve uluslararası arenada etkin bir koruma mekanizması bulunmamaktadır. Ulus devletler ve uluslararası örgütler tarafından bu konu zaman zaman ele alınmış olsa da, veri kaybı gibi siber saldırı sonuçlarının cezalandırılması konusunda henüz bağlayıcı kararlar ele alınmamıştır.

Kritik Altyapıda Eşitsizlik; Kritik altyapı teknolojisi için küresel bir ağ altyapısının olmaması, siber güvenlik açısından çeşitli zorluklar ve zayıflıklar sunmaktadır. Dolayısıyla ulus devletlerin kritik altyapı teknolojilerinin siber güvenlik hazırlığı, siber güvenliğe yatırım düzeyi, altyapının karmaşıklığı ve siber tehditlerin karmaşıklığı gibi faktörlere bağlı olarak büyük ölçüde değişiklik göstermektedir. Ülkelerin kritik altyapılarının ve siber güvenliklerinin kalitesine göre kesin olarak sıralama yapmak zordur. Bununla birlikte, bazı ülkelerin diğerlerine göre daha zayıf kritik altyapıya ve siber güvenlik sistemlerine sahiptir.

Zayıf kritik altyapıya sahip ülkelerin örneklerinden biri İran'dır. İran, 2010 yılında ülkenin nükleer programına zarar veren Stuxnet virüsü de dahil olmak üzere, uzun bir süre çok sayıda siber saldırılarla karşı karşıya kalmıştır. Ayrıca elektrik şebekesi dahil olmak üzere zayıf kritik altyapısı nedeniyle de eleştirilmektedir (United Against Nuclear Iran [UANI], 2022).

Ukrayna 2017'de ülkenin altyapısına önemli ölçüde zarar veren NotPetya kötü amaçlı yazılım saldırısı da dahil olmak üzere birçok büyük siber saldırının kurbanı olmuş ve enerji sektörü de dahil olmak üzere kritik altyapısıyla ilgili zorluklarla karşı karşıya kalmıştır (Bowen, 2021, s. 17). Venezuela, Bangladeş, Yemen, Haiti, Suriye, Somali gibi ülkeler de yıllar içinde

çok sayıda siber saldırıyla karşı karşıya kalan ve zayıf kritik altyapıyla mücadele eden ülkeler arasındadır.

Gelişmiş kritik altyapıya sahip ülkeler arasında yer alan Singapur, kritik altyapı koruması ve siber güvenlik alanında dünya lideri olarak tanınmaktadır. Ülkenin ulusal bir siber güvenlik stratejisi ve kritik altyapının korunması için çalışan Siber Güvenlik Ajansı adıyla özel bir devlet kurumu mevcuttur. Almanya, Japonya, ABD, İngiltere, Çin de siber güvenliğe büyük yatırımlar yapan, gelişmiş kritik altyapı koruma programına, gelişmiş ulusal siber güvenlik stratejisine, siber güvenlik yasalarına ve kritik altyapının korunması için çalışan özel devlet kurumlarına sahip ülkeler arasındadır.

2.3.3 Fırsatlar

Metaverse; Metaverse, Sosyal etkileşimler, eğitim, küresel siyaset ve yeni ekonomilerin inşa edilmesi dahil birçok alanda etki gösteren Metaverse, özellikle küresel teknoloji şirketlerinin eylemlerine, ulus devletlerin yatırımlarına, kamusal uygulamalarına ve siyasi faaliyetlerine yön vermekte ve yeni fırsatlar sunmaktadır (Yetgin & Özkan, 2022 , s. 209). Ulus devletler, ekonomik kalkınmayı yönlendirmek için Metaverse platformunda sanal işletmeler ve istihdam fırsatları yaratarak hem dijital ekonomilerin büyümesine katkıda bulunabilir hem de GSYİH'lerini artırabilir ve yeni gelir kaynakları yaratabilir. Fırsatlar doğrultusunda daha fazla yatırımı çekmeye yardımcı olabilecek iyileştirilmiş küresel markalaşmanın yanı sıra vatandaşlara yeni çevrimiçi hizmetlere ve kamusal alanlara erişim de sağlamaktadır. Ayrıca ulus devletler, kültürlerini ve miraslarını tanıtmak için Metaverse platformunu kullanmaktadır. Geleneklerini, tarihlerini ve sanatlarını sanal müzeler ile sergileyerek kültürel kimliklerini koruyan ve geliştiren sanal alanlar yaratabilme imkanına sahiptir. Sanal müzelere ek olarak Metaverse platformu, ülkeler arasındaki diplomatik ilişkiler ve şirketler arasında işbirliği çabaları, zirve toplantıları ve müzakereler için sanal platform görevi görmektedir.

Fintech; Ulus devletler, Fintech endüstrisindeki gelişmekte olan işletmelere destek sağlayarak, yenilikçiliği ve girişimciliği teşvik eden politikalar oluşturarak ulusal ekonomik büyümeyi destekleyebilir, blok zinciri ve yapay zeka gibi teknolojilerin kullanımıyla hükümetlerin finans sektörünü daha etkin bir şekilde düzenlemesine yardımcı olabilir, özellikle finansal işlemleri izlemek, dolandırıcılığı tespit etmenin ve uyumluluğu iyileştirmenin yanı sıra veriler ve analizler sağlayarak riskleri daha etkin bir şekilde yönetmek için araçlar geliştirebilir. Uluslararası ticaret ve yatırım üzerindeki olumlu etkisi ise sınır ötesi işlemlerin maliyetini ve karmaşıklığını azaltmaya yardımcı olabilmesi ve çok uluslu şirketler için nakit akışının iyileştirilmesi için yeni finansman seçeneklerinin sunulmasını içermektedir. Genel olarak finansal süreçleri iyileştirmek, maliyetleri düşürmek ve rekabet avantajı elde edilebilmesi için birçok fırsat sunar.

2.3.4 Tehditler

Çin Menşeli Telekomünikasyon Sektörüne Yönelik ABD Tehdidi; Çin ve ABD ilişkileri 21. yüzyılın en önemli ikili ilişkilerini temsil etmektedir. ABD ve Çin arasındaki jeopolitik çatışma, "teknoloji savaşları" adı altında yeni bir çatışma türüne doğru kaymasıyla sonuçlanmıştır. Bu çatışma ABD hükümetinin, Çin'in teknolojik gelişimini sınırlama ve Çinli şirketlerin kilit sektörlerde baskın oyuncular haline gelmesini engellemeye yönelik daha geniş çabaların bir parçası olarak Huawei gibi şirketlerin doğrudan hedef alınmasını içermektedir.

