T.C.

YALOVA ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

STRATEJİK BİR BELİRSİZLİK ALANI OLAN SİBER UZAYDA NORM OLUŞTURMA ÇABALARININ İNCELENMESİ

YÜKSEK LİSANS TEZİ

Tuba FIRAT

Enstitü Anabilim Dalı: ULUSLARARASI İLİŞKİLER

Enstitü Bilim Dalı: ULUSLARARASI İLİŞKİLER

Tez Danışmanı: Dr. Öğretim Üyesi Övgü KALKAN KÜÇÜKSOLAK

TEMMUZ 2021

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ YÜKSEK LİSANS İNTİHAL YAZILIM RAPORU BEYAN BELGESİ

Tez Başlığı: STRATEJİK BİR BELİRSİZLİK ALANI OLAN SİBER UZAYDA NORM OLUŞTURMA ÇABALARININ İNCELENMESİ

Yukarıda başlığı belirtilen tez çalışmamın toplam 108 sayfalık kısmına ilişkin aşağıda belirtilen filtrelemeler uygulanarak alınmış olan ve 16/05/2021 tarihinde aşağıda ismi yazılı araştırma görevlisi tarafından şahsıma iletilen Turnitin intihal tespit programı raporuna göre tezimin benzerlik oranı %3'tür.

Uygulanan filtrelemeler:

1. Kaynakça hariç,
2. Alıntılar dâhil,
3. 5 kelimeden daha az örtüşme içeren metin kısımları hariç.

Bu bilgiler doğrultusunda tez çalışmamın herhangi bir intihal içermediğini; aksinin tespiti halinde doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

İmza

Adı Soyadı : Tuba FIRAT
Öğrenci Numarası : 187207001
Ana Bilim Dalı : Uluslararası İlişkiler
Programı : Uluslararası İlişkiler
Türü : ( ) Proje (*) Yüksek Lisans Tezi ( ) Doktora Tezi

Danışman
Dr. Öğretim Üyesi Övgü KALKAN KÜÇÜKSOLAK,
16.05.2021
İmza

ÖNSÖZ

Siber uzayda stratejik olarak inşa edilen siber normların bir rekabet unsuru haline geldiği sahada, stratejik norm inşası sürecinin hem devletler hem de devletler ile özel şirketler gibi diğer paydaşlar arasında çeşitli mücadelelere sahne olduğu görülmektedir. Bu çerçevede siber alandaki normların şekillendirilmesi süreci; devletlerin ulusal mülahazaları çerçevesinde verdikleri güç mücadelelerini, özel sektörün norm girişimciliği rolüyle kendi hareket alanını geliştirme çabalarını ve uluslararası örgütlerin kendi kurumsal prensipleri ve hedefleri doğrultusunda geliştirdiği söylemleri barındıran çok yönlü bir süreci ifade etmektedir. Bu kapsamda çalışmaya Türkiye özelinde bir bölüm konulmasına karar verilerek çalışmanın Türkiye'ye bu alanda farklı bir perspektif açması ve alternatif fikirler oluşturması noktasında katkı sağlaması hedeflenmektedir.

Bu tez çalışmasının planlaması ve yazım süreci boyunca siber uzaya olan ilgimi teşvik edip beni cesaretlendirerek ilerlememi sağlayan, kafamdaki soru işaretlerini tutarlı bir şekilde gidererek yönümü belirleyen ve orijinal bakış açısıyla bana ilham vererek maddi manevi desteğini koruyan sevgili danışman hocam Dr. Öğretim Üyesi Övgü KALKAN KÜÇÜKSOLAK'a teşekkürlerimi arz ederim. Bu tez çalışması bugünlere geldiyse kendisi sayesindedir.

Buna ek olarak, sürecin en başında siber uzay üzerine Türkiye'de erken yaşta çalışmaya başlayan sayılı kişilerden olmam için beni yüreklendiren Siber Bülten'in kurucusu Minhac ÇELİK'e teşekkürlerimi mutlaka sunmak isterim.

Sonunu, ötesini bilmeden çıktığım bu yolda bana ortak olma kahramanlığını göstererek tezimin başından sonuna kadar geçen her aşamasında yanımda olan, işlerimi kolaylaştıran, tertemiz enerjisiyle gücüme güç katan, benimle aynı yolun yolcusu olduğunu bildiğim sevgili dostum Baha Ahmet YILMAZ'a en içten teşekkürlerimi sunmayı bir borç bilirim. Ayrıca tez çalışmam boyunca yoğunluktan başımı kaldıramadığımda dahi bir mesajıyla kalbimi fetheden, bana olan anlayışını ve sevgisini daima hissettiğim kıymetli dostum Betül KURT'a en derin teşekkürlerimi sunmak isterim. Bunun yanı sıra bu tez çalışması daha sadece giriş aşamasındayken umutsuz bir gecede elimden tutup bir daha hiç bırakmayan ve her defasında tüm manevi desteğini yansıtan Büşra Dilara ARVAS'a sonsuz teşekkürlerimi sunarım.

Çalışma boyunca buraya yazamayacağım kadar sayısız yolla yükümü hafifleten, başarmak istediklerime giden yolda ilk aşamayı tamamlarken aktif desteğini sürdüren, heyecanımı paylaşan, bugünlere gelmem için türlü fedakârlıklarda bulunan, aydınlık ve çağdaş fikir yapısı ve güçlü duruşuyla bana örnek olan sevgili annem Zeynep KAYTANOĞLU'na ve maddi manevi her boyutta daima yanımda olduğunu hissettiğim bir tanecik kardeşim Bilal FIRAT'a teşekkürlerimi bir borç bilirim. Son ama en önemli kısımda ise, benim ilk öğretmenim olan, fiziki olarak yanımda olamasa dahi her daim benimle gurur duyduğuna inandığım rahmetli babam Mustafa FIRAT'a kalbimin en derin köşesinden gelen sonsuz teşekkür ve sevgiyi iletmeyi borç bilirim.

Tuba FIRAT

14.07.2021

İÇİNDEKİLER

KISALTMALAR LİSTESİ

AAD: Avrupa Adalet Divanı
AB: Avrupa Birliği
ARPA: Gelişmiş Araştırma Projeleri Ajansı
ARPANET: Gelişmiş Araştırma Projeleri Ajansı Ağı
ASEAN: Güneydoğu Asya Uluslar Birliği
BİT: Bilgi ve İletişim Teknolojileri
BM: Birleşmiş Milletler
BT: Bilgi Teknolojileri
CAC: Çin Siber Uzay İdaresi
CDMB: Siber Savunma Yönetimi Kurulu
CERN: Avrupa Nükleer Araştırma Merkezi
CERT: Bilgisayar Acil Durum Müdahale Ekipleri
ECPA: Elektronik İletişim Gizlilik Yasası
ENISA: Avrupa Ağ ve Bilgi Güvenliği Ajansı
GCSC: Siber Uzayın İstikrarı Hakkında Küresel Komisyon
GGE: Hükümet Uzmanları Grubu
IANA: İnternete Atanmış Numaralar Kurumu
ICANN: İnternet Tahsisli Sayılar ve İsimler Kurumu
ICPA: Uluslararası İletişim Gizliliği Yasası
IGF: İnternet Yönetişim Forumu
IP: İnternet Protokolü
ITU: Uluslararası Telekomünikasyon Birliği
NAC: Kuzey Atlantik Konseyi
NATO: Kuzey Atlantik Anlaşması Örgütü
NISA: Ulusal Nükleer Güvenlik Ajansı
NIST: Ulusal Standartlar ve Teknoloji Enstitüsü
NSFNET: Ulusal Bilim Vakfı Ağı
NTIA: Ulusal Telekomünikasyon ve Bilgi İdaresi
OEWG: Açık Uçlu Çalışma Grubu
S/CCI: Siber Sorunlar Koordinatörlüğü Ofisi
SGK: Siber Güvenlik Kurulu
SİSAMER: Siber Savunma Merkezi
STK: Sivil Toplum Kuruluşu
USOM: Ulusal Siber Olaylara Müdahale Merkezi
WGIG: İnternet Yönetişimi Çalışma Grubu
WSIS: Dünya Bilgi Toplumu Zirvesi

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

FOTOĞRAFLAR LİSTESİ

ÖZET

Tezin Başlığı: Stratejik Bir Belirsizlik Alanı Olan Siber Uzayda Norm Oluşturma Çabalarının İncelenmesi	
Tezin Yazarı: Tuba FIRAT	**Danışman:** Dr. Öğretim Üyesi Övgü KALKAN KÜÇÜKSOLAK
Kabul Tarihi: 16.06.2021	**Sayfa Sayısı:** x (ön kısım) + 108 (tez)
Anabilim Dalı: Uluslararası İlişkiler	**Bilim Dalı:** Uluslararası İlişkiler

Soğuk Savaş sonrası dönemde siber uzay, çok farklı ve artan sayıda aktörün rekabetine konu olan bir stratejik operasyonel alan olarak öne çıkmaktadır. Siber uzayın sınırsız ve dinamik yapısı bir taraftan çeşitli fırsatlar sunarken, diğer taraftan da yarattığı belirsizlikler üzerinden aktörlerin meydan okumalarla karşı karşıya kalmalarına sebebiyet vermektedir. Bu çerçevede önümüzdeki dönemde uluslararası sistemin işleyişinde artan düzeyde etkili olacağı düşünülen siber uzay kapsamında farklı düzeylerdeki aktörlerin norm oluşturma çalışmaları yaptıkları gözlenmektedir. Zira normlar üzerinden siber uzayın belirsiz yapısına çeşitli açılardan netlik kazandırılmaya ve bu bağlamda siber alandaki operasyonlara bir çerçeve kazandırılmaya çalışılmaktadır. Bu tez çalışmasında, Soğuk Savaş sonrası dönemde siber uzayda öne çıkan başlıca devletlerin, özel şirketlerin ve örgütlerin norm oluşturma çabaları incelenmiş ve Türkiye'nin bu alandaki çalışmalarına ışık tutulması hedeflenmiştir.

Stratejik bir belirsizlik alanı olan siber uzayda norm oluşturma çabalarının irdelendiği bu çalışmanın ilk bölümünde "siber uzay", "norm" ve "siber norm" kavramları tanımlanarak içeriklerine netlik kazandırılmıştır. İkinci bölümde ise, Soğuk Savaş sonrası uluslararası sistemde yaşanan dönüşüm detaylı bir şekilde ele alınmış, Kopenhag Ekolü üzerinden genişleyen ve derinleşen güvenlik ortamı irdelenmiş ve siber normların analizinde yararlanılan Sosyal İnşacılık yaklaşımı kapsamlı şekilde değerlendirilmiştir. Siber yönetişimin tartışılması kapsamında da bir yönetişim ağı tasarısında yer alabilecek unsurlara değinilmiş, siber normların pratiğe dökülmesi sürecinden bahsedilmiş ve çok paydaşlı yönetişim ile siber egemenlik modellerinin uygulanabilirliği sorgulanmıştır. Üçüncü bölümde ise, ikinci bölümde yer alan siber egemenlik ve çok paydaşlı yönetişim modelleri ABD, Çin, Rusya ve Türkiye örnekleri üzerinden tartışılmış, devletlerin söz konusu yaklaşımlar üzerinden geliştirdikleri politikalar incelenmiştir. Devletlerin yanı sıra siber uzayda önemli rol oynayan diğer paydaşlar olarak özel şirketler başlığı altında norm girişimcileri olarak nitelendirilen Microsoft, Google, Siemens ve Nornickel'in süreçteki rollerine değinilmiş, ortaya koydukları temel mülahazalar irdelenmiştir. İnternet yönetişiminde önemli rol oynayan uluslararası örgütler başlığı altında ise NATO, GCSC ve BM'nin çalışmaları değerlendirilmiş, bu platformlarda tartışılan prensipler bütüncül bir çerçevede analiz edilmiştir.

Siber uzayın coğrafi bir sınıra tabi olmaması, saldırganların tespitinin zorluğu ve hesap verilebilirlik konusunda herhangi bir netliğin bulunmaması bu operasyonel alanda devletten bireye uzanan bir ölçekte aktörlerin çok çeşitli kırılganlıklarla karşı karşıya kalmasına sebebiyet vermektedir. Bu belirsizlik ortamının aşılmasında sürecin paydaşları tarafından geliştirilecek olan siber normların etkili olması beklenmektedir. Bu kapsamda son derece kritik bir öneme haiz olan normların geliştirilmesi bağlamında uluslararası sistemdeki yerini ve nüfuzunu genişletmek isteyen aktörlerin stratejik bir norm inşası sürecine girdikleri görülmektedir. Uluslararası sistemi şekillendirmek isteyen aktörlerin benimsedikleri prensipler üzerinden normlar geliştirerek uygulamalar aracılığıyla bunları davranış kalıpları haline getirmeye çalıştıkları görülmektedir. Siber uzayda stratejik olarak inşa edilen siber normların bir rekabet unsuru haline geldiği sahada, stratejik norm inşası sürecinin hem devletler hem de devletler ile özel şirketler gibi diğer paydaşlar arasında çeşitli mücadelelere sahne olduğu görülmektedir. Bu çerçevede siber alandaki normların şekillendirilmesi süreci; devletlerin ulusal mülahazaları çerçevesinde verdikleri güç mücadelelerini, özel sektörün norm girişimciliği rolüyle kendi hareket alanını geliştirme çabalarını ve uluslararası örgütlerin kendi kurumsal prensipleri ve hedefleri doğrultusunda geliştirdiği söylemleri barındıran çok yönlü bir süreci ifade etmektedir.

Anahtar Kelimeler: Siber Uzay, Siber Güvenlik, Siber Normlar, Sosyal İnşacılık, İnternet Yönetişimi

SUMMARY

Thesis Title: Examining Norm Formation Efforts in Cyber Space Which is a Strategic Area of Uncertainty	
Thesis Author: Tuba FIRAT	**Advisor:** Assist. Prof. Dr. Övgü KALKAN KÜÇÜKSOLAK
Date of Acceptance: 16.06. 2021	**Total Number of Pages:** x (pre text) + 108
Department: International Relations	**Field of Study:** International Relations

Cyberspace in the post-Cold War period stands out as a strategic operational area which increasingly become a theatre of competition for diverse and increasing numbers of actors. While the limitless and dynamic nature of cyberspace offers various opportunities on the one hand; on the other hand, it causes the actors to face challenges through the uncertainties it creates. Within this framework, it is observed that actors at different levels work on creating norms within the scope of cyberspace, which is thought to be increasingly effective in the functioning of the international system in the upcoming period. Because, through norms, it is tried to clarify the uncertain structure of cyberspace from various angles and in this context to give a framework to the operations in cyberspace. In this thesis study, the efforts of the primary states, private companies, and organizations that came to the fore in cyberspace in the post-Cold War period were examined and it is aimed to shed light on Turkey's studies in this field.

In the first chapter of this study, where the efforts to form norms in cyberspace, which is a strategic uncertainty area, are examined, the concepts of "cyberspace", "norm", and "cyber norm" have been defined and their scopes have been clarified. In the second chapter, the transformation in the international system after the Cold War is discussed in detail, the security environment expanding and deepening over the Copenhagen School is examined, and the Social Constructivism approach used in the analysis of cyber norms is comprehensively evaluated. Within the scope of the discussion of cyber governance, the elements that can be included in a governance network design were mentioned, the process of putting cyber norms into practice was expressed, and the applicability of multi-stakeholder governance and cyber sovereignty models was questioned. In the third chapter, the cyber sovereignty and multi-stakeholder governance models in the second chapter are discussed through the examples of the USA, China, Russia, and Turkey, and the policies developed by the states through these approaches are examined. The roles of Microsoft, Google, Siemens, and Nornickel, which are considered as norm entrepreneurs under the title of private companies, as other stakeholders playing an important role in cyberspace, as well as states, were addressed and the basic considerations they put forward were examined. Under the title of international organizations that play an important role in Internet governance, the studies of NATO, GCSC, and the UN were evaluated, and the principles discussed in these platforms were analyzed in a holistic framework.

The fact that cyberspace is not subject to a geographical boundary, the difficulty of identifying attackers, and the lack of clarity about accountability cause actors to face a wide variety of vulnerabilities in this operational area on a scale from the state to the individual. It is expected that the cyber norms to be developed by the stakeholders of the process will be effective in overcoming this uncertain situation. In this context, it is seen that actors who desire to expand their position and influence in the international system in the context of the development of norms, which are provided with critical importance, have entered into the process of a strategic norm-construction. It is seen that the actors who desire to shape the international system try to develop norms based on the principles they have adopted and transform them into behavioral patterns through practices. In the field where cyber norms, which are strategically constructed in cyberspace, have become a competitive element, it is seen that the strategic norm construction process is the scene of various struggles between states and other stakeholders such as states and private companies. In this context, the process of shaping the norms in cyberspace; represents a multi-faceted process that includes the power struggles of states within the framework of their national considerations, the efforts of the private sector to develop their movement area with the role of norm entrepreneurship, and the discourses developed by international organizations in line with their own corporate principles and goals.

Keywords: Cyberspace, Cybersecurity, Cyber Norms, Social Constructivism, Internet Governance

GİRİŞ

Endüstri 4.0, Nesnelerin İnterneti, 3D yazıcılar, yapay zekâlar gibi birçok yenilikle beraber teknolojik bir dönüşümün yaşandığı 21. yüzyılda; siber normlar, siber uzaydaki güvenlik ve istikrar üzerinde söz sahibi olmak amacıyla devletler tarafından tercih edilen bir araç konumundadır. 1998 yılında Birleşmiş Milletler'de (BM) "Güvenlik bağlamında bilgi ve telekomünikasyon alanındaki gelişmeler" adı altında sunulan bir taslak ile başlayan ve ardından 2015 yılında BM Hükümet Uzmanları Grubu'nun (GGE) siber uzayda devlet davranışlarını düzenleme üzerine normlar önermesiyle raporlar şeklinde devam eden siber normlar, uluslararası toplumda önemli bir araç olarak varlığını sürdürmektedir.

Kara, hava, deniz ve uzaydan sonra beşinci operasyonel alan olan siber uzayda fiziksel olarak bir sınır bulunmamaktadır. Bu nedenle siber saha, devletlerin iç işlerinin ötesine uzanan, asimetrik gücün söz konusu olduğu ulusaşırı bir işlevsel alandır. Öte yandan küresel olarak ortak bir siber uzay tanımının dahi olmadığı bu sahada, devletlerin sınırlarını belirlemeleri oldukça zordur. Bu bağlamda devletler, belirsizlikleri bir nebze azaltabilme arzusuyla siber uzayda norm oluşturma sürecine girmişlerdir.

Bir topluluk içerisinde karşıdaki aktörden beklenen uygun davranış biçimi olan normlar, keskin ve değişmez bir anlaşma maddesi olmaktan ziyade yoruma göre değişebilen bir sosyal inşa ürünüdür. Siber uzayda inşa edilen normlar olan siber normlar ise, devletlerin kültür, kimlik ve algısına bağlı olarak siber uzayı düzenleyici etkilere sahip olan davranış gerekliliklerdir. Siber uzayda net bir sınır olmadığı için siber normları da belli bir çerçevede sınırlandırmak mümkün değildir. Zira bir inşa süreci olan norm oluşturma süreci, aktörlerin çıkarlara bağlı olarak sabit kalmayacak ve dönüşüme uğrayacaktır. Uluslararası sistemdeki devletlerin kendilerine özgü kültür ve kimlikleri söz konusu olduğundan, buna bağlı olarak çıkarlarının da değişiklik göstereceğini ifade etmek mümkündür. Diğer beş sahadan farklı olarak etki alanı daha geniş olan siber uzayda söz sahibi olmak isteyen büyük güçler, siber uzayda norm oluşturma konusunda güç mücadelelerine girmekte ve rekabet içerisinde bu süreci ilerletmektedirler.

Devletler ve uluslararası örgütlerin, normları geliştirme ve teşvik etme üzerine yaptığı çalışmaların yanı sıra, Microsoft, Google, Siemens ve Nornickel gibi bilgi ve iletişim teknolojileri (BİT) alanında söz sahibi olan özel şirketlerin de norm oluşturma sürecinde başlıca aktörler olarak yer aldığını öne sürmek mümkündür. Özetle bu çalışmada; ABD'nin İnternet yönetişimi liderliğinden, Çin'in güvenli şehir teknolojisiyle Orta Asya'daki nüfuzuna ve Rusya'daki bölgedeki faaliyetlerine, BM GGE raporlarından, Estonya saldırıları sonucu NATO'nun siber saldırılar noktasında oluşan ciddiyetine, Microsoft'un endüstrideki norm öncülüğünden, Google, Siemens ve Nornickel'in siber uzayda gerçekleştirdiği düzenlemelere uzanan siber norm oluşturma sürecinde yer alan dinamikler anlatılacak ve devletlerarası güç mücadeleleri ve rekabetin yer aldığı uluslararası sistemdeki dönüşüme yer verilerek ulusüstü bir siber yönetişime varma konusunda bir analiz yapılacaktır. Son olarak belirtmek gerekir ki; yapılan bu çalışmayla, uluslararası sistemde söz sahibi olmak isteyen devletlerin siber sahada norm oluşturma çabaları ortaya konularak, Türkiye'nin bu alanda izleyeceği siber norm oluşturma sürecine ışık tutulması amaçlanmaktadır.

Çalışmanın Konusu

Bu tez çalışmasında, uluslararası sistemde önemli bir etkiye sahip olan siber uzayda norm oluşturma çabaları, merkezde devletler olmak üzere; devletler, uluslararası örgütler ve özel şirketler üzerinden tartışılmaktadır. Tehditlerin belirsiz olduğu ve coğrafi sınırların bulunmadığı beşinci operasyonel alan olan siber uzayın artan şekilde aktörlerin mücadele ve işbirliklerine konu olduğu görülmektedir. Siber uzay üzerinden şekillenebilecek olan uluslararası sistemde aktörlerin norm inşası alanında çalışmalarına hız vererek belirsizliklerin üstesinden gelmeye ve sistemi şekillendirmeye çalıştıklarını söylemek mümkündür. Bu noktada siber normların bizzat kendisinin bir rekabet alanı haline geldiği ve norm inşası sürecinin devletlerarası güç mücadelelerine sahne olduğu gözlemlenmektedir.

Çalışmanın ilk bölümünde; "siber uzay", "norm" ve "siber norm" kavramlarının açıklanması ve tartışılmasıyla çalışmanın ilerleyen bölümlerinde bu kavramların ifade ettiği anlam konusunda oluşabilecek karmaşanın önüne geçilmesi amaçlanmıştır. İkinci bölümde ise, Soğuk Savaş sonrası uluslararası sistemde yaşanan dönüşüm detaylı bir şekilde ele alınmış, Kopenhag Ekolü'nün siber uzayın anlaşılması konusundaki açıklayıcılığının önemine değinilmiş ve çalışmanın devamında siber normların analizinde kullanılan Sosyal İnşacılık yaklaşımı irdelenmiştir. Buna ek olarak, siber uzayın konusu olduğu bir yönetişim ağı tasarısında yer alabilecek unsurlara değinilmiş, siber normların pratiğe dökülmesi sürecinden bahsedilerek çok paydaşlı yönetişim ile siber egemenlik modellerinin uygulanabilirliği tartışılmıştır.

Üçüncü bölümde ise, siber egemenlik ve çok paydaşlı yönetişim modelleri ABD, Çin ve Rusya'nın incelenmesinde kullanılan modeller olarak çalışılmış ve devletlerin faaliyetleri bu modellerin unsurları kapsamında değerlendirilmiştir. Çok paydaşlı yaklaşım çerçevesinde özel şirketler başlığı altında Microsoft, Google, Siemens ve Nornickel'in, norm girişimcileri olarak rollerine değinilirken uluslararası örgütlerin farklı konulardaki inisiyatifleri ve norm çalışmaları üzerinde durulmuştur.

Çalışmanın Önemi

Siber uzay kullanıcılarına bir taraftan pek çok fırsat sunarken, diğer yandan da artan karşılıklı bağımlılıklar üzerinden kırılganlıkların ve tehditlerin pek çok düzeyde kendini göstermesine yol açmaktadır. Bu çalışmada da siber uzayın kırılganlıkları ve fırsatları bir arada bulunduran söz konusu çok boyutlu yapısına paralel olarak, bir mücadele alanı haline gelen siber norm oluşturma süreci özgün bir yaklaşımla Sosyal İnşacılık teorisinin sunduğu perspektifle ele alınmıştır. Aktörlerin norm oluşturma sürecini kendi çıkarları doğrultusunda şekillendirme çabaları ise, realist bir yaklaşımla güç mücadeleleri kapsamında irdelenmiş ve analiz edilmiştir.

Siber uzayda devletlerin norm oluşturma sürecinde özellikle de özel şirketlerin artan öneminin vurgulanması konusunda literatürde bir boşluk söz konusudur. Bu çalışma ile birlikte hedeflenen noktalardan biri; söz konusu boşluğun doldurularak kendi alanlarında söz sahibi olan şirketlerin, normların geliştirilmesi ve uygulanması konusundaki katkılarının ortaya konulmasıdır. Buna ek olarak, devlet odaklı norm inşası çabaları

karşısında özel şirketlerin hak ve özgürlükler temelli yaklaşımlarının farklılıklarına ve kesişimlerine de yer verilmektedir.

Çalışmada siber uzayın son derece stratejik bir alan olduğu ortaya konularak, bu alanda gerek devletler, gerek özel şirketler gerekse uluslararası örgütler çerçevesinde norm inşası kapsamında yapılan kapsamlı çalışmalara odaklanılmaktadır. Uzun dönemde stratejik önemi gitgide artacak olan söz konusu alanda Türkiye'nin çabalarına hız vermesi gerektiği aşikârdır. Bu minvalde, Türkiye'deki mevcut çalışmalara değinilmesi, önümüzdeki dönemde atılabilecek olan adımların irdelenmesi ve bir tartışma ortamı yaratılmasına katkı sunması bu tezin başlıca amaçları arasında yer almaktadır.

Çalışmanın Hipotezleri

Stratejik bir alan haline gelen siber uzayın farklı düzeylerdeki aktörler arasında, norm inşası kapsamında çeşitli mücadele ve işbirliklerine konu olduğu bu çalışmanın temel hipotezi olarak öne sürülmektedir.

Siber uzayın belirsizliklerini aşmak ve kendi çıkarları doğrultusunda bu alanın şekillenmesini isteyen aktörleri siber uzayda stratejik bir norm inşası sürecinden geçmektedirler. Siber uzayda stratejik olarak inşa edilmekte olan siber normların kendisinin hem bir rekabet hem de işbirliği alanı haline gelmesi hipotez olarak çalışmada yer almaktadır.

Siber norm oluşturma çabaları çok boyutlu bir çerçevede sürmektedir. Devletlerin yanı sıra endüstrideki özel şirketlerin de stratejik bir alan olarak gördükleri siber uzaydaki norm inşası sürecine kendi çıkarları doğrultusunda ciddi katkılarda bulunduğu öne sürülmektedir. Çok paydaşlı yaklaşım çerçevesinde uluslararası örgütler de faaliyet gösterdikleri farklı konularda norm oluşturma çabalarına destek vermekte ve hatta kimi alanlarda öncülük etme çabası içerisinde oldukları iddia edilmektedir.

Çalışmanın Amacı

Bu çalışmada, siber alanda norm oluşturma çabalarının farklı aktörler ve mülahazalar üzerinden sorgulanması ve bu çabaların sistemi şekillendirme çalışmalarının bir parçası olup olmadığının tartışılması amaçlanmıştır. Devletler başta olmak üzere çeşitli düzeylerdeki aktörlerin siber norm oluşturma çabalarının tartışılması kapsamında Türkiye'nin önümüzdeki dönemde yürüteceği siber güvenlik politikalarına farklı bir perspektif sunulması ve siber norm oluşturma sürecindeki girişimlerine ışık tutulması amaçlanmaktadır. İfade edilen amaçlar doğrultusunda bu çalışmada aşağıdaki araştırma sorularına yanıt aranmıştır:

- Soğuk Savaş sonrası dönemde siber uzayın uluslararası sistem ve güç mücadeleleri açısından taşıdığı önem nedir?

- Siber uzayın stratejik bir belirsizlik alanı olmasında etkili olan başlıca faktörler nelerdir?

- Siber normların inşasında etkili olan faktörler nelerdir?

- Devletlerin siber normların inşası sürecinde öne çıkan mülahazaları nelerdir?

- Siber normların oluşumu, güç mücadelelerinde nasıl bir rol oynamaktadır?

- Türkiye'nin siber norm oluşturma çabalarında öne çıkan unsurlar nelerdir?

- Türkiye siber norm oluşturma çalışmalarında hâlihazırda hangi aşamadadır?

Çalışmanın Yöntemi ve Teknikleri

Bu çalışmada; siber uzaydaki norm oluşturma sürecinde devletlerin faaliyetlerini, uluslararası şirketler ve özel şirketlerin bu süreçteki yerini incelerken kullanılacak olan yaklaşımlar Sosyal İnşacılık ve Yönetişimdir. Sosyal İnşacılığa göre, uluslararası sistemin işlevsel hale gelmesini sağlayan nokta; sistemin değerler, kurallar ve kurumlar aracılığıyla devletler tarafından kabul görmesidir. Aktör ve yapının karşılıklı bir şekilde birbirini inşa ettiğini savunan inşacılar, aktörlerin davranışlarını kimlik ve kültür gibi kavramlar çerçevesinde açıklamaya çalışmaktadırlar. Ülkelerin çıkarları, bu iki kavramın etkisiyle şekillenmektedir. Soğuk Savaş sonrası siber uzaydaki bilinmezlik etkisi göz önüne alındığında, devletlerin kimliklerini de bu ölçüde şekillendirmelerinin gerekli olduğunu öne sürmek mümkündür. Bu noktada devreye giren kısım ise, bu kimlikleri stratejik olarak inşa etmek için devletlerin norm oluşturma sürecine girmeleridir. Norm oluşturma stratejik bir inşa sürecidir ve aktör ve yapının, diğer bir deyişle devletler ve sistemin karşılıklı olarak birbirleriyle etkileşime girmesi sonucu oluşmaktadır. İnşa edilen kimliklere bağlı olarak çıkarların da şekillendiğini söylemek mümkündür. Bu bağlamda, norm oluşturma sürecinin, devletlerin çıkarlarına yönelik bir gelişme olduğu ileri sürülebilir. Bu çalışmada norm oluşturma süreci, uluslararası sistemdeki güç mücadeleleri doğrultusunda ele alınmakta ve devletlerin siber alanda norm oluşturma çabalarının sistemi şekillendirme, dolayısıyla yeniden inşasını sağlama çabası olduğunu iddia etmek mümkündür. Bu nedenle, bu çalışmada kullanılacak olan uluslararası ilişkileri teorisi Sosyal İnşacılık olarak belirlenmiştir.

Kullanılacak olan diğer bir perspektif olan yönetişimle ise, siber uzayda sağlanabilecek bir siber yönetişimin olup olmayacağı sorgulanmakta; İnternet yönetişim tasarı ve modelleri incelenerek pratikteki uygulanabilirliği belirlenmekte ve bununla birlikte devletlerin faaliyetleri belirlenen bu modeller üzerinden analiz edilmektedir. Bir yönetişim ağı tasarlamak için gerekli olan unsurlar olarak anarşik, hiyerarşik, demokratik ve karşılıklı mutabakata dayalı tasarıların belirlendiği çalışmada, oluşturulan yönetişim planı sonucunda uygulanabilirlik açısından siber egemenlik ve çok paydaşlı yönetişim modellerinin kullanılmasına karar verilmiştir.

Literatür İncelemesi

Soğuk Savaş sonrası yeni düzende, siber uzayın amorf yapısı (Küçüksolak, 2018) sonucu bilinmezlikler çağına girildiğini söylemek mümkündür. Küreselleşmenin geldiği evreyle birlikte, siber saldırıların uluslararası siyasete olan etkisi göstermiştir ki, siber uzay diğer operasyonel alanlar üzerindeki etkisi sayesinde uluslararası sistemde başat bir alan olma özelliğine sahiptir. Diğer yandan, uluslararası ilişkilere getirdiği boyutla birlikte hava, kara, deniz ve uzay gibi diğer dört alandan ayrılmaktadır (Akyeşilmen, 2018: 179). Hava, kara, deniz ve uzaydan sonra beşinci işlevsel alan olan siber uzayın mekânsal karakterini kontrol edebilmek için daha sistematik bir yaklaşıma ihtiyaç vardır (Lambach, 2020).

Siber uzay bilinmezliklerle dolu olsa da sınırsız değildir. Hukuk ve normlar tarafından sınırlanmakta ve kendisini oluşturan kodlar tarafından şekillendirilmektedir. Siber uzayda, gerçek dünyadan farklı olarak kişiye kimliğini saklama imkânı veren "anonimlik" söz konusudur. Gerçek dünyada bu özellik, açığa çıkabilecek bir altyapıya sahip olsa da, siber uzayın mimari yapısı anonimliği destekler niteliktedir. Öte yandan siber uzay, mimarisi gereği düzenlenemez niteliktedir. Ancak anonimliğe izin vermeyen normların gelmesiyle bu mimaride düzenleme yapılabilir. Dolayısıyla devletler, siber normların mimariyi düzenlemesine izin verecek bir düzenleme ile siber uzayda daha sistematik bir yaklaşım benimseyebilirler. Egemen devletlerin odaklanması gereken ve uluslararası bir İnternet yönetişimine gitmelerini teşvik edecek kilit nokta ise, siber uzayın mimarisinde bulunan kodun kendisinin "egemen" olduğudur. Diğer bir deyişle devletlere kurallarını dayatan, siber uzayın kendisidir (Lessig, 1998). Bu bağlamda, beşinci operasyonel alan olarak öne sürülen siber uzayda (Küçüksolak, 2018), devletler bu egemen yapıdan sıyrılarak kendi egemenliklerini dayatmak için rekabete girmektedirler (Lessig, 1998). Bu nedenle norm oluşturma süreci devletlerarası bir rekabet oluşturmaktadır. Uluslararası sistemin anarşik olduğunu, ancak bu anarşik sistemde bir inşa sürecinin gerçekleşebileceğini savunan Sosyal İnşacılık ise, burada devreye girmektedir. Çünkü normlar, bir grup içerisindeki aktörlerin etkileşimleri sonucu oluşarak gelişen sosyal çıktılardır (Finnemore ve Hollis, 2016). Katzenstein'in tanımıyla "*belirli bir kimliğe sahip aktörlerin uygun davranış sergilemeleri üzerine kolektif bir beklenti*" olan normlar (Katzenstein, 1996: 8), siber uzaydaki oluşum sürecinde beraberinde getirdikleri rekabetle birlikte güç mücadelelerine sebep olmaktadırlar.

Finnemore ve Hollis'e göre, bir davranışın norm olabilmesi için, belirli bir grubun üyeleri tarafından uygun bir davranış olarak paylaşılması gerekmektedir. Sosyal bilimcilerin, normları "sosyal yapılar" olarak adlandırdığı göz önüne alındığında; normlar, grup üyeleri veya diğer bir deyişle uluslararası sistemdeki aktörler tarafından kabul edilmeli ve bu kabul durumu sonucu bir beklenti oluşmalıdır. Bunun sonucu norm inşasının gerçekleştiğini söylemek mümkündür. Bir davranış, yalnızca diğer aktörler onu kabul ettiği sürece bir anlam ifade etmekte ve norm değeri kazanmaktadır (Finnemore ve Hollis, 2016). Siber normlar ise, bilinmezlikle dolu siber uzayda tahmin edilebilirliği, güveni ve istikrarı artırmayı, yanlış anlaşılmalara bağlı çatışmalardan kaçınmayı hedefleyen, uluslararası sitemdeki devletler ve devlet-dışı aktörler tarafından kabul edilen ortak davranış beklentileridir (Horenbeeck, 2018). Siber normları inşa edebilmek için devletler, temel içerikler ve ortak davranışsal beklentiler konusunda net olmalı ve işbirliğine gitmelidirler (Finnemore ve Hollis, 2016). Buradan hareketle; norm oluşturmanın bir sosyal inşa ürünü olduğu öne sürülerek; bu belirsizlik döneminde, uluslararası sistemi şekillendirmek isteyen devletlerin, norm oluşturma çabalarına ışık tutabilmek için kullanılacak olan teori Sosyal İnşacılık olarak belirlenmiştir.

Uluslararası toplumdaki siber norm arzusu yeni değildir. BM Birinci Komitesi'nde 1998 yılında Rusya tarafından sunulan ve sonraki yıl kabul edilen "Güvenlik bağlamında bilgi ve telekomünikasyon alanındaki gelişmeler" başlıklı taslak bu anlamda önem arz etmektedir (*Resolution Adopted by the General Assembly on the Report of the First Committee,* 1998). Bu bağlamda, BM'de 1998'den beri BİT konusunun gündemde

olduğunu söylemek mümkündür. GGE, o yıldan beri BİT'lerin kullanımı üzerine tavsiyelerde bulunmaktadır. 2015'te ise, Genel Kurul tarafından tüm üye devletlere BİT kullanımı konusunda rehberlikte bulunma çağrısında bulunulmuştur (BM Genel Kurulu, 2015). Uluslararası toplumdaki etkisi sebebiyle, GGE'nin BİT kullanımı konusundaki raporları devletlere rehberlik etmesi açısından önemlidir. BM'nin yanı sıra, NATO Kooperatif Siber Savunma Mükemmeliyet Merkezi de, siber alandaki aktivitelerin, uluslararası hukuk kuralları, anlaşmalar ve normlar ile nasıl düzenleneceğini değerlendirerek siber norm oluşturma sürecine katkıda bulunmaktadır (Horenbeeck, 2018).

Soğuk Savaş sonrası konuların ve aktörlerin çeşitlenmesiyle birlikte, özel şirketlerin artan önemi göz önüne alındığında; norm oluşturma sürecinde özel şirketlerin etkisini yadsımamak gerekir. Altyapısının büyük bir bölümü özel sektöre aidiyet gösteren çok uluslu bir ağ olan İnternet (Nye, 2018), özel şirketleri de norm oluşturma sürecine itmektedir. Buradan yola çıkarak, özel şirketler de siber uzayın bilinmezliğiyle mücadele etmek için, endüstrideki diğer şirketlerle normatif ittifaklar kurma yoluna gitmek zorundadırlar. Özel şirketlerin de dahil olduğu siber norm oluşturma süreci, devletleri, diğer şirketleri ve vatandaşları etkilemektedir. Dolayısıyla, "norm girişimcileri" olan özel şirketler de devletlerin norm oluşturma sürecine katkıda bulunmaktadırlar (Fairbank, 2019). Bu çalışmada özel şirketler başlığı altında ele alınacak olan Microsoft, Google ve Siemens ise; yaklaşımları, kapsamları ve nüfuz edebilirlikleri açısından kritik örneklerdir. Dijital Cenevre Sözleşmesi'ni (*Digital Geneva Convention*) benimseyerek siber saldırıları sınırlandırmaya çalışan Microsoft (Fairbank, 2019); belirli standartlar içeren Bulut Çağı İçin Yeni Yasal Çerçeve'yi (*New Legal Framework for the Cloud Era*) öneren Google (Eggenschwiler, 2018); 16 şirketle bir araya gelerek Güvenli Bir Dijital Dünya İçin Güven Bildirgesi (*Charter of Trust for a Secure Digital World*) imzalayan Siemens (Siemens AG, 2020b); ve son olarak kurumsal olarak siber güvenliğe vurgu yaparak Kritik Endüstriyel Tesisler İçin Bilgi Güvenliği Sözleşmesi'ni öne süren Nornickel, uluslararası sistemde norm girişimcileri olarak yerlerini korumaktadırlar.

Siber uzayda devam eden norm tartışmalarının yanı sıra, küresel bir İnternet yönetişimi oluşturma yönünde de tartışmalar söz konusu olmaktadır. "Sis esnasında yolunu bulmak" şeklinde ifade edilebilecek siber uzayda, yönetişim oluşturmak için bir yandan ulaşılabilirlik ile birlikte uygun ortam oluşurken; diğer yandan ise, sınırların ortadan kalkmasıyla ortaya çıkan yeni zorluklar söz konusudur. Çünkü bu noktada egemenlik kavramı devreye girmektedir. İnternet yönetişimi bu doğrultuda, siber uzayda egemenliğin nasıl kurulacağı ve nasıl şekilleneceği soruları temelinde ilerleyecektir (Shen, 2016).

BÖLÜM 1: SİBER UZAYIN BEŞİNCİ OPERASYONEL ALAN OLARAK GELİŞİMİ VE GÜVENLİK ORTAMINA YANSIMASI

1.1. Realizmin Güvenlik Anlayışı

Uluslararası siyasette temel aktörleri devletler olarak gören ve devletlerin ulusal çıkarlarını merkeze alan güç temelli bir uluslararası ilişkiler yaklaşımı olan Realizm; devletleri kara kutular olarak görmesi, güç maksimizasyonu sonucu ortaya çıkan güvenlik ikilemiyle kuşku ve endişe ortamını arttırması, yüksek politika – alçak politika şeklinde bir ayrıma gitmektedir. Gerek sayılan unsurların kısıtlılıkları gerekse günümüz güvenlik ortamının kapsamı sebebiyle günümüzde beşinci operasyonel alan olarak ele alınan siber uzayı açıklamada yetersiz kalmaktadır.

Sanayileşme, milliyetçilik ve emperyalizmin uluslararası sistemdeki etkisi sonucu 1914 yılında cereyan eden (Knutsen, 2015: 275) I. Dünya Savaşı'nın ardından entelektüeller, düşünürler ve siyasetçiler tarafından; savaşın neden çıktığı, gelecekte oluşabilecek savaşların nasıl önlenebileceği ve daimi barışın nasıl sağlanabileceği üzerine birtakım akademik görüşler ortaya çıkmıştır (Gözen, 2015: 67). Uluslararası İlişkiler disiplini içerisinde "İdealizm" teorisi olarak isimlendirilen bu görüşlerin başarısız olduğunu eklemek gerekmektedir. Örneğin, İdealizm ışığında barış içinde yeni bir düzen oluşturmak için ortaya atılan Wilson'un 14 İlkesi, Wilson'un kendi ülkesinden dahi destek görememiştir (Gözen, 2015: 74). Buna ek olarak, uluslararası hukuk kuralları açısından da önünde bir adım olarak kurulan Milletler Cemiyeti ise, İngiltere ve Fransa'nın ulusal çıkarlarının dayatıldığı bir kuruma dönüşmüştür. Wilson İlkelerinin etkisizliği ve Milletler Cemiyeti çatısının Hitler ve Mussolini'nin adımlarını durdurmada yetersiz kalması sonucunda da II. Dünya Savaşı patlak vermiştir. İdealizmin daimi barışı ve düzeni sağlama anlayışının aksine dönemin büyük devletlerinin, Makyavelli'nin Realist yaklaşımına benzer bir şekilde politika izledikleri görülmektedir (Gözen, 2015: 81).

Realist teori, iki savaş arası dönemin hâkim görüşü olan İdealizmin II. Dünya Savaşı'nı öngörememesine tepki olarak modern Uluslararası İlişkiler disiplini çerçevesinde ortaya konmuş ve sonraki dönemlerde de dominant bir konuma gelmiştir. Geleneksel güvenlik anlayışı olarak kabul edilen Realizm, tarihsel açıdan değerlendirildiğinde ise, Thucydides, Makyavelli ve Hobbes'a kadar uzanan uzun bir geleneğe sahiptir. Thucydides'in Atina ve Sparta arasında M.Ö. 431 yılında meydana gelen güç savaşlarını anlattığı "Peloponezya Savaşları" adlı eseri, uluslararası ilişkiler tarihinde güç unsuruna vurgu yapan önemli bir örnek olarak görülmektedir. Thucydides söz konusu eserinde insan doğasının kötücül olması üzerinde durarak iktidar unsuruna yaptığı vurgu ile ahlakı geri plana atması çerçevesinde klasik Realizm geleneğindeki ilk yazar olarak kabul edilmektedir (Korab-Karpowicz, 2006: 233). Thucydides'e göre Peloponez Savaşlarının ortaya çıkmasının temel sebebi, Atina'nın gücünün artmasına bağlı olarak Sparta'nın kendi güvenliğine yönelik hissettiği korkudur (Thukydides, 2010: 21). Zira Sparta, Helen dünyasındaki egemen konumunu kaybetme endişesine kapılarak gücünü artırma ve kurduğu ittifaklar çerçevesinde önlemler alma yoluna gitmiştir. Atina'nın da aynı şekilde karşılık vermesi neticesinde, iki tarafın karşılıklı olarak güçlenmesinin ve ittifaklar kurmasının ortaya çıkardığı korku ve kuşku çatışmayı kaçınılmaz kılmıştır. Devletler sisteminde risk ve

tehditlerin sürekli olduğu, kuşku ve güvenlik endişesinin hakim olduğu bu durumdan kaçınmanın mümkün olmaması da Realizmin güvenlik ikilemi tanımlanmasında ortaya konmaktadır.

Klasik Realizmin temeli, Hobbes'un (1588-1679) öne sürdüğü şekilde, insan doğasının kötücül olması üzerine odaklanmaktadır. Hobbes'un bu karamsar yaklaşımının, kendi doğumundan kaynaklandığı düşünülmektedir. Zira 1588 yılında İspanyol donanmasının yaklaştığını duyan annesinin korkuyla erken doğum yaptığı (Martinich, 1999: 2), Hobbes'un doğumundan aktarılan bu korku travmasının "Korku benim ikiz kardeşimdir" şeklindeki ifadesinden de anlaşılacağı üzere hayatının geri kalanında etkili olduğu ve eserlerine yansıdığı gözlenmektedir. Thomas Hobbes'un bir ifadesi olan "homo homini lupus" (insan insanın kurdudur) da yine insan doğasının kötücüllüğüne yönelik yaklaşımını ortaya koymaktadır. Hobbes'un görüşleri çerçevesinde klasik Realizmin özüne inildiğinde, "güvende olmama" ve "güvensizlik" kavramlarının başat olduğu görülmektedir. Klasik Realizmde insan doğasının kötücül olmasından, diğer bir deyişle bireyden başlanarak, tümevarım yöntemiyle devletlerarası ilişkilerin güvensizlik, güç ve çıkar faktörlerine dayandığı yargısına varılmaktadır. Bireylerin Toplum Sözleşmesiyle kurdukları Leviathan yani devlet yapısı ile anarşi ortamından kurtulabildikleri devlet düzeyinden, devletler üstü bir Leviathan'ın oluşturulmasının mümkün olmadığı uluslararası sistemin anarşik yapısına doğru giden bir analiz yöntemi söz konusu olmaktadır.

Klasik Realizmin odaklandığı bir diğer unsur olan güç konusunda da güç maksimizasyonu öne çıkmaktadır. Devletin tek bir akıl ve irade ile hareket etmesi anlamına gelen bilardo topları benzetmesi, güç maksimizasyonunun bir ifadesi olarak klasik Realizm anlayışı içerisinde yer almaktadır (Jackson ve Moore, 2016: 454). Anarşik sistem içerisinde güvensiz hisseden devletler, güvenliklerini temi edebilmek amacıyla güçlerini maksimize etme yoluna gitme ihtiyacı hissetmektedirler. Ancak uluslararası sistemin anarşik yapısının, diğer devletlerin güç maksimizasyonunu da içerdiği göz önüne alındığında, devletler gücün maksimize edilmesini bir tehdit olarak algılamakta ve sonucunda güvenlik ikilemi unsuru ortaya çıkmaktadır. Güvenlik ikilemi ise, Atina ve Sparta arasındaki gücü arttırmanın güvenliğe yönelik korku ve endişe oluşturması şeklindeki tehdit algısı gibi, klasik Realizmde bir güç çıkmazını ifade etmektedir. Siber uzaydaki bilinmezlik ortamının devletleri korku ve endişeye sevk etmesi klasik Realist anlayışın insan insanın kurdudur düsturunu hatırlatmakta ve bu bilinmezlik ortamında devletlerin çok daha fazla güvensiz hissetmesine sebep olmaktadır.

Realizme göre; ulusal çıkarlarını gücüne göre belirleyen devletler, devletlerarası çıkar çatışmaları sebebiyle sürekli gücünü arttırmak zorunda kalmaktadır. Bu durum ise "güvenlik ikilemi"ne sebep olmaktadır. Üst bir otoritenin bulunmadığı anarşik uluslararası sistem çerçevesinde güvenlik ikilemini aşmak için, devletler kendi güç kapasitelerine güvenmek zorundadırlar. Güvensizliğin ve güç maksimizasyonunun hâkim olduğu uluslararası yapı devletleri literatürde *self-help* şeklinde ifade edilen "kendi kendine yetme" durumuna yönlendirmektedir. Güvensizliğin, korkunun, çıkar çatışmalarının yer aldığı uluslararası sistemde her devlet kendisine güvenmek zorundadır.

"Kendi kendine yetme" denildiğinde akla gelen önemli bir isim olan Makyavelli'nin (1469-1527) yaşadığı dönem olan 16. yüzyıl, realist yaklaşımın ilk önermelerinin çıktığı dönem olmuştur. Makyavelli, temel eseri olan Prens'te, güçlerine maksimize edebilmeleri için devlet adamlarına tavsiyelerde bulunmaktadır. Ona göre temel mesele, prensin bekasıyla bir tutulan devletin bekasının devamlılığıdır. Eserinde, tüm devletlerin birbiri için tehdit olduğunu ileri sürerek son derece olumsuz bir yaklaşıma sahiptir. Makyavelli'ye göre yöneticinin temel sorumluluğu her zaman kendi ulusal çıkarını korumak ve bekayı sağlamaktır. Zira devletin çıkarı, prensin çıkarıyla eşdeğerdir zira güçlü lider güçlü devlet anlamına gelmektedir. Eğer devlet güçten düşerse diğer devletlerin avı olacaktır. Diğer yandan, ordu iktidara ne kadar bağlıysa devletin güvenliği de o kadar sağlam olacaktır. Bu nedenle, prens gerektiğinde devletin ulusal çıkarlarını korumak için acımasız davranabilme lüksüne sahiptir. Makyavelli, ulusal çıkarlar karşısında ahlak ve etik gibi kavramları da göz ardı ederek, devlet adamlarının tedbirli davranmak ve zafiyetlerine dikkat etmekten başka alternatifleri olmadığını öne sürmektedir. Ancak Makyavelli'nin ortak ahlaki bir düzenin yokluğu sebebiyle bir uluslararası toplumun oluşturulamayacağı iddiası, uluslararası siyaseti bir asker oyunu olarak görmesi ve buna bağlı olarak dar bir şekilde kısıtlaması anlamına gelmektedir (Jackson ve Moore, 2016: 454).

Klasik Realizmin, güvenlik bağlamında uluslararası ilişkilere önemli katkıları söz konusu olmakla beraber öne sürdüğü çeşitli unsurların ve katı sınırların siber alan gibi günümüz koşullarının önemli unsurlarını açıklamakta yetersiz kaldığı görülmektedir. Klasik Realistlere göre devletlerin temel amacı hayatta kalmak ve ulusal çıkarlarının korunması olduğu için, güvenlik konuları da devletin güvenliğini sağlamak üzerine ilerlemektedir. Yüksek politika ve alçak politika şeklinde bir ayrıma giden klasik Realistler, güvenlik konuları yüksek politika konuları içerisinde değerlendirirken; ekonomi, enerji, çevre gibi konular ise, alçak politika kapsamına alınarak ikincil öneme sahip şekilde sınıflandırılmaktadır. Buna ek olarak realistler, analiz yaparken iç ve dış politika ayrımı yaparak, devlet içi politikaları uluslararası siyasetten ayrı tutmaktadır (Stone, 1994: 469). Siber uzaydaki aktör ve konu çeşitliliğine bakıldığında, realizmin güvenlik yaklaşımının bu konuda yetersiz kaldığını öne sürmek gerekmektedir. Konu bağlamında alçak ve yüksek politika ayrımına gidilerek uluslararası siyaseti kısıtlaması, siber uzayı incelemede realizmi geri plana atmaktadır. Diğer yandan sadece askeri araçlara odaklanılması günümüzün yumuşak güç ve akıllı güç unsurlarının göz ardı edilmesine yol açmaktadır.

Klasik Realizmin yetersizliklerine bir eleştiri olarak 1970'lerde ortaya çıkan Neorealizm de gerek uluslararası ilişkiler disiplinini konularının ve aktörlerinin açıklanması gerekse uluslararası sisteme yaklaşım anlamında farklı bir perspektif ortaya koymaktadır. İç ve dış politika arasında bir ayrım ortaya koyan ve Soğuk Savaş çerçevesinde ortaya koydukları büyük stratejilerle analiz yapan klasik Realistlerin gerek petrol krizinin etkilerini gerekse Vietnam Savaşı'nı ve etkilerini açıklamakta etkisiz kaldıkları görülmüştür. Klasik Realizme yönelik oluşan hayal kırıklığı üzerine Kenneth Waltz'un 1979 yılında yayınladığı "Uluslararası Politika Teorisi" adlı kitabıyla birlikte Neorealizm kavramının literatüre girdiği görülmektedir. Devlet davranışlarını belirleyen unsurun uluslararası sistem olduğunu iddia eden Waltz, uluslararası sistemin yapısına vurgu yaparak, teorinin yapısal realizm şeklinde de anılmasını sağlamıştır (Darıcılı, 2017: 19).

