ISSN: 2587-1218

CYBERPOLITIKJOURNAL
Siber Politikalar Dergisi

A Peer Review International E-Journal on Cyberpolitics, Cybersecurity and Human Rights
Volume 1, Number 1 Winter 2016

Research Articles / Araştırma Makaleleri

Gözetim Kavramının Tarihsel Gelişimi ve Elektronik Gözetim - Özgün ÖZGER
Cybersecurity and Human Rights : Need for a Paradigm Shift? - Nezir AKYEŞİLMEN
Siber Güvenlik ve İlintili Kavramsal Çerçeve - İbrahim KURNAZ
Siber Güvenlik ve Uluslararası Güvenlik İlişkisi - Cihan DABAN
Ulusal Güvenlik Çerçevesinde Siber Güvenlik Yaklaşımı Oluşturma Sorunu - Vahit GÜNTAY
Risk Toplumu ve Refleksif Modernleşme Çerçevesinde Siber Terörizm: Tanımlama ve Tipoloji Sorunu - Mehmet Emin ERENDOR
Politik İdealizm ve Siber Uzay ile Dönüşen Uluslararası İlişkiler - Fatma ÇAKIR
Uluslararası İlişkilerde Siber Caydırıcılık - Sevda KORHAN

Opininons / Yorumlar

Siber Çağda ABD Seçimleri ve Siber Bir Mit Olarak Trump - Bilal SAMBUR
Siber Dünyada Demokrasinin Dönüşüm İmkanları: Yasama Meclisi Örneği - Davut ATEŞ

Reviews / İncelemeler

Cyberpolitics in International Relations - Bilal SAMBUR
Cybersecurity and International Relations: The U.S. Engagement with China and Russia -Durukan AYAN

ISSN: 2587-1218

CYBERPOLITIKJOURNAL
Siber Politikalar Dergisi

A Peer Review International E-Journal on Cyberpolitics, Cybersecurity and Human Rights

2

www.cyberpolitikjournal.org

Winter 2016

ISSN: 2587-1218

ABOUT THE JOURNAL

Owner/Sahibi

İnsan Hakları Eğitimi Derneği adına

Assoc.Prof. Dr. /Doç.Dr. Nezir Akyeşilmen

Peer Review

All articles in this journal have undergone meticulos peer review, based on refereeing by anonymous referees. All peer review is double blind and submission is online. All submitted papers (other than book and article reviews) are peer reviewed.

The Journal

Cyberpolitik the journal aims to promote a better understanding of the relationship between cyberspace and politics. While the focus is on cyberpolitics, the journal also builds on the other issues related to society and cyber domain and their analysis.

The languages of the Journal are both Turkish and English.

ISSN …….

Cyberpolitik (CP) aims to publish peer-reviewed scholarly articles and reviews as well as significant developments regarding cyber world, cybersecurity, cyberpolitics and human rights.

Cyberpolitik consists of the following sections:

Research Articles: Each Volume would publish a selection of Articles covering aspects of cyber politics and human rights with a broad universal focus.

Comments: This section would cover recent developments in the field of cyber politics and human rights.

Book/Article Reviews: Each Volume aims to review books on cyber politics, cybersecurity and human rights.

Cyberpolitik Award: Each year one '*Cyberpolitik*' prize will be awarded, for the best article from material published in the previous year.

ISSN: 2587-1218

CONTENTS / İÇİNDEKİLER

EDITORIAL 7

RESEARCH ARTICLES / ARAŞTIRMA MAKALELERİ 10

Özgün ÖZGER

GÖZETİM KAVRAMININ TARİHSEL GELİŞİMİ VE ELEKTRONİK GÖZETİM 11

Nezir AKYEŞİLMEN

CYBERSECURITY AND HUMAN RIGHTS: NEED FOR A PARADIGM SHIFT? 38

İbrahim KURNAZ

SİBER GÜVENLİK VE İLİNTİLİ KAVRAMSAL ÇERÇEVE 62

Cihan DABAN

SİBER GÜVENLİK VE ULUSLARARASI GÜVENLİK İLİŞKİSİ 84

Vahit GÜNTAY

ULUSAL GÜVENLİK ÇERÇEVESİNDE SİBER GÜVENLİK YAKLAŞIMI OLUŞTURMA SORUNU 101

Mehmet Emin ERENDOR

RİSK TOPLUMU VE REFLEKSİF MODERNLEŞME ÇERÇEVESİNDE SİBER TERÖRİZM: TANIMLAMA VE TİPOLOJİ SORUNU 120

Fatma ÇAKIR

POLİTİK İDEALİZM VE SİBER UZAY İLE DÖNÜŞEN ULUSLARARASI İLİŞKİLER 140

Sevda KORHAN

ULUSLARARASI İLİŞKİLERDE SİBER CAYDIRICILIK 153

OPINIONS / YORUMLAR 168

Bilal SAMBUR

SİBER ÇAĞDA ABD SEÇİMLERİ VE SİBER BİR MİT OLARAK TRUMP 169

Davut ATEŞ

SİBER DÜNYADA DEMOKRASİNİN DÖNÜŞÜM İMKANLARI: YASAMA ÖRNEĞİ 176

ARTICLE AND BOOK REVIEWS / MAKALE VE KİTAP İNCELEMELERİ 184

Bilal SAMBUR

BY NAZLI CHOUCRI, CYBERPOLITICS IN INTERNATIONAL RELATIONS 185

Durukan AYAN

BY NIR KSHERTI, CYBERSECURITY AND INTERNATIONAL RELATIONS: THE U.S. ENGAGEMENT WITH CHINA AND RUSSIA 188

For Authors / Yazarlar İçin 192

ISSN: 2587-1218

EDITORIAL

Dear Readers,

The periodical *Cyberpolitik* Journal - A Peer Review International E-Journal on Cyberpolitics, Cybersecurity and Human Rights - which we started working on in 2016, is proud to present its first issue. Due to the fact that it is the first academic journal study in cyberpolitics and cyber security in Turkey, we have realized the main mission of our journal is to contribute to the literature of this important field which is in its infancy stage in the international relations literature of Turkey.

The dynamic nature of international relations necessitates constant evolving and changing relationships which has been transformed with technological developments into different dimensions that have added new issues to the literature, including new concepts. The Internet, which is the last phase of the optical science that is speeding through the contributions of Ibn al-Haytham, is at the forefront of these new issues. Especially since 2000, technological developments have spread faster with the internet. States and other organizations have come to recognize the power of the internet, its potential opportunities and vulnerabilities, causing a new era in international relations. The new era of cyber power has also required the development of new frameworks and security strategies that take into consideration cyber space alongside with more conventional dimensions e.g. land, sea and air. Cyber security has gained greater attention and prioritization by governments and international organizations following cyber attacks, such as the denial-of-services attacks in Estonia 2007 and the industrial sabatoge such as Stuxnet in Iran in 2010. States have begun to form cyber security policies on one side, while on the other side has also aimed to reduce the cost of war by setting up cyber army. The cyber attacks or the cyber force that has taken an important place in itself in the case of the Hybrid War, which Russia implemented in the Crimea, is a phenomenon that the international community has encountered in recent years and may face more and more in the future. This new domain of international relations requires the identification of new ideas and security policies.

The goal of the *Cyberpolitik* Journal is to contribute to the discipline of international relations both nationally and internationally, by analyzing the technological developments, the state's political and security policies, its legal systems and more importantly its democratic

structures. From this point of view, the main purpose of the *Cyberpolitik* Journal is to contribute to a better understanding of the relationship between cyberspace and international relations. Although *Cyberpolitik* Journal focuses on cyber policy, other important issues such as society, security, peace, international relations, international law and human rights will also be critically analyzed in the journal.

As we have set out on this journey, seeking to contribute to the academic life and international relations literature, there have been a number of people who have made the realization of this journal possible. We would like to extend a debt of gratitude to all of our valued colleagues in the advisory and editorial board, authors, who have supplied us with their invaluable articles for the first issue, and those involved in the refereeing process.

Cyberpolitik Journal Editors Board

*****

EDİTÖRDEN

Değerli Okuyucu,

2016 yılı itibariyle çalışmalarına başladığımız *Cyberpolitik Journal,* başka bir ifade ile *Siber Politikalar Dergisi (A Peer Review International E-Journal on Cyberpolitics and CyberSecurity)* ilk sayısını yayınlamış bulunmaktadır. Türkiye'de siber güvenlik ve siber uzay alanında ilk akademik Dergi çalışması olması nedeniyle, Türkiye'nin uluslararası ilişkiler literatüründe eksik olan önemli bir alana katkıda bulunularak dergimizin ana misyonunu gerçekleştirmiş bulunuyoruz.

Uluslararası ilişkilerin dinamik doğası gereği sürekli olarak gelişen ve değişen ilişkiler, teknolojik gelişmelerle farklı boyutlara taşınmış ve literatüre yeni kavramlar dahil olmak üzere yeni konular eklemiştir. İbn-i Heysem'in katkılarıyla hız kazanan optik biliminin geldiği son safhayı teşkil eden internet bu yeni konuların başında gelmektedir. Özellikle de 2000'li yıllardan itibaren teknolojik gelişmelerin internet ile beraber daha hızlı yayılması, internetin gücünün devletler ve diğer örgütler tarafından keşfedilmesine ve buradan hareketle de bu gelişmelerin karşı devlete ya da düşmana karşı kullanılmaya başlanması, uluslararası ilişkilerde yeni dönemin başlamasına neden olmuştur. Siber güç olarak adlandırabileceğimiz

bu yeni dönemde, internetin ve teknolojik gelişmelerin farklı amaçlar çerçevesinde kullanılabilirliğinin keşfedilmesi ile birlikte güvenlik olgusu da değişmeye başlamış, devletlerin artık kara, deniz ve hava güçleri gibi temel argümanlarının yanına siber güç olgusu da eklenmiştir. 2007 Estonya siber saldırıları ile uluslararası alanda hem devletler hem de uluslararası örgütler bağlamında daha fazla endişe yaratan bu yeni olgu, devletlerin ve uluslararası örgütlerin siber güvenlik politikalarına daha fazla ağırlık vermelerine neden olmuştur. 2010 yılında İran'a karşı gerçekleştirilen Stuxnet saldırısı ile beraber siber güvenliğin devletler için ne kadar önemli olduğu bir defa daha ortaya çıkmış ve devletler bir yandan siber güvenlik politikaları oluşturmaya başlarken, diğer taraftan da siber ordular kurarak savaş maliyetlerini daha da aşağıya çekmeyi hedeflemiştir. Rusya'nın Kırım'da uygulamış olduğu Karma (*Hybrid*) Savaş olgusu içerisinde de kendisine önemli bir yer edinen siber saldırılar ya da siber güç, uluslararası toplumun son yıllarda karşılaştığı ve ileride de daha fazla karşı karşıya kalabileceği bir olgu olması nedeniyle hem araştırılması gereken hem de bu alanda yeni fikirlerin ve güvenlik politikalarının ortaya çıkarılması gereken bir alandır.

Cyberpolitik Journal olarak amacımız teknolojik gelişmelerin, devletlerin hem siyasi hem de güvenlik politikalarına, hukuksal sistemlerine ve daha da önemlisi demokratik yapılarına olan etkisini inceleyerek Uluslararası İlişkiler disiplinine hem ulusal hem de uluslararası alanda katkıda bulunmaktır. Bu noktadan hareketle, *Cyberpolitik Journal*'ın ana amacı siber uzay ile uluslararası ilişkiler ve uluslararası politika arasındaki ilişkiyi daha iyi anlamaya katkıda bulunmaktır. *Cyberpolitik Journal*'ın odak noktası her ne kadar siber politika olsa da, dergi içerisinde toplum, güvenlik, barış, uluslararası ilişkiler, uluslararası hukuk ve insan hakları gibi diğer önemli konular da eleştirel bir biçimde analiz edilecektir.

Akademik hayata ve uluslararası ilişkiler literatürüne katkı sağlamak üzere yola çıktığımız bu yolculukta, Derginin kurulum aşamasında emeği geçen herkese, bizleri kırmayarak desteklerini esirgemeyen danışma ve yayın kurulundaki değerli hocalarımıza teşekkürü bir borç biliriz. Ayrıca ilk sayımız münasebetiyle bizlere kıymetli yazılarını gönderen kıymetli yazarlarımıza ve bu makalelerin hakem süreçlerinde emeği geçen hocalarımıza teşekkür ederiz.

Cyberpolitik Journal Editörler Kurulu

ISSN: 2587-1218

RESEARCH ARTICLES / ARAŞTIRMA MAKALELERİ

ISSN: 2587-1218

GÖZETİM KAVRAMININ TARİHSEL GELİŞİMİ VE ELEKTRONİK GÖZETİM

Özgün ÖZGER*

Özet

Gözetim insanlık tarihi kadar eskiye dayanmaktadır. İlkçağlardan itibaren, iktidarlar ve egemenlik ilişkileri açısından gözetim pratikleri, insan yaşamının her alanına etki eden bir özelliğe sahip olagelmiştir. Enformasyon çağı olarak adlandırılan günümüzde ise, gözetim pratikleri hiçbir dönemde sahip olmadığı önemi kazanmıştır. Tümüyle yüksek teknolojinin imkanlarına dayalı bir karakteristiğe bürünen gözetim, artık sadece toplumsal denetimi sağlamakla yetinmemiştir. Dijital teknolojilerin kişisel veri işleme kapasiteleriyle birlikte kişiler, dijital kodun birer parçası haline gelmeye başlamıştır. Bu çalışmada gözetim kavramı ve gözetimin tarihsel arka planı incelenmiştir. Çağın gözetleme sistemi olan elektronik gözetim, gözetleme araçlarına da yer verilerek ele alınmıştır.

Anahtar Kelimeler: Gözetim, Gözetim Tarihi, Elektronik Gözetim, Elektronik Gözetim Araçları.

ELECTRONIC SURVEILLANCE AND HISTORICAL DEVELOPMENT OF SURVEILLANCE CONCEPT

Abstract

Surveillance is as old as human history. Since ancient times, the practice of surveillance in terms of governments and sovereignty has become a feature affecting every aspect of human life. In today's world-termed as information era, surveillance practices have gained importance which has never had before. Surveillance, which is based on the means of purely high technology, has no longer been satisfied with just providing social control. With the personal data processing capacities of digital technology, individuals are beginning to become part of the digital code. In this study, the concept of surveillance and the historical background of surveillance have been examined. Electronic surveillance, which is a surveillance system of this age, has also been taken into consideration, including surveillance instruments.

Key Words: Surveillance, Surveillance Date, Electronic Surveillance, Electronic Surveillance Vehicles.

Giriş

Bu çalışmada, gözetlemeyi incelemenin temel nedeni günümüz toplumunda önemli bir yere sahip olmasıdır. İnsanlık tarihi kadar eski bir kavram olan gözetimin resmi olarak yazının bulunuşuyla birlikte başladığı söylenebilir. Yazı, modern olmayan devletlerin gözetleme

* Doktora Adayı, Selçuk Üniversitesi, Uluslararası İlişkiler Bölümü. ozgunozger@hotmail.com adresinden ulaşılabilir.

faaliyetleri açısından birçok anlam taşımaktadır. Yazı, devlet aygıtını hem nesneler hem de kişiler üzerinde uyguladığı idari denetimin kapsamını genişletmek üzere kullanılabilecek bir şifreleme bilgisi sağlamaktadır. Hem devletin kayıtları için gerekli bilgiler hem de bireylerin özel alanlarıyla ilgili malumat, yazı kanalıyla toplanmaktadır (Giddens, 2008, s. 66). Ancak bu dönemdeki söz konusu gözetim, sadece kısıtlı faaliyetlerden ibarettir. Askerlik hizmetini düzene koyma, vergileri düzgün olarak toplama amaçları dışında etkin bir gözetimin varlığından söz etmek mümkün değildir.

Matbaanın keşfiyle birlikte, gözetimde yeni bir aşamaya geçilmiştir. İletişimin mekanizasyonundaki ilk önemli adım olan matbaa; belge ve metinleri geniş çapta ulaşılabilir kılmıştır. Matbaa, devletin gözetim operasyonlarında çok büyük bir ilerleme sağlamıştır. Matbaayla birlikte devlet gözetimi, özellikle kurumlar üzerinde baskı unsuru haline gelmiştir (Giddens, 2008, s. 66).

Sosyal hayatın kurumsallaşmış bir şekilde yaygın olarak gözetimi, modernizm ile birlikte ortaya çıkmıştır. Modern toplumu oluşturan; sınai kapitalizm, sanayi kentlerinin artışı ve yoğunlaşma hızı, ulus-devletin iç ve dış tehlikelere karşı korunma güdüsü, askeri örgütlenmeler, devlet idaresi, bürokratik yapılanma ve kapitalist işletme sayısındaki artışlar gibi bileşenler, gözetlemenin hızla yayılmasına imkan tanımıştır (Dolgun, 2005, s. 61). Ancak içinde bulunduğumuz dünyada gözetim, çok daha akıl almaz bir hal almıştır. Bu, gündelik hayatın neredeyse sürekli gözetim altında olduğu bir dünyadır. İnsanlar gün doğumundan batımına kadar olası her yerde bilgisayar destekli ve ağ tabanlı teknolojilerin kuşatması altındadır. Tüm çevremiz insanların nerede olduğunun, ne yaptığının, nereye gittiğinin bilinmesini sağlayan kablolu ve kablosuz bağlantılarla kuşatılmış durumdadır (Lyon, 2013, s. 11). Belli bir amaca hizmet eden bir izleme, etiketleme, dinleme, seyretme, kaydetme ya da kimlik belirleme aracına yakalanmadan, güvenli bir ortam ya da yapacak bir uğraş bulmak giderek güçleşmektedir (Lyon, 2006, s. 11).

Gözetimin sıradan insanların hayatına girmesine neden olan etken, yeni enformasyon teknolojilerinin artan kullanım oranı ve amacıdır. Günümüzde gözetleme, küreselleşmenin bir sonucu olarak artık sınırların çok ötesine geçmiştir. Gözetimin bu sınırları aşan şekliyle birlikte bireylerin günlük hayatları elektronik izlerinin kontrol altında tutulmasına olanak sağlayan kimlik kontrollerinden, gözetleme kameralarına, vücut kontrollerine, parmak izi ve veri tabanlarına, internet izleme programlarına, kredi kartı kullanımıyla yer tespitinin

yapılabildiği ve cep telefonlarının dinlenebildiği bir dünyaya doğru evrilmiş ve evrilmeye devam etmektedir.

Kişisel bilgilerin her gün binlerce kuruluş ve onlarca devlet tarafından toplanarak mahremiyetin ya da özel alanın yok edilme durumuyla karşı karşıya bulunulması, gözetim araçlarının, hızla artmasına engel olamamıştır. Çünkü gözetlemenin tebaasına sunduğu avantajlar, itaatten rahatsızlık duyulmamasını sağlamıştır. Telefonun veya kredi kartının sunduğu kolaylık bizim aramalarımızın ve işlemlerimizin takip edilebilir olduğu ve başkalarının bu verileri kullanarak kar sağladığı gerçeği üzerine tekrar tekrar düşünmemizi sağlar. Yol kazalarını azaltılması amacıyla bir kavşakta kamera kurulmuş olduğu gerçeği yeteri kadar akla uygun gelmektedir (Lyon, 2006, s. 15). Bu akla uygunluğun asıl sebebi teknoloji ve toplum arasındaki ilişkidir. Bireyler, tekno-ütopyacı söylemlerin etkisinde kaldıklarında, gözetim teknolojileri de dahil olmak üzere bütün teknolojileri devrimci bir nitelikte görmektedirler. Robins'in de belirttiği gibi, bireyler, bu teknolojik gelişmelerle birlikte ayaklarının yerden kesileceği ve her şeye güçlerinin yeteceği duygusunu taşımaktadırlar (Robins, 1999, s. 73).

Gözetim Kavramı

Literatürde kullanılan kavramsal anlamından önce sözcük anlamına bakmanın fayda sağlayacağı göz önünde tutularak; Türk Dil Kurumu Büyük Türkçe Sözlüğü'ne göre, Gözetim "1.Gözetme işi, nezaret; 2.Himaye; 3.Gözaltı" şeklinde tanımlanmaktadır (TDK, Büyük Türkçe Sözlük). Ceza Yargılama Yöntemi Yasası Terimleri Sözlüğü'nde Gözetim; "Küçüklerin, ana babalarınca korunması ve idarenin her türlü eylem ve işleminin de yargının denetimi altında olması durumu" olarak karşılık bulmaktadır (Erdoğdu, 1972, s.72). Medeni Hukuk Terimleri Sözlüğü'ne göre; "Nezaret makamı" şeklinde tanımlanırken (Sungurbey, 1966), Sinema ve Televizyon Terimleri Sözlüğünde ise; "Mesleğe yeni başlayan, yapımcının tam güvenini taşımayan ya da çok büyük bir yapıma girişen bir yönetmenin çalışmalarının güvenilir bir kimsece denetlenmesi" anlamını taşımaktadır (Özön, 1981). Son olarak, Yöntembilim Terimleri Sözlüğü'nde; "Bir çalışma ya da uygulama sürecini etkinlik ve amaca uygunluk bakımından yakından denetleme" şeklinde karşılık bulmaktadır (Sencer, 1981, s. 74.)

Literatürde ise, "Gözetim" kavramı ilk kez Jeremy Bentham'ın, 1791 yılında, Londra'da basılan, aynı sene Fransız Devrimci Millet Meclisi tarafından hızlı bir şekilde Paris'te yayımlanan *Panoptikon* adlı kitabında karşımıza çıkmaktadır. Bentham gözetimi, "bugüne

kadar örneği olmayan, zihin üzerinde zihinsel iktidar elde eden yeni bir yöntem" olarak tanımlamaktadır (Bentham, 1995, ss. 11-12).

Her ne kadar 'gözetim' sözcüğü genellikle bireysel faaliyetlerin casuslukla, gizli soruşturmalarla takip edilmesini akla getiriyorsa da, aynı zamanda rutin, gündelik, faaliyetlere işaret eden dolaysız çağrışımları da içerir. Fransızcada 'bakarak olmak' anlamına gelen *surveiller* fiilinden türetilen gözetim, boş merakın çok ötesinde, belli insan davranışlarının dikkate alındığı süreçlere işaret eder (Lyon, 2013, s. 30).

Anthony Giddens 'gözetimin' birbiriyle ilişkili iki tür olguya tekabül ettiğine işaret eder. Bunlardan ilki, hakkında toplandığı bireylerin eylemlerini yönetmek üzere kullanılabilen "şifrelenmiş bilgi" birikimini oluştururken; diğeri ise, bazı bireylerin eylemlerinin, bunlar üzerinde otorite kuran diğer bazı bireyler tarafından doğrudan izlenmesini içerir (Giddens, s.24-25) . Bunlardan ilki "depolayarak gözetim", ikincisi ise "izleyerek gözetim" şeklinde isimlendirilebilir. Çalışma konumuz olan elektronik gözetim, gerek depolayarak gözetimi, gerekse de izleyerek gözetimi içinde barındırdığından, her iki gözetime de çalışma boyunca sıklıkla rastlanılacaktır.

"Gözetim" kavramına literatürde sağladığı ciddi katkılarla öne çıkan David Lyon, temel sav olarak ilk solukta, gözetimin etkileme, yönetme, koruma, yönlendirme gibi amaçlarla kişisel enformasyona dönük odaklı, sistemli ve düzenli ilgi olduğunu öne sürer (Lyon, 2013, s.31). Gözetim, dikkatini en nihayetinde bireylere verir, bireylere odaklanır. Sistemli bir şekilde kişisel enformasyonlara yoğunlaşan bu odağın tesadüfi, ender görülür ya da kendiliğinden olmadığının altını çizen Lyon'a göre gözetim; kasıtlıdır ve belli protokollere ve tekniklere dayanır (Lyon, 2013, s.31). Artık rutin, olağan gözetleme, hayatın her alanında yer almaktadır ve bu durum, onu bürokratik yönetime ve belli enformasyon teknolojilerine bağlı olan bütün toplumlarda gündelik hayatın olağan bir parçası haline taşır. Genellenmiş, rutin, gündelik gözetlemedeki asıl husus, bir kuralı çiğnemeyi veya kanunu ihlal etmeyi bırakın, sıradanın haricinde hiçbir şey yapmamış olmanıza rağmen işlemlerinizin, takaslarınızın, konuşmalarınızın, hareketlerinizin ve aramalarınızın önemli olmasıdır (Lyon, 2006, s. 14).

Gözetim iki yüze sahiptir. Bu durum gözetimin daima bir muğlaklık içermesine yol açarken, bu muğlaklık da, gözetimi hem ilgi çekici hem de oldukça hassas kılmaktadır (Lyon, 2013, s. 31). Lyon, gözetlemenin iki yüzüne ait en güzel örneğin, günlük e-posta karşılaşmalarında

görülebileceğini öne sürmektedir. Çok şeyi mümkün kılan ve yeni özgürlüklere bir araç olarak sunulan bir şeyin, başka bir bakış açısıyla da az çekici olan bir tarafını da görmek mümkündür. Bir araç olarak e-posta, eşzamanlı olarak mesafe ve zaman engellerinin üstesinden gelen esnek bir iletişim biçimine olanak sağlarken, ama aynı zamanda kağıt mektuplara nazaran mesajların ele geçirilmesini çok daha kolay kılmaktadır (Lyon, 2006, s. 15.)

Bunun yanında, 'gözetim' sözcüğünün olumsuz çağrışımlarına karşın, etki, idare ve denetimin ille de kötü, topluma karşı olduğunu düşünmemek gerekir. Yasal gereklilikler konusunda teşvik ve uyarı görevi de görür; idare, yardım ve hizmetler gibi belli yetkilerin layıkıyla yerine getirildiğinden emin olmak için var olabilir ve denetim de olumsuz olayları sınırlayabilir (Lyon, 2013, s. 33.)

Özetle, gözetim bir yandan bir uygulamalar bütünü iken, diğer yandan belli amaçlarla ilişkilidir. Gözetleme uygulamaları genellikle, gözetleyenlerin imtiyazlı olduğu güç ilişkilerini içermektedir. Ancak, gözetim sıklıkla gözetlenenin rol oynadığı bir katılımı da içermektedir. Görme ile ilgilidir ancak, tek boyutu bu değildir; gözetim aynı zamanda görünürlük ile ilgilidir.

Gözetim Kavramının Tarihsel Arkaplanı

Sosyal bilimlerdeki kuramlarda gözetim olgusu, her ne kadar modernite paralelinde ulus-devlet ve çağdaş örgütlerle ilişkilendirilse de; ilk çağlardan bu yana gerek dinlerin gerekse kabile yapıları ile geleneksel devletlerin, toplumsal denetim amaçlı olarak gözetime başvurdukları bilinmektedir (Dolgun, 2005, s. 25) Bu açıdan, gözetim, sadece içinde bulunduğumuz döneme ait bir kavram olmamakta, insanlık tarihi kadar eskiye dayanmaktadır. Örneğin "listeleme tekniği" Antik Yunan uygarlığında vergi, askerlik hizmetleri ve göç gibi amaçlarla nüfus kayıtlarının tutulmasında kullanılmıştır. Hatta o tarihlerde göçebe bir topluluk olan İsrailliler bile İ.Ö. 15. yüzyılda halkın nüfus sayımlarını ve evlilik kayıtlarını tutmuşlardır. Bu kayıtlar, ileride başıboş dolaşanların Filistin'e yerleştirilmesi sırasında toprağın paylaştırılmasında kullanılmıştır (Lyon, 1997, ss.39-40). Ancak bu dönemdeki söz konusu gözetim, sadece bu sınırlı faaliyetlerden ibarettir. Askerlik hizmetini düzene koymak, vergileri düzgün olarak toplama amaçları dışında etkin bir gözetimin varlığından söz etmek mümkün değildir.

İktidarlar ve egemenlik ilişkileri açısından gözetim pratikleri, ilk çağlarda kabilelerin, imparatorlukların ve monarşilerin gücünü daha çok şiddet ve baskı araçları yoluyla veya askeri amaçlarla pekiştirirken; bu, modern toplumlarda daha sistematik hale getirilmiş, şiddet/baskı araçlarının yerini, gözetmenler ile yöneticilerin uyguladığı çağdaş teknikler almıştır (Dolgun, 2005, s. 25). Enformasyon toplumu olarak adlandırılan günümüzde ise, gözetim pratikleri tümüyle yüksek teknolojinin imkânlarına dayalı bir karakteristiğe bürünmüştür (Dolgun, 2005, s. 25) .

İlk Dönemlerde Gözetim Olgusu

Giddens'ın düşüncelerine yer verirken belirtildiği gibi, iktidarların ve egemenlik yapılarının gücünü destekleyici bir araç olarak gözetim, iki temel unsur içermekteydi: Birincisi, devlete tabi nüfusun eylemlerini yönetmek üzere kullanılabilen "şifrelenmiş bilgi" birikimi iken; ikincisi de, bu eylemlerin iktidarlar tarafından doğrudan denetlenmesiydi. Bunlardan ilki olan "şifrelenmiş bilgi" yazının toplumsal açıdan oynadığı rolle yakından ilişkilidir (Dolgun, 2008, s. 29).

Giddens, insanlık tarihi kadar eski bir kavram olan gözetimin resmi olarak yazının bulunuşuyla başladığını ifade etmektedir. (Giddens, 2008, s. 66). Giddens yazının, modern olmayan devletlerin gözetleme faaliyetleri açısından birçok anlam taşıdığına işaret etmektedir. Yazı, devlet aygıtını hem nesneler hem de kişiler üzerinde uyguladığı idari denetimin kapsamını genişletmek üzere kullanılabilecek bir şifreleme bilgisi sağlamaktadır (Giddens, 2008, s. 66). Giddens'ın ifadeleri bize gösteriyor ki; hem devletin kayıtları için gerekli bilgiler hem de bireylerin özel alanlarıyla ilgili malumat, yazı kanalıyla toplanmaktadır. Yazı, elektronik olmayan bir bellek aygıtıdır. Malumatların depolanmasını ve faaliyetlerin düzenlenmesini sağlamaktadır. Böylece yazı, insanların listeleme tekniğini keşfetmelerini sağlamıştır (Lyon, 1997, ss.39-40.) . Listeleme tekniği, nesneleri veya kişileri sayan ve bunları birbirlerine göre sıralayan bir formüldür. Yazı, zaman-mekan ayrıştırmasını artırmış, yani toplumsal ilişkilerin, sözlü kültürlerde olduğundan daha geniş zaman ve mekan aralıkları boyunca uzamasını mümkün kılmıştır (Giddens, 2008, s. 66) .

Ne var ki, listeleme ile birlikte gözetleme, üretebildiği iktidar bakımından ister istemez sınırlı kalmıştır. Bu alan ancak geleneksel metinlerin gelişimiyle birlikte edebi metinlerin gelişimine paralel olarak artmıştır. Giddens'a göre yazılı metinler, "anlamlı *(semantic)* bir içerik

yaratmak üzere işaretleri bir araya getirdiklerinde, artık yalnızca olayları, nesneleri ya da kişileri sınıflandırmaz, bunların tanımlanmasını da mümkün kılarlar" (Giddens, 2008, s. 66).

Metinlerin tanımlanmasıyla birlikte anlamlı bir içeriğe sahip olan yazı, nüfusun itaatsiz kesimlerinin faaliyetlerini tanımlamak ve izlemek üzere doğrudan kullanılabilir hale gelmiştir. Yazıyla birlikte ayrıntılı "resmi istatistikler "in tutulması, "vaka kayıtları" ve bireylerin gündelik yaşamlarına ilişkin oldukça ayrıntılı başka belgelendirme biçimleri, modern devletlerin ve örgütlenmelerin kendine has özelliklerinden olmuştur (Giddens, 2008, s. 67).

Matbaanın keşfiyle birlikte gözetimde yeni bir aşamaya girilmiştir. Giddens'ın ifadesiyle matbaa; "iletişimin mekanizasyonundaki ilk önemli adımdır ve belge ve metinleri geniş çapta ulaşılabilir kılmakla Avrupa kültürünün maddi, entelektüel ve sanatsal alanlarda taklit suretlerden uzaklaşma sürecini başlatmıştır" (Giddens, 2008, s. 37). Giddens'a göre matbaanın mümkün kıldığı ve mutlakıyetin pekişmesi aşamasında artan biçimde kullanıldığı şey bunun devletin gözetim operasyonlarında çok büyük bir ilerleme sağlamasıdır (Giddens, 2008, s. 37) Matbaayla birlikte devlet gözetimi özellikle kurumlar üzerinde baskı unsuru haline gelmiştir.

Sonuç olarak yazı ile gözetim pratikleri arasındaki ilişki, stratejik bir kaynak olan bilginin ve dokümantasyon işlemlerinin, yazının gelişimine paralel biçimde derlenmeye başlandığı ve iktidar/egemenlik ilişkilerinin bunun bir sonucu olarak şekillendiği tarihsel süreç içinde açık olarak görülmektedir. Ayrıca, tekniğin değişmesi ve bu alanda yaşanan ilerlemeler de, gözetim pratikleri üzerindeki uygulamaları ve hakimiyeti büyük ölçüde kolaylaştırmıştır. Antikitede kil ve parşömen üzerinde kayıta geçirilerek toplumsal denetimin ilk örneklerini veren bilgilerin, iktidarlara yeni bir güç sağlamasındaki gibi; matbaanın bulunması da, toplumsal denetim ve gözetim faaliyetlerine yeni bir boyut kazandırmıştır (Dolgun, 2005, s. 33) .

Modern Dönem Öncesi Cemaat Toplumlarında Gözetim

Modern öncesi cemaat toplumlarında bireylerin güvenliğini sağlama adına etkin bir devlet gözetimi bulunmamaktaydı. Bu sebepten ötürüdür ki; modernlik öncesi çağda yaşayanların güvenliklerini savunmak ve tehlikeye karşı savaşmak için kullanmayı öğrendikleri tek silah, ne kadar güçsüz de olsa, kendi "yoğun sosyallikleri" ve "insan ilişkilerinin karmaşık oyunu" idi (Bauman, 2012, s.51)

> *Köylüler de, kasabalarda oturanlar da kendi güvenliklerini korumak için kendilerinden destek almak zorundaydılar – psikolojik açıdan olduğu kadar fiziksel açıdan da. Güvenlik, bir dizi toplumsal dayanışma aracılığıyla sağlanmaya çalışılıyordu. Ayazdan korunmak için bedenlerine giysiler giydikleri gibi, kendilerini aile, akrabalık, köy ya da kasaba cemaati adına verdikleri, birbiri ardı sıra gelen insan ilişkileri katmanlarıyla kuşattılar…*
> *Kasaba cemaati; aile, dostluk, komşuluk ve çeşitli meclisler gibi tüm boyutlarıyla, etkili ve gerçek dayanışma ilişkilerine nihai biçimini verdi. Şehrin simgesi surlar gibi bunlar, tehlikeli "dışarısı" ile çeşitli topluluk bağlarının insanları birbirine bağladığı "içerisi" arasındaki sınırları belirliyordu…*
> *Bu, dönemin sosyalliğinin kendisini tam olarak ifade edebilmek için, görece kısıtlı bir alana, yakın ve sık temaslara, çok sayıda ya da çok uzak olmayan buluşma mekanlarına gerek duyduğu anlamına gelmektedir.* (Muchembled, 1978, ss. 45-52).

"Yoğun sosyallik" zeminine dayalı güvenlik, genişletilmiş ya da akışkan bir toplumsal ortama aktarılamazdı. Çünkü üretiminde kullanılan temel beceri "öteki"ni bilinir kılmak, onu bilinen dünya içinde sabit bir konumu olan, tamamen bildik bir bireye dönüştürmekti (Bauman, 2012, s. 52) . Bir köy ya da kasabanın sakinleri, karşılaşabilecekleri kişinin çoğunu tanıyorlardı. Çünkü birbirlerini tüm işlevleriyle ve çok farklı durumlarda izleme olanağına sahiptiler. Modern ütopya yazarlarının, ideal toplumun bir göstergesi olarak hayalini kurdukları bu "şeffaflık", cemaat toplumlarının günlük yaşamlarının gerçeğiydi. Ancak şeffaflığın sağladığı bu güvenlik hissi de, sadece birbirini tanıyan bireylerin oluşturduğu bu küçük yerleşim alanlarının içerisiyle sınırlıydı (Bauman, 2012, s. 52) Dolayısıyla bu dönemde, cemaat şeklinde örgütlenmiş bireylerin, birbirlerine karşı uyguladıkları denetim, sadece izleyerek gözetimden ibaretti.

Modern çağ öncesi insanının bu küçük ve istikrarlı, dolayısıyla sıkı sıkıya denetlenen dünyası için 16. yüzyılla birlikte tehlike çanları çalmaya başlamıştır ve bir sonraki yüzyılda geri döndürülmesi olanaksız biçimde parçalanmıştır. Hızla artan nüfus ile birlikte herkesin birbirini tanıdığı küçük yerleşim yerlerinin yerini, birbirini daha az tanıyan insanların oluşturduğu nispeten büyük şehirler almaya başlamıştır. Nüfus patlaması bir yana, toprak mülkiyetinin yeniden düzenlenmesi ve tarım teknolojisinin verimliliğindeki artış, geleneksel köy cemaatlerinin yeni nüfusa iş ve yiyecek sağlamasını engellemiştir. Artan sayıda erkek ve kadın ekonomik açıdan bir fazlalık ve bunun sonucu olarak toplumsal açıdan "yurtsuz" hale gelmiştir (Bauman, 2012, s. 52).

Modern öncesi çağda yaşanan değişimin her ikisi de gözle görülür olan birbiriyle bağlantılı iki sonucu olmuştur. Bunlardan ilki, "efendisiz insanların" aniden belirişi ve sayısal olarak genişlemesiyken; ikincisi, "aylakların" yerel cemaatlerin küçük ve esnek olmayan dünyasına ani okunu olmuştur. Efendisiz insanları; herhangi bir yere ait olmayan, davranışlarından ötürü toplumsal sorumluluk taşıyacak bir üstleri ve geçimlerini sağlama karşılığında onlardan itaat talep edebilecek somut bir cemaatleri olmayan bir kesim olarak tanımlamak mümkündür. "Aylaklar" ise, geleneksel tanıdık kılma ve topluluğun bir parçası haline getirme yöntemiyle ehlileştirilemeyecek ve cemaatin yaşamına uyumlu kılınamayacak kadar kaygısız ve kalabalık bir topluluktu (Bauman, 2012, s. 53).

"Efendisiz insanlar-aylaklar" diye isimlendirilen bu kimseler, cemaat toplumundaki bireyler gibi iyi gözetlenemediklerinden, toplum için tehlike olarak görülmeye başlanmışlardır. Toplumsal düzenin temel birimleri olarak cemaatleri parçalayan bu kütlesel fazlalığın en önemli etkisi, uzun vadede, toplumun yeniden üretiminde devletin rolünü tamamıyla değiştiren bir dizi hukuksal girişimi harekete geçirmek olmuştur. Nitekim eskinin cemaat toplulukları, bu kitleyle başa çıkamıyorlardı. Bunun nedenleri arasında yeterli ekonomik kaynaklarının olmaması gösterilebilir. Belki de hepsinden önemlisi, eskiden sorunsuz bir şekilde işleyen "*Ben seni gözetliyorum, sen beni gözetliyorsun*" şeklindeki cemaat denetim sistemi çatlamıştı. Bunun sonucu olarak ortaya çıkan kriz, toplumsal iktidarın yeniden düzenlenmesini gerektiriyordu (Bauman, 2012, s. 55).

Michel Foucault her ne kadar "gözetim" ya da "yola getirici iktidar"ın belirmesini, modern çağın başlarında meydana gelen "toplumsal denetimde göz tekniğinin gelişimiyle paralel görse de, bu tür bir iktidar yeni değildir. Bu iktidar modern çağın gelişiyle doğmamıştır. Modernlik öncesi dönem boyunca önemli bir toplumsal denetim yöntemi olarak varlığını sürdürmüştür. Erken modern çağda olan şey, gözetim gücünün geleneksel faillerinin iflas etmesi olmuştur. O nedenle, disipline dayalı denetim geçmişte olduğu gibi sıradan bir şey olarak yapılamaz olmuştur. Artık bu sorun, görünür hale gelmiştir ve özenle ele alınması, tasarlanması, örgütlenmesi, idare edilmesi ve bilinçli bir şekilde üzerine eğilmesi gerekmiştir. Bu görevi ise yerine getirecek yeni, daha güçlü bir fail gerekiyordu. Yeni fail "Devlet"ti (Bauman, 2012, s. 55) .

Bu dönemde kanun koyucular, efendisiz ve aylakları daha görünür kılmak ve böylelikle gözetlenebilirliklerini arttırmak için değişik araçlara yönelmişlerdir. En basit yöntem hemen

her sığır yetiştiricisinin bildiği damgalama yöntemiydi. Bu dönemde sığırları ayırmak ve başıboş sığırları belirlemek için kullanılan bu yöntemin uygulanması, başıboş insanları kapsayacak şekilde genişletilmiştir. 1604 tarihli kanun damgayla ilgili şu talimatı vermekteydi: "deriye ve ete o şekilde dağlanıp işlenmeli ki, 'R' (Rogue-Serseri) harfi görülsün ve böyle bir serserinin üzerinde yaşam boyu sürekli bir işaret olarak kalsın." İşaret sayesinde en azından özellikle tehlikeli insanların ayırt edilip, yakın gözetim altına alınabileceği ve böylece bu kimselerin hareket halinde oluşlarının doğuracağı sonuçların ortadan kaldırılabileceği umuluyordu (Bauman, 2012, s. 57).

Ancak cemaate dayalı denetimin iflasına yönelik tepkiler arasında en önemli sonuçları doğuracak olanı, zorunlu kapatılmanın icadıydı.

Moderniteye Geçiş Döneminde Kapatılma Pratikleri

Moderniteye doğru evrilen geçiş dönemindeki gözetim etkinlikleri, biçimlenmekte olan toplumsal yapıda 'kapatılma pratikleri' şeklinde ağırlığını duyurmaya başlamıştır (Dolgun, 2005, s. 53) Cemaatleşmeye dayalı gözetimin iflasına neden olan, görünmez efendisiz-aylakları daha görünür kılmak ve rahat gözetleyebilmek için alınan tedbirlerin arasında en önemli sonuç doğuran "zorunlu kapatılma" olmuştur. Bu aşamada ortaya çıkan söz konusu pratiklerin, Batı'ya dinamizmini kazandıran kapitalizm ve sanayi devriminin işleyiş mantığına hizmet eder şekilde bir işlevsellik yüklendikleri görülmektedir (Dolgun, 2005, s. 53).

Gözetimin modern anlamda kurumsallaşması açısından, Batı'daki kapatılma pratikleri ilk aşamayı oluşturmaktadır. Foucault'un büyük kapatılma olarak ifade ettiği bu olaylar zinciri, 17. yüzyılda, bu efendisiz ve aylaklarla birlikte, toplumda onlar gibi başıboş dolaşan veya tehlike arz eden suçlu, deli, sarhoş ve hastalıklıların (cüzzamlı ve vebalı gibi) da kapalı mekânlarda zoraki olarak gözetim altında tutulmalarını ifade etmektedir (Foucault, 1995, s. 83).

"Büyük kapatılma" fikrinin doğuşunda, vebalı bölgelere uygulanan gözetimin büyük etkisi olmuştur. Nitekim 17. Yüzyılın sonuna ait bir yönetmeliğe göre, bir kentte veba salgını çıktığında alınması gereken tedbirler ortaya konulmuştur. Yönetmeliğe göre öncelikle katı bir mekânsal çerçeveleme yapılmalıdır. Mekânsal çerçeveleme; kentin ve mücavir alanın kapatılması, buradan dışarı çıkmanın yasaklanması, aksine davranışların ölümle

cezalandırılması, başıboş hayvanların hepsinin öldürülmesi, kentin her birinin başına yetkili bir eminin getirildiği ayrı mahallelere bölünmesini içermektedir. Yönetmelikte ayrıca belirtilen günde herkesin evine kapanması emredilmektedir. Bu bağlamda evden çıkmak ölümle yasaklanmıştır. Yönetmeliğe göre her cadde bir temsilcinin yönetimine verilmektedir; o da burayı gözetim altında tutmaktadır; buradan ayrılması söz konusu olduğunda ise ölümle cezalandırılmaktadır. Ayrıca yine yönetmelikte emredildiği üzere, temsilci herkesin kapısını bizzat dışarıdan kapatmakta ve anahtarları götürüp mahalle eminine teslim etmektedir; o da bu anahtarları karantina bitene kadar muhafaza etmektedir. Bütün bunlara ek olarak, her aile erzak yığmış olmalıdır; ancak şarap ve ekmek için caddede ve evlerin arasında küçük tahta kanallar yapılmıştır. Bunlar mal sağlayıcılarla halk arasında iletişim olmadan, herkesin ihtiyacını karşılamasını sağlamaktadır. "Büyük Kapatılma"da teftişler sürekli, bakışlar her yerde uyanıktır (Foucault, 1995, ss.289-290) . Vebalı kentler için getirilen bu uygulamalar göstermiştir ki; bireylerin sabit bir yere kapatılmaları, en küçük hareketlerin bile denetlendiği, bütün olayların kaydedildiği, kesintisiz bir yazı faaliyetinin merkez ile çevreyi birbirine bağladığı, iktidarın sürekli ve hiyerarşik bir biçimde icra edildiği; her bireyin kapalı, parçalara ayrılmış ve her noktası itibariyle gözetlendiği disiplinsel bir düzeneği oluşturmaya olanak tanımaktadır (Foucault, 1995, s. 292).

Foucault'nun "Büyük Kapatılma"sının mimari biçimi ise Jeremy Bentham'ın *Panopticon*'udur. Foucault Hapishane'nin Doğuşu adlı çalışmasında bize Bentham'ın *Panopticon* fikrini ve bunun yorumunu vermektedir. David Wood'a göre, Foucault için *Panopticon*, modern projede anahtar, uzamsal bir figür ve ayrıca modern kişiliğin yaratılışında, diğer bir deyişle insanların ve toplumun görüşlerinde, modernliğin imajında anahtar bir mekân tasarımıdır (Wood, s. 235).

Jeremy Bentham, 1791 yılında yayınladığı *Panopticon* planıyla ceza, reform ve yönetimde yeni bir çağın doğuşunu ilan etmektedir. Bentham'ın zamanındaki hapishaneler, her türden mahkûmun çok kötü yaşam koşullarında bir arada bulunduğu türdendi. Bentham'ın amacı ise bütün bunları hatta daha fazlasını değiştirmektir.

Bentham'ın bu projesi Hapishanelerin idare şeklinde köklü bir değişiklik yapmayı amaçlamaktadır. Bentham bu projeyle birlikte hem mahkûmları gözetleyerek bilgilenmeyi hem de onları ıslah etmeyi amaçlamaktadır. Güvenli nezaret, "hapishane, inziva, zorunlu emek ve talimdir." Bunlar uslanmazları cezalandırmaya, delileri denetlemeye, suçluları ıslaha,

sanıkları tevkife, aylakları çalıştırmaya, muhtaçlara yardım etmeye, hastaları tedavi etmeye, isteyene istediği sanayi dalında eğitim vermeye ya da eğitim yolunda artan yarışı düzenlemeye yetecek faktörlerdi. *Panopticon*'un görüşü, kötülük kin ya da nefretten örülmüyordu; bu bilerek zulmeden bir şey de değildi. Sonuçta insani ilerlemenin muhteşem vizyonu ile sarhoş olan ve bu ilerlemeyi hızlandırma güdüsü ile güdülenen gerçek bir reformcu olarak Bentham'ın düşündüğü, her şeyde aradığı, "insanın mutluluğuydu." O gözetlemenin bireyler arasındaki belirsizliği ortadan kaldırarak, bireyleri huzura ve mutluluğa ulaştıracağına inanıyordu (Bauman, 2001, s. 146)

Foucault Bentham'ın *Panopticon*'unun mimari tasarımını şu şekilde açıklar:

> *Çevrede halka halinde bir bina, merkezde bir kule; bu kulenin halkanın iç cephesine bakan geniş pencereleri vardır; çevre bina hücrelere bölünmüştür, bunlardan her biri binanın tüm kalınlığını kat etmektedir; bunların, biri içeri bakan ve kuleninkilere karşı gelen, diğeri de dışarı bakan ve ışığın hücreye girmesine olanak veren ikişer pencereleri vardır. Bu durumda merkezi kuleye tek bir gözetmen ve her bir hücreye tek bir deli, bir hasta, bir mahkum, bir işçi veya okul çocuğu kapatmak yeterlidir. Geriden gelen ışık sayesinde, çevre binadaki hücrelerin içine kapatılmış küçük siluetleri olduğu gibi kavramak mümkündür. Ne kadar kafes varsa, o kadar küçük tiyatro vardır, bu tiyatrolarda her oyuncu tek başınadır, tamamen bireyselleştirilmiştir ve sürekli olarak görülebilir durumdadır.*

Bu mekânsal organizasyon şekli toplum için kapsamlı bir projeyi, bir tür ütopyayı desteklemektedir. Hatta Bentham bu ideal modelin "gözetim altında tutulacak her çeşit insanın bulunduğu her türlü kuruma ve özellikle de cezaevlerine, hapishanelere, işçi evlerine, ıslah evlerine, düşkünler evine, karantina bölgelerine, fabrikalara, hastanelere, akıl hastanelerine ve okullara uygulanabileceğini düşünmüştü (Mattelart, 2012, ss.13-14) Bentham'a göre bu projeyle birlikte "ahlak kuralları reforme edilmiş, sağlık politikaları iyileştirilmiş, endüstri güçlendirilmiş, eğitim yaygınlaştırılmış, ekonomi eskisi gibi sağlam temellere dayandırılmış ve bütün bunlar basit mimari düşünce ile gerçekleştirilmiştir (Mattelart, 2012, s. 14) Yine Bentham, bu projeyi az sayıda personelle ve az maliyetle yapmayı hedeflemiştir. Bu nedenle az maliyetle işletilebilecek bu çok amaçlı projenin, iktidarların büyük ilgisini çekeceğini düşünen Bentham, bundan iyi bir kazanç elde etmeyi ummuştur. Ancak hayatı boyunca bu projeyi gerçekleştirememiş ve proje onun açısından büyük bir zaman ve para kaybı olarak kalmıştır. Buna karşın Bentham'dan sonra özellikle 19.yüzyılın ilk yarısında inşa edilen hemen tüm hapishaneler bir şekilde Bentham'ın bu projesine atfen, onun bazı uygulamalarını örnek almak suretiyle yapılmışlardır (Foucault, 2003, s. 86) Dolayısıyla Bentham'ın bu projesi hem tam anlamıyla hiçbir zaman

gerçekleşmemiş hem de bir yönüyle defalarca uygulanmış bir proje olarak kabul edilmektedir. Son olarak şu hatırlatılmadır ki, *Panopticon* bize doğrudan Bentham tarafından ulaştırılmamıştır. Ceza teorisi ve ceza infaz sistemleri üzerine çalışan pek çok bilim adamı *Panopticon*'un önemine çok önceden vakıf olmalarına rağmen, *Panopticon*'un bilinebilirliği ve gözetime ilişkin hemen her yazında kullanılması, Foucault'un onunla ilgilenmesi ve Hapishanenin Doğuşu adlı eserinde ona geniş yer vermesiyle artmıştır (Lyon, 1997, s. 92).

Modern Toplumlarda Gözetim

Ernest Gellner, kültürlerin de bitkiler gibi, yabani ve ıslah edilmiş türlere ayrılabileceğini söyler. Yabani olanları insan hayatının bir parçası olarak kendiliğinden yetişir ve yeniden ürer. Hiçbir topluluk ortak bir iletişim ve normlar sisteminden yoksun olamaz; bu tür yabani kültürler, bir kuşaktan ötekine kendilerini bilinçli bir tasarım, nezaret, gözetim ya da özel beslenme olmaksızın yeniden üretirler. Buna karşın ıslah edilmiş ya da bahçe kültürleri, genelde okuryazarlıkla ve uzman personelle desteklenmiş bir karmaşıklık ve zenginliğe sahiptirler (Gellner, 2006, s. 130) Yeniden üretmek için tasarıma ve nezarete gereksinimleri vardır; onlarsız bahçe kültürleri çürüyüp gider, her yanı yabani otlar kaplardı. Her bahçede güvenlikten yoksun bir yapaylık duygusu vardır; bahçe bahçıvanın sürekli dikkatini gerektirir, çünkü bir anlık ihmal ya da dalgınlık onu başlangıçtaki durumuna döndürebilir. Ne kadar iyi yapılmış olursa olsun, kendini yeniden üretmesi konusunda bahçe tasarımına güvenmek olanaksızdır; benzeri biçimde, kendi kaynaklarıyla kendini yeniden üretmesi konusunda bahçeye güvenmek olanaklı değildir. Dayatılan düzenin kırılganlığını vurgulamak üzere yabani otlar oradadır; bunlar, hiç bitmeyen nezaret ve gözetim gerekliliği konusunda bahçıvanı uyarırlar (Bauman, 2012, s. 65).

İşte modernitenin ortaya çıkışı, böylesi bir vahşi kültürlerin bahçe kültürlerine dönüşmesi süreci olarak yorumlanabilir. Gellner botanik benzeşime ek olarak, bu yeni durumu betimlemekte başka bir benzetme daha kullanmıştır:

> *Tarım insanı, doğal çevrede yaşamını sürdürebilen doğal bir türe benzetilebilir. Sanayi insanı ise doğal atmosferde artık güçlükle nefes alabilen yapay olarak üretilmiş ya da doğmuş, ancak yeni düzen, özel bir karışımı olan ve yapay olarak beslenen bir hava ya da ortamda etkili biçimde iş görebilen ya da yaşayabilen bir türle karşılaştırılabilir. Yani sanayi insanı, bir tür dev akvaryum ya da solunum odasına benzeyen, özel bir biçimde sınırlandırılmış ve inşa edilmiş birimlerde yaşamaktadır; ancak bu odaların inşa edilmesi ve bakımının yapılması gerekir. Bu dev havuzların içindeki hayat veren ve koruyan havanın ya da sıvının bakımı*

> *otomatik değildir. Özel bir bitkiye ihtiyaç vardır. Bu bitkinin adı da ulusal eğitim ve iletişim sistemidir. Tek etkin bakıcısı ve koruyucusu da devlettir* (Gellner, 2006, s. 132).

Gellner bu benzetmeyle, oldukça devletçi bir anlayış sergilemektedir. Gellner'in bakış açısı, bir yönüyle gözetimi elzem olarak gören ve hatta hayati gören bir bakış açısıdır.

Modern toplumlarda gözetim olgusuna geçmeden önce modernizmin tanımını yapmak faydalı olacaktır. Modernizm, 17. Yüzyılda Avrupa'da başlayan ve sonrasında neredeyse tüm dünyayı etkisi altına alan, toplumsal yaşam ve örgütlenme biçimini ifade eder (Giddens, 2004, s.11) Bir başka deyişle modernizm, 17. Yüzyıldan itibaren sosyal, ekonomik ve kültürel alanda yaşanan büyük değişimler sürecine verilen isimdir. Bu sürecin üç temel sacayağı bulunmaktadır. Birincisi, ekonomik alanda sanayileşme başlamış, üretim tarzı ve ilişkileri geleneksel yöntemlerden tamamen farklılaşmıştır. İkinci olarak sanatta, mimaride ve kültürde bir yenileşme ve farklılaşma yaşanmıştır. Üçüncüsü ise düşünsel alanda olmuştur. Bu dönemle birlikte bilimsellik ve akılcılık ön plana çıkmış, bilginin tek kaynağı olarak akıl ve bilim kabul edilmiş ve Aydınlanma yaşanmıştır. Şunu da ifade etmek gerekir ki; ileri sürülen bu sav, bugün post modernizm tarafından sorgulanmaktadır.

Önceki bölümlerde de belirtildiği üzere gözetim, tarihin tüm dönemlerinde var olmuş ve iktidarların en güçlü toplumsal denetim mekanizmalarının başında gelmiştir. Ancak kurumsallaşmış ve temel nitelikteki gözetim teknikleri, sınai kapitalizm doğrultusunda ortaya çıkan ve enformasyon toplumuyla birlikte tüm yaşamı egemenliği altına alan biçimde, sadece modern ve özellikle de post-modern toplumlara özgü bir kavramdır (Dolgun, 2005, s.60). Bauman'a göre; insanlık tarihinin modernliğe denk gelen bölümü boyunca devlet, egemenliği altındaki insanları, koyduğu yasalarla uyumlu-itaatkar bireylerden oluşan bir toplum haline getirmeyi misyon edinmiştir. Bauman'a göre, akla dayalı, rasyonel şekilde oluşturulan böyle bir toplum, modern devletin nihai amacı olarak görülmekteydi (Bauman, 2003, s. 24) Fakat bu noktada asıl sorgulanması gereken durum, hakikatin bu olup olmadığıdır. İşin aslı geçekten Bauman'ın ifade ettiği gibi akla dayalı bir toplum mudur, yoksa yönetici elitin çıkarlarına mı dayalıdır?

Modern devlet, hedefi olan toplumu oluşturmak için sosyal hayatın büyük bir bölümüne müdahale ederken ve toplumu istediği şekilde yönlendirmek için kurallar koyarken, bir taraftan da bunlara uyulup uyulmadığını denetlemek ve kendi öngördüğü toplum düzenine

karşı gizli bir takım faaliyetler yürütülüp yürütülmediğinin bilgisine sahip olmak istemektedir. Ayrıca toplumda baş gösteren rahatsızlıklar ve sosyal gerilimler de ancak iyi bir gözetimle önceden öngörülebilecektir. Bu nedenle modernizmin getirdiği tüm teknolojik imkanları kullanarak, toplum içerisindeki gözetimi sürekli kılabilmek, modern devlette görülen en güçlü eğilimlerdendir (Lyon, 1997, s. 73) Dolayısıyla bireysel mahremiyet ve özgürlüklerini elden geldiğince kısmak ve kontrol etmek istemektedir.

Özetle, sosyal hayatın kurumsallaşmış bir şekilde yaygın olarak gözetimi, modernizm ile birlikte ortaya çıkmıştır. Gözetlemenin modernizm kavramıyla birlikte yayılmasının temel unsurlarını; sınai kapitalizm, sanayi kentlerinin artışı ve yoğunlaşma hızı, ulus-devletin iç ve dış tehlikelere karşı korunma güdüsü, askeri örgütlenmeler, devlet idaresi, bürokratik yapılanma ve kapitalist işletme sayısındaki artışlar gibi bileşenlerin oluşturduğu modern toplumda bulmak mümkündür (Dolgun, 2005, s. 61). Bu unsurlara bağlı olarak gözetim, sosyolojik açıdan modernitenin belirleyici özellikleri içinde en önemli unsurlardan birini oluşturmaktadır.

Ancak modern dünyada gözetim, "verilerin derlenmesi" gibi göze batmayan yollardan yayılım göstermektedir. Bununla bağlantılı olarak, öncelikle ordu, okul, fabrika, devlet daireleri gibi kurumlarda ortaya çıkan gözetim pratikleri, gelişimlerini gündelik yaşamın tüm alanlarını kapsayacak şekilde devam ettirmiştir. Bu anlamda gözetim; mevcut düzeni devam ettirme, statükoyu koruma ve büyük toplulukların faaliyetlerini koordine etmenin temel bir aracı olarak her türlü fiziki zorlamanın yerini alarak modernitenin kaçınılmaz bir boyutu haline gelmiştir. Nitekim gözetim, yerel özellik taşıyan veya bölünmüş parçalardan oluşan kısmi alanlardan öte, bunları tümüyle aşmış bulunan toplumsal analiz ve siyasi eylem biçimlerini gerektirmektedir (Lyon, 1997, ss.12, 309).

Modernite her ne kadar mevcut kimliğini sınai kapitalizm içinde kazanmış olsa da, bilginin yapılanmasına bağlı olarak farklı bir devlet oluşumu ile örgütlenme biçimlerine sahiptir. Bu sürecin ilk aşaması olan ulus devlet içinde, iktidarın yeni mekanizmalarını oluşturmak amacıyla kurduğu bilgi sistemleri ile gözetim teknikleri birbirlerinin içine girer ve "epistemolojik iktidarı" gündeme getirirler (Giddens, 2001, s. 85) . Foucault'un ifadesiyle, bireylere bilgi nesnesi olarak yaklaşan bu iktidar, siyasi-hukuki-idari ve ekonomik alanlara yönelik olarak, toplumsal olarak zaten sıkı şekilde gözetim altında olan bireyler hakkında her türlü bilgiyi de elde etme peşine düşer:

> *Fabrika gibi bir kurumda, işçi emeği ve işçinin kendi çalışması üzerine bilgisi, teknik iyileştirmeler, küçük icat ve keşifler, işçinin çalışma sırasında yapabileceği mikro-uyarmalar anında not edilir ve kaydedilir; dolayısıyla, işçinin kendi pratiğinden elde edilir, gözetleme aracılığıyla onun üzerinde uygulanan iktidar tarafından biriktirilir. Bu şekilde, işçinin çalışması, yavaş yavaş, denetimin güçlenmesini sağlayacak olan belli bir üretkenlik bilgisine ya da teknik bir üretim bilgisine dahil olur. Böylelikle, bireylerin davranışlarından yola çıkarak bizzat kendilerinden elde edilen bir bilginin nasıl oluştuğu görülür. Ayrıca, bu durumdan yola çıkarak oluşan ikinci bir bilgi vardır. Bireylerin gözetlenmesinden, sınıflandırılmasından, kaydedilmelerinden ve davranışlarının karşılaştırmalarının analizinden doğan, bireyler üzerine bir bilgi. Böylece, bu teknolojik bilginin yanı sıra bütün kapatma kurumlarına özgü bir gözlem bilgisinin, psikiyatri, sosyal- psikoloji, kriminoloji gibi bir tür klinik bilginin doğduğu görülür. Böylece, üzerinde iktidar uygulanan bireyler, ya kendilerinin oluşturduğu ve yeni normlara göre biriktirilecek olan bilginin elde edildiği yerdir, ya da yeni denetim biçimlerine imkân tanıyacak bir bilginin nesneleridir.* (Foucault, 2000, s. 251).

Bu anlamda pozitivist Aydınlanma düşüncesine dayanan moderniteyi, geleneksel toplumdakine benzemeyen keskinlikteki radikal kopuşları ortaya çıkartan bir süreç olarak tanımlamak mümkündür. Artık bilimsel bulgular ve teknolojik yenilikler, bireyleri yaşamın tüm alanlarında etkisi altına almaktadır. Moderniteyle birlikte doğan yaşam tarzları, modern insanı geleneksel toplumlara ait düzen biçimlerinden söküp almıştır. Bu dönüşümleri yaygınlıkları ve yoğunlukları açısından ele alan Giddens; "Yaygınlık açısından, küresel düzeyde toplumsal bağlantı biçimlerinin kurulmasında etken olurlarken; yoğunluk açısından da, gündelik yaşamın en kişisel ve mahrem yanlarını gözetim altında tutma gücüne sahiptirler" (Giddens, 2004, s. 14.) şeklinde yorumlamıştır.

Elektronik Gözetim

Gözetim teknolojileri günden güne baş döndürücü bir hızla gelişmektedir. Bunları tanımlama ve sınıflandırma konusunda farklılıklar göze çarpmaktadır. Belki de en kapsamlı sınıflandırmayı yapanlardan ABD Teknoloji Değerlendirme Bürosu, gözetim teknolojilerini beş kategori içinde değerlendirmiştir:

> *İşitsel gözetim, telefon dinleme aletleri ve gizli mikrofonlar gibi minyatür ileticiler ile telli sistemleri kapsar. Görsel gözetim, fotoğraflamayı, televizyonu (sokaklardaki ve alışveriş merkezlerindeki kameralar gibi), karanlıkta da gören aygıtları ve uydu temelli gözlemi kapsar. Veri gözetimi, dağıtılmış bilgi işlem, bilgisayar ağları, uzman sistemler ve örüntü tanıma gibi yazılımların o bildik zeminini kapsar. Algılayıcı teknolojisinin ise çeşitli türleri vardır: manyetik, sismik, kızılötesi, mekanik gerilim ve elektromanyetik. Öteki aygıtlar arasında, telsiz halk bandı,*

> *taşıtların yerini saptama sistemleri, manyetik şeritler, poligraflar, insan sesindeki psikolojik gerginliğin analizi, konuşma anlama, lazer yol kesme ve telsiz yer alır* (Lyon, 1997, ss. 147-148).

1960'lardan beri, iletişim ve bilgi teknolojileri sadece fax ve sabit telefonları değil, aynı zamanda, e-posta, kredi kartı işlemleri, cep telefonları ve interneti de günlük hayatın içine sokmuştur. Mitchell bu durumu şöyle özetler:

> *İki taraflı elektronik iletişim cihazları çoğaldıkça ve çeşitlendikçe, hayatlarımız siber uzayda daha bütünlüklü ve ayrıntılı izler bırakmaya başladı. geniş çaptaki kullanıma ulaşan bu türdeki ilk cihaz telefon olmuştur. Çok kısa sürede, görüşmelerin ne zaman, nerede, kim tarafından yapıldığını gösteren fatura bilgilerine ulaşılmıştır. Sonra ATM, para çekme makineleri ve perakende satış mağazalarındaki satış noktalarında yapılan işlemlerin kayıtları tutulmaya başlanmıştır. Kişisel bilgisayarlar ticari online ağlarına bağlanmaya başlayınca, onlar da elektronik izler bırakmaya başladılar. Artık anahtarlı video ağları alışveriş, banka işlemleri, film seçimi, sosyal iletişim, siyasi toplantılar gibi günlük amaçlar için kullanıldıkça, önceden elde edebildiklerinden çok daha ayrıntılı özel yaşam görüntülerimize sahip olmaya başlamıştır* (Mitchell, 1996, ss. 156-159).

Bu noktadan hareketle, bu başlık altında; bilgisayar, internet, e-mail, cep telefonları ve yeni ekonomi içerisindeki gözetim araçlarına ilişkin temel nitelikte teknik bilgiler verilerek sayısal verilerle elektronik gözetimin insan hayatındaki rolü gösterilmeye çalışılacaktır.