Ulus devletlerin endişesi, Çin'in 2017 Ulusal İstihbarat yasası uyarınca, tüm Çinli şirketlerin ve kuruluşların yasal olarak Çin hükümeti adına istihbarat çalışması yürütülebilme

analizinden kaynaklanmaktadır. Bu analize göre istihbarat toplamak ve fikri mülkiyeti çalmak için Huawei'nin 5G ağlarını kullanma yeteneği olduğu ve şirketin hükümet taleplerine boyun eğebileceği ve bir ülke üzerinde baskı uygulamak için ağları devre dışı bırakabileceği konusunda endişeleri beraberinde getirmektedir.

ABD hükümetinin, Huawei'yi ABD şirketlerinin hükümet onayı olmadan Huawei ile iş yapmasını fiilen yasaklayan Varlık Listesi'ne alması (Aydın, 2021, s. 60), Huawei çalışanlarına yönelik diplomatik kısıtlamalar getirmesi, Çin hükümetinin şirket üzerindeki potansiyel etkisine ilişkin endişeler nedeniyle müttefiklerini Huawei'nin 5G ağlarına katılımını sınırlamaya çağırması (Gong, 2021, s. 40-41), Huawei'yi ABD'nin İran'a yönelik yaptırımlarını ihlal etmekle suçlaması (Aktan, 2019), Biden yönetiminde ABD şirketlerinin çip üretimi için kullanılan ekipmanları özel bir lisans almadıkları sürece belli Çinli üreticilere satmalarını engelleyen yeni ihracat kontrolleri yayınlaması, akıllı telefon çiplerinin büyük bir oranını tedarik ettiği TSMC'nin ABD ihracat kontrollerini gerekçe göstererek Çin ile işbirliğini durdurması, ABD müdahaleleri arasında yer almaktadır (Berman, Maizland, & Chatzky, 2023).

Huawei, Çin hükümetiyle iddia edilen bağları ve teknolojisini siber casusluk için olası kullanımı konusundaki endişeler nedeniyle ABD hem ekonomik çıkarlar hem de ulusal güvenlik kaygıları neticesinde Huawei'nin pazara girişini kısıtlama çabalarında birkaç müttefikin desteğiyle pazar erişimini kısıtlayarak kendi ekonomisini güçlendirme fırsatı bulmuştur. Çin ekonomisi büyük ölçüde ihracata bağımlı olduğu için, ABD pazarındaki kısıtlama ekonomisine zarar vermektedir. Ayrıca Çin'in ABD ürünlerine ulusal alternatifler geliştirme çabaları, teknolojik uzmanlık ve temel bileşenlere erişim eksikliği nedeniyle engellenmektedir.

ABD müttefiklerinden gelen kısıtlamalar arasında; Hindistan'ın gelecek projelerde Huawei ekipmanının kullanımını aşamaları olarak kaldırma kararı, Fransa'nın telekomünikasyon operatörlerinin süresi dolduğunda Huawei ekipmanlarının lisanslarını yenilemeyeceği ve şirketin ülkedeki varlığını aşamalı olarak kaldırma kararı, Vietnam'ın Huawei'yi tamamen olmasa da 4G ve 5G ağlarında kullanımını kaldırma kararı, İtalya'nın Huawei ile telekomünikasyon sağlayıcısı Fastweb arasında Huawei'yi 5G ağının tek tedarikçisi olarak kullanılmasına dair anlaşmayı veto etmesi, Kanada'nın Huawei'yi 5G ağlarından çıkarma kararı yer almaktadır. Belçika, Hırvatistan, Finlandiya, Yunanistan, Norveç, Portekiz, Singapur ve İspanya ise Huawei'ye karşı aleni bir duruş sergilememiş olsa da 5G ağlarını kurmak için Huawei'nin rakipleri arasında yer alan Ericsson ve Nokia ile sözleşme yapmayı tercih etmiştir (Sacks, 2021).

Kuzey Kore'nin Saldırgan Siber Yetenekleri; Rejimin devamlılığını sağlama, dış müdahalelerden bağımsız bir ulus haline gelme ve Kore'yi Kuzey Kore hükümetinin kontrolü altında birleştirme hedefiyle politikalar yürüten Kuzey Kore'nin saldırgan siber yetenekleri, uluslararası güvenlik için önemli bir tehdit oluşturmaktadır. Ülkenin siber operasyonları siyasi ve ekonomik hedeflerine ulaşmak için önemli bir araç olarak gördüğüne inanılmakta ve bir dizi yüksek profilli saldırı yapmakla suçlanmaktadır.