Klasik Realizmde, insan doğasının kötücül yapısından uluslararası sisteme doğru ilerleyen bir tümevarım yöntemi kullanılmakta; insan doğasında yer alan kötülük, devletleri doğa durumunda olmaya itmekte ve uluslararası sistemde çıkar çatışmalarıyla birlikte şekillenen anarşik bir yapı meydana getirmektedir. Neorealizme göre ise; büyük güç, orta güç ve küçük güç şeklinde ifade edilen uluslararası sistemdeki güç dağılımı, devletlerin çıkarlarını, dış politikalarını ve bu politikalara yönelik eylemlerini etkilemektedir. Zira uluslararası sistemdeki anarşik yapı devlet davranışlarını düzenleyici bir etkiye sahiptir. Buradan yola çıkarak, Neorealizmde, sistemden devlete doğru ilerleyen tümdengelimci bir yaklaşım kullanıldığını belirtmek gerekmektedir.

Sistemin yapısı üzerinden uluslararası ilişkileri yorumlayan Neorealist yaklaşım çerçevesinde devletler benzer fonksiyonlara sahip olmakla beraber kapasiteleri bakımından farklılık göstermektedirler. Güç dağılımı üzerinden sistemi yorumlayan Neorealistler devletlerin güvenliklerini sağlayabilmek için ne kadar güce sahip olmaları gerektiği sorusu üzerinden saldırgan ve savunmacı realistler olarak ikiye ayrılmaktadırlar. Saldırgan realizmin savunucusu olan John Mearsheimer'e göre, bir devlet için uluslararası sistemdeki en ideal durum sistemdeki hegemon güç olmaktır. Çünkü devletlerin güvenliklerini sağlamalarının en iyi yolu, sistemdeki en güçlü devlet olmaktan geçmektedir. Devletler o seviyeye ulaşana kadar güçlerini sürekli artırmalıdırlar. Diğer yandan savunmacı realistlere göre gücün maksimize edilmesi çabası yaratacağı endişe ortamı üzerinden karşı tarafın ittifaklar kurarak Hitler ve Napolyon örneklerinde görüldüğü gibi devlet güvenliğini tehlikeye düşürecek bir sonuç yaratabilecektir. Bu doğrultuda savunmacı realistlere göre politikaların hedefi gereken güç dengesini koruyacak şekilde yeterli düzeyde gücün elde edilmesine yönelik olmalıdır.

Sovyetler Birliği'nin dağılışını ve Soğuk Savaşın bitişini öngöremeyen realist görüşün, yeni düzeni açıklamakta da yetersiz kaldığı yaygın bir şekilde öne sürülmektedir. Zira Soğuk Savaş sonrası konuların ve aktörlerin çeşitlenmesi; iç-dış politika ayrımının zayıflamasını, genişleyen güvenlik spektrumu çerçevesinde alçak-yüksek politika gibi sınıflandırmaların ortadan kalkmasını beraberinde getirmiştir. Soğuk Savaşın katı kısıtlamaları çerçevesinde devlet yegâne aktör olarak öne çıkarken, Soğuk Savaş sonrası dönemde küreselleşmenin de hız kazanan etkileriyle birlikte bireylerin, STK'ların, uluslararası örgütlerin, çok uluslu şirketlerin, ulus aşan suç örgütlerinin ve terör örgütlerinin de güvenlik ajandasında ön plana çıktığı görülmüştür.

Devlet merkezli bir yaklaşım olan Realizmde temel aktör devlet olduğu için konular da devleti ilgilendiren askeri güvenlik, nükleer silahlanma, devletlerarası çatışma, ideolojik rekabet ve enerji kaynakları gibi konulardan oluşmaktadır (Efegil, 2012: 18). 1970'lerden başlayan ancak Soğuk Savaş sonrası dönemin koşullarında gündemde ön sıralarda yer almaya başlayan aktörlerin artan çeşitliliğine bağlı olarak konular da genişlemiş, ekonomi, enerji güvenliği, insan hakları, çevre gibi konular politikalarda belirleyici konuma gelmişlerdir. Tüm bu faktörler ışığında kara kutular olarak ele aldığı devlet ve askeri güç odaklı, klasik Realizm anlayışı bu tezin konusu olan siber uzayın dinamiklerinin açıklanmasında yetersiz kalmaktadır. Ancak gerek konuların ne derece genişlediği, aktörlerin ne derece çeşitlendiği ve gündelik yaşamdan devlet politikalarına varıncaya dek

yaratmış oldukları etkinin nereden nereye geldiğinin anlaşılması açısından klasik Realizmin ve unsurlarının anlaşılması önemlidir.

Realizm anlayışı siber uzayı açıklamada yetersiz olsa da güvenlik ikileminin farklı unsurlarla sürmesi ve siber uzayda kuşku ve endişe araçlarının ve kanallarının artması, aslında Hobbes'un betimlediği şekilde bir ortamın siber uzayda cereyan ettiğini ortaya koymaktadır. 2007 yılında Estonya'ya yapılan siber saldırılarda olduğu gibi, vatandaşların devlete erişimlerinin üç hafta kesintiye uğraması durumunda, günlük hayatın neredeyse her unsurunu etkileyebilen bu kaotik ortamın siber alan üzerinden siber enstrümanlarla yaşanabileceğini göstermektedir.

Bütün bu dinamikler değerlendirildiğinde, özellikle de Soğuk Savaş döneminde etkili olan, realist siyasetin Soğuk Savaş sonrası güvenlik çevresinde yaşanan dönüşüme bağlı olarak aşağıdaki unsurlar çerçevesinde yetersiz kaldığını söylemek mümkündür:

- İç ve dış siyaset ayrımının kalkması
- Yüksek politika ve alçak politika ayrımının ortadan kalkması
- Aktörlerin çeşitlenmesi
- Aktör çeşitliliğine bağlı olarak konuların genişlemesi ve derinleşmesi

1.2. Kopenhag Ekolü Kapsamında Güvenlik Çevresinde Yaşanan Dönüşümün Değerlendirilmesi

Soğuk Savaş sonrası, küreselleşmenin geldiği noktayla birlikte, özellikle dinamik teknolojik değişikliklere bağlı olarak uluslararası sistemdeki dönüşümler hızlanmıştır. Yukarıda anlatıldığı üzere Kopenhag Ekolü, güvenliği kapsamlı bir şekilde ele almasıyla Realizmin yetersizliklerine alternatif olarak ortaya çıkmaktadır. Bu nedenle, bu tezde Kopenhag Ekolü'nden yararlanılmıştır.

1945 yılında ABD'nin, 1949'da ise, Sovyetlerin atom bombasını bulması akabinde tetiklenen Soğuk Savaş ortamı, "Altın Çağ" (*Golden Age*) olarak adlandırılan 1955-1965 yılları arasında sürecek ve baskın bir biçimde nükleer konulara odaklanan bir dönemi beraberinde getirmiştir. Ancak diğer yandan aynı dönem başlayan bir sıcak çatışma olan ve etik konularla eşleşmeyen Vietnam Savaşı (1955-1975) ise, sert güç bağlamında güvenlik kavramının sorgulanmasına yol açmıştır. Devamında 1970'lerde uluslararası siyaset gündemine giren "*détente*" süreci ile birlikte, ekonomik ve sosyal konular gibi askeri olmayan başlıkların konuşulduğu, barış üzerine yapılan çalışmaların arttığı ve ardından askeri gibi görünmeyen konuların bile güvenlikle olan bağlantısının sorgulandığı bir periyod yaşanmıştır.

II. Dünya Savaşı'ndan sonra Soğuk Savaş'ın kurgulandığı bir dönüşüm sürecine gidilmiştir. 31 Aralık 1991 tarihinde Sovyetler Birliği'nin dağılması sonucu Soğuk Savaş düzeni sona ermiştir. Uluslararası sistemin kısa bir tarihsel süreçte önemli bir dönüşüm geçirmesi, belli başlı tartışmaları da beraberinde getirmiştir. Soğuk Savaş düzeni sona ermiş ve günümüzde hala tam olarak netleştirilemeyen bir şekilde belirli bir düzene evirilmiştir. Liberal ekonominin üzerinde yükselen ancak belirsizliklerle dolu olan bir düzen oluşmuştur. Bu belirsizlikler akabinde ise, aktörler Fukuyama'nın öne sürdüğü "Tarihin Sonu mu?" tezini sorgulamaya doğru bir yön izlemiştir. Sovyetlerin dağılması,

liberalizmin hâkimiyetini gözler önüne sermiş; komünizmin düşüşüyle birlikte, ABD'nin hâkimiyetinde ilerleyen tek kutuplu bir sistem olduğu iddiası ortaya çıkmıştır. Zira Sovyetler Birliği düşüşe geçerken, ABD ise, yeni sistemde üstünlük kurmaya devam etmiştir.

Birinin kazancının diğerinin yıkımı olacağı bir sıfır toplamlı oyun olan Soğuk Savaş siyaseti, çift kutuplu sistemin taraflarından biri olan Sovyetler Birliği'nin çözülmesiyle birlikte sistemde bir belirsizliği de beraberinde getirmiştir. Zira Soğuk Savaş döneminde iki kutup arasında nükleer silahlanma ve gerginliğin hâkim olduğu bir düzen söz konusu olmuş ve bu duruma bağlı olarak taraflar özelinde savunma ve strateji endeksli önlemler yerini korumuştur (Bayır, 2013: 173). Küba Füze Krizi vakasında görüldüğü şekilde gerginlik, Soğuk Savaş boyunca taraflar arasında güvenliğin tehdit altında olduğu bir anlayış meydana getirerek güvenliği dar bir kutuda muhafaza etmiştir. Ancak Schrödinger'in kedisinde olduğu gibi güvenlik hem bu kadar dar, hem de hiç olmadığı kadar geniş bir kavramdır. Soğuk Savaş sürecinin bitişiyle artan küreselleşme, STK'ların etkilerinin artması, uluslararası siyasette aktörlerin çeşitlilik göstermesi ve buna bağlı olarak konuların da çeşitlenmesi, bireylerin güvenliğinin de gündeme alınmaya başlanması, iç ve dış politika arasındaki sınırların kalkması, Soğuk Savaş döneminde nükleer çekişmenin ön planda olduğu geleneksel askeri düzenden farklı bir uluslararası sistem ortaya koymuştur. Tüm bunların ardından güvenliğin daraltıldığı kutunun açılması sonucu, güvenliğin daha geniş bir perspektiften oluştuğunu öne süren çalışmalar ortaya çıkmıştır.

Buna ek olarak, 11 Eylül 2001 saldırıları da bu bağlamda önem arz etmektedir. 11 Eylül öncesi, ABD'nin ağırlığı üzerinden şekillenen yeni sistemde, 11 Eylül saldırıları ABD gibi süper bir gücün bile terörizm tehdidinden muaf olmadığını göstermiştir. Ekonomik olarak Dünya Ticaret Örgütü'nün, askeri olarak ise, Pentagon'un hedef alındığı saldırılarda; bir yandan ABD'nin sistemdeki gücü sorgulanırken, diğer yandan terör gruplarının dünya siyasetinde aktörler olarak önemi ortaya çıkmıştır. Ardından, saldırılar sebebiyle gerçekleştirilen 2003 Irak Operasyonu ile de ABD'nin askeri ve ekonomik gücünde zayıflama meydana gelmiştir (Efegil ve Musaoğlu, 2009: 14). Bu zayıflama, ABD'nin sistemdeki tek egemen aktör olmadığını ortaya koymuş ve çok kutuplu bir sistemin sinyallerini vermiştir.

Sistem yapısına, diğer bir deyişle güç dağılımına bakıldığında; 1980'lerden itibaren başlayan konulardaki çeşitlenme süreci akabinde özellikle Soğuk Savaş'ın sonra ermesiyle, uluslararası sistemin doğası konusunda bir anlamlandırma sürecine girilmesi söz konusudur. Bu anlamlandırma sürecini ele alırken, devletlerarası ilişkilerin dinamiklerindeki değişikliklerden bahsetmek gerekmektedir. Sovyetler Birliği'nin dağılması sonucu uluslararası sistemdeki kutupluluk değişmiş, çift kutuplu sistemden çok kutuplu sisteme bir geçiş yapılmıştır. Çift kutuplu sistemin çökmesi sonucu, devletlerin uluslararası sistemdeki rolü değişim sürecine girmiştir. Zira devletlerin temel aktör olarak kabul edildiği Soğuk Savaş döneminin aksine, Soğuk Savaş sonrası süreçte devletlerin yanı sıra uluslararası örgütler, STK'lar, ulus aşırı şirketler, özel şirketler ve bireyler gibi çok sayıda aktörün anlam kazandığı yeni bir düzen oluşmuştur. Sistemde rol sahibi olan yeni

aktörlere bağlı olarak konularda da çeşitlilik ortaya çıkmıştır. Konularda ortaya çıkan çeşitlilik ise, yeni yaklaşımların ortaya çıkmasına olanak vermiştir.

Uluslararası İlişkilerdeki geleneksel teorilerin temelinde yer alan "güç" ve "güvenlik" kavramlarının, Soğuk Savaş sonrası değişen süreci analiz etmekte yetersiz kalması sonucu, bu anlayışlar eleştirilerek kavramsal olarak yeniden düşünülmeye başlanmıştır. Literatürdeki bu kavramsal tartışmalara bağlı olarak ortaya çıkan ekollerden biri ise, Kopenhag Ekolü olmuştur. Bu ekol, Kopenhag Barış Çalışmaları Merkezi üzerinden çalışmalar yapan bir grup akademisyenin kavramsal analizleri sonucu, "Kopenhag Okulu" veya "Kopenhag Ekolü" olarak adlandırılarak uluslararası ilişkilere kazandırılmıştır. Bu teorik yaklaşım, 1990 sonrası değişen güvenlik ortamını açıklayabilmek için birtakım kavramlar öne sürerek literatüre katkıda bulunmayı hedeflemiştir. Güvenlik bağlamının analiz çerçevesini genişleten; güvenlikleştirme teorisi, bölgesel güvenlik kompleksleri, güvenlik objeleri ve yeni güvenlik sektörleri gibi kavramlar bu katkılar arasındadır (Coşkun, 2014: 179).

Güvenliği, sektörler bazında çok boyutlu ve kapsamlı bir şekilde tanımlayan Kopenhag Ekolü; Realizmdeki gibi devleti temel aktör olarak ele almak yerine analiz birimi olarak devlet ve toplumu beraber almakta ve iki aktör arasında denge gözetmeye çalışmaktadır (Buzan, 1984: 121). Barry Buzan'ın öne sürdüğü "genişletilmiş bir güvenlik yaklaşımı" kavramının etkin olduğu Kopenhag Ekolü'nde, askeri konuların yanı sıra siyasal, ekonomik, çevresel ve toplumsal konuların da gündeme alındığını ifade etmek mümkündür.

Güvenlikleştirme kavramının temel meselesi, günlük bir konunun güvenlik gündemine yerleştirilmesi, inşa edilmesidir. "Hayatta kalmak", "silahın doğrultulması" gibi konular en başından itibaren güvenlik çerçevesinde ele alınırken, güvenlikleştirme teorisine göre ise, gündelik bir konu tehdit olarak söylem yoluyla inşa edilmekte ve böylelikle bir güvenlik konusu haline getirilmektedir. Güvenlikleştirmenin işlerliğini sağlayan unsur ise söylemdir. Söylem yoluyla, bir kavramın tehdit olarak inşa edilmesi mümkün kılınmaktadır. Bir olguyu tehdit olarak etiketleyerek güvenlikleştirmek için kullanılan araç ise, "bir şey söylemek" olarak ifade edilebilecek olan söz edimi (*speech act*) argümanıdır. Ekole göre, bir eylem ağızdan çıktığı an gerçeğe dönüştüğü için aslında güvenliğin kendisi "söz edimi"dir ve ekolün yapıtaşı söz edimi argümanı olmaktadır (Coşkun, 2014: 185). Diğer yandan söylenen tüm sözler güvenlikleştirmeye sebep olmaz. Böylesi bir durumdan kaçınmak için güvenlikleştirme üç aşamadan oluşturulmaktadır. İlk aşamada varoluşsal bir tehdit unsuru belirlenerek durum tespiti yapılmakta; ardından ikinci aşamaya geçilerek eyleme geçmenin aciliyeti kabul edilmektedir (Taureck, 2006: 55). Son aşamada ise, tehdidi ortadan kaldırabilmek için olağanüstü tedbirler almanın gerekliliği kabul edilmektedir (Coşkun, 2014: 184). Bütün bunlar yapılırken, devlet ve toplum düzeyinde analiz yapıldığını unutmamak gerekir. Zira siyasetçilerin bir konuyu güvenlik meselesi haline getirmek için toplumun onayını almaları gerekmektedir.

Önde gelen bir güvenlik meselesi haline gelen siber güvenliğin tarihi, 1991 yılında Bilgisayar Bilimi ve Telekomünikasyon Kurulu tarafından yayınlanan rapora kadar uzanmaktadır. "Risk Altındaki Bilgisayarlar: Bilgi Çağında Güvenli Programlama

(*Computers at Risk: Safe Computing in the Information Age*)" adlı raporda, güvenlik kavramı "*bir sistemdeki verilerin istenmeyen bir şekilde ortaya çıkarılmasına, değiştirilmesine veya yok edilmesine karşı koruma ve sistemlerin kendilerinin korunması*" olarak tanımlanmıştır (Hansen ve Nissenbaum, 2009: 1160). Bir sonraki bölümde bahsedilecek olan 1990'lardan 2000'e kadar geçen süreçte İnternet teknolojisinin geçirdiği dönüşüm göz önünde bulundurulduğunda, geleneksel uluslararası ilişkiler yaklaşımlarının siber uzayı ve siber uzayın etkilerini anlamada yeterliliği sorgulanmaktadır.

Kopenhag Ekolü, özellikle genişletilmiş güvenlik yaklaşımıyla konu çeşitliliğini karşılaması açısından siber uzayı analiz etme noktasında işlevsel bir teoridir. Kopenhag Ekolü'nün doğrudan bir ilişki içerisinde olduğu Barry Buzan; askeri, çevresel, ekonomik, politik ve toplumsal olmak üzere güvenliği beş geleneksel sektöre ayırmaktadır. Bu sektörler bağlamında devlet, tek referans nesnesi konumunda görünmektedir. Ancak bu noktada bir sorun göze çarpmaktadır. Eğer güvenlik daima referans nesnesi olan devlet içinse, buradan 'toplumsal güvenliğin devletin topluma karşı güvenliği olduğu', diğer bir deyişle toplumun kendisinin güvensiz olduğu ancak toplumsal güvenliğin yüksek olduğu anlamı çıkacaktır (Hama, 2017: 4). Bu nedenle Ole Wæver, devleti beş güvenlik sektöründen dördünde referans nesnesi olarak görmekte; toplumsal güvenlikte ise, referans nesnesi olarak toplumu merkeze almaktadır. Zira toplumun bekası, devletin hayattan kalmasından farklı olmaktadır. Toplumsal güvenlik üzerine örnek vermek gerekirse, devlete karşı ortaya çıkan her dış tehdidin toplum tarafından bir tehdit olarak görülmek yerine, hedef devlet içindeki bir azınlığı özgürleştirme girişimi olarak görülebilmektedir. Bu bağlamda, devletin ve toplumun bekasının farklılık gösterdiğini iddia etmek mümkündür. Dahası, devlet sınırları sabit olsa da bir toplumun sınırları sabit kalmadığı için, çoğu vakada toplumun güvenliği devletin güvensizliğini arttırmaktadır (Hama, 2017: 4-5). Örneğin, Ermenistan bir ülke olarak sabit sınırlara sahipken; bir etnik grup ve millet olan Ermeniler ise, sınır gözetmeksizin birçok ülkede varlıklarını sürdürebilmektedir. Kopenhag Ekolü özünde güvenlik çevresinde yaşanan dönüşüm sonucu, toplumsal güvenlik üzerinde yoğunlaşmasıyla diğer ekollerden ayrılmaktadır.

İnsan eliyle inşa edilmiş beşinci operasyonel alan olan siber uzaydaki belirsizliğin üzerine ise, referans nesnesi olarak devlet yerine bireyi merkeze alan ve güvenlik çalışmalarına büyük ölçüde katkı sağlayan insan güvenliği yaklaşımı eklenmiştir. Bu yaklaşıma göre, Soğuk Savaş süreci boyunca gerçekleşen iç çatışmalar, felaket, yoksulluk gibi birçok sebepten dolayı, insan aktörü müthiş bir tehdit ile yüzleşmiştir. Yaklaşımın temelinde devletin kendi halkının güvenliğini sağlayıcı bir rolde olduğu reddedilmekte; bunun yerine devletlerin, diğer devletlerin insan güvenliğini tehdit etmesi gibi ideal şartlarda bireyler için güvenliği sağlayıcı bir role sahip olması kabul edilmektedir. Bu bağlamda, yaklaşım çerçevesinde devlet merkezli yaklaşım sorgulanmakta ve mutlak egemenlikten şartlı egemenliğe giden bir yol izlenmektedir (Hama, 2017: 15)

Geleneksel güvenlik yaklaşımının, güvenliği, devletlerin diğer askeri saldırılarına karşı güvenliği olarak sınırladığını ve dolayısıyla devletleri güvenliğin tek referans nesnesi olarak görerek güvenlik kavramını genişletme yönünde bir adım atmayı reddettiğini belirtmek gerekmektedir. Kopenhag Ekolü tarafından bu yaklaşıma meydan okunmakta ve

güvenliğin devlet güvenliği ve toplumsal güvenlik olarak ikiye ayrıldığı öne sürülmektedir. Buna ek olarak, siber uzayın devletler ve özel oluşumlar arasındaki ilişkiyi dönüştürdüğü, bunun akabinde ise, özellikle teknolojik özel şirketlerin sahip olduğu özerk yapıdan yararlandığını belirtmek mümkündür. Ancak bilgi ve iletişim teknolojilerindeki yenilikler sonucu giderek artan siber tehditler, bu tehditler karşısında hükümetin ve özel sektörün rollerinin belirsizliği sonucu güvenlik açıklarına sebep olmaktadır. Uluslararası örgütler tarafından alınan önlemlerde çıkan egemenlik sorunu ise, güvenlik noktasında başka bir belirsizliği beraberinde getirmektedir. Bütün bu bahsedilenlerin ışığında, Soğuk Savaş sonrası oluşan belirsizliğe, siber uzayın getirdiği belirsizliğin de eklenmesiyle realist yaklaşımın siber uzayın getirdiği güncel güvenlik sorunlarına hitap etmede eksik kaldığı görülmektedir.

1.3. Siber Uzayın Gelişimi

Hayatın her alanında olduğu gibi teknolojinin uluslararası ilişkilerdeki etkisi gün geçtikçe artmaktadır. Küreselleşmenin geldiği evreyle birlikte İnternetin gelişimi siber uzayın oluşmasında en temel noktayı teşkil etmektedir. İnternetin ortaya çıkışı ve bilgi sistemlerinin kullanımının artması, insan yaşamında büyük değişikliklere neden olmuştur. Bu değişikler bağlamında, ticaretin önündeki birçok engel kalkmış; buna ek olarak, sınıf, coğrafi konum ve dönemin getirdiği geleneksel engeller ne olursa olsun dünyanın her yerinden insanlar iletişim kurma, işbirliği yapma ve fikir alışverişinde bulunma olanağına sahip olmuşlardır. Bu durum, beşinci operasyonel alan olarak ifade edilen siber uzayda küresel rekabeti artırmaktadır. Buna bağlı olarak uluslararası siyasette hükümetler, özel şirketler, uluslararası örgütler ve bireyler siber uzay teknolojilerini gittikçe daha fazla benimsemektedirler. Girilen bu rekabetin altyapısında, üretkenliğe sahip olmak ve kâr elde etme amaçları yer almaktadır. Örnek vermek gerekirse siber uzay araştırma, geliştirme ve inovasyon için birçok iyi seçenek sunmakta; böylelikle bir yandan ekonomik büyüme ve refaha giden bir yol ortaya çıkmakta, diğer yandan ise hızlı ilerleyen bir biçimde bilgi toplumları oluşmaktadır (Mbanaso ve Dandaura, 2015: 17).

Endüstri 4.0, uzay madenciliği, dijitalleşme, 3D yazıcılar, yapay zekâlar, karanlık fabrikalar ve daha nice yeniliklerin ortaya çıkışıyla, dünya yeni bir boyutta şekillenmektedir. Teknoloji giderek daha hızlı gelişmekte, beraberinde ise, bu yeni dünyaya karmaşıklığı ve belirsizliği getirmektedir. Siber uzaydaki popülasyon artmaya devam ettiği sürece, rekabet de artmaktadır. Dolayısıyla siber uzay, aktörler ve paydaşlar için çekici bir alan haline gelmektedir. Bu noktadan yola çıkarak, siber uzay ile birlikte pek çok fonksiyonun fiziksel dünyadan sanal dünyaya geçişi sağlayan bir portal açıldığını ve teknolojik ilerlemeler vasıtasıyla bu portalın giderek daha çok büyüdüğünü öne sürmek mümkündür.

Siber uzayın kilidini açabilmek için öncelikle bu alanın anahtar kelimesi olan İnternetin gelişimine inilecek ve ardından, bir sonraki adımda İnternetin tarihi konusundaki süreç ifade edilecektir İnternetin tanımlanmasına yönelik çalışmalar, genellikle kavramı bir donanım ve yazılım seti olarak teknik bir şekilde tanımlama eğiliminde olurken; Janet Abbate ise, tek bir doğru tanımın olmadığını kabul etmekte ancak yine de tarihçileri kullandıkları tanımların politikaları konusunda dikkatli olmaya ve kavramın çıkış

noktasının ABD merkezli olarak çerçevelendirilmesi konusunda detaylı bir incelemeye çağırmaktadır (Abbate, 2017: 1). Bir ağ olarak ifade edilen ve geçmişi II. Dünya Savaşı sonrası yıllara kadar uzanan İnternetin evrimini; askeri bir deneyden başlayarak sivil bir hizmet kuruluşu haline gelmesini içeren süreç ve ağın ticarileştirilmesine evirilen süreç şeklinde iki aşamada ele almak mümkündür (Naughton, 2016: 7)

1967-1995 yılları arasındaki süreci ifade eden birinci aşamaya geçmeden önce, arka planda bu sürecin oluşmasına iten altyapıyı anlatmak gerekmektedir. İnternetin Soğuk Savaş ekseninde ortaya çıktığı gerçeğinden yola çıkılarak, ilk safhanın ABD-Sovyetler Birliği arasındaki nükleer uzlaşmayı yöneten "karşılıklı kesin yıkım doktrini" stratejisi ile bağlantılı olduğunu ifade etmek mümkündür. Bu strateji, taraflardan birinin nükleer bir saldırı başlatması durumunda, diğerinin misilleme ile karşılık vereceğini garanti altına alarak ulusal güvenliği sağlamayı amaçlayan bir içeriğe sahip olsa da mantıksal olarak kusurlu bir strateji olduğu açıktır; zira saldırıyı başlatan tarafın önleyici saldırısı (*pre-emptive strike*) misilleme yapacak tarafın komuta ve kontrol sistemini etkisiz hale getirecek kadar yıkıcıysa, karşıdan herhangi bir saldırı gelmesi mümkün olmayacaktır (Naughton, 2016: 7). Bu sebepten dolayı Soğuk Savaş döneminde tarafların ihtiyacı olan şey, yıkıcı bir nükleer saldırıdan sağ çıkabilecek bir iletişim sisteminin tasarlanması olmuştur. RAND Corporation'da araştırmacı olarak bu görevi üstlenen kişi olan Paul Baran, yüksek seviyelerde çoklu bağlantıya dayalı bir örgüsel ağın ve çoklu iletişim cihazları arasındaki bağlantıyı sağlamanın yanı sıra veri iletimi konusunda da daha başarılı olan "paket anahtarlama" adı verilen bir dijital iletişim teknolojisinin dizaynını yaparak, analog sisteme sahip iletişim ağlarının baskın olduğu ve anahtarlama biçimi olarak devre anahtarlamanın kullanıldığını bir dönemde radikal fikirlere sahip olarak değerlendirilmiş ve bu nedenle bürokrasi engeline takılarak fikirlerini pratiğe dökememiştir (Naughton, 2016: 7).

Diğer yandan, aynı dönemde İngiltere Ulusal Fizik Laboratuvarında çalışan Donald Davies'in de paket değiştirme konusunda çalışmaları söz konusudur. Davies, sivil uygulamalar için tasarlamak üzere yeni bir iletişim ağı üzerinde çalışmaktaydı. Çalışmadaki bulgularına göre, analog telefon sisteminin bu ağ için yeterli olmadığı konusunda farkındalığa ulaştı ve bu sistemden bağımsız bir paket değiştirme fikri tasarladı. Bu fikrin arkasında yatan amaç ise, büyük mesafelere duyarlı, interaktif zaman paylaşımlı bir bilgi işleme sistemine sahip olmaktı (Naughton, 2016: 7).

Sürecin devamı, Naughton'un makalesinde ele alındığı üzere; 1957 yılında Sovyetler Birliği'nin Sputnik uydusunu başarılı bir şekilde fırlatmasını içermektedir. Bu olay sonucu, 1958 yılında ABD Savunma Bakanlığı bünyesinde bir devlet kurumu olan Gelişmiş Araştırma Projeleri Ajansı (ARPA) kurulmuştur. Bu ajans, sonrasında Pentagon birimlerine dâhil edilmiştir. ARPA, ajansla araştırma sözleşmeleri olan bazı üniversitelerin bilgisayarları konusunda finansman sağlamaktaydı. Ancak bu bilgisayarlar birbiriyle uyumsuz olduğu için araştırmacılar için kaynakların paylaşılması konusunda sıkıntı yaşanmaktaydı. Tam bu noktada, bu kaynakların paylaşılmasını sağlayacak bir ağ fikri ortaya atılmıştır: ARPANET (Gelişmiş Araştırma Projeleri Ajansı Ağı). ARPANET sayesinde her biri bir ana bilgisayara bağlı olan özdeş mini bilgisayarlardan oluşan bir alt ağ oluşturulması fikri ortaya çıkmıştır (Naughton, 2016: 8). Bu fikir teknik olarak oldukça

zor olsa da, hızlı bir şekilde inşa edilmiştir. 1972 yılına gelindiğinde; öncesinde fikri temelleri atılan ağ, on beş orijinal sitenin tümünün bağlantılı ve çalışır duruma ulaşmasıyla tamamlanmıştır. ARPANET aslında teknolojilerin sosyal olarak inşa edildiğini ortaya koyan güzel bir örnektir. Zira ağın şekillendirilmesi kullanıcılar tarafından yapılmıştır; kişiler ağın tasarımına aktif olarak dâhil oldukları için hem tasarımcı hem de kullanıcı olmuşlardır. Diğer yandan, ağın bir kaynak paylaşım tesisi olması amaçlansa da, kullanıcılar sistemi daha çok dosya paylaşmak, e-posta göndermek ve almak gibi iletişim kurma biçiminde kullanmaktaydı (Abbate, 1999: 108). Esasında buradaki önemli nokta, kullanıcı topluluğunun ağ oluşturmanın manası konusunda yeni bir anlayış geliştirmiş olmasıdır. Kullanıcılar tarafından inşa edilen bu anlayışa göre, ARPANET bir bilgi işlem sistemi değil, bir iletişim sistemi olarak görülmektedir (Abbate, 1999: 111).

1.3.1. Siber Dünyaya Giriş: Şili'nin Küresel Dünyaya Meydan Okuyan Cybersyn Projesi

İnternetin ikinci aşamasına geçmeden önce, bir noktaya dikkat çekmek gerekmektedir. İnternet etiketini taşıyan ilk bilgisayar iletişimleri sisteminin, ABD tarafından finansa edilen ARPANET tarafından oluşturulduğu bir gerçektir. Ancak günümüzde gelinen noktada "İnternet" kavramının tek kaynağının ARPANET'in çalışmaları olduğunu iddia etmek eksik bir bakış açısı sunmaktadır. Zira 1971 yılında ARPANET henüz faaliyete geçmeden önce, *Cybersyn* adı verilen ve ABD merkezli olmayan bir altyapı çalışması da mevcuttur. Cybersyn Projesi, Şili'nin siyasi karmaşıklığı sebebiyle günümüze kadar dayanıklılık gösteremese de, bu durum onun İnternetin gelişimindeki önemini ortadan kaldırmamaktadır (Abbate, 2017: 3). Kökeni itibariyle Antik Yunan'daki dümenci (kontrolü ele alan kişi) sözcüğüne dayanan ve karmaşık sistemlere uygulanan kontrol teorisi anlamına gelen sibernetiğin (The Editors of Encyclopaedia Britannica, 2014, parag. 2) önde gelen kuramcılarından biri olan Stafford Beer; 1970'li yıllarda Şili'de demokratik yollarla seçilmiş Marksist bir lider olan Salvador Allende'nin danışmanı olarak göreve getirilmiştir. Allende'ye göre, sosyalizme giden yolda Şili hükümetinin kontrol etmesi gereken çok fazla detay söz konusuydu. Beer, Allende'ye danışmanlık yaparken, sosyalizmi bilgisayar çağına taşıyabilecek bir bilgi sistemi sunma görevine sahip olmuştur. Tasarladığı sisteme verdiği isim ise, *cybernetics* (sibernetik) ve *synergy* (sinerji) kelimelerinin bir araya gelmesiyle oluşan "Cybersyn Projesi"ydi (Morozov, 2014: parag. 4). 1973'ün Ocak ayında Birleşik Krallık merkezli *The Observer* gazetesinin manşetlerinden biri "Bilgisayar tarafından yönetilen Şili" olmuştur. Cybersyn Projesi'nin merkezinde, ekonomi hakkında sibernetik olarak sağlam kararların alınacağı bir Operasyon Odası vardır.

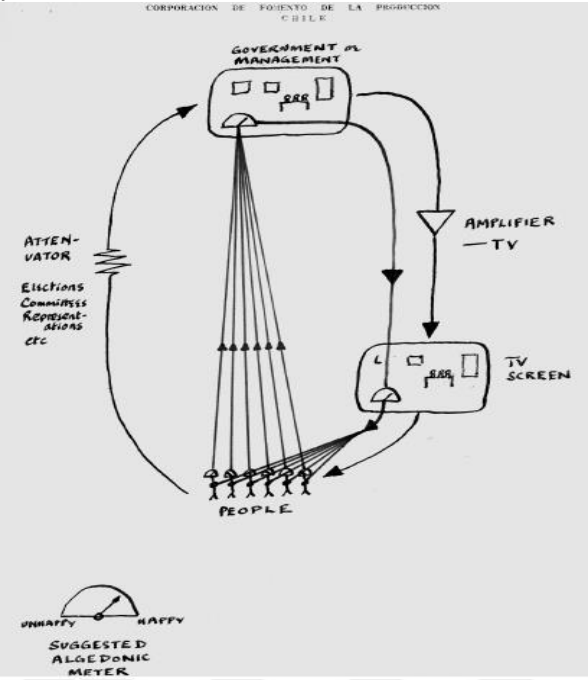
Fotoğraf 1. Cybersyn Operasyon Odası

Kaynak: (Espejo, 2014: 84)

Operasyon odasının amacı, ülkenin dört bir yanından gelen fabrika verilerini eşzamanlı olarak toplayarak gözden geçirmektir. Bu proje aslında Şili'nin küresel dünyaya meydan okuması olmuştur (Morozov, 2014, parag. 5). Şili ekonomisinin gelecekteki durumunun simülasyonu olarak planlanan projeye göre, tek bir düğmeye dokunulması sonucu dört ekranda yüzlerce resim ve figür gösterilecek; böylelikle üretim hakkında tarihsel ve istatistiki verilere ulaşılabilecekti. El ile çizilmesi gereken ekran görüntüleri için ise, dört grafiker kadın görevlendirilmişti. Bu projeyle birlikte, üretim kotalarını veya fiyatları belirlemeden önce kararın nasıl sonuçlanacağı konusunda bilgi sahibi olunabilmesi amaçlanmıştır.

Operasyon odalarının bir kısmı ise, sadece Şili ulusunun mutluluk seviyesini gerçek zamanlı olarak izlemenin hedeflendiği Cyberfolk Projesi için ayrılmıştır. Beer, vatandaşların evlerinde otururlarken aşırı mutluluktan tam mutluluğa kadar değişen ruh hallerini ifade eden bir cihaz yaparak, bu cihazları TV ağlarına bağlamıştır. Cihazdaki ibre, hükümet politikalarına verilen tepkilerden yola çıkarak ulusal mutluluk seviyesini göstermek için sahte bir ölçüm sunmaktadır.

Fotoğraf 2. Beer'in, Cyberfolk Projesi'nin Hükümet ve Şili Halkının Birbirine Uyum Sağlamasına Nasıl Yardımcı Olabileceğinin Çizimi



Kaynak: Medina, E. (2011: 90).

Bütün bunlardan yola çıkarak öne sürülebilir ki; ARPANET faaliyete geçmeden önce Beer tarafından Sosyalist bir ideoloji çerçevesinde öne sürülen Cybersyn Projesi, adeta bir geleceğe dönüşü ifade etmektedir. Günümüzde gerçek zamanlı bir şekilde aktarılan veriler ve bir bütün halinde toplanan Büyük Veri (*Big Data*) adı verilen kavram Cybersyn Projesi'nin devamı şeklindedir. Bu noktada, 1970'lerden günümüz dünyasında kadar geçen süreçte, özellikle hükümetler ve özel şirketler tarafından kullanılan gerçek zamanlı bilgi toplama ve analiz etme yöntemleriyle birlikte, birçok açıdan Beer'in sibernetik hayalinin gerçek olduğunu iddia etmek mümkündür (Morozov, 2014: parag. 8).

1971 yılında İngiliz sibernetikçi Stafforr Beer'in sibernetik ve teknolojinin yapısal ve siyasal değişimini incelemek için ortaya attığı proje olan Cybersyn, ardından Eden Medina'ya da ilham olmuştur. Bu projeden tam 30 yıl sonra 2011 yılında Medina'nın kaleme aldığı ve Cybersyn projesinin izlerini takip eden, Sibernetik Devrimciler: Allende'nin Şili'sinde Teknoloji ve Siyaset (*Cybernetic Revolutionaries: Technology and Politics in Allende's Chile*) adlı kitabı da oldukça önemli bir eserdir. Medina bu eserinde, ARPANET ortaya çıkmadan önce ABD'den bağımsız olarak Şili'de tasarlanan Cybersyn Projesini anlatarak bu alandaki tüm yeniliklerin Kuzey kökenli olmadığını ortaya koymak istemektedir (Abbate, 2017: 3).

1.3.2. İnternetin Gelişiminin İkinci Aşaması: Siber Uzay

İnternetin ikinci aşamasına gelindiğinde; bu kısım Naughton'a göre (2016: 12) 1995'ten günümüze kadar olan süreci ifade etmektedir. "Siber uzay" kavramı ise 1980'lerde, yazar William Gibson tarafından kaleme alınan "Neuromancer" adlı kitapta yayınlanan şekilde, bilgisayar ekranının arkasındaki sanal dünyayı tanımlamak için icat edilmiştir (Gibson, 1984).

İnternetin ikinci aşamasındaki iki gelişme, siber uzay ve fiziksel dünya arasında var olan ayrımı aşındırarak birleşmelerine neden olmuştur. Bu gelişmelerden birincisi, ABD Ulusal Bilim Vakfı'nın, ağın ticarileştirilmesi kararı alarak ağı İnternet Servis Sağlayıcılara devretmesidir. Bu karar, sıradan insanların ağa erişebilmesi anlamına gelmektedir. Gelişmelerden ikincisi ise, World Wide Web'in ortaya çıkışıdır.

Web, CERN'de çalışan fizikçi ve bilgisayar bilimcisi Tim Berners-Lee tarafından yaratılmıştır. Fikrin altında yatan nokta, dünyanın dört bir yanındaki İnternet sunucularında depolanan belgeleri yayınlamanın, yerini tespit etmenin ve erişmenin bir yolunu bulmak olmuştur (Naughton, 2016: 13). İsviçre'deki Avrupa Fizik Laboratuvarı CERN'de araştırma yaparken belgelerin kontrolünü sağlamak için faydalı olacağı düşünülmüştür. Berners-Lee bu kontrolü sağlamak için şöyle bir yöntem bulmuştur: yerleşik bir teknoloji olan *hypertext*'i alıp İnternet üzerinde çalışmasını sağlamak. Hypertext teknolojisini basitçe ifade etmek gerekirse, bir metnin ilgili bölümleri ve o bölümlerle ilişkili grafikler arasında, çapraz referans ile kapsamlı bir şekilde belgeler oluşturan bir teknolojidir (Naughton, 2016: 13). Hypertext teknolojisini İnternete uyarlayan Bernes-Lee; 1990 yılının sonunda, üç ay içinde "World Wide Web" adını verdiği bir prototip yaratmayı başarmıştır. Geçmişte çok fazla heyecan uyandırmayan Web projesi, Mart 1991'de CERN'den gerekli izinler alındıktan sonra Berners-Lee tarafından info.cern.ch adresinde halka açık bir sunucu açılmıştır. Ancak tüm bu gelişmelere rağmen, 1991-1992 yılları arasında Web'in yayılması hızı düşüktür; bu durum 1993 bahar aylarına kadar bu şekilde devam etmiştir. 1993 yılının baharında, Illinois Üniversitesi'nde çalışan Marc Andreessen ve Eric Bina Web için yazmış oldukları, grafikleri satır içi olarak görüntüleyen ilk tarayıcı olan *Mosaic*'i piyasa sürmüştür. Mosaic'in piyasaya sürülmesi, hem Web'in hem de İnternetin evriminde dönüm noktası olması açısından oldukça önemlidir. Ayrıca Web'i kullanmak için İnternet gerektiğinden, halk arasında İnternet bağlatmak isteyen kişi sayında artış söz konusu olmuştur; bu durum Web'in ticari potansiyelini ortaya koymaktadır (Naughton, 2016: 14).

Mosaic'in sebep olduğu dönüşümü şöyle ifade etmek mümkündür: Mosaic ortaya çıktığında, İnternet trafiğinin yüzde 1'den azı World Wide Web'deyken iki yıl sonra tüm trafiğin yaklaşık dörtte birini oluşturan Web, İnternet'teki en popüler şey olmuştur. Mosaic'in, kullanıcılarına sağladığı en önemli avantaj ise, grafik görüntülerinin metinlerin yanında görüntülenebilmesine olanak sağlaması olmuş; bu sayede renksiz metinlerin yer aldığı ortam bir anda gökkuşağı gibi renkli bir yere dönüşmüştür (Cassidy, 2003 : 57).

1.3.3. İnternetin Ticarileştirilmesi: Netscape

Mosaic'i yazan isimlerden biri olan Andreessen, 1994 yılında Illinois Üniversitesi'nden ayrılarak Jim Clark ile birlikte Web'den ticari olarak yararlanmak amacıyla kurulan ilk şirket olan Netscape şirketini kurmuştur. Şirketin ilk ürünü; birçok bilgisayar sistemi için sürümlere sahip olması sebebiyle piyasada baskın hale gelen *Netscape Navigator* adlı tarayıcıdır. 1995 yılında Netscape'in halka arz edilerek yüksek bir değere ulaşmasıyla birlikte, İnternet'e olan ilgi yoğun bir şekilde tetiklenmiştir. Robert Schiller, bu İnternet patlamasını "dot-com balonu (*dot-com bubble*)" olarak adlandırmaktadır. Patlamayı tetikleyen şey, pazarda yeni olmasına rağmen, Netscape'i takiben çok sayıda Web tabanlı şirketin borsada yoğun ilgi görmesi olmuştur. Az gelir olan hatta bazen hiç geliri olmayan

dot-com şirketleri, hatırı sayılır gelire sahip köklü şirketlerden çok daha yüksek borsa değerine sahip olmaktaydı. Balon bir süre daha devam şişmeye devam etse de 2000 yılının Mart ayında patlayarak, dot-com şirketlerinin yarısından fazlasını piyasadan sildi. Bunun sonucunda ise, İnternet olgusunun, tıpkı "şişirilmiş balon" gibi abartılmış bir olgu olduğu kanısına varılmış ve toplumda bir hayal kırıklığı oluşmuştur. Ancak bu anlaşılabilir bir durum olarak görülmelidir. Zira 1990-2000 yılları arasında, diğer bir ifadeyle yirminci yüzyılın son on yılında; İnternet teknolojisi, yatırımcıların beklentilerini karşılayacak kadar olgunlaşmamıştır (Naughton, 2016: 15). Digital 2020 raporuna göre, 2020 itibariyle dünya nüfusunun %60'ı İnternete erişim sağlarken, 2000 yılında ise, bu oran sadece % 6.5 olarak kalmıştır (Kemp, 2020)

Tablo 1. 1990-2000 Yılları Arasında İnternet Kullanımı ve İnternetin Gelişimi

Dünya nüfusuna göre küresel düzeyde İnternet kullanım oranı		**Gelişmeler**
1990	% 0.049	-CERN'deki araştırmacılar World Wide Web'i geliştirdi.
1991	% 0.079	-İlk web sayfası yayınlandı. -İlk web tarayıcı piyasaya sürüldü.
1992	% 0.125	
1993	% 0.179	-Mosaic web tarayıcı piyasaya sürüldü.
1994	% 0.36	-Netscape web tarayıcı piyasaya sürüldü.
1995	% 0.681	-Ebay, Yahoo ve Amazon.com -Internet Explorer
1996	% 1.323	- Anlık mesajlaşma programı olan ICQ piyasaya sürüldü.
1997	% 2.037	-Google araması
1998	% 3.136	
1999	% 4.63	-Alibaba ve Napster
2000	% 6.526	

Kaynak: The World Data Bank, Individuals using the Internet (% of population), 2020; Our World in Data, Internet, 2020

İnternet o dönem yeteri kadar olgunlaşamasa da, gelecekte olgunlaşması gerekli teknolojik altyapıyı yaratmıştır. İnternet bir balon olarak şişmeye başladığında bazı gözlemciler; durumu, 1848 yılında yaşanan Kaliforniya Altına Hücum Dönemi'ne (*California Gold Rush*) benzetmiştir. Altına Hücum döneminde Kaliforniya'da en çok para kazananların madenciler ya da altın arayanlar olması beklenirken; tam tersine kazma ve kürek satan tüccarlar olduğu görülmüştür. Bu tüccarların 1990'lardaki karşılığı ise, geniş fiber optik kablo ağları ve sunucu çiftliği (*server farms*) inşasına büyük yatırımlar yapan telekomünikasyon şirketleri olmuştur (Naughton, 2016: 15). İnternetin beklentileri karşılayamayarak patladığı o yıllarda; bu şirketlerin çoğu iflas etse de geriye inşa ettikleri kritik altyapıları bırakmışlardır. Ekonomist Bradford LeLong, inşa edilenlerin kârlı olmadığını ancak büyük bir kısmının çok faydalı olacağını ifade ederek bu görüşü desteklemektedir (LeLong, 2003).

Askeri bir deney olarak başlayan İnternet (Naughton, 2016: 7); günümüzde devletlerin, kuruluşların ve bireylerin, gerçekleştirdiği tüm faaliyetlerde bağlı olduğu bir kaynak haline gelmektedir. Bu bağlılık, bağımlılık yaratmakta olduğu için siber güvenlik kavramı aktörlerin gündeminde her geçen gün daha da fazla önem kazanmaktadır.

Bilgi ve iletişim teknolojilerinin unsurlarının anbean gelişimi, dijital bileşenlerdeki gelişmeleri de beraberinde getirerek maliyetlerde düşüşe olanak sağlamaktadır (Mbanaso ve Dandaura, 2015: 17). Bu durum ise, İnternetin dünya çapında daha kolay erişilebilir hale geldiğini göstermektedir. Tablo 2'de listelenen veriler, küresel düzeyde değerlendirildiğinde, giderek çok daha fazla insanın İnternette ve dijital dünyada aktiflik gösterdiğini kanıtlamaktadır.

Tablo 2. Ekim 2018, 2019 ve 2020 - Dünya Çapındaki Dijital Veriler

	Toplam nüfus	**Mobil telefon kullanıcıları**	**İnternet kullanıcıları**	**Aktif sosyal medya kullanıcıları**
Ekim 2018	7. 65 milyar (% 55)	5.11 milyar (% 67)	4.17 milyar (% 55)	3.39 milyar (% 44)
Ekim 2019	7.73 milyar (% 55)	5.15 milyar (% 67)	4.47 milyar (% 58)	3.72 milyar (%48)
Ekim 2020	7.81 milyar (% 56)	5.20 milyar (% 67)	4.66 milyar (% 60)	4.14 milyar (% 53)

Kaynak: (Kemp, 2018, 2019, 2020)

DataReportal'ın Ekim 2020 raporundaki sayılar incelendiğinde; dijital platform, mobil cihazlar ve sosyal medyanın küresel olarak insanların günlük yaşamında kaçınılmaz ve güçlü bir etkiye sahip olduğu net bir şekilde görülmektedir. Rapora göre, 2020'nin başında 4,5 milyardan fazla insan İnternet kullanmaktadır. Sosyal medya kullanıcıları ise, 3,8 milyar gibi bir sayıya ulaşmıştır. Aktif sosyal medya kullanıcılarının yüzdesi küresel nüfusu yarılarken; çevrimiçi olma durumuna bakıldığında ise, hâlihazırda dünya nüfusunun yaklaşık %60'ının çevrimiçi olduğu görülmektedir (Kemp, 2020). Ekim 2018 ve 2019 yıllarına bakıldığında özellikle İnternete erişim bağlamında yüksek oranda artış olduğunu görmek mümkündür. Zira 2018 yılında dünya çapında 4.17 milyar insan çevrimiçiyken, bu oran 2020 yılında 4.66 milyara ulaşarak neredeyse yarım milyar insanı İnternet ortamına aktarmıştır (Kemp, 2018, 2019, 2020).

1.4. Siber Uzayda Etkili Olan Güvenlik Unsurları

İnternetin gelişimi, teknolojik altyapı anlamında siber uzay için önemli olsa da, iki kavramın birbirinden farklı olduğunu vurgulamak önemlidir. İnterneti, siber uzayı mümkün kılan teknoloji olarak ele almak gerekmektedir. İnternet teknolojisi, geniş sosyal boyutlara sahip bir olgu olan siber uzayı kolaylaştırmakta ve onunla kaçınılmaz bir şekilde iç içe geçmektedir. İnternet, teknik bir mimariye sahip bir alan iken; siber uzay ise, mekânsal bir yapıya sahip bir alandır. Siber uzayın mekânsal coğrafyası, beşinci operasyonel alan olarak değerlendirilen yeni alanın sınırlarını yeniden kodlamakta ve dünyayı yeniden programlamaktadır (Blount, 2019 : 17).

Siber uzay, insan eliyle inşa edilen bir alandır. İnsanlar artık daha önce hiç deneyimlemedikleri yollar ile iletişim ve ilişki kurabilmektedir. Gerçek uzayın asla izin vermeyeceği bir tür toplumu vaat etmekte olan siber uzay; vadettiği bu toplum içerisinde anarşi olmadan özgürlük, hükümetsiz kontrol, iktidarsız fikir birliği gibi kavramları bulundurmaktadır. Bunu destekler nitelikte, siber uzayın mekânsal ortamını tanımlayan bir manifestodaki şu sözler önemlidir: "Kralları, başkanları ve oylamayı reddediyoruz. Kabataslak fikir birliğine ve çalışan koda inanıyoruz (Lessig, 2006 : 17)."

Siber uzayın ilginç yönlerinden birinin, teorik olarak herhangi bir kimse tarafından yönetilmeyen özgür ve sınırsız bir alan olduğunu ifade etmek mümkündür. Ancak sınırsız, özgür ve yöneticinin olmadığı bu alan, fırsatları olduğu kadar riskleri de beraberinde getirmektedir. Siber uzayın altyapısını oluşturan veriler, ağlar ve sistemler; dünyanın herhangi bir yerinden herhangi biri tarafından gerçekleştirilen saldırılarda bozulabilme ve tehlikeye girme durumuna sahiptir. Teknolojinin getirdiği dönüşümlerle birlikte siber uzaydaki fırsatlar ve riskler değişiklik göstermektedir. Küresel siyasette, tüm ülkelerin siber uzayı algılama biçimi birbirinden farklıdır. Bu nedenle, ortaya çıkan fırsatlar ve riskler ile beraber siber uzay şekillendikçe, ülkelerin siber uzayı algılama biçimi de yeniden şekillenmektedir (Mbanaso ve Dandaura, 2015: 18). Bir diğer ifadeyle, elbette siber uzayın insanlık için birçok kolaylığı ve imkânı beraberinde getirdiği gerçeği söz konusu olmaktadır; ancak diğer yandan tıpkı Truva atı gibi, ulusları içerden etkilemekte ve egemenlik kavramını sorgulatarak uluslararası sistemdeki barışın ve güvenliğin sağlanması konusunda tehlike sinyalleri vermektedir. Diğer yandan siber uzayda inovasyonlara yön veren kapasite ve kabiliyet kavramları, tarihsel analoji metodu ile uluslararası ilişkileri Peloponezya Savaşlarına bir yolculuğa çıkarak, çatışma tehdidi konusunda uyarılarda bulunmaktadır. Tıpkı Sparta'nın güçlenmesinin ve kapasitesini artırmasının Atina'da yol açtığı korku ve sonrasında güvenlik ikilemiyle kendini gösteren savaş gibi; siber uzaydaki aktörler de siber uzayda kapasitenin arttırılması ve kabiliyetlerin zenginleşmesi konusunda teknolojik olarak rekabete girmektedir. Rekabetin söz konusu olduğu bu yeni atmosferde aktörler siber uzaydaki belirsizliği netleştirmede söz sahibi olmak istemektedirler (Mbanaso ve Dandaura, 2015: 20).

