ISSN: 2587-1218

CYBERPOLITIKJOURNAL

Siber Politikalar Dergisi

A Peer Review International E-Journal on Cyberpolitics and Cybersecurity

Volume 2, Number 4, Winter 2017

CYBERPOLITIKJOURNAL
Siber Politikalar Dergisi

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

www.cyberpolitikjournal.org

ABOUT THE JOURNAL

Owner/Sahibi

On behalf of Association for Human Rights Education / 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

The languages of the Journal are both Turkish and English.

ISSN 2587-1218

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

Indexing/Endeksler

Cyberpolitik Journal is being indexed by;

* Scientific Indexing Services (SIS) and.
* Eurasian Scientific Journal Index (ESJI).
* Academia Social Science Index (ASOS).
* Directory of Research Journal Indexing (DRJI).

Cover Design: Adem Bozkurt

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.

CONTENTS / İÇİNDEKİLER

EDITORIAL PREFACE

Dear Readers,

I am very pleased and proud to present and introduce the fourth issue of the *Cyberpolitik* Journal to you.

The cyberspace that has contributed our life in every field from day to day, from health to safety, to transportation from finance to scientific field, is gradually becoming widespread and developing. Cyber space has become a major revolution for humanity and the main source of knowledge. Scientific discussion and debate of such an important revolution has already begun and is proceeding at a very rapid pace. As a *Cyberpolitik* Journal, we will consider ourselves happy if we can contribute to this field. I would like to express that we are expecting the support and contribution of all scientists while making this contribution.

Just like every other area, there will be, and should be, people who make trade and enjoy the fun of this area and deal with its magazine. But also some others have to deal with the scientific dimensions of the cyberspace and inform and train the society.

We should be aware that Cyber space offers opportunities to facilitate and improve our life, as well as generates threats. We should also see the harms along with their blessings, and we must develop measures accordingly. For this reason, cybersecurity is very important and vital for all humanity. We have to argue and learn this without securitizing or making it a source of fear.

It is a fact that we will make more efforts in this matter if we know the fact that the user is the weakest link in cybersecurity. For this reason, a mobilization of awareness, information and training should be initiated in the society. This job is so important and comprehensive that it is should not be left to only technicians. Again, we will make more efforts in this regard if we know that the failure of cybersecurity is far more political than being technical. As long as politicians and decision-makers are unaware of this issue, it is difficult to reach a healthy and secure internet. For this reason, in addition to comprehensive and well-designed regulations and policies, highly educated and informed society will benefit more from the profits of cyberspace.

In this regard, all of us are responsible and have to accept our commitments. We hope this issue will serve this.

As in the previous issues, this number is also rich in terms of topics and content. This issue of Cyberpolitik involves many contemporary topics ranging from security to globalization, from theoretical approaches to the cases, to a series of scientific topics as well as deep web-dark web and virtual money such as Bitcoin. The interest of researchers in cyber, cyberpolitics and cybersecurity issues is increasing day by day, as developments in Information and Communication Technologies (ICT) penetrate in our life. We continue to accept publications that are original, diverse, innovative and disciplined. We predict and hope that these efforts will feed our readers' understanding of cyberpolitics, cybersecurity and human rights issues.

The most discussed problem/topic in this issue is cybersecurity. Due to the fact that cybersecurity is a political issue and at the same time it is a technical subject, it continues to be the most curious and debated issue due to its interesting nature. There are articles in this issue that discuss all these issues in detail in parallel with the controversy, such as cyber conflicts, cyber warfare, and cybersecurity that becoming a component of international security. In addition, articles cover some up-to-date issues that enrich and deepen debates such as human rights in national cybersecurity strategy documents, cybersecurity in education, deep web and Bitcoin. It will be healthier for us not to securitize cyberspace but to be aware of the threats at the same time. The topics discussed in this issue serve this purpose. It has been prepared without going away from science, but considering science principle for the society as well as science principle for the science.

I would like to remind you that all our readers are precious for us and that your feedbacks are important and valuable to us.

Nezir Akyeşilmen, PhD

Editor-in-Chief

RESEARCH ARTICLES / ARAŞTIRMA MAKALELERİ

SİBER UZAY VE GÜVENLİK POLİTİKASI ÜZERİNE TEORİK BİR YAKLAŞIM

Vahit GÜNTAY*

Özet

Siber güvenliğe ve siber uzaya olan ilgi her geçen gün artarken Uluslararası İlişkiler gibi alanlarda güç kavramının katettiği yol, siber alanda kendi bütünlüğüyle tartışılmaktadır. İki kutuplu yapıya dayanan Soğuk Savaş'ın bitişi, en azından zihinlerdeki sınırları kaldırırken çok yönlü ve daha dinamik bir güvenlik kavramını ortaya çıkarmıştır. Güvenliğin bile tanımı üzerinde kesin bir cümle kurulamazken siber güvenlik gibi bir kavramın saldırı-savunma stratejisi içinde değerlendirilmesi ya da politikalar oluşturulabilmesi oldukça düşündürücüdür. Güvenlik ikileminin beslendiği boyut teknolojik alandan ve gelişmelerden daha keskin şekilde etkilenmektedir ve küresel risk toplumunda siber politikalar artık daha karmaşık bir hal almıştır. Yaklaşımın çeşitliliği siber politikalar oluşturmada devletlerin elini güçlendirmektedir fakat güvenlik algısını da ortak bir barış kavramı içerisinde ütopik boyutlara taşımaktadır. Bu çalışmada siber güvenliğin algısal olarak yeni bir boyut kattığı Uluslararası İlişkiler disiplini farklı bir yönüyle irdelenmiştir. Yaklaşım oluşturmak oldukça zor bir husus olsa da çalışmanın kurgusu siber güvenlik ve uluslararası ilişkilere dair bir deneme niteliği taşımaktadır.

Anahtar Kelimeler: Siber Güvenlik, Uluslararası İlişkiler, Güvenlik İkilemi, Siber Uzay, Siber politikalar

A THEORETICAL APPROACH ABOUT CYBER SPACE AND SECURITY POLICY

Abstract

The interest about the cyber security and cyber space is increasing day by day and developing power concept is discussed with its own integrity in cyber area at International Relations discipline. After the Cold War with its bipolar system, borders were removed in minds and multiple security concept shaped with its more dynamic qualities. While it is not possible to make sentence about the concept of security, it is challenging to evaluate cyber security concept in offensive-defensive strategy or establish a policy. The dimension of the security dilemma is affected excessively by technological developments and cyberpolitics become more complicated in global risk society. The diversity of approach strengthens the states but it carries the security perception to utopic dimensions in the common peace concept. In this study, international relations discipline has been examined with its different aspect in which cyber

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

security added a new dimension as a perception. Also it is very problematic issue to construct an approach, the concept of the study is to try an essay about cyber security and International Relations.

Keywords: Cyber Security, International Relations, Security Dilemma, Cyber Space, Cyberpolitics

Giriş

Siber güvenliğe ilişkin gelişmeler günümüzde yeni bir çatışma alanı mı oluşturdu ya da yeni ufuklar mı açtı gibi soruların cevabını vermek oldukça zor fakat siber savaş kavramının tartışıldığı bir boyutu şekillendirmiştir dersek yanılmış olmayız. Teorik olarak uluslararası sistem açısından güvenlik yaklaşımlarında bir paradigma oluşturmak zordur. Özellikle yakın zaman itibariyle uluslararası alandaki tüm ilişkiler elbette çatışma veya savaş bağlamında gelişmemiştir fakat yaklaşım oluşturma zorluğu ya da siber güvenlik alanında sadece çatışmacı bir yaklaşımla uluslararası ilişkiler disiplininde bir arayış içerisinde olmak da mantıklı gözükmemektedir. Çünkü uluslararası sistem içerisindeki gelişim tek taraflı olarak devletler temelinde ele alınamaz. Bireysel ve toplumsal beklentiler de siber güvenlik alanındaki strateji düzeyini farklı alanlara taşıyacaktır.

Siber uzayda meydana gelen tüm gelişmeler ortaya çıkış mekanizması ve gelişimi itibariyle artık tespit edilebilir düzeydedir. Siber tehdidin kimleri nasıl etkilediği ya da ilgilendirdiği boyutu bir sorunsala sahiptir. Bireylerin ya da kurumların, şirketlerin tehdit içerisinde olduğu alan ile uluslararası aktörlerin tehdit içerisinde olduğu alan aynı teorik zeminde incelenemez. Bu konu sosyolojiyi, felsefeyi ve hatta psikolojiyi de ilgilendiren bir husustur. Büyük hasarlara yol açan bir siber saldırı bireysel bir etkinlik de olabilir ya da geniş ve planlı bir siber saldırıyı durduran, açığa çıkaran sadece bir birey olabilir. Bu paradoks dahilinde siber savaş gibi bir kavramı açıklığa kavuşturmak ve kesin bir tanımını yapmak oldukça zordur. Bu doğrultuda siber güvenliğe ilişkin güncel çalışmaların temeli bir yaklaşım denemesinin de ötesine geçememektedir. Hal böyle iken devletler üzerinden çıkarım yapmak ya da kesin sonuçlardan bahsetmek bir o kadar zorlaşmaktadır.

Siber tehditler evrilen bir forma sahiptir. Bu formun değişimi bağlı olduğu alanın genişlemesiyle ilgili bir durumdur. Soğuk Savaş sonrasındaki tehdit parametreleri değişince ve devletler siber uzaya bağlı hale geldikçe uluslararası ilişkiler düzeyindeki sorular da çeşitlenme imkanı bulmuştur. Teorik zemini oldukça zor tartışılan bu alan eldeki somut verilerle ve bazı gelişmelerle analiz de edilebilmektedir. Bu çalışma dahilinde bu sorulardan bir kaçına yanıt aranmaya çalışılmıştır. Zor olan, alana ilişkin siber güvenlik çerçevesi ele alınacaksa bunun hangi teorik temellerle tartışılacağı hususudur. Siber saldırılar kesin bir şekilde sonuçlandırılabilir mi ya da yapılan siber savaş tanımlarından yola çıkılarak bir siber barış ilan edilebilir mi gibi soruların değerlendirilmesi ciddi bir bakış açısına ihtiyaç duymaktadır. Artık uluslararası hukukun ilgi alanına girmiş olmanın da ötesine geçen siber alan hukuk normlarıyla da adından söz ettirmektedir.

Bu çalışma dahilinde uluslararası ilişkilerin bazı temel hususları siber uzay kavramıyla değerlendirilmiş ve bir yaklaşım denemesi ortaya konmuştur. Güvenlik ikileminin siber uzayda aşılması söz konusu mudur ya da siber silahlar ile uluslararası ilişkiler içindeki saf hali tartışma aritmetiğinin olasılığı üzerine bir çıkarım yapılmıştır. Uluslararası ilişkilerde güvenlik algısındaki değişim küresel risk toplumu ve güvenliğin bölgesel politikalara çekilmesiyle siber politikalara yakınlaştırılarak teorik bir deneme sergilenmiştir.

Uluslararası Güvenlikte Politika Üretme Sorunu

Uluslararası siyaset açısından güvenliğin içeriği, korunması gereken değerle birlikte üretilecek politikanın nasıl olması gerektiği sorusuna verilecek cevapla şekillenmektedir. Güvenlik açısından "*Kimin güvenliği?"* ya da "*Neyin güvenliği?"* sorularının cevabı güvenlik politikalarının temelini oluşturmaktadır. Güvenlik çalışmalarında bu soruların cevapları *devlet odaklı güvenlik* ya da *birey odaklı güvenlik* olması açısından iki temel yaklaşımı ortaya çıkarmıştır (Birdişli, 2016: 21).[1]

Devletin yaşamsal sınırları vardır ve bu sınırlar dahilinde uluslararası politikada aktör olma konumu güçlendirilerek güvenlik çerçevesi oluşturulmaktadır. Devlet odaklı güvenlikte var oluş ve bu varlığı devam ettirme adına kimi zaman başka devletlerdeki bireyler gözardı edilebilmekte, müdaheleler gerçekleştirilebilmekte ya da yaşanan olaylara sessiz kalınabilmektedir. Realist paradigmanın da sık sık atıf yaptığı bu durumla ilgili insan doğasının güvenilmezliği devlet odaklı güvenlik anlayışını güçlendirmektedir.

Yaşam hakkı, inanç özgürlüğü ya da mülkiyet hakkı gibi temel hak ve özgürlüklere ilişkin devletin güvenlik politikaları oluşturması ve bu politikaların merkezinde bireyin olmasına ilişkin görüşler ve çalışmalar da bir hayli fazlalaşmıştır. Siber güvenliğin içerdiği kavramsal çeşitlilikle birlikte birey-devlet ilişkisi, teknolojik gelişmelerle birlikte uluslararası yapılanmaların etkileşimi bu tartışmalar içerisinde politika üretiminde inşacı perspektifi ön plana çıkarmaktadır.

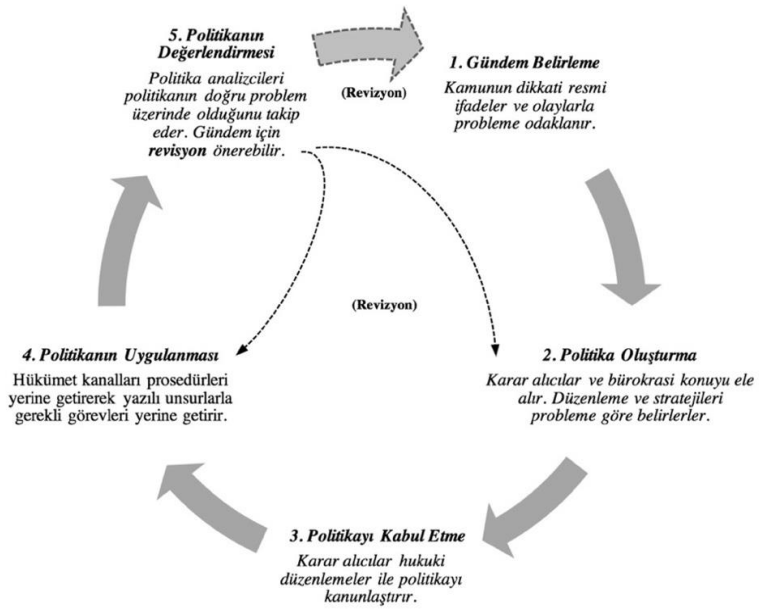
Uluslararası güvenlik açısından, devlet-birey-güvenlik üçgeninde karar alıcıların politika üretmesi ve bunun siber uzayda karşılık olarak çıkarsal bir döngü haline gelmesi, en az teorik yaklaşım kadar önemlidir ve ciddi bir birikim istemektedir. Bu durumu önemli kılan ise kimi zaman tehdit algısının ortaya çıkması ve doğru algılanması, kimi zaman ise çıkarsal bir durumun arzulanmasıdır. Sonuç olarak devletlerin varlık sebebi bu mücadelede üstün gelinmesidir.

[1] Farklı yaklaşımlar arasında *"siber güvenlik"* ve *"ulusal güvenlik"* gibi kavramların resmi dokümanlarda kullanılışında doğrudan bir kıyaslama yapılmaktan kaçınılmaktadır. Bunun sebebi "siber güvenlik" kavramının kabul edilen ortak bir tanımının olmayışıdır (Hathaway ve Klimburg, 2012:20).

Üretilecek politikaların teorik çerçevesi sosyal bilimler gibi alanlarda kurgusal olarak daha zordur ve oluşturulan politik çerçeve bir o kadar temel düzeyde kalmaktadır. Uluslararası güvenliğe ilişkin sergilenecek bir yaklaşımın temeli, uluslararası politikada teori oluşturulmasıyla benzerlikler gözetmektedir. Sönmezoğlu (2014: 94) teori oluşturmaya ilişkin başlıca üç noktayı şu şekilde tanımlamıştır:

- *Teoriyi oluşturan önerme ve genellemelerin birbirleri ile mantıklı ve tutarlı bir bağlantı içerisinde bulunmaları,*
- *Bu önerme ve genellemelerin olgularla bağlarının kurulabilmesi,*
- *Söz konusu önermelerin belirli ölçülerde betimleme, açıklama ve tahmin kapasitesine sahip olmaları gereği.*

Şekil 1. Politika Oluşturma Diyagramı



Kaynak: The Texas Politics Project, 2016

Uluslararası politika açısından yaklaşacak olursak siber savaşlar için de benzer bir teori oluşturma mantığından söz edebiliriz. Örgütler, bireyler, uluslararası kuruluşlar ve devletler düzeyindeki farklılık, analiz düzeyini inşacı teoriye yaklaştırmaktadır. Olayların siber uzayda kendi içerisindeki döngüsel ağı, politik bir düzlem oluştururken, teori oluşturma mantığıyla benzer işlemektedir (Sard, 2014:4). Bu noktada güvenlik ikileminin siber boyutta ne ifade ettiği, küresel risk toplumunda siber politikalar ve doğal olarak karşımıza çıkacak yeni güvenlik algısı çerçeveyi ana hatlarıyla anlamamıza yardımcı olacaktır.

Güvenlik İkileminin Siber Uzayda Aşılması

"Güvenlik İkilemi (security dilemma)"[2] kavramı hem Uluslararası İlişkiler disiplini, hem de karar alıcılar için üzerinde düşünülmesi gereken önemli bir hususdur. *Güvenlik ikilemi* en temel anlamıyla bir devletin başka devletten tehdit algılayıp silahlanması durumunda, bunu tehdit olarak algılayan devletin de aynı şekilde cevap vermesi anlamına gelmektedir. Karar alıcılar, güvenlik sorunlarını nasıl çözebilecekleri konusunda farklı seçeneklerle karşı karşıya kaldıkları sürece güvenlik ikilemi hep var olacaktır.[3]

Güvenlik kaygısını ortadan kaldırma adına yasa ya da yasal bir otorite olmadığı için devletler kendi güvenliklerini kendileri sağlamakta ve kimi zaman sorunun temeline ilişkin benzer ülkelerle ortak hareket etmektedir. Her devletin kendi bünyesinde alternatifler üretmesi ve silahlanma gibi benzeri adımlarla hareket etmesi güvenlik ikilemi açısından diğer devletin güvenliğinin de azalması anlamına gelmektedir. Güvenlik ikilemi bu noktada alana ilişkin paradoksların başında gelmektedir (Karabulut, 2015: 40).

Özellikle Soğuk Savaş sonrası dönemde *güvenlik ikilemi* kavramının gelişmesinde önemli parametreler vardır. Bunlardan ilki yeni güvenlik sorunlarının artan şekilde dünya siyasetini etkilemesidir. İkinci durum ise, sorunlar uluslararası ilişkiler disiplininin dünya politikasına bakışı, sorunları algılayışı ve tanımlayışında değişikliklere yol açmıştır (Bilgiç, 2012: 339). Özellikle silahlanma yarışı hız kesmeden yoluna devam ederken, siber güvenliğe ilişkin algı da devletleri birbirlerine karşı önlemler almalarına ve harcamaların artışına neden olmuştur (Tang, 2009: 590).

Dünya siyasetini meşgul eden siber güvenlik yeni olmasının yanında, güvenlik ikilemi açısından uluslararası ilişkiler disiplinine siber savaş olgusunu da eklemiştir. Savaş olgusu ise pratikte çoğu zaman birlikteliklere ve ortak güvenlik kaygısına sebep olmuştur. Devletler arasındaki siber mücadelenin boyutu da konvansiyonel mücadelenin temelindeki çatışma olgusuyla örtüşmeye başlamıştır ve devletler bu konuda saldırı unsurlarını geliştirme seçeneklerini masaya koymuştur.

Uluslararası alanda egemenlik tartışması sadece çatışmaların oluşması yönünde adımları getirmemektedir. Aynı zamanda statükoya ilişkin ortak çıkar halini de beraberinde getirmektedir. Devletlerin farkında olduğu şey anarşinin, statükonun dağılması durumunda kötüye gidişi cesaretlendirici etki yaptığıdır (Jervis, 1978: 167). Siber uzaydaki faaliyetler tam bu noktada söz konusu durumu teşvik edici niteliktedir. Siber uzayda güvenlik ikileminin geldiği nokta, gelişen her unsurun savaşa ve çatışmaya neden olabileceği yönündeki yaklaşımla daha çok örtüşmektedir.

---

[2] *Güvenlik ikilemi*, uluslararası ilişkiler terminolojisine John H. Herz'in yazdığı *Politik Realizm ve Politik İdealizm* kitabıyla girmiştir. Ayrıca yine aynı döneme ait Hurbert Butterfield'ın *Tarih ve İnsan İlişkileri* adlı kitabında da benzer bir durum farklı bir üslupla dile getirilmektedir.

[3] *Güvenlik ikilemi* kavramının ilk ortaya konuş biçimi, Soğuk Savaş döneminde disipline egemen olan realist düşüncenin öğelerini yansıtır. Öncelikle, güvenlik ikilemi kavramı devlet-merkezci bir yaklaşım dahilinde üretilmiştir.

Neden olunan çatışma, sadece çıkarsal veya egemenlik alanına ilişkin mücadelenin sonuçlarını birer çıktı olarak devletlere vermemektedir. Örneğin; 1998 yılında ortaya çıkan ve *Çernobil Virüsü* olarak da bilinen *CIH virüsü*, 1999 yılında etkin hale gelmiş ve birçok kullanıcının verilerini kaybetmesine yol açmıştır. 2000 yılında *Mellisa, Love Bug* ve *Killer Resume* gibi büyük mali kayıplara neden ola virüsler yine bu durumun çeşitliliğine ilişkin bir örnektir (Bayraktar, 2015: 155).[4]

Gelişen her unsur sahip olduğu altyapıyla birlikte devletlerin çıkar arzusunu körüklemektedir. Güvenlik ikileminin de temelinde bu durum vardır. Uluslararası ortamda güvenlik oluşturma adına caydırıcı olma, kendi sınırlarını aşıp çatışmaya dönüşmektedir (Booth, 2012: 481). Uluslararası düzenleme ve yasa koyucu olmadıkça şartlar daha da ağırlaşmaktadır. Konu kendi içerisinde döngüsel bir soruna dönüşmektedir. Şekil 2'de görüldüğü üzere A devletinden tehdit algılayan B devleti silahlanabilmekte, ittifaklara katılabilmekte ve siber mücadele içinde siber saldırı seçeneklerini kullanabilmektedir. Fakat B devletinin silahlanması bu kez A devletinin güvenlik kaygılarını ön plana çıkarmakta ve bu durumda A devleti de silahlanma kapasitesini artırmaktadır.[5]

Şekil 2. Ülkeler Arasındaki Güvenlik İkilemi Diyagramı

Kaynak: Krickovic, 2016: 116

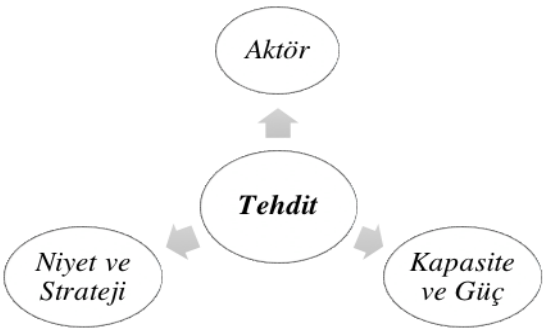
Küresel Risk Toplumunda Siber Politikalar

[4] Diğer bir husus ise siber uzayın toplum ve kitle hareketleri üzerindeki etkisini gösteren Facebook, Twitter, Youtube gibi sosyal paylaşım siteleri üzerinden yaşanan Arap Baharı örneğidir. Arap Baharı'nı *"Facebook Devrimi"* olarak nitelendiren ve Arap Baharı'nda sosyal medyanın gücü görüldükten sonra, siber uzayın politik gücünün önemli bir savaş yeteneği olduğunu niteleyenlerin sayısı oldukça fazladır.

[5] Türkiye ve Yunanistan'ın 1990'lı yıllar boyunca birbirlerine karşı silahlanmaları bir güvenlik ikilemi oluşturmuştur. Özellikle yakın coğrafyalarda sorunlar yaşayan devletlerin attıkları her adım belirli düzeylerde tehdit boyutu dahilinde algılanmaktadır.

Modernliğin beraberinde getirdiği çevresel, ekonomik ve güvenliğe ilişkin kimi riskleri konu alan *risk toplumu* yaklaşımı, riskin sosyolojik boyutunu inceleyen çalışmalar arasında önemli bir yere sahiptir. Modern toplumların birer risk toplumu haline dönüştükleri iddiasına ilişkin tartışmalar büyük oranda Çernobil'deki nükleer facia sonrasında alevlenmiştir (Elmas, 2013: 101).[6] Şekil 3'te görüldüğü üzere Soğuk Savaş döneminde tehdidin boyutları aktör, strateji ve güç arasında sıkışmışken günümüzde bu duruma öngörülemez tehditler de eklenmiş ve risk toplumu yaklaşımı açısından gelişmeleri olumsuz yönde etkilemiştir. Coğrafi olarak kırılganlıkların artışında risk toplumu yaklaşımıyla açıklanabilecek ciddi veriler vardır.[7] Risk toplumu açısından oluşturulacak politikalarda tehdidin çok yönlülüğü içerisine siber tehditler de yerleşmiştir.

Şekil 3. Soğuk Savaş Döneminde Tehdidin Üç Boyutu



Kaynak: Williams, 2005: 7.

Özellikle 11 Eylül 2001 tarihindeki İkiz Kulelere saldırı uluslararası güvenlik politikaları, toplumsal analizler açısından en az Soğuk Savaş'ın sona erdiği Berlin Duvarı'nın yıkılışı kadar önemli bir yere sahiptir. Alman sosyolog Ulrich Beck (2009: 157), ortaya attığı risk toplumu kavramı ile beraber küresel terörizm probleminin bu noktaya gelişinde Batı medeniyetinin teknoloji, ordu ve disiplin aracılığıyla Asya'dan Amerika'ya siyasi anlamda baskın bir rol izlemesinin önemli rol oynadığını düşünmektedir.

Teknoloji, ordu ve disiplin modern toplumların gündemine dahil ettiği siber güvenlik politikalarının yönünü değiştirmiştir. Sadece teknolojik gelişmelere ilişkin riskler değil, aynı zamanda uluslararası alanda yeni bir mücadele alanı olarak toplumların değişen riski haline gelen siber savaşlar kaygıları artırmıştır. Geçmişte yaşanan facialar bilinen haliyle kaza gibi görünse de, devletlerin ve farklı grupların kritik altyapılara müdahale edebilir yöndeki gelişmişlikleri ve olanaklar *küresel risk toplumu*

[6] Çernobil gibi kaza anında sebep olduğu yıkımlardan ziyade bu gibi teknoloji ürünü facialarının meydana getirdiği asıl problem, bilimsel otoritelerin geleceğe dair topluma inanılır cevaplar verememesi ve buna bağlı olarak da bireylerin gelecek yaşamlarının kendilerine ne getireceğini kestirememesinde yatmaktadır.

[7] Risk toplumu tartışmalarına ilişkin yaklaşımı sadece felaket toplumuna dönüşüm olarak algılamamak gerekir. Anthony Giddens (1998), bu duruma ilişkin şu tespiti yapmaktadır: *"Risk toplumu düşüncesi, dünyanın daha tehlikeli bir hal aldığını iddia ediyormuş gibi görünebilir, ancak bu gerçekte böyle değildir. Aksine bu, devamlı artan bir biçimde geleceği üzerine kendisini meşgul ederek risk düşüncesini ortaya çıkaran bir toplumdur."*

yaklaşımıyla örtüşmekte, teknik ve bilimsel ilerlemenin, bireyin hayatını daha da kolaylaştıracağı yönündeki savunma geri planda kalmaktadır.

Elmas (2013: 113) risk toplumunda belli risklerin gerçek olması durumunda ortaya çıkabilecek kimi felaketlerin varlığından bahsetmekte ve bu felaketlerin kontrol edilemeyen etkilerinin söz konusu olduğunu vurgulamaktadır. Bu durum risk toplumu yaklaşımının kaos ve anarşi dolu yeni bir toplum modeli ortaya koymaya çalıştığı şeklinde değerlendirilmemelidir. Bu yaklaşım modern sanayileşmenin ve modern teknolojilerin dolaylı olarak ve istemeden sebep olduğu etkilerinin, modern kurumlar tarafından kontrol edilememesi ve nasıl yönetileceğinin bilinememesi durumunu tartışmaya açmaktadır. Siber politikalar oluşturma ya da oluşturamama arasındaki itici güç de bir yönüyle buradan kaynak almaktadır.

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 (Erendor, 2016: 119). Bu açıdan bakıldığında siber politikalar oluşturulması ve uluslararası alanda etki doğurmasına ilişkin risk toplumunun algısal değişimi ve gelişimi önemli bir çerçeveyi oluşturmaktadır. Kritik altyapılara ilişkin oluşabilecek tehlikeli girişimler moderniteyi karşı bir silaha dönüştürebilir. Karar alıcıların algısal düzeyi ve gelecek vizyonu moderniteyle doğru orantılı şekilde yükselmelidir.[8]

Yeni Güvenlik Algısı ve Siber Uzay

Küreselleşme süreci ile birlikte güvenliğe yönelik tehditlerin farklılaşması yeni bir güvenlik tanımlamasını gerekli kılmıştır. Geleneksel tehdit algılamaları ve bu unsurlarla mücadele yöntemleri yeni güvenlik tehditleriyle mücadele konusunda yetersiz kalmaktadır. Bu yetersizlik yeni bir güvenlik tanımlamasının yanı sıra bu tanımlamadan hareketle yeni mücadele araçlarını da devreye sokmayı gerekli kılmaktadır (Karabulut, 2015: 119). Yeni mücadele araçları ise sadece fiziksel ya da sanal boyuttaki unsurları kapsamamaktadır. Toplumlar arasındaki hareketlenmeler ve çoğu zaman bu toplumlar arasındaki dini ve etnik farklılıklar dahi kapsam dâhilinde olabilmektedir.

Mücadele araçları içerisinde gelişimini ve farklılaşmasını hızla sürdüren siber saldırı araçları geleneksel tehdit anlayışını yeni güvenlik yaklaşımı içerisinde belirginleştirmiştir. NATO'nun tehdit tanımlamaları, ABD'nin özellikle siber güvenlik alanında vermiş olduğu öncelik ve yeni bir harekat alanı oluşturan

[8] Danışmanlık şirketi Marsh&McLennan'ın Davos Zirvesi için hazırladığı *"2016 Yılı Küresel Riskler Raporu"* çevresel sorunlardan zoraki göçe, enerji fiyatlarından siber saldırılara kadar birçok alanda dünyanın en riskli dönemini yaşadığını ortaya koymuştur. Raporda ilk kez; beş kategoriden dördü, yani çevresel, jeopolitik, toplumsal ve ekonomik riskler ilk beş en yüksek etkiye sahip riskler arasında yer almıştır. Teknolojik risklere de dikkat çekilirken, siber saldırıları kapsayan teknoloji riski hem gerçekleşme olasılığı hem de etkisi bakımından 11. sırada yer almıştır. Siber saldırılar, 27 ekonominin ilk beş riski arasında yer almaktadır.

siber savaş bu temel değişim içerisinde en somut tespitlerdir. 1990'lardan itibaren küreselleşme olgusunun hız kazanmasıyla *"artık hiç bir şey eskisi gibi olmayacak"* sözünü doğrularcasına, her alanda çok hızlı ve önüne geçilemez bir değişim süreci başlamıştır. Böylece önceki devirlerde benimsenen ekonomik, politik ve güvenlik stratejilerinin dayandırıldığı parametrelerin çoğunun sarsıldığı ya da ortadan kalkmaya yüz tuttuğu bir sürece girilmiştir. Bireyler arasında etkileşimin arttığı günümüzde politik alan farklı unsurlarıyla genişlemeye başlamıştır.

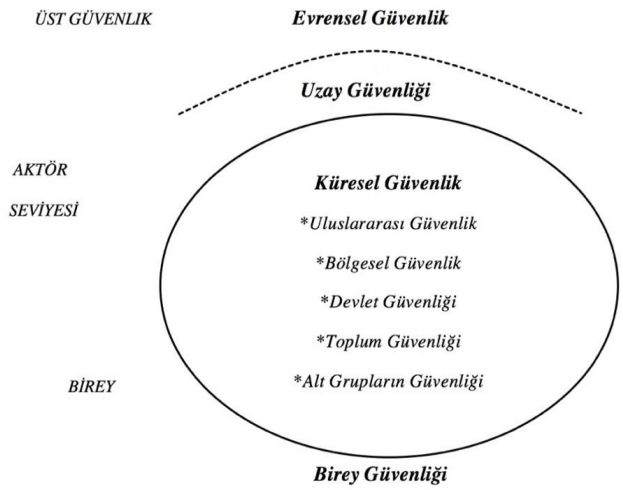
Soğuk Savaş sonrası dönemde küreselleşme sürecinin itici gücüyle tehdit olgusunda niceliksel bir artış, niteliksel boyutta bir çeşitlenme meydana gelmiştir. Bu yeni dönemde öncelikle askeri olduğu kadar ekonomik, sosyal, dini ya da kültürel, ideolojik, çevresel, toplumsal ve sağlıkla ilgili yeni tehdit unsurları ortaya çıkmıştır (Erdoğan, 2013: 269). Siber terör de bu boyutta etken bir araç olarak yerini almıştır.[9] Siber terörün kendi içerisindeki boyutsal nitelik ile uzayda yapılan çalışmalar, insanların sosyal hayatta yaşadıkları her yeri içerisine dahil etmiştir (Der Derian, 2009: 121).

Güvenliğin derinleşmesi ve genişlemesi, temel olarak güvenlik tehditlerinin çoğalmasıyla doğru orantılı bir süreçtir. Bunun yanı sıra tehditlerin küresel bir şekilde ele alınmasının gerekliliği, tehditlerin teknolojik gelişim ve küreselleşme gibi etmenlerle daha yaygın bir hale gelmesidir. Bu bağlamda güvenlik, küreselleşme ve teknoloji ilişkisini irdelemek gerekmektedir. Küreselleşme ve teknolojinin ortaya çıkardığı akışkanlık ve sınırların geçirgenliği, bireye ve devlete yönelik tehditlerin dozunu da artırmıştır (Aksu ve Turhan, 2012: 71).

Yeni güvenlik anlayışının siber güvenlik boyutu, Şekil 4'te görüldüğü üzere tüm güvenlik unsurlarının temelde, belirli verilere sahip olmasıyla da kapsayıcılık açısından en üst düzeyde yer almaktadır. Küresel güvenlik açısından ele alınan tüm unsurlar uzay boşluğunda teknolojik unsurlarla birbirlerine yakınlaştığı ölçüde siber teröre maruz kalabilecektir ve sorunsal alan daha da genişleyecektir. Verilerin artan bir hızla entegre edildiği siber alan kaygıları daha da artırmaktadır.

Şekil 4. Güvenliğin Katmanları

[9] Küreselleşmenin, dolayısıyla *kültürel emperyalizmin* aktörleri olarak algılanan gelişmiş ülkelere karşı gösterilen reaksiyonların belki de en basit örneği tek kişilik ordu konumuna gelebilmiş hackerların siber ortamda gerçekleştirdikleri saldırılar olmuştur.



Kaynak: Yılmaz, 2014: 12

Güvenliğin Bölgeselleşmesi ve Siber Politikalar Oluşturma

Bölgesellik ve güvenlik birbiriyle pek çok farklı şekilde ilişkilendirilebilmektedir. Özellikle Barry Buzan'ın (1991: 190), *"bir grup ülkenin temel güvenlik kaygılarının, gerçekçi bir şekilde birbirinden ayrı düşünülemeyecek kadar birbirine bağlanması"* şeklindeki tarifi özellikle siber güvenlik ve oluşturulacak politikalar açısından açıklayıcıdır. Bölgesel olarak çatışmalarda, devletlerarasındaki belirleyici faktörler siber politikaları etkilemektedir ve ittifak arayışında yakın coğrafyadan uzaklaşılmasını sağlamaktadır ki bu durum siber politikalar açısından çoğu zaman tehlikeli bu durumdur.

Özellikle kritik altyapılar açısından yakın coğrafyalardaki ülkelerin birbirine bağlılığı düşünülecek olursa ittfak arayışının ve siber politikalar oluşturmada güvenliğin bölgeselleşmesi farklı yaklaşımlar oluşturma gayesinde önem kazanacaktır. Bu yaklaşım ile ilgili olarak özellikle Türkiye gibi ülkelerin çevresindeki devletlerde, siber saldırılara ilişkin olay döngüsü, yakın coğrafyalardaki ortak samimiyeti gerekli kılmaktadır. Bunun temelindeki etken yakın coğrafyalar arasındaki hafızadır.

Şu ana kadar dünyanın farklı bölgelerinde oluşturulan bölgesel güvenlik çerçeveleri, Avrupa dışında gelişme aşamasındadır ya da başarıya ulaşamamıştır. Bundaki temel etken, devletlerin *Avrupa Birliği* yapılanmasına her yönden benzemeye çalışmasıdır. Avrupa'nın bu konudaki çıkarımı tarihsel olarak gergin ve savaşa eğilimli Almanya-Fransa çatışmasının tanımladığı güvenlik yapısını, bölgesel işbirliği ile savaşın artık çatışmaları çözebilmek için seçenek dahi olmadığı bir güvenlik topluluğuna dönüştürmüştür ve ciddi bir supranasyonal nitelik ortaya çıkmıştır (Hettne, 2012: 357).

Siber politikada çıktılar oluşturma adına genelde G-8, özelde ise bu çatı altındaki İngiltere, Fransa, Almanya, İtalya ile Japonya, Kanada, Rusya ve ABD arasındaki siber suçlarla olan mücadelede güvenliğin bölgeselleşmesi açısından eldeki veriler kayda değerdir. Yapılan toplantılarda, 1995 yılından beri bölgesel gelişmelerle birlikte siber suçlarla mücadele konusu ele alınmaktadır. Bu toplantılar

neticesinde çalışma grupları oluşturulmuş, siber suçlarla mücadelede eylem planları hazırlanmış ve faaliyete geçirilmiştir.

Diğer taraftan *Siber Savunma Politikası* hedefi altında NATO, siber saldırılara karşı önem teşkil eden tüm iletişim ve bilgi sistemlerinin korunmasını, ittifak üyelerine sağlamak için NATO yeteneğinin kuvvetlendirilmesi hususunda müdahalelerde bulunmuştur. NATO'nun en üst karar organı olan Kuzey Atlantik Konseyi, *Siber Savunma Programı*'nı desteklemektedir (Keleştemur, 2015: 440).[10]

Etkileşimin yoğunluğu siber politikalar oluşturma açısından güvenliğin bölgeselleşmesi adına karşımıza örneklerini verdiğimiz NATO gibi yapılanmalara benzer şekilde örgütlenme mantığını ve politikalar üretme gereğini karşımıza çıkarmaktadır. İttifak ve strateji oluşturma anlayışının oluşmasında yakın çevredeki gelişmeleri takip etme ve siber güvenlik adına bu gelişmeleri doğru okuyabilme, işbirliği oluşturulabilmesi adına daha kazançlı gözükmektedir. Siber alanda girişimler, günümüz gerçekliğinde rasyonel boyutlarda tartışılmalıdır.

Güvenliğin bölgeselleşmesi perspektifinden bölgesel işbirliği, bölgesel bütünleşme ve bölgesel birlik açısından ülke içi yapılanmalar da önemli bir yere sahiptir. Bölgeselleşme düzeyinin gevşek olduğu bölgesel işbirliğinde bu yapılanmalar sorunlara sebep olabilmektedir ve bu yüzden daha küçük, mikro yapılarda bölgesel birlikler daha da yapıcı kararlar alabilmektedir ve manevra yetenekleri daha kuvvetli olabilmektedir.

Sonuç Olarak

Uluslararası ilişkiler adına güvenlik en temel haliyle devletleri daha çok ilgilendiren bir husus gibi görünse de değişen dünya kavramı bu hususu temellerinden sarsmıştır. Bireyler ve devletlerin etkileşimi teknolojik gelişmelerle birlikte iç içe geçmiştir. Devlet odaklı düşünülen bir uluslararası ilişkiler perspektifi de bu konuda güvenlik algısının anlaşılmasını zorlaştırmaktadır. Çalışma içerisinde vurgulanan güvenlik ikilemi ve risk toplumu gibi kavramların tartışıldığı boyut çok yönlü ilişkiler ağında dikkat çekicidir. Her şeyden önce insan doğasındaki çatışma güdüsü ve bu doğaya güvenilmezlik her türlü aracın şiddete evrilmesi yönüyle önemli tespitlerdir.

Uluslararası güvenlik açısından, devlet-birey-güvenlik ilişkisi karar alıcıların adımlarında çıkar kavramını yine ön plana çıkarmaktadır. Siber uzay bu bağımlılığın çehresini genişletmiştir. Bu konuya ilişkin teorik bir yaklaşım sergilemede, olgusal bütünlüğün açıklanamayışı ciddi bir sorundur. Devletlerin varlık sebebinin mücadeleye dayandığı düşünülürse siber uzay oldukça karanlık ve tehlikeli bir seçenektir. *"Siber güvenlik"* kavramının içindeki güvenlik aslında savunma odaklı bir anlayışın

[10] NATO da tıpkı ülkeler gibi siber saldırılara maruz kalmaktadır. Özellikle yığın e-posta saldırıları, web sitelerinin çökmesine yönelik saldırılar ve NATO sunucularına karşı sürekli saldırılar düzenlenmektedir. Diğer taraftan NATO, siber casusluk faaliyetlerinin de artmakta olduğunu, bu konuyla ilgili olarak da savunma faaliyetlerinin artması ve güçlendirilmesi gerektiğini belirtmektedir.

ürünüdür. Siber alandan kendini koruma ya da en az zararla sorunları atlatma aslında kavramın bütünlüğü açısından daha açıklayıcıdır.

Uluslararası politika temelinde tanımının bütünlüğü yönüyle dahi zorlandığımız *siber savaş* gibi kavramlar hukukunun ve temellerinin belirlenemediği bir düzeydir. Güvenlik ikileminin siber boyutta ne ifade ettiği ya da küresel risk toplumunda siber politikaların uygulanabilirliği gibi hususlar konuya sadece bir yaklaşım sunabilmektedir. Siber güvenlikte teknik hususlarda kesin sonuçlar ve tanımlar karşımıza çıkarken siber politikalar üretmek ya da siyaset bilimi çerçevesinde analizler yapmak bir hayli zordur. Uluslararası alanda bir yasal otorite olmadığı için devletler kendi güvenliklerini sağlamada maliyetsiz ve daha az rahatsız edici seçeneklere yönelmektedir.

Dünya siyasetini meşgul eden siber güvenlik bireyler ve devletler adına cazip bir seçenektir ve amaç çıkar mücadelesi ise daha iyi bir seçenek de günümüz koşulları adına yoktur. Konvansiyonel ya da nükleer mücadeleye dayalı güç çarpışmaları yıkıcı etkilerini daha kesin şekillerde göstermektedir. Siber uzay bu konuda daha kapalı ve çoğu zaman da yıpratıcı tercihleri bizlere sunmaktadır. Aslında gelişen ve değişen her silah, şartlar devletlerin çıkar arzusunu körüklemektedir. Yeniliğin beraberinde getirdiği çevresel, ekonomik ve güvenliğe ilişkin sorunlar da siber güvenliğin çehresinde gerçekleşmektedir.

KAYNAKÇA

Aksu, Muharrem ve Turhan Faruk (2012), "Yeni Tehditler, Güvenliğin Genişleme Boyutları ve İnsani Güvenlik", *Uluslararası Alanya İşletme Fakültesi Dergisi,* 4(2), 69-80.

Bayraktar, Gökhan (2015), *Siber Savaş ve Ulusal Güvenlik Stratejisi,* İstanbul: Yeniyüzyıl Yayınları.

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

Bilgiç, Ali (2012), "Güvenlik İkilemini Yeniden Düşünmek: Güvenlik Çalışmalarında Yeni Bir Perspektif", Mustafa Aydın ve diğerleri (Ed.), *Uluslararası İlişkilerde Çatışmadan Güvenliğe,* 1. Baskı içinde (337-352), İstanbul: İstanbul Bilgi Üniversitesi Yayınları

Birdişli, Fikret (2016), *Teori ve Pratikte Uluslararası Güvenlik: Kavram-Teori-Uygulama,* Ankara: Seçkin Yayıncılık.

Booth, Ken (2014), *Dünya Güvenliği Kuramı*, (Çev. Çağdaş Üngör), İstanbul, Küre Yayınları.

Buzan, Barry (1991), *People, States & Fear: An Agenda For International Security Studies in the Post Cold War Era,* 2nd Ed., Hemel Hampstead: Harvester Wheatsheaf Publishing.

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

Der Derian, James (2009), *Critical Practices of International Theory Selected Essays,* New York: Routledge Publishing.

Elmas, M. Salih (2013), *Modern Toplumun Güvenlik Çıkmazı: Tehdit, Risk ve Risk Toplumu Perspektifinden Güvenlik,* Ankara: USAK Yayınları.

Erendor, Mehmet Emin (2016), "Risk Toplumu ve Refleksif Modernleşme Çerçevesinde Siber Terörizm: Tanımlama ve Tipoloji Sorunu", *Cyberpolitik Journal,* 1(1), 114-134.

Erdoğan, İbrahim (2013), "Küreselleşme Bağlamında Yeni Güvenlik Algısı", *Gazi Akademik Bakış Dergisi,* 6(12), 265-292.

Giddens, Anthony (1998), *Ulus Devlet ve Şiddet,* (Çev. Cumhur Atay), İstanbul: Kalkedon Yayınları.

Hathaway, Melissa E. ve Klimburg, Alexander (2012), "Preliminary Considerations: On national Cyber Security", Alexander Klimburg (Ed.), *National Cyber Security: Framework Manual,* 1. Baskı *içinde* (1-44), Tallinn: NATO CCD COE Publication.

Hettne, Björn (2012), "Teori ve Pratikte Güvenliğin Bölgeselleşmesi", Mustafa Aydın ve diğerleri (Ed.), *Uluslararası İlişkilerde Çatışmadan Güvenliğe,* 1. Baskı *içinde* (353-365), İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Jervis, Robert (1978), "Cooperation Under the Security Dilemma", *World Politics,* 30(2), 167-214.