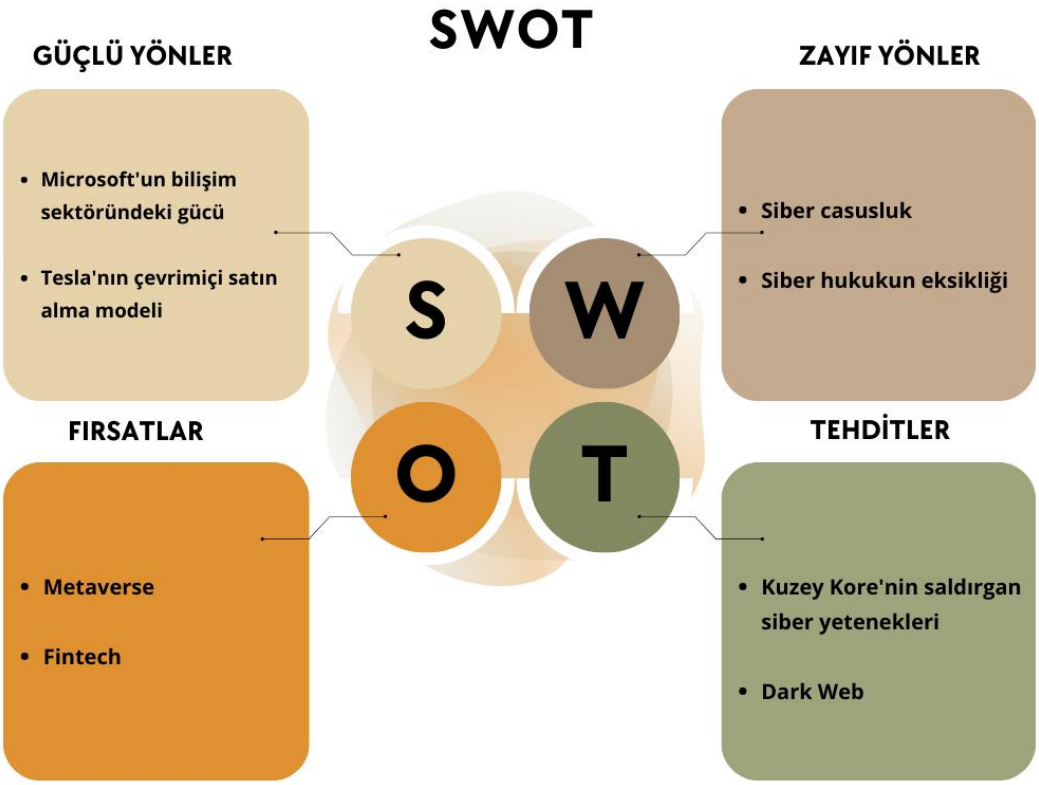
Kuzey Kore'nin, kuruluşları, bireyleri ve rakip ulus devletlerin operasyonlarını bozmayı hedeflediği kötü amaçlı yazılımlar geliştirdiği ve dağıttığı bilinmektedir. 2017'de yine Kuzey Kore destekli Lazarus grubuna atfedilen WannaCry fidye yazılım saldırısı, dünya çapında yüz binlerce bilgisayarı etkileyerek büyük bir maddi hasara sebep olmuştur (Kaspersky, tarih yok). Genel olarak, Kuzey Kore'nin saldırgan siber yetenekleri ve faaliyetleri, savaş eşiğini geçmeden ülkelerin ekonomilerine ve ulusal güvenliklerine önemli zararlar verdiğini ve uluslararası toplum için önemli bir tehdidi temsil ettiğini göstermektedir.

Dark Web; Dark Web, siber tehdit aktörleri, teröristler ve devlet destekli casuslar tarafından yasa dışı faaliyetleri yerine getirmek ve çeşitli siber suç türleri için en zorlu ve izlenemez bir pazar yeridir. Dark Web üzerinde faaliyet gösteren siber tehdit aktörleri hassas bilgileri çalmak, kritik altyapıları bozmak, casusluk yapmak veya siber saldırılar başlatmak için ulus devletleri ve çok uluslu şirketleri hedef alabilmektedir. Dark Web hem ateşli silahlar, patlayıcılar ve kimyasal silahlar gibi yasa dışı silahlar için bir pazar yeri hem de uyuşturucu ve insan kaçakçılığının satışı, dağıtımı için bir merkezdir. Dolayısıyla bu tehditlerden etkilenen ulus devletler ve vatandaşlar üzerinde önemli sosyal, ekonomik ve politik etkiler doğurabilmektedir.

Dark Web'de özellikle terör örgütleri ulusal güvenlik için büyük bir tehdittir. El Kaide IŞİD gibi terör örgütleri, Dark Web'i propaganda yapmak, para toplamak ve üye kazanmak için kullandığına dair veriler bulunmaktadır. Örneğin 2014 yılında çevrimiçi olarak yayınlanan "Bitcoin wa Sadaqat al-Jihad" (Bitcoin ve Cihad Hayır Kurumu) makalesi, Bitcon'i ve anonim bağış sistemini kullanarak cihatçı grupların finansal sistemdeki kısıtlamaları aşma ve ekonomik desteği kolaylaştırma stratejilerini ele almaktadır (Weimann, tarih yok).

2.4 Çok Uluslu Şirketler için SWOT Analizi

Şekil 4'te şirketler ile ilgili SWOT analizi şekli verilmiştir.



2.4.1 Güçlü Yönler

Microsoft'un Bilişim Sektöründeki Gücü; Apple, piyasa değeri açısından ilk sırada yer alan ve Microsoft'tan daha büyük şirket olsa da, Microsoft kendisini, Apple, Amazon, Meta ve Google dahil olmak üzere diğer piyasa değeri yüksek teknoloji şirketlerinden çeşitli yönlerden ayrılmaktadır. Apple tüketici donanımına (iPhone, iPade, Mac) güçlü bir vurgu

yaparken, Amazon e-ticaret ve bulut bilgi işlemde hakim bir konumdadır. Google, arama, çevrimiçi reklamcılık ve internet hizmetlerinde uzmanlaşırken, Meta öncelikle sosyal medyaya ve sanal gerçeklik gibi girişimlere odaklanır.

Dünyanın en ünlü ve en büyük bir piyasa değerine (2,09 trilyon dolar) sahip Amerikan çok uluslu teknoloji şirketlerinden biri olan Microsoft, yazılım ve bulut bilişim teknolojisinde küresel pazar lideridir. Windows işletim sistemi, Microsoft Office programları, bulut bilişim platformu Azure, Office 635, Dynamics 365, uzaktan çalışma çözümü Microsoft Teams, Mesh, sanal asistan Cortana gibi çeşitli yazılım ürünleri ve hizmetleri geliştirerek, 1975 yılından beri teknoloji endüstrisinde güçlü bir pazar varlığı oluşturmuş ve önemli bir aktör olmuştur. Bu ürünler hem kişisel hem de profesyonel ortamlarda vazgeçilmez olmakla birlikte, Microsoft, özellikle otomotiv, enerji ve finans sektörleri de dahil olmak üzere çeşitli sektörlerdeki çok uluslu şirketler için lider bir dijital stratejik ortak haline gelmiştir. Yenilikçi teknolojileri ve hizmetleri sayesinde Microsoft, çok uluslu şirketlerin operasyonlarında daha fazla dijitalleşme ve verimlilik elde etmelerini sağlarken, aynı zamanda kendi pazarlarında büyüme ve rekabet gücünü artırmıştır.

Microsoft, çeşitli şirketleri satın almasıyla ve çeşitli alanlara yatırımlarda bulunmasıyla yeni teknolojilerle de ilgilenmektedir. Örneğin Sony'nin Playstation oyun konsoluna rekabetçi bir şekilde Microsoft tarafından oluşturulan Xbox (Microsoft, tarih yok) oyun konsolu donanımı ile eğlence ve oyun sektöründe de öncü olmayı hedeflemektedir.