"Siber" teriminin tarihsel ve felsefi köklerinin, Platon'un Devlet eserindeki mağara alegorisinde yattığı düşünülmektedir (Choucri, 2012: 7). Mağara alegorisi, çocukluklarından beri mahkûm olan kişilerin yaşadığı, gün ışığından uzak karanlık bir yeraltı mağarasını anlatmaktadır. Bu kişilerin bacaklarında ve boyunlarında zincirler bulunmakta, mağaranın önünde ise, bir duvar mevcut olmaktadır. Duvarın arkasında, ellerinde bazı objeler taşıyan insanlar ve ateşle aydınlatılan bir ortam vardır. Mahkûmlar ise, yanan ateşin etkisiyle duvara yansıyan gölgeleri görmektedir. Karanlıkta kendilerince bir gerçekliğe sahip olan mahkûmlar; ilk defa gözledikleri gölgeler nedeniyle bu gerçekliği sorgulamakta ve görünenin ardındakileri fark etmeye yönelmektedir. Alegoriye göre mahkûmlar öncesinde zincirlerini kıramamışlardır; çünkü alışkanlıklarına yönelik bağımlılık sergilemektedirler. Bağımlılıklarından kurtularak zincirlerini kırmak istediklerinde ise, arkada kimin ve neyin olduğu konusunda fikir sahibi değillerdir. (Canbek, 2018: 77).

Fotoğraf 3. Mağaranın alegorisinin günümüz gerçekliğine yansıması: TV'den mobil cihazlara

Kaynak: (Canbek, 2018: 77)

Fotoğraf 3'te görüldüğü üzere günümüzde de bağımlılık sona ermemekte; mağaranın duvarına yansıyan gölgelerden, sinema, TV, bilgisayar ve mobil cihazların ekranlarına doğru bir dönüşüm gerçekleşmektedir (Canbek, 2018: 77).

Modern çağ çerçevesinde düşünüldüğünde, kavramın Norbert Weiner'in 1948 yılında yayınladığı "Sibernetik: veya Hayvan ve Makinede Kontrol ve İletişim" adlı kitabındaki sibernetik teriminden türetildiği öne sürülmektedir. 1984 yılına gelindiğinde William Gibson, şu an siber uzay olarak ifade ettiğimiz yeni alanın adının geçtiği kısa bir öykü kaleme almıştır ve siber uzay terimi ilk defa Gibson'un bu hikâyesinde geçmektedir (Choucri, 2012 : 7).

Canbek'in, makalesinde (2018: 63-64) yer verdiği siber uzay kavramının tasvirini kolaylaştıran hikâye bu anlamda güzel bir örnek olmaktadır. Mevlana, karanlık bir odada bazı insanlara bir fil sergileyen Hinduların hikâyesini anlatmaktadır. Oda zifiri karanlık olduğundan, sergilenen filin nasıl bir şey olduğu hakkında fikir edinmenin tek yolu elle dokunmak, hissetmek ve tahmin etmektir. Rumi'nin anlattığı hikâyenin devamında ise, her dokunan farklı bir algıya kapılmıştır. Kimi ayağını hissederek sütun olduğu tahmininde bulunurken; diğeri ise, kulağını hissederek filin bir pervane olduğu fikrine kapılmıştır. Her dokunan kişi, hissettiği kısma göre hayvanın farklı bir tanımını yapmıştır. Canbek ise, yeni, karmaşık ve kafa karıştırıcı bir kavram olan siber güvenliği, hikâyedeki "karanlıktaki file" benzetmektedir. Hikâyede tahmin etmek için dokunmak, hissetmek gibi davranışları ise, sanal alanın "karanlığında" yönünü bulmak isteyen insanların eylemleri olarak görmektedir (Canbek, 2018: 63-64).

1.4.1. Siber uzayın etimolojisi

Siber uzayın etimolojisi, Gibson'ın Neuramancer romanının ötesine yani sibernetik dünyaya kadar uzanmaktadır (Lessig, 2006 : 18). Kavram üzerinde küresel ortak bir tanıma varılmasa da, tanımlamak basitleştirmek olduğu için, bu noktada siber uzayı tanımlamak önem arz edecektir. Öncelikle siber uzayın özelliklerinden bahsetmek kavramı anlamak konusunda yol gösterici olacaktır. Mbanaso ve Dandaura'ya göre siber uzay, bilgi sistemleri ve İnternet tarafından yönlendirilmekte; ekonomik büyümeye katkıda bulunarak insanların birbiriyle etkileşime girmesi ve işbirliği yapabilmesi için yeni araçlar ortaya koymakta, nihayetinde ise, dönüştürücü bir etkiye sahip olmaktadır (Mbanaso ve Dandaura, 2015: 17).

ABD Hava Kuvvetleri emekli generali Larry D. Welch, "Beşinci Operasyonel Alan Olarak Siber Uzay" adlı makalesinde; terazinin bir kefesine siber uzayı diğer kefesine ise, kara, deniz, hava ve uzay gibi diğer operasyonel alanları yerleştirmektedir. Bu kıyaslama sonucu ise, iki kefenin de zorluklar ve fırsatlarla başa çıkarken benzer özelliklere sahip olduklarını iddia etmektedir. Bu bağlamda siber uzayın daha iyi anlaşılabilmesi için, bir görev olarak değil de yeni bir saha olarak ele alınması gerekmektedir (Welch, 2011: 2).

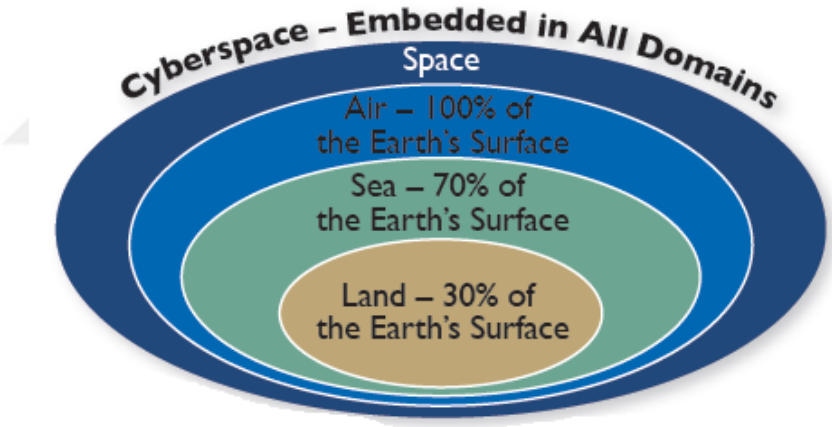
Siber uzaya ilişkin askeri hedeflere bakıldığında; temel noktaların kara, deniz, hava ve uzay şeklinde sıralanan dört operasyonel alan ile aynı olduğu görülmektedir. Beşinci operasyonel alan olan olarak ele alınmanın amaçlandığı siber uzayda ve siber uzay boyunca geçerli olan temel amaç, hareket etme özgürlüğüdür. Bu temel amacın doğal bir sonucu

olarak, seçilen yer ve zamanda rakiplerin/düşmanların hareket etme özgürlüğünün bloke edilmesi ortaya çıkmaktadır. Welch'e göre bir aktörün; hem hareket etme özgürlüğüne, hem de rakibinin/düşmanının hareketini engelleme yeteneğine sahip olması ise, aktöre askeri üstünlük sağlamaktadır (Welch, 2011: 2).

Siber uzay ile birlikte beş tane olarak kabul edilen operasyonel alanlardaki askeri üstünlük ihtiyacına ve askeri üstünlüğün doğasına bakıldığında, aynı şekilde benzerlikler görülmektedir (Welch, 2011: 2). Örnek vermek gerekirse, karadaki üstünlüğün sağlanabilmesi için tüm kara sınırlarının tüm zamanlar için kontrol edilmesine gerek yoktur; seçilen belirli bölgeler sürekli kontrol altında tutulurken, kalan bölgelerin ise, sadece belirli dönemlerde kontrol edilmesine ihtiyaç duyulmaktadır. Aynı durum siber uzay için de geçerli olmaktadır. Ancak elbette ki, küresel bir siber uzay tanımının dahi olmadığı göz önüne alındığında, siber üstünlük kavramı hakkında da net bir yargıda bulunmak zor olmaktadır.

Siber uzay ve diğer dört operasyonel alan arasında temel benzerlikler söz konusu olduğu kadar, bazı temel farklılıklar da mevcuttur. Bu farklılıklardan ilki, şekil 2'de de görüleceği üzere, doğası gereği diğer operasyonel alanların hiyerarşisinin jeofiziksel olmasıdır (Welch, 2011: 3).

Şekil 2: Tüm Alanlara Gömülü Siber Uzay (Welch, 2011)



Kaynak: (Welch, 2011: 2)

Şekil 2'de görselleştirildiği biçimde, kara, hava deniz ve uzay hiyerarşik bir biçimde dizilmektedir. Dünya yüzeyinin %30'unu oluşturan kara en alt tabakada yer almakta; ardından karayı da çevreleyen bir şekilde %70'i kapsayan bir alan ile deniz gelmekte; tüm dünya yüzeyini kapsayacak şekilde hava alanı gelirken; uzay ise, tüm dünyayı içine alarak daha geniş bir operasyonel alanı oluşturmaktadır. Tüm bu hiyerarşik düzen içerisinde siber uzayın konumlandırılması ise, ilginçtir. Zira siber uzay tüm alanlardan ayrı bir alan olarak değil, tüm alanların içine gömülü bir alan olarak konumlandırılmaktadır. Bu nedenle, siber uzayda ve siber uzaydan gerçekleşen tüm operasyonlar, diğer dört operasyonel alanın işleyişi konusunda belirleyici niteliğe sahip olmaktadır (Welch, 2011: 3).

Siber uzay ve diğer dört operasyonel alan arasındaki ikinci temel farklılık ise, siber uzayın insan eliyle inşa edilmiş bir alan olmasıdır. İnsan faktörü söz konusu olduğunda değişimin kaçınılmaz olduğunu belirtmek gerekir. Bu nedenle, siber uzay sabit bir alandan ziyade

sürekli değişen bir operasyonel alan olarak inşa edilmektedir. Siber uzaydaki askeri etki, ağların kullanım hâkimiyeti üzerinden belirlenmektedir. Bu ağlar dostane ve düşman/karşıt operasyonlar için kullanılabilmektedir. Etki ağlarının çoğu birbirine bağlı olduğu için siber uzayın da tek bir ağ olduğu şeklinde yanlış bir algı söz konusudur. Ancak bu doğru değildir. Tıpkı diğer alanlarda olduğu gibi, hareket özgürlüğünün zorunlu olduğu siber uzay içinde, içinden ve aracılığıyla da eylemin gerekli olduğu siber uzay bölümlerini tanımlamak gerekmektedir (Welch, 2011: 3).

Siber güvenlik kavramına bakıldığında; kavramın, özel sektör ve hükümetler tarafından bilgi güvenliği terimi ile ifade edildiğini görmek mümkündür. Özel sektörde e-ticaretin korunması noktasında bir ihtiyaç söz konusudur. Ticari kaygılar güden özel sektör nezdinde siber güvenlik; bilgiyi ve bilgi sistemlerini yetkisiz erişimden ve dış müdahalelerden korumak şeklinde tanımlanmaktadır. Hükümetler nezdinde ele alındığında, örneğin ABD hükümeti tarafından bilgi güvenliği konusunda kapsamlı bir tanım mevcuttur. ABD hükümetine göre bilgi güvenliği terimi; bilgiyi ve bilgi sistemlerini yetkisiz erişim, kullanım, ifşa, kesinti, değiştirme ve imha gibi tehditlerden korumak anlamına karşılık gelmektedir. Tanıma göre bilgi güvenliğinin sağlanmasının amaçları üç maddede ifade edilmektedir (Public Printing and Documents, 2002: 147):

I. Bütünlük, uygunsuz bilgi değişikliğine veya bilginin imhasına karşı koruma sağlamak anlamına gelmektedir. Bütünlüğün sağlanmasıyla, bilginin gerçekliğini sağlamak amaçlanmaktadır.

II. Gizlilik, kişisel mahremiyeti ve kişisel bilgileri koruma araçlarını da içeren bir şekilde, erişim ve ifşaya ilişkin koruma sağlanması anlamına gelmektedir. Amaç, yalnızca yetkili kişilerin ulaşımına izin vererek gizliliği sağlamaktır.

III. Ulaşılabilirlik/Uygunluk ise, bilgiye zamanlı ve güvenilir erişimin sağlanmasını içermektedir. Böylelikle bilgilerin kullanılmasına imkân tanınmaktadır.

Özel sektörün bilgi güvenliği veya diğer bir deyişle ticari bilgi güvenliği, ticari kaygıya sahip uluslararası örgütler tarafından da ele alınmaktadır. Ekonomik temelli olarak kurulan ve ardından taşma *(spill-over)* etkisiyle siyaset gibi diğer konulara da ilerleyen Avrupa Birliği'nin (AB) Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) girişimi bu konuda güzel bir örnektir. Bu ajansın odak noktası, meşru e-ticaret akışını kolaylaştırmaktır. ENISA girişiminin tüzüğünün 2. Maddesinde yer alan şekilde ajansın amacı, "*Topluluğun, Üye Devletlerin ve iş dünyasının ağ ve bilgi güvenliği sorunlarını önlemek, vurgulamak ve yanıt vermek*" olarak tanımlanmaktadır (Avrupa Parlamentosu ve Konsey, 2004).

1.4.2. Siber uzayın getirdiği fırsatlar ve yenilikler

Siber uzay, belirsizliklerle dolu yeni bir dünyayı tanımlamaktadır. Bu yeni dünya içerisinde ise; fırsatlar ve yenilikler, güvenlik açıkları, tehditler ve riskler, çatışmalar ve savaşlar yer almaktadır (Mbanaso ve Dandaura, 2015: 18). Siber uzay dönüştükçe yeni dünya içerisindeki bu özellikler de dönüşmektedir; diğer yandan bu özelliklerin de siber uzayı da dönüştürdüğünü ifade etmek gerekir. İki unsur birbirini karşılıklı olarak inşa etmektedir.

Bu noktada, siber uzayın getirdiği fırsatlara ve yeniliklere değinmek gerekmektedir. Siber uzayın ortaya çıkışı, dijital devrimin fırsatlarını artırmaktadır. Dijital devrime biraz daha

yakından bakıldığında, "bilgi ekonomisi" kavramının temelini oluşturduğunu öne sürmek mümkün olacaktır. Bilgi ekonomisi, oldukça ilginç bir yapıya sahiptir; diğer endüstrilerin aksine, bilginin birincil hammadde ve değer olarak kabul edildiği bir ekonomi olarak tanımlanmaktadır (Mbanaso ve Dandaura, 2015: 18). Hızla gelişen bilgi ekonomisiyle birlikte siber uzayın dinamikleri de değişmektedir. Bu nedenle, devletler önceliklerini bu alana kaydırmak için çeşitli stratejiler izlemelidir. Dijital devrim, fiziksel dünyadaki devrimlere oranla insan girişiminin her yönünü kapsamaktadır; zira ölçek ve kapsam açısından icat ve yeniliklere daha hızlı tanıklık etmektedir (Mbanaso ve Dandaura, 2015: 18). Dijital dünyadaki girişimlerin büyük bir hızla çoğalmasının sebebi, insan-teknoloji-bilgi üçlüsü arasındaki kaçınılmaz bağlantıdan kaynaklanmaktadır ve siber uzayın canlılığı ve gücü, bu üçlüye bağlı olarak inşa edilmektedir.

Yeniliklerin ve buluşların bu derece hızlı evirilmesinin sebebi, İnternetin ve dolayısıyla siber uzayın "açık" özelliklere sahip olmasıdır. Diğer bir ifadeyle, araştırmacılar, yenilikçiler ve geliştiriciler fikirlerini pratiğe dökmek için herhangi bir otoriteden onay olmak zorunda değildir. Açık siber uzayda bir buluş ortaya koyulduğunda; bu buluş küresel anlamda binlerce buluşa ve yeniliğe kapı açmaktadır. Mucidi ise, temel kavramlara atıfta bulunduktan sonra kimseye başvurmadan sürece devam etmektedir. Diğer yandan, insan doğasında mevcut olan iştah ve hızlı çözüm oluşturabilme yeteneği, bu buluşları ve yenilikleri teşvik eden tetikleyiciler olarak ele alınabilmektedir (Mbanaso ve Dandaura, 2015: 19). Kara, deniz, hava ve uzay gibi operasyonel alanların, tabiatın işleyişi sonucu çeşitli coğrafi olaylar sonucu oluşması söz konusuyken; diğer alanlardan farklı olarak insan eliyle inşa edilmiş bir operasyonel alan siber uzay ise, insan bileşenine sahip olması nedeniyle daima değişime ve sürprizlere açık bir alan olmaktadır. Bu değişim ve sürprizler olumlu veya olumsuz sonuçlar doğurabilmektedir.

Web sitelerin başında yer alan "WWW" harfleri, etkisinin büyüklüğü İnternetin gelişimindeki önemli bir olay olarak ifade edilmektedir. Açılımı "*World Wide Web*" olan buluşun mucidi Sir Bernets Lee'dir. Lee'nin 1989 yılındaki bu buluşuyla İnternetin manzarasını tamamen değiştirdiğini ve bu buluşun siber uzaydaki teknolojik ilerlemelerin artışının katalizörü olduğunu iddia etmek mümkündür (Mbanaso ve Dandaura, 2015: 19). Zira bu buluşun açtığı yolda ilerleyen birçok yenilik ortaya çıkmıştır. 1998 yılında kurulan Google, bu örneklerden biridir. Google, birçok teknolojiyi tek bir arayüzde birleştirerek sürekli olarak yenilikler ortaya koyan başarılı bir oluşumdur.

1.4.2.1. Nesnelerin İnterneti ve bulut bilişim

Dijital devrimdeki fırsatlar ve yenilikler söz konusu olduğunda, Nesnelerin İnterneti (*Internet of Things*) kavramına da değinmek gerekmektedir. Nesnelerin İnterneti teknolojisi, giderek daha fazla gelişmekte ve insan yaşamını tahmin edilemez etkilerle dönüştürmeye devam etmektedir. İnsan unsurunun devrede olması sebebiyle, ortaya konulan bu teknoloji de baz alınarak; siber uzayda hayal gücünün sınırsız, fırsatların ise tahmin edilmez olduğu anlamını çıkarabilmek mümkündür. İnsan-teknoloji-bilgi üçlüsündeki etkileşimler sonucu siber uzayda ortaya çıkabilecek buluşların sınırı yoktur. Bu üçlüye ek olarak Nesnelerin İnterneti teknolojisinin etkileri de göz önüne alındığında,

iyi etkileşimler ile bilginin gücünün daha da artacağı öngörüsünde bulunmak mümkün olacaktır (Mbanaso ve Dandaura, 2015: 19).

Dijital devrimdeki buluşlardan biri olan ve gitgide evirilen bir paradigma olan Bulut Bilişim (Mell ve Grance, 2011: 1), siber uzaydaki sanal sınırları daha da bulanıklaştırması ve hatta ortadan kaldırması sebebiyle oldukça kritik öneme sahiptir (Mbanaso ve Dandaura, 2015: 19). Ulusal Standartlar ve Teknoloji Enstitüsü'nün (NIST) raporunda yer verdiği tanıma göre;

> "Bulut Bilişim, minimum yönetim çabası veya servis sağlayıcı etkileşimiyle, hızlı bir şekilde temin edilebilen ve piyasaya sürülebilen ağlar, sunucular, depolama, uygulamalar ve servisler gibi yapılandırılabilir bilişim kaynaklarının paylaşım havuzuna ulaşılabilir, kullanışlı, isteğe bağlı ağ erişimini mümkün kulan bir modeldir (Mell ve Grance, 2011 : 2) ."

Daha basit bir biçimde ifade etmek gerekirse; Bulut Bilişim, siber uzaydaki kullanıcıların ihtiyaç ve talebine bağlı olarak her zaman ve her yerde bilişim kaynaklarına erişmelerini ve bu kaynakları kullanmalarını sağlayan bir ortamdır (Mbanaso ve Dandaura, 2015: 19). Bulut bilişim, doğası gereği küreselleşmiş bir teknolojidir (Dannatt, 2012: 1). Sunduğu imkânlar bağlamında, yukarıda bahsedildiği gibi siber uzaydaki sınırları bulanıklaştırarak ve ortadan kaldırarak büyük çaplı etkilere sebep olmaktadır.

1.4.2.2. Siber güvenlik endüstrisi

Yenilikler bağlamında bir diğer oluşum ise, siber güvenlik endüstrisidir. Siber güvenlik sektörü, siber uzayın sürekliliğini ve güvenliğini sağlamayı amaçlamaktadır. Devletler, siber tehditler konusunda önlemler alabilmek için çeşitli siber güvenlik merkezleri kurmaktadır. Gerçekleştirdikleri faaliyetleriyle siber güvenlik alanında ileri düzey rekabete ve kabiliyet üstünlüğüne sahip ülkelerin, siber uzaydaki hâkimiyet derecesinin doğru orantılı bir şekilde arttığı iddia edilebilir. Bu anlamda, "gelişmiş ülkeler gelişmekte olan ülkelere kıyasla siber uzayda daha fazla hâkimiyete sahip midir?" sorusu tartışmalı bir soru olmaktadır. Burada vurgulanmak istenen nokta, siber uzaydaki güvenlik kontrolünü sağlayan araçların, anlaşmazlıklar ve savaşlar karşısında güçlü etkilere sahip olacak şekilde dönüştürülebilmesidir. Bu tez çalışmasının konusu olan siber normlar ise, bu kritik araçlardan biri olmakta ve devletler arasında güçlü bir rekabet unsuruna dönüşmektedir. Bu noktada ülkeleri ileriye taşıyan kısım, siber uzayı yeni bir dünya olarak kabul edip bu alana adapte olabilmek için gerekli teknolojik dönüşümleri gerçekleştirmek üzere ulusal çabayı eşit bir şekilde dağıtarak harekete geçmeleridir. "Siber uzay neler sunmaktadır ve neler sunacaktır?" sorusuna cevap verebilmek için farkındalığa ulaşmak üzere, araştırma ve geliştirme yoluyla ülke içindeki tüm aktörlerin eyleme geçmesi gerekmektedir. Siber uzayın temel bileşeni olarak insan unsurunun söz konusu olması; insan doğasındaki merak duygusunun bu alanda kullanılmasıyla birlikte insan-bilgi-teknoloji üçlüsünü mevcut alanda aktifleştirerek yenilikleri ve buluşları kolaylaştırmak için imkân sağlayacaktır. Burada aktörlere düşen en önemli nokta sorumluluk alınmasıdır. Tıpkı fiziksel dünyanın işleyişi için tüm sektörlerin aldığı sorumluluklar gibi, siber uzay alanındaki sektörler de belirli sorumluluklara sahip olmalıdır. Zira belirsizliklerin hâkim olduğu bu yeni dünyada rekabete uyum sağlanabilmesi için tüm sektörlerin kendi yönünü belirlemesi, o yönde lider olması ve rekabet edebilmeyi ve büyümeyi teşvik etmesi gerekmektedir. Ancak avantaj bağlamında değerlendirildiğinde; bilgi ve iletişim teknolojileri bağlamında daha uzun bir

geçmişe ve sağlam bir altyapıya sahip olan ülkelerin, AR-GE ve yenilikler anlamında diğer ülkelere oranla daha avantajlı olduğu iddia edilebilmektedir (Mbanaso ve Dandaura, 2015: 22).

1.4.3. Siber Uzaydaki Zayıflıklar, Tehditler ve Riskler

Siber uzaydaki fırsatlar ve yeniliklerin yanı sıra; zayıflıklara, tehditlere ve risklere de değinmek gerekmektedir. Siber uzayın sürekli geliştiği barizdir; öyleyse ondan kaynaklanan tehditlerin ve zorlukların da gelişmesini beklemek şaşırtıcı olmayacaktır. Fiziksel ve sanal bileşenler arasındaki etkileşim sonucu ortaya çıkan karşılıklı bağımlılık; öngörülemeyen zayıflıklara, tehditlere ve risklere yol açmaktadır. Bahsedilen bu açıklar; yazılım, donanım ve insan faktörünü kapsamaktadır. Yazılım bağlamındaki tehditler içerisinde; virüsler, solucanlar, kullanıcının bilgisi dışında kişisel veriler toplayan casus yazılımlar, korsanlık amaçlı programlar, yetkisiz kodlar, protokol istismarları bulunmaktadır (Mbanaso ve Dandaura, 2015: 20). Donanım kısmında ise, Truva atı virüsü yer almaktadır. Bu virüs; istenmeyen, kötü niyetli, önceden tasarlanmış bir şekilde elektronik devrelere yerleştirilerek değişikliklere sebep olmaktadır.

Bir diğer faktör ise, insan faktörüdür. İnsan faktörüne bağlı olarak içeriden veya dışarıdan tehditler ortaya çıkabilmektedir. Kötü niyetli eylemler ortaya çıkabileceği gibi, kasti olmayan eylemler sonucu da yolunda gitmeyen durumlar oluşabilmektedir. Eylemlerin tehdidi bir yana, eylemsizlik de bir tehdit olarak yerini almaktadır (Mbanaso ve Dandaura, 2015: 20). Zira öngörülemeyen tehditlerin ve risklerin olduğu bu sahada; planlama, tasarım, uygulama veya işletimde eylemsiz olmak insan faktörünün getirdiği zayıflıklardan biridir. İnsanın getirebileceği risklere bağlı olarak, bu faktörün saf dışı bırakılması öne sürülebilir. Ancak insan eliyle inşa edilen ve bileşenlerinden birinin insan olduğu siber uzayda bu mümkün görünmemektedir. Bilgi sistemlerinde insan kavramı esastır. Zira bazı öznel kusurlar ortaya çıksa da, tüm bu sistemleri tasarlayan, çalıştıran ve yönetenler insanlardır. İnsanın olduğu yerde hata ve kusur kaçınılmazdır; ancak bu hata ve kusurlar güvenlik açıklarını yaratmaktadır. İnsana olan ihtiyaç ve bu ihtiyaç sonucu oluşan güvenlik boşluğu düşünüldüğünde, mevcut durumda bir dilemma ortaya çıktığını öne sürmek mümkündür. Dolayısıyla bu dilemmanın da etkisiyle, belirsizliklerin hâkim olduğu siber uzayda öngörülemeyen riskler artmaktadır.

Tablo 3. BM Hükümet Uzmanları Grubu Raporlarına Göre Devlet ve Devlet-Dışı Aktörler Tarafından Bilgi ve İletişim Teknolojilerinin Kötüye Kullanılmasını İçeren Olaylar

Siber saldırı araçları	**Eksik veya yanlış bilgilendirme**	**Casusluk**	**Fiziksel altyapıyı etkileyen siber saldırılar**	**Siber altyapıyı etkileyen fiziksel saldırılar**
Trojan	Propaganda	Bilgi almak için hedeflerin gizlice gözetlenmesi	Nükleer enerji santraline siber saldırı	Veri merkezlerinin bombalanması
Solucan	Sahte haber	Endüstriyel sırların çalınması	Elektrik şebekesine siber saldırı	**Denizaltı kablolarını kesmek**
DOS – hizmet engelleme	Gizli bilgilerin sızdırılması	Gizli belgelerin çalınması	Ulusal bankacılık sistemine siber saldırı	Elektro-manyetik silahlar
Fidye yazılım				

Kaynak: BM Silahsızlanma İşleri Ofisi, Cyberdiplomacy Course, 2020

Bilgi ve iletişim teknolojilerinin kullanımı birçok fırsatı da beraberinde getirmekte ve uluslararası arenada artan bir öneme sahip olmaktadır. Ancak diğer yandan potansiyel bazı tehditlere yol açtığını ifade etmek gerekmektedir. Küresel düzeyde bilgi ve iletişim teknolojilerinin kullanımında kötücül vakalarda artış söz konusudur. Bu artışı sağlayanlar ise, hem devletler hem de devlet-dışı aktörlerdir. Bilgi ve iletişim teknolojilerinin kötü niyetli kullanımı tüm devletler için risk oluşturmaktadır. Uluslararası barış ve güvenliğe zarar verebilme potansiyeline sahip bu risklerin incelenmesi gerekmektedir (BM Silahsızlanma İşleri Ofisi, 2019).

Günümüzde yüzleştiğimiz tehditler konusunda Benjamin Ang'ın öne sürdüğü şu üç tehdit önemlidir:

- Nesnelerin İnterneti teknolojisindeki güvenlik açığı
- Siber güvenlik konularından ziyade, teknolojideki ilerlemelere ve gelişmelere odaklanılması
- Hedef kitlenin davranışını etkilemek için güç kullanımını ifade eden etki operasyonlarında siberin kullanılması. Bu operasyonlarda siberin kullanılmasıyla; insanların hedef alınması ve yanlış bilgi aktarılması konusunda endişeler ortaya çıkmaktadır (BM Silahsızlanma İşleri Ofisi, 2019).

BM Silahsızlanma İşleri Ofisi'nin belirttiği üzere; insan unsuru, bilgi ve iletişim sistemlerinde en yüksek riski oluşturan unsurdur. Diğer bir deyişle, sistemdeki tüm sorunlar teknik değildir. İnsanlar, bilgisayar korsanları tarafından bir sisteme erişim sağlayabilmek için sömürülmektedir. Bu saldırılara "sosyal mühendislik saldırıları" adı verilmektedir. En yaygın toplum mühendisliği saldırı türleri arasında oltalama (*phishing*) ve hedefli oltalama (*spear phishing*) teknikleri yer almaktadır. Sıradan bir oltalama saldırısı şu şekilde gerçekleşmektedir: Kişinin kullanıcı hesaplarından birine, bankadan veya çevrimiçi hesaplardan bilgi güncellemesi şeklinde e-posta gönderilerek bankacılık bilgileri veya oturum açma bilgiler istenmektedir. Asılsız iddialar ile kişiler kandırılmakta ve bunun sonucu ise, kişinin hassas bilgileri ele geçirilmektedir. Daha tecrübeli kişiler ise, hedefli oltalama tekniğini kullanmaktadır. Bu teknikte, bireyler tanıdıkları ve güvendikleri birinden e-posta aldıklarını sanmaktadır; ancak e-posta sahtedir. Hedefli oltalama yöntemi, ağa sızmak ve hassas bilgileri çalmak için sıklıkla kullanılmaktadır (BM Silahsızlanma İşleri Ofisi, 2019). İki yöntem arasındaki farka göre; oltalama saldırıları, rastgele kişilere toplu e-postalar atılarak gerçekleştirilirken; hedefli oltalama ise, belirli bir kişinin hedeflenerek onun hakkında bilgi toplanması ve böylece daha ikna edici bir yöntemle e-posta atılması yoluyla gerçekleşmektedir (Editör, 2016).

E-posta temelli saldırılarda kişileri yazılımı indirme veya sistemdeki açıkları aktifleştirme konusunda harekete geçiren Trojan virüsü, kullanıcının bilgisayarında bir kez aktive edildiğinde ardından gelecek birçok saldırıya kapı açmaktadır. Saldırgan, aktifleşmiş virüs sayesinde bilgisayardaki birçok veriye sızabilmenin yanı sıra, sızılan bilgisayarı diğer bilgisayarlara saldırmak için bir platform olarak kullanabilmektedir. Diğer bilgisayarlara adeta bir köprü geçişi sağlayan bilgisayara "bot" adı verilmektedir. Tecrübeli bir saldırgan, Trojanları onlarca hatta yüzbinlerce bilgisayarı içeren ağlar oluşturmak için kullanabilme potansiyeline sahiptir. Bunu gerçekleştirdiğinde oluşan ağ zincirine "botnet" denmektedir

(BM Silahsızlanma İşleri Ofisi, 2019). 2013 BM Hükümet Uzmanları Grubu Raporuna göre, devletler veya devlet-dışı aktörler tarafından botnet gibi kötücül araçların ve tekniklerin geliştirilmesi ve yayılması sonucu kasti olmasa da gerginlikler oluşma riski söz konusudur. Buradan çıkarılabilecek ders, bilgi ve iletişim teknolojilerinin kullanımıyla ilgili olarak kabul edilebilir devlet davranışı oluşturmak üzere ortak bir anlayışa sahip olunmasının gerekliliğidir. Aksi takdirde bu durum uluslararası barış ve güvenliğe zarar verebilme potansiyeline sahiptir (BM Genel Kurulu, 2013).

Siber teknolojinin etkisi üzerine bir örnek vermek gerekirse, dünyanın üçte ikisini kaplayan okyanusların, petrolden bile daha değerli bir kaynağa ev sahipliğini yaptığını söylemek mümkündür. Deniz tabanı boyunca uzanan 300 civarı okyanus aşırı fiber optik kablo vardır. Bu okyanus aşırı fiber optik kablolardan ses ve İnternet trafiğinin %95'i geçmektedir. Uluslar doğru önlemler almadığında gerçekleşen saldırılar sonucu kesintiye uğrayabilecek bu kablolar, askeri iletişim verilerini ve yılda 4 trilyon dolardan fazla yapılan finansal işlem verilerini içermektedir. Temelleri, Atlantik Telgraf Şirketi'nin Atlantik Okyanusu üzerinden ilk telgraf iletişimini kurduğu 1858 yılına dayanan denizaltı kabloları; bugün dünya üzerindeki tüm okyanuslara uzanmış olup, telefon görüşmelerinden sosyal medya yayınlarına ve diplomatik mesajlara kadar birçok veriyi içermektedir. Uluslararası ilişkilerde istikrarın, tahmin edilebilirliğe ve saldırıları tespit edip uygun şekilde müdahale etme yeteneğine bağlı olduğu göz önüne alındığında; kırılma konusunda hassas oldukça hassas olan denizaltı kabloları konusunda ortaya çıkabilecek tehditler, günümüz istikrarını baltalama riski taşımaktadır (Clark, 2016: 237).

Dünya çapında İnternete bağlı cihazların sayısı arttıkça ve cihazların siber ağlara ve birbirlerine olan bağlantısı arttıkça, bunu manipüle edecek saldırıların da beraberinde gelebileceği göz önünde bulundurulmalıdır. Dijitalleşmenin artışıyla birlikte, bireylerin ve toplumun güvenliğine tehdit oluşturan kötü niyetli eylemlerde de artış beklentisi söz konusu olmaktadır. Van Der Meer'e göre; enerji tedarik sistemleri, hastaneler, nükleer tesisler, hava yolu, demiryolu trafiği, selden korunma ve su idare sistemleri veya ödeme sistemlerine erişebilmeyi başarabilen siber teröristlerin ciddi tahribatları söz konusu olacaktır. Bu bağlamda düşünüldüğünde, genel olarak terörizm için geçerli olan tehlike algısının siber terörizm için de geçerli olması gerektiği ifade edilebilmektedir. Siber terörist saldırıların olasılığı istatistiki verilere göre daha düşük olsa da, olması durumunda yıkıcı etkilerinin siber olmayan terörist saldırılara göre daha ağır olması beklenmektedir. Zira en güçlü geleneksel silah sistemleri bile, siber teknolojiye sahip bir rakip tarafından engellenebilme riskine sahip olduğunu öne sürmek mümkündür (Van Der Meer, 2015b: 195-196).

BÖLÜM 2: STRATEJİK SOSYAL İNŞA SÜRECİNDE SİBER NORMLARIN ÖNE ÇIKAN UNSURLARI VE TARTIŞILAN SİBER YÖNETİŞİM MODELLERİ

2.1. Sosyal İnşacılık

Siber uzayın bilinmezliğinin ve kuralsızlığının getirdiği tehditlerle mücadele edebilmek için çeşitli yöntemlere başvuran devletler bu rekabet ortamında güç mücadelelerine gitmektedirler. Devletlerin güç mücadeleleri çerçevesinde değerlendirildiğinde bu çalışmada, siber uzayda uygun devlet davranışını belirlemeyi amaçlayan norm formasyonunun bir mücadele aracı haline geldiği öne sürülmektedir. Norm kavramının bizzat kendisinin bir rekabet alanı haline gelmesinin söz konusu olduğu devletlerarasındaki bu mücadele doğrultusunda normların bir inşa sürecinden geçtiğini söylemek mümkündür. Bu tez çalışmasında, siber normların geçtiği sosyal inşa sürecinin, aktörlerin politikalarına hizmet etmesi çerçevesinde stratejik bir sosyal inşa süreci içerisinde evirildiği iddia edilmektedir. Bahsi geçen inşa sürecini analiz edebilmek için çalışmada Sosyal İnşacılık teorisinden faydalanılacaktır.

Finnemore ve Sikkink'e (1998) göre stratejik sosyal inşa; norm girişimcileri veya norm önderleri olarak adlandırılan aktörlerin, kendi faydalarını maksimize edebilmeleri doğrultusunda diğer aktörlerin faydalarını da değerlendirmeye alarak araç ve amaç ilişkisi üzerine detaylı bir hesaplama yapılması çerçevesinde normların şekillendirilmesidir. Stratejik sosyal inşaya başvurulmasının sebebi, norm oluşturma sürecinin oldukça karmaşık olmasıdır. Bu bağlamda araç ve amaç ilişkisine yönelik ayrıntılı bir hesaplama yaparak bu karmaşık süreci anlamlandırmaya çalıştıkları için norm girişimcilerinin rasyonel aktörler olduğunu belirtmek gerekmektedir (Finnemore ve Sikkink, 1998: 910).

Sosyal İnşacılık, Soğuk Savaşın bitişiyle birlikte düşünsel unsurları da uluslararası siyasete dahil eden, uluslararası ilişkileri bir sosyal olarak inşa edilen bir alan olarak gören teorik bir yaklaşımdır. Sosyal İnşacılık kavramının uluslararası ilişkiler literatürüne kazandırılması, 1989 yılında Nicholas Onuf'un, insanların sosyal gerçekliği inşa ettiğini ve o gerçekliğin de sosyal bir karaktere sahip insanları yapılandırdığını iddia ettiği "*The World of Our Making: Rules and Rule in Social Theory and International Relations*" adlı kitabıyla gerçekleşmiştir (Onuf, 1989: 1).

Sosyal İnşacılığın savunucularından Nicholas Onuf'a göre, İnşacılığın temeli insanların sosyal varlıklar olması ve eğer sosyal ilişkiler olmasaydı insan olunamayacağı iddiasına dayanmaktadır. Dolayısıyla söz konusu iddiaya göre, insanı insan yapan etmenin sosyal ilişkiler olduğu öne sürülmektedir. Bahsedilen sosyal ilişkileri oluşturan ve buna bağlı olarak insanı bugünkü haline dönüştüren eylem ise, "konuşmak"tır (Kubalkova, Onuf, ve Kowert, 1998: 59).

Sosyal İnşacılık; insanların toplumu, toplumun ise insanları oluşturduğunu öne süren karşılıklı bir sürece sahiptir. Doğrunun bir noktasında insanların, bir noktasında ise toplumun olduğu düşünüldüğünde, süreci anlamlandırmaya iki ucu birbirine bağlayan orta noktadan başlanması gerekmektedir. Onuf'a göre, insanları ve toplumu birbirine

bağlayarak karşılıklı olarak birbirlerini oluşturmaya yönlendiren orta nokta "sosyal kurallar"dır (Kubalkova vd., 1998: 59).

Şekil 1. Sosyal İnşacılık Süreci

Kaynak: (Kubalkova v.d., 1998: 59)

İnsanlara ne yapılması veya ne yapılmaması gerektiğini söyleyen bir ifade olarak tanımlanan kurallar, insanların davranışları için ortaya konulan bir standart olmakta ve davranışların standartlarla eşleştirilmesini gerektiğini söyleyerek bir gereklilik durumu ortaya çıkarmaktadır. Kurallara uyulması veya uyulmaması fark edilmeksizin, insanların kurallara yönelik eylemleri "pratik" olarak adlandırılmaktadır. Bu bağlamda, kuralların içeriğini öğrenebilmek için pratikte insanların eylemlerine bakılmasının çoğu durumda yeterli olacağını öne sürmek mümkündür (Kubalkova vd., 1998: 59).

Şekil 1'de de görüldüğü üzere insanlar ve toplumlar şeklindeki iki noktayı birbirine bağlayan kurallar, Sosyal İnşacılar tarafından "ajanlar (*agents*)" veya "temsilciler" olarak ifade edilmekte ve toplumdaki aktif katılımcıların kimler olduğunu ifade etmeye yardımcı olmaktadırlar. İnsanlar ise, toplumda kuralların olduğu durumlara katılmayı mümkün kıldıkları sürece temsilciler olarak görülmektedirler. Diğer bir deyişle, temsilcilerin bireyselle sınırlandırılmadığı görülmektedir. Zira temsilcilik bireysel değil sosyal bir durum olarak ifade edilmektedir. Bu bağlamda düşünüldüğünde, insan topluluğundan oluşmalarından ve belirli bir ülke adına hareket etmelerinden dolayı, hükümetlerin sosyal bir yapı olduğunu söylemek mümkündür (Kubalkova vd., 1998: 60).

Sosyal İnşacılığa göre, kurallar temsilcilere seçenekler sunmaktadır. En temel seçim, kurala uymak ve dolayısıyla kurala bağlı olarak yapılması gerekenin yapılması veya yapılmaması gereken şeyin yapılmamasıdır. Burada uygulanılması gereken nokta, seçimi yapanın insan olmasıdır. Zira sadece insanlar, seçim yapacak ve aldıkları kararların olası sonuçlarını düşünecek zihinsel altyapıya sahiptir. Bu seçimler hangi amaçla gerçekleştirilirse gerçekleştirilsin, olası sonuçlar sosyal yapıyı etkilemektedir. Siber uzayda da aktörlerin birey düzeyinde değerlendirilmesi ve onların hareketlerini sosyal yapıya dönüştürmesi gibi unsurlar bu çerçevede bize önemli bir noktayı göstermektedir. Temsilciler toplumun ortaya koyduğu kurallar çerçevesinde belirlenmiş hedefleri yerine getirmek için harekete geçmektedirler (Kubalkova vd., 1998: 60). Siber uzay çerçevesinde değerlendirildiğinde bireyin hem etken hem de edilgen olması ciddi bir güvenlik unsuru haline gelmesi devletlerin bu alanda stratejik hedefler ortaya koymasına ve normları inşa etmesine sebebiyet vermektedir.

Alexander Wendt'e göre "*anarşi, devletlerin ondan ne anladığıdır"* (Wendt, 1992). Bu bağlamda siber uzayın amorf yapısındaki varlık gösteren tehditler, aktörlerin siber uzayı nasıl algıladığına bağlı olmaktadır. Zira Sosyal İnşacılığa göre dünya ve dünya hakkında bildiklerimiz sosyal olarak inşa edilmektedir. Örneğin, beş yüz İngiliz nükleer silahının mı, yoksa beş Kuzey Kore nükleer silahının mı ABD için tehdit olduğu sorusuna Alexander

Wendt'in cevabı Kuzey Kore'nin tehdit olduğu yönündedir (Theys, 2018). Zira maddi unsurların yanında düşünsel unsurların da tehdit algılamalarını etkilediğini ifade etmek gerekmektedir. Buradaki esas nokta, maddi unsurların perspektifini belirleyen "algı" kavramıdır.

Sosyal İnşacılık kuramının kurucusu Alexander Wendt'in "Uluslararası Siyasetin Sosyal Teorisi" adlı kitabında yer aldığı üzere, Sosyal İnşacılığın hemfikir olunan iki temel ilkesi bulunmaktadır. Birinci ilkeye göre, insan topluluğunun sahip olduğu inşalar, maddi güçlerden ziyade maddi ve düşünsel unsurlar tarafından ortak olarak belirlenmektedir. Düşünsel unsurları geri plana atan realist yaklaşımlara bir tepki olarak her iki unsurun da önemli olduğunu ifade eden İnşacılık, insan topluluğu kavramına yaptığı vurguyla sosyal niteliğini vurgulamaktadır. Geleneksel yaklaşımlara meydan okuyarak yeni bir inşayı savunması sebebiyle İdealizmi andırdığını söylemek mümkündür. İkinci bir ilke ise, belirli bir amaca sahip aktörlerin sahip oldukları kimlik ve çıkarların doğa tarafından kendiliğinden verilmesinden ziyade, maddi ve düşünsel unsurlar tarafından inşa edildiğini öne sürmektedir. Sosyal İnşacılık, yalnızca materyalist bakış açısını merkeze almayıp iki bakış açısını da birlikte ele almasıyla ve doğada bulunan unsurların ötesine geçerek diğer etkenleri de vurgulamasıyla bütüncül bir yaklaşım olarak kabul edilmektedir (Wendt, 2016: 15).

Rasyonalizm akımı tarafından göz ardı edilen güvenliğin ontolojik ve epistemolojik olarak farklı yönlerini dikkate alan sosyal inşacılar, uluslararası sistemdeki aktörlerin çıkarlarında; normların, kimliğin ve bu unsurlara bağlı olarak ortaya çıkan sosyal etkileşim sürecinin önemini vurgulamaktadırlar (Karacasulu ve Uzgören, 2007: 36). Ancak sosyal inşacılara göre normlar eylemleri belirlememekte, normların değişmesi yalnızca devletlerin çıkarlarını değiştirerek yeni çıkarlar ortaya çıkarmaktadır (Karacasulu ve Uzgören, 2007: 37). Realist yaklaşımın aksine maddi yapıların yanı sıra düşünsel unsurların da olduğunu öne süren Sosyal İnşacılık yaklaşımına göre, sosyal etkileşime bağlı olarak maddi yapıların sosyal anlamları yeniden tanımlanabilmektedir. Siber uzay bağlamında düşünüldüğünde, ABD'nin siber uzayda tehdit olarak gördüğü faktörler ile Çin'in tehdit olarak gördüğü faktörler devletlerin kültürlerine ve kimliklerine göre değişiklik göstermektedir. "Tehdit", devletlerin bu kavramdan anladığı şeydir ve dolayısıyla sadece materyal unsurlar üzerinden değil kültür ve kimlikler çerçevesinde sosyal olarak inşa edilmektedir.

Norm kavramının kullanımı 1980'lere kadar uzansa da, normların disiplinde önem kazanmaya başladığı dönem Sosyal İnşacılık yaklaşımının uluslararası ilişkilerde pozitivizm ve post-pozitivizm arasındaki tartışmalar ile birlikte etkisini arttırmasıyla birlikte gerçekleşmiştir (Tabak, 2014: 20). Norm, sosyal bir kavramdır. Bu sosyal niteliğini, aktörün bağlı olduğu grup tarafından gerçekleştirilen yaptırımlardan ve beklentilerin grup içerisinde paylaşılmasından almaktadır (Tabak, 2017: 140-141). Bu nedenle bu tez çalışmasında, temelinde sosyal bir kavram olan norm kavramından yola çıkılarak siber norm oluşturma sürecini açıklayabilmek amacıyla Sosyal İnşacılık teorisinden yararlanılmıştır.

2.2. Normların Siber Uzay Çerçevesinde Artan Önemi

Devletlerin birçoğu siber uzayı tehdit, güvensizlik ve istikrarsızlığın hâkim olduğu bir alan olarak değerlendirmektedirler. Sınırları olmayan siber uzayın belirsiz yapısı, pek çok unsurun tehdit halini almasına ya da devletler tarafından tehditler olarak algılanmalarına sebebiyet vermektedir. Zira siber uzayda varlık gösteren tehditlerin, nükleer enerji santrallerine saldırı veya ulusal bankacılık sistemine saldırı gibi fiziksel dünyayı etkileyen yönü de göz önünde bulundurulduğunda, devletler açısından kritik ve stratejik bir operasyonel alan olduğunu söylemek gerekmektedir.

Katzenstein'e göre norm, sosyolojik anlamda "*belirli bir kimliğe sahip aktörlerin uygun davranışları için kolektif beklentiler* (Katzenstein, 1996: 5)" olarak tanımlanmaktadır. Bu tanımdan yola çıkılarak bir normun varlığı için kimlik, davranış, kolektif beklentiler ve uygunluk olmak üzere gerekli dört bileşen olduğunu öne sürmek mümkün olacaktır (Finnemore ve Hollis, 2016: 439). Bir normun etki yaratabilmesi için aktörlerin kendilerini bir toplulukla özdeşleştirmeleri gerekmektedir; "kimlik" ise, normu oluşturan aktörün sahip olduğu grubu ifade etmektedir (Finnemore ve Hollis, 2016: 439). Sosyal İnşacılık yaklaşımında da önemli kavram olan kimlik çıkarları, çıkarlar ise politikayı belirlemektedir.

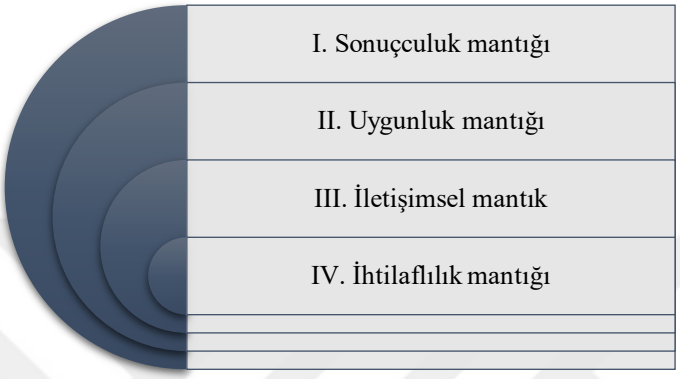
Aktörlerin kendilerini özdeşleştirdiği, aidiyet içeren gruplara örnek olarak verilebilecek olan BM GGE, siber uzayda norm oluşturmak isteyen tüm aktörlerin sahip olduğu bir grubu ifade ederken; ASEAN ise, bölgesel bağlamda siber norm öneren bir grup olarak uluslararası sistemdeki yerini korumaktadır. Diğer yandan özel şirketlerin, STK'ların veya iki devletin bir araya gelerek norm oluşturmasının da aynı şekilde aidiyet içeren bir grup olarak değerlendirilmesi mümkündür. Bir normun varlığı için gerekli ikinci bileşen olan "davranış", topluluk normunun gerektirdiği belirli eylemleri ifade etmekteyken; bir diğer bileşen olan "kolektif beklentiler" ise, normu oluşturan aktörün yer aldığı grubun üyeleri tarafından ortaya konulan çıkarları ifade etmektedir. Son ve en kritik bileşen ise, norm kavramının anlamıyla özdeşleşen "uygunluk"tur. Bir uluslararası sistemin inşasında uygunluğu belirleyen normlardır, bu nedenle en son ulaşılan nokta uygunluk olacaktır. Beşinci operasyonel alan olan siber uzayda aktörler arası rekabeti oluşturan nokta, esasında uygunluğun tanımlanması üzerine olmaktadır.

Sıklıkla prensipler/ilkeler ya da kanunlar ile aynı cümlede kullanılan normların, bu kavramlardan farklı olmakla beraber onlara bağlı olduğunu da belirtmek gerekmektir (Finnemore, 2017: 441). Bir grubun neyi başarmak istediğine dair bir hedef olan prensiplerin anlaşmalar aracılığıyla ifade edilmesi, normlara göre daha kolaydır. Zira bir hedefe sahip olmak ve uygunluğa giden yolda ortak bir beklentiyi paylaşmak birbirinden farklı şeylerdir. Örneğin, bir grup içerisinde kişisel verilerin gizliliğinin sağlanması bir prensip olabilir, ancak diğer yandan normlar gibi kişisel verilerin gizliliği üzerine ortak bir inanç ve beklenti oluşturmak, bir hedef oluşturmak kadar kolay olmayacaktır. İki kavram arasındaki bir diğer fark ise, normlar belirli aktörleri uygun davranışa açıkça bağlarken; bir prensip, yapılması gerekeni belirsiz bir şekilde tanımlayarak hangi aktörün hangi davranışı gerçekleştirmesi gerektiği noktasında bir muğlaklık oluşturmaktadır (Finnemore, 2017: 2). Bu nedenle şunu söylemek gerekir ki; bir prensip sorumlulukları paylaştırmaktaysa ve bu

anlayışlar belirli aktörler tarafından yaygın olarak paylaşılırsa, bu prensip artık bir norm olagelmiştir (Finnemore, 2017: 2).

Eylemlerin belirli prensipler etrafında şekillendirilmesini öngören normlar, eylem odaklı olmakta ve bu nedenle aktörün davranışıyla ilintili olmaktadır (Tabak, 2017: 154). Tabak'ın "Normlar, Uluslararası İlişkiler ve Dış Politika" adlı makalesinde belirttiği üzere, uluslararası ilişkiler disiplininde normu tetikleyen eylemlerin mantığı dikkate alındığında, eylemler mantıksal açıdan dörde ayrılmaktadır.

Tablo 4. Eylemin Mantığı Üzerinde Yorum Sunan Dört Farklı Eylem Mantığı



Kaynak: (Tabak, 2017: 154)

Makaleye göre (Tabak, 2017) birinci mantık türü olan sonuçculuk mantığı, aktörün kendi çıkarlarını gözetmeye eğilimli olduğunu ve eylemlerin ise, fayda-maliyet ekseninde ve normların zorlaması sonucu oluştuğunu öne sürmektedir. Bu çerçevede düşünüldüğünde, eylemlerin önceden tahmin edilebilir olması bariz olarak görülmektedir. Diğer yandan, bir eylem sadece sonuçculuk mantığıyla ele alındığında, kimlikler, kurallar ve kurumlar gibi aktörlerin davranışı üzerinde önemli bir etkiye sahip olan unsurlar göz ardı edilmektedir. Bu göz ardı durumuna tepki olarak ise, uygunluk mantığı ortaya çıkmakta ve Katgenzstein'in norm tanımında olduğu gibi "*belirli bir kimliğe sahip aktörlerin uygun davranışları için kolektif beklentiler*" biçiminde bir anlayış öne çıkmaktadır (Katzenstein, 1996a). Diğer bir deyişle, aktör açısından bir davranışın norma ve dolayısıyla sahip olunan kimliğe uygunluğunun sağlanması son derece önemli bir nokta olmaktadır. Zira aktör, bağlı bulunduğu grubun kimliği doğrultusunda "doğru şeyi yapmak" için uğraş vermekte; doğru şeyi yapmadığında ise, sosyal ayıplama, kınama ve dışlama gibi reaksiyonlara maruz kalacağını öngörmektedir. Ancak uygunluk mantığı, sonuççuluk mantığında olduğu gibi normların aktör davranışını doğrudan etkilediğini veya eylemlerin önceden belirli olduğunu iddia etmemektedir. Bu mantık türüne göre normlar, aktörlerin davranışları üzerinde yaptırım doğurmak yerine, onlara davranışları konusunda belirli yükümlükler yüklemektedirler. Bunun sağlanması için ise, eylemlerin oluşumu noktasında aktörlere yön göstermektedirler (Tabak, 2014: 157-158).