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

Keleştemur, Atalay (2015), *Siber İstihbarat*, İstanbul: Level Kitap.

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.

Sard, Michael (2014), "Cyber-Politics: The Technological Arms Race between States and Citizens", *Eurasia Group,* https://www.pwc.com/jp/en/japan-knowledge/arch ive/assets/pdf/cyber-politics-1408.pdf (14.06.2016).

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

Tang, Shiping (2009), "The Security Dilemma: A Conceptual Analysis", *Security Studies,* 18(3), 587-623.

The Texas Politics Project (2016), "Policy Making and Policy Implementation", https://texaspolitics.utexas.edu/archive/html/bur/features/0303_01/policy.html (09.06.2016).

Williams, Michael (2005), *The Politics of Risk: The US, Europe and Proactive Security in the 21st Century,* http://citation.allacademic.com/meta/p_mla_apa_research_citation /0/7/1/0/6/pages71061/p71061-1.php (09.08.2016).

Yılmaz, Sait (2014), *Uzay Güvenliği,* İstanbul: Milenyum Yayınları.

KÜRESELLEŞME SÜRECİNDE DÖNÜŞEN GÜVENLİK ALGISI VE SİBER GÜVENLİK

Onur YILMAZ[*]

Özet

Küreselleşmeyle beraber güvenlik konusunda da çeşitli dönüşümler yaşanmıştır. Özellikle teknolojik gelişmelerle beraber dünya adeta küçük bir köye dönüşmüş, mesafelerin bir anlamı kalmamıştır. Teknolojideki bu değişim, bilgi kaynaklarının bağlantılı hale gelmesi, dünyadaki birçok devletin siber ortamda bütün hizmetleri sunması gibi nedenler güvenlik anlayışının da değişmesi gerektiğini ortaya koymaktadır. Artık güvenlik tehditlerine sadece devletler tarafından ve silahlı olarak değil; şirketler, terör örgütleri ve hatta bireyler tarafından da hem de siber uzay dediğimiz sanal alandan maruz kalınabilmektedir. Devletlerin siber güvenlik alanına karşı ilgileri gecikmiştir. Fakat özellikle Estonya, Gürcistan, NATO gibi devlet ve örgütlere yapılan saldırılar sonrası bu konu daha iyi anlaşılmıştır. Bu makalede siber güvenliğin ne olduğu ve güvenlik alanındaki değişimler, siber saldırı örnekleri üzerinden anlatılmaya çalışılmıştır.

Anahtar Kelimeler: Siber, Siber Güvenlik, Güvenliğin Dönüşümü, Siber Saldırılar, Küreselleşme.

Abstract

Along with globalization, there have been diverse transformations in security. The technology advancement in the world has transformed the globe into a miniature pie and this has lead to an absence of borders. The diverse change in technology reveals that the security accepts the change as the sources of facts become linked and almost every state in the world endeavors all services in cyber space. Regarding cybersecurity the states have been late in dealing with it. However, on the other hand it has shown to be better understood exclusively after the attacks on states and organizations such as Estonia, Georgia and NATO.

Within this context this work tries to explain what the cybersecurity is and the changes in the security patch through the examples of the cyber attacks.

Key Words: Cyber, Cybersecurity, Transition of Security Perception, Cyber Attacks, Globalization.

[*] Master Öğrencisi, Kocaeli Üniversitesi, İİBF-Uluslar arası İlişkiler Bölümü, E-mail: onrylmz1993@gmail.com

GİRİŞ

Küreselleşme ortaya çıktığı ilk andan itibaren hem olumlu hem olumsuz anlamda birçok gelişmeyi de beraberinde getirmiştir. Küreselleşmenin ne olduğu üzerine birçok tartışma bulunmasına rağmen; üzerinde mutabakat sağlanan nadir özelliklerinden biri yönü onun değiştirici ve dönüştürücü özellikleridir. Küreselleşme hayatın her yönünde ve her aktöründe bir değişim işlevi görmüştür ki bireyler, ekonomi, toplum, kültür, devletler ve sistemler de buna dâhildir. Diğer taraftan ekonomi, siyaset, toplum, kültür ve hatta bireylerin bu sürece uyum göstermesi ulus devletlere nispeten daha az sancılı olmuştur. Ulus devletler, küreselleşmenin kendilerine etkilerinin fazla olmayacağını, uluslararası alanda egemenliklerine bir tehdit doğurmayacağını düşünmüş olsalar da sonrasında ekonomik anlamda egemenlikleri çokuluslu şirketlerce; dış egemenlikleri uluslararası ve ulus ötesi örgütlerce; iç egemenlikleri sivil toplum örgütlerince müdahalelere konu olunca bu sefer de küreselleşme kavramına endişe ile yaklaşmışlardır.

Günümüzde ise küreselleşme sürecinin değiştirici ve dönüştürücü özelliklerinin yadsınamaz gerçekliği devletler tarafından da kabul edilmekte ve bu anlamda tespitler yapılmakta, olumsuz olabilecek etkileri anlamında ise önlemler alınmaktadır. Ulus devletlerin egemenlik, sınırsal belirlilik ve güvenlik üzerinde temellendiği düşünüldüğünde bu üç olgunun da küreselleşme ile değişime ve dönüşüme uğradığı bir gerçektir. Makalede ise bu üç olgudan küreselleşmenin güvenlik üzerinde oluşturduğu değişim ve bu değişimin bir parametresi olarak ortaya çıkan siber güvenlik üzerinde durulacaktır.

Bilindiği üzere Westphalia barışı sonrası ortaya çıkan yenidünya düzeninde sistemin yeni oyuncuları ulus devletler olmuş; dolayısıyla uluslararası sistem de bu aktörler üzerinden tanımlanıştır. Westphalian sistemin özünde ise realist bir okumanın olduğu aşikârdır. Nitekim güvenlik algılaması da bu anlamda realist bir algılamayla tanımlanmıştır. Buna göre güvenlik, devletlerin uluslararası alanda var olabilmeleri için olmazsa olmazdır. Öyleyse devletler somut güç araçlarını etkinleştirmeli, savunma ve saldırı kabiliyetlerini arttırmalıydılar. Güçlü bir askeri ordu aynı zamanda devletlerin uluslararası sistemde başat aktör olabilmeleri adına önemli bir unsur sayılmaktaydı. Sistemin temel aktörleri olarak ulus devletlerin görülmesi tehdit yaratabilecek unsurların da genel anlamda devlet odaklı olacağı düşüncesini

doğurmuştur. Fakat küreselleşmeyle birlikte bu güvenlik yaklaşımının pek de geçerli olmadığı görülmüştür. Realist paradigmanın yön verdiği, merkezi orduların güç potansiyelleriyle ve belirli sınırlar üzerinden algılandığı güvenlik olgusu da değişime uğramıştır. Çünkü artık sistemde sadece devletler değil, çokuluslu şirketler, ulus ötesi örgütler, küresel terör örgütleri, sivil toplum örgütleri gibi yeni yapılar ve yapılanmalar da var olmuştur.

Küreselleşmenin getirmiş olduğu birbirine bağlılık, bağlantılılık ve bağımlılık ilişkileri içerisinde dünya üzerinde var olan her şey birbiriyle ilişkili hale gelmektedir. Özellikle teknolojinin de gelişmesi ve yaygınlaşmasıyla birlikte bu bağlantılar mesafeleri engel tanımaksızın gelişmekte ve iç içe geçmektedir. Bilgisayar sistemleri, kodlama programları ve diğer dijital gelişmelerle saniyelerle ölçülebilecek kadar kısa süreler içerisinde bu bağlantıları kurma ve kurulan bağlantıları harekete geçirme imkânı da kolaylaşmıştır. Küreselleşmenin bütün bu olanakları sunmuş ve sunuyor olması da diğer taraftan devletleri güvenlik yönünden yeni bir tehlikeyle yüz yüze getirmektedir: Siber güvenlik.

Küreselleşme sonrası değişen güvenlik algılamaları paralelinde, küreselleşmenin ulus devletleri en çok zorladığı alanlardan biri de şüphesiz siber güvenlik alanı olmuştur. Çünkü hemen hemen bütün ulus devletlerde teknolojiyle birlikte bir dijitalleşme meydana gelmiştir ve bu dijitalleşmeden devletlerin bürokratik, ekonomik, politik ve hatta savunma sistemleri de payını almıştır. Yani artık devletler de hemen hemen birçok alanda ve kurumlarında dijitalleşmeyi gerçekleştirmişler, hizmetlerini çevrimiçi olarak sunmaya başlamışlardır. Bu durum yeni güvenlik tehditleri ortaya çıkarmıştır ki bu tehditlerin hepsi sadece devletler tarafından değil bireyler, şirketler, suç örgütleri, dolandırıcılar ve hatta küresel terör örgütleri tarafından yaratılmaktadır. Bu oluşumlarla mücadele etmenin yolu ise askeri anlamda ordular değil, siber alanda oluşturulacak olan siber ordular olarak düşünülmektedir. Siber güvenlik alanı devletlerin uzun bir süre kavrayamadıkları ve yeteri önemi vermedikleri bir alandır. Ancak siber saldırıların devletleri kilitleyebilecek duruma getirebileceğinin örnekleri görüldüğü zaman bu alanın ciddiyeti kavranabilmiştir.

ABD, Rusya, Çin ve NATO gibi güçlü yapıların dahi siber saldırılara maruz kaldığı düşünüldüğünde siber alandaki güvenlik okumalarının yeniden düşünülmesi gerektiği devletler tarafından da anlaşılmıştır. Yeni rekabet alanlarından biri olan siber uzay, hem devletlerin birbirleriyle yarışacağı hem de birbirlerinden, küresel terör örgütlerinden, suç

organizasyonlarından ve hatta bireylerden gelebilecek tehditleri bertaraf etmeleri gereken yeni bir durum yaratmaktadır.

Makalede öncelikle küreselleşme ile değişen güvenlik algısından bahsedilmiş ve bu anlamda yeni olan siber güvenlik alanı ve bu alana dâhil kavramsal çerçeveye yer verilmiştir. Daha sonra kavramların ve değişen güvenlik algısının devletlere ne gibi tehditler getirdiğinin anlaşılabilmesi adına siber alanda gerçekleşen önemli saldırılara örnekler verilmiştir. Devletlerin bu siber saldırılar sonrası güvenlik algılamalarında ne gibi değişikler olduğu üzerinde durulmuş, yeni güvenlik mekanizmaları ise bu başlıklar altında incelenmiştir.

Küreselleşmenin Güvenlik Üzerine Etkileri

Küreselleşme her ne kadar üzerinde mutabakata varılamamış bir kavram olarak belirse de, kabul edilen en önemli özelliği onun değiştirici ve dönüştürücü etkileridir. Bu etkisiyle de özellikle 1990 ve sonrası dönemde hızlı bir şekilde yoluna devam eden bu süreç klasik kabullerle şekillenmiş siyaset, ekonomi ve güvenlik tanımlamalarını, algılarını ve kavramsallaştırmalarını da değiştirmiş ve dönüştürmüştür. (Erdoğan, 2013: s. 266).

Küreselleşme süreciyle beraber güvenlik algılamasının nasıl değiştiği üzerinde durabilmek adına; klasik anlamda realizmin sınırlarını çizdiği güvenlik algısından bahsetmek gerekecektir. Realizmin klasik güvenlik kavramının özünü ve sınırlarını çizdiği açıktır. Klasik realist teoride güvenlik; devletlerin tekelinde ve anarşik olan uluslararası sistemde bir güvensizlik ortamında şekillenmektedir. Bu anlamda güvenlik kavramı bizatihi devletlerin sahip olduğu askeri güç ile orantılı ve büyük ölçüde bağlantılı olduğu düşünülmektedir. (Sandıklı ve Emeklier, 2014: s. 5). Bu anlamda kurulan Westphalian düzen de bu realist paradigma ekseninde, hem başat aktörlerin devlet olması hem de genel anlamda güç ilişkileri üzerinde temellenen bir sistem öngörmüştür. Fakat küreselleşmenin ortaya çıktığı dönemde ne devletler artık uluslararası arenada tek aktördürler ne de etkileme kapasiteleri askeri güçleriyle sınırlıdır.

Tüm alanlarda devleti egemen güç olarak gören realist paradigma özellikle uluslararası örgütler paralelinde ekonomik anlamda bu hakimiyetini sorgulatır hale gelmiş, daha sonra ulus ötesi (Aksoy, 2016: s. 3). Yapılanmalar baş gösterince siyaset yapmada, dış politika yapmada, iç politikada sınırsız bir egemenlikten taviz verir hale gelmiştir. Ekonomik, politik alanlardaki bu

değişimlerden güvenlik algısı da payını almıştır. Özellikle bir tehditle karşılaşıldığında, klasik realist çerçeveden bunun bir askeri çözümle halledilmesi gerektiği anlayışı yavaş yavaş terk edilmiştir. Çünkü tehdit kaynağının sadece bir diğer devlet olması durumu söz konusu değildir. Güvenlik artık sadece devletlerarası bir ilişki değil, daha çoğul ve çoklu bir görünüme evirilmiştir. Güvenlik alanındaki bu çeşitlenmenin kaynağında küreselleşmenin olduğu açıktır. Fakirlik, çevre sorunları, salgın hastalıklar, iç çatışmalar, soykırım, nükleer, radyolojik, biyolojik silahlar, küresel terörizm, uluslararası suçlar (Demiray ve İşcan, 2008: s. 155) gibi birçok yeni güvenlik sorunu devletlerin başa çıması ve vatandaşlarını koruması gereken diğer taraftan onun egemenliğini sorgulayan ve hatta sorgulatan bir sürece götürmüştür.

Küreselleşmenin en önemli özelliği; onun sınırları yumuşatma, belirginsizleştirme ve hatta birçok manada da birleştirmesidir. Özellikle teknolojik gelişmeler sonrası artık dünyanın her bölgesi, birbiriyle ilişkili ve etkileşimli hale gelmiştir. Bu manada devletlerin artık iç egemenlik-dış egemenlik alanları da belirginsizleşmiş, paralelinde iç güvenlik-dış güvenlik ayrımı da anlamını eskisine oranla yitirmiştir. Teknolojik gelişmelerle beraber her ne kadar devletler daha teknolojik ve yıpratıcı silahlar elde etmişlerse de bunları kullanma kabiliyetleri de eskisine oranla azalmıştır. Çünkü küreselleşmenin getirdiği bilgi yayılımı, bir devletin kazandığı askeri anlamda üstünlüğü diğerinin de takip etme ve aynısını kısa bir sürede kazanma-elde etme olasılığını arttırmıştır. Diğer taraftan bu teknolojik silahların kullanılmasının sınırlandırılmasına yönelik uluslararası toplum nezdinde antlaşmalar da imzalanmıştır. Böylece mesela; nükleer bir silaha sahip olmak devletler için her ne kadar daha güvenlikli hissedilmesini (Adaoğlu, 2008: s. 9) sağlasa da hem bunun birçok devlet tarafından kısa bir sürede edinilmesinden hem de 1925 Cenevre Protokolü uyarınca bu silahların kontrol altına alınmış olması bu manada kullanılmasının önünde engelleyici bir durum yaratmaktadır. Şüphesiz bunun altında yatan ana etmenlerden birisi de devletlerin özellikle bu alanda tek başına karar verme ya da gücü oranında bu silahları kullanabilme yetisini elinden alan; küreselleşme süreciyle etki alanı bulmuş olan sivil toplum örgütleri, insan hakları platformları gibi yeni aktörler olmuştur.

Yeni aktörlerden biri olan ve bu anlamda güvenlik dönüşümünün nasıl keskin olabileceğinin anlaşılması yönünden en iyi örneklerden biri de küresel terörizm ve küresel terörist örgütlerdir. Çünkü bu örgütler de artık hem nükleer silahlara sahip olabilmekte hem de bunları kullanarak küresel anlamda terör faaliyetleri uygulayabilmektedir. (Sancak, 2013: s. 130). 11 Eylül 2001 terör saldırıları küresel terör örgütlerinin, küresel faaliyetlerinin ulus devletlerin, Westphalian

güvenlik anlayışının yani realist güvenlik anlayışının eksik yönlerini daha doğrusu miladını doldurduğunu göstermesi açısından önemlidir. 11 Eylül saldırılarının Küreselleşmeyle bağlantılı bir noktada durmasının en önemli nedeni; saldırıyı gerçekleştiren örgütlerin oluşum süreçlerinde de küreselleşmenin getirdiği şartların yatmasıdır. Öyle ki küreselleşme; El-Kaide gibi terör örgütlerinin, terör faaliyetlerini yapmalarını kolaylaştırmıştır. Çünkü bu örgütler bilgi ve teknolojinin yaygınlaşmasıyla, uluslararası örgütleri taklit ederek kendi örgütsel şemalarını oluşturabilmekte, kuruldukları bölgenin çok çok uzağındaki yerlerle iletişim imkânlarını bulabilmekte, para aklama yöntemleriyle de kendilerine finansman sağlayabilmektedir. Özellikle küreselleşmeyle beraber çok küçük maliyetlerle, telekomünikasyon teknolojisi (Türköz, 2016: s. 154) yardımıyla da büyük tahribatlar yaratabilmektedirler. Sınırların eskisi kadar sert ve denetimli olmaması da bu durumu kolaylaştırmaktadır.

Küreselleşmenin bütün kolaylıklarından faydalanarak 11 Eylül gibi bir terör hareketi gerçekleştirebilen bir örgüt; devletlerin uluslararası alanda etkileme kabiliyeti olan tek aktör olmadığını, realist paradigmanın bu anlamda yanıldığını, dahası klasik anlamda güvenlik tanımlamalarının da artık geçerli olmadığını göstermiştir. Küreselleşmeyle beraber artık ülkeselliğin, tehditleri dışarıda tutma özelliğini yitirdiği gerçeğiyle karşı karşıya kalınması, güvenlik kavramının genişletilmesi ve yeniden düşünülmesi gerektiğini de gün yüzüne çıkarmıştır. (Ağır, 2011: s. 159).

Devletler, bu değişen güvenlik durumuna yeni önlemler getirmek gerektiği inancına varmış olsalar da küreselleşmenin getirdiği bir diğer olguyla da karşı karşıya kalmaktadırlar ki bu yeni güvenlik perspektifine de hazırlıklı olmadıkları bir gerçektir: Siber Güvenlik.

Siber İle İlgili Kavramlar

Siber politika ve siber güvenlik konuları, sosyal bilimlerde henüz hak ettiği değeri bulamadığından, bu alanda - giderek artsa bile - yapılan çalışma sayısı arzu edilenin çok gerisindedir. Bu nedenle, siber politika ile ilgili çalışmalarda hala kavramsal tartışma önem arz etmektedir. Bu makalede de başta siner olmak üzere, siber uzay, siber tehditler ve siber güvenlik gibi kavramların tartışılmasında yarar görülmüştür.

Siber Nedir?

Siber terimi; sibernetik kelime kökünden türetilmiş olup ilk olarak 1958 yılında canlılar ve makinalar arasındaki iletişim disiplinini inceleyen Sibernetik biliminin babası sayılan Louis Couffignal tarafından kullanılmıştır. (Sesli Sözlük, 2017). Yalnız güncel anlamda bu kavram kullanıldığında sanal alan ve bu alana ilişkin olarak anlaşılmaktadır.

Siber Uzay Nedir?

Siber Uzay, siber olana yönelik en geniş kavram olarak karşımıza çıkmaktadır. Çünkü siber uzay; bilgisayar ağları ve bu ağlar vasıtasıyla ulaşılabilen her türlü veri kaynağını kapsayan alan olarak tanımlanmaktadır. (Karaçay, ty: s. 1). Yani telefon, radyo, televizyon gibi elektronik olarak kumanda edilebilen her türlü cihaz, kayıt edilebilen ses ve görüntüler, grafikler, projeler, banka işlemleri, e-ticaret, e-devlet üzerinden yapılan her türlü işlem de ayrıca siber uzay tanımlamasına tabidir.

Siber uzaya yönelik bir diğer tanım ise ABD Savunma Bakanlığı tarafından yapılmıştır. Buna göre siber uzay; ‘‘İnternet iletişim ağları, gömülü işlemci ve kontrol birimlerini içeren, bilgi teknolojileri altyapılarından meydana gelen, bir birine bağlı ağların oluşturduğu bilgi ortamındaki bir küresel alandır.’’ (Ceylan, 2014: s. 1).

Her ne kadar siber uzay ya da siber ortam internetle birlikte ve bağlantılı bir kavram olarak düşünülse de, siber uzay internetten çok daha fazlasını ifade etmektedir. Çünkü gerçek dünyada meydana gelmeyen bir işlem dahi, siber uzayda meydana gelebilir kabiliyettedir. Örneğin basit bir çipteki hesaplama dahi bir siber uzay olayıdır ki bunun yapılması sırasında herhangi bir internet bağlantısı da gerekmemektedir. (Fentz, 2005: s. 1).

Bazı tanımlamalarda ise siber uzayda birer kullanıcı olarak cihazlardan cihazlara da bir iletişim ve etkileşim olabileceği anlaşılmaktadır. Fakat çalışmada bu tanımlamaları dikkate almamak durumunda kalınmaktadır çünkü çalışmada asıl olan insan amaçlarının siber uzaydaki etkileri ve sonuçlarıdır. (Ottis and Lornes, ty: s.1).

Siber Tehdit Nedir?

Kişisel ve kurumsal verilerin gizliliğini yasal olmayan şekillerde aşarak bunlara ulaşmak veya tahrip etmek amacıyla yapılan her türlü siber saldırı ve saldırı girişimine siber tehdit denir. Sunucu web servis hizmetlerini durdurma, virüsler veya trojenler bu tehditlere örnek olarak verilebilir. (Şahinaslan, 2003: s. 2-8).

Siber tehditler gelişen bilişim sistemleriyle beraber hem devlet hem de devlet dışı aktörler için; yeni tehditler ortaya çıkarmaktadır ki bu tehditlerin soyut alandan geliyor olması, tespit edilebilme özelliğinin az olması gibi etkenler, tehditlerin sonuçları açısından bir öngörülmezlik durumu doğurmaktadır. Bir diğer taraftan bu tehditlerin merkezi bir yapıya sahip olmaması da belirsizliğini arttırmaktadır. Bu anlamda tehdidin kaynağı tek bir birey (hacker); birey toplulukları (hacker grupları), terör örgütleri veya bizatihi devletler de olabilmektedir. (Kurnaz, 2016: s. 65).

Siber Tehdit Türleri

Teknolojik gelişmenin hızla artması ve küreselleşmeyle beraber, dünyada iletişim ve bağlantılılık yönünden çok sıkı bir ilişki söz konusu olmuştur. Bu durumun iyi yönleri olduğu gibi güvenlik alanında olduğu gibi tehlikeli bir durum da oluşabilmektedir. Siber saldırılar - fiziksel altyapıya yönelik saldırılar ve sosyal mühendislik dışında - genellikle internet üzerinden yapılan saldırılar olarak gerçekleşmektedir ki bunları şöyle sıralayabiliriz;

1) Bilgi ve istihbarat sağlama amacıyla kullanılan casus yazılımlar aracılığıyla yapılan saldırılar,
2) Portal ve internet hizmetinin aksatılması veya engellenmesine yönelik yapılan saldırılar,
3) Yemleme(phishing) olarak adlandırılan ve illegal yollardan yanıltma amacıyla yapılan saldırılar,
4) İstem dışı elektronik posta olarak adlandırılan Spam yöntemiyle zararlı dosyalar göndererek yapılan saldırılar,
5) Ağ trafiğini dinleyerek yapılan saldırılar, (Şahinaslan, 2003: s. 8).
6) Sosyal medya kullanarak yapılan saldırılar,
7) Sosyal Mühendislik,
8) Arama Motorları,
9) Ücretsiz Web Hizmeti Sunma.

Bu siber saldırı araçlarıyla etki yaratmak isteyen grupların temelde farklı hedefleri olmasına rağmen bu amaçlar aşağıdaki şekilde özetlenebilir;

1) Devletler genellikle düşman ya da hedef devleti, örgütü zayıflatmak, çökertmek, istihbarat sağlamak adına,
2) Siyasi örgütler kendi amaçları doğrultusunda toplumu manipüle etmek, propaganda amacıyla,
3) Kurum içi veya kurum dışı rakip ya da düşmanlar haksız rekabet araçlığıyla sektörde üstünlük sağlamak adına,
4) Suç örgütleri propaganda yapmak, ekonomik olarak finanse edilmek ve militan devşirmek amacıyla bu saldırıları gerçekleştirebilirler. (Çetinkaya, 2011: s. 1).

Peki, bu saldırılarla ne amaçlanmaktadır ya da neler yaşanabilir?

Telekomünikasyon şirketlerine sızılarak istihbarat sağlanabilir, özel bilgiler elde edilebilir, özel hayat ifşa edilebilir.

1) Nükleer tesislerde yangın çıkarılıp patlama yapılabilir.
2) Uçaklar havada çarpışabilir
3) Bankacılık sektörü tamamen işlemez hale getirilebilir.
4) Elektrikler kesintilerine sebebiyet verilebilir.
5) Sağlık bilgi sistemleri ele geçirilerek hasta kayıt bilgileri çalınabilir.
6) Hava yolları, hava ve deniz kontrolleri, demiryolları, otoyollar ve sinyalizasyon sistemleri gibi ulaşım sistemleri ele geçirilerek sistemin işleyişine müdahaleler gerçekleştirilebilir.
7) Medya kurumlarına yapılan müdahalelerle karşı propaganda içerikleri paylaşılabilir hatta ülkenin tamamen uluslararası toplumla iletişimi kesilebilir.

Bütün bu tehditlerin gerçekleştirilmesi ise son derece basit ve az maliyetli şekilde olabilmektedir. Dünyanın herhangi bir yerinde internete bağlı olunması koşuluyla bu saldırılardan birini gerçekleştirmek bugünkü teknolojiyle mümkün olmuştur. Bu nedenle devletlerin siber tehlikelerden kendilerini koruyabilmeleri için; kendi siber güvenlik alanlarını oluşturmaları bir zorunluluk halini almaktadır.

Siber Güvenlik Nedir?

Siber ortamda var olan bilişim sistemlerini saldırı ve tehditlerden korumak, bu ortamda korunmak istenen bilginin gizliliğini sağlamak, bu tehdit ve saldırıların mahiyetini ve kaynaklarını tespit etmek, bu müdahalelere karşı müdahaleler ve hamleler geliştirmek amacıyla oluşturulmuş olan ulusal hukuk, uluslararası hukuk ve insan haklarına uygun her türlü önlem ve sistemleri siber güvenlik olarak tanımlayabiliriz. (Kara, 2013: s. 5-6)
Bir diğer tanımlama yine paralellik göstermektedir. Buna göre siber güvenlik; siber uzayda kullanıcıların ve kurum-kuruluşların güvenliklerini sağlamak amacıyla kullanılan; araçlar, güvenlik politikaları, kılavuzlar, eğitimler, uygulamalar, güvenlik teminatları ve her türlü teknolojik altyapılanmadır. (Bilgi Teknolojileri ve İletişim Kurumu[BTK], 2008: s. 1-13).

Bu güvenlik önlemleri sayesinde, siber tehditler yok edilebilmekte yahut etkileri azaltılabilmektedir. Bu önleyici adımları atmak yakın zamanda hayati öneme haiz olmuştur. Çünkü siber saldırılar bir ülkedeki bütün hayatı durdurabilecek, felaketlere yol açabilecek mahiyette gerçekleşmektedir ki yakın zamanda Estonya'ya yapılan siber saldırı bu anlamda iyi bir örnek teşkil etmektedir. Tehditlerin hızlıca artarak güvenliği tehlikeye düşürmesi sonucu birçok devlet, güvenlik politikalarında siber güvenlik konusuna da yer vermek durumunda kalmışlardır. Bu anlamda devletler özellikle bu politikaları hayata geçirmek adına kalifiye kadroları oluşturma, altyapı hizmetlerini sağlamak gibi büyük yatırımlar yapmaktadırlar. (Yıldız, 2014: s. 58).

Görüldüğü üzere yeni güvenlik paradigmasına paralel olarak, siber güvenlik tanımlamalarının hiçbirinde somut anlamda ordulardan, silahlardan ve hatta diplomasiden bahsedilmemektedir. Buradan yola çıkarak yeni güvenlik algılamasının da devletler nezdinde anlaşılabilmesi adına bu perspektifi edinebilmeleri gerekmektedir. Güç olgularını sadece iyi, disiplinli, modern silahlarla donatılmış ordular üzerinden algılayan devletlerin, siber alandaki tehditlere göğüs geremeyecekleri de aşikârdır.

Devletlerin temel olarak siber alanında öncelikli olarak güvenliklerini sağlamaları gereken alanlar; bilişim, enerji, mali işler, gıda, sağlık, su, ulaşım, kamu güvenliği, savunma, nükleer-biyolojik ve kimyasal tesislerdir. (T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2012: s. 12). Özellikle savunma tesisleri ve araçlarında dışa bağımlı ülkeler adına, siber alanda tehlikeler de büyümektedir. Çünkü yeni savunma araçlarının hemen hemen hepsi siber alanda kontrol edilebilmekte ve bu anlamda kodlamalar üretici diğer ülke veya şirketlerin müdahalesiyle

yönlendirilebilmektedir. Bu anlamda özellikle kritik düzeydeki bu alanlarda milli teknolojilerin üretilip kullanılması temel öncelik olmalıdır.

Ulus devletler siber alanda birincil nitelikteki hedeflerden ilkini teşkil etmektedirler. Çünkü organize suç örgütlerinin siber alanda hareket kabiliyetleri artarken ulus devletlerin bu alanda görece yavaş kaldıkları görülmüştür. Her ne kadar bu terör organizasyonları bu alanda hareket kabiliyeti bulabiliyor olsalar da devlet kurumsallığı, istikrarı ve finansmanı gibi özelliklerden yoksun olmaları devletler tarafından avantaja çevrilebilir.

Her ne kadar siber alanda asıl hedeflerin ulus devletler, tehdit kaynaklarının da terör organizasyonları, suç örgütleri, bireysel dolandırıcılar olduklarını düşünsek de bu alanda devletlerin de birbirlerine rakip oldukları, üstünlük arayışı içinde oldukları da açık ve kesindir. Yakın zamanda siber saldırıların artması ve bu saldırıların devletleri işleyemez, yönetilemez duruma düşürebileceği gerçeğini ortaya koyması sonucu Birleşmiş Milletler, AB ve NATO gibi uluslararası örgütler de siber güvenlik alanında önlem almak durumunda kalmışlardır.

Eurastat tarafından yapılan araştırmaya göre AB üyesi ülkelerde internet kullanıcılarının siber alanda tehditle karşılaşma oranları %25 olarak gerçekleşmektedir. Bunun anlamı AB üyesi ülkelerdeki her dört kullanıcıdan biri güvenlik sorunlarıyla karşı karşıya gelmektedirler. Birlik içerisinde en fazla tehditle karşılaşan ülkeler %42, %39 ve %36 ile sırasıyla Hırvatistan, Macaristan ve Portekiz iken; en az tehditle karşılaşan ülkeler ise %10, %11 ve %13 ile sırasıyla Çek Cumhuriyeti, Hollanda ve Slovakya'dır. (Eren, 2017: s. 36). Bu araştırmadan da yola çıkarak AB'nin bu alanda politikalar geliştiriyor olması, güvenlik önlemleri alıyor olması da gayet doğal karşılanmaktadır.

2005 yılı Eylül ayı itibariyle de Avrupa Ağ ve bilgi Güvenliği Ajansı (ENISA) faaliyetlere başlamıştır. 2007 yılında ise Avrupa Polis Ofisi (EUROPOL) öncülüğünde ''Web'i Kontrol Et'' adında bir program başlatılmıştır. Yine 2010 yılında Avrupa Birliği Bakanları, kurulan siber güç ajansına gerekli teşviklerin sağlanması adına Komisyona çağrıda bulunmuştur. Avrupa Polis Ofisi e-dolandırıcılık, spam, botnet, internet üzerinden kimlik hırsızlığı, menkul kıymetler borsasında faaliyet gösteren hackerlar, yazılım yoluyla yöneltilen tehditler ve bazı cihazlardan kaynaklanan güvenlik eksiklikleri konusunda güvenlik önlemleri almakta, çeşitli sistemler oluşturmaya çalışmaktadırlar. AB idari birimleri tarafından bildirildiği üzere bu sistem ve çalışmaların maliyeti 750 milyar Euro'ya mal olmaktadır. (Yıldız, 2014: s. 93).

NATO ise özellikle 2000 yılından sonra siber tehditlere maruz kalınca bu alandan bir politika geliştirmek durumunda kalmıştır. Özellikle 1999 yılında NATO'nun Sırbistan müdahalesi sonrası Çin ve Rusya orijinli olduğu düşünülen siber saldırılar NATO'nun da bu tarz saldırılara karşı zayıf olduğu gerçeğini ortaya koymuştur. Bu münasebetle 2002 Prag Zirvesi'nde Siber Savunma Programı kabul edilmiş ve üye devletlerin ve NATO'nun bu tarz siber saldırılara karşı korunması gerektiği vurgulanmıştır. Mukabilinde Bilgisayar Olaylarına Müdahale Gücü Teknik Merkezi, Prag Yetenekler Taahhüdü, Kapsamlı Siyasi Yönerge gibi araçlarla bu alanda savunma teknikleri gerçekleştirilmeye çalışılmıştır. Estonya'ya yönelik yapılan siber saldırılar sonucu, ülkenin haftalarca yönetilemez hale gelmesi sonucu, NATO da siber güvenlik meselesini öncelikli risk alanı olarak kabul etmiştir. (Seren, 2006: s. 16-17).

Tüm bu adımlarla beraber NATO'nun amacı üye ülkelerde olası siber tehditlere karşı anında ve hızlı bir şekilde müdahale ederek, tehditleri bertaraf etmektir. Nitekim NATO gibi büyük bir askeri gücün, karar alma mekanizmaları açısından etkinliği uluslararası sistemde birçok devletten daha üstün nitelikteki yapısıyla üyelerine bu alanda da güvenlik sağlaması beklenen bir durumdur.

Güvenlik kavramının bu derecede değiştiği, dönüştüğü bir ortamda ulus devletlerin de bu alanda varlıklarını sürdürebilmeleri adına, adapte olabilme kabiliyetleri son derecede önem arz etmektedir. Realist paradigmanın önceledığı manada bir güvenlik algılamasının tek başına yeterli olmadığı bu gelişmeler karşısında devletlerin egemenliklerini kanıtlamaları gereken yeni bir alan olmuştur siber uzay…

DÜNYA'DA SİBER SALDIRI ÖRNEKLERİ

Siber güvenlik saldırılarına gerçekleşmiş örnekler üzerinden yaklaşmak hem konunun anlaşılması adına, hem de güvenlik sorunsalının ne denli tehlikeli olabileceğini kavramak açısından son derece önemlidir. Bu anlamda bir siber savaş durumunun yaşandığı olaylar da mevcuttur ki bu savaşların hiçbiri realist paradigmada öngörüldüğü üzere askeri ordularla yapılmamaktadır.

Bu da bizlere göstermektedir ki yeni güvenlik anlayışı, yeni güvenlik önlemleri yaratılması gereken bir mahiyettedir. Aksi takdirde, aşağıda örneklerini göreceğimiz şekilde vahim sonuçlarla karşılaşılabilir, normal hayatın seyri beklenilmedik müdahalelere maruz kalabilir ve devletlerin yönetme kabiliyetleri dahi elinden alınabilir.

Siber saldırılar elbette sadece devletlerarasında gerçekleşmemektedir. Çok taraflı saldırıların gerçekleştiği bir alan olarak siber alanın aktörleri bireyler, terör örgütleri, aktivist örgütlenmeler ve devletler olabilmektedir. Diğer taraftan bu grupların da birbirleriyle sürekli etkileşim içerisinde oldukları gözlemlenebilmektedir. Yani devlet gibi bürokratik ve merkezi yapılanmalar, tek bir birey tarafından siber alanda tehlike altında kalabilmektedir.

Çalışmada ise esas güvenlik tartışması ve aktör olarak devlet temellendirildiği için devletlerarasında cereyan eden ve siber savaş olarak niteleyebileceğimiz siber saldırı ve savaşlardan bahsedilecektir.

Sibirya Doğalgaz Patlaması (Logic Bomb)

1982 yılında Sibirya'da doğalgaz boru hatlarına yönelik yapılan siber saldırılar sonucu meydana gelen büyük patlama, siber anlamda da ilk saldırı olma niteliği göstermektedir. Çünkü ilk defa siber teknolojiler kullanılarak bir saldırı düzenlenmiştir.

Bu siber saldırının aktörleri ABD ve Sovyet Rusya olmuştur. ABD öncülüğünde Sovyetler Birliği'ne ambargo uygulanan bu yıllarda, Sovyetler bu ambargoyu bir şekilde aşmak niyetiyle Kanada'da bir şirketin doğalgaz boru hatlarını kontrol etmekte kullandıkları sistemi ele geçirmişlerdir. Aslında tam olarak ele geçirdiklerini düşünmüşlerdir oysa ABD bu girişimin farkına varmış ve CIA (Amerikan Haberalma Örgütü) bu yazılımların içerisine ''*Logic bomb''* (www.gizmocrazed.com, ty: s. 1). adında bir nevi saatli bomba yerleştirmiştir. İşte 1982 yılında gerçekleşen bu büyük patlamanın arkasında yatan basit bir aldatmacayla yapılan siber saldırıdır. (Tandoğan, 2010: s. 1).

Bu olaya mukabil yeni güvenlik anlayışının ve savaş alanının siber alana kaydığı ve artık bu alanda egemenlik sağlanılması gerektiğinin anlaşılması adına önemli bir örnek olmuştur.

Ay Işığı Labirenti (Moonlight Moze)

Siber saldırı tarihine ‘’Moonlight Moze’’ olarak geçen bu saldırı ABD’nin NASA, ABD Enerji Bakanlığı, Pentagon ve üniversitelerine yönelik olarak gerçekleşmiş; askeri haritalar, askeri tesislere ait bilgiler üniversite araştırma-geliştirme projeleri gibi son derece gizli bilgiler çalınmıştır. (Işık, 2017: s. 1).

Saldırıların arkasında her ne kadar kabul etmeseler de Rusya’nın olduğu ABD tarafından yapılan teknik takiplerle tespit edilmiştir. CIA bu saldırıyı daha önce benzeri görülmemiş şekilde koordineli bir saldırı olduğunu açıklamıştır. (Doman, 2016:cs. 1). Yani CIA daha baştan bunun arkasında bir devletin olduğunu belirtmiş ve bu tarz bir siber saldırının bir grup hacker tarafından yapılamayacağını belirtmiştir.

ABD’nin de bu saldırıyı tespit etmesi aslında 2 yıl gibi uzun bir süre almıştır. Çünkü saldırı aslında 1996 yılından itibaren şekillenmeye başlamış, 1998 yılında ise ABD bu sızmayı tespit edebilmiştir. (Hürriyet Gazetesi, 2017)

Bu saldırı ABD gibi bir süper gücün dahi, siber alanda tehditlere maruz kalabileceğini ve bu tehditlerin boyutlarının ne denli ağır olabileceğini göstermesi açısından çok önemlidir.

Kosova Krizi-NATO

NATO 1990’lı yıllarda Yugoslavya’nın da sonunu getiren çatışmalarda zaman zaman müdahalelerde bulunmuştur. Özellikle NATO’nun 1999 yılında yapmış olduğu hava saldırıları sonrası Sırp lider Miloseviç’in sonunu getirmiş olması, beraberinde birçok eleştiri de getirmiştir. Bu eleştirilerin harekete geçirdiği grupların bazıları ise hackerlardı ki özellikle NATO’nun bilgi sistemlerine yaptıkları basit sızmalarla ses getirmeyi başarmışlardır. NATO’nun siber uzaydaki gücünün sorgulanmasına sebep olan bu saldırılar neticesinde gerekli adımları atmak gerektiğini düşünen NATO, 2002 Prag Zirvesi’yle siber olaylara anında ve etkili bir şekilde müdahalede bulanabilecek bir merkez oluşturmasını kararlaştırmıştır. (Yener, 2014: s.1).

Saldırılar süresince NATO kendi içerisindeki koordinasyonu sağlayamamış, üye ülkelerle online iletişime geçememiştir. Bu saldırıların önemli bir özelliği ise NATO'ya karşı yapılan ilk siber saldırı olmasıdır. Soğuk Savaş süresince karşısında somut düşmanları olan NATO doğal olarak savunma stratejilerini de bu yönde oluşturmuştur. Fakat Soğuk Savaş sonrası dönemde artık bu güvenlik algısının değiştiği ve yeni savunma teknikleri oluşturma ihtiyacının doğduğu da bu saldırılar neticesinde NATO nezdinde de anlaşılmıştır.

Estonya'ya Yönelik Siber Saldırılar

Estonya 1991 yılında bağımsızlığını ilan ettikten sonra yıllar içerisinde teknoloji ve iletişim alanında büyük reformlar gerçekleştirerek, Avrupa içerisinde en kablolu ülke olma yoluna girmiştir. Ülkede yaşayan vatandaşlarının %65'ten fazlasının internete erişim sağlayabildiği ülkede, hükümet fonksiyonlarının birçoğu da çevrimiçi ortamda yapılabilmektedir. Bu işlemlerin içerisinde bankacılık işlemleri, vergi ödeme işlemleri ve hatta oy verme işlemleri de dâhildir. Estonya adına söylenmesi gereken bir diğer önemli husus ise meclislerince internet ulaşımının bir temel insan hakkı olarak nitelendirilmesidir. (W. Beidleman, 2009: s. 2-5). Bütün bu teknolojiyle iç içe geçmişlik Estonya'yı siber uzayda bir hedef haline getirdiğinde ise bu olumlu hava tersine dönmüştür.

2007 yılına gelindiğinde Estonya hükümeti, İkinci Dünya Savaşı'ndan (SSCB dönemi) kalma Tallinn şehrindeki Bronz Asker Heykelini şehrin dışına taşımak isteyince özellikle ülkede yaşayan Ruslar bu duruma büyük tepki göstermişlerdir. (Boyraz, 2015: s. 32-40). Bu tepkiler 27 Nisan 2007 tarihine gelindiğinde ise Rusya'nın da müdahil olduğu bir şekle bürünerek siber saldırı niteliğine dönüşmüştür. Estonya gibi iletişim ve teknolojik ilerlemenin her türlü faydasından yararlanabilen ve Avrupa'da bu anlamda önemli bir yere sahip olan ülkede üç hafta boyunca hayat durma noktasına gelmiştir. Estonya devlet sistemlerine, bankacılık sektörüne, kolluk kuvvetlerine, medya şirketlerine ve internet altyapılarına yapılan bu saldırılarla adeta, ülkede işlem yapmak imkânsız hale gelmiştir. (Geers, 2008: s. 1).

Estonya örneği diğer devletler açısından da önemli olmuştur çünkü belki de ilk defa teknolojik olarak güçlü bir devlette 3 hafta gibi bir sürece, hemen hemen hayatın durduğu görülmüş ve hükümet ise bu krizden etkilenmiştir. Ülkeyi yönetilemez hale getiren bu siber saldırılarda

NATO da müttefik ülkeyi koruma sorumluluğu dolayısıyla her ne kadar saldırıları durdurmada yardımcı olmuşsa da itibarı sarsılan bir diğer yapı da yine NATO'nun kendisi olmuştur.

Gürcistan'a Siber Saldırılar

2008 yılında Gürcistan'a karşı gerçekleştirile siber saldırıların arkasında Rusya Federasyonu'nun olduğu iddia edilmektedir. Bu siber saldırıların arkasında ise tarihi sorunlar yatmaktadır. Güney Osetya ve Abhazya bölgeleri Sovyetler Birliği dağıldıktan sonra de facto bir şekilde özerk bölge gibi hareket etmekteydiler. Fakat 2008 yılında buradaki milliyetçi söylemler ve girişimler artınca Gürcistan ordusu ülkenin toprak bütünlüğünü savunmak amacıyla Güney Osetya'ya müdahalede bulunmuştur. Bunun üzerine Rusya Federasyonu da Osetya'ya girince iki ülke arasındaki gerginlik tırmanmıştır. Olayların perde arkasında ise Gürcistan'ın Batı'ya daha sıcak bakması ve ayrıca NATO üyesi olmak istemesi yatmaktadır. (Darıcılı, 2014: s. 7.)

Gürcistan'a karşı gerçekleştirilen siber saldırılar ise 2007 Estonya siber saldırısına benzerlik göstermektedir. 2008 yılında gerçekleşen bu saldırıların Gürcistan hükümeti bilgi altyapı sistemlerine yönelen ağır bir siber saldırı olduğu görülmüştür. Saldırıların ise sadece Rusya tarafından değil birkaç farklı bölgeden yapıldığı kaydedilmiştir. NATO ise Gürcistan'a yapılan bu saldırılarda ülkeye yardım edememiştir çünkü Gürcistan bu tarihte henüz NATO üyesi bir ülke değildir. Yine de saldırılar arttığında Gürcistan hükümetinin talepleriyle, birkaç kişiden oluşan uzman bir ekip gönderilmiştir. Saldırılardan uzun bir süre sonra bu uzman ekibin de yardımıyla ülkedeki bilgi sistemi normale döndürülebilmiştir. (Boyraz, 2015: s. 5).

Ancak saldırıların bitmesine kadar geçen süre Gürcistan adına bir somut savaştan daha fazla olumsuz anlamda etkiler doğurmuştur. Ülkenin dış dünyayla olan bağlantıları koparılmış, dışarıya bir e-posta bile göndermesi imkânsız hale gelmiştir. Gürcistan'daki banka sistemleri de tehlike altında kalmış, kredi kartları ve mobil telefonlar kullanılamamıştır. Her ne kadar Gürcistan tehlikeleri atlatmak adına Rusya ile olan iletişimini siber alanda bloke etmeye çalışsa da bu sefer siber saldırılar başka ülkeler üzerinden ülkeye yöneltilmiştir. Elbette Rusya ne Estonya ne de Gürcistan saldırılarını yaptığını kabul etmese de; saldırıların Rusya ile olan anlaşmazlık olaylarından hemen sonra gerçekleşmesi bu iddiaları güçlendirmektedir. (Kara, 2013: s. 49).