Yazılım geliştirme projeleri için web tabanlı bir kod deposu hizmeti olan GitHub'ı 7,5 milyar dolara satın alması (Microsoft, tarih yok(a)), sosyal iş ağı sitesi LinkedIn'ı 26,2 milyar dolara satın alması (Microsoft, tarih yok(b)), dünya oyunu olan Minecraft'ı 2,5 milyara satın almasıyla (Microsoft, tarih yok(c)) yeni gelir akışları elde etmiştir. Aynı zamanda Microsoft'un çeşitli kullanıcı tabanlarından faydalanmasına ve kritik sektörlerdeki varlığını güçlendirmesine olanak sağlamıştır.

Microsoft'un ABD'deki ekonomik etkisi ise son derecek önemlidir. Şirketin ülkedeki yatırımları, ekonomik büyümeyi artırmaya yardımcı olmakta ve ülkenin GSYİH 'sına katkı sağlamaktadır. Ayrıca Microsoft, ABD'deki hükümet kurumlarındaki, özel ve kamu şirketlerindeki bilgi işlem ihtiyaçlarına güvenilir çözümler sunmaktadır.

Tesla'nın çevrimiçi satın alma modeli; Covid-19 salgını sırasında birçok sektör salgının etkisinden olumsuz etkilenmiş ve dünya çapındaki fabrikaların çoğu kapanmıştır. Özellikle pandemi sürecinde yaşanan sokağa çıkma kısıtlaması sebebiyle küresel otomobil satışları düşmüş ve otomotiv endüstrisinin tamamı Covid-19 pandemisi sürecinde büyük bir gerileme yaşamıştır. Ancak bu koşullar altında elektrikli araç pazarında lider bir marka olan Tesla, üretim ve satışlarında artış sağlayarak sipariş hacmini büyütmüştür. Şirketin operasyonlarının çoğu virüsten büyük ölçüde etkilenmemiş ve 2020'nin ilk çeyreğinde 88.496 araba satmıştır. 2020'den beri %271 oranında marka değerini artırmış ve 2022'de marka değerini 46,0 milyar dolara yükseltmiştir. Bu oran yerleşik otomobil üreticileri tarafından bildirilen rakamların daha üstündedir. General Motors, Ford Motor, Fiat Chrysler ABD satışlarının 2020'nin ikinci çeyreğinde %30 ve daha fazla düştüğünü bildirirken, Tesla %5'lik bir düşüş yaşamıştır (Boudette, 2020).

Tesla'nın satış modeli, pandemi sırasında çevrimiçi satış ve teslimat stratejisine dayanmaktadır. Çevrimiçi mağaza modeline dayalı stratejisi, müşterilerin evlerinden çıkmadan araçlarını satın almalarına ve teslim almalarına olanak sağlamıştır. Farklı bölgeler için eve teslim hizmetiyle satın alma ve satın alım sonrasında şarj etme gibi ihtiyaçlara yönelik çevrimiçi

danışmanlık hizmetleri sunması, Tesla'nın Covid-19 pandemisi sırasında üretimde pozitif satış büyümesi elde etmesini sağlamıştır.

Fransız danışmalık firması Brand Finance'ın 2023 tarihli araştırmasına göre Tesla, şu anda 66,2 milyar dolar değerindeki markasıyla dünyanın en değerli otomobil markası olan Mercedes-Benz ve Toyota'yı geride bırakmıştır. Elektrikli otomobil üreticisi sıralamasında ise sırasıyla 58,8 milyar dolar ve 52,5 milyar dolar değerindeki Mercedes ve Toyota'dan daha yüksek bir değere sahiptir (BrandFinance, 2023). ABD'de elektrikli otomobil pazarı, satılan tüm elektrikli araçların yarısından fazlasını oluşturduğu için Tesla'nın hakimiyetindedir.

2.4.2 Zayıf Yönler

Siber Casusluk; Çok uluslu şirketler ticari sırları, mali bilgiler, müşteri verileri, diğer gizli ve özel bilgiler nedeniyle hedef alınabilir ve genellikle değerli fikri mülkiyet, ticari sırlar ve finansal verilere sahip oldukları için siber casusluk faaliyetlerine karşılan devlet destekli ve diğer bağımsız aktörlerden gelen önemli tehditlerle karşı karşıyadır. Hedef alınan şirketin ağlarına yönelik siber saldırılar, şirketin önemli mali kayıplarla ve itibar zedelenmesiyle sonuçlanabilmektedir.

GhostNet, bireyleri, kuruluşları ve hükümetleri gözetlemek için kullanılan büyük ölçekli bir elektronik casusluk programı olarak bilinmektedir. Saldırıda virüs içerikli ekler ve web sitesi bağlantıları içeren e-postalar kuruluşlara gönderilmiş ve virüs açıldıktan sonra siber tehdit aktörleri tarafından ana bilgisayar arka planda ele geçirilerek veri gönderme alma gibi faaliyetlere izin verilmiştir. Siber tehdit aktörleri, ağırlıklı olarak Güneydoğu Asya'daki hükümetlere odaklanarak, iki yıllık bir süre içinde 103 ülkede 1295 bilgisayarı gözetleyerek veri ihlalleri gerçekleştirmiştir. 10 ayılık araştırma sürenin sonunda İran ve Endonezya da dahil olmak üzere birçok ülkenin dışişleri bakanlıklarında, Hindistan, Güney Kore, Tayvan, Portekiz, Almanya ve Pakistan büyükelçiliklerinde dinlenen bilgisayarlar tespit edilmiştir ve siber tehdit aktörlerinin Çin'de yerleşik olduğu doğrulanmıştır (Glaister, 2009).

Siber Hukukun Eksikliği; Çok uluslu şirketler açısından siber hukukun eksikliğini şirketlere yönelik ve topluma yönelik olarak ayırabiliriz. İlk olarak şirketlere yönelik durumda güçlü siber yasaların eksikliği, siber saldırılara, veri ihlallerine ve fikri mülkiyet hırsızlığına karşı savunmasız bırakabilmekte ve siber tehdit aktörlerini sorumlu tutmak için yetersiz mekanizmalara sahip olmasına neden olmaktadır. Örneğin finansal hizmetler sektöründe siber güvenlik açığı finansal istikrar için açık bir tehdittir. IMF'nin 51 ülkeyi kapsayan bir anketine göre, yükselen piyasalar ve gelişmekte olan ekonomiler açısından çoğu mali denetçi siber güvenlik düzenlemeleri getirmemiş ve bunları uygulamak için kaynak oluşturmamıştır. Merkez bankalarının %56'sının finans sektörü için ulusal bir siber stratejisi bulunmamakta, %42'i özel bir siber güvenlik veya teknoloji risk yönetim yönetmeliğine sahip değil, %68'i uzmanlaşmış bir risk birimine sahip değil, %64'ü siber güvenlik önlemlerinin test edilmesini ve uygulanmasını zorunlu hale getirmemekte, %54'ü özel bir siber olay raporlama biriminden yoksun ve %48'inin siber suç düzenlemeleri mevcut değildir (Adrian & Ferreira, 2023).