Tabak'ın makalesine göre (2017), Sosyal İnşacılık, gerçeklerin verili olduğunu reddetmesi ve kurulu olduğunu kabul etmesiyle, uygunluk mantığını benimsemektedir. Sosyal İnşacılık yaklaşımına göre aktörler normları takip ederlerken stratejik bir hesap yapmakta ve çıkarlarını göz önüne almaktadırlar. Burada vurgulanması gereken kritik nokta,

çıkarların da belirli sosyal süreçler sonucu inşa edildiği, dolayısıyla verili olmadığı gerçeğidir. Bu nedenle yukarıdaki tabloda ifade edilen dört farklı eylem mantığının temel bileşeni olan uygunluğun belirleyicisi olan rasyonellik unsurunun Sosyal İnşacılık yaklaşımıyla eşleştiğini iddia etmek mümkündür. Finnemore ve Sikkink'in de öne sürdükleri üzere, normları ve rasyonaliteyi birbirinden ayırmak mümkün değildir (Finnemore ve Sikkink, 1998: 888). Ancak buradaki rasyonalite "doğru şeyi yapma"nın temel olduğu, aktörlerin bağlı oldukları gruptaki kimliklerinin gerektirdiği yükümlülükleri ve grubun beklentilerini karşılama çabasında oldukları normatif bir rasyonalite olarak ifade edilmektedir (Tabak, 2017: 157).

Üçüncü mantık türü olan iletişimsel mantık ise, düzenleyici ve kurucu role sahip eylemi değerlendirirken, aktör tarafından ortaya çıkarılan söylem üzerinden tanımlamakta ve sürecin iletişimsel yönünü merkeze almaktadır. İletişimsel mantığa göre, aktörlerin çıkarları ve tercihleri verili olmamakta, tam tersine söylemler, çıkarlar ve normlar üzerindeki anlamlara yönelik tartışmalar, müzakereler ve iknalar gibi iletişimsel süreçlere göre değişiklik göstermektedir. Bu iletişimsel süreçler sonucu bir uzlaşma sağlandığında, normlar grup üyeleri tarafından paylaşılmış hale gelmiş olmaktadır. Bu bağlamda iletişimsel mantığa göre, normların, kurulan iletişim sonucu ortak bir anlama ulaşmak için bir araç olduğu öne sürülebilmektedir. Eylemlere anlam kazandırmak, tartışmalar ile eylemleri eleştirmek ve uzlaşıya varılması sonucu ise eylemlerin meşru gösterilmesini sağlamak gibi amaçlar, iletişimsel mantığın normlara yüklediği roller olarak ifade edilebilmektedirler. Bu tez çalışmasında üçüncü bölümde incelenecek olan aktörlerin politikaları üzerinde uzlaşıya varılması ve bu anlamda çıkarlarını gerçekleştirmeye çalışmaları norm tartışmalarının bir anlamda fonksiyonel bir rol oynadığı iletişimsel süreçlere işaret etmektedir.

Tabak'ın makalesinde yer alan son mantık türü ise, anlamsal bağlamda iletişimsel mantığa karşı çıkarak herkes tarafından uzlaşmaya varılan bir bilginin olmayacağını savunan ihtilaflılık mantığıdır. Diğer bir deyişle ihtilaflılık mantığına göre, bilme eylemi sübjektif olmakta ve aktörlerin tecrübelerine bağlı olarak oluşmaktadır. Bu nedenle ihtilaflılık mantığı, normların anlamlarının sabit olmadığını savunarak, bilginin, tecrübeler ve iletişimsel süreçler sonucu değişiklik göstermesiyle normların da anlamlarının değişikliğe uğrayacağını savunmaktadır. Kısacası normların özünün ihtilaf içerdiği iddia edilmekte; geçerliliğinin ise sadece spesifik kültürel bağlamlarda mümkün olmasından ötürü, normların evrensel olmadığı öne sürülmektedir. Bu doğrultuda, küresel bir yapı çerçevesinde farklı kültürlerde farklı şekilde algılanabilecek ve insan hakları, ifade özgürlüğü gibi konularda değişken yorumlara kapı açabilecek normların siber alanda şekillendirilmesi ve uygulanması konularının zorluklarını vurgulamak mümkündür.

Bu tez çalışmasında kullanıldığı üzere normların; uluslararası sistemde devletlerin diğer devletlerin haklarını ihlal etmelerini önlemek için uluslararası örgütler çerçevesinde, özel şirketler bağlamında veya devletlerarası ikili anlaşmalar aracılığıyla siber uzayda belirli kurallar ve ilkeler doğrultusunda nasıl davranılacağını belirleyen bir anlayış olarak ifade edilmesi planlanmaktadır. Siber uzayda norm oluşturulması, devletlerin egemenliğinin korunmasını sağlamakta ve aynı zamanda norm oluşturma sürecinde yer alan devletlerin

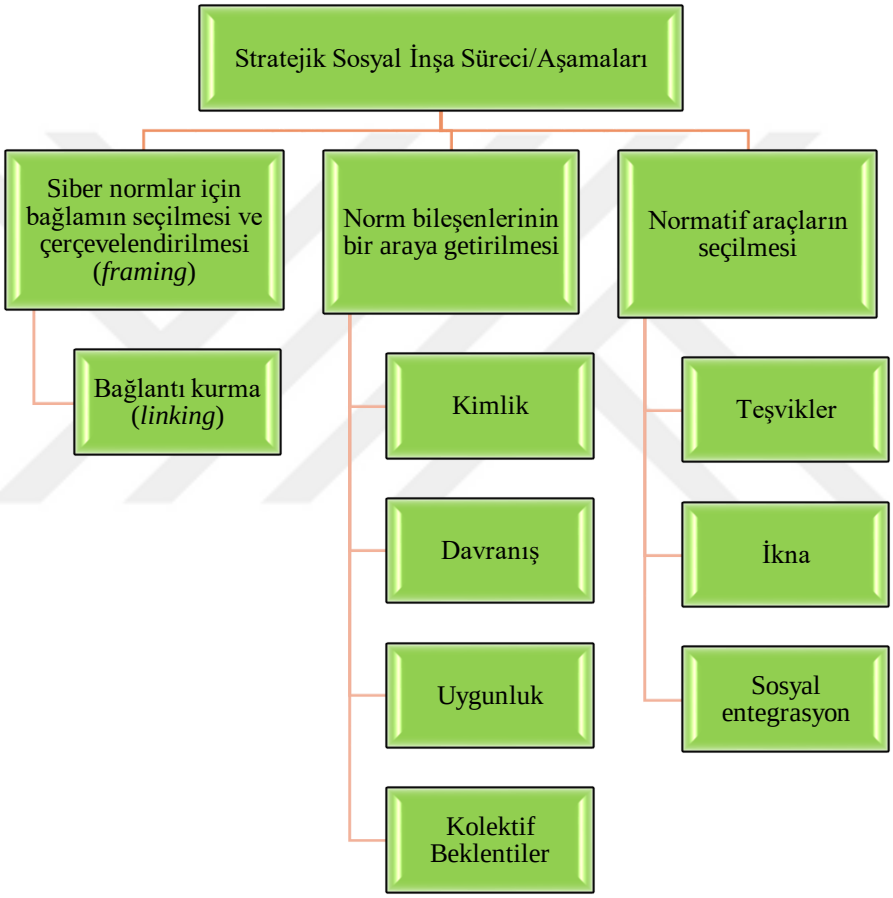
sistemde söz sahibi olmasına izin vermektedir. Devletler siber uzayda; kimlikleri, algıları, çıkarları ve değerleri doğrultusunda dâhil oldukları bu süreçte kendi gerçekliklerini inşa etmektedirler (Romaniuk ve Grice, 2018).

2.3. Siber Normların İnşası

Bu tez çalışmasında, norm oluşturma sürecinin gerçekleşmesi, diğer bir deyişle yeni siber normların geliştirilmesi stratejik sosyal yapının bir uygulaması çerçevesinde ele alınmaktadır.

Finnemore ve Hollis'in (2016) makalesinde ifade edildiği üzere stratejik sosyal inşanın aşamaları üç basamaktan oluşmaktadır.

Şekil 2. Stratejik Sosyal İnşa Süreci/Aşamaları



Kaynak: Finnemore ve Hollis'in (2016) makalesinden yararlanılarak yazar tarafından tasarlanmıştır.

Siber normların stratejik sosyal inşası, çerçeveleme (*framing*) ile başlayan bir süreç olarak kendini göstermektedir. Çerçevelemenin önemini anlayabilmek için bir bilgi ekosistemi olan siber uzayın (Akyeşilmen, 2018: 53); sürekli değişim halinde olan, bilinmezliklerle dolu ve dolayısıyla da geniş bir yelpazeye sahip tehditlerden oluşan bir saha olduğunu belirtmek gerekmektir. Farklı katmanlardan oluşan siber uzayda aktörler de devletten bireye, terör örgütlerinden STK'lara ulaşan bir yelpazede çeşitlilik arz etmektedir. Aktör, teknoloji ve konular açısından bağlam farklılığı gösteren siber uzayda tehditleri sınıflandırabilmek için siber norm girişimcilerinin veya diğer bir ifadeyle siber norm önderlerinin sorunlar arasındaki öncelikleri belirlemesi ve o sorunu çerçeveleyerek

sınırlaması gerekmektedir. Norm girişimcilerinin, odak noktasına alınan problemle mücadele edebilecek veya edemeyecek grupları belirlemesi kritik bir noktadır. Zira norm teşvik sürecinin içinde yer alan aktörler çerçevelemeyi doğrudan etkilemektedir. Bu nedenle çerçevelemenin dikkatli ve titiz bir şekilde yapılması önem arz etmektedir.

Çerçevelemenin ilk aşamada yer almasının ve bu denli önemli olmasının sebebi, bir problem ile bağlantılı diğer sorunlarla da bağlantı kurulması (*linking*) ve ilişkilendirilebilmesidir. Örneğin, yapılan bir siber saldırı ekonomik anlamda zarara sebep olsa da aynı zamanda hükümetin kurumlarına verdiği zararlarla birlikte ulusal güvenlik gündemine de dâhil olabilmektedir. Burada dikkat çeken nokta, Sosyal İnşacılık yaklaşımında yer alan söylem kavramıyla benzerlik göstermesidir. Başka bir örnek vermek gerekirse, bir devlet başkanı, yapılan saldırıyı ulusal güvenliğe yapılan yaşamsal bir saldırı olarak tanımlarsa söylemsel açıdan konuyu güvenlik meselesi haline getirmektedir. Bu nedenle norm oluşturma sürecindeki stratejik sosyal inşada, çerçeveleme ilk aşamada yer almaktadır. Stratejik sosyal inşanın ilk aşaması olan çerçeveleme; siber güvenlik alanındaki birincil problemi belirlemekte, problemi çözebilecek ve çözüm sürecinin dışında kalacak grupları tespit etmekte, ardından problemin ilintili olduğu diğer konular ile olan bağlantıyı sağlamakta ve son olarak problemi belirli bir bağlamda kavramsallaştırarak çerçeveleme sürecini tamamlamaktadır.

Stratejik sosyal inşa sürecindeki ikinci aşama ise, normun içeriğini oluşturmaktan geçmektedir. Bu oluşumda yer alan unsurlar; kimlik, davranış, uygunluk ve kolektif beklentilerin karşılanması olmaktadır. Uluslararası ilişkilerin çeşitli yönlerini etkileyen normların, siber uzayı düzenlemek için siber normlar adı altında kümelenerek norm oluşturma sürecini canlandırmasının temelinde, bu yeni operasyonel alanda kuralları koymak isteyen devletlerin rekabeti yatmaktadır. Hava, kara, deniz ve uzayda devletlerin sınırlarını belirleyen fiziksel etkenler mevcutken, siber uzayda fiziksel sınırların bulunmaması sebebiyle, devletler faaliyetlerini yürütürken diğer devletlerin egemenliğini dikkate almak zorundadır. İnterneti ve siber faaliyetleri harekete geçiren fiziksel altyapı ülkelerin egemen topraklarında bulunsa da, bulunmadığı durumlar da söz konusu olmakta veya "anonimlik" sebebiyle yapılan saldırıların nerelerden kaynaklandığı belirlenememektedir. Bu bağlamda egemenliğin temsili olarak devletlerin, siber uzayda düzeni sağlamak için belirli kurallara, diğer bir deyişle normlara ihtiyaç duyması söz konusu olmaktadır. Burada vurgulanmak istenen nokta, normların sosyal bir inşa sürecinden geçtiğidir. Zira normlar verili olmamakta ve aktörlerin çıkar ve kimliklerine bağlı olarak bir süreç içerisinde inşa edilmektedir.

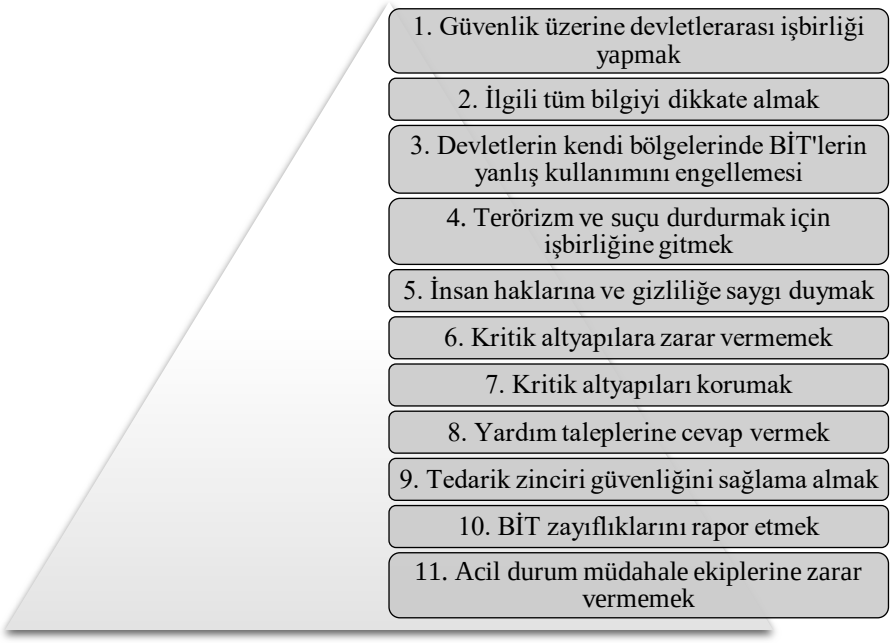
Stratejik sosyal inşa sürecindeki üçüncü aşama ise, teşvikler, ikna, sosyal entegrasyondan oluşan normatif araçların seçilmesi olarak belirtilmektedir. Aktörler, özellikle de güçlü devletler, teşvik aracı yoluyla destekledikleri normları yaymak için ellerinde geniş kaynaklara sahiptirler. Bu kaynakların kullanılmasının yanı sıra, norm teşvikinde her yerde bulunan ikna aracını da bilgi alışverişi ve tartışma gibi bilişsel süreçler yoluyla kullanarak normların yayılmasını ve içselleştirilmesini sağlamaktadırlar. Somut teşviklerin veya bilişsel çerçevelerin ve bağlantıların ötesinde, aktörler arası ve aktörler içinde kurulan sosyal ilişkiler de normlar üretebilmekte ve bu normların yayılmasına katkı sağlamaktadır.

Bu nedenle stratejik sosyal inşa sürecinde sosyal entegrasyon da normatif bir araç olarak ele alınmaktadır.

Uluslararası siyasetteki siber norm oluşturma arzusu yeni ortaya çıkmamıştır. 1998 yılında Rusya tarafından BM Birinci Komitesi'ne sunulan "Güvenlik bağlamında bilgi ve telekomünikasyon alanındaki gelişmeler" başlıklı taslak, bilgi ve iletişim teknolojilerinin uluslararası güvenlik anlamındaki geçmişinin 1998 yılına kadar uzanmasını ortaya koyması açısından önem arz etmektedir. O dönemden beri BM Hükümet Uzmanları Grubu tarafından bilgi ve iletişim teknolojilerinin kullanılmasıyla ortaya çıkan tehditler, uluslararası güvenlik bağlamında vurgulanarak devletlere belirli tavsiyeler verilmektedir. Bu tavsiyeler ile birlikte ortaya çıkan raporlar zaman içerisinde normatif bir çerçeve oluşturulmasına doğru bir yol izlenmesini sağlamıştır. 2015 yılında BM Genel Kurulu tüm üye devletlere bilgi ve iletişim teknolojilerinin kullanımında rehberlik edebilme çağrısında bulunacak bir karar çıkarmıştır. 70/237 sayılı bu karara göre, tüm üye devletlerin bilgi ve iletişim teknolojileri doğrultusunda izledikleri politikalar ve aldıkları kararlar konusunda BM Hükümet Uzmanları Grubu aracılığıyla öneriler ve değerlendirmeler yapılacaktır (BM Genel Kurulu, 2015).

BM Hükümet Uzmanları Grubu'nun 2010, 2013 ve 2015 yıllarındaki raporlarında, siber uzaydaki "sorumlu devlet davranışı" üzerine ülkelerin fikir birliğine vardıkları 11 norm bulunmaktadır. Bu normların uluslararası hukukun siber uzayda nasıl uygulanacağını belirlemede önemli önemli bir rol oynadığı unutulmamalıdır. Zira normlar uluslararası hukukun sadece bir parçasıdır.

Tablo 5. BM Hükümet Uzmanları Grubu Tarafından Fikir Birliğine Varılan 11 Norm



Kaynak: Avustralya Hükümeti Dış İşleri ve Ticaret Departmanı, UN Norms Responsible Bookmark. 2021

Tablo 5'te yer alan ve tez çalışmasının üçüncü bölümünde referans verilen on bir norm, siber uzaydaki sorumlu devlet davranışını kontrol altına almak amacıyla ortaya konulmaktadır. Ancak siber uzaydaki güvenlik anlayışının kimlikler, çıkarlar ve kültürlere bağlı olarak ülkeler arası farklılık gösterdiği göz önüne alındığında, normların uygulanması yönünde özel şirketlerin, STK'ların ve diğer aktörlerin desteğine ihtiyaç duyulmaktadır.

Siber norm oluşturma ihtiyacı öncelikli olarak gerçekleştirilmiş olan siber saldırıların vermiş olduğu zararlardan kaynaklanmaktadır. 1971 yılında, bir deney sonucu tarihteki ilk bilgisayar solucanı olarak kabul edilen "*The Creeper*" adlı bir program üreten Bob Thomas, farkında olmadan ilk siber saldırıyı gerçekleşmiştir. Ancak bulunduğu dönemde planlanmış bir şekilde ortaya çıkmayan solucanın diğer bilgisayarlar üzerindeki etkisi "Ben sürüngenim, yapabiliyorsan beni yakala" şeklinde bir mesaj bırakmak olmuştur.

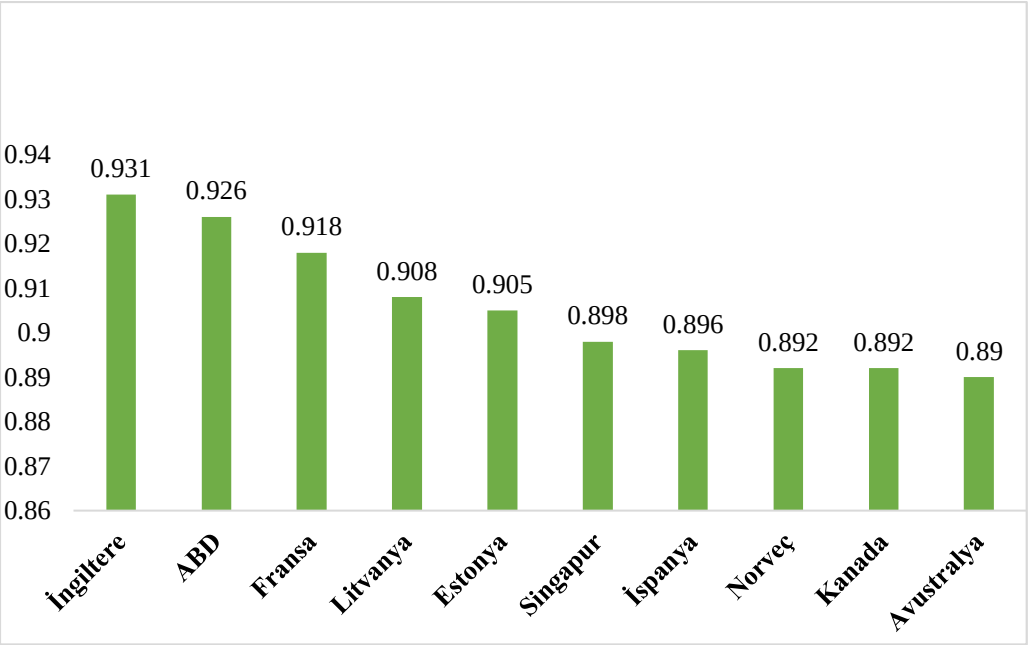
Fotoğraf 4. Creeper Virüsünün Mesajı

Kaynak: HistoryofInformation, The Creeper Worm, the First Computer Virus, 1971

1971 yılında üretilen ve siber güvenlik tarihinde literatüre geçen ilk vaka olan The Creeper vakasından 2020 FireEye ve SolarWinds saldırılarına uzanan sürece bakıldığında, güçlü ve küresel bir siber güvenlik inisiyatifinin ortaya konmasına olan ihtiyaç kendini göstermektedir (Smith, 2020). Oluşan bu ihtiyacı karşılama arzusu ise, siber uzaydaki aktörlerin siber norm oluşturma isteğini hızlandırmıştır.

13 Aralık 2020 tarihinde ABD merkezli bir yazılım şirketi olan SolarWinds'in uzantısı olan Orion adlı ağ platformunun saldırganlar tarafından hedef haline gelmesi sonucu, güncelleme yapan yaklaşık 18 bin kullanıcının ağına sızılarak siber saldırı gerçekleştirilmiştir (Editör, 2020). ABD'deki Ulusal Nükleer Güvenlik Ajansı'na (NISA) varıncaya kadar birçok kurumu etkileyen saldırı (Usta, 2020) stratejik bağlamda değerlendirildiğinde, 2 Kasım 2020 ABD Başkanlık Seçimlerinin odak nokta olduğu sıralarda seçimle alakalı siber güvenlik tedbirlerinin alındığı ve bunun sonucu diğer kurumlarda oluşan siber açık ile birlikte saldırının gerçekleştirildiği anlaşılmaktadır (Editör, 2020). Bu durum da bize siber saldırıların varmış olduğu kapsamlı noktayı, diğeriyle karşılaştırılınca ne kadar farklı yönleri kapsadığını, siyasi sonuçlarının olduğunu ve bu yüzden de devletlerin inisiyatifleri arttırdığını göstermektedir. Bu çerçevede, ülkeler hem inisiyatif almakta hem de Şekil 3'te de görüldüğü üzere siber saldırılara ciddi anlamda hazırlık yaparak siber güvenliklerini arttırmaktadırlar.

Şekil 3. CompariTech 2020 Verilerine Göre Siber Saldırılara En Hazırlıklı 10 Ülke



Kaynak: Comparitech, Which countries have the worst (and best) cybersecurity?, 2021

Şekil 3'ten yola çıkılarak bir değerlendirme yapıldığında, CompariTech tarafından 76 ülkenin baz alınmasıyla yayınlanan verilere göre siber saldırılara en hazırlıklı ülkeler arasında ABD'nin ikinci sırada yer aldığı görülmektedir. Ancak FireEye ve SolarWinds saldırıları göz önüne alındığında, siber saldırılara en hazır ikinci ülkenin kurumlarının dahi yeteri kadar güvende olmadığı görülmektedir. Bu da bize aslında devletlerin tek başlarına ne derece yeterli olabileceğini sorgulatmakta ve aktörlerin katılımcılığını öncelikli kılan siber yönetişimin önemini göstermektedir.

2.4. Siber Yönetişim Ağ Tasarıları ve Modelleri

Uluslararası sistemde 11 Eylül 2001 terör saldırılarının büyük oranda tetiklediği yönetişim ihtiyacı; devletlerin terörizm, çevre kirliliği, iklim problemleri, nükleer eylemler, insan kaçakçılığı, uyuşturucu ticareti, sınıraşan suç örgütleri vs. gibi durumlarla başa çıkmada tek başlarına yetersiz olması sonucu gündeme gelmiştir. STK'lar, düşünce kuruluşları, bireyler gibi aktörlerin katılımı olmadan eksik kaldığı farkına varılan problem çözme sürecinde, birtakım faaliyetlerin sadece devletler nezdinde çözülemeyeceği görülmektedir. Bu nedenle bu faaliyetlerin sağlıklı işleyişini sağlayabilmek için yönetimin dışına çıkılarak yönetişim anlayışına başvurmak gerekmektir (Haksever, 2018: 39).

Siber yönetişimi anlayabilmek için öncelikle yönetişim kavramının ne olduğunu açıklamak gerekmektedir. Oluşan ve oluşmaya devam eden bir süreç olduğu ifade edilen küresel yönetişim, Robert Keohane ve Joseph Nye'a göre ise; prensiplerin, normların, kuralların ve prosedürlerin oluşması, tanınması ve herkes tarafından meşru görülerek uygulanmasıdır (Willke ve Willke, 2012: 79). Bu standartların herkesçe uygulanması ve ardından bir hareket biçimi haline gelmesi sonucu küresel yönetişim sağlanmış olmaktadır. Küresel yönetişim kavramının ortaya çıkışına bakıldığında; 1980'lerde Dünya Bankası'nın, kredi vermek amacıyla iyi yönetişimin tanımını ortaya koyduğunu ifade etmek mümkündür. İyi yönetişim adı altında kredi almak isteyen ülkelere bazı kriterler belirleyen Dünya Bankası,

bu kriterler bağlamında hukukun üstünlüğünün sağlanması, yolsuzlukla mücadeledeki kararlılık, bazı mali, ekonomik ve parasal ticaret politikalarını formüle etmedeki yetenek gibi özellikler ileri sürmüştür (The World Bank, 1992: 39).

Küresel yönetişim kavramı gün gittikçe daha da önem kazanmaktadır. Sistem yapısına, diğer bir deyişle güç dağılımına bakıldığında; bunun sebebinin özellikle Soğuk Savaş'ın sonra ermesiyle, uluslararası sistemin doğası konusunda bir anlamlandırma sürecine girilmesi olduğu görülmektedir. Bu anlamlandırma sürecini ele alırken, devletlerarası ilişkilerin dinamiklerindeki değişikliklerin ortaya çıktığını ve çok kutuplu sisteme dönüşüm sonucu aktörlerin çeşitlenmesiyle birlikte, konuların da çoğaldığını ifade etmek gerekmektedir. Konularda ortaya çıkan çeşitlilik ise yeni yaklaşımların ortaya çıkmasına olanak vermiştir (Wallerstein, 1993). Soğuk Savaş sonrası süreçte, küresel yönetişimin bir süreç olarak evirilişine bakıldığında, *Global Governance* dergisinin ilk sayısında insan hakları ve demokrasi gibi konuların uluslararasılaşmasına vurgu yapan BM Genel Sekreteri Boutros Boutros-Ghali'yi örnek vermek mümkündür. İnsan hakları ve demokrasi gibi konularla bağlantılı olarak meydana gelen sorunlar, daha öncesinde devletlerin kendi sınırları dahilinde ele alması gereken konular olarak düşünülürken, Boutros Ghali, bu sorunların uluslararası siyasete taşındığından bahsetmiştir (Finkelstein, 1995). Küresel yönetişim kavramı, devam etmekte olan bir süreci ifade etmekte olduğundan bu süreç; Soğuk Savaş sonrası aktörlerin çeşitlenmesine bağlı olarak, işbirliği bağlamında uluslararası örgütler, STK'lar, özel kuruluşlar, çok uluslu şirketler ve bireyler gibi birçok aktörün etkisini içermektedir. Özellikle bireylerin önemine bakıldığında, normların, prensiplerin, kuralların uygulanması açısından bireylerin farkındalığı ayrı bir önem taşımaktadır (Jang vd., 2016).

Küresel yönetişim tanımı siber uzaya uyarlandığında, siber uzayda prensiplerin, normların, kuralların ve prosedürlerin oluşması, tanınması ve herkes tarafından meşru görülerek bir davranış biçimi haline gelmesine siber yönetişim adı verilmektedir. Etkili bir siber yönetişimin sağlanabilmesi için ise şu özelliklere ihtiyaç vardır (Dünya Bankası, 1992):

- Bilgi ve Şeffaflık
- Katılımcılık
- Hesap verilebilirlik
- Yasal çerçevenin oluşturulması
- İnsan Hakları
- Kısıtlamalar

İşleyen bir siber yönetişimde olması gereken ilk unsur bilgi ve şeffaflık olmalıdır. Zira insan faktörü söz konusu olduğu için son derece hızlı gelişmelerin yaşandığı dijital bilgi çağında şeffaflığın olmadığı, bilginin gizlendiği bir yönetişimin sağlıklı işlemeyeceğini belirtmek gerekmektedir. İkinci unsur ise, katılımcılıktır. Yönetişime katılımcı sayısının fazla olması uygulanabilirliği arttıracak ve dolayısıyla işleyişin kolaylaşmasına olanak sağlayacaktır. Örneğin, AB ülkeleri arasında sağlanacak siber yönetişime katılımcı sayısının az olmasının, bölgede istikrarı sağlamada zayıflığa sebep olacağını söylemek mümkündür. Bir diğer unsur ise, hesap verilebilirliğin sağlanmasıdır. İyi bir siber yönetişimde hesap verilebilirlik maddesi olmadığında ülkelerin siber faaliyetlerini takip

etmenin olanaksız olacağı açıktır. Yasal çerçevenin oluşturulacağını ve bunun doğrultusunda hesap verilebilirlik kriterinin aranacağını kabul eden aktörler, şeffaflık, insan hakları ve yasal çerçeveye aykırı durumlarda belli kısıtlamalarla karşılaşacaklarını bilerek iyi bir siber yönetişimin sağlanması için gerekli kriterleri sağlamaktadırlar.

Uluslararası sistemde etkisini gösteren ABD ve Çin gibi büyük güçlerin rekabeti siber uzayda da söz konusu olmakta, devletler teknolojinin getirilerini kullanarak güçlerini arttırma yoluna gitmektedirler. Bunun yanı sıra, söz konusu rekabet ve çekişmenin belirli normlar ve ilkeler çerçevesinde ilerlemesini de talep eden aktörler, böylelikle beşinci operasyonel alan olan siber uzayın kurallarını belirleyen ülkeler olarak uluslararası sistemdeki güç mücadelelerini devam ettirmeyi arzu etmektedirler. Ancak tam bu noktada bir çelişki göz çarpmaktadır; zira devletler bir yandan siber uzayı normatif bir çerçeveye oturtarak normların söz konusu olduğu siber yönetişimi savunmaktayken, diğer yandan da bu normlar aracılığıyla siber uzayda hâkimiyet gösterme amacı taşımaktadırlar (Bayrak, 2018).

İnternetin 1991 yılından itibaren ticarileşme sürecine girmesi sonucu, İnternetin nasıl düzenleneceği üzerine birtakım tartışmalar ortaya çıkmıştır. O yıllarda bu tartışmalarda düzenlemeyi oluşturacak olan opsiyon devlet aktörü olarak görülürken; 90'lı yılların sonuna doğru ise, İnternet düzenlemeleri konusunda çeşitli yaklaşımlar ortaya çıkmıştır.

2.4.1. Yönetişim ağı tasarısının unsurları

Bir yönetişim ağının nasıl tasarlandığını anlayabilmek için öncelikle bu tasarının unsurlarını ortaya koymak gerekmektedir.

2.4.1.1. Anarşik

Malatesta'nın Anarşi (1974) adlı eserinde, otoriteye dayalı tüm siyasal düzenin yıkılarak çıkarların uyumuna ve toplumsal sorumlulukların yerine getirilmesinde herkesin gönüllü katılımına dayanan özgür ve eşit üyelerden oluşan bir toplum yaratılması olarak tanımlanan (Malatesta, 1974: 13) anarşi kavramı, İnternet yönetişimi bağlamında dikkate alınması gereken bir yapıdır. Zira Bruce Sterling tarafından 1993 yılında gerçek, modern, işlevsel bir anarşinin nadir bir örneği olarak tanımlanan İnternet mimarisi, birkaç yıl sonra da John Perry Barlow tarafından yayınlanan Siber Uzayın Bağımsızlık Bildirgesi (*Declaration of Independence of Cyberspace*) ile anarşik yapının etkisini vurgulamaya devam etmiştir (Malcolm, 2008: 184).

Aktörler; siber uzayda yer alan VPN gibi bazı teknolojiler aracılığıyla veya anonim veya *nickname* (takma ad) ile hareket ederek, kendilerine *cipherspace* olarak da ifade edilebilecek olan şifreli alanlar oluşturarak birtakım içerik düzenlemelerinden, telif haklarından ve vergilendirme gibi konulardan kendilerini soyutlamakta ve böylelikle bir anarşik düzen oluşturmaktadırlar (Malcolm, 2008: 184). Örneğin, dizi, film, şarkı ve kitap gibi içeriklerin ücretsiz indirilebildiği, telifin göz ardı edildiği birçok web sitesi bulunmaktadır. Bu web siteleri tespit edilmediği takdirde telif hakkı ödememektedirler. Bunun yanı sıra, sosyal medyada takma ad (*nickname*) aracılığıyla kimliğini gizleyerek bireyleri taciz veya tehdit eden birçok kullanıcı vakası söz konusu olmaktadır.

Çok paydaşlı yönetişimi anlayabilmek için, BM Genel Sekreteri tarafından bir araya getirilen ve İnternet yönetişimi bağlamında bir diyalog oluşturmayı amaçlayan bir küresel çok paydaşlı forum olan İnternet Yönetişim Forumu'na (IGF) değinmek gerekmektedir (Editör, 2021).

Günümüzde teknolojinin geldiği evreye bakıldığında, İnternetin topolojisini veya yüzeyini yönlendirme fonksiyonunun, merkezden uzaklaştırıldığını ve dağıtılmış bir örgüsel ağa tabi olduğunu belirtmek gerekmektir. Ağın örgüsel olarak ifade edilmesinin nedeni ise, ağdaki belirli bir düğümün, çok sayıda olası güzergah üzerinden başka herhangi bir düğümle iletişim kurabilmesinin mümkün olmasıdır. Baştaki düğüm bu iletişimi kurarken herhangi bir merkezi nokta üzerinden hareket etmemekte olduğundan, tüm ağa zarar verecek merkez bulunmamakta, dolayısıyla da örgüsel ağ başarısızlıklara karşı daha dayanıklı hale gelmektedir. Örgüsel ağ vurgusu önemlidir; zira İnternetin geçmişine kısaca göz atıldığında, 1985 yılında kurulan Ulusal Bilim Vakfı Ağı (NSFNET) döneminde İnternet'e bağlanan ağların doğrudan vakfın ağıyla bağlantı kurmasının gerektiği hiyerarşik bir düzenlemenin söz konusu olduğundan bahsetmek gerekmektedir. Bu noktada bir örnek vermek gerekirse, örneğin, X Üniversitesi ağının verileri Y Üniversitesi'ne iletilmek istenmektedir. Bu noktada doğrudan iki üniversite arasındaki bağlantı üzerinden hareket etmek yerine hiyerarşik yapıya göre, veriler öncelikle Ulusal Bilim Vakfı Ağı'na gönderilmekte, ardından ise o ağ tarafından Y Üniversitesi'ne gönderilmekteydi. Hiyerarşik bir düzenlemenin olduğu bu yapıya "yukarıdan aşağıya (*top-down*)" yapı adı verilmektedir (Malcolm, 2008: 181-182). Eşler arası (*peer-to-peer*) yapı olarak adlandırılan ve mutabakata dayalı olan örgüsel ağ, yukarıdan aşağıya yapıyla zıtlık oluştursa da, hiyerarşik bir düzen ifade etmemesi amacıyla "aşağıdan yukarıya" yapı olarak isimlendirilmemektedir. Günümüz dünyasında İnternette uzlaşmaya dayalı bir yapı söz konusu olurken; örgütlerde ise, mutabakata dayalı bir yapı söz konusu olmaktadır. Diğer yandan, anarşinin otorite eksikliği anlamına gelmediğini; bir uzman ve meslektaşları arasındaki otoritenin anarşizm tarafından doğal karşılandığını belirtmek gerekmektedir. Bu bağlamda anarşizm, eşler arası bir yönetişim ağı bağlamında oldukça doğal bir yapı olarak düşünülmektedir. Bu biçimde yapılandırılan tutumlar; bölümsel, çok merkezli, entegre ağlar (SPIN) olarak isimlendirilmektedir (Malcolm, 2008: 184).

Anarşizm ve İnternetin yapısı arasındaki bu bağlantı, yönetişim konusunda da anarşizm ilkelerinin kullanılıp kullanılmayacağı konusunda bir sorgulama ortaya çıkarmaktadır. Anarşizm ve İnternet arasındaki benzerliklere bakıldığında, şu maddeleri sıralamak doğru olacaktır:

- Özerkleştirme
- Açıklık
- Eşitlikçilik
- Anonimlik
- Kozmopolitlik

Bu benzerlikler çerçevesinde, hiyerarşik bir yapı üzerine kurulan yönetişime kıyasla anarşik ilkelere dayalı bir yönetişimin başarılı olması daha muhtemel görünmektedir (Malcolm, 2008: 191) Bu noktada, anarşizmin İnternet yönetişimine nasıl uygulanacağı

sorusu gelmektedir. Jeremy Malcolm'a göre, bunun anlamı tüm paydaşları İnternet yönetişimine dâhil etmek ancak paydaşlardan herhangi birinin diğerini zorlamaması demektir (Malcolm, 2008: 192). Bu zorlama, demokratik veya liyakate göre üstünlüğün söz konusu olduğu meritokratik kavramlar üzerinden dahi olsa gerçekleşmemelidir. İnternet ve anarşizm üzerine çalışmalar yürüten Joseph Reagle'ye göre, bir politikanın başarısı otoriteye değil, toplum tarafından benimsenmesine dayanmaktadır (Reagle, 1998).

Malcolm'a göre; gücünü hiyerarşiden almayan kuralların, anarşist bir yönetişim ağı doğrultusunda pazar, normlar ve mimari olmak üzere üç mekanizma üzerinden kolektif olarak benimsenmesi daha kolay gerçekleşecektir. Bu çalışmanın konusu olan normlar kısmına gelindiğinde, anarşist bir ulusötesi ağ için normların kullanılmasına yönelik bir örnek vermek gerekirse, Londra Eylem Planı'ndan (*London Action Plan*) bahsetmek yerinde olacaktır. Londra Eylem Planı; hükümetin düzenleyici ve yürütücü topluluğunun temsilcilerini ve ilgili endüstri üyelerini içermekte olup, yıllık toplantılar ve iki ayda bir telekonferanslar yapmakta, üyelerin birbiri ile bağlantıda kalmasını sağlamakta ve *spam* olarak adlandırılan istenmeyen postaların önlenmesine yönelik düzenlemeler ve yaptırımlar ile uğraşan tüm kuruluşlar için kritik olan bilgileri paylaşmaktadır (UCENet, 2021). Londra Eylem planında üyeler arası bir işbirliği olduğu doğrudur; ancak yasal olarak bir mecburiyet durumu söz konusu olmamaktadır. Burada söz konusu durum, üyeler arasında kabul edilen ortak normlar üzerinden işbirliğine gitmektir (Malcolm, 2008).

Anarşist yönetişim ağı mekanizmasının olumlu yanları olduğu kadar eleştirilmesi gereken yanları da söz konusu olmaktadır. Örneğin, ağın, anarşist ilkelere göre donatılması sonucu paydaşların katılım göstermesi kolay olmayacaktır. Bir örgütün meşru olduğunu anlayabilmek için temelde hesap verilebilirlik ve şeffaflığa bakılmakta olduğundan, anarşist yönetişim modeli bazı eksikliklere sahip olmaktadır. Hükümetler, özel şirketler, sivil toplum kuruluşları gibi birçok paydaşın söz konusu olduğu çok paydaşlı yönetişim, paydaşların birbirlerine danışarak hareket etmelerini içermekteyken; anarşik yapı bağlamında ise, örneğin hükümetler sivil topluma ve diğer paydaşlara danışmadan kendi aralarında bazı düzenlemelere girebilme potansiyeline sahip olmaktadırlar. Bunun tam tersi durumda ise, diğer paydaşlar hükümetlere danışmadan düzenlemelere gidebilme durumunu içlerinde barındırmaktadırlar (Malcolm, 2008: 194).

Anarşist yönetişim ağının bir diğer açığı olan şeffaflığa örnek olarak ise, üyeleri dışında faaliyetlerinin bir kısmını kamudan gizleyen Londra Eylem Planı gibi ağlar verilebilmektedir. Buradan anlaşıldığı üzere, resmi etkisi azaldıkça yönetişim temelli kuruluşların şeffaflığı azalmaktadır (Malcolm, 2008).

2.4.1.2. Hiyerarşik

Bir yönetişim ağının devletler, özel şirketler, uluslararası örgütler ve STK'lar gibi tüm paydaşları içermesi ve tüm paydaşların yeterli ölçüde söz sahibi olması gerekmekte, ağın hiyerarşik olması durumu ancak bu şekilde kabul edilmektedir. Zira bir kurumun diğerinden üstün olduğu bir yönetişim ağı İnternet'in özüne uygun görülmemektedir. Bunun yanı sıra bir yönetişim ağının hiyerarşik olarak dönüştürülebilmesi için öncelikle bir organizasyon olarak var olması gerektiğinden, oluşturulacak yapının nasıl ve kim tarafından kurulacağı konuları baskınlık gerektiren bir durum olması sebebiyle bir soru

işareti ortaya çıkarmaktadır. Bir yönetişim ağı oluştururken hiyerarşik model dikkate alınmaktadır; zira bu modelin vurguladığı nokta otoriterlik değil bürokrasi ve oligarşi gibi yukarıdan aşağıya bir sıralama olarak alınması gerektiğidir.

- **Bürokrasi**

Weber tarafından bir organizasyonun alabileceği en etkili yapı olarak görülen bürokratik model, genellikle yönetişim ağlarında, özellikle de hükümetlerin başrolü üstlendiği ağlarda bulunmaktadır (Malcolm, 2008: 197). Bu yönetişim ağı, çok paydaşlılık ile uyumsuz değildir zira yetkili kişiler, astlarının resmi kanallar aracılığıyla yönetişim sürecine katkıda bulunmalarına izin vermektedirler. Ancak burada çok paydaşlılıktan farklı olarak iş bölümüne uygun olarak resmi kurallarla tanımlanmış roller söz konusudur. Oysa bir yönetişim ağının tüm paydaşları içermesinin nedeni, kendi değerlerini temsil etmeleridir. Bürokratik olarak yapılandırılmış bir yönetişim ağına katılan paydaşların, resmi kurallarla kesin olarak tanımlanmış rollerde hareket etmelerini zorunlu kılmak çok paydaşlı yönetişim modeline benziyor gibi görünse de, paydaşların ilk etapta sürece dâhil etmelerinin esas sebebi olan kendi değerlerini temsil etme durumunu tamamen ortadan kaldırmaktadır (Malcolm, 2008: 198).

- **Oligarşi**

Oligarşik yönetişimin en büyük avantajı, iktidarın küçük bir grup ile sınırlı olması sebebiyle, karar alırken demokrasilere göre daha hızlı ve çekişmenin az olduğu bir süreç izlenebilmesidir. Ancak diğer yandan bu avantajların bir bedeli olarak; yönetilenlere hesap verilebilirlik ve onları temsilciliğini yapma durumu minimum düzeyde tutulmakta ve buna ek olarak tiranlığa karşı daha az koruma sağlanmaktadır (Malcolm, 2008: 198). Oligarşik yöntem tüm bunları ortaya koyarken yönetişim bağlamında değerlendirildiğinde ise, üç paydaş grup olan hükümetler, özel sektör ve sivil toplum kuruluşlarının tümünün çıkarlarının gözetilebileceği ulusüstü bir yapının mevcut olmadığını belirtmek gerekmektedir. Bu bağlamda, en azından nihayetinde böyle bir yönetişim ağı kurulana kadar geçen süreçte, demokratik temsile kıyasla oligarşi de yüksek bir alternatif olarak yerini korumaktadır (Malcolm, 2008).

Burada amaç oligarşiyi savunmaktan ziyade, Michels'in "oligarşinin demir kanunu (*iron law of oligarchy*)" olarak öne sürdüğü noktayı ifade etmektir. Bu kanuna göre bürokrasi, demokrasi veya anarşi fark etmeksizin tüm bu yapıların zaman içerisinde gücün küçük bir grubun iktidarı altında toplandığı bir yönetime dönüşme ihtimali bulunmaktadır. Diğer bir ifadeyle, başkalarını yönlendirmek isteyen elitler, hem güce hem de iradeye sahip olduklarından iktidarda baskınlık gösterme olanağına sahip olmaktadırlar (Malcolm, 2008: 199).

2.4.1.3. Demokratik

Demokratik yönetişim ağı, kurumların hem kendi içlerinde hem de diğer kurumlarla etkileşimlerinde demokratik süreç ve normlara göre işlerlik gösterdiği bir yönetim sistemidir (OSCE, 2021). 28 Ekim 2019'da Strazburg'da Avrupa Konseyi çerçevesinde düzenlenen İyi Demokratik Yönetişimin On İki İlkesi Üzerine Uluslararası Konferans'ın çıktılarına göre; demokratik yönetişimin on iki ülkesi şunlardır (Council of Europe Centre of Expertise for Good Governance, 2019):

- Katılım, temsil, seçimlerin adil bir biçimde yürütülmesinin temele alındığı birinci ilkeye göre;

-Yerel seçimler adil bir şekilde gerçekleştirilmelidir.

-Vatandaşlar, kamusal aktivitenin merkezinde olmalıdır.

- Erkek ve kadın fark etmeksizin tüm cinsiyetten insanlar, doğrudan veya menfaatlerini temsil eden meşru kurumlar aracılığıyla karar almada söz hakkına sahip olmalıdırlar. Bu bağlamda, vatandaşlara ifade özgürlüğü, toplanma özgürlüğü ve örgütlenme özgürlüğü sağlanmalıdır.

- Azınlığın haklarına ve meşru menfaatlerine saygı duyulmalıdır, ancak kararlar çoğunluğun iradesine göre alınmalıdır.

- İkinci ilke olan cevap verebilirlik ilkesine göre;

-Kamu hizmetleri çerçevesinde talep ve şikâyetler makul bir süre içerisinde yanıtlanmalıdır.

- Hedefler, kurallar ve prosedürler vatandaşların meşru beklenti ve ihtiyaçlarına göre uyarlanmalıdır.

- Üçüncü ilke olan insan hakları, kültürel çeşitlilik, sosyal bütünlük ilkesine göre; insan haklarına saygı duyulmalı, korunmalı ve haklar uygulanmalıdır. Buna ek olarak kültürel çeşitlilik bir değer olarak ele alınmalı ve sosyal uyumun sağlanması için dezavantajlı kesimin entegrasyonu teşvik edilmelidir.
- Dördüncü ilke olarak ele alınabilecek olan hesap verebilirlik ilkesi bağlamında; kolektif ve bireysel tüm karar vericiler kararlarının sorumluluğunu almalıdır. Alınan kararların hak ihlali oluşturduğu durumlarda ise, etkili hukuk yolları bulunmalıdır.

Devamındaki ilkeler, verimlilik ve etkililik ilkesi, açıklık ve şeffaflık, hukukun üstünlüğü, etik davranış, kabiliyet ve kapasite, inovasyon ve değişime açıklık, sürdürülebilirlik ve uzun vadeli yön belirleme, sağlam mali yönetimdir.

2.4.1.4. Karşılıklı mutabakata dayalı

Hükümetlerin demokratik yönetişim ağlarında tek taraflı hareket etme yönündeki yıkıcı eğilimleri sonucu gündeme giren karşılıklı mutabakata dayalı anlayış, yönetişim grupları içinde ve arasında demokratik olarak mutabık kalınan herhangi bir teklif konusunda paydaş grupları arasında fikir birliğine varılmasını ve böylece her bir paydaş grubuna bunu veto etme yetkisi verilmesini içermektedir. Çok paydaşlı yönetişim ağları doğaları gereği uzlaşmaya dayalı yapılar olduklarından ve kararlarını uygulamak için yalnızca yumuşak güce sahip olduklarından, paydaş grupları arasında resmi bir uzlaşma gerekliliğinin tanınması da bu yönetişim mekanizması için demokratik oylamadan daha doğal bir durum olarak görülmektedir (Malcolm, 2008).

2.4.2. Siber egemenliğe odaklı yönetişim modeli

Siber uzayda suç ve tehditler artarken adil bir yönetişim rejiminin nasıl kurulacağı üzerine bir yaklaşım olan Siber Egemenlik yaklaşımı; uzlaşmayı reddeden üç farklı aktör olan

devlet, vatandaş ve uluslararası toplumun çıkar ve taleplerini ortaya koyarak siber uzaya farklı düzeylerden bakmayı önermektedir (Yeli, 2017).

BM Hükümet Uzmanları Grubu'nun raporları üzerinden fikir birliğine varmayı hedefleyen uluslararası toplum, bazı açılardan görüş farklılıklarına düşmektedir. Bu görüş farklılıklarından bahsedildiğinde, öncelikle siber egemenlik anlayışı ve İnternetin ruhu arasında bir çelişki olduğunu belirtmek gerekmektedir. Siber uzayda geleneksel devlet egemenliğinin kullanılması, İnternetin tabiatında var olan kısıtlanmamış bağlantı kurma niteliğine aykırı bir duruma sebep olmaktadır. Dolayısıyla siber uzayın *sui generis* yapısını içeren şekilde bir egemenlik anlayışına dayalı olan siber egemenlik kavramı ortaya çıkmaktadır. Ancak diğer yandan, geleneksel devlet egemenliği yerine kısıtlanmanın olmadığı siber egemenlik yaklaşımının vurgulanması, uluslararası sistemdeki her bir ülkenin kendi başına bir siber alan oluşturmasına, diğer bir deyişle İnternetin parçalı bir yapıya dönüşmesine sebep olabilme riskine sahip olmaktadır (Yeli, 2017). Bir diğer çelişki ise, insan hakları konusunda yaşanmaktadır. İnternetin ruhunda ifade özgürlüğü ilkesi yer almaktayken, siber egemenlik yaklaşımının içeriğinde kısıtlamalar olması sonucu serbest bilgi akışı kısıtlanmakta ve ortaya devlet müdahalesini içeren bir çeşit gerilim çıkmaktadır. Son çelişkinin temelinde ise, hükümetin yönlendirdiği siber egemenlik yaklaşımı ve çok paydaşlı yönetişim anlayışı arasındaki tartışmalar yatmaktadır (Yeli, 2017).

Tablo 6. Siber Egemenlik Yaklaşımı Bağlamında Ortaya Çıkan Karşıtlıklar

Karşıtlıklar	İlgili Aktörler
Siber egemenlik X İnternetin ruhu	Devlet ve uluslararası Toplum
Siber egemenlik X İnsan Hakları	Devlet ve vatandaş
Siber egemenlik X Çok paydaşlı yönetişim	Devlet, vatandaş ve uluslararası toplum

Kaynak: (Yeli, 2017: 110)

Siber uzayda uluslararası kurallar oluşturulmasını savunan siber egemenlik yaklaşımının, farklılıkları göz ardı ederek fikir birliğine varması noktasında zorluklar söz konusu olmaktadır. İşbirliğine giden yolda uluslararası sistemde fikir birliğine ulaşmayı mümkün kılabilmek için geleneksel egemenlik yaklaşımını siber uzaya adapte edebilmek ve Tablo 6'da yer verildiği üzere ulus-devlet, vatandaş ve uluslararası toplumu dikkate alarak üç boyutlu ve kapsamlı bir uyarlamada bulunmak gerekmektedir (Yeli, 2017: 110).