Wikileaks Belgeleri

Irak'ta da görev almış ve ABD ordusuna mensup kıdemli er Bradley Manning tarafından, ABD Dış İşleri Bakanlığı'nın 1996-2010 yılları arasındaki gizli yazışmaları, ordu veri tabanındaki gizli bilgiler 2010 yılında Wikileaks sitesi üzerinden dünyaya yayılmış, sızdırılmıştır. (Kara, 2013: s. 17).

Wikileaks sitesini 2006 yılında kuran Julian Assange bu site üzerinden Kenya'daki yargısız infazlar, Fildişi sahillerine bırakılan zehirli atıklar, Guantanamo kampındaki insanlık dışı uygulamalar hakkında pek çok gizli bilgiyi kamuoyuna sızdırmaya başlamıştır. 2010 yılında gelindiğinde ise ABD'nin Irak ve Afganistan gibi ülkelere yaptığı hukuk dışı uygulamaları da sızdırınca büyük paniğe neden olmuştur. (Adaklı, 2011: s. 1).
Wikileaks sitesi üzerinden yapılan açıklamaya göre bu girişimin amacı kamuoyunu bilgilendirmek, politik etik yaratmak ve hükümetlerin etik olmayan politikalarını ifşa etmektir.

Wikileaks belgelerinin sadece ABD'ye yönelik olarak düşünülmemesi gerekmektedir. Çünkü buradaki diplomatik kayıtlarda her ülkeyle yapılan gizli temaslar aşama aşama basına sızdırılmış, diplomatik anlamda kısa vadede olmasa da uzun vadede birçok şeyi değiştirebilecek bilgiler, belgeler ortaya çıkmıştır. Zaten belgelerin ortaya çıkmasından hemen sonra Wikileaks belgelerini bu site üzerinden yayımlayan Julian Assange birçok tehditle karşılamıştır. (Arsoy, 2011: s. 1).
ABD'nin küresel anlamda en güçlülerden biri olduğu aşikârdır fakat bu gücü siber alanda, hem de hiç beklemediği bir aktör -kendisi adına çalışan ABD'li yetkililer- tarafından böyle bir saldırıya maruz kalmasına engel olamamıştır.

Wikileaks belgelerinin bu makale açısından önemli olmasının altında yatan ana sebep; onun bir devletten bir devlete karşı değil; bireyden devlete karşı olarak gerçekleşmesidir. Bu anlamda makalenin başından beri vurgulanan güvenliğin dönüşümünü en iyi yansıtan örneklerden biridir. Küreselleşmeyle beraber artık tehditlerin çok yönlü olduğunun, bireyden şirkete, kurumsal yapılardan tekil yapılanmalara kadar bu alanda her aktörün etkin olabileceğinin en somut örneklerinden biridir. Bu da devletlerin artık bu alanda güvenlik sağlamayı bir öncelikli alan haline getirmeleri gerektiğini ortaya çıkarmaktadır.

SONUÇ

Küreselleşmeyle beraber dünyanın her bölgesinin birbiriyle bağlantılı hale geldiği açıktır. Bu anlamda hiçbir birimin ve sistemin uluslararası alandan izole bir şekilde varlığını sürdürmesi yahut bir etkileşim içerisinde olmaması pek gerçekçi değildir. Ekonomi, toplum, kültür, siyaset ve hatta bireyler bu küreselleşme sürecinin birer parçalarıdır ve bu değişim-dönüşüm sürecine de dâhildirler. Elbette uluslararası sistemde halen başat aktör olma vasfını koruyan ulus devletler de küreselleşme sürecinde değişim ve dönüşüm içerisinde olmuşlar, olumlu ve olumsuz etkilerden kendilerini azade tutamamışlardır.
Küreselleşme sonrasında değişen-dönüşen bir diğer kavram da güvenlik olmuştur. Realist paradigmanın klasik öğretilerinden olan güçlü askeri ordu ve ülkesel anlamda sınırların kontrolüyle tam anlamıyla bir ülkenin güvenliğini sağlamak gerçekçi durmamaktadır. Çünkü artık tehditler somut değil, soyut alanda belirmekte fakat sonuçları itibariyle somut dünyayı ağır bir şekilde etkileyebilmektedir. Estonya ve Gürcistan siber saldırılarında da görüldüğü üzere bir ülke bütün kurumlarıyla beraber saldırı altında kalabilir, ülkede hükümet etme imkânsız bir hale bürünebilmektedir. Bütün bunlar olurken de bu düşman saldırının aktörleri savaş meydanlarında değil; aksine dünyanın herhangi bir bölgesinde internete bağlantısı olan sıradan bir yerde bulunabilmektedir.

Ulus devletler, son yıllarda siber uzayda hâkimiyet kurmanın gerekliliğini ve önemini idrak edebilmişler, kendi savunma ve güvenlik algılamalarını da buna göre düzenlemeye başlamışlardır. Birçok ülke bu anlamda siber güvenlik yasaları oluşturmuş, bu alanda uzman kadrolar elde etmek adına yatırımlar yapmaya başlamıştır. Uluslararası alanda da siber güvenlik alanında bir takım işbirlikleri oluşturulmaya çalışılmaktadır. NATO, üyesi olan ülkelere bu anlamda da bir güvenlik şemsiyesi sunma çabasındadır. Yine Avrupa Birliği ve Birleşmiş Milletlerin de bu yönde çalışmaları bulunmaktadır.

Devletler siber alanda her ne kadar gecikmeli olsa da hâkimiyet sağlama anlamanda eli en güçlü yapılardır. Çünkü diğer hiçbir yapılanma bu konuda süreklilik, yatırım ve merkezileşmeyi görece devletlerden daha iyi gerçekleştirememektedir. Ayrıca siber güvenlik alanı her ne kadar bir risk alanı olarak görülse de burada elde edilebilecek bir üstünlük, uluslararası sistemde belirleyicilik anlamında da bir hareket kabiliyeti yaratabilecektir. Diğer taraftan siber

teknolojilere sahip ülkelerin, bu teknolojileri pazarlama imkânları da yüksek ve ekonomik olarak karlı görülmektedir. Son zamanlarda devletlerin siber alana ilgilerinin artmasının bir diğer önemli sebebi de bu ekonomik dürtüler olmuştur.

Sonuç olarak her ne kadar küreselleşmenin olumlu birçok sonucu olsa da bu süreçte değişim yönünde doğru, zamanında ve uygun adımlar atılmazsa çeşitli sorunlarla karşılanması yüksek ihtimaldir. Küreselleşmeyle değişen güvenlik algılaması paralelinde siber güvenlik de bunlardan biridir. Eğer devletler bu alanda hâkimiyetlerini sağlayabilirlerse uluslararası sitemde varlıklarını sürdürebilmeleri daha kolay olacaktır aksi takdirde güvenlik tehlikeleriyle yüz yüze gelmeleri ve beka sorunu yaşamaları kaçınılmazdır.

KAYNAKÇA

ADAKLI Gülseren. (2011). "Wikileaks Versus Kapitalizm", Bianet Online Haber Portalı, http://www.bianet.org/bianet/bianet/127079-wikileaks-versus-kapitalizm erişim tarihi: (07.12.2017).

ADAOĞLU Hacer Soykan. (2008). ''Küreselleşme ve Egemenlik Kavramının Değişmesine Yol Açan Etmenler.'' İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 166, Sayı 1, sayfa 9.

AĞIR Bülent Sarper .(2011). ''Güvenlik Kavramını Yeniden Düşünmek: Küreselleşme, Kimlik ve Değişen Güvenlik Anlayışı.'' Güvenlik Stratejileri, Sayı 22, sayfa 109.

AKSOY Merve .(2016). , "Küreselleşme ile Değişen Güvenlik Algısı Bağlamında Bush Doktrini.", İHH İnsani ve Sosyal Araştırmalar Merkezi. Sayfa 3, http://insamer.com/wp-content/uploads/2016/04/K%C3%BCreselle%C5%9Fme-ile-De%C4%9Fi%C5%9Fen-G%C3%BCvenlik-Alg%C4%B1s%C4%B1-Ba%C4%9Flam%C4%B1nda-Bush-Doktrini.pdf (28.11.201).

ARSOY Helin .(2011). Ankarabarosu.org, http://www.ankarabarosu.org.tr/siteler/ankarabarosu/hgdmakale/2011-1/12.pdf erişim tarihi: (07.12.2017).

BOYRAZ H.M. .(Aralık, 2015), "NATO'nun Siber Güvenlik Politikası: Tarihsel Süreç ve Kırılma Noktaları" Cilt IV, Sayı 12, s.32-40, *Türkiye Politika ve Araştırma Merkezi (Research Turkey), Londra:* Research Turkey. http://researchturkey.org/?p=10236&lang=tr erişim tarihi: (03.12.2017).

Btk.gov.tr https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FSayfalar%2FSiberGuvenlik%2FUlusalVeUluslararasiBoyutlariileSG.pdf erişim tarihi: (01.12.2017).

CEYLAN Haluk. .(2014). Halukceylan.wordpress.com. https://halukceylan.wordpress.com/2014/11/13/siber-alan-siber-uzay-nedir/ erişim tarihi:(30.11.2017).

DARICILI A.Burak .(2014). ‘’Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıların Analizi.’’ Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Cilt 7, Sayı 2, Sayfa 7.

DEMİRAY Muhittin ve İşcan İsmail Hakkı. (2008). ‘’Uluslararası Sistemde Güvenlik Kavramının Değişimi Ekonomik ve Jeopolitik Arka Planı.’’ Dumlupınar Üniversitesi Sosyal Bilimler Dergisi, Sayı 21, sayfa 155.

DOMAN Chris .(2016). ‘’ The First Cyber Espionage Attacks: How Operation Moonlight Maze Made History.’’ https://medium.com/@chris_doman/the-first-sophistiated-cyber-attacks-how-operation-moonlight-maze-made-history-2adb12cc43f7 erişim tarihi: (03.12.2017).

ERDOĞAN İbrahim. (2013), ‘’Küreselleşme Olgusu Bağlamında Yeni Güvenlik Algısı.’’ Akademik Bakış, Cilt 6, Sayı 12, sayfa 266.

EREN Mehmet. (2017). ‘’Avrupa Birliği’nin Siber Güvenlik Stratejisi İçin Kuramsal Çerçeve ve Strateji Belgesi Öncesi AB’nin Eylemleri’’. Cyberpolitikjournal, Cilt 2, Sayı 3, sayfa 36. http://cyberpolitikjournal.org/wp-content/uploads/2017/07/Journal-Vol_2_No_3_17.pdf erişim tarihi: (02.12.2017).

FENTZ Stefan. .(2005). Univie.ac.at. http://www.univie.ac.at/frisch/isegov/aushaengUniWien/CyberpaceSecurity_Fenz.pdf erişim tarihi: (30.11.2017).

GEERS Kenneth .(2008). ‘’Cyberspace And The Changing Nature of Warfare.’’ SC Media, https://www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/554872/ erişim tarihi: (03.12.2017).

Hürriyet Gazetesi .(2017). http://www.hurriyet.com.tr/bugunku-siber-saldirilar-20-yil-oncesiyle-baglantili-40417840 erişim tarihi: (03.12.2017).

IŞIK Ezgi. ‘’Dünden Bugüne Siber Savaşlar.’’ http://www.bookmark.com.tr/dunden-bugune-siber-savaslar/ erişim tarihi: (03.12.2017).

KARA Mahruze. (2013). Siber Saldırılar-Siber Savaşlar ve Etkileri. Yüksek Lisans Tezi. İstanbul Bilgi üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

KARAÇAY Timur. Başkent.edu.tr http://www.baskent.edu.tr/~tkaracay/etudio/agora/bt/siber.html erişim tarihi: (30.11.2017).

KURNAZ İbrahim. (2016). ‘’Siber Güvenlik ve İlintili Kavramsal Çerçeve’’. Siber Politikalar Dergisi, Cilt 1, Sayı 1, sayfa 65. http://cyberpolitikjournal.org/wp-content/uploads/2017/02/Journal_Dergi_pdf.pdf erişim tarihi: 01.12.2017.

OTTIS Rain. Lornes, Peeter. Erişim: 01.12.2017, https://www.researchgate.net/publication/287868009_Cyberspace_Definition_and_implications

SANCAK Kadir .(2013). ‘’Güvenlik Kavramı Etrafındaki Tartışmalar ve Uluslararası Güvenliğin Dönüşümü.’’ Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Sayı 6, sayfa 130.

SANDIKLI Atilla ve Emeklier Bilgehan .(2014). ‘’Güvenlik Yaklaşımlarında Değişim ve Dönüşüm’’, sayfa 5, http://www.bilgesam.org/Images/Dokumanlar/0-81-2014040746sandikli_emeklier.pdf (28.11.2017).

SEREN Merve .(2006). ‘’Siber Tehditlerle Mücadelede Farkındalık ve Hazırlık.’’ Siyaset, Ekonomi ve Toplum Araştırmaları Vakfı(SETA), Sayı 183, Sayfa 16-17.

Sesli Sözlük, https://www.seslisozluk.net/cyber-nedir-ne-demek/ (30.11.2017).

ŞAHİNASLAN Önder .(2003). Siber Saldırılara Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma. Doktora, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.

T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2012). http://www.bilgiguvenligi.org.tr/wp-content/uploads/2016/03/Ulusal_Siber_Guvenlik_Stratejisi.pdf erişim tarihi: (02.12.2017).

TANDOĞAN Uğur .(2010). Dünya Gazetesi. https://www.dunya.com/kose-yazisi/savasa-hazir-miyiz/7527 erişim tarihi: (03.12.2017).

TÜRKÖZ Şükrü .(2016). ‘’Küresel Terörizm Sorununa Güvenlik Perspektifli Bir Yaklaşım.’’ Niğde Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi.’’ Cilt 9, sayı 2, sayfa 154.

W. BEIDLEMA ve Lieutenant Colonel Scott .(01.2009). Defining and Deterring Cyber War. http://indianstrategicknowledgeonline.com/web/DEFINING%20AND%20DETERRING%20cyber%20war.pdf erişim tarihi: (03.12.2017).

YENER Yavuz .(2014). ‘’NATO Ve Siber Güvenlik 2-Strateji.’’ Siber Bülten https://siberbulten.com/makale-analiz/nato-ve-siber-guvenlik-2-strateji/ erişim tarihi: (03.12.2017).

YILDIZ Mithat. (2014). Siber Suçlar ve Kurum Güvenliği. Uzmanlık Tezi. Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

CYBERCONFLICTS: AN EFFECT OF GLOBALIZATION ON CONFLICT ECOSYSTEM

Hüseyin ORUÇ[*]

Abstract

In this study we aim to understand how does globalization changed / expanded the international conflict ecosystem by introducing a newcomer: Cyber-conflicts. For the purpose of such an understanding first of all in the introduction part we revisit and integrate a number of theories and concepts such as conflict, cyberspace, imperialism, globalization theories and trans-nationality concept in order to have a theoretical framework about cyber-conflicts. Then we focus on the differences and relations between the conventional / kinetic conflicts and cyber-conflicts. Although this study is based on qualitative analysis of what is called cyber-conflicts, we also include some quantitative data in order to clarify the current changes in international conflict ecosystem. In the conclusion part we reach a new conceptualization about cyber-conflicts as globalization of war and criticise the lack of peace mechanisms.

Keywords: Conflict Ecosystem, Cyber-conflicts, Kinetic Conflicts, Globalization of War

Özet

Bu çalışmanın amacı, küreselleşme sürecinin yeni bir olgu olan siber-çatışmaları ortaya çıkarmak yoluyla uluslararası çatışma ekosistemini nasıl değiştirdiğini / genişlettiğini anlamaya çalışmaktır. Bu amaçla, çalışmanın giriş bölümünde, siber-çatışmalar hakkında kuramsal bir çerçeve oluşturmak için çatışma, siber-uzay, emperyalizm, küreselleşme kuramları ve ulus-aşırılık bir dizi kavram ve kuram yeniden ele alınmakta ve birbirleriyle ilişkilendirilmektedir. Sonraki bölümlerde ise geleneksel / kinetik çatışmalar ile siber-çatışmalar arasındaki farklılık ve ilişkilere odaklanılmaktadır. Her ne kadar bu çalışma, siber-çatışmalar hakkında nitel bir analiz olarak tasarlanmış olsa da uluslararası çatışma ekosistemindeki güncel değişimleri açıklığa kavuşturmak amacıyla bazı nicel verilere de yer verilmiştir. Sonuç bölümünde ise siber-çatışmalar hakkında, savaşın küreselleşmesi gibi yeni bir kavramsallaştırmaya ulaşılmakta ve barış mekanizmalarının eksikliği eleştiri konusu kılınmaktadır.

Anahtar kelimeler: Küreselleşme, Çatışma Ekosistemi, Siber Çatışmalar, Kinetik Çatışmalar, Savaşın Küreselleşmesi

[*] MA Student, Program of Peace and Conflict Studies, Social Sciences Universty of Ankara, can be accessed via onur_tercume@hotmail.com

INTRODUCTION

In peace and conflict studies discipline, even the basic concepts are still elusive. The debates around the basic concepts of the discipline can be attributed to not only the relatively "new" characteristics of the discipline but also can be considered as an expression of different points of view about the economic and political aspects of the international system. Therefore the definitions of basic concepts reflect the ideological biases and orientations. As Jackson points out, "there is ..a real need to encourage an openly "critical turn" in the field" (Jackson, 2015, p. 19). The mainstream in peace and conflict studies, due to the dominance of the positivist social scientific paradigm and narrowly determined basis of positivist ontology and epistemology (Jackson, 2015, p. 21); shows a weak appearance in revealing the broader social relations, structures, history, culture and contexts that is to say the international economy-political system behind the conflict issues.

Conflicts are tried to be explained from a behaviourist perspective reducing the issues to the behaviours of the parties. Therefore, it will not be an exaggeration to say that the mainstream peace studies separate and isolate the individual conflict cases from its root causes which rise on the basis of the domination systems. This separation and isolation approach is also valid in theory; the mainstream peace and conflict theories do not reflect the debates in broader social theories. Behind a claim of impartiality, mainstream peace studies are oriented as a "problem-solving"/stability tool for the existing system on national and international levels. On the basis of the statements above and critical theory´s acknowledgement of subjectivity in social science, this study will consider the definitions from a critical, historical and economy-political perspective. This subjectivity can be expressed in Galtung´s words: "As in all other types of social science, the goal should not be an 'objective' social science freed from all such value premises, but a more honest social science where the value premises are made explicit" (Galtung, 1971, p. 83)

Conflict and Conflict Ecosystem

The founder of the discipline Galtung defines conflict as a relation where the "actors (are) in pursuit of incompatible goals" (Galtung, 1973, p. 23). This definition which at the first sight seems as a behaviourist approach, with his well-known conflict triangle consisting of

A(Attitudes) + B(Behaviours) + C (Contradiction) transforms into a multi-dimensional approach (Galtung, 2007, p. 22). Contradiction is about inequality structures and structural violence is the root of direct violence. Galtung´s one of the basic but undervalued contribution to the discipline is his Imperialism theory which considers the domination relations in international arena as a structural violence between the center and periphery (Galtung, 1971).

However one can observe that Galtung´s relatively critical approach could not be deepened by the newcomers of the discipline. His emphasis on the structure shifted towards the behaviours:

> *The starting point for this paper is the traditional definitions of conflicts (presented below), according to which a conflict is the result of opposing interests involving scarce resources, goal divergence and frustration. The paper then addresses more recent perceptions of the conflict concept. We suggest that conflicts should not be defined simply in terms of violence (behavior) or hostility (attitudes), but also include incompatibility or "differences in issue position" (Position differenzen) Such a definition is designed to include conflicts outside the traditional military and is based on* ***behavioral dimensions***. (Swanström & Weissmann, 2005, p. 7).

A different variant of this extreme-emphasis on behaviours is the "perceptions" approach: "A relationship between two or more interdependent parties in which at least one of the parties perceives the relationship to be negative or detects and pursues opposing interests and needs. Both parties are convinced that they are in the right." (Leonhardt, 2001, s. 7)

Not be misunderstood, it should be noted that the effect of perceptions in formation of a conflict is undeniable. However the shortcoming of this perceptions approach is the overestimation of the psychological processes in perceptions. Since the perceptions occur on the basis of an historical, social and political processes determined by power and domination relations, it could be noted that the perception itself is a social process.

Some of the researchers define conflict on the basis of economic reason by transferring "scarce resources" term from economics into peace and conflict studies: "a social situation in which a minimum of two actors (parties) strive to acquire at the same moment in time an available set of scarce resources*."* (Wallensteen, 2007, p. 15). The pre-acceptance of scarcity of resources in itself is a variant of economic determinism and "homo-economicus" concept.

Also there is confusion about the appearance or formation of conflict; especially about whether violence is an integral part of a conflict or not. Due to this confusion, in some definitions the distinction between contradiction and conflict disappears:

> *The word conflict has a confusing range of meanings. It sometimes is used to refer to war or other violent social relationships; but sometimes, it refers to a difference in interests between parties that is unrecognized by them. I use the word here to refer to a social relationship in which two or more persons or groups manifest the belief that they have incompatible objectives. That definition indicates that a conflict may be waged in a variety of ways, varying in coerciveness and many other dimensions.* (Kriesberg, 2012, p. 150)

At this point, Galtung´s powerful approach to violence, as structural and direct/physical violence will be helpful to solve the confusion. Direct/physical violence is not a must for a conflict, but structural violence is an integral part of any conflict. Otherwise one cannot make a distinction between conflict and contradiction.

Also there is another debate about the role of the conflict in social change. Marx had defined the class struggle as the *engine of the history*. Marx´s point of view is shared by some of the mainstream opinions from a different perspective. This perspective can be summarised as: conflict is something that can be used to restore the social l relations ultimately in order to re-construct the existing system: "Conflict is an essential ingredient of social change. What is important is that conflicts should be solved in a peaceful and constructive manner. - In these Guidelines we use a narrower definition of the term "conflict" referring to a situation where there is a potential for violence to occur between groups or where violence has already occurred. These are the conflicts with which development cooperation is increasingly preoccupied" (Leonhardt, 2001, s. 7)

Another specific issue to be addressed is the dynamic and relational nature of the conflict:

> *A conflict is* ***not a static situation, but a dynamic one*** *– the intensity level changes over a conflicts' life cycle. An understanding of the* ***conflict cycle*** *is essential for an understanding of how, where and when to apply different strategies and measures of conflict prevention and management. Over time, numerous suggestions and models of*

> *conflict patterns have been put forward. Among these models and suggestions, a number of patterns stand out. Conflicts tend to be described as* ***cyclical*** *in regard to their intensity levels, i.e. escalating from (relative) stability and peace into crisis and war, thereafter deescalating into relative peace. Most scholars also agree that these cycles are reoccurring. This proposition is strongly supported by empirical research on conflict patterns* (Swanström & Weissmann, 2005, pp. 9-10).

However conflict is dynamic and cyclical not only in its specific form, but also in relation to the other types of conflicts. For example an intra-national conflict can be transformed into an international conflict and vice versa. Nearly all the macro-level conflicts include different conflict types. Conflicts occurred in a specific space can spread towards different spaces, horizontally but also vertically just like an ecosystem. Ecosystem is defined as:

> ***Ecosystem****, the complex of living organisms, their physical environment, and all their interrelationships in a particular unit of space… An ecosystem can be categorized into its abiotic constituents, including minerals, climate, soil, water, sunlight, and all other nonliving elements, and its biotic constituents, consisting of all its living members. Linking these constituents together are two major forces: the flow of energy through the ecosystem, and the* ***cycling*** *of nutrients within the ecosystem* (The Editors of Encyclopædia Britannica, 2017).

At the crossroads of the different definitions above and from a broader social, historical and structural perspective we can define conflict as a violence-prone and dynamic relationship between at least two parties who have or perceive to have incompatible goals, interests or positions on the basis of some root causes based on social, historical or structural power and domination relations. From the perspective of this definition we reach to the definition that cyber-conflict is a new component of global conflict ecosystem.

Ocurrence of new spaces does not cause the previous spaces to be excluded or a replacement; on the contrary we observe the integration of the newcomers with the previous spaces. This integration complicates each space in itself and also creates a much more complicated system of warfare in which each component effect and feed each other. This is the **conflict ecosystem**.

Time, Space, Technology and International Politics: Economy Politics of War

Cyberspace is defined as a new / fifth space of international politics which is the first human-made space. The four kinetic spaces of international politics, that is to say the Land, Sea, Air and Outer-Space have also been the scene of war, naturally due to the fact which was briefly expressed by Clausewitz´s words as "war is a continuation of politics by other means". Economy-political point of view to history considers politics on a basis called economy. A brief look into the history of war shows us that the occurrence, formation, expansion and concentration of these four spaces have been changed and shaped in time by a special factor called "technology" (Friedman & Friedman, 2015) which is a multiplier in production / economy. Although ancient Greek and especially Roman Empire had used ships mainly to transfer their troops, until the 16th century, war was an act primarily performed in the land, because the economy was based on agricultural production and labour force and the (Leonhardt, 2001)international commercial lines such as Silk Road were located in the land. Beginning from the 16th century geographical discoveries and new technologies gave rise to huge navies in order to control commercial lines starting to shift towards the oceans because the economy was based on commercial capitalism led by merchants trying to cross the borders. Massive production of raw materials and commodities led by 19th century´s modern industrial capitalism and its structural need of surplus value transfer between capitalist and underdeveloped countries have been most important cause of the instinct of controlling the oceans. Therefore big powers of the international arena were the big naval powers. WWI was not only the evidence of critical importance of naval power in victory but also has been the scene for a newcomer. The first military aeroplanes used in WWI were a discovery and introduction of the third space in international politics and war. Technology and war had a dialectical relation and the effective use of air raids during WW2 has proven the importance of this new space. Jet engine, ballistic missiles and satellites developed on the basis of the new technological developments following WW2 has introduced the fourth, outer- space. This brief summary shows us that the occurrence of new spaces does not cause the previous spaces to be excluded or a replacement; on the contrary we observe the integration of the newcomers with the previous spaces. This integration complicates each space in itself and also creates a much more complicated system of warfare in which each component effect and feed each other. However each space has a specific relation with or the specific product of a specific historical economy-political development. On the basis of the facts stated above, the coincidence of globalization process and cyber-conflict cannot be considered as casual. Therefore, in order to understand the cyber-conflict phenomenon, the globalization process needs to be discussed.

Globalization Theories: Free circulation of capital, labour and conflicts!

Only a short glance to the main components of what is called "globalization" shall be sufficient to perceive the parallelism between the globalization and cyber-conflicts. However before underlining this parallelism, it would be helpful to draw an outline of globalization. Due to its coincidence with the collapse of Soviet Union and related developments in the international politics, globalization is a highly ideological concept. Beginning from 1990´s it has been declared as the "end of history", or "ultimate triumph of western liberal capitalism" (Fukuyama, 1992). However this "optimistic" perspective to history has collapsed within only a few years and the "peaceful" discourse surrounding the international politics disappeared and Huntington has been the precursor of the new "clash of civilizations" four years before the September 11 and the start of *War on Terror* (Huntington, 1996). According to one`s ideological stance and association with politics the definition and implications of "globalization" vary. Nonetheless, without denying the author`s subjectivity, we may define globalization as a new restructuring phase of capitalism on the basis of new technological developments especially in communications which enables and accelerates the circulation of capital, labour, ideas and dominant cultural products on a global scale. Such an inclusive definition will enable us to avoid from technological and economic determinism (Kellner, 2002). As Kellner points out is a "highly complex, contradictory and thus ambiguous set of institutions and social relations" (Kellner, 2002, p. 286). It could be noted that, the "contradictory" nature of globalization can be attributed to its dual nature first as an objective technological and economical fact and secondly as an ideological discourse which is utilised to legitimate the western neo-liberal system and imperialism as a centre – periphery relation. (Galtung, 1971) . In this chapter we will analyse the technological – economical aspect of globalization which is in parallel to the formation of cyberspace and cyber-conflicts.

Technical background of globalism has been formed by the technological developments especially in communication industry. New communication instruments have enabled the free circulation of capital, labour and ideas faster than ever. The space of these "new communication instruments" was internet. And when we call "cyberspace", mostly we mean internet and the infrastructure to sustain and use it. According to a US military definition, "Cyberspace...is the Domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures";

(Podins, J., & M., 2013, p. 419). Since the cyber-conflicts are the extension of the kinetic conflicts in cyber-space, it can be suggested that cyber-conflicts would be impossible without internet and the very occurrence of internet itself has been the key factor or foundation for the extension of kinetic conflicts to a new space. "The Joint US Military definition for "cyber warfare" is "an armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyber attack, cyber defence, and cyber enabling actions." (Podins, J., & M., 2013, p. 420). Here, we may suggest that globalization has enabled the free circulation of conflicts also.

WHAT IS NEW?

First man made space in international relations: cyberspace

Conventionally international relations take place on physical spaces which "provide opportunities for expanding power and influence in world politics" (Choucri, 2012, p. 5). These conventional physical spaces are described as land, sea, air and outer space (Kosenkov, 2016). These conventional spaces all were natural spaces and prior to the hegemony struggles of the international actors. Cyberspace as a new domain of international relations is radically different from the other four spaces. Although it is not a completely virtual space (because it comprises a physical infrastructure and as Choucri points out it includes logical building blocks, information content and actors (Choucri, 2012, p. 8); precisely it is not natural and the first man made space. This feature of cyberspace, on the contrary to the conventional spaces, makes the very formation and occurrence of this space an organic part of hegemony formation in globalization age. Conventional spaces were the arenas of hegemony struggle which were already existent but tried to be dominated by the hegemonic powers in international relations. Cyberspace is a domain which is at the very beginning created and expanded by the hegemonic powers who were able to produce and use the technical instruments necessary for the formation of this new domain. Therefore it can be defined not only as a conflict domain but also as a product of international conflict.

Transnational actors on the scene: Corporate involvement

Conventional spaces in international conflict were the scene of a limited number of actors including the states, international organizations and some non-government organizations. However cyberspace has been a new scene which includes extremely much more actors especially the private companies (Gamero-Garrido, 2014), corporations, transnational companies and activists who are triggered by a wide variety of motives. A recent study on international cyber-conflicts shows that the 16 out of 17 cases analysed involved the corporations as actors in either attack of defence position (Gamero-Garrido, 2014) and the same study shows that all the analysed cases are an extension of the ongoing conflicts in kinetic spaces. Imperialism and globalization theories (Galtung, 1971) (Arı, 2013) (Held & McGrew, 2003) underline the dominant position of the corporate actors in general and transnational companies in particular in the international system. Involvement and active status of the transnational companies in this new domain have a difference from the previous period. In imperialism theories before the globalization period, monopolies had a national character and their interests were represented by the nation states. However in globalization period the transnational companies, due to their multi-national capital structure cannot be identified with a specific state. Therefore these transnational companies can be defined as completely "private" actors of which interests are represented by the global financial system and the very involvement and active status of these transnational companies in international cyber-conflicts can be considered as a factor which reinforces the already existent anarchy in international system. United Nations systems and some other international organizations, despite their weak and debatable characteristics, have acted as instruments which soften the anarchy and conflict-full nature of the international relations based. In globalization phase, these new actors (transnational companies) do not have any regulating superior authority. Although a few conferences are organized (Podins, J., & M., 2013), still there is not a regulating authority.

Military front changing shape: Diffusion of the front

Only a short glance to the cyber-conflicts shows the fact that due to the erosion of the nation state borders against free circulation of capital, labour, ideology and conflicts on the basis of new technologies, armed conflict and "war" has changed its shape and diffused / spread out and globalized into a new type of conflict ecosystem. Derian, while addressing this fact, uses the word "virtual continuation of war by other means" (Derian, 2000, p. 771) According to Derian, this "virtuous war" actualizes violence from a distance with no or minimal casualties (Derian, 2000, p. 772). Cheap, diffused, globalized but crowded: these are some of the features of the

new “front”. Gregory defines this diffusion and globalization as the “the everywhere war” (Gregory, 2011) and empathizes the dominant status of United States in cyberspace and therefore cyber-conflicts. Tierney, by emphasizing the “war on terror” and “clash of civilizations / religions” discourses in global age, uses the words “globalization of war” (Tierney, 2006). Bousquet after defining the globalization as a “network society” emphasizes the importance of cyber networks for the future of military organization. (Bousquet, 2008).

Decentralization

Just like globalization, cyberspace and cyber-conflicts has a decentralized appearance and again just like globalization, behind this decentralized appearance there is the dominance of hegemonic powers also for cyber-space and cyber-conflicts. Real time cyber-attack maps show that vast majority of the attacks are originated from the dominant powers struggling for global hegemony like US, China and Russia. “The United States, still the world's pre-eminent military superpower, is not the only nation preparing to fight the 'next war' in cyberspace. By the start of 2010 China, India, and Russia alongside the US, the UK and South Korea are among the first group of countries to establish formal command and control (C2) over military assets in the cyber-domain”. (Hughes, 2010, p. 523). Derian and Bousquet also emphasize the this domination. (Derian, 2000) (Bousquet, 2008). However, besides this seemingly “decentralization”, in fact there is an actual decentralization in the cyberspace. Unlike the conventional spaces where violent conflicts requires the possession of weapons and an infrastructure which are mostly expensive, in cyberspace only a personal computer is enough to become an actor in cyber-conflict. The massive production of computers and other electronic / mobile devices has made the inclusion of millions of actors in cyber-conflicts. Nearly all the literature emphasize this feature as a distinctive characteristic of cyberspace in comparison to the conventional spaces. (Bousquet, 2008) (Delpech, 2012) (Derian, 2000) (Friedman P. W., 2014) (Gamero-Garrido, 2014) (Gregory, 2011) (Hughes, 2010) (Kosenkov, 2016) (Lewis, 2013) (Libicki, 2012) (Libicki, 2012) (Podins, J., & M., 2013) (Schmitt, 2012).

Inner drive of global capitalism for massive production and free circulation of electronic and software products has given rise to the access of millions to the products which can easily be used as cyber-conflict instruments. The very nature of these products enables transforming them into weapons. This can and is used as a potential for the resistance against global capitalist system by large masses of activists. Some of these activists are the parts of democracy or human

rights based movements like global anti-capitalist movements, new social movements, Occupy Wall Street, etc. and from a wider and democratic perspective can be considered as an opportunity for democratic participation of the masses. However the same space and instruments are also used for terrorism purposes, like ISIS, Al Qaeda, etc.

Rapid, accessibility and non-visibility are some of the main characteristics of both globalization and cyberspace. Therefore non-visible attackers using easily accessed and rapidly developed instruments are the one of the basic characteristics of the cyber-conflicts. This makes warning and deterrence nearly impossible in cyber-conflicts and makes the cyber space much more anarchic than the conventional spaces. (Delpech, 2012) Also when we take into account that the regulation in cyber-space is not developed effectively, lack of accountability for destructive actions in cyberspace is one of the main problems to be solved.

CONCLUSION

As we have seen above, globalization and cyber-space / cyber-conflicts, with their common features, have strict parallelism. From an economy-political perspective it can be suggested that cyber-conflicts are the new form of conflicts in the globalization age. This new form as an extension of the ongoing kinetic conflicts makes the global conflict ecosystem much more complicated and difficult to challenge. Despite this anarchic atmosphere in cyberspace, it should be noted that this space can be used as an opportunity for a more democratic and human rights based participation to global politics. The oppressed voices of the plurality, the disadvantaged and vulnerable social groups can have an opportunity to express themselves.

However usage of cyberspace for terrorism purposes by terrorist organizations and for hegemony purposes by dominant international powers can be defined as the two main problems encountered in cyberspace. In order to challenge these problems, a framework for regulation of cyberspace with the attendance of all the stakeholders including the democratic activists is a must. As the current status, the absence of such an inclusion, and frameworks including all the hegemonic / dominant powers will disable any peace process and mechanism which will effectively manage the cyber-conflicts.

REFERENCES

Arı, T. (2013). *Uluslararası İlişkiler Teorileri: Çatışma,Hegemonya, İşbirliği* (8. Baskı ed.). Bursa: MKM Yayıncılık.

Bousquet, A. (2008, September). Chaoplexic Warfare or the Future of Military Organization. *International Affairs (Royal Institute of International Affairs), 84*(5), 915-929.

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

Delpech, T. (2012). Space and Cyberdeterrence. In T. Delpech, *Nuclear Deterrence in the 21st Century* (pp. 140-157). New York: RAND Corporation.

Derian, J. D. (2000, October). Virtuous War / Virtual Theory. *International Affairs (Royal Institute of International Affairs), 76*(4), 771-788.

Friedman, G., & Friedman, M. (2015). *Savaşın Geleceği:21.Yüzyılda Güç, Teknoloji ve Amerikan Dünya Egemenliği (The Future of War).* İstanbul: Pegasus Yayıncılık.

Friedman, P. W. (2014). *Cybersecurity and Cyberwar:What Everyone Needs to Know.* New York: Oxford University Press.

Fukuyama, F. (1992). *The End of History and the Last Man.* New York: Free Press.

Galtung, J. (1971). A Structural Theory of Imperialism. *Journal of Peace Research, 8*(2), 81-117.

Galtung, J. (1973). *Theories of Conflict: Definitions, Dimensions, Negations, Formations.* Hawaii: University of Hawaii Press.

Galtung, J. (2007). Introduction: peace by peaceful conflict transformation – the TRANSCEND approach. In C. Webel, & J. Galtung, *Handbook ofPeace and Conflict Studies* (pp. 14-32). New York: Routledge.

Gamero-Garrido, A. (2014). *Cyber Conflicts in International Relations:Frameworks and Case Studies.* Boston: MIT and Harvard University.

Gregory, D. (2011, September). The Everywhere War. *The Geographical Journals , 177*(3), 238-250.

Held, D., & McGrew, A. (2003). *Küresel Dönüşümler:Büyük Küreselleşme Tartışması (The Global Transformations Reader).* Ankara: Phoenix Yayınevi.

Hughes, R. (2010, March). A Treaty for Cyberspace. *International Affairs (Royal Institute of International Affairs), 86*(2), 523-541.

Huntington, S. (1996). *The Clash of Civilizations and the Remaking of World Order.* New York: Simon and Schuster.

Jackson, R. (2015). Towards critical peace research: lessons from critical terrorism studies. In I. Tellidis, & H. Toros, *Researching Terrorism, Peace and Conflict Studies:Interaction, synthesis, and opposition* (pp. 19-37). New York: Routledge.

Kellner, D. (2002, November). Theorizing Globalization. *Sociological Theory, 20*(3), 285-305.

Kosenkov, A. (2016). Cyber Confllicts as a New Global Threat. *Future Internet, 8*(45), 1-9.

Kriesberg, L. (2012). Mediation in Conflict Systems. *Systems Research and Behavioral Science, 29*, 149-162.

Leonhardt, M. (2001). *Conflict Analysis for Project Planning and Management: A Practical Guideline Draft.* Berlin: Deutsche Gesellschaft für Technische Zusammenarbeit (GTZ) GmbH.

Lewis, J. A. (2013). *Conflict and Negotiation in Cyberspace.* Washington: CSIS (Center for Strategic and International Studies).

Libicki, M. C. (2012). *Crisis and Escalation in Cyberspace.* New York: RAND Corporation.

Paul, C., Porche, I. R., & Axelband, E. (2014). Confirming the Analogy: How Alike Are Prfe-U.S. Speciial Operations Command Forces and Contemporary Cyber Forces. In C. Paul, I. R. Porche, & E. Axelband, *The Other Quiet Professionals* (pp. 31-46). New York: RAND Corporation.

Podins, K., J., S., & M., M. (2013). 5th Conference on Cyber Conflicts:Proceedings. Tallin: NATO CCDCOE.

Schmitt, M. (2012). Classification of Cyberconflict. *Journal of Conflict and Security Law, 17*(2), 245-260.

Swanström, N. L., & Weissmann, M. S. (2005). *Conflict, Conflict Prevention and Conflict Management and beyond:a conceptual exploration.* Uppsala: Central Asia-Caucasus Institute and Silk Road Studies Program.

The Editors of Encyclopædia Britannica. (2017, December 6). *Ecosystem.* Retrieved from Encyclopædia Britannica: https://www.britannica.com/science/ecosystem

Tierney, N. (2006). Religion, the Globalization of War, and Restorative Justice. *Buddhist-Christian Studies, 26*, 79-87.

Wallensteen, P. (2007). *Understanding Conflict Resolution:War, Peace and the Global System.* London: SAGE Publications.

THE NEW FACE OF THE WAR: CYBER WARFARE

Mehmet Emin ERENDOR[*]

Gürkan TAMER[**]

Abstract

With the development of the information technologies, computers and internet have played a crucial role in our life in the last decades. States, governments, NGO's, businesses, and other organizations take the advantages of these developments in terms of trade, economy, education

[*] PhD. Research Assistant, Department of Political science and International Relations-Çukurova University, can be accessed via mehmeterendor@gmail.com

[**] Undergrad, Department of Political science and International Relations-Çukurova University, Adana-Turkey.

and so on. Although technological developments enhance the ability of organizations to conduct activities in terms of cost-effective and efficient manner, it also has some disadvantages for the international community. Over the past decade, these technological developments have been used by some people, states or terrorist organizations to damage target states to improve their gains or impose their ideas or cut off the electrical power. Also, the Computer and internet was used a part of the war in Ukraine by Russia in 2015. In this study, the concept of cyber warfare will be analysed and its importance points and why states need to tackle with this situation will be explained.
Keywords: Cyber warfare, Cyber Disarming, Cyber Space, NATO, Estonia, Russia

Özet

Bilişim teknolojilerinin gelişmesiyle birlikte, bilgisayarlar ve İnternet geçtiğimiz on yıllarda hayatımızda önemli rol oynamıştır. Devletler, hükümetler, STK'lar, işletmeler ve diğer kuruluşlar, bu gelişmelerin avantajlarını ticaret, ekonomi, eğitim vb. gibi alanlar açısından kullandılar. Teknolojik gelişmeler, örgütlerin kabiliyetlerini etkin ve uygun maliyetli bir şekilde yürütme yeteneğini arttırmasına rağmen, aynı zamanda bu gelişmeler uluslararası topluluk için bazı dezavantajlara da sahiptir. Son on yılda, bu teknolojik gelişmeler, bazı insanlar, devletler veya terör örgütleri tarafından hedef ülkelere zarar vererek kazançlarını arttırmak veya fikirlerini dayatmak veya elektrik enerjisini kesmek için kullanılmıştır. Ayrıca, Bilgisayar ve İnternet, 2015 yılında Rusya'nın Ukrayna'daki savaşının bir parçası olarak da kullanıldı. Bu çalışmada, siber savaş kavramı analiz edilerek, önemi vurgulanacaktır ve devletlerin bu durumla niçin mücadele etmesi gerektiği açıklanacaktır.
Anahtar Kelimeler: Siber Savaş, Siber Silahsızlanma, Siber Uzay, NATO, Estonya, Rusya

INTRODUCTION

Although the identification of cyber weapons and the conceptualization of the cyber warfare are too difficult by the international community, these concepts have not commonly defined as it is the case for concept of terrorism. Besides, another problem of the international community is to generate disarmament regime (such as the International Atomic Energy Agency or the Chemical Weapons Prohibition and Prohibition Authority), but this requires a method of verification to achieve disarmament regimes involving cyber weapons (e.g. the NPT regime or the European Conventional Treaty). Although it is crucial to implement the rules of

disarmament, countries have continued to adopt new policies to improve their cyber capabilities. For example, cyber commanders are established, cyber-space and cyber instruments are used together with other elements of the war in the sense of common warfare.

In this article, our aim is to explain the basic principles of the cyber warfare and then analyse some possible effects of cyber warfare and cyber capabilities which can cause conflicts or wars in the international arena.

THE CONCEPT OF THE CYBER WAR

Cyber-attackers' capabilities not provide crucial manipulation and disinformation in conflicts also their capabilities create chaos in peace time. It has always been a critical target to penetrate masses' behaviours and perceptions through knowledge. During the Cold War, particularly during the periods of 1970s and 1980s, espionage was one of the most important influencing political tool which was used by the Soviet Union's intelligence agencies against the U.S. Nowadays, the espionage is using by states with using cyberspace and cyber space and cyber security, which have an important place today, can be portrayed as the access of important information through the use of computer and communication technologies. As a matter of fact, the work on the subject reveals that propaganda and manipulation activities of 'web robots' called 'bots' in social media are systematic, especially in the case of international crisis. There are also experts who interpret this as *'weaponizing information'*.[11]

It is not possible to evaluate the above-mentioned topics as a cyber-warfare. Obviously, in order to understand what the concept of cyber warfare is, it is necessary to first explain the truth 'what not'. Because, in popular usage of cyber warfare, any international competition activity using cyber instruments can be launched as a 'cyber war'. It would be unrealistic to evaluate cybercrime and even cyber espionage directly under the cyber warfare. Indeed, though it is possible that the world may be drifting into a "Cyber-Cold War" period with interventions in information, propaganda and even democratic election processes, but some scholars argued that there has not yet been a sizeable conflict that could be described as a "war" by military and military sciences in cyber-space. It would also be inconvenient for the concept of 'cyber warfare' to be used instead of 'cyber security', 'cyber-attack' or 'cyber espionage', and it is important to

[11] Sidney E. Dean Editor, Weaponizing Information: Propaganda Warfare in the 21st Century

provide terminological co-operation between the security science academy. It might be thought that cybernets are only made up of the internet. However, cyber-space also includes closed control systems that manage infrastructures and facilities that exist in physical dimensions beyond the internet, which is open to everyone and even encouraged. Due to the physical effects of the cigarette aggressors on the subject systems (e.g., general power interruptions or manipulation of SCADA systems in critical installations) can result in extensive loss of life and property. Here, the discussions about cyber warfare are coming to light because of these physical influences.

Finally, even if the above-mentioned problems are overcome, how will the collateral damage can be measured in spite of the inevitable, or when a cyber-attack on military targets creates the expected consequences? Today, armed forces with intelligent ammunition and sophisticated combat networks can overcome such concerns with technological-intensive operations. However, for cyber weapons, such an advantage may not be the case for all cases.