Bilgisayar

Günümüz toplumunun dinamik bir gücü olan bilgisayarlar, zaman ve mekan kavramlarını önemsizleştirerek, dünyanın farklı coğrafi bölgelerinde yer alan bilgi işlem merkezleri arasında her tür iletişimin kurulmasını mümkün kılmışlardır. Aynı zamanda enformasyon depolama, sınıflandırma, işleme, iletme ve yeniden oluşturma gibi özelliklere sahip olan bilgisayarlar, büyük miktarlarda bilgiye zahmetsiz ve hızlı şekilde ulaşma imkanı da sunmaktadırlar (Dolgun, 2005, s. 41).

Bilgisayar, gözetlemenin işlevlerini geliştirmek için 1960'lardan bu yana önemli rol oynamaktadır (Lyon, 2006, s.222). Ancak gözetime yönelik devrimsel nitelikteki gelişme, 'bilgisayar eşleştirmeleri' sonucunda ortaya çıkmıştır. Bilgisayar sistemlerinin, çeşitli kaynaklardan ve farklı amaçlarla toplanmış verileri ilişkilendirme gücüne dayanan bilgisayar eşleştirmeleri, devlet daireleri tarafından 1970'lerin sonlarında kullanılmaya başlanmıştır. Bu durum 1990'lara gelindiğinde tümüyle yaygınlık kazanmıştır. Oluşturulan veri bankaları

aracılığıyla, hem bireyler hem de toplum sıkı bir gözetime dahil edilmiştir (Dolgun, 2005, s. 129).

Günümüzde en önemli gözetleme aracı, toplanan verilerin saklanması, eşlenmesi, geri getirilmesi, işlenmesi, pazarlanması ve dolaştırılmasına olanak yaratan bilgisayarlardır (Lyon, 2006, s. 13). Bilgisayarların bu özellikleri, sıradan insanların kişisel yaşamlarına ait her tür ayrıntının, devlet daireleri/istihbarat örgütleri ve büyük şirketlere ait veri bankalarında toplanması/işlenmesi/yorumlanması ve eşleştirilmesine olanak tanımaktadır. Örneğin, FBI Ulusal Suç Bilgi Merkezi'nin veri bankasında, 20 milyon civarında kişisel kaydın bulunduğu ve günde yaklaşık bir milyon işlem gerçekleştirildiği bilinmektedir. Britanya Ulusal Polis Bilgisayarında ise, suçlu adları, parmak izleri, aranan ve kayıp kişiler, cezası kesinleşmiş sabıkalılar ve ehliyeti iptal edilmiş sürücülere ait 50 milyon civarında kayıt bulunmaktadır. Bilgisayar eşleştirmeleri ile her yıl 11 milyon suçlu ve 13 milyon motorlu araç, bu veri tabanına dayalı olarak denetlenmektedir (Lyon, 1997, s. 157).

Bunların yanı sıra sürekli gelişmekte olan teknoloji, gözetim faaliyetlerine katkıda bulunmaya devam etmiştir. Bütün yolları kapsayan bir bilgisayar sistemi içinde araçların yerini hatasız olarak belirlemeyi mümkün kılan "Bütün Yerküre Üzerinde Yer Saptama Yöntemi (Long-Range Navigaton) adlı program geliştirilmiştir (Negroponte, 1995, s. 198). Uzaysal ve birbiriyle ilişkili verileri toplama/ yönetme ve analiz etmeye imkanı tanıyan bilgisayar sistemlerine dayanan coğrafi bilgi sistemleri (GIS) üzerinde yükselen bu teknoloji, yollar/parklar ve caddeler yanında evler ile onların odalarını da kapsayacak yoğunluktaki konumsal unsurların gözetimine olanak sağlamaktadır (Infomag, 2002, s. 20).

Bilgisayarlar artık gündelik yaşamda gözetimin alanını inanılmaz derecede genişletmiş; gözetim faaliyetleri telefon dinleme gibi klasik yöntemlerin çok daha ötesine taşarak, bir yandan uydular/optik sistemler/kameralar ve internet gibi yan alanlarla yaptığı işbirliği sonucunda en üst düzeylere ulaşırken, diğer yandan da kendi başına apayrı bir güç olmuştur (Dolgun, 2005, s. 131). Bilgisayar üzerinden yapılan en önemli gözetim, "İletişim Takibi"dir. Birçok teknik yöntem kullanarak kişisel bilgisayarlar üzerinde yapılan İnternet gezintileri, e-posta trafiği, anlık ileti trafiği tespiti yapmak mümkündür. Kullanıcıların İnternet üzerinden hangi siteyi, ne kadar sıklıkla ziyaret ettiği, kime e-posta gönderdiği, kimden e-posta aldığı, kiminle anlık ileti yoluyla temas kurduğunu tespit edebilecek casus yazılımlar bilgisayarlara yüklenebilmektedir. Bu işlemi sadece casus yazılımlar değil; casus klavye, casus hafıza kartı,

casus kablo gibi araçlar da yapabilmektedir. Bu uygulama işyerlerinde de personelin bilgisi dahilinde ya da dışında olarak şirket içinde kullanılan bilgisayarlarla bağlantılı ana bilgisayar işlevi gören sunucular aracılığıyla da yapılabilmektedir. Yasal izleme durumlarında ise Telekomünikasyon İletişim Başkanlığı (TİB), İnternet servis sağlayıcı şirketler aracılığıyla bilgisayar üzerinden gerçekleştirilen iletişim trafiğini İnternete çıkışı sağlayan IP (İnternet Protokol Numarası) adresi üzerinden takip etmektedir("İletişim Özgürlüğüne Müdahale Raporu", 2009).

Her geçen gün yaygınlaşmakta olan bilgisayar kullanımını, Türkiye İstatistik Kurumu'nun verileri de desteklemektedir. Türkiye İstatistik Kurumu tarafından yapılan ve 2004-2013 yılları arasını kapsayan "Hane halkı Bilişim Teknolojileri Kullanım Araştırması" sonuçlarına göre; Türkiye'de bilgisayar kullanım oranı 2004 yılında %23,6 iken, bu oran 2013 yılında %60,2'ye yükselmiştir (TÜİK, 2013).

İnternet

Kamusal ve özel alan ayrımı tanımadan tüm dünyayı elektronik ortamda birbirine bağlayan İnternet, günümüz toplumunda dönüştürücü bir rol oynamaktadır.

İnternet, içe dönük ve sıkılgan kişilik yapıları nedeniyle gündelik yaşamda toplumsallaşamayan bireylerin, diğerleri ile iletişime girmelerine imkan tanıyan ve kişileri adeta görünmez sicimlerle birbirine bağlayan yeni bir kamusal alana dönüşmektedir (Sayar, 2002, s. 65). Kısa süre öncesine kadar, hayal dahi edilemeyecek kadar gelişkin bir kamusallık alanı olarak görülen İnternet; sunduğu çeşitli imkanların yanında, iktidar yapılarını ve eşitsizlikleri sabitleme potansiyeline de sahiptir. İnternetin olumlu ve olumsuz birçok faktörü beraberinde getirmesi, insanlığa umut yanında çeşitli kaygılar da aşılamaktadır (Dolgun, 2005, s. 168).

İnternet üzerine bugüne kadar etkili olan iki yaklaşımdan söz etmek mümkündür. Bu yaklaşımlardan birincisi; "ilerlemeci" bir anlayış içerisinde İnternetin "özgürleştirici" etkisini ön plana çıkartmaktadır (Mathews, 1997). "Bilgi parmaklarınızın ucunda" sloganında olduğu gibi, birinci yaklaşıma göre İnternet, bilgiyi bir yerden başka bir yere olağan üstü bir hızla taşımaktadır. Bilginin güç olarak algılandığı bir çağda bu teknoloji, birçok araştırmacı ve uygulamacı için olağanüstü geniş imkanlar sunmaktadır.

Öte yandan, İnternetin "anarşist" karakteri, denetimden uzaklığı, zaman ve mekandan bağımsızlığı, otoriter yönetimleri çok daha fazla sınırlandırma yetkisine sahiptir. "Zaman ve mekanla bölünmüş, ancak fiziksel giriş araçlarının oluşturduğu şebeke ile birbirine bağlanan ve dilin sayısal temsilleri ve duyusal deneyimlerini kullanarak paylaşılan bir zihin durumu (Whittle, 1997, s.25)" olarak tanımlanan siber-uzayda insanlar, otoriter yöneticilerden bağımsız, taleplerini daha kolay ifade edebilir hale gelmişlerdir. Özellikle de otoriter yönetimler içerisinde yer alan muhalif gruplar bu teknoloji sayesinde, uluslararası normlara ters düşen uygulamaların önlenmesi konusunda dış dünyadan daha kolay destek görmeye başlamışlardır (Bozkurt, 2000). Ölçek kavramının siber-uzayda, fiziki mekana göre daha az önemli hale gelmesiyle birlikte, bireyler geçmişte hiç olmadıkları kadar önemli hale gelmişlerdir. İnternetin "anonim" karakterinden faydalanan insanlar, her türlü düşünceyi gözlerden uzak ifade edebilir hale gelmişlerdir. Diğer yandan İnternet, yöneticiler üzerinde bir toplumsal denetim aracı haline dönüşebilmektedir. Bunun örneği, Monica Lewinsky skandalında görülmektedir. Bu görüştekiler kendilerine, aralarının iyi olduğu dönemde "Sovyetler Birliğinde uluslararası haberleşmeyi sağlayacak dev bir telefon santrali kuralım" diyen Troçky'e, Stalin'in "Zamanımızda bundan daha büyük bir karşı devrim düşünemiyorum" sözünü baz almışlardır. Bunlara göre Stalin'in bahsettiği "karşı devrim" gerçeklemiştir ve enformasyon devriminden sonra, artık yeni bir Stalin'in çıkması imkansız hale gelmiştir (Bozkurt, 2000).

Sonuç olarak bu görüşe göre, İnternet ya da diğer bir ifadeyle Enformasyon çağı toplumları, artık daha özgür ve demokratik toplumlardan oluşacaktır. Bu "teknolojik determinist" yaklaşım, modern sosyal teorideki ilerlemeci gelenek ile örtüşmektedir.

Bu görüşün karşısında yer alan ikinci yaklaşım ise, teknolojik determinizm geleneğine karşı çıkmakta ve teknolojinin de sosyal olarak inşa edildiğini savunmaktadır. Bu görüştekiler, İnternet gibi enformasyon teknolojilerinin tek başına bir değişim ajanı olamayacağını, tam aksine kurulu düzenleri pekiştirici bir etki yapacağını savunmuşlardır (Laszlo, 1992, s. 237-249). Diğer taraftan belki de İnternet'in en ironik tarafı, büyük ölçüde anarşistler tarafından inşa edilmiş, fakat ordu için finanse edilmiş olmasıdır. İki taraf da teknolojinin rüyalarını gerçekleştireceğine inanmıştır. Anarşist ya da diğer bir ifadeyle tekno-liberteryanların rüyasına göre, bilgisayarlar vücutsuz özgürlüğü mümkün kılacaktır. Ordu ise İnternet'in dev bir bürokrasi inşa edeceğine inanmıştır. İşin ilginç yanı şudur ki; iki taraf da haklıdır (Brown, 1998).

İnternet bir taraftan özgürlüğün teknolojik altyapısını hazırlarken, diğer taraftan da sıradan insanlar hakkında kişisel enformasyonun hiç hayal edilmedik düzeyde ortaya çıkmasına yol açmıştır. Öyle ki; günümüzün global köyünde postane müdiresi, artık bütün köylüler hakkında her şeyi bilir hale gelmiştir (McCune, 1999, ss. 10-12). Artık ağ üzerindeki milyonlarca insanı ya da belli ülkelerdeki potansiyel muhalifleri izlemek, dünyayı izlemekle görevli resmi otoriteler için çocuk oyuncağı haline gelmiştir.

Eli "mouse" tutan herkesin kullanabileceği bir kolaylığa kavuşturulmuş olan İnternet, baş döndürücü bir hızla yaygınlaşmakta ve her geçen gün ağ trafiği daha da yoğunlaşmaktadır. Bu yoğunluğu, İnternet kullanıcı sayısındaki artışla daha net bir şekilde ifade etmek mümkündür. Türkiye İstatistik Kurumu tarafından 2004-2013 yıllarını kapsayan "Hanehalkı Bilişim Teknolojileri Kullanım Araştırması" sonuçlarına göre; Türkiye'de 2004 yılında İnternet kullanımı %18.8 iken, bu rakam 2013 yılında %48,9'a ulaşmıştır (TÜİK, 2013).

Her geçen gün kullanıcı sayısı artan bu teknolojiyle birlikte kullanıcılar, yerlerinden kalkmadan bir tuşla fatura yatırma, bankacılık işlemleri, alışveriş yapma, kitap-gazete okuma, kütüphanelerde gezinti yapma ya da yeni insanlarla tanışabilme olanağına sahip olmaktadır.

Elektronik Posta (E-Mail)

Elektronik posta olarak Türkçeleştirebileceğimiz "electronic mail" ya da kısa yazımıyla e-mail, her şeyden önce göndericisi tarafından belirlenen varış yerine ulaşana ve okunana kadar bir bilgisayardan diğerine zincirleme şekilde iletilen dosyadır.

İnternet e-mail sistemi, Simple Mail Transfer Protocol (SMTP) tabanında çalışmaktadır. E-mail gönderim sürecinde; hazırlayan ve gönderen kişinin, alıcı kişinin ve aradaki iletişimi sağlayan kişinin bilgisayarı olmak üzere minimum üç bilgisayara ihtiyaç duyulmaktadır.

Bu teknik özelliklere sahip olan e-mail, eşzamanlı olarak mesafe ve zaman engellerinin üstesinden gelen esnek bir iletişim biçimine olanak tanır. E-mail sayesinde istediniz herhangi bir ülkedeki arkadaşlarınıza ulaşmak artık çok kolaydır. E-mail gönderilen kişinin bulunduğu zaman dilimi, gönderen kişinin bulunduğu zaman diliminden farklı olsa dahi, gönderilen kişinin gün başlarken mailini okuyabilmesi mümkündür. Ama ne yazık ki aynı araç kağıt

mektuplar kadar masum değildir ve mesajların ele geçirilmesini çok daha kolay kılar. Örneğin Echelon sistemi, aynı aracın zaman ve yer sınırlarını aşabilme avantajını kullanan kişilerin seçilmiş elektronik mesajlarının anahtar sözcük taraması ile detaylı bir araştırmasını mümkün kılar(Lyon, 2006, s.15).

Elektronik postalar ve diğer belgeler uzun zaman boyunca İnternet ortamında saklanmaktadır. Peki bu durumun ne gibi bir tehlikesi vardır? McCune bu durumu güzel bir örnekle açıklar (McCune, 1999, s.10): "Varsayalım ki, on yıl önce Tüketici Ürünleri Şirketine sinirli bir mail gönderdiniz ve sizin göndermiş olduğunuz bu eleştiri içerikli mail henüz silinmedi. Ve şu anda aynı şirkete iş görüşmesine gidiyorsunuz. Elbette ki bu durumda potansiyel işvereniniz elektronik bilgileri kurcalayarak sizin için küçük bir ön çalışma yapacaktır. Bu nahoş mailin üzerinden yıllar geçmiş dahi olsa hayalinizdeki işi almada şansınız azalmıştır."

Cep Telefonları

İletişim, günümüzde birçok disiplinin terminolojisi içinde yer alan bir kavram olduğu için içeriği de oldukça zengindir. İletişim süreci bireyin ait olduğu toplumdan ve o toplumu yönlendiren uluslararası kurumlardan etkilenmektedir. Öte yandan iletişim süreci bireyin toplumsal yaşamıyla birlikte ortaya çıkmakta, toplumsal ilişkileri yönlendirmektedir(Önür, 2002, s.1).

Günümüzün en yaygın iletişim aracı olan cep telefonlarının tarihsel gelişimine baktığımızda; literatürde "1G", diğer bir ifadeyle birinci kuşak mobil iletişim sistemleri olarak adlandırılan analog mobil iletişim sistemi NMT (araç telefonu), yirminci yüzyılın son çeyreğinde, 1981 yılında kullanıma açılmıştır. Bu sistemler, kullanıcıların zamanla artan ses kalitesi, kapasite, kapsama alanı gibi ihtiyaçlarına cevap vermekte yetersiz kalmış ve "2G" ikinci nesil sayısal teknolojiye geçilmiştir. GSM standartlarındaki cep telefonları 2G kablosuz telefonlarındandır. 2G kablosuz telefonları, 1991 yılında piyasaya sürülmüş ve kullanımı büyük bir hızla yaygınlaşmıştır. Kablosuz telefonların veri iletişiminde kullanımı, günlük yaşamın vazgeçilmez bir unsuru haline gelmesine neden olmuştur. 2000'li yıllar kablosuz iletişim sistemlerinde "3G" üçüncü nesil teknolojilerin kullanımını gerektirmiştir. 3G standartların Uluslararası Telekomünikasyon Birliği tarafından geliştirilmesi ve IMT-2000 olarak adlandırılması ile mobil ve kablosuz iletişimde güncel ihtiyaçları karşılayacak yeni sistemler üretilmiştir (Özkan, 2005, s.17). Günümüzde ise, "4G" olarak adlandırılan "her zaman, her

yerde en iyi ve en hızlı bağlantı" ilkesini amaç edinmiş hücresel telefon sistemleri etkindir. Gelişme sürecindeki 5G'nin çalışmaları ise 2008 yılında Güney Kore'de başlamış ve 2020'li yıllara gelindiğinde, bu teknolojinin dünyanın her yerinde kullanılır hale geleceği tahmin edilmektedir.

Hızla gelişen teknoloji ile paralel olarak kullanıcı sayısında da yıllara göre kayda değer artışlar yaşanmaktadır. Bilgi Teknolojileri ve İletişim Kurumu tarafından yapılan "Elektronik Kimlik Bilgisini Haiz Cihazlara Dair İstatistikler"e göre; 2010 yılında ithalatçı başvurusu ile kayıt altına alınan toplam sayı 14.280.730 iken; bu değer 2013'ün sadece ilk 9 aylık döneminde 10.698.099'a ulaşmıştır. Yine 2010 yılında imalatçı başvurusu ile kayıt altına alınan toplam sayı 894.282 iken; 2013'ü ilk 9 aylık döneminde bu değer 411.800'ü yakalamaya başarmıştır (Bilgi Teknolojileri ve İletişim Kurumu, 2013).

Teknolojide yaşanan bu gelişmelerden toplumlar pozitif anlamda yararlandıkları gibi, ne yazık ki bu durum özgür ve demokratik yaşam biçimini içselleştirememiş ülkelerde; teknolojik sistem ve cihazlarla temel hak ve hürriyetlere müdahale, yaşam kültürü haline dönüştürülmeye çalışılmaktadır.

Cep telefonlarıyla yapılabilen, "dinleme" ve "izleme" olaylarını üçe ayırmak mümkündür:

Trafik İzleme (Kim, Kiminle, Ne Zaman İletişim Kuruyor?)

Cep telefonu işletmecileri; kimin, kimi, ne zaman aradığı ya da kısa mesaj gönderdiği ve kiminle ne kadar süre konuşma yapıldığına ilişkin bilgi sahibidirler. Aynı zamanda, bu kayıtları istenildiği zaman Telekomünikasyon İletişim Başkanlığı'na (TİB) iletmektedirler. Bu kayıtların geriye dönük olarak en az dokuz ay süreyle saklandığı bilinmektedir. Dinleme ve izleme amaçlı olmasa dahi, cep telefonu işletmecileri faturalandırma yapabilmek ve fatura ayrıntısını kullanıcıya da iletebilmek için bu tür kayıtları zaten tutmaktadırlar. CD-R listeleri denilen bu kayıtlar üzerinden geriye dönük trafik takibi yapılabilmektedir. Bu uygulama, bir telefon numarasına sahip kullanıcıyı rahatsız eden aramaların tespiti gibi hukuki anlamda ve insanların iletişim özgürlüğünün korunması açısından gerekli görülmektedir. Bunun yanı sıra, cep telefonları ile trafik takibi, bazı şirketlerin çalıştırdıkları personele yönelik olarak daha kapsamlı yaptıkları dinleme ve izleme sistemleri içerisinde yer alan bir uygulamadır. Cep telefonu içindeki yazılımlarla gelen ve giden aramaların tespiti yapılabilmektedir. Ayrıca

dinleme ve izleme olanağı sağlayan her türlü teknik, cep telefonları ile yapılan görüşme ve yazışmalara ilişkin olarak trafik takibi olanağı da sağlamaktadır ("İletişim Özgürlüğüne Müdahale Raporu", 2009, s. 9).

Konum Belirleme (Kim Nerede Bulunuyor, Kiminle Beraber Bulunuyor? / Yer Tespiti)

Cep telefonu kullanımında kişinin konumunu belirlemek üzere, hangi baz istasyonundan trafiğin gerçekleştiği bilgisiyle yer tespiti yapılabilmektedir. Eğer çok sayıda baz istasyonunun bulunduğu şehir merkezi gibi bir bölgeden arama yapılmışsa mahalle, semt, cadde, sokak hatta bina gibi daha ayrıntılı bir yer tespiti de mümkün olmaktadır. Cep telefonu işletmecileri, ticari hizmet kapsamında bazı şirketlere araç takip sistemleri (fleet management – filo yönetimi) aracılığıyla görüşme ve konum takibi olanağı sağlamaktadır. Bunların dışında cep telefonu işletmecileri yasal bir talep olması durumunda konuşmanın yapıldığı yere ilişkin lokasyon kaydı tutmakta ve TİB'e bildirmektedirler ("İletişim Özgürlüğüne Müdahale Raporu", 2009, s.11).

İçerik Takibi (Kim Kime Ne Diyor?)

Casus yazılımlar, havadan dinleme, ortam dinleme gibi dinlemenin değişik boyutlarıyla, cep telefonları aracılığıyla içerik takibi yapılmaktadır. Casus yazılımı içeren bir cep telefonu, her türlü izleme, kayıt işini yapabilmektedir. Kim kiminle, ne zaman, ne konuştuğu; ne zaman hangi yazılı kısa ileti alımı ve gönderimi yapıldığı, cep telefonuna indirilen dosyalar, cep telefonundan yapılan İnternet erişimleri, bu çerçevede her türlü elektronik iletişim (e-posta, anlık ileti) içeriksel olarak takip edilebilmektedir.

Cep telefonu görüşmelerinin dinlenmesine yönelik olarak anten aracılığıyla havadan dinlemeler de yapmak mümkündür. Belli bir mesafe içerisinde yapılan cep telefon görüşmelerini havadaki GSM elektromanyetik dalgaları bir kodlama programıyla deşifre ederek kaydetmektedirler. Antenlerin ciddi bir mesafede etkin olabildikleri ifade edilirken, bu cihazlarla bölge içindeki çok sayıda cep telefonu görüşmesi kaydı tutabildiği gibi, görüşmelere ilişkin olarak kelime bazlı kayıt tutulması olanağı da bulunmaktadır. Yani içinde belirli kelimeler geçen görüşmeler seçilerek bunun kaydı gerçekleştirilebilmektedir("İletişim Özgürlüğüne Müdahale Raporu", 2009, s. 13).

Sonuç

Bu çalışmada, günümüz toplumunda anahtar bir konu olan "gözetim" olgusu ele alınmaya çalışılmıştır. Çalışma kapsamında; gözetimin tarihsel arka planına, elektronik gözetim araçlarına yer verilmeye gayret gösterilmiştir. Cep telefonları, kredi kartları, bilgisayarlar, internet gibi elektronik gözetim araçlarının incelendiği çalışmada, günümüz gözetleme sistemlerinin gücünü kapitalist pazar ekonomisinden aldığı saptanmıştır. Çalışmada, kişilerin yeni enformasyon teknolojilerinin vaatlerinden yararlanmak istemelerinin, tüketicilerin gözetimini kolaylaştırdığı ve tüketicilerle ilgili kişisel bilgilerin elde edilmesine olanak sağladığı görülmüştür. Fakat her ne olursa olsun, tüketicilerin bu durumu görüp, kabul ettiği gerçeği saptanmıştır. Ne kadar rahatsız edici olsa dahi, masum görünen tüketiciyi etkileme veya tüketicinin kimliğini tasdik etme çabalarına boyun eğildiği gözlemlenmiştir.

Etienne de la Boetie'nin "Gönüllü Kulluk Üzerine Söylev" adlı çalışması durumu özetler niteliktedir:

> *Sizin üzerinizde hakimiyet kurmak isteyen bu kişinin de sadece iki gözü, iki eli, tek bir vücudu vardır, şehrinizdeki yaşayanlar arasından en az bir adamın sahip olduğundan fazla değil; o gerçekten, sizi yok etmek için ona verilen güçten daha fazla bir şeye sahip değildir. Eğer onlara kendininkileri vermezsen, o seni gözetlemek için yeterli gözü nereden bulacak? Senden ödünç almamışsa, seni yenmek için bu kadar çok kola nasıl sahip olabilir? Şehirleri ezdiği ayaklar senin değilse onları nereden aldı? Senin yardımın olmadan senin üzerinde nasıl güce sahip olur? Eğer onunla işbirliği yapmasaydın sana saldırmaya nasıl cesaret ederdi? Eğer sen kendin seni soyan hırsızla dolap çevirmeseydin, seni öldüren katilin suç ortağı olmasaydın, sizler vatan haini olmasaydınız o size ne yapabilirdi? ... Daha fazla hizmet etmemek için çöz ve bir defada kurtul* (Boetie, 1576).

Kaynakça

Bauman, Z. (2001). *Parçalanmış Hayat: Postmodern Ahlak Denemeleri.* (İ. Türkmen,Çev.) İstanbul: Ayrıntı.

Bauman, Z. (2003). *Modernlik ve Müphemlik*. (İ. Türkmen, Çev.) İstanbul: Ayrıntı.

Bauman, Z. (2012). *Yasa Koyucular ile Yorumcular*. (K. Atakay, Çev.) İstanbul: Metis.

Bentham, J. (1995). *Panopticon. M. Bozoviç içinde, The Panopticon Writings.* Londra: Verso.

Bilgi Teknolojileri ve İletişim Kurumu, "Elektronik Kimlik Bilgisini Haiz Cihazlara Dair İstatistikler", http://www.btk.gov.tr/kutuphane_ve_veribankasi/istatistikler/2013-EKBHCDI-9Aylik.pdf.

BOETİE E. (1576). *Le Discours de la Servitude Volontaire*.

Bozkurt, V. (2000)."Gözetim Toplumu ve İnternet", *Birikim Dergisi*, No: 136.

Brown, A. (1998). "Why Geeksare Heroes of Democracy", *New Statesman*, Vol. 127, Issue. 4416.

Dolgun, U. (2008). *Şeffaf Hapishane yahut Gözetim Toplumu,* İstanbul: Ötüken.

Dolgun, U. (2005). *Enformasyon Toplumundan Gözetim Toplumuna: 21. yüzyılda gözetim, toplumsal denetim ve iktidar ilişkileri…* Bursa: Ekin.

Erdoğdu, A. (1972). *Ceza Yargılama Yöntemi Yasası Terimleri Sözlüğü*. Ankara: Türk Dil Kurumu.

Foucault, M. (1995). *Deliliğin Tarihi*. (M. A. Kılıçbay, Çev.) Ankara: İmge.

Foucault, M. (2000). *Büyük Kapatılma*. (I. Ergüden, F. Keskin, Çev.) İstanbul: Ayrıntı.

Foucault, M. (2003). *İktidarın Gözü*. (I. Ergüden, Çev.) İstanbul: Ayrıntı.

Gellner, E. (2006). *Uluslar ve Ulusçuluk*. (B. Ersanlı, G. G. Özdoğan, Çev.) İstanbul: Hil.

Giddens, A. (2001). *Modernliği Anlamlandırmak*. (S. Uyurkulak, M. Sağlam, Çev.) İstanbul: Alfa.

Giddens, A. (2004). *Modernliğin Sonuçları*. (E. Kuşdil, Çev.) İstanbul: Ayrıntı.

Giddens, A. (2008). *Ulus Devlet ve Şiddet.* (C. Atay, Çev.) İstanbul: Kalkedon.

Infomag dergisi, "Coğrafi Bilgi Sistemleri", Infomag Dergisi, 2002, No: 24.

"İletişim Özgürlüğüne Müdahale Raporu" (2009). Elektrik Mühendisleri Odası http://www.emo.org.tr/ekler/6dcc0fceeee647c_ek.pdf?tipi=4&turu=H&sube=0

Laszlo, E. (1992). "Information TechnologyandSocialChange: An EvolutionarySystems Analysis", *BehavioralScience*, Vol. 37, Issue. 4.

Lyon, D. *Günlük Hayatı Kontrol Etmek: Gözetlenen Toplum*. (2006). (G. Soykan, Çev.) İstanbul: Kalkedon.

Lyon, D. (1997). *Elektronik Göz: Gözetim Toplumunun Yükselişi*, (D. Hattatoğlu, Çev.) İstanbul: Sarmal.

Lyon, D. 2013. , *Gözetim Çalışmaları: Genel Bir Bakış.* (A. Toprak, Çev.) İstanbul: Kalkedon

Mathews, J. T. (1997). "Are Networks BetterThan Nations?", *New PerspectiveQuarterly*, Cilt: 14, Sayı: 2.

Mattelart, A. (2012). *Gözetimin Küreselleşmesi: Güvenlileştirme Düzeninin Kökeni*. (O. Gayretli, S. E. Karacan, Çev.) İstanbul: Kalkedon.

McCune, J. J. (1999). "BigBrother is WatchingYou", *Management Review*, Vol. 88, Issue. 3.

Mitchell, William J. (1996). *City of Bits*. Cambridge: MIT Press.

Muchembled, R. (1978). *Culturepopulaire et culturedeselites dans la France moderne*. Paris: Flammarion.

Negroponte, N. (1995). *BeingDigital*. New York: Alfred A. Knopf.

Önür, N. (2002). *Küreselleşen Dünya'da İletişim ve Toplum*, Ankara: Alp Yayınları.

Özkan, A. (2005). "Mobil İletişim Teknolojilerinde Nereden Nereye?", *Genç Bilişim Dergisi*.

Özön, N. (1981). *Sinema ve Televizyon Terimleri Sözlüğü*. Ankara: Türk Dil Kurumu.

Robins, K. (1999). *İmaj: Görmenin Kültür ve Politikası* (N. Türkoğlu, Çev.). İstanbul: Ayrıntı.

Sayar, K. (2002) "Doğunun Hikmeti ile Batının Aklı Birleşmeli", *Infomag Dergisi*, No: 22.

Sencer, M. (1981). *Yöntembilim Terimleri Sözlüğü*, Ankara: Türk Dil Kurumu.

Sungurbey, İ. (1966). *Medeni Hukuk Terimleri Sözlüğü: Osmanlıcadan Türkçeye-Türkçeden Osmanlıcaya*. Ankara: Türk Dil Kurumu.

TDK. *"Büyük Türkçe Sözlük"*. http://www.tdkterim.gov.tr/

Whittle, D. B. (1997) *Cyberspace: The Human Dimension*, New York: W.H. Freeman&Company.

ISSN: 2587-1218

CYBERSECURITY AND HUMAN RIGHTS: NEED FOR A PARADIGM SHIFT?

Nezir AKYEŞİLMEN*

Abstract

This paper analyzes the impact of cybersecurity on human rights with a particular focus on international human rights protection mechanisms. It will focus on the anarchic nature of the cyberspace, its relevance with international relations and the philosophy of international law. It also questions the validity and possibility of traditional state-centric international human rights law for protection of human rights in the cyber domain. Furthermore, it questions whether cyberspace made international relations much more complicated, anarchic and uncertain. Finally the work is going to develop policy proposals and necessary steps for protecting human rights more effectively through some national strategic action plans, regulations and initiatives .

Key words: Cybersecurity, Human Rights, Cyberspace, Anarchy, malware.

SİBER GÜVENLİK VE İNSAN HAKLARI: YENİ BİR PARADİGMA İHTİYACI MI?

Özet

Bu çalışmada, siber güvenliğin insan hakları üzerindeki etkisi uluslararası insan hakları koruma mekanizmaları dikkate alarak analiz edilecektir. Bunun için öncelikle, siber uzayın anarşik doğası ve kendisi gibi anarşik olan uluslararası ilişkiler ve uluslararası hukukun felsefesiyle ilintisi irdelenecektir. Aynı zamanda, siber uzayın uluslararası ilişkileri çok daha karmaşık, anarşik ve belirsiz hale getirip getirmediği de sorgulanacaktır. Ayrıca, siber alanda insan haklarının korunması için geleneksel devlet merkezli uluslararası insan hakları hukukunun geçerliliği ve etkinliği araştırılacaktır. Son olarak, bazı ülkelerin ulusal siber güvenlik strateji eylem planlarına, hukuki düzenlemelerine ve inisiyatiflerine odaklanarak insan haklarının daha etkin korunabilmesi için atılması gereken adımlar ve öneriler üzerinde durulacaktır.

Anahtar kelimeler: Siber Güvenlik, İnsan Hakları, Siber Uzay, Anarşi, Zararlı yazılım.

Login

Technological developments have affected, accelerated, changed and transformed human life as well as communication and interactions between human beings thorughout history. Today

* Assoc.Prof.Dr., Department of International Relations, Selcuk University, Konya-Turkey. The author can be reached via e-mail: nezmen@yahoo.com or twitter@nezmen.

people can communicate and make trade easily without taken into consideration the borders and distances as a result of developments in telecommunication and information technologies. The thing that makes these interactions and communication possible is cyberspace that consists of hardwares, softwares, electronic data and global nertworks. Cybersapace, "is apparently dominateing social life day by day" (beceni, 2008). Unlike physical spaces such as air, land and sea the cyberspace has been created by human beings and it has a tremendous effects on our life including politics in general, human rights and freedoms in particular. Yet, how far it is possible to set up a balance between the right to life, liberty and security in this new space?

Login in virtual reality - the cyberspace - has been the issue of 50 years, however, the questions it raises about security and human rights remains a relatively new phenomenon (Australian Human Rights Commission, 2015:5). It has affected international relations in many respects including peace, security, instability, trade and human rights. Therefore, is has been a problematic issue in the sense that who is going to control it? or should it be controlled? "Cyberspace has created both great opportunities for, and serious threats to, states and non-state actors. This has led to a common understanding that behaviour pertaining to the use of information and communication technologies (ICTs) has to be limited in order to prevent conflicts that endanger international peace and security" (Osula and Roigas, 2016:11). Created as an open, transparent and information-sharing platform, cyberspace, beginning in the 1980s, has faced malicious activities and security problems. Since the appearance of Elk Cloner (the first computer virus) in 1982 (Landesman, 2011), types of malicious programs and the concepts related to cybersecurity have been developed tremendously. Today cybersecurity is one of the uppermost issues of the individual, national and international security agendum. Almost 40% of the world population that corresponds to 3.4 billion people has internet connection around the world (Internetlivestatas,2016) and more than 30% of computers in the world are infected with malware (Dottech, 2013).

There are numerous malwares and cyber attacks that effect computers differently. As pointed out by Green and Rossini (2011), "Threats to cyber security can include computer viruses, spam, identity theft, data breaches, denial of service attacks, and cybercrime, and attackers can range from hackers to activists to petty criminals to businesses to national governments"(Green and Rossini, 2011). Cyber security threats are not limited to malicious programs, on the contrary they are quite divergent, including physical offences. Hence these

threats go beyond the security of individuals and companies. National critical infrastructure, such as e-state agencies, energy, electricity, transportation and financial institutions are among top targets of cyber attacks. "Indirect and non-military threats just as the targets of physical warfare are the machinery of state, financial institutions, the national energy, transport infrastructure and public morale, so too are they the prime targets in cyber warfare (Cornish, 2010:6).

Cyberspace, as a new and a distinct space provides every and each actor in the space with different threats and opportunities. As the USA Policy Review puts forward: "Cyberspace touches practically everything and everyone. It provides a platform for innovation and prosperity and the means to improve general welfare around the globe. But with the broad reach of a loose and lightly regulated digital infrastructure, great risks threaten nations, private enterprises, and individual rights (The White House, 2009:i)".

The relationship between human rights and cybersecurity has been twofold: creating a secure cyberspace for all the users and also a safe environment for human rights in the cyber domain. These two relatively new realities, namely cybersecurity and human rights, are deeply interrelated and interconnected. We cannot have one without the other in the cyberworld. Thus, we need to develop an international mechanism that would be able to provide both. For such a global and reliable mechanism, a number of questions need to be answered:

What is cybersecurity? Is a secure cyberspace possible? Do we have adequate and/or accurate national and international instruments, regulations, standards and policies to withstand cyber threats? What sort of regulations, institutions and policies have national governments developed for cybersecurity? What are the similarities and differences between the anarchic nature of international relations and the anarchic order of the cyberspace? What kind of role does human rights concerns play in designing national mechanisms, such as national action plans, cyber army, cyber institutions etc.? What are the sources of vulnerability for online human rights? Which human rights are being directly threatened by cyber attacks? What are the core human rights apprehensions when dealing with cybersecurity? Are cyber security and human rights reconcilable?

Dealing with all these and many more questions in the cyber domain has become one of the new and unfamiliar issues in international relations. Henceforth, cyber threats targeting critical infrastructures, governmental espionage, and national confidential information etc. has made cybersecurity a top priority of national security agendas. National governments have been developing documents and initiatives such as national action plans to survive in the cyberdomain and provide their critical infrastructures and citizens with cybersecurity. As powerful actors, states are not only security providers in the cyber realm, but also security threats particularly when it comes to human rights and freedoms.

This research will be initially focusing on the nature of the cyberspace, how it has been conceptualized, its components, and its similarities and differences with the anarchic international system. Then it will analyze the relationship between cybersecurity and human rights. Finally, before the concluding remarks, it will end up with online human rights and the human rights dimensions of national policies and initiatives related to the cyber domain.

Cyberspace and Its Anarchic Nature

Being a newer issue in general, and in international relations in particular, the conceptualization of cyberspace and cybersecurity remains contested and undecided, along with other terms related to cyberspace including information security, critical infrastructure, cybercrime, cyberwarfare, cyberthreat, hacktivism, cyberpolitics etc... Therefore, they mean different things to different persons or disciplines. Scientific research, for the sake of clarity and accuracy, needs working definitions for the concepts it uses. On that account, the phenomenon of cyberspace and cybersecurity will be thoroughly investigated in the proceeding section.

Cyberspace: Virtual or Real?

Human beings were able to use two physical spaces, namely the land and the sea until the very end of the 19th century. Then the third one, the aerospace was added, but it was primarily used for military purposes. Then in late 1950s the fourth physical space, outer space, was added to the mix. "Each of these four physical domains is marked by radically different physical characteristics, and they are usable only through the use of technology to exploit those characteristics". Finally, through human exploration, the fifth space was added,

the cyberspace which has dissimilar characteristics than the previous four physical spaces (Kuehl,2009). The last three spaces were developed initially for military purposes, then they spread out to incorporate economic, social and political issues.

The concept of *cyber* has been a very usable adjective in daily language and in academic literature in the last two decades. cyberspace, cybersecurity, cyberpolitics, cyberlaw, cyberconflict, cyberethics, cyberpower, cyberdeterrence, cybersurveilence etc. Indeed, "In recent years the term "cyber" has been used to describe almost anything that has to do with networks and computers" (Ottis, 2016). The term *cyber* evolved from the work by Norbert Wiener in 1948, while the concept of Cyberspace was used first time by William Gibson in his science fiction titled as Neuromancer in 1984 (Moen, 2010). Gibson describes cyberspace as a:

> *consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding... (1984).*

This definition is still valid today, but many would argue that it is incomplete. There is no universal or widely agreed on definition for cyberspace, yet a bulk number of thinkers have offered useful insights that have helped shape thought on this issue in the last quarter century. Kuehl for example, posits a comprehensive definition for cyberspace that encompasses many dimensions of the cyber realm. He defines cyberspace as "an operational domain whose distinctive and unique character is framed using electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interconnected information-communication technology (ICT) based systems and their associated infrastructures" (2009:4). His definition focuses on inputs, processes and the structure of the cyberspace that comprises both software and hardware. Yet still there are some missing components of the cyberdomin in this comprehensive definition. Laying out the central concepts for cyberspace and to suggest definitions that capture correctly the logic behind these concepts is not an easy task.

Almost all definitions suggested so far have some missing points, such as the user.i.e. human being. In this respect, IOS and TCP/IP layering reference models in computer science can help us to enshrine an arrange of cornerstone upon which a reliable and all-inclusive

definition can be built. Since networking is a very complex phenomenon, it needs to be divided into components in order to be better worked out. Thus, the layering model "aids this division and provides the conceptual basis for understanding how software protocols together with hardware devices provide a powerful communication system." (Z-World, 2001:15). Indeed, the layering model, helps to understand the components of the internet and their specific functions on each layer. Layering model of IOS and TCP/IP divide the internet into seven and four (Pathfinder, 2011:2) units respectively. The units of IOS reference model are application, presentation, session, transportation, network, data link and physical ones while the constituents of the TCP/IP are application, transport, internet, network and physical (Z-World,2001:15). A more inclusive definition of cyberspace requires the incorporation of all of these layer units and more. Pathfinder describes cyberspace as " a virtual domain, similar but discretely different, to the physical domains of air, sea, land and space. [It] has four distinct components— Information, Physical Systems, Cognitive Actions, and People. • People and their manipulation of information are central to conducting operations in cyberspace (Pathfinder, 2011,p.2). Therefore, a more precise definition of cyberspace should take into consideration an enlarging spirit of perpetually changing decisions and information, caused by the interaction of users, information, cognitive logic and physical infrastructure of the internet (Pathfinder,2011:2).

Numerous definitions have evolved for cyberspace over the years. National cybersecurity strategies of different countries have different definitions for the cyberspace. National Cybersecurity Strategy 2016-2019 of Turkey defines cyberspace as, "The numeric environment composed of information systems spread over the entire world and space, the networks interconnecting these systems or independent information systems" (UDHB,2015:7). This definition focuses on hardware and data, while The UK Cybersecurity Strategy paper includes other information system that support business, infrastructure and services: "Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services" (United Kingdom,2011a:11).

Germany and Japan's cybersecurity strategy documents stess the global nature of cyberspace and interconnectedness of the networks. German strategy documents define cyberspace as, "the virtual space of all IT systems linked at data level on a global scale. The basis for

cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks" (Germany,2011:9). According to Japan cybersecurity strategy, cyberspace states, "global virtual spaces such as the internet, composed of information systems, information communications networks and similar systems and which circulate large quantities of a large variety of information, have rapidly expanded and begun permeating real-space" (Japan,2013:5).

National Strategy Framework of Italy includes the artifiality of Cyberspace, suggesting it is a "man-made domain essentially composed of ICT nodes and networks, hosting and processing an ever-increasing wealth of data of strategic importance for States, firms, and citizens alike, and for all political, social and economic decision-makers" (Italy,2013:9). The US Department of Defense, for example, calls cyberspace “A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers” (Department of Defence, 2010:58). Almost all definitions bring up the physical component, hardware and even software but fail to include the application, user or the human component.

As put forward by some of the defitions above, Hathawey and Clinburg affirms that "Cyberspace is more than the internet, including not only hardware, software and information systems, but also people and social interaction within these networks" (Hathaway and Climsbur, 2012:8). The European Information Society Dictionary decribes the term cyberspace as “It describes the virtual space in which the electronic data of worldwide PCs circulate"(ComputerDictionaries, 2016). It's comprehensible that this definition also focuses on data and network and even physical infrastructure can be inferred from wording but human copmponent is missed. Unlike other four physical spaces, "cyberspace is man-made and an ever-expanding environment, and that therefore the definitions are also constantly changing"(Hathaway and Klimsbur, 2012:9).

People and information are the central to the cyberspace. Other important feature of cyberspace is that it is being driven largely by private actors and unlike physical spaces, it has no boundries. It's for the most part a virtual domain and as Pathfinder expostulates it "is not physically identifiable in the natural world while the other domains are clearly recognisable. It

is essentially a networked terrain that has no geographic boundaries. Further, it is largely owned and operated by private sector entities, many of them multinational corporations"(Pathfinder, 2011:1).

Cyberspace is far larger than imaged. It's constantly expanding and dynamic. Therefore, the concepts related to it are also invariably changeing and snowballing.

The Nature of Cyberspace: Decentralized and Anarchic

Cyberspace is "essentially a networked terrain that has no geographic boundaries. Further, it is largely owned and operated by private sector entities, many of them multinational corporations"(Pathfinder, 2011:1). It empowers the individuals rather than the states. It's claimed that government has no chance to control or manage the internet. John Perry Barlow assertively states that "I declare the global social space we are building to be naturally independent of the tyrannies you [the governments] seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear (Wu, 1997:649; Lewis, 2013:1)). The cyberspace system runs exclusively by private actors and the state system is a late comer in this domain - private sector run it, nonprofit and for profit involve, state want to catch up, development of groups and firms that promote anonymity and rate at which use access goes up. In physical world state dominate but in cyber world no one control but private individual and private actors are effective. In general, systems like internet that are “open” seem to be associated with weak or decentralized control, and limited allocation of power to one actor (Clark, 2010:1). Cyber world with multi-stakeholders is enlarging and getting complicated day by day, but there is contention over future management: who will govern cyberspace? This question leads to the idea of cybersecurity.

Cybersecurity or Cyberinsecurity?

After discussing the conceprt of *cyberspace* it is essential to define the security in the context of cyber realm. The term cybersecurity is even much more ambiguous than the cyberspace. Although, term cybersecurity has been widely used by cyber literature in the recent years, it lacks a proper definition. It meant different things to different persons (Akyeşilmen, 2010). It fits to different agendas. Anja and Hawtin verify this reality by claiming that:

> *At present, the term "cyber security" lacks definition as it is used to cover a vast range of concerns: in different contexts and by different actors the term is used to refer to security of national infrastructure; security of Internet infrastructure; security of applications and services; security of users (ranging from businesses to individual users); to the stability of the State and of political structures. This inexact terminology points to one of the primary concerns about this growing discourse: the terminology covers an agenda which is inexact, mixes legitimate and illegitimate concerns and conflates different types and levels of risk. This prevents genuine objective scrutiny, and inevitably leads to responses which are wide-ranging and can easily be misused or abused (Kovacs and Hawtin, 2017:2).*

As mentioned above cybersecurity has a definition problem. The Organization for Security and Co-operation in Europe (OSCE) funded a project called *the Global Cyber Definitions Project* which is designed to collect existing definitions on cybersecurity (Cyberdefinitions, 2016). For the sake of working definition we will focus on several of them. National Cyber Security Strategy-2 of Netherland describes cyber security as the "efforts to prevent damage caused by disruptions to, breakdowns in or misuse of ICT and to repair damage if and when it has occurred. Such damage may consist of any or all of the following: reduced reliability of ICT, limited availability and violation of the confidentiality and/or integrity of information stored in the ICT systems"(Netherland, 2016:7).

The European Union (EU) defines cybersecurity as "the safeguards and actions available to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure"(Europa, 2016).And International Telecommunication Union(ITU) defines it as the "collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets (ITU, 2016).

The US national strategy defines cybersecurity as the "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" (Department of Defence, 2010:57). Fenz puts emphasizes the social aspect of security in the cyber world: "Not only the technical view of cyberspace security has to be considered, also the social aspect is an important one. A lot of damage is caused by social engineering. In such a case the attacker is not hacking a system;

he simply asks the victim for his password or uses another social engineering method to gather user credentials (Fenz, 2016:4).

National cybersecurity strategy documents of several cyberpowers also define cybersecurity in terms of protecting internet compenents. For instance, Information Systems Defence and Security of France lays stress on the availibility, integrity and confidentiality of the services: "The desired state of an information system in which it can resist events from cyberspace likely to compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible" (France, 2011:21). While the UK describes it as "to defenses against electronic attacks launched via computer systems"(United Kingdom, 2011b:1). Almost all these definitions focus on the defence and policies for resisting cyber attacks. Almost none is defining cybersecurity.

The USA Cyber Policy Review (2009:iii) discusses it in a rather long text and highlights numerous policies, activities and operations going on on the internet. It underlines that;

> *Cybersecurity policy includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. The scope does not include other information and communications policy unrelated to national security or securing the infrastructure.*

Last but not least, it is essential to look through definitions shown fort by national cybersecurity strategies of Estonia and Turkey. Estonia cybersecurity strategy aims primarely "to reduce the inherent vulnerabilities of cyberspace in the nation as a whole (Estonia, 2008:5). Turkey's definition however, takes head of confidentiality, integrity and availability of information and counter measures against cyber attacks. It describes cybersecurity as the "Protection of information systems forming cyber space from attacks, assuring confidentiality, integrity and availability of information/data processed in this environment, detection of attacks and cyber security incidents, activation of counter-response mechanisms and recovering systems to conditions prior the cyber security incident"(UDHB, 2015:10).

It comes out clearly from the quotations afore that there is not an internationally agreed definition of cybersecurity. Almost each state and each international organization has its own definition which also increases the level of vulnerability. Indeed, it is also inferred from the aforementioned discussions that the concept of cybersecurity is taken for granted. What we really mean when we address the term cybersecurity? The defitions lay out the measures and policies to be taken against cyber threats instead of describing it. The most vital question to be asked is whose security? But the definitions commonly harp on security of what? Rather than whose security?

Whose security by enunciating term cybersecurity, we make sense of? Is it the state, company, individual or all? National cybersecurity strategies evidently give the state priority. But is it possible to have cybersecurity to cast out any stakeholder of the cyberspace? Can a stakeholder be proivded with security without the others in cyber realm? or simply is cybersecurity ever possible?

A documentary on Animalplanet asserts that "none of the babies is safe in savanna[1]" whether it belongs to a lion, a tiger, antelope, zebra or gazelle"(AnimaPlanettv, 2016) Because “no one can be sure about the real intension of their neighbours"(AnimaPlanettv, 2016). The same rule is valid for the cyberspace. No one is safe in this realm. Since none can be sure about the real intention and the power of their neighbours (everyone is neighbour on the net). It is pontificated that globalization has transformed the world into a global village.[2] But now, the internet has converted the world into a an apartment that makes everyone (every netizens) neighbours to each other.

If we continue with a similar methaphor from the wild life, despite security threats we shall go on using the internet. Just because the internet is not just about in/security but also it is about the opportunities and benefits. When the immigration season arrives more than 200 thousand antilopes can are organized and start their journey. They get out for a very dangerous voyage. Thousands of them are unable to finish the journey. They do not give up travelling in fear that

[1] A **savanna** or **savannah** is a mixed woodland grassland ecosystem characterised by the trees being sufficiently widely spaced so that the canopy does not close.

[2] "The term global village was coined in the 1960s to describe how human beings are increasingly connected by electric (or electronic) technologies, which virtually eliminate the effects of space and time so that the globe contracts into one interconnected, metaphorical ‘village" in Gibson, T and Murray, S.J., "Global Village", in Danesi, M. (ed), *Encyclopedia Entry in Encyclopedia of Media and Communşcation,* Toronto: University of Toronto Press, 2012, p.312.

it is hazardous and risky (Animaux,2016). One might as well say that, we should not give up using internet thinking that it is dengerous and risky.

Cyber Attacks: A Real Threat or Theatrical?

Cybersecurity is a reality and a fact of daily life. But until very recently the states did not give too much attention to the internet and considered it as a matter of low politics and/or a business of private sector. But today they consider it as a national security issue and rush to catch up as Choucri and Clark (2012:2; Lewis, 2015:1) asserted.

> *Until recently cyberspace was considered largely a matter of low politics – the term used to denote background conditions and routine decisions and processes. By contrast high politics is about national security, core institutions, and decision systems that are critical to the state, its interests, and its underlying values. We now see cyberspace shaping the domain of high politics, and high politics shaping the future of cyberspace. The field of international relations, rooted in 20th century issues and theories, has not kept pace with the emerging significance of cyberspace.*

Cyber insecurity is a natural part of our daily life in the cyber age. In this new virtual space we face a range of threats and attacks from diverse and many times unknown sources. Maurer and Morgus (2014:72) lay emphasizs on the obscurity of their sources, ambiguity of their targets and their complicated nature by asserting that:

> *Threats in cyberspace are difficult to define as it is hard to identify the source of attacks and the motives that drive them, or even to foresee the course of an attack as it unfolds. The identification of cyber threats is further complicated by the difficulty in defining the boundaries between national, international, public and private interests and actors. Because threats in cyberspace are global in nature and involve rapid technological developments, the struggle to meet them is ever-changing and increasingly complicated. It requires high-level training, an advanced legal framework, effective organisational co-operation and the allocation of considerable resources.*

There exist a sequence of threats and risks in cyberspace. It's designed not-for security but for transparency and information sharing. The creators of internet, initally did not think about security. Thus, the nature of cyberspace is open to attacks. There exist somewhat abundant types of attacks in the cyber domain. But before we discuss types of attacks, it is necessary to describe them. US Department of Defence defines cyber attacks as "Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves" (United States of America,2011:75). While National Strategic Framework of Italy designates them as "Activities that are conducted in and through the cyberspace in order to manipulate,

obstruct, deny, downgrade or destroy information stored in the ICT networks or in the computer systems, or the ICT networks or in the computer systems themselves" (Italy,2015:41).

United Kingdom Parliamentary Office of Science and Technology higlights the types and motives behind cyber attacks. It pictures them as "the term cyber attack can refer to anything from small-scale email scams through to sophisticated largescale attacks with diverse political and economic motives. Large-scale attacks may have a number of interrelated aims such as: gaining unauthorised access to sensitive information; causing disruption to IT infrastructure; or causing physical disruption (e.g. to industrial systems)" (United Kingdom, 2011b:1).

Types and quantities of cyber attacks are multiplying day by day. They are increasing in volume, sophistication, and coordination and they are attracted to high-value targets. For instance energy, transportation, communication, water and sanitation, finance, industrial processes and government administrations. There is a wide variety of cyber attacks.[3] Such as intrusion detection[4], defacements, domain name server attacks, distributed denial of service attacks(DDoS)[5], device compromise[6], data exfiltration[7], bad data injection[8], viruses[9], trojan horse[10], botnets[11], social engineering[12], logic bomb[13], time bomb[14], worms[15], rootkit[16], routing

[3] The following definitions are withdrawn from both ISACA, Cybersecurity Fundemantals Glossary, 2016, pp.1-35. http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_ glossary.pdf [Accessed on 29.12.2016] and Lu, Miao and Reevese, Jason, *Types of Cyber Attacks, UNDAVIS, 2014*, https://tcipg.org/sites/default/files/rgroup/tcipg-reading-group-fall_2014_09-12.pdf [Accessed on 29.12.2016].

[4] The process of monitoring the events occurring in a computer system or network to detect signs of unauthorized access or attack

[5] An assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate.

[6] To obtain total control of a device.

[7] To steal sensitive information from a target.

[8] To submit incorrect data to a system without detection.

[9] A program with the ability to reproduce by modifying other programs to include a copy of itself Scope Note: A virus may contain destructive code that can move into multiple programs, data files or devices on a system and spread through multiple systems in a network.

[10] Useful program containing hidden code that, when invoked, performs some unwanted or harmful function.

[11] It is typically planted on thousands of computers belonging to unsuspecting third parties. Often used to launch denial-of-service (DoS) attacks.

[12] tricking users to assist in the compromise of their own systems or personal information. Usually in the form of Spam E-Mail.

[13] Code embedded in the malware that is set to execute when certain conditions are met.

[14] Triggers action when specified time occurs.

[15] A programmed network attack in which a self-replicating program does not attach itself to programs, but rather spreads independently of users' action.

[16] A software suite designed to aid an intruder in gaining unauthorized administrative access to a computer system

operations, critical infrastructures[17], cyber espionage, compound attacks. These attacks are for the most part goes up by classic hackers, mercenary hackers, hacktivists, script kiddie, rogue insiders and nation-states(Levy,1994).

To sum up, in cyberspace there is hardly cybersecurity but rather cyber insecurity. IT's resembling a crystal house. Everyone (indeed expert ones) is able to follow one's moves and actions on the net. They can easily intervene and launch a cyber attack. This is dues to the nature of cyberspace.

Cybersecurity has been one of the vital questions in recent years for all the stakeholders of the internet. As the risks and threats increased the security concerns of the users - potential targets - also goes up. The focal point is that anything networked can be attacked and hacked. The bad thing is that everything is being networked. Thus everything is vulnerable. Yet worse still, there is no solution, no ample technology and no global agreement for a secure cyberspace.

Cybersecurity and Human Rights

In the beginning, the internet was often described as a utopian term for the promotion and protection of human rights. It represented a freedom of domain that would liberate all knowledge, empower the people, and weaken the state by making it more transparent and accountable, leading to the realization of democratization and human rights. Yet, PoKempner claims that "These heady days are largely past, and a grimmer appreciation of the threats facilitated by cyberspace and the attacks possible against a secure and free use of cyberspace is prevalent. Private and state actors vie to control and monitor electronic communications, posing serious challenges to the idealistic view of a global commons"(PoKempner, 2013:259).

Governments try to develop documents and initiatives at the national level including national strategic action plans and institutions for the cybersecurity. Most of these documents are based on traditional (realist indeed positivist) understanding of international relations and national security perception. But what governments need at this stage, is a new

[17] Systems whose incapacity or destruction would have a debilitating effect on the economic security of an enterprise, community or nation.

understanding that is compatible with the cyber philosophy. To catch up with the virtual reality, national strategic action plans and initiatives need to frame the key issues concerned and identify the important questions in addressing cyber issues, balancing human rights with national security considerations, and developing the international cooperation needed to address cyber threats. Because it is a completely new realm and therefore, in order to cope with it and related problems, we need new tools and measures. Richard Clarke explains this new situation by focusing on cyber conflict arguing that 'cyber war is a wholly new form of combat, the implications of which we do not yet fully understand'. Cyberspace has merely extended the battlefield and should be viewed as the fifth battlespace alongside the more traditional arenas of land, air, sea and space (Cornish,2010:11). Being aware of this, some countries have tried to develop policies, initiatives and take some measures.

The USA, Russian Federation, China, Germany, Israel, the European Union(EU), Japan, Vietnam, Turkey and many more countries that are being target online the most[18] declared cybersecurity issue particularly cyberattacks on their governments and citizens as national security threats and have taken some measures such as national strategic action plans, initiatives and introducing new laws. "Such cybersecurity initiatives and strategies normally outline the country's primary goals, concerns, set of principles or norms, and actions to be taken related to cyber security. Initiatives also can set up the creation of new agencies to deal with cyber security domestically or outline the role of already existing agencies, such as law enforcement, military, defense and foreign affairs ministries, in implementing cyber security policies"(Green and Rossini, 2011:3). Developing new initiatives and action plans seems to be a creative idea, but do they work? Is it possible for states to create a secure cyber environment alone? Or do we need a global cooperation to succeed? Or all these regulations and initiatives securitize cyberspace which is also a serious threat to human rights? Is securitization of cyberspace worsening the situation?

Some Weak Trials for Global Internet Regime

Despite having various approaches with different understandings of international relations, the international system is being constructed on the notion of nation-states. Nation states are the main actors of the system, if not the only ones. Being anarchic i.e. non-existence of a

[18] For cyberthreats real time map see. https://cybermap.kaspersky.com/(Last visit: 15.06.2016).

global government makes the interstate relationships fragile and leaves the international law without enforcement. Anarchy in international relations prioritized role of power in internation al relationas and requires the primacy of security in political life (Donnallly, 2000, pp.9-13). Therefore, the application of the international law is based on the consent of the states. Thus, if the sates cooperate and agree on basic international values and standards, there is possibility to have a secure international environment in which protecting human rights is relatively possible.

Globalization process has brought new actors or non-state actors such as Transnational Companies (TNCs), intergovernmental organizations, transnational religion communities, NGOs and armed groups in international relations who also violate human rights. These actors have been violating human rights across the globe - despite the existence of different approaches with different views on their human rights responsibilities - but the valid international law is claimed not to be binding on them (Akyeşilmen, 2009). Usually these actors were able to escape from responsibility due to deficiency in international law, the principle of territoriality of national laws and limits of jurisdiction. Therefore, they escape from responsibility and make human rights much more vulnerable in the globalization era. Yet, despite, all these difficulties human rights are being promoted and protected at the international level to some extend as long as the states cooperate.

International relations is getting more and more complex and complicated day by day. Therefore, old strategies and policies sometimes can be impractical. One of the main characteristics of the international structure is that it is based on states' physical boundaries and jurisdiction. However, being decentralized and anarchic in nature, the cyberspace has no boundaries, no clear jurisdiction and no one single actor being predominantly deterministic at the system level. Many private actors are much stronger than many states in terms of managing and manipulating the domain. Furthermore, many individual hackers are able to launch as destructive attacks as the states and/or companies do. Therefore, unlike the real world, we have much more equivalent multiple actors or stakeholders conducting activities in the cyber world. Having no boundaries and being open to attacks the cyberspace, leave human rights with less or no protection. There are many actors that can violate human rights of anybody from any part of the world and escape from their international responsibilities. States and non-state actors (indeed, it is also questionable to use the concept of non-state actors in cyber domain because the system is not a state-centric anymore) can and do often

violate human rights online and so far there is no agreed international standards to apply these cases. There are no international hard law regulations except for some regional initiatives such as the Council of Europe Convention on Cybercrime (Coe, 2001).

There have been some attempts initiated by Russia and China at the UN level for an international code of conduct for information security but there is no concrete outcome so far. There have been some soft law regulations but their effectiveness is being questioned. Another international attempt was initiated by the ITU in 2007, when it adopted a Global Cyber Security Agenda as a framework for international engagement between Member States on cybersecurity issues (Green and Rossini, 2011:6). Some regional intergovernmental organizations such as NATO and OSCE have adopted some principles and urged member states for cooperation on capacity building, combating cybercrimes and applicability of international law including human rights. Likewise, there have been some attempts at the Europe, Asia, Africa and Latin America regions (Green and Rossini, 2011:5). Despite all these constructive efforts, there is unwillingness at the international level for cooperation on cyberspace and protecting human rights. Even if there is a strong cooperation, is it possible to protect human rights in cyberspace with the existing state-centric paradigm of international relations? This is a crucial question that needs to be addressed.

Towards a Secure Online Human Rights?

Cyberspace has been used as a platform to promote and protect human rights globally but, it is also being used to limit and even violate them. Technology is neutral; it can be used for bad or good. Thus, so far we have witnessed both regarding human rights.

All human rights guaranteed primarily by International Bill of Human Rights which consist of the Universal Declaration of Human Rights (UDHR-1948), the International Covenant on Civil and Political Rights (1966) and International Covenant on Economic, Social and Cultural Rights(1966) and other basic international human rights treaties (OHCHR, 2016). Freedom of expression, right to privacy, freedom of speech, freedom of association and right to security and liberty are the core human rights that are directly related to cyber world. "Access to cyberspace, and freedom to communicate and receive information online, are enabling, lynchpin freedoms, important not just in themselves, but as necessary conditions

for the realization of a much wider set of human rights. Cyberspace technologies have not only placed the realization of many fundamental rights within the reach of many more people, but the exercise of these rights is increasingly dependent on the protection and safeguarding of the internet and, in particular, the internet as a domain of freedom"(PoKempner, 2013:259). UN Human Rights Council on its 20th session shortly and clearly stressed that "The same rights that people have offline must also be protected online"(UN Human Rights Council, 2012), because "Access to information is not only a right in itself, but is also a necessary condition of the fulfillment of many others"(POkEmpner, 2013:246).

Electronic surveillance and limiting access to internet are the leading sources of human rights violations on the web. As mentioned above, states are not the only actors which violate human rights online but also other stakeholders have the capacity to violate them. In cyberspace there is a three-fold Surveillance. i.e. governments can watch citizens and citizens can watch governments or citizens can watch each other. Therefore, there is the problem of privacy: who control all data? What we can do? There is no a clear answer. Since technology works for openness and transparency, indeed privacy is in danger. But there are some international attempts to decrease risks and threats online. International Principles on the Applications of Human Rights to Communication Surveillance sets up the criteria in determining when the electronic surveillance is legitimate.

> *Privacy is a fundamental human right, and is central to the maintenance of democratic societies. It is essential to human dignity and it reinforces other rights, such as freedom of expression and information, and freedom of association, and is recognized under international human rights law. Communications Surveillance interferes with the right to privacy among a number of other human rights. As a result, it may only be justified when it is prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued (NecessaryandProportinate,2016:2).*

Human rights and cybersecurity are also under threat from all internet stakeholders who exploit the cyberpower for their personal benefits or the sake of political or national security. But, at the same time, "Attacks that threaten online communications and networks, and the rights these enable, will activate a State's responsibility to protect. The State is constrained by international law in its response, under principles of necessity and proportionality which are common to both human rights and humanitarian law"(PoKempner, 2013:242). These international regimes are applicable to both physical and cyber world. But the problem is that state responsibility with regard to human rights protection is limited with its territory and

jurisdiction. But in practice much of cyberattacks and malicious activities have transborder character.

Therefore, it's hard to control the internet and attempts to do so will only make things worse. The cyber world is an unknown domain with actors, rules and borders that have completely different powers than the real world. In order to have a cybersecurity and well protected human rights we might need a new (social) contract.

It can be inferred from the analysis above that the state-centric international system is hardly applicable at the cyber level. Thus, there is a need for an international order and international law that is binding, not only on the states, but also on individuals and private companies. Having binding regulations on all cyberspace actors is also not enough for the promotion and protection of human rights in this new domain, but it also needs to be enforced at the global level. Thus there is a need for a global enforcement body that goes beyond the nature of anarchic international order. But how? Indeed, the bigger question is, what should the new social contract be? The answer for this question will most probably determine the future of human rights and cybersecurity.

How do current theories of international relations and international law correspond to this need? Which theory best fits to the cyber realm? State-centric theories or theories with multiple actors? Or for a safer cyberspace and human rights do we really need a paradigm shift in international relations?