Teknolojiye artan güven ve çok uluslu şirketler tarafından yürütülen büyük miktarda veri, yeni zorluklar ve güvenlik açıkları yaratmaktadır. Kişisel verilerin çok uluslu şirketler tarafından toplanması, saklanması ve kullanılmasıyla ilgili potansiyel riskleri vurgulayan en önemli vakalardan biri Cambridge Analytica skandalıdır. Firma, milyonlarca Facebook kullanıcısının kişisel bilgilerini izinleri olmadan toplamış ve analiz etmiştir (Meredith, 2018). Veriler ise 2016 yılında ABD başkanlık seçimleri ve Birleşik Krallık Brexit referandumu gibi siyasi kampanyalar sırasında hedefli kampanyalar oluşturmak için kullanılmıştır. Dolayısıyla

bireylerin mahremiyetini korumak ve verilerin şirketler tarafından kötüye kullanılması çerçevesindeki yasalarda önemli zayıflıklar görülmektedir.

2.4.3 Fırsatlar

Metaverse; Metaverse tanıtım, markalaşma ve pazarlama için benzersiz bir ortam sağlamaktadır. Çok uluslu şirketler için fırsatlar, Metaverse aracılığıyla gelişmiş müşteri ilişkileri ve küresel bir kullanıcı kitlesine ulaşma becerisini içerebilir. İşletmelere ürünleri ve hizmetleri sanal bir ortamda test etmeleri için yeni fırsatlar sunarak, maliyetleri düşürmeye ve verimliliği artırmaya yardımcı olabilir. Ayrıca Metaverse, yeniliği hızlandırmaya ve üretkenliği artırmaya yardımcı olabilecek yeni iş birliği ve bilgi paylaşımı biçimleri sağlayabilir. ABD'de Amazon, Google, Meta, Roblox, Facebook, Epic Games, Disney, Snapchat (Bitmoji), Nvidia, Microsoft (Microsoft için Mesh), Decentraland, Apple; Çin'de Tencent (Kings Metaverse), Alibaba, ByteDance, NetEase, Zqgame, Wondershare; Güney Kore'de, Samsung, SK Telecom, Urbanbase, Metaverse Alliance; Japonya'da Sony, Hassilas, GREE, Avex; İngiltere'de Sotheby's, Maze Theory; Fransa'da Stage11; İtalya'da Gucci çok uluslu şirketleri Metaverse vizyonuna yatırım yapmış ve ürün geliştirmiş şirketlere örnektir (Lopez-Diez, 2021, s. 302).

Metaverse'ün gelişmekte olan bir dijital ortam olduğunu ve potansiyelinin tamamının henüz gerçekleştirilmediğini belirtmek önemlidir. Bu nedenle Metaverse ‘ün tam potansiyelini ortaya çıkarmak için gerçekleşmesi muhtemel olanaklarını ve durumları rakiplerden önce keşfederek bir stratejinin belirlenmesi gerekmektedir.

Fintech; Geleneksel bankalardan daha hızlı değişime uyum sağlayan ve modern pazarlama kanallarını kullanan Fintech sektörü, finansal hizmet sağlayıcıları ve tüketiciler arasındaki etkileşimi daha kolay hale getirerek, müşterilerin finansal işlemlerini daha hızlı ve verimli bir şekilde gerçekleştirmelerini sağlar (Kim, Park, Choi, & Yeon, 2015 , s. 137). Geleneksel bankacılık ve ödeme sistemlerine kıyasla, yetersiz hizmet alan müşteriler dahil herkes tarafından erişilebilir düşük işlem maliyeti sunar. Blok zinciri gibi yeni teknolojileri kullanarak kullanıcıların finansal işlemlerini daha güvenli ve şeffaf olmasına yardımcı olur ve yapay zeka, makine öğrenimi gibi teknolojiler aracılığıyla da finansal hizmet sağlayıcılarının daha verimli operasyonlar gerçekleştirmesine olanak sağlar. Geliştirilen mobil uygulamalar ve sanal asistanlar aracılığıyla müşterilerin daha kolay işlem yapmasını sağlar. Fintech şirketleri, dijital ödemeler, borç verme, sigorta ve para yönetimi gibi alanlarda yenilik yaparak finans sektöründe önemli ilerlemeler kaydetmiştir. Dolayısıyla mobil ve çevrimiçi bankacılığın yükselişiyle birlikte bankalar, dijital bankaların ve Fintech girişimlerinin artan rekabetiyle karşı karşıya kalmaktadır. Küresel FinTech endüstrisinin önümüzdeki yıllarda hızla gelişmeye devam etmesi ve hem yeni başlayanlar hem de sektördeki tüm aktörler için sayısız fırsatlar sunması beklenmektedir. The Brainy Insights tarafından hazırlanan rapora göre küresel finansal teknoloji pazarının büyüklüğü 2021'de 115,34 milyar dolardır. Dijital ödemelerin ve cüzdanların artan kullanımı ve teknoloji tabanlı çözümlere yapılan artan yatırımlarla, 2022'den itibaren %36,2'lik yıllık büyüme oranıyla, 2030 yılına kadar 936,51 milyar dolara ulaşması beklenmektedir (The Brainy Insights, 2021).

FinTech, finansal hizmetlerin iyileştirilmesi ve ekonomik büyümenin hızlandırılması açısından ulus devletler ve çok uluslu şirketler için önemli fırsatlar sunmakta ve finansal teknoloji endüstrisindeki potansiyel pazar ve büyüme fırsatlarını içermektedir. Fintech, kırsal veya düşük gelirli bölgelerde geleneksek bankacılık işlemlerini gerçekleştiremeyen nüfuslara mobil ödeme ve dijital bankacılık hizmetlerinin sunulmasını sağlayarak, finansal hizmetlere erişimin genişletilmesini içermektedir.