Speaking of which, collapse of internet networks and services in a country will certainly cause damage to civilians (Ball, 2017), Again, due to the unique nature of the cyber weapons, it is difficult for the offensive side to anticipate the possible consequences of the military planners. Only the mentioned qualities cause initiatives similar to the weapons of mass destruction of cyber instruments or disarmament initiatives to conventional capabilities to come to an end.

THE CONTROL OF CYBER WEAPONS AND CYBER DISARMING

At this point, it is crucial to understand whether international relations and international law frameworks on disarmament and arms control can be extended to 'cyber weapons'. Because, how and which parameters of cyber weapons can be limited/constrained to stuck to a single structure. Will the context of the restriction of cyber weapons be more similar to nuclear weapons or conventional weapons? Will it move from a different requirement?

The disarmament and restraint regimes differ from each other in terms of their causes and consequences. Such regimes may limit weaponry in terms of quality and quantity (e.g. European Conventional Force Treaty), prohibit the use of certain kinds and qualities of weapons (e.g. the Ottawa Convention), limit the trial activities of some weapons (e.g. Partial Nuclear Testing Prohibition Treaty) or prevent the production and stockpiling of certain weapons (e.g. the Convention on the Prohibition of Chemical Weapons). All these regimes are different from

the law of armed conflict. The purpose of such regimes is not to regulate state behaviour during the wartime but rather to prevent conflict and climbing itself (Geers, 2017).
What constraints should be made regarding offensive cyber skills - if so - by what conditions and parameters? Regulations on disarmament and arms restraint are made to achieve certain categorical results. This includes motivations such as minimizing military imbalances among states, raising predictability, avoiding the development of new weapons as much as possible, restricting spending on arming, or preventing irreversible and grave damage in case of armed conflict. Of course, at this point, it is of great importance to identify what is the offensive (cyber) weapon and, if possible, to categorize it.

Some scholars believe that there are two main categories of 'cyber weapons': those that do not need direct access to target computer systems (e.g., viruses that span the internet), those that have direct access to target computer systems (e.g. cyber agents that can penetrate SCADA systems and generate indirect kinetic effects) in the category. According to this approach, the elements to be subject to a possible regime of disarmament or arms control will be identified in the second category.

In order for cyber weapons to be subject to any international control regime, it is important for military and political circles to consider them in the context of 'strategic weapons', such as weapons of mass destruction or ballistic missiles. Studies of the subject state that the first and most important condition for the evaluation of the cyber skills used for military purposes in the 'strategic arms' segment is the catastrophic damage to the critical national infrastructure of an individual country. Until now, there has been no concrete evidence that cyber weapons have developed a destructive equivalent to nuclear weapons, which could upset the existence of a state (Schmitt, 1999). On the other hand, such a threat is not negligible, especially for countries that are carrying critical national infrastructures and economies to computer networks. Moreover, while the nuclear weapons regime is based on the non-use of these weapons, cyber skills can be used even in peace situations. Moreover, a state that is under attack cannot detect the actor who is attacking its own sovereignty. There is almost no such a situation for a nuclear attack. Offensive cyber skills are therefore frequently referred by international community.

In the case of 'Attribution', that is to say the source of the attack, it will be more realistic to compare offensive cyber skills with biological weapons. Because in some cases it may take time for an under-threatened country to understand that the threat it is facing an epidemic or a

biological warfare activity. Moreover, just as some bio-agents can be concealed for a period of time due to their incubation time, then a cyber-agent can also go through an 'incubation-like' process in computer systems.

The site is based on dual-use technologies that can be exploited for civil and military purposes, such as 'cyber weapons', the same chemical and biological weapons. In addition, while nuclear weapons are now monopolized by states, terrorist trends by the last ISIS threat and Al-Qaeda groups show that chemical weapons can also be used by non-state groups. This is also another case for cyber weapons.

However, although disarmament and arms control regimes for chemical weapons are exemplified, there is still a significant legal challenge in limiting cyber weapons. Because malware can be used to harm a system, spyware can also be used for espionage activities to learn about system vulnerabilities or information and information. However, spyware is the subject, and then the destructive malicious software that might come after it. Duqu malware, which contributes to the famous Stuxnet software, is a good example in this context. More explicitly, if Stuxnet, whose implicit kinetic influence, is the subject of a cyber-disarmament agreement, where would it be to put Duqu malware in this context?

It should be underlined that the greatest challenge for experts in any control regime concerning cyber weapons is to determine whether the parties are non-compliance. It is clear that governments will not look forward to a verification regime that will scan computer systems. Thus, even if a consensus is reached on the restriction of a cyber-weapon, which does not have an international mechanism with regulatory and sanctioning power, or where the verification regime is absent or limited, the situation that will arise is very similar to the Convention on the Prohibition of Biological Weapons, i.e. the control mechanisms will be ineffective.

It should be emphasized that weapons restriction and disarmament regimes are based on political-military considerations as well as international legal considerations. For example, the strategic evaluations of the Russian Federation and the US no longer needed chemical weapons after the Cold War brought with them the Regulation on the Prohibition of Chemical Weapons and the control of related weapons. Therefore, the main parameter to monitor of such consensus is found in the important and rising cyber actors of the international community.

As a matter of fact, an attempt by the Russian Federation, the People's Republic of China, Tajikistan and Uzbekistan in the UN in 2011 did not reach the conclusion due to the different ideas of Washington and Moscow. What is noteworthy here is the concern that a cyber-control regime has been used by authoritarian states as a censorship tool for the Internet and the flow of information. Another issue is that actors, such as the United States, who hold the technological superiority, must refrain from limiting and controlling these abilities by international mechanisms. It is difficult to analyse the concrete steps of the cyber warfare capacity without the barrier being overcome. Of course, while the need to prevent a cyber-space, armed race is increasing day by day, the world's leading armed forces continue to adopt new cyber policies and cyber instruments - at varying speeds.

In this framework, cyber commandments are established in many countries, and cyber-space and cyber instruments are used together with other elements of the war in the sense of a common warfare. In 2013, the Turkish Armed Forces took an important step by transforming the Cyber Defense Center into a Cyber Command. The establishment of the subject-matter command, which functions under NATO standards, is an important development in terms of the development of the Capacity of Communication and Electronic Information Systems of the Armed Forces and the national cyber defence solutions (Sofaer, et.all, 2000).

Also, cyber skills and electronic warfare are inseparable military tasks today. In this context, the recent breakthroughs of the Turkish Armed Forces and the Turkish Defense Industry are striking. The protocol signed with ASELSAN at the beginning of 2017 aims to increase the electronic warfare abilities significantly during the three years period (Aselsan, 2017).

Turkey is still far away from cyber warfare. First of all, it is a critical necessity to establish mechanisms and concepts to ensure regular and effective cooperation of academia, public, private sector and think tanks related to the subject. Secondly, and more importantly, the fact that the controversial offensive cyber skills debate in the world is not being done in Turkey adequately demonstrates that a more intensive intellectual effort is needed in the direction of the development of cyber military modernization. Thirdly, the increase in air defence capacities, especially in the immediate vicinity of Turkey, shows that it is vital that cyber and electromagnetic capacitance is seriously developed and integrated into deep attack capabilities. In defence modernization, more comprehensive steps are needed in this direction. In addition to what is stated, it should be noted that the cyber catcher had a grey area under the battlefield.

It is critical that the coordination of cyber-electromagnetic military developments with the efforts made by various institutions in our country and the formation of the vision for the situations under the war zone are critical.

HOW TO DEFINE A LEGITIMATE TARGET?

Armed conflicts related to the execution of cyber warfare is an important in terms of the application of the international law, and the 'legitimate aim' is who and what will constitute. Throughout history, the separation of civilians and military personnel has been based on sharp parameters. The use of uniforms by soldiers and the fact that military facilities have distinctive signs have created the first sign of this. Again, throughout history, the 'war zone' phenomenon has allowed civilians and civilian settlements to be precisely separated from conflict zones. On the other hand, the distinction between civilian and military targets is increasingly blurred. The trends that have developed in particular with the Second World War show that there are serious difficulties in protecting civilians from military operations and therefore the difficulties in question have increased (Ganuza, Hernandez and Benavente, 2011). The conflicts of 21st century, a hybrid profile exhibiting warfare in the residential neighbourhood made the civilizations a direct environmental factor. When it comes to cyber warfare, it is very difficult to distinguish between civilian and military targets. In fact, some experts consider that cyber warfare is a threshold from which the distinction between civilian soldiers and soldiers will be totally absent during the history of the war.

The question needs to be answered at this point with a meaningful consensus by the international community as: is there any of the cyber-attacks which is to be considered as a cause of war? and can the military response be legitimate?

Many experts suspicious of this suggest that cyber-attacks have limited - yet - ability to damage, and that the damage centre of the damage is mostly economic targets or consequences and therefore cannot be considered in a purely military framework. Those who come to the issue more differently think that the indirect kinetic effects of cyber-attacks, such as general electricity interruptions, can be regarded as a weapon attack, which can lead to life loss and cause death and damage to life in a country. From the point of view, there will be little difference between the direct kinetic effect (for example, by destroying the electrical

infrastructure with ballistic effect) and the indirect kinetic effect between the electrical infrastructure and the offensive cyber skills.

Cyber war - or possible future cyber wars - is another obstacle for armed conflicts, which makes the concepts of sovereignty of the state connected to geography and geography meaningless at a certain level. International relations have an organic relationship between the sovereignty of modern states and political geographies and borders. On the other hand, the geography that the state will use the sovereignty rights to date has, naturally, been defined according to physical qualities such as airspace and territorial waters. So, can a virus that targets a computer network be considered to have violated the political sovereignty of a state geographically? Because Article 2 of the UN Convention bans actions for the territorial integrity of states, the territory of the country, and the sovereign rights and independence of these territories. In that case, can the cyber agent mentioned in the above example be considered as a violation of the relevant article of the UN Convention? If indeed cyber instruments - such as conventional arms and weapons of mass destruction - are perceived as a threat to the basic parameters of the sovereignty and independence of the UN Convention, the restriction of disarmament and arms to these instruments would be based on a sounder basis of the regime.

Another issue that is crucial to the handling of cyber warfare as a military issue is the creation of doctrine. Because, in the literature, military doctrine means "belief system" for a military force. Military doctrines determine how the forces of the armed forces will fight, how they will perceive the environment of war and operation, the codes of enterprise and strategic culture, concepts and concepts. In this framework, military doctrines are prepared to respond to technical, tactical, operational, strategic questions and to cooperate with tens of thousands of staff to think and act.

If NATO is to be described as an operational environment with cryptic, space-based military functions, NATO has finally taken such a step - what elements would it contain as a cyber-warfare doctrine? The question we ask here goes beyond the different perspectives of different countries towards cyber warfare. Almost every national security document in the world has to make a threat definition and order. So, whichever country is prepared, the preparation of a cyber-warfare has to include some elements of the essence.

The studies in the literature focus on three main points in this respect. The first is related to how the perpetrator of the cyber-attack will be found and how it will be perceived (attribution problem). Because, at present, many states use surrogate groups for cyber-attacks. At this point,

it is very important to determine who to respond to in response to a cyber-attack. To give a more striking example for Turkish readers, at the end of 1990s, the Republic of Turkey has developed a new concept in the struggle with the PKK terrorist organization, focusing on the issue of 'deputy war', and on the Syrian Baath regime led by Hafız Asad, expressing his right to self-defence, directly putting pressure through the threat of war. In the 21st century, it is a very critical point that any state that is exposed to a cyber-attack by proxy will react to the sponsor state, whether it is a non-state proxy element or a cyber-attack.

Secondly, it is a matter that a cyber-warfare doctrine should absolutely address, how to do 'damage detection' about the consequences of a cyber-attack and how to assess the damage of a 'casualty' that an offensive cyber intervention gives to the enemy. At this point, measuring indirect effects is the greatest challenge.

Thirdly, and finally, taking into account the principle of proportionality, how and with which instruments a cyber-attack will be responded to is another key element in which a Cybercrime doctrine must respond. The point is that a state will respond to cyber warfare threats in a comprehensive and holistic manner.

Despite the above, there is a serious challenge to define the cyber warfare in the context of modern international relations and armed conflicts. Almost all the cyber-attacks are happening under the battlefield, and there are serious problems with their association with the offensive state. Experts who bring a holistic viewpoint to the cyber warfare and suggest that this new phenomenon should not be considered separately from the other elements of the warfare indicate that the cyber-attack and cyber warfare situations will not be limited to the cyber dimension due to the electromagnetic spectrum and will spread to the physical geographical dimensions. The most important argument of this hypothesis is that Russia has recently used and is currently using cyberspace as part of its overall escalation strategy in its interventions towards the former Soviet geography (lastly in Ukraine). In this context, attention is drawn to Moscow's' preparing the 'war zone' for special and covert operations, first with cyberspace.

Another noteworthy aspect of cyber warfare conceptualization is that there may be different approaches to the concepts of cyber war and cyber conflict. At this point, the main criticism of experts on the idea of cyber warfare is that all the cyber activities carried out in military or military-governmental institutions are regarded as a war effort. According to this

understanding, instead of treating cyber warfare as a separate element, it is necessary to understand that war for all organizations of armed forces based on computer and network technologies is 'cybersized' with every dimension. According to this understanding, the painting that emerges as the result of interaction with the physical four dimensions of the cyber-size (black-air-sea / ocean-space) shows that the armed cliché is gradually becoming "cyber".

CYBER WAR AND MILITARY ALLIANCES: NATO CASE

War is not just military technology and technology, it is an important element of international law and international relations. If Cyber is to be mentioned in words, it is also necessary to analyse the frame of the military options, such as the right to self-defence within the scope of the UN Convention, as well as military alliances and casus foederis against cyber-attacks, is required. Article 5 of NATO's founding treaty (Washington Treaty or North Atlantic Treaty) is one of the most concrete and dissuasive examples of what is now casus-foederis .

Is it possible for NATO to operate the 5th item in the face of an attack on one of the allied member states? As a result of 2014 Wales and finally the 2016 Warsaw summit, the North Atlantic Alliance today officially states that the cyber defence is part of NATO's collective defence mandate. Moreover, NATO emphasizes that international law can be applied to include cyber-space . Finally, the fact that cyber-space is an operational area at the Warsaw Summit gives an important idea about the political-military direction of the alliance's cyber skills.

NATO Secretary-General Jens Stoltenberg said in an interview at the press conference of the Defence Ministers in 2016 that the Der Spiegel correspondent would be able to trigger the collective defence clause in question against the question of whether the 5th article could be operated against a cheater attack on one or more members of the alliance, He replied that there was no obligation to operate the 5th article (Arimatsu, 2012). Indeed, it can be said that this 'vague' approach reveals both the process of adaptation of the alliance against cyber threats and the choice of flexibility in response options. It is frightening for the international community that the environment of cigarette conflict, which is still in its infancy, is causing a climb involving conventional and even nuclear weapons. As a matter of fact, Secretary General Stoltenberg said that the Russian Federation's intervention in the US presidential elections, which is one of the questions raised during the above-mentioned press conference, indicates that NATO's cyber skills do not target any country, and that the word 'Russia' preferred.

Nevertheless, the views gained in the latest Cyber Conference (CyCon 2017) organized by NATO's Centre for Civil Defence Excellence (Tallinn - Estonia) will leave open the way for Article 5 in case of a cyber-attack-like attack in Estonia that took place in 2007 it would be a much more rigorous response. Even at the level of diplomatic rhetoric, even in the face of cyber threats and taking an event as a scale, the imposition of a collective defence item gives an important idea about the future of NATO and cyber warfare. Of course, the views and analyses produced by the centres of excellence are not binding for the North Atlantic Alliance. However, it should not be forgotten that the analytical inputs mentioned may have serious consequences in some cases on the aspects of the North Atlantic Council and the elites who manage the NATO member countries.

GEOPOLITICAL CHARACTERISTICS OF THE CYBER-SPACE

Cyber-space has a sizeable impact on societies that cannot be compared to other dimensions of the warfare. Moreover, contrary to other known dimensions of warfare, cyber space is much faster than other dimensions, as cyber space cannot be physically controlled by a single state. More importantly, as the technological capacity of an actor increases, the land-sea-air-space systems and platforms become more dependent on cyberspace. Therefore, a weakness in cyber-space could lead to serious negative consequences for other dimensions, especially in terms of developed states.

The cyber-space is essentially 'in one form' in the other four dimensions of the warfare. More precisely, for example, the information transmissions from the sensors of war vessels cruising at sea or from airborne platforms and the data complexes stationed on the land are elements complementing cyber-space. There is a special relationship between space, the fourth dimension of warfare, and cyber space. Both dimensions are directly related to telecommunication and network technologies. In addition, operations performed in space are dependent on the capabilities of the cyber-space, operations performed on the cyber-space, and cyber electromagnetic activities are also dependent on support from the space dimension.

From a military point of view, cyber-space has important differences compared to other dimensions of land-air-sea-space quadrants. First of all, cyber-space, contrary to the historical and natural dimensions of war, is not qualified to be defined by known laws of physics. Of

course, the warfare also has social and political consequences of events that are of a physical nature. However, the kinetic effects of events in the field of warfare (eg, the shooting of a ballistic missile head with a target in the air, the shooting of an air platform with anti-aircraft fire, the shooting of an underwater platform of a submarine, the shooting of a military suit in orbit, shooting etc.) are also limited to the physically identifiable qualities of the physical warfare area or the fields. Many cyber-electromagnetic military activities can reach very complex and multi-dimensional domains of computation. For example, a computer virus can spread to countries that are not primarily targeted in various parts of the world, after affecting the systems of the target country. For this reason, it is very complicated to calculate the 'effective range' or the probability of undesired damage in cyber-space, as stated in the international legal review. Because cyber-space is a domain created for the use of information, for inter-human interaction, and for intercommunication. The field continues to exist together with the electromagnetic spectrum through telecommunication systems. More precisely, the mentioned telecommunication systems use the electromagnetic spectrum to form cyber-space by forming a global network.

Of course, due to the above-mentioned original qualities, the deterrence of cyber-space is also a difficult subject to understand from a traditional point of view. In particular, the basic components of the Cold War theories of deterrence, such as defence capabilities, credibility of threats, and the effective transmission of military-political messages, have to change for today's cyber parameters.

CYBER WARFARE'S FUTURE

Especially in the recent period, the revolutionary advances in electronic network-based communication have led to similar developments in battle networks. During the First World War, the use of telephone and radio lines to communicate with sea and land elements at long distances is regarded as the first battle network by some experts. Modern combat networks consist of command-control systems, target detection sensors & other discovery-surveillance-intelligence facilities, weapons systems and platforms, and electronic communication-based communication capabilities that connect all these elements together. The electronic revolution in communication facilities and capabilities has brought about significant changes in the understanding of military geography. In the first period when the 'human' began to fight as a species, the distance between the centre of administration and the elements of combat was to be the distance that the human voice could or could see. Today, as this distance has reached a

revolutionary point, network-cantered warfare also recognizes the possibility of engaging in weapons systems with targets that they cannot detect under normal conditions. Therefore, it is stated that battle networks competition has been experienced especially with the increasing speed from the Second World War, and this trend will continue to rise with great acceleration in the coming period (Geers, 2010).

In the age of cyber skills, such as the acquisition of information superiority, which is the basic principle of the network-based war, sharing information among friendly associations participating in the war and taking the common situational awareness to the top, out of the linear plane of the operation and effective use of synchronization. Moreover, the acquisition of knowledge superiority, that is to share with the friendly forces the most accurate and maximum information available on the battlefield in the fastest possible way, is to make the enemy as deprived of the same possibilities as possible, becoming a more important force multiplier in the cyber world.
As will be shown below, the network-based harness components show a great acceleration both quantitatively and technologically.

A study by the Defense Industry giant Raytheon has shown that among the technological trends that will determine in the future's war and in the third 'offset strategy' of the USA, the main artificial intelligence, innovations that will raise human-machine interaction, intelligent production technologies, micro- drones, weapons, cyber warfare, small & smart ammunition, and atomic particles.

Developments in the field of computer and robotic technology show that the future of automated systems in warfare environment will leave its place with autonomous systems. Unlike autonomous systems, autonomous systems will operate with a range of behavior options and state analyzes, rather than a single behavioral pattern. In this case, it will be an important part of both the strategic and military-ethical issues in the future of the war, although it is fundamentally a question of 'how robots think' based on software.

In sum, it is likely that developments in cyber skills will accelerate the transition of military strategies and concepts from platform-centric approaches to network-centric approaches. It is clear that the superiority of cyberspace in the future war and operation environment will naturally provide an advantageous position in information superiority and network-centered

capabilities. The 'Fruit Garden Operation *' - Mivtza Bustan * - which Israel carried out in 2007 with the aim of breaking the nuclear program of the Syrian Ba'th regime is a striking example of the use of cyber-electromagnetic activities as an attack in network-centered operations. Within the scope of the operation, al-Kibar was destroyed by the Israeli Air Force, a nuclear facility with strong suspicions that Syria was carried out with the help of North Korea and for military purposes. It is reported that some Israeli aircraft fuel tanks have also been left in Turkey.

Open-source publications on the subject indicate that Israeli F-15 and F-16s benefit from integrated intelligence, electronic warfare and cyber warfare capabilities to overcome the Syrian air defense complex. Accordingly, the series of projects that BAE Systems contracted and was called Suter was designed for tasks such as infiltrating enemy computer networks and manipulating radars, and began experiments at Nellis Air Base in early 2000. Suter is being conducted concurrently with the NCCT (Network-Centric Collaborative Targeting), an advanced, network-centric intelligence-discovery-surveillance-targeting precision ammunition-based offensive complex for the US Air Force.

Technical reviews of the topic reveal that Suter is more of a 'hacker' than a JAMMER, and it is stated that 'hacking' technologies and concepts related to computers have been combined with electronic espionage activities. It is also noted that Israel has used its 'Suter-like' systems since the Second Lebanon War in 2006 and benefited from these systems during the 2007 Fruit Garden Operation, as well as receiving instant data support from the US regarding the situation of Syrian air defence systems.

CONCLUSION

Although it seems certain that the cyber skills will be a serious game changer in the future of the war environment, it is not possible to say that a cyber-warfare has yet to be fully met by the armed conflicts law. Likewise, it is difficult to be optimistic about the establishment of a regulatory international mechanism for offensive cyber skills and the establishment of a verification regime. Because almost no country will be willing to open its own information and computer infrastructure to international control. In addition, some steps to date in the disarmament of cyberspace come from authoritarian regimes such as the Russian Federation and the People's Republic of China, causing serious doubts about the possibility that packages

on the Internet where individual freedoms are put in jeopardy under the name of trustworthy measures. In addition to those mentioned, it is unlikely that countries that have achieved significant advantages over technological capabilities, particularly in the United States, will be able to make an international bargain on the subject capabilities and capabilities.

On the other hand, it is important to establish an international legal norm and even an international mechanism for cyber-space conflicts. Serious problems can be encountered if these are not achieved, because it is considered that the cyber technology will reach 'critical mass' in the coming years. The 'critical mass' stage will then become a game-changing force multiplier in terms of the national power capacity of the developmental level countries in cyber-electromagnetic technologies, as well as the kinetic effects and secondary damage capacity will reach the limits of control.

It should be noted that not only 'weapons' but also 'targets' in this frame feed the trends outlined above. As the level of technological development increases, the economies of the countries, critical national infrastructure and social interactions become increasingly digital, becoming more dependent on computer networks and telecommunication facilities. Therefore, 'target options' of offensive cyber skills are expanding more and more every day. More crucially, facility infrastructure used for scientific research and civilian purposes, as well as for military programs in the CBRN field (chemical-biological-radiological-nuclear), is increasingly based more on SCADA systems. For this reason, it is a serious requirement to limit offensive cyber skills and attempt to establish norms for cyber-space conflict situations before the conclusion of the previously reported 'critical mass' phase.

In this period of dizzying development, it is useful to underline a few points as advice in the production of cybercrime for Turkish decision-makers. The first and most important parameter is the timing. Nations that are making the necessary investment in the technology competition today are expected to face a serious erosion in the national power capacities of the states that do not make investments in the years 2010, while the 2020s will overtake their investments in all areas of international competition (including peace and war periods) in the 2020s. Prerequisites for such investments are: scientific, innovative thinking with doctrine, human capital, inter-institutional coordination and coordination. Secondly, it is very important to be absolutely active in the cyber-space international legal normative process and to determine the diplomatic position. Because, the game rules in cyber-space are still in the process of being

determined. Thirdly, it is vital that Turkey focuses sensitively on the size of the cigarette in the risk and threat assessments that may arise either from other states or from terrorist organizations. In the national security analyzes mentioned, the main objective should be to minimize the strategic surprise factors that may arise from 'lack of imagination'. Finally, it is imperative that the academic resources and think-tanks in our country be encouraged to conduct research and debate on the fields of cyber conflict and cyber technology.

The wider framework of cyber conflicts, the narrower framework of cyber warfare, the basic finding of this work will be at the forefront of the other aspects of war and the nature of its partnership with technological developments. In this context, to focus on combinations such as cyber warfare and electronic warfare, cyber warfare and space technology, and even cyber warfare and biological warfare, can provide a more realistic vision of future predictions.

In today's and tomorrow's warfare environment, cyber-electromagnetic abilities will be critical in terms of network-centred joint operations against complex defences, especially called A2 / AD (Anti-Access / Area Denial). Therefore, this study will show that the centre of future wars will be shaped around C4ISR (military command-control-communication-intelligence-surveillance-exploration) networks, military satellite communications capabilities, cyber-electromagnetic facilities and capabilities and information- It foresees. It is likely that the main tasks will be to protect the subject systems from enemy penetration, and to stop the similar systems of the enemy.

Finally, it seems essential to develop a new paradigm, especially in the conflict situations that the West and NATO define in the classical sense 'under the battlefield'.

REFERENCES

Arimatsu, L. (2012). A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations. *4th International Conference on Cyber Conflict*, Available at: https://ccdcoe.org/publications/2012proceedings/2_3_Arimatsu_ATreatyForGoverningCyber-Weapons.pdf (Accessed at: 18/12/2017).

ASELSAN.(2017). Strategic Plan Summary. Availabe at: http://www.aselsan.com.tr/en-us/InvestorRelations/financial-data/Documents/Investor%20Presentations/ASELSANStrategicPlanSummary2017-2021.pdf (Accessed at: 18/12/2017).

Ball, Y. D. (2017). Protecting Falsehoods with a Bodyguard of Lies: Putin's Use of Information Warfare. *Research Paper NATO Defense College*, Available at: http://www.ndc.nato.int/news/news.php?icode=1017 (Accessed at: 18/12/2017).

Ganuza, N., Hernandez, A. and Benavente, D. (2011). An Introductory Study to Cyber Securıty in NEC. *CCDCOE*.

Geers, K. (2017).Cyberspace and the Changing Nature of Warfare. *Keynote Speech*, Available at: http://www.csl.army.mil/SLET/mccd/CyberSpacePubs/Cyberspace%20and%20the%20Changing%20Nature%20of%20Warfare.pdf (Accessed at: 18/12/2017).

Ottis, R. and Lorents, P. (2010). Cyberspace: Definition and Implications. *CCDCOE*.

Schmitt, M. N. (1999).Computer Network Attack And The Use Of Force In Internatıonal Law: Thoughts On A Normatıve Framework. *Columbia Journal of Transnational Law*, Vol. 37.

Sofaer, A. D., Goodman, S. E., Cuellar, M.F., Drozdova,E.A., Elliott, D.D., Grove, G.D., Lukasik, J.S.,Putnam, T.L., Wilson,G.D. (2000). A Proposal for An International Convention on Cyber Crime and Terrorism. Stanford University, Available at: http://cisac.fsi.stanford.edu/sites/default/files/sofaergoodman.pdf (Accessed at: 18/12/2017).

SİBER UZAYDA AKTÖR - GÜÇ İLİŞKİSİ

Sevda KORHAN[*]

Özet

Siber alanın hızla büyümesi dünya siyasetinde önemli bir bağlamdır ve siber, gücü kendisine bağlamaktadır. Anonimlik unsuru, güvenlikte asimetrilerin varlığı, siber araçlara erişmenin maliyetinin düşük olması gibi sebepler devletdışı aktörlerin de siber alanda sert ve yumuşak bir güç sunma kapasitesine sahip olmalarını kolaylaştırmaktadır. Siberin doğasında var olan özellikler, aktörler arasındaki güç farklılıklarını önemli oranda azaltmakta ve bu durum 21. yüzyılda küresel siyaseti simgeleyen başat unsurların "gücün dağılımı" veya "gücün yayılması" gibi konular üzerinde şekillenmesine sebebiyet vermektedir. Devletlerin, özellikle büyük güçlerin kara, deniz veya hava gibi alanlarda söz sahibi oldukları gibi siber alanda da hâkimiyet kurmaları kolay değildir. Dolayısıyla devletler, siber alanda devlet-dışı aktörler tarafından güçlü bir meydan okumayla karşı karşıya kalmaktadırlar.

Anahtar Kelimeler: Siber Alan, Güç, Aktör, Devlet, Devletdışı Aktör

ACTOR - POWER RELATIONSHIP IN CYBERSPACE

Abstract

The rapid growth of the cyberspace is an important domain in world politics, and cyber is connecting its power to itself. The anonymity, the presence of safety asymmetries, and the low cost of accessing cyber tools make it easier for non-state actors to have a hard and soft power delivery capability in the cyberspace. The inherent characteristics of cyberspace considerably reduce the power disparities between actors, and this leads to the formation of dominant

[*] Master Öğrencisi, Selçuk Üniversitesi, İİBF-Uluslar arası İlişkiler Bölümü, E-mail: korhansevda@gmail.com

elements, which symbolize global politics in the 21st century, on issues such as "distribution of power" or "diffusion of power". It is not easy for the states, particularly great powers to dominate the cyberspace, as they have a say in domains such as land, sea or air. Therefore, the states are faced with a strong challenge by the non-state actors in the cyberspace.
Key Words: Cyberspace, Power, Actor, State, Non-State Actors

Giriş

Genellikle uzmanlar arasında kürselleşme süreciyle beraber uluslararası ilişkilerin temel koşullarının değiştiğinden kuşku duyulmamakta (Zacher, 1992:58) ve bilgi devrimi sıklıkla değişimin önemli bir sürücüsü olarak adlandırılmaktadır (Castells, 1996:16). Modern hayatın pek çok alanında bilginin egemen olması ve yayılması bu dönemin 'bilgi çağı' olarak adlandırılmasına neden oldu. 'Bilgi toplumu', 'siber-terörizm', 'siber-alan', 'e-ticaret' gibi terimlerin yanı sıra "bilgi devrimi", "bilgi çağı" hatta "bilgi çağı ötesi" ya da "post-information age" gibi ifadeler de bu süreçle beraber literatüre girmiş oldu. Bu konuda esas tartışma yaratan durum ise, bilgi devriminin devleti ve uluslararası sistemi nasıl etkilediği meselesi olmuştur.

Siber, küresel bir alandır. İnternet bağlantısına sahip bir bilgisayara, bir akıllı telefona veya başka herhangi bir mültimedya cihazına erişebilen herkes tarafından kullanılabilir. Dolayısıyla bu alanda farklı ihtiyaçlar, amaçlar ve niyetler taşıyan birçok aktör mevcut. Bazıları yalnız başına davranırken bazıları ise daha resmi yapılarla birlikte hareket etme eğilimindedir. Roller duruma göre değişebilir veya birbiriyle örtüşebilir. Aktörler ise zaman içinde veya mevcut hedeflerine bağlı olarak kategoriler arasında dolaşabilirler. Dolayısıyla siber uzayın meydana getirdiği yoğun ve hızlı etkileşimler, uluslararası ilişkilerin önemli iki kavramı olan "güç" ve "aktör" üzerinde ciddi değişikliklere yol açmış ve varsayımlarını zor duruma düşürmüştür.

Literatürde bu konuyla alakalı çeşitli argümanlar ileri sürülürken, yaygın olarak küresel bilgi ağının ulus ötesi mimarisinin, hayali olan sınırları tamamen ortadan kaldırdığı düşünülmüştür. Bilgi teknolojilerinin hem askeri hem de sivil alana uygulanması, siyasal, askeri ve sivil alanlar arasındaki sınırların bulanıklaşmasına yol açmış ve devlet-dışı aktörlerin de bilgi teknolojisine sahip olarak daha da güçlenmesine yol açmıştır. Dolayısıyla gücün dağılımı uluslararası sistemin bir parçası olarak yalnızca devletlerarasında değil, aynı zamanda özel işletmeler, politikacılar ve ulus ötesi kuruluşlarla birlikte giderek daha karmaşık hale gelmiştir (Papp ve Alberts, 1997:285).

Yeni bilgi ve iletişim teknolojilerinin dünya çapında uygulanmasının bireysel, ekonomik, siyasi ve kültürel tüm aktörler için uygun ortam sağladığı düşünülmekte ve her türlü bilgiye erişimin ve bilgi akışının yaygınlaştırılmasının önemini vurgulamaktadır. Aynı zamanda bu teknoloji geniş ölçüde, bu toplumsal aktörlerin devlete karşı güçlenmesine yol açmaktadır. Bu teknolojik araç uygulamalarının devlet kurumlarının etkinliğini arttırdığına ve devlet ile toplum arasında daha yakın bir işbirliği kurma potansiyeline sahip olduğuna inanılmaktadır. Bununla birlikte, bilgi toplumu kavramı ile bağlantılı olarak, birçok kuramcı ve siyasetçi bilgi çağında internetin demokratik bir etkiye sahip olduğunu iddia etmektedir (Loader, 1997:1-19).

Genel itibariyle bakıldığında esasında siber uzayda güç ve aktörün ne olduğu ve ne noktada birbiri ile ilişkili olduğu bu çalışmada tartışılacaktır. Akademik çerçevede çokça tartışılan ve derin fikir ayrılıklarına sebep olan bu konunun çalışılmaya ihtiyacı vardır. Nitekim aktörler arasında gücün dağılımı konusunda bir uzlaşmaya varılamaması ve bunun sonucunda ortaya çıkan çelişkiler de bu çalışmanın konusu olacaktır. Öte yandan, devletlerin ve devlet-dışı aktörlerin siber alanda güç sahibi olabilmek için ihtiyaç duydukları araçlar ve bunları kullanabilme kapasitelerinin önünde ortaya çıkan engeller de çalışmada analiz edilecektir. Son olarak, çalışmanın kilit noktasını oluşturan güç dağılımı üzerinde durulacaktır.

SİBER UZAYIN KAVRAMSAL ÇERÇEVESİ

"Siber" kelimesi William Gibson tarafından 1984 yılında yayınlanan *Neuromancer* adlı kitabında kullanılmıştır. Gibson siberi, insan sisteminde bilgisayarlardan soyutlanan her bir verinin grafiksel bir gösterimi olarak tanımlamaktadır. Diğer taraftan Gibson, daha soyut bir tanımlamaya giderek bu kavramı rızaya dayalı bir halüsinasyon türü veya düşünülemez karmaşıklık olarak da tanımlamıştır (Gibson, 1984:128). Günümüzde sibere kavramsal bir çerçeve kazandırmak pek de kolay bir durum olmamakla beraber, siber kavramı çeşitli şekillerde tanımlanmaya çalışılmaktadır.

Son otuz yıldır siber, 'günlük yaşamın dokusuna dokunmuştur' ve bugün modern toplumun tüm alanlarına nüfuz etmektedir. En yeni rakamlar, Haziran 2017 sonu itibariyle, 4.8 milyar insan ya da dünya nüfusunun %51'nin internet kullanıcısı olduğu yönünde(internetlvestats, 2017). 2000 yılından bu yana internet kullanıcıları sayısı hızla artmaktadır (Buchan, 2016:11). Gerçekten de teknoloji, yaşam biçimimizi büyük ölçüde değiştirdi. Bilgi çağında yaşadığımızı hissettiğimiz sınırsız araç mevcut. Kültür, ticaret, eğlence ve araştırma gibi çeşitli sektörleri de

içine alan sanal bir dünya, tüm kesimlerde devrim niteliğinde değişikliklere yol açtı. Bilgisayar ve telekomünikasyonun angaje olması ve bu teknolojilerin düşük bir maliyetle dünya çapında erişime açılması bir dönüşüm yarattı. Ancak siber alan tarafından sunulan muazzam fayda ve fırsatlara rağmen siber alanın yarattığı tehdit ve zaaflarda da artış göstermiştir. Günümüzde bilgi iletişim teknolojisinin gittikçe artan önemi konusunda fikir birliğine varılmış olmasına rağmen, bu gelişimin güvenlik ve diğer konulardaki etkisini de belirlemekte yarar var.

Siber alana olan bağımlılık pek çok yerde yaygınlaştığından, siber saldırı ve siber istihbarat gibi tehditlerin de aynı oranda artış gösterdiği gözlenmektedir. Her gün sayısız siber saldırının gerçekleşmesi önemli tehditleri önemsiz tehditlerden ayırmayı zorlaştırmaktadır (Haley, 2016). Bilgi teknolojisinin yaygınlaşmasıyla beraber, devletlerin zayıf yönlerinin sömürülmeye açık hale gelmesi, çeşitli aktörlerin ciddi yıkımlara sebep olabilecek güç ve yeteneklere daha kolay bir şekilde sahip olmasının yolu açılmıştır (Nagorski, 2010:1). Bugün sivil kuruluşların çoğunun fiziki altyapısının ve hizmetlerinin, ciddi oranda internet ve bilgi ağlarına bağımlı olduğu görülmektedir. Enerji, trafik, su, bankacılık, eğitim, sağlık, borsa, ulaşım gibi birçok hizmet internete bağımlı hale gelmiştir ve bu durum, bu alanlardan herhangi birindeki güvenlik açığının diğer bütün alanlara büyük zararlar verebileceğinin ve ülkenin kritik altyapılarını çökertebileceğinin işaretidir.

İnternetin gelişmesiyle beraber içinde yaşadığımız gezegen daha küçük bir hal alarak sınırlar arasında önemli derecede etkileşimi artırmıştır. Fakat internetin sınır-aşan özelliği sebebiyle siber uzay siber suçlular, siber saldırganlar ve organize suçlular için uygun bir ortam yaratmıştır. Bu sebeple ülkeler, etkili bir siber güç ve caydırıcılık politikasını sağlamak için çalışmalar yürütmeye başlamışlardır (Nagorski, 2010:9). Siberle ilgili faaliyetler, devletlerin sınırlarını aşarak geniş bir alana ulaşabildiklerinden dolayı, devletin geleneksel askeri şiddet unsurlarından oldukça farklıdırlar. Şimdiye kadar 140'tan fazla devlet siber silahlara sahip olmuş ve 30'dan fazla ülke ise askeri birimlerinde siber alanla ilgili birlikler ya da siber ordular kurmuşlardır (Jensen, 2012:780).

SİBER UZAYDA AKTÖRLER

Uluslararası İlişkiler disiplini içerisinde, uluslararası olarak adlandırılan geniş sahanın, aktörlerinin ve bu aktörlerin ilişki biçimlerinin tanımlanması daima önem teşkil etmiştir. Ulus-devletler, siber alanın yönetiminde, izlenmesinde ve düzenlenmesinde önemli bir rol

oynamasına rağmen devletlere karşı bağımsız olarak güçlerini kullanan devlet dışı aktörler de mevcuttur. Siber alanda farklı motivasyonlara sahip çok sayıda aktörün varlığı, anonimlik, ve kimliğini gizleme gibi yöntemlerle nedeniyle siber uzayda tam olarak ne olup bittiğini ve sorumlunun kim olduğunu belirlemeyi zorlaştırmaktadır. Bu belirsizlikler sadece siber eylemin amacını karmaşıklaştırmakla kalmaz, saldırıya uğrayanların misilleme yapma yeteneklerini de zorlaştırmaktadır. Çünkü siber alanda atıf yapmak zor olmaktadır (Grohe, 2015:9-10).

Siber uzayın, gün geçtikçe daha fazla insanı ve diğer aktörleri içine sürükleyerek kendi alanında aktör sayısını maksimize etme eğiliminde olduğu görülmektedir. Bireyler ve toplumlar ağlar aracılığıyla sınırlar dâhilinde veya sınır aşan biçimde sosyalleşmeye başlamışlardır. Van den Berg ve Boeke şu anda hangi aktörlerin farklı bir rol oynadıklarını; kavramsal olarak olayların türleri, bu aktörleri neyin yönlendirdiği ve amaçlarının neler olduğu gibi sorunları netleştirmeye yönelik yeni yöntemler geliştirmektedirler (Berg ve Boeke, 2016). Çalışmanın bu bölümünde siber uzayda etkili olan devlet ve devlet-dışı aktörlerin rolleri incelenecektir.

Devletler

Realistlere göre, uluslararası ilişkilerde devlet dışı aktörlerin pek önemi yoktur. Devlet her koşulda diğerlerinin hareket alanını belirleyen temel ya da merkez aktördür (Aydın, 2004:36-38). Edward Hallett Carr, George F. Kennan, Hans Morgenthau gibi realist yazarlar uluslararası sistemin başlıca aktörü olarak devleti görmüşlerdir (Carr, 1946; Kennan, 1966; Morgenthau, 1948). Realizmin aksine liberalizm ise birey de dâhil olmak üzere devlet dışı aktörleri siyasal ve toplumsal süreçlerin işleyişinde önemli görmektedir. Dahası liberaller, devlet tercihlerini ve davranışlarını hem ulusal hem de uluslararası sivil toplum tarafından kısıtlanmış ve etkilenmiş olarak görmektedir (Moravcsik, 1997:513). Ancak realist paradigmaya göre devletler güvenliklerini garanti altına almak ve güçlerini arttırmak için başat aktörler olarak kabul edilmiştir. Fakat ilerleyen bölümlerde değineceğimiz gibi siber alan, devletin bu başat konumuna meydan okumaya başlamıştır.

Küreselleşme süreciyle beraber Wesphalya ulus-devlet düzenine karşı kritik birtakım güçler sivrilmeye başlamıştır. Küreselleşme sürecinin ortaya çıkmasıyla beraber ulusal sınırları aşan "uluslararası toplum", "karşılıklı bağımlılık", "küresel işbirliği" gibi fikirler 20. Yüzyılın ikinci yarısından itibaren uluslararası sistemde geniş yer tutmaya başladı. Bu durum, birçok ulusal

hükümet, uluslararası kurum ve sivil toplum aktörlerinin küresel sorunlarla yüzleşmek için birlikte hareket etmeye başlamasıyla sonuçlandı.

Çevre, insan hakları, ekonomi, küresel ısınma gibi küresel bazı sorunların çözümünün küresel işbirliğiyle mümkün olabileceği gerçeği gün geçtikçe anlaşılmıştır. Küresel iletişim ağı, teknolojideki yenilikçi gelişmelere dayalı hızlı bir gelişme göstermeye devam ederken, devletin ulusal ağlarını koruma altına alma ya da güçlendirme yeteneği giderek hizmet sağlayıcıları, özel sektör, uzmanlar, ajanslar ve işbirliği yapan hükümetler arasındaki karşılıklı bağımlılığa dayanmaya başlamıştır. Dolayısıyla uluslararası işbirliği, ağ güvenliği, ağ standartlarının geliştirilmesi ve uygulanmasına yönelik bir çözüm olarak görülmüştür (Felicia ve Hensel, 2007:6). Dolayısıyla siber alandaki devletler ve devlet dışı aktörler arasında çizgilerin kısmen bulanıklaştığı söylenebilir çünkü ulus devletler, siber alanda amaçlarını gerçekleştirmek için "güçlendirme" yoluna başvurmaktadırlar. Hedeflerini yerine getirmeleri için paralı askerleri harekete geçirmektedirler. Örneğin, ABD seçimlerine Rusya'nın siber saldırı iddialarına yönelik olarak Demokratik Ulusal Komite ve Obama Yönetimi tarafından yapılan "yalnızca Rusya'nın en üst düzey yetkililerinin bu faaliyetlere izin vereceğine inanıyoruz" şeklinde yaptıkları açıklamada ABD'nin saldırıyı Rusya'nın kendi eliyle gerçekleştirmiş veya kontrol ettiği ve yönlendirdiği bazılarının olduğunu ima ettiği görülmektedir(Ackerman, 2016).

Bu işbirliği ve yönlendirmeye rağmen devletler güvenlik odaklı bir yaklaşımla bu alanda da devamlılığını sağlamaya çalışmaktadır. Birçok devlet tarafından "*beşinci muharebe alanı*" olarak adlandırılan siber uzay (diğerleri hava, kara, deniz ve uzaydır), devletlerin bu alandaki güçlerini garanti altında tutmak veya maksimize etmek için çeşitli stratejiler geliştirdikleri bir alan haline gelmiştir (Çelik, 2015:32). Siber uzayda devletlerarasında başlamış olan rekabetin doğal bir sonucu olarak devletler, gerek siber savunma stratejilerini geliştirmek için, gerekse siber saldırı kapasitelerini arttırmak için siber ordulara önemli ölçüde yatırımlar yapmaktadırlar.

Bununla beraber devletler, yalnızca rekabet etmenin rasyonel bir davranış olmadığını bilen varlıklar olarak, fiziki alanda olduğu gibi, sanal alanda da taraflarını belirleyerek, savunma ve istihbarat sistemini güçlü tutmaya çalışmakta ve bu amaçla ittifaklar kurmaktadırlar. Örneğin, Eski ABD Başkanı Barack Obama, 2016 itibariyle güvenliği arttırmak maksadıyla siber alana ayırdıkları bütçeyi %35 oranında arttırdıklarını ilan ederek, bu alana verdikleri önemi bir kez daha vurgulamıştır (Gücüyener, 2016). ABD'nin ulusal istihbarat direktörü Mike McConnell,

2010'da kaleme aldığı *Kaybettiğimiz siber savaşı nasıl kazanacağız* adlı çalışmasında, dünyanın 1950'li yıllara döndüğüne işaret ederek nükleer gücün artması için uğraşan devletlerin artık siber saldırılarla baş etmede kullanabileceği yöntemler geliştirmesi gerektiğini savunmuştur (Nagorski, 2010:1).