REFERENCES

Akyesilmen, Nezir.(2009). *Who is Responsible for Human Rights: The State or Corporations.* Ankara: orion Kitabevi.

Akyeşilmen, Nezir.(2016).Siber Güvenlik ve Özgürlük. http://www.ilksesgazetesi.com/yazar/siber-guvenlik-ve-ozgurluk-3816.html [Accessed on 27.12.2016].

Animal Planettv.(2016). Documentary titled as Queens of Savannah. 21.08.2016, time: 13.50-14.40.

Animaux.(2016).Africa Dream., 16.09.2016, time: 16.55-17.40.

Australian Human Rights Commission.(2015). *Background Paper:Human rights in cyberspace,* September, https://www.humanrights.gov.au/sites/ default/files/document/ publication/human_rights_cyberspace.pdf [Accessed on 24.12.2016].

Beceni, Yasin.(2008).Siber Uzay Kavramı ve Toplkumsal etkileri. http://bilgitoplumuhukuku.blogspot.com.tr/2008/09/bilgi-ve-iletiim-teknolojileri-hukuku_8713.html [Accessed on 111.01.2017].

Choucri, Nazli and Clark, Clark (2012). *Integrating Cyberspace and International Relations: The Co-Evolution*, Boston: MIT Working paper-29.

Clark, David.(2010).Characterizing Cyberspace: Past, Present and Future. available on https://projects.csail.mit.edu/ecir/wiki/images/7/77/ Clark_Characterizing_cyberspace_1-2r.pdf[Last visit: June 17, 2016].

CoE.(2001).Convention on Cyber Crime.available at http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf [Last access: 21.09.2016].

ComputerDictionaries.(2016). Cyberspace. available at http://www.computerdictionaries.org/GT/TCP/cyberspace [Accessed on 25.12.2016].

Cornish, Paulet.al. (2010). *On Cyner Warfare,* London: Chatham House.

Cyberdefinitions.(2016).Global Cyber definitions Database. http://cyberdefinitions.newamerica.org[Accessed on 27.12.2016].

Department of Defence.(2010). *Dictionary of Military and Associated Terms.* http://www.dtic.mil/ doctrine/new_pubs/jp1_02.pdf[Accessed on 25.12.2016].

Donnelly, Jack. (2000). *Realism and International Relations.* Cambridge: Cambrigde University Press.

Dottech. (2013). 32% of computers around the world are infected with viruses and malware, according to Panda Security. https://dottech.org/96627/32-of-computers-around-the-world-are-infected-with-viruses-and-malware-according-to-panda-security/(Last visit: June 16, 2016).

Estonia.(2008).*Cyber Security Strategy*.

Europa. (2016).Glosary. available on https://ec.europa.eu/digital-single-market/en/glossary#c (Last visit: June 17, 2016).

Fenz, Stefan.(2016).,Cyberspace Security: A definition and a description of remaining problems. available at

http://www.univie.ac.at/frisch/isegov/aushaengUniWien/CyberpaceSecurity_Fenz.pdf[Accessed on 25.12.2016].

France.(2011).*Information Systems Defence and Security: France's Strategy.*

Germany.(2011). *Cyber Security Strategy for Germany*.

Gibson, T and Murray, S.J.(2012).Global Village. in Danesi, M. (ed), *Encyclopedia Entry in Encyclopedia of Media and Communşcation,* Toronto: University of Toronto Press.

Gibson, William.(1984). *Neuromancer,* New York, Ace Books.

http://project.cyberpunk.ru/lib/neuromancer/ [Accessed on 25.12.2016].

Green, Natalia and Rossini, Carolina.(2011).Cyber Security and Human Rights. available at https://www.gccs2015.com/sites/default/files/documents/Introduction%20Document%20for%20GCCS2015%20Webinar%20Series%20-%20Cybersecurity%20and%20Human%20Rights%20%281%29.pdf (Last visit: June 2, 2016).

Hathaway, Melissa and Klimsbur, Alexander.(2012).Preliminary Considerations: On National Cyber Security. in Alexander Klimburg, *National Cyber Security Framework Manual*, Tallin: NATO CCD COE Publication.

Internetlivestatas. (2016). Internet Users in the World. http://www.internetlivestats.com/internet-users/(Last visit: June 16, 2016).

ISACA.(2016).Cybersecurity Fundemantals Glossary. http://www.isaca.org/ knowledge-center/ documents/glossary/cybersecurity_fundamentals_glossary. pdf [Accessed on 29.12.2016]

Italy.(2013). National Strategic Framework for cyberspace security.

ITU.(2016). Definition. available at http://www.itu.int/net/ITU-R/asp/terminology-definition.asp?lang=en&rlink={4B499A4A-3E11-4AE6-9B03-46FB1A662507}(Last visit: 17.06.2016).

Japan.(2013). Cybersecurity Strategy: Towards a world-leading, resilient and vigorous cyberspace.

Kovacs, Anja and Hawtin, Dixie. (2017). Cyber Security, Cyber Surveillance and Online Human Rights. available at, http://www.gp-digital.org/wp-content/uploads/pubs/Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf[Accessed on 23.01.2017].

Kuehl, Daniel T.(2009).From Cyberspace to Cyberpower: Defining the Problem.*Cyberpower and National Security*, Washington: National Defence University Press. available at http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf [Accessed on 25.12.2016].

Landesman, Mary.(2011).A Brief History of Malware. available at http://antivirus.about.com/od/whatisavirus/a/A-Brief-History-Of-Malware-The-First-25-Years.htm (Last visit: June 1, 2016).

Levy, Steven.(1994). *Hackers: Heroes of the Computer Revolution*, New York: Dell Publishing. available at http://www.temarium.com/wordpress/wp-content/documentos/Levy_S-Hackers-Heroes-Computer-Revolution.pdf[Accessed on 29.12.2016].

Lewis, James A.(2013).*Conflict and Negotiation in Cyberspace.* Washington: CSIS.

Lu, Miao and Reevese, Jason. (2014). *Types of Cyber Attacks, UNDAVIS available at* https://tcipg.org/sites/default/files/rgroup/tcipg-reading-group-fall_2014_09-12.pdf [Accessed on 29.12.2016].

Maurer, Tim and Morgus, Robert. (2014).*Compilation of Existing Cybersecurity and Information Security Related Definitions*. available at https://na-production.s3.amazonaws.*com/documents/compilation-of-existing-cybersecurity-and-information-security-*related-definitions.pdf[Accessed on 27.12.2016].

Mello, John. (2014).Report: Malware Poisons One-Third of World's Computers. available at http://www.technewsworld.com/story/80707.html [Last visit: June 16, 2016].

Moen, Johan Shubert. (2010). *From Noise to Filter: Cybernetics, Information and Communication in Thomas Pynchon's The Crying of Lot 49 and William Gibson's Neuromancer*, MA Thesis submitted to University of Agder. available at https://brage.bibsys.no/xmlui/bitstream/handle/11250/139274/Johan%20Schubert%20Moen.pdf?sequence=1[Accessed on 25.12.2016].

Netherland.(2016).*National Cyber Security Strategy 2*. available at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (Last visit: 17.06.2016).

Necessaryandproportunate.org.(2016). International Principles on the application of Human Rights to Communication Surveillance. available at https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf (Last visit: 18.06.2016).

OHCHR. (2016).The International Bill of Human Rights. available at http://www.ohchr.org/Documents/Publications/FactSheet2Rev.1en.pdf[Last access: 21.09.2016].

Osula, Anna-Maria- Roigas, Henry.(2016).Introduction. in Anna-Maria Osula and Henry Roigas (eds), *in International Cyber Norms Legal, Policy & Industry Perspectives*, Tallin: NATO Cooperative Cyber Defence Centre of Excellence. available at https://ccdcoe.org/sites/default/files/multimedia/pdf/ InternationalCyberNorms_ full_book.pdf [Accessed on 25.12.2016].

Ottis, Rain and Lorents, Peeter. (2016).Cyberspace: Definition and Implications. available at https://www.etis.ee/.../7d491419-9237-4de0-b324-62d597a.... [Accessed on 25.12.2016].

Pathfinder.(2011).What is cyberspace? examining its components.*Pathfinder*. Issue no. 153. Available on http://airpower.airforce.gov.au/publications/ Details/446/153-What-is-Cyberspace-Examining-its-Components.aspx (Last visit: June 17, 2016).

PoKempner, Dinah.(2013).Cyberspace and State Obligations in the Area of Human Rights. in Kathrina Ziolkowski. *Peacetime Regime for State Activities in Cyberspace:International Law, International relations and Diplomacy*.Talinn: NATO Cooperative Cyber Defence Centre of Excellence.

TheWhiteHouse.(2009). *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 2009, available at *https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf [Accessed on 25.12.2016]*.

UDHB.(2015).*National Cyber Security Strategy 2016-2019. available at* http://www.udhb.gov.tr/ doc/siberg/Ulusal Sibereng.pdf[Accessed on 25.12.2016].

UN Human Rights Council.(2012). 20th session, UN Doc. A/HRC/20/L.13, 29 June.

United Kingdom.(2011).Parliamentary Office of Science & Technology, POSTnote Number 389: Cyber Security in the UK.

United Kingdom.(2011a).*The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*.

United Kingdom.(2011b). Parliamentary Office of Science & Technology, POSTnote Number 389: Cyber Security in the UK.

United States of America.(2009). Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.

United States of America.(2011).Department of Defense Dictionary of Military and Associated Terms.(JP 3-13).

Wu, Timothy S.(1997).Cyberspace Sovereignty? - The Internet and the International system. *Harvard Journal of Law and Technology*, Vol.10, no.3.

Ziolkowski, Katharina.(2013).Foreword.*Peacetime Regime for State Activities in Cyberspace, International Law,International Relations and Diplomac.* Talin: NATO CCD COE Publication.

Z-World.(2001). *An Introduction to TCP/IP: For Embedded System Designers*, Califronis: Dynamic. available at http://www1.frm.utn.edu.ar/tecnicad2/tec_dig2/ doc/tcpintro.pdf[Accessed on 24.12.2016].

Wu, Timothy S.(2013).Cyberspace Sovereignty? - The Internet and the International system. *Harvard Journal of Law and Technology*, Vol.10, no.3.

Ziolkowski, Katharina.(2013).Foreword.*Peacetime Regime for State Activities in Cyberspace, International Law,International Relations and Diplomac.* Talin: NATO CCD COE Publication.

Z-World.(2001). *An Introduction to TCP/IP: For Embedded System Designers*, Califronis: Dynamic. available at http://www1.frm.utn.edu.ar/tecnicad2/tec_dig2/ doc/tcpintro.pdf[Accessed on 24.12.2016].

ISSN: 2587-1218

SİBER GÜVENLİK VE İLİNTİLİ KAVRAMSAL ÇERÇEVE

İbrahim KURNAZ*

Özet

21. yüzyılda eklendiği her sözcüğe bilinen anlamından öte anlamlar yükleyerek yeni bir hareket alanı kazandıran siber, kendine has anarşik yapısı ile eşsiz özelliklere sahiptir. Bilişim ve iletişim ağlarını içeren ve şekillendiren bir platform olarak siber uzay, verileri saklayan bilgisayarlara ek olarak bu verilerin akışını sağlayan sistem ve altyapıları birleştirerek sanal dünya ile fiziksel dünyayı bir bütün haline getirmektedir. Belli başlı fiziki sınırlılıklardan ve yasalardan yoksun ortamdan kaynaklı saldırıların, tehdit, saldırı ve de güvenlik gibi olguların önüne siber kelimesi eklendiğinde artık siber uzaya dair görüş ve algıların metaforik bir soyutlamadan ziyade gerçeklik alanı haline dönüşü ifade etmektedir. Dolayısıyla bu çalışma temelde bilişim ve teknolojinin tekâmülü ve bununla ilintili olarak siber ortamdan türeyen tehditler, saldırılar, terörizm gibi güvenliğin radarındaki kavramların nihai çerçevesinin boyutlarının genişlemesi bakımından bahse konu ortamın temel kavramlarına dair belli başlı bir çerçeve çizilmesini amaçlamaktadır.

Anahtar Kavramlar: Siber Güvenlik, Siber Uzay, Tehdit, Terörizm, Saldırılar.

CYBERSECURITY AND INTEGRATED CONCEPTUAL RAMEWORK

Abstract

In the 21st century, a new field of action emerged, cyber, which has its own unique anarchic structure and unique features. As a platform that includes and shapes information and communication networks, cyber space uses the flow of these data in addition to computers that store data, combining the system and infrastructures into a virtual and physical world. When cybercrime is added to certain physical frequencies and the lack of laws, such as threats, attacks, terrorism and security, it is now accepted that the cyber space is far from being a metaphorical abstract of views. Therefore, this study aims to draw a specific framework on the basic concepts of the subject environment in terms of expanding the dimensions of the ultimate framework of the concepts of security and technology such as threats, aggressions, terrorism, which originate from cyberspace.

Key Words: Cyber Security, Cyber Space, Threat, Terrorism, Attacks.

Giriş

* Selçuk Üniversitesi İktisat ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Bölümü, Araştırma Görevlisi
İbrahimkrnz.01@gmail.com

Küreselleşme süreciyle birlikte bilgi-iletişim-teknoloji alanı devrimsel nitelikli birçok gelişmeye tanık olmuştur. İnternetin icadı, bilgisayarların boyutlarının giderek küçülmesi buna mukabil işlevselliklerinin artması, sosyal paylaşım ağlarının ulusal suni sınırları aşarak toplumlar arası etkileşimi arttırması, bununla ilintili olarak yığınların mobilizasyonunun artması ve dolayısıyla kontrol edilebilirliklerinin azalması, internet ortamının finans kapitalin uluslararasılaşmasını daha da kolaylaştırması gibi fenomenler, bahse konu gelişmelerin örneklerindendir. Dolayısıyla 20. yüzyılın ortalarında bilgisayarın icadı ile oluşmaya başlayan siber alan, 21. yüzyılın başlarında bırakınız kendi alanını genişletmeyi, fiziksel alanları bile etkiler hale gelmiştir. Başka bir anlatımla bilgisayar ve onun kendisine yarattığı siber alan, günümüzde örneğin banka işlemlerini, haberleşmeyi ve e-devleti kendisine bağımlı hale getirmiştir. Dolayısıyla siber alanın gelişmesi ve genişlemesi durumunun Uluslararası İlişkiler disiplini kapsamında değerlendirilmesi bir zaruret halini almıştır. Zira daha önce de vurgulandığı üzere siber alan, küreselleşme ile ilintilendirilerek devlet egemenliğini ve dolayısıyla Uluslararası İlişkiler'i etkilediği düşünülen gelişmelerle kıyaslandığında sanal olmasına rağmen bu alanda gerçek bir etki yapmıştır.

İlk olarak siber alan ile kast edilen şey, temelinde ve yaratımında bilgisayar olan sanal dünyadır. Başka bir anlatımla, siber alan bilgisayarın icadı ile başlayan ve günümüzde gerçek alanları bile etkisini altına alan sanal âleme refere etmektedir. Bununla birlikte kavramın tanımında dikkat çeken birkaç husus bulunmaktadır. İlk olarak kavram sanal yani görünürde gerçek olmayana tekabül etse de aslında ve yarattığı etki bakımından tamamen gerçektir. İkinci olarak, siber alan gerçek alandaki durumu asimetrik olarak katlayan bir yapıdadır. Başka bir anlatımla örneğin gerçek alanda etkinliği ve yetkinliği oldukça az olan bir birey siber alan sayesinde ve bu alanda yaptıklarıyla etki ve yetkinliğini üst düzeylere taşıyabilmektedir. Üçüncü olarak siber alan büyük ölçüde gerçek kimliklerin askıya alındığı ve dolayısıyla gerçek dünyadaki hukuki sorumluluk ve yaptırımların işlemesinin sekteye uğradığı bir alandır.

Tüm bu noktalardan hareketle, henüz olgunlaşmamış küresel bir platformu teşkil eden siber ortamın uluslararası sistemde yeni aktörler ve strateji belirleyen bir alan olduğunu iddia eden bu çalışma, i) siber alanın bizatihi kendisini, ii) güvenlik, tehdit ve terörizmle olan ilişkisini ve bahse konu kavramların tasvirini yapmayı amaçlamaktadır.

Siber Güvenlik

Siber güvenlik kavramı ve onunla ilintili kavramlar ve durumlar son çeyrek asırda baş döndürücü bir hızla gelişmiş ve gelişmeye devam etmektedir. Bilişim ve enformasyon teknolojilerindeki gelişmelere pararlel olarak bu alandaki kavramlar da oldukça dinamik ve hızlı bir şekilde üretilmekte ve çoğalmaktadır. Öğun ve Kaya bu gelişim sürecini özetlemektedir:

> *Siber güvenlik ilk defa 1990'lı yıllarda bilgisayar mühendisleri tarafından, ağa bağlı bilgisayarlarla ilgili güvenlik sorunlarını ifade etmek için kullanılmış fakat akabinde bu güvenlik sorunlarının yıkıcı sosyal sonuçlar doğurabileceğinin ortaya çıktığı gelişmeler meydana gelince bunlar zamanla politikacılar, özel şirketler ve medya tarafından batı dünyasına büyük bir tehdit olarak değerlendirilmiş ve "Elektronik Siber Pearl Harbor"lar olarak dile getirilmiştir. 11 Eylül olayları, bilgi teknolojileri, bilgisayarlar güvenliğe odaklanılmasını sağlamış, özellikle de bilgi teknolojileri altyapılarının korunması, elektronik gözetleme, teröristlerin interneti iletişim vasıtası olarak kullanmasına dikkat çekmiştir.*

Siber güvenliğe yönelik ağlar üzerinden tehdit oluşturan temel saldırı araçları da ortamın kendine has doğası itibariyle farklıdır. Ağlar üzerinden casus yazılımlar, ağ şebeke trafiğinin dinlenmesi, manipüle edici yemlemeler, istem dışı elektronik postalar, servis dışı bırakma, kurtçuklar ve köle bilgisayar anlamına gelen bootnetler bahsi geçen siber ortamdaki saldırı araçlarıdır.

Joseph Nye bu noktada devletlerin siber güvenliğine yönelik temel tehditleri devletlerin birbirlerine karşı oluşturduğu siber tehditler ve devlet dışı aktörlerin devletlerin siber güvenliğine yönelik tehditler şeklinde sınıflandırmıştır. Bu sınıflandırmaya göre de, siber çatışmalar ve ekonomik temelli casusluk ve istihbarat tehditleri daha çok devletler ile ilintilendirilirken, siber ağlar aracılığıyla işlenen suçlar ve siber terörizm ise devlet dışı aktörler ile ilişkilendirilmiştir (Nye, 2011).

Siber uzayın karmaşık ve çok boyutlu kendine has ortamı siber güvenlik nosyonunu öncelikli güvenlik alanlarından biri haline getirmiştir. Siber ortamdaki her türlü bilginin korunması şeklinde tanımlanan siber güvenlik, aynı zamanda bilginin üretimi, depolanması, işlevsel kılınması ve iletimiyle de ilgilidir. Bu çerçevede en genel manada siber güvenlik siber ortamda, kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan; araçlar, politikalar, güvenlik kavramları, risk yönetimi yaklaşımları, faaliyetler, eğitimler ve teknolojiler bütünü şeklinde tanımlanabilmektedir (Stevens, 2015: 20-41). Güvenliğin bu yeni boyutunun nihai hedefine ulaşabilmesi için siber ortamda bazı güvenlik kriterlerinin ve

niteliklerin sağlanması gerekmektedir. Bunlar; gizlilik, özgünlük, doğruluk, bütünlük, tutarlılık, güvenilirlik, süreklilik, erişilebilirlik ve ölçülebilirlik şeklinde olmalıdır (Gorman, 2006: 239-257). Bilginin haiz olduğu bu nitelikler, devletler düzleminde kullanılan bilişime dayalı sistemler ile varlıklarının yine karşı bilişim sistemlerinden türeyen saldırılar sonucunda vereceği hasar ve güvenlik açığı göz önünde bulundurulursa yaşanacak olan kaos ortamı devletleri zor duruma düşürecektir. Örneğin, 2007 yılında Estonya'da meydana gelen siber saldırı, bir ülkenin kritik altyapılarının internetten gelen tehlikeler karşısında ne kadar savunmasız olabileceğini gözler önüne sermiştir. Estonya açısından bu tehdidin hayati olarak algılanmasının sebebi, ülkedeki kamu ve özel sektöre ilişkin birçok faaliyetin internet üzerinden yürütülmesidir (Gücüyener, 2015: 18). Yine, Avustralya'da öfkeli bir işçinin bilgisayar sistemlerini manipüle ederek nehir ve parklara saldığı atık sular, yazılımlar aracılığıyla ABD'de 11 kişinin ölümüne yol açan ve 50 milyon kişinin çaresiz kalmasına neden olan elektrik sisteminin aksatılması ve İran'a nükleer tesislerine yönelik gerçekleştirilen Stuxnet saldırıları akla gelen örnekler arasındadır.

Siber güvenliğin katmanlarını uygulama güvenliği, hizmet güvenliği ve altyapı güvenliği şeklinde, kapsadığı alanı ve boyutlarını erişim denetimi, kimlik doğrulama, veri gizliliği, iletişim güvenliği, veri bütünlüğü, ulaşılabilirlik ve devletlerin mahremiyeti şeklinde sınıflandıran Ünver ve Canbay'a göre bu katmanlar ve ürettikleri boyutlara yönelik yok etme, hasar verme, silme, ifşa etme, engellemeye yönelik tehdit ve saldırılar siber güvenliğin muhteviyatını belirlemektedir (Ünver vd., 2009: 3). Bunun içinde siber güvenliğin kilit faktörü konumundaki bilginin teminat altına alınması ancak bilginin erişilebilirliği (umulmadık olay ve saldırılara karşılık gereksinim duyulduğunda erişilebilir, kullanıma hazır ve işlevsel bir halde bulunma durumudur), bütünlüğü (transfer edilen ve paylaşılan verilerin doğruluğuna karşı kritik altyapıların veri bütünlüğünün sağlanması için bilişim sistemleri aracılığıyla iletilen, alınan ya da bilişim sistemlerinde saklanan verilerin noksan ve manipüle edilmeden depolanması durumudur), gizliliğidir (bilişim sistemleri üzerinden gerçekleştirilen iletişim ve haberleşmenin gizlenen verilerin muhafazasını konu edinmektedir. Özellikle önemli ve hassas verilerin tamamının iletimi ve haberleşme süresince devlet dahil kullanıcının mahremiyetinin korunmasını gizlilik yoluyla korumaktır). Bu kapsamda da bilgiyi ve sahip oldukları nitelikleri korumayı hedefleyen siber güvenlik, siber tehdit ve saldırılarla birlikte bilişim sistemlerinden neşet eden güvenlik açıklarını asgari düzeye indirmeyi hedeflemektedir (Ünver vd., 2009).

Bu hususlar ışığında, güvenliğin sağlanması noktasında yapılan çalışmalar ulusal politika ve bu politika çerçevesinde hazırlanmış bir siber güvenlik stratejisi gerektirmektedir. Siber saldırıların, genellikle mala ve ihtimal dahilinde de olsa cana etki eden sonuçları olası olduğundan siber güvenliğin sağlanmasında bu sonuçların ve bu sonuçlara yol açan fiil ve yöntemlerin suç olarak tanımlanması ve cezalandırılması, özellikle siber saldırganların caydırılması noktasında, büyük önem arz etmektedir. Teknolojik gelişmelere paralel olarak siber saldırı araç ve yöntemlerinin değiştiği göz önünde bulundurularak ülke mevzuatının gözden geçirilmesi gerek esasa gerekse de usule ilişkin varsa eksikliklerin giderilmesi gerektiğinden bu konuda yasal bir çerçevenin oluşturulması da gerekmektedir. Ayrıca yazılım, donanım ve iş süreçlerinin kalitesinin artırılarak daha güvenli kılınması için teknik tedbirlerin geliştirilmesinin yanı sıra siber güvenlik konusunda kurumsal yapılanmanın belirlenmesi, ulusal bazda iş birliği ve koordinasyonun sağlanması ve kapasitenin geliştirilmesi, farkındalığın artırılması, uluslararası iş birliği ve uyumun sağlanması siber güvenliğin sağlanmasında önemli unsurlar olarak göze çarpmaktadır.

Siber Uzay

1980'li yıllarda bilim-kurgu alanından türeyen ve Türkçe'ye siber alan, siber ortam ve/ya siber uzay şeklinde tercüme edilen (Çifçi, 2013: 2) *cyberspace* kavramı, 21. yüzyılda kavramsal olarak kayda değer gelişim göstermiştir. Özellikle internetin ve bilgi ve iletişim teknolojilerinin gelişimine paralel bir şekilde gelişim seyri izleyen siber uzay, yeni dünya düzeni olarak tabir edilen bu yüzyılda yeni bir anlaşmazlık ve çatışma alanı olarak doğarken, ekonominin tüm sistemlerinin de dâhil olduğu daha geniş toplumsal düzlemde ise bilgilenme ve bilgilendirme katmanı olarak görülmüştür (Dunne, 2009: 101-150). Öyle ki, 21.yüzyıl itibariyle siber uzayın etkinlik alanlarına erişim ve katılım dünya genelindeki devletler ve insanlar için kullanılabilir hale gelmiştir. 2016 sonu itibariyle dünyada yaklaşık olarak 3.5 milyar insan yani dünya nüfusunun yarısı, internete rahatlıkla erişebilmektedir (Dijital Ajanslar, 2016).

Siber uzay nosyonuna dair bilinmesi gereken ve üzerinde oydaşmaya varılan nokta, kavramın uzay son ekinin algılarda bilinen sonsuzluğa karşılık gelen boşluk anlamındaki uzay olmadığıdır. Çünkü siber uzay en başta insan yapımıdır. Bu alanda üretilen, paylaşılan ve toplanılan bilgi ortamını kuran ve idamesini sağlayan insandır. Yine, siber uzay nosyonun olmazsa olmazı olan dijital aletlerin kullanımının ve yönlendirmesinin çok boyutlu ve işlevsel çözümlemelerinin faili insandır (Reed, 2012: 44-78). Dolayısıyla siber uzay insan toplulukları

aracılığıyla özellikle kritik altyapıları da içeren bilgi ortamıyla beraber bilginin depolanması, ağlar aracılığıyla paylaşılması ve yayılması gibi fiziksel altyapıları barındırmasından dolayı bir zamanlar atfedildiği gibi sanal âlemden öte bir konumdadır (Rheingold, 1991: 14-26). Bu nedenle siber uzay ile fiziksel katman bir bütün haline gelmiştir.

Kavramın kökenbilimi incelendiğinde yakın dönemde tanımlanan ve anlam kazanan semantiğinin bir hayli uzağında ve farklı alandan türediği görülmüştür. Siber ifadesi, eski Yunan medeniyetleri döneminde Kübernetes olarak telaffuz edilmiş olmakla beraber 1948 yılında ise matematikçi Norbert Weiner tarafından hayvanlar ve makinalar arasındaki kontrol ve iletişim disiplinini inceleyen bir bilim dalı olarak tebarüz eden sibernetik kavramı tekrardan diriltilip detaylandırılmıştır (Heylighen ve Cliff: 2001:3). Ön ek konumundaki siber kelime anlamı olarak bilgisayar ve elektronik merkezli teknolojileri refere etmektedir (Nye, 2011: 19).

Siber uzay kavramı da sibernetik sözcüğünün ilk öbeği ve uzay kelimesinin birleşmesi ile oluşmuş bir kavramdır. Kavramın bu şekildeki yapılanmasının mimarı olan Gibson siber uzay kavramını 1982 yılında yayınladığı kısa hikâyede karmaşık değişkenleri içeren teknik bir alan olarak yorumlarken, 1984 yılında Neuromancer adlı romanında ise daha kapsamlı ve teknik temayülde milyarlarca ağlar tarafından karşılıklı olarak transfer edilen iletilerin zihinde canlandırılması zor olan ve muazzam derecede karmaşıklıkları içeren grafiksel bir platform olarak tanımlamıştır (Heylighen ve Cliff: 2001).

Siber uzayın boyutlarının gösterdiği etki sadece teknik boyutlarda değil, siyasi ve toplumsal katmanlarda da yer bulmuştur. Bir zamanlar iletişim amaçlı kullanım alanı bulan siber uzay 21. yüzyılda ise bankacılık sektöründen, ulaşım, haberleşme, sağlık ve enerji tesisleri gibi daha birçok kritik altyapıları da ihtiva eder hale gelmiştir. Bu sebeple farkına varılan siber uzayın münhasıran bir alan olarak billurlaşmasına değin özünde internet ve ağ şebekeleri üzerinden tanımlanmış ve gün geçtikçe ilave kavramlarla alanını daha da genişletmiştir (Bomse, 2001: 1717-1749). Örneğin kavram uzmanlarca 1990'lı yıllarda bilgisayar aracılığıyla sürdürülen, erişilen ve üretilen küresel ağ bağlantılı sanal ve yapay iletişim alanı olarak tanımlanırken (Benedikt, 1991: 119-224) 2000'li yıllarda ise ayrı bilgisayarlar arasındaki etkileşimi barındıran sistem şeklinde tanımlanmıştır. Sanal mekândan öte olduğunu vurgulamak için de bilgisayarlar arasındaki etkileşimi muhafaza eden ve düzenleyen unsurun insan olduğuna istinaden kavramın fiziksel alana daha yakın olduğu dile getirilmektedir (Chang, 2002; 1-18).

Reel dünya ile sanal dünyanın kesişen varlığı siber uzaya dair yekpare bir alan tartışması 21. yüzyılın yeni ortamında anlamsızlaşmaktadır. Çünkü siber uzay artık hem fiziksel hem de sosyal yapı unsurlarına aynı anda sahiptir. Fiziksel yapıya sahiptir çünkü bilgi teknolojileri altyapıları tarafından hareket alanı bulmaktadır. Sosyal yapıya sahiptir çünkü alan insanlar, kurumlar tarafından dikkate alınmaya, konuşulmaya ve düşünülmeye başlanmıştır.

Siber uzay tabanlı bilgi teknolojilerinde kaydedilen gelişmeler ve bu bilgi teknoloji araçlarının arka planında yer alan dijital dünyanın yerlisi konumundaki insan olgusunun doğal olarak bu alandan kaynaklı problemleri üretmede ve çözmede gerekli sürecin içerisinde yer alması, alanın toplumsal ve siyasal temelli değişimlere yön vermesine neden olabilmiştir. Gün geçtikçe artan yüksek teknoloji araçlarının ve bilgi sistemlerinin yanı sıra bununla ilintili olarak artan kullanıcı sayısı, siber uzayda insanlar, şirketler, suç örgütleri ve diğer devletlerden gelebilecek tehditlere karşı hedef konuma gelen devletler ve kullanıcılar nezdinde olumlu yanlarını barındırdığı gibi olumsuz yanlarını da barındırmıştır. Bu alandan neşet eden tehditlerin kimden geldiğinin belinemezliği ve muhteviyatının ne derecede olduğunun geç fark edilmesi gibi unsurlardan dolayı, siber uzay toplumlar ve devletler için 21. yüzyılda yaklaşan en büyük tehdit alanı olarak görülmektedir. Çünkü bu alan devlet ötesi suç örgütlerinin ve bireylerin hedefleri doğrultusunda herhangi bir devletin ulusal güvenliğine hasar verebilecek fırsatları da vermektedir. Ve doğası gereği siber uzay birey, suç örgütleri ve devlet gibi farklı düzeydeki aktörlere eşit kullanım ve faydalanma imkânı sunmakla birlikte aynı zamanda riskler ve tehditler oluşturmada açıklıklar oluşturmaktadır.

Kısaca, yukarıda farklı ve dönemsel boyutlarıyla yapılan tanımlamalar ışığında siber uzay, zamana bağıtlı bir şekilde gelişen birbiriyle bağlantılı bilgi sistemleri ve bu bilgi sistemleriyle etkileşim içerisinde olan insan kullanıcıları dizisinden oluşan ve kendine has gayrı merkeziliğiyle ve muhteviyatı ile sanal ve fiziki katmanları da barındıran bir platformdur. Burada zikredilen birbiriyle bağlantılı bilgi sistemlerinden kasıt, elektronik ortamdaki bilgi, yazılım, donanım ve bilgisayar sistemli programları birbirine bağlayan iletim ortamıdır. Siber uzay alanının kilit unsurunu oluşturan insan kullanıcıları da özünde yapaylığı barındıran alana bu özelliği kazandıranın ve inşa edenin insan amilinin olduğu vurgusudur (Punday, 2000: 194-213, Giles, 2006: 464). Çünkü elektronik aygıtların ve bilgisayar sistemli programların arka planındaki çeşitli sorunların ve bu sorunların çözümünde önemli rol oynayan kullanıcı ve tüketici konumundaki insan amili olmadan siber uzay dinamikliğini kaybedecek ve bir tehdit

unsuru olmaktan çıkacaktır. Ayrıca, tanımlamalarda üzerinde durulmayan ancak önem arz eden bir diğer kayda değer sorunsal alanın mahiyetinin zamana bağıtlı bir biçimde geçirdiği dönüşümdür. Bu sebeple, haiz olduğu dinamik yapı sebebiyle sürekli gelişim gösteren alan, doğal olarak statiklikten de azade bir konumdadır. Bu durumda alanın karmaşık yapısı doğru orantılı bir şekilde artırmaktadır. Dolayısıyla kavramın tanımlamasına, içeriğine ve etki ölçeğine dair yapılan açıklamalar zamana bağlı değişkenlik vurgusunu elzem kılmaktadır.

Siber Tehdit

Siber alandan kaynaklanan tehditler, her ne kadar önceki dönemlerde yaşansa da özellikle bilişim ve iletişim teknolojilerinin kullanıldığı 11 Eylül saldırıları (Weimann, 2004: 3-21, Heidenreich ve Gray, 2013: 8-23, Lovelace, 2015: 86), akabinde Estonya'ya yönelik siber saldırılar sonrasında farkındalığı uluslararası toplumun nezdinde artmış ve devletlerin güvenlik politikalarının merkezinde yer edinmiştir (O'Connell ve Arimatsu, 2012: Korns ve Kasternburg, 2009: 60-70). Anavatanı siber uzay olan bilgi ve iletişim araçlarının yaygınlaşması ve maliyetinin de düşüklüğü ile beraber düşünüldüğünde, devletler için olduğu kadar, bireyler ve devlet dışı aktörler için de başvurulması gereken zaruri bir alan haline gelmiş olan alan erişilebilirliği, kullanım kolaylığı, ispat edilemezliği ve etkisiyle bağımlılık yaratmıştır. Devlet dışı aktörlerin bilişim teknolojileri araçlarına gün geçtikçe daha bağımlı hale gelmesi, geleneksel güvenlik anlayışının tehdit algısının aksine, niteliği ve niceliği bakımından asimetrik yeni tehditlerin uluslararası sistemde boy göstermesine yol açmıştır.

Gelişimi ve yayılma evresi devam eden siber uzay, uluslararası sistemin başat aktörü devletlerin güvenliğini siber tehditler diye adlandırılan yeni bir tehditle baş başa bırakmıştır. Siber tehditler; siber uzay teknolojilerinin sağlamış olduğu olanakların araçsallaştırılmasıyla devlet gibi siyasal, devlet ötesi gibi toplumsal birimlerin siyasal, toplumsal ve ekonomik öz değerlerine yönelik içe ve dışa dayalı düzenlerini hasara uğratma olasılığı taşıyan tehlikeler kategorisine girmektedir (Berner, 2003: 4). Ayrıca amaç ve araç olarak siber uzayda üreyen ve gelişen bilginin kötüye kullanılması, kamuoyuna afişe edilmesi ya da sistemli saldırılarla erişilebilirliğinin engellenmesi gibi arzu edilmeyen durumlara ve sonuçlara sebebiyet verme tehlikesi olarak tanımlanmıştır (Ünver, vd., 2009). Bu tanımlamada siber tehditler sadece bilgi ve iletişim teknolojilerinden türeyen tehlikeler olduğu için bilişim araçlarının ve sistemlerinin araç olarak kullanıldığı vurgulanmıştır. Bu tanımlamaya uygunluk teşkil eden yerinde örneklemlerden biri ise Wikileaks belgeleridir. Kasım 2010 'da ABD'nin Irak savaşı ile ilgili kayıtlarının ve diplomatik elektronik yazışmalarının Wikileaks web sitesinden yayınlanması

teknolojik bağımlılığı yüksek olan devletler nezdinde siber uzayın bir tehdit oluşturacağı kanısını güçlendirmiştir. Öyle ki, kimilerince diplomasinin 11 Eylülü olarak tabir edilen Wikileaks belgelerinden sonra Foreign Policy dergisi siber alanı yaklaşan en büyük tehdit olarak nitelendirmiştir (Singer and Friedman, 2015). Çünkü Wikileaks gelişen teknoloji araçları ve hizmetleri ile devletlerin gizli kalması gereken politikalarını ifşa etmekle kalmamış, bilgisayar ortamında peşi sıra ABD dışındaki ülkelerin büyükelçiliklerinin ve konsolosluklarından gelen tüm resmi yazışma ve mesajları paylaşmış ve çoğaltmıştır.

Siber güvenlik tehditlerinin varlık alanında tanımlanmış, belirgin ve açık bir düşman tanımı mevcut değildir. Saldırganlar 12-19 yaş grubu arasındaki ergen çocuklar olabileceği gibi, terörizme destek veren "haydut devletler", ya da bir takım ideolojilere sahip teröristler ya da çıkarları doğrultusunda hareket eden devletler de olabilmektedir. Siber tehditlerin gayrı-merkeziliği ve karmaşıklığı saldırganların hasmane niyetlerinin ve tehditlerinin doğrulanabilir ve gerçekliği kanıtlanabilirliliğini zorlaştırmaktadır. Bilgisayar sistemli araçlara sahip bir kişi, dünyanın başka bir coğrafyasında başka birine ve kuruma ait bilgisayara kısa sürede erişebilir ve bu bilgisayarları kontrolü altına alabilir. Çünkü teknolojinin ileri sevideki gelişmiş hali bu kolaylığı sağlamaktadır (Edwards, 2010: 30-33). Sahip olduğu deneyim, olanaklar ve kapasitelerle birlikte gereksinim duyduğu saldırı teçhizatlarına da erişebilen saldırganlar, böylelikle devletlerin bilişim sistem güvenliğindeki açıklıklarından yararlanarak siber saldırılar gerçekleştirebilmektedir. ABD'nin federal kurumlarına ait bilgisayarlarına sızan ve lojistik bilgi sistemlerine dair bilgilere erişip bu bilgileri hükümetin farklı kurumlarına zarar vermek için kullanan kişi 21 yaşındaki bir çocuktu. Yine ABD'nin uzay çalışmalarının yürütüldüğü kurum olan NASA'ya ve hükümetin diğer savunma bakanlığına ait kurumlara sızıp bilgilere erişen kişi 16 yaşındaydı (Wordpress, 2015). İnternet ortamında hareket eden ve tehlikeli kişi olarak adlandırılan bu ergen çocuklar *skript kiddies* olarak adlandırılmıştır. Skript kiddiesler hackerlığın mertebeler silsilesinde en alt sınıfı oluşturan tehdit unsurlarıdır. Bunlar genelde kendi yazılımlarını geliştiremeyen daha çok internetten hazır bir şekilde indirdikleri yazılımları ve kodları indirip kullanarak sıkıntılarını ve meraklarını gidermek isterler (Pctools, t.y.).

Gözlemlendiği üzere bilişim sistemdeki yaygın açıklıklar bu alana dair bilgiye, beceriye ve kısmen de olsa deneyime sahip olan saldırganlar için arzulanan ortamı rahatlıkla olanaklı kılmaktadır. Zaten alanın gayrı-merkeziliği, zor ve yüksek maliyetli olmayışı ve isnat sorunu gibi kendine özgü sunmuş olduğu olanaklar, bilişim teknolojilerinin gelişimine paralel

saldırganların da niceliğini artırdığından tehditlerin de sayısını artırmıştır. Çünkü siber tehditler, bilişim altyapılarından türeyen kötü niyetler ve amaçlar taşıyan kötücül ve zararlı yazılım ve donanımların kullanılması neticesinde gelişim bulduğu için bilgi teknolojileri ortamının değişen karakteristiği bu alandan kaynaklı oluşacak tehdit algılarını şekillendirmektedir.

Ulusal güvenlik ve bununla ilişkili olarak tehdit algısında ve politikasında 21. yüzyılda siber alandan kaynaklı bir diğer göze çarpan unsur, bireysel ya da sayıca az olan grupların saldırıları ve bunun sonucunda yaratmış oldukları tehditlerdir (Kibaroğlu, 2002: 4). Klasik güvenlik anlayışında devletlerarasında zuhur eden askeri temelli tehditlere karşılık etkin bir müdahale ile cevap verilebiliyordu. Ancak 21. yüzyılın güvenlik anlayışının genişleyen ve nitelik bakımından değişen tehditleri ve bu tehditleri amaçları doğrultusunda kullanabilme imkânına ve deneyimine erişebilen devletler ve devlet-ötesi aktörleri ile beraber yeni dönemde saldırganların kimliği devletler nezdinde karşılık vermede mühim sorunsallar teşkil etmiştir. Tehditler devlet-ötesi gruplardan devletlere yönelik arz ettiğinde devletlerin vereceği karşılıklar görünürde yasalar bağlamında tecelli edeceğinden bu durumda tehditlerin şiddetine ve isnatlığına dair bir takım cevapsız soruları beraberinde getirmektedir. Örneğin, saldırıyı gerçekleştiren saldırgan ya da saldırganların kimliği belli midir? Kimin ya da neyin tehdit edildiği belirlenmiş midir? Ve özellikle siber uzayın küresel doğasının kimlik ve lokasyon bağlamında sunmuş olduğu bir takım avantajlardan mütevellit, siber güvenlik tehditlerinin arkasında devlet düzeyinde kimin olduğu belli midir? türü sorular, siber tehditleri devletler nezdinde daha da dikkate alınması gereken güvenlik sorunsalı olarak gün yüzüne çıkarmaktadır (Shackelford, 2014; 3-51).

Bilgi, birikim ve etki bakımından en üst kademesini oluşturan ve politik, sosyal ve dini saikleri olan ileri düzeydeki hektivistler, siber uzayı kullanarak özellikle devletlerin ulusal güvenlik bağlamında önemli yer tutan kritik altyapılarına gerçekleştirdikleri siber saldırılarla tehdit unsuru oluşturan diğer önemli gruplardır (Hua ve Bapna, 2012: 104-105). Devletlerin kamuya ait neredeyse tüm finansal, askeri ve sağlık, enerji ve iletişim gibi altyapıya dair sunmuş olduğu hizmetlerin büyük kısmının kritik altyapısının bilişim sistemlerine bağlı olması bilgi, beceri ve deneyimleri ile siber ortamı iyi kullanabilen hackerlere saldırı amaçlı tehdit oluşturmada farklı nitelikte bir hareket sahası ve tarzı yaratmıştır (Caplan, 2013: 93-108).

Hekleme teknik ve yöntemlerini kullanarak devletlerin hem bilişim sistemlerine hem de bu bilişim sistemlerine bağlı olarak çalışan kritik altyapılarına karşı ciddi hasarlar vermeyi amaçlayabilen bu gruplar, devletlerin web sitelerine yapılan DDOS (Distributed Denial of Service) saldırıları, bombalı mail mesajları, virüsler, içerik bozma ve manipüle edici yazılımlar ve donanımlar, internet hizmetlerinin kesilmesi ve kurtçuklar ve botlar gibi saldırı araçları kullanabilmektedir. Pratik bağlamda haktivistlerin aktif katılım gösterdiği ve gerçekleştirdikleri siber uzay kaynaklı saldırılar ilk olarak Kosova savaşında dikkatleri çekmiştir (Dun, 2008: 21, Geers, 2011: 2).

Kosova savaşının yanı sıra, 2007 yılında gerçekleşen Estonya ile Rusya arasındaki gerginlikte, 2008 İsrail'in Suriye'de Kuzey Kore'nin inşa etmek istediği nükleer tesislerin altyapısını bilişim sistemlerini kullanarak yok etmesinde (Eran, 2009; Follath ve Stark, 2009) Pakistan-Hindistan arasındaki Kaşmir anlaşmazlığında (Al Jazera, 2010) ve İsrail-Filistin çatışmalarında kullanılan yoğun siber saldırılar (Allen ve Chris, 2003) rakip devletler arasında gözlemlenebilen siber temelli çatışma örnekleri olarak göze çarpmaktadır.

Siber uzay kaynaklı siber tehditlerin doğal olarak araçları da siber ortama özgü uyarlanmış olacaktır. Örneğin bu alandan neşet eden siber güvenlik tehditleri genelde önemli ve gizli olan verilerin rakip devletlerden askeri, siyasi ve ekonomik fayda sağlamak için illegal bir şekilde iletişim ağları, donanım ve yazılımlar aracılığıyla çalınması, siber casusluk tehdidini meydana getirirken; hizmet dışı bırakma yöntemi ise rakip devletlerin hâlihazırdaki bilgi sistemlerini çalışamaz duruma getirme de bir başka yeni siber tehdit türünü meydana getirmektedir. Bununla birlikte, özellikle bilişim sistemlerinden uydular kullanılarak rakip devletlerin askeri araçlarının hasara uğratılması ve petrol, doğal gaz, elektrik, bankacılık ve ulaşım hizmetlerini içeren altyapılara yönelik saldırılar da diğer önemli siber güvenlik tehdit türleridir.

Siber Terörizm

Global değişimin katalizörü olarak siber uzaydan türeyen (Karagül ve Özkan, 2015) hızlı ve seri gelişmeler, bir yandan toplumların ve devletlerin sosyo-ekonomik ve siyasi pratiklerini olumlu yönde etkilerken, bir diğer yandan da asimetrik ve çok boyutlu tehdit unsuru oluşturmak isteyen suç örgütleri için de politik hedeflerine erişmelerinde, güç ve kamuoyu oluşturmada etkinlik aracı olma fırsatı taşımıştır. Özcan'ın suçbiliminin suçların fırsatları takip etmesi şeklindeki deterministik düsturundan hareketle siber uzay bilişim teknolojileri vasıtasıyla kötü niyetli terörist gruplara yeni yol ve yöntemlerle yeni tehdit unsuru

oluşturabilecek olanaklar sağlamıştır (Özcan, 2004). Siber ortamın sunduğu fırsatlar sayesinde küreselleşen bilgiden devletlerin yanı sıra suç örgütleri de önemli oranlarda yararlanmakta ve internet üzerinden bomba yapım tekniklerini anlatma gibi olanaklara sahip olabilmektedir. Bunun yanında organize suç gruplarının ve terör örgütlerinin ellerinde bulundurdukları kara para ile teknik altyapılarını hızla geliştirmesi, oyunu hukuka bağlı olan/olması gereken güvenlik güçlerinin aksine bir kurala bağlı olmaksızın oynaması ve gerektiğinde bu alana çok büyük mali kaynaklar aktarması gibi olanaklar, devletlerin bilişim suçları ile mücadelede ciddi zorluklar ile karşılaşmasına neden olmaktadır (Özcan, 2002 ve 2004).

Günümüzde her türlü bilgisayar aletleri, yazılımlar, internet ağları ve iletişim araçları gibi siber ortamın dâhilindeki tüm araçları büyük oranda terör grupları tarafından rahatlıkla ve kolaylıkla kullanılabilmektedir. Örneğin, IŞİD internet dünyasında faaliyette bulunan Siber Halife Ordusunu (CCA) saldırılar icra etme kapasitesi bakımından yetersiz bulmuş, bunun yerine istihbaratı ve tam teşekküllü saldırıları yapma kapasitesini artırmak için siber ordu kurma gayreti içine girmiştir. IŞİD üyeleri siber saldırı adımlarını ayrıntılarıyla paylaşarak kendi gruplarıyla ilintili siber asker ağını genişletmeye yönelik online bir kurs açarak, IŞİD sempatizanı bir kişi batı istihbaratını hedefleyen "nasıl siber saldırı yapılır" dersleri vermeye başlamıştır (Siber Bülten, 2016).

Devletler askeri, ekonomi ve hizmet sektörlerinde bilişim sistemlerini yaygın bir biçimde kullanırlar. Devletlerin bilgi teknolojilerine ve ağlar sistemine bağımlı hale gelmesi, sadece meşruluğa uygun kabul edilen birimler tarafından değil, aynı zamanda kötücül niyetlere sahip saldırganların, teröristlerin, sınır aşan suç örgütleri gibi diğer suç unsuru teşkil eden birimlerin de siber ortamdan faydalanmak için istifade ettikleri göze çarpmaktadır. Yakın döneme kadar klasik konvansiyonel savaş araçlarına erişemeyen terör grupları devletlere yönelik tehdit unsuru olma ve eylemleri aracılığıyla ses getirme şansını siber ortamın devletler aleyhine yaratmış olduğu açıklıklardan ve zafiyetlerden faydalanma olanağı ile yakalamış ve devletlere karşı meydan okumalarda neredeyse eşit şartlar sunmuştur (Taliharm, 2010; 65-66; Schmid ve Jongman, 1988: 12-15). Dolayısıyla devletlerin ve toplumların bilişim teknolojilerine artan bu bağımlılığı, terör gruplarına devletlerin ulusal savunma ve kritik altyapı sistemlerine yönelik saldırı hedeflerini gerçekleştirmede farklı türde ve nitelikte saldırı imkânı yaratmaktadır (Weiman, 2004).

Terörizmin tanımlanmasına dair uluslararası düzeyde ve entelektüel camiada ihtilaf ne kadar yüksekse siber terörizmin tanımlanmasına yönelik ihtilaflar da o kadar yüksektir. Ancak yine de siber terörizme dair yapılan tanımlamalar ve ileri sürülen bulgular en nihayetinde üst küme konumundaki geleneksel terörizmin niteliklerinin siber ortamda hangi şekillerde tecessüm ettiğinin ortaya konması durumunda tanımlamayı bir nebze de olsa kolaylaştıracaktır. Sonuçta siber ortamın yeni ve ileri seviyedeki teknolojik araçlarına erişebilen ve sahip oldukları bu teknolojileri araç olarak kullanabilen terör grupları, politik bir gaye ve korkutulması hedeflenen bir kamuoyu kitlesi gibi amaçlarını bu alanda gerçekleştirebilirler. Siber terörizme ve tehditlerine ilişkin göze çarpan ezber bozucu okuma yeni yüzü ve boyutlarıyla bilimezliği ve bilgi yoksunluğu ya da daha da kötüsü haddinden fazla yanlış ve manipüle edilebilen bilgi ve bilgilendirme sorunudur. Öncelikle geleneksel terörizm ile siber terörizm bu minvalde kayda değer boyutlarda teknolojiden ve terörizmden kaynaklı iki önemli modern korku biçimini aynı çatı altında toplamaktadır. Bu tehditler yakın dönemde bilinen tehditlerden daha ileri düzeyde tehditkâr olarak algılanabilmektedir (Rathmell, 1997: 40-45).

Aslında siber terörizm kavramı özellikle 21. yüzyılın başından günümüze değin uluslararası yazılı ve görsel basında yer almış ve bu süre zarfında da sürekli güvenlik tehditleri sıralamasında ve algısında üst sıralarda sayılmıştır (Cox, 2012: 31-36). Küresel medya, özellikle kritik altyapılara yönelik potansiyel felaket getirici tehditleri geçmişte yaşanan trajedilerle benzeşimler kurarak göz alıcı hikâyelerle meseleyi irdelemeye çalışmıştır. Siber terörizm nitelendirilmesi de 11 Eylül'den itibaren ABD basınında sıklıkla vurgulanmış ve neredeyse basit hekleme suçundan, ciddi finansal zararlara sebep olan siber saldırılara, olası yaralamalara ve ölümlere sebep olmaya kadar her vaka ve gelişme hemen hemen siber terörizm olarak adlandırılmıştır (Conway, 2008). Bu durum kavramın anlaşılır ve tutarlı bir tanımlama çerçevesini oluşturmada birtakım engeller yaratsa da, şüphesiz hatırı sayılır medya ilgisi - sayısız güvenlik raporlarının sunduğu avantajlarla - bahse konu varsayımların incelenmesinde ve siber terörizmin telaffuz edilmesinde önemli bir rol oynamıştır.

Buradan hareketle, teorik çerçevesi çizilmeden komplovari bir temele dayanan ve sanılan tehlikeler ile siber terörizm olarak kabul edilecek etkinlikler arasındaki kurgusal ve semantik boşluk siber terörizm etrafında dönen tartışmaları daha da tetiklemektedir. Örneğin, bazıları siber ortamın teröristler için devletlere yönelik yeni bir dijital Pearl Harbor tehlikesi oluşturan realist bir senaryo arz ettiğini iddia ederken (Sınger ve Friedman, 2015) karşıt bir diğer grup ise geleneksel terörizm yöntemlerinin ve motivasyonlarının kısmen siber terörizmde de

gözlemleneceğini belirtmekle birlikte "Dijital Pearl Harbor" şeklindeki analojilerin abartılı bulduğunu ve bu senaryo şeklinde ileri sürülen tehditlerin kavramın ciddiyetine ve kuramsallığına zarar vereceğini ileri sürmüştür (Denning, 1999: 67-70, Weiman, 2004).

Siber terörizm kavramını ilk defa 1990'li yıllarda dile getiren Collin'e göre siber terörizm, uluslararası ortamda bilgi sistemlerinin, network ağlarının tüm bileşenleri ile teröristlerce kötüye kullanım şeklinde tarif edilmiştir (Collin, 1996). Collin'den sonra kavram uzmanlar tarafından güvenliğin sözlüğüne dâhil edilmiş ve literatürde tedricen adından söz ettirmeye başlamıştır. Kavramı 1998 yılı Center for Strategic and Internatıonal Studies kuruluşunun raporu ise önceden planlanan devlet altı gruplar ve bireyler tarafından bilgi ve bilişim sistemlerine, bilgisayar programlarına, veri tabanlarına yönelik şiddet hadiseleri ile sonuçlanmayı hedefleyen ve savaşçı olmayan birimlere yönelik tehdit ve hasar verici saldırılar olarak tanımlamıştır (Zheng ve Lewis, 2015).

Devletler bazında siber terörizm kavramını terörizm yasasında ilk yer veren ülke konumundaki İngiltere'nin yasasına göre siber terörizm, hükümeti ve toplumu etkilemek ya da baskı oluşturma saikiyle resmi birimlerin elektronik sistemlerine sızmak ve saldırılarla sistemi bozmak şeklinde tanımlanmıştır (UK Terorism Act, 2000). Kavram gün geçtikçe yapılan tanımlamaların parametrelerini aşmış ve geleneksel terörizm kavramının temel unsurlarını da ihtiva ederek kapsamını genişletmiştir. Farz-ı mahal 2000'li yılların ortasında yapılan bir başka tanımlamada kavram bir örgüt tarafından politik, psikolojik, sosyo-ekonomik, prestij ve de en önemlisi güvenlik tehdidi oluşturma gayesine erişmek maksadıyla bilişim sistemlerinin devlet kurumlarına yönelik olarak yıldırma, göz dağı verme ya da baskı altında tutmak amacıyla kullanılması şeklinde tanımlanmıştır (Sever, 2006: 2). ABD'nin iç istihbarat ve güvenliğinden sorumlu FBI'n tanımında ise siber terörizm iletişim ve bilişim imkânları dâhilinde bilgisayar kullanıcıları tarafından hükümetleri ya da toplumu belirli politik, sosyal ve ideolojik gündemlerine intibak ettirmek için kamu hizmetlerini sağlayan kritik altyapı sistemlerine yönelik bozma ya da işleyişi durdurma niyetiyle ve bunun sonucunda toplum içerisinde karmaşıklığa sebep olarak bir korku yaratma eğilimindeki suç teşkil eden fiiller olarak tarif edilmiştir. Kevin de kavramın küresel bilgi altyapısına yönelik saldırıları içermesi gerektiğini belirterek teröristlerin bu bilgi altyapılarına saldırarak sadece korku değil aynı zamanda şiddet iklimini sürekli kılmayı planladıklarını belirtmiştir (Kevin, 2006: 15).

Geleneksel terör mantalitesinin bir türü olarak kabul gören anlayış doğrultusunda siber terörizm politik güdülere sahip grupların bilgisayar, bilgi, gelişmiş ağlar ve teknolojik altyapılar kanalıyla yıkıcı ve kötü niyet barındıran eylemlerini yerine getirmek için kullandıkları bir terör türüdür. Bilişim sistemleri ve internet vasıtasıyla idare edilen bu kritik öneme sahip temel unsurlar göz önünde bulundurulduğunda birçok uzman siber terörizmin 21. yüzyılda geleneksel terörizmden daha tehlikeli hal alabileceğini ileri sürmektedir (Rogers 1999, Lynch ve Ryder, 2012: 264-265). Bu bağlamda gerçek şu ki, siber terörizm eylemleri ile ilgili hedefler ve riskler hükümetlerin değerli kayıtlarına, hava trafik kontrollerine, barajların denetimine, tıbbi kayıtlarına ve de finansal ve ticari altyapılarına yönelik tehdit oluşturmaktadır (Hansen ve vd., 2007: 1362-1374).

Yukarıdaki tanımlamalar ışığında siber terörizme dair gözlemlenen okuma, eylemlerin politik ve sosyal motivasyonları barındırması ve hedef olarak da bilgisayar, network ağları ve bilgi sistemleri şeklinde lanse edilmesi, amaç olarak da yaralama, ciddi hasar, korku iklimi ve ölüme sebebiyet verme gibi hedef odaklı güdüleri ihtiva etmiş olmasının gerekliliği üzerine yapılan vurgulardır. Maras da hedef odaklı yapılan tanımlamalardan hareketle siber teröristlerin politik, dini ve ideolojik sebeplerden dolayı devletlerin gözünü korkutma ya da onları amaçları doğrultusunda kritik altyapılara saldırmayı hedeflediklerini belirterek siber terörizme dikkat çekmiştir. Bu nedenle 21.yüzyılın bu yeni tehdidinin ABD'nin ekonomik unsurlarına zarar vermek için kritik altyapılarını hedef alabileceğini ve yaşam kayıplarına bile sebebiyet verecek cinste olduğunu belirtmiştir. Öte yandan Maras'a göre siber ortamdan kaynaklı bireylerin ya da organize olmuş terör gruplarının gerçekleştireceği her eylem ya da saldırı siber terörizm teşkil etmeyebilir. Conway ile beraber Maras siber terörizmin ortak tanımlamalarında akla ilk gelen noktalarının yıkıma ve hatta ölüme sebep olması gerektiği ve politik ve sosyal güdülerle eyleme dökülmesi gerektiğini ifade etmiştir (Maras, 2015: 6-8; Conway, 2002: 2). Bu durumda Maras ve Conway'ın ifadelerine göre siber terörizmin başlı başına büyük ölçekli yıkımlara ya da ölümlere sebebiyet veren gelişmeler olması durumunda terörizm kategorisine dâhil edilebilir.

Dorothy Denning de tam olarak hangi eylemlerin ve saldırıların ya da yapılış usullerinin siber terörizm kategorisinde yer alabileceğini belirttiği çalışmasında kavramı şu şekilde tanımlamıştır.

> *Siber terörizm genel olarak bilgisayarlara, ağlara ve buralarda gizli tutulan bilgiye yöneltilen kanun dışı saldırı ve de saldırı tehditlerinin siyasi ya sosyal amaçlara*

> *erişmek saikiyle bir hükümet ya da çalışanlarına baskı yapmak ve gözdağı vermek maksadıyla yapılması şeklinde anlaşılmaktadır. Buna ilaveten, bir saldırının siber terörizm olarak nitelendirilebilmesi için kişiler ya da mala karşı şiddetle sonuçlanması ya da en azından korku yaratacak kadar zarar verici olması gerekmektedir. Ölümle ya da yaralanma ile neticelendirilen saldırılar, patlamalar, uçak kazaları, su kirlenmeleri ve ciddi ekonomik kayıplar misal olarak gösterilebilir. Kritik altyapı sistemlerine karşı yapılan saldırılar etkilerine başlı olarak siber terörizm şeklinde adlandırılır. Hayati önemi olmayan hizmetlere yönelik akamete uğratıcı ya da çoğunlukla düşük profilde rahatsızlık veren saldırılar siber terörizm olarak adlandırılmaz (Denning, 1999: 269).*

Denning'in bu tanımlama ve yorumlaması, öte yandan siber terörizmin kavramsallaştırılmasına zarar veren karmaşıklığın giderilmesine kısmen hizmet etmiştir. Çünkü Denning siber teröristler ile kötücül korsanlar, bilgisayar ortamında haşarı olarak (prankster) nitelendirilenler, kimlik hırsızlığı yapanlar, sanal zorbalar ya da casuslar arasında amaçları ve motivasyonları bakımından ayrım yaparak sınıflandırmıştır (Denning, 1999: 9). Denning ve Maras'ın çizmiş olduğu kavramsallaştırma siber terörizmin politik, sosyal motivasyonları ve aynı zamanda ciddi hasar vermesi ve korku iklimi yaratma gibi geleneksel terörizm pratiklerine istinaden tanımlanması ve sınıflandırılmasını gerektirmektedir.

Yine Denning'in siber terörizmin tanımlamasına ilişkin çizmiş olduğu bir diğer önemli parametre ciddi hasar verme ölçütüdür. Buna göre bir eylemin siber terörizm olarak adlandırılması için politik ve sosyal motivasyonları içermesinin yanı sıra geleneksel terörizmde olduğu gibi korku ve kaos ortamı yaratmak için büyük ölçüde de ciddi hasara yol açma koşulunu içermesi gerekmektedir. Elektrik üretim tesisleri, haberleşme sistemi, su üretim sistemi, petrol ya da doğal gaz üretim sistemi ve de finansal kuruluş gibi kritik altyapılara ait ciddi derecede yıkıcı ve işleyişi durdurmaya yönelik saldırılar siber terörizm dâhilinde değerlendirilebilmektedir. Benzer argümanla Brenner de terörizm bağlamında değerlendirdiği hasar verme ölçütünü halkın moralini ve psikolojisini bozma niyeti olarak ele almıştır. Böylelikle teröristler maddi ve manevi değerleri tahrip etmeye, yaralanma ya da ölüme sebebiyet vererek öncelikli ve doğrudan doğruya temel motivasyonlarından biri olan hedef ülkenin halkına saldırıya açık olduklarını gösterme amacındadırlar. Brenner bu noktada, tıpkı klasik terörizm anlayışında olduğu gibi, siber terörizmin de benzer amaçlara ulaşmayı hedeflediğini ancak bunu yaparken tarz olarak toplumun bu modern dönemde önemli derecede işleyişine bel bağladığı bilgiye ve bilgi sistemlerine olan güveni sarsmak için yine teknolojiyi kullandıklarını iddia eder. Bu doğrultuda 1998 yılında ABD'de yazılımları manipüle edip elektrik sistemlerine saldırılar gerçekleştiren ve 11 kişinin ölümüne sebep olan saldırı türü siber terörizme en çarpıcı ve açık bir örnek teşkil etmektedir (Brenner, 2007: 386).

Bununla birlikte, siber terörizmin geleneksel terörizmin teorik konsepti ile uyumlu olan bir diğer önemli parametresi de korku unsurudur. Bu bağlamda, korku unsuru tıpkı geleneksel terörizmde olduğu gibi siber terörizm kavramı etrafında da ele alındığında etki odaklı ve niyet odaklı şeklinde tanımlama yapılabilmektedir. Buna göre, etki odaklı tanımda siber terörizm bilişim sistemlerinden herhangi biri aracılığıyla gerçekleştirilen ve yeterli düzeyde yıkıcı etkiye sahip saldırılar sonucunda oluşturulan korku havası şeklinde tanımlanırken, niyet odaklı tanımlamada ise siber terörizm yasa dışı ve politik saiklerle devletleri ve bu devletlerin toplumlarının gözünü korkutmak ya da bu birimleri kendi siyasal, ideolojik ve sosyal hedeflerine erişmede kabule zorlamak için bilişim sistemleri aracılığıyla gerçekleştirilen yasa dışı eylemler, şeklinde tanımlanmıştır.

Özetle, yukarıda kavramsal ve niteliksel özellikleri çizilen siber terörizmin hem geleneksel terörizme kıyasla hem de kendine has sunduğu olanaklarla kötücül niyetler barındıran birimlerin ilgi duymasının nedenleri oldukça fazladır. Öncelikle siber ortamın finansal ve de beşer bakımından daha az maliyetli olması, ileri derecede teknolojik araçların kullanımına ihtiyaç duyulmadan (kimi zaman bir cep telefonu, kimi zaman da tablet ve laptop vs.) metotların daha kolayca uygulama alanı bulması, faillerin kimliklerinin anonimliği ve bilinmezliği, aynı anda birden fazla hedeflerin kısa sürede hedeflenebileceği, saldırının tür olarak yeniliği ve dolayısıyla çekiciliği hasebiyle basında ve görsel medyada daha rahat ve etkili propaganda şansı vermesi gibi etmenler, terör gruplarına amaçlarına ulaşmada ihtiyaç duydukları ortamı sağlamaktadır.

Sonuç

Fiziksel olmayan güvenlik kategorisine dahil olan siber alan, 21. yüzyılın önemli güvenlik tehditlerindendir. Ağlara dayalı bilgi teknolojilerinin gelişimi ile beraber siber tehdit, saldırı, terörizm ve çatışma şeklinde adlandırılan siber güvenlik tehditleri eyleme dönüşmüş en ciddi çıktılar olarak göze çarpmaktadır. Bu bağlamda kendine has özellikleri ile siber uzaydan kaynaklı siber güvenlik tehditleri ve bu tehditlere karşı alınan tedbirlerin siber güvenlik olarak adlandırıldığı durum artık uluslararası sistem de, geleneksel güvenlik anlayışının dayattığı paradigmaları hasara uğratmıştır. Nereden geldiği belli olmayan ve uluslararası hukukta henüz kapsamına dair açıklayıcı tanımlamalar yapılmayan bu tehditler, güçlü ya da güçsüz farkı gözetmeksizin internete bağımlı her devleti ve toplumu hatta bireyi aynı ölçüde saldırıya açık ve vurulabilir duruma sokmaktadır. Dolayısıyla ilk etapta hem alana dair farkındalığı artırmak

hem de siber güvenliğin anlaşılmasını kolaylaştırmak adına bu alandan türeyen kavramlara odaklanmak bir ihtiyaçtır.