2.4.4 Tehditler

Kuzey Kore; Kuzey Kore'nin 2014 yılında Sony Pictures'ı hedef alan siber saldırısı göz önüne alındığında hem stratejik avantaj elde etmek amacıyla hükümetlerden, askeri kuruluşlardan ve ileri düzey bilgi içeren özel şirketlerden hassas bilgileri çalmak amacıyla hem de savunma, imalat ve ileti teknoloji gibi belirli hedeflere yönelik ekonomik siber casusluk yürüttüğü söylenebilir (Beaumont-Thomas, 2014).

Kuzey Kore'nin nükleer silah geliştirme faaliyetlerini finanse etmek ve yaptırımlardan kaçınmak amacıyla enerji şebekeleri ve finansal hizmetler gibi kritik altyapıya karşı saldırgan siber operasyonlar düzenleme kabiliyetine sahip olduğuna inanılmaktadır. 2016 yılında Bangladeş Merkez Bankası'na yönelik siber saldırıda, Kuzey Kore destekli Lazarus grubu ile bağlantılı olduğu iddia edilen siber tehdit aktörleri, küresel bir finansal mesajlaşma ağı olan SWIFT'in kimlik bilgilerini ele geçirerek işlemlerle 81 milyon dolar çalmıştır (Kaspersky, 2017). Ayrıca Kuzey Kore'nin kripto para borsalarını ve kullanıcıları kendi ekonomik kazancı için dijital para birimlerini çalmayı hedeflediği de bilinmektedir.

Dark Web; Çok uluslu şirketler, özel bilgileri, ticari sırları ve finansal verileri çalmaya çalışan siber tehdit aktörleri tarafından sıklıkla hedef alındıklarından, Dark Web tehditlerine karşı savunmasızdır. Özellikle Dark Web üzerinden faaliyet gösteren siber tehdit aktörleri, dolandırıcılık ve kimlik hırsızlığı gibi eylemleri şirketler ve bireyler için önemli mali kayıplara neden olabilmekte ve ulusal güvenlik için bir tehdit oluşturabilmektedir. Örneğin Black Merket Reloded, Dark Web üzerinden Bitcoin aracılığıyla Avustralya, ABD, Hollanda Almanya, Fransa dahil birçok ülkeye elektronik cihazların için yerleştirilmiş ateşli silahların posta yoluyla satışını gerçekleştiren ve 500 dolara satılan bir tabancayı, Dark Web üzerinden 3.400 dolara satarak kar elde eden bir pazar olarak bilinmektedir (U.S. Attorney's Office, 2018).

3. SONUÇ

Çok uluslu şirketlerin ve ulus devletlerin siber uzay üzerindeki etkisini anlamaya odaklanan araştırmalar, günümüzün dijital çağında büyük önem taşımaktadır. Siber uzaya katılımlarını, güç dinamiklerini ve siber uzayın çeşitli boyutları üzerindeki etkilerini inceleyerek, aktörler arasında karmaşık etkileşime ve bunun sonucunda ortaya çıkan sonuçlara ilişkin önemli bulgular elde edilmektedir. Bu bilgi, bilgiye dayalı karar verme, etkili dijital yönetişim, güçlü siber güvenlik uygulamaları ve bireylerin, toplumların ve ulusların benzer şekilde çıkarlarını korurken dijital devrimin tüm potansiyelinden faydalanmak için gereklidir.

Siber uzayın ve dijitalleşmenin yararları toplumun her düzeyinde kendini göstermektedir. Finans, endüstri, eğlence, iş yaşamı, savaş, rekabet gibi birçok sektör ve alanda uygulamaları dönüştürmüş, yapay zekâ, bulut bilişim, nesnelerin interneti, artırılmış gerçeklik gibi Endüstri 4.0'ın tüm unsurlarının gelişimini hızlandırmıştır. Bununla dönüşüm, hem olumlu ve olumsuz sonuçlarla birlikte kendini göstermiş hem de siber güvenlik, siber savunma ve siber savaş konularında artan farkındalık ihtiyacına yol açmıştır. Dolayısıyla siber uzaya artan güven, iki ucu keskin kılıç olarak tanımlanabilecek bir saha yaratmıştır.

Siber uzay, hem süper güçler hem de daha küçük devletler tarafından kullanılan etkili bir araç haline gelmiş ve tüm ulus devletlerin kendilerini eşit düzeyde bulabilecekleri asimetrik savaş modelini oluşturmuştur. Askeri yeteneklerdeki eşitsizlikler nedeniyle siber uzayda dinamikler değişmekte ve daha küçük devletler, daha güçlü ulusların güvenlik açıklarını hedeflemek için siber yeteneklerini kullanmaktadır. Bununla birlikte, siber uzay asimetrik savaş için fırsatlar sunarken, süper güçler ile daha küçük devletler arasındaki güç eşitsizliklerini tamamen ortadan kaldırmadığına dikkat etmek önemlidir. Büyük ulus devletler daha gelişmiş siber yeteneklere ve kaynaklara sahip olduğu için siber uzayın şekillenmesinde hala önemli bir rol oynamaktadır.

Bir ulus devlet için siber egemenlik, bilginin stratejik bir kaynak olması nedeniyle yüksek önceliğe sahiptir. Kritik altyapıyı korumak, siber tehditlerle mücadele etmek ve siber barışı sağlamak ulusal güvenlik için elzemdir. Bilgiyi korumak, telekomünikasyon, endüstri, ekonomi, hükümet ve ordu dahil olmak üzere ulus içindeki çeşitli sektörlerin işleyişi için hayati önem taşımaktadır. Dolayısıyla siber uzayın kullanımı, birden fazla tehdidi beraberinde getirerek, devletleri dijital altyapılarının savunması için siber güvenliğe öncelik vermeye ve potansiyel siber savaşa karşı saldırı ve savunma yeteneklerini geliştirmeye sevk etmektedir. Siber savaş durumu birçok araştırmacı için bir efsane gibi görünse de siber uzayda dünyanın farklı bölgelerinden güçlü aktörlerin karıştığı vakalar, siber savaşın gerçekliğini göstermektedir. Siber savaş, özellikle ekonomik ve politik güçlerin temelini oluşturan dijital altyapılar açısından, devletlerin iç ve dış egemenliğine yönelik bir tehdit oluşturmaktadır.