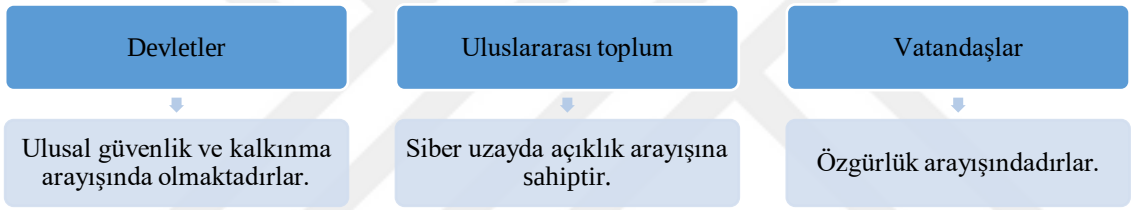
İşbirliği oluşturmak fikir birliğine gitme gereksinimini oluştururken, fikir birliğine gitmek ise, diyalog sürecinin başlatılması ihtiyacını vurgulamaktadır. Diyaloğa gitmek için gereken ortamı yaratmak için, ortak zemini oluşturmak ve böylelikle siber uzaydaki tüm aktörlerin temsil edilebileceği bir görüş alanı oluşturmak önemli bir nokta olarak kendini göstermektedir. Böylelikle geleneksel realist anlayışın aksine uluslararası sistemdeki diğer aktörlerin göz ardı edilmediği bir yaklaşım ortaya çıkmaktadır (Yeli, 2017).

DataReportal'a göre, 2021 yılının başında dünya çapında 4.66 milyar olarak tespit edilen İnternet kullanıcısı (Editör, 2021) her koşulda kişisel hak ve özgürlüklerini elde etmek istemektedir. Ancak tüm İnternet ortamındaki tüm bireylerin hak ve özgürlüklerini sağlayabilmek için siber uzayda geçerli bir kurallar bütününe ihtiyaç vardır. Bu kuralları oluşturmak ve uygulayabilmek için hükümet düzeyinde bir yaklaşım yeterli olmayacaktır. Zira uluslararası sistemdeki aktörler yalnızca hükümetlerden oluşmamaktadır. Ayrıca

teknoloji geliştikçe beraberinde güvenliği ve korumayı getireceğini düşünmek kısıtlı bir görüş olmaktadır. Siber uzayda korumayı sağlayabilmek için yasaya ve dolayısıyla da egemenliğe ihtiyaç duyulmaktadır. Bu güvenliği sağlayacak olan temel aktörlerden biri olan devletin, insan yapımı siber alanı düzenlemek üzerine müdahalede bulunması aslında vatandaş ve devlet arasındaki ilişkiyi ifade etmektedir. Ancak diğer yandan, ulusal egemenliğinin bir kısmını uluslararası topluma aktararak işbirliğine gitme ve güvenlik üzerine fikir birliğine varma çabalarını teşvik edecektir. Uluslararası toplum ise, işbirliği temelinde kültürel alışveriş, ekonomik ve güvenlik üzerine fırsatlar sunarak devletin kalkınmasına katkıda bulunacaktır. Buradan çıkarılacak olan sonuç şudur ki; devlet ve uluslararası toplum arasında bir karşıtlık olmasına karşın, iki aktör zıtlıkların birliğini sağlayarak düalitenin ötesine geçmeyi başaracak kapasiteye sahip durumdadır (Yeli, 2017).

Uluslararası toplum bağlamında bakıldığında ise, küresel bir yapıya sahip olan İnternet söz konusu olduğunda, eğer devletlerin varlığı kabul ediliyorsa ulusal egemenliğin göz ardı edilmesi mümkün görünmemektedir. Bu noktada yapılması gereken şey, siber kapasitesi geniş olan devletlerin siber kaynaklarını dijital uçurumu kapatmak için paylaşma konusunda girişimci olmasıdır (Yeli, 2017).

Şekil 4. Siber Uzayın Bileşik Yapısında Aktörlerin Arayışları

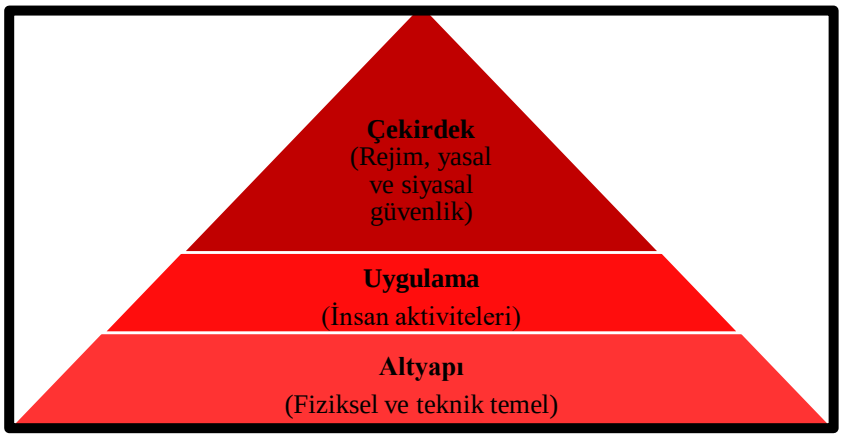


Kaynak: (Yeli, 2017: 111-112)

Buradan çıkarılacak sonuca göre, devletler ulusal güvenlik ve kalkınma ihtiyaçlarını karşılayabilmek için uluslararası toplum ile işbirliğine gitmelidirler. Vatandaşlar, özgürlük arayışlarını karşılamak için devlet güvencesine ihtiyaç duymaktayken; uluslararası toplum ise tüm bu aktörleri bünyesinde toplamakta ve uluslararası sistemdeki kültürel ve ulusal çeşitliliği dikkate alarak siber uzayda açıklık sağlama yoluna gitmelidir. İnternetin birbirine bağlılığı veya diğer bir deyişle bileşik yapısını gösteren bu yorum, bu bileşikliği işbirliğine ve dengeye götürmenin yolunun farklılıkların dikkate alınmasından geçtiğini öne sürmektedir (Yeli, 2017).

Geleneksel egemenlik anlayışında dış kontrol kabul edilmese de, siber egemenlik yaklaşımında kontrolün sağlanması bağlamında hangi unsurların transfer edilebileceği üzerine düşünülmelidir. Burada egemenliğin tamamıyla devrinden değil, kısmi bir şekilde bazı unsurların devrinden bahsedilmektedir. Uluslararası toplumun devletlerin egemenlik konusundaki sınır noktalarını iyi tespit etmesi ve bunlara saygı duyması gerekmektir. Siber elçiler, siber savaş ekipleri oluşturan ülkeler bir yandan kendi siber uzaylarını yaratmaktadırlar. Bunun tehdide dönüşmemesi ve uluslararası sistemde dengenin muhafaza edilebilmesi için ülkelerin, egemenliklerinden belli noktalarda taviz vermelerine ihtiyaç duyulmaktadır. Siber egemenliğin hangi unsurlarının devredilebilir hangilerinin dokunulmaz olduğunu belirlemek için aşağıdaki şekilde yer aldığı biçimde katmanlı bir yaklaşıma ihtiyaç bulunmaktadır (Yeli, 2017).

Şekil 5. Siber Egemenliğe Katmanlı Bir Yaklaşım



Kaynak: (Yeli, 2017: 113)

Şekil 5'te, en düşük seviye olan siber uzaydaki altyapıdan başlayarak en yüksek seviye çekirdeğe kadar uzanan bir piramit görülmektedir. Teknik olarak tek tipleştirme (standardizasyon) ve bağlantı kurmayı ifade eden altyapı seviyesi; siber kapasitesi düşük devletlerin bu düzeyde sahip oldukları otoritelerini gelişmiş siber kapasiteye sahip devletlere devretmelerini, gelişmiş devletlerin ise, dijital uçurumu kapatma noktasında esnek davranmaları gerektiğini öne süren bir yaklaşıma sahiptir (Yeli, 2017).

Piramitteki orta seviye olan uygulama seviyesi ise, teknik temelin ardından pratiğe dökülen ve teknoloji, kültür, ekonomi gibi birçok sektörü birbiriyle bütünleştiren İnternet platformunu ifade etmektedir. Orta seviyede, çok taraflılık ve yerel koşullar arasındaki egemenlik-düzen dengesinin sağlanması gerekmektedir. Bu seviye, piramidin bel kemiği olup müzakere edilebilir konuları içermektedir (Yeli, 2017).

Rejim, hukuk, siyasal güvenlik ve ideolojiler gibi devletlerin temel çıkarlarını içeren piramidin çekirdek seviyesi; devletlerin sahip oldukları farklı kültürel geçmişler ve ulusal şartlar nedeniyle meşru bir farklılık ortaya çıkarmakta olduğundan hoş görülmesi gereken bir düzeydir. Zira insan unsurunun temelinde çeşitlilik ve farklılık söz konusu olmaktadır. Bu nedenle, insan faktörü olduğu sürece farklılıklar olması doğaldır ve buna bağlı olarak uluslararası sistemde geçerli tek tip bir kültürün olmayacağını öne sürmek mümkündür. Bu bağlamda mevcut çeşitliliklerin oluşumuna saygı duyulmalı ve bu farklılıkları hoş görme yoluna gidilmelidir (Yeli, 2017).

Çok taraflı yönetişim ve çok partili yönetişim arasındaki farkı anlayabilmek için bu üç düzeyin netlik kazanması gerekmektedir. İki yönetişim tarzı birbiriyle çelişmemektedir. Ancak, farklı siber uzay düzeylerinde farklı uygulanabilirliğe sahiptirler. Ulusal hükümetlerin; ideoloji, siyaset, hukuk, kurumsal güvenlik ve hükümet güvenliği gibi konular bağlamında diğer düzeylerde çok partili yönetişimi kabul etmeleri sonucu, çok taraflı yönetişimi benimsemenin olumlu yanlarını görmeleri mümkündür (Yeli, 2017).

Uluslararası sistemdeki her bir ülkenin kendi başına bir siber alan oluşturmasıyla İnternetin parçalı bir yapıya dönüşmesine sebep olan siber güvenliği uygulamak İnternetin ruhuyla ters düşse de, sınırlı bir siber egemenlik anlayışına sahip olunması sorunu çözmektedir. Böylelikle devletlerin, küresel İnternet yönetişimine eşit şekilde katılmaları, sorumluluğu paylaşmaları ve ara bağlantının kalitesine katkı sağlamaları mümkün olacaktır. Kısacası

İnternetin sınırsız ruhu ve siber egemenlik arasındaki tutarsızlığı dengelemenin en iyi yolu siber egemenliğin sınırlanmasıdır (Yeli, 2017).

Siber uzayda siber egemenlik ve çok paydaşlı yönetim arasında bir gerilim olduğu doğru olsa da, birinin savunulması diğerinin reddedilmesi anlamına gelememektedir. Zira hükümetler çok paydaşlı yönetişimdeki paydaşlardan biri olmaktadır. Bu nedenle hükümetler, çok partili yönetişime bağlı olarak; işletmeler, uzmanlar ve düşünce kuruluşları vb. gibi kurumlara saygı duymak ve onları yönetişime teşvik etmek gibi önemli bir role sahiptirler (Yeli, 2017) .

Küreselleşmenin geldiği evreyle birlikte, beşinci operasyonel alan olan siber uzayda geçerli olan siber egemenlik kavramı aşağıdaki şekilde karakterize edilerek bölünebilmektedir:

-Dokunulmaz olan çekirdek seviye

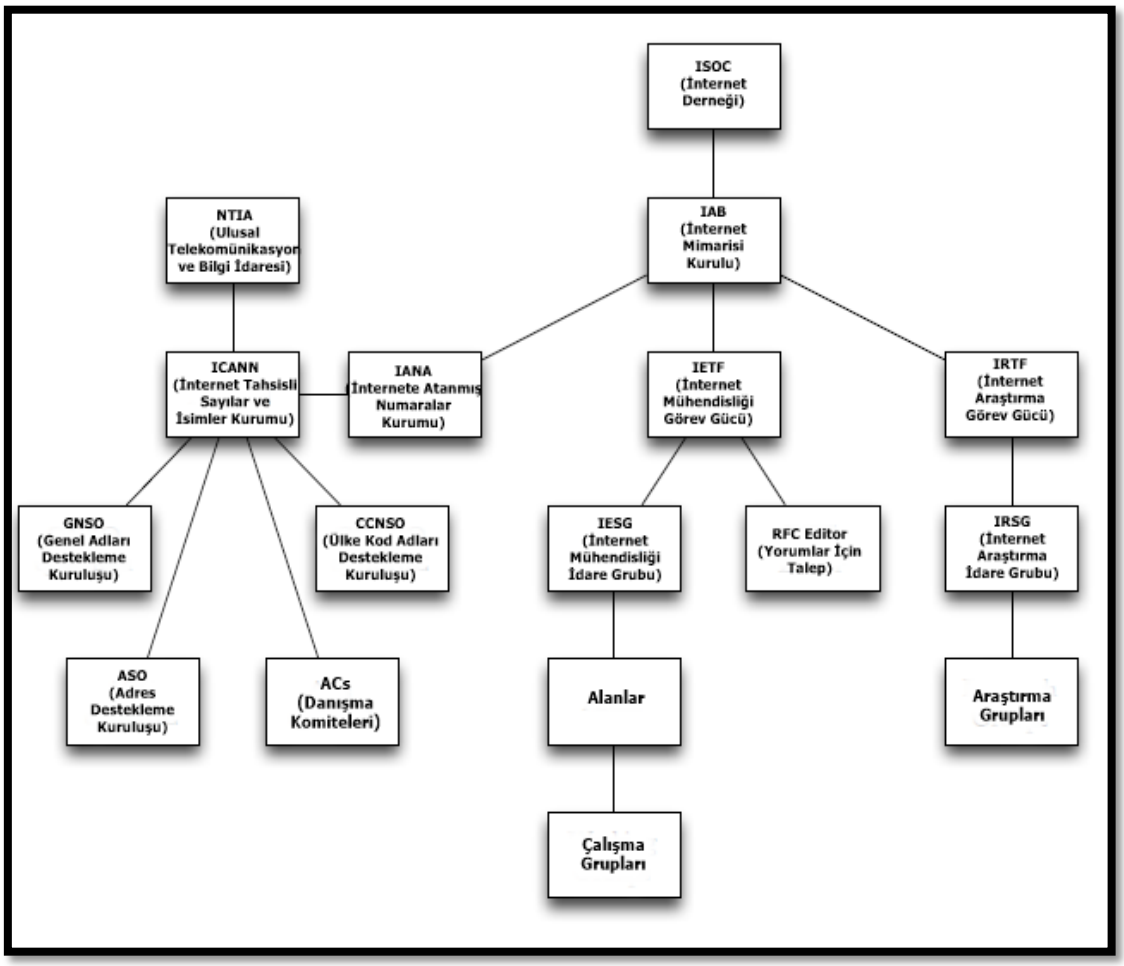
-Açık ve paylaşılan bir devredilebilirliğe sahip olan altyapı ve uygulama seviyeleri

İnternet bağlantısını kötücül amaçlarla kullanarak devletlerin temel çıkarlarına meydan okumak yasaklanıyorsa, siber uzayda geleneksel egemenlik anlayışını dayatarak İnternetin temelini sarsmak da yasaklanmalıdır. Diğer bir deyişle vahşi batıda geçerli kanunların yerini farklılıklara saygı, hoşgörü, dayanışma ve paylaşım gibi değerler almalıdır (Yeli, 2017).

2.4.3. Çok paydaşlı İnternet yönetişimi modeli

2005'te Dünya Bilgi Toplumu Zirvesi (DBTZ) tarafından tanımlandığı üzere İnternet yönetişimi: *"hükümetler, özel sektör ve sivil toplum tarafından, İnternetin gelişimini ve kullanımını şekillendiren ortak ilkelerin, normların, kuralların, karar alma prosedürlerinin ve programların kendi rollerinde geliştirilmesi ve uygulamasıdır* (WGIG, 2005)*."* İnternet yönetişiminin temelinin kurumlara dayandığını, diğer bir deyişle İnterneti hangi kurumların yöneteceğini ve bu kurumların nasıl organize olacaklarını belirtmek gerekmektedir. Siber uzaydaki belirsizlikleri azaltacak, tarafların etkili bir şekilde uygulayabileceği karma modelin oluşturulması çerçevesinde çeşitli modeller incelenmekte, bunlardan birini ise, çok paydaşlı İnternet yönetişimi teşkil etmektedir. Bu bağlamda çok paydaşlı İnternet yönetişim incelenirken, sorulacak olan başlıca soru "ağı kimin yönettiği" olmalıdır. İnternetin babası (Editör, 2011) olarak adlandırılan Vinton Cerf tarafından söylenen şu alıntı bu anlamda önemli olmaktadır*: "Ağı kim yönetiyor? Bir dereceye kadar sen, ben ve 600 milyon kişi* (Malcolm, 2008: 181)*."*

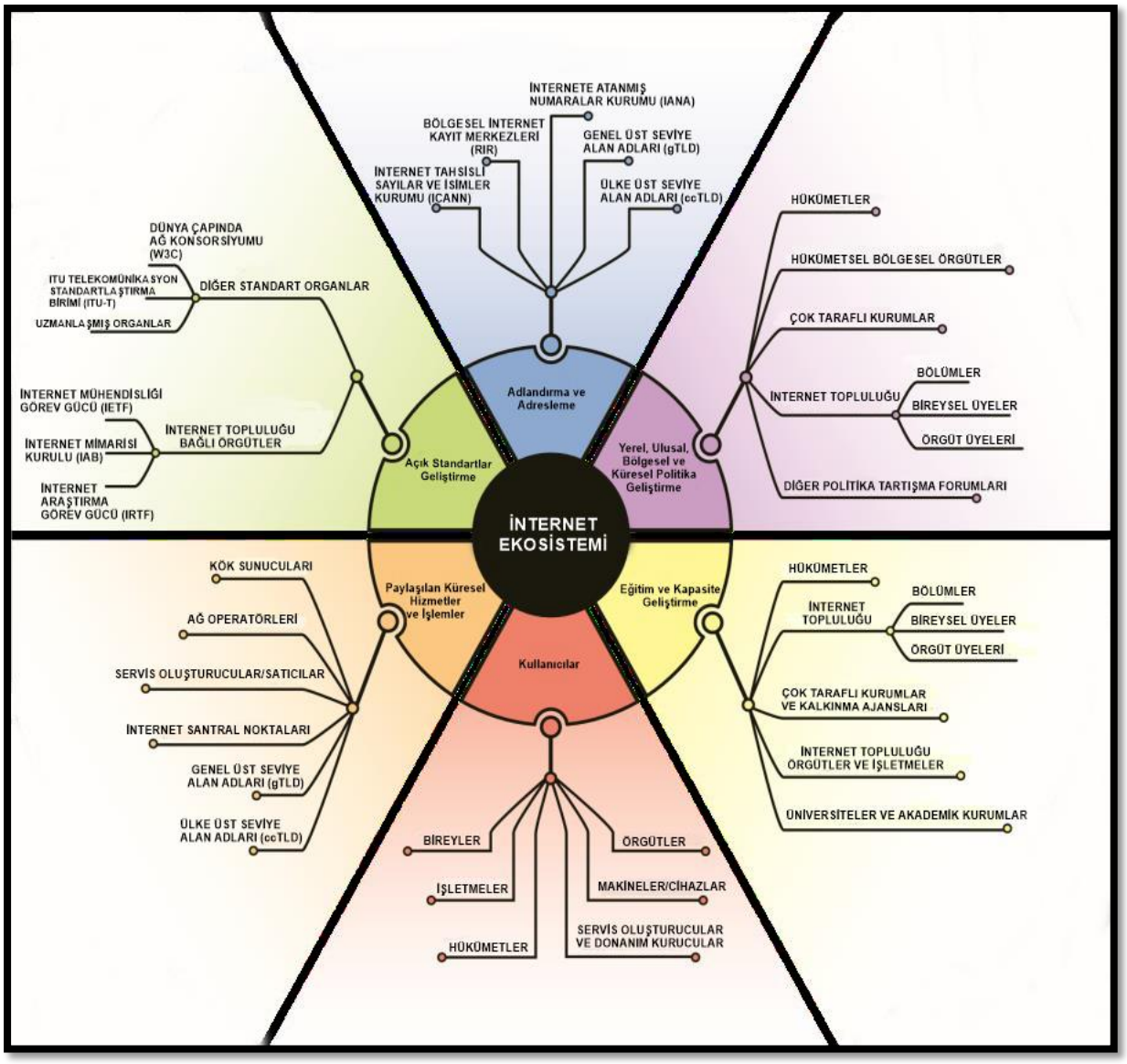
Şekil 6. İnternet Yönetişim Örgütleri



Kaynak: (Malcolm, 2008: 38)

Şekil 6'da İnternet yönetişim örgütlerinin çeşitliliğinden de anlaşılacağı üzere İnternet ortamı kompleks bir ortamdır ve bu alanda gereken her türlü işbirliğine ihtiyaç vardır. 2014 yılında Kleinwächter'in benzetmesi üzerinden açıklanacak olursa, İnternet yönetişiminin ekosistemi tıpkı yağmur ormanlarını anımsatmaktadır (Kleinwächter, 2017). Yağmur ormanlarında, sayılamayacak kadar çok çeşitte bitki ve hayvan bir arada yaşamaktadır. İnternet de sanal yağmur ormanları olarak ele alındığında, sonsuz ve büyüyen bir ağa; hizmete, uygulamalara, rejim ve diğer özelliklerin ortak çeşitliliğine sahip olduğu görülmektedir. Bu sanal yağmur ormanları içerisinde aktörler karşılıklı bağımlı bir iletişim, koordinasyon ve işbirliği mekanizması içinde varlıklarını devam ettirmektedirler. Buradaki kritik nokta ise, yağmur ormanlarının bir bütün olarak ne yönetilebilir ne de kontrol edilebilir olduğu, ancak zarar görebilme ve yok edilebilme olasılığına sahip olduğudur. İnternet yönetişim ekosistemi çok sayıda aktörü, inovasyonu, pazar fırsatlarını, kullanıcı ihtiyaçlarını ve siyasi çıkarları bünyesinde barındırarak yerel, ulusal, bölgesel ve uluslararası düzeylerde etkiye sahip olmaktadır. İnternet yönetişimi ekosistemi üzerine öne sürülen sanal yağmur ormanları benzetmesinin ardından ekosistemin Şekil 9'da ayrıntılı bir şekilde görülmesi mümkündür.

Şekil 7. İnternet Ekosistemi



Kaynak: Internet Society, Internet Governance – Why the Multistakeholder Approach Works, 2016

Şekil 7'de İnternetin ekosistemini gösteren şema incelendiğinde, İnternet'in açık, dağıtımlı, birbiriyle bağlantılı ve ulusaşan niteliklere sahip olduğu bilgilerini çıkarmak mümkündür (*Internet Governance: Why the Multistakeholder Approach Works*, 2016). İnternet'in işleyişinin bu biçimde olduğu göz önüne alındığında, İnternet yönetişiminin de bu sisteme dayandığını, zira İnternet yönetişiminin İnternet ekosisteminden ayrı tutulamayacağını ifade etmek gerekmektedir. Aktörler bir yandan teknolojinin İnternete getirdiği dönüşümleri pratiğe dökmeye çalışırken, bir yandan da İnternetin bağlantılı niteliğinin etkisiyle diğer aktörlerin ekosistemdeki yerinin farkında olmakta ve çözüm bulma amacıyla kolektif bir karar alma süreci olan çok paydaşlı İnternet yönetişimi anlayışını benimsemeye doğru yönelmektedirler (*Internet Governance: Why the Multistakeholder Approach Works*, 2016).

Çok paydaşlı yönetişimin ihtiyaç duyulmasının altında yatan sebeplere bakıldığında; bu modelin altyapı, yönetişim ve insan unsuru olmak üzere üç bileşenden oluşmakta olduğu

görülmektedir. İnternetin açık, dağıtılmış, birbirine bağlı ve ulus ötesi olduğu da göz önüne alındığında İnternet yönetişimi için çok paydaşlı yaklaşım modelinin kullanılmasının, özünde İnternet'in kendi DNA'sından büyüyen ve gelişen bir süreç olduğu ortaya çıkmaktadır (Internet Society, 2016). Buna ek olarak çok paydaşlı karar verme, hesap verebilir, sürdürülebilir ve hepsinden önemlisi etkilidir ve bu nedenle girdiler ne kadar iyi ve süreç ne kadar kapsayıcı olursa, çıktılar ve bunların uygulanması o kadar sonuç alınabilir olmaktadır. İnternet Toplumu (*Internet Society*), evriminin bir sonraki aşamasına rehberlik etmek için başarılı birçok paydaşlı karar verme üzerine dört özellik ortaya koymaktadır: kapsayıcılık ve şeffaflık; kolektif sorumluluk; etkili karar verme ve uygulama; dağıtılmış ve birlikte işlerliğin sağlandığı bir yönetişim yoluyla işbirliği (Internet Society, 2016). Tüm bu özelliklerin, çok paydaşlı model içerisinde İnternetin evrimiyle birlikte evirileceği öne sürülmektedir.

BÖLÜM 3: SİBER NORMLARIN İNŞASI SÜRECİNDE ETKİLİ OLAN AKTÖRLER VE İZLEDİKLERİ POLİTİKALAR

Siber uzayın yönetişimi, oldukça karmaşık ve tartışmalı bir süreç olarak yerini korumaktadır. Bu bölümde, bir yandan geleneksel güvenlik anlayışının aksine çoklu aktörlerin söz konusu olduğu siber yönetişimde kimlerin yer alması gerektiği sorusu irdelenirken, diğer yandan ise, devletlerin, özel şirketlerin ve örgütlerin siber yönetişim üzerindeki rolü üzerinde durdukları temel unsurlar üzerinden değerlendirilmekte ve siber yönetişime bakış açıları tespit edilerek devletler bağlamında ve küresel anlamda siber yönetişime sağlayabilecekleri katkılar üzerinde durulmaktadır.

3.1. Devletler

Küreselleşmenin geldiği noktayla birlikte toplumlar, vatandaşlar, işletmeler ve hükümetler arasındaki bağlantıyı arttırarak dijital dünyada bıraktıkları izleri genişletmekte, bununla birlikte siber vakalarda ciddi bir artış görmüştür. Bir yandan birey düzeyinde finansal motivasyonlarla saldırı faaliyetleri artış gösterirken, devlet düzeyinde de casusluk, keşif ve sabotaj gibi yöntemlerle askeri operasyonlara destek olma durumu İnternet aracılığıyla giderek artmaktadır.

Ulus devletler askeri planlamalarına siber kabiliyetlerini dâhil ederek bu yetenekleri arttırma yoluna gitmekte, ancak bu kabiliyetlerin kullanımına ilişkin bir yol haritası veya rejim bulunmamaktadır. Bu nedenle, siber uzaydaki belirsizliğin dikkate alınması ve bu belirsizliği hafifletmek için belli başlı normların ortaya konması önem teşkil etmektedir. Zira kritik altyapıların dahi siber saldırılar aracılığıyla zarar görebileceği göz önüne alındığında, siber risk ve tehditler noktasında ortak bir anlayış geliştirilmesi ve siber güvenlik bağlamında ortak normlar oluşturulması gerekmektedir. Bu noktada, devletler bazında iki seçenek tartışmaya konu olmaktadır Birincisi, devletlerin askeri operasyonlarını siber araçlar üzerinde tamamıyla geri çekmeleri ikincisi ise, belirsizliği azaltmak amacıyla siber güvenlik üzerine devletler bazında bazı davranış normları ortaya koymaktır. İlk seçeneğin tercih edilmeyeceği aşikârdır. Dolayısıyla, risk ve tehditler ile ortak ve çok taraflı mücadele etmeyi amaçlayan ve siber güvenliği güçlendiren siber normların oluşturulmasının devletler için -özellikle de önümüzdeki dönemde- yaşamsal bir öneme haiz olacağını öne sürmek doğru olacaktır.

3.1.1. ABD

Siber uzayda İnternetin yönetişimi bağlamında çok paydaşlı İnternet yönetişim modelini savunan ABD, çok paydaşlılığı korumakta ve tüm paydaşların bu sahada söz sahibi olmasını desteklemektedir. ABD'nin siber yönetişim anlayışı ülkenin 68. Dışişleri Bakanı John Kerry tarafından şu şekilde açıklanmaktadır: "Temelde yukarıdan aşağıya olan birçok hükümet modelinden farklı olarak İnternet'in, tüm paydaşların – özel sektör, sivil, toplum, akademisyenler, mühendisler ve hükümetler – masada koltuk sahibi olmasına izin verdiğini anlamaktayız. Bu teknolojinin dinamik doğası nedeniyle, ufukta sürekli yeni sorunlar görünmektedir. Ancak çok paydaşlı yaklaşım, bu zorlukları çözebilmenin en adil, en iyi ve en etkili yolu olmaya devam etmektedir (Kerry, 2015)."

ABD Hükümeti Yayıncılık Ofisi'nin, 2015 yılının Şubat ayında Senato'nun daimi komitesi olan ABD Ticaret, Bilim ve Ulaşım Senato Komitesi önderliğinde gerçekleşen duruşma çıktılarına bakıldığında, "İnternet Yönetişimin Çok Paydaşlı Modelini Koruma" adlı bir başlığa sahip olduğu göze çarpmaktadır. ABD Senatörü John Thune tarafından yapılan açılış konuşmasında duruşmanın temel amacı, otoriter rejimler tarafından parçalanmayan ve gasp edilmeyen tek bir küresel İnternet oluşturulmasına yönelik talep olarak belirtilmektedir (U.S. Senate, 2015). Sorgulanan nokta ise, bu talebin sağlanması yolunda nasıl aksiyon alınacağı olmuştur. Bu duruşma, Komite'nin İnternet yönetişimine yönelik ilk duruşması olsa da, 2014 yılında ABD Ulusal Telekomünikasyon ve Bilgi İdaresi'nin (NTIA) işlevlerini hükümet önderliğinden çıkararak küresel çok paydaşlı bir topluluğa duyurma açıklamasını yapmasının ardından, otuz beş Senatör tarafından İnternet yönetişiminde aşağıdan yukarıya ve çok paydaşlı bir yaklaşımı destekleyen bir kararlılık ortaya koyulmuştur.

Aynı belgede, İnternet yönetişimi üzerine, NTIA tarafından sunulan kriterler şunlar olmuştur (U.S. Senate, 2015):

- Çok paydaşlı modelin desteklenmesi ve geliştirilmesi;
- Internet DNS'sinin güvenliğinin, istikrarının ve esnekliğinin korunması;
- Küresel müşterilerin ve ortakların ihtiyaç ve beklentilerinin IANA tarafından karşılanması;
- İnternetin açıklığının korunması.

İnternet yönetişimine kısaca bir göz atıldığında, Alan Adı Sistemi olarak adlandırılan DNS'nin, küresel altyapı bakımından kritik bir unsur olduğunu belirtmek gerekmektedir. İnternetin adres defteri olan DNS, 165.211.126.523 gibi sayısal ağ adresleri yerine Yalova.edu gibi anlaşılması kolay tanımlamalar yaparak kullanıcıların web-sitelerini ve posta sunucularını düzenlemeye yaramayan önemli bir sistemdir. 1998 yılının Haziran ayında alınan karara göre, NTIA'nın yayınladığı bir DNS Teknik Raporu ile DNS'e ait temel işlevlerin özel sektör yönetimi altında gerçekleştirilmesi sonucuna varılmıştır (Brotman, 2015: 1). Burada amaç, İnternet işlemlerine küresel katılımın kolaylaşmasını sağlamak olmuştur.

Yukarıda bahsedilen amaca ulaşabilmek ve böylece DNS politikasını koordine etmek ve yönetmek için NTIA tarafından kar amacı gütmeyen bir şirket ile bir anlaşma imzalanmıştır (Brotman, 2015: 1). Bu bağlamda, İnternet Tahsisli Sayılar ve İsimler Kurumu'nun (ICANN) da taraf olduğu bir uzlaşı belgesi hazırlanmıştır. Bu belgeye göre DNS koordinasyonu ve yönetimsel işlevler NTIA'nın gözetimine tabi tutulacaktır. Uzlaşı belgesi, İnternet'in sürekli olarak verimli bir şekilde işlerliğini sağlamak amacıyla, 2000 yılında NTIA'nın tüm İnternet Tahsisli Sayılar Otoritesi'ne ait işlevlerini tek bir kaynakta toplayan bir sözleşme ile değiştirilmiştir.

ABD'nin yönetişim kısmındaki bir diğer faaliyeti ise, Bulut bilişim konusunda olmaktadır. Bulut bilişim, doğası gereği konum, coğrafya ve sınırları aşmaktadır. Bir diğer ifadeyle, bir ülkede erişilen veriler dünyanın yarısında hatta birden çok ülkedeki sunucularda saklanabilmektedir. Uluslararası hukuk ise, doğası gereği dünyayı konum, coğrafya ve bölgesel sınırlarla bağlantılı olan çeşitli yargı alanlarının penceresinden görmekte ve dijital

dünyaya geleneksel bir bakış açısı sunmaktadır. Bu sebeple, bulut bilişim ve uluslararası hukukun etkileşime girmesi sonucu birtakım problemler ortaya çıkabilmektedir. Örneğin, 2013 yılının Aralık ayında ABD Federal Hükümeti tarafından 1986 Elektronik İletişim Gizliliği Yasası kapsamında Microsoft'a bir arama emri maddesi sunulmuştur. Bu maddeyi baz alan ABD Hükümeti, e-postalarının içeriği ve diğer bilgileri Microsoft tarafından depolanan bir kullanıcının hesabıyla ilişkili bilgilerin aranması ve el koyulması için bir arama emri başvurusunda bulunmuştur (Electronic Frontier Foundation, 2021). Bunun üzerine Microsoft tarafından, içerik dışı kayıtların ABD'de saklandığı ancak bahsi geçen e-postaların içeriğinin Dublin'deki bir sunucuda depolandığı fark edilmiştir. E-postalar yalnızca İrlanda'da bulunduğu için Microsoft, ABD'li bir yargıcın yurtdışında saklanan kayıtlar için arama emri çıkarma yetkisinin olmadığını ileri sürmüş ve bu karara itiraz etmiştir. ABD Hükümeti ise, verilere ulaşmak için izlenen adımların ABD sınırları içerisinde gerçekleştirilmesi sebebiyle uluslararası hukuk tarafından desteklendiğini öne sürerek e-postaların teslimini istedi (Electronic Frontier Foundation, 2021).

Microsoft'un bir sonraki itirazı ise, bölge mahkemesine yapılmış; mahkemede, ABD hükümeti tarafından yurtdışına yönelik çıkarılan arama emrinin geçerli olamayacağı ve durumu çözebilmek adına ABD-İrlanda karşılıklı adli yardım anlaşmasının yapılması gerektiği öne sürülmüştür (Electronic Frontier Foundation, 2021). Bu kararın da reddi sonucu, İkinci Daire'ye temyize giden şirket, polis tarafından ABD dışında depolanan dijital içeriğin açığa çıkarılması için zorlanamayacağı şeklinde bir karar elde etmiştir. 2017 yılına gelindiğinde ABD Yüksek Mahkemesi davayı incelemiş ve 2018 yılı başlarında Bulut Yasası'nın da kabulüyle, davanın tartışmalı olduğu gerekçesiyle Microsoft'un aleyhine çıkan kararları iptal etmiştir (Electronic Frontier Foundation, 2021).

2017 Mayıs ayında ABD Adalet Bakanlığı tarafından Elektronik İletişim Gizlilik Yasası'nı (ECPA) değiştirecek ve ABD'li servis sağlayıcılara, kayıtların ve haberleşme içeriklerinin, hukuka uygun bir süreç izleyen, insan haklarını dikkate alan ve gizlilik standartlarına uyan yabancı hükümetlere açıklanması için bir yasa sunulmuştur. ECPA'nın bu bağlamda güncellenmesi sonucu, kanuni yaptırımlar noktasındaki dijital kanıtlara bakılması taleplerinin verilerin konumuna göre değil kullanıcının konumuna ve uyruğuna göre dikkate alınması gerektiği öne sürülmektedir (Walker, 2017). Bir devlet ve özel şirketi karşı karşıya getiren ABD-Microsoft vakasından da anlaşıldığı üzere, uluslararası hukukun geleneksel yaklaşımlarının aksine, dijital çağa adapte olacak yeni norm ve kurallara ihtiyaç duyulmaktadır. Bu sürecin desteklenmesi için tüm aktörlerin işbirliğine gitmesi ve sürecin anlamlandırılarak belirsizliğinin azaltılması yolunda çalışmalar gerçekleştirmesi gerekmektedir.

ABD dış politikası, ulusal güvenlik, insan hakları ve ekonomik zorunlulukları etkileyen tüm uluslararası siber politika konularıyla bütünleşen Siber Sorunlar Koordinatörlüğü Ofisi (S/CCI), siber sorunların sadece ABD için değil tüm dünya için bir dış politika önceliği olduğunu öne sürmektedir (Office of the Coordinator for Cyber Issues, 2021). Siber uzayda istikrar ve güvenliği teşvik eden kurum 2011 yılında kurulmasından bu yana, yirmiden fazla ülkeye ilham vererek dışişlerine bakanlığa bağlı benzer siber kurumlar kurmalarını sağlamıştır.

Yaklaşık yirmi yıl boyunca İnternet adlandırma ve adresleme sistemini denetledikten sonra Ekim 2016'da sorumluluğu teknolojik şirketler, STK'lar ve hükümet paydaşlarından oluşan bir koalisyona devreden ABD hükümeti, bu adım noktasında çok sayıda aktörden destek ile karşılaşmıştır (Stifel, 2017: 1). Ancak diğer yandan İnternet yönetişimi üzerine ABD'nin liderliğinin geri plana atıldığı bir durum görülmekte olduğundan, devletin bu alandaki etkisini devam ettirmek için alternatif yollar bulması önemlidir. ABD'nin bunu yapabilmek için seçeceği en uygun yöntem, güvenlik açıklarını ortadan kaldırmak, İnternetin güvenilirliğini ve dayanıklılığını arttırmak için teknoloji şirketleriyle işbirliğine girmek ve gelişmekte olan İnternet piyasalarındaki liderlerin yetişmesi üzerine gerçekleştirilebilecek çabaları çoğaltmaktır (Stifel, 2017: 1).

ABD hükümeti, ABD'nin finanse ettiği araştırma anlaşmalarının, bireylerin ve onlardan sorumlu şirketlerin oluşturduğu dağınıklık üzerinde bir düzen sağlamak ve tüm bu sorumlulukları yüklemek amacıyla, İnternetin işlerliğini sağlayan IANA'yı 2000 yılına kadar özelleştirmeye çalışmıştır (Stifel, 2017: 1). Ancak özelleştirme için son tarihin kaçırılması sonucu NTIA tarafından IANA'ya ait işlevlerin yürütülmesi için ICANN ile sözleşme yapılmıştır. Bu durum, aktörlerden birçoğunun İnternet'in kontrolünün ABD hükümetine ait olduğu yönünde bir algıya sahip olmalarına sebep olmuştur (Stifel, 2017: 1).

ABD'nin İnternet'teki hâkimiyeti üzerine oluşan bu algı sonucu, tartışmalar kapsamında iki grup ortaya çıkmıştır. Gruplardan ilkini Batılı hükümetler ve özel sektör oluştururken, ikincisini ise, Rusya ve Çin oluşturmaktadır. Birinci gruba göre İnternet; işletmeler, kamu yararına çalışan gruplar, uzmanlar ve hükümetler gibi paydaşların uzlaşmalarına dayalı karar içeren bir yapıya sahip olmaktadır. Rusya ve Çin tarafından öncülük edilen ikinci grup ise, interneti yönetmek için ulusal hükümetlerin çevrimiçi düzeyde ana kural koyucular olacağı hükümetler arası bir yaklaşım önermektedir. Tartışmalar sürmeye devam ederken, 2013 yılında Edward Snowden'in ABD istihbarat programlarını ifşa etmesiyle birlikte, ülkeler ABD'nin internet trafiği merkezi olarak kabiliyetlerini istihbarat amaçlı kullanmasını büyük ölçüde eleştirmişlerdir. Gelen yoğun eleştiriler sonucu internet paydaşlarını ICANN'dan ABD'nin nüfuzunun kaldırıldığı bir çözüm bulmasını talep etmişlerdir. ABD idaresinden vazgeçilmesiyle birlikte otoriter hükümetlerin kontrolü ele alacağı endişelerine sahip olan bir kesim olsa da, çok paydaşlı yaklaşımı savunan aktörler tarafından bu fikir desteklenmiş olup 2016 yılının Ekim ayında IANA işlevlerine ilişkin NTIA sözleşmesinin süresi sona ermiş ve doğrudan ABD yönetimi olmaksızın İnternet yönetişiminde yeni bir dönem başlamıştır (Stifel, 2017: 1-2).

İnternet yönetişimi tartışmalarının merkezinde, çok paydaşlı süreç ve paydaşların bu sürece katılımı, İnternet'in yönetimi hakkında teknik kararları kimin alması gerektiği ve İnternet ile ilgili kamu politikasını kimin oluşturması gerektiği soruları yer almaktadır. Bu konuya yönelik ABD'nin tutumu ise, İnternet'in geleceği hakkında kararlar alındığında özel sektör, sivil toplum, akademisyenler, teknik uzmanlar ve hükümetlerin aynı masada oturması gerektiğini savunmak ve tercih ettiği çok paydaşlı yönetişim modeli çerçevesinde İnternetle ilgili ulusal düzeyde kamu politikalarının geliştirilmesi için çok paydaşlı süreçler geliştirme

noktasında devletleri teşvik etmeye devam etmektir (Office of the Coordinator For Cyber Issues, 2015: 2).

IANA sözleşmesinin bitmesinin ardından, İnternet esnek bir platform olarak yerini korumakta olsa da sürdürülebilir bir liderlik olmadan uzun vadede faydasını sınırlayabilecek teknik ve politik zorluklarla karşılaşma olasılığı söz konusu olmaktadır (Stifel, 2017: 2-3). Zira otoriter hükümetler, küresel ekonomik büyümeyi sınırlayabilecek ve ciddi içerik kontrolü ile sonuçlanabilecek bu zorluklardan yararlanma eğilimi gösterebilme potansiyeline sahiptirler. ABD'nin stratejik çıkarları doğrultusunda bir değerlendirme yapıldığında, İnternet yönetişimi ABD için öncelik olarak kalmaya devam etmeli ve bahsedilen zorlukları önlemek amacıyla devlet tarafından atılacak adım ise, İnternetin güvenilirliğini ve dayanıklılığını artırmak için teknik çözümlerin geliştirilmesini desteklemek ve kalan kullanıcıları da çevrimiçi hale getirmek için tüm paydaşların dâhil olduğu girişimlere katılmak olmalıdır (Stifel, 2017: 3).

3.1.2. Çin

Teknolojinin gelişmesiyle birlikte, siber teknoloji bir yandan refah yaratırken diğer yandan ise, siber suçları, casusluğu ve potansiyel olarak siber savaşın önünü açmaktadır. Bu tez çalışmasında, Çin'in siber güvenlik ve İnternet yönetişimi konularında gerçekleşen uluslararası müzakerelerde siber egemenlik kavramını dayattığı ve bu kavramı güçlendirmek için bazı hedeflere sahip olduğu öne sürülmektedir. Öncelikle siber egemenlik kavramının siber güvenlikten farklı olduğunu belirtmek gerekmektedir. Zira siber güvenlik İnternet'e bağlı altyapı ve süreçlerin korunmasını içerirken, siber egemenlik ise, İnternet tarafından sağlanan bilgi ve içeriğe odaklanmaktadır. Lindsay'in öne sürdüğü üzere (Lindsay vd., 2015), siber egemenliğin merkeze aldığı iki temel ilke söz konusudur. Birinci ilkeye göre, bir devletin, bilgi alanında istenmeyen bir etkiye veya müdahaleye maruz kalması yasaklanmalıdır. Diğer bir deyişle, siber egemenlik bağlamında bu madde detaylı bir şekilde okunduğunda, rejim tarafından zararlı görülen fikir ve görüşlerin vatandaşlara tesirini engellemek olarak ifade edilebilmektedir. Siber egemenliğin ikinci ilkesi ise, İnternetin yönetişiminin uzmanlar ve şirketler gibi devlet-dışı aktörlerin yer aldığı sistemden, devletlerin temel aktörler olduğu BM gibi bir uluslararası foruma geçirilmesini ifade etmektedir. Bu madde, çok paydaşlı yönetişimin gündemden düşürülerek gücün devletler tekelinde toplanacağı bir rejim tahayyülü ortaya koymaktadır.

İnternet yönetişimindeki yaklaşımlardan biri olan siber egemenliğin Çin tarafından net bir duruş şeklinde desteklenmesi, tanımlanması, yorumlanması, geliştirilmesi ve teşvik edilmesi Çin'in siber uzaydaki perspektifini ve rolünü anlamak açısından önemlidir. Yukarıda bahsi geçen siber egemenlik ilkelerini, Çin'in nasıl yorumladığına bakmak gerekmektedir. Çin'e göre siber egemenlik yaklaşımı; ülke, ulus ve parti anlatılarını kontrol etmek üzerine kurulu olup, bilgi güvenliği gibi kritik olan bir sahada Çin için, temel değerlerin korunması noktasında bir araçtır (Schia ve Gjesvik, 2017). İnternet ve içeriğinin kontrolü ve yönetimi sağlandığında siber egemenlik yaklaşımı pratiğe dökülmüş olmaktadır. Bütün bunların sağlanması için ise, siber güvenliğin devlet odaklı bir yorumu çerçevesinde teşvik edilmesi önemlidir. Zira siber güvenlik sağlanmadan kontrol ve yönetimi sağlamak olası görünmemektedir.

Çin'in İnternet yönetişimine yaklaşımında, İnternet altyapısı gibi teknik konuların yanı sıra İnternet'in içeriğinin de oldukça kıymetli olduğu bir perspektif görülmektedir. İnternet'e erişim oranının sürekli artış gösterdiği Çin'e, siber egemenliğin uzun vadede getirisi, Çin'in Batı yapımı teknolojilerden özgürleşerek teknolojik bağımsızlığa ulaşması olacaktır (Schia ve Gjesvik, 2017). Bu süreç sonuçlanana kadar ise, İnternet içerisindeki bilgi akışını kontrol etme yönünde faaliyetlerde bulunan Çin, böylece iç istikrarını korumaya çalışmaktadır.

Çin'in İnternet yönetişimine yaklaşımı konusundaki gelişmelerine bakıldığında, 2016 yılının Aralık ayında Çin Siber Uzay İdaresi (CAC) tarafından yeni bir siber güvenlik stratejisi sunulduğu göze çarpmaktadır. Bu strateji; İnternet'in vatana ihanet, ayrılma, isyan, hükümeti devirme ve devlet sırlarının çalınması ve sızdırılması doğrultusunda kullanılmasının cezalandırılacağı şeklinde bir uyarı içermektedir (Schia ve Gjesvik, 2017).

İlki 2014 yılında gerçekleşen ve kaynaklarda adı Dünya İnternet Konferansı olarak da geçen Wuzhen Zirvesi, Çin'in dış politikasını ve siber güvenlik konusundaki duruşunu teşvik ettiği ana alandır. Aynı yıl, Başkan Xi Jinping'in liderliğini üstlendiği Siber Güvenlik ve Bilgilendirme için Merkezi Lider Grubu'nun kurulduğunun duyurulması ise, Çin'in dış politika anlamında reformlarını derinleştirdiği, ulusal güvenliği ve ulusal çıkarları koruma noktasındaki tedbirlerini arttırdığı ve bilgi teknolojisinin gelişimini teşvik ettiği konusundaki kararlılığını yansıtmaktadır (China Copyright and Media, 2014)

2015 yılına gelindiğinde ise, CAC başkanı Lu Wei tarafından siber egemenliğin çok paydaşlı ve çok taraflı iki yaklaşım arasındaki fark olarak tanımladığına rastlanmaktadır. İki yaklaşım arasındaki fark, devletin üstünlüğünün siber alanda ne ölçüde geçerli olduğu üzerinedir; çok paydaşlı yaklaşımda tüm aktörlerin söz sahibi olduğu bir durum geçerliyken, çok taraflı yaklaşımda ise, ikiden fazla devletin aynı amaç uğruna bir araya gelmesini ifade etmektedir. Siber egemenlik, ne çok paydaşlı yaklaşım kadar devleti geri plana atmakta; ne de çok taraflı yaklaşım kadar devleti merkeze almaktadır.

Ekonomik büyüme için çözüm ve fırsatlar sağlaması hedeflenen Çin'in "Güvenli Şehirler Projesi"nin arka planında, Çin şehirlerinin kentleşmeye bağlı olarak daha fazla insan gücü ve tüketici ihtiyacını karşılamak için olağanüstü oranlarda büyümesi yer almaktadır (Lin, 2015). Çin Hükümeti, proje bağlamında daha fazla ekonomik büyüme elde edebilmek için 2025 yılına kadar 250 milyon kişiyi kırsal kesimden şehirlere yerleştirerek ülkesini yeniden yapılandırmayı planlamaktadır. Öncesinde 650 şehirde en son teknoloji ile kamu güvenliği altyapılarını iyileştirmeyi amaçlayan ülke çapında kapsamlı bir program başlatılmıştır ve bu program yavaş yavaş Güvenli Şehirler Projesi olarak adlandırılan bir projeye dönüşerek Orta Asya ülkelerine nüfuz edecek kadar gelişme göstermiştir. Proje kapsamında, altyapıların iyileştirilmesi konusunun kapsamı, eğilimleri ve tahminlerine ilişkin analizler sağlamak için büyük verilerin toplanmasından yararlanmak ve böylelikle sorunlara ilişkin çözümler üretebilmek hedeflenmektedir (Lin, 2015). Güvenli şehirlerin inşası süreci, 2003 yılında dört pilot şehir olarak seçilen Pekin, Jinan, Hangzhou ve Suzhou ile başlayarak günümüze kadar gelmiştir. Çin, güvenli şehirlerin inşasını temel altyapı, ağ entegrasyonu, üst düzey uygulamalar ve tüm bu uygulamaların entegrasyonu şeklinde dört aşamaya ayırdığı bir plan izlemektedir (Lin, 2015). Tüm bu idealist yaklaşımlarının yanında proje

kapsamında gözetim ekipmanlarının yerleştirilmesi ve arttırılması konusunu merkeze alan Çin, vatandaşların izlenmesi ve İnternetin yönetilmesi için bir sistem sunmaktadır.

Orta Asya ülkelerinde de oldukça etkisini gösteren Güvenli Şehirler Projesi bağlamında, 12 Şubat 2019 tarihine Kırgızistan'ın Bişkek kentinde başlatılmış olup, şehirdeki 10 kavşağa ve 2 üst geçide sabit kameralar kurulmuştur. Bişkek otoyoluna da 15 kameranın yerleştirildiği projede, güvenli şehir kameralarının kayıt boyunca takip edeceği kırmızı ışıkta geçme, geri geri gitme; kaldırımlara, bisiklet yollarına ve yeşil kuşaklara giden motorlu taşıtlar; yaya geçidine geçme; yayalara kaba davranma; aşırı hız; yasadışı park etme olarak yedi ihlal belirlenmiştir (Ruowei, 2019b). Kuralları ihlal edenlerin 30 gün içinde para cezası ödemeleri gerektiğinden, süreci hızlandırmak için cezanın son ödeme tarihinden sonra, her gün para cezasının % 1'i tutarında ek gecikme ücreti uygulanmasına karar verilmiş olup, ek gecikme ücreti ilk para cezasına eşit olduğunda ihlal davasının mahkemeye intikal etmesi şeklinde bir süreç işlenmesi planlamıştır.

Tacikistan'da ise, 1 Kasım 2013'te projenin başlatılmasından şu ana kadar başkent Duşanbe'deki 95 kavşağa toplam 1.200 kamera, halka açık alanlara ve parklara da 800 kamera yerleştirilmiştir. Proje, Çinli Huawei tarafından hayata geçirilmiş ve 20.91 milyon doları Şanghay İşbirliği Örgütü çerçevesinde Çin tarafından verilen bir kredi olmak üzere 22 milyon ABD dolarına mal olmuştur (Ruowei, 2019b). Tacikistan hükümeti, proje kapsamındaki ihlallerden toplanan para cezalarını, krediyi 20 yıl içinde geri ödemek için kullanmayı planlamaktadır.

Fotoğraf 5. Tacikistan'da Güvenli Şehir Kameralarından Şehrin Düzenini Takip Eden Yetkililer

Kaynak: Weixin, "**道路千万条　安全第一条**" **中**亚各国"**安全城市**"项目来了！(Çev. Orta Asya ülkelerinde "Güvenli Şehirler" projesi burada!), 2019

Projeye yönelik 2006 yılında harekete geçen Kazakistan'ın Astana şehrinde ise, proje kapsamında toplam 2.000 kamera kurulmuştur (Ruowei, 2019b).

Fotoğraf 6. Astana'da Güvenli Şehir Projesi Kapsamında Kameraların Dağılım Haritası

Kaynak: Weixin, "**道路千万条　安全第一条**" **中**亚各国"**安全城市**"项目来了！(Çev. Orta Asya ülkelerinde "Güvenli Şehirler" projesi burada!), 2019

Kazakistan'da proje kapsamında yer alan Kırmızı Hız sistemi; kırmızı ışıkta geçme, çizgileri geçme, çizgilere basma, geri gitme, yasadışı park etme, karayolu ile demiryolunun kesiştiği kavşaklarda trafik kurallarının ihlali gibi birçok ihlali tespit etmektedir.

Türkmenistan'da ise, Haziran 2009'da başlayan projeye bağlı olarak Aşkabat'ın ana yollarına ve ana caddelerine 133 kamera yerleştirilmiştir (Ruowei, 2019b).