KAYNAKÇA

Al Jazera, (2010).Asia. http://www.aljazeera.com/news/asia/2010/12/20101241373583977.html (Erişim Tarihi: 11.10.2015).

Allen, Patrick D. And Demchak, Chris C. (2003). The Palestinian-Israel: Cyberwar. *Academıc Journal Article Military Review,* 83(2), 52.

Benedikt Mıcheal (1991). *Introduction & Cyberspace: Some Proposals, in Cyberspace: First Steps,* London: MIT Press

Berner, Sam (2003). Cyber-Terrorism: Reality or Paranoia? *South African Journal of Information Management.* 5(1), 1-4.

Bomse, Amy Lynne (2001). The Dependence of Cyberspace. *Duke Law Journal,* 50(6), 1717-749.

Caplan, Nathalie (2013). *Cyber War: the Challenge to National Security,* Global Security Studies, 4(1), 93-115.

Chang,Yu Li (2002). *Cyberspatial Cognition Approach to Thread Digital City in Physical City.* California State Polytechnic University, Pomona.

Collin, Barry (1996). The Future of CyberTerrorism, Proceedings of the 11th Annual International Symposium on Criminal Justice Issues, The University of Illinois at Chicago. http://www.acsp.uic.edu/OICJ/CONFS/terror02.htm (Erişim Tarihi: 14.04.2016).

Conway, Maura (2002). Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet, *First Monday,* 7(11), 1-9.

Conway, Maura (2008). Media, Fear andthe Hyperreal: The Construction of Cyberterrorism as the Ultimate Threat to Critical Infrastructures, Working Papers in International Studies Centre for International Studies Dublin City University.

Cooper, Barry (2004). *New Political Religions, Or an Analysis of Modern Terrorism.* Columbia: University of Missouri Press.

Cox, Christopher (2012). Cyber Capabilities and Intent of Terrorist Forces. *Information Security Journal: A Global Perspective*, 24(1-3), 31-38.

Curan, Kevin and Concannon Kevin (2007). Cyber Terrorism Attacks. (Edited By: Lech J. Janczewski and Andrew M.Colarik). Cyber Warfare and Cyber Terrorizm. London: IGI Global. 1-6.

Çifçi, Hasan (2013). *Her Yönüyle Siber Savaş.* Ankara: Tübitak Popüler Bilim Kitapları.

Denning Dorothy (2001). Is Cyber Terror Next?http://essays.ssrc.org/sept11/essays/denning.htm (Erişim Tarihi: 01.13.2016).

Denning, Dorothy (1999). Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy. (Edited By: John Arquilla ve David Ronfeldt).*Networks and Netwars, Rand Cooperatıon*, 239-288.

Denning, Dorothy (1999). *Informatıon Warfare and Security*. New York: Addison –Wesley

Dunn, Myriam Cavelty (2008). *Cyber Security and Threat Politics, US Efforts to Secure the İnformation Age.* London: Routledge Taylor and Francis Group.

Dunne, Robert (2009). *Computers and the Law An Introduction to Basic Legal Principles and Their Application in Cyberspace,* New York: Cambridge University Press.

Edwards Dave (2010). Robust ICSs Critical for Guarding Against Cyber Threats. *Journal American Water Works Association,*102 (11), 30-33.

Eran, Oded (2009). Operation Cast Lead: The Diplomatic Dimensio. *Strategic Assessment*. Volume 11(4), 13-17.

Follath Erich and Holger Stark (2009). The Story of 'Operation Orchard', How Israel Destroyed Syria's Al Kibar Nuclear Reactor. http://www.jmhinternational.com/news/news/selectednews/files/2009/11/20091103_SpiegelOnline_TheStoryOfOperationOrchard.pdf(Erişim Tarihi: 21.01.2016).

Geers, Kenneth (2011). Sun Tzu and Cyber War, Cooperative Cyber Defence Centre of Excellence (CCD COE). https://ccdcoe.org/sites/default/files/multimedia/pdf/Geers2011_SunTzuandCyberWar.pdf (Eriim Tarihi: 08.01.2016).

Giles, David (2006). Constructing Identities in Cyberspace: The Case of Eating Disorders. *British Journal of Social Psychology*. 45, 463–477.

Gorman, Sean P. (2006). A Cyber Threat to National Security? (Edited By: Philip E. Auerswald, Lewis M. Branscomb, Todd M. La Porte, and Erwann O. Michel-Kerjan). *Seeds of Disaster, Roots of Response.* Cambridge: Cambridge University Press, 239-257.

Gücüyener, Ayhan(2015). Kritik enerji Altyapılarına Yönelik Gerçekleşmiş Siber Saldırılara İlişkin Bir Değerlendirme. (Editör: Mesut Hakkı Caşın). Uluslararası Kritik Enerji Altyapı Güvenliği: Yeni Tehditler ve Fırsatlar. *Hazar Strateji Enstitüsü*.18-39

Hackers and What They are Into (2015). https://ohitsmerivera.wordpress.com/tag/20-and-robert-lyttle/(Erişim Tarihi: 29.11.2015).

Hansen, James Lowry, Paul B. Meservy Rayman and McDonald, Dan (2007). *Genetic Programming for Prevention of Cyberterrorism Through Dynamic and Evolving Intrusion Detection*. Decision Support Systems, 43(4), 1362-1374.

Heidenreich, Brianna and David H. Gray (2013). Cyber-Security: The Threat of the Internet.*Global Security Studies*, 4(3), 17-26.

Heyligen, Francis and Joslyn Cliff (2001). Cybernetics and Second-Order Cybernetics. (Edited By: R.A. Meyers).*Encyclopedia of Physical Science & Technology*. (Thırd Edition), New yok: Academic Press.

Heylighen, Francis and Joslyn Cliff (2001). Cybernetics and Second-Order Cybernetics. (Edited By: R.A. Meyers).Encyclopedia of Physical Science & Technology. (Thırd Edition), New yok: Academic Press.

Hua, Jian and Bapna Sanjay (2012). How Can We Deter Cyber Terrorism? *Information Security Journal: A Global Perspective.* 21(2), 102-114.

Karagül, Özkan (2015). Bilgi Teknolojileri ve Uluslararası ilişkilerde Fırsat-Tehdit Paradoksu. *Bilgi Ekonomisi ve Yönetimi Dergisi,* 10(1), 115-126.

Kibaroğlu, Mustafa (2002). 11 Eylül Ardından Strateji, Tehdit ve Caydırıcılık. Foreign Policy, http://www.mustafakibaroglu.com/sitebuildercontent/sitebuilderfiles/Kibaroglu-11EylulArdndanStratejiTehditCaydiricilik-22dec01.pdf (Erişim Tarihi: 02.09.2016).

Korns, Stephen W and Kasternburg, Joshua E. (2008-09). Georgia's Cyber Left Hook. *Parameters*, 60-76.

Lovelace, Douglas (2015).*The Cyber Threat, After September 11*. Oxford University Press.

Lynch Orla and Ryder Christophr (2012).Deadliness, Organisational Change and Suicide Attacks: Understanding the Assumptions İnherent in the Use of the Term 'New Terrorism.,*Critical Studies on Terrorism*, 5(2), 257-275.

Maras, Marie-Helen (2015). *Computer Forensics: Cybercriminals, Laws, and Evidence*. Sudbury, MA: Jones & Bartlett Learning.

Nye, Joseph, Jr. (2011). Nuclear Lessons for Cyber Security? Strategic Studies Quarterly, Wınter-2011, 18-38.

O'Connell, Mary Ellen and Louise Arimatsu (2012). Cyber Security and International Law, International Law: Meeting Summary.*Chatham House*, 1-12

Öğün Mehmet Nesip, Kaya Adem, (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler, Security Strategies Year: 9 Issue: 18, 145-181.

Özcan, Mehmet (2002). Siber Terörle Mücadelede Karşılaşılan Zorluklar-I. http://www.turk-internet.com/portal/yazigoster.php?yaziid=4099 (Erişim Tarihi: 03.04.2016).

Özcan, Mehmet (2004). Yeni Milenyumda Yeni Tehdit: Siber Terör, *Türk Harb-İş Dergisi*, 210, 39-40

Punday, Daniel (2000). The Narrative Construction of Cyberspace: Reading Neuromancer. Reading Cyberspace Debates, *College English*, 63(2), 194-213.

Rathmell, Andrew (1997). Cyber-terrorism: The Shape of Future Conflict?*The RUSI Journal*,142(5).

Reed, Chris (2012). *Making Laws for Cyberspace*.Oxford: Oxford University Press.

Rheingold, Howard (1992). *Virtual Reality: The Revolutionary Technology of Computer-Generated Artificial Worlds - and How It Promises to Transform Society*. New York: A Touchstone Book Simon & Shuster.

Rogers M. (1999). *Pyschology of Computer Criminals, In Proceedings of the Annual Computer Securiy Instıtute Conference*. St. Louis, MO.

Schmid Alex P. and Albert J. Jongman (1988). Political Terrorism: *A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature.* London: Transaction Publishers.

Sever, Muhammd (2006). *Siber Terörizm vee Karşı Tedbirler*. Ankara: Terörizmle Mücadele Mükemmliyet Merkezi.

Shackelford, Scott J. (2014). *Managing Cyber Attacks in International Law, Business, and Relations.* New York: Cambridge University Press.

Singer P.W and Friedman Allan (2015). *Siber Güvenlik ve Siber Savaş*. Ankara: Buzdağı Yayınevi

Singer, David, J. (1958).Threat-Perception and the Armament-Tension Dilemma. *The Journal of Conflict Resolution, Studies on Attitudes and Communication*, 2(1), 90-105.

Stevens, Tim (2015). *Cyber Security, Community, Time, Cyber Security and the Politics of Time.* Cambridge: Cambridge University Press.

Susan W. Brenner (2007). At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare.Journalof Criminal Law. & Criminology, 97(2), 379-476.

Taliharm Anna-Maria (2010). Cyberterrorism: in Theory or in Practice? *Defence Against Terrorism Review*, 3(2), 59-74.

United Kingdom Terrorism Act of 2000 (2000). http://www.legislation.gov.uk/ukpga/2000/11/pdfs/ukpga_20000011_en.pdf (Erişim Tarihi: 13.02.2015).

Ünver Mustafa, Canbay Cafer ve Mirzaoğlu A.G (2009). Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut durum ve Alınması Gereken Tedbirler. *Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı,* Mayıs 2009.

Weimann, Gabriel, (2004). Cyberterrorism How Real Is the Threat? Unıted States Instıtute of Peace, 2004, Special Report.

What is a Script Kiddie? http://www.pctools.com/security-news/script-kiddie/ (Erişim Tarihi: 03.02.2016).

Zheng Denise E. and James A. Lewis, (2015). Cyber Threat Information Sharing Recommendations for Congress and the Administration, A Report of the CSIS Strategic Technologies Program

IŞID siber saldırı düzenleyebilir mi? https://siberbulten.com/strateji-guvenlik/isid-siber-saldiri-duzenleyebilir-mi/ (Erişim Tarihi: 01.09.2016).

http://www.dijitalajanslar.com/internet-ve-sosyal-medya-kullanici-istatistikleri-2016/ (Erişim Tarihi: 22.08.2016)

ISSN: 2587-1218

SİBER GÜVENLİK VE ULUSLARARASI GÜVENLİK İLİŞKİSİ

Cihan DABAN*

Özet

Güvenlik kavramı, insanoğlunun varoluşundan bugüne dek varlığını sürdürmüştür. Toplumsal yaşamın bir parçası haline gelen kavram, tarihsel olaylar ve teknolojik değişimler ışığında çeşitli evrelerden geçmiştir. Bu evrelerden biri de, II. Dünya Savaşı sonrası dönemi kapsamaktadır. 20. yüzyılın ikinci yarısında İnternetin icat edilmesi ve teknolojik gelişmelerin çeşitlilik arz etmesi, güvenlik algısına yeni bir bakış açısı kazandırmıştır. En basit tanımıyla güvenlik; korunma, barınma ve tehlikelerden uzak olma anlayışını sağlamaktadır. Ancak internetin ortaya çıkması ve bilgisayarların giderek yaygınlaşması ile birlikte bu anlayış saldırılara maruz kalmıştır. Bu durum güvenlik algısını olumsuz etkilemiştir. Güvenliğin olumsuz etkilenmesi sadece toplumsal veya ulusal bağlamda olmamıştır. Bu etki uluslararası alana da yayılmıştır. Bu etkinin engellenmesi veya tamamen ortadan kalkması amacıyla uluslararası alanda siber güvenlik politikaları üretilmeye çalışılmıştır. Bu bağlamda makale, siber güvenlik ile uluslararası güvenlik ilişkisini ele almakta ve ne tür önlemlerin alınması gerektiği konusuna da vurgu yapmaktadır.

Anahtar Kelimeler: Siber Saldırılar, Güvenlik, Siber Güvenlik, Uluslararası Güvenlik,

LINKS BETWEEN CYBERSECURITY AND INTERNATIONAL SECURITY

Abstract

Security term has been subsisted since existing of human being. The term that became a part of social life has been various phases under the light of historical events and technological changes. One of those phases covers Period of after World War II. Invention of internet, variety of technological developments in the second half of century 20 gained a new aspect to security sense. “Security” in the simplest definition provides protection, accommodation and to be far from dangers. However, this understanding exposed to attacks upon occurring of internet and becoming common of computers. This case affected security sense negatively. Affecting negatively of security was not only social or national aspects. This affect didn’t common into international area. Cyber policies had been tried to be produced in international area to prevent this affect or to remove it completely. In this mean, this article considers relation between cyber security and international security and what kind of precautions should be taken is emphasized.

Key Words: Cyber attacks, Security, Cyber Security, International Security.

* Selçuk Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Bölümü, ÖYP Araştırma Görevlisi, dabancihan@gmail.com

Giriş

Uluslararası ilişkilerde güvenlik algısı en önemli unsurlardan biridir. Güvenlik, sadece uluslararası ilişkilerde değil, ulusal alanda da önem arz etmektedir. Çünkü ulusal güvenlik, uluslararası güvenliğin bir bütünün parçası gibidir. Bu bağlamda güvenlik algısı devletlerin vazgeçilmez bir parçası haline gelmiştir. Böyle bir duruma gelmesindeki en önemli faktör ise, bireyler ve toplumlardır. Çünkü bireylerin veya toplumların güvenliği sağlanamadığı sürece devletlerin güvenliği de tehdit altına girebilmektedir. Böyle bir durum ise ciddi sorunlara yol açabilmekte hatta devletlerin parçalanmasına kadar gidebilmektedir. Bundan dolayı güvenlik kavramı herkesçe (birey-toplum ve devlet liderleri) önem arz etmektedir(Baylis, 2008: 74-75).

Uluslararası güvenlik, devletlerin ve uluslararası kuruluşların karşılıklı koruma ve güvenliği sağlamak adına oluşturmuş oldukları önlemlerdir. Başka bir ifadeyle, uluslararası güvenliğin sağlanması konusu hem devletlerin hem de uluslararası kuruluşların gerekli tüm tedbirleri almakla yükümlü oldukları bir alandır. Fakat bu alan, bazen sekteye uğratılabilmektedir. Bu durumda güvenliğin tehdit altına girdiği veya saldırılara maruz kaldığı görülebilmektedir. Özellikle II. Dünya Savaşı'ndan sonra tüm dünya coğrafyası büyük bir saldırının eşiğinde olmaya başlamıştır. Bu saldırı, doğrudan askeri kuvvet kullanımıyla müdahale edilmeye başlandığı gibi dolaylı olarak da sistemik bir yapıyla oluştuğu da görülmüştür/görülmektedir(Yılmaz, 2007: 72-76).

Dolaylı olarak yapılmaya başlanan bu saldırı/saldırılar internetin ortaya çıkması ve bilgisayarların kullanılmasıyla etkisini göstermiştir. İnternetin ortaya çıkması, bilgisayarların giderek artması ve yeni teknolojik aletlerin icat edilmesi, dünya coğrafyasındaki saldırıların yöntemini değiştirmiştir. Başka bir deyişle, yüzyıllar boyu süre gelen doğrudan müdahale etme yöntemi, az da olsa dolaylı bir yönteme dönüştüğü görülmüştür. Özellikle 21. yüzyıl, internetin bir mermi gibi etkili olduğu bir yüzyıl olmuştur(Bilgiç, 2011: 130-135). Çünkü II. Dünya Savaşı'ndan sonra uluslararası alanı kapsayan bir güvenlik kaygısı ortaya çıkmış ve bu durum 21. yüzyılda farklı bir dönüşüme yol açmıştır. Bunun en temel nedeni ise internetin yaygınlık kazanması ve siber denilen tehdidin oluşmasıdır. Siber veya sibernetik denilen bu tehdit, bireylerin, toplumların ve devletlerin güvenliğini ciddi oranda sarsmıştır. Siber veya sibernetik yeni bir kavramdır. Nitekim hızlı bir yayılım göstermiş ve birçok alanı etkilemiştir. Makalede siber güvenliğin uluslararası güvenlikle ilişkili olduğu alan ele alınmıştır. Ayrıca siber ile ilgili bazı kavramlara da yer verilmiştir(Sandıklı, 2012: 3-4).

Kavramsal Tanımlamalar

Son yıllarda siber saldırılar tarafından artan tehditler çok sayıda ülkeyi endişelendirmektedir. Bu saldırıların giderek artması ülkelerin güvenliğe dair yeni politikalar üretmesine yol açmıştır. Bu ülkelerden bazıları, ekonomik anlamda zengin olduğundan yatırımların büyük bir kısmını siber güvenliğe harcamıştır. Çünkü hem sosyal yaşamın hem de milli güvenliğin sanal dünya ile giderek iç içe olmaya başlaması, beraberinde güvenliği de riske atmıştır/atmaktadır. Siber güvenlik alanına büyük yatırımlar yapan devletler, bu alanda insanları uzmanlaştırmak amacıyla birçok stratejiler geliştirmeye başlamıştır(Ünver-Canbay, 2010: 96-97).

Ekonomik olarak zayıf olan devletler ise, bu durumu geriden takip etmekte ve büyük devletleri örnek almaktadır. Başka bir ifadeyle ekonomik anlamda zayıf olan devletler, güçlü devletlerin stratejilerini geriden takip etmeye çalışmışlardır. Çünkü siber denilen olgu, saldırılarda, tehditlerde, güvenliği sarsma da sayılabilecek birçok alanda önemli etkiler oluşturmakta ve dünya devletlerini birbirine düşürebilmektedir. Bu nedenle 21. yüzyılın en önemli konularından birisi olan siber algısı, neredeyse tüm dünya devletlerini endişelendirmektedir. Siber algısını anlayabilmek için temel bazı kavramlara göz atmak ve bu kavramlarla olan ilişkisini incelemek yerinde olacaktır(Bıçakçı, 2013: 1-4).

Güvenlik

Güvenlik terimi, insanoğlunun var oluşundan itibaren geçirdiği her bireysel ve toplumsal evrede kullanılan bir kavram olarak süregelmiştir. Öte yandan birçok anlam içermektedir. Bireyin güvenliği, ailenin güvenliği, toplumun güvenliği, bölgenin güvenliği ve devletin güvenliği gibi birçok alanla iç içedir. Bundan dolayı yaşamsal bir zorunluluk gibi görülmektedir(Dedeoğlu, 2003: 9-14). Batı geleneğinde bu kavram zihnin felsefi ve psikolojik durumunu ifade eden anlamında ilk kez Cicero ve Lucretius tarafından *securi*tas olarak kullanılmıştır. Ardından 1. yüzyıldan itibaren *Pax Romana* bağlamında siyasi bir nitelik kazanmıştır. Güvenliğin bir diğer anlamı da Thomas Hobbes ile başlayan bu kavramın süper devletin doğuşu ile ilgili olmasıdır(Brauch, 2008: 3).

Uluslararası ilişkilerde devlet en önemli unsurlardan biridir. Devletin güvenliği sağlandığı sürece diğer alanlarda da (birey, aile, toplum ve bölgesel) güvenliğin sağlanacağı anlayışı hâkimdir. Çünkü devlet, tehditlere ya da saldırılara maruz kaldığında devlet çatısı altında olan tüm yerlerin de aynı şekilde tehditlere ve saldırılara maruz kalacağı aşikârdır. Bu nedenle

uluslararası ilişkilerde güvenlik algısı, devletin bekası için önemli bir faktör olmuştur(Özlük, 2014: 103-105). Toplum yaşamında ise güvenlik; yasal düzenin herhangi bir aksaklığa uğratılmadan yürütülmesi ve bireylerin korkulara kapılmadan yaşayabilmesi durumudur. Toplumsal yaşamda en önemli araçlardan biri şüphesiz iletişimdir. İnsanoğlu tarih boyunca farklı metotlar ve araçlar kullanarak iletişim ağını geliştirmiş ve sürekli etkileşim halinde olmuştur. Duvarlara çizilen resimler, güvercinlerin parmak uçlarına konulan mektuplar ve ateşlerden çıkan dumanlar gibi birçok metot kullanılarak insanlar arasında iletişim/haberleşme sağlanmaya çalışılmıştır(Ünver-Canbay, 2010: 94).

19. yüzyılda insanlar arasında farklı bir iletişim ağı olmuştur. Çünkü bu yüzyılda hem telgraf hem de telefon ağı önemli iletişim aracı olarak kullanılmaya başlanmıştır. 20. yüzyılın ortalarında ise radyo ve televizyonun icadı ile uluslararası alanda kitlesel iletişim sağlanmıştır. 20. yüzyılın sonlarına doğru bilgisayarların, mobil iletişim araçlarının ve internetin icadı tüm dünya coğrafyasında büyük bir etki oluşturmuş ve iletişim kanallarının yaygınlaşmasına sebebiyet vermiştir. İnternetin 21. yüzyılın başlarından itibaren hızla ticarileşerek gelişmesi ve yayılması, insanoğlunun yaşamında önemli köklü değişimlere yol açmıştır. Bilgisayar, mobil iletişim kanalı ve internet ağı uluslararası ilişkilerde ciddi oranda kolaylıklar sağlamıştır. Ancak diğer taraftan da siber denilen yeni bir risk ortamını da beraberinde getirmiştir. Bu durum bir kısım sorunların ortaya çıkmasına da yol açmıştır(Bıçakçı, 2013: 1).

Siber Ortam

Siber kavramı, Fransızca kökenli *sibernetik* kelimesine dayandırılır. İngilizcedeki *cyber* kelimesinin Türkçeleştirilmiş halidir. Siber kavramı, internetin icadıyla birlikte yaygınlık kazanmış ve çok sık ifade edilmeye başlanmıştır. Bu durum yeni bir alana veya ortama zemin hazırlamıştır. Siber ortamın oluşmasında en önemli unsur sanal âlemdir. Sanal âlem denildiğinde ise internet ortamı akla gelmektedir. Bundan hareketle siber ortam kavramı internet ortamını da kapsayan bir üst terim olarak görülmektedir. Bilgisayar, internet ve cep telefonlarının kullanımı, bilişim sistemlerindeki hızlı gelişimi takip etmek, insanlar tarafından oldukça yaygınlık kazanmıştır. Bilişim sistemlerindeki bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmetin tüm dünyaya ve hatta uzaya yayılmış durumda olması ve bunları birbirine bağlayan ağların mevcut olması siber ortamı oluşturmaktadır. Uzaya yayılmış olan siber ortam bir nevi siber uzayı ortaya çıkarmaktadır. Siber Uzay kavramını ise ilk defa bilim kurgu romanlarıyla bilinen William Gibson tarafından 1980'li yılların başında kullanılmıştır(Kara, 2013: 4).

Siber uzay terimi, günümüzde halen etkisini sürdürmektedir. Siber uzay teriminin yerine Ulusal Siber Güvenlik Stratejisinde siber ortam terimi tercih edilmiş ve tanımlanmıştır. Çünkü siber ortam, birçok alanda ve bölgede etkili olmaktadır. Kısacası tüm dünya devletleri siber ortamdan etkilenmekte ve bu ortama göre hareket etmektedir. Çünkü her türlü hizmet siber ortamda gerçekleşmektedir. Başta internet olmak üzere, internetin olmadığı ve bilgisayarların sayısal verilere ulaştığı alanlarda da siber ortam söz konusu olmaktadır. Bu nedenle sadece internetin olduğu alanlar değil, internetin olmadığı alanlarda da etkisini göstermektedir. Özetle siber ortam için şu ifade kullanılabilir: internet ağının olduğu alanlar başta olmak üzere, internetin olmadığı ancak bilgisayarlar aracılığıyla elde edilen sayısal veriler, öte yandan elektronik teçhizat vasıtasıyla da ulaşılabilen tüm imgesel (rüya gibi.) alanlar siber ortamı oluşturmaktadır(Hill and Hughes, 1998: 17-21).

Siber ortam fayda sağladığı gibi önemli zararlara da yol açmaktadır. Bu yolların çoğu internet ortamında gerçekleşmektedir. Örneğin, internet aracılığıyla iletişim teknolojilerini kullanıp, herhangi bir kimseyi rahatsız etmek veya küçük düşürücü sözlerde bulunmak gibi faaliyetler veya bir kimseye ait bilgilerin ele geçirilip o bilgilerle kişinin tehdit edilmesi gibi durumlar sayılabilir. Bu zararlar genel olarak güvenliği tehdit etmekte ve güvensizlik ortamına sebebiyet vermektedir. Bu durum siber güvenlik kapsamına girmekte ve yeni bir alan oluşturmaktadır. Kısacası siber ortamı oluşturan bilişim sistemlerinin saldırılardan/saldırganlardan, virüslerden, hackerlardan ve tehditlerden korunması amacıyla siber güvenlik alanları/ortamları oluşturulmaya çalışılmıştır. Bu kapsamda siber güvenlik, siber ortama zarar verebilecek saldırıları önlemeye çalışmakta veya bu zararları en aza indirmeye ya da tamamen ortadan kaldırmaya yönelik faaliyetler gerçekleştirmektedir denilebilir(Nojeim, 2010: 125-126).

Siber Saldırılar/Saldırganlar

20. yüzyılın en önemli icatlarından biri olan internet, elektronik haberleşmeyi sağladığı gibi hızlı ve kolay bir şekilde işlerin yürütülmesini de insan hayatına kazandırmıştır. Haberleşme alanındaki gelişmeler iletişim ağını genişletmiştir. Bu durum fayda sağladığı gibi bazı önemli sorunları da beraberinde getirmiştir. Mobil iletişim ağlarından cep telefonlarının kullanılmaya başlanması gibi yeni bir dönem başlatmıştır. Bu kullanım, fayda sağlayıcı bir durum olarak görülmektedir. Ancak kişisel kullanım aracı olarak kabul edilen cep telefonu, günlük hayatta insan vücudunun bir organıymış gibi görülmesi sağlık açısından bazı sorunlara yol açmıştır.

Sürekli telefonla uğraşılması sonucu gözlerde meydana gelen bozukluklar örnek gösterilebilir(Kara, 2013: 14-15).

Kişisel akıllı telefonların giderek artması ve geniş bir alan bulması, siber saldırılar bakımından önemli bir yer tutmaktadır. Twitter, Facebook, Instagram ve Swarm gibi hesapların akıllı telefonlarda mevcut olması ve kişilerin bu hesapları kullanması birer siber saldırı yöntemi olarak görülebilir. Facebook üzerinden paylaşılan bir resim veya bir yazı bazen sosyal medyada bazı kişilerce eleştirilebilmekte ve paylaşımı yapan özneye sosyal medya üzerinden yorumlar yapılarak siber saldırılarda bulunulabilmektedir. Bu durum siber saldırı yöntemlerinden birini oluşturmaktadır. Çünkü özne, sosyal medya üzerinden bir saldırıyla karşı karşıya kalmaktadır. Öte yandan tehditlere de maruz kalabilmektedir. Tüm bunlar siber saldırılar/saldırganlar olarak görülmektedir(Hoffman and Schweitzer, 2015: 72-74).

Siber saldırganlar, sadece kişisel akıllı telefonlarda görülmemektedir. Devlet kurum ve kuruluşlarında da görülebilmektedir. Bu anlamda siber saldırganlar, hedefledikleri kurum ve kuruluşlar karşısındaki eylemlerine göre içeriden kaynaklanan saldırılar ve dışarıdan kaynaklanan saldırılar olmak üzere iki gruba ayrılabilir(Bıçakçı, 2012: 214). İçeriden kaynaklanan saldırılar, kurum tarafından bilişim sistemlerine erişim yetkisi verilen kişilerce yapılan saldırılardır. Dışarıdan kaynaklanan saldırılar ise; kurum dışındaki kişilerce yapılmaya çalışan saldırılardır. Yani kurumda çalışmayan kişiler tarafından kurum içi eylemlere müdahale edilmeye çalışılmasıdır. Bu çalışmalar, kötü amaçlı olup, hackerlar, vandallar ve suçlular tarafından uygulanmaktadır (Kara, 2013: 9).

Bazı hackerlar, can sıkıntısından yola çıkarak gizliliği esas alınmış ya da kısıtlanmış olan bilgiyi elde etmeyi hedeflemektedir. Vandallar, olabildiğince en büyük zararı vermeyi amaçlamaktadır. Suçlular ise; maddi kazanç elde etme fikriyle, hedefine ulaşmak için başta casusluk, yolsuzluk, hırsızlık ve bu gibi her türlü kötü taktiği kendilerine meslek edinebilmektedir. Bu durumlar siber ortamda birer saldırı yöntemini oluşturmaktadır(Han ve Çelikpala, 2016: 81). Bu söylemler bağlamında; kısıtlanmış herhangi bir bilgiyi ele geçirmek, sosyal medya üzerinden psikolojik tehdit oluşturmak, devlet kurum ve kuruluşlarına yönelik iç ve dış baskıda bulunmak ve siber ortamdaki güvenliği ortadan kaldırmak gibi amaçlar doğrultusunda gerçekleştirilen tüm bu faaliyetlere siber saldırılar yöntemi denilebilir. Bu durum siber güvensizlik ortamına da sebebiyet vermektedir.

Siber Güvenlik

İletişim, haberleşme ve paylaşma alanı olarak ortaya çıkan internet, aynı zamanda tüm dünya coğrafyasını hızlı bir şekilde etkilemiştir. Özellikle 21. yüzyıl, dünya coğrafyasının internet ağıyla iç içe olma yüzyılı olmuş ve olmaya devam etmektedir. Çünkü internet aracılığıyla tüm dünya insanları birbirleriyle hızlı bir şekilde iletişim içerisine girmiş ve uluslararası ilişkiler alanında devletlerarasında önemli ticari, siyasi, ekonomi ve sosyokültürel alanlarda güçlü bir bağ oluşmuştur. Tüm bunlar internet aracılığıyla daha hızlı yapılmaktadır. İnternetin üç temel başat unsuru vardır. Bunlar; bilgisayar, kullanıcı ve ağdır(Bıçakçı, 2013: 4-8).

Giderek değişen bilgisayar teknolojileri ve çeşitli yeteneklere sahip olmaya başlayan kullanıcı kesimleri sayesinde ağ teknolojilerinin de geliştiği görülmüştür. Bu durum devlet kurum ve kuruluşlarında etkisini göstermiş/göstermektedir. Bilişim sistemleriyle daha hızlı hizmet veren kurum ve kuruluşlar, sadece ulusal alanda değil, uluslararası alanda da bir güvenlik sorunuyla karşılaşmaktadır. Çünkü bilişim sistemleri, bilgi ve iletişim teknolojileriyle sağlanan her türlü hizmeti sunmaya çalışmaktadır. Bu hizmet, internet aracılığıyla sadece ulusal ortamda değil uluslararası ortamlarda da sunulduğu için bazen önemli güvenlik sorunlarına yol açmaktadır. Bu nedenle hem kurum ve kuruluşların hem de kullanıcıların varlıklarını korumak amacıyla siber güvenlik ortamı sağlanmaya çalışılmıştır(Ünver-Canbay, 2010: 94).

Siber güvenliğin sağlanmasında ise temel bazı maddeler söz konusudur. Bunlar; teknolojik gelişmeler, iyi üretilmiş politikalar, yol gösterici yöntemler, güvenliğe dair eğitimler, eğitime dair uygulamalar, güvenliğin sarsılmasına yönelik tehditlerin ortadan kaldırılmasına dair projeler ve oluşabilecek risk yönetimine karşı alınacak tedbirler gibi birçok madde sayılabilir. Siber güvenlik daha çok tehdit ve risklere karşı önlem alır. Tehdit, bir kurumun veya sistemin zarar görmesi sonucu istenmeyen bir olayın veya durumun ortaya çıkmasıdır. Ancak bu durum ortaya çıkmadan önce siber güvenlik, gerekli tedbirleri almakla görevlidir. Risklerin oluşmasına karşı da siber güvenlik ön planda olmaktadır. Risk, oluşan tehditlerin bir veya birden çok bilgi açıklığına ulaşmayı ve gerekli zararları vermeyi amaçlamaktadır. Fakat siber güvenlik tarafından bu risklerin engellenmeye çalışıldığı görülmektedir(Güntay, 2015: 477-489).

Sonuç olarak siber güvenlik alanı üç temel aşamada sağlanabilir. Bunlar; erişim kontrolü, kimlik denetimi ve yetkilendirme görevidir. Bu bağlamda siber güvenlik; bilgiye erişimin

denetlenmesini, bilgi sistemlerine yetki görevi olmadan erişmenin engellenmesini, kullanıcı düzeyinde olmayan varlıkların erişime ulaşmasına izin verilmemesini, kurum ve kuruluşlardaki hizmetlerin korunmasını, yetkisiz işlemlerin tespit edilmesini, çalışma ortamlarındaki bilginin korunmasını ve herhangi bir kişiye/varlığa ait kimliklerin denetilmesini sağlamaktadır(Akyeşilmen, 2016: 1). Başka bir deyişle siber güvenlik; hackerlar, iç ve dış siber saldırganlar, virüsler, casus yazılımlar kısacası zararlı yazılımlar tarafından gelebilecek tüm olumsuz/zararlı eylemleri engellemesidir. Çünkü zararlı yazılımların temel amacı insanlara, teknolojilere ve süreçlere karşı bir saldırı ortamını oluşturmaktır. Buradaki en temel nokta ise zararlı yazılımlar tarafından sistemlere yetki erişimi olmadan müdahale edilebilmesidir. Böylelikle yetki hakkı olmadan istenilen verilerin/bilgilerin elde edilmesi sağlanmış olacaktır. Ancak siber güvenlik tüm bu yetkisiz erişimleri ya en aza indirgemekte ya da tamamen yok etmektedir. Bundan dolayı siber güvenlik hem ulusal hem de uluslararası ilişkilerde önemli bir yer tutmaktadır(Kara, 2013: 52-54) .

Uluslararası İlişkilerde Güvenlik Algısı

Uluslararası ilişkiler alanında güvenlik teriminin önemli bir yeri vardır. Birey, toplum ve devlet düzeyinde ele alınan güvenlik terimi bir ülkenin hem iç meselelerinde hem de dış meselelerinde önem arz etmektedir. Siyasi, ekonomik, sosyokültürel vb. gibi birçok alanda etkisini göstermektedir. Bireyler için güvenlik ne kadar önemli ise devletlerarası ilişkilerde de o kadar önemlidir. Güvenliğin birden çok tanımı mevcuttur. Ancak tüm tanımlarda ortak olan görüş saldırılardan, tehlikelerden ve korkulardan uzak kalma anlayışı olmuştur(Özcan, 2011: 447).

Uluslararası ilişkilerde sistemi anlamaya ve açıklamaya yönelik farklı yaklaşımlar söz konusudur. Bu yaklaşımlar genellikle güvenlik algısını ele almıştır. Machiavelli'ye göre, devletin varlığını koruması, tehlikelerden ve tehditlerden uzak olması güç ile mümkün görülmektedir. Çünkü güçlü olan devlet güvenliğini daha iyi sağlayabilmektedir. Uluslararası alanda devletler birbirlerine karşı birer tehdit unsurudur. Böyle bir alanda Machiavelli'ye göre devletin güvenliği iyi yönetimle örtüşük kabul edilmektedir. Yönetim iyi bir şekilde sağlanırsa devletin güvenliği de güce bağlı olarak iyi sağlanmış olacaktır(Machiavelli, 2001: 64-75).

Hugo Grotius ise, uluslararası sistemi anarşik olarak değerlendirmektedir. Anarşik olmasının sebebini de bu sistemi belirleyecek bir üst otoritenin olmadığını vurgulamaktadır. Çünkü her devlet, çıkarları doğrultusunda hareket etmekte ve ona göre politikalar yürütmektedir. Bu durum devletler için tehdit oluşturmakta ve güvenlik sorununu ortaya çıkarmaktadır. Grotius'a göre güvenlik algısı ikiye ayrılmaktadır. İlki, devletin güvenliğinin uluslararası alanın tümünü düzenleyen güvenlik algılarıyla ilişkili olmasıdır. İkincisi ise, devletlerin kendilerini dışarıdan gelen tehlikelere ve saldırılara karşı savunması/korumasıdır. Buradan hareketle devletler birbirlerine birer tehdit olarak görülmektedir(Grotius, 2011: 20-27).

Grotius ile aynı dönemde (17. yüzyıl) yaşamış olan Thomas Hobbes, *Leviathan* adlı eserinde insan davranışlarından yola çıkarak uluslararası sistemi değerlendirmiştir. Eşit ve akıllı varlıklar olarak dünyaya gelen insanların, amaçlarına ulaşmak için istek ve arzularının peşinden koştuğunu ve bu durumun onları kaçınılmaz olarak bir mücadelenin içine sürüklediğini vurgulamaktadır. Bu mücadelenin temelinde ise insanın kendisine olan güvensizliği, öte yandan herkesten üstün olma arzusu ve birbirlerine olan rekabetleri yatmaktadır. Bu gelişmelerin oluşmasında Hobbes, eşitliği güvensizliğin temel bir nedeni olarak, güvensizliği de çatışmanın ve saldırmaların bir unsuru olarak görmektedir(Hobbes, 2005: 9-13).

18. ve 19. yüzyıllarda ortaya çıkan Fransız İhtilali, Sanayi Devrimi ve sömürgecilik faaliyetleri gibi olaylar dünya coğrafyasında güvenlik algısına yeni bir boyut kazandırmıştır. Özellikle sömürgecilik faaliyetlerinin başlaması hem dünya coğrafyasının siyasi haritasını hem de devletlerin birbirleriyle olan rekabet ortamını ve güvenlik algısını derinden etkilemiştir. Bu rekabetlerin temelinde ekonomik kazanç elde etme ve önemli bir güç sahibi olma arzusu yatmıştır. Bu arzular Avrupa'yı sarstığı gibi dünyanın diğer bölgelerini de derinden sarsmıştır. Tüm bu olayların gerçekleşmesinde ise askeri güç kullanımı ön planda olmuştur. Askeri alt yapısı güçlü olan devletler, genellikle zayıf devletlerin topraklarını işgal, istila ve ilhak etmişlerdir. Böyle bir durum uluslararası alanda güvensizlik ortamını oluşturmuş, tehdit algısını ön plana çıkarmış ve saldırıların yayılmasına yol açmıştır(Rude, 2015: 247-253).

Böylelikle devletler birbirlerini sahip oldukları ordularla tehdit etmiş ve çatışmışlar. Zamanla nükleer silahlar, atom bombaları ve diğer teknolojik silahların da geliştirildiği ve kullanıldığı görülmüştür. Ancak 20. yüzyılda ortaya çıkan internet ağı, güvenlik algısı, yöntemi, araçları

ve savaş taktiklerinin değişmesine yol açmıştır. Çünkü internet ağlarının gelişmesi ve giderek yaygınlık göstermesi sonucu dünya devletleri birbirlerini internet ağları üzerinden tehdit etmeye çalışmış, bölgesel hatta ulusal güvenliklerine zarar vermeye başlamışlardır. Bu durum 21. yüzyılda belirgin olarak etkisini göstermiştir. Örneğin; 2007 yılında Estonya'da yaşayan Ruslar ile Estonyalılar arasında gerginlik yaşanmıştır. Bu gerginlik sonucu Estonya'da en çok kullanılan internet siteleri çökmeye başlamıştır. Öte yandan 2008 yılında Gürcistan-Rusya Savaşı sonucu Ruslar, Gürcistan'ın dış dünya ile bağlantısını kesmek için web sitelerine saldırmıştır(Kara, 2013: 47-48). Bu olaylar, ulusal güvenliğin tehdit altına girmesine zamanla da uluslararası güvenliğin zarar görmesine sebebiyet vermiştir. Hem bilgisayarların giderek artması hem de internet ağlarının yaygınlık kazanması, beraberinde siber güvenlik algısını da ortaya çıkarmıştır(Castells, 2010: 357-361).

Siber Güvenlik ve Uluslararası Güvenlik İlişkisi

Uluslararası sistemin anarşik yapısı çerçevesinde kavramsallaştırılan devlet-merkezli ve askeri odaklı güvenlik algısı, 1990'lardan sonra yeniden ele alınmaya başlanmıştır. Birkaç yüzyıl boyunca dünya coğrafyası, sınırları çizilmiş egemen devlet anlayışı üzerine kurulan Vestfalya Anlaşmasıyla devam etmiş/etmektedir. Bu anlayışa göre her devlet, kendi sınırları içinde hem bağımsızdır hem de en yüksek otorite sahibidir. Ayrıca diğer devletlerin bağımsızlığına karşı saygılı olmayı ve hiçbir devletin iç işlerine karışmamayı da ön görmektedir. Bunun yanı sıra uluslararası alanda egemenliğin korunması ve hukuki eşitliğin sağlanması gibi temel unsurların kabul edilmesi de güvenliğin güvence altına alınmasında önemli bir karardır(Ateş, 1994: 41-45).

Fakat küreselleşme süreciyle beraber, uluslararası güvenliğin daha çok tehdit altına girdiği görülmüştür. Çünkü küreselleşme, birden çok parçaların bir araya gelerek bir bütünlük oluşturmasıdır. Başka bir ifadeyle kavram; ürünlerin, düşüncelerin/fikirlerin, kültürlerin ve dünya görüşlerinin hızlı bir şekilde birbirleriyle alış veriş yapmasıdır veya dünya coğrafyasının herhangi bir yerinde meydana gelen olaylardan haberdar olunmasıdır. Lesotho'nun herhangi bir köyünde meydana gelen bir olayın Norveç'te veya Dağıstan'dan da izlenip öğrenilmesi küreselleşmeye örnek olarak gösterilebilir(Steger, 2009: 5-9).

Böyle bir durum daha önce mümkün değilken, 20. yüzyılın ortalarından itibaren hatta Soğuk Savaş'ın bitiminden bu yana daha çok yaygınlık göstermesi, küreselleşmenin en iyi izlenimi olmuştur. Tüm bunların gerçekleşmesinde ise internet ağının 20. yüzyılın ortalarından beri

dünyada kullanılıyor olmasıdır. Çünkü internet ağı, dünya coğrafyasını çepeçevre sarmış bulunmaktadır. Bu anlamda internet, önemli bir veri olarak tüm dünya devletleri tarafından kullanılmakta ve işlenmektedir. Hatta bireysel bir ağ olarak da herkesçe kullanılmaktadır. Facebook, Instagram, Swarm, Tiwitter, E-bankacılık, E-devlet ve E-voting gibi sosyal medya hesaplarının bireysel olması, internet ağının toplumu tüm katmanlarıyla nasıl çepeçevre sardığının bir göstergesidir(Horowitz, 2004: 130-140).

Küreselleşme teriminin en önemli etkenlerinden biri, olası etkilerinin çok sayıda ve çeşitli olduğu izlenimi vermesidir. Birçok düşünürün de belirttiği gibi küreselleşme teriminin çok boyutlu olması ve çok çeşitlilik arz etmesi onu, sınırlarını çizme uğraşını bile zora sokmuştur/sokmaktadır. Bu bağlamda küreselleşme, her alanda yaygın bir kavram olmakla birlikte genellikle bir durumdan daha çok bir akımı veya zihniyeti ima eder hale gelmiştir. Bireyleri ve toplumları derinden etkileyen küreselleşmenin, devletleri de etkilediği görülmüştür. Hatta devletlerarasındaki ilişkilerin değişime uğramasına da yol açmıştır. Bu değişim Roland Robertson'a göre; Küreselleşme olgusunun çok sayıda farklılık göstermesine rağmen, küreselleşme olarak isimlendirilen şeyi anlamanın en iyi yolunun, dünyanın *birleşik* bir duruma gelmesidir fakat kesinlikle safdil işlevselci tarzda bütünleşmediği öte yandan *biçim sorunu* üzerinde yoğunlaştığıdır(Robertson, 1999: 12-16).

Robertson burada şunu ifade etmektedir: küreselleşme denilen olgu, sadece bir alan üzerinde değil birçok alanda etkisini göstermektedir. Bu etki, ekonomi, siyasi, teknoloji, askeri ve sosyokültürel olmak üzere birçok alanda görülebilmektedir. Küreselleşmenin bu kadar yaygınlık göstermesinin temelinde internet ağı yatmaktadır. Çünkü internet her alanda kullanılabilmekte ve internetle her işlem yapılabilmektedir. Hatta insan hayatının bir parçası haline geldiği de görülmektedir. İnsan yaşamını o kadar çok değiştirmiştir ki bu durum, devletlerarasındaki ilişkilere de yansımıştır. Özellikle bilgisayarların gelişip yaygınlaşmasıyla birlikte insanlar sosyal medya hesapları açmış ve bu hesaplar üzerinden dünyanın birçok yerindeki insanlarla iletişim haline geçmiştir/geçmektedir. Bu iletişim ağı, insanların farklı kültürlerle tanışmasını ve birbirlerinden etkilenmesini sağlamıştır(National Research Council, 2003: 57-62).

Nitekim sadece insanlar değil, devletlerin de birbirleriyle iletişim haline geçtiği görülmüştür. Devletlerarasındaki ilişkilerde iki durum söz konusu olmaktadır. İlki, internet üzerinden sağlanan iletişim veya ilişkilerin suiistimal edilmeye çalışılması, ikincisi de iyi niyetler

üzerinden yapılan iletişim veya ilişkiler bütünü olmasıdır. Birinci durum gerçekleştiğinde bir güvenlik sorunu ortaya çıkmaktadır. Bu güvenlik sorunu, internet üzerinden birçok teknolojik cihazları kullanılamaz hale getirebilmektedir. İnsan hayatının bir parçası olan tüm teknolojik aletler ansızın işlevsiz hale gelebilmekte ve devre dışı bırakılabilmektedir. Tüm bu gelişmeler internet aracılığıyla devletlerin teknolojik sistemlerine karşı siber saldırı yöntemiyle yapılmaktadır. Fakat bu saldırıların durdurulması veya önlenmesi siber güvenlik yöntemleriyle mümkün görülmektedir(Choucri, 2000: 241-249).

Siber güvenlik yöntemleri 21. yüzyıl dünyasında önemli bir yer kaplamıştır/kaplamaktadır. Bu nedenle çok sayıda ülke, Ulusal Siber Güvenlik Stratejileri ve Eylem Planları yapmıştır/yapmaktadır. Bu çerçevede, Ulusal Siber Güvenlik Stratejileri geliştirilmeye çalışılmıştır. Bu stratejilerin temelinde olası siber güvenlik saldırılarına ve bu saldırıların ortadan kaldırılmasına yönelik olmuştur. Uluslararası güvenliğin sağlanmasında önemli bir yeri olan siber güvenlik algısı, birçok alanda olumlu/olumsuz etkiler oluşturmaktadır. Bu etkilerden olumlu olanı, genel olarak uluslararası güvenliğin sağlanmasına yöneliktir. Başka bir ifadeyle uluslararası güvenliğe yapılan saldırıların önlenmesine/engellenmesine yönelik faaliyetlerdir. Bu faaliyetler; uluslararası politika ve stratejilerin geliştirilmesi, uluslararası işbirliği ve ticaretin sağlanması, ulusal alanda yapılan seçimlerin iç ve dış saldırılardan korunması, bilgi ve iletişim sistemlerinin muhafaza edilmesi gibi birçok alanda olumlu faaliyetlerin yapılması olarak örnek gösterilebilir(Jordan, 1999: 202-215).

21. yüzyıl, uluslararası güvenliğin tehdit edilmeye başlandığı bir yüzyıl olmuş ve olmaya devam etmektedir. 14 Aralık 2007 tarihindeki seçimler sırasında Kırgızistan Merkezi Seçim Komisyonu sistemlerine yönelik yapılan saldırılar neticesi tüm sistem birden çalışamaz hale gelmiş ve devre dışı bırakılmıştır. Aynı şekilde 2008 yılının Nisan ayında Almanya'nın gizli haber alma servisi (BND: Bundesnachrichtendienst) tarafından Der Spigel dergisinde, Afganistan Sanayi ve Ticaret Bakanlığı'nın tüm elektronik iletişimini casus yazılımlar kullanarak izlediğini haber olarak yayması ile birlikte iki ülke arasında önemli bir gerginlik yaşanmıştır. 2009 yılında meydana gelen saldırılardan biri Çin, Kuzey Kore, Amerika Birleşik Devletleri (ABD) ve Güney Kore'ye yapılmıştır. Çin ve Kuzey Kore kaynaklı saldırılar ile ABD'nin ve Güney Kore'nin çok sayıda bilgi ve iletişim teknolojilerinin kilitlenmesine ve devre dışı bırakılmasına sebebiyet verdiği görülmüştür. Bu gibi durumların yaşanması uluslararası güvenliği ciddi oranda sarsmıştır(Ünver-Canbay, 2010: 99).

Bu bağlamda uluslararası güvenliğin daha sağlam temeller üzerine inşa edilmesi gerekliliği bir kez daha ortaya çıkmıştır. Tüm bu saldırılar siber yoluyla yapılmakta olup bunun önlenmesi de siber yoluyla olmaktadır. Başka bir ifadeyle siber saldırılar, siber güvenlik yoluyla önlenmeye çalışılmaktadır. Her yüzyıl kendi içerisinde farklılık yaratır ve o zamanki koşullar içerisinde yaşanan saldırılar o zamana göre en büyüğüydü. Ancak hem internetin doğuşu hem sibernetik disiplininin ortaya çıkışı hem de bilgisayarların giderek artan bir durum alması savaş taktiğini değiştirmiştir. Bu değişim, özellikle de Soğuk Savaş'ın bitmesiyle daha net ortaya çıkmıştır. 21. yüzyıl bu anlamda önemli bir yüzyıl olmuştur/olmaktadır. Çünkü saldırıların evrim geçirmeye başladığı bu yüzyılda artık silahların, bombaların ve askeri kuvvet kullanımlarının giderek azalacağı onun yerine elektronik ortamda saldırıların yaşanmaya başlanacağı bir duruma geçiş sağlanmaktadır(Kara, 2013: 40-43).

Elektronik ortamdaki saldırılar, artık bir düğmeye basılacak kadar yakın olmuştur. Bu durum dünya insanları açısından büyük bir tehdit oluşturmakta ve uluslararası güvenlik kaygısını giderek artırmaktadır. Ancak insanların önemli bir kısmı bu saldırıların pek de farkında değildir. Somut bazı olaylar gerçekleştikçe bu saldırıların ne kadar önem taşıdığı ortaya çıkmaktadır. Örneğin; 10 Kasım 2009 tarihinde Brezilya ve Paraguay'ın ortaklaşa kullandıkları Itaipu Barajı ve Hidroelektrik Santraline yapılan saldırı bunun en somut göstergesidir(Ünver-Canbay, 2010: 99). Çünkü buralara yapılan saldırılar sonucu hem baraj çalışamaz hale gelmiş hem de yaklaşık bir gün boyunca iki ülkenin büyük bir kısmında elektrik kesintisi yaşanmıştır. Bu somut olay, insanlar tarafından endişeyle karşılanmış ve bir siber saldırıya maruz kaldıklarını anlamışlardır. 2010 yılında ortaya çıkan Stuxnet virüsü ve 2011'de İsrail'in Suriye'ye saldırması da önemli somut olaylardan bazılarıdır(Akyeşilmen, 2016: 1).

Aslında NATO Güvenlik Danışmanı Rex Hughes'in, "yakın gelecekte çıkabilecek büyük bir savaşta ilk mermi internette atılacaktır", sözü çoğu şeyi özetlemektedir(Hughes, 2009: 1-4). Tüm zararlı yazılımların, virüslerin, elektrik kesintilerinin, seçimlere müdahale edilmelerin ve daha birçok olayların altında internet ağının olduğu söylenebilir. Bu kapsamda, NATO harekâtlarından Sırbistan-Kosova örneği gösterilebilir. 1998 yılında Kosova, Sırbistan tarafından işgal edildi. Ancak Sırbistan'a yönelik ABD-NATO hava harekâtı başlamadan önce Sırbistan Hava Savunma Sistemleri kontrol altına alınmıştır. Böylelikle Savunma Sistemleri, kilitlenmiş ve hiçbir işlem yapılamaz hale getirilmiştir. Bu durum, artık güvenliğin

zedelenmesinin sadece bir düğmeye basmakla olabileceği anlayışını güçlendirmiştir. Öte yandan NATO Güvenlik Danışmanı Hughes'in ifade ettiği mermi, etkisini göstermeye başlamıştır(Hughes, 2009: 3-7).

21. yüzyılın mermisi, her ne kadar internetten atılmaya başlansa da söz konusu güvenlik olduktan sonra birey, toplum ve devlet, güvenliği sağlamak için her türlü çabayı göstermek zorundadır. Çünkü güvenlik sadece devletleri ilgilendiren bir durum değildir. Bireyin veya toplumun güvenliği tehdit altında olursa devletin güvenliği de tehdit altında olur/olacaktır. Fakat güvenlik meselesi, gerekçe gösterilerek insan hakları çiğnenmemeli veya kısıtlanmamalıdır. Bu bağlamda demokratik haklar başta olmak üzere özgürlük, temel hak ve hürriyetler, ifade özgürlüğü, barışçıl ortam kısacası insan haklarına zarar verilecek hiçbir tutum ve faaliyetlerde bulunulmaması gerekmektedir. Tüm bu zararlı faaliyetlere karşı sıkı bir önlem alınmalı ve denetlenmelidir. Önlem ve denetlenmelerin yapılabilmesi için siber güvenlik çalışmalarının belirli ilkeler doğrultusunda yürütülmesi en iyi seçeneklerden biri olarak görülecektir. Bu ilkelerin başında insan haklarının korunması gelmektedir. Zira insan haklarının korunması bireysel ve toplumsal güvenliğin sağlanmasında anahtar bir kavramdır. Siber güvenlik birey güvenliği, ulusal güvenlik ve uluslararası güvenliği kapsayan ve birbirine bağlayan geniş bir kavramdır. Başka bir ifadeyle, demokratik toplum yapısının kurallarına uyulması, toplumda barışı sağlayıcı ilkelerin oluşması, güvenlik algısının suiistimal edilmemesi, uluslararası işbirliği ortamının sağlanması, öte yandan ifade özgürlüğü başta olmak üzere, temel hak ve hürriyetlerinin güvence altına alınması ve hukuki işlemlerin çiğnenmemesi gerekmektedir. Tüm bunlar siber güvenlik çalışmalarının işlevselliği açısından önem taşımaktadır. Çünkü siber güvenlik, toplumsal ve uluslararası güvenliğin sağlanmasında en önemli yapı taşlarından biridir(Bıçakçı, 2012: 205-226).

Sonuç

Güvenlik kavramı, bireyler başta olmak üzere toplum, kurum ve devletleri yakından ilgilendirmektedir. Bireyler için mutlak biçimde güvenli bir yaşam alanı vazgeçilmez görülmektedir. Bireylerin güvenliğine yapılan saldırılar ve tehditler sadece birey yaşamını değil, tüm toplumları daha da ötesi tüm devletleri ilgilendirmektedir. Bu saldırılar bazen savaş yöntemiyle yapılmakta bazen de diplomatik temaslarla gerçekleştirilmektedir. Fakat son yıllarda başka saldırı türlerinin de ortaya çıktığı görülmüştür. Buna siber saldırılar örnek gösterilebilir.

Siber saldırılar, her zaman internet ortamında gerçekleşmektedir. Özellikle elektronik işlemlerin yapılmasında etkisini göstermektedir. Ancak bazı insanlar bunun farkında olmayabilir. Örneğin; internette gezinirken bilgisayarın kenarlarında göze çarpan "100 TL hediye çeki kazandınız" veya "bugün en şanslı gününüz ve bizden tatil yeri kazandınız hemen tıklayın", gibi görüntüler çoğunluklu olarak virüstür ve bilgisayarları bir kuşatma altında tutmaktadır. Bu tür programlar tıklandığı andan itibaren bilgisayar büyük bir virüs tehdidi altına girer ve neredeyse kişiye ait tüm bilgiler üzerinde istenilen işlemler yapılabilir. Böyle bir durumda tıklanmaması ve bu tür programların kapatılması önerilmektedir.

Burada bireye, topluma, kurum ve kuruluşlara yönelik bir saldırı söz konusu olmuştur. Öte yandan devletleri ilgilendiren saldırı yöntemleri de mevcuttur. Devletlerin güvenliğine yapılan saldırılar genel olarak gizli belgelere ulaşmak, kritik altyapılara saldırılar veya seçimlerin gidişatını değiştirmek amacıyla yapılmaktadır. Tüm bu gelişmeler doğrultusunda ister birey ister uluslararası alandaki tüm aktörler olsun, varlıklarını koruma, sürdürme ve geliştirme bağlamında hepsinin güvenliklerini sağlamada öncelikli olarak davrandıkları bir gerçektir. Bu anlamda siber saldırıların önlenmesinde veya tamamen ortadan kaldırılmasında siber güvenlik çalışmaları ortaya çıkmıştır. Siber güvenliğin sağlanması her aktör için önemli bir unsurdur. Siber güvensizlik büyük bir sorun olsa da, sorunun çözülmesinde kullanıcılar gizliliği, erişilebilirliği, özgürlüğü veya teknoloji gelişiminde gerekli olan yeniliği tehdit etmemelidir.

Çünkü tehditler, ulusal ve uluslararası güvenliği sarsmakta ve önemli sorunlara yol açmaktadır. Böyle bir durum karşısında sadece ulusal değil, uluslararası alanda tüm devletlerin ortak bir politika oluşturmaları gerekmektedir. Ortak bir politika üretilmediği sürece, uluslararası güvenliğin her zaman tehdit altında kalacağı bir ortam varlığını sürdürür. Bundan hareketle uluslararası güvenliğin birey ve toplumsal güvenlikten bağımsız düşünülemeyeceği söylenebilir. Bu güvenliğin sağlanmasında ise, en önemli temel yapı taşlarından birisi de siber güvenliktir. Çünkü siber güvenlikte erişim, gizlilik ve bütünlük esastır. Sanal âlemden gelecek her türlü zararlı yazılımların ve virüslerin engellenmesi ya da tamamen yok edilmesi de siber güvenlik tarafından gerçekleşebilmektedir. Bu nedenle bireylerin, toplumların, kurum ve kuruluşların güvenli bir ortama kavuşabilmesi için öncelikli olarak uluslararası güvenliğin, siber güvenlik politikalar bağlamında hayata geçirilmesi gerekmektedir. Bu politikalar ise, dünya devletleri tarafından oluşturulacak ortak bir stratejik plana, anlaşmaya ve kurumsallaştırmaya bağlıdır.

Kaynakça

Akyeşilmen Nezir. (2016). "Siber Güvenlik ve Özgürlük", *İlkses Gazetesi*.

Ateş Toktamış. (1994). *Siyasal Tarih*, 3. Baskı, İstanbul: Der Yayınları.

Baylıs John. (2008). "Uluslararası İlişkilerde Güvenlik Kavramı", *Uluslararası İlişkiler Dergisi*, Cilt 5, Sayı 18.

Bıçakçı Salih. (2012). "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", *Uluslararası İlişkiler*, Cilt 9, Sayı 34.

Bıçakçı Salih. (2013). "21. Yüzyılda Siber Güvenlik", Mustafa Aydın (ed.), İstanbul: Bilgi Üniversitesi Yayınları.

Bilgiç Ali. (2011). "Güvenlik İkilemini Yeniden Düşünmek Güvenlik Çalışmalarında Yeni Bir Perspektif", *Uluslararası İlişkiler Dergisi*, Cilt 8, Sayı 29.

Brauch Hans Günter. (2008). "Güvenliğin Yeniden Kavramsallaştırılması: Barış, Güvenlik, Kalkınma ve Çevre Kavramsal Dörtlüsü", *Uluslararası İlişkiler Dergisi*, Cilt 5, Sayı 18.

Buzan Barry. (1983). *People, States and Fear: The National Security Problem in International Relations*, Brighton: University of North Carolina Press.

Castells Manuel. (2010). *The Rise of the Network Society*, West Sussex: Wiley-Blackwell Press.

Choucri Nazlı. (2000). "Introduction: Cyber Politics in International Relations", *International Political Science Review*, Cilt 21, Sayı 3.

Dedeoğlu Beril.(2003). *Uluslararası Güvenlik ve Strateji*, İstanbul: Derin Yayınları.

Grotius Hugo. (2011). *Savaş ve Barış Hukuku*, (çev.) Seha L. Meray, İstanbul: Say Yayınları.

Güntay Vahit. (2015). "Uluslararası İlişkiler Bağlamında Güvenlik Algısı ve Siber Güvenlik; Akdeniz, Karadeniz ve Avrupa Bölgeleri Üzerine Bir Değerlendirme", *The Journal of Academic Social Science Studies*, No 37, Autumn I.

Han Ahmet Kasım ve Çelikpala Mitat. (2016). "Uluslararası Çerçevede Siber Güvenlik ve Nükleer Enerji", Sinan Ülgen (ed.), *Türkiye'de Siber Güvenlik ve Nükleer* Enerji, İstanbul: Ekonomi ve Dış Politika Araştırmalar Merkezi Yayınları.

Hill Kevin A. and Hughes John E. (1998). *Cyberpolitics: Citizen Activizm in the Age of the Internet*, Lanham & Maryland: Rowman & Littlefield Press.

Hobbes Thomas. (2005). *Leviathan*, (6. Baskı), (çev.) Semih Lim, İstanbul: Yapı Kredi Yapıtları.

Hoffman Adam and Schweıtzer Yoram. (2015). "Cyber Jihad in the Service of the Islamic State (ISIS)", *Strategic Assessment*, Cilt 18, No 1.

Horowıtz Shale. (2004). "Restarting Globalization after World War II; Structure, Coalitions, and the Cold War", *Comparative Political Studies*, Vol 37, No 2.

Hughes Rex B. (2009). "NATO and Cyber Defence: Mission Accomplished?", *Atlantisch Perspectief*, Cilt 1, No 4.

Jordan Tim. (1999). *Cyber Power: An Introduction to the Politics of Cyberspace*, London: Routledge.

Kara Mahruze. (2013). *Siber Saldırılar-Siber Savaşlar ve Etkileri*, Yayınlanmamış Yüksek Lisans Tezi, İstanbul: Bilgi Üniversitesi.

Machiavelli Niccolo. (2001). *Prens*, (3. Baskı) çev. Semra Kunt, İstanbul: Alkım Yayınları.

National Research Council. (2003). *Innovation in Information Technology*, Washington D.C.: The National Academies Press.

Nojeim Gregory T. (2010). "Cybersecurity and Freedom on the Internet", *Journal of National Security Law & Poiıcy*, Vol 4, No 119.

Özcan Arif Behiç. (2011). " Uluslararası Güvenlik Sorunları ve ABD'nin Güvenlik Stratejileri", *Selçuk Üniversitesi İİBF Sosyal ve Ekonomik Araştırmalar Dergisi*.

Özlük Erdem. (2014). *Uluslararası İlişkilerde Devlet: Tanım, Teori ve Devlet İstisnacılığı*, 2. Baskı, Konya: Çizgi Kitabevi.

Robertson Roland. (1999). *Küreselleşme: Toplum Kuramı ve Küresel Kültür*, (çev.) Ümit Hüsrev Yolsal, Ankara: Bilim ve Sanat Yayınları.

Rude George. (2015). *Fransız Devrimi*, (çev.) Ali İhsan Dalgıç, İstanbul: İletişim Yayınları.

Sandıklı Atilla ve Emeklier Bilgehan, (2012). "Güvenlik Yaklaşımlarında Değişim ve Dönüşüm", (ed.) Atilla Sandıklı, *Teoriler Işığında Güvenlik, Savaş, Barış ve Çatışma Çözümleri*, İstanbul: BİLGESAM Yayınları.

Steger Manfred B. (2009). *Globalization: A Very Short Introduction*, Hampshire: Oxford Univeristy Press.

Ünver Mustafa ve Canbay Cafer. (2010). "Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik", *Elektrik Mühendisliği Dergisi*, Sayı 438.

Yılmaz Sait. (2007). "Güçsüz Güç", *Güvenlik Stratejileri Dergisi*, Cilt 3, Sayı 5.

ISSN: 2587-1218

ULUSAL GÜVENLİK ÇERÇEVESİNDE SİBER GÜVENLİK YAKLAŞIMI OLUŞTURMA SORUNU

Vahit GÜNTAY*

Özet

Siber tehdit uluslararası sistem açısından, bilgi teknolojilerinin farklılaşması ile birlikte siber uzay ortamında farklı bir çatışma konsepti olarak karşımıza çıkmaktadır. Bunun yanında konvansiyonel anlamdaki savaşlardan ve hatta nükleer caydırıcılıktan daha önemli bir basamağı oluşturma yolunda hızla yol almaktadır. Soğuk Savaş ve sonrasında güvenlik algılamalarındaki farklılık, tehdit parametrelerinin değişimiyle bu konunun gelişimini hızlandırmıştır. Devletlerin siber uzayda bir aktör haline gelmesi, farklı aktörlerle ilişkilendirildiğinde günümüz gelişmeleri açısından artık bir gerçekliktir ve uluslararası ilişkiler temelinde daha çok gündemde olmaktadır. Bu boyutlarda ele alındığında, siber çatışmaların günümüzde çağdaş devletler açısından bir tehdit oluşturduğu, ciddi bir problem sahası ve tartışma merkezi haline geldiği bir gerçektir. Eksik olan ise, uluslararası ilişkilere ilgi duyanlar açısından konunun hangi teorik yaklaşımlarla ele alınacağıdır. "Uluslararası güvenlik temelinde siber güvenliğin özüne ilişkin bir yaklaşım sergilemek mümkün müdür?" ya da "Bu konuda nasıl bir yol izlenebilir?" gibi sorular bu çalışmanın cevabını aramaya çalıştığı yol haritası olmuştur.