Geleneksel devlet-güç siyasetinin siber uzayda oynadığı rolün farklı bir biçimde işlediği görülmektedir. Siber, yalnızca uluslararası güvenlik alanlarında aynı aktörler tarafından kullanılan bir araç ya da silah olarak adlandırılabilir. Siberin yönetilemeyen alanında, devlet-iktidar politikası halen yürürlüktedir. Ancak geleneksel saldırı biçimlerinin aksine burada kurallar yoktur ve ulus devletler tarafından sıkı bir şekilde uygulanabilen kısıtlamalar mevcut değildir (The Cipher Brief, 2016). Dolayısıyla Sony, DNC veya OPM'ye karşı yürütülen saldırılar gibi büyük ölçekli saldırılar artık yalnızca ulus devletler tarafından gerçekleştirilebilecek eylemler olmayabilir (Schmitt, 2014).

Devlet-Dışı Aktörler

Devlet dışı aktörler siber alanı, bir çatışma aracı olarak kullanmaktadır. Devlet-dışı aktörlerle ilgili bu varsayımlar beş noktada özetlenebilir:

- Devlet dışı aktörler çatışmalarda siber alanı kullanır;
- Yenilgiye uğratmak, siber faaliyet alanlarındaki nihai hedefidir;
- Bu, stratejik bir anlatı yaymak ve yumuşak güç kurmak suretiyle yapılır;
- Amaçlarına ulaşmak için gerilla taktikleri kullanırlar;
- Etkinlik, organizasyonun ve kaynakların seviyesine göre belirlenir (Cathrine ve Wilhelmsen, 2014:5).

Aktör	**Motivasyon**	**Hedef**	**Yöntem**
Sıradan vatandaşlar	Hiçbiri veya zayıf	Herhangi biri	Dolaylı
Çocuklar	Merak, heyecan, ego	Bireyler, şirketler, hükümetler	Daha önce yazılmış komut dosyaları ve araçlar

Hackerlar	Siyasi veya toplumsal değişim	Karar vericiler veya masum kurbanlar	Hizmet durdurma veya DDoS saldırısı vasıtasıyla protesto gösterileri
Siyah Şapkalı Hackerlar	Ego, kişisel düşmanlık, ekonomik kazanç	Herhangi biri	Zararlı yazılımlar, virüsler, güvenlik açığı istismarları
Beyaz şapkalı hackerlar	İdealizm, yaratıcılık, yasalara saygı	Herhangi biri	Penetrasyon testi, yama
Gri şapkalı hackerlar	Belirsiz	Herhangi biri	Çeşitli
Vatansever Hackerlar	Vatanseverlik	Kendi ulus-devletinin düşmanları, dolandırıcılık, diğer kurbanlar	DDoS saldırıları, yolsuzluklar
Siber İçerikler	Finansal kazanç, intikam, şikâyet	İşveren	Sosyal mühendislik, arka kapılar, manipülasyon
Siber teröristler	Politika veya toplumsal değişim	Devletler, Ötekiler ya da diğer kurbanlar	Bilgisayar tabanlı şiddet veya imha
Kötü yazılım yazarları	Ekonomik kazanç, ego, kişisel düşmanlık	Herhangi biri	Güvenlik açığının kötüye kullanımı
Siber dolandırıcılar	Finansal kazanç	Bireyler, küçük şirketler	Sosyal mühendislik
Organize siber suçlular	Finansal kazanç	Bireyler, şirketler	Dolandırıcılık, kimlik hırsızlığı,

			şantaj için DDoS kötü amaçlı yazılım
Şirketler	Finansal kazanç	BİT tabanlı sistemler ve altyapılar (özel ya da kamu)	Saldırı veya etki operasyonları için çeşitli teknikler
Siber casusluk ajanları	Finansal ve siyasi kazanç	Bireyler, şirketler, hükümetler	Bilgi edinme teknikleri
Siber savaşçılar	Yurtseverlik, mesleki gelişme	Kendi ulus devletinin düşmanları, bireyler, şirketler	Grup yetenekleri

Tablo 1. Siber Uzayda Devlet-Dışı Aktörler (Sigholm, 2013:11).

Tablo-1'den de görüldüğü üzere, devlet-dışı aktörler siber uzayda farklı motivasyon, hedef ve yöntemlerle hareket ederek bu alanda faaliyetlerini yürütmektedirler. Kimi devlet açısından kolaylıklar sağlarken kimisi ise büyük sorunlara sebep olabilmektedir. Katharina Ziolkowski, siber uzaydaki birçok devlet dışı aktörün ortaya çıkardığı kötü niyetli eylemlerin kim tarafından yapıldığının belirlenmesi ve bu doğrultuda misilleme yapılmasının zorluğuna işaret etmektedir(Pihelgas, 2013:40). East West Enstitüsü'nün (EWI) *Siber Uyuşmazlığı Yönetmek İçin Kurallar: Siber Uzayda Cenevre ve Lahey Sözleşmelerinin Oluşturulması* başlıklı çalışmasında, siber alanda devlet dışı aktörlerin sorunlarına değinildi. Raporda Rusya, ABD ve diğer ilgili taraflar, siber savaşçıların devlet dışı aktörler olabileceği gerçeğinden hareketle sözleşme ilkelerinin nasıl en iyi şekilde yürütülebileceğini değerlendireceklerdir (Rauscher, 2011). Fakat devlet dışı aktörlerin siberle olan ilişkisi hakkındaki bu değerlendirme, henüz sonuçlanmamıştır. Devlet dışı aktörlerin giderek artan önemi küreselleşme sürecinin hız kazanmasıyla beraber uluslararası ilişkilerin her alanında belirginleşmiş bir meseledir (Gady, 2011).

Sonuç olarak siber uzay, yarattığı olumlu havanın yanı sıra, aynı zamanda uzun süredir çatışmada kullanılan bir araç haline gelmiştir. Siber uzayda rekabet eden hacker çeteleri aktif olarak birbirleriyle etkileşim halindeyken, protesto grupları fikirlerini sanal vandalizm yoluyla

seslendirmekte, suç örgütleri kolay kazanç sağlamak amacıyla kötü amaçlı yazılımları yaymakta ve gizli aktörler ise yasadışı istihbarat topluluğuna hizmet etmektedir. Devlet dışı aktörlerin yaygınlaşmasında siber alan, on yıllar öncesinden başlayan bir süreci hızlandıran ve güçlendiren bir "güç çarpanı" olarak karşımıza çıkmaktadır. Bununla birlikte, devlet dışı aktörlerin belirsiz ve farklı karakterleri, bu aktörlerin hareketlerini izleme güçlüğü ve kritik altyapılar üzerinde yaratabilecekleri yıkıcı güç nedeniyle siber alanda benzersiz bir sorun teşkil etmektedir.

SİBER UZAYDA AKTÖRLER ARASINDA GÜÇ DAĞILIMI

Bu bölümde özellikle yumuşak bir güç unsuru olarak siber uzay, güç araçları, aktörlerin gücü kullanma kapasiteleri ve devletdışı aktörlerin siber uzayda güçle ilişkisi gibi konular tartışılacaktır.

Yumuşak Güç Unsuru Olarak Siber Güç

Uluslararası İlişkiler teorisyenleri 20. yüzyılın başından itibaren gücün ne olduğunu ve güç edinmenin amacını sorgulamışlardır. Özellikle realistler güç üzerinde çalışmalar yapmış ve realist teori, gücü daima maksimize edilmesi gereken nihai bir hedef olarak görmüştür. Genel anlamda güç kavramın, "başka aktör üzerindeki etki kapasitesi" olarak tanımlanır. Aslında realizmin güç tanımı, bir *hard power (sert güç)* unsuru olan askeri güç ile ilişkilendirilir ve diğer unsurlar göz ardı edilir. Realistler için uluslararası arenada güvenlik ikileminin (*security dilemma*) yarattığı çatışmayı önlemek veya çıkar maksimizasyonunu sağlamakta rol oynayan en önemli olgu güçtür (Guzzini, 2001:18). Dahası güç, Realist teori için devletin uluslararası politikada temel önceliklerini şekillendiren ve bu önceliklere ulaşmasını sağlayan ana unsurdur.

Bu bağlamda Realist teori gücü daima maksimize edilmesi gereken nihai bir amaç olarak görmekte ve genellikle bu gücü askeri güç ile bağdaştırma eğiliminde olmaktadır. Ancak 21. Yüzyılda gücün en önemli kaynağı olarak bir *Soft power* (*yumuşak güç*) unsuru olan "bilgi teknolojisi" gösterilmektedir (Nye, 2011). Bilgi teknolojisine veya siber güce sahip devletlerin, diğer devletlerden daha güçlü olduğu yönünde iddialar bulunmaktadır. 21. yy'da Joseph Nye'ın kavramsallaştırdığı *soft power*'ın varlığı önem kazanmaya başlamış, bu bağlamda "siber güç" de bir yumuşak güç unsuru olarak karşımıza çıkmıştır (Nye, 2011).

Peki, siber güç nedir? Bu kavram, klasik güç anlayışından çok da soyutlanamayacak bir tanımlamaya sahip. Siber güç; "Siber alanı, güç araçları aracılığıyla diğer aktörleri etkilemek için kullanabilme yeteneği" olarak tanımlanabilir. Realist teorinin iyi okuyamadığı küreselleşme süreciyle beraber akademisyenler, diğer konulara ek olarak gücün siber alana kayması durumuna dikkat çekmeye başlamışlardır. Çünkü ağlar üzerinden yapılan faaliyetler arttıkça devletler altyapılarını bu ağlar üzerinden sağlamaya çalışmışlardır.

Geleneksel savaş döneminin konusunu, çoğunlukla devletler arasındaki güç mücadelesi oluşturmuştur. Çatışma ve güç oyunlarının dünya siyasetine hâkim bir özelliği olduğu, realist teori tarafından sık sık vurgulanmıştır. Realist yazarlar, devlet gücünün bir indeksi olarak askeri gücün önemini vurgulamışlardır. Yumuşak gücün gerçekliği ve önemi çok tartışmalı bir konu olmakla beraber realistler doğal olarak bu kavramın en büyük eleştirmenleri arasındadır. Realistler ekonomik faktörleri, ulusal gücü yansıttıkları ya da etkiledikleri ölçüde önemli gördükleri halde, asıl gücün askeri güç olduğunu iddia etmektedirler.

Görüldüğü üzere geleneksel anlamda temel güç faktörleri olarak askeri ve ekonomik güçler görülürken şimdi ise "siber güç" de önem kazanmıştır. Bu nedenle bilgi, inanç ve düşünce üzerindeki kontrol, askeri ve ekonomi gibi somut kaynakları kontrol altına almanın bir tamamlayıcısı olarak görülmektedir. Bu düşüncenin büyük kısmını, savaş alanının sibere yayılması nedeniyle savaşın doğasında önemli bir değişikliğe gidildiğine olan inanç oluşturmaktadır (Vlahos, 1998:497-525). Bu tartışmayla ilgili en yaygın olarak kullanılan etiket, baskıdan ziyade kendine çekme yoluyla hedeflere ulaşma yeteneği olarak tanımlanan 'yumuşak güç'tür (Keohane ve Nye, 1998:81-94). Yumuşak güç; iletişim, eğlence ve fikirleri ifade eder ve güçlü bir kültürel ve psikolojik bileşeni vardır. Yumuşak güç ayrıca, başkalarını istenen davranışları üreten normlara ve kurumlara uymaya ikna ederek ya da onları kabul ettirerek hareket eder. Aslında burada dikkat çeken nokta, yumuşak güç kavramı ile yapısal gücün birbirine yakın olduğudur (Hart, 1976:294). Ancak uluslararası aktörler, daha az görünür olan bir güç biçimi olan yapısal gücü daha çok kullanmayı tercih ederler çünkü güç sahibi baskıya gerek duymaksızın hareket etme yeteneğine sahiptir (Volgy, Kanthak, Fraizer ve Ingersoll, 2004).

Öte yandan siber uzayın yarattığı güvenlik tehdidi ile birlikte realist okula bağlı güvenlik uzmanları, karar mercilerine hızlı bir şekilde siber dünyanın militarizasyonunu kabul etmeleri çağrısında bulunmuşlardır. Ayrıca devletlerin saldırgan ve savunma amaçlı siber yeteneklerini

geliştirmeleri gerektiğini savunmuşlardır. Stratejik planlamacılar tarafından yürütülen siber bir bileşenle ulusal güvenlik politikalarını geliştirme çabası birçok ülkede gerçekleştirilmiştir. Aynı şekilde, Avrupa Birliği ve NATO, ortak savunma politikaları geliştirmeye başlamışlardır (Bendiek, 2016). Bu doğrultuda devletin siber uzayda yeniden doğuşunu ve siber güç arayışı içerisinde olduğunu reddetmek zordur.

Siber Uzayda Güç Araçları

Siber alanda hizmetler, sunucular, web sayfaları vb. araçlar birbirine bağlıdır ve her bölüm farklı bir fiziksel bölgede yer alır. Ancak bu araçlar karşılıklı olarak birbirlerine bağımlı oldukları için birlikte çalışırlar. Bununla birlikte, her alanın farklı zorlukları vardır ve her alan üzerindeki hâkimiyet farklı bir teknoloji gerektirir. Siber uzayın büyük oranda fiziksel bir alan olmadığı gerçeğinden yola çıkarak siber alanda hâkimiyetin de önemli ölçüde farklı olduğu görülmektedir. Çünkü siber alanda fiziksel araçlar önemli oranda hâkimiyetini kaybeder ve yerini farklı taktik ve teknolojiye bırakır.

Siber uzay dört bileşenden oluşur. Bunlar kullanıcı, yazı, video, resim gibi paylaşılan bilgi, yazılımlar-protokoller ve fiziksel altyapıdır. Martin Libicki, siber alandaki katmanların her birine hükmetmek için gerekli olan araçları açıklamıştır. Libicki'ye göre ilk katman; fiziksel kablolardan ve anahtarlardan oluşur ve bu katman tahrip edici fiziki güç tarafından yönetilebilir. İkinci katman, bu sistemlerin kontrolünü elinde bulundurarak hâkimiyetini sağlayabilir. Üçüncü katman ise veri ile ilgilidir ve sansürleme yöntemiyle hâkimiyet kurabilir veya bilgiye erişimi kontrol edebilir. Dördüncü katmana gelindiğinde ise, bilişsel ya da pragmatik katmanın hakimiyetinin varlığı söz konusudur (Schmidt, 2016). Bu dört katman göz önüne alındığında siber alanda bilginin analiz edilmesi gerektiği ve her bilgi yeteneğinin geliştirilmesinin siber uzayda bir güç sahibi olmak için önem teşkil ettiği söylenebilir.

Siber alanda devletler, saldırılara karşı güvenliklerini koruyabilmek için çeşitli güç araçlarına ihtiyaç duymaktadırlar. Tüm devletlerin, anarşik, rasyonel ve güç mücadelesi içerisindeki birimler olduğunu kabul ettiğimizde siber uzay, uluslararası ilişkilerin bu temel oyuncularına yeni bir rekabet alanı sunmaktadır (Valeriano, 2016:142). Teknik açıdan bu yeni 'ortamın' gerçek dünyadan bağımsız olduğu düşünülse de siber uzayda yaşananlar, gerçek dünyadaki güç ilişkilerinin bir devamıdır. Tıpkı klasik anlamdaki ulusal güvenlik ve güç anlayışındaki gibi

devletler, siber alanda da güvenliklerini arttırmaya ve güçlerini maksimize etmeye çalışmakta ve bu bağlamda da etkili stratejiler geliştirmektedirler.

Devletler bu doğrultuda ilk adım olarak siber ordular kurmaktadırlar. Bugün dünya üzerinde resmi ve gayri resmi olarak faaliyet gösteren bir sürü siber ordu mevcut ancak ABD, Rusya, Almanya, Çin, İsrail, İran ve Kuzey Kore'nin siber ordularının olduğu bilinmekte. Onun dışında devletler eylem planlarıyla ya da caydırıcılık stratejileriyle savunma pozisyonu almakta ve bu durum daha çok güvenlik odaklı bir yaklaşımı temsil etmektedir. Diğer yandan devletler, *hard* ya da *soft power* araçlarıyla saldırıya geçmekte ya da etki alanlarını genişletmeye çabalamaktadırlar. Bu da daha çok güç odaklı bir yaklaşımı temsil etmektedir.

Devletler sert güç unsurlarını daha çok sistemleri çökertecek ya da fikri mülkiyet haklarını çiğneyebilecek şekilde kullanmakta ve hükümetler bunu genellikle ekonomik kaynaklarını artırmanın veya siyasi üstünlük sağlamanın bir yolu olarak yapmaktadır. Örneğin Çin, bu tür faaliyetlerde bir numaralı ülke olarak gösterilmektedir. Çin'in özellikle Batılı şirketlerin ticari sırlarını ele geçirdiği, ayrıca büyük çaplı savunma ve silah projelerinin gizli bilgilerine ulaşmaya çalıştığı iddia edilmektedir. Yumuşak güç uygulamasında ise genellikle siber bilgiler, başka bir ülkedeki vatandaşları cezbetmek veya bir ideolojiyi yaymak amacıyla kullanılabilmektedir. Bu durum bir çeşit "siber kamu diplomasisi" olarak da adlandırılabilir.

Devletlerin siber alanda yaptığı bir diğer faaliyet, siber uzmanlığı arttırmak ve bu alanda hacker yetiştirmektir. Ancak derin bilgisayar uzmanlığı bir avantaj olmasına rağmen siber alanda stratejik etki üretmek için çok yetersiz bir yol olarak görülmektedir. Bu konuda Col Stephen Korns'ın işaret ettiği gibi, birçok siber "silah" artık metod haline getirildi ve kişisel bir bilgisayara indirilebilen yazılımlar var. Estonya ve Gürcistan saldırılarında kanıtlanmıştır ki, çoğunluğu programlama veya bilgisayar bilimi olmayan uzman bireyler bile hazır programlarla saldırı düzenleyebilmektedir. Bu nedenle uzmanlaşmayı bir güç kıstası olarak almak yanlış olacaktır ve gücün buna göre ölçülmesi de eksik kalacaktır (Sheldon, 2011:97).

Aynı şekilde gücü ölçen bir diğer araç, Booze Allen Hamilton tarafından geliştirilen Cyber Power Indeks (CPI) aracıdır. CPI siber saldırılara dayanma ve güvenli bir ekonomi için gerekli olan dijital altyapıyı dağıtma becerisi olarak devletin siber gücünü ölçmek için kullanılan bir araçtır. Bu amaçla, bir devletin siber gücüne katkıda bulunan dört genel bileşen önerilmektedir. Bunlar; mevcut hukuki ve düzenleyici çerçeveler, ekonomik ve sosyal bağlam, teknoloji

altyapısı ve endüstri uygulaması bileşenlerinden oluşur. CPI, bir devletin savunma ve saldırı gücünü açıkça ölçmeye çalışır. CPI tarafından sağlanan bu ölçme işlemi aracılığıyla güce atıfta bulunmak cazip gelebilir fakat bu da misilleme söz konusu olduğunda güç ölçümü için yetersiz kalmaktadır. Çünkü bir devlet, misilleme sonucu oluşabilecek önemli bir hasarın farkındaysa, siber gücünü eksiksiz bir şekilde kullanmak istemeyebilir. Dolayısıyla bu durum CPI'e güçsüzlük olarak yansıyacaktır ve bu da sonuçların tutarsızlığını doğuracaktır (Gomez, 2013:3).

Yine bir güce atıfta bulunmak için geliştirilmiş bir diğer yöntem teori geliştirmek olmuştur. Zaten uluslararası ilişkiler öğrencileri için teori üretmeden yapılan bir güç tanımı eksik kalacaktır. Bir kavramın teorisini oluşturmak, kavramı anlamak açısından fayda sağlayacaktır. Biz de siber gücü bir teori olarak değerlendirmeye kalktığımızda "Bu teori pratikte nasıl kullanılabilir?" sorusu gündeme gelecektir. Böyle bir teori oluşturulduğunda nasıl bir etki yaratabilir ya da bu teori ne gibi görünmelidir? Bu konuda Harold Winston, siber alana uygulanabilen veya en azından herhangi bir girişimde bulunabilecek bir siber güç teorisinin oluşturulması için gerekli beş kriter ortaya koymuştur. Bunlar; (Winston, 2011:19-35).

- ***Alanı tanımlamak:*** Bu kriter, siber alan ve siber gücün ne olduklarıyla ilgili bilgi verir. Siber güç stratejik uygulaması araştırmaları, bu alanın olgunlaşmadığını kanıtlayan en az 14 siber uzay tanımı ortaya koydu. Dolayısıyla siber uzay ve siber güç tanımları konusunda bir fikir birliğine varmak, makul bir teori oluşmasına katkı sağlayacaktır.
- ***Seçilen parçaları kategorize etmek:*** Bu konuda Winston bir benzetmeye başvurarak şöyle bir öneride bulunuyor: "Siber gücü turuncu bir meyve olarak düşünün, dilimler halinde kesip, her birini inceleyin ve ardından bütünü yeniden oluşturmak için onları bir araya getirin." Winston'a göre bu şekilde siber gücü oluşturan parçalar veya araçlar daha kolay tanımlanabilir.
- ***Açıklamak:*** Burada siber gücün stratejik ortamda bozulma, aldatma, reddetme gibi istenen etkileri nasıl sağladığını açıklamak gerekir. Dahası bir teori, siber güçlerin en etkili olacağı koşulları belirlemeye çalışmalıdır.
- ***Diğer alanlara bağlamak:*** Bir teori, siber gücü daha geniş bir evrene bağlayabilmelidir, çünkü siber gücün hangi yönlerde diğer alanlarla etkileşime girdiğinin analiz edilmesi önemlidir. Örneğin siber güç; sürtüşmelerden, kültürler arası farklılıklardan, ekonomi gibi alanlardan ne yönde ve ne kadar etkilenir? Buna yönelik ayrıntılı bir açıklama olmalıdır.
- ***Tahmin etmek:*** İyi bir teori, siber gücün toplumu ve teknoloji üzerinde yaratacağı muhtemel etkileri tanımlamalıdır. Ancak burada beklenti ve tahminin aynı olmadığı

unutulmamakla beraber siber gücün gelecekte ölçülebilir olan daha büyük etkilerini belirlemek mümkündür.

Güç Kullanma Kapasitesi

Dünya, devletlerin siber saldırı, sömürü ve casusluk yeteneklerini arttırmaya çalıştıkları bir siber "silahlanma yarışının" yanı sıra, aynı işlemlere karşı savunma için siber güvenlik önlemlerini arttırmaya çalıştığına da tanıklık etmektedir. Siber uzay kavramı NATO tarafından da kara, deniz, hava ve uzay'dan sonra muharebenin beşinci boyutu olarak kabul edildi (Yüksel, 2017). Enformasyon devrimi ve yukarıda aktarılan pek çok noktada literatürün çoğunun ortak bir özelliği, "bilgi çağında" bilginin iktidarın ana kaynağı haline geldiğine olan inançtır. Örneğin, 'yumuşak güç' kavramı, 'gücün sermaye zenginden bilgi zenginine geçtiği' tartışmalarına dayanır. Sonuç olarak bu, enformasyon devrimine en iyi şekilde liderlik edebilecek bir ülkenin, diğerlerinden daha güçlü olacağı anlamına gelir. Ancak, bu durum birçok ülke için asimetrik bir etki yaratabilir. Çünkü altyapılarını siber teknolojiye bağımlı hale getiren ülkeler, siber saldırılara karşı daha açık bir konuma gelmiştir. Bu durum devletlerin gücü edinme ve kullanma kapasitelerini kısıtlayan bir durum olsa da devletler güçten ve güçlü olmaktan vazgeçmemektedir.

İçinde bulunduğumuz dönem itibariyle en ileri siber savaş kapasitesine sahip olduğu düşünülen ülkeler ABD, Rusya, Çin, İngiltere ve İsrail olarak görülmektedir. Devletler siber savaş kapasitelerini arttırabilmek için siber savunmaya belli bir bütçe ayırmaktadırlar. Bugün siber alanda savunma harcamaları için ABD 19 Milyar Dolar, Rusya 11 Milyar Dolar, İsrail 6 Milyar Dolar ve İngiltere 860 Milyon Pound ayırmaktadır (Yüksel, 2017). NATO, Mükemmeliyet Merkezi (Cooperative Cyber Defence Center of Excellence) adlı siber savunma sistemini kurarak siber kapasitesini arttırmaya yönelik önemli bir adım atmıştır. NATO'nun yanı sıra Avrupa Birliği de siber alana yönelik önemli girişimlerde bulunmuştur. Bilhassa 2010'da Avrupa Konseyi (Council of Europe) bünyesinde imzalanan Siber Suçlar Sözleşmesi, uluslararası işbirliği yolunda önemli girişimler arasında yer almaktadır (Yüksel, 2017).

ABD ise bu alanda maliyet önlemi yoluyla saldırganları caydırmaya çalışmaktadır. Bu önlemler, ABD aleyhinde siber saldırı veya diğer kötü niyetli siber faaliyetlerde bulunmayı seçen düşmanlara karşı cezalandırma ve maliyeti arttırma amacıyla eylemler gerçekleştirmek üzere tasarlanmıştır. Bu önlemler, ABD Hükümetinin geçerli uluslararası yasalara uygun ve

uyumlu olan tüm gerekli vasıtalarla siber saldırılara cevap verme kabiliyetini ve istekliliğini kullanmaktadır. Bu tür tedbirler, kanun uygulama önlemlerini almak, kötü niyetli siber aktörleri cezalandırmak, saldırgan ve savunma amaçlı siber operasyonlar yürütmek, hava, kara, deniz ve uzay yoluyla güç sunmak ve mevcut tüm seçeneklerin tükenmesinden sonra askeri güç kullanmak gibi görevleri içermektedir (Federal News, 2015). "Caydırıcılık" terimi, ABD politika belgelerinde de merkezi ve belirleyici bir rol oynamaktadır. Örneğin, Birleşik Devletler Doğu Batı Enstitüsü ve Rusya Bilişim Güvenliği Enstitüsü 2011 yılında siber ve bilgi güvenliği için kritik şartları tanımlayan ortak bir Rus-Amerikan raporu yayınladı. Bu rapor belirli şartlar için kabul edilmiş tanımları içermektedir. Rapor, Rusya ve ABD tarafından hükümet düzeyinde siber meselelerde olası işbirliğine iyi bir örnektir. Raporun bir diğer amacı, her iki tarafın siber alanla ilgili belirli terimlere ilişkin anlayışını açıklamasıdır (Lin, 2017).

Bradley Manning ve Edward Snowden ABD'nin siber gücü ile ilgili bazı açıklamalarda bulunmuşlar ve ABD'nin siber yeteneklerini şöyle özetlemişlerdir: "ABD dünyada başkalarının yapabileceği her şeyi yapabilir ancak yapabileceği her şeye karşı bir savunma sistemi geliştiremez."(Carafano, 2013). Çünkü siber yeteneklerini ve gücünü arttırmaya çalıştıkça saldırıya maruz kalma riskini de doğru orantılı olarak arttırmaktadır. ABD bu yüzden siber alanda davranışlarını kısıtlamak zorunda olan bir ülke haline gelmiştir. ABD'nin teknolojik altyapısı ne kadar güçlüyse, siber saldırılara karşı da o denli savunmasızdır. Çünkü Rusya ve Çin gibi ciddi rakiplerine oranla sivil ve askeri altyapısını büyük oranda siber alana angaje etmiştir. Dolayısıyla ABD, siber alanda hem savunmacı hem de saldırgan pozisyonu itibariyle en üst düzeyde olan devlet konumunda görünmektedir (Marmon, 2011). 2016 ABD seçimlerine Rusya tarafından bir müdahale gerçekleştiği yönünde iddialar bulunmaktadır. Obama yönetimi, seçimlere müdahale etmesi nedeniyle Rusya'ya yönelik bir dizi yaptırım uygulayacağını açıklamıştır. Bu yaptırım ve tehditlerin ileride olabilecek herhangi bir Rus saldırısına karşı caydırıcılık unsurunu devreye sokacağı düşüncesi söz konusudur (Rojansky, 2016).

Ulusal Güvenlik Ajansı (NSA) gözetim merkezleri ise, siber alana yönelik politikalarının gerekçesi olarak; "birisinin bunu yapması gerektiği" ve "bunu başka herhangi birinden daha iyi yapabileceğimiz" fikrini öne sürmüşlerdir (The Guardian, 2014). Eski NSA Çalışanı Edward Snowden, ABD'nin "İstihbaratın Beş Gözü" adı verilen bir yapı kurduğunu açıkladı. Devletlerarasında siber istihbarat ve veri paylaşımında bulunan bu yapıya üye olan ülkeler; ABD, İngiltere, Kanada, Yeni Zelanda ve Avusturya'dır. Bu devletler dünyanın çeşitli yerlerinden edindikleri bilgileri ekonomik, askeri ve istihbari stratejilere dönüştüreceklerdir.

Ayrıca bu devletler rakiplerinin güvenlik açıklıklarını tespit etme veya onları dinleme gibi faaliyetleri de yerel taşeron örgütlere yaptırmaktadırlar (Yüksel, 2016).

Siber tehdit ciddi bir ulusal güvenlik meselesidir, çünkü orada saldırmayı bekleyen online düşmanlar mevcuttur. Ancak Choney'e göre burada da düşmanlar eşit olarak yaratılmamıştır. Özellikle Amerikan bir bakış açısıyla yaklaşan Choney, ABD'nin karşısındaki en büyük rakipler olarak Çin ve Rusya'yı görmektedir. Ancak bu durum, diğer devletlerin bir tehlike oluşturmadığı anlamına gelmemektedir. Zira K.Kore, Suriye ve İran gibi ülkeleri de azımsamamak gerekir. Örneğin ABD eski başkanı Obama Suriye'ye yönelik yaptırım kararı aldığında, Suriye Siber Ordusu'nun New York Times, Twitter ve ABD Deniz Piyadeleri web sitelerine başarıyla saldırdığını gösteren medya raporları ortaya çıkmıştır (Choney, 2013).

Suriye gibi siber yetenekleri sınırlı olan bir ülkenin bile siber silahlanma yarışında yer alması, bütün devletlerin gelecekte bu yarışa katılacağı yönündeki beklentileri arttırmaktadır (Grohe, 2015:15). Sosyal medyadaki haber kuruluşları ve videoların yanı sıra, siber bölgedeki iç savaşı etkileyen en önemli aktör Suriye Siber Ordusu Syrian Electronic Army (SEA) olarak adlandırılan bir gruptur.

SEA, halka açık alanlardan yıkıcı siber saldırı ve sömürüye kadar uzanan ve siber casusluğa işaret eden bazı kanıtlarla faaliyet gösteren bir rejim yanlısı hack grubudur. Mayıs 2011'in başından itibaren SEA, Suriye Bilgisayar Topluluğuna ait çeşitli kurucu üyelerle birlikte Beşar Esad'a yakın bir ilişki içinde ve bilgi teknolojisi alanını Suriye toplumuna dâhil etmekle yükümlüdür (Perlroth, 2013). Suriye kadar siber altyapısı zayıf olan bir ülke bile, sosyal medya ve haber kuruluşlarının raporlarını genişletebilir, arttırabilir veya aşabilir. Haber kuruluşları bir olayı işleme ve sunma kapasitesini kaybettiğinde, sosyal medya bu boşluğu doldurabilir. Suriye'deki çatışmanın tarafları, olaylara ilişkin görüşlerini yaymak için sosyal medyanın gücünden faydalandılar. SEA'nın Beşar Esad rejimiyle dolaylı ilişkilerine rağmen, grubun rejim adına siber operasyonlar gerçekleştiren fiili bir ulusal siber güç olduğu açıkça görülmektedir (Grohe, 2015:9).

Estonya da küçük ülkeler arasında yer almasına rağmen siber alanda ilerleme kaydeden ülkeler arasında yer almaktadır. Estonya'nın post-Sovyetler Birliği'nden hızlı bir şekilde kopması dünyanın önde gelen bilgi devletlerinden biri haline gelmesini ve güvenliğe de daha hızlı ulaşmasını sağlamıştır. Estonya, dijital kimlik kartları ve veri tabanları oluşturmada oldukça

başarılı bir ülke olarak görülmektedir. Estonya ayrıca, yurtdışındaki büyükelçilik konutlarının yanı sıra, ulusal verilerini yedekledikleri güvenli bölgelerde "veri elçilikleri" de kurarak bölgede sanal bir ülke olarak yeniden yapılandırmasını sağlamaktadır (Khanna, 2015).

Estonya şimdi NATO'nun Siber Savunma Birimine ev sahipliği yapmaktadır. 2015 yılının başında da Microsoft Windows gibi işletim sistemleri aracılığıyla saldırılara karşı koruma amaçlı bir "eğitim kilidi" olan "Locked Shield" operasyonu için bir düzine NATO müttefikleriyle toplanmıştır. (NATO Cooperative Cyber Defence Centre of Excellence, 2017). Temmuz 2015'te Estonya; içerisinde İngiltere, Güney Kore, İsrail ve Yeni Zelanda'nın bulunduğu dünyanın önde gelen resmi siber ittifakının kurucu üyesi olmuş ve bu ittifaka göre birbirinden farklı ancak gelişmiş ülkeler birbirlerinin sunucularını güvenli bir şekilde barındırmayı kabul etmiştir. "Digital Five" olarak adlandırılan bu ittifak bir yer veya coğrafya adını almaksızın siber bir ittifak olarak kurulmuştur (Ramishvili, 2016).

Siber uzayla ilgili bilinmesi gereken bir diğer mesele, tüm tehditlerin devlet destekli olmadığıdır. Bazı devlet-dışı aktörlerin gücü kullanma kapasitesi devletlerden daha etkili olabilmektedir. Bazı ülkeler, siber alanlarında kötü aktörlere karşı korkunç bir mücadele vermektedir. Örneğin Pakistan, bir siber suç merkezi haline geldi. Pak Cyber Pyrates (PCP), belki de en çok aktif olan Pakistan hacker topluluğudur ve yüzlerce Hindistan karşıtı saldırıda bulunmaktadır. PCP, 9 Ekim 2011 tarihli bir yazı ile Keşmir ve Filistin gibi devletler için yaptığı "Özgür Filistin, Özgür Keşmir" sloganında esas amacını bildirmiştir (Ahmad, 2012).

Görüldüğü üzere bütün bu stratejilere ve güç kullanımına rağmen özellikle büyük güçlerin siber alanda karşı karşıya kaldığı ciddi bir sorun var. O da şu ki; büyük ülkelerin altyapılarının siber alana aşırı derecede bağımlı hale gelmiş olması, bu ülkeler için dış veya iç güçler tarafından kolayca istismar edilebilir zayıflıklar yaratmaktadır. Bu da temel güvenlik açıklarının onlar için daha büyük bir sorun haline gelmesine sebep olmaktadır. Bunun yanında, siber alanda etki yaratmanın maliyeti oldukça düşük olduğundan küçük devletler siber alanda önemli bir etki yaratabilmekte ve bu durumda ABD, Rusya, Çin gibi büyük ve zaten güçlü olan devletlerin siber alanda istedikleri gibi hâkimiyetlerini sürdürmeleri pek de mümkün olmamaktadır (Nagy, 2012:15). Bunun sonucu olarak siber alanda güvenli bir ağ oluşturmak fazlasıyla zor olduğundan, iletişim daha az korumalı bir hal almaktadır. Dolayısıyla güvenlik açığından kaynaklı olabilecek herhangi bir saldırının niteliği çok daha kötü sonuçlar doğurabilecektir. Bu nedenle siber alanda ihtiyaç duyulan şey, düşmanın siber ayak izlerinin "görselleştirilmesini"

sağlayan bir yazılım, toplanan verilerin belirlenmesine yardımcı olan analitik araçlar ve bilgiyi yorumlama ve aktarmada yetenekli kişilerdir (Carafano, 2013).

Güç Kullanmanın Önünde Ortaya Çıkan Engeller

Siber alanda gücün sağlanabilmesi yalnızca devletlerin kapasitelerine ve becerilerine bağlı bir durum olarak algılanmamalıdır. Çünkü siber uzayda bir güç olarak sivrilebilme veya saldırıları caydırabilme noktasında bütün bu saydığımız nedenlerin dışında siber alanın doğası gereği de ortaya çıkan bazı engeller mevcuttur. Her şeyden önce siber uzayda düşmanı silahsızlandırmak ya da yok etmek ya da etkili bir şekilde karşı-kuvvet stratejileri kullanma yeteneği sınırlıdır. Dolayısıyla siber alanda caydırıcılık mümkündür ancak bir saldırı kaynağının atfedilmesi sorunları nedeniyle zorluklar meydana getirir. Bir devletin siber alanda gücünü arttırması veya saldırıları caydırabilmesinin önünde engel olarak beliren üç faktör vardır. Bunlar; asimetri, gizlilik ve süper güçlendirme unsurlarıdır. Ortaya çıkan bu engel ve zorlukları bir siber güç gösterisi örneği olan 2007'de Rusya'nın Estonya'ya saldırısı üzerinden değerlendirmek daha açıklayıcı ve anlaşılır olacaktır (Guzman, 2017).

- ***Anonimlik (Atıf Sorunu):*** Anonimlik, savunmacı için oldukça büyük bir engel olarak karşımıza çıkmaktadır. Patrick Morgan'ın altını çizdiği kimlik ve motivasyon unsurlarının bilinmezliği, verilecek mesajın doğruluğu konusunda da engel teşkil etmektedir. Yani siber uzayda saldırıyı kimin gerçekleştirdiğini öğrenmek için birine atıf yapmak veya saldırganın niyetini tespit etmek oldukça zordur (Graham, 2010:104). Ancak saldırının niteliği ve buna verilecek tepki önemli bir aşama olduğu için istihbarat kapasitesi ve kaynakları olan ulus devletler bile kendilerine yönelik bir saldırıya doğrudan atıfta bulunmak için doğrudan doğruya yetki sahibi olamazlar (Schmitt, 2011:570). Estonya örneğine baktığımızda saldırının hala Rusya tarafından yapılıp yapılmadığı şaibeli bir durumdur. Bu yüzden anonimlik faktörü burada önemli rol oynamıştır (Nye, 2010:10).
- ***Asimetri:*** Zayıf tarafın daha güçlü tarafa karşı onun zayıf taraflarından da istifade ederek farklı taktik veya rastgele yöntemlerle yürüttüğü mücadele olarak adlandırılabilir. Örneğimiz bağlamında baktığımız zaman; uzmanlara göre Rusya Estonya'ya karşı siber bir saldırı gerçekleştirmiş olsa bile bu alanda Estonya için meydan okuyabileceği bir alan bırakmayabilir. Bu durumda Estonya, Rusya'ya herhangi bir saldırı gerçekleştirmek istese bile Rusya Estonya için bu saldırıyı gerçekleştirebileceği ortamı ortadan kaldırmış olabilir. Bu da siber alanın asimetrisini ortaya çıkarır (Betz, 2012:695).

- ***Süper Güçlendirme:*** Estonya saldırıları, internet üzerinde var olan süper yetkili aktörlerin nasıl oluştuğunu göstermektedir. Her ne kadar Estonya, bu saldırının Rusya tarafından gerçekleştiğinden emin olsa da bu konuda yalnızca Rus kökenli bir Estonyalı hüküm giymiştir. Bu da, yalnızca bir kişinin (bireyin) devlet kapasitesinde bir saldırı gerçekleştirerek siber alanda nasıl güç sahibi olabileceğini göstermiştir. Bu durum, hem devletin gücünün sarsılması konusunda hem de rakiplerin caydırılması konusunda büyük sorunlar yaratmaktadır (Reinbold, 2010). Zira bir devleti caydırmak veya bir devletle rekabet etmek bu denli zor iken, "bireylerle" baş etmek imkânsız görünmektedir (Goodman, 2010:113).

Estonya'nın arkasında ABD ve Avrupa ülkeleri olduğundan, Rusya'nın saldırısından en az zararla çıkabilmeyi başardı. Ancak siber saldırılar yalnızca Estonya gibi sınırlı alanlara yayılabilen küçük ülkelerle sınırlı kalmamakta ya da bu şekilde geçici zararlar vermemektedir. Aksine büyük güçler siber saldırılara karşı daha savunmasız durumdadırlar. Dolayısıyla büyük güçlerin uğradığı saldırıların neticesi çok daha büyük hasarlarla sonuçlanabilir. Asya ve Avrupa gibi bölgeler bilgi ağlarına güvenirken, ağlarında oluşabilecek hasarlara karşı oldukça savunmasız görünmektedirler. Dolayısıyla siber saldırı için kullanılan araçların artması siber uzayda kötü niyetli aktörlerin de teknik kapasitesini arttırmakta ve bu durum siber alanda savunmasızlıkların yükselmesine neden olmaktadır.

Devlet – Devlet-dışı Aktör Arasında Güç Dağılımı Tartışması

Uluslararası ilişkilerde realist paradigma devletler arasında itici bir güç olarak gücün dağılımına odaklanır. Realistler, dünya siyasetini anarşi koşulları altında devletlerarasındaki mücadeleler olarak nitelendirerek devletlerin güvenliklerini en üst düzeye çıkararak hayatta kalmayı garanti altına aldıklarını savunmaktadırlar. Devletler kendilerini korumak için daha yüksek bir otoriteye güvenemediğinden, nihai olarak diğer devletlerin saldırılarından kendilerini korumak için *self-help* denen kendi çabalarıyla hayatta kalma stratejisine bağlıdırlar. Realizm, uluslararası davranışları belirlemekte devlet dışı aktörlerin rolünü kabul ederken, bu aktörlerin devletlerin ve devlet çıkarlarının uluslararası siyasette önceliğine halel getirmediğini vurgulamaktadır (Walt, 1997:931).

Bir devletin egemenliğini askeri güç kullanarak kontrol etme yetkisi, konvansiyonel (askeri) araçları inşa etme ve onları kullanabilme yetkisine sahip olmak demektir. Bu yetenek genellikle

devletlere aittir ve bireyler bu tür özel araç ve ekipmanları tasarlayıp üretme konusunda bilgi ve kapasiteye sahip değildir. Fakat söz konusu siber alan olduğunda bir birey siber altyapıyı oluşturan bazı sistem ağlarını kullanarak bir bölgeyi kontrol etme konusunda bilgi ve yeteneğe sahip olabilir. Dolayısıyla bu durum doğrudan bireyleri, dolaylı olarak da devlet dışı aktörleri güçlendirir. Ancak bunlar yalnızca devlet-dışı aktörleri değil, bizatihi devletin kendisini de güçlendirebilir. Bunun kanıtı olarak devletlerin bugüne kadar hiçbir izole siber saldırıya atfedilmemiş olması gösterilebilir. Böyle bir durumda uluslararası hukuk, bir devletin durdurulması veya caydırılması için yararlı olmayacaktır (Schmidt, 2016:36). Bu durumda herhangi bir siber saldırı eyleminde bulunmayı planlayan devletler kimliğin ortaya çıkarılması sorunundan yararlanacaklardır. Ancak bu devlet güçlenmesinin arka planında da bir çelişki söz konusu olabilmektedir. Çünkü saldırıda gizlilikten, bilinmezlikten yararlanan devlet, bir operasyonu gizli bir şekilde yürütmek istediğinde operasyonun gerçekleşmesi safhasında bir devlet dışı aktörle işbirliği yapabilir veya direkt olarak saldırıyı ona yüleyebilir. Bu da devletin devlet dışı aktörleri kendi eliyle güçlendirmesi anlamına gelecektir.

Siber alan konusunda temel argümanlardan biri, teknolojik gelişmenin, devletten daha etkili olabilecek aktörlerin çeşitlendirilmesine ve bununla bağlantılı olarak güç yapılarında bir değişime yol açtığıdır. Bu iki merkezi ve birbirine bağlı gelişme, siber uzayla beraber uluslararası sistemde var olan güç ve gücün yeniden dağılımındaki değişimin doğasını ortaya koymaktadır. Niteliğin değişen doğası, bilgi teknolojilerinin giderek artan öneminin bir sonucu olarak görülmektedir. Eğer bir devlet siber bilgiye sahipse, onu yürütmek için geliştirmek, icat etmek veya ortaya çıkarmak zorunda değildir. Çünkü siber gücü kullanma maliyeti sıfıra yakındır. Bu durumda siber gücü edinmek veya geliştirmek, geleneksel bir askeri gücü geliştirmekten ve üretmekten daha ucuza mal olacaktır. Fakat burada devletler açısından bazı problemler ortaya çıkacaktır. Bu problemlerden en önemlisi, bu siber gücün devlet dışı aktörlerin de elinde olabileceği gerçeğidir. Bu nedenle, geleneksel olmayan şiddet yöntemleriyle daha az masraflı saldırıların devlet-dışı aktörler tarafından gerçekleştirilmesi kaçınılmaz bir hal almaktadır. Üstelik siber alanın saldırı kaynağında yarattığı atıf istismarı göz önüne alındığında bu ihtimalin tırmanması daha kolay hale gelmektedir (Choucri, 2012:4). Bunun dışında siber alanda uzaklığın olmaması, kapsadığı alan bakımından bir sınırlama olmaması, hedeflerin fiziksel alana ihtiyaç duyulmadan gerçekleştirilebilmesi ve geleneksel zaman kavramının yerini anlık zamanlara bırakması sebebiyle aktörlere daha rahat olabilecekleri bir ortam sağlar (Libicki, 2007:276).

Schmidt ve Cohen gibi yazarlar siber uzayı, devlet dışı grupları devlete karşı güçlendiren bir araç olarak tanımlamaktadır. Schmidt ve Cohen siber alanda, potansiyel kazananlar ve kaybedenler arasında yapılan bir yarışmanın varlığından söz etmektedirler. Bu durumda, küçük ve otokratik rejimler, rejim istikrarı için uğramış oldukları tehdidi azaltmaya çalışmaktadır. Fakat öte yandan, siber teknolojinin mevcut yapılandırmasında en çok fayda sağlayacak olan tarafın, Batı'nın büyük ve demokratik devletleri olduğunu savunmaktadırlar (Schmidt ve Cohen, 2010:75-86). Murphy ise, "erdemsiz" kimlik tabanlı ulus-ötesi grupların kamusal alanda olabilecek etkisini şöyle değerlendirmektedir: Daha "erdemli" sivil toplum grupları gibi, erdemsiz gruplar da siber teknoloji tarafından güçlendirilmektedir."(Murphy, 2009:138-139). Drezner ise birçok yazarın aksine devlet otoritesinin azalmadığını ve uluslararası siber yönetişimdeki sonuçların sistemdeki en güçlü ülkelerin çıkarları tarafından belirlendiğini savunmaktadır (Drenzner, 2004:480).