Çok uluslu şirketler, siber uzayda inovasyon ve teknolojik ilerlemeleri yönlendiren ekonomik güç merkezleri olarak hizmet vermektedir. Geniş kaynakları, araştırma yetenekleri, platformları ve hizmetleri geliştirerek dijital ortamı şekillendirmektedir. Dolayısıyla çok uluslu şirketlerin siber uzayın teknolojik gidişatını şekillendirmede, ekonomik büyümeyi desteklemede ve endüstriler genelinde dijital dönüşümü yönlendirmede oynadığı rol önemlidir.

Araştırmada ele alınan ABD, Çin, Rusya ve İran açısından bilişim sektöründe ve jeopolitik çerçevede siber uzaydaki rekabetleri, devlet destekli siber güvenlik stratejilerinin oluşmasını gerekli kılmıştır. Bunun yanında Metaverse alanında Microsoft, Samsung ve Apple gibi çok uluslu teknoloji şirketlerinin girişimleri ve Fintech alanında finansal teknoloji şirketleriyle işbirliği yapan JPMorgan, Goldman Sachs, Citigroup, Deutsche Bank, BBVA ve Bank of Beijing gibi çok uluslu finans kurumlarının rekabette ön planda olduğu ve bununla ilgili çok önemli fırsatların meydana geldiği anlaşılmıştır. Kuzey Kore ve İran gibi ülkelerin saldırı yeteneklerinin, telekomünikasyon veya finans gibi hayati sektörlere yönelik saldırılarının ve Dark Web'in varlığının önemli bir tehdit oluşturduğu anlaşılmıştır. Ayrıca Çin ve ABD arasındaki ticaret savaşlarında Çinli telekomünikasyon şirketlerine yönelik getirilen kısıtlamaların incelenmesiyle ABD'den Çin'e yönelik bir tehdit algısının varlığı sonucuna varılmıştır. Bu yönüyle uluslararası hukukun güçlendirilmesi ve ilgili devletlerin birbiri arasındaki rekabetteki bu yönüyle siber casusluk gibi faaliyetlerin daha denetlenebilir ve daha hukuki olarak gözlemlenebilir olarak ele alınması BM barış ve güvenlik misyonuna daha yakın bir yaklaşım olarak görülecektir.

Siber yeteneklerin kullanımını kontrol edebilecek merkezi bir otoritenin bulunmaması, siber savaşın ortaya çıkmasına ve bireysel, örgütsel ve küresel düzeylerde çeşitli siber stratejilerin geliştirilmesine yol açmıştır. Ancak gelişmiş siber güvenlik yeteneklerine sahip ulus devletler tarafından uygulananlar da dahil olmak üzere ulusal siber stratejilerinin, siber tehdit aktörlerinin faaliyetlerini caydırma, düzenleme veya engellemede yetersiz kaldığı kanıtlanmıştır. Bunun nedeni, siber uzayın ulusal çıkarların gözetilebileceği bir alan sunduğu algısı ve kullanıcı faaliyetlerini denetleyen merkezi bir kontrol biriminin olmamasından kaynaklanıyor olabilir.

Sonuç olarak, siber tehdit aktörleri tarafından devletlerin, şirketlerin ve bireylerin veri havuzlarına izinsiz girişler, veri tabanlarına yapılan başarılı saldırılar devam etmektedir. Bu mevcut durumlar ise uluslararası ilişkilerde ekonomik, siyasi ve güvenlik konusunda etkiler göstermektedir. Hukuksal çerçevede ise bireysel, devletsel ve kurumsal unsurlar içerisinde boşlukları meydana getirmektedir.

Çatışma Beyanı:

- Araştırmacıların katkı oranları eşittir.

- Makalenin yazarları arasında çıkar çatışması bulunmamaktadır.

KAYNAKÇA

Adrian, T., Ferreira, C., (2023). *IMF Blog.* https://www.imf.org/en/Blogs/Articles/2023/03/02/mounting-cyber-threats-mean-financial-firms-urgently-need-better-safeguards adresinden alınmıştır

Aktan, S. (2019). *ABD'den Huawei'ye yeni suçlamalar: Çinli teknoloji devi neden hedefte?* . https://tr.euronews.com/2018/12/12/huawei-veliahtinin-tutuklanmasi-gelecegin-dunyasi-icin-oynanan-satrancin-bir-parcasi-mi adresinden alınmıştır

Argaman, S., & Siboni, G. (2014). Commercial and Industrial Cyber Espionage in Israel. *Military and Strategic Affairs, 6(1)*, 43-58.

Aydın, Ö. (2021). 5. Nesil Mobil İletişim Teknolojisi ve Uluslararası Yansımaları. *Teknoloji ve Uluslararası İlişkiler* (s. 41-65). içinde Ankara: Nobel Akademik Yayıncılık .

Beaumont-Thomas, B. (2014). *North Korea complains to UN about Seth Rogen comedy The Interview.* https://www.theguardian.com/film/2014/jul/10/north-korea-un-the-interview-seth-rogen-james-franco adresinden alınmıştır

Berman, N., Maizland, L., & Chatzky, A. (2023). *Is China's Huawei a Threat to U.S. National Security?* Council on Foreign Relations .

BrandFinance. (2023). *Tesla dépasse Mercedes-Benz et Toyota pour prendre la pole position en tant que marque automobile la plus valorisée au monde.* https://brandfinance.com/press-releases/tesla-depasse-mercedes-benz-et-toyota-pour-prendre-la-pole-position-en-tant-que-marque-automobile-la-plus-valorisee-au-monde adresinden alınmıştır

Boudette, N. E. (2020). *Tesla Shines During the Pandemic as Other Automakers Struggle.* https://www.nytimes.com/2020/07/02/business/tesla-sales-second-quarter.html adresinden alınmıştır

Bowen, A. S. (2021). *Russian Military Intelligence: Background and Issues for Congress.* Congressional Research Service (CRS): https://sgp.fas.org/crs/intel/R46616.pdf adresinden alınmıştır

Chandel, S., Jingji, Z., Yunnan, Y., Jingyao, S., & Zhipeng, Z. (2019). The Golden Shield Project of China: A Decade Later—An in-Depth Study of the Great Firewall. *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)* . Guilin: IEEE.

CompaniesMarketCap.com. (2023). *Largest tech companies by market cap.* https://companiesmarketcap.com/tech/largest-tech-companies-by-market-cap/ adresinden alınmıştır.