Anahtar Kelimeler: Siber Güvenlik, Uluslararası İlişkiler, Ulusal Güvenlik

THE QUESTION OF FORMING CYBERSECURITY APPROACH IN THE CONTEXT OF NATIONAL SECURITY

Abstract

Cyber threat is a unique conflict concept at cyberspace with differentiating information technologies in the context of international system. Besides, cyber threat proceeds rapidly in generating more important step than conventional based wars even nuclear deterrence. The difference in security perceptions of Cold War and Post Cold War Era has accelerated the development of this subject with changing threat parameters. States have become actors in cyberspace and that fact is a reality when correlated with other stake-holders in the cyberspace. This reality also remains to be a prominent agenda issue of international relations. When it is evaluated with these dimensions, it is a fact that cyber conflicts are real threats for modern states nowadays and serious problem area that generates disputes at the international arena. The missing subject for international relations researchers, is which theoretical approach going to be applied. The questions such as "Is it possible to apply an approach for

* Dr., Karadeniz Teknik Üniversitesi, İİBF, Uluslararası İlişkiler Bölümü. E-posta: vahitguntay@gmail.com

cyber security in the context of international security?" or "What way needs to be followed?" are road maps of this study.

Keywords: Cyber Security, International Relations, National Security

Giriş

Teknolojik olarak ve yapısal anlamda toplumsal hareketlenmeler, çoğu zaman askeri teknolojilerin tür ve seviyesine göre farklılık göstermektedir. Teknolojik olarak bu düzeyi sadece askeri sistem veya düzlem temelinde düşünmemek gerekir. Bu düzlemin tartışıldığı boyut güvenlik anlamında farklılaşmayı ve tartışma alanını daha da ciddi bir kapsama oturtmuştur.

Siber alan ve uluslararası ilişkiler boyutunda *"siber politikalar"* adı altında çalışma aritmetiği bulan siber güvenlik, devletlerin kendilerini korumak için ve siber saldırılar ile birlikte yeni bir çalışma alanını karşımıza çıkarmıştır. Ulus devletlerin veya bu düzeyde tartışma niteliği gösteren güncel çalışmalar da siber güvenlik konseptine ve özüne atıflarda bulunmaktadır. *Askeri işlerde ve gelişmelerde devrim* olarak adlandırılan bu durum elektronik, ileri teknolojik çatışma unsurlarının ortaya çıkmasıyla çok boyutlu bir paradoks haline dönüşmüştür.

Siber çatışma ve savaş gibi bir olgunun askeri teknolojiler açısından önemli olduğu, konvansiyonel ve nükleer silahlar ile bunların caydırıcılığı gibi unsurlar bakımından artık ortak bir hiyerarşide yer alması ayrı bir başlığı oluşturmaktadır. Bu başlığın şekillenmesinde uluslararası ilişkiler temeli açısından kritik altyapıların, iletişim sistemlerinin ya da özelde hava savunma sistemleri gibi birçok unsurun tehlikede olması ve caydırıcı bir özellik kazanması siber güvenliği önemli bir analiz düzeyine taşımaktadır.

Siber savaş belli yönleri itibariyle asimetrik çatışmalara benzetilmektedir ve bunu güçlendiren en önemli gösterge, zayıf durumda olanın da kimi manevralarla güçlü veya baskın olanı alt edebileceği ile ilgilidir. Uluslararası ilişkiler boyutundaki tartışma alanı ve konunun ele alındığı boyut bu yönde yoğunlaşmaktadır. Uluslararası aktörler adına makro savaş teorileri açısından kimi zaman tarafların ihtiyacı olan basit bir bilgisayar ve yazılım olabilmektedir. Bu derece basite indirgenen bir durumla ilgili de doğal olarak ilk eleştiri siber çatışmalarda kullanılan silahların, iyi birer silah olmadığı ile ilgili durumdur ve düşmana ciddi, yıkıcı zararlar vermediği için kışkırtma açısından bir riski içinde barındırabileceğidir. Bu nedenle

teknik kapasite açısından, özellikle siber alanda gelişme arzusu içinde olan devletler temelinde bir yaklaşım denemesi tartışma aritmetiği bulmaktadır.

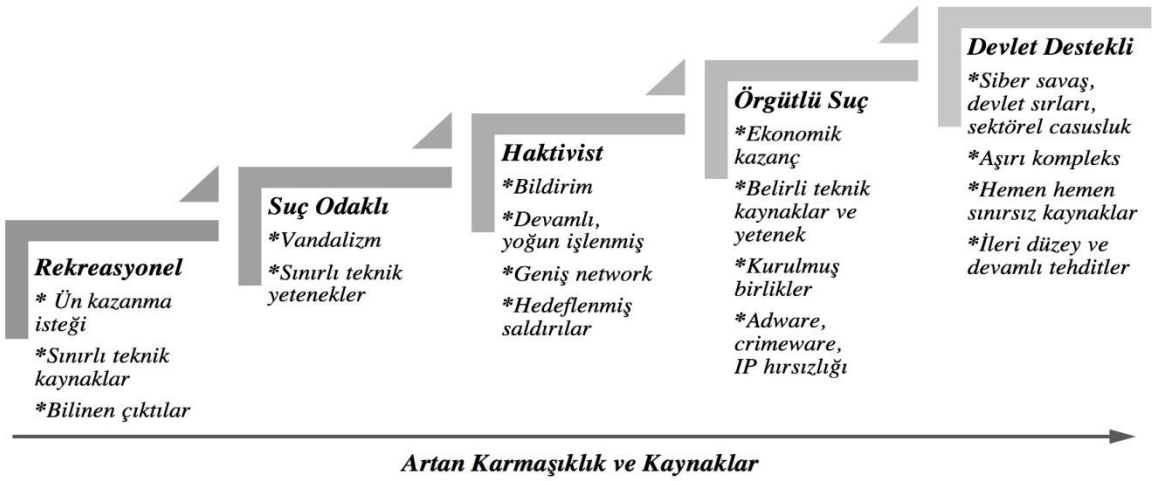
Değişen Uluslararası Sistemde Siber Güvenlik Yaklaşımı Oluşturma

Güvenlik çalışmalarının tarihi, sosyal bilimlerin ilerlediği mekanizmaları uluslararası güvenlik temelinde ortaya koymaktadır. Uluslararası ilişkilerin diğer alanları gibi güvenlik çalışmaları da bilginin diğer dallarından faydalanmıştır. İlerlemenin diğer kaynağı rakip teoriler arasındaki mücadeledir. Rekabet, mücadele eden yaklaşımların argümanlarını incelemeye ve daha iyi ampirik destek aramaya teşvik etmektedir (Walt, 2003:101).

Siber güvenlik yaklaşımı oluşturma farklı yaklaşımlar arasında kimi zaman komplo teorileri, kimi zaman gelecek beklentileri arasında zorlaşmaktadır. Özellikle sosyal bilimler içerisinde uluslararası ilişkilere dair konuların eklektik düzlemde ele alınması ve tartışılması, siber güvenlik gibi konularda bölgeler arası ayrım yapmada ve strateji geliştirmede bazı zorluklar içermektedir.

Siber güvenlik içerisinde zaman ve mekan algısının klasik çatışmalara göre farklı şekillerde ortaya çıkışı, saldırgan profillerinin farklı düzeylerde ve amaçlarda faaliyetlerini sürdürüşü güvenlik yaklaşımı oluşturmada zorlaştırıcı unsurlardır. Şekil 1'de görüleceği üzere, saldırı ve savunma perspektifinde siber güvenlik bireylerin sınırlı teknik kaynaklarıyla oluşturdukları saldırılardan, devlet destekli siber orduların saldırı ve savunma kapasiteleriyle çok daha geniş bir alana yayılmıştır. Her düzeyde farklı kaynaklara ihtiyaç duyan bu alan daha ileri altyapılara ihtiyaç duymaktadır. Artan kaynaklar ve kapasitesi genişleyen aktörlerle birlikte karmaşıklık daha da fazlalaşmaktadır. Farklı düzeylerdeki aktörlerin, çatışma kültürü içinde siber güvenlik alanındaki çıkar mücadeleleri profillerin daha da çeşitleneceği imajını ortaya koymaktadır. Uluslararası ilişkilerdeki boyutu da bu yaklaşımla birlikte genişleyecektir.

Şekil 1. Değişen Saldırgan Profilleri



Kaynak: McAfee Labs Threat Report, 2015:9

Uluslararası sistem kendi içinde değişimini kendine has özellikler ile sağlarken, stratejik bir değişim algısı oluştuğu yadsınamaz bir gerçekliktir. Stratejik sorunlar ve siber güvenlik temelinde geleneksel tehditlerle birlikte, siber tehditlerin de dönüşümü bu temeli farklılaştırmaktadır. Güvenlik stratejilerini siber uzayda uygulayabilme ve ittifak oluşturabilme mantığı gibi yaklaşımlar, siber güvenlik içinde tartışılabilen yeni kavramsal özellikleri oluşturmaktadır. Bu özelliklerin geliştirilmesi ve ele alınış biçimi devletlerin konuya olan ilgisiyle daha da belirginlik kazanmaktadır. Uluslararası ilişkilerin ana aktörlerinden olan devletler belirleyici unsur haline gelmiştir.

Stratejik Değişim Algısı ve Siber Uzay

Genel olarak aktörler güvenlikleri adına öncelikle barışçıl stratejiler denemektedirler. Bunlardan amaçları doğrultusunda sonuç alamadıklarında ya da alamayacakları algısı oluştuğunda çatışma stratejisine yönelmektedirler. Hangi türü seçilirse seçilsin, güvenlik stratejilerinin tümü belirli yöntemler ve operasyonlar içermektedir. Bu yöntemlerin yine neredeyse tümü, şiddet ya da şiddet kullanma tehdidi içermektedir (Dedeoğlu, 2003:108).

Şiddet ve şiddet kullanma tehdidi ile birlikte, küreselleşme sürecinin güvenlik alanına etkisi genellikle yeni tehditler üzerine odaklanılarak ele alınmıştır. Bu yaklaşım doğru olmakla birlikte eksik kalmaktadır. Küreselleşmenin ortaya çıkardığı tehditler konunun yalnızca bir yönünü temsil etmektedir (Karabulut, 2015:190). İnşacı perspektifin değişen tehditlere ilişkin

analiz düzeyi de bu yöndedir. Devletlerin küresel aktör olarak uluslararası örgütlenmelerin de merkezinde yer aldığı uluslararası sistem birçok farklı unsurdan etkilenebilmektedir.

Stratejik olarak değişimden anlaşılması gereken tercihlerin farklılaşması ve bu alanda uzmanlaşılmasına yönelik adımlar atılmasıdır. Sadece teorik bir zeminin ortaya çıkması yetmemektedir. Stratejik olarak atılacak adımın bir sonucunun oluşması, özellikle değişim algısının doğru yönlendirilmesi açısından bir zorunluluktur.

Siber saldırılar içindeki teorik yaklaşım, pratikteki boyutuyla stratejik anlamda kendi içerisinde zorlaşmaktadır. Siber alanda stratejik değişim algısına yönelik olarak ülkelerin siber savaş stratejilerinin etkileyeceği hususlar Çifçi'ye (2012:66) göre şu şekildedir:

- *Siber alana doğrudan veya dolaylı olarak uygulanabilecek olan ulusal, uluslararası yasal düzenlemeler ve ülkeler arası sözleşmeler,*
- *Ülkenin rejimi, insan hakları ve demokrasiye olan yaklaşımı,*
- *Ülkenin uluslararası camiada kendini konumlandırmak istediği yer ve bu kapsamda mücadelesini hangi alanlara taşıyacağı,*
- *Ülkenin siber alanı kullanma yaygınlığı ve siber alana olan bağımlılığı,*
- *Ülkenin siber savunma ve saldırı kabiliyetleri.*

Siber alana ilişkin değişimde güvenlik stratejilerinin küreselleşmesi ile ters orantılı olarak çatışma stratejileri de şekillenmiştir. Tehdit olarak algılanan olgu ve aktörlerin artışı, güvenlik halkaları arasındaki ayrımın giderek azalması, diğer bir ifadeyle uluslararası çevrede tehdit olan her unsurun doğrudan bireyi etkiler hale gelmesi, güvenlik stratejilerinin içten çok dışa göre düzenlenmesine yol açmaktadır (Dedeoğlu, 2003:111).

Şekil 2. Ulusal Güvenlik Problematiğinin Bileşenleri

Kaynak: Dreyfus, 2002

Siber güvenlikle ilgili dışa göre düzenlenecek stratejik değişim döngüsünde rakibin yok edilmesi gibi bir husus söz konusu olmadığı için tercih edilecek unsur olarak saldırının dönüştürülmesi ya da düşmanın durdurulması amaçlanmaktadır. Bu durum uzun vadede çatışmaların boyutunu siber alanda güçlendirecek ve genişletecektir. Stratejideki değişim algısındaki bu süreç özellikle ulusal güvenlik açısından ciddi bir tehdit oluşturmaktadır. Ulusal güvenlik açısından önemli bileşenler haline gelen güvenlik çevresi siber saldırılar ile ciddi bir travmayı yaşarken, siber tehditler bu alanda değişimle birlikte daha çok çeşitlenecektir.

Güçlenen ve genişleyen siber alandaki tehditlere karşın stratejilerin *"ulusal"* olması devletlerin elini güçlendirecektir. Ulusal stratejiler, stratejik değişim algısıyla siber şoklara karşı direnç de gösterebilmektedir. Çok yönlü ve çok üyeli uluslararası yapılanmalar ve örgütlenmeler siber güvenlik anlayışında ulusal stratejilerin gelişimini zorlaştırmaktadır (Bejtlich, 2015:164). Özellikle siber stratejinin devletleri ilgilendiren uluslararası yönünde devletlerin sahip olduğu güç, benzer kapasiteli güçlerle kıyaslanabilir. Stratejik değişim algısıyla birlikte *"ulusal siber stratejiler"* geliştirilirken izlenecek yolu Ian Wallace[19] (2014) şu şekilde tarif etmektedir:

> ➢ *"Strateji yalnızca nasıl davranılması gerektiğini değil, aynı zamanda nasıl bir politika izleneceğini de ortaya koymalıdır.*
> ➢ *Değişimin yanında devamlılığa da odaklanılmalıdır. Yeni ulusal koordinasyon yapılanmaları siber zorluklara cevap verebilecek nitelikte olmalıdır.*
> ➢ *Stratejiler özü itibariyle "ulusal" olmalıdır. Ulusal stratejiler genel olarak, hükümetlerin siber güvenlikteki rolüne işaret etmektedir.*
> ➢ *Stratejilerin güvenilir olması sağlanmalıdır. Strateji oluştururken kullanılan kaynakların belirtilmemesi hatasına düşülmemelidir.*
> ➢ *Siber güvenlik gerçeğiyle birlikte planlar yapılmalı ve sürdürülebilir amaçlar gözetilmelidir. Siber stratejiler, gelecekte yaşanması kaçınılmaz saldırılara ve bu saldırılardan doğabilecek olası sonuçlara göre tasarlanmalıdır."*

Geleneksel Tehditlerin Dönüşümü

Uluslararası sistemin anarşik yapısı çerçevesinde kavramsallaştırılan devlet merkezli ve askeri odaklı güvenlik anlayışı, Soğuk Savaş'ın sona ermesi ve küreselleşme sürecinin etkisiyle birlikte yeniden ele alınmaya başlamıştır. Bu çerçevede, yeni/eleştirel güvenlik yaklaşımları,

[19] *Ian Wallace*, Brookings Institute'de, 21. Yüzyıl Güvenlik ve İstihbarat Merkezi uzmanıdır. İngiltere Savunma Bakanlığı'nda ulusal siber stratejilerinin geliştirilmesinde görev almıştır.

güvenliğin nesnesi olarak devletin yanına ya toplumsal grupları ve bireyi alarak güvenliği daha geniş sosyal, ekonomik, çevresel ve politik amaçlarla birleştirmektedir (Ağır, 2011:99). Daha geniş amaçlarla birleşen güvenlik konuları özellikle küreselleşme ile birlikte hiçbir dönemde olmadığı kadar çeşitlenmiş ve yoğunlaşmıştır. Geleneksel tehditler açısından başta terörizm olmak üzere birçok farklı başlık kendi içerisinde dönüşmeye başlamıştır. Özellikle *terörizm, yoksulluk, çevre kirliliği, etnik sorunlar, nükleer, kimyasal* ve *biyolojik silahların varlığı* ve de *siber terörizmin* şekil değiştirmesi 21. yüzyılda uluslararası güvenlik açısından tehdit boyutunu farklılaştırmıştır.[20]

Savaş teknolojilerinde meydana gelen gelişmeler, bu teknolojilerin insan kayıplarını artıracak kapasiteye erişmesi ve yıkıcı etkiler, devletlerin doğrudan doğruya savaşa girmelerinin risklerini daha da fazlalaştırmıştır. Savaş teknolojilerindeki gelişmeler her iki dünya savaşından beri bu yönde bir endişeye neden olmuştur, ancak özellikle kimyasal silahların yaygınlaşması ve nükleer silahlara sahip olan ülkelerin sayılarının artmasıyla savaşın yol açabileceği tehlikeler farklı boyutlara taşınmıştır (Karabulut, 2015:193). Silah ve teknolojinin birbiri ile ilişkili olduğu düzlem artınca terörist grupların hem konvansiyonel silahlara ulaşmadaki teknoloji kabiliyetleri hem de siber alandaki faaliyetleri etkinlik kazanmıştır (Lutz ve Lutz, 2008:28).

Geleneksel tehditler arasından günümüze boyut değiştirerek gelen askeri tehditler yanında ekonomik, çevresel, toplumsal konuların da güvenlik alanı içine dahil edilmesi süreci başlamıştır. Özellikle geleneksel olarak tehdit algısının yoğunlaştığı birey kavramı daha makro bir hal alarak büyümüş ve tehdit boyutunda daha karmaşıklaşarak siber uzaya yayılmıştır. Küreselleşme sürecinde yaşanan tehdit çeşitlenmesi geleneksel tehditleri daha karmaşık hale getirmiştir.

Güvenlik algılamalarında özellikle geleneksel tehditlerin dönüşümündeki en önemli sebeplerden birisi tehdidin tek boyutlu, devletten devlete olma boyutundaki klasik halinden çıkarak, asimetrik ve çok boyutlu bir konuma ulaşmasıdır. Bu durum, günümüz tehditleri ile mücadelede klasik yapılanma ve anlayışların geçerliliğini tamamen yitirdiğini göstermektedir.

[20] *Küreselleşme,* Soğuk Savaş dönemi sonrasında oldukça tartışılan kavramlardan birisidir. Akademik anlamda kavramı ilk kullanan Thedore Levit'tir. Bu bağlamda küreselleşmenin ilk halkasının coğrafi keşiflerle, ikinci halkasının 1870-1914 yılları arasında, son halkasının ise iki kutuplu düzenin yıkılmasıyla oluştuğu kabul edilmektedir.

Küreselleşme ile ortaya çıkan asimetrik tehdit ile birlikte saldırganın muhatabından göreceli olarak daha zayıf olmasına karşın, değişen tehdit unsurlarıyla birlikte, ani ve hazırlıksız saldırılarla dengeleri değiştirebildiği gözlenmiştir. Bu sebepten dolayı birçok uzman, devletlerden öte sivillere yönelik olan ve askeri olmayan güvenlik anlayışı içinde mücadele edilmesi gereken hususları ön plana çıkarmaya başlamıştır. Küreselleşme süreci ve etkileriyle beraber geleneksel tehdit algısındaki değişimin etkilendiği durumları Önen (2015) şu şekilde gruplandırmıştır:

- *Güvenlik alanında yeni tehditlerin ortaya çıkmasının yanında siber terör, bilimsel çalışmaların siber uzaydaki saldırganlığı ve uyumu da bozacak şekilde hızla ilerlemesi, ekolojik dengeyi genetik bilimiyle bozma girişimleri ve yeni tür hastalıklar.*
- *Geçmişte var olan fakat güvenlik alanı içinde düşünülmeyen konuların güvenlik alanına eklemlenmesi; birey güvenliği ve çevre güvenliği gibi.*
- *Geleneksel güvenlik tehditlerinde terör, savaş, organize suçlar gibi hususların kabuk değiştirmesi.*

11 Eylül 2001 terör olayları güvenlik kavramının kapsamının küresel terör, örgütlü suç şebekeleri, uyuşturucu, silah ve insan ticareti, yasadışı göç, etnik ve dinsel nitelikli çatışmalar ve kitle imha silahlarındaki artış gibi tehditlerle daha da genişlediğini göstermiştir. Geleneksel tehdidin dönüşümünde Soğuk Savaş dönemi sonrasında ABD'nin hegemon güç olması uluslararası ortamı yumuşatmamış; küreselleşmenin ekonomik ve sosyal bakımdan getirmiş olduğu olumsuz sonuçlar, ABD ve Batı karşıtı terörü körükleyen farklı etkenler olmuştur. Devletler ve bireyler adına tehdidin her an ve her yerde faaliyette olabileceği düşüncesi korkutucu boyutlarla dönüşüme uğramıştır (Yorulmaz, 2014:121).

Siber Tehdidin Dönüşümü

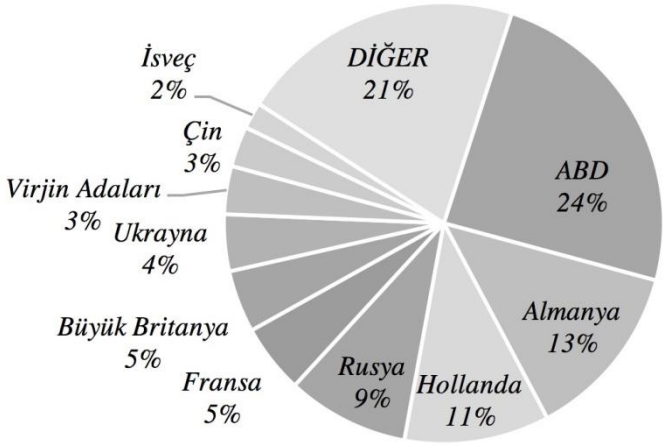
Siber alanda gerçekleştirilen saldırıların geleneksel saldırılardan önemli farklılıkları bulunmaktadır. Her şeyden önce siber saldırılar ışık hızında gerçekleştirilebilme olanağına sahiptir. Bununla birlikte modern toplumlardaki altyapının yüksek teknolojiye ihtiyaç duyması nedeniyle, sanal dünya üzerinden gerçekleştirilen saldırıların etkileri konvansiyonel silahlar kadar büyük olabilmektedir. Ayrıca siber saldırıların maliyeti geleneksel saldırılarla mukayese edilemeyecek kadar düşüktür ve siber saldırının hedefinde yer alan objenin kasten mi yoksa kazayla mı saldırıya maruz kaldığının anlaşılması kolay değildir (Gürkaynak ve İren, 2011:265). Siber tehdidin fiziksel etkisinin olması cazip olan farklı bir yönü ortaya çıkararak küresel bir değişim algısını da bizlere sunmaktadır. Bilginin küresel düzeyde

birbirine bağlı olduğu teknolojik alt yapı kendi içerisinde ayrı bir karmaşıklığı meydana getirmektedir (Eriksson ve Giacomello, 2007:174).

Siber saldırıların hedeflerindeki anlaşılması zor olan durum özellikle, birçok olayın miladı olan 11 Eylül 2001 sonrasında ivme kazanarak daha da farklı bir hal almıştır. Bunun en önemli sebebi İkiz Kuleler ile birlikte tehdit konusundaki geleneksel anlayışın da değişmesidir. Devletlerin toprak sınırlarının yanı sıra askeri mekan ve zaman kurallarının da anlamsız hale gelmesi siber uzaydaki faaliyetlerin yönünü değiştirmiştir.

Siber tehditlerin dönüşümü farklı verilerle de tartışılmaktadır. Özellikle zararlı yazılımların, faaliyet alanlarının bağımlı olunan siber ortamda evrim geçirmesi son yıllarda dikkat çekici bir durumdur ve devletlerin tehdit algısında da hissedilmiştir. Grafik 1'de görüldüğü üzere çevrimiçi kaynakların zararlı yazılımlar üzerinden dağılımı, ülkelerin siber ortamda faaliyetlerinin artışıyla doğru orantılıdır. Başta ABD olmak üzere Almanya, Hollanda, Fransa, İngiltere gibi ülkeler bu konuda en çok etkilenen ülkelerin başında gelmektedir. Siber alana artan bağımlılık bu noktada riski daha da artırmaktadır. Siber alanda gelişmekte olan ülkelerin, bu alanda gelişmiş ülkeleri takibi ve siber saldırılarda savunmaya ilişkin kapasitelerini artırmaya çalışması kısmi olarak avantaj sağlayabilecektir. Önemli olan husus kısa ve uzun vadeli politikaların belirlenmesidir.

Grafik 1. Çevrimiçi Kaynakların Zararlı Yazılımlar Üzerinden Dağılımı



Kaynak: Kaspersky Security Bulletin, 2015:62

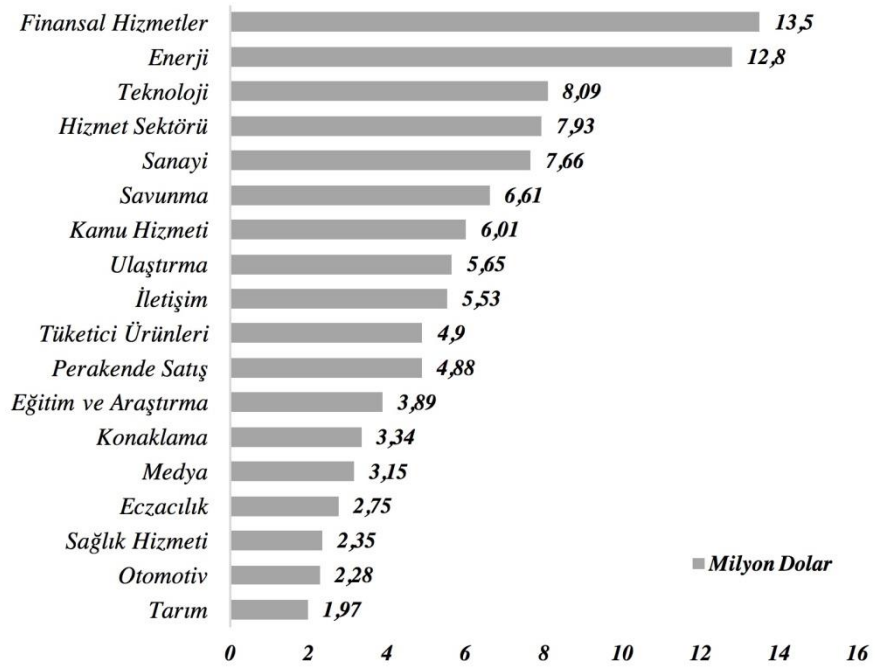
Siber saldırıların uzunca bir süre risk olduğu farkında olunan bir hususta, fakat zarar kapsamı önemsenmemiş ve sınırlı olduğu düşünülmüştür. Bu algı 11 Eylül ile birlikte hem siber istihbaratın önemini artırmış, hem de 2007 yılında Estonya'da yaşanan olaylardan sonra siyasi çevrelerin de dikkatini çekmiştir. NATO'nun elektronik iletişime bağımlı toplumlarının aynı zamanda siber cephede son derece savunmasız olmalarının ortaya çıkması, ciddi bir tehdit dönüşümünü siber alanda ortaya çıkarmıştır.[21]

2008 yılında, ABD askeri bilgisayar sistemlerine yapılan kapsamlı saldırılarla birlikte siber casusluk daimi tehdit haline gelmiştir. Buna benzer olayların tekrarlanması ve artması ile birlikte dünyada ciddi bir farkındalık oluşmuştur. Ortaya çıkan çok sayıdaki siber olaylarla birlikte sıkı korunan devlet verilerinin kötü niyetli kişilerin eline geçmesi, tehdit algısının boyutunu uluslararası aktörlere taşımıştır.

Siber tehdidin dönüşümü sadece casusluk ve devletlerin verilerine ilişkin bir problemi devletlerin gündemine sokmamıştır. Aynı zamanda siber tehdidin mali olarak, küresel anlamda devletlere ve kurumlara verdiği zarar çok ciddi boyutlara ulaşmıştır. Grafik 2'de görüldüğü üzere başta finansal hizmetler olmak üzere, kritik altyapıların da bağlı olduğu enerji, teknoloji, sanayi ve savunma birimlerine verilen zarar, tehdidin dönüşümü açısından ve oluşturulacak politikaların yetkinliği merkezinde önemli bir yere sahiptir.

[21] NATO'da, ciddi boyutlu bir olay olarak ilk defa Kosova Krizi'nde karşılaşılan siber saldırı dalgası ile birlikte ittifakın e-posta hesabı günlerce ziyaretçilere kapatılmış ve NATO web sitesi kullanılamaz hale gelmiştir. Çatışmanın siber boyutu sadece NATO'nun istihbarat kampanyasını engellemek için girişilmiş bir çaba olarak algılanmıştır.

Grafik 2. 2015 Yılı Siber Saldırıların Küresel Düzeyde Sektörlere Verdiği Zarar



Kaynak: Ponemon Institute, 2015a:10

Yakın coğrafyalardaki ülkelerin kritik altyapılarının, özellikle kimi enerji nakil hatlarında birbirlerine olan bağlılığı ve rakip ülkelerle olan ilişkilerde önemli bir kart oluşu siber tehdidin dönüşümünde dış politika yaklaşımı oluşturmayı da gerekli kılmaktadır. Gelişen ülkeler açısından bu hatların korunmasına ilişkin oluşturulacak ittifaklarda tehdidin dönüşümü bulunulan coğrafyaya göre avantaj dahi sağlayabilecektir. Enerji diplomasisi ve bağlı olduğu kritik altyapıların korunması siber ittifaklarda caydırıcılık oluşturacaktır.

Güvenlik Stratejilerini Siber Çatışmalara Uygulayabilme

Kimi zaman otoriteleri kimi zaman da fiziksel anlamda bireyleri etkileyen olaylar karşısında, güvenlik stratejilerinin siber saldırılarla birlikte nasıl uygulanacağı konusunda çeşitli tartışmalar vardır. Siber saldırılar ve siber çatışma anına ilişkin güvenlik stratejilerinde, uluslararası güvenliğe ilişkin çatışmacı stratejileri uygulayabilmenin hangi durumlarda hayata geçirileceği hususu hem uluslararası hukuk alanında, hem de devletlerin birbiriyle olan ilişkilerinin politik teori zemininde oturmamıştır.

Güvenlik stratejileri açısından, çatışmacı bir boyutta ekonomik yaptırımların siber saldırılara ilişkin, hangi zamanlarda ve nasıl uygulanacağına dair bir düzenleme yapılmamıştır. Bu

noktada örneklendirilebilecek olay da yok denecek kadar azdır. Ekonomik anlamda sarmalın daha da yoğunlaştığı uluslararası sistemde ekonomik yaptırımlar yönünde karar almak zaten zorken siber olaylara ilişkin adımlar gelecek açısından oldukça düşündürücüdür. Bu durumun en önemli sebebi siber saldırılara ilişkin verilerin artık tüm uluslararası aktörleri etkilediği yönündedir ve ekonomik olarak zorlamaların bu tür saldırılardan sonra ciddi paradoksları doğuracağıdır.

Siber saldırıların fiziki olarak bir sonuç doğurması akıllara daha çok askeri yöntemleri getirmektedir. Askeri yöntemler, aşamalı şiddet uygulamasına dayanmaktadır. Farklı yöntemler sonrasında sonuç alınmadığı zaman ortaya çıkan uygulamalarda siber saldırıların boyutu ve verdiği zarar sonrası karşı tarafın kullanacağı askeri bir unsurun da olabileceği kesinlikle düşünülmesi gereken bir husustur. Bu konudaki en önemli sorun saldırıların siber uzayda manipüle edilip, bilinmeyen aktörler tarafından çatışmayı diğer aktörler ya da unsurlar adına körüklemesidir. Siber orduların da askeri birimler olarak yerini aldığı günümüzde, askeri bir karşılık olarak yine siber bir müdahele mi olacağı ya da konvansiyonel unsurlara mı başvurulacağı devletlerin kararlarına ve etkilemek istediği alana bağlıdır. Siber harekatlarda siber saldırıların da fiziksel bir hasar oluşturucağı unutulmamalıdır.[22] Bu durumu Şekil 3, gelişim itibariyle ortaya koymaktadır.

Şekil 3. Siber Harekat Spektrumu

Kaynak: Doğru (t.y.), "Siber Harekatın Uluslararası Hukuk Çerçevesinde Analizi"

[22] Özellikle Gürcistan-Rusya çatışması sırasında Gürcistan hükümetinin servis sunucularına karşı yapılan saldırılar, siber savaş terimine daha da somut bir nitelik kazandırarak çatışmacı güvenlik stratejilerine yerleşecek bir müdaheleyi gözler önüne sermiştir. Yapılan müdaheleler fiziksel bir zararı gözle görülecek şekilde ortaya koymamıştır fakat çatışmanın önemli bir bölümünde Gürcistan hükümetini zayıf düşürmüştür.

Siber saldırıların öngörülemez oluşu ve gerçekleşme hızının saniyelerden daha az zaman dilimleriyle ölçülmesi özellikle tarafların konuyu müzakere etmesi açısından olanaksız görünmektedir. Bunun en önemli sebebi siber savaşa karşı etkili bir caydırıcı niteliğin olmaması ve uluslararası hukuka bağlı kalmanın olanaksızlığıdır. Bu şartlar altında askeri bir misilleme, hem yasal hem de siyasi açıdan zorunlu gözükmektedir.[23]

2010 yılında Stuxnet'in yıkıcı siber savaş yeteneklerindeki öz, güvenlik stratejilerinin siber saldırılarla buluştuğu noktada, önemli bir atılım yaşandığına dikkat çekmiştir. 45000 Siemens kontrol sisteminin etkilendiği saldırılar İran'daki nükleer enerji santralleri açısından, çok önemli olan teknik süreçlerin manipüle edilebileceğini göstermiştir (Denning, 2012:675). Yapılan saldırı, enerji arzını ve trafik ağlarını yöneten kritik bilgisayar sistemlerini etkileme riskini açığa çıkarmıştır. Siber saldırıların ciddi felaketlere yol açabileceği yönündeki algı, güvenlik stratejileri açısından siber müdahele yöntemlerini askeri unsurlar içerisine oturtmuştur.

Siber müdahele yöntemlerinin etkinliğinin artışıyla savunma boyutu yanında devletler saldırı ve çıkar arzusuyla ittifaklar da kurabilecektir. Özellikle tarihsel boyutta güven ilişkilerinin geliştirilebildiği yakın coğrafyadaki devletler bu konuda çıkarsal olarak geçici ittifaklar oluşturabilir ve amaçlar masaya konulabilir.

Siber Uzayda Ortak Güvenlik ve İttifak Oluşturma

Devletlerin dış politika stratejileri açısından en çok sözü edilen konulardan birisi de ittifaklardır. Günümüz dünyasında ise izolasyon türünden bir dış politika stratejisi izleyen ülke sayısı oldukça azdır. Daimi tarafsızlık gibi istisnai nitelikteki durumları da hariç tutulursa, uluslararası sistemde yer alan devletlerin çok büyük bir bölümü dış politikalarını sürdürmekte ittifak oluşturma stratejisinden geniş bir şekilde yararlanmaktadır (Sönmezoğlu, 2014:425).

[23] Devletlerin askeri amaçla kullanılabilecek siber yeteneklere büyük yatırım yapmakta ve siber ordular oluşturmaktadır. İlk bakışta dijital silah yarışı açık ve kaçınılmaz bir mantığa dayanıyor gibi gözükse de siber savaşların çeşitli avantajları mevcuttur. Bu savaş asimetrik, oldukça maliyetsiz ve sadıranın avantajlı olduğu bir durumu ortaya çıkarmaktadır.

İttifak oluşturma ve özelde siber uzayda ortak hareket edebilme, uygulanabilirlik açısından olumlu ve olumsuz yönleriyle, siber politikaların uluslararası düzeyinde irdelenmesi gereken bir hususdur. Özellikle iki kutuplu sistemin çöküşü ile birlikte, siber uzaydaki çatışma alanı ittifak oluşturma adına, kimi gelişmekte olan ülkeler açısından daha da önemli bir yere sahiptir ve pratikte veriler mevcuttur.

Zaten çatışmalı olan bir sistemde siber saldırılar gibi bilinmez bir boyutta, siber alanda gelişme zemini arayan devletler niçin ve nasıl ittifak kurmalıdır? Oluşturulabilecek ittifakların devamlılığı ya da süresine ilişkin ne tür kararlar alınacaktır? Bu ve benzeri soruların altında yatan temel neden, siber saldırılar sonrasında rakip tarafın vereceği tepkinin ölçülemeyecek oluşudur.

Temelde benzer birçok sorunun cevabında devletlerin belirli bir amaca ulaşmak açısından yeterli imkanlara sahip olmakla beraber, bu amaca meşru yollardan ulaşmak veya bu nedenle girişeceği dış politika eylemlerinin sorumluluğunu başka ülkelerle paylaşmak istediğinden diğer ülkelerle ittifaklar yapabilir (Sönmezoğlu, 2014:428). Bu noktada siber ittifaklara yönelik olarak değinilmesi gereken husus tepkinin öngörülemezliği neticesinde sorumluluğun paylaşılması ve hafifletilmesi olabilir.[24] Gücün ittifaklar içinde dengelenmesi veya zayıf toplumların güçlendirilirek, ittifak adına uzun dönemli amaçlar güdülmesi dış politika çıktısı olarak geliştirilebilir (Morgenthau, 2004:126).

İttifak örnekleri bazında, özellikle siber çatışmalar açısından bazı devletlerin NATO bayrağı altında ortak hareket etmesinde, temel olarak farklı nitelikler göze çarpmaktadır. NATO ittifakı altındaki siber müdahelelerde temel olarak sorun, gündemin belirlenmesinde belli devletlerin baskınlığıdır. Bunun farkında olan ABD, denetim imkanlarını arttırmak adına NATO bünyesinde siber güvenliğe ilişkin farklı projelere imza atmakta ve askeri boyutla ilgili baskın bir şekilde olaylara müdahil olmaktadır.

NATO zaten var olan bir örgütlenme olarak siber güvenliğe ilişkin düzenlemeler yaparken, oluşturulacak farklı siber ittifakların işlerliği açısından *casus foederisin*, yani ittifaka ilişkin antlaşmada yer alan taraflara ilgili hak ve yükümlülüklerin hangi koşullar altında geçerli

[24] 1950 yılında, ABD'nin Kuzey Kore'ye müdahelesinde Birleşmiş Milletler bayrağı altında hareket etmek, eyleme meşruiyet kazandırılması açısından önemli bir düşünceydi. ABD'nin bu konudaki sorumluluğunun diğer ülkelerle paylaşılması sağlanmıştır. Türkiye'nin 1974 Kıbrıs Harekatı öncesinde İngiltere'ye başvurarak duruma beraberce müdahele edilmesini istemesi de esas olarak bu türden bir girişimdir (Sönmezoğlu, 2014:429).

olacağının belirlenmesi de önemli hususlardan birisidir. Uluslararası aktörler açısından, özellikle devletler adına siber saldırıların tespiti ve atılacak ortak adımlar üzerinde anlaşılması zor hususların varlığı sorunsalın başında gelmektedir. Siber güvenliğin gelişimine ilişkin ivmeyi de düşünecek olursak sadece çıkarların gözetilmesi, ittifak bünyesindeki her birimin temel önceliği olacaktır.

NATO gibi bölgesel yapılanmalarda, askeri harekat alanlarına siber çatışmaların dahil edilmesi, olaylara müdahil olmada manevra yeteneği de sağlamaktadır. Bu noktada özellikle savunma konseptinde oluşturulan birliklerde seviye eğer bölgeselse bu niteğini korumakta ve kapsam güvenlik boyutuyla beraber çıkar elde etme güdüsüne dönüşmektedir. Özellikle NATO gibi örgütlenmelerin siber güvenliğe ilişkin attığı adımlarda etkinlik kurma arzusu buna iyi bir örnektir. Tablo 1'de görüleceği üzere NATO gibi bölgesel seviyede faaliyet gösteren ve aynı şekilde güvenlik kapsamında oluşturulmuş birliktelikler azımsanmayacak kadar çoktur. Fakat başarı konusunda NATO, siber güvenlik alanında ciddi bir yol katetmiştir.

Tablo 1. Uluslararası Güvenlik/Savunma Örgütleri ve Kapsam

Birlik/Örgüt	***Seviye***	***Kapsam***
BM	*Evrensel*	*Genel Güvenlik*
NATO	*Bölgesel*	*Güvenlik ve Savunma*
AB (AGSP)	*Bölgesel*	*Güvenlik ve Savunma vd.*
OSCE	*Bölgesel*	*Güvenlik*
Şangay İşbirliği Örgütü	*Bölgesel*	*Güvenlik ve Savunma vd.*
Amerika Devletleri Teşkilatı (OAS)	*Bölgesel*	*Güvenlik ve Savunma*
Afrika Birlikği Örgütü (OAU)	*Bölgesel*	*Güvenlik ve Savunma vd.*
Arap Birliği	*Bölgesel*	*Güvenlik vd.*
İslam Konferansı Örgütü	*Bölgesel*	*Güvenlik vd.*
Avrupa Polis Bürosu (EUROPOL)	*Bölgesel*	*Güvenlik ve İstihbarat*
INTERPOL	*Evrensel*	*Suçla Mücadele*
OPANAL	*Bölgesel*	*Nükleer Güvenlik*
SAARC	*Bölgesel*	*Ekonomi ve Güvenlik*
GCC	*Bölgesel*	*Güvenlik ve Savunma vd.*

Kaynak: Yılmaz, 2015

Sonuç Olarak;

Siber güvenlik çalışmalarının uluslararası güvenlik perspektifine kattıkları yanında, uygulama alanına ilişkin yaptığı katkı önemli gözükmektedir. Uluslararası ilişkiler ve güvenlik ile ilgili temel yaklaşımlarda, Soğuk Savaş'ın bitimiyle birlikte, büyük güçlerin çatışma alanlarının azalacağı gibi bir algının siber alanın ele alındığı bütünlük içerisinde anlamsız olduğu ortaya konulmuştur. 11 Eylül olaylarının yeni tehditleri beraberinde getirdiği yaklaşım hem siber güvenlik anlayışında hem de siber alandaki çeşitlilik benzer çalışmaların da konseptini oluşturmuştur. Siber alandaki savunma ve saldırı çeşitliliği güçlü ülkelerin her an tetikte olmaları gerektiğini göstermiştir. Birçok devlet için ise Soğuk Savaş'ın bitimi, güvenlik sorunları bağlamında çözümleri zor paradoksları oluşturmuştur. Siber kapasiteye dayandırılan unsurlar için ekonomik çıkar ve düşmanı zarara uğratma gibi arayışlar kendini hissettirmeye başlamıştır.

Siber güvenlik kavramının dahil olduğu uluslararası güvenlik temelinde, nükleer caydırıcılığın hala ulusal güvenlik konusunda en büyük tehlike olduğu ortadadır. Nükleer, kimyasal ve biyolojik kitle imha silahlarının yaygın olduğu sorunlarla birlikte, farklı sorunların devletleri meşgul ettiği süreçte güvenlik yaklaşımı ve yaklaşımın çeşitlendiği siber alandaki tehditsel durum her geçen gün artmakta ve bu durum politik girişimlerin rasyonelliğinin tartışılmasını gerekli kılmaktadır. Farklı alanlarda olduğu gibi devletler güvenlik temelindeki tehlikeleri bertaraf etmek için rasyonel olduklarını zannettikleri birçok konuda, çoğu zaman ittifak arayışlarına girmektedir.

Sürecin geldiği boyut farklı şekilleriyle anılırken güvenlik temelinin birçok noktasıyla Soğuk Savaş ile ilişkilendirilmesi, dönüşümü devletler bazında kısır bir noktaya sıkıştırmaktadır. Süreç kendi içerisinde, teknolojik gelişmelerle ortaya çıkan farklı imgeleri özgün bir şekilde üretmiştir. Bu sürecin hissedildiği nokta 11 Eylül olmuş, fakat dinamikler kendini özgün nitelikleriyle kurgulamıştır. Siber güvenliğin geldiği noktada devletlerin illegal yapılarla iş birliği içerisinde olması ve güvenlik algısının şaşırtıcı alt başlıklar halinde çeşitlenmesinde bu neden etkili olmuştur.

Uluslararası güvenlik çalışmaları perspektifinde strateji oluşturulmasına ilişkin oluşturulacak ajandalar, bu alanda atılım yapmak isteyen ülkeler adına kaçınılmaz gözükmektedir. Strateji

oluşturulmasına ilişkin siber alanın gelişimi uzun vadeli politikalarla desteklenmezse, veri kayıplarının olması ve ekonomik zararların hissedilmesi kaçınılmaz gözükmektedir. Atılacak adımların uluslararası ilişkiler temelinde, uzmanlık alanlarının oluşturulmasıyla gerçekleşeceği açık bir şekilde hissedilmektedir. Farklı kurumlar aracılığıyla oluşturulan yapılanmalar bu durumun en açık örnekleri haline gelmiştir.

Siber güvenlik temelindeki gelişmelerle birlikte askeri teknolojilerin belirli noktalara taşındığı kara, hava, deniz unsurlarında ve nükleer mücadelede kendini hissettiren siber alandaki çıkar birliktelikleri, hedef unsurlara karşı özgüveni artırmaktadır. Siber alanın güç mücadelesinde, ülkelerin savunma sistemlerine saldıracak ve etki edecek daha gelişmiş yöntemler üzerinde tartışmalar sürmektedir. Bu yaklaşımlar dahilinde, klasik olarak güç algısı yerine farklı araçlarla gücün kapsamını artırma, yeni teorik bir yaklaşımın çıkış noktası olarak dikkate değerdir.

Siber uzayın uluslararası güvenlik açısından tartışılması ve beraberindeki etkileşim, devletlerin dış politikada ve iç politikada sahip olduğu çıktılara dair nedensel bir düzlem sağlamaştır. Siber alanın uluslararası ilişkiler açısından bir savaş alanı olup olmadığına dair eleştiriler olsa da, dijital ortamdaki kaynakların sonlandırılması imkansıza dönüştüğü için yersiz kalmaktadır. Siber alanın beslendiği tüm kaynaklar son bulsa da, verilerin görünmeyen bir sanal ortamda varlığını sürdüreceği gözlerden kaçırılmamalıdır.

KAYNAKÇA

Ağır, Bülent Sarper (2011), "Güvenlik Kavramını Yeniden Düşünmek: Küreselleşme, Kimlik ve Değişen Güvenlik Algısı", **Güvenlik Stratejileri Dergisi**, Sayı 22, 97-131.

Bejtlich, Richard (2015), "Strategic Defence in Cyber Space: Beyond Tools and Tactics", Kenneth Geers (Ed.), **Cyber War in Perspective: Russian Aggression against Ukraine**, 1. Baskı *içinde* (159-170), Tallinn: NATO CCD COE Publications.

Choucri, Nazli ve diğerleri (2013), "Institutions for Cyber Security: International Responses and Global Imperatives", **Information Technology for Development**, 20(2), 96-121.

Choucri, Nazli (2012), **Cyberpolitics in International Relations**, Cambridge: MIT Press.

Çifçi, Hasan (2012), **Her Yönüyle Siber Savaş**, Ankara: TÜBİTAK Bilim Kitapları.

Dedeoğlu, Beril (2003), **Uluslararası Güvenlik ve Strateji**, İstanbul: Derin Yayınları.

Delibasis, Dimitrios (2008), "Information Warfare Operations within The Concept of Individual Self-Defence", Athina Karatzogianni (Ed.), **Cyber Conflict and Global Politics**, 1. Baskı *içinde* (95-113), London: Routledge Chapman Hall.

Denning, Dorothy E. (2012), "Stuxnet: What has Changed?", **Future Internet**, Volume 4, 672-687.

Dewar, Robert S. (2014), "The 'Triptych of Cyber Security': A Classification of Active Cyber Defence", P. Brangetto ve diğerleri (Ed.), **6th. International Conference on Cyber Politics Proceedings**, 1. Baskı *içinde* (7-21), Tallinn: NATO CCD COE Publications.

Doğru, Murat (t.y.), **Siber Harekatın Uluslararası Hukuk Çerçevesinde Analizi**, http://ab.org.tr/ab16/bildiri/106.pdf (24.04.2016).

Dreyfus, Pablo Gabriel (2002), **Border Spillover Drug Trafficking and National Security in South America**, Yayınlanmamış Doktora Tezi, Universite de Geneve, Institut Universitaire de Hautes Etudes Internationales.

Eriksson, Johan ve Giacomello, Giampiero (2007), **International Relations and Security in The Digital Age**, New York, Routledge Publishing.

Galtung, Johan (2009), **Çatışmaları Aşarak Dönüştürmek: Çatışma Çözümüne Giriş**, (Çev. Havva Kök), Ankara: USAK Yayınları.

Gartzke, Erik (2013), "The Myth of Cyberwar: Bringing War in Cyberspace back down to Earth", **International Security**, 38(2), 41-73.

Gürkaynak, Muharrem ve İren, Adem Ali (2011) "Reel Dünyada Sanal Açmaz, Siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, 16(2), 263-279.

Hansen, Lene ve Nissenbaum, Helen (2009), "Digital Disaster, Cyber Security and The Copenhagen School", **International Studies Quarterly**, Volume 53, 1155-1175.

Hare, Forrest (2010), "The Cyber Threat to National Security: Why can't We Agree?", C. Czosseck ve K. Podins (Ed.), **Conference on Cyber Conflict Proceedings**, 1. Baskı *içinde* (211-225), Tallinn:CCD COE Publications.

Hemme, Kris (2015), "Critical Infrastructure Protection: Maintenance is National Security", **Journal of Strategic Security**, 5(8), 25-39.

Hunter, Eve ve Pernik, Piret (2015), **The Challenges of Hybrid Warfare**, Tallinn: ICDS Analysis.

Karabulut, Bilal (2015), **Güvenlik: Küreselleşme Sürecinde Güvenliği Yeniden Düşünmek**, Ankara: Barış Kitabevi.

Kaspersky Lab. (2015), "Kaspersky Security Bulletin", https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin2015_FINAL_EN.pdf (13.07.2016).

Krickovic, Andrej (2016), "Catalyzing Conflict: The Internal Dimension of the Security Dilemma", **Journal of Global Security Studies,** 1(2), 111-126.

Libicki, Martin C. (2007), **Conquest in Cyberspace: National Security and Information Warfare**, Cambridge: Cambridge University Press.

Lindstrom, Gustav ve Luiijf, Eric (2012), "Political Aims & Policy Methods", Alexander Klimburg (Ed.), **National Cyber Security: Framework Manual**, 1. Baskı *içinde* (44-66), Tallinn, NATO CCD COE Publication.

Lupovici, Amir (2011), "Cyber Warfare and Deterrence: Trends and Challenges in Research", **Military and Strategic Affairs**, 3(3), 49-62.

Lutz, James M. ve Lutz, Brenda J (2008), **Global Terrorism**, New York: Roudledge Publishing.

McAfee Labs (2015), "Threat Report, August 2015", http://www.mcafee.com/mx/resources/reports/rp-quarterly-threats-aug-2015.pdf (11.02.2016).

McQuade, Samuel C. (2009), **Encyclopedia of Cybercrime**, London: Greenwood Press.

Morgenthau, Hans (2004), "'The Balance of Power','Different Methods of The Balance of Power' and 'Evaluation of The Balance of Power' from Politics Among Nations: The Struggle for Power and Peace", Karen A. Mingst ve Jack L. Snyder (Ed.), **Essential Readings in World Politics**, 2. Baskı *içinde* (124-130), New York: Norton Publishing.

Ponemon Institute (2015), "2015 Cost of Cyber Crime Study: Global", http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states (06.02.2016).

Sönmezoğlu Faruk (2014), **Uluslararası Politika ve Dış Poltiika Analizi**, 6. Baskı, Der İstanbul: Der Yayınları.

Wallace, Ian (2014), "Ulusal Siber Güvenlik Stratejilerinin Geliştirilmesi", **Analist**, http://www.analistdergisi.com/sayi/2014/06/ulusal-siber-guvenlik-stratejilerinin-gelistirilmesi (13.12.2015).

Walt, Stephen M. (2003), "Güvenlik Çalışmalarının Rönesansı", **Avrasya Dosyası**, 9(2), 71-107.

Yılmaz Sait (2015), **Dünyanın Çivisi Neden Çıktı?**, http://www.ulusalkanal.com.tr/dunyanin-civisi-neden-cikti-makale,5016.html (17.05.2016)

Yorulmaz, Murat (2014), "Değişen Uluslararası Güvenlik Algılamaları Bağlamında Türkiye-Yunanistan İlişkilerinde Değişmeyen Güvenlik Paradoksu", **Balkan Araştırma Enstitüsü Dergisi**, 3(1), 103-135.

ISSN: 2587-1218

RİSK TOPLUMU VE REFLEKSİF MODERNLEŞME ÇERÇEVESİNDE SİBER TERÖRİZM: TANIMLAMA VE TİPOLOJİ SORUNU

Mehmet Emin ERENDOR*

Özet

İki kutuplu dünyanın sona ermesi ile birlikte uluslararası ilişkilerde yeni bir dönem başlamış ve bu dönem özellikle de NATO tarafından riskler ve belirsizlikler ile ifade edilmiştir. Gerçekten de tarihsel süreç içerisinde bakıldığında, Soğuk Savaş sırasında belirgin olan tehdit kavramı, Soğuk Savaş sonrası belirsizleşmiş ve yerini başarısız devletler, ekonomik problemler, terörizm gibi risklere ve belirsizliklere bırakmıştır. Bu makalede Soğuk Savaş sonrası ortaya çıkan ya da giderek daha fazla belirginleşen siber suçlar ve siber terörizm gibi riskler ve tehditler ile ilgili kavramsal konulara yer verilecek ve bu kavramlar açıklanmaya çalışılacaktır.

Anahtar Kelimeler: Beck, Risk Toplumu, Refleksif Modernleşme, Internet, Siber Terörizm

CYBER TERRORISM IN THE CONTEXT OF RISK SOCIETY AND REFLEXIVE MODERNIZATION: THE PROBLEM OF IDENTIFICATION AND TYPOLOGY

Abstract

A new era has begun in international relations with the end of the bipolar world, and this period has been expressed as risks and uncertainties by NATO. Indeed, in the historical process, the concept of threat was apparent during the Cold War, but it has become unclear after the Cold War, and it left its place to risks and uncertainties such as failed states, economic problems and terrorism. In this article, the conceptual issues, risks and threats such as cybercrime and cyber terrorism, which emerging or becoming clearer after the Cold War will be tried to be explained.

Keywords: Beck, Risk Society, Reflexive Modernization, Internet, Cyber Terrorism

Giriş

Soğuk Savaş sırasında hem Batı hem de Doğu Bloku için belirgin olan tehdit kavramı, Soğuk Savaş'ın sona ermesi ile birlikte uluslararası ilişkilerde yerini yeni risklere ve belirsizliklere bırakmıştır. Soğuk savaş sonrası ortaya çıkan başarısız devletler, etnik düşmanlıklar ve toprak anlaşmazlıkları (NATO 1991 Stratejik Konsept) gibi yeni riskler ve belirsizliklere teknolojinin gelişmesi ile birlikte siber suçlar ve siber terörizm gibi yeni sorunlar eklenmiştir. Yeni dönemin Soğuk Savaş döneminden en büyük farkı tehditlerin kolayca belirlenebilmesine rağmen, riskleri ve belirsizlikleri belirlemenin zorluğu ve bunların her yerden gelebilme

* Dr., Southampton University. mehmeterendor@gmail.com adresinden ulaşılabilir.

ihtimalidir. Soğuk Savaş sonrası risk kavramı üzerine çalışmalar yoğunlaşmış ve özellikle de Ulrich Beck ve Anthony Giddens "Risk Toplumu" tezini geliştirmişlerdir. Beck risk kavramını ve risk toplumu bizim endüstrileşmiş yaşam biçimimizin yani modernliğin yan etkileri olarak adlandırmaktadır (Sorensen and Christiansen, 2013: 22). Soğuk Savaş sonrası teknolojinin hızlı bir şekilde gelişmesi ile birlikte bilginin paylaşımı hızlanmış, teknolojik gelişmeler, internet gibi, insanların günlük ihtiyaçlarını karşılamak için kullanılmaya başlamıştır. Bu gibi gelişmeler ile birlikte teknoloji kendi amaçları dışında kullanılmaya başlanmış ve internet üzerinden dolandırıcılık gibi basit suçlar zamanla terör saldırılarına dönüşmeye başlamıştır. Yaşanan bu gelişmeler, Beck'in de belirttiği ettiği gibi modernliğin ya da kendi yaşam biçimimizin yan etkileri olarak düşünülebilir.

Teknolojinin getirmiş olduğu ya da diğer değişle modernliğin yan etkilerinin ortaya çıkarmış olduğu bu yeni riskler, uluslararası toplumun, terörizm gibi uzun zamandır hem tanımlama hem de uluslararası hukukun bu tür risklere ve tehditlere uygulanabilirliğini sorgulaması açısından benzer sorunlara maruz kalmıştır. Bu çalışmada siber suçlar ve siber terörizm üzerindeki tanımlama sorunları üzerine farklı bakış açısı getirilerek tanım sorunu giderilmeye çalışılacaktır, fakat bunun öncesinde Beck ve Giddens'ın belirtmiş olduğu Risk Toplumu ve Refleksif Modernleşme 'den kısaca bahsedilecektir.

Risk Toplumu ve Refleksif Modernleşme

Sorensen ve Christiansen de (2013: 22) Beck gibi riskleri modernliğin istenmeyen yan etkileri olarak tanımlamakta ve bu yan etkilerin planlanmadığını, istenen bir şey olmadığını ve tahmin edilemediğini söylemelerine rağmen, bu yan etkilerin başarılı olan her endüstri toplumunda ortaya çıktığını savunmaktadırlar. Buradan hareketle Beck'in (2009: 9) de belirtmiş olduğu risklerin modern hayatın bir parçası ve ürünü olduğunu ve geleceğe etkisi olan olaylar bütünü olarak değerlendirebilir. Burada önemli olan konu risklerin şu anda meydana gelmediği ama ileri de olabileceğidir (Mythen, 2004: 14). Myhten, Ewald'ın görüşlerini yorumlayarak, "Modern söylemde, risk geleceği kontrol etme ve tahmin etme arzusuyla ilgilidir: Bir riski ustalık zamanında hesaplamak, geleceği disiplin etmektir. Geleceği sağlamak sadece günden güne yaşamak ve kendini kötü şansa karşı silahlandırmak değildir, ama bir taahhüdü matematikleştirmek demektir" (Mythen, 2004: 14). Risk toplumunu Myhten'in görüşleri bağlamında bir modernlik eleştirisi olarak değerlendirebilir ve tahminlerin ya da

değerlendirmelerin risk toplumunda dünyanın geleceğini kurtarmak için kullanılan temel bir araç olduğu değerlendirilebilir.

Risk toplumu tezine göre, 1986 yılında meydana gelen Çernobil kazası/faciası risk toplumu karakteristiğinin en önemli örneklerinden bir tanesidir (Abbott, Wallace ve Beck, 2006: 105). Abbott, Wallace ve Beck (2006: 105) bu facianın sonuçlarının belirsiz olduğunu, nedenlerinin karmaşık olduğunu ve gelecekteki etkilerinin tahmin edilemeyeceğini söylemektedirler. Diğer yandan Zinn (2008: 11) Çernobil'de meydana gelen patlama devletlerin bu büyük ölçekli teknolojileri kontrol etme yeteneğini göstermektedir. Çernobil faciası devletlerin hem kendi toprakları üzerindeki kontrolün ve güvenliğin sorgulanmasına neden olmuş hem de risklerin kontrol altına alınamayacağını fazlasıyla ortaya çıkarmıştır (Beck, 1992: 13). Ayrıca, Beck (1998: 14) risk kavramını iki farklı aşamaya ayırmıştır. Beck'in risk kavramını iki farklı aşamada incelemesi sadece modernlik eleştirisi altında incelenebilir, çünkü ilk aşamada risk, modernliğin etkisinden hoşlanmayan ya da diğer bir değişle zevk almayan bir yerinden gelebilmesine rağmen, ikinci aşamada risk, insanların ve modernliğin üretimi sonucu ortaya çıkar. Beck (1998: 10-12) bu durumun modern toplumların riskleri ve tehditleri kontrol altına almaya çalışmasından kaynaklandığını fakat bu çaba sonucunda risk durumunun daha da gelişmesine yardımcı olduğunu iddia etmektedir. Sorensen (2013: 23) modern toplumların bu yüzden modernliğin istenmeyen yan etkileri ile karşı karşıya kaldığını söylemektedir.

Aslında tarihsel süreç içerisinde de incelendiği zaman, risk kavramının nasıl değiştiği görülebilmektedir. Beck ve diğerlerinin (2003: 2) risk kavramını modernliğin aşamalarına göre incelemesi de risk kavramının zamanlara göre değişmesinden kaynaklandığı görülmektedir. Lash'a göre (2003: 50) basit modern toplumlarda ya da modernliğin ilk aşamasındaki toplumlarda topluluk yapısının doğrusal olduğunu ve bir dengenin olduğunu söyleyerek, bu toplumlardaki risklerin yalnızca dış unsurlardan gelebileceğini ve sistemin ancak dış kuvvetlerle değişebileceğini ifade etmektedir. İkinci modernlik aşamasında ya da döneminde ise riskler ilk döneme oranla her yerden gelebilmektedir. Beck (1992: 49) bu durumu şu şekilde açıklamaktadır; "sınıf toplumlarının ya da ilk toplumların itici gücü tek bir cümle de özetlenebilir 'Açım!'. Diğer yandan risk toplumu tarafından harekete geçirilen olgu şu şekilde ifade edilmektedir: 'Korkuyorum'' Endişe ortaklığı ihtiyaç ortaklığının yerine geçer." Buradan da anlaşılacağı gibi ilk ve ikinci modern tolum arasında kuvvetli bir fark vardır, çünkü endüstrileşme ve teknolojik gelişim, toplum içerisinde korku yaratabilmektedir

ve bu gelişmeler sadece sosyal amaçlar için kullanılmamakta ve ayrıca teröristler ve diğer unsurlar tarafından topluma karşı acı vermek için de kullanılmaktadır.

Beck (1992: 19-20) ayrıca risk toplumu ile ilgili çalışmasında şunu belirtmektedir:

> *Modernleşme refleksif hale gelmektedir, kendi kendisinin ana teması hale gelmektedir. Teknolojinin gelişimi ve istihdamı ile ilgili sorular (doğa, toplum ve kişilik alanlarında) fiilen veya potansiyel olarak kullanılan teknolojik keşiflerin riskleri -uygulanması, kabul edilmesi/onaylanması, önlenmesi veya saklanması gibi özel şekilde tanımlanmış görüş ile ilgili- risklerin siyasi ve ekonomik yönetimi ile ilgili soruları nedeniyle gölgede bırakılmaktadır.*

Beck'in bu görüşleri son dönemde uluslararası arena da yaşanan yeni risklerle ve tehditlerle örtüşmektedir, çünkü teknolojik ve ekonomik gelişmeler, devletlere ve toplumlara refah getirirken, diğer taraftan siber suçlar ve siber terörizm gibi yeni risklerin de ortaya çıkmasına neden olmaktadır. Bu teknolojik gelişmelerin teröristler veya hackerler tarafından kendi siyasi, ekonomik ve diğer ideolojik amaçlar için kullanılması, toplumlar için yeni risklerin ve tehditlerin ortaya çıkmasına neden olmaktadır. Aslında bu durum bir anlamda modernliğin rastgele ve bilinçsiz bir şekilde yaşandığını (Çuhacı, 2007: 131) ve modernlik içerisindeki bu gelişmelerin sonucunun daha önceden tahmin edilemediğini ya da diğer bir değişle Beck'in de bahsettiği gibi risklerin önceden görülemediğini ve onlara karşı önlem almanın zor olduğunu gözler önüne sermektedir.

Beck'in açıklamaya çalıştığı bu yeni dönem, yani ikinci modernlik dönemi refleksif modernlik olarak adlandırılmaktadır (Beck, Bonss ve Lau, 2003: 1). Beck ve diğerlerine göre (2003: 1), "Refleksif Modernleşme ile ikinci dönem kastedilmektedir: modern toplumun modernleşmesi. Modernleşme belirli bir aşamaya geldiğinde kendisini radikalleştirir. Sadece ana kurumları değil aynı zamanda toplumun ilkelerini ikinci defa dönüştürmeye başlar. Fakat bu defa dönüştürülen ilkeler ve kurumlar modern toplumun ilkeleri ve kurumlarıdır." Williams (2008: 30) refleksif modernleşme sürecine 'refleksif' denmesinin nedenini toplumun dışsal durumlarla yüzleşmesinden ziyade kendisi ile yüzleşmesinden dolayı söylendiğini ifade etmektedir. Buradan anlaşılacağı gibi refleksif modernleşmede modernlik kendisini eleştirerek kendisini yeni ve gerçek bir modernliğe dönüştürmek için alternatif yollar aramaktadır. Bu duruma en güzel örnek NATO'nun1991 Stratejik Konsepti gösterilebilir, çünkü, örgütün kuruluş amacı Sovyetler tehdidine karşı üyelerini korumak olmasına rağmen, Sovyetlerin dağılmasıyla birlikte kendi kimliğini uluslararası alanda yeniden geliştirmek/değiştirmek zorundaydı ve bu durum da Beck'in de bahsetmiş olduğu refleksif modernliğe uymaktadır.