Bu konudaki en uç bakış açısı, "küresel köyler"in ve devlet-dışı aktörlerin ulus devleti tamamen ortadan kaldıracağı fikridir. John Perry Barlow'un 1996'da yayınladığı bağımsız bir siber uzayın manifestosu, yeni bilgi ve iletişim teknolojilerinin (BİT) özgür pazarının hükümet müdahalesi olmadan gelişmesine izin verdiği ve hükümetlerin halk üzerinde herhangi bir güce sahip olmadığı ütopik bir dünyayı imgeleştirmektedir (Barlow, 1996). Ayrıca burada coğrafi konum yerine ortak inanç ve değerler önem taşımaktadır. Burada seçilmiş bir hükümetten, otoriteden ve yaptırımdan bağımsız bir alanda konuşlanmış olan bir topluluktan söz edilmektedir (Kreiss, 2010). Barlow gibi düşünürler bilgi devrimini, kaçınılmaz ve geri döndürülemez biçimde yaşamın her alanını dönüştüren teknolojik bir sıçrama olarak görmektedir (Toffler, 1993). Bazı tahminlere göre gelecekte artan ölçüde, devlet dışı aktörlerin kendilerini devlet kontrolünden kurtarmaları ve bağımsız bir rol oynamaları beklenmektedir. Aynı zamanda bağımsız bir rol oynamakla kalmayıp daha fazla güç kullanma kapasitesine sahip olabileceklerdir. Örneğin; kendi yasalarını yapacak, kendi adalet sistemlerini geliştirecek, kendi vergilerini alacak ve hatta kendi paralarını basmaya başlayacaklardır (Joey, 2014).

Bu tür radikal fikirler kısa vadede uygulanabilir olmasa da, devletin uluslararası meselelerde merkezi aktör olarak öncelikli konumuna rakip olarak çıkabilmektedir. Siber, devletin ana görevlerinden ikisi olan güvenliği ve ekonomik refahı sağlama rolünü tehlikeye atarak devleti bu rollerinden vazgeçmeye zorlamaktadır. Örneğin devletler, siber savaş ve siber terörizm tehditlerine karşı güvenliği sağlamakta zorluk çektiğinden ve ekonomik faaliyetler giderek devletlerin sınırlarını aşmaya başladığından, devletlerin onları güvence altına alıp kontrol etme

yetenekleri de azalmaya başlamıştır. Siber nedeniyle, çok uluslu şirketler (ÇUŞ) ve bazı sivil toplum örgütleri (STK) gibi bir coğrafya tarafından sınırlandırılmayan uluslararası aktörler, devletlerin taleplerini dikkate almaksızın uluslararası alanda istedikleri gibi hareket edebilmektedirler.

Bu gibi radikal görüşlerin yanı sıra daha şüpheci gözlemciler, bilgi teknolojilerinin sınırlı ekonomik ve sosyal etkisine işaret etmekte ve değişim sürecinin evrimsel niteliğini vurgulamaktadırlar. Bu gözlemciler ayrıca toplumun ve siyasetin değişen doğasına teknolojik olarak deterministik bir yaklaşım getirmektedirler (Kitchin, 1998; Keohane, 1998). Örneğin Dunn'a göre siber alan BİT'i devlet dışı aktörlerin eline geçirse de, çoğunlukla bilgi avantajına sahip olan devlettir. Çünkü stratejik bilgi yaygın değildir ve devlet-dışı aktörler çoğunlukla bilgileri toplamak ve düzenlemek için gerekli olan yetenekler ve kaynaklardan yoksundurlar (Dunn, 2012:59).

Devlet ve siber uzaydaki kötü aktörlerin ilişkisine baktığımız zaman ise, Paul Rosenzweig, devletin kötü aktörlerle olan siber işbirliğinin her zaman kötü bir fikir olduğunu belirtmektedir. Ancak Rosenzweig'in aksine bu konuda Lin şöyle diyor: "Kötü aktörlerle işbirliği yapmak hep kötü bir fikir olsaydı, düşmanlarla asla anlaşma yapmazdık." Lin bu sözünü ise düşmanlarla yapılan anlaşmalarla örnekleyerek desteklemiştir. Lin'e göre böyle bir durumda silahlı çatışma yasalarında herhangi bir anlaşma, silah kontrol anlaşmaları veya deniz kanunları olmayacaktı (Lin, 2017).

Görüldüğü üzere siber alana ilişkin üç ana tema üzerinde durulmaktadır. Bunlar; atıf-kaynak ya da saldırıyı yapanı belirleme sorunu, devlet-iktidar siyasetinin rolü ve hem hükümet hem de özel sektörün sorumluluklarındaki değişimdir (Kostadinov, 2013). İki temel çatışma, gücün yeniden dağılımı üzerinde tartışmalara yol açmaktadır. Birincisi, bilgi devriminin, STK'lar ve aktivistler gibi uluslararası aktörlerin yeni biçimlerini güçlendirdiği ve dolayısıyla devletin uluslararası sistemdeki en büyük aktör olması fikridir. İkincisi ise, küresel bir elektronik pazarın ortaya çıkmasının kaçınılmaz olarak, şirketlerin ekonomik sınırlarını yok ettiğini ve bununla birlikte devletin ekonomi direğinin çöküşünün gerçekleşmiş olduğu iddiasıdır (Rothkopf, 1998:211). Geleneksel olarak, özel sektör ulusal güvenlik araçlarını geliştirir ve hükümet bu araçları kullanarak çalışır. Fakat şu anda özel şirketler, ülkeleri bir başka ulus devletin eylemlerine maruz kaldıklarında ulusal güvenlik giderleri konusunda sorumluluk sahibi olmaya başlamıştır. Bu zaten olması gereken bir durumdur çünkü siber alanda ayakta kalabilmek için

kamu-özel arasında istihbarat ve bilgi alışverişi olmalıdır. Çünkü bu durum, hükümetin daha gizli bir bağlamda çalışmasını ve şirketlerin daha fazla paylaşımda bulunmasını gerektirir. Bugün az sayıda şirket, Devlet Güvenliği Departmanı ile veri paylaştığından dolayı bazı uzmanlara göre bu durum ele alınması gereken ciddi bir konu olarak görülmektedir (The Cipher Brief, 2017).

Sonuç

Bilgi devrimi, mevcut geleneksel askeri yeteneklerin yanı sıra stratejik dünyadaki bilgilerin önemini önemli ölçüde artırdı ve bilgi, savaşta kilit unsur olmaya başladı. Edward Snowden, siber-politiğin uluslararası ilişkilerin incelenmesinde "yüksek politika" konusu haline geldiği hususunda bir fikir birliğinin bulunduğunu iddia etmektedir (Ralston, 2014:2). Nazli Choucri ise siberi 'düşük politika' ile 'yüksek politika' arasındaki ilişkinin bir meselesi olarak görmektedir. Yani Choucri siberi; siber- politik ve siber güvenlik ile uluslararası politika ve ulusal güvenlik arasındaki kritik bir nokta olarak görmektedir (Choucri, 2012:3). Gerçekten de internet, fiziksel bir çerçevede mantıksal yapı taşları ve etkileşim aracılığıyla “katmanların" her biri için gerçek siyasi sonuçlar doğurmaktadır.

Bu doğrultuda siberin yeni çatışma biçimlerine yol açtığı görülmektedir. Siber alanda savaş kayıplarına maruz kalma olasılığının düşük olması, çatışmaya girme maliyetinin düşük olması ve fiili savaşçıların kimliklerini gizleyebilme becerisi nedeniyle savaş açmak ya da saldırıda bulunmak çok daha kolay hale geldi. Savaş alanının insan algısını ve sanal alanı kapsayacak şekilde genişlemesi, çatışmalarda devlet-dışı aktörlerin daha fazla yer almasına sebep oldu. Dolayısıyla devletler yumuşak gücün eşit olmayan dağılımının bir sonucu olarak ortaya çıkacak olası güvenlik tehditlerine işaret etmek zorunda kalacaklardır.

Hâlihazırda ekonomik sıkıntı çeken ve siyasi ve kültürel yabancılaşmaya maruz kalan ülkeler, bölgeler ve çeşitli grupların, siber alanın faydalarını kolayca hissetmeleri pek muhtemel değildir. Fakat gelişmiş ülkeler, bilgi teknolojisi tarafından kendilerine tanınan fırsatlardan istifade ederken; altyapılarını bu teknolojiye angaje ettikleri durumda rakiplerinin saldırı ve tehditlerine daha açık bir konuma geldiklerini de göz önünde bulundurmak zorundadırlar. Zira bilgi teknolojisine en fazla sahip olan devletler, saldırıya en açık olan devletlerdir. Bu nedenle özellikle bu alanda daha güçlü olan devletlerin güvenlik risklerini minimize etmek için çabalaması gerekmektedir. Ancak güvenlik risklerinin azaltılması, yalnızca çok taraflı

işbirliğinin artırılmasını değil, aynı zamanda bilgi sistemine sahip olan devlet dışı aktörlerle, özel sektördeki kişilerle, marjinal gruplarla, devletlerle ve bölgelerle olan ilişkinin arttırılmasını gerektirmektedir (Dunn, Hensel ve Mauer, 2007:12).

Esas olarak siber, ülkeleri birbirine yakınlaştırmıştır. Çünkü askeri güce dayalı geleneksel fetih anlayışı, çevre, ordu, sermaye gibi faktörler sanal devlet için değersizdir. Bu fikrin en dikkat çekici yönü, nihai olarak bu devletlerin bilgi kaynakları için rekabet edeceği fikridir. Bugünün gelişmiş devletlerinin artık siyasal hâkimiyet için mücadele etmek yerine, küresel bilgiye ulaşmak için mücadele edeceği gibi görüşler de mevcuttur. Bu görüşe göre siber alan özellikle toprak faktörünü ortadan kaldırdığı için devletler ek topraklara ihtiyaç duymamakta ya da bunu arzulamamaktadır.

KAYNAKÇA

Ackerman, S. and S. Thielman. (2016). US Officially Accuses Russia of Hacking DNC and Interfering with Election. https://www.theguardian.com/technology/2016/oct/07/us-russia-dnc-hack-interfering-presidential-election (Erişim Tarihi: 21.08.2017).

Ahmad T. (2012). Pakistani Cyber Armies Hacking Indian Websites, Using Twitter, Facebook and YouTube to Cause Ethnic Conflicts in India. http://cjlab.memri.org/uncategorized/pakistani-cyber-armies-hacking-indian-websites-using-twitter-facebook-and-youtube-to-cause-ethnic-conflicts-in-india/ (Erişim Tarihi: 18.08.2017).

Aydın, M. (2004). Uluslararası İlişkilerin 'Gerçekçi' Teorisi: Kökeni, Kapsamı, Kritiği. *Uluslararası İlişkiler Dergisi*. Cilt 1. Sayı 1.

Bendiek, A. (2016). Making States Responsible for Their Activities in Cyberspace: The Role of the European Union. https://www.cfr.org/blog/making-states-responsible-their-activities-cyberspace-role-european-union (Erişim Tarihi: 30.08.2017).

Betz, D. (2012). Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed. *The Journal of Strategic Studies*. Vol 35, No 5.

Boeke, S. (2016). Who Determines the Cyber Security Agenda?. *Journal of Security and Global Affairs*. No 1.

Buchan, R. (2016). Special Issue: Non-State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence. *Journal of Conflict and Security Law*. Vol 21, No 3.

Carafano, J. J. (2013). Fighting on the Cyber Battlefield: Weak States and Nonstate Actors pose Threats. http://www.heritage.org/defense/commentary/fighting-the-cyber-battlefield-weak-states-and-nonstate-actors-pose-threats (Erişim Tarihi: 18.09.2017).

Carr, E. H. (1946). The Twenty Years' Crisis, 1919–1939: An Introduction to the Study of International Relations. Oxford University Press.

Castells. M. (1996). *The Rise of the Network Society*. Oxford: Blackwell Publishers. ,

Choney, S. (2013). New York Times Hacked, Syrian Electronic Army Suspected. https://www.nbcnews.com/technology/new-york-times-hacked-syrian-electronic-army-suspected-8c11016739 (Erişim Tarihi: 04.10.2017).

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

Craig, A. and B. Valeriano. (2016). Conceptualising Cyber Arms Races. *8th International Conference on Cyber Conflict: Cyber Power*.

Çelik, M. (2015). Siber Ordu Kurmak İçin Devletler Özel Sektör ile Çalışıyor. *TMMOB Bilgisayar Mühendisleri Odası Dergisi*. Sayı 5.

Drezner, D. W. (2004). The Global Governance of the Internet: Bringing the State Back In. *Political Science Quarterly*. Vol 199, No 3.

Dunn, M. (2012). *Information Age Conflicts Myriam Dunn A Study of the Information Revolution and a Changing Operating Environment*, Zurich: Zürcher Beiträge. http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/ZB_64.pdf (Erişim Tarihi: 21.08.2017).

Dunn, M., S. F. Krishna-Hensel and V. Mauer. (2007). *Power And Securıty In The Informatıon Age: Investigating the Role of the State in Cyberspace.* Ashgate Publishing.

Gady, F. (2011). From the Middle Ages to the Cyber Age: Non-State Actors. http://www.huffingtonpost.com/franzstefan-gady/from-the-middle-ages-to-t_b_818650.html (Erişim Tarihi: 28.08.2017).

Gibson, W. (1984). *Neuromancer*. Ace Books.

Gomez, M. A. (2010). Identifying Cyber Strategies vis-a-vis Cyber Power. http://cybersummit.info/sites/cybersummit.info/files/Identifying%20Cyber%20Strategies%20vis-a-vis%20Cyber%20Power.pdf_Miguel%20Gomez.pdf (Erişim Tarihi: 07.09.2017).

Graham, D. E. (2010). Cyber Threats and the Law of War. *Journal of National Security Law and Policy*. Vol 87. No 4.

Grohe, E. (2015). The Cyber Dımensıons of the Syrıan Cıvıl War: Implications for Future Conflict. *The Johns Hopkıns Unıversıty Applıed Physıcs Laboratory.* Vol 14. No 7.

Guzman, G. (2017). Cyberpower – the Great Equalizer: Estonian Cyberpower Development. https://www.iapss.org/shop/budapest/uploads/2512_guzman_g_cyberpower_the_great_equalizer_03_2017_politikon_ela.pdf (Erişim Tarihi: 15.10.2017).

Guzzini, S. (2001). The Enduring Dilemmas of Realism in International Relations. *Copenhagen Peace Research İnstitute*.

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: 19.08.2017).

Haley, C. (2016). A Theory of Cyber Deterrence. http://journal.georgetown.edu/a-theory-of-cyber-deterrence-christopher-haley/ (Erişim Tarihi: 01.09.2017).

Hart, J. (1976). Three Approaches to the Measurement of Power in International Relations. *International Organization*. Vol 30. No 2.

Hensel, S. F. Krishna. (2007). Cybersecurity: Perspectives on the Challenges of the Information Revolution. Myriam Dunn Cavelty, Victor Mauer, *Power and Security in the Information Age Investigating the Role of the State in Cyberspace.* Ashgate Publishing.

Jensen, E. T. (2012). Cyber Deterrence. *Emory International Law Review*. No 26.

Joey, S. (2016). The Role of Non-state Actors in International Relations. http://www.academia.edu/5124220/The_Role_of_Non-state_Actors_in_International_Relations (Erişim Tarihi: 05.09.2017).

Kennan, G. F. (1966). *Realities of American Foreign Policy*. New York: The Norton Library.

Keohane, R. O. and J. S. Nye. (1998). Power and Interdependence in the Information Age. *Foreign Affairs*. Vol 77. No 5.

Kitchin, R. (1998). Cyberspace: *The World in the Wires.* Chichester: Wiley-Blackwell.

Kostadinov, D. (2013). The Attribution Problem in Cyber Attacks. http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/#gref (Erişim Tarihi: 11.08.2017).

Kreiss, D. (2010). A Vision of and for the Networked World: John Perry Barlow's A Declaration of the Independence of Cyberspace at Twenty. https://danielkreiss.files.wordpress.com/2010/05/kreiss_barlow202.pdf (Erişim Tarihi: 18.10.2017).

Libicki, M. (2007). *Conquest in Cyberspace National Security and Information Warfare*. Cambridge.

Lin, H. (2017). On Cooperating with Bad Actors in Cyberspace. https://www.lawfareblog.com/cooperating-bad-actors-cyberspace (Erişim Tarihi: 17.09.2017).

Loader, B. D. (1997). The Governance of Cyberspace: Politics, Technology, and Global Restructuring. B. D. Loader (eds). *The Governance of Cyberspace.* New York: Routledge.

Marmon, W. (2011). Main Cyber Threats Now Coming From Governments As "State Actors". https://www.europeaninstitute.org/index.php/136-european-affairs/ea-november-2011/1464-main-cyber-threats-now-coming-from-governments-as-state-actors (Erişim Tarihi: 03.10.2017).

Moravcsik, A. (1997). Taking Preferences Seriously: A Liberal Theory of International Politics. *International Organization.* Vol 51. No 4.

Morgenthau, H. J (1948). *Politics Among Nations: The Struggle for Power and Peace*. New York: Mc Graw Hill.

Murphy, E. C. (2009). Theorizing ICTs in the Arab World: Informational Capitalism and the Public Sphere. *International Studies Quarterly*. Vol 53. No 4.

Nagorski, A. (2010). Global Cyber Deterrence: Views From China, The U.S., Russia, India, and Norway. *East- West Institute*.

Nagy, V. (2012). The Geostrategic Struggle in Cyberspace between the United States, China, and Russia. *AARMS*. Vol 11. No 1.

Nye, J. S. (2010). Cyber Power. *Harvard Kennedy School,Belfer Center for Science and International Affairs*. No 18.

Nye, J. S. (2011). The Future of Power. *Los Angeles World Affairs Council*. http://www.lawac.org/speech-archive/pdf/1596.pdf (Erişim Tarihi: 10.10.2017).

Papp, D. S. and D. Alberts. (1997). The Impacts of the Information Age on International Actors and the International System. Papp and Alberts (eds). *The Information Age: An Anthology of its Impacts and Consequences*. CCRP Publication Series.

Parag, K. (2015). How Small States Prepare for Cyber-War. http://edition.cnn.com/2015/09/02/opinions/estonia-cyber-war/index.html (Erişim Tarihi: 05.10.2017).

Perlroth, N. (2013). Hunting for Syrian Hackers Chain of Command. New York Times.

Pihelgas, M. (2013). Back-Tracing and Anonymity in Cyberspace. Katharina Ziolkowski (ed.) *Peacetime Regime for State Activities in Cyberspace*. Tallinn: NATO CCD COE Publication.

Ralston, R. J. (2014). *Ontological Security: State Identity and Self-Image in the Digital Age.* Master of Arts in Political Science. Virginia Polytechnic Institute and State University.

Ramishvili T. (2016). Estonia's D5 Presidency. https://www.fpri.org/2016/01/estonias-d5-presidency/ (Erişim Tarihi: 09.10.2017).

Rauscher, K. F. (2011). First Joint Russian-U.S. report on Cyber Conflict. https://www.eastwest.ngo/idea/towards-rules-governing-cyber-conflict-0 (25.08.2017).

Reinbold, M. (2010). Superempowerment, Networked Tribes and the End to Business as We Know It. http://igniteshow.com/videos/super-empowerment-networked-tribes-and-end-world-we- know-it (Erişim Tarihi: 16.10.2017).

Rojansky, M. (2016). Russia and America's Cyber Deterrence Dilemma. http://nationalinterest.org/feature/russia-americas-cyber-deterrence-dilemma-18900 (Erişim Tarihi: 20.10.2017).

Rothkopf, D. J. (1998). Cyberpolitik: The Changing Nature of Power in the Information Age. *Journal of International Affairs*. Vol 51. No 2.

Schmidt, E. and J. Cohen. (2010). The Digital Disruption: Connectivity and the Power of Diffusion. *Foreign Affairs* Vol 89. No 6.

Schmidt, N. (2016). Super-empowering of Non-State Actors in Cyberspace. http://www.academia.edu/10088487/Super-empowering_of_Non-State_Actors_in_Cyberspace (Erişim Tarihi: 02.09.2017).

Schmitt, M. (2014). International Law and Cyber Attacks: Sony v. North Korea. https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/ (Erişim Tarihi: 24.08.2017).

Schmitt, M. N. (2011). Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review*. Vol 56.

Sheldon, J. B. (2011). Deciphering Cyberpower: Strategic Purpose in Peace and War. *Strategic Studies Quarterly*. No 18.

Sigholm, J. (2013). Non-State Actors in Cyberspace Operations. *Journal of Military Studies,* Vol 4. No 1.

Toffler, A. and H. Toffler. (1993). *War and Anti–War*: *Survival at the Dawn of the 21st Century.* New York.

Vandenberg, J. (2013). From Information Security to Cyber Warfare: Security to Cyber Warfare: Some Paradigm Shifts and Research Callenges. http://www.w-i-c.org/MWM2013/VanDenBerg_paradigmshifts.pdf (Erişim Tarihi: 15.08.2017).

Vlahos, M. (1998). Entering the Infosphere. *Journal of International Affairs*.

Volgy, T. J., K. Kanthak, D. Frazier, and R. S. Ingersoll. (2004). Structural Versus Relational Strength: The Cohesion of the G7 and the Development of the Post-Cold War International System. *Fifth Annual Pan European International Relations Conference*.

Walt, S. M. (1997). The Progressive Power of Realism. *The American Political Science Review*. Vol 91. No 4. 1997.

Wilhelmsen, V. C. R. (2014). *Soft War in Cyberspace: How Syrian Non-state Actors Use Hacking to Influence the Conflict's Battle of Narratives*. Master's Thesis - Political Science, Universıty of Oslo.

Winston, H. R. (2011). On the Nature of Military Theory. Charles Lutes (ed.). *Toward a Theory of Spacepower: Selected Essays*. Washington: NDU Press.

Yüksel, M. (2016). 3. Dünya Savaşı Öncesi Siber Güç Testinde Zayiat Büyük. http://www.yenisoz.com.tr/3-dunya-savasi-oncesi-siber-guc-testinde-zayiat-buyuk-makale-16757 (Erişim Tarihi: 01.10.2017).

Yüksel, M. (2017). Siber Savaş Oyunları. http://www.yenisoz.com.tr/siber-savas-oyunlari-makale-22631 (Erişim Tarihi: 09.09.2017).

Zacher, M. W. (1992). The Decaying Pillars of the Westphalian Temple: Implications for International Order and Governance. James N. Rosenau and Ernst-Otto Czempiel (eds). *Governance Without Government*: *Order and Change in World Politics*. Cambridge University Press.

ULUSAL SİBER GÜVENLİK STRATEJİ BELGELERİNDE İNSAN HAKLARI

Gül Nazik ÜNVER[*]

Özet

Bu çalışmada, siber alanda ABD, Türkiye, İngiltere, Almanya ve Hollanda'nın ulusal siber güvenlik strateji belgelerinde insan haklarının nasıl işlendiği, uluslararası insan hakları koruma

[*] Doktora Öğrencisi, Selçuk Üniversitesi, İİBF-Uluslar arası İlişkiler Bölümü, E-mail: gulunver@outlook.com

mekanizmaları da dikkate alınarak bu düzenlemelerin insan hakları üzerindeki etkileri analiz edilmektedir. Bunun için öncelikle, ulusal siber güvenlik perspektifiyle ortaya koyarak ülkelerin güvenlik yaklaşımlarına, hukuki düzenlemelerine odaklanarak yeni bir bakış açısı ve farklı bir boyut getirmesi açısından gereken adımlar ve öneriler üzerinde durulacaktır. Özellikle çalışma, belirli bir ulusun siber güvenliğe ilişkin hukuki yaklaşımı bağlamını netleştirmek için, ulusal bilgi toplumu ile ulusal siber güvenlik stratejisi hedeflerinin bir literatür taramasını sunmaktadır.
Anahtar Kelimeler: Siber Güvenlik, Strateji Belgesi, İnsan Hakları, Koruma mekanizmaları

HUMAN RIGHTS IN NATIONAL CYBERSECURITY STRATEGY DOCUMENTS

Abstract

In this paper, the United States, Turkey, United Kingdom, Germany, the Netherlands and Belgium's national cyber security strategy documents and their impact on human rights and international human rights protection mechanisms are being analyzed in the cyber space. First of all, this work will focus on steps and suggestions with a new outlook for bringing a different dimension by focusing on legal regulations of countries, the security approaches of countries by putting forward the perspective of national cyber security. In particular, the paper describes security and strategic management tasks. To clarify the context of the legal approach to a specific nation's cyber security, it presents a literatute review of the objectives of the national information society and the national cyber security strategy.
Key Words: Cybersecurity, National Strategy Document, Human Rights, protection mechanisms.

Giriş

Yirminci yüzyılda yaşanan teknolojideki hızlı gelişmeler, insan yaşamını etkilemiş, hızlandırmış, değiştirmiş ve dönüştürmüş, aynı zamanda siber alanda büyük ilerlemelere neden olmuştur. Siber uzay, yaşamın her noktasını ve toplumun her tabakasını birçok açıdan etkilemekle beraber, internet kullanımı yaşam tarzını da değiştirmektedir. Siber alanda yaşanan ilerlemeler ile bilgi dijital ortamda yani siber ortamda üretilebilmektedir. Siber ortamda bilginin çoğaltılması, erişilmesi ve paylaşılması oldukça kolay hale gelmiştir. Fakat geçmişte de değerli olan bilginin, elektronik hale gelmesi ve bilişim sistemleri ile yoğun bir şekilde paylaşılması maruz kaldığı tehdidi artırmakta ve bilgi güvenliği kavramına yeni bir boyut kazandırmaktadır. Bu sayede ülke sınırlarının, mesafelerin, mekânın ve zamanın kısıtlamalarından kurtularak, her türlü bilgiye erişebilen yeni bir dünya oluşurken, bunun yanı sıra bilginin güvenliğini sağlamak

zorlaşmakta, bilginin bulunduğu ve iletildiği siber ortam güvenliği de önem kazanmaktadır. Böylece faaliyet alanlarını zorunlu olarak siber uzaya taşıyan ülkeler için ulusal güvenlik, siber uzaydaki güvenlik çerçevesinde yeniden değerlendirme mecburiyetini ortaya çıkarmıştır (Bayraktar, 2015: 18-19).

Bugün insanlar, telekomünikasyon ve bilgi teknolojilerindeki gelişmeler sonucunda sınırları ve mesafeleri göz önünde bulundurmadan kolayca iletişim kurabilirler. Siber uzayın getirdiği sınırsız özgürlük ortamında oluşturulan sanal kavramlar, giderek gerçek dünyayı, kişileri ve devletleri etkileyecek güvenlik sorunlarını da beraberinde getirmiştir. İnternete bağlantılı herhangi bir bilgisayar sisteminin veya ağının başka bilgisayar sistemleri veya ağlarına karşı kötü amaçlı eylemler gerçekleştirmek maksadı ile kullanılması, çağımızın siber suçlara karşı alınacak siber güvenlik önlemlerini sorgulamamızı gerektirmektedir. İnternetin ortaya çıkışı ile beraber siber tehditler de artmaya devam etmiştir. Siber uzayda bulunan bilginin değiştirilmesi, bilginin açığa çıkarılması, erişilebilirliğinin kesintiye uğraması gibi istenmeyen durumlara neden olan siber tehditler, bilgi ve iletişim teknolojilerinin getirdiği imkânların araç olarak kullanıldığı, klasik suçların siber ortama uyarlanmasını sağlamıştır (Ünver, Canbay ve Mirzaoğlu, 2009: 8). Bu durum siber güvenliğin bireysel, ulusal ve küresel alanda önemini artırmış ve alınması gereken önlemler için hukuki boyutunu da vurgulamıştır.

21. yüzyılda insanlar adeta iki ayrı dünyada yaşar hale gelmiştir. Bir yanda ülke sınırlarının, ulusal egemenliklerin, hukuki düzenlemelerin, özgürlüklerin ve hakların bulunduğu, herkesin belirli bir kimlikle tanımlandığı fiziki gerçek dünya yer alırken; diğer yanda ise fiziksel ve özgürlük anlamında sınırların, hukuksal düzenleme ve güvenlik tedbirinin bulunmadığı, kimliklerin gizlenebildiği siber alan yer almıştır (Bayraktar, 2015: 15). Ancak, bu yeni ortamda yaşam, özgürlük ve güvenlik hakkı arasında bir denge kurmak ne kadar mümkündür? Siber alan güvenlik, istikrarsızlık ve insan hakları da dâhil olmak üzere birçok açıdan uluslararası ilişkileri etkiledi. Bu nedenle, kimin kontrol edeceği? ya da kontrol edilmeli mi? anlamında sorunlu bir konu olmuştur (Akyeşilmen, 2016: 39).

Devletlerin siber tehditlere ne kadar açık olduğunun ilk ölçütü, ülkenin kendi yetenekleri, insan hakları boyutu ve siber güvenlik algısıdır. Güncel meseleler daha çok sanal çerçevede gelişme gösterdiği için bireye ve topluma yönelik bilinmeyen bir konumdan, hızlı ve çabuk tehdit türlerini de beraberinde getirmiştir. Bu tehditler özellikle siber uzayda karşımıza çıkarak, küreselleşmeyi, teknolojik ilerleme ve yeniliği de ortaya çıkarmaktadır. İnsan hakları açısından

temel hak ve özgürlüklerin ulusal strateji belgelerinde yoğun bir şekilde göz ardı edilmesi ve hatta siber saldırılarda bireyin ve kamu kurumlarının almış olduğu tehditlere karşı siber güvenliğin strateji belgelerinde yetersiz kalması en önemli sorunların başında gelmektedir. Sorumlular tespit edilse dahi, bu konuda gerekli yaptırımları uygulamaya yardımcı olacak hukuki açıdan herhangi bir uluslararası mekanizma yoktur. İnsan hakları ve siber güvenlik arasındaki ilişki iki yönlüdür: tüm kullanıcılar için güvenli bir siber alan oluşturmak ve siber alanda güvenli bir insan hakları ortamı oluşturmak. Siber güvenlik ve insan hakları gibi nispeten yeni olan bu iki gerçek birbiriyle derin ilişkili ve birbirine bağlıdır. Her ikisini de sağlayabilecek bir uluslararası mekanizma geliştirmeliyiz. Çalışmanın yanıt aradığı temel soruları şu şekilde sıralamak mümkündür:

"Genel kabul görmüş ulusal siber güvenlik tanımı var mı?"
"*Siber güvenliği ele alırken temel insan hakları endişeleri nelerdir?"*
"Ulus-devletlerin hukuki açıdan birey ve kurumların temel hak ve özgürlüklerini kısıtlayıp kısıtlamaması siber güvenlik strateji belgelerinde nasıl değerlendirilmektedir?"
"ABD, Türkiye, İngiltere, Almanya, Hollanda'nın ulusal siber güvenlik anlayışı nasıl şekillenmektedir?"
"Ulus-devletlerin siber güvenlik strateji belgelerine, insan hakları boyutu açısından sağladığı eylemler nelerdir?"

Yukarıdaki sorulardan yola çıkılarak yapılan araştırmalar sonucu, bu çalışmanın temel noktası, ulusal siber güvenlik strateji belgesinin kurgusal temel olarak siber güvenlik yaklaşımı ve insan hakları kavramının açıklanabildiği ve ulusal strateji belgeleri ile bu savı güçlendirdiğidir. Bu çalışmada; siber güvenliği tanımlayarak, strateji belgesinin ne olduğu, siber güvenlikte insan haklarının nasıl olması gerektiği ve ne gibi önlemler alınması gerektiği üzerine tartışılmaktadır. Ardından tarihsel süreç içerisinde ABD, Türkiye, İngiltere, Almanya ve Hollanda'nın ulusal siber güvenlik strateji belgelerinde somut gelişmelerin insan hakları boyutu üzerine etkili olup olmadığı ve her bir ülkenin siber güvenlik kabiliyetlerini incelemektedir. Bu nedenle ulus-devletlerin ulusal güvenliğini de tehdit edecek seviyeye gelen siber alanda ve insan hakları boyutunun etki alanını kapsayan siber alanda, saldırılara karşı alınan ve uygulamaya konulmaya çalışılan önlemler için ulusal siber güvenlik strateji belgelerinin varlığı bu çalışmaya esin kaynağı olmuştur. Ayrıca devletlerin ulusal strateji belgeleri üzerinde almış olduğu önlemlerin insan hakları bağlamında ele alınarak sonuç kısmında kısa bir değerlendirme yapılacaktır.

Siber Güvenlik ve İnsan Hakları

Siber güvenlik, tanımları nispeten değişken, çoğunlukla öznel ve bazen de bilgi sahibi olunmadan geniş yelpazede kullanılan bir terimdir. Siber güvenliğin çok boyutlu olmasını yakından tanımlayan özlü, genel kabul edilebilir bir tanımın bulunmaması, karmaşık siber güvenlik sorunlarını çözmek için uyumlu olarak hareket etmesi gereken disiplinleri birbirinden ayırırken, pratikte de sorunlara neden olabilmektedir. Literatürde çok çeşitli tanımlara rastlamak mümkündür. Örneğin, *Defining Cybersecurity* başlıklı makalede "Siber güvenlik, siber-alan ve siber-alan sistemlerini fiili (de facto) mülkiyet haklarından hukuka (de jure) aykırı olaylardan korumak için kullanılan kaynakların, süreçlerin ve yapıların organizasyonu ve toplanması" olarak tanımlanmıştır (timreview, 2017). Diğer bir tanımda siber güvenlik, "siber alanda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünü*"* olarak tanımlanabilmektedir (Ünver, Canbay ve Mirzaoğlu, 2009: 1-2). Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımlarını, personeli, altyapıları, uygulamaları, hizmetleri, telekomünikasyon sistemlerini ve siber ortamda iletilen veya saklanan bilgilerin tümünü kapsamaktadır. Siber güvenlik, elektronik ortamı oluşturan bilişim sistemlerinin zarar verilmesini, bu sistemlere yetkisiz bir şekilde erişilmesini veya bu sistemlerin suiistimal edilmesini önlemeyi içermektedir. Dolayısıyla siber güvenlik, gizlilik bütünlük, erişilebilirliği sağlamayı amaçlamaktadır (Ünver, Canbay ve Özkan, 2010: 36-37).

Siber güvenlik, teknik bir disiplinden stratejik bir konsepte hızla dönüşmüştür. Küreselleşme ve internet, sürekli gelişmekte olan ağ teknolojisi üzerine kurulu bireylere, örgütlere ve uluslara olağanüstü yeni bir güç vermektedir. Siber güvenlik için devletlerin tek başına çabaları yetmez, işbirlikleri ve hatta devlet dışı aktörlerle birlikte hareket etmeleri önemlidir. En başarılı uluslararası siber güvenlik anlaşması, 2001'de imzalanan Avrupa Siber Suç Sözleşmesi'dir. Bu antlaşma, telif hakkı ihlali, dolandırıcılık, çocuk pornografisi ve ağ güvenliği politikasının ihlal edilmesi konularını kapsıyor. Veri kesme ve bilgisayar ağlarının aranmasına ilişkin kolluk kuvvetleri için kurallar sunmaktadır. Nihai amacı ulusal mevzuat ve uluslararası işbirliği vasıtasıyla dünya çapında siber suç konusunda ortak bir politika oluşturmaktır. Hâlihazırda, kırk yedi taraf imzacıya sahiptir, otuza kadar ulus-devlet onaylamıştır ve ulus devletler için siber güvenlik açısından temel yasal sözleşmedir (Geers, 2011: 29-30).

Siber uzaydaki tehditlerin çoğunluğu birden fazla değişken ile ortaya çıkmaktadır. Tehdidin çok boyutlu olması, savunma ve koruma içinde benzer bir yaklaşımı zorunlu kılmaktadır. Hamleler gizlilik gerektirdiği durumda, gelişmiş ağ güvenlik çözümleri ortaklıkların kurulmasına ihtiyaç duymaktadır (Bıçakçı, 2013: 39). Başlangıçta, internet genellikle insan haklarının geliştirilmesi ve korunması için ütopik bir terim olarak tanımlanmıştı. Demokratikleşmenin ve insan haklarının hayata geçirilmesine yol açarak, tüm bilgiyi özgürleştiren, bireyleri güçlendiren ve devleti daha şeffaf ve hesap verebilir hale getirerek zayıflatacak olan bir alanı temsil ediyordu (Akyeşilmen, 2016: 51).

İnsan hak ve özgürlükleri evrenseldir. Evrensel insan hakları, kozmopolitan bir dünya görüşü ve siyaset modeli öngörmektedir. Kozmopolitan anlayış uluslararası ilişkiler yaklaşımına göre, bireyi ve insan gruplarını başlangıç noktası olarak ele almaktadır. İnsan hakları ülkeden ülkeye farklılık göstermeyen, esasında insan onurunun korunarak bireyin insanca yaşamasını sağlayan temel haklardır. Birleşmiş Milletler kurucu yasası, İnsan Hakları Evrensel Bildirgesi ve Sivil ve Siyasal Haklar ile Sosyal ve Ekonomik Haklar Sözleşmelerinde imza atmış olan bütün ulus-devletler, insan haklarının "ulusal" olmakla beraber "uluslararası bir nitelik ve boyut" taşıdığını kabul etmişlerdir (Dağı, 2010: 219-222).

Strateji Belgesi Nedir ve Nasıl Olmalıdır?

Ulusal bir siber güvenlik stratejisinin hazırlanması görevi karmaşıktır. Siber tehditlere yönelik önlemler bir takım farklı alanlardan gelmektedir: politik, teknolojik, yasal, ekonomik, yönetsel veya askeri nitelikte olabilirler. Dahası belirli risklere uygun diğer disiplinleri içine alabilirler. Bu yetkinliklerin hepsi, güvenliği güçlendirecek ve tehditlere karşı direnebilecek tepkiler sunmak için bir araya gelmesi gerekmektedir. Birçok ülke kendi ulusal strateji belgelerinde siber güvenlikle ne kastettiklerini tanımlamaktadır. Hükümetler, işletmeler ve vatandaşlar, siber dünyanın insan yapımı olduğunu, sezgisel ve giderek genişleyen bir çevre olduğunu bilmektedir. Bu nedenle tanımlar daima değişmektedir. *"National Cyber Security Framework Manual"* kılavuzunun yayınlanmasından bu yana elliden fazla ülke, güvenliğin gelecekteki ulusal ve ekonomik güvenlik girişimleri için ne anlam ifade ettiğini belirten bir çeşit siber strateji belgeleri yayınlamıştır. Strateji Belgesi, belirli hükümet kollarının ve bilgi güvencesi ilkelerinin, kamu, özel ve ilgili uluslararası Bilgi ve İletişim Teknolojileri sistemlerine ve bu

sistemlerin doğrudan ulusal güvenlik ile ilgili olduğu içerikle ilişkili olarak uygulanmasıdır (Klimburg, 2012: 12).

Nispeten yakın zamana kadar, "ulusal güvenlik" terimi yalnızca Amerika Birleşik Devletleri'nde kullanılıyordu. Birçok OECD ülkesinde "ulusal güvenlik stratejileri"nin (NSS) yaygın olarak tanıtılması, birkaç özel "tehdit"e odaklanarak, sayısız riske karşı olan fikri stratejik düşünce değişiminde katı biçimde bağlı olduğu görülen yeni bir olgudur. Örneğin, 2007 sonrası stratejilerin neredeyse tamamında, siber güvenlik kilit bir ulusal güvenlik meselesidir. Nitekim bazı durumlarda, "siber güvenlik" (hatta "ulusal siber güvenlik") konusu, ulusal güvenlik stratejisinin oluşturulmasını öngörmektedir ve bazen daha kapsamlı bir ulusal paradigmaya kayma için bir rehber gibi işlev görmektedir. Stratejilerde devlet sadece çeşitli risklere karşı önlem alınması gerektiğini değil, devlet dışı aktörlerle birlikte çalışarak da risklerin çözümlenebileceğini kabul etmektedir (Klimburg, 2012: 20).

Hükümetler, ulusal düzeyde stratejik eylem planları ve siber güvenlik için kurumlar da dâhil olmak üzere ulusal düzeyde belge ve girişimler geliştirmeye çalışmaktadırlar. Sanal gerçekliği yakalamak için, ulusal stratejik eylem planları ve inisiyatiflerin, ilgili kilit konuları çerçevelemesi ve insan hakları ile ulusal güvenlik hususlarını dengelemesi ve siber tehditlere yönelik uluslararası işbirliğinin geliştirilmesi konularında önemli sorunları tanımlaması gerekmektedir (Akyeşilmen, 2016: 51-52).

Bir stratejinin oluşturulması, politika yapıcılar için bir araçtır. İyi gelişmiş bir strateji, politika yapıcılara temel hedefler, gerekli kaynaklar ve bunları en etkin şekilde nasıl kullanabilecekleri konusunda rehberlik yapmalıdır. Belirli bir alanı kapsayan tek başına bir strateji söz konusu olduğunda, özellikle karar verme ve politika yapıcılar arasında farkındalık düzeylerinin yükseltilmesi için uygulamayı kolaylaştırmak önemli olabilir (Klimburg, 2012: 64). Her bir hükümet sistemi, ele alınması gereken kendi özel durum kümesini sağlayacak ve her belirli strateji bireysel yetkileri vurgulamak isteyecektir. Optimal bir dünyada, ulusal bir siber güvenlik stratejisi (veya NCSS) oluşturmanın tüm süreçlerinin basamak basamak alt süreçlerden oluştuğunu görmek mümkündür. Bu nedenle, strateji belgesinin sunabileceği en önemli katkı bir NCSS'deki en kritik meselelere ilişkin farkındalık yaratmak ve nasıl tanımlanabileceğini belirlemektir (Klimburg, 2012: 191).

ENISA, Nisan 2013'te Ulusal Siber Güvenlik Stratejisini belirleyen ülkeleri kendi web sitesinde sıralamıştır. ENISA'nın 2010 yılından itibaren siber güvenliği sağlamada daha önemli rol oynayabilmesi için yetkileri artırılmıştır. ENISA ile ABD İç Güvenlik Bakanlığı bu alanda işbirliği yapmak adına *'Cyber Atlantic'* adı altında bir faaliyet de düzenlemiştir. Faaliyet çeşitli siber saldırılar için senaryolar üretmek ve bunlara karşı koymak üzere yapılacak çalışmaları içermektedir (sibersavunmalar, 2017). Her strateji, siber faydalar ile siber riskler (veya tehditler) arasındaki dengesiz dengeyi vurgularken, siber dünyanın önemini ve dijital bir toplumun kazanımlarını onaylamayla başlar.

Ulusal bir siber güvenlik stratejisi (NCSS) genellikle teröristler, dış ülkeler, casusluk, organize suç veya siyasi aktivizm dâhil olmak üzere tehditler üzerine bir bölüm içermektedir. Stratejiler genellikle önemli terimleri de tanımlamaktadır. Bununla birlikte, kesin tanımlar, açıklamalarda kullanılan tanımlar ve anlamdaki açıklığa göre daha az önem taşıyabilmektedir. Bütün NCSS'ler aynı tanımları kullanmamaktadır. Örneğin, bazıları *"siber alanı"* sadece internet için, diğerleri ise daha geniş bir tanımlamayı benimsemektedir. Herhangi bir ulusal strateji gibi, bir NCSS'de hükümet birimlerinin vizyonunu tutarlı ve uygulanabilir politikalara çevirmesini sağlamalıdır. Hükümetin uluslararası meselelerde nasıl davrandığını açıklayan ve diğer ilgili stratejilere bağlantı oluşturan bir strateji belgesi oluşturulmalıdır (Klimburg, 2012: 196).

Bazı Ulusal Siber Güvenlik Strateji Belgelerinde İnsan Hakları

Soğuk Savaş'ın sona ermesiyle beraber interneti sağlayan ağlar giderek artmıştır. Soğuk Savaş döneminde öncelik verilen durum bilgi güvenliği üzerine olmuştur. Bilgisayar teknolojisinin kullanımının yaygınlaşması ile kişisel bilgilerin saklanması ve şifrelenmesi noktasındaki ihtiyaçlar ortaya çıkmıştır. Siber güvenlik alanındaki tehditlerin birçoğu farklı çeşitlerde kendini göstermiştir. Tehdidin çok boyutlu olması, sınırlarının belirlenememesi, saldıranın kimlik ve yerinin bilinememesi, insan haklarını siber alanda savunmayı güçleştiren nedenler arasında sayılmaktadır. Siber alan kullanıcısına sınırsız fayda sağlarken, insan hakları ihlaline açık hale getirmiştir.

New York ve Washington'da 11 Eylül 2001 tarihinde yolcu uçaklarını çeşitli hedeflere çarparak yapılan terör saldırıları, uluslararası sistemdeki güvenlik tanımlarını değiştirmiştir. Soğuk Savaş'ın ardından ulusal güvenlik üzerine yapılan görüşler birçok ülkenin listesinde yeniden ilk sıraya çıkmıştır. Terörizme karşı savaş yalnızca saldırıya uğrayan ulus-devletin değil,

neredeyse sistemdeki tüm aktörlerin gündemine girmiştir. Saldırılardan hemen sonra internet üzerinden iletişim kurmuş olduklarının ve kullandıkları uçakları daha önce simülasyon uygulamasında çalışmış olduklarının fark edilmesi üzerine internet ortamının terörist saldırılar için kullanılmakta olduğu düşüncesini giderek artırmıştır (Thomas, 2003: 115-121). Siber güvenliğin ihlali çok farklı şekillerde yapılmış durumdadır. Ulusların siber sistemlerine yönelik saldırılarla ülkenin durumunu derinden zedeleyecek olan ekonomik ve diğer kritik alt yapılara hasar verilerek etkisiz hale getirilebileceğine inanılıyordu. Bu tür kaygıların ulusal güvenlik ile yakın olarak bağlantılı olduğu düşüncesi ile devam etmiş ve izleyen süreçte birçok ülke siber güvenlik stratejilerini ulusal güvenlik belgelerine eklemişlerdir. Bundan dolayı ulusal strateji belgeleri düzenli olarak güncellenmektedir (Bıçakçı, 2013: 32-33).