Çoban, B., & Karakaya, Y. E. (2010). Geleceği Planlamada Stratejik Yönetim Ve Swot Analizi: Kavramsal Yaklaşımlar. Social Sciences, 5(4), 342-352. https://Doi.Org/10.12739/10.12739

Çahmutoğlu, E. (2021). *İran'ın Siber Gücü.* Ankara : İram Yayınları.

DOD. (2010). *Department of Defense Dictionary of Military and Associated Terms. U.S. Department of Defence*. Federation of American Scientist.

FAS. (2000). *James Adams* . https://irp.fas.org/congress/2000_hr/030200_adams.htm adresinden alınmıştır

Financial Times. (2022). *Ukraine war is chip industry's kryptonite.* https://www.ft.com/content/950072f0-8c22-4050-bc63-631fa4b481eb adresinden alınmıştır

Gerasimov, V. (2016). The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations . *Military Review*, 23-26.

Glaister, D. (2009). *China accused over global computer spy ring.* The Guardian: https://www.theguardian.com/world/2009/mar/30/china-dalai-lama-spying-computers adresinden alınmıştır

Gong, X. (2021). *5G and China-US Relations: Competition and Intervention.* Halifax : Dalhousie University

Huawei. (tarih yok). *Company Facts.* https://www.huawei.com/en/media-center/company-facts adresinden alınmıştır

Kaspersky. (tarih yok). *Fidye yazılımlarının tanınması – şifrelenmiş Truva atlarından farkı nedir?* https://www.kaspersky.com.tr/resource-center/threats/ransomware-attacks-and-types adresinden alınmıştır

Kaspersky. (2017). *Chasing Lazarus: A Hunt for the Infamous Hackers to Prevent Large Bank Robberies.* https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies adresinden alınmıştır

Kumar, D. K. (2020). *Oil prices jump after U.S. air strike kills top Iranian commander.* Reuters: https://www.reuters.com/article/us-global-oil-idUSKBN1Z2030 adresinden alınmıştır

Kim, Y., Park, Y.-J., Choi, J., & Yeon, J. (2015). An Empirical Study on the Adoption of "Fintech" Service: Focused on Mobile Payment Services. *Advanced Science and Technology Letters, Vol:114*, 136-140.

Lopez-Diez, J. (2021). Metaverse: Year One. Mark Zuckerberg's video keynote on Meta. *Pensar public, 15(2)*, 299-303.

Mbanaso, U., & Dandaura, E. (2015). The Cyberspace: Redefining A New World. *IOSR Journal of Computer Engineering (IOSR-JCE), 18(3)*, 17-24.

McKew, M. K. (2017, 09 05). *The Gerasimov Doctrine.* https://www.politico.eu/article/new-battles-cyberwarfare-russia/ adresinden alınmıştır

Meredith, S. (2018). *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal.* https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html adresinden alınmıştır

Microsoft. (tarih yok). *Xbox.* https://www.microsoft.com/en-us/store/b/xbox?icid=CNavDevicesXbox adresinden alınmıştır

Microsoft. (tarih yok(a)). *Microsoft acquires GitHub.* https://news.microsoft.com/announcement/microsoft-acquires-github/ adresinden alınmıştır

Microsoft. (tarih yok(b)). *Microsoft buys LinkedIn.* https://news.microsoft.com/announcement/microsoft-buys-linkedin/ adresinden alınmıştır

Microsoft. (tarih yok(c)). *Microsoft purchases 'Minecraft'.* https://news.microsoft.com/announcement/microsoft-purchases-minecraft/ adresinden alınmıştır

NATO. (2020). *Allied Joint Publication-3.20 Allied Joint Doctrine for Cyberspace Operations* . NATO STANDARDIZATION OFFICE (NSO).

O'Connell, M. E. (2012). Cyber Security and International Law . *Chatham House*.
Quadri, L. A., & Rasaq, M. O. (2020). Cyber Theatre a Fifth Domain of International Politics:Africa and the rest of the world in the Cyberspace. *Akdeniz Havzası ve Afrika Medeniyetleri Dergisi, 2(2)*, 98-11.
Sacks, D. (2021). *China's Huawei Is Winning the 5G Race. Here's What the United States Should Do To Respond.* CFR: https://www.cfr.org/blog/china-huawei-5g adresinden alınmıştır
Sajedi, F., & Ariani, M. G. (2014). Cyber-Crimes in Iran: Definition and Analysis. *The International Conference on Cyber-Crime Investigation and Cyber Security* (s. 7-10). Kuala Lumpur : Asia Pacific University of Technology and Innovation.
Schmitt, M. (2018). *In Defense of Sovereignty in Cyberspace*. Just Security: https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/ adresinden alınmıştır

The Brainy Insights. (2021). Fintech Market. s. https://www.thebrainyinsights.com/report/fintech-market-12704.
Tropeano, R. (2019). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. National Security Archive: https://nsarchive.gwu.edu/news/cyber-vault2019-04-24/tallinn-manual-20-international-law-applicable-cyber-operations adresinden alınmıştır
UNCCT. (tarih yok). *Cybersecurity and New Technologies.* UN Counter-Terrorism Centre: https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity adresinden alınmıştır
UN General Assembly. (2003). *57/239. Creation of a global culture of cybersecurity.* United Nations .
United Against Nuclear Iran [UANI]. (2022). *The Iranian Cyber Threat.*
U.S. Attorney's Office. (2018). *Darknet international gun traffickers sentenced.* https://www.justice.gov/usao-ndga/pr/darknet-international-gun-traffickers-sentenced adresinden alınmıştır
Wolff, J. (2018). *Trump's Reckless Cybersecurity Strategy.* The New York Times: https://www.nytimes.com/2018/10/02/opinion/trumps-reckless-cybersecurity-strategy.html adresinden alınmıştır
Westby, J. R. (2020). *Russia Has Carried Out 20-Years Of Cyber Attacks That Call For International Response*. Forbes: https://www.forbes.com/sites/jodywestby/2020/12/20/russia-has-carried-out-20-years-of-cyber-attacks-that-call-for-international-response/?sh=1f6f532c6605 adresinden alınmıştır
Weimann, G. (tarih yok). *Going Darker? The Challenge of Dark Net Terrorism.* Wilson Center .
Yetgin, M. A., & Özkan, S. (2022). Metaverse, Küresel Şirketler, Ulus Devletler ve Yeni Bir Uluslararası Sistem. *5th International New York Academic Research Congress* , (s. 209-2015). New York .