Ayrıca Rasmussen (2001: 298) NATO'nun içinde olduğu bu durumu refleksif modernlikle açıklamakla birlikte, NATO'nun inşa döneminde olduğunu belirtmektedir ve bu durumu refleksif modernliğin ana karakteristik özelliklerinden birisi olarak açıklamaktadır. NATO kendisini yeni bir güvenlik gündemi oluşturduğu yapıcı karakterle tanımlamaktadır. NATO'nun kendisine yeni güvenlik gündemi oluşturması ve ilerleyen dönemlerde de bu güvenlik gündemine siber risk ve tehditleri eklemesi, inşa sürecinin gündelik olarak devam ettiğini ya da bu sürecin uluslararası ilişkilerin hızlı değişen yapısına bağımlı olarak hareket ettiğini göstermektedir.

Rasmussen refleksif güvenlik politikalarını açıklamaya çalışırken, Beck'in geliştirmiş olduğu risk toplumu tezini kullanmakta ve ona göre refleksif güvenlik ancak üç temel başlık altında incelenebilir; risklerin yönetilebilirliği, geleceğin varlığı ya da geleceğin bugünden yaşanması ve son olarak bumerang etkisi olarak tanımlamaktadır (Rasmussen, 2001: 298). Rasmussen (2006: 4) refleksif güvenlik politikalarını açıklarken, risk kavramını bir senaryo olarak tarif etmekte ve bunu bir senaryonun gerçekleşme ihtimalinin nasıl önleneceğine ilişkin bir politika önerisinin izlediğini ifade etmektedir. Refleksif modernlik içerisindeki riskin en temel farkı bitiş noktasının olmamasıdır, çünkü eğer bir devlet bir riski ortadan kaldırmaya çalışırsa, yeni bir riskin ortaya çıkma ihtimali vardır. Rasmussen'e göre Foucault'un önermiş olduğu Modern Yönetim örneği gibi politikalar da devleti güvenli limanlara ulaştırabilir ve ona göre risklere yönelik alınacak kararlar bu güvenli limana ulaşabilmek için önemlidir (Rasmussen, 2001: 291-292).

Risk kavramı üzerindeki en önemli nokta kararlardır ve alınacak her karar, riskin ölçeğini ve önceliğini belirleyecektir. Williams (2008:62) geleceğin bugünden yaşanmasını/geleceğin varlığını şu şekilde açıklamaktadır; "Yönetim süreci, gelecekte meydana gelebilecek olası olayları yönetmekle ilgilidir; bu olaylar henüz gerçekleşmemiştir, bugünün harekete geçme nedenidirler." Buradaki temel inanç, riskin varlığıdır ve henüz meydana gelmemiştir, fakat bugünü motive eden en temel kavramlardan bir tanesidir. Beck'in (1992: 34) de bahsettiği gibi risk bilincinin temeli gelecekte yatmaktadır ve icat edilmiş, kurgulanmıştır. Amerika'nın Irak'a düzenlemiş olduğu askeri harekât bu duruma verilecek en güzel örneklerden bir tanesidir. Bush'un askeri harekât öncesi yapmış olduğu konuşmaların temelinde de bu düşünce yatmaktadır (Williams, 2008: 62-63).

Son olarak, Rasmussen'in refleksif güvenliği açıklamak için kullandığı Bumerang etkisi ise, riskin kendi üreticilerine yani kaynağına dönmesidir. Kısaca belirtmek gerekirse, devletlerin ya da toplumların riskleri engellemek için başvurduğu yollar yeni risklere neden olmakta ve bundan dolayı da riskin kontrol altına alınamamasına neden olmaktadır. Tekrar belirtmek gerekirse, Irak'a yapılan askeri müdahale Bumerang etkisine verilecek önemli örneklerden bir tanesidir. Çünkü Irak müdahalesinin ana amacı kimyasal silahların geliştirilmesinin ve kullanılmasının önüne geçmekti, fakat Williams'a göre (2008: 63) her ne kadar bu risk ortamı ortadan kaldırıldıysa da, Washington bu müdahalesiyle Irak'ın kapılarını teröristlere açmış ve onlar için burası en iyi terörist eğitim alanına dönüşmüştür. Açıkça görüldüğü gibi, her ne kadar bir risk ortadan kaldırılmış olsa da yeni risklerin ortaya çıkması engellenememiştir ve bu durum Rasmussen'in (2006: 39) de belirttiği gibi risk tuzağına dönüşmüştür.

Risk toplumu ve refleksif modernlik teorisinde de görüldüğü gibi, devletlerin ya da toplumların kendilerini daha üst düzeye çıkarma çabaları sonucu ortaya çıkan hem teknolojik hem de ekonomik gelişim, yeni risklerin ortaya çıkmasına ve bunun sonucunda da bu risklerin ana üreticilere dönüşmesine neden olabilmektedir. Son dönemlerde meydana gelen gelişmelerle düşünüldüğü zaman, siber suçların ya da daha dar kapsamlı siber terör faaliyetlerinin modernleşmenin getirmiş olduğu risklerden ve tehditlerden olduğu açıkça görülmektedir. Son yıllarda uluslararası arenada devletler hem kendi kurumlarını hem de kendi ilkelerini dönüştürmekte ve siber risk ve tehditlere yönelik politikalar üretme yoluna gitmekte ve bu durum siber orduların ortaya çıkmasına neden olmaktadır. Görüldüğü üzere bu dönüşüm süreci sürekli olarak devam etmekte ve refleksif modernleşme süreci ortaya çıkacak risklere ve tehditlere göre varlığını sürdürecektir.

Bu bölümde risk toplumu ve refleksif modernleşme analiz edilmeye çalışıldı. Gelecek başlık altında teknolojik ve ekonomik gelişmeler sonucu ortaya çıkan ve modern toplumun son dönemlerde karşılaştığı en büyük risklerden ve tehditlerden bir tanesi olan siber güvenlik sorunları kavramsal olarak açıklanmaya çalışılacaktır.

Siber Terörizm

Soğuk Savaş sonrası, modern toplumların gelişmesi ya da diğer bir ifadeyle refleksif modernleşme ile birlikte bilgi teknolojilerinin (veri transferi, hızlı iletişim gibi) gelişmesi ve farklı toplumlar arasındaki kültürel etkileşimin artması ile birlikte yeni bir dönem başlamıştır.

Ayrıca ortaya çıkan bu gelişmeler Beck'inde ifade ettiği gibi risk toplumunun oluşmasına ve yeni risklerin ve tehdit unsurlarının meydana gelmesine neden olmuştur. Çünkü ortaya çıkan yeni durumla birlikte yani bilgi alışverişinin hızlanması ile birlikte bilgi transferini engellemek, bilgisayar teknolojileri ile ilişkili diğer unsurları ya da riskleri engellemek artık daha da zorlaşmıştır. Teknolojik gelişmelerin farklı amaçlar çerçevesinde kullanılması sonucu hem devletler hem de uluslararası örgütler bilgisayar ya da diğer bir değişle siber dünyanın riskleri ve tehditleri ile yüzleşmek zorunda kalmışlardır. 1999 yılında NATO[25] ve 2007 yılında Estonya'ya [26] yapılan siber saldırılar, bu risk ve tehditlerin giderek artmasına neden olmuştur.

Teknoloji ve bilgi teknolojilerindeki hızlı gelişme, siber uzayın teröristler tarafından devletlere ve uluslararası örgütlere karşı kullanılması yaygınlaşmıştır. Özellikle, 2007 yılında Estonya'ya karşı yapılan ve üç hafta süren saldırılar, siber saldırıların insanların hayatlarına zarar verebilme ihtimali üzerinde daha fazla düşünülmesine neden olmuş ve özellikle de hükümetlerin prestijini önemli derecede olumsuz etkileyebileceği açıkça görülmüştür.

[25] Kosova Savaşı sırasında NATO ilk defa siber saldırılarla yüzleşmiştir. 30 Ocak 1999 tarihinde NATO Konseyi, NATO Genel Sekreteri'ne Yugoslavya içerisindeki Sırp hedefleri vurma konusunda yetki vermiş ve 24 Mart 1999 tarihinde bu hedeflerin vurulmasına yönelik direktifin verilmesi ile birlikte NATO'ya karşı ilk siber saldırı gerçekleştirilmiştir. Buradaki temel amaç NATO'ya karşı Sırp halkının tepkisini göstermek ve NATO saldırılarını önlemektir. Detaylı bilgi için: NATO (1999), *Statement by the North Atlantic Council on Kosovo*, 30 January, Available at: http://www.nato.int/docu/pr/1999/p99-012e.htm (Erişim Tarihi at: 25/01/2017); Healey, J. and Bochoven, L.V. (2012). NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow. *Atlantic Council Issue*, February.

[26] Estonya Soğuk Savaş sonrasında ülke içerisinde bulunan Sovyetler Birliği zamanlarından kalma anıtları ve heykelleri kaldırma ya da farklı lokasyonlara taşıma kararı almıştır. Ülke içerisinde Bronze Soldier olarak adlandırılan Bronz Asker heykeli Sovyetlerin Nazi Almanya'sına karşı kazanmış olduğu zafer sonrası dikilmiş ve Estonya hükümeti aldığı karar ile bu heykeli 2007 yılı içerisinde Tallinn merkez konumdan Askeri mezarlığa taşımak istemiştir. Sovyetler Birliği'nin kendi kontrolündeki ülkelerde uygulamış olduğu nüfus politikası çerçevesinde Estonya'ya da Rus nüfusu yerleştirilmiş ve ülkedeki nüfus dağılımı dengelenmeye çalışılmıştır. Estonya hükümetinin almış olduğu bu karar ülke içerisindeki Rusların tepkisine neden olmuş ve bu durum Rusya'ya kadar sıçramıştır. Estonya içerisindeki Ruslar ana topraklarındaki Ruslarında desteği ile birlikte Estonya siber altyapısına saldırılar yapmış ve bu saldırılar yaklaşık olarak üç hafta sürmüştür. Bu saldırılar sırasında Estonya hükümet yetkilileri NATO'ya başvurarak 5. maddenin uygulanmasını istemiş, fakat bu saldırılar 4. madde çerçevesinde değerlendirilerek Estonya'ya siber güvenliği sağlaması için destek verilmiştir. Daha fazla bilgi için: Traynor, I. (2007). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (Erişim Tarihi: 08/01/2017); Associated Press (2007). *Removal of Soviet War Memorial Sparks Deadly Riots in Estonia*. http://www.foxnews.com/story/2007/04/27/removal-soviet-war-memorial-sparks-deadly-riots-in-estonia/ (Erişim Tarihi: 08/01/2017); Malksoo, M. (2007). *The Fallen 'Bronze Soldier' …(A Response to: Is This the Order we wanted?)*, http://www.icds.ee/index.php?id=73&tx_ttnews%5Btt_news%5D=164&tx_ttnews%5BbackPid%5D=99&cHash=bcff323714 (Erişim Tarihi: 08/01/2017); Lehti, M., Jutila, M., and Jokisipila, M. (2009). Never Ending Second World War: Public Performances of National Dignity and Drama of the Bronze Soldier. *Journal of Baltic Studies*, Vol. 39(4), http://blogs.helsinki.fi/majutila/files/2009/07/nesww.pdf (Erişim Tarihi: 08/01/2017); Ehala, M. (2009). *The Bronze Soldier: Identity Threat and Maintenance in Estonia*. http://lepo.it.da.ut.ee/~ehalam/pdf/Identity%20threat.pdf (Erişim Tarihi: 08/01/2017); Nazario, J. (2009). Politically Motivated Denial of Service Attacks. Czosseck, C. and Geers, K. (eds.) (2009), *The Virtual Battlefield: Perspectives on Cyber Warfare*, CCDOE Publications, Estonia: IOS Press.

İnsanlığın yararı için geliştirilen fakat gelecekteki olumsuz etkileri hesaplanamadan insanların kullanımına sunulan bazı gelişmeler, teröristler ve ya kötü niyetli insanlar tarafından farklı amaçlar çerçevesinde kullanılmaya başlanılarak, terörizmden daha tehlikeli bir olgu yaratılmasına neden olmuştur. Hawks (2011: 1) teröristlerin artık eski taktikler dışında daha az maliyetli imkanlar kullanarak devletlere saldırabileceğini ve özellikle de kritik öneme sahip bilgisayar sistemlerine virüsler göndererek bir ülkenin ya da kıtanın askeri, siyasi ve ekonomik kaynaklarını felce uğratabileceklerini belirtmektedir.

Terörizmin bu yeni yüzünün daha etkili olabileceği ve devletler üzerindeki baskıyı daha fazla arttırabileceği mümkündür. Devletlerin giderek teknolojik gelişmelere bağımlı olması ve SCADA sistemlerinin, elektrik santrallerinin ya da daha da önemlisi nükleer santrallerin bilgisayar teknolojilerine bağlı olması, buralara yapılacak bir saldırıda etkilenecek insan sayısının artmasına neden olacaktır. Ayrıca belirtmek gerekir ki, siber terörizm geleneksel terörizm faaliyetlerinden daha az maliyetlidir ve sadece bilgiye dayanarak kilometrelerce öteden başka bir ülkeyi etkileyebilme kapasitesine sahiptir. Weimann (2004: 6) bu durumu şu şekilde açıklamaktadır:

> *Siber terör, geleneksel terörizm biçimlerine göre daha az fiziksel eğitim, psikolojik yatırım, daha az ölüm riski ve seyahat riski gerektirir ve bu da terör örgütlerinin takipçileri işe alıp tutmalarını kolaylaştırır… Siber terörist hükümetlerin, bireylerin, kamu hizmetlerinin, özel havayollarının ve benzerlerinin bilgisayarlarını ve bilgisayar ağlarını hedef alabilir. Potansiyel hedeflerin sayısı ve karmaşıklığı, teröristlerin bunların zayıflıklarını ve zayıf noktalarını bulma ihtimallerini arttırıyor.*

Bu nedenlerden ötürü diğer terörizm türlerinden bağımsız olarak hükümet ve kamu hizmetlerine yönelik saldırılar toplum üzerinden daha fazla korku yaratma ve daha fazla başarı sağlama eğilimine sahiptir.

Siber terörizm de geleneksel terörizm kavramı gibi uluslararası toplum tarafından kabul edilmiş ortak bir tanım sorununa sahiptir. Siber terörizm farklı yazarlar tarafından tanımlanmaya çalışılmıştır. Bu çerçevede, Dorothy Denning şu tanımı tercih etmiştir:

> *Siber terörizm, siber boşluk ve terörizmin bileşimidir. Siber terörizm, siyasi ve sosyal mercilere ve kişilere gözdağı vermek, baskı oluşturmak maksadıyla resmi birimlerin bilgisayarlarına, network sistemlerine, bilgi ve veri tabanlarına yapılan yasadışı tehdit ve zarar verici saldırılardır. Daha da ötesi, bir saldırının siber terörizm olarak tanımlanması için bireye ya da mala karşı şiddet içermesi gerekmektedir. En azından "korku*

> *yaratacak kadar hasara" yol açmalıdır. Siber terör ölümcül olan ya da fiziki hasara yol açan, şiddetli ekonomik kayba neden olan saldırılar olarak örneklenebilir. Kritik altyapı odaklarına yapılan ciddi saldırılar yarattığı etkiye göre siber terörizm olarak tanımlanabilir. Önemli olmayan servislere verilen rahatsızlıklar siber terörizm olarak tanımlanamaz.* (TASAM, 2004: 5; Denning, 2003: 1).

Denning'in tanımı uygun koşullar göz önüne alındığı zaman şiddet içermeyen eylemlerin de (en azından korku yaratmak için yeterli derece de zarar verme eylemi) siber terörizm olarak kabul edilmesi gerektiğini ifade etmektedir. Taliharm (2010: 65) Denning'in siber terörizm tanımlamasının siber teröristler ile kötü niyetli bir hacker, kimlik hırsızı, düzenbaz, klavye delikanlısı veya siyasi motivasyona bağlı kurumsal casus arasında ayırım yaptığını düşünmektedir. Ayrıca bu tanımın korsanlık, spam, kimlik avı ve bilgisayarın kötüye kullanımı ile alakalı diğer türlerden ayırdığını ifade etmesine rağmen, siber teröristlerin de bu taktikleri kullanabileceğini belirtmektedir. Denning'in siber terörizm tanımlamasının ilk tanımlamalardan biri olması ve zamanın koşullarına göre en iyi tanımlamalardan bir tanesi olmasına rağmen siber terörizmi dar kapsamlı bir şekilde ele almaktadır. Jarvis, Nouri ve Whiting'e göre (2014: 28), siber terörizmin ana hedefi ya da diğer bir değişle bir saldırının ana hedefi, siber terörizmi siyasi bir amaç için motive edilmiş diğer saldırı tiplerinden farklı kılmaktadır. Kısaca belirtmek gerekirse, Denning'in tanımına göre bir saldırının bir bilgisayar aracılığıyla işlenmesi gerekmez, ama saldırıların ana ya da temel amacı bilgisayarlar veya ağlardır.

Stratejik ve Uluslararası Çalışmalar Merkezi (CSIS) 1998 yılında siber terörizmi, siyasi olarak motive edilmiş alt ulusal gruplar, gizli ajanlar veya bireyler tarafından bilgi ve bilgisayar sistemlerine, bilgisayar programlarına ve verilere karşı yapılan savaş dışı hedeflere yönelik önceden planlanmış saldırılar olarak tanımlamaktadır (Colarik, 2006: 46). Bu tanım da Denning'in siber terörizm tanımlaması gibi dar kapsamlıdır, çünkü bu tanıma göre siber terörizmin olması için saldırının bilgisayar aracılığı ile yapılmasına ihtiyaç duymamaktadır ve yalnızca siyasi olarak motive edilmiş saldırıları siber terörist saldırı olarak kabul etmektedir. Diğer yandan Lewis (2002: 1)'de siber terörizmi dar kapsamlı bir şekilde tanımlamaktadır. Ona göre, siber terörizm bilgisayar ağı araçlarının kritik ulusal altyapıların yani enerji, ulaşım ve hükümet operasyonları gibi altyapıların kapatılması veya bir hükümeti veya sivil nüfusu zorlamak veya yıldırmak için kullanılması olarak tanımlamaktadır. Bu tanım dar kapsamlı olmakla beraber bir saldırının siber terör saldırısı olabilmesi için gerekli olan zorlama ve yıldırma seviyesini belirtmediğinden ve aynı zamanda da siber altyapıların bilgisayar ağı

aracılığı ile nasıl kapatılabileceğini belirtmemesinden dolayı kapsamlı bir siber terörizm tanımı olarak kabul etmek zordur.

Fidler (2014: 8) Lübnan Özel Mahkemesinin uluslararası terörizm suçunun, cezai bir eylem, ulus ötesi bir unsurun dahil edilmesi ve halk arasında korku yaymak veya doğrudan veya dolaylı olarak ulusal yada uluslararası bir otoritenin bazı eylemlerde bulunmasına veya almasına engel olmak amacıyla yapılan eylemler olmak üzere üç unsurdan meydana geldiğini belirtmiş ve bu terörizm formülünün bilgisayar sistemlerine yetkisiz erişim yönünden siber terörizm ile uyum içerisinde olduğunu belirtmiş olmasına rağmen, bu tanım da belirsizdir.

Kısaca, siber terörizmin bir tanım sorunu olduğunu ve genel olarak yapılan tanımlamalarda siber terör saldırılarının ideolojik veya siyasi amaçlar doğrultusunda korku, ekonomik zarar, siyasi veya sosyal hedeflere yönelik şiddet içerdiği ya da içerebileceği belirtilmiştir. Bana göre siber terörizm, iletişim, ulaşım, enerji, güvenlik, SCADA, bankacılık sistemleri ve aynı zamanda kişisel bilgiye yönelik, devletlere ve uluslararası topluma korku vermek amacıyla, ulusal ve uluslararası kritik altyapıyı bozmak ve /ya yok etmek amacıyla hedef devletlere karşı teröristler, saldırganlar veya alt ulusal grupların siber uzayı kullanarak siyasi, kültürel veya ekonomik amaçlar doğrultusunda yapmış olduğu saldırılardır. Ayrıca Stanford Taslağı 3. Maddesinin (f) fıkrasına göre uluslararası terörizm sözleşmelerinde bahsedilen herhangi bir siber sisteme karşı yapılacak saldırı da siber terörizm olarak kabul edilmektedir (Sofaer ve Goodmani, 2000: 28).

Siber terörizm genel olarak bu şekilde tanımlanmakla birlikte, bilim adamları siber terörizmin saldırı tiplerini farklı tipolojiler altında incelemektedirler. Jalil (2003: 8) siber terörizm içerisindeki saldırıları beş farklı kategori altında incelemektedir.

1- Saldırı: siber teröristin temel amacı bir ağa erişerek bilgi elde etmek ya da sistem içerisindeki bilgileri değiştirerek diğer tarafa karşı avantaj elde etmek istemektir. (Gizli hükümet bilgilerini ve kişisel bilgileri çalmak gibi).

2- Tahribat: isminden de anlaşılacağı gibi asıl amaç bilgisayar sistemlerini yok etme veya zarar verme. 2007 Estonya saldırıları verilebilecek en önemli örneklerden bir tanesidir.

3- Dezenformasyon: bu tip saldırıların amacı söylentiler aracılığıyla hedef devlet içerisinde korku ve kaos ortamı yaratmaktır.

4- Hizmet Dışı Bırakma: bu tip saldırıların amacı çevrimiçi bilgisayar sistemlerini kilitlemektir.

5- Web siteleri Tahrif Etme: bu tip saldırılarda ise amaç web sitelerini bozmak ya da tahrif etmektir. Yani amaç web sitesi içerisindeki bilgileri tahrif ederek terör örgütlerinin propagandasını yapmak için elverişli hale getirmektir.

Jalil siber terörizmin saldırı şekillerini beş farklı başlık altında incelerken, Zanini ve Edwards (2001: 41-46) daha dar kapsamlı olarak üç farklı başlık altında değerlendirmektedirler. Zanini ve Edwards bu başlıkları şu şekilde sıralamaktadırlar; ilk olarak, yeni üyeler kazanmak, teröre finansman sağlamak ve toplum üzerinde etki bırakmak için internet üzerinden algı yönetimi ve propaganda yapmak; ikinci olarak, interneti ve bilgisayar sistemlerini kullanarak hedef sistemleri bozmak ve son olarak teknolojiyi kullanarak hava trafiği kontrol merkezi, su ve enerji sistemleri gibi kritik altyapılara zarar vermek olarak sınıflandırmaktadırlar. Görüldüğü üzere siber terörizmin sınıflandırmasına yönelik çeşitli yaklaşımlar bulunmasına rağmen, bu yaklaşımlar değişen dünya şartları içerisinde dar kapsamlı olarak kalmaktadırlar.

Avrupa Konseyi de siber terörizm çerçevesindeki saldırıları daha kapsamlı olarak sınıflandırma yoluna gitmiştir. Aşağıda ki tabloda da görüldüğü gibi Avrupa Konseyi siber saldırıları üç farklı gruba ayırmakta ve internetin kullanım amacına göre terör örgütleri ve teröristler tarafından güdülen politikaları belirtmektedir.

Ayrıca Avrupa Konseyi siber saldırı tipolojisini belirlerken teröristlerin ve terör örgütlerinin neden internet ve diğer bilgi teknolojilerini tercih ettiklerini belirtmektedir. Avrupa Konseyi'ne göre (COE, 2008: 16-17) teröristler, saldırıları dünyanın her tarafından başlatabilir, daha hızlı saldırılar düzenleyebilir, gizli hizmetler kullanılabilir, internet ortamında daha kolay saklanılabilir, saldırıyı yapanı kimliğini bulmak zordur ve internet kullanımı daha ucuzdur ve küçük bant genişliğine bağlantısı ile istediğini gerçekleştirebilir. Avrupa Konseyi'nin yapmış olduğu bu açıklama aslında bir anlamda da siber terörizmin geleneksel terörizmden farkını ortaya koymaktadır.

Tablo 1: Avrupa Konseyi Siber Olaylar Tipolojisi

A. İnternet Üzerinden Saldırılar	B. İçeriğin Yaygınlaştırılması	C. İnternetin Diğer Amaçlar İçin Kullanılması

A) Altyapı Saldırıları a) Türleri - Büyük Ölçekli Saldırılar - Bilgisayar Korsanlığı Saldırıları - Karma (Hybrid) Saldırılar - Fiziksel Hasarla Sonuçlanan Saldırılar	C) Teröristlerin Görüşlerinin Sunulması	G) Bireysel İletişim
B) İnsan Hayatına Yönelik Saldırılar - Kontrol Sistemlerini Kullanarak Yapılan Saldırılar - Uzun Vadeli Gelişmeler	D) Propaganda ve Tehditler	H) Internet'in Planlama ve Destek Aracı Olarak Kullanılması
	E) Asker Toplama ve Eğitim	
	F) Para Toplama ve Finans	

Kaynak: The Council of Europe (2008), *Cyber terrorism: The Use of The Internet for Terrorist Purposes*, Strasbourg: Council of Europe Publishing.

Yukarıda farklı siber terörizm tipolojileri verilmiş ve kapsamlı bir şekilde sınıflandırılmıştır. Bu sınıflandırmalara karşı 2000'lerin başında Ballard, Hornik ve McKenzie tarafından yapılan ve siber terörizm saldırı tiplerini dört farklı gruba ayıran yaklaşım da o dönem ki en kapsamlı sınıflandırmalardan bir tanesidir.

Tablo 2'de de görüldüğü üzere Ballard ve diğerlerine göre siber terörizm içerisindeki taktikler ve saldırılar dört farklı başlık atında incelenebilir. Ballard ve diğerlerine göre (2002: 1008) bilişim saldırıları web sitelerini bozma veya yok etme ve hizmeti engelleme saldırıları gibi farklı şekillerde görülebilir. Bilişim saldırıları ayrıca zararlı kod veya kötü amaçlı yazılım şeklinde de kendini göstermektedir.

Tablo 2: Siber Olaylar Tipolojisi

Kategori	**Tanım veya Açıklama**
Bilişim Saldırıları/Bilgi Saldırıları	Siber terör saldırıları daha çok elektronik dosyaların, bilgisayar sistemlerinin veya

	diğer çeşitli materyallerin içeriğini değiştirmeye veya yok etmeye odaklanmıştır.
Altyapı Saldırıları	Siber terör saldırılar gerçek donanımı, işletim sistemini veya bilgisayar ortamındaki programlamayı hedef alarak onu bozmaya ya da yok etmeye yöneliktir.
Teknolojik Kolaylaştırma	Siber iletişimi terör saldırıları için planlar göndermek, saldırıya teşvik etmek veya geleneksel terör saldırılarını veya siber terörizmi kolaylaştırmak için kullanmaktır.
Para Toplama ve Tanıtım	İnterneti şiddetli siyasi bir eylem için para toplamak, şiddeti destekleyen bir örgüte destek sağlamak veya şiddet içeren bir ideolojiye yöneltmek için kullanmaktır.

Kaynak: Ballard, J. D., Hornik, J. G. and McKenzie, D. (2002), "Technological Facilitation of Terrorism: Definitional, Legal, and Policy Issues", *American Behavioral Scientist*, Vol: 45(6), Available at: http://scholarworks.gvsu.edu/cgi/viewcontent.cgi?article=1007&context=scjpeerpubs (Accessed at: 01/04/2015), p. 1009

Bu tip saldırılar genellikle Truva atları, virüsler veya solucanlar aracılığıyla yapılmakta ve bu tip saldırılarla bilgi sistemlerini çökertebilir ve işletim sistemlerinin geçici olarak kullanılmasını engelleyebilir. (Charvat, 2009: 84). Bhagyavati (2008: 190), Truva atlarını güvenli bir uygulama gibi görünen ama kendini gizleyen kötü niyetli bir program olarak tanımlamakta ve bu tür programların kendilerini çoğaltma yetenekleri olmadığını fakat bilgisayar programlarına kendilerini kopyalayan virüsler kadar zararlı olduklarını belirtmektedir. Başka bir ifade ile, bu tür saldırılarda amaç bilgisayar sistemlerine zarar vermek ve önemli bilgilere ulaşarak onları değiştirmektir. Diğer saldırı tip olan virüsler ise kullanıcıların bilgisi olmadan bir e-mail programına veya diğer indirilebilir dosyalara eklenebilir ve bu şekilde virüs kendini kopyalayarak diğer bilgisayarlara da yayılabilir (Mishra ve Mishra, 2008: 224). En bilinir ve zararlı virüslerden bir tanesi I LOVE YOU virüsüdür ve 2000 yılı içerisinde 8.7 milyar ABD Doları zarara neden olmuştur (Dünya'nın En Etkili Bilgisayar Virüsleri).

Altyapı saldırıları olarak sınıflandırılan ikinci tür saldırılar ise bilişim saldırılarına göre daha kapsamlı ve etkilidir. Jalil (2003: 4) siber teröristlerin hedefinin genellikle bir ulusun kritik altyapıları olduğunu ve amaçlarının da fiziksel ve psikolojik etkiler yaratmak olduğunu ifade etmektedir. 2007 Estonya saldırıları bu anlamda kritik altyapıların hedef alınması ve hükümet kontrolündeki sistemlere saldırılması dolayısıyla bu saldırı tipine örnek olarak verilebilir. Ayrıca Hardy ve Williams (2014: 1) bu tip saldırıların ekonomik kaos yaratmak, toplu ölümlere yol açmak veya çevreye zarar vermek için yapıldığını vurgulamaktadır. Hava trafik kontrol sistemleri, nükleer enerji santralleri, SCADA sistemleri, hastaneler ve bunlar gibi diğer kritik öneme sahip altyapılar her zaman siber teröristlerin ana hedefleri arasında olduğunu vurgulamakta ve toplum üzerinde geleneksel terörizmden daha fazla etki bırakmak istediklerini belirtmektedirler. 31 Mart 2015 tarihinde ve ayrıca daha sonra da Türkiye'nin enerji santrallerine yönelik siber saldırılar olmuş, İstanbul, Ankara ve İzmir gibi metropol şehirler ve diğer şehirler bu saldırılardan etkilenmiş ve uzun bir müddet elektrik bu şehirlere verilememiştir. (Elektrik Kesintisi: Türkiye Bir Gün Elektrik Alamadı; Taner Yıldız: Siber Saldırı mıdır? Söyleyemem!; 79 İlde Elektrik Kesintisinin Nedeni Siber Saldırı mı?; Türkiye'de Büyük Çapta Elektrik Kesintisi: Siber Saldırı İhtimali Araştırılıyor) Bu siber saldırı ve saldırı türünden de anlaşılacağı üzere siber saldırılarının zamanını, yerini ve toplum üzerindeki etkisini tahmin etmek kolay değildir. Hem Estonya hem de Türkiye'ye yapılan saldırılar siber saldırıların ve siber terörizmin uluslararası toplum için etkisini ve bu konuda önlemlerin alınması gerektiğini gözler önüne sermektedir.

Ballard ve diğerleri (2002: 1010) siber terörizmin saldırı sınıflandırmasında üçüncü sırasında yer alan teknolojik kolaylaştırmayı, siber teröristler tarafından terörizmi veya siber terörizmi körüklemek amacıyla kullanılabileceğini iddia etmektedirler. Diğer bir değişle, teknolojik imkanlar aracılığıyla teröristler kendi örgütlerini şekillendirebilir ve birbirleri arasında daha rahat iletişim sağlayabilirler. Birleşmiş Milletler Uyuşturucu ve Suçla Mücadele Ofisi (2012: 24) internetin teröristler tarafından etkili bir şekilde kullanıldığını ve özellikle de basit e-mail hesaplarının elektronik ya da sanal ölü bırakma haberleri için kullanılabileceğini belirtmekte ve gönderilmemiş halde ya da diğer bir değişle taslak olarak bırakılan e-maillerin elektronik iz bırakma ihtimalinin çok az olduğu ve bu mesaja dünyanın bir diğer ucunda ki teröristin erişilebileceği için teröristler tarafından daha yoğun olarak tercih edildiği belirtilmektedir. Buradan da anlaşılacağı gibi teröristler mesajlarını şifreleyerek özgürce ve korkmadan iletişim kurmakta ve yeni operasyonlar için planlarını paylaşabilmektedirler. Lecse bu durumu terör

uzmanları için endişe verici olarak yorumlamaktadır (Ballard, Hornik and McKenzie, 2002: 1010).

Ballard ve diğerlerinin sınıflandırmasında bulunan para toplama ve tanıtımdan amaç Birleşmiş Milletler Uyuşturucu ve Suçla Mücadele Ofisi (2012: 7) tarafından dört ayrı başlık altında sınıflandırılmaktadır. Bunlardan birincisi doğrudan taleptir. Terör örgütleri destekçilerinden bağış istemek için sohbet grupları, web siteleri ve benzeri internet kaynakları kullanılır. İkinci kategoride ise e-ticaret bulunmaktadır. Bu, e-ticaret siteleri üzerinden terör örgütleri destekçilerine kitap, müzik ve buna benzer diğer öğelerin satılmasını içermektedir. Üçüncü kategoride ise, internet üzerinden ödeme araçlarının kullanılmasıdır. Yani teröristler kimlik ve kredi kartı hırsızlığı ve açık artırma dolandırıcılığı ile gelir elde etmeye çalışır. Birleşik Krallık v. Younis Tsouli davası terörizmin finansmanı ile alakalıdır ve Tsouli 180 farklı web sitesi aracılığıyla El-Kaide propagandası yapmak, kredi kartı bilgilerini çalmak ve terör örgütüne 1.6 milyon İngiliz Sterlini kaynak sağlamaktan dolayı yargılanmıştır (Birleşmiş Milletler Uyuşturucu ve Suçla Mücadele Ofisi, 2012: 7).

Son kategori de ise hayır kurumları aracılığıyla para toplama ve tanıtım yapma vardır. Benevolence International Foundation, Global Relief Foundation, ve the Holy Land Foundation for Relief and Development gibi yardım kuruluşları, terör örgütlerine maddi destek sağlamak ve tanıtımını yapmak amacıyla kurulan hayır kurumlarına verilebilecek en güzel örneklerdir. (Birleşmiş Milletler Uyuşturucu ve Suçla Mücadele Ofisi, 2012: 7).

Bugün terör örgütleri çok dilli web sitelerine sahiptir ve bunlar üzerinden kendi ideolojilerini yaymak ve para toplamaktadırlar. Son dönemlerde DAEŞ de internetin gücünü kullanarak dünyanın dört bir yanından kendisine asker ve para toplamakta ve etkisini arttırmaya çalışmaktadır. Siviller, siber terörizmin varlığı ile geleneksel terörizm saldırılarından daha fazla etki altına alınmaya başlanmış. Bu durum sivillerin hem maddi hem de manevi olarak kayıplarına yol açmaya başlamıştır. Makalenin ilk bölümünde de belirtildiği üzere modernleşmenin getirmiş olduğu yenilikler her ne kadar insan hayatını kolaylaştırsa da modernleşme sonucu ortaya çıkan gelişmeler ve yeni riskler insanların yaşam şartlarını etkilemektedir. Beck'inde bahsettiği gibi modernleşme bir anlamda risk toplumu yaratmakta ve insanların kaygılarının artmasına neden olmaktadır.

Sonuç

Risk kavramı tarihsel süreç içerisinde farklı aşamalardan geçmiş ve zamana göre, farklı anlamlar yüklenmiştir. Beck (1992: 99) geçmişte risk kavramının ve buna bağlı olarak uygulanan sigortacılığın mükemmel olduğunu ve geçmişteki riskin bireyleri etkilediğini söylemektedir, fakat günümüz şartlarına bakıldığı zaman risk kavramı başta insanlar olmak üzere tüm toplumu ilgilendirmekte ve etkilemektedir. 18. veya 19. Yüzyıllarda kabul edilen risk kavramı ile günümüz risk kavramı arasındaki fark tabiri, fil ile fareyi kıyaslamak gibidir.

Modernleşme ile birlikte teknolojinin gelişmesi ve kullanımının artması yeni riskleri de beraberinde getirmiştir. Geleneksel terörizmden etkilenen ya da tarih boyunca sömürülen, uluslararası sistem dışına itilen toplumlar asimetrik savaş olguları bağlamında denge kurabilmek amacıyla teknolojinin getirmiş olduğu yeniliklerden ve etkilerden faydalanmış ve sistem içerisinde etkili olmaya çalışmışlardır. Risk toplumu ve refleksif modernleşme olgusu içerisindeki bumerang etkisi bir anlamda kendi üreticilerini vurmuş ve Soğuk Savaş sonrası dönemde büyük devletlerin ekonomik anlamda zarara uğramalarına neden olmuşlardır. Ayrıca son dönemlerde Hibrit Savaş ya da diğer adıyla Karma Savaş içerisinde de önemli bir yer edinen siber saldırılar günümüz modern dünyasına şekil vermekte ve devletlerarasında ya da terör örgütlerinin devletler üzerindeki etkisinde önemli roller oynamaktadır.

Siber terörizm makale içerisinde de bahsedildiği gibi geleneksel terörizmden daha etkili ve daha az maliyetlidir ve ilerleyen dönemlerde devletler üzerindeki etkisini hızlı bir şekilde arttırabilir. 2007 Estonya saldırısı devletlere ve uluslararası örgütlere siber güvenliğe önem vermeleri yönünde önemli bir ölçüt sağlamış ve siber savunmanın önemini gözler önüne sermiştir.

Devletlerin yapılacak çalışmalarda ve programlarda geleneksel terör saldırıları dışında siber terörizme yönelik çalışmalar yapması ve modernleşmenin getirmiş olduğu risklerin de göz önüne alınması gerektiği özellikle Birleşik Krallık vs. Younis Tsoulü davasında görülmüş ve son zamanlarda DAEŞ'in de bu alandaki varlığı bu önemi daha fazla arttırmıştır.

Teknolojik gelişmeler her ne kadar insanlar ve devletler için kolaylıklar tahsis etse de, siber uzayın sadece insanın refahı için kullanılmaması ve siber uzayın hem devletler hem de uluslararası örgütler bakımından artık güvenlik bağlamında öncelikli hale gelmesi ve tarihsel süreç içerisinde yaşanan siber saldırılar, Beck'in de bahsetmiş olduğu risk toplumu tezini

güçlendirmekte ve bu tür gelişmelerin ya da risklerin varlığını sürdüreceği ve toplumun bu baskı altında yaşaması ihtimallerini de arttırmaktadır.

Referanslar

Abbott, P., Wallace, C. & Beck, M. (2006). Chernobyl: Living with Risk and Uncertainty,. *Health, Risk& Society, Vol. 8 (2),* 105-121. https://www.abdn.ac.uk/socsci/documents/AWB2006.pdf (15/12/2016)

Bhagyavati, B. (2008). Social Engineering In Janczewski, L. J. and Colarik, A. M. (Eds.), *Cyber Warfare and Cyber Terrorism*, London: Information Science Reference

Ballard, J. D., Hornik, J. G. & McKenzie, D. (2002). Technological Facilitation of Terrorism: Definitional, Legal, and Policy Issues. *American Behavioral Scientist, Vol: 45(6),* 989-1016. http://scholarworks.gvsu.edu/cgi/viewcontent.cgi?article=1007&context=scjpeerpubs (Accessed at: 01/01/2017)

Beck, U. (1992). *Risk Society: Towards a New Modernity*, London: SAGE Publications

Beck, U. (1998). Politics of Risk Society In Franklin, J. (Ed.), *The Politics of Risk Society*, Cambridge: Polity Press

Beck, U. (2009). *World at Risk*. Cambridge: Polity Press

Beck, U., Bonss, W. And Lau, C. (2003), The Theory of Reflexive Modernization: Problematic, Hypotheses and Research Programme, *Theory, Culture&Society, Vol. 20 (1),* 1-34. Doi:10.1177/0263276403020002001

Charvat, J. (2009). Cyber Terrorism: A New Dimension in Battlespace. In Czosseck C. and Geers, K. (Eds.), *The Virtual Battlefield Perspectives on Cyber Warfare*, Amsterdam: IOS Press

Colarik, A. (2006). *Cyber Terrorism Political and Economic Implications*. London: Idea Group Publishing

Çuhacı, A. (2007. Ulrich Beck'in Risk Toplumu Kuramı. *Sosyoloji Dergisi 3. Dizi 14. Sayı,* 129-157. http://tjs.istanbul.edu.tr/wp-content/uploads/2015/12/13165-29620-1-SM.pdf (05/01/2017)

Denning, D. E. (2003), *Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism, H. Comm. on the Armed Services,* 1-5. https://pdfs.semanticscholar.org/7fdd/ae586b6d2167919abba17eb90e5219b7835b.pdf (Accessed at: 07/01/2017)

Fidler, D. P. (2014). Overview of International Legal Issues and Cyber Terrorism. *International Law Association*

Hardy, K. and Williams, G. (2014). What is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions of Terrorism. In Chen, T. M., Jarvis, L. and Macdonald, S. (Eds.), *Cyberterrorism: Understanding Assessment, and Response.* London: Springer

Hawks, B. B. (2011), *Cyber Terror: The Borderless Danger*, http://www.inter-disciplinary.net/wp-content/uploads/2011/05/banuhawksepaper.pdf (Accessed at: 11/01/2017)

Healey, J. and Bochoven, L.V. (2012). NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow. *Atlantic Council Issue*, February.

Jalil, S. A. (2003). Countering Cyber Terrorism Effectively: Are We Ready To Rumble?, *SANS Institute*, 1-17. http://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154 (Accessed at: 01/01/2017)

Jarvis, L., Nouri, L. and Whiting, A. (2014). Understanding, Locating and Constructing Cyberterrorism. In Chen, T. M., Jarvis, L. & Macdonald, S. (Eds.), *Cyberterrorism: Understanding, Assessment, and Response*. London: Springer

Lash, S. (2003). Reflexivity as Non-Linearity.*Theory, Culture&Society, Vol. 20 (2)*, 49-57

Lehti, M., Jutila, M., and Jokisipila, M. (2009). Never Ending Second World War: Public Performances of National Dignity and Drama of the Bronze Soldier. *Journal of Baltic Studies*, Vol. 39(4). http://blogs.helsinki.fi/majutila/files/2009/07/nesww.pdf (Erişim Tarihi: 08/01/2017)

Lewis, J. A. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. *CSIS*, 1-12. http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (Accessed at: 11/01/2017)

Mishra, A. and Mishra, D. (2008). Cyber Stalking: A Challenge for Web Security. In Janczewski, L. J. and Colarik, A. M. (Eds.), *Cyber Warfare and Cyber Terrorism*, London: Information Science Reference

Mythen, G. (2004). *Ulrich Beck: A Critical Introduction to the Risk Society.* London: Pluto Press

NATO (1991), *The Alliance's New Strategic Concept*, 7 November, http://www.nato.int/cps/en/natolive/official_texts_23847.htm (Accessed at: 10/01/2017)

NATO (1999), *Statement by the North Atlantic Council on Kosovo*, 30 January, Available at: http://www.nato.int/docu/pr/1999/p99-012e.htm (Erişim Tarihi at: 25/01/2017)

Nazario, J. (2009). Politically Motivated Denial of Service Attacks. Czosseck, C. and Geers, K. (eds.) (2009), *The Virtual Battlefield: Perspectives on Cyber Warfare*, CCDOE Publications, Estonia: IOS Press.

Rasmussen, M. V. (2001). Reflexive Security: NATO and International Risk Society. *Millennium: Journal of International Studies, Vol. 30 (2)*, 285-309

Rasmussen, M. V. (2006). *The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century.* Cambridge: Cambridge University Press

Sofaer, A. and Goodmani S. (2000). *A Proposal for an International Convention on Cyber Crime and Terrorism*, 1-45. http://cisac.fsi.stanford.edu/sites/default/files/sofaergoodman.pdf (Accessed: 12/01/2017)

Sorensen, M. P. and Christiansen, A. (2013). *Ulrich Beck: An Introduction to the Theory of Second Modernity and the Risk Society*. London: Routledge

Taliharm, A. M. (2010). Cyberterrorism: in Theory or in Practice?. *Defence Against Terrorism Review, Vol. 3 (2)*, 59-74.

TASAM (2004). *Siber Terörizm*. http://www.tasam.org/files/pdf/raporlar/siber_teror__639c0ad9-f639-4c64-9220-3bbc07f81993.pdf (13/01/2017)

The Council of Europe (2008). *Cyber terrorism: The Use of The Internet for Terrorist Purposes.* Strasbourg: Council of Europe Publishing

The United Nations Office on Drug and Crime (2012). *The Use of the Internet for Terrorist Purposes.* United Nations: Vienna. http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (Accessed at: 05/01/2017)

Traynor, I. (2007). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (Erişim Tarihi: 08/01/2017)

Weimann, G. (2004). Cyberterrorism: How Real Is the Threat?. *United States Institute of Peace Special Report No.119*, http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=14122&lng=en (10/01/2017)

Williams, M. J. (2008). (In) Security Studies, Reflexive Modernization and the Risk Society. *Cooperation and Conflict: Journal of the Nordic International Studies Association, Vol. 43 (1)*, 57-79

Zanini, M. and Edwards, S. J. A. (2001). The Networking of Terror in the Information Age. In Arquilla, J. and Ronfeldt, D. (Ed.), *Networks and Netwars: The Future of Terror, Crime and Militancy*. Santa Monica: RAND

Zinn, J. O. (2008). *Social Theories of Risk and Uncertainty: An Introduction*. Oxford: Blackwell Publishing

Internet Kaynakları

Associated Press (2007). *Removal of Soviet War Memorial Sparks Deadly Riots in Estonia*. http://www.foxnews.com/story/2007/04/27/removal-soviet-war-memorial-sparks-deadly-riots-in-estonia/ (Erişim Tarihi: 08/01/2017)

Dünya'nın En Etkili Bilgisayar Virüsleri. http://www.milliyet.com.tr/fotogaleri/44071-yasam-dunyanin-en-tehlikeli-bilgisayar-virusleri/6 (02/01/2017)

Ehala, M. (2009). *The Bronze Soldier: Identity Threat and Maintenance in Estonia*. http://lepo.it.da.ut.ee/~ehalam/pdf/Identity%20threat.pdf (Erişim Tarihi: 08/01/2017)

Elektrik Kesintisi: Türkiye Bir Gün Elektrik Alamadı. http://www.bbc.com/turkce/haberler/2015/03/150331_elektrik_rengin (02/01/2017)

Malksoo, M. (2007). *The Fallen 'Bronze Soldier' …(A Response to: Is This the Order we wanted?)*, http://www.icds.ee/index.php?id=73&tx_ttnews%5Btt_news%5D=164&tx_ttnews%5BbackPid%5D=99&cHash=bcff323714 (Erişim Tarihi: 08/01/2017)

Taner Yıldız: Siber Saldırı mıdır? Söyleyemem!. http://www.radikal.com.tr/turkiye/taner_yildiz_siber_saldiri_midir_soyleyemem-1325196 (02/01/2017)

Türkiye'de Büyük Çapta Elektrik Kesintisi: Siber Saldırı İhtimali Araştırılıyor. http://tr.sputniknews.com/turkiye/20150331/1014730458.html (02/01/2017)

79 İlde Elektrik Kesintisinin Nedeni Siber Saldırı mı?", http://www.aktifhaber.com/79-ilde-elektrik-kesintisinin-nedeni-siber-saldiri-mi-1147527h.htm (02/01/2017).

ISSN: 2587-1218

POLİTİK İDEALİZM VE SİBER UZAY İLE DÖNÜŞEN ULUSLARARASI İLİŞKİLER

Fatma ÇAKIR*

Özet

Uluslararası ilişkiler, yaklaşık bir asırlık geçmişi olan ve ana sorunsalı savaşların önlenmesi olan bir disiplindir. Ancak, bugün bu genel tanımlamanın yanında geleneksel uluslararası ilişkiler diye bir ifade de kullanılmaktadır. Geleneksellikten bahsetmek aynı zamanda bir yenilikten ve değişimden söz etmektir. Bu noktada uluslararası ilişkiler disiplinini etkileyen önemli bir gelişme küreselleşme ve beraberinde gelen siber uzayda yaşanmıştır. Siber uzay ile birlikte yaşanan hızlı ve yoğun etkileşimler uluslararası alandaki temel parametreleri etkilemiş, bu bağlamda disiplinin ilk yaklaşımlarından olan ve genel çerçevesini çizen İdealizmin varsayımlarını da zorlaştırmıştır.

Anahtar Kelimeler: Siber Uzay, İdealizm, İşbirliği, Ticaret, Uluslararası İlişkiler.

POLITICAL IDEALISM AND TRANSFORMATION OF INTERNATIONAL RELATIONS WITH CYBERSPACE

Abstract

International relations is a discipline that is about a century old and main problematic is the prevention of wars. However, today, in addition to this general description, there is also an expression of traditional international relations. Talking about tradition is talking about innovation and change at the same time. At this point, an important development affecting the discipline of international relations has been experienced in globalization and the cyber space that comes along. Rapid and intense interactions with cyber space have influenced the basic parameters in the international arena and have made it more difficult to assume the idealistic assumptions that is one of the initial approaches and draws the general framework of the discipline.

Keywords: Cyberspace, Idealism, Cooperation, Trade, International Relations.

Giriş

Siber uzay, günlük hayatımızın her alanında, temas ettiğimiz, bir nevi parçası haline geldiğimiz bir dünyayı ifade eder. Yirminci yüzyılın ortalarında kavramsal olarak literatüre girmiş olan bu kavramın işaret ettiği dünya, sosyal, kültürel, ekonomik, siyasal ve güvenlik gibi pek çok noktada içinde yaşadığımız dünyada etkilerini göstermektedir. Yakın zamana kadar uluslararası ilişkilerde yüksek politika konuları arasında yer almayan bu konu, bugünlerde yüksek politika konularının hepsini ilgilendiren belki de en yüksek politika

* Araş. Gör. Selçuk Üniversitesi Uluslararası İlişkiler Bölümü. Ulaşmak İçin: fatmacakir021@gmail.com

konusu olmaya adaydır. Zira askeri, güvenlik ve ekonomi gibi devletlerin önem verdiği alanların ve bunlarla ilgili kurumların büyük ölçüde internetleştiği dolayısı ile siberleştiği düşünüldüğünde bu çıkarımın doğruluğu görülecektir.

Bu makalede, siber uzayın uluslararası ilişkilerde yarattığı dönüşümler ve bu dönüşen uluslararası ilişkilerin İdealizmin temel argümanları ile ne kadar örtüştüğü analiz edilecektir.

Siber Uzay

Siber uzay, diğer bir deyişle siber ortam ekranımızın ardındaki dünyayı işaret eden bir kavramdır. (Klimburg ve Mirtl, 2012, s.9) 20. yüzyılın ikinci yarısından itibaren internet teknolojisinin gelişmesi ve internet kullanımının artması ile bu alan daha da genişlemiştir. Küresel ölçekte çalışmalar yürüten dijital pazarlama ajansı We Are Social tarafından hazırlanan *"Digital in 2016"* raporunda 7.395 milyar dünya nüfusunun içinde 3.419 milyar insanın internet kullandığı ifade edilmiştir. (We Are Social, 2016) Buradan hareketle, dünya nüfusunun yaklaşık yarısının internet üzerinden etkileşim halinde olduğu sonucuna varılabilir.

Siber Uzay kavramı ilk kez Kanadalı bilim kurgu yazarı William Gibson tarafından kullanılmıştır. 1984 yılında yayınladığı *Neuromancer* adlı kitabında siber uzay kavramını "kabul görmüş halüsinasyon" olarak tanımlamıştır. (Klimburg ve Mirtl, 2012, ss.9-10) Kavram üzerine günümüzde pek çok tanımlama mevcuttur. Bunlardan biri, 11 Eylül saldırılarından sonra 2003 tarihinde yayınlanan Amerika'nın "Ulusal Siber Savunma Stratejisi"-dir. Belgede siber uzay ülkenin kritik altyapılarını etkileyen sinir sistemi olarak tanımlanmış, ülkenin ekonomisi ve ulusal güvenliği için sağlıklı çalışan bir siber uzaya dikkat çekilmiştir. (The White House, Washington, 2003) Öte yandan Türkiye'nin 2016-2019 Ulusal Siber Güvenlik Stratejisi'nde siber uzay kavramı, tüm dünyaya ve uzaya yayılmış bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam olarak bahsedilmiştir. (T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2016-2019) Bu örneklerden hareketle siber uzayın standart bir tanımı olmadığını görmekle birlikte, en kapsamlı tanımına David Clark'ın yaptığı katmanlı modelde ulaşıyoruz. Dört katmandan oluşan bu tanımlamada, ilk katmanı fiziksel temeller, altyapılar oluşturmaktadır. Bu bağlamda, bütün donanım aygıtları bu katmanı oluşturur. İkinci katmanı ise, fiziksel altyapıyı etkinleştiren, destekleyen mantıksal yapılar oluşturmaktadır ki bu kısım da yazılımları ifade eder. Üçüncü katman, içerik katmanıdır, bu da siber uzayda depolanan, iletilen, dönüştürülen bilgiye tekabül eder. Son olarak, dördüncü katman ise, aktör, kullanıcı

katmanıdır ve verileri, bilgileri kullanan insana karşılık gelir. (Choucri, 2012, s.8) Bu tanımlama ile birlikte, siber uzay ve siber uzaya dair diğer kavramsallaştırmalar da daha anlaşılır olmaktadır.

Günlük hayatta kullandığımız kavramların başına siber ön ekinin eklenmesi ile boyut kazanan bu yeni dünyanın aktörlerine gelince, sıradan kullanıcıların yanında, ülkelerin milli çıkarları için çeşitli motivasyonlarla oluşturulmuş "hükümet destekli yapılar", büyük menfaatler gözeten "organize suç yapıları", belli bir düşüncenin ve görüşün propagandasını yapmak için eylemde bulunan "hacktivistler", intikam almak gibi amaçları olan "iç tehditler", sistem açıklarını, zafiyetlerini fark ederek bundan menfaat sağlamaya çalışan "fırsatçılar" ve "dahili hatalı kullanıcılar" şeklinde sıralanabilir. (www.siberoloji.com)

Siber uzay konusu günümüzde en çok güvenlik bağlamında ele alınmaktadır. Bunun nedeni ise, içinde bunduğumuz dönemde, hayatımızın her alanına internetin girmiş olmasından kaynaklanır. Hayatımızı her yönden kapsayan bu alanının güvensizliği ise, insanları, grupları, şirketleri ve devletleri dehşete düşürmektedir. Peki, siber güvenlikten kastedilen nedir? Bu konuda kabul edilmiş standart bir tanım olmamakla birlikte, devletler ve uluslararası örgütler tarafından yapılan tanımların temel ortak noktası, 21. yüzyıl küresel ekonomisine nüfuz eden kritik altyapıların ve hükümet sırlarının korunması ve ulusal savunmanın etkinleştirilmesi olarak ortaya çıkmaktadır. (Klimburg, 2012, s.13) Ancak, devlet güvenliğini ve ulusal güvenliği merkeze alan bu tanımlamanın eksik kaldığını belirtmek gerekir. Zira, internetleşen sadece devletler değildir. Bireyler, çok uluslu şirketler ve sivil toplum kuruluşları gibi devlet dışı aktörlerin de büyük ölçüde internetleştiğini düşündüğümüzde yukarıdaki tanımın daha da genişletilmesi gereği ortaya çıkar. Bu bağlamda internetleşen bütün paydaşlar için olmazsa olmaz kabul edilen siber güvenlik ilkelerinden bahsetmek gerekir ki bunlar; "gizlilik", "bütünlük" ve erişilebilirliktir. Türkiye 2016-2019 Ulusal Siber Güvenlik Stratejisi'nde yer alan siber güvenlik tanımı da siber ortamda işlenen veri ve bilgilerin bu üç etmenle güvence altına alınması durumunu ifade eder. Yine aynı belgede siber güvenliğin yalnızca devlet güvenliğini değil, sistemdeki tüm paydaşların güvenliğini kapsadığı da belirtilmiştir. (T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2016-2019)

Siber Uzay ve Uluslararası İlişkiler

Siber uzay, uluslararası ilişkilere etkisini "etkileşim" üzerinden gösterir. Başka bir deyişle, siber uzay ile beraber dünya üzerinde farklı şekillerde ve yoğunlukta etkileşimler yaşanmakta,

bu da uluslararası ilişkileri etkilemektedir. Bu bağlamda siber uzay, egemenlik kavramını, uluslararası hiyerarşik güç ilişkilerini etkileyerek çağdaş uluslararası ilişkiler teorilerinin varsayımlarını zorlaştırmıştır denilebilir. Siber ortamın sağladığı ekonomik, siyasal ve sosyal imkânlar dünya genelinde yayıldıkça, güç ve siyaset ilişkileri değişime uğramaktadır. (Choucri, 2013, ss.3-4)

Yukarıdaki açıklamadan hareketle, siber uzay ile uluslararası ilişkilerin ilk dönüşümünün *aktörler düzeyinde* olduğunu söyleyebiliriz. Küresel erişim ve internetin anonim olması gibi siber uzayın sağladığı imkânlar, uluslararası alanda *yeni aktörlerin* ortaya çıkmasında ve var olan aktörlerin güçlenmesinde etkili olmuştur. Sanal ortamda bireylerin, grupların ve devlet dışı diğer aktörlerin etkinlikleri artmakta, bu durum uluslararası ilişkilerdeki asimetrik ilişkileri etkilemektedir. Devlet merkezli klasik uluslararası ilişkiler anlayışını dönüştüren bu yeni dünyada hacker denilen bireysel aktörlerin başlarda merak, itibar, görünürlük ve meydan okuma heyecanı ile bilgi teknolojisi hizmetlerini hacklemesi zamanla internet güvenlik zafiyetinin farkına varması ile organize olması uluslararası sisteme etki etmelerini sağlamıştır. İkinci olarak, ekonomik amaçlı çokuluslu şirketlerin siber uzaydan faydalanarak kâr elde etmesi, ekonomik açıdan ulus-devletlerle yarışır hale gelmesi dünya siyasetini etkileyen kararlar almasını sağlamıştır. Öte yandan, siyasi amaçlı terör örgütleri de siber uzay ile birlikte boyut değiştirmiş, bölgesel sınırlı düzeyde etki yaratan terör gruplarından küresel ölçekte eylem ve faaliyetlerde bulunan terör örgütlerine dönüşüm yaşanmıştır. Tüm bunların yanında küresel ölçekte faaliyet yürüten sivil toplum kuruluşları, siber dünyanın düzenlenmesine dair kurulan uluslararası kurumlar da çok aktörlülüğü beslemektedir. (Czosseck, 2003, ss.3-4) Buradan hareketle, uluslararası sistemdeki çok aktörlü yapının ortaya çıkmasının *devletlerin zayıflamasına* yol açtığı ifade edilebilir. Ancak siber uzay devletleri yalnızca dışarıda değil içeride de olumsuz yönde etkilemektedir. Siber imkânlar bir yandan devletlere egemenlik alanındaki vatandaşlarını ve gelişmeleri kontrol imkânı sağlarken, diğer yandan egemenliğini ve sınırlarını sarsmaktadır. Zira siber ortam vatandaşlara mevcut düzene ve otoriteye karşı meydan okuma imkânı sunar. İnternetin imkânları ile daha da özgürleşen insanlar siber imkânlar dâhilinde çok daha kısa sürede ve çok katılım sağlayarak örgütlenebilir ve devlet otoritesi için tehdit oluşturabilirler. Tüm bunlardan hareketle, siber uzay, devletleri hem uluslararası ilişkilerde hem de içeride sınırlarının muğlaklaşması, merkeziyetçiliğinin ve egemenliğinin sarsılması bakımından zayıflatmıştır denilebilir.

Siber uzayın geleneksel uluslararası ilişkilere bir diğer etkisi de geleneksel güç dengelerinin bozulduğu uluslararası ilişkilerde *yeni tehditlerin* ortaya çıkmasıdır. Birey, grup ya da devletler için hayati olan bilgilerin siber ortamda kötü niyetli kullanıcılar tarafından ele geçirilebilmesi ciddi tehditler yaratabilmektedir. Bu bağlamda siber tehdit ve silahlar kullanılarak ülkelerin kritik altyapılarına saldırılar yapılabilmekte, bu kritik altyapıların bilgileri ve kontrolü ele geçirilebilmekte dahası bir daha çalışamaz hale getirilebilmektedir. Bu şekilde, yeni tehditlerin ortaya çıkması ile birlikte, bireysel veya ulusal güvenliği sağlamak daha da zorlaşmış, güvenlik kavramı yeni bir boyut daha kazanarak *siber güvenlik* ortaya çıkmıştır. Siber güvenlik çerçevesinde, bireylerin, ulusların veya grupların temel amaçları ise, gizlilik, bütünlük, erişilebilirlik, inkâr edilemezlik ve kimlik doğrulama gibi unsurları sağlamak gerekmektedir. (Ünver, Canbay ve Mirzaoğlu, 2009, s.22)

Uluslararası güç ve güvenlik anlayışındaki gelişmelere paralel olarak siber uzayın bir diğer etkisi de savaş olgusu üzerinden olmuştur. Siber silahlar ve saldırılar ile birlikte savaş kavramı yeni bir boyut kazanmış ve *siber savaş* kavramı ortaya çıkmıştır. Siber savaşın ortaya çıkması ile, karşı tarafta mali, psikolojik yenilgi yaratmak için gizli, görünmez olarak yapılan siber saldırılar veya bu tür saldırılara karşı yapılacak müdafaa ve karşı saldırılar için siber ordular kurulmuştur. Bu noktada, Çin Halk Kurtuluş Ordusu'nun ağlarını dış siber saldırılardan korumak için eğitilmiş 30 siber savaşçıdan oluşan "Mavi Ordu"su bu duruma örnek gösterilebilir. (Milliyet, 27.05. 2011)

Diğer yandan, siber uzay ile birlikte bu alanı düzenlemek için *uluslararası yeni kuruluşların* ortaya çıktığı görülmektedir. Bunlardan bazıları ICANN (Internet Corporation for Assigned Names and Numbers and Internet Engineering Task Force) gibi siber etkileşimleri yönetmek için bazıları ise CERTS (Consortium for Electric Reliability Technology Solutions) gibi siber güvenliği desteklemek için kurulmuştur. Ayrıca bu yeni kuruluşların siber uzayı yönetme konusunda meşruiyetini sorgulamak için ITU (International Telecommunications Union) gibi geleneksel kurumlar da mevcuttur. Buradan hareketle, belirsiz yetkilerle ve çakışan görev tanımlamaları ile siber alan hakkında birçok karar vericinin ortaya çıktığını görmekteyiz ve bu durum sorumluluklar, meşruiyetler gibi birçok noktada yeni belirsizliklere neden olmaktadır. Yine, bu yeni kuruluşlardan hareketle çıkarılacak bir başka sonuç da siber çatışmaların büyümesini engellemek ve küresel siber normları belirlemek için siber işbirliğine ihtiyaç duyulduğudur. (Choucri, 2013, s.9)

İdealizm ve Siber Uzay İle Dönüşen Uluslararası İlişkiler

İdealizm, köken olarak geleneksel liberal felsefi teoriye dayanmaktadır. Birinci Dünya Savaşı'ndan sonra ciddi bir yükseliş gösteren teori, savaşın yol açtığı felaketlerin tekrar yaşanmaması, barışçıl bir düzenin kurulması için tezler öne sürmüştür. Kendilerine "idealist", "ütopyacı" ismini ise, disiplinin birinci büyük tartışmasında karşısında yer alan realistler vermiştir. (Arı, 2011, ss.102-103)

Bu dönem idealizminin temel argümanlarına bakıldığında ilk olarak, "*devlet"*i, uluslararası sistemin temel aktörü olarak kabul ettiklerini görmekteyiz. (Ateş, 2003, s.61) Uluslararası sistemi ve ilişkileri açıklarken, devleti temel aktör olarak baz almakta ve bunun üzerinden tezler ileri sürmektedir. Ancak günümüz uluslararası ilişkilerde devlet dışı diğer aktörlerin de en az devletler kadar etkili olduklarını ve kademeli ve sistematik bir şekilde artış gösterdiklerini göz önünde bulundurduğumuzda teorinin bugünü açıklamada eksik kaldığı anlaşılabilir. Siber imkânlarla birlikte, sınırları aşan ve tüm dünyaya yayılan ekonomik amaçlı kuruluşlar, insan hayatını iyileştirmek için çabalayan gönüllü STK'lar, siyasi amaçları doğrultusunda küresel faaliyet gösteren terör örgütleri ve bu yeni aktörlerin küresel ölçekteki eylemlerinin etkinlikleri idealistlerin devlet temelli aktör anlayışına ters düşmektedir.