Peki insan hakları bu belgelerde nasıl işlenmektedir? Birkaç örnek üzerinden bu konuyu irdelemek yararlı olacaktır.

Amerika Birleşik Devletleri ve Siber Strateji Düzenlemeleri

Savunma Bakanlığı Siber Kullanım Stratejisi, Mayıs 2011'den beri siber faaliyetlerini ve operasyonlarını ABD'nin ulusal çıkarlarını desteklemek için rehberlik etmiştir. Amerika Birleşik Devletleri Savunma Bakanlığı (DoD), ABD vatanını ve ABD'nin çıkarlarını siber alanda meydana gelebilecek saldırılar da dâhil olmak üzere saldırıdan korumaktan sorumludur.

> *ABD ve uluslararası hukuka uygun bir şekilde, Savunma Bakanlığı, barış, kriz veya çatışma dönemlerinde ABD ulusal çıkarlarına zarar vermeye çalışan herhangi bir düşmana karşı saldırıları caydırmaya ve ABD'yi savunmaya çalışmaktadır. Bu amaçla Savunma Departmanı, siber operasyonlar için yetenekler geliştirdi ve bu yetenekleri, Birleşik Devletler hükümetinin diplomatik, askeri, ekonomik, finansal ve kanuni uygulama araçları da dahil olmak üzere ABD'nin ulusal çıkarlarını savunmak için kullandığı tüm araçlara entegre etti* (USA, 2015: 3).

DoD, bir etki yaratabilecekleri siber saldırıları engellemek, kolluk kuvvetleri, istihbarat ve diplomatik araçları dahil etmek için çeşitli seçenekler ve yöntemler geliştirmek üzere diğer kamu kurumlarıyla yeteneklerini senkronize etmeyi amaçlamaktadır (USA, 2015: 4). ABD'nin, tehdit ve riskler konusunda daha fazla kamuoyu bilincini geliştirmesi ve ulusun güvenlik

ihtiyacı anayasa ve yasalarla güvence altına alınan gizlilik haklarına ve kişisel özgürlüklere ulusal taahhüdüne yönelik entegre bir yaklaşım sağlamak için siber güvenlik konusunda ulusal bir diyalog yürütmesi gerekmektedir (USA, 2011: 13-15).

Strateji belgesine göre, Birleşik Devletler'de İnternetin açık, güvenli ve erişilebilir olmasının sağlanması ve insan hayatının korunmasının gerekli olduğu gibi, her zaman kısıtlayıcı bir doktrin kapsamında siber operasyonlar yürütülmesi de gereklidir. Siber alanda Savunma Departmanı daima, hukukun üstünlüğünü destekleyerek, ifade özgürlüğüne ve gizliliğine saygı duyarak, ABD'nin değerlerini koruyarak, bilgi, ticaret ve fikirlere önem vererek özgür hareket edecektir. Savunma Bakanlığı kanun uygulaması (law enforcement), istihbarat, karşı istihbarat ve politika kuruluşlarının tamamı DoD'nin ağlarını ve bilgi teknolojisi sistemlerini kuran ve işleten bireyler gibi aktif bir role sahiptir. Uygulanabilir tüm kanunlara ve politikalara uygun olarak, DoD, küresel ağlar ve sistemler, düşman yetenekleri ve kötü amaçlı yazılım aracıları ve pazarları hakkında ayrıntılı, öngörülebilir ve uygulanabilir istihbarat gerektirmektedir (USA, 2015: 24).

Son dönemde yayınladığı ulusal siber güvenlik strateji belgesinde Amerika, sadece ülke içinde değil küresel çapta da insan haklarının korunmasına vurgu yapmaktadır: "Sözlerimiz ve eylemlerimizle birlikte baskıcı rejimler altında yaşayan insanlara, özgürlük, kişisel onur ve hukukun üstünlüğünü arayanlara destek vereceğiz. Özgür ve müreffeh toplumumuzun çıkarlarını baskıcı rejimlere ve insan haklarını kötüye kullanan toplumlara sunma yükümlülüğümüz bulunmamaktadır" (USA, 2017: 42). ABD için sınırları ve göç sistemini kontrol altına almak ulusal güvenlik, ekonomik refah ve hukukun üstünlüğü için merkezi bir noktadır (USA, 2017: 8).

Türkiye'nin Siber Güvenlik Strateji Raporları

Uzun süre Türkiye'de yetkililer siber tehditleri yalnızca siber suç seviyesinde değerlendirmiş ve önemli güvenlik kurumlarına yönelik yapılan saldırılar, terörle mücadele çerçevesinde ele alınmıştır. TÜBİTAK (Türkiye Bilimsel ve Teknolojik Araştırma Kurumu) bünyesinde kurulan birimler ve ulusal bilgi güvenliği kapısıyla devlet kurumlarındaki siber güvenliğe yönelik bilinçlenme çalışmaları giderek hızlanmıştır. Milli Güvenlik Kurulu 27 Ekim 2010 tarihinde siber tehditler üzerine toplantıda bu konuyu tartışmıştır. Toplantıda siber tehditler kavramının Milli Güvenlik Siyaset Belgesi'ne girmesine karar verildiği duyurulmuştur. 25-28 Ocak 2011

tarihlerinde TÜBİTAK ile Bilgi Teknolojileri ve İletişim Kurumu (BTK) işbirliği ile *"Birinci Ulusal Siber Güvenlik Tatbikatı"* icra edilmiştir(TÜBİTAK ve BTK, 2011). Tatbikatın ardından yayınlanan raporda, Türkiye'nin siber saldırılara karşı savunmasız ve açık olduğunu, kamu kuruluşlarının konuyla yeterince ilgilenmediklerivurgulanmıştır.

2012 yılında *"Redhack"* adlı grubun Türkiye'de birçok kamu kuruluşuna yaptığı saldırılar ve bu saldırıların medyada yer alması, Türkiye'de siber tehdit algısının oluşmasını hızlandırmıştır. Bunun üzerine 20 Ekim 2012 tarihinde toplanan Bakanlar Kurulu, *"Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar"*ı onaylamıştır (Bıçakçı, 2013: 45-46). Bu kararda siber güvenlik kurulunun strateji belgesi ve eylem planı olarak Ulaştırma, Denizcilik ve Haberleşme Bakanlığı başkanlığınca oluşturulmasına karar verilmiştir. Bu kurulun görevi "kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda yer alan sistemlerin güvenliğinin sağlanmasına ve gizliliğin korunmasına yönelik tedbirlerin alınması ve bilgi ve iletişim teknolojilerine ilişkin kritik altyapıların işletiminde yer alan gerçek ve tüzel kişilerce uyulması gerekli usul ve esasları düzenlemek" olarak açıklanmıştır (Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, 2012).

Türkiye bu düzenlemelerin ardından artan tehdit göz önüne alınarak ikinci Ulusal Siber Güvenlik Tatbikatı yapılmıştır. 25 Aralık'ta başlayan ve sekiz aşamalı olan tatbikata katılan altmış bir kurum ve kuruluşa gerçek siber saldırılar düzenlenmiştir. NATO'nun yeni oluşan tehditler karşısında geliştirdiği politikasıyla eşgüdümlü olarak Türk Silahlı Kuvvetleri 21 Ocak 2013 tarihinde Siber Savunma Merkezi Başkanlığı'nı oluşturduğunu açıklamıştır. Bu başkanlığın Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ile koordineli çalışacağı, NATO tatbikatlarına katılacağı da belirtilmiştir (Bıçakçı, 2013: 46-47).

Türkiye'nin ilk belgesi olan 2013-2014 Ulusal Siber Güvenlik Strateji Belgesi'nde siber güvenlik ve insan hakları için, "…teknik boyutun yanı sıra; hukuki, idari, ekonomik, politik ve sosyal boyutlarda güçlü ve zayıf yönlerin, tehditlerin ve fırsatların belirlenmesini içeren bütüncül bir yaklaşım benimsenir. Hukukun üstünlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması ilkeleri temel esas kabul edilir" (Türkiye, 2013, 14-15). Ulusal siber güvenliğin sağlanması konusunda gerek kurum ve kuruluşların görev, yetki ve sorumluluklarını tanımlayan, gerekse ihtiyaç duyulan alanlarda mevcut eksiklikleri gidermeyi amaçlayan mevzuatın oluşturulması çalışmaları yapılacağı belirtilmektedir. Söz konusu bu çalışmalar, ceza

hukuku, medeni hukuk, idari yargı ve bunlara ilişkin tüm usul hükümlerinin düzenlenmesine destek olacak bir nitelik arz etmektedir. Ayrıca, kavram kargaşasının önüne geçmek amacıyla siber güvenlik terminolojisi ve sözlüğünün oluşturulacağı ifade edilmiştir:

> *Uluslararası hukuk kuralları çerçevesinde, siber saldırılara maruz kalan tarafların haklarının korunabilmesi için, saldırı kaynağının tespiti ve saldırılan sistemler ile bu sistemlerden hizmet alan taraflarda hangi boyutta etki oluştuğunun belirlenmesi gerekir. Bu bilgilerin üretilmesi için ulusal siber ortamın günün teknolojisine uygun ve güvenilir kayıt mekanizmaları ile donatılması gerekmektedir*(Türkiye, 2013: 18).

2016-2019 için Türkiye'nin ikinci ulusal siber güvenlik strateji belgesi yayımlanmıştır. Türkiye, diğer ülkelerin strateji dokümanlarında olası siber güvenlik risklerine ve riskleri ortadan kaldıracak eylemler uygulanmasını göz önünde bulundurmuştur. Bu nedenle ikinci strateji belgesinde bu ilkelere yer verilmekte, risklerin ve ilkelerin ülkeden ülkeye çok fazla değişiklik arz etmediği gözlemlemektedir. Bu noktada göz önünde bulundurulan insan hakları ve hukukun üstünlüğünü de dikkate alan ilkeler şunlar olmaktadır:

> *Siber güvenliğin sağlanması için tüm paydaşların siber güvenlik risklerini bilmeleri, bu risklerin yönetilmesine ilişkin yaklaşımlarının kendileri kadar başkalarını da etkileyebileceğinin bilincinde olmaları gerekir. Bu farkındalık ve yetkinliğin sağlanması için tüm paydaşların gerekli eğitim ve deneyimi kazanmaları sağlanır. Teknik boyutun yanı sıra; hukuki, idari, ekonomik, politik ve sosyal boyutları da içeren bütüncül bir yaklaşım benimsenir. Tüm paydaşlar, siber uzay güvenliğinin sağlanması için çalışırken, hukukun üstünlüğü, ifade özgürlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması ilkelerini gözetir (Türkiye, 2016: 11).*

Alıntıdan da anlaşıldığı üzere, siber güvenliğin temelinde yer alan kavramlarından birisi hukukun üstünlüğü ve insan haklarıdır. Bu çerçevede, atılacak adımların bu ilkelere uygun olması önem arz etmektedir.

İngiltere Siber Güvenlik Strateji Belgesi

Ulusal güvenlik stratejisi gibi sadece devletin değil, vatandaşların da korunmasını öngören siber güvenlik strateji belgesi, bütün kesimlerin dolandırıcılığın her türünden, kimlik hırsızlığından ve teknoloji kullanılarak işlenen siber suçlardan korunmasının yollarını belirlemektedir

(timeturk, 2009). İngiltere'nin 2010 yılında yayınlamış olduğu strateji belgesinde ulusal çıkarlarının; "hukukun üstünlüğü, demokrasi, özgür ifade, hoşgörü ve insan hakları*"* karşısında ülkenin inancı ile bağdaşarak ilerlemesini sağlamaktır. Bunlar, İngiltere'nin dünyada sahip olduğu nitelikler ve "biz onları ilerletmeye devam etmeliyiz, çünkü değerlerimiz dünyada saygı görürse İngiltere daha güvenli bir konumda olacaktır" (İngiltere, 2010: 4). Stratejisi, olmak istedikleri ülkeyi yansıtarak; değerlerine ve fikirlerine güvenen refah sahibi, güvenli, modern ve dış görünüşlü bir ulus oluşturmaktır. Ülkenin milli menfaati güvenlik, refah ve özgürlüktür. Güvenli ve dayanıklı bir İngiltere inşa etmek ve dengeli bir dünyanın şekillenmesine yardımcı olmak için ulusal gücün tüm araçlarını bir araya getirebilen bir ulus olmaları gerektiğini vurgulamaktadırlar. "Bizim bakış açımız, esneklik ve esneklik ile karakterize edilecek ve insan haklarına, adalete ve hukukun üstünlüğüne olan bağlılığımız tarafından desteklenecektir" (İngiltere, 2010: 10).

Kurallara dayalı uluslararası sistemi uygulamak için BM gibi mevcut uluslararası kurumları ve G20 gibi ortaya çıkan kuruluşları güçlendirmeyi amaçladığını ileri sürmektedir. Güvenliğimizi destekleyen yapılardaki gelişmelere adapte olmak ve bunları etkilemek için de değişime ihtiyaç olacaktır. "ABD'yle olan ilişkimiz merkezli ve kalıcı olacak ancak gelişmeye devam etmesini beklemeliyiz. NATO yeni stratejik konseptini formüle edecek ve uygulayacak; AB'nin uluslararası rolü gelişecek; BM Güvenlik Konseyi de reforma tabi tutulabilir. Uluslararası hukuk ve normları şekillendirmede aktif bir rol oynamaya devam edeceğiz*"* (İngiltere, 2010: 15).

Başlangıç olarak, Birleşik Krallık, tüm hükümetlerin siber alanda ve ulusal ve uluslararası hukuka uygun olarak orantılı olarak hareket etmesi gerektiğine inandığını ifade ediyor. Bu, fikri mülkiyete saygı ve ifade ve dernek kurma özgürlüğüne ilişkin temel insan hakları da içermektedir (İngiltere, 2011: 27). Siber ortamda uluslararası insan hakları hukuku çerçevesinin nasıl uygulanacağını ve bu hakların garanti altına alınmasında yeni zorlukları tartışmak için çok taraflı ve iki taraflı kanallar kullanmayı öncelikli kıldığını ifade etmektedir (İngiltere, 2011: 40).

2016-2021 Ulusal Strateji Belgesine göre; ulusal ve uluslararası kanunlara uygun olarak hareket etmeleri ve başkalarının da aynı şeyi yapmasını beklediklerini ifade etmektedir. Temel değerlerin titizlikle koruması ve desteklenmesi gerektiği vurgulanmaktadır. Bunlara demokrasi dâhildir. Hukuk Kuralı, özgürlük, açık ve hesap verebilir hükümetler ve kurumlar, insan hakları

ve ifade özgürlüğü, İngiltere vatandaşlarının özel hayat ve mahremiyetlerini koruyacaklarını belirtmektedir. Hükümetin öncelikli görevi, ülkeyi diğer devletlerin saldırılarına karşı savunmak, vatandaşlarına ve ekonomilerine zarar vermeden çıkarlarını korumak, temel haklarını korumak ve suçluları adalete teslim etmek için ulusal ve uluslararası çerçeveyi oluşturmaktır (İngiltere, 2016: 25).

Siber güvenlik sadece teknoloji ile ilgili değildir. Başarılı siber saldırılardan hemen hemen tümünün katkıda bulunduğu bir insan faktörü vardır. Bu nedenle, hükümette çalışan herkesin siber bir riskin bilincinde olmasını sağlamak için halkına yatırım yapmayı devam edeceğine değinilmektedir. Risklerin arttığı alanlarda spesifik bir siber uzmanlık geliştirecektir ve bu riskleri etkili bir şekilde yönetmek için doğru süreçleri bulunduklarından emin olunacaktır (İngiltere, 2016: 38).

Siber meselelerde uluslararası işbirliği, daha geniş küresel ekonomik ve güvenlik tartışmalarının önemli bir parçası olmuştur. Tek bir uluslararası vizyon olmadan hızla gelişen bir politika alanıdır. İngiltere ve müttefikleri, kurallara dayanan uluslararası sistemin bazı unsurlarının yerine getirilmesini sağlamada başarılı olmuştur. Online olarak yaptıkları gibi insan haklarının geçerli olduğunu ve çok paydaşlı yaklaşımın, İnternet yönetiminin karmaşıklığını yönetmenin en iyi yolu olduğu konusunda geniş bir fikir birliğine varılmıştır. Ancak, ulusal güvenliği bireysel haklar ve özgürlükler ile uzlaştırmanın ortak meydan okumalarını nasıl ele alınacağına dair giderek artan bir bölünme ile birlikte, küresel uzlaşma hala kırılgan kalmaktadır (İngiltere, 2016: 63).

Almanya ve Siber Alanda İnsan hakları

2011’in başında yayımlanan Almanya Siber Güvenlik Strateji Belgesinde siber alan, tüm bölgesel sınırların ötesinde internet üzerinden erişilebilen tüm bilgi altyapılarını içermektedir. Almanya'da sosyal ve ekonomik yaşamın her noktasında, siber olanaklar kullanılmaktadır. Gittikçe birbirine bağlı bir dünyanın parçası olarak, Almanya’daki devlet, kritik altyapılar, işletmeler ve vatandaşlar, bilgi ve iletişim teknolojisinin ve internetin güvenilir çalışmasına bağlı olmaktadır. Almanya’da bilgi altyapılarının artan karmaşıklığı ve güvenlik açığı göz önüne alındığında, siber güvenlik durumu gelecekte de kritik olarak kalacaktır.

Siber güvenlik, hak ve hürriyetlerin uygulanması ve kritik bilgi altyapılarının korunmasını sağlamaktadır. Ayrıca devletin hem ulusal düzeyde hem de uluslararası düzeyde ortaklarla işbirliği yapmasını gerektirmektedir. Devlet, endüstri ve toplumun paylaştığı sorumluluklar göz önüne alındığında, bir siber güvenlik stratejisi tüm kişilerin ortak hareket edip görevlerini yerine getirmesi ile başarılı olacaktır. Aynı şey, uluslararası durum için de geçerlidir. Bilgi ve İletişim Teknolojileri sistemleri küresel ağlarda birbirine bağlandığından, diğer ülkelerin bilgi altyapılarındaki olaylar dolaylı olarak Almanya'yı etkileyebilmektedir. Bu nedenle siber güvenliği güçlendirmek için uluslararası yönetişim kurallarını, standartlarını ve normlarını uygulanması gerekmektedir (German NCSS, 2011: 2).

Siber güvenlik kapsamlı bir yaklaşıma dayalı olmalıdır. Bu, daha da yoğun bilgi paylaşımı ve koordinasyon gerektirmektedir. Siber Güvenlik Stratejisi ağırlıklı olarak sivil yaklaşımlara ve önlemlere odaklanmalıdır. Bilgi ve iletişim teknolojisinin küresel doğası göz önüne alındığında, uluslararası koordinasyona, yabancılara ve güvenlik politikası yönlerine odaklanan uygun ağlar vazgeçilmez olmaktadır. Buna sadece Birleşmiş Milletler'de değil, aynı zamanda AB, Avrupa Konseyi, NATO, G8, AGİT ve diğer çokuluslu örgütlerde işbirliği de dâhildir. Amaç, uluslararası toplumun siber alanı korumak için tutarlılık ve yeteneklerini sağlamaktır. Alınacak stratejik hedefler ve önlemler olarak;

Kritik bilgi ve altyapıların korunması,
Almanya'da güvenli Bilgi ve İletişim Teknolojileri sistemlerinin oluşturulması,
Kamu yönetiminde Bilgi ve İletişim Teknolojileri sistemlerinin güçlendirilmesi,
Ulusal siber güvenlik konseyi ve yanıt merkezinin kurulması,
Siber alanda da etkili suç kontrolünün yapılması,
Avrupa'da ve dünyada siber güvenliği sağlamak için etkin ve uyumlu bir eylem koordine edilmesi,
Güvenli ve güvenilir bilgi teknolojisinin kullanılması,
Siber saldırılara tepki veren araçların yapılması gerekmektedir (German NCSS, 2011: 3-8).

2016 yılında hazırlanan Almanya Ulusal Siber Güvenlik Strateji Belgesinde insan haklarına vurgu yapılmaktadır:

Almanya'nın ekonomik ve siyasi ağırlığı, insan haklarını, özgürlüğü, demokrasiyi, hukukun üstünlüğünü ve uluslararası hukuku savunmak için Avrupalı ve transatlantik

ortaklarımızla birlikte işbirliği içinde olmasını gerektirmektedir. Dahası Avrupa güvenliğiyle ilgili sorumluluğu üstlenmek bizim görevimiz anlamına gelmektedir. Paylaşılan değerlerimiz için daha da ayağa kalkmalı güvenlik, barış ve bugüne kadar yaptığımızdan daha fazla kurallara dayalı bir düzen üzerine büyük bir bağlılık göstermeliyiz. (German, 2016: 6).

Alman anayasasının başlangıcında Almanya, "birleşik bir Avrupa'da eşit bir ortak olarak dünya barışını destekleme*"* kararlılığını belirtmektedir. Birleşmiş bir Avrupa temelinde, Almanya'nın arzusu aynı zamanda insanların birlikte yaşamasının koşullarını sürdürülebilir bir şekilde iyileştirmek ve uluslararası insan hakları normlarını korumak ve güçlendirmektir (German, 2016: 22). Alman hükümetinin amacı, vatandaşları için özgürlük, güvenlik ve refah sağlamak, barışı geliştirmek ve hukukun üstünlüğünü güçlendirmek olarak ifade edilmiştir. Alman güvenlik politikası değerlerine bağlıdır ve çıkarları tarafından yönlendirilmektedir. Ulusal çıkarları için yol gösterici ilkeler, özellikle insan onuru ve diğer temel haklar (Avrupa Hukuku ve Uluslararası Hukuk, özellikle Evrensel İnsan Haklarının Korunması ve Barışın Sağlanması), demokrasi ve hukukun üstünlüğü gibi anayasanın değerlerini vurgulamaktadır (German, 2016: 34).

Hollanda Siber Güvenlik Stratejisinde İnsan Hakları

Hollanda, güvenli ve güvenilir Bilgi ve İletişim Teknolojisini (BİT-ICT1) ve açık, özgür bir internetin korunmasını desteklediğini ifade etmektedir. Toplumun BİT'e büyümekte olan bağımlılığı, giderek BİT'in kötüye kullanımını ve bozulmasını sağlayarak savunmasız kılmaktadır. Bu nedenle, Hükümet geniş bir yelpazeye yayılmış kamu ve özel kurumlardan, bilgi kurumlarından ve sivil toplum kuruluşlarından gelen girdi ile bir Ulusal Siber Güvenlik Strateji Belgesi hazırladı. 2011'de yayımlanan NCSS1'in amacı, kamu-özel ortaklıklarına dayalı bir entegre siber güvenlik yaklaşımı ile güvenli, güvenilir ve esnek dijital alan yaratmak ve ardından toplum için fırsatları en iyi şekilde değerlendirmek olarak belirtilmiştir.

Haziran 2011'de yayımlanan Strateji, iki kısma ayrılmıştır. Birinci bölümde, sorunun analizi sunulmakta, siber güvenlik için politika ilkeleri anlatılmakta ve hedefler belirlenmektedir. İkinci kısım, her biri hükümet tarafından uygulanacak olan siber güvenliği artırmak için öncelikli hedefler içeren ve diğer taraflarla işbirliği içinde olmak üzere birçok eylem dizisi belirtmektedir. Hollanda Strateji Belgesi ve Eylem Planı'nda BİT, vatandaşları ve ekonomileri

için büyük önem teşkil etmektedir. Siber Güvenlik'te amaç, BİT'nin bozulması, kesilmesi veya yanlış kullanımı yüzünden tehlike veya hasardan kaçınmaktır. Karışıklık, bozulma veya yanlış kullanımdan kaynaklanan tehlike veya zarar, BİT'in varlığı veya güvenilirliği üzerindeki sınırlamalardan, BİT'te saklanan bilgilerin gizliliğinin ihlalinden veya bu bilgilerin bütünlüğünden kaynaklanıyor olabilir (Kaska, 2015: 6-7).

> *Güvenli ve güvenilir BİT, refahımız için vazgeçilmezdir ve daha sürdürülebilir ekonomik büyüme için bir katalizör görevi görmektedir. Avrupa'da verimlilik artışının% 50'si BİT'in kullanımından kaynaklanmaktadır. Hollanda, dijital toplumun" güvenliğini garanti ederken dünyayı BİT kullanımında liderlik etmeyi amaçlıyor. Hollanda, Avrupa Dijital Ağ Geçidi olmak istiyor.* (Netherlands, 2011: 3-4).

Dijital ortamdaki mevcut tarafların ulusal ve uluslararası düzeyde işbirliği yapması gerektiği vurgulanmaktadır. Siber çatışmalar ortaya çıktığında, yalnız, bir örgüt, bir devlet veya üçünün bir kombinasyonu olabilecek faili tanımlamak genellikle zordur. Siber tehdidin doğası da genellikle net değildir. Ancak birçok siber saldırı aynı teknik ve yöntemleri içermektedir. Belirli tehdit türleri üzerinde çalışan kamu kurumları, ağ ve bilgi altyapısını koruyan işletmeler ve bilgi kurumları da dâhil olmak üzere siber güvenlikle ilgili taraflar arasındaki daha fazla işbirliğinin önemini göstermektedir. Siber saldırılar ve aksamalar ulusal sınırları, kültürleri ve hukuk sistemlerini anında aşmaktadır. Genellikle veri iletiminde hangi hukuk yetkisi uygulanacağı belirsizdir ve yasanın her zaman etkin bir şekilde uygulanıp uygulanamayacağı genellikle belirsizdir.

Strateji belgesi sivil ve askeri kurumlar, kamu ve özel kurumlar ile ulusal ve uluslararası taraflar arasındaki tüm güvenlik sistemi boyunca işbirliğine öncelik verilmesini amaçlamaktadır. Ancak o zaman, BİT altyapısının kritik sektörlerdeki dayanıklılığını, siber saldırılara hızlı ve etkili bir tepki ve dijital alanlardaki yasal korumayı sağlayabileceğini belirtmektedir. Siber güvenlik alanında çok şey yaşanmaktadır. Ancak tutarlılık birçok alanda eksiktir. Bu gözlem, Siber Suç ve Dijital Güvenlik Eğilimlerine Dair 2010 Ulusal Raporu ve Ulusal Güvenlik Think Tank'in Bilişim Teknolojileri Güvenlik Açığı ve Ulusal Güvenlik hakkındaki raporunun bulgularıyla ortaya çıkmıştır (Netherlands, 2011: 5).

Hükümet mümkün olan yerlerde mevcut girişimleri inşa edecek ve gerekirse yenilerini geliştirecektir. Tüm kullanıcılar (bireyler, işletmeler, kurumlar ve kamu kurumları), kendi BİT

sistemleri ve ağlarını güvence altına almak ve diğerlerine karşı güvenlik risklerini ortadan kaldırmak için uygun önlemleri almalıdır. Hassas bilgileri depolarken ve paylaşırken dikkat etmeli ve diğer kullanıcıların bilgi ve sistemlerine saygı göstermeleri gerekmektedir. Bakanlıklar arasındaki sorumlulukların bölünmesi Güvenlik ve Adalet Bakanı, ulusal güvenlik stratejisi uyarınca, siber güvenlikle ilgili tutarlılık ve işbirliğinden sorumludur. Aynı zamanda, siber güvenlik sistemindeki her partinin kendi görev ve sorumlulukları vardır. Tehditlerin sınır ötesi doğası, uluslararası işbirliğini teşvik etmeyi gerekli kılmaktadır. Uluslararası düzeyde bir oyun alanı hedeflemeliyiz. Birçok önlem, ancak uluslararası kabul veya koordine edilmesi durumunda etkili olabilir. Hollanda, AB'nin Avrupa için Dijital Gündemi ve İç Güvenlik Stratejisi, NATO'nun yeni stratejik vizyonu olan İnternet Yönetim Forumu ve diğer ortaklıkların bir parçası olarak siber savunma politikasının geliştirilmesi gibi çabaları desteklemekte ve aktif olarak katkıda bulunmaktadır. Hollanda, Avrupa Konseyi Siber Suçlar Konvansiyonunun yaygın olarak onaylanmasını ve uygulanmasını savunmaktadır (Netherlands, 2011: 11).

2011 Strateji Belgesinde önlemlerin orantılı olmasını, insan haklarına saygılı olmasını ve paydaşlar arası işbirliğinin gerekliliğini vurgulanmaktadır:

> *%100 güvenlik diye bir şey yok. Siber güvenlik faaliyetlerinde Hollanda, risk değerlendirmesine dayalı seçimler yapar. Bunu yaparken, gizlilik, başkalarına saygı, ifade özgürlüğü, bilgi toplama ve temel haklar gibi toplumumuzun başlıca değerlerini korumayı amaçlıyoruz. Hâlâ kamu ve ulusal güvenliğe olan arzumuz ile temel hakların korunması arasındaki dengeye ihtiyacımız var. Önlemlerin orantılı olması gerekir. Bu amaçla, mevcut denetleme araçları da dâhil olmak üzere gerekli yerlerde güçlendirilmesi, korunması ve test mekanizmalarının oluşturulması yoluna başvuracağız. Gerektiğinde mevzuat kamu ve özel sektör, öncelikle kendi kendini düzenleme yoluyla aradıkları BİT güvenliğini sağlayacaktır. Özdenetim çalışmazsa, Hükümet mevzuatın kapsamını inceleyecektir. Ancak mevzuat üç şartı karşılamalıdır: rekabeti gereğinden fazla bozmamalı ve mümkün olduğunca düzgün bir oyun alanı sağlamalıdır; idari yük, orantısız bir şekilde arttırılmamalıdır ve maliyetler yararları ile makul orantılı olmalıdır. Hızlı hareket eden bir dünyada yaşıyoruz ve mevzuat kısa sürede eskimiş hale gelebilir. Hükümet, mevzuatın BİT'teki gelişmelere göre ayarlanması gerekip gerekmediğini değerlendirecektir.* (Netherlands, 2011: 12-15).

Güvenlik, özgürlük ve sosyal ekonomik faydalar arasında korelasyon, hem ulusal hem de uluslararası tüm paydaşlar arasında sürekli olarak açık ve pragmatik bir diyalog içinde gerçekleştirilmesi amaçlanan dinamik bir dengedir. Kişisel bilgilerin işlenmesi ve gizliliğin korunması, kısmen Avrupa mevzuatına dayanan katı standartlara ve denetime tabidir (Netherlands NCSS2, 2014: 7-8). Temel hak ve değerleri korumak birçok tarafın çaba sarf etmesini ve tercihen ulusal ve uluslararası bağlamda yer almasını gerektirmektedir. Önerilen yaklaşım uluslararası standartların geliştirilmesini bağlı kılmaktadır. Hükümetlerin yanı sıra, özel sektör kurumları ve sosyal organizasyonlar tarafından önemli bir rol oynanabilir. Hollanda, Birleşmiş Milletler'de, Londra, Budapeşte ve Seul'de düzenlenenler gibi uluslararası siber konferanslar sırasında, İnternet Yönetim Forumu gibi diğer çoklu paydaş ortamlarında, Dünya Ekonomik Forumu tarafından yayınlanan siber güvenlik ilkelerini teşvik etmektedir. Ayrıca güven inşası geliştirmek için Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT) gibi devletlerarasındaki önlemleri uluslararası düzeyde desteklemektedir (Netherlands NCSS2, 2014: 18).

Ulusal Siber Güvenlik Strateji Belgesi'nde İnsan Hakları Nasıl Düzenlenmelidir?

Ulusal güvenlik stratejilerinin (NSS) formülasyonu oldukça yeni bir olgudur. 1990'ların sonlarına veya 2000'lerin başına kadar ulusal güvenlik stratejisine sahip ülkelerin çoğunluğu ilk güvenlik stratejilerini değerlendirmeye almış ve takip etmişlerdir (Klimburg, 2012: 45). Siber güvenlik, ulus-devletler tarafından farklı anlamlarda kullanılmaktadır. Küresel çapta BM tarafından bu konuda kabul edilen bir anlaşma olmadığı için, dünya üzerinde uzlaşılan ve kabul edilen yegâne bir tanımı da yoktur. Her ülke kendi ulusal siber güvenlik strateji belgesini yayınlamış ve siber güvenlik kavramına farklı tanımlar yapmıştır. Dolayısıyla siber güvenlik alanındaki tanımlar farklı ülkelerce yapılsa da benzer noktaları olmuştur. Ancak tanımların bir kısmı benzer olsa bile çeşitli tanımlar yapıldığı için bu durum ulus-devletleri farklı önlemler almaya itmiştir. Her ülke kendi tanımını yapmakta ve yaptığı tanımı doğru kabul etmektedir. Bu doğrultuda dikkatlerden kaçan en önemli nokta, ulusal strateji belgelerinde sorulması gereken "kimin için, ne için ve nasıl bir siber güvenlik" sorularıdır. Ancak ulusal strateji belgelerinde bu soruların yanıtlarını bulmak oldukça güç olmuştur (Akyeşilmen, 2016).

Genel olarak, ulusal bir strateji farklı hedeflere sahip olabilir: Bunlar, (1) Bütün hükümet kurumlarını aynı bakış açısına sahip kılmak, (2) Kamu ve özel planlamayı tutarlı bir şekilde odaklamak, koordine etmek ve tüm paydaşlar arasında öngörülen rolleri, sorumlulukları ve

ilişkileri ilerletmek, (3) Bir kişinin ulusal niyetini diğer uluslara ve paydaşlara iletmek (Klimburg, 2012:60).

Franklin ve diğerlerine göre, insan hakları ve internet ilkeleri yönetmeliğinde yaşam, özgürlük ve güvenlik hakları çevrimiçi olarak saygı görmeli, korunmalı ve yerine getirilmelidir. Bu haklar çevrimiçi ortamda ihlal edilmemeli veya diğer haklarını ihlal etmemelidir (Franklin, Bolde ve Hawtin, 2014: 7). Erişim hakkında, herkesin yararlanması için internet sağlanmalı ve yasalarca sağlananlar dışında herhangi bir kısıtlamaya tabi olunmamalıdır.

Demokratik bir toplumda ulusal güvenlik, kamu düzeni, halk sağlığını veya ahlakını veya başkalarının haklarını ve özgürlüklerini korumak için bu haktan yararlanma hakkı mevcut sözleşmede tanınan diğer haklarla uyumlu olmalıdır. UDHR'nin 3. maddesinde belirtildiği üzere: *"*Herkesin yaşama hakkı, kişilik özgürlüğü ve güvenliği hakkı vardır". Tüm güvenlik önlemleri uluslararası insan hakları hukuku ve standartlarıyla uyumlu bir biçimde olmalıdır. Bu, güvenlik önlemlerinin istisnai koşullar haricinde başka bir insan haklarını (örneğin gizlilik hakkı veya ifade özgürlüğü hakkı) kısıtladıkları durumlarda yasadışı olacağı anlamına gelmektedir. Tüm kısıtlamaların kesin ve dar bir şekilde tanımlanmış olması gerekmektedir. Tüm kısıtlamalar, Uluslararası Hukuk uyarınca yasal olarak kabul edilen ve bu ihtiyaçla orantılı olarak gerçek bir ihtiyacın karşılanması için gereken asgari düzeyde olması önem teşkil etmektedir. Sınırlamalar, her hakka özgü ek ölçütleri de karşılamalıdır. Bu katı sınırların dışındaki sınırlamalar yasaktır. Herkes, internette güvenli bağlantıların keyfini sürme hakkına sahiptir. Buna virüsler, kötü amaçlı yazılımlar ve kimlik avı gibi İnternet'in teknik işlevini tehdit eden hizmetlerden ve protokollerden korunma da dâhildir (Franklin, Bodle, Hawtin, 2014: 13-15). BM Sivil ve Siyasi Haklar Anlaşmasında ortaya konduğu gibi, ifade özgürlüğü hakkı belirli kısıtlamalara tabi olabilir, ancak bunlar yalnızca kanunlar tarafından sağlanan ve başkalarının haklarına veya itibarlarına saygı duyulması için ulusal güvenliği, kamu düzeni, kamu sağlığı, ahlakın korunması için gereklidir (Franklin, Bodle, Hawtin, 2014: 16).

Ulusal strateji belgelerinde yapılan siber güvenlik tanımlarında bilgi, bilişim ve ağların güvenliğinden bahsedilmektedir. Oysa siber alanın en önemli bileşeni kullanıcı olmaktadır. Ancak stratejilerde yapılan tanımlamalarda kullanıcı genel olarak göz ardı edilmektedir. Bilgi ve İletişim Teknolojisinde sürekli olarak kullanıcı yani insan en önemli bileşen olarak vurgulanmasına karşın, güvenlik tartışmalarında bu unsur göz ardı edilmeye devam etmektedir. Bundan dolayı kimin için güvenlik ya da ne için güvenlik sorusu büyük önem arz etmektedir.

Siber uzayın paydaşları kişiler, şirketler ve devletlerdir. Bütün paydaşların istek ve taleplerinin dikkate alındığı böyle bir strateji ile ancak siber güvenlik sağlanabilir.

Günümüzde Bilgi ve İletişim Teknolojisi'nde yaşanan hızlı gelişmeler yeni fırsatlar sunarken bir yandan da tehditlere karşı savunmasız kılmaktadır. Hukuki açıdan yaşanan bazı boşlukları da ortaya çıkarmaktadır. Yasal boşlukların bulunması, yasalardaki yetersizlikler yani bir ülkede tehdit ve suç unsuru sayılabilen bir fiilin, bir başka ülkede tehdit veya suç unsuru sayılmaması ve söz konusu fiile ilişkin herhangi bir mevzuatın bulunmaması siber saldırganlar için o ülkede güvenli sığınaklar oluşturmaktadır. Dünyada internet kullanımı arttıkça mağdurları ve suçluları tespit etmek zorlaşmakta, delil toplama gibi temel soruşturma aşamaları değişmese de bu aşamalarda kullanılan usule ilişkin mevzuatın yetersizliğini ortaya çıkarmaktadır. Siber saldırıları nasıl önlemek gerektiğine ve delillerin nasıl toplanıp değerlendirileceğine karar verilebilmesi için ülkeler arasında izlenecek bir işbirliği ile usule ilişkin mevzuata ihtiyaç duyulmaktadır (Ünver, Canbay ve Mirzaoğlu, 2009: 27). Sanal dünyanın sınır tanımayan küresel yapısı gereği, siber ortamda yargılama yetkileri, insan hakları, uluslararası hukuk, yaşama ve kişilik özgürlüğü gibi hukuki kavramların belirsizliğini beraberinde getirmiştir. Oysa gerçek dünyada, her ülkenin yargılama yetkisi dâhilinde olan bölge coğrafi sınırlarla belirlenmiş ve uluslararası işbirliği içerisinde uygulanan çoğu hukuki yetkileri de belirlemiştir. Sanal dünyada suçu oluşturan eylemleri hangi adli makamın soruşturacağı ve cezalandıracağı hususunda belirsizlik ve karmaşa halen yaşanmaktadır (Ünver, Canbay ve Mirzaoğlu, 2009: 28).

Ulusal siber güvenlik strateji belgesinin yasal boyutunda yaşanan güçlüklerin azaltılması, soruşturma ve kovuşturmanın etkin rol üstlenebilmesi için yapılması gereken çalışmalarda tedbirlerin alınması gerekir. Bundan dolayı; Yasal boşluklar giderilmelidir. Usule ilişkin yasal eksiklikler ortadan kaldırılmalıdır. Siber ortamda koruma ve gözetme yetkileri belirlenmelidir. Sanal dünyada bireyin haklarını sınırlayan her türlü fiile ilişkin, ulus-devletler arasında insan hakları kavramı üzerine değinilmesi ve ortak bir mevzuatın çıkarılmasını gerekli kılmaktadır. Ülkeler arasında siber suça iştirak eden saldırganların iadesine ilişkin uzlaşma usulleri belirlenmelidir. Siber alanda yargılama yetkileri belirlenmelidir (Ünver, Canbay ve Mirzaoğlu, 2009: 30).

Sonuç

Siber uzayın mevcudiyeti ve siber ortamdaki verilerin bütünlüğü, gizliliği ve erişilebilirliği 21. yüzyılın can alıcı soruları haline gelmiştir. Siber güvenliğin sağlanması hem ulusal hem de uluslararası düzeyde devlet, iş dünyası ve toplum için önemli bir hal almıştır. Siber Güvenlik Stratejisi, bu alandaki çerçeve koşullarını iyileştirmek için hazırlanan bir belge olmuştur. Günümüze kadar oluşan gelişmeler de sınırlarının nerede başlayıp nerede bittiğini bilemediğimiz siber alanın getirdiği faydaların günbegün artması ile beraber, güvenlik açısından sorunların sayısı da artmıştır.

Siber alanın gelişen ortamı henüz uluslararası sistem ve hukukun bütünüyle kapsayabildiği bir alan değildir. Birçok ülkeler "ulusal" siber stratejiler oluşturmaya çalışmaktadırlar. Ülkelerin kendine yönelik bir saldırı olduğunda interneti kapatma çabaları, kapalı internet oluşturma gayretleri sınırların belirlenememesinde olumsuz bir durum yaşatmaktadır. Aktörlerin belirsiz olması ve siber alanın hızı ulus-devletleri internet karşısında güçsüz bırakmaktadır. Siber tehditlerin niteliğini anlamak, alınacak önlemlerin tutarlılığını artıracaktır.

Ulus-devletler siber alanın büyük önem taşıdığının daha yeni farkına varmış ve bunun için siber alanı ulusal güvenlik stratejilerine eklemişlerdir. Sınırları belli olmayan bir alan için ulusal strateji belgesi ve eylem planı belirlemek tek başına yeterli olmamaktadır. Dolayısıyla orantılı güç kullanımı olmalı ve ülkelerin işbirliği içerisinde siber alanda ortak bir yargılama yetkisi belirlenmelidir.

Devlet merkezli uluslararası sistemin siber düzeyde çok az uygulanabilir olduğu söylenebilir. Bu nedenle, ulus-devletlerde, bireylerde ve özel şirketlerde de bağlayıcı nitelikte uluslararası bir düzen ve uluslararası hukuka ihtiyaç duyulmaktadır. Siber aktörler üzerinde bağlayıcı yasal düzenlemeler yapmak da, bu yeni alanda insan haklarının geliştirilmesi ve korunması için yeterli değildir. Ancak küresel düzeyde de uygulanmasını gerekli kılmaktadır. Dolayısıyla, anarşik uluslararası düzenin ötesine geçen küresel bir uygulama organına ihtiyaç duyulmaktadır. Ama nasıl olması gerekir? Daha da önemlisi, yeni toplumsal sözleşme ne olmalıdır? Bu sorunun cevabı muhtemelen insan haklarının ve siber güvenliğin geleceğini belirleyecektir.

Siber dünyada devletlerin, kurumların, bireyin güvenliği ve özgürlüğü sağlanmadan, ulusal güvenlik muhtemel değildir. Siber alanda interneti tamamen kapatmak bir güvenlik önlemi değildir. Siberi güvenlikte erişilebilirlik, bütünlük ve gizlilik amaç olmalıdır. Erişimin

kesilmesi, siber güvenliğin mümkün olmaması, insan hak ve özgürlüklerin kısıtlanması anlamına gelmektedir. İnsan hak ve özgürlüklerinin korunmasını temel dayanak noktası almayan hiçbir siber güvenlik önlemi, gerçek anlamda bir güvenlik sağlayamamaktadır.

Bilgi ve İletişim Teknolojisi'nin getirdiği özgürlük ortamının genişlemesi ulus-devletlerin olayların kontrolden çıkabileceği bir medyanın var olduğu hissiyatını vermektedir. Bu durumda ulus-devletler internet üzerinden bireysel hak ve özgürlükleri ihlal edecek şekilde insanları izlemeye başlamışlardır. Fakat bunu fark eden bireylerin (*hacker*lar gibi) önderliğinde muhalefet grupları da oluşmaya başlamaktadır. Ulus-devletlerin kontrolü arttıkça buna karşı oluşan saldırganların sayısı da artmaktadır. Ortaya çıkan çatışma ise siber güvensizliği arttırmakta ve siber çatışma ihtimalini sık sık gündeme getirmektedir.

Günümüzde siber tehdidin belirsizliği veya imkânsızlığı haline bakılmaksızın genişleyen siber güvensizlik alanı ve onun ekonomisi, varlıklarını anlamlandırmak için çatışmayı teşvik eder hale gelmeye başlayabilir. Böyle bir sürece engel olmak siber güvenlik ve uluslararası hukuk için atılacak en büyük adım çatışmayı önlemek olacaktır. Günümüz güvenlik algılarının ve insan hak ve özgürlüklere uygunluğu açısından bu denli değişimlere ihtiyacı vardır. Ulus-devletlerin siber alanın oluşturduğu sanal gerçekliği detaylı incelemesi ve buna uyumlu strateji belgeleri oluşturmaları zorunlu kılmaktadır. Bu süreç tam anlamıyla gerçekleşinceye kadar siber güvenliğin sağlanması ve insan haklarının korunması kolay olmamaktadır. İnsan haklarının siber alanda açık bir şekilde güvenliğe ilişkin zafiyeti bulunmaktadır. Uluslararası hukuk kurallarının siber güvenliğin sağlanmasında yaptırımı olabilir mi? veya ulus-devletler kendi güvenliklerini uluslararası hukuk sayesinde sağlayabilirler mi? insan hakları kavramında aklımıza gelen başlıca sorulardır. Güvenliğin sağlanabilmesi için bütün aktörlerin karar alma mekanizmalarında olması gerekir. Siber güvenlik ve iyi korunan insan haklarına sahip olmak için yeni bir (sosyal) sözleşmeye ihtiyaç duyulabilir.

KAYNAKÇA

Akyeşilmen, Nezir. (2016). *Siber Güvenlik ve Özgürlük.*http://www.ilksesgazetesi.com/yazar/siber-guvenlik-ve-ozgurluk-3816.html [Erişim Tarihi: 13.12.2017].

Akyeşilmen, Nezir. (2016). *Cybersecurity And Human Rights: Need For A Paradigm Shift.? Cyberpolitik Journal*, Siber Politikalar Dergisi, Volume1, Number 1&2 Winter 2016, ss.38-61.