Fotoğraf 7. Aşkabat'ta Güvenli Şehir Projesi Kapsamında Kameraların Dağılım Haritası

Kaynak: Weixin, "**道路千万条　安全第一条**" **中**亚各国"**安全城市**"项目来了！(Çev. Orta Asya ülkelerinde "Güvenli Şehirler" projesi burada!), 2019

Bir diğer ülke olarak Özbekistan'daki Güvenli Şehir projesi 17 Mart 2017'de başlatılmış olup şehrin 115 kavşağına 883 kamera yerleştirilmiştir (Ruowei, 2019b). Mevcut düzende kamera yalnızca kırmızı ışıkta geçme ve aşırı hız gibi ihlalleri kaydedebilse de, gelecekte sürücünün emniyet kemeri takıp takmadığını tespit etme işlevini de gerçekleştirmesi hedeflenmektedir. Özbekistan'da ihlali tespit edilen sürücüler cezayı iki ay içinde ödemek zorundadır, aksi takdirde taşıta el koyulması şeklinde bir cezalandırmaya gidilmektedir.

Fotoğraf 8. Taşkent İçişleri Genel İdaresi İzleme Merkezi

Kaynak: Weixin, "**道路千万条　安全第一条**" **中**亚各国"**安全城市**"项目来了！(Çev. Orta Asya ülkelerinde "Güvenli Şehirler" projesi burada!), 2019

Kırgızistan ulusal haber ajansına göre, proje sayesinde yoldaki kaos ortadan kalkmış ve taksi şoförleri rotalarında dürüstçe kuyruğa girmeye başlamıştır. Dönerken sollama veya karşı şeride girme ortadan kalkmıştır. Ancak diğer yandan birçok Bişkek vatandaşının

trafik sıkışıklığı nedeniyle hedeflerine zamanında ulaşamadıklarından şikâyet ettikleri görülmüştür.

Çin'in Güvenli Şehirler Projesi bağlamında Orta Asya'da büyük çaplı bir etkiye sahip olacağı aşikârdır. Bu çalışmada, altyapısı yeterli olmayan Orta Asya devletlerinin Çin'den teknoloji düzeyde destek aldığı ve almaya devam edeceği çıkarımı yapılmaktadır. Burada önemli olan nokta ise, Orta Asya'da önemli bir nüfuza sahip olan Rusya'nın bu konuda izleyeceği politikalar olacaktır.

3.1.3. Rusya

Rusya, İnternet yönetişimi anlamında son yıllarda aktif bir şekilde Çin'in siber egemenlik yönetişimi modelini taklit etmektedir. Bu durum bir yandan Putin'in siyasi gruplar karşısındaki konumunu güçlendirirken; diğer yandan ise, Rusya'nın ulusal güvenliğine zarar verme ve yakın ülkeler üzerindeki nüfuzunu azaltma riskini de beraberinde getirmektedir (Weber, 2020). İnternet üzerinde tüm devletlerin bir noktaya kadar egemenlik iddiası söz konusu olsa da; Rusya ve Çin siber egemenlik üzerine, liberal demokrasilerin meşru siyasi görüşler olarak gördükleri şeylerin kontrolünü içeren daha geniş kapsamlı bir tanım benimseme eğiliminde olmaktadırlar (Weber, 2020).

Yaklaşımın arka planına göz atıldığında; 2018 yılında Rusya, BM Genel Kurulu'nda egemenlik ve iç işlerine müdahale edilmemesine vurgu yaparak devlet gözetimini ve sansürü meşrulaştırdığını iddia edilen bir karar önermiştir. Bu önerinin ardından BM GGE ile paralel olarak çalışması amacıyla 72/27 sayılı karar çerçevesinde, Genel Kurul tarafından tüm üye devletlerin katılmaya davet edildiği bir Açık Uçlu Çalışma Grubu (OEWG) kurulmuştur. OEWG, ABD'deki siber normlar noktasında ikiliğe sebep olurken Rusya için ise, GGE raporlarının Rusya'nın İnternet yönetişimi tercihleriyle yeniden yorumlanabilmesi için bir forum fırsatı olarak düşünülebilmektedir. Zira çok taraflı forumlarda Rusya ve Çin, siber alandaki normları egemenlik ve devlet odaklı bir yaklaşımla ele alırken; GGE raporları tarafından ise, devletlerin bahsedilen normların uygulaması üzerinde durulmakta ancak devletlerin bu normları nasıl ve hangi çerçevede uygulayacaklarına dair bir plan sunulmamaktadır. Bu nedenle devletler arasında siber normların uygulanması evresinde ciddi farklılıklar yaşanmakta sansür yasalarından ağı kapatmaya kadar birçok yöntem kullanılmaktadır. Örneğin, geçmiş uygulamalara bakıldığında Rusya'nın siber egemenliği uygulama biçiminin, dijital ortamın kontrolünü ağlamak için muhalifleri sessizliğe itmek gibi genellikle çevrimdışı yöntemler içermekte olduğu görülmektedir. 2012 yılında Rusya'da kapsamlı bir siyasi reformun talep edilmesi sonucu gerçekleşen protestolara bağlı olarak Çin'in bilgi kontrolü yaklaşımını benimseyen Rusya, o yıldan beri Çin gibi küresel İnternetten uzak durmaya çalışmakta, VPN kullanımında kısıtlamayı takip etmekte ve kapsamlı sansür araçlarının konuşlandırılması yönünde ilerlemektedir (Weber, 2020).

Rusya'nın İnternet yönetişimi anlayışının şekillendiği bu süreçte bir diğer önemli nokta ise, Rusya'nın düzenli olarak Çin'e bu konuda danışmasıdır. Küresel bilgi alanını şekillendiren yeni BİT'lerin geliştirilmesi ve uygulanmasındaki önemli ilerlemeleri dikkate alarak 2015 yılında uluslararası bilgi güvenliğinin sağlanmasında işbirliğine gitmeyi amaçlayan bir siber güvenlik anlaşması imzalayan iki devlet, devletlerin egemenliklerini ve

güvenliklerinin zayıflatılması ve içişlerine müdahale edilmesi niyetiyle gerçekleşebilecek uluslararası tehditlere karşı endişelerini dile getirmişlerdir (Rusya Federasyonu Hükümeti ve Çin Halk Cumhuriyeti Hükümeti, 2015). Anlaşmaya göre, Şangay İşbirliği Teşkilatı çerçevesinde ortak çalışmayı vurgulayarak, iki devlet kendi topraklarındaki altyapı, güvenlik ve bilgi ve telekomünikasyon ağı olan İnternet ile ilgili konularda kamu politikaları belirleme ve uygulama konusunda egemen haklara sahip olduklarını öne sürmektedirler. Anlaşmada taraflar bilgi güvenliğini; bireylerin, toplumun ve hükümetin bilgilerine yetkisiz erişim gerçekleştirilmesi, bilgilerin izinsiz kullanılması, ifşa edilmesi, aksatılması, değiştirilmesi, incelenmesi, denetlenmesi, kaydedilmesi ve imha edilmesine karşı koruma uygulamaları şeklinde tanımlamaktadır (Government of the Russian Federation and Government the People's Republic of China, 2015). Buna ek olarak bilgi ve telekomünikasyon ağının uluslararasılaşmasını kontrol etmek için çok taraflı, şeffaf ve demokratik bir İnternet ortamı oluşturmaya çalışmak ve devletlerin demokratik yönetişim de dahil olmak üzere bu sürece eşit katılım haklarına sahip olmasını içeren anlaşma bağlamında belirlenen tehditler ise, şu şekildedir (Government of the Russian Federation and Government the People's Republic of China, 2015):

- Devletlerin egemenliğini, güvenliğini, toprak bütünlüğünü ihlal eden ve uluslararası barış, güvenlik ve stratejik istikrarı tehdit eden saldırgan eylemler
- Bilgi altyapısı üzerinde yıkıcı hasarlar oluşturan ve ekonomik anlamda zarara sebep olan eylemler
- Terörist amaçlar için gerçekleştirilen eylemler
- Verilere yetkisiz erişimi de içine alan saldırı ve suçlar
- Devletlerin içişlerine, kamu düzeninin ihlaline, etnik, ırksal ve dinsel nefretin kışkırtılmasına, yabancı düşmanı fikirlerin propagandasına, nefret ve ayrımcılığa, şiddete ve istikrarın bozulmasına neden olan her türlü propaganda eylemleri, sosyo-ekonomik durumun istikrarsızlaştırılması, hükümete saldırı gibi eylemler
- Diğer devletlerin sosyo-politik ve sosyo-ekonomik sistemlerine, manevi, ahlaki ve kültürel çevresine zarar verebilecek bilgilerin yayılmasını içeren eylemlerdir.

2015 yılındaki anlaşmanın ardından 2019 yılında ise, İnternetteki yasa dışı içerikleri yönetmek için uluslararası bir anlaşma imzalamıştır. Bu anlaşma sonucu Rusya yetkililer, İnternette Çin tarzı kontroller uygulamaya çalışmakla suçlanmışlardır (Tsydenova ve Balmforth, 2019). Rusya Devlet Başkanı Putin ve Çin Devlet Başkanı Xi Jinping yönetiminde İnternet kontrollerinin sıklaştırılmasına sebep olacak bu işbirliğinin, İnternet özgürlüğünü savunan taraflar tarafından tepki çekeceği öngörülmektedir (Tsydenova ve Balmforth, 2019). ABD'nin İnternet platformunda yer alan büyük çaplı nüfuzu devam ederken, Çinli bilgisayar korsanlarının ABD'nin kritik altyapısına yönelik büyüyen bir tehdit oluşturduğu, askeri ve politik sırları çalmak için kampanyalar yürüttüğü, aynı şekilde Rus bilgisayar korsanlarının da siber casusluk tehdidi oluşturduğu, operasyonları etkilediği ve ABD ve müttefiklerinin altyapısına saldıracak faaliyetlerde bulunduğu unutulmamalıdır (Segal, 2020). Bu bağlamda siber uzayı kendi imajlarında yeniden yaratmaya çalışan taraflar, ABD'nin etkisini azaltmak için İnterneti yeniden şekillendirme amacıyla işbirliğine gitmekte olup, 2015 yılından bu tarihe kadar İnternet üzerindeki kontrolleri

sıklaştırmak için birlikte çalışmakta ve ABD'nin siber uzayın küresel yönetişimi üzerindeki etkisini azaltmak için siber egemenlik fikrini teşvik etmektedirler (Segal, 2020).

Diğer yandan Rusya, Çin ile olan işbirliğine rağmen siber egemenlik modelini taklit etmekte zorluklarla karşı karşıyadır. Çin geniş bir iç pazara ve şirketleri aracılığıyla sosyal medya platformlarını ve yerli kitleleri tatmin eden yerli içerikler sağlama gibi kabiliyetlere sahipken, Rusya ise, bu koşullardan yoksun olup derin paket inceleme araçlarının ülke çapında kurulumunu geciktiren teknik zorluklarla karşılaşmaktadır (Weber, 2020). Örneğin, ülke içinde oldukça popüler olan Telegram'dan, kullanıcıların şifrelenmiş mesajlarına erişim izni verilmesini talep eden Rusya, Telegram'ın bu karara uymayı reddetmesi sonucu uygulamayı ülkede yasaklamıştır (Kolomychenko, 2018). Ancak hizmeti engellerken, Viber, Volvo ve Xiaomi gibi birçok çevrimiçi hizmete erişimi engelleyen Rus yetkililer, bu aksaklık nedeniyle Telegram'ı engelleme girişimini askıya almıştır. Sorun, Telegram trafiğini barındıran İnternet Protokolü (IP) adreslerinin birçok hizmet için trafiği barındırması olmuştur. Derin Paket İnceleme sistemi, İnternet trafiğini analiz eden ve tamamını engellemek yerine belirli bir hizmetin veri akışını engelleyen daha sistematik bir işleyiş ortaya koymaktadır (Kolomychenko, 2018). Ancak diğer yandan, Kremlin ve federal hükümetin kabinesi arasında ortaya çıkan anlaşmazlık nedeniyle, bu sistemin kurulumunda gecikme yaşanmaktadır. Kabine tarafından bu ekipmanın kurulumu desteklenirken, Kremlin yetkililerinin açıklaması ise yeni İnternet izolasyon yasasının teknik olarak yürürlüğe girdiği ancak ülkenin her yerinde fiilen uygulanamayacağı üzerinedir (The Bell, 2019).

Çin'in siber egemenlik modelini taklit eden Rusya için bu durumun temelde iki olumsuz sonucu bulunduğunu söylemek gerekmektedir (Weber, 2020). Bunlardan birincisi, ulusal güvenlik ve istihbarat anlamında riskleri beraberinde getireceği, diğer bir deyişle Çin modelini kopyalamanın Çin teknolojisinin ithalatı ve bağımlılığı anlamına gelmesi ve dolayısıyla Rusya'nın Çin casusluğuna maruz kalabileceği anlamına gelmektedir. Ancak Rusya yabancı ekipmanı yasaklamak istese de, altyapısı buna izin vermeyebilir. Örneğin, ülke içinde bulunan yüz tanıma kameraları Rus yazılımını kullansa da Çin donanımıyla çalışmakta; Huawei Rusya'nın 5G altyapısını oluşturmaktadır. Tüm bunlar düşünüldüğünde Moskova'nın güvenlik endişelerine sahip olması doğal olsa da teknik zorluklar bu endişeleri gölgede bırakmaktadır. İkinci olumsuzluğa gelindiğinde, Rusya, Orta Asya'ya bilginin kontrolü üzerine fikirlere ve teknolojiye sahipken ve bu imkânları bölgeye sunmak isterken, bölgenin tercih ettiği güvenlik ekipmanlarının Çin'e ait olduğu gerçeğiyle yüzleşmektedir. Özellikle, gözetim ekipmanlarının tercih edildiği bölgede Çin tarafından sunulan "güvenli şehir teknolojisi" oldukça rağbet görmektedir. Örneğin, 2019 yılında Huawei ve CITIC Guoan adlı şirketler tarafından Özbekistan'ın altyapısını geliştirmek için 1 milyar dolarlık yatırım sözü verilmiştir (Ruowei, 2019a). Buna ek olarak, Tacikistan'ın başkenti Duşanbe'de de 22 milyon dolara mal olan benzer bir gözetim projesi gerçekleştirilirken; Kırgızistan ve Kazakistan'ın başkentlerinden de konuşlandırılan Çin'in güvenli şehir teknolojisi, gözetim ekipmanlarını arttırmakta ve vatandaşların izlenmesi ve İnternetin yönetilmesi için bir sistem sunmaktadır (Fergana Agency, 2019; Rickleton, 2019).

Diğer yandan, Rusya'nın altyapısı giderek Çin'e benzemekte olduğu için Rusya'nın siber egemenlik modelinin "Çinlileşme (*Sinicization*)" yolunda gittiği görülmektedir. Bu bağlamda değerlendirildiğinde, teknolojik olarak Çin'den yararlansa da model olarak Rusya'yı taklit etmeye çalışan Orta Asya devletlerinin, aslında Çin'i taklit ettiği sonucuna varılmaktadır. Bu durum açığa vurulmaya devam edildikçe doğrudan Çin'e yönelmesi beklenen bölgenin, Rusya'yı rol model olarak görmekten vazgeçeceği ve bölgedeki İnternet yönetişimi standartlarının zaman içerisinde "Çin Malı" (*Made in China*) olarak yerleşeceği, nihayetinde ise, Pekin'in bölgedeki nüfuzunun güçleneceği çıkarımı yapılmaktadır (Weber, 2020).

3.1.4. Türkiye

Türkiye'nin siber güvenlik anlamındaki çalışmalarına bakıldığında, siber güvenlik önlemlerinin belirlenmesi, siber güvenlik çalışmalarının yürütülmesi, uygulanması ve koordine edilmesi amacıyla 20 Ekim 2012 tarihinde yürürlüğe giren 2012/3842 sayılı karara göre, Siber Güvenlik Kurulu'nun (SGK) oluşturulduğu görülmektedir. Ulusal siber güvenlik çalışmalarının yürütülmesi, yönetilmesi ve koordinasyonuna ilişkin karar; bilgi teknolojileri (BT) aracılığıyla sağlanan her türlü hizmet, işlem ve verinin yer aldığı sistemlerin güvenliğinin sağlanması, gizliliğinin korumasına yönelik tedbirlerin alınmasını içermektedir. Buna ek olarak, BİT'lerin bağlantılı olduğu kritik altyapılar üzerine uyulması gereken esasları düzenlemeyi amaçlayan kararın ilkeleri ise şu şekildedir (Bakanlar Kurulu, 2012):

- Ulusal siber güvenliğin sağlanması noktasında Ulaştırma Denizcilik ve Haberleşme Bakanlığı'nın yayınladığı plan, program, usul, esas ve standartlara uyulması gerekmektedir.
- Ulusal siber güvenlik üzerine gerçekleştirilen çalışmalar için gereken altyapıda mümkün olduğunca milli kaynakların kullanılması esastır.
- Ulusal siber güvenlik bağlamında kamu kurum ve kuruluşları tarafından yapılacak çalışmalarda gereken maddi kaynak planlaması ve kaynakların tahsisinin öncelikli olarak yapılması gerekmektedir.

İlkelerin ardından SGK'nın görevleri ise şu şekilde listelenmektedir (Bilgi Teknolojileri ve İletişim Kurumu, 2017):

- ✓ Siber güvenlik alanındaki politika, strateji ve eylem planlarının onaylanması ve ülke genelinde verimli bir biçimde uygulanmasına yönelik gerekli kararları alınması,
- ✓ Kritik altyapıların belirlenmesine ilişkin tekliflerin karara bağlanması,
- ✓ Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşların belirlenmesi,
- ✓ Kanunlarla verilen diğer görevlerin yapılmasıdır.

Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşan SGK, ilk toplantısını 21 Aralık 2012 tarihinde eski Ulaştırma, Denizcilik ve Haberleşme Bakanı Binali Yıldırım'ın başkanlığında yapmıştır (Bilgi Teknolojileri ve İletişim Kurumu, 2017). 20 Haziran 2013

tarihinde yapılan ikinci toplantının ardından ise, Ulusal Siber Olaylara Müdahale Merkezi'nin (USOM) kurulmuştur.

Savunma Sanayii Müsteşarlığı siber uzaydaki tehditleri izlemek ve önlem almak amacıyla ortaya konulan Siber Savunma Merkezi (SİSAMER) Projesi bağlamında, 2017 yılında bir Siber Savunma Harekât Merkezi oluşturulmuştur (T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı, 2020). TSK Siber Savunma Komutanlığı bünyesinde Türkiye çapında veri akışının sağlanacağı merkezin, savunma odaklı stratejiler izlenmesi planlanmaktadır. Tablo 7'de Türkiye'nin Ulusal Güvenlik Strateji Belgelerindeki prensipler görülmektedir.

Tablo 7: Türkiye'nin 2013-2023 Yılları Arası Ulusal Siber Güvenlik Stratejileri Belgelerinde Sıralanan Prensipler

2013-2014 Ulusal Siber Güvenlik Stratejisi	2016-2019 Ulusal Siber Güvenlik Stratejisi	2020-2023 Ulusal Siber Güvenlik Stratejisi
• Siber güvenlik, risk yönetimini esas alan etkin ve sürekli iyileştirmeye dayalı yöntemler aracılığıyla sağlanır.	• Siber güvenlik, risk yönetimini esas alan etkin ve sürekli değerlendirmeye ve iyileştirmeye dayalı yöntemler aracılığıyla sağlanır. Oluşturulan risk yönetimi metotlarının tehdit ve açıklıkları ele alarak bunlardan dolayı ortaya çıkacak riskleri belirlemesi, bu riskleri kabul edilebilir düzeye indirmek için yöntemler sunması hedeflenir.	• Siber güvenlik, ulusal güvenliğin ayrılmaz bir parçasıdır. Ulusal güvenliğin tam olarak sağlanabilmesi, siber güvenlik alanında belirlenen hedeflere ulaşılabilmesine dayanır.
• Siber güvenlik için teknik boyutun yanında hukuki, idari, ekonomik, politik ve sosyal boyutlardaki tehdit ve fırsat unsurlarının ortaya çıkarıldığı bütüncül bir yaklaşıma sahip olunmalıdır.	• Siber güvenliğin sağlanması için tüm paydaşların siber güvenlik risklerini bilmeleri, bu risklerin yönetilmesine ilişkin yaklaşımlarının kendileri kadar başkalarını da etkileyebileceğinin bilincinde olmaları gerekir. Bu farkındalık ve yetkinliğin sağlanması için tüm paydaşların gerekli eğitim ve deneyimi kazanmaları sağlanır. Teknik boyutun yanı sıra; hukuki, idari, ekonomik, politik ve sosyal boyutları da içeren bütüncül bir yaklaşım benimsenir.	• Siber güvenlik alanındaki faaliyetler; geçmişten geleceğe kazanımlar açısından kurumsallık, süreklilik ve sürdürülebilirlik kriterlerine göre yürütülmelidir.
• Risk yönetiminde, teknik zaafların giderilmesi, saldırı ve tehdidin önlenmesi ile muhtemel zararın en aza indirgenmesi unsurları esas alınır.	• Risk yönetimi, teknik zaafların hızla giderilmesini, saldırı ve tehditlerin önlenmesini, fark edilmesini, yanıtlanmasını ve muhtemel zararın en aza indirgenmesini içerir. Zararların asgari düzeyde tutulması için siber olaylara karşı bir hazırlık ve süreklilik planının bulunmasına ve uygulanmasına önem verilir.	• Başarılı ve sürdürülebilir bir dijitalleşme sürecinin gerçekleştirilebilmesi durumu, siber güvenliğin sağlanması ile iç içe geçmektedir. Bu prensibe göre siber güvenlik, dijitalleşme için oldukça hayati bir öneme sahiptir.
• Siber güvenliğin sağlanmasında birey, kurum, toplum ve devletin tüm hukuki ve sosyal sorumluluklarını yerine getirmesi esas kabul edilir.	• Siber uzay güvenliğinin sağlanması ve sürdürülmesinde; kamu, özel sektör, üniversiteler, sivil toplum kuruluşları ve bireyler dâhil tüm paydaşlar arasında işbirliğinin yanı sıra uluslararası işbirliği ve bilgi paylaşımı esas kabul edilir ve güven inşa edilir.	• Siber güvenlik çalışmaları, paydaşların etkin iletişiminin gerçekleştiği ve koordinasyonun sağlandığı bir düzen içerisinde yürütülmelidir.

• Kritik altyapıların güvenliğini sağlamak amacıyla karar mekanizmalarına katılımı da içerecek şekilde özel sektörle tam işbirliğine gidilmelidir.	• Tüm paydaşlar, siber uzay güvenliğinin sağlanması için çalışırken, hukukun üstünlüğü, ifade özgürlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması ilkelerini gözetir.	• Paydaşlar, siber uzaydaki risklerin yönetimi ile ilgili sorumluluklarını yerine getirme noktasında şeffaflık, hesap verebilirlik ve etik gibi değerleri göz önünde bulundurmak zorundadır.
• Kamu, özel sektör, üniversiteler ve STK'larla işbirliğinin yanı sıra uluslararası işbirliğine de gidilerek bilgi paylaşımında bulunulması esastır.	• Paydaşlar siber uzaydaki risklerin yönetimi ile ilgili sorumluluklarını yerine getirirken şeffaflık, hesap verilebilirlik ve etik değerleri göz önünde bulundurur.	• Siber güvenlik riskleri etkin bir şekilde belirlenmekte ve yönetilmektedir.
• Uluslararası işbirliğine ve bilgi paylaşımına başvurulurken diplomatik, teknik ve kolluk kanallarının sürekli ve etkin bir şekilde kullanılması sağlanmalıdır.	• Alınan siber güvenlik önlemlerinin ilgili risklerle orantılı olması, olumlu ve olumsuz etkilerinin değerlendirilmesi ve dengelenmesi sağlanır.	• Özellikle kritik altyapılar aracılığıyla verilen hizmetlerin kesintisiz ve etkin olarak sunulması gerekmektedir.
• Siber güvenliğe yönelik mevzuat geliştirilirken uluslararası anlaşma ve düzenlemeler göz önünde bulundurulmalıdır.	• Siber güvenlik gereksinimlerinin karşılanmasında yerli ürün ve hizmet kullanımı teşvik edilir, bunların geliştirilmesi Ar-Ge projeleri desteklenir, yenilikçilik anlayışı esas kabul edilir.	• Hizmet ve ürünlerin ortaya konmasında, tasarımından son kullanıcıya erişimine kadar baştan sona tüm süreçlerde siber güvenlik kavramının dikkate alınması esastır.
• Hukuk üstünlüğü, temel insan hakları ve özgürlükleri, ve mahremiyetin korunması temel esaslar olarak kabul edilmelidir.		• Yürütülen iş ve işlemlerde bilginin "gizlilik-bütünlük-erişilebilirlik" dengesinin sağlanması ve "bilmesi gereken prensibi"ne sadık kalınması önemlidir. Bu prensibe göre, bir konu veya iş hakkında bilgi sahibi olmak ve o mevzuya nüfuz edebilmek ancak görevi yerine getirmekle ve korumakla yükümlü kişilerin yetkisindedir (Millî Savunma Bakanlığı, 2010).
• Siber ortamda şeffaflık, hesap verilebilirlik, etik değerler ve ifade özgürlüğü desteklenmelidir.		• Güçlü hukuki temeller üzerine güçlü bir siber güvenlik inşa edilmesi esastır.
• Güvenlik ile kullanılabilirlik arasında denge kurulmalıdır.		• Ar-Ge, yenilikçilik ve güçlü teknolojik altyapı anlayışı ile siber güvenlikte yerli ve milli ürün ve hizmet kullanımı teşvik edilir.
• Denetleyici ve düzenleyici kurumlar sorumlu oldukları alanlarda siber güvenliğin sağlanmasını gözetirler.		
• Siber güvenlik gereksinimlerinin karşılanmasında yerli ürün ve hizmet kullanımı teşvik edilir, bunların geliştirilmesi		

için AR-GE projeleri desteklenir, yenilikçilik anlayışı esas kabul edilir.

Kaynak: Ulaştırma ve Denizcilik Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2013; Ulaştırma ve Denizcilik Bakanlığı, 2016-2019 Ulusal Siber Güvenlik Stratejisi, 2016; Ulaştırma ve Denizcilik Bakanlığı, 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2020.

Tablo 7'de öncelikle 2013-2014 ve 2016-2019 yılları arasındaki strateji belgelerine bakıldığında siber güvenliğin risk yönetimi üzerinden tanımlandığı görülürken, 2020-2023 ulusal siber güvenlik stratejisinde ise, siber güvenlik ulusal güvenliğin ayrılmaz bir parçası olarak tanımlanmaktadır. Ulaştırma ve Altyapı Eski Bakanı Adil Karaismailoğlu'nun da "Siber güvenlik milli güvenliğimizin ayrılmaz bir parçasıdır" şeklindeki açıklamasıyla (Türkiye Bilişim Derneği, 2020) vurguladığı üzere, 2020-2023 belgelerinde Türkiye'nin ulusal güvenliğinin sağlanmasının bir yolunun da siber güvenliğin sağlanmasından geçtiği çıkarımı söz konusu olmaktadır. Ulusal siber güvenliğin sağlıklı bir şekilde işleyebilmesi için ise bu belgeler aracılığıyla belirli kurallar ve normlar aracılığıyla oluşturulması hedeflenmiştir.

2016-2019 Strateji Belgesi'nde süreklilik kriterinin yer aldığı, 2020-2023 Ulusal Siber Güvenlik Strateji Belgesi'nde ise, bu kritere kurumsallık ve sürdürülebilirlik kriterlerinin de eklendiği görülmektedir. Bu sayede siber güvenlik seviyesinin yükseltilmesinin amaçlandığı çıkarımı yapılmaktadır. Ayrıca 2020-2023 Strateji Belgesi'nde dijitalleşmenin ayrılmaz bir parçası olarak değerlendirilen siber güvenlik, 2013-2014 ve 2016-2019 Strateji Belgelerinde ise yalnızca risk yönetimi

2013-2014 Strateji Belgesi'nde siber güvenliğin teknik, hukuki, idari, ekonomik, politik ve sosyal boyutlarda bütüncül bir yaklaşım ile ele alınması gerektiği öne sürülmekte; 2016-2019 Strateji Belgesi'nde de aynı şekilde bu yaklaşım desteklenmekte ve buna ek olarak aynı belgede risk yönetimi noktasında tüm paydaşların gerekli bilinç düzeyine çıkabilmeleri için eğitim ve deneyim kazanma noktasına vurgu yapıldığı görülmektedir.

Tablo 9'un devamında, 2013-2014 Strateji Belgesi'nde risk yönetimi bağlamında teknik zaafların giderilmesi, saldırı ve tehditlerin önlenmesi ve buna bağlı olarak muhtemel zararın en aza indirilmesi hedeflenmekte; 2016-2019 Strateji Belgesi'nde ise, bu duruma ek olarak siber vakalara karşı bir hazırlık ve süreklilik planının bulunması noktası vurgulanmaktadır.

Paydaşlar noktasından tablo üzerinde bir inceleme yapıldığında, 2013-2014 Strateji Belgesi'nde siber güvenliği sağlamada kamu, özel sektör, üniversiteler ve STK'lar ile işbirliğine gidilmesi vurgulanmakta ve bunun yanı sıra uluslararası işbirliği ve bilgi paylaşımı konularının da esas olduğu belirtilmektedir. 2016-2019 Strateji Belgesi'ne bakıldığında önceki belgedeki paydaşlara ek olarak bireylerin de dâhil olduğu bir işbirliği sürecinden bahsedilmektedir.

Tüm strateji belgelerinde şeffaflık, hesap verilebilirlik ve etik gibi değerlere yer verildiği göze çarpmaktadır. Aradaki fark ise, 2013-2014 Strateji Belgesi'nde genel bir ifade kullanılırken, 2016-2019 ve 2020-2023 Strateji Belgelerinde paydaşların siber uzaydaki

risk yönetimi üzerindeki sorumlulukları üzerinden bu değerlerin ele alınması söz konusu olmaktadır.

2013-2014 Strateji Belgesi'nde kritik altyapıların güvenliğine ve bu bağlamda karar aşamasını da kapsayacak şekilde özel sektörle gerçekleştirilebilecek işbirliğine değinilmektedir. 2016-2019 Strateji Belgesi'nde prensipler kısmında yer verilmeyen kritik altyapılar konusuna belgenin bir diğer alt başlığı olan "siber güvenlik riskleri" kısmında yer verildiği görülmektedir. Kritik altyapılara yönelik 2020-2023 Strateji Belgesi'ne bakıldığında, hizmetlerin kesintisiz ve etkin olarak sunulmasına dikkat çekildiğini söylemek mümkündür.

Strateji Belgeleri'nde göze çarpan bir diğer nokta, tüm belgelerde yerli ürün ve hizmet kullanımının yanı sıra, yenilikçilik ve Ar-Ge projelerinin teşvik edilmesidir. Ancak 2020-2023 Strateji Belgesi'nde tüm bunlara ek olarak "milli" kavramına da yer verildiği göze çarpmaktadır. Bunun sebebinin Türkiye'nin 2023 vizyonu kapsamında siber güvenlik alanında da öncü olma arzusu olduğu çıkarımı yapılmaktadır. Bu vizyon çerçevesinde diğer uluslararası belgelerin de incelenmesi sonucunda siber uzayın artan önemini fark eden Türkiye'nin 2020-2023 Strateji Belgesi'nin ilk prensibinde siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olmasını vurgulaması tesadüf değildir. Türkiye kendisini siber uzayda öncü bir aktör olarak konumlandırma yoluna gitmektedir.

Yeni nesil teknolojilerin entegre edildiği yerli ve milli siber güvenlik çözümlerinin sayısının artırılması ve kullanımının yaygınlaşması ülkemizin 2023 vizyonu kapsamındaki hedeflerine ulaşmamıza katkı sağlayacaktır. Ülke olarak siber güvenlik alanında öncü olmak hedefi ile yürütülen çalışmalar kapsamında özel sektörün gelişimi, büyümesi, ihracat kapasitesini artırarak ekonomiye katkı sağlaması ve teknolojiye yön veren bir konumda olması temel hedeftir.

Strateji belgelerindeki bir diğer unsura bakıldığında, 2013-2014 Strateji Belgesi'nde hukukun üstünlüğü, temel insan hakları ve özgürlükleri ve mahremiyetin temel esaslar olarak değerlendirildiği görülürken; 2016-2019 Strateji Belgesi'nde tüm bu esaslara ek olarak ifade özgürlüğü konusunun da gündeme alındığı görülmektedir.

Hem sıralanan prensiplere hem önceki strateji belgelerine hem de Türkiye'nin uyguladığı politikalara bakıldığında, Türkiye'nin hibrit bir yaklaşım ortaya koyduğunu görülmektedir. Türkiye coğrafi konumu itibariyle Avrupa veya Asya'nın bir parçası olması sebebiyle yurt içinde ve yurt dışında bölgesel kimlik itibariyle de bir belirsizlik içerisindedir. Bu durum bir yandan Batı odaklı siber uzay yönetişimine yönelmesine, diğer taraftan ise, iç İnternet politikaları bağlamında devlet egemenliği üzerinden yükselen Rusya-Çin eksenine benzeyen bir siber uzay yönetişim politikasına sahiptir (Eldem, 2020). Türkiye'nin NATO üyeliğinin Türkiye'yi Batının bir parçası yapmaya yetmediğini söyleyen uzmanlar, Türkiye-AB ilişkilerindeki bozulmanın da bölgesel kimlik belirsizliğini arttırdığını ifade etmektedirler. Tüm bu coğrafi ve bölgesel kimlik belirsizliğinin siber uzay politikasına yansıdığını belirtmek gerekmektedir. Siber uzay yapısı itibariyle belirsizlik ve bilinmezliklerin hâkim olduğu bir alan olmaktayken, Türkiye'nin belirsizliğinin bu alana yansıması da ülkenin siber uzay politikasının dış politikaya yansımasında bir netlik ifade etmemektedir. Bir yandan, Türkiye'nin çeşitli paydaşlarla birlikte güvenli, açık, dağıtılmış

bir küresel iletişim ağını destekleyen Avrupa-Atlantik ittifakıyla güçlü güvenlik ilişkilerine sahip olduğu görülmekte; Türkiye bu doğrultuda siber alanı yönetmek ve güvenliğini sağlamak için çok paydaşlı yönetişim modelini desteklemektedir (Eldem, 2020). Buna ek olarak, siber alanda devletlerin sorumlu davranışları için norm ve kurallara bağlı olduğunu belirten Türkiye, ulusal ve küresel düzeyde siber uzayda güvenliği sağlamak ve sürdürmek için bilgi paylaşımında bulunmakta, teknik olarak kapasitesini geliştirmekte ve uluslararası işbirliği faaliyetlerine aktif olarak katılmaktadır. Ayrıca Türkiye'nin siber suç mevzuatını, siber ortamda özgürlüklerin, insan haklarının ve güvenliğin korunması ve risklerin azaltılması amacıyla ortaya konulan Budapeşte Sözleşmesi ile uyumlu hale getirdiği ve NATO'nun siber uzayı bir operasyonel alan olarak tanımlaması sonucu Türkiye'nin de siber savunmayı ayrı bir askeri olan olarak tanıdığı görülmektedir. Diğer yandan ise, Türkiye'nin yerel internet politikası çerçevesinde dijital egemenliğini ve bilgi güvenliğini gizlilik ve İnternet özgürlüklerinden daha fazla ön planda tuttuğu görülmekte, dolayısıyla bu durumun Türkiye'yi küresel internet yönetişimi tartışmalarında Rusya-Çin eksenine yaklaştırdığı öne sürülmektedir (Eldem, 2020). Türkiye'nin iç siyasi karmaşalara bağlı olarak son yıllarda neo-Hobbesçu bir siber uzay görüşünü benimsediği ve bu alanda ikinci ve üçüncü nesil bilgi kontrollerini kullanarak egemenlik sağlamaya çalıştığı ifade edilmektedir. Türkiye iyi gelişmiş bilgi güvenliği kabiliyetlerine sahip olsa da aynı zamanda önemli veya yaygın filtreleme ve sansür uygulamalarına da katıldığı için, siber uzay bağlamında Avrupa-Atlantik ittifakından uzaklaştığını söylemek mümkündür (Eldem, 2020).

3.2. Özel Şirketler

Cisco Systems'in eski CEO'su John T. Chambers'ın; "iki tür şirket vardır: saldırıya uğramış olanlar ve saldırıya uğradıklarını bilmeyenler" şeklindeki alıntısı, hiç kimsenin ve hiçbir şirketin siber saldırılardan muaf olmadığını ifade etmesi bakımından önemlidir (Barnes, 2018). Facebook'un 50 milyon kullanıcısının verilerinin bir danışmanlık şirketi olan Cambridge Analytica tarafından 2014 yılından itibaren toplanması sonucu ortaya çıkan veri ihlalinin, ABD seçimlerini etkileyecek çapta büyük bir skandala dönüşmesi, özel sektörün siber güvenlik tartışmalarındaki kilit rolünü ortaya koymuştur (Llorente, 2018). Bahsedilen örnekten de anlaşılacağı üzere özel sektör, siber güvenliğin dışında kalmak bir yanadursun tam merkezindedir (Llorente, 2018).

İsviçre Federal Dışişleri Bakanlığı tarafından 1-2 Kasım 2018'de Cenevre'de düzenlenen Siber Uzaydaki Sorumlu Davranış Üzerine Cenevre Diyaloğu, mevcut normatif çabalara bir yol haritası çizmekte ve siber uzayın kötü amaçlı kullanımına karşı uluslararası barış, güvenlik ve istikrarı sağlamada özel sektördeki aktörlerin rollerini ve sorumluluklarını ortaya koymaktadır (Eggenschwiler, 2018).

Bu diyalog gerçekleşirken yapılan beyin fırtınası sonucu iki grubun ortaya koyduğu bazı çıktılar söz konusu olmuştur. İdealist bir yaklaşıma sahip olan birinci gruba göre özel sektördeki aktörlerin rolleri şu şekilde ayrılmaktadır:

Tablo 8. İdealist Gruba Göre Özel Sektördeki Aktörlerin Siber Uzaydaki Barışı, Güvenliği ve İstikrarı Sağlamadaki Rolleri

Rol	Görevi
Proaktif norm girişimcileri	Norm önermek

Reaktif norm uygulayıcıları	Özellikle BM Hükümet Uzmanları Grubu tarafından şart koşulan normları uygulamak
Bağımsız norm koruyucuları	Norm ihlalinin olup olmadığını doğrulamak
Norm yürütücüleri	Normların ortaya koyduğu davranışı olanaklı kılmak veya o davranıştan men etmek

Kaynak: (Eggenschwiler, 2018: 17)

İlk gruba göre bir derece daha gerçekçi olan ikinci grubun özel sektöre atfettiği roller ise, özel sektördeki aktörlerin, kritik altyapıların (iletişim sistemleri, havaalanları, metro istasyonları, petrol ve gaz boru hatları vb.) korunmasıyla daha fazla ilgilenmesi, tasarlanan ürünleri kapsamlı bir güvenlik testinden geçirmesi ve son olarak hükümetin olaylara müdahil olmasına yardımcı olmak ve kamuya yönelik oluşan riskleri üstlenmektedir (Eggenschwiler, 2018).

Beyin fırtınası sonucu belirli rollerin özel sektöre atfedilmesinin ardından bu rollerin nasıl uygulanacağına yönelik bazı pratik örnekler ortaya konulmuştur.

Örnek 1: Özel sektördeki aktörlerin 2015 BM Hükümet Uzmanları Grubu'nun ortaya koyduğu normları uygulamak için diğer aktörlerle işbirliği yapması gerekmektedir.

Uygulaması: Gerekli tehdit bilgisinin edinilmesi, açık savunma ve direnç protokollerinin oluşturulması, ortak cevap protokollerinin ortaya konulması, çok taraflı ittifak sağlanması ve son olarak oluşturulacak özel bir senaryo ve stres testinin hazırlanmasıyla işbirliği sağlanabilecektir.

Örnek 2: Özel sektördeki aktörlerin kamu risklerini üstlenmesi gerekmektedir.

Uygulaması: Açık risk tanımı oluşturulmalı, gerekli güvenlik sorumlulukları tanımlanmalı ve yöntemi ortaya koyarken uzman bir kuruluşa başvurulmalıdır.

Cenevre Diyaloğu'na göre, dijital dünyada barış ve güvenliğin sağlanabilmesi için hem kamu hem de özel kuruluşlardan oluşan bir yönetişim anlayışına ihtiyaç vardır. Siber güvensizlikten siber istikrara giden yolda özel sektör aktörlerinin norm oluşturma faaliyetlerinin söz konusu olması ise, daha işbirlikçi yönetişim biçimlerine ihtiyaç duyulduğuna işaret niteliğindedir (Eggenschwiler, 2018). Dolayısıyla buradaki tabloda belirtilen normlar ve görevler çerçevesinde, özel sektörde şirketler üzerine bir tartışma yapıldığı görülmektedir.

3.2.1. Microsoft

2016 yılında Microsoft içinde yayılan "Siber güvenlik olmadan ulusal güvenlik olmaz" cümlesiyle başlayan ve şirketi, uluslararası güvenlik dünyasına doğru yönelten süreç, Microsoft'un kendi çerçevesini ortaya koyarak, siber güvenlik anlamında belirli normlar önerdiği ve böylece bir norm girişimcisi profiline kavuştuğu bir aşamaya doğru evirilmiştir.

Siber uzaydaki sorumlu davranışa yönelik tartışmaları ilk başlatan özel paydaşlar arasında yer alan Microsoft; 2013, 2014 ve 2016'daki çabalarını takiben 2017 yılının Şubat ayında, dijital platformdaki kötücül eylemleri önlemek amacıyla devletler içinde ve devletlerarasında özel sektör ve sivil toplumun işbirliğini öne süren Siber Uzayı Korumaya Yönelik Dijital Cenevre Sözleşmesi fikrini ortaya atmıştır (Eggenschwiler, 2018).

Dijital platformdaki kötücül eylemleri önlemek için devletler arasında ve devletler ile özel sektör ve sivil toplum arasındaki köklü bir işbirliğinin gerekli olduğunu savunan Dijital Cenevre Sözleşmesi'nde öne çıkan temel noktalar şu şekildedir (Eggenschwiler, 2018):

- Yıkımı, vatandaşların emniyetini ve güvenliğini olumsuz etkileyecek sistemlere (hastaneler, elektrik şirketleri gibi kritik altyapılar) saldırmaktan kaçınmak
- Yıkımı, küresel ekonomiye zarar verebilecek veya büyük küresel aksaklıklara (örneğin, bulut tabanlı hizmetler) neden olabilecek sistemlere saldırmaktan kaçınmak
- Seçim süreçlerinde yer alan gazeteciler ve vatandaşlar tarafından kullanılan kişisel hesapları veya kişisel verileri *hack*lemekten kaçınmak
- Diğer şirketlere karşı avantaj elde etmek maksadıyla ticari sırlar ve gizli iş bilgileri de dahil olmak üzere, özel şirketlerin fikri mülkiyetini çalmak için bilgi ve iletişim teknolojisini kullanmaktan kaçınmak
- Kitlesel pazardaki teknoloji ürünlerine arka kapı eklemekten kaçınmak
- Kitlesel pazardaki ürün ve hizmetlerin güvenlik açıklarının edinilmesi, alıkoyulması, güvence altına alınması, kullanılması ve raporlanması için net bir politika üzerinde anlaşmak
- Siber silah geliştirme noktasında sınırlamaya gitmek ve geliştirilenlerin sınırlı, hassas ve tekrar kullanılamaz olmasını sağlamak. Devletler özelinde ayrıca, silahların kontrolünün güvenli bir ortamda sürdürülmesini temin etmek
- Siber silahların yayılmasını sınırlamayı kabul etmek. Hükümetler siber silahları dağıtmamalı veya başkalarının dağıtmasına izin vermemeli ve bunu yapanlara karşı istihbarat, kanun yaptırımı ve mali yaptırım araçlarını kullanmalıdır.
- Sivil altyapıya veya tesislere toplu hasar vermekten kaçınmak için siber saldırı operasyonlarına katılımı sınırlamak
- Özel sektörün siber saldırıları tespit etme, kontrol altına alma, müdahale etme ve kurtarma çabalarına destek olmak. Özellikle, Bilgisayar Acil Durum Müdahale Ekipleri (CERT'ler) de dâhil olmak üzere, müdahale ve kurtarma için gereken temel yetenekleri veya mekanizmaları etkinleştirmektir.

Dijital alanın ulusal güvenlikte giderek artan bir role sahip olduğu küresel ortamda, siber güvenlik politikalarının oluşturulmasında teknoloji şirketlerinin daha etkin bir rol oynaması gerekmektedir. Özel sektördeki aktörlerin norm oluşturma çabaları üzerindeki faaliyetleri üzerinden bir değerlendirme yapıldığında, sektörün teknoloji üzerine sahip olduğu uzmanlığı ve etkiyi görmezden gelmek, siber güvenlik alanındaki potansiyel fırsatları yok saymaktır (Llorente, 2018). İhtiyaç duyulan değişim ise, Dijital Cenevre Sözleşmesi'nde somutlaştırılmaktadır.

Özel sektörün siber güvenlik politikasında oynaması gereken rolün ne olduğu ve devletlerin sorumluluklarıyla nasıl bir arada var olabileceği sorusunu ortaya çıkaran Dijital Cenevre Sözleşmesi, eleştiriler almış olsa dahi burada odaklanılması gereken nokta, özel bir şirketin kendisini uluslararası güvenlik ortamında önemli bir oyuncu olarak konumlandırma yönünde bir adım atmış olmasıdır (Llorente, 2018).

Dijital Cenevre Sözleşmesi, gerçekleşen siber saldırıları analiz edecek ve faillerini tespit edecek bir atıf örgütü, vatandaşları koruyacak ortak ilkeler ve davranışların oluşturulacağı bir endüstri anlaşması ve son olarak ulus devletler için bağlayıcı kurallar şeklinde üç öneri ortaya koymaktadır.

Sözleşme'nin mantığı, bir yandan devletler imzacı olurken diğer yandan ise, özel sektörün kendi endüstri anlaşmasını taahhüt etmesi ve bir sivil toplum kuruluşunun siber saldırıları soruşturma noktasında sorumluluk alması şeklinde bir temele oturtularak çok paydaşlı yönetişime farklı bir bakış açısı getirmektedir. Sözleşme'nin vurguladığı noktalardan bir diğeri, siber saldırıların sadece teknolojik şirketlerin katkısı sonucu çözülebilecek küresel bir insani sorun olarak betimlenmesi olmuştur. İnsani sorun kısmını vurgulamak isteyen Microsoft, sözleşme ile alakalı konuşurken bilgi teknolojileri şirketlerinin rolünü Kızıl Haç ile eşleştirmekte ve siber saldırılara ilk müdahaleyi yapacak ekiplerden bahsetmektedir. Böylelikle bu durumu insani savunuculuk şeklinde ilerleterek kendisinin ahlaki bir aktör olma durumunu öne çıkarmaktadır.

Buna ek olarak, Microsoft tarafından başlatılan bir hareket olan ve 170 ülkeden 130 bin vatandaşı içeren *Digital Peace Now* hareketi, "dijital barış olmadan barış olmaz" mottosunu baz alarak, ulusların siber savaşa girmeyi bırakması ve dijital dünyada başlayan ancak fiziksel dünyadaki vatandaşları etkileyebilecek saldırılardan koruyan uluslararası anlaşmalar oluşturma yönünde adımlar atmasını öne sürmektedir. Küresel dijital toplumu savunmak için seslerini duyurmaya çalışan ve oylarını bu yönde şekillendireceğini söyleyen vatandaşlar, dünya liderlerinin onların güvenliğini sağlamak için harekete geçmeleri gerektiğini vurgulamaktadır. Microsoft'un belirttiği üzere, Dijital Barışa ulaşma çabası, tek başına hareket eden hiçbir şirket tarafından yapılamaz. Bu nedenle, birkaç şirketle birlikte hareketi destekleyen Microsoft, hükümetler, STK'lar, uzmanlar gibi birçok aktörün de koalisyonuna ihtiyaç duyduğunu belirterek aktörleri işbirliğine teşvik etmektedir.

Saldırı kabiliyetlerinin artmasıyla birlikte, siber uzaydaki hükümet davranışlarından hangilerinin yetki sınırlarının dışında olması gerektiğini tanımlayabilmek için siber güvenlik normlarına ihtiyaç duyulduğunu belirten Microsoft, çatışmaları sınırlamayı ve siber savaşın ortaya çıkmasını engellemeyi hedeflemektedir. Siber güvenlik normlarının etkili olabilmesi için ise, Microsoft tarafından dört temel kriter ortaya konulmaktadır. Öncelikle bir davranışın norma dönüşebilmesi için uygulanabilir olması gerekmektedir. İkinci olarak, çatışmaya sebep olabilecek siber olayların risklerini azaltması gerekmekte; üçüncü olarak ise, devletler, şirketler, STK'lar, bireysel paydaşlar ve kullanıcılar için siber güvenlikte fark yaratan bir davranış değişikliği ortaya çıkarmasına, diğer bir deyişle gözlemlenebilir olmasına ihtiyaç duyulmaktadır. Son olarak, etkili bir norm oluşturulabilmesi için mevcut risk yönetimi kavramlarından yararlanılmalı ve ilgili tarafların potansiyel eylemlerine yönelik bilgiler edinilmelidir.

Tüm bur kriterler göz önüne alınarak, Microsoft tarafından siber güvenlik üzerine altı norm önerilmektedir:

- **Norm 1:** Devletler, BİT şirketlerini güvenlik açıkları eklemeye veya kamuoyunun ürün ve hizmetlere olan güvenini zayıflatacak eylemlerde bulunmaya yöneltmemelidir.
- **Norm 2:** Devletler; ürün ve hizmetlerdeki güvenlik açıklarını stoklamak, satın almak, satmak veya kullanmaktan ziyade, satıcılara bildirmeye yönelik açık bir ilkeye dayalı bir politikaya sahip olmalıdır.
- **Norm 3:** Devletler, siber silah geliştirmede tedbirli davranmalı ve geliştirilen silahların ise, sınırlı, hassas ve tekrar kullanılamaz olmasını sağlamalıdır.
- **Norm 4:** Devletler, siber silahlara ilişkin eylemlerin yayılmasını önlemeyi taahhüt etmelidir.
- **Norm 5:** Devletler, kitle oluşturmaktan kaçınmak için siber saldırı operasyonlarına katılımlarını sınırlamalıdır.
- **Norm 6:** Devletler, özel sektörün siber uzaydaki olayları tespit etme, kontrol altına alma, müdahale etme ve bunlardan kurtulma çabalarına yardımcı olmalıdır.

Tablo 9. Norm Oluşturma Bileşenlerine Göre Microsoft'un Dijital Cenevre Sözleşmesi

Kimlik	Davranış	Uygunluk	Normların Formu	Kolektif Beklentiler
Devletler	Bahsi geçen normları içermektedir.	Uluslararası hukuku temel almaktadır.	Sözleşme (öneri)	-

Kaynak: (Ilona, 2018: 7-8)

Tablo 9'da Microsoft'un norm oluşturma bileşenlerine yönelik sınıflandırması yer almaktadır. Bir norm teşvik edicisi olan Microsoft tarafından kimlik olarak devletlerin hedeflendiği Dijital Cenevre Sözleşmesi, davranış olarak yukarıda belirtilen normları dikkate alırken, uygunluk ise, uluslararası hukuk ilkelerine göre şekillendirilmektedir. Normların formu, bir sözleşme önerisi olarak ifade edilebilecek niteliğe sahiptir. Kolektif beklentiler uzun vadeli bir süreci beraberinde getirmesi sebebiyle, analize dâhil edilmemiştir.

Siber uzaydaki tahmin edilemezlik düşünüldüğünde, normların kendi başlarına bir amaç olmadıkları aşikârdır; ancak uygun şekilde geliştirilir ve pratiğe dökülürlerse davranışta ciddi değişikliklere yol açabileceğini düşünmek gerekmektedir (Microsoft, 2021). Siber güvenlik önceliklerine ilişkin küresel bir anlayış geliştirmek, siber uzayın uzun vadeli istikrarı ve güvenliği için gereklidir ve hükümetler arasında işbirliğinin sağlanması ihtiyacını beraberinde getirmektedir. Özetle; Microsoft, siber güvenlik normlarına ilişkin uluslararası tartışmaların temelini oluşturması gereken ilkeler olarak uyumlaştırma, risk azaltma, şeffaflık, orantılılık ve işbirliği gibi noktalar ortaya koymaktadır (Microsoft, 2021).

3.2.2. Google

Dünyanın dört bir yanındaki devletlerin, vatandaşlarını güvende tutmak için kanıt toplamaya ihtiyacı vardır. Savcılar, polisler ve bu alanda çalışan diğer görevliler evleri arayarak, teknolojinin gelişmesiyle telefon kayıtları aracılığıyla kanıt toplayarak güvenliği sağlamaya çalışmışlardır. Ancak dijitalleşmeyle birlikte devletlerin artık geleneksel

kanıtların ötesinde dijital kanıtlara erişime ihtiyaçları vardır. Bu bağlamda, İnternet endüstrisindeki özel şirketler, cezai soruşturmalarda dijital bilgi sağlama konusunda hükümetlerden gelen yoğun bir baskı ile karşı karşıya kalmaktadır (GIP Digital Watch, 2021). Bu süreci yönetirken kullanılacak olan araçlar olarak uluslararası iş birliği ve geleneksel kanallar ise, yavaş ve kullanışsızdır. Buna ek olarak; Karşılıklı Adli Yardım Anlaşması olarak isimlendirilen ve kanunların uygulanması için bilgi toplanmasını içeren anlaşmalar ise en az on ay gibi bir sürece tabi olmaktadır (Google, 2021). Bu nedenle, Google tarafından yasal sistemi dijital çağın hızına ayak uyduracak şekilde geliştirmek ve buna bağlı olarak yabancı hükümetlere dijital kanıt sağlanması için bazı yeni normlar önerilmiştir. Dijital güvenlik ve kanuni prosedür üzerine normlar öneren Google, devletlerin ihtiyaç duydukları bilgileri elde etmek istediklerinde, önerilen çözümlerden dolayı mahremiyet ve güvenlik açısından yüksek bir bedele maruz kaldıklarını öne sürmektedir (GIP Digital Watch, 2021). Google'ın öne sürdüğü normlar ise, kanunu uygulayan makamların gizliliğinin korunmasını sağlamakta ve vakaların daha hızlı araştırılması için gerekli dijital kanıtları elde etmeyi kolaylaştırmaktadır.