İkinci olarak idealizmin uluslararası sisteme bakış açısından bahsetmek gerekir. İdealistler uluslararası ilişkilerin *anarşik* bir yapısının olduğunu kabul etmekle birlikte bu anarşik durumun ve neden olacağı sorunların önlenebileceğini iddia ederler. Bu bağlamda *"uluslararası işbirliği"* idealistlerin temel argümanlarından birini oluşturur. Ekonomik, sosyal, siyasal, hukuksal olarak her alanda yapılacak bir işbirliği, uluslararası ilişkilerin temel sorunu olan savaşı ve çatışmayı önleyecektir. (Gözen, 2016, s.90) Bu noktada, insan doğasından hareketle, devletlerin iyiye, barışa ve işbirliğine yatkın olduğunu savunan idealistler, savaşların önlenebilmesi için "*uluslararası örgütlenme"* gibi işbirliği imkânlarına dikkat çekmektedir. İdealistlerin bu yaklaşımının günümüz uluslararası ilişkiler ile uyumuna bakacak olursak, öncelikle anarşik bir uluslararası sistem kabulünün bugünü yansıttığı söylenebilir. Aktörler için üst bir otoritenin yokluğu, yaptırımı olan bağlayıcı kuralların olmaması anlamına gelen bu özellik, klasik uluslararası ilişkilerde olduğu gibi siber dünya ile dönüşen uluslararası ilişkilerde de kendini göstermekte hatta daha da keskin hissedilebilmektedir. Siber uzay ile yeni hareket ve güç alanlarının oluşması, yeni aktörlerin ortaya çıkması, siber imkânları kullanan bu çok çeşitli aktörlerin sistemi etkileyebilme şansının da artmış olması kontrolü neredeyse imkânsız anarşik bir uluslararası sistem profili

çizmektedir. Ancak bu artan anarşinin yanında, idealistlerin sınırlanabilir anarşi tanımlamasındaki işbirliği reçetesinin de günümüzde geçerli olduğunu belirtmek gerekir. Zira teknolojinin gelişmesi ile birlikte işbirliği imkânlarının geniş ölçüde arttığı günümüzde, aktörlerin ortak çıkarlarını elde etmek veya ortak tehditlerden kaçınmak için siyasi, ekonomik, kültürel, güvenlik v.b. her alanda işbirliğine, örgütlenmelere gittiği görülmektedir. Bu duruma siber tehditlere karşı 33 ülkenin taraf olduğu Avrupa Konseyi'nin hazırladığı 23 Kasım 2001 tarihinde imzalanan "Sanal Ortamda İşlenen Suçlar Sözleşmesi" örnek gösterilebilir. Bu sözleşme çerçevesinde devletler ortak siber tehdide karşı uluslararası etkin bir işbirliği rejimi kurmayı hedeflemiştir. (Council of Europe, 2001) Böylelikle siber tehditlerin yol açacağı olası sorunlar, çatışmalar idealistlerin sunduğu işbirliği yöntemi ile önlenmeye çalışılır.

Üçüncü olarak idealistler, savaşların önlenmesi için uluslararası sistemde aktörlerin sıkı sıkıya bağlı oldukları *"uluslararası hukuk"* düzeninin tesis edilmesi gerektiğini zira böyle bir hukukun savaş ve çatışma durumlarına karşı ön alıcı işlev gördüğünü belirtir. (Ateş, 2003, s.61) İdealistlerin bu önerisi bağlamında, günümüzde, belli oranda ilerleme sağlandığı söylenebilir. Nitekim uygulamada bir takım sorunlar yaşansa da günümüzde uluslararası düzeni sağlayan, devletleri bağlayan ihlali durumunda sorumluluklar yükleyen bir hukuk mevcuttur. (Denk, 2001, s.68) Ancak savaş, suç ve tehdit kavramlarının siberleştiği ortamda küresel ölçekte siber saldırılar ve siber suçlar artmakla birlikte bu suçların önemli bir kısmı yaptırımsız kalmaktadır. Zira, bu tür siber suçlara karşı evrensel bağlayıcı hukuk kuralları henüz oluşmamıştır. (Türkay, 2003, s.1207) Avrupa Konseyi'nin siber suçlar ile mücadele için imzaladığı sözleşme ise bölgesel anlamda uluslararası hukukun gelişimi için önemlidir.

Dördüncü olarak idealistlere göre, uluslararası ilişkilerde *"ahlâk"* önemli yer tutar. (Kodaman, 2013, s.133) Ahlâk kavramı burada devletler tarafından genel kabul görmüş, karşılıklı ilişkileri düzenleyen ilkeleri (örn; ahde vefa ilkesi) ifade eder. Geleneksel uluslararası hukuk kuralları da ahlâkı yansıtır ve tüm bu ilkeler sistemdeki aktörlerin faaliyetleri üzerinde sınırlayıcı etki görür. Ancak, uluslararası ilişkilerde anarşi vardır ve bu anarşik ortamda aktörler kendilerini ve eylemlerini sınırlandırmak istemezler. Özellikle siber uzay ile dönüşen uluslararası ilişkilerde anarşinin ve sistem içinde faaliyette bulunan aktörlerin sayısının artması ve dolayısı ile siber uzayın kontrolünün zor olması idealistlerin "ahlâk" ilkesinin uygulanılabilirliğini düşürmektedir.

Beşinci olarak idealizm, savaşların sebebini silahlanma yarışı olarak görmekte bu sebeple de *"silahsızlanma"*-yı sağlayacak uluslararası düzenlemelerin yapılmasını önermektedir. (Heywood, 2007, s.184) Ancak uluslararası sistemde rol alan aktörlerin çeşitlendiği, siber imkânların gizli siber saldırıları mümkün kıldığı düşünüldüğünde tüm kesimlerin onaylayacağı bir silahsızlanma düzenlemesinin zor olduğu görülmektedir. Birey, grup veya devletlerin kolayca sahip olabileceği siber silahların çeşidi de her geçen gün artmakta, bu silahlarla donanan siber ordular kurulmaktadır. (Bkz. U.S. Army Cyber Command)

Altıncı olarak idealizm açısından önemli bir nokta *"uluslararası ticaret"*-tir. Uluslararası ilişkilerde high/low politics ayrımı yapmayan idealistler, devletlerarasındaki ticaret hacminin artmasının *"karşılıklı bağımlılık"* yaratacağını bu durumun da çatışma riskini azaltacağını ifade ederler. (Link, 1986, s.536) İdealistlerin yaptığı bu çıkarımın göreceli olarak, bugün uygulamada geçerli olduğu görülmektedir. Nitekim teknolojik gelişmeler ve siber uzayın sağladığı imkânlar, uluslararası ticareti geliştirmektedir. Günümüzde e-ticaret üzerinden küresel ölçekte ticaret oranı artmakta, bireyler, şirketler, örgütler ve devletler bu ticaret hacminden büyük paylar elde etmektedirler. (Sezgin, 2013, s.2) Böylelikle uluslararası aktörler arasında karşılıklı bir bağımlılık oluşmakta, ortak çıkar paydaları çoğalmakta, sonuç itibariyle çatışma ihtimâlleri düşmektedir. Ancak bu değerlendirmenin yanında uluslararası ticaretin her zaman ortak çıkar doğurmadığından, bazen çıkar çatışmalarına neden olduğundan da bahsetmek gerekir. Bu noktada karşılıklı bağımlılıktan ziyade ekonomik çıkar doğrultusunda rekabet ön plana çıkmaktadır. Öte yandan, uluslararası ticaretin her zaman ortak çıkar oluşmadığını göstermesi açısından silah ticareti meselesine de bakmak gerekir. Silah ticareti ile yüksek gelirler elde eden aktörler için barışın tesisi ortak çıkar paydası değildir. Örneğin bugün Ortadoğu'da olası bir barışın yaşanması ve savaşın sona ermesi başta siviller olmak üzere bir kesimin çıkarına olacakken, silah satışı ile bu savaşlardan gelir elde edenler için istenmeyecek bir durumdur. Siber imkânlarla birlikte silah ticaretinin kapsam, hız ve yoğunluğunun arttığı düşünüldüğünde, bu durum, savaş ve güvensizlikten başka bir sonuç doğurmayacaktır.

Yedinci olarak idealistler, *"demokratik yönetim"*e vurgu yapmaktadırlar. Zira doğası itibari ile iyi olan insanları ve devletleri savaşa sürükleyen kötü yönetimlerdir. Bu sebeple insan doğasına en uygun yönetim demokrasidir ve demokratik ülkelerde savaş daha az görülür. (Ateş, 2003, s.61) Günümüz uluslararası ilişkilere bakıldığında ise, savaşların en çok da demokratik olmayan Afrika ve Orta Doğu gibi bölgelerde olduğu görülmekte, bu durum da

idealistlerin bu çıkarımlarının geçerliliğini göstermektedir. Zira diktatörler tarafından yönetilen ülkelerde bireylerin siber imkânlardan faydalanarak bilinçlenmesi ve internet üzerinden örgütlenebilmesi kötü yönetime karşı ayaklanmalarını sağlamakta bu durumda da sonuç iç savaşla bitmektedir. Ayrıca, siber uzayın sağladığı imkânlar açısından herkesi fırsat eşitliği ve imkânlar açısından eşit hale getirmesi, uluslararası ilişkilerin hiyerarşik düzeninin aksine demokratik bir yapı oluşturması "yönetişim"i artırmıştır denilebilir.

İdealizmin tezlerini bu şekilde açıkladıktan sonra, literatürde genellikle birbirinin yerine kullanıldığı liberalizmin tezlerine bakmak ve günümüzde geçerliliğini sorgulamak da faydalı olacaktır. Liberalizm idealistlerle ortak özellikler taşıdığı gibi idealistlerden ayrıldığı noktalar da mevcuttur. Buna örnek olarak, idealistlerin devleti temel aktör görmesine karşı, liberalizmin genel olarak *"sınırlı devlet"* den bahsetmesi ve *"bireyciliği"* savunması gösterilebilir. (Arı, 2011, s.104) Liberalizm, bireycilik anlayışı çerçevesinde *"insanların temel hak ve özgürlükleri"*-nin olduğunu ifade etmektedir. Devlet *"hukukun üstünlüğü"* ilkesine bağlı kalarak hareket etmeli ve bireyin hakları korunmalıdır. Liberallerin bu savunusu hakkında siber uzay ile birlikte, günümüzde eskiye nazaran gelişme kaydedildiği görülmektedir. Siber uzayın da etkisi ile, günümüzde Westphalian devlet anlayışı sarsılmış, devletler sınırlanmıştır. Yani siber imkânlar bir yandan ülkeyi ve vatandaşları kontrol için devlete imkan sağlarken diğer yandan aynı devlet aynı imkanları kullanan birey, grup veya başka devletler tarafından her an tehdide açık hale getirilmiştir. Dünya genelinde internet üzerinden etkileşimlerin artması ile, devletin katı somut sınırları ortadan kalkmış, bireyler "hak ve özgürlükleri"- ni talep için internet üzerinden kendisine karşı örgütlenebilmiştir.

Liberallerin özgürlükçü düşünceleri çerçevesinde idealistlerin de savunduğu bir diğer savları da *"serbest girişim"*dir. Ekonomide devlet müdahalesini istemeyen liberaller serbest ticaret ve serbest girişime vurgu yaparlar. (Burchill, 2015, ss.95-96) Serbest piyasa ekonomisinin hâkim olduğu günümüzde, genelde teknolojik imkânlar özelde ise internetin yaygın kullanımı ve işlevselliği insanların ve çok uluslu şirketlerin piyasa ekonomisine daha iyi entegre olabilmelerini sağlamaktadır. Bireysel özgürlüklerin daha da arttığı siber ortamda serbest girişim dâhilinde ekonomik faaliyetler daha hızlı ve yoğun gerçekleşmektedir. Sonuç itibari ile, milyar dolarlık sermayeleri ile şirketler, ulus-devletler ile yarışmakta ve dünyadaki gelişmeleri etkileyebilmektedir.

İkinci dünya savaşından sonraki soğuk savaş döneminde yaşanan bir takım gelişmeler idealist paradigmayı tekrar canlandırmıştır. Soğuk savaş koşulları, 1973 petrol krizi, detant süreci, Vietnam savaşı gibi gelişmeler realistlerin pek çok savını boşa çıkarmış, genel olarak "neo-idealizm" (Heywood, 2007, s.184) olarak bilinen neo-liberalizm ortaya çıkmıştır. İdealizmdeki pek çok noktayı benimsemekle birlikte neo-liberalizmin temel savlarından ilki *"çoklu meseleler"* ve *"çoklu kanallar"*- dır. Yani, devlet-devlet, devlet-STK, STK-Şirketler v.s kombinasyon şekilde çoklu kanalların olduğunu, bu kanallar üzerinden high/low politics ayrımı yapmadan güvenlik, güç, siyaset gibi meselelerin yanında ekonomik, sosyal, kültürel meselelerin de görüşüldüğü bir uluslararası sistemden bahsedilmektedir. (Koç, 2015, ss.94-95) Neo-liberallerin bu çoklu kanallar ilişkisi siber uzayla birlikte daha da görünür olmuştur. Nitekim siberle birlikte ciddi aktör çeşitliliği olmuş, güç ilişkileri değişmiş, devletler ve diğer aktörler sürekli birbiri ile etkileşim içinde olmuşlardır. Yine bu aktörlerden önemli bir kısmının ekonomik amaçlı şirketler olması, siber ortamla birlikte kültürel tek tipleşmeden yakınılması güç, güvenlik konularının yanında bu tür meselelerin de önemli olduğunu göstermiştir.

Diğer yandan neo-liberallere göre güç kavramı, sadece askeri güç anlamına gelmemektedir. Realistlerin askeri temelli güç anlayışına karşı neo-liberaller, özellikle soğuk savaş dönemi ve sonrası dönemde bu anlayışı değiştiren gelişmelere dikkat çekerler. Bu bağlamda, ekonomik güç, teknolojik güç gibi "*yeni güç alanları"*- nın ortaya çıktığını savunurlar. Günümüzde ise, neo-liberallerin bu anlayışını doğrulayan gelişmeler yaşanmış, siber uzay ve imkânları ile birlikte, uluslararası güç anlayışına bir de "siber güç" boyutu eklenmiştir.

Son olarak, neo-liberallere göre uluslararası sistemin niteliği (karakteri) *yönetişim*dir. (Koç, 2015, s.100) Yönetişim kavramının standart bir tanımı olmamakla birlikte basit şekilde, hayatınızı etkileyen kararları etkileyebilme şansımızın olması durumu olarak tanımlanabilir. Bu kavram günümüz uluslararası ilişkilere uyarlandığında ise, devlet dışı aktörlerin etkinliğinin artması ile bu aktörlerin uluslararası siyasi, ekonomik, sosyal, kültürel konularda çıkarları doğrultusunda gelişmeleri etkileyebilme yeteneklerini ifade eder. Küreselleşme ile birlikte çok uluslu şirketlerin ve uluslararası sivil toplum kuruluşlarının bu yönde gelişme kaydettiği görülmektedir. Bunun da ötesinde, siber uzay ve siber imkânlarla birlikte yönetişim pratiğinin daha da geliştiği görülmektedir. E-diplomasinin (dijital diplomasi) ortaya çıkması ve devlet adamlarının, diplomatların bu yöntemleri kullanması ile birlikte geleneksel egemenlik, yönetim anlayışları bypass edilmiş, kitlelerin talepleri ve beklentilerinin bu

bürokratik kesimler tarafından duyulması kolaylaşmıştır. (Yücel, 2016, s.758) Ayrıca siber ortamda özgürleşen bireyler talepleri doğrultusunda örgütlenerek yönetimleri etkileyebilme imkânına da sahip olmuşlardır.

Sonuç

Siber uzay hayatın her alanını etkilediği gibi uluslararası ilişkilerde de ciddi değişimler yaratmıştır. Devletlerin temel ve en güçlü olduğu uluslararası ilişkilerden çok aktörlü paydaşlardan oluşan ve güç dengelerinin tamamen değiştiği bir uluslararası ilişkilere geçiş yaşanmıştır. Siber alanının yönetimi, güvenliği gibi konularda çalışan yeni uluslararası kurumsal yapılar oluşturulmuş, bu durumda devletlerin görece dışarıda kaldığı özel sektör tarafından kurulan bir siber dünya ortaya çıkmıştır. Elbette tüm bu kurumsallaşmaların olması aynı zamanda bu yeni alanda işbirliği taleplerinin olduğuna da işarettir. Öte yandan, siber uzayın sınırsız, serbest, anonim gibi doğasından kaynaklanan özellikleri yeni güvenlik tehditlerinin ve yeni çatışma alanlarının oluşmasına neden olmuş, temel sorunsalı savaşların önlenebilmesi olan uluslararası ilişkiler disiplini savaşın yeni boyutlarıyla karşı karşıya kalmıştır. Tüm bu köklü değişimler ise, disiplinin doğduğu ilk yıllarda ortaya çıkan idealizmin bu kadar değişimi açıklamasını zorlaştırmıştır. Ancak yine de idealizmin serbest, özgürlükçü, çoğulcu anlayışı ile ortaya attığı argümanlar siber ortamın sağladığı yeni serbest, özgürlükçü ve çoğulcu sistemle örtüşmektedir.

Kaynakça

Arı, Tayyar. (2011). *Uluslararası İlişkiler ve Dış Politika*, Bursa: Mkm Yayıncılık, 9. Baskı.

Ateş, Davut. (2003). *Uluslararası Politika, Dünyayı Anlamak ve Anlatmak*, Bursa: Dora Yayıncılık.

Burchill, Scott. (2015). "Liberalizm", Scott Burchill, vd.(ed.), Muhammed Ağcan, Ali Aslan(çev.) *Uluslararası İlişkiler Teorileri*, Küre Yayınları.

Choucri, Nazli. (13-15 October 2013). *Co-Evolution of Cyberspace and İnternational Relations: New Challenges fort he Social Science*, Wold Social Science Forum (WSSF), Monreal, Canada.

Choucri, Nazli. (2012). *Cyberpolitics in İnternetional Relations*, The MIT Press, Cambridge, Massachusetts.

Council of Europe, "Convention of Cybercrime", (2001), http://www.europarl.europa.eu/meetdocs/ 2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf , Erişim Tarihi: 18.12.2016.

Czosseck, Christian. (2003). "State Actors and their Proxies in Cyberspace", Katharina Ziolkowski (ed.), *Peace Time Regime For State Activities in Cyberspace, İnternational Law, İnternational Relations and Diplomacy*, NATO CCD COE Publication, Tallinn.

Denk, Erdem. (2001). "Uluslararası Antlaşmalar Hukukunda Jus Cogens Kurallar", *Ankara Üniversitesi SBF Dergisi*, cilt 56, sayı 2.

Gözen, Ramazan. (2016). "İdealizm", Ramazan Gözen(der.), *Uluslararası İlişkiler Teorileri*, İstanbul: İletişim Yayınları.

Heywood, Andrew. (2007). *Siyaset*, Bircan Şahin(çev.), Buğra Kalkan(ed.), Ankara: Adres Yayınları.

Klimburg, Alexander (ed.). (2012). *National Cyber Security*, Framework Manuel, NATO CCD COE Publication, Tallinn.

Klimburg, Alexander ve Mirtl, Philip. (September-2012). *Cyberspace and Governance-A Primer*, Working Paper 65.

Koç, Cansu. (2015). "Neoliberalizmde Devlet ve Kamusal Alan Üzerine Bir Bakış", *TBB Dergisi*.

Kodaman, Timuçin ve Akçay, Ekrem Yaşar. (Güz-2013). "The Idealism- Realism Debate in International Relations and Idealists' Ways Of Ensuring The Peace", *Mehmet Akif Ersoy Üniversitesi SBE Dergisi*, cilt 5, sayı.9, ss. 131-136.

Link, Arthur S. (1986). "Woodrow Wilson's Fourteen Points", *The Papers of Woodrow Wilson*, vol 45.

Milliyet, "Çin'in Gizli Süper Ordusu", (2011) http://www.milliyet.com.tr/cin-in-gizli-super-ordu-su-ortaya-cikti/dunya/dunyadetay/27.05.2011/1395440/default.htm , Erişim Tarihi: 16.12.2016.

Sezgin, Aslı G. Şat. (Nisan- 2013). "Dünyada ve Türkiye'de E-Ticaret Sektörü", İktisadi Araştırmalar Bölümü, *Türkiye İş Bankası*, https://ekonomi.isbank.com.tr/userfiles/pdf/ar_04_2013.pdf , Erişim Tarihi: 18.12.2016.

Siberoloji, "Siber Uzay Tanımı ve Aktörleri", http://www.siberoloji.com/arastirma/siber-uzay-tanimi-aktorleri/ , Erişim Tarihi: 30.12.2016.

T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, "2016-2019 Ulusal Siber Güvenlik Stratejisi", http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf , Erişim Tarihi: 19.12.2016.

The White House, Washington, "The National Strategy to Secure Cyberspace", (February 2003), https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf , Erişim Tarihi: 19.12.2016.

Türkay, Şeyda. (2003). "Siber Savaş Hukuku ve Uygulama Sorunsalı", *İÜHFM,* cilt LXXI, sayı 1, ss. 1177-1228.

U.S. Army Cyber Command and Second Army, http://www.arcyber.army.mil/Pages/ArcyberHome.aspx , Erişim Tarihi: 18.12.2016.

Ünver, Mustafa. Canbay, Cafer ve Mirzaoğlu, Ayşe Gül. (Mayıs-2009) "Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler", *Bilgi Teknolojileri ve İletişim Kurumu*.

We Are Social, "Digital in 2016" http://wearesocial.com/uk/special-reports/digital-in-2016 , Erişim Tarihi: 16.12.2016.

Yücel, Gökhan. (Temmuz 2016). "Dijital Diplomasi", *TRT Akademi*, cilt 1, sayı 2.

ISSN: 2587-1218

ULUSLARARASI İLİŞKİLERDE SİBER CAYDIRICILIK

Sevda KORHAN*

Özet

Günümüzde devletler, kendi güvenlik altyapılarını, ekonomilerini ve diğer bütün varlıklarını savunmak amacıyla askeri ve siber alanda caydırıcılığı etkili bir araç olarak kullanmaktadırlar. Siber saldırılar, her ne kadar nükleer alanda oluşabilecek saldırılarla kıyaslanamasa da, uluslararası güvenlik için ciddi bir tehdit oluşturmaktadırlar. Yakın zamanda gerçekleşen siber saldırı örnekleri, gelecekte oluşabilecek uluslararası çatışmalarda siber saldırıların öncü rol oynayacağının sinyallerini vermiştir. Bu nedenle devletler, siber güvenliklerini sağlayabilmek adına siber caydırıcılık alanındaki faaliyetlere ağırlık vermeye başlamışlardır. Bu çalışmada, siber caydırıcılığın uygulanması noktasında ortaya çıkan engeller mevcut örnekler üzerinden incelenerek devletlerin siber saldırıları minimize etmek için geliştirdikleri stratejiler ele alınacaktır.

Anahtar Kelimeler: Siber Caydırıcılık, Siber Alan, Saldırı, Strateji

CYBER DETERRENCE IN IENTERNATIONAL RELATIONS

Abstract

Today, states use military and cyber deterrence as an effective tool to defend their security infrastructure, their economy and all their other assets. Cyber attacks are a serious threat to international security, although they are incomparable to the attacks that may occur in the nuclear field. Recent examples of happening cyber attacks have signaled that cyber attacks will can play a leading role in future international conflicts. For this reason, the states have begun to focus on activities in the area of cyber deterrence in order to provide cyber security. In this study, the obstacles to the application of cyber deterrence will be examined through the existing examples and the strategies developed by the states to minimize the cyber attacks will be handled.

Key Words: Cyber Deterrence, Cyberspace, Attack, Strategy

Giriş

Devletler ve devlet dışı aktörler tarafından gerçekleştirilen siber operasyonlar şiddetli bir şekilde artış göstermektedir. Bu nedenle çoğu devlet, ağlarını ve altyapısını korumak için

* Yüksek Lisans Öğrencisi, Selçuk Üniversitesi Uluslararası İlişkiler Bölümü. sevdakorhan@hotmail.com adresinden ulaşılabilir.

mücadele ederken, aynı zamanda siber alana caydırıcılık ilkelerini uygulamaya çalışmaktadırlar. Devletlerin siber alana uyguladıkları caydırıcılığı anlayabilmek için, geleneksel anlamda caydırıcılığı tanımlamak gerekir. Bir kavram olarak caydırıcılık, "korkutarak uzaklaştırmak ya da korkutmak" anlamına gelen Latince'deki "*déterrere*" kavramına dayanmakta ve "vazgeçirmek, bir karardan geri döndürmek" ya da "korku ile sınırlandırmak" olarak tanımlanmaktadır (Bendiek ve Metzger, 2015:5). Caydırıcılık kavramı, taraflardan biri için başka bir tarafın harekete geçmeden bir diğeri tarafından tehdit altına alınması şeklinde de tanımlanabilecek bir kavramdır (Urgancı, 2014). Caydırıcılığın amacı, eylem risklerinin faydalardan daha az olmasını sağlayarak agresif eylemi önlemektir (Jensen, 2012:779). Caydırıcılığın kelimesinin bir kavram olarak gelişimini incelediğimizde, kavramın hala gelişim safhasında olduğunu ve gerek teoride ele alınma biçimi, gerekse de pratik anlamda faaliyete geçmesinin zaman içerisinde değiştiğini görüyoruz (Mehmetçik, 2011:33).

Caydırıcılık, saldırılara karşı kısıtlama getirmek amacıyla kullanılan etkili bir araçtır. Ancak zaman içerisinde caydırıcılığın kullanım alanları değişmiştir. Caydırıcılık, güvenlik politikasında bir araç olarak kalmaya devam etse de, caydırıcılık teorisinin ele alınması noktasında, askeri ve daha özelde nükleer alana yapılan sınırlamanın yetersiz olduğu kabul edilmiştir (Bendiek, 2015:5). Bu nedenle, devletlerin varlıklarını idame etmede etkin olarak kullandıkları ulusal çıkar, ulusal güvenlik, ulusal egemenlik gibi faktörler, bu doğrultuda gelenekselden farklı olan yeni saldırı ve savaş metotlarının ortaya çıkmasını gerektirmiştir. Bu savaş ve saldırı metotlarını bir kategori halinde incelediğimizde, "Siber Terörizm", "Siber Saldırılar", "Siber Caydırıcılık", "Siber Güvenlik", "Siber Savaş", "Karma Savaş(Hybrid War)" gibi kavramlar karşımıza çıkmaktadır. Dolayısıyla siber alanda yaşanan bu gelişmelerin uluslararası arenada farklı bir çatışma alanını meydana getirdiği tezi, gerçekliğini koruyan bir durumdur (Güntay, 2015:479).

Sanal entegrasyon her yerde yaygınlaştığından, sanal saldırı veya casusluk tehlikesi de her geçen gün artmaktadır. Günde binlerce siber saldırı meydana gelmekte ve ciddi tehditleri önemsiz tehditlerden ayırmak gittikçe zorlaşmaktadır (Haley, 2013). Bilgi teknolojisinin ve internetin yaygınlaşması, kolaylıkla sömürülebilecek açıkların ve zayıf yönlerin üremesi için de gerekli zemini oluşturmaktadır. Dolayısıyla bu koşullar, bir kişinin dünyanın herhangi bir yerinde zarar verebilecek araç ve yeteneklere daha kolay sahip olmasına izin vermektedir (Nagorski, 2010:1). Bugün birçok sivil kurum, teknik altyapı ve hükümet hizmetleri, önemli ölçüde internet ve diğer bilgi ağlarına bağlanmıştır. Trafik kontrol sistemi, enerji sistemleri, su temini, bankacılık, eğitim ve sağlık hizmetleri, ulaşım, borsa gibi faaliyetler bile bugün

internet üzerinden yürütülmektedir. Dolayısıyla bu sektörlerden herhangi birindeki savunmasızlık, diğer sektörlere de ciddi zararlar verecektir ve ülke altyapısını çökertebilecektir.

Soğuk Savaş dönemindeki, küresel güvenlik yapısına statik ve iki kutuplu bir sistem hâkimdi. ABD ve onun ekseninde birleşen kapitalist müttefiklerine karşılık, Sovyetler Birliği ve komünist müttefikleri yer alıyordu. Bu dönem büyük bir tehlike arz etmesine rağmen iki kutupluluk, ülkelerin ulusal güvenlik politikasını oldukça basit bir şekilde oluşturmasına yardımcı olmuştu. Soğuk Savaş'ın yürütülmesi her ne kadar zor ve maliyetli olsa da en azından sisteme belirsizlik yerine netlik ve kararlılık hâkimdi. Düşmanlar oldukça fazla ve güçlü olmasına rağmen sayıları sınırlıydı ve kimlikleri tespit edilebilirdi. Amaçları ve eylemleri bakımından da öngörülebilirlik düzeyleri oldukça yüksekti. Dolayısıyla bunların hepsi her iki tarafın da caydırıcılık politikalarının gelişimini kolaylaştırdı (Kugler, 2009:9). Soğuk Savaş döneminde nükleer caydırıcılık ABD ve Sovyetler Birliği'ni kontrol altında tutmayı başardı. Bu mantığa dayanarak, siber caydırıcılığın da bilgi çağında benzer bir rol oynayabileceği düşünülmektedir. Ancak makalenin ilerleyen bölümlerinde göreceğimiz gibi anonimlik, küresel erişim ve bilgi ağlarının birbirine bağlılığı, gibi siber caydırıcılığın etkinliğini büyük ölçüde azaltan faktörler nedeniyle siber caydırıcılığın etkin olamayacağı da düşünülmektedir (Nagorski, 2010:1).

Siber Caydırıcılık Nedir?

İnternetin gelişmesi dünyamızı daha küçük bir alan haline getirmiş ve sınırlar arasında iletişim ve etkileşimin yolunu açmıştır. İnternet sayesinde dünya küçük bir köy halini almakta ve dünyanın her yeri herkes için aynı uzaklıkta olmaktadır (Arzu Yıldırım, 2014:57). Ancak internetteki sınırların eksikliği aynı zamanda siber alanın saldırganlar ve siber suçlular için verimli bir üreme alanı haline gelmesine sebebiyet vermiştir. Bu nedenle ülkeler, etkili bir siber caydırıcılık sistemini hukuksal bir düzenleme oturtabilmek için yeni yasalar oluşturmaya çalışmışlardır (Nagorski, 2010:9). Ancak oluşturulmaya çalışılan bu hukuksal yapı geleneksel hukuk anlayışının dışında olmak durumundadır. Çünkü siber uzaydaki faaliyetler sadece devletlere özgü olmayıp geniş bir yelpazeye erişebilme yeteneğine sahiptir ve siber uzayın getirmiş olduğu yeni imkânlar, şiddet unsuru içerebilecek birçok silahtan farklıdır. Mesela, uluslararası alanda çok az devlet nükleer kapasiteye sahipken, 140'tan fazla ulusun siber silahlara sahip olduğu ve 30'dan fazla ülkenin de kendi askeri birimleri içerisinde siber

birlikler kurduğu iddia edilmektedir (Jensen, 2012:780).

Siber caydırıcılık, Uluslararası İlişkiler disiplininde etkin olan oyun teorileri bağlamında bakıldığında yararlı bir olgu olarak görülmektedir (Ermiş ve Özdal, 2013:279). Ancak, ABD Savunma Bakanlığı'nda görev yapan Eric Rosenbach, 2014'te yaptığı bir konuşmada uluslararası ilişkiler alanında uzmanlaşan kişilerin siber caydırıcılıktan çok, nükleer caydırıcılık üzerinde durduğuna vurgu yapmıştır. Rosenbach ayrıca yaptığı konuşmada, caydırıcılık üzerine yapılan çalışma ve araştırmaların üç aşamasından söz ederek bunlardan ilkinin, suçluların bir kez daha aynı suçu işlemelerini engellemek maksadıyla kullanılan "hukuki caydırıcılık"; ikincisinin, Soğuk Savaş döneminde ABD ve Sovyetler Birliği'nin birbirlerine karşı hareketlerini kısıtlayan "nükleer caydırıcılık" ve sonuncusunun da bugün geldiğimiz noktada etkin olarak kullanılan "siber caydırıcılık" olduğunu ifade etmiştir. Rosenbach ayrıca saldırı kavramının siber alandaki kullanımının nükleer alandaki kullanımdan farklı bir biçimi olduğunu anımsatarak nükleer caydırıcılığın siber caydırıcılığa kıyasla daha kolay olduğunu ifade etmiştir (Siber Bülten, 2014).

Devletlerin çoğu tarafından siber alan "*beşinci muharebe alanı*" şeklinde tanımlanmıştır (Çelik, 2015:32). Dolayısıyla devletler bu alanda güçlerini koruyabilmek ve caydırıcılık konusunda gücünü maksimize edebilmek maksadıyla çeşitli stratejiler oluşturup bunları uygulamaya başlamışlardır. Siber uzaydaki rekabetin bir uzantısı olarak, uluslararası arenanın birincil aktörleri, siber caydırıcılığın etkilerini hesaba katarak hem siber savunma hem de siber saldırı kapasitelerini arttırmakta hem de siber ordulara muazzam düzeyde yatırımlar yapmaktadırlar. Bunun yanı sıra devletler taraflarını belirleyerek, siber alanda savunma ve istihbarat sağlanması konusunda birçok ittifaka imza atmışlardır. Örneğin, Eski ABD Başkanı Barack Obama, 2016 senesinde siber alandaki güvenliği sağlamak için bütçeyi %35 arttırmış ve 19 milyar dolar olarak ilan etmiştir (Gücüyener, 2016). ABD'nin ulusal istihbarat direktörü Mike McConnell, 28 Şubat 2010'da Washington Post'a "Kaybettiğimiz siber savaşı nasıl kazanacağız" başlıklı bir yazısında, dünyanın 1950'lere döndüğüne dikkat çekerek, nükleer silahların çoğalması için kullanılan yöntemlerin artık siber tehditlerle baş etmede kullanılması gerektiğini belirtmiştir (Nagorski, 2010:1).

Caydırıcılık ve siber savaş arasındaki bağlantı üzerine gelişen tartışmalara aynı unsurlar hâkimdir. Caydırıcılık stratejisi ve siber savaş üzerine yapılan araştırmaların çoğu Amerikan bakış açısına dayanmaktadır (Lupovici, 2011:49). Yapılan araştırmalar, siber saldırıları

önlemek için caydırma stratejisini başarılı bir şekilde uygulamanın imkânlarını inceler veya ABD'nin karşılaştığı diğer tehditleri caydırmak için ABD'nin siber savaşı kullanma biçimini analiz eder. Ancak İsrail, Japonya ve Hindistan gibi siber güvenlik alanında gelişmiş ülkeler göz ardı edilmemelidir (Çelik, 2015:32). ABD'nin bu kadar önde olmasının nedeni siber saldırılara karşı oldukça açık bir ülke olmasıdır. Rusya ve Çin gibi ülkelere oranla askeri ve sivil altyapıları önemli ölçüde siber alana bağımlıdır. Dolayısıyla ABD'nin siber savaş alanında hem savunmacı hem de saldırgan olarak en ileri konumda olan devlet olduğu düşünülmektedir (Marmon, 2011).

Siber Caydırıcılığın Unsurları

Caydırıcılığın unsurları incelenirken literatürde çoğunlukla benzer bileşenler listelenir. Goodman'a göre caydırıcılık sekiz unsuru bünyesinde barındırmaktadır; çıkar, caydırıcı beyan, engelleyici önlemler, cezalandırıcı önlemler, inanılırlık, güvence verme, korku ve fayda-maliyet avantajının hesaplanması. Bu bileşenler birlikte güçlü ve etkili bir caydırma stratejisi oluşturmaktadır (Goodman, 2010:105). Thomas Schelling de bu şartlardan güvenilirliğe vurgu yapar. Caydırma stratejisinin başarılı olabilmesi için, bir devletin niyetlerini açıkça bildirmesi ve güvenilir bir iletişime sahip olmasıdır. Mevcut bağlamda, bu çerçeveye başka bir unsur daha eklenir. Güvenilir bir caydırıcılık oluşturmak için, devletin saldırının kaynağını tanımlama yeteneğine sahip olması gerekir (Bate, 2015). Bu bileşenler ayrı ayrı ele alındığında, devletlerin caydırıcılığı çıkarlarını korumak için kullandıkları göze çarpmaktadır. Bu durumda devlet, çıkarlarını korumak adına bir beyanda bulunmak zorundadır. Devletin yapacağı beyan, kendi çıkarlarına saldırıldığı zaman, savunmacı olmalıdır. Aynı zamanda saldıran devlete ceza verebilecek derecede saldırgan bir tutum sergilemelidir (Ermiş, 2015).

Diğer devletlerin caydırıcılık beyanını ciddiye alması için, beyan inandırıcı olmalıdır. Güvence vermek; potansiyel bir düşmana, çıkarlara saldırmaması için bir sebep vermek demektir. Güvence vermek çoğu zaman da karşılıklı güvenlik garantileri şeklinde kendini gösterir; yani devlet, diğerlerinin söylenen şeyi yapması halinde kendi faaliyetinden vazgeçmeyi taahhüt eder. Bu unsurların hepsi olumsuz bir fayda-maliyet hesaplamasına neden olur (Goodman, 2010:106).

> *Caydırıcılığın sağlanabilmesi için gerekli olan sekiz unsurun yanında, caydırıcılığın siber uzayda etkin olabilmesi için özellikle beş unsura dikkat etmek gerekir. Goodman tarafından genel olarak tespit edilen başlıklar şunlardır:*
> *a.Devletler, saldırı ve savunma kapasitelerini koruyucu önlemler almalıdır.*

b.Devletler arasında güvence faktörünün yokluğu siber caydırıcılık aracılığıyla kurulan ilişkiye zarar verebilir.
c.Saldırgan, karşı saldırıya geçmeden kimliğinin tespiti yapılmalıdır.
d.Devletler, siber çatışma sırasında iletinin saldırgan tarafından anlaşılmasını sağlamalıdır.
e.Devletin ilk saldırıdan sonra kapasitesini güvence altına alması gerekir. (Ermiş, 2015).

Goodman'ın sıraladığı bu beş unsurdan "kimliğin tespit edilmesi gerektiği" unsuru, siber alanda caydırıcılığın etkili olması konusunda en çok sorun yaratan unsurlardandır. Siber alanda yapılan saldırılarda saldırganların kimliğini gizleyebilmesi, devletleri aldıkları önlemler noktasında da etkisiz hale getirebilmektedir. Dolayısıyla bu durum Goodman'ın vurguladığı önlemleri devre dışı bırakabilmektedir.

Siber Caydırıcılığın Etkili Olmasında Ortaya Çıkan Engeller

Caydırıcılık, saldırı kaynağını belirlemenin(*attributing*) güçlükleri ve siber alandaki devlet ve devlet dışı aktörlerin sayısının çokluğu nedeniyle siber uzayda/alanda istenildiği düzeyde etkili bir strateji değildir (Nye, 2015). Patrick Morgan *"Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm"* isimli çalışmasında klasik caydırıcılıkta önem arz eden ancak, siber caydırıcılığın sağlanması noktasında sorunlu olan öğelerin varlığına dikkat çekmiştir. Morgan'ın üzerinde durduğu bu unsurlar kimlik ve motivasyon unsurlarıdır (Ermiş, 2015). "Soğuk Savaş döneminde nükleer caydırıcılığın uygulanması esnasında saldırı eyleminde bulunan aktörün kim olduğu ve nasıl bir motivasyonla mobilize olduğu açıkça bilinmektedir. Siber alanda ise saldırganın kimliğinin belirlenmesi mümkün olmayabilirken, motivasyonu da belirsiz olan saldırgana verilmesi gereken asıl tepkinin ne olacağını bilmek de güçtür."(Ermiş, 2015).

Siber caydırıcılık kavramını klasik/geleneksel anlamda kullanılan caydırıcılıktan ayırt eden başat unsur, saldırı kaynağının tespit/isnat edilmesi durumudur. Siber uzayda sanal âlemin tabiatı gereği meydana getirdiği anonimlik misilleme faktörünün doğru kaynağa yapılması noktasında engel teşkil etmektedir (Ermiş ve Özdal, 2013:279). Eğer bir misilleme yapılacaksa, öncelikle bilinmesi gereken, saldırının kimin tarafından gerçekleştirildiğidir. Şayet caydırıcılık, ilk aşamada yapılacak olan misilleme meydana gelmeden önce devreye girecekse, diğerleri de, caydıran devletin kendisine kimin saldırdığını kesin olarak bileceğinin farkında olmalıdırlar. Aksi takdirde devlet yanlış kişiye saldırılmış olacaktır ve bu durum yeni

düşmanların türemesine sebebiyet verecektir (Ermiş ve Özdal, 2013:280).

Siber caydırıcılık, henüz emekleme döneminde ve neredeyse nükleer caydırıcılığın 1950'de olduğu yerdedir. Siber araçlar, siber olmayan bölgelere de zarar verebilir. Bunun gerçeğe dönüştüğü yer, literatüre "Blended Attacks" olarak geçen ve İran nükleer tesislerini çalışmaz duruma getiren 2010 Stuxnet vakasıdır. Bu saldırı, siber saldırıların fiziksel dünyada da yıkıcı sonuçlar doğurabileceğini göstermiştir (Paul Mueller ve Babak Yadegari, 2012:1). Siber çatışmalar, "çok kutuplu" ortamlarda gerçekleştiğinden dolayı, bazen iç tehditler uluslararası tehditlerle iç içe girer. Siber silahların etkileri anlık olabildiğinden, diğer caydırıcılık türlerinden çok daha güvensiz bir ortam oluşturabilmektedir. Ayrıca siber silahlar siviller ve hedef aldığı diğer aktörler arasında ayrım yapmaz ve sivilleri hedef almaktan kaçınmaz. Son olarak, bu tür saldırıların niteliği ve motivasyonu önceden tahmin edilemez. Her operasyonun beklenmedik sonuçları olabilmektedir. Bu da siber dünyada caydırılmayan birçok aktörün var olmasına yol açmaktadır (The Cyber Wire, 2016). Ancak tehdit algılamaları hem etkin bir ulusal strateji geliştirilmesi hem de caydırıcılık teorisinin uygulanması için merkezi bir rol oynamaktadır. Bir ülkenin veya bir kuruluşun tehdidi değerlendirme şekli, stratejik yanıtlarını anlamak açısından önemlidir. Bu nedenle bir siber saldırıya verilecek karşılığın etkili olabilmesi konusunda tehdidin doğası, tehdit unsurları, kullanılan teknik araçlar ve potansiyel hedef önemlidir (Bendiek, 2015:3).

Siber Caydırıcılığın Sağlanabilmesi İçin Geliştirilen Stratejiler

Etkili bir siber caydırıcılık stratejisinin oluşturulabilmesi için siber saldırıları engelleyebilecek güçlü bir savunma sistemini kurmak ve siber saldırıları minimum düzeyde tutabilmek gereklidir. Siber saldırılar çoğu zaman yalnızca hasar vermek amacıyla değil, politik ve stratejik hedeflere ulaşmak amacıyla da yapılmaktadır (Kugler, 2009:9). Dolayısıyla devletler; sözleşme, pazarlık veya zorlama araçlarını kullanarak, saldırganları bu tür eylemleri yapmaktan alıkoyabilecek stratejiler geliştirme yoluna giderler. Örneğin, ABD ve AB arasında 2010 yılından bu yana siber güvenlikte işbirliği mekanizması oluşturulmaya çalışmaktadır (Gücüyener, 2016). Bu nedenle, siber caydırıcılık stratejisi, ülkelerin ulusal güvenlik politikasının bir parçasıdır ve diğer bileşenlerden ayrı tutulamaz. Siber caydırıcılık stratejisinin temel amacı, orta büyüklükteki saldırıları düşük düzeyli olaylara dönüştürmek ve büyük saldırıların neredeyse tamamen caydırılmasını sağlamaktır (Kugler, 2009:14).

Bugüne kadar hem hükümetler hem de uluslararası kuruluşlar siber güvenlik ve caydırıcılık konusunda birçok adım atmışlardır. Bazı ülkeler, olaylarla başa çıkabilmek için Bilgisayar Acil Müdahale Ekipleri (CERTs) kurma yoluna gitmektedir. ABD ve İngiltere, siber güvenlik politikalarını oluşturan diğer ülkelere göre önde olan model ülkelerdir. Bazı ülkeler de, siber tehditlere karşı ulusal bir organizasyon oluşturmayı başarabilmişlerdir. Örneğin; Brezilya'da federal hükümet, 2009'da Bilgi ve İletişim Güvenliği Departmanı altında Kritik Altyapı Koruması Bilgi Güvenliği Çalışma Grubu'nu kurdu. Oluşturulan bu grup, bilgi güvenliğinin sağlanması ve olaylar karşısında verilecek tepkilerin planlaması üzerinde çalışmalarını sürdürmektedir (Kugler, 2009:12).

Savunma amaçlı kurulmuş bölgesel bir örgüt olan NATO da etkili siber caydırıcılık stratejileri geliştirmeye çalışmaktadır. NATO, siber engelleme yeteneklerini merkezi bir savunma sistemi altında birleştirmeyi hedefliyor. Ayrıca bu alana yönelik stratejisini ulusal siber savunma yeteneklerini geliştirmek ve koordine etmek için kullanmaktadır. NATO bunu yaparken, planlama sürecini kullanmaya özen göstermenin yanı sıra, tüm NATO organlarını siber koruma altına alıp daha iyi bir entegrasyon sağlayarak hareket etmektedir. NATO bu şekilde daha fazla siber saldırıyı önlemeye ve tespit etmeye çalışmakta, aynı zamanda savunma ve kurtarma yeteneğini geliştirmeyi hedeflemektedir. (Doğrul, Aslan, Çelik, 2011:39). Bu doğrultuda NATO, Oberammergau'da bulunan NATO Okulu ve Portekiz'deki Siber Akademisi vasıtasıyla geniş bir çerçeve oluşturan eğitim, öğrenim ve tatbikat fırsatları sunmaktadır. NATO tarafından oluşturulup Talin'de yer alan İşbirliğine Dayalı Siber Savunma Mükemmeliyet Merkezi de bu konuda önemli rol üstlenmektedir. NATO'nun buradaki diğer bir amacı, siber bilinç ve farkındalık konusunda üye ülkeleri de bilgilendirmektir. NATO'nun bu konuda izlediği yol, müttefiklerin toplu siber savunma hedeflerini oluşturmak için katılacakları iki yıllık bir süreçtir (NATO Dergisi, 2016).

ABD strateji belgelerinin çoğunda siber saldırıların önlenmesi ele alınmaktadır. Örneğin, ABD, siber tehditlerin artması ihtimaline karşı 2003'te Güvenli Siber Alan Ulusal Stratejisi'ni yayınlamıştır. Bu strateji, üç büyük hedefi içermektedir. Birincisi, siber saldırıları önlemek; ikincisi, ABD'nin güvenlik açığını azaltarak saldırılar neticesinde oluşabilecek herhangi bir hasarı minimum düzeye indirmek; üçüncüsü ise, saldırılara mümkün olduğunca hızlı bir şekilde karşılık verebilmek. Ancak bu stratejinin eksikliği, siber saldırıların nasıl önleneceği

konusunda çok az şey içeriyor olmasıdır. 2005'te de benzer içerikli bir strateji geliştirilmiştir. Burada da etkili güvenlik koşulları teşvik edilmeye çalışılmıştır (Kugler, 2009:2). Diğer ABD strateji belgeleri arasında en önemlisi, Beyaz Saray tarafından 2006'da yayınlanan ABD Ulusal Güvenlik Stratejisi'dir. Belgede, fiziksel ve siber alanlarda gerçekleşebilecek saldırılara yönelik caydırıcılık sağlayabilecek bir askeri kuvvet inşasının talimatı verilmiştir (Kugler, 2009:3).

Yakın zamanlı stratejilere bakacak olursak, ABD 2015'te yayınladığı Ulusal Askeri Stratejisi'nde, Kuzey Kore'nin siber saldırılarla bir ABD şirketine büyük zarar verdiğini ve bunun devamının gelebileceğini ifade etmiştir. Stratejide ayrıca siber güvenlik, füze savunması, deniz güvenliği ve afetlerin hafifletilmesi için Avustralya, Japonya, Kore Cumhuriyeti, Filipinler ve Tayland ile ittifakların güçlendirilmesi gerektiği; ayrıca Hindistan Yeni Zelanda, Singapur, Endonezya, Malezya, Vietnam ve Bangladeş'le olan ortaklıkların inşa edileceği vurgulanmıştır (Joint Chiefs of Staff, 2015). Burada geçen siber güvenlik için oluşturulması planlanan ittifakların, fiziksel alanda olduğu gibi, siber alanda da gerekli olduğunu göstermektedir. ABD, son olarak 2016'da yayınladığı Ulusal Karşı İstihbarat Stratejisi'nde yabancı istihbarat biriminin faaliyetlerinden kaynaklanan çeşitli siber tehditler ve zorluklarla karşı karşıya olduğunu ifade etmiştir (National Counterintelligence and Security Center, 2016).

Siber Caydırıcılık Örnekleri

En ünlü uluslararası siber çatışmalardan biri, 27 Nisan 2007'de Estonya'nın ülke çapında siber saldırıyla uğramasıdır (Jensen, 2013:801). Estonya, bu yıllarda, dünyanın en ileri teknolojisine sahip ülkelerinden biri olmuş ve bu yönde etkili olabilecek ulusal girişimlerde bulunmuştu. Aynı zamanda ülkenin altyapısı derin bir şekilde internete bağımlı hale gelmişti. Hemen hemen tüm hükümet hizmetleri elektronik ortama entegre edilmiş ve satış noktalarındaki alımlar internet işlemleri ile gerçekleştirilmeye başlanmıştı. Ülke bu süreçte ping saldırıları ve DDOS (Distributed Denial of Service Attack) saldırılarına maruz kaldıktan sonra ekonomi zor bir süreç yaşadı (Mowbray, 2010:2). Hükümet, bu saldırıların, başkent Tallin'deki tartışmalı Kızıl Ordu anıtının kaldırılmasından sonra (anıt, birçok Estonyalı için baskıcı Sovyet dönemini simgelediği gerekçesiyle kaldırılmıştı) başladığını iddia etmiştir. 22 gün süren yoğun kitle saldırıları, 18 Mayıs'ta ancak izole edilebildi ve saldırılar belli oranda hafifletilebildi (Goodman, 2010:111).

Saldırılara Estonya'nın başlangıçtaki cevabı ağlarının bazı bölümlerini uluslararası trafiğe kapatmak şeklinde olmuştur. Estonyalı yetkililer, saldırılarda Putin'in kabinesine ait IP adreslerinin kullanıldığını iddia etmiştir. Rusya ve Estonya, saldırılardan sonra Estonya'nın çağrıda bulunduğu karşılıklı bir hukuki yardım anlaşmasına rağmen, Rusya Estonya'nın anlaşmak için gösterdiği çabaları sonuçsuz bırakarak anlaşmayı reddetmiştir. Rusya'nın bu reddi, saldırıların derinlemesine soruşturulmasını imkânsız hale getirmiş ve saldırıların Rusya tarafından yapıldığı gerçeğini gözler önüne sererek, Rusya'nın suçluluğu konusundaki şüpheleri artırmıştır (Goodman, 2010:111). Ancak birkaç yıl sonra yalnızca Rus kökenli bir Estonyalı'nın hüküm giymiş olması, bütün gözlemlere rağmen Rus hükümetinin suçluluğuna ilişkin net bir kanıt bulunmasının önünde bir engel teşkil etmiştir (BBC, 2007). Burada siber caydırıcılık yönünde verilen mesajların karşılıklı olarak birbirini güçlendiren üç faktörden dolayı tartışılabilir olduğunu göstermektedir. Bu faktörler; gizlilik, asimetri ve süper güçlendirme olarak karşımıza çıkmaktadır (Goodman, 2010:113).

2007 Estonya davası aynı zamanda siber alanın asimetrisini de örneklendirmektedir. Araştırmacılara göre Estonya siber alanda herhangi bir karşı saldırıya geçmek istediğinde Rusya, Estonya'nın karşılık vermesine imkân sağlayacak bir alan bırakmayabilir. Yani devletlerin fiziksel dünyada orantılı etkiler yaratmaya çalışması sırasında, bir meydan okumayla yüzleşme ihtimalleri oldukça yüksektir. Süper güçlendirme faktörüne değinecek olursak, 2007 Estonya siber saldırıları, internetteki süper yetkili aktörlerin nasıl oluştuğunu göstermektedir. Estonya, başkalarının da saldırıya dâhil olduğu konusunda ısrarcı olmasına rağmen, bu davadan yalnızca bir kişi hüküm giymiştir. Dolayısıyla bir kişi, bir devlet gücünde saldırı kapasitesine sahip olabilmiş demektir. Bu durum, devletlerin etkili bir siber caydırma stratejisi geliştirmeye çabaladıkları esnada, bariz sorunlar ortaya çıkarabilir. Çünkü siber alanda devletlerin caydırılması yeterince zor iken, kişilerin caydırılması çok daha zor görünmektedir (Goodman, 2010:113).

Benzer şekilde, Ağustos 2008'de Rusya ile Gürcistan arasındaki çatışmada Rusya Gürcistan'a karşı bir siber saldırı başlattı (Alagöz, 2012). Rusya DDOS'u kullanarak, ülkenin iletişim sistemlerinin çoğunu kullanılmaz hale getirmiştir.(Mowbray, 2010:2) Saldırıya maruz kalan Gürcistan hükümeti, Rusya'dan gelen tüm saldırıları engellemeyi başarmıştır fakat Rusya bu defa bütün saldırılarını Çin üzerinden yapmaya başlamıştır. Rusya böylece Gürcistan'ı hem siber alanda savunmasız bırakmış hem de aldığı önlemleri devre dışı bırakmayı başarmıştır (Kara, 2013:48-49). Rusya ile Gürcistan arasında çatışma devam ederken gerçekleşen siber

saldırıda jeopolitik faktörler, siber caydırıcılığın teorik zorluklarını ortaya çıkarması bakımından elzemdir. (Goodman, 2010:110)

2008'de Rusya'nın Gürcistan'a karşı yürüttüğü operasyon, siber caydırıcılığın birkaç sorununu daha ortaya çıkarmıştır. Bunlar, ölçülebilirlik ve zamansallık sorunlarıdır. Siber dünyada kullanılan tek bir araç, büyük ölçüde geniş bir etki yaratabilmektedir. Dolayısıyla bu durum, saldırı göstergelerinin ve uyarıların saldırı ölçeğini tahmin etmesini ciddi oranda zorlaştırmaktadır. Gürcistan örneğine baktığımızda yapılan saldırılar sırasında, hackerlar hükümetin web sitelerini çökertmişti. Ancak buna rağmen, bu durum hafif bir hasara yol açarak uzun vadeli bir bozulmaya sebebiyet vermedi. Gizli ve zamana duyarlı virüsleri hükümet sistemlerine bıraktılar ve müdahaleler bittikten sonra Gürcü şebekelerinde tahribat yarattılar. Bir diğer sorun olan zamansallık ise, siber saldırıların anlık niteliğini ifade eder. Savunmacılar, saldırılara karşı erken uyarı yaparlar. Fakat bu dijital sinyallerin ne zaman, kime karşı, ne amaçla meydana geldiği belli değildir. Fiziksel sinyaller ise bu bilgilerin çoğunu veya tamamını sağlarlar. (Goodman, 2010:116)

Gürcistan ve Estonya, gerçekleşen saldırıların üstesinden gelebilmiştir. Ancak Gürcistan ve Estonya örneği bir gerçeği daha daha ortaya çıkarmıştır. Şöyle ki, gelecekteki saldırıların bu gibi küçük ülkelerle sınırlı kalacağı ya da bu denli geçici zararlar vereceğinin garantisi yoktur. Aslında, herkesin bu tür saldırılara karşı savunma güçlerinin fazla olmadığını söylemek mümkün. Çoğu ülkenin bu konuda hazırlıksız olması ve siber alanda yapılan saldırıların ülkelerin altyapılarını çökertebilecek potansiyele sahip olmasından dolayı bu tür saldırılar büyük hasarlara neden olabilirler. Avrupa ve Asya gibi diğer bölgeler de benzer şekilde bilgi ağlarına güveniyorlar, fakat burada meydana gelebilecek herhangi bir bozulmaya karşı savunmasız görünüyorlar. Siber saldırı araçları yaygınlaştıkça, siber alandaki siyah şapkalı saldırgan aktörlerin teknik kapasitesi de gelişmekte ve bu durum siber zayıflıkların artmasına sebebiyet vermektedir (Kugler, 2009:9). Örneğin Türkiye, siber saldırıya uğrayan ülkeler arasında Avrupa'da 1, dünyada ise 3. Sırada yer almaktadır (Göksel Yıldırım, 2016). Siber saldırılara büyük devletlerin de maruz kalabileceğinin en yakın örneğini, 2016 ABD seçimlerine Rusya'nın müdahale ettiği yönündeki iddialar oluşturmaktadır. Obama yönetimi, Rusya'nın 2016'daki başkanlık seçimlerine müdahale ettiği gerekçesiyle Rusya kaynaklı siber saldırılarıyla ilgili yaptığı sert uyarıların ardından Rusya hedeflerine karşı bir dizi yaptırım ve cezalandırma önlemi uygulandı. Batı yaptırımları, genellikle Rusya siyasi sisteminde büyük bir reforma neden olmamıştır. Ancak, yaptırımlar bazı savunucuların iddia ettiği gibi,

gelecekteki Rusya eylemlerine karşı etkili bir caydırıcılık unsuru oluşturabilirler.(Rojansky, 2016)

ABD'nin Rusya müdahalesine yönelik kullandığı "orantılı" tabiri tartışılan konular arasında yer almakta ve ABD'nin Rusya'ya gizli bir yanıt vermeyi planladığı ihtimali üzerinde durulmaktadır. Ancak bir taraftan da ABD'nin gerçekten bir tepki verip vermeyeceğine yönelik bazı kesimlerde şüpheler var. Beyaz Saray'a karşı bu şüphelerin sebebi ise, ABD'nin Kuzey Kore'nin Sony'e yönelik saldırısına tepki vereceğini söylediğinde de aynı dili kullanmış olmasıydı. Hâlbuki Kuzey Kore'ye yönelik herhangi bir yaptırımda bulunmamıştır. (Hennessey, 2016). Dolayısıyla bu durum, ABD'nin siber alandaki tehditlerini yerine getirebilecek kadar caydırıcı bir güce sahip olmadığı yönünde tartışmalara yol açmıştır.

Sonuç

Siber caydırıcılığın ortaya çıkmasıyla beraber, asırlardır fiziki alanlarda (kara, deniz, okyanus) kendileri için avantaj sağlamak için uğraşan devletler bugün anlaşma ve saldırı alanlarını çok daha farklı bir alan olan siber uzaya taşımaya başlamışlardır (Gücüyener, 2016). Sonuç olarak, insan medeniyetinin gelecekteki büyümesi ve gelişmesinin, siber uzayın büyümesi ve gelişimi ile bağlantılı olduğu ve bu gerçeğe karşı daha fazla kamuoyunun farkında olması gerektiği söylenebilir. Bir sonraki savaşın fiziksel uzay yerine siber uzayda olabileceği yönündeki öngörüler, Estonya ve Gürcistan örneklerinde doğrulanmıştır. Bu saldırılardan sonra Estonya ve Gürcistan gibi ülkeler de dahil olmak üzere tüm ülkeler, siber caydırma stratejileri konusunda uluslararası bir konsensüs oluşturmak için gerekli adımları atmalıdır (Nagorski, 2010:10).

Siber caydırıcılığın etkili olup olmayacağına yönelik tartışmalarda genel olarak caydırıcılığın siber alandaki saldırılar için nihai çözüm olmadığı sonucuna varılır. Siber caydırıcılık pek çok önemli yönden nükleer çeşitlilikten farklıdır ve bu nedenle uygulamada ne kadar etkili olursa olsun tüm saldırıların oluşumunu ortadan kaldırmak pek olası değildir. Siber alanda yapılan saldırılarda saldırganın kimliğinin tespit edilememesi, saldırının nasıl bir motivasyonla yapıldığının bilinmemesi, misillemenin doğru kaynağa yapılması yönünde problemlerin ortaya çıkması ve devletlerin henüz bu konuda yeterli deneyime sahip olmaması bunun en büyük sebepleri arasında gösterilebilir. Bununla birlikte, caydırıcılık, toplam saldırı sayısının nispeten düşük bir maliyetle yönetilebilir bir seviyeye indirilmesinde kritik bir rol oynayabilir (Haley, 2013). Sonuç olarak, üst düzey sanayi ve hükümet yetkilileri, bu yüzyılda hayatımızın tamamında yer alan siber boyutun güvenli bir şekilde çalışmasını sağlamak için cesur yeni önlemler almak durumundadırlar (Nagorski, 2010:1).

Yukarıda da değinildiği gibi genel olarak, siber caydırıcılığın etkin bir şekilde sağlanamayacağı düşünülüyor. Siber caydırıcılığın başarısız olmasına sebep olan faktörler sıralanıp bunlara bir çözüm getirilmediği zaman, siber saldırganlar kendilerini "dokunulmaz" olarak görüp daha fazla cesaretlenebilmektedir (Kugler, 2009:14). Stratejistler tarafından geliştirilecek etkili ve güvenilir bir caydırıcılık stratejisi saldırganları yapacakları saldırılar konusunda belli oranda caydırmakta başarılı olabilir. Bunun yanında geliştirilen stratejinin saldırganların haberdar olabileceği şekilde beyan edilmesi, fiili savaş durumunda saldırganları geri püskürtme konusunda katkıda bulunabilir (Marmon, 2011).

Şimdiye dek ülkeler, büyük siber saldırıları kesin olarak caydırabilecek potansiyelleri olduğunu net bir şekilde gösterememişlerdir. Yine de saldırganların bir kısmı herhangi bir ülkeyle siber rekabete girmek konusunda caydırılabilirse, fiili siber saldırganlık tehlikeleri de belli oranda azalacaktır. Bunun sağlanabilmesi için devletlerin teknik, siyasi ve sosyal koşulları yerine getirmesi gerekir. Ayrıca devletlerin kararlılığını, yeteneğini ve imajını sunabilme kapasitesi de bunda büyük rol oynayacaktır. Siber caydırıcılığı güçlendirmek için atılabilecek adımlar, siber güvenliği geliştirmek, aktif savunma yöntemlerini kullanmak ve siber alan için uluslararası normlar oluşturabilmektir (Denning, 2016).

Kaynakça

ALAGÖZ, E. (2012). Sürekli Artan Önemi Işığında Siber Güvenlik. http://www.bilgesam.org/incele/1207/-surekli-artan-onemi-isiginda-siber-guvenlik/#.WJJEqPmLTIW (Erişim Tarihi: 30.01.2017).

BATE, Laura K. (2015). In Search of Cyber Deterrence. http://warontherocks.com/2015/09/in-search-of-cyber-deterrence/ (Erişim Tarihi: 13.12.2016).

BENDİEK, A. ve T. Metzger. (2015). Deterrence Theory In The Cyber-Century. *SWP-Berlin*. Sayı 2.

ÇELİK, M. (2015). Siber Ordu Kurmak İçin Devletler Özel Sektör ile Çalışıyor. *TMMOB Bilgisayar Mühendisleri Odası Dergisi*. Sayı 5.

DENNİNG, D. (2016). Cybersecurity's Next Phase: Cyber-Deterrence. http://observer.com/2016/12/cybersecuritys-next-phase-cyber-deterrence/ (Erişim Tarihi: 05.01.2017).

DOĞRUL, M., A. Aslan ve E. Çelik. (2011). Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism. *Third International Conference on Cyber Conflict*.

ERMİŞ, U. (2015). Geleneksel Caydırıcılığın Siber Alanda Uygulanabilirliği Üzerine Bir İnceleme. https://siberbulten.com/makale-analiz/geleneksel-caydiricilik-kavramlarinin-siber-alanda-uygulanabilirligi-uzerine-bir-inceleme/ (Erişim Tarihi: 13.12.2016).

ERMİŞ, U. (2015). Siber Caydırıcılık: Teoriği Kolay, Pratiği Zor. https://siberbulten.com/makale-analiz/siber-caydiricilik-teorigi-kolay-pratigi-zor/ (Erişim Tarihi: 13.12.2016).

ERMİŞ, U. ve B. Özdal. (2013). Martin C. Lıbıckı'nin "Siber Caydırıcılık" Kavramının Nükleer Caydırıcılık Olgusu İle Karşılaştırılmalı Analizi. *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*.

GOODMAN, W. (2010). Cyber Deterrence: Tougher in Theory than in Practice?. *Strategic Studies Quarterly*.

GÜCÜYENER, A. (2016). 21. Yüzyılda "Siber" Rekabet: Yeni Hedef Kritik Altyapılar mı?. https://www.linkedin.com/pulse/21-y%C3%BCzy%C4%B1lda-siber-rekabet-yeni-hedef-kritik-m%C4%B1-ayhan-gucuyener (Erişim Tarihi: 11.12.2016).

GÜNTAY, V. (2015). Uluslararası İlişkiler Bağlamında Güvenlik Algısı Ve Siber Güvenlik; Akdeniz, Karadeniz ve Avrupa Bölgeleri Üzerine Bir Değerlendirme. *The Journal of Academic Social Science Studies*. Sayı 37.

HALEY, C. (2013). "A Theory of Cyber Deterrence", http://journal.georgetown.edu/a-theory-of-cyber-deterrence-christopher-haley/ (Erişim Tarihi: 13.12.2016).

HENNESSEY, S. (2016). Is US Cyber Deterrence Strategy More than (Russian) Roulette?. https://www.lawfareblog.com/us-cyber-deterrence-strategy-more-russian-roulette (Erişim Tarihi: 17.12.2016).

JENSEN, Eric T. (2012). Cyber Deterrence. *Emory Internatıonal Law Revıew*, Sayı 26.

KARA, M. (2013). *Siber Saldırılar - Siber Savaşlar Ve Etkileri*, Yüksek Lisans Tezi, İstanbul: Bilgi Üniversitesi.

KUGLER, Richard L. (2009). Deterrence of Cyber Attacks. http://ctnsp.dodlive.mil/ (Erişim Tarihi: 14.12.2016).

LUPOVICI, A. (2011). Cyber Warfare and Deterrence: Trends and Challenges in Research. *Military and Strategic Affairs*, Cilt 3. Sayı 3.

MARMON, W. (2011). Main Cyber Threats Now Coming From Governments As "State Actors". https://www.europeaninstitute.org/ (Erişim Tarihi: 15.12.2016).

MEHMETÇİK, H. (2011). 21. Yüzyıl İçin Caydırıcılık: Teori ve Pratikte Neler Değişti?. *Güvenlik Stratejileri*, Sayı 22.

MOWBRAY, Thomas J. (2010). Solution Architecture for Cyber Deterrence. *The SANS Institute*.

MUELLER, P. ve B. Yadegari. (2012). The Stuxnet Worm. https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf (Erişim Tarihi: 31.01.2017)

NAGORSKİ, A. (2010). Global Cyber Deterrence: Views From China, The U.S., Russia, India and Norway. *East- West Institute*.

NYE, Joseph S. (2015). Can Cyber Warfare Be Deterred?. https://www.project-syndicate.org/ (Erişim Tarihi: 21.12.2016).

ROJANSKY, M. (2016). Russia and America's Cyber Deterrence Dilemma. http://nationalinterest.org/ (Erişim Tarihi: 18.12.2016).

URGANCI, B. Caydırıcılık (Deterrent Policy). http://www.tuicakademi.org/ (Erişim Tarihi: 11.12.2016).

YILDIRIM, A. (2014). İnternetin Görünen Yüzü. *KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi*. Sayı 1.

YILDIRIM, G. (2016). Akıllı Çözümler Hackerların Iştahını Kabartıyor. http://aa.com.tr/tr/bilim-teknoloji/akilli-cozumler-hackerlarin-istahini-kabartiyor/670532 (Erişim Tarihi: 30.01.2017).

ISSN: 2587-1218

OPINIONS / YORUMLAR

ISSN: 2587-1218

SİBER ÇAĞDA ABD SEÇİMLERİ VE SİBER BİR MİT OLARAK TRUMP

Bilal SAMBUR[*]

Özet

Amerika'nın yeni başkanı Trump, bütün dünyada dikkatlerin üstünde odaklandığı kişi konumundadır. Seçim kampanyası sırasında Rusya'nın Trump lehine Demokratların seçim bilgilerini ve e-postalarını çalarak kamuoyuna sızdırdığı şeklindeki iddialar yoğun tartışmalara neden olmuştur. Rusya'nın siber yollardan Amerika seçimlerine müdahale ettiği iddiası, Amerika'da ve Batıda demokrasiye yönelik büyük bir tehdit olarak algılanmıştır. Rusya ile ilgili siber müdahale iddialarının yanında Trump'ın bizzat kendisinin demokrasi, Amerika ve dünya için tehdit olduğu algısı dünyada yaygınlaşmaktadır. Medyayı kendisine baş düşman ilan eden Trump, hayatı boyunca medya ile iç içe olmuş bir kişidir. Trump'ın büyük ölçüde medya ürünü bir kurgu olduğu açıktır. Trump ve medya karşılıklı olarak birbirini beslemektedir. Bugün artık Amerika politikaları için Beyaz Saray'ın açıklamalarına veya Kongre'nin faaliyetine bakmıyoruz. Dünya, artık Amerika politikalarını Trump'ın twitter hesabından yapmış olduğu paylaşımlara bakmaktadır. Trump, siber popülizm olarak ifade edebileceğimiz bir yolla kamuoyunun duygularına hitap ederek politikalarını ve söylemlerini yaygınlaştırmaktadır. Trump, karşımıza sadece Amerika Başkanı olarak değil, aynı zamanda siber bir mit olarak çıkmaktadır.

Anahtar Kelimeler: Trump, Siber Saldırılar, ABD Seçimleri, Siber Güvenlik, Medya.

US ELECTIONS IN THE CYBER AGE AND TRUMP AS A CYBERMYTH

Abstract

New U.S. President Donald Trump has became the most popular figure in the World today. During election campaign, it had been claimed that Russia intervened into the election centers through cyber attacks. Russian cyber attacks have been perceived as one of the most important threats against American democracy and its existence. Cybersecurity has became the key critical component of USA national security policies. Some people argue that America has cybersecurity problem, as well as Trump problem. Trump considers media as the chief enemy and main opposition party. Although Trump detests media too much, he has spent his whole life with media. It is not exaggeration to say that Trump himself is a media production, nothing more. Media and Trump mutually feed each other. One cannot be thought without the other. Now, the world is learning US policy from Trum's twitter

[*] Prof.Dr., Yıldırım Beyazıt Üniversitesi, Psikoloji Bölümü. bsambur@yahoo.co.uk adresinden ulaşılabilir.

account. Trump's way is the way of cyber populism. Trump spreads his ideas through the utilizing cyber means. Trump appears to be a global cyber myth, rather than a real politic figure.

Key Words: Trump, Cyber Attacks, US Elections, Cybersecurity, Media.

Giriş

Amerika Başkanlık seçimleri her açıdan dünyada yoğun tartışmalara neden olan bir süreç olmuştur. Seçim sürecinin başaktörü ve seçimin galibi hiç şüphesiz Trump'tır. Seçim kampanyası boyunca bütün dünyada ırkçı ve İslamofobik söylemleriyle gündem oluşturan Trump, galibiyetiyle ve başkanlık icraatlarıyla da gündem olmaya devam etmektedir.

Trump kadar tartışılan bir başka konu Amerika seçim sonuçlarının güvenliği ve güvenirliği sorunudur. Amerika'nin siber güvenliği ve adayların birbirlerine yönelik suçlamaları, seçim sonuçlarının güvenilirliğine dair yoğun tartışmaların yapılmasına neden olmuştur.

Rus hackerlerin Trump'ı desteklemek için siber müdahalede bulundukları iddiaları çok konuşulmaktadır. Amerika, seçim mekanizmalarına yönelik ileri sürülen siber saldırı iddiası yeni değildir. Değişik zamanlarda seçmen kayıtlarına yönelik birçok eyalette siber saldırıların olduğu hep ileri sürülmüştür. Şu anda hayatın her alanı gibi, seçim süreçleri de siber müdahalelerin ve saldırıların hedefi konumundadır.

Hackerler aracılığıyla Rusya'nın Amerika seçimlerine müdahale ettiği iddiaları, dünyanın en kurumsallaşmış demokrasisi sayılan Amerika'nın bile çok ciddi bir tehdit altında olduğunu göstermesi açısından çok kaygı verici bir gelişmedir. Birçok Amerikalı, Rusya'nın Amerika'nın sadece seçim sistemine değil, bir bütün olarak Amerika demokrasisine saldırıda bulunduğunu düşünmektedir.

Rusya'nın seçimlere yönelik siber saldırıda bulunduğu hadisesi, bir iddiadan öte çok önemli bir temele sahip bulunmaktadır. Obama yönetimi, değişik şekillerde Rus hükümetinin Demokrat Parti ve diğer siyasi organizasyonlara saldırılarda ve sızmalarda bulunduğunu ifade etmiştir. Rusların seçimlere siber saldırıda bulunduğu iddiasını, Watergate skandalının günümüzdeki bir versiyonu olarak değerlendirilebilir.

Kim(ler Siber Korsan?

Rusya'nın siber saldırılarla Trump lehine seçimlere müdahale ettiği iddiası, gerçekten çok ciddi bir gelişmedir. Amerika'da yüz yirmi milyon seçmenin oy kullandığı dikkate alınırsa, büyük bir demokratik seçim sürecinin gerçekleştiği görülmektedir. Her eyaletin kendi koyduğu kurallar ve

teknolojik araçlar olduğu dikkate alınırsa, seçimlere sonuçları değiştirecek bir siber saldırının zorluğu ortadadır.

Rusya'nın siber saldırılar yoluyla seçimlere müdahale ettiği iddiası, dünyanın en kurumsallaşmış demokrasisi sayılan Amerika'da Trump'ın seçim zaferinin demokratik meşruiyetinin sorgulanmasına neden olmuştur. Trump'ın seçim zaferinin demokratik meşruiyeti tartışılırken, aynı zamanda seçim alt yapısının yetersizliği, eskiyen teknoloji ve yeni teknik araçların etkin olarak kullanılmaması şeklinde sorunlar gündeme gelmiştir. Başka bir ifade ile, Rusya'nın siber saldırı iddiaları, Amerika seçim sisteminin siber güvenlik açısından bütünüyle radikal bir şekilde yenilenmesinin Amerikan demokrasisi için bir hayati ihtiyaç olarak hissedilmesini sağlamıştır.

Amerika seçim sisteminin siber teknolojik açıdan yenilenmesi acil bir ihtiyaç olarak görülmesine rağmen, Amerikan seçim teknolojisine müdahale etmenin sanıldığı kadar kolay olmadığının anlaşılması lazımdır. Demokratların seçim çalışmalarına birtakım sanal müdahaleler ve onların iç yazışmalarının dışarıya sızdırılması şeklinde birtakım gelişmeler yaşanmasına rağmen, bu durum Amerikan seçim sistemini etkisiz kılma anlamına gelmemektedir. Mevcut şartlarda Amerika seçim araçlarına siber saldırılar yoluyla müdahale etmek ve seçim sonuçlarını manipüle etmek mümkün gözükmemektedir. Bir partinin seçim merkezlerine sızma ile resmi seçim mekanizmasını manipüle etmek aynı şey değildir. Başkanlık seçiminde seçim sonuçlarını değiştirecek radikal bir siber saldırı veya müdahalenin gerçekleşmemiş olduğu görülmektedir. Amerika'da elli ayrı seçim merkezinin olduğu dikkate alınırsa bir siber korsanın seçim sonuçlarını bütün olarak değiştirecek bir manipülasyonda bulunması zor gözükmektedir. Eyaletlerin seçim güvenliği konusunda yetersiz kaldıkları hallerde federal yardım aldıklarını ayrıca not etmeliyiz.

Amerika seçim mekanizmalarını bütünüyle hackleyecek bir saldırı için büyük kaynakların ve büyük güçlerin olması gerekmektedir. Rusya'nın siber müdahalede bulunduğu söylemi, mevcut şartlar altında Amerika seçim sonuçlarının güvenilirliğini sorgulamaya yetmemektedir. Ancak burada asıl olan konu, Rusya'nın siber müdahale iddiasının boyutları değildir. Burada asıl sorun, bu iddianın Amerika gibi güçlü bir seçim geleneğine ve altyapısına sahip bir ülkede siber tehdit korkusunun ortaya çıkarmış olmasıdır.

Seçmen kayıt listelerine müdahalelerde bulunmak ve seçmenlere yönlendirici e-postalar atmak her zaman mümkündür. Yerel düzeyde siber saldırılarda bulunmanın daha kolay olduğu bir dönemdeyiz. Seçmen kayıtları ile dijital kayıtlar her zaman birbiriyle tam olarak uyuşmamaktadır. İnternet yaygınlaşmadan öncede siber saldırılar her zaman yapılmaktaydı. Fiziksel oylamanın yapılmadığı hallerde, dijital ortamda yapılan oylara hacklemelerin belirli ölçülerde mümkün olduğu ortaya çıkmış bulunmaktadır. Amerika seçimleri bağlamında yapılan siber müdahale iddiaları, hiçbir elektronik

sistemin yüzde yüz güvenli olduğu ve siber saldırıya dayanacağı anlamına gelmediğini göstermektedir. Bu durum bize seçim dahil hiçbir demokratik sürecin ve mekanizmanın siber tehdidin dışında olduğu şeklinde bir ayrıcalığa sahip olmadığını göstermektedir. Demokratik siyasetin üstünde siber tehdidin gölgesi karanlık bir bulut gibi dolaşmaktadır.

Amerika seçim sürecine siber yollardan müdahale eden güç olarak Putin ve Rusya gösterilmektedir. Putin'in Rus siber korsanlarını Amerika seçimlerini manipüle etmekle görevlendirdiği iddia edilmektedir. Amerika'nın güvenlik birimleri, Rusya'nın bu girişimini bir an önce durdurmasını talep etmişlerdir. Rusya Avrupa ve Asya'da değişik zamanlarda kamuoyunu etkilemek için siber müdahalelerde bulunmaktadır. Rusya, seçim sonuçlarını bütünüyle değiştirmek yerine, kamuoyunun algısını değiştirecek siber operasyonlarda bulunmayı daha etkili bir yol olarak değerlendirmektedir. Rusya gibi bir gücün siber müdahalelerine karşı Amerika yönetimi, eyaletlere siber güvenlik konusunda daha fazla federal yardımda bulunmayı gündemine almıştır. Rusya'nın tek başına Amerika seçim süreçlerine müdahale anlamına gelecek siber algı operasyonlarında bulunduğu iddiasını yüzde yüz doğrulamak mümkün değildir. Ancak Rusya'nın Suriye ve nükleer silahlar konusunda kendisine yakın bulduğu adayı, yani Trump'ı desteklediği ve Demokratların adayı Clinton'dan kurtulmak istediği bilinmeyen bir şey değildir. Rusya'nın yanında İran ve Çin'in de Demokratların seçim yazışmalarının kamuoyuna sızdırılmasında rol oynayabileceği ayrıca belirtilmektedir. Amerika, siber tehdidi esas alarak yeni bir düşman sıralaması yapmaktadır. Trump için en büyük siber düşman Çin, İran ve Rusya'dır. Obama yönetimi, siber düşman olarak Rusya'ya odaklaşırken Trump, siber tehdidin esas merkezinin Çin ve İran olduğunu düşünmektedir.

Siber İttifaklar Şart

Hiçbir devletin veya devlet dışı aktörün tek başına, siber bir güç oluşturması mümkün gözükmemektedir. Devletlerin veya devlet dışı aktörlerin işbirlikleri sayesinde siber saldırıların gerçek yıkıcı tehditler olarak algılanabileceği değerlendirmesi yapılmaktadır. Küresel sistem, gelecekte siber tehditlere karşı siber ittifaklar şeklinde ifade edebileceğimiz yeni bir çizgide şekillenmeye doğru gitmektedir. Ancak mevcut durumda Amerika gibi büyük bir güç, seçim sistemleri dahil bütün kritik altyapıların güvenliğinden endişe duymakta ve siber uzayda düşmanlarının kim olduğunu tam olarak bilmemenin korkusunu ve kaygısını yaşamaktadır.

Rusya, Çin veya İran'ın Amerika seçimlerine müdahale ettiği şeklindeki iddialar ve söylemler, Amerika demokrasisine ve açık seçim işleyişine olan güveni sarsmış durumdadır. Amerika'da yapılacak her seçim, bundan böyle tartışmalar, şüpheler ve soruların gölgesinde yapılacaktır. Amerika seçimlerinin hukuk ve şeffaflık içinde yapılıp yapılmadığına dair tartışmalar, bundan sonra her zamankinden daha fazla yoğunlaşacaktır.

Trump ve Yeni Dünya Düzeni

Tump'a destek anlamına gelecek her şey, bugün Amerika'yı ve demokrasisini itibarsızlaştırmaktadır. Trump, bugün Amerika'yı itibarsızlaştıran bir markanın adı olmuştur. Hiçbir Amerika başkanı, Trump kadar Amerika'yı dünyanın gözünde itibarsızlaştırmamış ve küresel bir tehdide dönüştürmemiştir.

Rusya'nın Demokrat Parti seçim merkezlerine siber müdahalede bulunduğu şeklindeki iddialarla gündeme gelen Trump, gerçekten sıradışı niteliklere sahip bir başkan görüntüsü vermektedir. Trump, her şeyden önce bilgiye, düşünceye, entelektüelliğe fazla önem vermeyen birisidir. Trump, medya üzerinden görüşlerini saldırgan, sığ, çatışmacı ve yıkıcı bir şekilde ifade eden ilkel bir Amerika milliyetçisi görüntüsü ortaya koymaktadır. Trump için tek gerçek, kendi inandıklarıdır. O, bütün dünyanın kendi inançlarını gerçek olarak kabul etmesini istemektedir. Trump konuşurken, ortaya bir fikir veya politika koymamaktadır. Trump, ortaya kendi inançlarını koymakta ve bunların tartışılmasını değil, kabul edilmesini beklemektedir. Trump'ın ortaya koyduğu ırkçı, İslamofobik ve göçmen karşıtı inançların, dünya kamuoyunda düşüncelerde, söylemlerde ve politikalarda niteliği ve derinliği arttıran bir katkısı olmamıştır. Trump, ırkçılığı, İslamofobiyi ve göçmen karşıtlığını dünya kamuoyunun gündemine yüzeysel, kontrol edilemez ve öngörülemeyen şekillerde getirmektedir.

Seçim kampanyası sırasında ırkçı, İslamofobik ve kamplaştırıcı söylemler kullanan Trump'ın başkan olduktan sonra eski söylemlerini bırakacağı, Amerika'nın ve dünyanın gerçekleriyle tanışacağı beklenmekteydi. Ancak seçimden sonraki süreçte ve başkan olduktan sonra da Trump'ın daha önce söylediklerini aynen tekrar ettiği ve söylemlerine uygun icraatlarda bulunduğu görülmektedir. Trump, söylediğini yapan kararlı başkan imajı vermeye çok özen göstermektedir. Trump, inançlarını değiştirecek bir karaktere benzememektedir. Bilakis Trump, dünyanın inançlarını değiştirmekle kendini görevli saymakta ve kafasına eseni söylemekten çekinmemektedir. Amerika ve dünyanın gerçeklerini umursamayan Trump, dünyaya ve Amerika'ya tek gerçeğin kendisi olduğunu dayatmaktadır. Trump, kendisi etrafında bir medyatik ve sibernetik mitin oluşumunu sağladıktan sonra, bu siber mitin siber gerçeklik olarak dünyada belirleyici olmasını hedeflemektedir.

Trump ve Medya

Trump, komple bir medya ürünüdür. Kendisi bir medya kurgusu olmasına rağmen, Trump, medyadan nefret etmektedir. Medyaya karşı savaş ilan eden Trump, gazetecileri en sahtekar kişiler olarak değerlendirmektedir. Trump, kendisi için muhalif olarak medyayı görmektedir. Medya ve siber araçlar üzerinden görüşlerini topluma ve dünyaya ulaştıran Trump'ın medyayı kendisine en büyük düşman olarak konumlandırması ilginçtir. Trump, medya karşıtlığını bir iletişim stratejisi olarak kullanarak, görüşlerinin kamuoyuna daha etkin bir şekilde ulaştırılmasını hedeflemektedir.

Trump, medya, siyaset ve diplomasi alanlarında agresif bir tutum takınmaktadır. Trump, herkesi kendisine rakip olarak görmekte ve onları bastırmak için saldırgan davranışlar göstermektedir.

Avustralya Başbakanının yüzüne telefonu kapatması, Trump'ın her alanda agresifliğini gösteren iyi bir örnektir. Trump, agresif olduğu kadar, düşünce ve ifade özgürlüğünü önemseyen biri de değildir. Ona göre medya, sadece dediklerini yazmalı, hiçbir şekilde eleştirel yayınlar yapmamalıdır.

Trump, başkanlık konuşmasında kendisiyle beraber iktidarın Washington'dan topluma devredildiğini ifade etmiştir. Trump, toplumu kullanarak kendisinin arkasında büyük bir sosyal desteğin olduğunu ifade etmeye çalışmaktadır. Toplumu tek referans aldığını söyleyen Trump için medya önemli değildir, önemli olan toplumla direkt ilişki kurmaktır. Trump, toplumla ilişki kurmak için twitter ve facebooku çok etkin bir şekilde kullanmaktadır.

Trump, yıllardır gayrimenkul zengini bir işadamı olarak medya üstünden bir imaj oluşturmaktadır. Medyada görünmek için her türlü fırsatı ve imkanı kullanan Trump, medya aracılığıyla kendisine ait bir imajın kurgulanmasını sağlamıştır. Trump, medya üzerinden kurgulanan *imajı* aracılığıyla politikada *mesajını* bütün topluma ulaştırmayı başarmıştır. Trump örneğinde öne çıkan, imaj ve mesajın bütünlüğüdür. Trump, imaj ve mesajın oluşumu ve aktarımı için gerekli olan araçları her zaman önünde hazır bulmuştur.

Bir Algı İnşacısı olarak Trump

Trump, kendi imajını ve mesajını gerçek olarak sunarken, onların taşıyıcısı olan medyayı ve sanal alemi ise yalan olarak sunmaktadır. Medyanın kendisi ve politikalarıyla ilgili gerçekleri ortaya koymasını şimdiden engellemeye yönelik bir stratejiyi uygulamaya koyan Trump'ın en büyük korkusu, imajının arkasındaki gerçek kişiliğinin ortaya çıkmasıdır. Trump, gerçeklerden çok rahatsız olan bir kişidir. Hayal dünyasını seven Trump, imajını ve mesajını sürekli olarak üretmenin çabasındadır.

Trump'ın medyayla olan kavgası, aslında kendi imajını ve mesajını üretme çabasıdır. Trump, bilişsel ve iletişimsel süreçleri ve araçları kullanarak Amerika ve dünya kamuoyunun dünyaya dair olan anlam haritalarını manipüle etmektedir. Hiçbir Amerika başkanının, Trump kadar, dünyanın anlam çerçevelerini negatif ve zayıflatıcı yönde etkilemediğini söyleyebiliriz. Trump, gerçekler ve veriler üzerinden politika yapma devrini kapatmış bir politikacıdır. O kitlelerin duygu dünyalarına temas eden büyük kurgusal anlatılar üzerinden politika yapmaktadır. Radikal İslami terörizm, göçmen düşmanlığı, Çin tehdidi, Amerika'yı tekrar büyük yapmak gibi anlatılar üzerinden popüler düzeyde var olan duygusal zafiyeti istismar ederek oluşturduğu anlam haritalarını manipüle ederek politika yapmaktadır. *Duygusal popülizm*, *duygusal politikaya* dönüşmüştür. Trump'ın imajı ve mesajı etrafında oluşturulan hikaye, kamuoyunun gerçek olaylarla olan bağını kesmekte, insanlar duygusallık temelinde demokrasi ve rasyonaliteye kör hale gelebilmektedirler.

İnsanlar, bugün günlük hayatlarının çoğunu sanal alemde geçirmektedirler. Sanal alem, insanları sanıldığının ötesinde duygularına mahkum hale getirmektedir. Siber uzay, bir duygular ve

duygusallıklar dünyasıdır. Trump, duygusal retorikle insanları ikna etmenin yolunu seçmektedir. Medyanın yalancılıktan başka bir alan olmadığı gibi argümanlarla kendi duygusal retoriğinin rasyonelliğini ve ikna edicilik düzeyini arttırmaya çalışmaktadır. Trump'ın duygusal popülist retoriği sayesinde haber ile uydurma olanı, gerçek ile kurguyu birbirinden ayırt edemeyen bir hale gelmiş bulunmaktayız. Trump hakkında söylenilen dedikodular, onunla ilgili gerçekliklerden daha fazla dünyanın gündemini işgal etmektedir.

İyi Bir Twitter Kullanıcısı Olarak Trump

Trump, tipik bir Amerikalının bütün özelliklerin taşımaktadır. Popüler ve medyatik bir isim olan Trump, büyük bir servete sahiptir. O, gayrimenkul alanındaki varlığıyla bilinmektedir. Zengin ve popüler bir isme sahip Amerikalı biri olarak Trump, Amerika'nın çıkarlarını her şeyin önüne koyma şeklinde tipik bir Amerika milliyetçiliği olarak ifade edebileceğimiz duygular, düşünceler ve niyetler taşımaktadır. Televizyon şovlarında boy gösteren Trump, bugün Beyaz Saray'da bütün dünyanın seyircisi oluğu bir şovu sergilemektedir. Trump, twitter hesabı üzerinden toplumla ve dünyayla doğal bir şekilde buluşan gerçek bir kişi imajı oluşturmaya çalışmaktadır.

Bütün dünya ve Amerika, Trump'ın twitter hesabı üzerinden yapacağı 140 karakterli paylaşımlara odaklanmış durumdadır. Trump, aslında twitter kullanımıyla doğallığını ve gerçekliğini değil, yapaylığını ve maskesini hepimize sergilemektedir. Twitter üstünden Trump'ın maskeli yüzünü bile dünya görmemektedir. Twitter'de bize yansıtılan 140 karakter üzerinden Trump'ın gerçekliğini, kendi kişisel yorumumuza göre değerlendiriyoruz. Trump, bize twitter üzerinden gerçekliği sunan bir kişi olarak değil, gerçeklikten kopuşu simgeleyen ve gerçekliği bozan bir figür konumundadır.

Trump, duygularıyla, sezgileriyle ve ihtiraslarıyla konuşan bir kişidir. Duygularının ve ihtiraslarının peşinden gitmesi ve bunlar yoluyla Amerika seçmeninin önemli bir bölümünü ikna etmesi, Trump'a Amerika başkanlığını getirmiştir. Sanal alemin duygular ve sezgiler dünyası olduğu gerçeğini iyi kavrayan Trump, kontrol edilemez, belirsiz ve kestirilemeyen bir kişilik profili sunmaktadır. Siber alemin en önemli özelliğinin orada hiçbir şeyin kontrol edilememesi, kestirilememesi, öngörülememesi ve güvenlikten yoksun oluşudur. Trump, siber uzayın bütün özelliklerini kendisinde ete bürüyen bir figür olarak dünyanın karşısındadır. Siber tehlikeler, hayatımızın her alanını tehdit ettiği gibi, siber bir mit olan Trump da dünyayla oynamakta ve tehdit etmektedir.

ISSN: 2587-1218

SİBER DÜNYADA DEMOKRASİNİN DÖNÜŞÜM İMKANLARI: YASAMA MECLİSLERİ ÖRNEĞİ

Davut ATEŞ[*]

Özet

Siber dünyada yaratılmış olan e-toplum ve e-devlet çağdaş demokratik siyasetin bildiğimiz konvansiyonel araçlarında önemli değişimler getirmeye gebedir. Özellikle temsili demokrasinin son birkaç yüzyıldır süren hükümranlığı siber teknolojilerin sunduğu imkanlar tarafından hiç olmadığı kadar tehdit edilmektedir. Demokratik uygulamalar temsil yerine daha fazla ‘‘doğrudan’’ biçimleri içerecek biçimde bir değişime zorlanmaktadır. Bu bağlamda tartışılması gereken en temel konulardan biri, temsili yasama meclislerinin günümüzün siber koşulları altında sahiden gerekli olup olmadığıdır. Bu analizde kısaca temsili demokrasiden doğrudan demokrasiye geçişi kolaylaştıran maddi altyapıyı hazırlamakta olan siber teknolojiler sayesinde modern demokrasinin abidesi konumundaki yasama meclislerinin her geçen gün meşruiyet kaybına uğramalarının ve nihayetinde ortadan kaldırılmalarının mümkün olduğu iddia edilmiştir. Çalışmanın amacı çağdaş demokrasilerde vazgeçilmez olan temsili karakterdeki mevcut yasama meclislerinin siber demokrasi döneminde tasfiyesine ilişkin muhtemel tedrici dönüşümün açıklanmasıdır.

Anahtar Sözcükler: Modern demokrasi, Siber teknolojiler, Yasama Meclisi, Doğrudan yasama.

POSSIBILITIES OF DEMOCRACY TRANSFORMATION IN CYBERWORLD: THE CASE OF LEGISLATION ASEMBLIES

Absract

E-state and and e-society created in current cyber world are to produce significant changes in conventional instruments of democratic politics. Particularly hegemony of representative democracy is being unprecedently challenged by advances provided by cyber technologies. Contemporary democratic practices are forced to transform into becoming more ‘‘direct’’ forms instead of representation. Within this context one of the important topic that should be debated is whether legislating assemblies are actually necessary or not under cyber conditions today. In this paper it is argued that legtimacy of legislating assemblies deemed as one indispensible of modern democracy is depreciating, which is going to lead even to their removal. The aim of the paper is to present some possibilities of gradual transformation and finally removal of legislating assemblies.

[*] Doç. Dr., Selçuk Üniversitesi Uluslararası İlişkiler Bölümü. Ulaşmak için davutates333@gmail.com

Key Words: Modern democracy, Cyber technologies, Legislation Assembly, Direct legislation.

Giriş

İletişim ve internet teknolojilerin son çeyrek yüzyılda yarattığı değişimler sonucunda gün geçmiyor ki ‘‘reel hayat’’ın bir bölümü daha ‘‘siber dünya’’ya (e-dünya, sanal dünya) devredilmemiş olsun. Haberleşme, bilgi, medya ve basın yayın, sosyal hayat, bankacılık, ticari ve mali işlemler, reklam, araştırma geliştirme, kamusal işlemler, eğitim bunlardan yalnızca bazılarıdır. Nihayet vatandaşın devletle olan işlemlerinin de neredeyse tamamının kısa süre içerisinde siber dünyaya aktarılması bekleniyor ki bunun altyapısını teşkil edecek olan e-devlet şimdiden faal durumdadır.

Peyderpey hayatın her bir alanını bünyesine katan siber dünyada demokrasinin nasıl işlevsel olacağı meselesi de genel gidişattan payını almaktadır. Eğer beşeri hayat siberleşiyorsa, bu gelişme kaçınılmaz olarak kamusal yönetim, yani devlet işlerinin, dolayısıyla demokrasinin de siberleşmesi sonucunu getirecektir. İçinde bulunduğumuz dönemde devlet işlerinin yalnızca vatandaşlık işlemlerinde bu noktada bir ilerleme kaydedilmiş bulunmakta, fakat önümüzdeki dönemde sadece vatandaşlık işleri değil, bizzat devletin kendisinin siberleşmesi, yönetim mekanizmalarının belirlenmesi ve bunların çalışma biçimlerinin yeni dünyaya uyum sağlaması gerekecektir.

Böyle bir gelişme büyük olasılıkla son birkaç yüzyıldır insanlığın alıştığı modern temsili demokrasinin ciddi bir gözden geçirmeye tabi tutulması sonucunu getirecektir. Devletin özüne ilişkin siberleşmenin temsili demokrasiyle bağlantılı biçimde gündeme gelmesinin en önemli nedeni tabi ki temsili demokrasinin oturduğu zeminin meşruiyetinin sorgulanacak olmasıdır. Bu kapsamda ilk ele alınması gereken konulardan biri elbette temsili yasama meclislerinin konumudur.

Siber Demokrasi ve Doğrudan Yasama

Doğrudan demokrasi yerine temsili demokrasinin modern dönemde bu kadar yaygınlaşması ve kabul görmesinin gerekçeleri üretilirken dayanılan noktalar bugün siber dünya tarafından

ortadan kaldırılmaktadır. ‘‘Neden temsil?’’ sorusuna karşılık öne sürülen ve herkesin zoraki kabullendiği gerekçeler, ülke coğrafyasının genişliği, nüfusun kalabalıklığı ve modern devlet işlerinin karmaşıklığı gibi oldukça ikna edici unsurlardı. Bu kadar geniş coğrafyalardan bu kadar kalabalık insan topluluklarının bir araya gelerek gündemi bir o kadar karmaşık devlet işlerini doğrudan yöntemlerle tartışıp bir sonuca ulaştırmaları imkansız olarak görülüyordu. Doğrudan demokrasinin modern topluma pek uygun bir yönetim şekli olmadığı sonucuna varmak hiç de zor değildi. Yönetim biçiminin demokrasi olması konusunda bir uzlaşı olacak ise işleri temsilcilere havale etmekten başka çıkar yol yoktu. Bu nedenlerle devletin en önemli iki organı olan yasama ve yürütme üyelerinin belirlenmesi amacıyla dönemsel seçimler yapılması ve seçilen temsilcilerin anayasal çerçeve içinde gerekli yasaları yapmaları ve devleti yönetmeleri uygun görülmüştü. Geniş kitleler bu gerekçelere ikna olmuş olacak ki, en azından birkaç yüzyıldır temsili demokrasi dünya üzerinde kabul gören bir yönetim şekli olmuştur.

Oysa bugün teknolojinin sunduğu imkanlar temsili demokrasiyi meşru kılan bütün gerekçeleri büyük ölçüde aşındırmaktadır. Günümüzde sosyal medya ağlarında milyonlarca insan bir araya gelebilmekte, birçok konuyu tartışıp bir sonuca vardırabilmektedir. Coğrafyanın genişliği ve nüfusun kalabalık olması artık temsili demokrasiyi meşrulaştıran zorluklar olmaktan çıkmış durumdadır. İnsanlar fiilen olmasa bile sanal ortamda toplanabilmektedir. Sayısal çokluk veya uzak mesafelerin dayattığı temsilci seçme zorunluluğu günümüzde büyük ölçüde aşınmıştır. Geriye yalnızca modern devlet işlerinin arz ettiği karmaşıklık kalmaktadır. Bunun herkes tarafından kolay anlaşılamayacağı, bu nedenle her bir insanın devlet işlerini ayrıntılı anlamaya çalışmak yerine anlama işini seçeceği temsilcilere devretmesi mecburiyeti bulunduğu ileri sürülebilir. Fakat bu karşı çıkış bile artık ikna edici olmaktan hızla uzaklaşmaktadır, çünkü yeni tasarlanan ve hayata geçirilen ‘‘akıllı makineler’’ ve bilgisayar programları sayesinde karşmaşık devlet işlerinin vatandaş için oldukça basite indirgenebileceği, böylece her bir vatandaşın temsilciye ihtiyaç duymadan devlet işleriyle ilgili neler yapması gerektiği konusunda bir fikre ulaşmasının hiç de zor olmadığı ortadadır. Bu kritik konuda bile yeni teknolojiler temsili demokrasiyi aşındırmaya devam edecek gibi görünmektedir.

Bu kapsamda cevabı aranması gereken en önemli sorulardan biri, siber dünyanın temsili demokrasinin öncelikle hangi unsurlarını gittikçe gereksizleştirdiğidir. Modern temsili demokrasilerde halk yasa yapma ve yönetme işlerini halletmek için iki ayrı temsilciler grubu

belirlemektedir. Yasa yapıcılar yasama meclislerini, yöneticiler ise yürütme erki diye tanımlanan hükümet veya kabineyi oluşturmaktadır. Yürütme erkinin siber demokrasi döneminde kısa vadede doğrudan halka devredilmesi ve temsili hükümetlerin sona erdirilmesi pek olası değildir. Elbette daha uzun vadede akıllı makinelerin yürütme işini üstlenmesi ve yönetimin sıfır hata ile yürütülmesi amacına matuf olmak üzere bu alanda beşeri temsilci belirlemenin gereksiz olacağı bir merhalenin gelmesi mümkündür. Böyle ileri bir aşamada yürütme işi de akıllı makineler yardımıyla doğrudan halk tarafından icra edilebilecektir.

Fakat içinde bulunduğumuz dönemde her geçen gün gereksizleşme süreci içinde görülen unsur temsili yasama meclisidir. Siber çağda demokratik yönetim biçimlerinde yasa yapmak üzere temsilciler belirlenmesi pratiği artık meşru zemininde gittikçe uzaklaşmaktadır. Her bir vatandaşın internete erişiminin bulunmaması, bir kısım vatandaşların bu yeni teknoloji konusunda yeterli bilgi seviyesine sahip olmaması ve ağ güvenliğinin henüz tam olarak sağlanamadığı noktalarından hareketle temsili yasama meclisleri belki bir süreliğine daha varlıklarını devam ettirebilir. Ancak kısa süre içerisinde bu gerekçelerin de ortadan kalkacağını öngörmek zor değildir. Zira siber alan dünyanın her bir noktasından erişilebilir konuma gelmekte, erişimin maliyeti gittikçe ucuzlamakta, hatta bazı ülkelerde ücresiz bulunmaktadır. Ayrıca bu yeni teknolojiye görece uzak kalacağı farz edilen yaşlı nesiller hiç beklenmediği biçimde sanal dünyaya uyum sağlamakta ve hızla yeni imkanları kullanmayı öğrenmektedir. Güvenlik önlemleri ise günden güne gelimekte ve daha güvenli bir sanal ortam geliştirilmektedir. Sanal ortamın yasama işinin doğrudan halka devredilebileceği güvenli bir araç olmadığı iddiası şimdilik kabul edilse bile, güvenlikle ilgili açıkların kısa süre içerisinde asgari düzeye indirilmesi mümkün görünmektedir. Bu konu belki de siber demokrasi dönemindeki güvenlik arayışlarının en önemli başlıklarından biri olacaktır. Halkın doğrudan yasa yapma sürecinin sanal ortamda hakerlar tarafından ele geçirilmesi riski tıpkı temsili sistemlerde yasama meclislerine karşı yapılan darbeler gibi değerlendirilebilir. Darbelerin önlenmesi için sistem ne tür önemler alıyorsa, buna paralel olarak sanal ortamda halkın iradesinin tecelli etmesini sağlayacak güvenlik önemlerinn de siber dünyada sağlanabilmesi gerekir.

Sahip olduğu bir kısım risklere rağmen, en azından yasama faaliyeti konusunda temsili demokrasiden doğrudan demokrasiye geçişin maddi imkanları mevcuttur. Bundan sonra yapılması gereken veya üzerinde düşünülmesi gereken husus, büyük olasılıkla bu geçişin teknik altyapısını sağlama meseleleridir. Bunun iki boyutu bulunmaktadır. *Birincisi* maddi

altyapıdır. Bir ülkedeki yetişkin bütün vatandaşların aynı platformda buluşmasını, görüş alışverişinde bulunmasını, gruplar oluşturmasını, öneriler sunulmasını, oylamalar yapılmasını sağlayacak imkan maddi altyapdı boyutunu ilgilendiren başlıca noktalardır. Esasında sosyal medya ağları bu alanda önenmli birer örnek olarak ortada durmaktadır. Bu ağların çalışma biçimleriyle e-devletin bilgi altyapısının (vatandaşlık kimliği ve e-imza gibi kritik bilgiler) birlikte ele alınmasıyla sanal ortamda gerçek bir ‘‘halk meclisi’’ oluşturulması mümkündür. Nüfusu birkaç milyon olan ülkelerde bu maddi altyapnınn oluşturulmasının daha kolay, nüfusu birkaç yüz milyon olan büyük ülkelerde ise biraz daha zor olacağı açıktır. Aslında buradaki kolaylık veya zorluk yalnızca sistemin merkezi işletim sisteminin hacmiyle ilgili bir konudur. Altyapının maddi boyutunun nasıl işler hale getirilebileceği konusunda bilgiyasar mühendisleri ve programcılarının yapacağı çalışmalar yol gösterici olacaktır.

İkincisi hukuki altyapıdır. Yetişkin bütün vatadaşların üye olduğu sanal ortamdaki halk meclisinin çalışma usul ve esasları bu kapsamdadır. Herhangi bir ülkedeki yasama meclisinin bir iç tüzüğü vardır. Burada meclisin çalışma usullerine ilişkin esaslar belirlenmiştir. Yasama meclisleri yaptığı bütün faaliyetlerde anayasaya paralel olarak söz konusu iç tüzüğe riayet etmek zorundadır. Sanal ortamdaki halk meclisinin de benzer bir çalışma tüzüğü olacaktır. Bu, mevcut temsili yasama meclisinin iç tüzüğünün halk meclisinin çalışma tüzüğü şeklinde güncellenmesi olarak da ele alınabilir. Yasa tekliflerinin en az kaç vatandaş tarafından verilmesi gerektiği, tekliflerin ne kadar askıda kalacağı, oylamanın nasıl ve hangi sürede yapılacağı, karar yeter sayısının ne olacağı, tekliflerle ilgili görüşmelerin nasıl yapılacağı, halk meclisinin gündeminin nasıl ve hangi orandaki çoğunluk tarafından belirleneceği gibi birçok nokta tıpkı meclis iç tüzüklerinde yapıldığı gibi belirlenebilir.

Günümüz koşulları dikkate alındığında maddi ve hukuki altyapının pek çok ülkede kısa süre içerisinde oluşturulması ve belirli bir geçiş dönemi neticesinde yasama faaliyetlerinin tamamının doğrudan halka devresilmesi olanağı bulunmaktadır. Hatta Avrupa Birliği’nin bazı kurumlarında yaygın biçimde uygulanmakta olan ‘‘vatandaş girişimi’’ bu alanda mini bir örnek olarak ele alınabilir. Özellikle batı Avrupa’daki gelişmiş liberal demokratik ülkelerin pek çoğunda yasama meclislerinin doğrudan halk meclisine evrilmesi sürecinin önümüzdeki orta vadede başlaması sürpriz olmayacaktır.

Yasama meclisinden halk meclisine dönüşümün ani ve keskin olmayacağı, bunun yerine yerel ölçekten ulusal ölçeğe doğru evrimi de içeren tedrici bir sürecin işleyeceği ileri sürülebilir.

Hatta bu evrim oldukça uzun bir geçiş dönemini kapsayabilir. Geçiş döneminin başlıca aşamaları aslında yasama meclisindeki yetkilerin parça parça doğrudan halk meclisine devri biçiminde gerçekleşecektir. Bu noktada dört ana evreden bahsetmek mümkündür:

1. Meclis gündeminin belirlenmesi. Yasama meclisi kanun yapmaya devam edecektir. Fakat hangi tekliflerin öncelikle görüşülmesi gerektiği hususunda nihai kararı verme yetkisi halka devredilebilir. Sanal imkanlar yoluyla halktan en çok sayıda oy alan tekliflerin mecliste öncelikle bir sonuca bağlanması zorunluluğu bulunur. Zaten birçok siyaset bilimci yasama meclisinin gündeminin belirlenmesinde halkın katılımının teşvik edilip edilmediği noktasını bir ülkedeki demokrasi seviyesiyle doğru orantılı olarak görür. Halk yasama meclisinin gündeminin belirlenmesine ne kadar etkin katılabiliyorsa, o ülkede demokrasinin iyi işlediği sonucu çıkarılır. Bu kapsamda siber dünya halkın yasama meclisinin gündeminin belirlenmesinde tek yetkili olmasına kısa vadede imkan verebilecek niteliktedir.

2. Yasa teklif yetkisinin devri. İkinci aşamada yasa teklifi getirme yetkisi halka devredilebilir. Yasama meclisi gelen tekliflerin kabulü veya reddi yönünde nihai kararı vermeye bir süreliğine daha devan eder, fakat yasa teklifi getirmez. Bunun yerine belirli sayıdaki vatandaşın katılımıyla ortaya çıkan girişimlerle halk hangi yasaya ihtiyacı olduğunu kendisi belirleyip, teklifi yasama meclisinin gündemine getirebilir. Buradaki kritik konu, yasama meclislerinin kanun teklifi yapma yetkisinin halka devredilmesidir. Siber dünya bunun için gerekli maddi altyapıyı kısa sürede hazırlayabilecektir.

3. Pilot yerel uygulamalar. Bu aşamada yerel ölçekteki meclis yetkileri doğrudan halka devredilebilir, hatta bu uygulama ulusal ölçek için pilot bir uygulama gibi ele alınabilir. Bir köyde, mahallede veya şehirde yerel meclisler yerine halk doğrudan yerel yönetimin yetki alanına giren konularda yasal düzenlemeyi kendisi yapabilir ki bu evre ulusal ölçeğe göre çok daha kısa vadede yaşanbilecek bir tecrübedir. Buradan yola çıkarak küresel düzeyde nüfusu daha az olan ülkelerde ulusal yasama meclislerinin yetkilerinin daha kısa vadede doğrudan halka devredilebileceği, oysa nüfusu daha kalabalık ülkelerde bu geçişin daha uzun bir dönemi gerektirebileceği sonucu da ortaya çıkar.

4. Tam egemen halk meclisinin tesisi. Son aşama ise halkın ulusal düzeyde yasa yapma yetkisini doğrudan kullanmasıdır. Bu evrede temsili yasama meclisleri artık tasfiye edilmiş olacaktır. Esasında bu durum hep ifade edilen ama her zaman belirli bir elit grubunun elinde

kalan ‘‘halk egemenliğinin sahiden inşa edilmesi’’ demektir. Nüfusun kalabalık ve coğrafyanın geniş olduğu gerekçeleriyle doğrudan demokrasi karşısında meşrulaştırılan temsili demokrasi böylece bazı alanlar itibariyle geride bırakılabilir. Muhtemeldir ki demokrasinin bu yüzyıldaki serüveninde halkın kendi temsilcilerinden esasen kendisine ait olan bir kısım yetkileri geri alması ve tedrici biçimde doğrudan demokrasiye geçişin hikayesi yazılacaktır.

Yasaları halkın doğrudan kendisi yapması, çağımızda temsili demokrasinin başka tür rejimlere dönüşmesi riskini büyük ölçüde izale edecektir. Çünkü temsilcilerin yaptığı yasaların pek çoğunun nihayetinde fiili oligarşinin ideolojik öncelikleri veya çıkarları ekseninde yapıldığı herkesçe malumdur. Üstelik toplumu kendi kendine yaşayan bir organizma gibi değerlendirirsek, yasa yapma işinde doğrudan demokrasiye başvurulması toplumun kendi tabii şartları içerisinde dönüşmesinin önünü açar. Oysa yasa yapma yetkisinin temsili meclislerde olduğu ve temsilcilerin seçim sistemlerinin kötüye kullanıma, manipülasyona ve propagandaya açık olduğu günümüzde, meclis çoğunluğuna güvenerek bir kısım kadroların kendi idealleri doğrultusunda toplumu zorla dönüştürme, toplumsal mühendislik uygulaması yapma imkanları mevcuttur. Toplumsal mühendislik, toplumsal organizmanın doğallığının bozulması, sonuçta birtakım ciddi çatışmaların ve sorunların ortaya çıkmasına zemin hazırlamaktadır. Bu bağlamda yasa yapma yetkisinin vekiller tarafından değil asıllar (halk) tarafından kullanılması temsili sistemde her zaman oluşmaya müsait oligarşilerin ortaya çıkış imkanlarını azaltacağı, böylece demokrasilerin temsilciler tarafından başka tür rejimlere dönüştürülme tehlikesini azaltacağı öngörülebilir.

Sonuç

Beşeri hayatın siber alana transfer edildiği bir ortamda, böylesi bir gelişmeden siyasal alanın muaf kalması olası değildir. Demokrasi de doğal olarak ‘‘siber demokrasi’’ haline gelecek ve alıştığımız bir kısım yol ve yöntemlerin kökten değişimiyle sonuçlanabilecektir. Nitekim son dönemde ortaya çıkan bir takım yeni sosyal hareketler tamamen sanal ortam merkezli biçimde organize olmakta ve harekete geçmektedir. Aslında siber ortamın siyasal sonuçlarının neler olabileceğine ilişkin yaşadığımız tecrübeler oldukça sınırlıdır. Fakat bu durum önümüzdeki dönemde siber dünyada siyasetin nasıl icra edileceği, özellikle de demokratikleşmenin hangi minvalde ivme kazanacağına ilişkin bazı öngörüler yapılmasına engel değildir.

Yüzyıllardır teknik gerekçelerle doğrudan demokrasiye karşı yüceltilmiş olan temsili demokrasi, siber teknolojinin gelişmesine paralel biçimde aslına, yani doğrudan demokrasiye dönüşme zorlamasıyla karşı karşıya kalmaktadır. Teknoloji gelişip vatandaşlar söz konusu teknolojiyi hayatın farklı alanlarında kullandıkça, siyasal alanda yasa yapmak üzere seçtikleri temsilcilerin halk adına doğru işler yaptıkları konusundaki şüpheler de artacaktır. Siber teknoloji siyasal alanda temsilcilerin meşruiyetini aşındırıcı ve azaltıcı bir işlev üstlenmektedir. Bu kapsamda teknik olarak halkın yasa yapmak üzere bir temsilciler grubu (meclis) seçmesinin gereksizliği daha fazla gün yüzüne çıkmaktadır. Vatandaşlar aynı anda aynı ortamda buluşabiliyorsa; sosyal, ticari ve eğlence amaçlı faaliyetlerin yanında kendilerinin tabi olacakları yasaları sanal ortamda kurulacak halk meclisinde yapma becerisini neden gösteremesinler ki?

ISSN: 2587-1218

ARTICLE AND BOOK REVIEWS / MAKALE VE KİTAP İNCELEMELERİ

ISSN: 2587-1218

Book Reviewed:

BY NAZLI CHOUCRI, CYBERPOLITICS IN INTERNATIONAL RELATIONS,

Cambridge : MIT Press, 2012, Paperback, $35.

Bilal SAMBUR*

Hayatımızın her alanının sanallaştığı, internetin bilgisayarlara hapsolan bir sanallık olmaktan çıkıp, hayatımızın kendisi olduğu bir dönem içindeyiz. Bizler hayatımıza ve kendimize dair her şeyi internete aktarma ve internette hayatımızı yaşama yarışı içindeyiz. İnsana dair her şeyin hızlı bir şekilde siber alemde dolaşıma sokulduğu günümüzde politika ve uluslararası ilişkilerin siber alem olgusunun dışında olması düşünülemez. Siber alem olgusu, politikayı ve uluslararası düzeydeki işleyişini teknik düzeyde belirlemenin ötesinde, bizzat politikanın ve uluslararası ilişkilerin muhtevasını değiştirici ve dönüştürücü bir dinamik durumuna gelmiştir.

Politika ve uluslararası ilişkilerin siber alem olgusu ışığında nasıl bir dönüşüm ve değişim içinde olduğu önümüzde büyük bir soru ve meydan okuma olarak durmaktadır. Nazlı Choucri'ye göre, geleneksel çerçevede politika veya uluslararası ilişkiler, artık yoktur; var olan artık siber politikadır ve siber uluslararası ilişkilerdir. Choucri'nin ortaya koyduğu çerçeve ışığında siber uzay olgusunun politikayı ve uluslararası ilişkileri tanımlayan temel güç olduğunu söyleyebiliriz. Ulusal güvenlik, küresel terörizm, savaş teknolojisi bütün kritik altyapıların işleyiş mekanizmaları ve karar alma süreçleri büyük ölçüde siber fenomen tarafından belirlenmekte ve tanımlanmaktadır.

Siber nitelikteki bir politikanın ve uluslararası ilişkilerin eskisi gibi olmayacağı açıktır, çünkü siber alan akıcı, anonim ve her yerde her zaman bulunma gibi özellikleri bulunmaktadır. Siber uzayın mistik olarak niteleyebileceğimiz akıcılığı, dinamizmi, zaman ve mekan sınırlarını aşan sınırsızlığı politika ve uluslararası ilişkiler alanında aktörlerin, tanımların ve teorilerin değişmesine neden olmuştur. Siber alemde, devletler hakim aktörler değildirler. Politikanın ve uluslararası ilişkilerin siberleşmesi olgusu, devletlerin, politikayı ve diplomasiyi belirleyen tek aktör olma şeklindeki ayrıcalıklı pozisyonlarını kaybetmelerine neden olmuştur. Choucri, geleneksel uluslararası ilişkiler ve politika yapma biçimleri ile siber uzay olgusunun birbirine nasıl entegre olacağı şeklindeki temel soruya ve meydan okumaya dikkatimizi çekmektedir.

Siber alemin akıcılığına, akışkanlığına, dinamizmine ve değişkenliğine uyum sağlama konusunda politika ve uluslararası ilişkiler alanının yeterince başarılı olmadığı görülmektedir. Siber alan

* Prof.Dr., Yıldırım Beyazıt Üniversitesi, Psikoloji Bölümü. bsambur@yahoo.co.uk adresinden ulaşılabilir.

olgusuna uymak yerine siber uzayla çatışmak ve onu kontrol altına almak suretiyle statükocu politika ve uluslararası yaklaşımların tekrarlandığı görülmektedir. Politika ve uluslararası ilişkiler, siber alem olgusuyla nasıl başa çıkacağını bilmemektedir. Choucri'nin ortaya koyduğu çerçeve ışığında politika ve uluslararası ilişkiler alanının siber alem karşısında bir panik, korku ve kaygı hali içinde olduğunu söyleyebiliriz. Siber aleme kendisini uyduramayan, siber olgu karşısında paniğe ve korkuya kapılan bir politikanın ve uluslararası ilişkiler yaklaşımın sürdürülebilir kalkınma modelini dünyada gerçekleştiremeyeceğini Choucri'nin kitabından öğreniyoruz.

Choucri, günümüzde insan, toplum ve devlet ilişkilerinde gelen değişiklikleri Yanal Baskı (Lateral Pressure) teorisiyle açıklamaktadır. İnsanların normalde içinde hareket ettikleri bir alanın olduğunu ifade eden Choucri, siber uzay sayesinde insanların ihtiyaçlarının, taleplerinin, arzularının büyük değişiklik gösterdiğini vurgulamaktadır. İnsanlar, artık bireysel ve toplumsal ihtiyaçlarını ve taleplerini normal çevre sınırları içinde değil, siber alemin genişleyen ve sınırsızlaşan alemi içinde ifade etmektedirler. Bireylerin sosyal ilişkilerini, Choucri'nin büyük değişkenler olarak ifade ettiği nüfus, teknoloji ve kaynaklar üçlüsü belirlemektedir.

Nüfus, teknoloji ve kaynaklar üçlüsü bireylerin sosyal etkileşimini ve aktivitesini belirlediği gibi, devletlerin profilini de belirlemektedir. Devletler, bireylerden ve toplumdan gelen talepler ile bu talepleri karşılamak için yeterli kapasiteye, kaynağa ve yeteneğe sahip olup olmama açmazıyla karşı karşıyadırlar. Devletler, bireylerin ve toplumların genişleyen taleplerini karşılamakta zorlandıkları gibi, uluslararası ilişkilerde de kolaylıkla tek yanlı olarak öteki devletin egemenlik alanına geçememektedirler. Choucri, uluslararası ilişkilerde tek yanlı olarak sorunlara çözüm bulma döneminin kapandığını, multi-lateralizmin yeni paradigma olarak karşımıza çıktığını söylemektedir. Siber alemde, hiç kimseye ait özerk bir alan bulunmamaktadır. Siber alan bireyin, devletin ve uluslararası ilişkilerin alanları iç içe geçmiş bulunmaktadır. Siber uzayın her bölgesi politika alanı haline gelmiştir. Hiçbir devlet profilinin, istikrarı ve güvenliği sağlamada, lateral baskıyı gidermede başarılı olamayacağını, Choucri'nin söz konusu çalışmasından çıkarsayacağımız bir başka önemli sonuçtur.

Choucri'nin kavramsallaştırmaları ve kurgulamaları, modern dünyada meydana gelen siber devrim ve sürdürülebilir kalkınma arasındaki ilişkiyi anlama konusunda çok önemli bakış açıları sunmaktadır. Choucri, siber alemde politika alanlarının iç içe geçmişliğinden hareketle işbirliği ve etkileşimi ön plana çıkarması önemli olmasına rağmen, siber alemin aynı zamanda rakip güçlerin kendisi için mücadele ettikleri bir iktidar alemi olduğunu unutmamak lazımdır. Siber alemde iktidar için mücadele eden güçler, siber savunma yöntemleri geliştirmekte ve devletler, süper devlet olmanın yolunun siber alemden geçtiğini fark etmişlerdir. Siber uzay, süper devletlerin, süper bireylerin ve süper grupların alanıdır.

Siber alan, gerçek varlıkların ve aktörlerin alemi değildir. Choucri, siber alemde imajlardan söz etmektedir. Siber alemin birinci imajını bireyler oluşturmaktadır. Siber dünyada internet kullanıcısı olarak yer alan birey, talep ve yetenekleriyle siber bir imaj olarak var olmaktadır. Siber uzayın ikinci imajı devlettir. Devlet, interneti regule etmek ve interneti kendi politikalarına hizmet etmek için çaba sarf eden ikinci siber imaj olarak siber alemde yer almaktadır. Siber alemin üçüncü imajı uluslararası organizasyonlar ve kuruluşlardır. Siber uzayda uluslararası kuruluşların ve yapıların üçüncü imaj olarak yer alması, devlet dışı aktörlerin ortaya çıkışını gösterdiği gibi, Amerika merkezli dünya sistemi modelinden uzaklaşma anlamına da gelmektedir. Siber alemin dördüncü imajı, bütün bu imajları kapsayan küresel sistemin tamamıdır. Dördüncü imaj, bireyin, devletlerin, devlet dışı aktörlerin çevre gibi büyük küresel sorunlar karşısındaki tutumlarını ortaya koyduğu için insanlığın ve dünyanın geleceğine dair farklı okumaları ve tahayyülleri , siber alemin bu dördüncü imajı üzerinden yapabiliriz.

Yirmi birinci yüzyılın problemleriyle başa çıkmak için siber politika, yeni bir yol olarak kullanılmaktadır. Choucri, siber politikayı anlamamıza yardımcı olan çok değerli bir kaynağı önümüze koymuştur. Devletler, artık politikalarını siber alemde finanse ettikleri siber aktivitelerle gerçekleştirmeye çalışmaktadırlar. Sert güç kullanımı ve savaş yoluyla gerçekleştirilmesi mümkün olmayan politik ideallerin ve amaçların, bugün siber aktiviteler yoluyla gerçekleşeceğine inanan devletler, siber alemdeki varlıklarını olabildiğince güçlendirmeye çalışmaktadırlar. Siber politika, herkesin politika yaptığı, ancak hiç kimsenin tek başına politik alanı kontrol edemediği, yönlendiremediği ve manipüle edemediği bir alandır. Devletler, interneti kontrol etmek için regülasyon birimleri kurmak şeklinde boş ve verimsiz bir çabanın içindedirler. Choucri'nin çalışması, siber alemin kontrol edilmezliği gerçeğini fark etmemizi sağlamaktadır. Choucri, politikanın ve diplomasinin, siber alemde dünyanın sonu gelmeyen dinamik ve yeni macerası olduğunu bize etkili bir şekilde tanıtmakla entelektüel dünyaya önemli bir katkıda bulunmuştur.

ISSN: 2587-1218

Article Reviewed:

BY NIR KSHETRI, CYBERSECURITY AND INTERNATIONAL RELATIOSN: THE U.S. ENGAGEMENT WITH CHINA AND RUSSIA, Buenos Aires, Argentina, 2014, Proc. FLACO-ISA Joint Conf.(FLACSO-ISA 14).

Durukan AYAN*

The article, "Cybersecurity and International Relations: The U.S. Engagement with China and Russia", by Nir Kshetri seeks to examine how formal treaties and frameworks as well as informal cooperation attempts influence the conflicts and divergences related to cybersecurity with bearing in mind organizational theory, game theory and international relations. Correspondingly, the U.S. relationships with Russia and China with regard to main cybersecurity topics, including the case of Edward Snowden, are exemplified. Following that, the article touches on different understandings and areas of disagreement about conception of the cybersecurity such as military, espionage and cybercrime dimensions. Above all, the research problem being addressed is whether informal institutions perform better than the formal ones in coping with international conflicts related to cyberspace.

Firstly, the article starts with comparison of formal treaties and ad hoc/informal mechanisms. It mainly argues that informal cooperation might be more effective than the formal treaties or frameworks in dealing with cyber conflicts. The reason behind this claim is pretty much based on the "flexibility" of informal or ad hoc cooperation methods. Following the suggestion of Lipson (1991, p. 500) as it is stated in the article "informal bargains are more flexible than treaties" since they are "willows, not oaks" and can be adapted to meet uncertain conditions and unpredictable shocks" (p. 8). Moreover this claim is supported with significant cybercrime examples to illustrate the success of informal practices on network-based cooperation.

The author includes some critical approaches on informal interactions as well. According to the critics informal networks depends on voluntary basis rather than compulsory and "engagement varies considerably across nations… informal cooperation is unlikely have a significant effect on domestic policy" (p. 8). This criticism demonstrates that informal

* Research Assist. in Department of International Relations, Afyon Kocatepe University and Graduate student in International Relations, Selçuk University Graduate School of Social Sciences, ayan.durukan@gmail.com.

cooperation is more likely to work in bilateral relations and it may accomplish a short term collaboration exclusive to the subject. However cybersecurity which is a multilateral matter requires extensive cooperation even if not at global or regional level. For this reason, formal treaties or frameworks seem more efficient to reduce the cybersecurity threats, perceptions and potential breaches. Moreover, based upon the examples which are given in the article it could be said that informal/ad hoc cooperation is quite likely to prevent cyber attacks targeting financial markets.

Secondly, the author refers to varied approaches of U.S. China and Russia regarding cooperation. With the exception of several cooperation attempts, ongoingness of the blame and counter blame circle on the cybersecurity dialogue between China and U.S. is underscored. Likewise, even though there was some uptrend in the past, the Russia-U.S. cooperation is excessively affected from the Snowden case. Having said that analysed relationships with regard to cybersecurity are mainly described on the basis of cybercrime. Furthermore, in relation to the Snowden case, the article attaches more importance to extradition concern of the U.S. rather than pointing out the distrust built by U.S. government's surveillance programs. The espionage here is evaluated as a one-sided matter and the rightful reactions and distrust of other countries are not taken into consideration decently. In respect to this, it is worth asking if cyber espionage activities are considered as legitimate acts of states in order to achieve national interests or such activities are considered legitimate as long as states act without being noticed. As a matter of fact the author specifies some worthwhile criticism about legitimacy mentioned as "strengthening" the critics' point of view: "U.S. is merely a victim and not a part of the problem, and that U.S. activities are legitimate, while those of some major economies are not" (p. 24).

Thirdly, it is being mentioned that "prior researchers have placed an emphasis on multidimensionality of security and multiple forms of security risks" (p. 18). In fact as the article gets close to conclusion, it indicates that formal treaties could be more effective rather than the informal ones. If cybersecurity should be taken as a multidimensional problem, then another question comes to mind in reference to the contributions of the aforementioned informal, ad hoc and considerably bilateral attempts. Accordingly, the most significant challenge observed from this article is addressing cybersecurity merely within the context of cybercrime.

Although cyberspace is a separate dimension, it is just another part of the reality and apart from reality it has no presence or importance. Therefore cybersecurity refers to nothing more than traditional security paradigms. Security concerns which increased with the cyberspace are directly related to national securities and the security of the international system or structure. When analyzed the existing conflicts in cyberspace, it could be seen that considerable amount of the cases are related to economic-based issues. For this reason as reported in the article, informal cooperation in suchlike security matters is more likely to be successful. Just because, as it was mentioned before, informal cooperation has more flexible practices over formal treaties.

Moreover, the game theory approach which stated in the article is worth to consider. According to this approach, interactions of the actors can be described as "infinitely repeated games" and "an outcome of such interactions is that over time, the actors are likely to expect regularities in behaviour. In this way, the bargaining processes among the game's actors lead to informal norms" (p. 24). In addition to that, "if the players' beliefs about each other's trustworthiness are confirmed by subsequent behaviour, there is a tendency of cooperative behaviour to enhance the prospects for successful further cooperation" (p. 25). Regularities in behaviour may lead to informal norms among the actors. But at the same time, it may cause deep-rooted conflicts if the behaviours regularly confront with one another. In regard to second quoted passage, it is quite true that there can be no realistic cooperation in the absence of trust-building measures. However it needs to be stated that, to be able to build mutual trust on cybersecurity undergoing economic, military, social and cultural distrusts need to be considered. The main reason for not being able to provide a realistic cooperation is that every state justifies only its own interests and preferences and disregards others' perspectives and viewpoints, as stated in the article (p. 30). Furthermore another important aspect is remarked in the article that there is a lack of ethical approach in cyberspace.

From the viewpoint of International Relations, it needs to be emphasised that while cybercrime is an important dimension, it is not the most noteworthy aspect of the cybersecurity. The foremost aspects of cybersecurity are, in my humble opinion, the threats perceived by states, cyber espionage programs, superiority of assault over defence and different types of cyberattacks mainly targeting critical infrastructures of the states such as DDoS attacks targeting governmental web resources of Estonia in 2007 and Georgia in 2008,

malware attacks just like STUXNET worm which possibly aims Iran's controversial nuclear facility in 2010, massive cyber assaults targeting electrical grid of Israel in 2016 and so on.

In brief, this article has a well written introduction and it starts with noting the failure of international formal agreements while informal cooperation is making some good progress. Later on the comparison of formal and informal cooperation is asserted fairly except that the success of informal cooperation is not clearly linked to cybercrime related conflicts. The examples, different approaches and criticism related to U.S. relations with Russia and China regarding cybersecurity matters are considerably extensive. Giving weight to the critical issues and areas of disagreement as a separate section and considering significant critical approaches makes this article valuable. Although there are some points worth to criticise on different points the article, when taken as a whole, is answering the questions which are asked above. Overall, this article is a favourable piece for the researches who wants to observe the cybersecurity issue with regard to relations between geopolitically significant economies.

ISSN: 2587-1218

For Authors / Yazarlar İçin

We would like to thank you for choosing to submit your paper to *Cyberpolitik*. In order to fasten the process of reviewing and publishing please take try to read and follow these notes in depth, as doing so will ensure your work matches the journal's requirements.

All works including research articles, comments and book reviews submitted to *Cyberpolitik* need to be original contributions and should not be under consideration for any other journal before and/or at the same time.

All submissions are to be made online via the Journal's e-mail address: cyberpolitik@gmail.com

The authors of a paper should include their full names, affiliations, postal addresses, telephone numbers and email addresses on the cover page of the manuscript. The email address of the author will be displayed in the article.

Articles should be **1.5-spaced** and with standard margins. All pages should be numbered consecutively. Please avoid breaking words at the end of lines.

The articles need to be between 5000 - 7000 words (including footnotes and references); comments between 2000-4000 words (including footnotes and references); and book - article reviews between 500 - 1500 words.

An abstract of up to 150 words should be added during the submission process, along with an average of five keywords.

Authors should make a final check of their article for content, style, proper names, quotations and references.

All images, pictures, maps, charts and graphs should be referred to as figures and numbered. Sources should be given in full for images, pictures, maps, tables and figures.

Comments in Cyberpolitic

A comment is a short evaluation of an expert regarding new issues and/or development in cyberpolitics.

Comments require journal's full reference style.

Book / article Reviews in Cyberpolitic

A book review should provide a fair but critical assessment of a recent (not older than 5 years) contribution to the scholarly literature on the themes and topics relevant to the journal.

A book review for Cyberpolitik:

- provides complete bibliographical references of the book(s) and articles to be reviewed.
- summarizes the content and purpose of the book, focusing on its main argument(s) and the theory, methodology and empirical evidence employed to make and support these arguments
- Critically assesses the author(s)' arguments, their persuasiveness and presentation, identifying the book's strengths and weaknesses
- presents a concluding statement that summarizes the review and indicates who might benefit most from reading the book

Book / article reviews should be preceded by full publication information, in the following form:

Education for Peace: Politics of Adopting and Mainstreaming Peace Education Programs in Post-Conflict Settings by Vanessa Tinker, Academica Press, 2015, $81.62 (Hardcover), ISBN 978-1680530070.

The reviewer's name, affiliation and email address should appear, on separate lines, at the top of the review, right after the bibliography of the book/article.

Journal style

Authors are responsible for ensuring that their manuscripts conform to *cyberpolitik*'s reference style.

Reference style of *Cyberpolitik* is based on APA 6th Edition.