ABD tarafından ortaya konulan Dijital Güvenlik ve Kanuni Prosedür Üzerine Bulut Çağı İçin Yeni Bir Yasal Çerçeve başlıklı belgenin benimsenmesini öneren Google, bu ilkelerin, bulut bazlı teknolojinin giderek büyümesi, karşılaşılan gerçek güvenlik tehditleri ve mahremiyet beklentileri ışığında oluşturulduğunu iddia etmektedir (Walker, 2017). Şirketler ve kullanıcılar için ulusal ve uluslararası hukuki yaptırımı ele alan bu belgenin iki temel ilkesi söz konusu olmaktadır. Birinci ilkeye göre; temel gizlilik, insan hakları ve kanuni prosedür ilkelerine saygı duyan ülkeler kendi sınırları içinde meydana gelen ciddi suçlarla ve kendi yetki alanlarındaki kullanıcılarla ilgili veriler için hizmet sağlayıcılara doğrudan talepte bulunabilmelidir (Walker, 2017). Birçok ülkede bu ilkeye karşı düzenlemeler olsa da, ABD'nin dijital kanıt yasalarını güncelleme üzerine öne sürdüğü politika reformu oldukça gerekli bir adımdır. Bu nedenle üzerine ciddi tartışmalar olması da bu konuya olan ilginin bir göstergesidir. Bir yasa tasarısı olan ICPA, verilerin nerede muhafaza edildiğine bakılmaksızın, hüküm süren kanuni hükümlerin elektronik iletişim verilerine erişimini düzenleyen bir çerçeve oluşturmaktadır (*H.R. 3718 (115th): International Communications Privacy Act*, 2017).

İkinci ilke ise, ülkelerin temel standartları karşılaması ve ABD'nin ECPA'yı değiştirmesi koşuluyla, ABD ve yabancı hükümetlerin gelecekte karşılıklı adli yardım anlaşması sürecine bir alternatif sağlayabilecek yeni anlaşmalar imzalamalarıdır. Bu durumda ikili anlaşmalar Adalet Bakanlığı tarafından öne sürülen mevzuatla yetkilendirilebilecek ve buna ek olarak, küresel gizlilik standartlarını iyileştirmek ve yabancı hükümetlerin soruşturmalar için dijital kanıt elde edebilmeleri için bir yol meydana gelecektir. ICPA'nın dayandığı ilkelerin sağlam olduğuna inanan Google, oldukça kapsamlı ve bir süreç olan bu reform süreci için "*eylemin karmaşıklığını eylemsizliğin bir nedeni olarak kabul edemeyiz*" şeklinde bir yorumda bulunmakta ve ardında kanun yapıcılar, düzenleyiciler, STK'lar, uzmanlar ve diğer şirketlerle işbirliğine gitmeye hazır olduğunu belirtmektedir (Walker, 2017).

Google Güvenlik Merkezi'nin prensiplerine bakıldığında, şu maddeler görülmektedir (Google Güvenlik Merkezi, 2021):

- ✓ **Prensip 1:** Hangi verilerin nasıl kullanıldığı ve nasıl korunduğu konusunda kullanıcılara ve kullanıcıların gizliliklerine saygı duymak
- ✓ **Prensip 2:** Hangi verilerin neden toplandığı konusunda şeffaf olmak
- ✓ **Prensip 3:** Kullanıcıların kişisel bilgilerinin kimseye satılmaması
- ✓ **Prensip 4:** Kullanıcıların, gizliliklerini kontrol edebilmelerine olanak sağlamak
- ✓ **Prensip 5:** Kullanıcıların, verilerine istedikleri zaman erişebilmeleri için verilerini inceleyebilme, taşıyabilme ve silebilmelerine imkân sağlamak
- ✓ **Prensip 6:** Google ürünlerinde en güçlü güvenlik teknolojilerini kullanmak
- ✓ **Prensip 7:** İnternetteki güvenliği herkes için geliştirmek ve bu konuda diğer aktörlere örnek olmayı amaçlamak

Google'ın şeffaflık ve gizlilik prensiplerine ek olarak, 10 Kasım 2020 tarihinde Avrupa Komisyonu'nun Google'a karşı başlattığı soruşturmadan bahsedilmesi gerekmektedir. Foundem adlı şirketin Google hakkında şikâyette bulunması ve devamında gerçekleşen bir dizi şikayete bağlı olarak Komisyon'un başlattığı soruşturmanın konusu, Google'ın arama motoru sonuç sayfalarında kendi ürünlerini tanıtarak rakip ürünlerin geriye düşmesine sebep olmak üzerine olmuştur. Zira bu durum, ürün ve hizmetlerin Google tarafından rekabete aykırı bir şekilde tanıtıldığını göstermekte; kullanıcılar ise, bu rekabetten mahrum kalarak seçim hakkına sahip olamamaktadır. Olayın ardından Foundem girişiminin web sitesinde Google'ın güven karşıtı durumu hakkında ayrı bir sekme açılmış ve Google'ın objektifliği sorgulanmıştır. On yıldan fazla süredir Avrupa'da %95 oranında bir pazar payına sahip olan Google'ın arama sonuçlarında tercihli muamelede bulunması ve tekel gücünü kötüye kullanması sonucu 27 Haziran 2017'de suçlu bulunan Google'a, Komisyon tarafından 2.42 milyar Euro para cezası verilmiştir (Avrupa Komisyonu, 2017). Karara itiraz eden Google, sunduğu hizmetlerin bölgenin dijital ekonomisine katkı sağladığını öne sürse de, Google Alışveriş vakasıyla ilgili araştırma yaparken, Google AdSense ile ilgili rekabet sorunlarıyla alakalı olarak da kanıtlar bulan Komisyon 14 Temmuz 2016'da bir şikâyet beyanı yayınlamış ve 20 Mart 2019 tarihinde Google'a çevrimiçi reklamcılıkta kötüye kullanım amaçlı uygulamalar kullanması sebebiyle 1.49 milyar Euro para cezası verilmiştir (Avrupa Komisyonu, 2019).

Fotoğraf 9. Google Tarafından Arama Ağı Reklamcılığındaki Hâkimiyeti Korumak İçin Gerçekleştirilen Adsense Kısıtlamalarının Avrupa Komisyonu Tarafından Görselleştirilmesi

Kaynak: Avrupa Komisyonu, Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising, 2019

Bilgi güvenliğinin üç ilkesi olan gizlilik, bütünlük ve erişilebilirliği merkeze koyan (Rekabet Kurumu, 2019) Türkiye'deki Rekabet Kurumu tarafından da arama ve konaklama fiyatı gibi sorgularda rakiplerini geri plana atarak kendi hizmetlerini öne sürmesi sebebiyle Google'a soruşturma açılmıştır. 14 Nisan 2021 tarihinde Kurum tarafından açıklanan nihai karara göre Google'a, gerçekleştirdiği ihlalden dolayı 296 milyon TL ceza kesilmiş, buna ek olarak altı ay içerisinde, rakip yerel arama hizmetlerinin ve konaklama fiyatı karşılaştırma hizmetlerinin genel arama sonuç sayfasında dezavantajlı olacakları durumunun sona erdirilmesine ve bu konuyla alakalı olarak beş yıl boyunca her yıl Kurum'a rapor sunulmasına karar verilmiştir (*Google 4054 Sayılı Rekabetin Korunması Hakkında Kanun'un 49. Maddesi Uyarınca Açıklanması*, 2021).

Johannes Gutenberg'in matbaayı icat etmesiyle bilgi ve fikirlerin seri bir şekilde üretime geçmesi sonucu ortaya çıkan ifade özgürlüğü, kendi içinde de önemli bir temel hak olmasının yanı sıra, diğer özgürlüklerin savunulması için de büyük öneme sahiptir. Bu bağlamda, iletişim araçlarının kullanılmasının ifade özgürlüğünün sağlanması için son derece gerekli olduğunu öne sürmek doğru olacaktır. 2014'ten beri Avrupa hukukunda yer alan, ancak bazı ülkelerde hala yabancı bir kavram olan "Unutulma Hakkı", Google gibi oldukça kapsamlı ve yaygın kullanım alanına sahip bir şirket için sorgulanması gereken bir konudur. Örneğin, x kişisinin Google'a başvurarak zarar verici kişisel bilgilerinin arama algoritmasından çıkarılmasını istemesi durumunun yasal olarak mümkün olup olmayacağı hatta politik açıdan bir talep olarak değerlendirilip değerlendirilmeyeceği noktasında bir meraka sahip olabilir. Avrupa Adalet Divanı (AAD), dijital platformda Google gibi bir arama motorunun Veri Koruma Direktifi'nin işleyişinden kaçınamayacağı sonucuna varmaktadır (Belbin, 2019). Zira arama motorlarının faaliyet alanı, verilerin yayılmasında belirleyici bir rol oynamayı içermektedir. Herhangi bir İnternet kullanıcısı, arama butonuna yazdığı konu sonucu ortaya çıkan verinin ortaya koyduğu içeriğe ulaşabilmekte, diğer bir deyişle arama motorunun algoritmasına uygun şekilde yönlendirilmektedir.

Google'ın Google Güvenlik Merkezi aracılığıyla prensipler ortaya koyarak norm girişimciliği konusunda aşama kat etmesi siber uzaydaki norm inşası süreci açısından ele

alınması gereken bir konudur. Ancak diğer yandan bizzat kendisinin ortaya koyduğu prensipler olan; *hangi verilerin neden toplandığı konusunda şeffaf olmak* (prensip 2), *kullanıcıların kişisel bilgilerinin kimseye satılmaması* (prensip 3) noktalarında kırılgan bir norm izleme sürecine sahip olduğunu belirtmek gerekmektedir. Zira Avrupa Komisyonu ve Rekabet Kurumu tarafından verilen cezalar bunu açıkça ortaya koymaktadır. Verilerin kendi amaçları doğrultusunda toplandığını açıklamayan Google'ın, bizzat kendi ortaya koyduğu şeffaflık ilkesini çiğnediğini; kişisel bilgileri kimseye satmasa da bu bilgiler doğrultusunda kendi çıkarlarını temsil eden reklamlar öne çıkarması sonucu bilgileri kendisi için satın aldığı izlenimi ortaya çıkmaktadır. Bütün bu noktalar dikkate alındığında, normların özel şirketler özelinde ticari çıkarlar doğrultusunda kullanılabileceği görülmekte, bu nedenle norm inşası sürecinde çok paydaşlılığın altı bir kez daha çizilerek gerekliliği vurgulanmaktadır.

3.2.3. Siemens

Özel şirketler tarafından siber saldırıların düzeyini farklı yollarla azaltmayı hedefleyen girişimler ağların, yazılımların, cihazların kötü niyetli faaliyetler doğrultusunda kullanılmasını engellemek, araştırma çabalarını ilerletmek ve siber güvenlik kültürünü teşvik etmek amacıyla faaliyetlerini sürdürmektedirler (Ilona, 2018). Buna ek olarak, her girişimin kendi uygunluk yaklaşımı söz konusudur. Siemens bünyesinde ise, dijital dönüşümün yaygınlaştırılabilmesi amacıyla bireyler ve kuruluşlar bağlamında teknolojilerin emniyetli olduğunu ifade eden "güven" kavramı merkeze alınmaktadır. Bunu sistematik hale getirmek için Siemens tarafından Güven Sözleşmesi (*Charter of Trust*) imzalanmıştır. Norm kavramının içerisindeki uygunluk bileşeni göz önüne alındığında, Siemens için uygunluğun güven ile bağdaştığını belirtmek mümkündür (Ilona, 2018).

Şubat 2018'de Münih Güvenlik Konferansı'nda Siemens'in yanı sıra sanayi sektöründen sekiz ortak tarafından daha fazla siber güvenlik için ortak bir tüzük olarak başlatılan Güven Sözleşmesi, imzalandıktan iki yıl sonra 17 üyeye ulaşmıştır. Siemens ve Münih Güvenlik Konferansı'nın desteğine ek olarak; AES, Airbus, Allianz, Atos, Cisco, Dell Technologies, Deutsche Telekom, IBM, Mitsubishi Heavy Industries, NXP Semiconductors, SGS, Total ve TÜV SÜD şirketleri de belgeye kendilerini adayarak siber güvenlik girişimine katkıda bulunmayı seçmişlerdir.

Siemens'in siber güvenliği koruma yönetimi başkanı Stefan Jost-Drummer, Microsoft'un girişim prensiplerinin Siemens'in Güven Sözleşmesi'ni tamamlayıcı nitelikte olduğunu ileri sürerek, Siemens tarafından desteklendiğini belirtmektedir (Bing, 2018). Bunun yanı sıra siber güvenliğin, bir emniyet kemeri veya hava yastığından daha fazlası olduğunu öne süren Siemens, siber güvenliği, dijital ekonominin başarılı olabilmesinin kilit unsuru olarak görmektedir. Şirket tarafından Güven Sözleşmesi'nin öne sürdüğü on prensip şunlardır (Siemens AG, 2020a):

- **Prensip 1 – Siber güvenlik ve bilgi teknolojilerinin güvenliği için mülkiyet ilkesi:** Bu ilkeye göre, belirli bakanlıklar ve kuruluşlardaki bilgi güvenliği görevlisi başkanları belirlenmeli ve bu belirlenen kişiler tarafından hükümet ve işletme düzeylerinde siber güvenlik sorumlulukları yerine getirilmelidir.

- **Prensip 2 – Dijital tedarik zinciri sorumluluğu:** Şirketler ve gerektiğinde hükümetler, açıkça tanımlanmış bir biçimde Nesnelerin İnterneti katmanlarında yeterli korumayı sağlayan risk temelli kurallar oluşturmalıdır. Diğer bir deyişle, şifreleme, kimlik ve erişim yönetimi, sürekli koruma gibi bazı temel standartlar geliştirilerek gizlilik ve güvenlik sağlanmalıdır.
- **Prensip 3 – Fabrika ayarı olarak güvenlik:** Bu ilkeye göre, cihazların teknolojilerinin tasarımından itibaren en yüksek güvenlik ve veri koruma düzeyi inşa edilmelidir.
- **Prensip 4 – Kullanıcı odaklılık:** Ürün, sistem ve hizmetlere ek olarak, müşterinin siber güvenlik ihtiyaçlarına ve risklerine dayalı bir rehberlik sağlama anlayışını benimsenmeli ve güvenilir bir ortak olarak hizmet verilmelidir.
- **Prensip 5 – İnovasyon ve birlikte geliştirme:** Yeni tehditlere adapte olabilmek amacıyla siber güvenlik önlemleri sürekli yenilenmeli ve buna ek olarak firmalar ve politika yapıcılar arasında siber güvenlik kuralları üzerine ortak bir anlayış teşvik edilmelidir.
- **Prensip 6 – Eğitim:** Bu ilkeyle birlikte üniversitelerde, okul müfredatlarında siber güvenlik üzerine dersler ve mesleki eğitimler verilmesi ve böylelikle gelecekte ihtiyaç duyulan becerilerin çekirdekten yetiştirilmesi amaçlanmalıdır.
- **Prensip 7 – Kritik altyapılara yönelik siber güvenlik çözümleri için sertifikasyon:** Şirketler ve ihtiyaç halinde hükümetler, kritik altyapı ve Nesnelerin İnterneti çözümleri için zorunlu ve bağımsız üçüncü taraf sertifikaları oluşturmalıdır.
- **Prensip 8 – Şeffaflık ve yanıt:** Endüstriyel bir siber güvenlik ağına katılım sağlanmalı ve kritik altyapıya odaklanan günümüz pratiklerinin ötesindeki olaylar rapor edilmelidir.
- **Prensip 9 – Yasal çerçeve:** Düzenleme ve standart oluşturma noktasında çok taraflı işbirlikleri teşvik edilmelidir. Örneğin; Serbest ticaret anlaşmalarına siber güvenlik kurallarının dahil edilmesi gibi.
- **Prensip 10 – Ortak girişimler:** Dünyanın farklı yerlerinde gecikmeler olmaksızın yukarıda bahsi geçen ilkeleri uygulamaya geçmek için ilgili tüm paydaşları içeren ortak girişimler yürütülmelidir.

Tablo 10. Norm Oluşturma Bileşenlerine Göre Siemens'in Güvenlik Sözleşmesi

Kimlik	Davranış	Uygunluk	Normların Formu	Kolektif Beklentiler
Devletler ve endüstri	Güven Sözleşmesi'nin on prensibini içermektedir.	"İnsanların ve kuruluşların dijital teknolojilerinin güvenli ve emniyetli olduğuna güvenmesi gerekmektedir; aksi takdirde dijital dönüşümü benimsemeleri mümkün değildir. "	Kamu mutabakatı	-

Kaynak: (Ilona, 2018: 7-8)

Tablo 10'da da görüldüğü üzere, Güvenlik Sözleşmesi ile devletler ve endüstri bazlı bir kimlik seçen Siemens, yukarıda bahsi geçen on sözleşme prensibini davranış olarak öne sürmekte, uygunluk noktasında ise, güven kavramını merkeze almaktadır. Tüm bunları

kamu mutabakatını sağlamak şeklinde ortaya koymakta olup, kolektif beklentiler bileşeninin analiz edilebilmesi için uzun vadeli bir süreç öngörülmektedir.

3.2.4. Nornickel

Rus merkezli bir nikel madenciliği şirketi olan Nornickel, faaliyet gösterdiği bölgeler üzerinde sosyal ve kültürel bir etkiye sahip olan büyük bir şirket olarak görülmektedir. Şirket, sanayi kenti Norilsk sakinlerine İnternet ve çoklu çevrimiçi hizmetler noktasında geniş bir bant erişimi sağladığı Kuzey Kutup Dairesi'nin yanı sıra, bin kilometrelik yüksek hızlı fiber optik hat gibi büyük çaplı projeler gerçekleştirmesi anlamında dikkate alınması gereken önemli bir şirkettir (Nornickel, 2018). Bu önemli konumuna bağlı olarak ise, şirket, kurumsal olarak siber güvenliğe ayrıca vurgu yapma ihtiyacı duymaktadır. Bu bağlamda önemli bir sözleşme olan Kritik Endüstriyel Tesisler İçin Bilgi Güvenliği Sözleşmesi, Nornickel tarafından ortaya atılmıştır. Sözleşmenin tarafları, ulusal ekonomiler üzerinde olumsuz etki oluşturabilecek herhangi bir aktiviteye katılmayı gönüllü olarak reddetmektedirler (Nornickel, 2018).

Sözleşme, Nornickel uzmanları tarafından, haksız rekabetle mücadele etmeyi ve BİT'lerin kötüye kullanımından kaynaklanan endüstriyel tesislere verilen zararları önlemeyi amaçlayan bir kurallar ve davranış standartları oluşturma amacı taşımaktadır (Industrial Cyber Security Club, 2018).

Tablo 11. Norm Oluşturma Bileşenlerine Göre, Nornickel'in Kritik Endüstriyel Tesisler İçin Bilgi Güvenliği Sözleşmesi

Kimlik	Davranış	Uygunluk	Normların Formu	Kolektif Beklentiler
Tüm aktörler	Kurallar ve davranış standartları	BM Genel Kurulu'nun BİT ile ilgili kararlarını temel almaktadır.	BM Kararları biçimindedir.	-

Kaynak: (Ilona, 2018: 8)

Tablo 11'de yer aldığı üzere, Sözleşme'nin hedef kitlesi tüm aktörler olarak belirlenirken, Nornickel, uygunluk noktasında BM Genel Kurulu kararlarındaki BİT çerçeveli konulara rotasını çevirmektedir. BM'nin örnek alındığı normların formu ise, söylem olarak BM Kararlarını andırması sebebiyle birbiriyle eşleştirilmektedir. Kolektif beklentiler sütunu uzun vadede devreye gireceği için analize dâhil edilememektedir.

3.3. Örgütler

Bu çalışmada siber norm oluşturma diyaloğunda uluslararası örgütlerin hukuk, politika ve stratejinin kesişimi, BİT'lerin geliştirilmesi ve kullanımına ilişkin normatif araçları sistematik bir şekilde kullanımına vurgu yapılmaktadır. Her örgütün kendi bağlamında farklı önceliklerden kaynaklanan yaklaşımlara sahip olduğu görülmekte ve kapasite ve yeteneklerdeki farklılaşmalara da bağlı olarak BİT'in yaygın kullanımındaki faydalar ve tehditler hakkındaki anlatılar değişiklik göstermektedir.

3.3.1. NATO

Kötücül yazılımların belirli özelikleri nedeniyle, silahların kontrolü, silahsızlanma ve silahların yayılmasını önleme gibi durumlar mevcut düzende olası görünmemektedir. Zira

doğrulamanın imkânsızlığı ortadadır. Ancak diğer yandan, siber alanda geliştirilecek olan normlar, bu tür saldırılara karşı bir direnç mekanizması oluşturabilir. NATO, BM Hükümet Uzmanları Grubu'nun 2013 Raporu'yla da uyumlu olacak şekilde, uluslararası hukukun siber uzay için de geçerli olduğunu iddia etmektedir. Sorumlu devlet davranışının gönüllü uluslararası normları ve siber uzay ile ilgili güven arttırıcı önlemler üzerine çalışma desteğini ilan etmekte olan NATO; bu durum müttefiklerin normlara dayalı, öngörülebilir ve güvenli bir siber alana açık olduklarını belirtmeleriyle de desteklenmektedir (Davis, 2019). Siber norm oluşturmak, siber uzaydaki belirsizliği azaltmak için etkili bir rehber olsa da, NATO'nun 29 üye ulusa sahip olduğu göz önüne alındığında, tüm üyelerin hemfikir olacağı normların üretilmesi kolay olmayacaktır. Bu nedenle, ittifakın tamamının aksiyon alması yerine, müttefik ülkeler tarafından bireysel olarak norm oluşturma çabaları yürütülmeli ve bu durum uluslararası toplumda teşvik edilmelidir (Davis, 2019).

NATO'nun, 3 Haziran 2020 tarihinde kötücül siber faaliyetlere ilişkin yaptığı basın açıklamasına (NATO, 2020) göz atıldığında, korona virüs etkeninin de dikkate alındığı altı maddeden oluşan bir demeç görülmektedir. İlk olarak, sağlık hizmetleri, hastaneler, araştırma enstitüleri gibi pandemiye karşı mücadele eden kritik konumdaki kişilere yönelik kötü niyetli siber faaliyetleri kınayarak başlayan NATO, böylesine kritik görevlere sahip olan sektörlere gerçekleşecek saldırıların vatandaşların hayatını tehlikeye atacağını belirtmektedir. Ardından salgına yanıt verme noktasında müttefikler ve ortaklarla birlikte sürece müdahil olduklarını söyleyen yetkililer, beraberinde ise, kötü niyetli siber faaliyetlerden etkilenenlerle dayanışma içinde olduklarını belirterek, temel hizmetleri etkileyen siber olaylara müdahale etmenin yanı sıra bilgi paylaşımı noktasında da yardım sunmaya hazır olduğunu belirtmektedir. Buna ek olarak, müttefiklerin ulusal sorumlulukları ve kabiliyetleri göz önüne alındığında, NATO'nun Siber Savunma Taahhüdü'nün uygulanacağını ve bununla birlikte kritik altyapıların korunması ve siber savunmalarını güçlendirmeleri noktasında kararlı olduklarını duyurmaktadır. 2018 yılında Brüksel'de gerçekleşen NATO Zirvesi'ne atıf yaparak siber savunmanın NATO'nun temel savunma görevinin bir parçası olduğunu ekleyen yetkililer, tüm siber tehditleri caydırmak, savunmak ve karşı koymak için siber yetenekler de dâhil olmak üzere NATO'nun tüm yeteneklerinin kullanılması konusunda kararlı bir duruş sergilemişlerdir. Devlet destekli aktörlere ek olarak devlet dışı aktörlerin de etkin olduğu siber tehdit ortamına uyum sağlamayı amaçlayan NATO, kurallara dayalı, öngörülebilir, açık, özgür ve güvenli bir siber alan hedefleyerek, uluslararası hukukun da siber uzayda geçerli olduğunu ve saygı duyulması gerektiğini belirterek tüm devletlerin kötü niyetli siber faaliyetlere karşı önemli bir role sahip olduğunu vurgulayarak demeci noktalamaktadır (NATO, 2020).

Tablo 12. Siber Normlar ve NATO

Örgüt	Siber Norm Hedefleri	Belirsizliği azaltmanın yolu
NATO	Kurallara dayalı, öngörülebilir, açık, özgür ve güvenli bir siber alan oluşturmak	Uluslararası Hukuk kurallarının uygulanması

Kaynak: Yazar tarafından tasarlanmıştır.

Yönetişim bağlamında NATO'nun Siber Savunma Politikası'nı anlamak, örgütün siber normlara yönelik yaklaşımını belirlemekte önemli olacaktır. Siyasi, askeri ve teknik

yetkililerin yanı sıra bireysel müttefikler tarafından da uygulanan Siber Savunma Politikası, örgütün en üst siyasi organı olan Kuzey Atlantik Konseyi'ne (NAC) bu noktada üst düzey siyasi gözetim yetkisi vermektedir (NATO, 2021b). NAC, siber olayların takibini yapmakta ve siber savunma bağlamındaki kriz yönetiminde ana yetkiye sahip olmaktadır.

Tablo 13. NATO'nun Siber Uzay Üzerine Faaliyet Gösteren Organları

Kurum	**Görevi**
Kuzey Atlantik Konseyi	• Siber Savunma Politikası'na göre üst düzey siyasi gözetim yetkisine sahiptir.
Siber Savunma Komitesi	• Siyasi yönetişim ve siber savunma politikası konusunda baş komitedir.
Siber Savunma Yönetimi Kurulu	• NATO'nun sivil ve askeri organları çerçevesinde siber savunmanın koordinasyonunu sağlar. • NATO içerisindeki politik, askeri, operasyonel ve teknik organların liderlerini bünyesinde barındır.
NATO Danışma, Kontrol ve Komuta Kurulu	• Siber savunmanın teknik ve uygulama yönleriyle ilgili danışma için ana komiteyi oluşturur
-NATO Askeri Yetkilileri -NATO Haberleşme ve Enformasyon Ajansı	• NATO'nun siber savunma yeteneklerinin operasyonel ihtiyaçlarının belirlenmesi, karşılanması, uygulanması ve işletilmesi ile ilgili tanımlama beyanında bulunur.
Müttefik Dönüşüm Komutanlığı	• Siber Koalisyon Tatbikatının yıllık planlanmasından ve yürütülmesinden sorumludur.
NATO Haberleşme ve Enformasyon Ajansı	• NATO genelinde teknik siber güvenlik hizmetlerinin sağlanmasından sorumludur.
NATO Bilgisayar Olaylarına Müdahale Yeteneği Koordinasyon Merkezi	• NATO içinde ve üye ülkelerle siber savunma faaliyetlerinin koordinasyonundan ve Siber Savunma Yönetimi Kurulu'na personel desteğinden sorumludur
NATO Bilgisayar Olaylarına Müdahale Yeteneği Teknik Merkezi	• NATO'yu etkileyen her türlü siber olaylara yanıt vermede kilit bir role sahiptir. • Olayları yönetir, olayla ilgili önemli bilgileri sisteme, güvenlik yönetimine ve kullanıcılara raporlar.

Kaynak: NATO, Cyber defence, 2021

NAC'a bağlı olan Siber Savunma Komitesi, siyasi yönetişim ve siber savunma politikası açısından baş komite olarak belirlenmiştir. NATO Siber Savunma Yönetimi Kurulu (CDMB) ise, NATO'nun sivil ve askeri organları çerçevesinde siber savunmanın koordinasyonunu sağlama sorumluluğuna sahiptir. CDMB, NATO içerisindeki politik, askeri, operasyonel ve teknik organların liderlerini bünyesinde barındırmaktadır (NATO, 2021b).

NATO'nun kavramsal olarak siber gelişimine bakıldığında, 2002'de Prag'da gerçekleşen NATO Zirvesi'nde "siber saldırılara karşı savunma kabiliyetlerini güçlendirmek" olarak başlayan süreç, siber savunmanın NATO'nun temel savunma görevinin bir parçası olduğunun kabul edildiği bir evreye gelmiştir (NATO, 2021b). Katzenstein'a göre, Soğuk Savaş'ın sona ermesinden sonra bir örgüt olarak NATO'nun dayanıklılığını açıklayabilmek için ittifaka yönelik ortak tehditlere bakmak gerekmektedir. Uluslararası siyasette devlet-dışı kurumların kabulü önemlidir. Böylece kültür ve normların bu yapılar içinde kendi başlarına nasıl geliştiğine odaklanılabilmektedir. Buna ek olarak, bahsedilen kültür ve normlar, dış baskılar tarafından da şekillenmektedirler. Bir kültür gelişerek bir kurumun içine yerleştiğinde, karar verme sürecine etki etmenin yanı sıra kurumun kimliğine de şekil vermektedir (Tosbotn, 2016). Kimlik ise, "NATO ve siber suçlular", "NATO ve bilgisayar korsanları" şeklinde hem kendisini hem de diğerini oluşturmaktadır. Normun tanımında yer

alan uygun davranış kısmını baz alarak, neyin uygun davranışı oluşturduğunu ortaya koyan ifadelere bakmak gerekmektedir. Örneğin, 2014 Galler Zirvesi'nin öncesinde "siber" ve 5. Madde ifadeleri bir arada bulunmamaktaydı. Eğer bir NATO müttefiki silahlı bir saldırıya uğrarsa, saldırıyı ittifakın tüm üyelerine karşı gerçekleştirilmiş olarak gören 5. Madde ve "siber" kelimelerinin bir arada bulunmamasının arkasında bir mantık söz konusudur (NATO, 2021a). Mantık ise şudur ki, eğer siber saldırılar da diğer operasyonel alanlardaki saldırılar ile eş değer görülürse, bu durum kolektif savunmanın ifade edildiği 5. Maddeyi tetikleyecektir. Bu bağlamda, NATO'nun kurumsal kimliğine karşı bir çıkarımda bulunurken ve dolayısıyla uygun davranışı oluştururken, kolektif savunma ve siber uzay arasındaki bu ilişkiyi göz önünde bulundurarak dikkatli bir yaklaşımda bulunmak gerekmektedir (Tosbotn, 2016). Bu tarz yerleşik algılar, NATO'da değişimin daha uzun süreli ve yavaş olabileceğini göstermektedir.

3.3.2. Siber Uzayın İstikrarı Hakkında Küresel Komisyon

Siber uzayın barışçıl kullanımına zarar verme riski taşıyan saldırgan siber faaliyetlerin artması durumu, istikrar ve güvenliğin bozulmasına yol açmaktadır. Bu bağlamda, tehditlere karşı koyabilmek için daha fazla diyaloğa ve girişime ihtiyaç duyulduğunu vurgulamak gerekmektedir. Diğer yandan, siber uzayı oluşturan ve üzerinde etkiye sahip olan birçok kurum bulunmasına rağmen, bazı topluluklar tarafından karşılıklı kabul noktasında sorun yaşanmakta, zira zayıf bir farkındalık söz konusu olmaktadır. Siber Uzayın İstikrarı Hakkında Küresel Komisyon (GCSC), diğer örgütlerden farklı olarak siber uzayda güvenlik ve istikrar üzerine politika ahengini desteklemeyi hedef olarak belirlemektedir. Uluslararası güvenlik ve istikrarın sağlanması, siber uzayda sorumlu devlet ve devlet-dışı davranışlara rehberlik etme amacıyla normlar ve politikalar için öneriler geliştirmek üzere tüm paydaşları bir araya getiren bir organizasyon olarak faaliyet göstermektedir. Komisyon, siber uzayın istikrarın; herkesin siber uzayı güvenli ve emniyetli bir şekilde kullanma yeteneğine güvenebileceği, sağlanan hizmetlerin ve bilgilerin güvence altına alındığı, değişimin göreceli bir barış için yönetildiği ve gerilimlerin çözüldüğü bir durum olarak açıklamaktadır (GCSC, 2019). GCSC, Kasım 2019 tarihinde Paris Barış Forumu'nda "Siber İstikrarı Geliştirme" başlıklı bir rapor yayınlamıştır. Raporda siber istikrarın geliştirilmesi için dört ilke, altı tavsiye ve sekiz norm önerilmektedir. Komisyon'a göre siber istikrarı sağlamak için gerekli normların temelinde yatan dört ilke vardır ve bu ilkeler sorumlu davranış normlarının önünü açmaya yardımcı olmaktadır:

- ✓ **Sorumluluk ilkesi;** siber uzaydaki istikrarı sağlama sorumluluğunun tüm aktörlere ait olduğunu ifade etmektedir.
- ✓ **Sınırlama ilkesi;** devlet veya devlet-dışı aktör fark etmeksizin hiçbir aktörün siber uzayın istikrarını bozan eylemlerde bulunmaması gerektiğini belirtmektedir.
- ✓ **Eyleme geçme gerekliliği ilkesine** göre; devlet veya devlet-dışı aktörler siber uzayın istikrarını sağlamak için uygun adımları gerçekleştirmelidir.
- ✓ **İnsan haklarına saygı ilkesi** ise; siber uzayın istikrarını sağlama yönündeki tüm çabaların, insan haklarına ve hukukun üstünlüğüne saygı göstermesi gerektiğini vurgulamaktadır.

Bahsi geçen dört ilke temelinde, Komisyon tarafından öne sürülen sekiz norm bulunmaktadır (GCSC, 2019):

- **Norm 1:** Devletler ve devlet-dışı aktörler, İnternetin kamusal çekirdeğini korumak, genel kullanılabilirliğine, bütünlüğüne ve dolayısıyla siber uzayın istikrarına kasıtlı ve büyük ölçüde zarar veren faaliyetlerde bulunmamalıdır.
- **Norm 2:** Devletler ve devlet dışı aktörler, seçimler, referandumlar veya halk oylaması için gerekli olan teknik altyapıyı bozmaya yönelik siber operasyonları takip etmemeli, desteklememeli veya izin vermemelidir.
- **Norm 3:** Devletler ve devlet dışı aktörler, geliştirme ve üretimdeki ürün ve hizmetlere müdahale etmemeli ve siber uzayın istikrarını önemli ölçüde bozabilecekse, bunların üzerinde onaysız değişiklik yapılmasına izin vermemelidir.
- **Norm 4:** Devletler ve devlet dışı aktörler, botnet olarak veya benzer amaçlarla kullanılmak üzere genel kamusal BİT kaynaklarına el koymamalıdır.
- **Norm 5:** Devletler, bilgi sistemleri ve teknolojilerinde farkında oldukları güvenlik açıklarını veya kusurları kamuya açıklayıp açıklamayacaklarını ve ne zaman ifşa edeceklerini değerlendirmek için prosedür açısından şeffaf çerçeveler oluşturmalıdır.
- **Norm 6:** Siber uzayın istikrarının bağlı olduğu ürün ve hizmetlerin geliştiricileri ve üreticileri güvenlik ve istikrara öncelik vermeli, ürün veya hizmetlerinin önemli güvenlik açıklarından arınmış olmasını sağlamak için makul adımlar atmalı ve zamanında önlemler almalıdır.
- **Norm 7:** Devletler, temel siber hijyeni sağlamak için yasalar ve düzenlemeler dâhil olmak üzere uygun önlemleri almalıdır.
- **Norm 8:** Devlet dışı aktörler saldırgan siber operasyonlara girmemeli ve devletler bu tür faaliyetleri engellemeli ve meydana gelirse müdahale etmelidirler.

3.3.3. Birlemiş Milletler

Siber uzay, 1998 yılında BM Birinci Komitesi'nde sunulan "Uluslararası Güvenlik Bağlamında Bilgi ve Telekomünikasyon Alanında Gelişmeler" adlı taslak ile birlikte, ilk kez masada yerini alarak bir BM sorunu haline gelmiştir. Taslakta, bilimsel ve teknolojik gelişmelerin, hem sivil hem de askeri pratiklere sahip olabileceği ve sivil pratikler açısından bilim ve teknolojideki ilerlemenin sürdürülmesi ve teşvik edilmesi gerektiği kabul edilmiştir (*Resolution Adopted by the General Assembly on the Report of the First Committee,* 1998).

Bu taslak, uluslararası toplumdaki siber norm arzusunun yeni olmadığını göstermesi açısından önem arz etmektedir. O yıllarda Batılı devletlerin çoğu genellikle "benzer düşünceye sahip devletler" terimi altında gruplandırılmaktadır ve onlara göre, siber uzay ve çevrimdışı dünya arasında büyük bir fark bulunmamaktadır. Bu nedenle de var olan uluslararası hukukun güncellenmesi yeterli olacaktır. Rusya'ya bakıldığında ise, o yıllardaki korkusunun tehlikeli bilgi silahlarının geliştirilmesi, üretilmesi ve kullanılması üzerine olduğu görülmektedir (Broeders ve Cristiano, 2020). Bu iki taraf arasındaki uzlaşmayı sağlayan ilk adım sözü geçen taslak olmuş ve 2002 yılında ilk BM Hükümet Uzmanları Grubu'nun (GGE) çalışmaları başlamıştır. GGE, siber uzayda ortaya çıkan

tehditleri ele almayı ve devletlerin BT'leri yönetmesi için kurallar oluşturmayı amaçlayan BM çalışma grubudur. Buna göre her grup iki yıllık bir süre için çalışmaktadır. 2002 yılından beri birbirini takiben altı farklı çalışma grubu, siber uzayda sorumlu devlet davranışının geliştirilmesi amacıyla BM'nin normatif bir güç olarak rolüne katkıda bulunmaktadır (Broeders & Cristiano, 2020).

2010 yılında BM Genel Sekreteri tarafından GGE'ye 15 devletten bir grup hükümet uzmanı atanmıştır. 2010 yılında yayınlanan 65/201 sayılı BM GGE Raporuna göre, tehdit kaynakları suçlular ve teröristler gibi devlet-dışı aktörler ve devletler olarak belirlenirken; BİT'lerin doğası gereği ikili kullanıma sahip olması sebebiyle, e-ticareti destekleyen aynı teknoloji, uluslararası barışı ve ulusal güvenliği tehdit etmek için de kullanılabilir şeklinde bir yaklaşım yer almaktadır. Zira telekomünikasyon ve İnternetin karmaşık bir şekilde birbirine bağlı olmasından dolayı, herhangi bir BİT cihazının kötüye kullanımın kaynağı veya hedefi olabilmesi mümkündür. Vakalarda failin kimliğinin tespit edilmesinin zor olabileceği ve buna bağlı olarak ortaya çıkan belirsizlik, ortak bir anlayışın olmaması durumu istikrarsızlığın ve yanlış bir algının ortaya çıkmasına sebep olabilmektedir. Diğer yandan da, devletlerin savaş ve istihbarat araçları olarak BİT geliştirdiklerine dair raporlarda artış görülmektedir. BM Uzmanları bu durumun bir endişe kaynağı olduğunu ve kötücül eylemlerin potansiyelini artıracağını öne sürmektedir. Tehdit olarak ise, BİT'lerin haberleşme, bilgi toplama, eleman seçme, organizasyonun sağlanması, fikirlerin ve eylemlerin teşvik edilmesi ve fonlama amacıyla teröristler tarafından kullanılması; atıf veya failin ilişkilendirilmesi sorunları, kritik altyapıların korunması, devletlerin BİT kapasitesi ve devletler arasındaki güvenlik anlayışındaki farklılıklar, BİT tedarik zinciri güvenliğinin sağlanması gibi örneklendirmelerde bulunulmaktadır.

2013 yılına gelindiğinde A/68/98 sayılı BM GGE Raporu incelendiğinde, tehdit kaynakları olarak devletler ve devlet-dışı aktörlerden bahsedilirken, normlar kısmında ise, GGE tarafından özel sektör ve STK'ların BİT'lerin güvenliğini arttırmak noktasında işbirliğine ihtiyaç duyulduğu vurgusu görülmektedir (BM Genel Kurulu, 2013). Bu anlamda GGE tarafından, BİT'lerin suçlar veya terör faaliyetleri için kullanımına karşı aktörlerin teşvik edildiği görülmektedir. BİT'lerin devletler tarafından kullanımında barış ve istikrarın teşvik edilmesi için öneriler sunma amacıyla ortaya konan 2013 GGE Raporu'na göre amacı itibariyle BİT'ler, meşru veya kötü amaçlı kullanım olarak ikiye ayrılan çift yüzlü teknolojilerdir ve küresel bağlantısallık, kırılgan teknolojiler ve anonimlik gibi etkenler BİT'lerin kötü amaçlı kullanımını arttırmaktadır (BM Genel Kurulu, 2013).

2015 GGE Raporu'na bakıldığında, tehdit kaynaklarının önceki rapordaki gibi devletler ve devlet-dışı aktörler olarak ele alındığı görülürken, sorumlu devlet davranışına yönelik gönüllü ve başlayıcı olmayan normlar ise, Tablo 5'te belirtilmektedir. BİT'lerin yanlış kullanımının uluslararası barış ve güvenliğe zarar verebileceğini vurgulayan Rapor, kapsamlı bir şekilde devletlere bir yol haritası çizmektedir. Ancak diğer yandan bu normlarının nasıl uygulanacağına dair keskin sınırlar çizilmemesi nedeniyle, otoriter devletlerin güvenliği sağlamada izleyeceği yol ile demokratik devletlerin izleyeceği yolun aynı olmadığı unutulmamalıdır.

Uluslararası örgütler çerçevesinde büyük bir öneme sahip olan BM, BİT'ler konusunda GGE Raporları ile devletlere tavsiyelerde bulunmakta, belirli normlar önererek siber uzaydaki davranış kurallarının düzenlenmesi anlamında çabalarını sürdürmektedir. Ancak BM Raporlarına yönelik yapılan eleştirilere göre normlar bağlayıcı olmalı ve ihlaller cezalandırılmalıdır. BM'nin caydırıcılık konusunda geride olduğunu söylemek mümkündür. 2004 yılında telekomünikasyon sistemlerinin güvenliğini arttırmak amacıyla kurulan GGE, 2017 yılına kadar küresel düzeyde siber güvenlik gündemini özetleyen ve uluslararası hukukun siber uzaydaki devlet davranışına uygulanabilirliğinden bahseden oturumlar düzenlemiştir. 2017 yılına gelindiğinde ise, GGE'nin 25 üyesi arasında meşru müdafaa ve uluslararası insani hukuk üzerine temel anlaşmazlıklar görülmüştür. Dolayısıyla 2017 yılında oturum konsensüs sağlanamadan bitirilmiştir. Konsensüsün sağlanması önemlidir zira siber norm inşası süreci diplomatik olarak konsensüsün sağlanması ile birlikte devletlerin siber uzaydaki davranışlarının şekillendirilebileceği fikrine bağlılık göstermektedir. GGE aracılığıyla BM'nin yukarıdan aşağıya hiyerarşik bir model baz alarak norm inşası süreci gerçekleştirmeye çalıştığı ve bu nedenle başarısız olduğu iddia edilmektedir.

Temel anlaşmazlıklara gelindiğinde, uluslararası hukuka göre gerçekleşen saldırıyla orantılı olarak güç kullanmayı ifade eden meşru müdafaa hakkının siber uzayda kullanımının zor olacağı açıktır. GGE ise bu konuyu netleştirmek için bir çözüm öne sürmemektedir. Uluslararası insani hukuk bağlamında ise, fiziksel dünyada gerçekleşen bir savaş içerisinde savaşçılar ve siviller arasında bir ayrım yapılmakta ve böylelikle savaş insani hukuk bağlamında yönetilebilmektedir. Ancak siber uzayda bu ayrımın yapılması kolay olmamaktadır. Zira bir siber saldırının ulusal güvenliğe yönelik tehdit oluşturabilmesi için hedefin geleneksel bir aktör olmasına gerek yoktur. Bu anlamda ilk anlaşmazlık 2015 GGE Raporu'nda ortaya çıkmış, Çin ve Rusya delegeleri konunun belgelerde açıkça belirtilmesine itiraz etmişlerdir. 2015 yılında sade kelimeler kullanılarak ortaya yol bulunmuş olsa da, 2017 yılındaki GGE oturumunda bu konunun aşılamaz olduğu ortaya çıkmış ve konsensüs sağlanamamıştır. Örneğin Küba Heyeti tarafından, BİT bağlamında bir savaş senaryosunu ve askeri eylemleri meşrulaştırdığı iddiası üzerine uluslararası insani hukukun siber uzaydaki uygulanabilirliği reddedilmiştir. Küba'nın ABD tarafından önceki çabaları geçersiz kılmakla suçlanması sonucu Küba, Çin, Rus delegeleri tarafından tam şeffaflığa ve kapsayıcılığa sahip, karar alma süreçlerinde eşit hakların verildiği yeni bir çalışma grubu kurulması fikri öne sürülmüştür. Tüm bu süreçler göz önüne alındığında BM bağlamında, yukarıdan aşağıya hiyerarşik model baz alınarak inşa edilmeye çalışan normların inşa sürecinde zorluklar yaşandığı görülmekte, ulusal güvenlik ve savunma konularını içeren normların konsensüse ulaşmasının zor olduğu, farklı bakış açıları arasında orta bir yolun bulunması ve böylelikle ilerlemenin sağlanabilmesi için ise, hükümetlerin fikir alışverişlerine açık olması gerektiği görülmektedir.

Bilgi ve telekomünikasyon çerçevesinde GGE'nin çalışmaları elzem olsa da, BM'deki diğer alt örgütler olan İnternet Yönetişim Forumu, Uluslararası Telekomünikasyon Birliği, Dünya Bilgi Toplumu Zirvesi ve İnternet Yönetişimi Çalışma Grubu gibi diğer alt örgütlerin BİT'ler noktasındaki faaliyetlerine de göz atmak gerekmektedir.

3.3.3.1. İnternet Yönetişim Forumu

IGF (İnternet Yönetişim Forumu) bünyesindeki yönetişim çalışmalarına bakıldığında, her yıl düzenlenen forumun, 2018 yılındaki açılışında Fransa Cumhurbaşkanı Macron tarafından "Siber Uzayda Güven ve Güvenlik için Paris Çağrısı" başlıklı bir bildirge sunulduğu görülmektedir. Bu bildirgenin hedefi, siber uzayın güvenliğini sağlamak için ortak ilkeler geliştirmeye yönelik çalışmalarda bulunmak olmuştur. Bildirgeyi özetlemek gerekirse (GIP Digital Watch, 2021):

- Hem barış zamanında hem de silahlı çatışma sırasında mağdurları desteklemeye davet etmek,
- Siber suçla mücadelede kilit araç olarak Budapeşte Sözleşmesi'nin yeniden tasdik edilmesi,
- Ürünlerin güvenliği için özel sektörün sorumluluğunu kabul etmek
- Geniş dijital işbirliği ve kapasite oluşturma çağrısında bulunmak gibi maddelerden oluştuğu görülmektedir.

Bu bağlamda Paris Çağrısı, hem devletler hem de özel sektör için geçerli olan dokuz temel prensip ortaya koymaktadır (GIP Digital Watch, 2021):

- **Prensip 1:** Kötücül faaliyetleri engellemek ve kurtulmak için bireylere ve altyapı tesislerine yardımcı olmak;
- **Prensip 2:** İnternetin kamusal çekirdeğini –paket yönlendirme ve iletme, adlandırma ve numaralandırma sistemleri, kimlik ve güvenliğin şifrelenmesi, fiziksel iletim ortamı (Global Commission on the Stability of Cyberspace, 2018)– korumak;
- **Prensip 3:** Seçim süreçlerini müdafaa etmek;
- **Prensip 4:** Fikri mülkiyet hırsızlığını önlemek;
- **Prensip 5:** Kötücül yazılımların ve uygulamaların yayılmasını önlemek;
- **Prensip 6:** Dijital süreçlerin, ürünlerin ve hizmetlerin güvenliğini güçlendirmek;
- **Prensip 7:** Siber hijyeni –sistem sağlığını korumak ve çevrimiçi güvenliği iyileştirmek (Brook, 2020)– geliştirmek;
- **Prensip 8:** Faile karşı geri saldırıda bulunmaktan kaçınmak
- **Prensip 9:** Uluslararası sorumlu davranış normlarının kabulünü ve uygulamalarını teşvik etmek.

Siber uzayda güven inşasının ve güvenliğin sağlanması için Paris Çağrısı çerçevesinde ortaya konan 9 prensip önem arz etmektedir. Çağrı, birçok anlamda diğer aktörlerin normlarını andırsa da, önemli olan nokta GCSC'nin yedinci normuna benzer şekilde burada da Prensip 7'de yer alan, sistemin sağlığını korumak ve çevrimiçi güvenliği iyileştirmek anlamına gelen siber hijyen kavramının norm inşası süreçlerindeki fikir alışverişlerinde kullanılmasının fayda sağlayacağının ön görülmesidir.

3.3.3.2. Uluslararası Telekomünikasyon Birliği

BM çerçevesindeki yönetişim örgütlerinden biri olan Uluslararası Telekomünikasyon Birliği'nin (ITU) temel görevi ise, BİT'lerin kullanımında emniyet ve güvenlik oluşturmak

olan bir BM kuruluşudur (International Telecommunication Union, 2021). ITU'nun çalışmalarını anlayabilmek için 2018 yılında çıkarmış olduğu Ulusal Siber Güvenlik Stratejisi Geliştirme Kılavuzu'na göz atmak gerekmektedir. Bu kılavuz kamu, özel sektör, akademik çevre ve STK'ları içeren on iki ortağın bilgi, deneyim ve uzmanlığı çerçevesinde hazırlanmış, başarılı bir siber güvenlik stratejisini oluşturan noktaları inceleyen kapsamlı bir çalışmadır (International Telecommunication Union, 2018). Siber güvenlik kapasitesi oluşturma konusunda uluslararası toplumda işbirliği ve koordinasyonu güçlendirme ihtiyacıyla bir araya gelen ortaklar siber güvenlik, siber hazırlık ve dayanıklılık hakkında stratejik düşünmenin sağlanması ve ulusal liderlere ve politika yapıcılara rehberlik etme amacını taşımaktadırlar.

3.3.3.3. Dünya Bilgi Toplumu Zirvesi

Dünya Bilgi Toplumu Zirvesi (WSIS), internet yönetişimin çok paydaşlı bir temelde yürütülmesi gerektiğinin ifade edildiği ilk zirve olarak kabul edilmektedir. Bilgi ve iletişim teknolojisine ve bu açıdan ilerlemeye odaklanacak bir zirve fikri 1998'de ITU tarafından geliştirilmiş ve 21 Aralık 2001'de BM Genel Kurulu'nun 56/183 sayılı kararıyla iki aşamada yapılması şeklinde yetkilendirilmiştir (WSIS, 2006).

İlk zirvesi Aralık 2003'te Cenevre'de, ikincisi ise Kasım 2005'te Tunus'ta gerçekleştirilen WSIS, iki aşamalı bir etkinlik olarak planlanmıştır.

- **10-12 Aralık 2003 Cenevre Aşaması:** Cenevre'de gerçekleştirilen ilk WSIS Zirvesi'nin amacı, tüm farklı çıkarları yansıtarak herkes için bir Bilgi Toplumunun temellerini oluşturmak için somut adımlar atmak olarak belirtilmiştir (WSIS, 2006). WSIS'ın Cenevre Aşaması'na 175 ülkeden yaklaşık 50 devlet/hükümet başkanı, 82 bakan ve 26 bakan yardımcısının yanı sıra uluslararası örgütler, özel sektör ve STK'lardan da üst düzey temsilcileri içeren 11 binden fazla kişi katılmış ve bu kişiler Aralık 2003'te kabul edilen Cenevre Prensipler Deklarasyonu ve Cenevre Eylem Planı'na siyasi desteklerini belirtmişlerdir (WSIS, 2006). ICANN'a yönelik eleştirilerin resmi olarak ifade edilebileceği bir forum imkânı sağlayan Cenevre Aşaması'nda Güney Afrika, Çin ve Brezilya hükümetleri, ICANN'ın mevcut İnternet yönetişim düzenlemelerinden memnun olmadıklarını ve ABD yanlı bir kuruluş olarak faaliyet gösterdiğini belirtmişlerdir (Mueller vd., 2007).

12 Aralık 2003'te WSIS tarafından ilan edilen Cenevre Prensipler Deklarasyonu'nun 48'inci paragrafında çok paydaşlılık şu şekilde ifade edilmektedir:

> "İnternet, halka açık küresel bir tesise dönüşmüştür ve internetin yönetimi Bilgi Toplumu gündeminin temel konusunu oluşturmalıdır. İnternetin uluslararası yönetimi; hükümetlerin, özel sektörün, sivil toplumun ve uluslararası kuruluşların tam katılımıyla çok taraflı, şeffaf ve demokratik olmalıdır. Kaynakların adil dağılımı sağlanmalı, erişim herkes için kolaylaştırılmalı ve çok dillilik dikkate alınarak İnternet'in istikrarlı ve güvenli işleyişi sağlanmalıdır (WSIS, 2003)."

İnternet yönetişiminin tüm paydaşları ve ilgili hükümetler arası ve uluslararası kuruluşları içermesi gerektiğini belirten Cenevre Deklarasyonu, insan merkezli bir Bilgi Toplumu oluşturmanın, tüm paydaşlar arasında işbirliği ve ortaklık gerektiren ortak bir çaba olduğunu vurgulamaktadır. Deklarasyonda; özel sektörün, hem teknik hem de ekonomik alanda İnternet'in gelişmesinde, STK'nın toplum düzeyindeki İnternet konularında,

hükümetler arası örgütlerin İnternet ile ilgili kamu politikalarının koordinasyonunu kolaylaştırmada, uluslararası örgütlerin ise, İnternet ile ilgili standartların geliştirilmesinde önemli rollere sahip olduğu ve olmaya devam etmesi gerektiği öne sürülmektedir (WSIS, 2003).

- **16-18 Kasım Tunus Aşaması:** İkinci aşama olan Tunus Aşaması'nın amacı, Cenevre Eylem Planı'nın taahhütlerinin yinelenmesine ek olarak İnternet yönetişimine ve finansal konulara odaklanmak olarak belirlenmiştir (WSIS, 2005). Önceki aşamadan farklı olarak çocukların korunmasında ve çocukların gelişiminin arttırılmasında BİT'in rolünü vurgulayan Tunus Taahhüdü, çocukları istismardan korumak ve BİT bağlamında haklarını savunmak için eylemleri güçlendirmeyi birincil olarak vurgulamaktadır. Bilgiye adil ve sürdürülebilir bir biçimde erişim sağlanabilmesi ve dijital ortamdaki bilgilerin korunması için belirli stratejilerin uygulanmasının gerekliliğini vurgulayan Tunus Taahhüdü, dijital uçurumun üstesinden gelmeyi planlamaktadır.

Cenevre ve Tunus Aşaması olarak iki aşamadan oluşan WSIS, çok paydaşlılığın vurgulandığı ilk zirve olarak uluslararası sistemdeki yönetişim çabalarını destekleyen büyük bir adım olmuştur. Farklı aktörlerin fikir alışverişinde bulunduğu WSIS, farklı çıkarları ortaya koyarak siber uzaydaki sorunlara ışık tutmayı amaçlamıştır.

3.3.3.4. İnternet Yönetişimi Çalışma Grubu

WSIS'ın Cenevre Aşaması ilkelere, Tunus Aşaması ise bu ilkelerin ve takip mekanizmalarının uygulanmasına odaklanmaktadır. Ancak WSIS'ın ilk aşaması olan Cenevre Aşaması İnternet yönetişimi konusundaki farklılıkları çözemediğinden, BM 7. Genel Sekreteri Kofi Annan tarafından WSIS'ın ikinci aşaması olan Tunus Aşaması'na İnternet yönetişimi alanında rapor vermesi amacıyla WGIG (İnternet Yönetişimi Çalışma Grubu) kurulmuştur (Malcolm, 2008). WGIG'ın İnternet yönetişimi üzerine araştırmalar yapmasının ve eylem önerilerinde bulunmasının yanı sıra önceki aşamalarda eksik kalan aşağıdaki başlıklar da görev tanımına eklenmiştir (WSIS, 2003):

-İnternet yönetişimi kavramını karşılayan bir tanım geliştirmek

-İnternet yönetişimi ile kamu politikası konularını belirlemek

-Hükümetler, hükümetlerarası kuruluşlar, uluslararası örgütler, özel sektör ve STK'ların rolleri ve sorumlulukları hakkında ortak bir anlayış geliştirmek

Kasım 2004 tarihinde kurulan WGIG; iş dünyası, hükümet ve STK'ları temsil etmek için kırk kişilik bir gruptan oluşmaktaydı. WGIG'in oluşumunun arkasında yatan en büyük gücün ICANN'e yönelik sahip olunan memnuniyetsizlik olduğunu söylemek mümkündür. Temmuz 2005'te yayınlanan rapor ile birlikte İnternet yönetişimi kavramı genişletilmiş, kavram İnternet ile ilgili her türlü kamu politikasını içerecek şekilde yeniden düzenlenmiştir. WGIG'ın 2005 Raporu'na göre İnternet yönetişimi; hükümetler, özel sektör ve sivil toplumun kendi rollerine uygun şekilde paylaştığı ilkeler, normlar, kurallar, karar verme prosedürleri ve İnternet'in evrimini ve kullanımını şekillendiren programların geliştirilmesi ve uygulanması olarak tanımlanmaktadır (WGIG, 2005) . Bu tanımdan, İnternet yönetişimi mekanizmalarındaki paydaşlar konusunda kapsayıcılığa sahip olduğu

ve her grubun farklı çıkarları ve rolleri üzerinden sürece katılım sağlanacağı çıkarımı yapılabilmektedir.

BM alt örgütleri olan IGF, ITU, WSIS ve WGIG, temelde İnternet yönetişimi konusunda ilerlemelerin sağlanmasının amaçlandığı, farklı aktörler arasında fikir alışverişinde bulunulan çeşitli ortamlar ve imkânlar sunan kuruluşlar olarak faaliyet göstermiştir. Çok paydaşlılığın temel alındığı ve farklı çıkarların tartışıldığı bu örgütlerin faaliyetlerinin İnternet yönetişimi bağlamında dikkate alınması esastır.

SONUÇ

Soğuk Savaş sonrası dönemde siber uzay, çok farklı ve artan sayıda aktörün rekabetine konu olan stratejik bir operasyonel alan olarak öne çıkmaktadır. Siber uzayın sınırsız ve dinamik yapısı bir taraftan çeşitli fırsatlar sunarken, diğer taraftan da yarattığı belirsizliklerle aktörlerin meydan okumalarla karşı karşıya kalmalarına sebebiyet vermektedir. Bu çerçevede önünüzdeki dönemde uluslararası sistemin işleyişinde artan düzeyde etkili olacağı düşünülen siber uzay kapsamında farklı düzeylerdeki aktörlerin norm oluşturmaya yönelik çalışmalar yaptıkları gözlenmektedir. Normlar üzerinden siber uzayın belirsiz yapısına çeşitli açılardan netlik kazandırılmaya ve bu kapsamda siber alandaki operasyonlara bir çerçeve geliştirilmeye çalışılmaktadır. Bu tez çalışmasında, Soğuk Savaş sonrası dönemde öne çıkan siber uzay çerçevesinde sistemin başlıca aktörleri olarak devletler, özel şirketler ve örgütler bağlamında ortaya konan norm oluşturma çabaları incelenmektedir.

Çalışma kapsamında aktörler bağlamında devletlerin, uluslararası örgütlerin ve özel şirketler çerçevesinde ağırlıklı olarak teknolojik şirketlerin faaliyetlerine değinilmiştir. Çalışmada devletlerin siber normları hangi çerçevede ele aldıkları araştırılmış ve bu bağlamda öncelikle yönetişim ağı tasarısının unsurlarından bahsedilmiştir. Bir yönetişim ağının tasarısında yer alabilen unsurlar olarak anarşik, hiyerarşik, demokratik, karşılıklı mutabakata dayalı tasarılardan bahsedilerek yönetişim planının unsurlarının anlatıldığı tez çalışmasında, uygulanabilirlik açısından ise, siber egemenlik ve çok paydaşlı İnternet yönetişim yaklaşımlarının geçerli olduğu görülmüş ve devletleri incelerken kullanılan modeller olarak bu iki yaklaşım dikkate alınmıştır.

Siber egemenlik ve çok paydaşlı yönetişim modellerinin unsurları üzerinden devletlerin siber uzaydaki norm oluşturma çabalarının incelendiği çalışmada, devletlerin teknik düzenlemeler ve normlar üzerinden geliştirdikleri söylemler bağlamında yönetişim anlayışları analiz edilmiştir. ABD'nin siber yönetişim anlayışının, siber uzaydaki sorunlarla mücadelede en adil ve en etkili yol olarak çok paydaşlı yaklaşım modelini seçtiği ve temel amacının ise, otoriter rejimlere karşı bir duruş sergileyerek parçalanmayan tek bir küresel İnternet oluşturmak olduğu kanaatine varılmıştır. Tez çalışmasının bütünü itibariyle düşünüldüğünde, ABD'nin tüm bu düzenlemelerini liberal fikirler üzerinde inşa ettiği ve aynı zamanda stratejik anlamda da çok paydaşlı yönetişim modelini, Çin ve Rusya ile mücadelede bir araç olarak şekillendirdiği sonucuna varılmıştır. ABD'nin siber alandaki norm oluşturma çabalarının temel itibariyle siber uzaydaki tekelini sürdürmek ve Çin tarafından geliştirilebilecek meydan okumaların önünü alabilmek çerçevesinde yükseldiği görülmüştür.

Çin'in norm oluşturma çabalarına bakıldığında da, uluslararası müzakerelerde siber egemenlik modelini empoze ettiği ve bu modeli güçlendirme hedefleri doğrultusunda faaliyetlerde bulunduğu görülmüştür. Siber egemenlik modelinin Çin'e göre yorumunun, zararlı görülen fikir ve görüşlerin vatandaşlara tesir etmesini engellemek olduğunu söylemek mümkündür. Buna ek olarak, Çin'in siber egemenlik çerçevesinde ele aldığı bir diğer önemli noktanın ise, İnternet yönetişiminde devletlerin temel aktörler olduğu BM benzeri bir uluslararası foruma geçilmesi yönünde olduğu görülmüştür. Geleneksel

yaklaşımları yansıtır şekilde birinci aktörler olarak devletleri ele aldığı görülen Çin'in, siber uzayda gücün devletlerin tekelinde toplanacağı bir rejim tahayyül ettiği kanısına varılmıştır. BİT şirketlerinin küresel olarak yayılması, iletişim ağlarından eş zamanlı iletişim sistemlerine kadar gelişen bir dizi yeni teknolojiyle kolaylaştırılmıştır. Çin tarafından bu genişlemenin sonucu olarak, kentsel bölgelerde her şeyi bilme vaadini ortaya koyan güvenli şehir sistemleri piyasaya sürülmüştür. Çok paydaşlı yönetişimi teşvik etmeyen Çin, Çin merkezli ZTE ve Huawei gibi özel şirketler ile faaliyetlerini sürdürmekte ve yapılan projelerde devlet ve özel şirketlerin birlikte hareket ettiği görülmektedir. Finansal ve organizasyonel araçlar kullanarak güvenli şehir sistemleri bağlamında dönüşüme öncülük eden Çin'in geliştirdiği projeler içerisinde özellikle de gözetim noktasında yoğunlaştığı görülmüştür. Bu tez çalışmasında, gözetim araçlarının pek de uzak olmayan bir gelecekte Çin'den başlayarak önce Rusya'ya, ardından da Orta Asya ülkelerine yayılarak nasıl bir hızla gelişebileceğine ve olası sonuçlarına dikkat çekilmiştir. Bu dönüşümü sağlayan temel dinamik, Çin'in siber egemenlik yaklaşımını normatif anlamda merkeze alarak projelerini gerçekleştirmesidir.

Rusya'nın norm oluşturma çabaları incelendiğinde ise, ABD'nin etkisini azaltmak amacıyla yeni düzenlemeler üzerinden İnternetin şekillendirilmesi kapsamında Çin ile işbirliğine gittiği görülmüştür. Çin'in siber egemenlik modelini taklit eden Rusya, teknik anlamda Çin'den bağımsız hareket etmek istemekte ancak altyapı zayıflığı nedeniyle bağımlılığı sürmektedir. Bu bağımlılığın yanı sıra Çin'in geliştirdiği siber teknolojiler üzerinden Orta Asya'da nüfuzu artmakta ve Çin'in güvenli şehir teknolojisi bu bölgede rağbet görmektedir. Çin'in gözetim teknolojileri Orta Asya hükümetleri son derece popülerdir. Kısa vadede, Putin ve diğer Rus liderler tarafından Çin'e olan bağımlılığın yönetileceği ve Çin'in Orta Asya'daki faaliyetlerine göz yumulabileceği şeklinde bir yaklaşım söz konusu olmakta; zira Rusya'nın Çin'in siber egemenlik modelini benimsemesinin ve Çin ekipmanlarını kullanmasının hükümetin iç istikrarını korumakta yardımcı olacağı düşünülmektedir. Diğer taraftan iki ülke arasında askeri ve ekonomik güç kabiliyetleri bağlamında asimetrik bir artış söz konusu olduğundan, uzun vadede bu yaklaşım belirsizliği de beraberinde getirmektedir. Güvenli şehir teknolojisinde görüldüğü üzere Çin etkisinin güçlenmesi, Rusya'nın Orta Asya'daki nüfuzunun azalmasına neden olmakta ve tüm bunlara ek olarak Çin yine de kendini bu alanda geliştirmeye devam etmektedir. Dolayısıyla Çin'in bu alandaki adımları, önümüzdeki dönem itibariyle Rus nüfuzuna yönelik bir meydan okuma olarak da görülebilecektir.

Özel şirketlerin ortaya koyduğu girişimler incelendiğinde, şirketlerin norm girişimcileri olarak süreçte yer aldıkları görülmektedir. İncelenen özel şirketlerin çabalarına bakıldığında ortak beklentiler arasında kötü niyetli eylemlerin engellenmesi ve Rusya merkezli Nornickel dışındaki şirketlerin çok paydaşlı yönetişimi teşvik etmesi yer almıştır. Aktörler olarak farklı gruplara seslenmeyi tercih eden şirketlerin hepsi şeffaflık, kişisel verilerin korunması ve güvenlik sistemlerinin güçlendirilmesi noktasında ortak prensiplere sahiptir. Diğer yandan, kolektif beklentilerden söz edilememekte zira bu girişimler henüz sadece öneri aşamasında kalmaktadır.

2016 yılında Microsoft içinde yayılan "Siber güvenlik olmadan ulusal güvenlik olmaz" cümlesiyle başlayan ve şirketi, uluslararası güvenlik dünyasına doğru yönelten süreç, Microsoft'un kendi çerçevesini ortaya koyarak siber güvenlik anlamında belirli normlar önerdiği ve böylece bir norm girişimcisi profiline kavuştuğu bir aşamaya doğru evirilmiştir. Microsoft tarafından dijital platformun küresel ortamdaki rolünün arttığının ve teknoloji şirketlerinin dijital manada önemli rollere sahip olduğunun somutlaştırıldığı Dijital Cenevre Sözleşmesi, Microsoft'un uluslararası güvenlik ortamında kendi önemini konumlandırması açısından önemli bir aşama olarak görülmüştür. Sözleşme ile gelen önemli noktalardan biri ise, Microsoft'un siber saldırıları küresel bir insani sorun olarak betimlemesi ve siber saldırı olduğunda müdahale edecek ilk yardım ekiplerinden bahsetmesidir. Microsoft'un Dijital Cenevre Sözleşmesi ise, anlaşma yoluyla ilkelerini bağlayıcı hale getirmeyi amaçlamaktadır

ABD'nin Dijital Güvenlik ve Kanuni Prosedür Üzerine Bulut Çağı İçin Yeni Bir Yasal Çerçeve dokümanını destekleyen Google ise, bulut tabanlı teknolojinin büyümesiyle beraber gerçek güvenlik sorunlarının arttığını ve mahremiyet konusunun gündeme geldiğini vurgulamıştır. Bu bağlamda ABD'nin Uluslararası İletişim Gizliliği Yasası olan ICPA'ya da destek vermeyi tercih eden Google, küresel gizlilik standartlarının iyileştirilmesi ve yabancı hükümetlerin soruşturmalar için kanıt elde edebilmeleri için bir yol izlemekte, bu kapsamlı süreçte reform olarak kabul edilebilen yasalar noktasında kanun yapıcılar, düzenleyiciler, STK'lar, özel şirketler ve uzmanlarla işbirliğine gitmeyi teşvik etmektedir. Diğer yandan Google'ın Avrupa Komisyonu ve Türkiye'deki Rekabet Kurumu'ndan aldığı cezalar göz önüne alındığında, kendisi normatif anlamda idealist bir bakış açısına sahipken, pratikte ise, kendi hizmetlerini öne süren, ticari kaygılar ve kâr peşinde koşan bir şirket olduğu ortaya çıkmıştır.

Güven Sözleşmesi'ni ortaya atarak dijital teknolojilerin güvenli ve emniyetli olmasını savunan Siemens'in ise, dijital dönüşümün benimsenmesi için bireylerin ve kuruluşların güven kavramını içselleştirmeleri gerektiği şeklinde bir bakış açısına sahip olduğu görülmüştür. Çalışmada, Siemens'in öne sürdüğü Sözleşme ile devletler ve teknolojik şirketleri hedeflediği tespit edilmiş, norm oluşturma yöntemi ise, öne sürülen prensipler üzerinde gerçekleşecek kamu mutabakatı olarak belirlenmiştir. Siemens, sektörün başlıca faaliyetlerini sürdürdüğü dijital ekonominin başarılı olabilmesinin olmazsa olmazı olarak siber güvenliği görmekte ve bu sözleşmenin de siber güvenliğin pratikte uygulanması için tamamlayıcı bir adım olduğunu öne sürmektedir.

Siber uzaydaki tehditlerin artması sonucu kritik altyapıların korunması devletlerin gündemine alınmıştır. Kritik Endüstriyel Tesisler İçin Bilgi Güvenliği Sözleşmesi ise, Rus merkezli Nornickel'in bu bağlamda öne sürdüğü bir adımdır. Sözleşmenin taraflarının, ulusal ekonomiler üzerinde negatif bir etki oluşturabilecek herhangi bir faaliyete katılmayı gönüllü olarak reddettikleri görülmüştür. Sözleşme çerçevesinde haksız rekabetle mücadele etmek ve BİT'lerin kritik endüstriyel tesislere verebileceği zararları önlemek için belirli kurallar ve davranış standartlarının oluşturulmasının hedeflendiği görülmüştür. Kuzey Kutup Dairesi'nde sağladığı İnternet ve bağlantılı hizmetlere ek olarak, bin kilometreye kadar uzanan fiber optik hatların olduğu projelere sahip olan Nornickel,

spesifik olarak sahip olduğu önemli konumdan dolayı siber güvenliğe yoğun bir şekilde vurgu yapmaktadır. Norm oluşturma biçimi olarak BİT çerçeveli BM Kararlarını örnek alan Nornickel'in, hedef kitlesini aktörler bazında sınırlamadığı görülmüştür.

Estonya Saldırısının ardından siber uzayın günlük olarak teknolojinin kullanılmasıyla sınırlı kalmadığı, bir strateji geliştirme alanına dönüştüğü görülmektedir. Siber uzaydaki belirsizlik dikkate alındığında, aktörlerin güvenliklerini etkileyen stratejik bir belirsizlik durumunun ortaya çıktığını söylemek mümkündür. Bu tez çalışmasında, norm oluşturma sürecinin gerçekleşmesi, diğer bir deyişle yeni siber normların geliştirilmesi stratejik sosyal yapının bir uygulaması çerçevesinde ele alınmıştır.

Estonya saldırılarından da görüldüğü üzere NATO üyelerine yönelik saldırıların artması, NATO'nun siber güvenlik anlamında çalışmalarını yoğunlaştırmasına ve bu noktada faal hale gelmesine sebep olmuştur. Kolektif savunma ilkesi çerçevesinde bir NATO üyesine yapılan saldırının diğerlerine yapılmış sayılması söz konusu olduğunda, değişen konjonktür ile birlikte aynı ilkenin siber uzaya uyarlandığı görülmektedir. Küresel bir yapı çerçevesinde farklı aktörler çerçevesinde farklı şekilde algılanabilecek olan insan hakları, ifade özgürlüğü gibi konularda ise, değişken yorumlara kapı açabilecek normların siber alanda şekillendirilmesi ve uygulanması durumunun da çeşitli dönüşümlere sahne olacağını öne sürmek mümkündür. Çeşitli aktörler tarafından vurgulanan insan hakları ve iade özgürlüğü konuları, çalışmadaki örneklendirmelerden anlaşılacağı üzere devletlerin yanı sıra özel sektör ve çeşitli paydaşların da etki alanına girmektedir. Normların şekillendirmesi çabalarının, uluslararası sistemin geleceği noktasında bireyler, özel şirketler ve diğer paydaşlar tarafından insani güvenlik düzeyinde çalışmalara kapı açabileceği düşünülmektedir.

Yukarıda ana hatları verilen çeşitli öneriler, hükümetlerin, özel şirketlerin ve uluslararası örgütlerin siber alanda nasıl davrandıklarını düzenleyen kapsamlı anlaşmaları kapsamakta ve daha küçük devlet veya şirket grupları için belirli konularda önerilerde bulunmaya çalışmaktadır. Esasında bu önerilerin her biri, 2015 yılında BM GGE raporunda öne sürülen normlara dayanmaktadır. GCSC, BM normlarını İnternet altyapısına ve seçim sistemlerine uygulamaktadır. Burada önemli olan, bu fikirlerin özel sektörden ve sivil toplum kuruluşlarından gelmesidir. Zira BM normlarından esinlenerek kendi normlarını oluşturan ve böylelikle siber uzayda norm oluşturma çabalarına katkı sağlayan aktörler belirsizliğin azaltılması yönünde önemli adımlar atmaktadır. Devletler bağlamında BM çalışma grubunun tekrar toplanması veya başka girişimler oluşturulması gerekirken, bu durum gerçekleşmediği takdirde -kabul edilen normların devletler tarafından kabul edilip edilmeyeceği net olmasa da- siber normların geleceğinin büyük oranda özel şirketlerin norm girişimciliği yönündeki faaliyetlerine bağlı olduğunu belirtmek gerekmektedir.

Bu tez çalışmasında açıkça görülmektedir ki, aktörler, stratejik bir belirsizlik ortamı olarak ele alınan ve beşinci operasyonel alan olan siber uzaydaki davranışları şekillendirebilecek normlar çerçevesinde kimi zaman farklı kimi zaman da örtüşen vizyonlara sahiplerdir. Siber uzaydaki bilinmezlik göz önüne alındığında, aktörlerin ortak bir paydada buluşmasının zor olduğu görülmektedir. Zira devletler, kendi aralarında veya uluslararası örgütler aracılığıyla ulusal çıkarlarını merkeze aldıkları yaklaşımlara sahip olmaktadırlar.

Çalışmada siber uzayda stratejik olarak inşa edilen siber normların kendisinin bir rekabet haline geldiği sahada, stratejik norm inşası sürecinin çok sayıda aktör arasında çeşitli konular üzerinden farklı mücadelelere sahne olduğu görülmüştür. Söz konusu belirsizliği azaltmak adına bir çerçeve oluşturabilecek olan siber normlar üzerinden ABD'nin siber uzaydaki hâkimiyetini arttırabilme olasılığına sahip olduğu; Çin'in Orta Asya üzerindeki nüfuz alanlarının genişlemesine ve dolayısıyla Rusya'nın nüfuzunun daralmasına sebebiyet verebileceği çıkarımında bulunulmuştur. Bu çerçevede Rusya ve Çin'in siber uzay üzerinden geliştirdiği işbirliğinin uzun dönemde farklı sonuçlar verebileceği ve uzun vadede bölge üzerinden bir hâkimiyet mücadelesine yol açabileceği tahmin edilmektedir.

Siber uzayda stratejik olarak inşa edilen siber normların bir rekabet unsuru haline geldiği sahada, stratejik norm inşası sürecinin hem devletler hem de devletler ile özel şirketler gibi diğer paydaşlar arasında çeşitli mücadelelere sahne olduğu görülmektedir. Bu çerçevede siber alandaki normların şekillendirilmesi süreci; devletlerin ulusal mülahazaları çerçevesinde verdikleri güç mücadelelerini, özel sektörün norm girişimciliği rolüyle kendi hareket alanını geliştirme çabalarını ve uluslararası örgütlerin kendi kurumsal prensipleri ve hedefleri doğrultusunda geliştirdiği söylemleri barındıran çok yönlü bir süreci ifade etmektedir.

KAYNAKÇA

H.R. 3718 (115th): International Communications Privacy Act, (2017) (testimony of 115th Congress). https://www.govtrack.us/congress/bills/115/hr3718

Abbate, J. (1999). *Inventing the Internet*. The MIT Press.

Abbate, J. (2017). What and where is the Internet? (Re)defining Internet histories. *Internet Histories*, *1*(1–2), 1–7.

Akyeşilmen, N. (2018). *Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik* (1st ed.). Orion Kitabevi.

Bakanlar Kurulu. (2012). *Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar*. Resmi Gazete. https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf

Barnes, S. (2018). *There are two types of companies: Those who know they've been hacked & those who don't*. Dynamic Business. https://dynamicbusiness.com.au/topics/technology/there-are-two-types-of-companies-those-who-know-theyve-been-hacked-those-who-dont.html

Bayır, Ö. E. (2013). Soğuk Savaş Sonrasında Güvenliğe Yönelik Teorik Tartışmalar. In H. Çomak & C. Sancaktar (Eds.), *Uluslararası İlişkilerde Teorik Tartışmalar* (1st ed., pp. 171–190). Beta Yayıncılık.

Bayrak, S. (2018). Cyber Governance Struggle Among Great Powers. *Cyberpolitik Journal*, *3*(5–6). http://cyberpolitikjournal.org/index.php/main/article/view/42

Belbin, R. (2019). When Google Becomes the Norm: The Case For Privacy and The Right To Be Forgotten. *Dalhousie Journal of Legal Studies*, *26*, 17–35. http://homepages.se.edu/cvonbergen/files/2019/06/When-Google-Becomes-the-Norm_The-Case-for-Privacy-and-the-Right-to-be-Forgotten.pdf

Bilgi Teknolojileri ve İletişim Kurumu. (2017). *Siber Güvenlik Kurulu*. BTK. https://www.btk.gov.tr/siber-guvenlik-kurulu

Bing, C. (2018). *Hoping to fill a global void, private companies push for "cyber norms."* Cyberscoop. https://www.cyberscoop.com/siemens-cybersecurity-charter-of-trust-airbus-dxp-cyber-norms/

Bischoff, P. (2021). *Which countries have the worst (and best) cybersecurity?* Comparitech. https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

Blount, P. J. (2019). *Reprogramming the World: Cyberspace and the Geography of Global Order*. E-International Relations Publishing. https://www.e-ir.info/publication/reprogramming-the-world-cyberspace-and-the-geography-of-global-order/

Broeders, D., & Cristiano, F. (2020). *Cyber Norms and the United Nations: Between Strategic Ambiguity and Rules of the Road*. ISPI. https://www.ispionline.it/it/pubblicazione/cyber-norms-and-united-nations-between-strategic-ambiguity-and-rules-road-25417

Brook, C. (2020). *What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More*. Digital Guardian. https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more#:~:text=Cyber hygiene is a reference,could be stolen or corrupted.

Brotman, S. N. (2015). *Multistakeholder Internet governance: A pathway completed, the road ahead*. https://www.brookings.edu/wp-content/uploads/2016/06/multistakeholder-1.pdf

Buzan, B. (1984). Peace, Power, and Security: Contending Concepts in the Study of International Relations. *Journal of Peace Research*, *21*(2), 109–125.

Canbek, G. (2018). Cyber Security by a New Analogy: "The Allegory of the 'Mobile' Cave." *Journal of Applied Security Research*, *13*(1), 63–88. https://doi.org/10.1080/19361610.2018.1387838

Cassidy, J. (2003). *Dot.con: How America Lost Its Mind and Money in the Internet Era*. HarperCollins.

China Copyright and Media. (2014). *Central Leading Group for Internet Security and Informatization Established*. https://chinacopyrightandmedia.wordpress.com/2014/03/01/central-leading-group-for-internet-security-and-informatization-established/

Choucri, N. (2012). *Cyberpolitics in International Relations*. The MIT Press.

Clark, B. (2016). Undersea cables and the future of submarine competition. *Bulletin of the Atomic Scientists*, *72*(4), 234–237. https://doi.org/10.1080/00963402.2016.1195636

Coşkun, B. B. (2014). Kopenhag Okulu ve Güvenlikleştirme: Değişen Güvenlik Ortamı, Zorluklar, Fırsatlar ve Meydan Okumalar. In T. Arı (Ed.), *Postmodern Uluslararası İlişkiler Teorileri -2: Uluslararası İlişkilerde Eleştirel Yaklaşımlar* (1st ed., pp. 179–202).

Council of Europe Centre of Expertise for Good Governance. (2019). 12 Principles of Good Democratic Governance. *Twelve Principles of Good Democratic Governance*. https://rm.coe.int/12-principles-brochure-final/1680741931

Dannatt, G. (2012). *How Cloud Computing Complicates the Jurisdiction of State Law*. E-IR. https://www.e-ir.info/pdf/26900

Darıcılı, A. B. (2017). *Siber Uzay ve Siber Güvenlik: ABD ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi* (1st ed.). Dora Yayıncılık.

Davis, S. (2019). *Nato In The Cyber Age: Strengthening Security & Defence, Stabilising Deterrence*. https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-10/REPORT 148 STC 19 E rev. 1 fin - NATO IN THE CYBER AGE.pdf

Editör. (2021). *About the Internet Governance Forum*. Internet Governance Forum. Retrieved February 28, 2021, from https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4099/481

Editör. (2011). *Vint Cerf — 'Father of the Internet.'* Stanford University. https://engineering.stanford.edu/about/heroes/2011-heroes/vint-cerf

Editör. (2016). *Bu kez oltalama saldırısı düzenlemek isteyenler oltaya geldi*. Siber Bülten. https://siberbulten.com/siber-guvenlik/bu-kez-oltalama-saldirisi-duzenlemek-isteyenler-oltaya-geldi/

Editör. (2020). *ABD'yi sarsan hacklemenin anatomisi: İşte SolarWinds saldırısının 8 maddelik özeti*. Siber Bülten. https://siberbulten.com/siber-saldirilar-2/abdyi-sarsan-hacklemenin-anatomisi-iste-solarwinds-saldirisinin-8-maddelik-ozeti/#1_SolarWinds_nedir

Editör. (2021). *Digital Around The World*. DataReportal. https://datareportal.com/global-digital-overview#:~:text=Roughly 4.66 billion people around,over the past twelve months.

Efegil, E. (2012). *Dış Politika Analizi: Ders Notları* (1st ed.). Nobel Akademik Yayıncılık.

Efegil, E., & Musaoğlu, N. (2009). Soğuk Savaş Sonrası Dönemin Uluslararası Sisteminin Yapısına İlişkin Görüşler Üzerine Bir Eleştiri. *Gazi Akademik Bakış*, *2*(4), 1–24. https://dergipark.org.tr/tr/download/article-file/73997

Eggenschwiler, J. (2018). *Geneva Dialogue on Responsible Behaviour in Cyberspace: Private Sector*. https://genevadialogue.ch/wp-content/uploads/Geneva-Dialogue-Role-of-the-Private-Sector.pdf

Eldem, T. (2020). The Governance of Turkey's Cyberspace: Between Cyber Security and

Information Security. *International Journal of Public Administration, 43*(5), 452–465.

Electronic Frontier Foundation. (2021). *In re Warrant for Microsoft Email Stored in Dublin, Ireland*. https://www.eff.org/cases/re-warrant-microsoft-email-stored-dublin-ireland

Espejo, R. (2014). Cybernetics of Governance: The Cybersyn Project 1971–1973. In G. S. Metcalf (Ed.), *Social Systems and Design* (pp. 71–90). Springer Japan. https://www.researchgate.net/publication/290742382_Cybernetics_of_Governance_The_Cybersyn_Project_1971-1973

European Commission. (2017). *Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service*. Europa. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_1785

European Commission. (2019). *Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising*. Europa. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770

European Parliament and of the Council. (2004). *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency*. Official Journal. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

Fairbank, N. A. (2019). The state of Microsoft?: the role of corporations in international norm creation. *Journal of Cyber Policy*, *4*(3), 380–403. https://www.tandfonline.com/doi/full/10.1080/23738871.2019.1696852

Fergana Agency. (2019, October 29). *Bişkek'te yüz tanıma özellikli 60 kamera kurulacak*. https://fergana.agency/news/112048/

Finkelstein, L. S. (1995). What Is Global Governance? *Global Governance, 1*(3), 367–372. https://doi.org/10.1163/19426720-001-03-90000007

Finnemore, M. (2017). *Cybersecurity and the Concept of Norms*. https://carnegieendowment.org/files/Finnemore_web_final.pdf

Finnemore, M., & Hollis, D. B. (2016). Constructing Norms for Global Cybersecurity. *American Journal of International Law, 110*(3). https://doi.org/https://doi.org/10.1017/S0002930000016894

Finnemore, M., & Sikkink, K. (1998). International Norm Dynamics and Political Change. *International Organization*, *52*(4). https://www.jstor.org/stable/2601361

GCSC. (2019). *GCSC Proposed Norms of Responsible Behavior in Cyber space*. https://cyberstability.org/norms/#toggle-id-3-closed

Gibson, W. (1984). *Neuromancer*. The ACE Publications.

GIP Digital Watch. (2021). *Industry cyber norms*. https://dig.watch/trends/cyber-norms#view-15373-4

Global Commission on the Stability of Cyberspace. (2018). *Definition of the Public Core, to Which the Norm Applies*. https://cyberstability.org/wp-content/uploads/2018/07/Definition-of-the-Public-Core-of-the-Internet.pdf

Google. (2021). *Digital Security & Due Process: Modernizing Cross-Border Government Access Standards for the Cloud Era*. https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/CrossBorderLawEnforcementRequestsWhitePaper_2.pdf

Google Güvenlik Merkezi. (2021). *Gizlilik ve Güvenlik İlkelerimiz*. Google. https://safety.google/principles/

Government of the Russian Federation, & Government the People's Republic of China. (2015). *On signing the Agreement between the Government of the Russian Federation and the*

Government of the People's Republic of China on cooperation in ensuring international information security. https://cyber-peace.org/wp-content/uploads/2013/05/RUS-CHN_CyberSecurityAgreement201504_InofficialTranslation.pdf

Gözen, R. (2015). İdealizm. In R. Gözen (Ed.), *Uluslararası İlişkiler Teorileri* (2nd ed., pp. 67–119).

Haksever, G. (2018). *İnternet ve çok-paydaşlı yönetişimi*. İstanbul Bilgi Üniversitesi.

Hama, H. H. (2017). State Security, Societal Security, and Human Security. *Jadavpur Journal of International Relations*, *21*(2). https://www.researchgate.net/publication/317710651_State_Security_Societal_Security_and_Human_Security

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*, 1155–1175. https://nissenbaum.tech.cornell.edu/papers/Digital Disaster.pdf

Horenbeeck, M. Van. (2018). Cybersecurity Culture, Norms and Values. *Internet Governance Forum: Best Practices Forum on Cybersecurity*. https://www.intgovforum.org/multilingual/filedepot_download/3405/1294

Ilona, S. (2018). Cybersecurity diplomacy: business and tech replacing the states? *ECPR General Conference*.

Industrial Cyber Security Club. (2018). *Event info*. https://club-bip.ru/en/events/mt-3#:~:text=The Charter for Information Security,of information and communication technologies.

International Telecommunication Union. (2018). *Guide to Developing a National Cybersecurity Strategy: Strategic Engagement in Cybersecurity*. http://handle.itu.int/11.1002/pub/811cf62d-en

International Telecommunication Union. (2021). *ITU Cybersecurity Activities*. https://www.itu.int/en/action/cybersecurity/Pages/default.aspx

Internet Governance: Why the Multistakeholder Approach Works. (2016). Internet Society. https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/

Internet Society. (2016). *Internet Governance – Why the Multistakeholder Approach Works*. https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/

Jackson, M., & Moore, T. (2016). Machiavelli's walls: The legacy of realism in international relations theory. *International Politics*, *53*(4), 447–463. https://www.researchgate.net/publication/304749985_Machiavelli's_walls_The_legacy_of_realism_in_international_relations_theory

Jang, J., McSparren, J., & Rashchupkina, Y. (2016). Global governance: Present and future. In *Palgrave Communications*. https://doi.org/10.1057/palcomms.2015.45

Karacasulu, N., & Uzgören, E. (2007). Explaining Social Constructivist Contributions to Security Studies. *Perceptions*, *12*, 27–48. http://sam.gov.tr/pdf/perceptions/Volume-XII/summer-autumn-2007/KaracasuluUzgoren.pdf

Katzenstein, P. J. (1996a). *The Culture of National Security: Norms and Identity in World Politics*. Columbia University Press.

Katzenstein, P. J. (1996b). *The Culture of National Security: Norms and Identity in World Politics*. Columbia University Press.

Kemp, S. (2018). *Digital 2018: Q4 Global Digital Statshot*. DataReportal. https://datareportal.com/reports/digital-2018-q4-global-digital-statshot

Kemp, S. (2019). *Digital 2019: Q4 Global Digital Statshot*. DataReportal. https://datareportal.com/reports/digital-2019-q4-global-digital-statshot

Kemp, S. (2020). *Digital 2020: October Global Statshot*. DataReportal. https://datareportal.com/reports/digital-2020-october-global-statshot

Kerry, J. (2015). *An Open and Secure Internet: We Must Have Both*. US Department of State. https://2009-2017.state.gov/secretary/remarks/2015/05/242553.htm

Kleinwächter, W. (2017). *Internet Governance Outlook 2017: Nationalistic Hierarchies vs. Multistakeholder Networks?* CircleID. https://www.circleid.com/posts/20160106_internet_outlook_2017_nationalistic_hierarchies_multistakeholder/

Knutsen, T. L. (2015). *Uluslararası İlişkiler Teorisi Tarihi* (2nd ed.). Açılım Kitap.

Kolomychenko, M. (2018). Russia tries more precise technology to block Telegram messenger. *Reuters*. https://www.reuters.com/article/us-russia-telegram/russia-tries-more-precise-technology-to-block-telegram-messenger-idUSKCN1LF1ZZ

Korab-Karpowicz, W. J. (2006). How International Relations Theorists Can Benefit by Reading Thucydides. *The Monist*, *89*(2), 232–244. https://www.jstor.org/stable/27903977%0A

Kubalkova, V., Onuf, N. G., & Kowert, P. (Eds.). (1998). *International Relations in a Constructed World*. Routledge.

Küçüksolak, Ö. K. (2018). Cyberspace: The Fifth Domain of Escalating Security Challenges. In *Current Debates in International Relations & Law Volume 24* (pp. 25–42). IJOPEC Publication. http://2018september.currentdebates.org/assets/vol24_cudes2018.pdf#page=26

Lambach, D. (2020). The Territorialization of Cyberspace. *International Studies Review*, *22*(3), 482–506.

LeLong, B. (2003). *Profits of Doom*. Wired. https://www.wired.com/2003/04/profits-of-doom-2/

Lessig, L. (1998). The Laws of Cyberspace. In *Readings in Cyberethics*. https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf

Lessig, L. (2006). *Code Version 2.0* (1st ed.). Basic Books. http://codev2.cc/download+remix/Lessig-Codev2.pdf

Lin, E. (2015). *China's safe cities serve as solutions and opportunities for growth*. Asmag. https://www.asmag.com/showpost/19628.aspx#:~:text=Safe Cities as a Solution,to as safe city projects.

Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (2015). *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press.

Llorente, R. V. (2018). *A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity*. LSE IDEAS Strategic Update. https://lseideas.medium.com/a-digital-geneva-convention-the-role-of-the-private-sector-in-cybersecurity-cd96ecd70622

Malatesta, E. (1974). *Anarchy*. Freedom Press.

Malcolm, J. (2008). *Multi-Stakeholder Governance And The Internet Governance Forum*.

Martinich, A. P. (1999). *Hobbes: A Biography*. Cambridge University Press.

Mbanaso, U. M., & Dandaura, E. S. (2015). The Cyberspace: Redefining A New World. *IOSR Journal of Computer Engineering*, *17*(3), 17–24. https://www.researchgate.net/profile/Uche_Mbanaso/publication/280101879_The_Cyberspace_Redefining_A_New_World/links/55a97a9508ae481aa7f9880f/The-Cyberspace-Redefining-A-New-World.pdf

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*.

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Microsoft. (2021). *International Cybersecurity Norms* (Microsoft Policy Papers).

Microsoft. (2021). *Five Principles for Shaping Cybersecurity Norms*. https://www.microsoft.com/en-us/cybersecurity/content-hub/five-principles-for-shaping-cybersecurity-norms

Morozov, E. (2014, October). The Planning Machine: Project Cybersyn and the origins of the Big Data nation. *The Newyorker*. https://www.newyorker.com/magazine/2014/10/13/planning-machine

Mueller, M., Mathiason, J., & Klein, H. (2007). The Internet and Global Governance: Principles and Norms for a New Regime. *Global Governance, 13*(2), 237–254. http://www.jstor.com/stable/27800656

NATO. (2020). *Statement by the North Atlantic Council concerning malicious cyber activities*. https://www.nato.int/cps/en/natohq/official_texts_176136.htm?selectedLocale=en

NATO. (2021a). *Collective defence - Article 5*. https://www.nato.int/cps/en/natohq/topics_110496.htm#:~:text=Article 5 provides that if,to assist the Ally attacked.

NATO. (2021b). *Cyber defence*. https://www.nato.int/cps/en/natohq/topics_78170.htm?

Naughton, J. (2016). The evolution of the Internet: from military experiment to General Purpose Technology. *Journal of Cyber Policy, 1*(1), 5–28.

Nornickel. (2018). *Osce to Support Nornickel's Initiatives In Global Cybersecurity*. https://www.nornickel.com/news-and-media/press-releases-and-news/osce-to-support-nornickel-s-initiatives-in-global-cybersecurity/

Nye, J. S. (2018). *Normative Restraints on Cyber Conflict* (Cyber Security Project).

Office of the Coordinator for Cyber Issues. (2021). *About Us – Office of the Coordinator for Cyber Issues*. US Department of State. https://www.state.gov/about-us-office-of-the-coordinator-for-cyber-issues/#:~:text=The Office of the Coordinator,human rights%2C and economic imperatives.

Office of the Coordinator For Cyber Issues. (2015). *Internet Governance*.

Onuf, N. G. (1989). *World of Our Making: Rules and Rule in Social Theory and International Relations*.

OSCE. (2021). *Democratic governance*. https://www.osce.org/odihr/democratic-governance

Reagle, J. M. (1998). *Why the Internet is Good: Community Governance That Works Well*. https://cyber.harvard.edu/archived_content/people/reagle/regulation-19990326.html

Rekabet Kurumu. (2019). *Bilgi Güvenliği Politikası*. https://www.rekabet.gov.tr/Dosya/geneldosya/1-bgp-pdf

Google 4054 Sayılı Rekabetin Korunması Hakkında Kanun'un 49. Maddesi Uyarınca Açıklanması, (2021) (testimony of Rekabet Kurumu). https://www.rekabet.gov.tr/Dosya/nihai-karar-aciklamalari-tefhim-duyurulari/google-yerel-arama-nihai-karar-20210414155035227-pdf

Rickleton, C. (2019). *Kazakhstan embraces facial recognition, civil society recoils*. Eurasianet. https://eurasianet.org/kazakhstan-embraces-facial-recognition-civil-society-recoils

Romaniuk, S. N., & Grice, F. (2018). *Norms, Norm Violations, and IR Theory*. E-International Relations. https://www.e-ir.info/2018/11/15/norms-norm-violations-and-ir-theory/#:~:text=A combination of social norms,action undertaken by a state.&text=One norm in international politics,'uncivilized' society or state.

Ruowei, L. (2019a). *华为和中信国安投资超10亿美元发展乌兹别克斯坦数字基础设施 (Çev. Huawei ve CITIC Guoan, Özbekistan'ın dijital altyapısını geliştirmek için 1 milyar ABD dolarının üzerinde yatırım yaptı.*) Sliuxgc. http://web.siluxgc.com/UZ/20190426/16656.html

Ruowei, L. (2019b). *"道路千万条 安全第一条" 中亚各国"安全城市"项目来了！(Çev. Orta Asya ülkelerinde "Güvenli Şehirler" projesi burada!)*. WeChat. https://mp.weixin.qq.com/s/z3l_UHX40W8OIJi61HaomA

Schia, N. N., & Gjesvik, L. (2017). *China's cyber sovereignty*. http://www.jstor.com/stable/resrep07952

Segal, A. (2020). *Peering into the Future of Sino-Russian Cyber Security Cooperation*. War on the Rocks. https://warontherocks.com/2020/08/peering-into-the-future-of-sino-russian-cyber-security-cooperation/

Shen, Y. (2016). Cyber Sovereignty and the Governance of Global Cyberspace. *Chinese Political Science Review, 1*, 81–93. https://link.springer.com/article/10.1007/s41111-016-0002-6

Siemens AG. (2020a). *Charter of Trust partners decide on further measures for more cybersecurity*. https://press.siemens.com/global/en/pressrelease/charter-trust-partners-decide-further-measures-more-cybersecurity

Siemens AG. (2020b). *The Charter of Trust takes a major step forward to advance cybersecurity*. Siemens. https://press.siemens.com/global/en/feature/charter-trust-takes-major-step-forward-advance-cybersecurity

Smith, B. (2020). *A moment of reckoning: the need for a strong and global cybersecurity response*. Microsoft. https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/

Stifel, M. (2017). *Maintaining U.S. Leadership on Internet Governance*. Council on Foreign Relations. https://www.cfr.org/report/maintaining-us-leadership-internet-governance

Stone, A. (1994). What Is a Supranational Constitution? An Essay in International Relations Theory. *The Review of Politics, 56*(3), 441–474.

T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı. (2020). *SİSAMER: TSK Siber Savunma Merkezi Projesi*. https://www.ssb.gov.tr/Website/contentList.aspx?PageID=1083&LangID=1

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2013). *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*. https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf. Erişim Tarihi: 1 Haziran 2021.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2016). *2016-2019 Ulusal Siber Güvenlik Stratejisi*. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf. Erişim Tarihi: 1 Haziran 2021.

TC. Ulaştırma ve Altyapı Bakanlığı. (2020). *2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı*. https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf. Erişim Tarihi: 1 Haziran 2021.

Tabak, H. (2014). Normlar ve Uluslararası İlişkiler: Türkçe Yazın için Geç Kalınmış bir Araştırma Gündemi. In İ. Demir (Ed.), *Türkiye'nin Dış Politikası* (pp. 19–46). Dora Yayınları.

Tabak, H. (2017). Normlar, Uluslararası İlişkiler ve Dış Politika. In E. Efegil (Ed.), *Sosyolojik Unsurların Dış Politikaya Etkisi* (pp. 139–175). Güdoğan Yayınları. https://www.researchgate.net/publication/322952460_Normlar_Uluslararasi_Iliskiler_ve_Dis_Politika

Taureck, R. (2006). Securitization theory and securitization studies. *Journal of International Relations and Development, 9*, 53–61.

https://doi.org/https://doi.org/10.1057/palgrave.jird.1800072

The Bell. (2019). *Russia is struggling to implement the nationwide DPI system it needs for 'Internet isolation.'* Meduza. https://meduza.io/en/news/2019/11/01/russia-is-struggling-to-implement-the-nationwide-dpi-system-it-needs-for-internet-isolation

The Editors of Encyclopaedia Britannica. (2014). *Cybernetics*. Encyclopedia Britannica. https://www.britannica.com/science/cybernetics

The Global Commission on the Stability of Cyberspace. (2019). *Advancing CyberStability*. https://cyberstability.org/report/#2-what-is-meant-by-the-stability-of-cyberspace

The World Bank. (1992). *Governance and Development*.

Theys, S. (2018). *Introducing Constructivism in International Relations Theory*. E-International Relations. https://www.e-ir.info/pdf/72842

Thukydides. (2010). *Peloponnesos Savaşları* (1st ed.). Belge Yayınları.

Tosbotn, R. A. (2016). *NATO and Cyber Security: Critical Junctures as Catalysts for Change* [Universiteit Leiden]. https://studenttheses.universiteitleiden.nl/handle/1887/42987

Tsydenova, N., & Balmforth, T. (2019, October 8). Russia and China to sign treaty on combating illegal online content. *Reuters*. https://www.reuters.com/article/us-russia-china-internet-idUSKBN1WN1E7

Public Printing and Documents, Pub. L. No. 116 Stat. 2947 (2002). https://www.govinfo.gov/app/details/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapIII-sec3542/summary

U.S. Senate. (2015). *Preserving the Multistakeholder Model of Internet Governance*. U.S. Government Publishing Office. https://www.govinfo.gov/content/pkg/CHRG-114shrg98129/html/CHRG-114shrg98129.htm

UCENet. (2021). *Engage International Spam Enforcement Cooperation*. UCENet. https://www.ucenet.org/

Resolution Adopted by the General Assembly on the report of the First Committee, (1998) (testimony of United Nations General Assembly). https://undocs.org/A/RES/53/70

United Nations General Assembly. (2013). *2012/2013 GGE: General Assembly Consensus report (A/68/98)*. https://undocs.org/A/68/98

United Nations General Assembly. (2015). *70/237 Resolution adopted by the General Assembly on 23 December 2015*. United Nations. https://undocs.org/A/RES/70/237

United Nations Office For Disarmament Affairs. (2019). *Cyberdiplomacy Course Module 2: Existing and Emerging Threats*. UNODA. https://www.disarmamenteducation.org/dashboard/scorm_frame.php?user_id=9008&course_id=20&session_id=118&module_id=351

Usta, O. (2020). *ABD'de SolarWinds fırtınası dinmiyor: Nükleer silahlar da siber saldırının hedefinde*. Siber Bülten. https://siberbulten.com/siber-saldirilar-2/abdde-solarwinds-firtinasi-dinmiyor-nukleer-silahlar-da-siber-saldirinin-hedefinde/

Van Der Meer, S. (2015). Enhancing International Cyber Security: A Key Role for Diplomacy. *Security and Human Rights*, *26*, 193–205. https://www.researchgate.net/publication/312066061_Enhancing_International_Cyber_Security_A_Key_Role_for_Diplomacy

Walker, K. (2017). *Digital security and due process: A new legal framework for the cloud era*. Google. https://www.blog.google/outreach-initiatives/public-policy/digital-security-and-due-process-new-legal-framework-cloud-era/

Wallerstein, I. (1993). The World-System after the Cold War. *Journal of Peace Research*.

https://doi.org/10.1177/0022343393030001001

Weber, V. (2020). *The Sinicization of Russia's Cyber Sovereignty Model*. Council on Foreign Relations. https://www.cfr.org/blog/sinicization-russias-cyber-sovereignty-model

Welch, L. D. (2011). *Cyberspace – The Fifth Operational Domain*. IDA. https://www.ida.org/~/media/Corporate/Files/Publications/ResearchNotes/RN2011/2011 Cyberspace - The Fifth Operational Domain.pdf

Wendt, A. (1992). Anarchy is what States Make of it: The Social Construction of Power Politics. *International Organization*, *46*(2), 391–425.

Wendt, A. (2016). *Uluslararası Siyasetin Sosyal Teorisi* (B. Özel (Ed.)). Küre Yayınları.

WGIG. (2005). *Report of the Working Group on Internet Governance*. https://www.wgig.org/docs/WGIGREPORT.pdf

Willke, H., & Willke, G. (2012). Political Governance of Capitalism. In *Political Governance of Capitalism*. Edward Elgar. https://doi.org/10.4337/9781781006191

WSIS. (2003). *Declaration of Principles* (WSIS-03/GENEVA/DOC/4-E). https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf

WSIS. (2005). *Tunis Commitment* (WSIS-05/TUNIS/DOC/7-E). https://www.itu.int/net/wsis/docs2/tunis/off/7.html

WSIS. (2006). *Basic Information: About WSIS*. https://www.itu.int/net/wsis/basic/about.html

Yeli, H. (2017). A Three-Perspective Theory of Cyber Sovereignty. *PRISM*, *7*(2), 108–115. https://cco.ndu.edu/Portals/96/Documents/prism/prism_7-2/10-3-Perspective Theory.pdf?ver=2017-12-21-110647-937

https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/ Erişim Tarihi: 3 Şubat 2021

https://www.dfat.gov.au/sites/default/files/un-norms-responsible-bookmark.pdf. Erişim tarihi: 31 Ocak 2021.

https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770 Erişim Tarihi: 6 Mayıs 2021

https://www.historyofinformation.com/detail.php?entryid=2860 Erişim Tarihi: 7 Nisan 2021

https://www.ida.org/~/media/Corporate/Files/Publications/ResearchNotes/RN2011/2011. Erişim tarihi: 21 Aralık 2020.

https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the multistakeholder-approach-works/. Erişim tarihi: 14 Şubat 2021.

https://www.nato.int/cps/en/natohq/topics_78170.htm?. Erişim Tarihi: 13 Mayıs 2021

ÖZGEÇMİŞ

Tuba FIRAT, ilk ve orta öğrenimini Kirazlı İlköğretim Okulu'nda tamamladıktan sonra lise eğitimini Barbaros Anadolu Lisesi'nde tamamlamıştır.

Yalova Üniversitesi Uluslararası İlişkiler (%100 İngilizce) Bölümünde lisans eğitimine 2013 yılında başlayan Fırat, 2018 yılında bölümden onur öğrencisi olarak mezun olmuştur. Aynı yıl Yalova Üniversitesi'nde Sosyal Bilimler Enstitüsü'nde yüksek lisans eğitimine başlayan Fırat, 2019/2020 eğitim-öğretim yılı bahar dönemini Erasmus+ Programı kapsamında Polonya'nın Olsztyn şehrinde bulunan 'Uniwersytet Warmińsko-Mazurski w Olsztynie'de tamamlamıştır.

Siber Bülten'in yazarları arasında yer alan Fırat, 2021 yılında Dr. Öğretim Üyesi Övgü KALKAN KÜÇÜKSOLAK danışmanlığında 'Stratejik Bir Belirsizlik Alanı Olan Siber Uzayda Norm Oluşturma Çabalarının İncelenmesi' başlıklı tez çalışmasını tamamlamıştır.