Alagöz Akçadağ, Emine. (15 Şubat 2015).Amerika'nın Yeni Güvenlik Stratejisi. http://www.bilgesam.org/incele/2032/-amerika-nin-yeni-guvenlik-stratejisi/#.WjP97VVl-00 [Erişim Tarihi: 14.12.2017].

Aytar, Ahmet K. (2015). ABD Ulusal Güvenlik Strateji Belgesi ve Türkiye. http://www.turkishnews.com/tr/content/2015/02/16/abd-ulusal-guvenlik-strateji-belgesi-ve-turkiye/ [Erişim Tarihi: 15.12.2017].

Bayraktar, Gökhan. (2015). *Siber Savaş ve Ulusal Güvenlik Stratejisi*, İstanbul: Yeniyüzyıl Yayınevi.

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

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

Bozdemir, Nazlı. (21 Temmuz 2013). Türkiye ve Siber Güvenlik Tehditlerin Farkında mıyız?. http://akademikperspektif.com/2013/07/21/turkiye-ve-siber-guvenlik-tehditlerin-farkinda-miyiz-3/[Erişim Tarihi: 14.12.2017].

Craigen, Dan, Diakun-Thibault, Nadia, Purse, Randy. Defining Cybersecurity, https://timreview.ca/article/835 [Erişim Tarihi: 14.12.2017].

Cyber Security Strategy Documents. https://ccdcoe.org/cyber-security-strategy-documents.html [Erişim Tarihi: 14.12.2017].

Dağı, İhsan D. (2010). Normatif Yaklaşımlar: Adalet, Eşitlik ve İnsan Hakları. *Devlet, Sistem ve Kimlik, Uluslararası İlişkilerde Temel Yaklaşımlar*. (12. Baskı).İstanbul: İletişim Yayınları, s.185-227.

Dünya. (17 Temmuz 2012) .Siber Güvenlik Stratejisi Hazır. https://www.dunya.com/gundem/siber-guvenlik-stratejisi-hazir-haberi-179657 [Erişim Tarihi: 12.12.2017].

Franklin, Marianne, Bodle, Robert, Dixie, Hawtin. (August 2014).*The Charter Of Human Rights And Principles For The Internet*, United Nations, 4th Edition
http://www.ohchr.org/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf [Erişim Tarihi: 20.12.2017].

Geers, Kenneth. (2011). Strategic Cyber Security.*NATO Cooperative Cyber Defence Centre Of Excellence Talinn, Estonia: CCD COE Publication*.

German. (01.01.2011) .National Cyber Security Strategy. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy-for-germany/view [Erişim Tarihi: 28.12.2017].

German. (2016). *National security and defence strategies*. On German Security Policy And The Future Of The Bundeswehr, The Federal Government, White Paper.

National Cyber Security Centre. https://www.ncsc.gov.uk/articles/academic-centres-excellence-cyber-security-research [Erişim Tarihi: 14.12.2017].

İngiltere. (2010) .A Strong Britain In An Age Of Uncertainty: The National Security Strategy. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf [Erişim Tarihi: 17.12.2017].

İngiltere. (2011) .*The UK Cyber Security Strategy*.http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf [Erişim Tarihi: 13.12.2017].

İngiltere. (2016). *UK National Cyber Security Strategy*.https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf [Erişim Tarihi: 13.12.2017].

Kaska, Kadri. (2015)Netherlands, *National Cyber Security Organization*.https://ccdcoe.org/ites/efault/files/multimedia/pdf/CS_organisation_NETHERLANDS_032015_0.pdf [Erişim Tarihi: 14.12.2017].

Klimburg, Alexander (Edited By). (2012) *National Cybersecurity Framework Manual, NATO* https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf [Erişim Tarihi:17.12.2017].

Netherlands. (2011-2013) *The Netherlands Cyber Security Strategy*. https://english.nctv.nl/inaries/cyber-security-strategy-uk_tcm32-83648.pdf [Erişim Tarihi: 15.12.2017].

Netherlands. (2014-2016) .*The Netherlands Cyber Security Strategy 2*.https://www.enisa.uropa.uopics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf [Erişim Tarihi: 14.12.2017].

Sarı, Arif. *Gelişmiş Ülkelerde Ulusal Siber Güvenlik Duvarı Projeleri* http://www.cezerisga.com/makale/Gelişmiş%20Ülkelerde%20Ulusal%20Siber%20Güvenlik%20Duvarı%20Projeleri [Erişim Tarihi: 15.12.2017].

Strat, Acos (Edited By), CHOD (Approved By). (2014).Belgium. *Cybersecurity Strategy For Defence*https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf [Erişim Tarihi: 17.12.2017].

Thomas, T. L. (2003).Al Qaeda and the Internet: The Danger of Cyberplanning. *Parameters*, Cilt 33 (1), ss.114-122.

Türkiye. (2016-2019.).lusal Siber Güvenlik Strateji Belgesi. http://www.udhb.gov.tr/oc/siberg/2016-2019guvenlik.pdf [Erişim Tarihi: 12.12.2017].

TÜBİTAK ve BTK. (2011).*I. Ulusal Siber Güvenlik Tatbikatı Sonuç Raporu* http://www.uekae.tubitak.gov.tr/uekae_content_files/siber_tatbikat_raporları/USGT_2011_tr.pdf [Erişim Tarihi: 15.12.2017].

Türkiye. (Haziran 2012). *Ulusal Siber Güvenlik Stratejisi.* http://www.bilgiguvenligi.org.tr/wp-content/uploads/2016/03/Ulusal_Siber_Guvenlik_Stratejisi.pdf [Erişim Tarihi: 15.12.2017].

Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi. (2012).Yönetilmesi ve Koordinasyonuna İlişkin Karar.http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf [Erişim Tarihi: 15.12.2017].

USA. (2009). *Cyberspace Police Review*. https://www.dhs.gov/sites/default/iles/publications/Cyberspace_Policy_Review_final_0.pdf [Erişim Tarihi: 17.12.2017].

USA. (April 2015).The DoD Cyber Strategy The Department of Defense https://www.defense.ov/ortals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_YBER_STRATEGY_for_web.pdf [Erişim Tarihi: 17.12.2017].

USA. (December 2017).*ational Security Strategy Of The United States Of America* https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf [Erişim Tarihi: 28.12.2017].

Ünver, M., Canbay, C., Mirzaoğlu, A.G. (2009).*Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler*. Bilgi Teknolojileri Üst Kurulu http://www.cybersecurity.gov.tr/publications/sg.pdf [Erişim Tarihi: 14.12.2017].

Ünver, M., Canbay, C., Özkan, H.B. (Mayıs 2010).ritik Altyapıların Korunması, Bilgi Teknolojileri Koordinasyon Dairesi Başkanlığı. https://www.btk.gov.tr/File/?path=OOT%2F1%2FDocuments%2FSayfalar%2FSiberGuvenlik%2FCIP_Rapor.pdf [Erişim Tarihi: 14.12.2017].

Yüksel, Mahir.(2017).k Siber Güvenlik Eylem Planı. http://www.yenisoz.com.tr/3-yillik-siber-guvenlik-eylem-plani-makale-15972 [Erişim Tarihi: 15.12.2017].

KRİPTO PARA: BİTCOİN VE ULUSLARARASI İLİŞKİLER

Müberra ALTINER[*]

Özet

Küreselleşen dünyada 1960'lı yıllarda teknik ve teknolojik alanda yaşanan gelişmeler insanoğlunun tarihsel gelişimde önemli bir rol oynayan parayı da etkilemiştir. Siber/dijital dünyada sanal bir para biriminin ortaya çıkması küresel ticarette yeni bir devrim niteliğindedir. Bitcoin, sanal para birimlerinin öncüsü olarak kabul edilmektedir. Bu makalede elektronik para (sanal para, dijital para, kripto para vb.) gibi birçok adlandırmaya sahip olan para birimlerinden bahsedilecek, ilklerden olan Bitcoin analiz edilecek olup, uluslararası ilişkilerde hayat sahası bulan devletler üzerindeki yansımaları karşılaştırmalı olarak ele alınacaktır. Bu çalışmada

[*] Master Öğrencisi, Selçuk Üniversitesi, İİBF-Uluslar arası İlişkiler Bölümü, E-mail: muberra.altiner@gmail.com

Bitcoin hakkında literatür taraması yapılmış olup, güncel kaynaklardan elde edilen nicel veriler ile makale desteklenmeye çalışılmıştır. Ayrıca belli başlı devletler bu makale de seçilerek, Bitcoin hakkındaki düzenlemeleri karşılaştırmalı olarak ortaya konulmaya çalışılmıştır.
Anahtar Kelimeler: Kripto Para, Sanal Para, Bitcoin, Uluslararası İlişkiler

Crypto Money: Bitcoin and International Relations

Abstract

In the globalizing world, developments in the 1960s, technically and technologically, have also affected the 'money' issue, which plays an important role in the historical evolution of human beings. The emergence of a virtual currency in the cyber / digital world is a new revolution. Bitcoin is regarded as the pioneer of virtual currencies. In this article, we will analyze currencies which have many nomenclature such as electronic money (virtual money, digital money, crypto money, etc.), discuss Bitcoin which is the first siber money and will compare the policies of some regarding Bitcon. In this article, literature review is done and it is also being supported by quantitative data obtained from current sources.
Keywords: Crypto Money, Virtual Money, Bitcoin, International Relations

Giriş

Son yıllarda yaşanan teknik ve teknolojik gelişmeler ile internet kullanımının yaygınlaşması dünya üzerindeki ekonomik faaliyetleri ve ticareti de etkilemiştir. Son dönemde yaygınlaşan internet kullanımı e-ticaret denilen uygulamaları da beraberinde getirmiştir. İnternet üzerinden yapılan ticari uygulamalar geniş bir ekonomik hacme ulaşmıştır(Tüm dünyada 10 trilyon dolar düzeyinde olduğu varsayılmaktadır). E-Ticaret uygulamaların ciddi boyutlara ulaşması kendi içerisinde sanal para birimlerinin oluşmasına ve bu para biriminin yaygınlaşarak alışveriş ve hesap birimi olarak kullanılmasını sağlamıştır. Bu uygulamaların yaygınlaşması, ülkelerin sahip olduğu merkez bankalarının ve otorite mahiyetindeki kuruluşların da bu alana dikkatini çekmiştir.

Sanal bir para birimi Avrupa Merkez Bankası tarafından 2012 yılında yayınlanan raporda; belli bir topluluk arasında topluluğun üyeleri tarafından kabul gören düzensiz dijital para türü olarak tanımlanırken, bu para birimleri de üç tipe ayrılmıştır. Bu para birimleri reel ekonomi de gerçek

para ile etkileşime bağlıdır. Tip-1 türünde ki sanal paralar çevrimiçi oyunlarda vs. kullanılanlar; Tip-2 satın alma işlevine sahip genelde tek yönlü olarak mal ve hizmeti satın alabilen paralar iken, Tip-3 olarak bahsedilen sanal paralar ise, çift yönlü akışa sahip olan, mal ve hizmet satın alabildiğiniz, iki döviz kuru ile birbirine dönüştürebilen paralardır. Bu paraların fiziksel bir karşılığı yoktur. Fiziksel olarak varlığı olmayan bu paraların elektronik para uygulamalarından ayrılmaktadır. Fiziksel varlığa sahip olmaması bu paraların üzerinde kontrol mekanizmalarını etkisiz bırakmaktadır. Bu paraların piyasadaki varlığı, kullanımı üzerinde kontrol mekanizmalarının kalkması, bu paraların yönlendirilmesi, kullanımı, ihracı gibi daha birçok faktörün uluslararası piyasaları belirsizliğe itmektedir. Bu belirsizlik küreselleşen dünyamızda olumlu ve olumsuz birçok etkiyi de beraberinde getirmektedir (European Central Bank, 2012: 6).

Tip-3 grubunda yer alan Bitcoin, çift yönlü akışa sahip olan, hem sanal hem de gerçek mal ve hizmetler için kullanılabilen, anonimlik derecesi oldukça yüksek olan, merkezi bir otorite tarafından üretilmeyen ve merkezi bir otoriteye sahip olmayan para gibi birçok özelliğe sahip olan yeni bir sanal para birimidir. Anonimlik seviyesinin oldukça yüksek olması uyuşturucu ve silah ticareti gibi yasadışı işlemleri kolaylaştırmakta, bu da küresel terörizm ve suçların artması tehlikesini beraberinde getirmektedir. Dengesiz bir üretim aralığına sahip olması ekonomik istikrarı tehdit etmektedir. Herhangi bir otorite tarafından denetlenememekte olan bu yeni sanal para birimi, yasal belirsizlikle birlikte devletler için risk taşımakta ve hem ekonomide hem de diğer alanlarda devlet kontrolünün ortadan kalkmasına sebebiyet verebilecek ölçüdedir.

Peki bu kadar karmaşık ve sorun üretme kapasitesine sahip olan Bitcoin nedir, nasıl üretilir ve nasıl işlemektedir?

Bitcoin: Bir Blok Zinciri Teknolojisi Ürünü

Döviz aracı, hesap birimi ve değerlerin kaydedilmesini sağlayan para, son teknolojik gelişmelerle ve özellikle internetin yaygın olarak kullanılmasından etkilenmiş ve yeni formlara doğru bürünmeye başlamıştır. 1990'lı yıllarla birlikte dünya da World Wide Web'in ortaya çıkması ve hızla artan internet kullanımını beraberinde sanal toplulukların ortaya çıkmasına sebebiyet vermiş ve sanal topluluklar arasında bir çeşit ticareti mümkün kılmıştır. Bu alıp verme işlemini sağlayan en temel araç para iken, siber dünyada para yeni bir form kazanmıştır. Bu sanal topluluklar sundukları malları ve hizmetleri değiş tokuş etmek için kendi dijital para

birimlerini yaratmış ve böylece yeni bir dijital para biçimi ortaya çıkmıştır. Bu dijital para formlarından öncü olan ve en bilinen örnek ise Bitcoin'dir.

Bitcoin, (sembolü: ฿, kısaltma: BTC) bir kripto para ve ödemeler sistemidir. Kripto kelimesi kriptolojiden gelmektedir ve öz olarak şifreleme bilimi olarak adlandırılmaktadır. Kriptografi kimlik bilgilerinin gizliliği, verilerin değişmezliğini, kimliğin doğrulanmasını sağlamakta ve böylece sisteme olan güveni artırmaktadır (Ateş, 2016: 352). Bitcoin de kripto paralar arasında yer almaktadır. Bitcoin ilk olarak 2008 yılında Satoshi Nakamoto tarafından dokuz sayfalık bir pdf (Portable Document Format; Taşınabilir Belge Biçimi) dosyasının kapalı bir mail grubuna gönderilmesi ile başladı. Satoshi Nakamoto'nun kim olduğu bugün bile tespit edilememiştir. Kim olduğuna dair farklı ve gizemli iddialar mevcuttur. Bu dosya Japonya üzerinden gönderilmiş olduğu tespit edilse de Satoshi Nakamoto'nun iyi derecede İngilizce konuşması, onun 37 yaşındaki Japon bir erkek olduğu iddialarını zayıflatmaktadır. Bu konu üzerinde tam bir netlik mevcut olmasa da gönderdiği pdf dosyasında Bitcoin'in ne olduğunu anlatmaktadır. İnsanlık tarihinin en önemli icatlarından sayılan parayı yeni bir forma kavuşturan bu belgenin başlığı şudur; Bitcoin: A Peer-to-Peer Electronic Cash System. Başka bir ifade ile Kişiden Kişiye Elektronik Para Sistemi.

Peer-to-Peer kısaca P2P olarak ifade edilen sistem, merkezi olmayan dağıtık bir ağ yapısı yani merkezi olmayan ya da ademi nerkeziyetçi demektir. Para ekonomide aracı kurumlar vasıtası ile (merkez bankaları, ticari bankalar, uluslararası kuruluşlar, finansal organizasyonlar) el değiştirirken P2P sisteminin ortaya çıkması ile bu aracı kurumların varlığı ortadan kalkmaktadır. Bu aracı kurumların kaynağı olan devletlerin, en temel varlık sebeplerinden biri de bu kurumların gereksiz hale gelmesi ile ortadan kalkmaktadır.

Bitcoin, ülkelerde var olan merkezi bir yapının yerine açık kaynak kodlu sistem olarak ifade edilen bir sistem yerini almaktadır. Açık kaynak kodlu yazılım demek; isteyen herkesin kaynağın kodlarını dilediği gibi indirip bunlar üzerinde değişiklik yapmasını sağlamaktadır. Bu yazılımlar herkes tarafından uygulanabilir, uyarlanabilir, sağlam, hızlı ve güvenilir olarak tanımlanırken daha sonra bu kodlar yeniden toplanarak yeni bir formda kullanılabilir hale getirilmektedir. Farkı daha iyi anlamamız için kapalı kaynak kod yazılımları bugün kullandığımız Office XP, Windows XP ya da Adobe Photoshop gibi birçok yazılım kapalı kaynak kodlu yazılımlardır ve siz bunlar üzerinde değişiklik yapamazsınız. Fakat Bitcoin açık kaynak kodlu yazılıma sahiptir ve değişiklik yapılabilmektedir.

Bitcoin'e benzer olarak üretilen ve Altcoin olarak adlandırılan bugün yaklaşık olarak sayısı 1300'lere ulaşan Altcoinler işlem görmektedir. Altcoinlere örnek vermek gerekirse; Ethereum (ETH), Ripple (XRP), Litecoin (LTC), Steem (STEEM), Ethereum Classic (ETC), Dash (DASH), NEM (XEM), MaidSafeCoin (MAID), NXT (NXT), ZCash (ZEC) örnek verilebilir (Gültekin & Bulut, 2014: 84). Bitcoin, bunlar arasında öncü ve bilinirliği çok, güvenilirliği daha fazla olduğu için diğerlerinden sıyrılmaktadır.

Bitcoin ve buna benzer olan Altcoinler bir çeşit blok zinciri olarak tanımlayabileceğimiz Block Chain denilen bir zincir sistemi kullanmaktadırlar. Block Chain diye tanımladığımız şey ise; Bitcoin sisteminde yapılan bütün parasal işlemler, para transferleri, ödemeler, alımlar vb. tüm işlemler block olarak adlandırdığımız bloklara yazılmaktadır. Kısa bir örnekle açıklarsak eğer; X, Y'den herhangi bir alım-satım ya da ödeme işlemi gerçekleştirdiğinde bu işlem anlık olarak bloklara yazılmaktadır. Geleneksel elektronik para saklama ve transfer işleminde aracı kurum söz konusu iken bu yeni sistemle aracı kurum buharlaşmakta her işlemin kaydı, ağ içerisindeki diğer madenciler tarafından kaydı tutulmaktadır. Yazılan her blok birbirlerine zincirlerle bağlanmaktadır. Böylece Block Chain denilen uygulama ortaya çıkmaktadır.

Blok zincir sisteminin sağlamlığı, adem-i merkeziyetçi bir mimariden ve internetin çok-düğümlü yapısının esnekliğine benzeyen tek bir arıza veya kontrol noktasının olmamasından kaynaklanmaktadır (Mainelli & Gunten, 2014: 10). Block Chain sisteminin herkese açık olması bu sistemin güvenilirliğini artıran unsurlar arasında yer almaktadır.

2008 yılından itibaren yapılan her Bitcoin işlemi indirilip görüntülenebilme özelliğine sahiptir. Satoshi Nakamoto, yazdığı makalesinde de bunu vurgulamıştır. E-ticaret uygulamalarında ihtiyaç duyduğumuz şey kanıtlanabilir şifreleme üzerine kurulu, istekli iki tarafın güvenilir bir üçüncü şahsa ihtiyaç duymadan birbirleriyle doğrudan işlem yapmasına izin veren bir elektronik ödeme sistemi olduğunu belirtmiştir (Nakamoto, 2008: 1).

Yapılan işlemlerinin hepsinin kaydının herkes tarafından tutulabiliyor olması, isteyen herkesin kayıtçı olabiliyor olması ve bunların sürekli olarak senkronizasyona tabi tutulması sistemin güvenliğini sağlayan temel unsurlardandır. Yani yapılan işlemler, alıcı ve satıcı dünyanın her bir yanında bulunan bütün sistemlere yazılıyor olması bu sistemi güvenli hale getirmektedir.

Bitcoin üzerinden alım-satım işlemleri gibi işlemler yapabilmek için bir Bitcoin hesabına yani bir nevi dijital bir cüzdana sahip olunması gerekmektedir. Bu hesap üzerinden işlemler gerçekleştirilirken bu hesabın güvenliğini sağlanmak için kriptoloji yani şifreleme işlemleri kullanılmaktadır. Bu şifreleme ile hesabınızın güvenliği en üst seviyeye çıkarılmaktadır. Her hesabın ya da diğer bir deyişle cüzdanın mevcut iki adet şifresi ya da anahtarı bulunmaktadır. Özel ve genel olarak ayırabilen bu iki şifreden özel olanı sadece sizin kişisel olarak bildiğiniz ve kullanabildiğiniz bir şifre iken genel anahtarı, Bitcoinlerle yaptığınız işlemlerde işlemin güvenliği için kullanılmaktadır. Bitcoin alım satım işleminde, işlemi genel anahtar aracılığı ile diğer tüm Bitcoin ağlarına gönderilip işlemin doğruluğu onaylatılmakta ve yapılan işlem bütün bloklara yazılmaktadır. Böylece yapılan işlemin kaydı tüm bloklarda kayda alınarak işlemin güvenirliği sağlanmakta ve de bu işlemle kimlik doğrulaması yapılmaktadır.

Nakamoto makalesinde bu durumu özetle bir işlemin varlığını ya da yokluğunu onaylamanın tek yolu, tüm işlemlerden haberdar olunması ile çözüleceğini düşünmektedir ve sistemi bu mantık üzerine oturtmuştur. Block Chain sisteminde tıpkı bir banka mantığı ile yapılan tüm işlemleri kontrol etmek, paranın miktarı, harcanma oranı ve yapılan işlemin tarih kayıtları gibi birçok faktörü kayıt altına tutmak zorundadır. Bunu sağlayan merkezi olmayan Bitcoin sisteminin aynı anda dünya üzerinde birçok işlemin gerçekleştiği ve Block Chain ağında aynı anda oldukça işlem kayıt altına alındığı düşünülürse bu işlemlerde fiziksel ya da software olarak adlandırabileceğimiz yazılımsal hataların ortaya çıkabilmesi olası bir problemdir. Bunu ortadan kaldırabilmek için Bitcoin sistemi kriptografik bir hash fonksiyonu ile bu sorunu çözmektedir.

Kriptografik Hash Fonksiyonu; değişken uzunluklu veri kümelerini, sabit uzunluklu veri kümelerine haritalayan algoritma ve alt programdır ki değişken uzunlukta bir verinin belli kod sistemlerine sıkıştırılarak daha az yer kaplamasını sağlamak, yapılan işlemi hızlandırmak, işlemlerin benzerliklerini ya da farklılıklarını ortaya koymaya yarayan bir fonksiyon olarak tanımlanmaktadır (Gültekin & Bulut, 2014: 85). Kısaca Hash fonksiyonu yapılan işlemi sıkıştırmakta, kodlamakta ve böylece birbirine benzemeyecek şekilde oluşturduğu kodlar ile doğru, hızlı ve güvenilir veriler elde edilmesini sağlamaktadır. Bu kodlama sistemi sadece Bitcoin sisteminde değil kullandığımız birçok programda bugün hash fonksiyonları kullanılmaktadır. Apple marka telefonlarımızdaki Iphone'larda parmak izi ya da bugün Iphone X'lerde kullanılan yüz tanıma teknolojisinde sizden sağladığı bilgiyi/şifreyi yani yüzünüzü ya da parmak izinizi tek taraflı hash fonksiyonu ile kod sistemine dönüştürerek parmak izimiz gibi dünyada sadece bize özel olabilecek bir kod/kimlik sağlar. Bitcoin'de de sadece bize ait olacak

bir anahtar/kod/kimlik sağlamaktadır ve bu sayede aynı anda yapılan belki de milyonlarca işlem arasından yapılan işlemi belirlemekte, sistemde olabilecek problemleri ise ortadan kaldırmaktadır.

Bitcoin, SHA-256 (256 bit Secure Hash Algorithm) olarak adlandırılan, diğer algoritmalara göre çok daha karmaşık bir sisteme sahip olan bir algoritma kullanmaktadır. Bu da Bitcoin'in güvenliğini en üst noktaya çıkarmaktadır. SHA-256 olarak adlandırılan algoritmanın Bitcoin'le yapılan bir işlemin onayının sağlanması için yüksek performanslı bilgisayarların yaklaşık olarak 10 dakika boyunca çalışması gerekmektedir. Bu işlemler için yüksek performanslı bilgisayarlara olan ihtiyacı beraberinde getirmekte, aynı zamanda elektrik tüketimini de oldukça fazla arttırmaktadır. Bu durum Venezüella gibi ülkelerde doğrudan problemlere sebebiyet vermekte ve hükümetin bu konuda önlemler alma ihtiyacını beraberinde getirmektedir (Epstein, 2017: 29).

Bitcoin işlemleri için güçlü ve hızlı performansa sahip olan bilgisayarlar gerekmektedir. Bitcoin sistemi, CPU'su (Central Processing Unit - Merkezi İşlem Birimi) yüksek bilgisayarlar tarafından sürekli olarak Bitcoin işlemlerinin yapılmasını ve bunlardan bloklara yazılarak Block Chain sisteminin güvenli bir şekilde oluşmasını bir tür ödül sistemi sağlanmaktadır.

Bitcoin Madem Yazılımı tarafından kullanıcılara sunulan ve oldukça zor karmaşık işlemleri içeren problemi çözen ilk kişinin hesabına bir Bitcoin üretilerek yüklenmektedir. Bu yeni Bitcoin P2P sistemi ile bütün hesaplara duyurulup kayıt altına alındıktan sonra yeni bir problem oluşturularak kullanıcıların çözümü için sunulmaktadır. Bu problemler her defasında daha da zor bir hal almakta ve verilen ödül yarıya düşürülmektedir. Bu uygulamanın bütününe Bitcoin Mining/ Bitcoin Madenciliği denilmektedir (Atik, Köse, Yılmaz, & Sağlam, 2015: 249).

Bitcoin ile son bir yılda ortaya çıkan önemli bir endişe ise, madenciliğin merkezileştirilmesidir. Bitcoin madenciliğinin merkezsizleştirilmiş olması vurgunun temel argümanlarından biri olsa da özel entegre devreler ve bilgisayarların her kullanıcı için mümkün olmaması ve blok zinciri protokolüyle ilgili hesaplama kaynaklarının %51'ine erişen Ghash.IO adlı bir madencilik havuzu şirketi, havuz üzerinde bir kontrol gücünü elinde bulundurması endişe verici bir güvenlik açığı olabilme potansiyeline sahiptir. Şirket bu havuz üzerinde haksız uygulamalar gerçekleştirebilme potansiyeline sahiptir (Mainelli & Gunten, 2014: 20).

Bitcoin Madenciliği'nin bir üst sınırı mevcuttur. Bitcoin'inin temel ayırıcı özelliklerinden birisi de budur. Bitcoin sistemi tarafından toplam da 21 milyon sayısı Bitcoin üretiminde üst sınır olarak belirlenmiştir ve bu sayıya ulaştıktan sonra yeni bir Bitcoin üretimi olmayacak yani Bitcoin madencilerine ödül verilmeyecektir. Her 10 dakikada 25 Bitcoin üretimi gerçekleştiği düşünülürse, bu üretimin 2140 yılı itibari ile biteceği hesaplanmaktadır. Kasım 2016 itibariyle ise sirkülasyonda ki toplam Bitcoin miktarı 16 milyon civarında olup toplam piyasa değeri 11 milyar doları aşmıştır (Khalilov, Gündebahar, & Kurtulmuşlar, 2017: 4). 31 Aralık 2017 yılı itibari ile sirkülasyondaki Bitcoinlerin toplam piyasa değeri 220 milyar dolar civarındadır. (Cryptocurrency Market Capitalizations, 2017, Aralık 30). Tabi bunun her gün ve saatte değiştiği gerçeğini unutmamak gerekir.

Bitcoinlerin sayısının sınırlı olması ve her Bitcoin üretiminin giderek daha da çok zorlaşması, paranın giderek değerleneceği tahminleri yapılmaktadır. Tıpkı altın gibi az ve değerli olması gibi özellikler taşıdığı için Bitcoin'e dijital altın ya da dijital para denilmektedir. Ama Bitcoin günümüz şartlarında deneysel olduğu göz önüne alınırsa ve insanların Bitcoin'e olan yöneliminin altında yatan sebepler kesin olarak netleşmediği göz önüne alınırsa her geçen gün inişli-çıkışlı dalgalı bir form izleyen Bitcoin'in güvenilirliği tartışılmaktadır. Devletlerin yeni bir para birimi olarak karşılaştığı Bitcoin hakkında ne gibi düzenlemeler, kurallar ve yasalar yapacakları belli olmadığı için ve bu konu hakkında uluslararası otoriteler net tavır almadıkları için Bitcoin hakkında çok net tahminler yürütmek oldukça zordur.

Bitcoin'in piyasa değeri Bitcoin'in USD cinsinden değeri ile ilişkilidir (Üzer, 2017: 45). 30 Aralık 2017 tarihinde BTCTurk adlı Türkiye'de faaliyet gösteren aracı kripto para borsasından alınan verilere göre 1 BTC'nin Türk Lirası karşılığı 57,950.00 TRY iken 24 saatlik işlem hacmi 381.70 BTC'dir (BTCTurk, 2017, Aralık 30). ABD ve tüm dünya da faaliyet gösteren dünyanın en büyük işlem hacmine sahip olan kripto para borsalarından biri olan Bitfinex'e göre 30 Aralık 2017 tarihinde 1 BTC'nin ABD Doları karşılığı 14,126,29 $ USD'dir ve günlük işle hacmi $2,276,880,941'dir (BITFINEX, 2017, 30 Aralık).

Bitcoinin Piyasalarda Sağladığı Avataj ve Dezavantajları

Bitcoin'in avantajlarını ve dezavantajlarını ele almamız gerekirse; Bitcoin, bankaya ihtiyaç duymaz, P2P Kişiden Kişiye Elektronik Para Sistemi'dir ve aracı bir kuruma ihtiyaç yoktur. Aracı kurumun ortadan kalkmasıyla yapılan işlemler için ödenen maliyet de ortadan

kalkmaktadır. Bitcoin işlem masrafları yok denecek kadar azdır. Bitcoin sisteminde sahip olduğunuz hesabınız dondurulamaz ve bloke edilemez. Günümüzde banka hesapları belirli otoritelerin devletlerin vs. kararları ile dondurulup, bloke edilebilirken Bitcoin hesabınız üzerinde böyle bir uygulamaya gerçekleşememektedir.

Bitcoin kullanımı için sahip olmanız gereken herhangi bir ön şart yoktur ve Bitcoin'i kullanım masrafı bulunmamaktadır. Bitcoin dünyanın hemen hemen her noktasında ödeme özgürlüğü sağlamakta ve dünyanın her noktasından aynı transfer komisyonuyla işlem gerçekleşir, arada fark oluşmamaktadır. Diğer uluslararası para transferi araçlarına göre daha ucuz ve çok kısa süre içerisinde işlemlerin gerçekleşmesine imkan sağlar.

Bitcoin yalnızca bir ödeme aracı değildir. Her geçen gün değerinin artması ile yatırımcılar tarafından bir yatırım aracı olarak da görülmektedir. Bitcoin sisteminde transferlerin ve hesapların kimliği gizlilik esasına göre tasarlanmıştır. Anonimlik seviyesi oldukça yüksektir. Bitcoin'in anonim işlem yapabilme özelliğine sahip olması, Bitcoin kullanımını ve hakkındaki endişeleri artırmıştır. 2012 yılında Bitcoin ile yapılan uyuşturucu ticaretinin büyük bir kısmının Silk Road isimli dark webde bulunan bir e-ticaret platformu üzerinden yapıldığı tahmin edilmektedir (Koçoğlu, Çevik, & Tanrıöven, 2016: 79).

Bitcoin normal bankaların ya da finans sistemlerinden farklı olarak tatil ya da herhangi bir sınırla bağlı olmamaktadır ve istediğiniz her an işlem yapabilme özgülüğüne sahip olunmaktadır. Block Chain uygulaması devrim niteliğindedir ve güvenliği en üst noktalara taşımaktaysa da hala siber saldırı riskleri göz önünde bulundurulmalıdır. Sahip olduğunuz paranın güvenliğini aracı kurumlar değil şahsi olarak kendiniz sağlarken, uluslararası seyahatlerinizde döviz değişiminde bulunma zorunluluğunuz ortadan kalkmaktadır.

Bitcoin belirli merkezler tarafından regüle edilemediği için dalgalı bir seyir izlemektedir. Her an inişler ve çıkışlar görülebilmektedir. Bu iniş ve çıkışlara sebebiyet veren temel nedenler tam olarak bilinmemektedir. Bu dalgalı yapıya sahip olması onun bir yatırım aracı olarak kullanılmasını engelleyen en önemli risklerdendir. Hareketli bir yapıya sahip olan Bitcoin'in hareketliliğinin diğer para birimlerine ve altına göre çok yüksek seviyede olması yatırımcıları büyük bir risk altına sokmaktadır (Koçoğlu, Çevik, & Tanrıöven, 2016: 80). Bitcoin borsasının batma ihtimali çok yüksektir, yarını öngörülememektedir.

Bitcoin sisteminde yapılan işlemlerin geri dönüşü olmaması diğer bir olumsuz faktördür. Sistemde yapabileceğiniz herhangi bir hata ya da sahip olduğunuz Bitcoin'lerin bulunduğu donanımsal yapıda gelebilecek bir sorun geri dönülemez sonuçları da beraberinde getirebilmektedir. Ayrıca Bitcoin sahibi olmanız için gereken cüzdan kaybolursa ya da bu cüzdanın bulunduğu cihaza herhangi bir zarar gerçekleşirse bu Bitcoinlere yeniden sahip olmanız mümkün değildir. The Guardian'ın haberine göre; 2013 yılında James Howells, içinde 7.500 Bitcoin olan bir hard diski kazara çöpe atmıştır. İçindeki verileri yedeklemeyen Howells, 4 milyon sterlin değerindeki Bitcoinlerinin bulunduğu diski Galler'de bulunan çöp toplama alanında haftalarca aramış olmasına rağmen sonuç alamamıştır (Hern, 2013, Aralık 13). Böyle durumlarda yaşanabilecek mağduriyeti şikayet edip hukuksal süreç başlatabileceğiniz herhangi bir kurum ya da kuruluş söz konusu değildir.

Genel otoriteler ve tüm devletler tarafından kabul edilen yasal bir temeli söz konusu olmadığı ve Bitcoin'in vergilendirilemediği düşünülecek olursa, devletlerin Bitcoin ile ilgili ne gibi sınırlar getirecekleri belli değildir. Devletlerin sahip olduğu para politikaları ile uyuşmayan durumlarda Bitcoin'i yasaklama eğilimi içerisindedirler. Bunlara örnek olarak İzlanda, Bangladeş, Bolivya, Ekvator, Tayland verilebilir. Yaşanılabilecek herhangi büyük bir elektrik kesintisi veya kriz durumunda Bitcoin'i yapacağınız işlemlerde kullanmak mümkün değildir.

Uluslararası İlişkilerde Sanal Para: Bazı Devletlerin Bitcoin Politikaları

Uluslararası ilişkilerin aktörleri arasında kabul edilen çok uluslu şirketler(ÇUŞler) tarafından 2015 yılından itibaren, Bitcoin üzerinden işlem yapmayı kabul eden şirket sayısı 100 bini aşmıştır. Bugün dünyanın önde gelen şirketleri arasında WordPress.com, Subway, Microsoft, Reddit, Wikipedia, Steam, Zynga, Bloomberg.com, Stripe, Dell, PayPal gibi daha birçok şirket içerik ve uygulamalarını satın almak isteyen müşterilerine Bitcoin'le ödeme yapma imkanı sunmuş durumdadır (bitcoin, 2017: Ağustos 15). Bu şirketler ile yapılan işlemlerde komisyon oranları güncel olarak kullandığımız kredi kartlarına göre daha düşük olması sebebiyle müşteriler tarafından tercih edilmektedir.

Bitcoin kullanımının kısa sürede bu kadar yaygınlaşması, Bitcoin ATM'lerinin her geçen gün Bitcoin ATM sağlayıcıları tarafından sayısının artırılmasını sağlamaktadır. Bugün dünya üzerinde Bitcoin ATM sayısının 1000 civarında olduğu tahmin edilmektedir. Bunların çoğunun ABD'nin önemli şehirlerinde bulunmaktadır. Bitcoin ATM sağlayıcıları olan Consource,

Bitstop ve Rockitcoin gibi sağlayıcılar tarafından bu sayısının artırılması için çaba içinde oldukları bilinmektedir (Sakmar, 2017, Temmuz 24).

Bitcoinlerin kullanımı hakkında ülkelerin sahip olduğu tutum farklılık göstermektedir. Uluslararası alanda bir politika bütünlüğünden bahsetmek söz konusu değildir. Kimi ülkeler Bitcoin kullanımına olumlu yaklaşırken bazıları olumsuz bir tutum içerisindedir. Genel itibari ile bir konsensüsün olmamasından dolayı pek çok ülke kripto paraların yasal düzenlemesi ve regüle edilmesi konusunda Amerika'nın alacağı tavrı ve yaklaşımı beklemektedir. Çünkü Amerika Birleşik Devletleri en çok kripto paraya ev sahipliği yapan ve dünya üzerindeki Bitcoin ticaret hacminin lideri konumundadır. Ancak 2013 yılında ABD Hazinesi, Bitcoin'i sanal bir para birimi olarak sınıflandırmasından sonra Emtia Vadeli İşlem Komisyonu (CFTC) Eylül 2015'te Bitcoin'i emtia olarak sınıflandırması ciddi bir adım olarak değerlendirildi. (blockchain.org, 2017) ABD'de hazineye bağlı çalışan Financial Crimes Enforcement Network (FinCEN) olarak adlandırılan kuruluşun 2013 yılında dünyanın ilk Bitcoin yasal düzenlemelerinden birini çıkarması, Ağustos 2013'de ABD'deki federal mahkemeler tarafından Bitcoin'lerin para yerine kullanılabileceği kararı, Kasım 2013'de ABD'de Senatosunun dijital para konusunda oturumlar düzenlemesi gibi uygulamalar genel olarak Bitcoin'e karşı ABD'nin tutumunun olumlu olduğu yönündedir (Avrasya BlockChain ve Dijital Para Araştırmaları Derneği, 2017, Nisan 18).

Estonya, Bitcoin'e karşı olumlu tavır alan bir başka ülkedir. Bitcoin'in arkasında devrim olarak nitelendirilen Block Chain teknolojisini sağlık, bankacılık ve elektronik tabanlı oylama sistemi için kullanmaya başlamıştır. (blockchain.org, 2017, Aralık 30) Bitcoin işlemleri yasal olarak kabul görürken, son dönemlerde Estonya 'Estcoint' adı verilen sanal para birimi uygulamasına geçeceğini açıklamış ve eğer bu projeye hayata geçirebilirse dünya üzerinde sanal para birimi kullanan ilk ülke olacaktır(Demirkan, 2017, Ağustos 27).

İsveç ve Danimarka da sanal para birimine olumlu bakan ülkeler arasında yer almaktadır. Bitcoin bu iki ülkede de işlem görmektedir ancak Danimarka Merkez Bankası Başkanı Lars Rohde tarafından devlet televizyonuna verilen demeçte, 'Ölümcül Bitcoin'den uzak durmalısınız' açıklaması Bitcoin üzerindeki şüpheleri yeniden artırmış gözükmektedir (Ekonomi, Sputnik, 2017, Aralık 19).

Bitcoin Madenciliği faaliyetlerinin ciddi anlamda yapıldığı ülkelerden biri olan Çin'in kendi dijital parası OneCoin üzerine çalışmalar yaptığı iddia edilmektedir. Çin'de faaliyet gösteren ICO'ları (Initial Coin Offerrings) yasakladığını duyurması üzerine kripto para çalışmalarına ciddi bir yavaşlamaya neden olmuştur. Bu durum Bitcoin'in değeri üzerinde ciddi düşüşlere sebebiyet vermiştir (Ekonomi, Hürriyet, 2017, Eylül 9).

Japonya, kripto paralar konusunda vizyoner ve hızlı adımların gerçekleştiği bir ülkedir. Japonya, yasal anlamda çıkardığı bankacılık kanunu ile Bitcoin ve diğer dijital paraların içerisinde yer alan kripto paraları da 'Sanal Para Birimi Kanunu' ile yasal ödeme aracı olarak kabul etmiştir (HaberTürk Ekonomi, 2017, Nisan 7). Japonya'da GMO İnternet Group adlı bir şirket 2018 yılı itibari ile çalışanların maaşlarının bir kısmını sanal para birimi Bitcoin ile ödeyeceğini açıklamıştır (Teknoloji, NTV, 2017, Aralık 13). Japonya, bankacılık sistemini değiştiren bir kanun ile Bitcoin ve diğer tüm dijital para birimlerini yasal olarak tanınmıştır. 'Sanal Para Birimi Kanunu' ismiyle yasalaşarak yürürlüğe giren kanunda, Bitcoin vb. dijital para birimleri ödeme aracı olarak kabul edilmiştir.

Dünyanın en büyük Bitcoin platformlarından biri olarak kabul edilen Japonya, Tokyo merkezli Mt. Gox adlı Bitcoin borsası/platformu Haziran 2013 DDoS saldırısı sebebiyle tüm kullanıcıların adres, hesap ve kimlik bilgileri çalınmış olup 850 binden fazla Bitcoin'in (günümüzde değeri 3.5 milyar dolar) çalındığı açıklanmıştır. Bu olay kripto paraya ve Bitcoin'e olan güvenin sarsılmasına neden olmuş ve Bitcoin ciddi bir düşüş yaşamıştır. Bu olaydan sonra Bitcoin'e yönelik ortaya çıkan şüpheler, para birimindeki likiditeyi azaltırken değerinin de yıllarca zedelenmesine yol açmıştır. İlerleyen dönemlerde aracı kurumlar alt yapılarını güçlendirip siber saldırıları önlemek için çeşitli önlemler almıştır. Ancak Bitcoin yeniden toparlanma sürecine girip değerini artmış olsa da bu saldırı 'Bitcoin gerçekten güvenilir mi?' sorularını güncel olarak tartışılmasına sebebiyet vermiştir (BirGün Ekonomi, 2017, Aralık 22).

İngiltere, Bitcoin'i FX (Foreign Exchange) işlemi yani döviz alım satım işlemi olarak kabul edip buna uygun olarak vergilendirileceğini açıklamıştır (Can, 2017, 28 Temmuz). İngiltere'de finans sektörünü düzenleyen ve denetleyen Finansal Hizmetler İdaresi'nin (FSA) Genel Müdürü Andrew Bailey, Bitcoin'in bir para birimi olmadığını, regüle edilemeyen bu formun, oynak bir emtia olduğunu belirtmiştir. Yatırımcılara tüm paralarını kaybetmeye hazır olmaları gerektiğini bunun ciddi bir uyarı olduğunu belirtmiştir (BBC Türkçe , 2017,Aralık 15).

Rusya, Bitcoin'in yasadışı aktivitelerde kullanılmaya yatkınlığı sebebiyle Bitcoin kullanımını yasaklamıştır. Ancak Bitcoin'in artan değeri sebebiyle 2016 yılında bu yasağı kaldırmıştır. Yaklaşık bir yıldır kullanımı serbest olan Bitcoin, Rusya Maliye Bakanı Anton Siluanov, Bitcoin'in Rusya'da hiçbir zaman rublenin yerine geçemeyeceğini belirtmiştir (SABAH , 2017, Ekim 30). Ancak Rusya İletişim Bakanı Nikolay Nikiforov, Moskova'da kapalı bir toplantıda Devlet Başkanı Putin tarafından kripto para geliştirilmesi yönünde talimat verildiğini, 'CryptoRuble' (Kripto Ruble)'nin oluşturulacağını açıklanmıştır. Böyle bir girişimde bulunulmasının nedeninin kendilerinin bu birimi oluşturmazlarsa Avrasya Ekonomik Topluluğu'ndaki komşularının yapacağını belirtmiştir (Milliyet Teknoloji, 2017, Ekim 10). Rusya, Bitcoin konusunda kripto para madenciliği yapılması planlanan yeni bir şehir kurmaya hazırlandığını açıklamıştır. Bitcoin Madenciliği için gerekli olan yüksek performanslı bilgisayarlar ve elektrik kullanımının ciddi anlamda gerekli olduğu bilinmektedir. Sibirya'nın, enerji maliyetlerinin düşük olması nedeniyle, kripto para madenciliğinde yükselen bölgelerden biri olabileceğine dikkat çekilmektedir (Dünya, 16 Kasım 2017).

Güney Kore Samsung ve LG gibi büyük teknoloji firmalarının bulunduğu ülke dünyanın en büyük sanal/kripto para birimi piyasasına sahip devletlerden birisidir. Bitcoin bir ödeme metodu olarak kabul görmüştür ve yaygınlaşmıştır. Bitcoin için tam bir yasa olmasa da Güney Kore hükümeti ödemeler, transferler ve ticareti kolaylaştırmak için Bitcoin hizmet sağlayıcılarını resmi olarak yasalaştırmıştır (Taşdemir, 2017, Temmuz 22). Güney Kore, sanal para birimi Bitcoin'i düzenleyici yeni adımlar atmış olup Bitcoin sahiplerinin, hesaplarında gerçek isimlerini kullanmalarını zorunlu kılacaklarını açıklamıştır. Ayrıca bir başka değişiklikle ilgili makamlara, sanal para bozdurma işlemlerini durdurma yetkisi vermektedir (Voice of America, 2017,Aralık 28).

Hollanda'da Bitcoin kullanımı hakkında yasal bir düzenleme bulunmamakla birlikte Hollanda'nın Finansal Denetim Yasası kapsamında da değildir. Ancak Bitcoin kullanımı alışveriş işlemlerinde kullanılabilmektedir. Hollanda'da bulunan Arnhem şehri bir Bitcoin şehri haline gelmiştir. Şehirde 100'den fazla Bitcoin'le alışveriş yapılabilen noktaları bulunmaktadır. Hollanda bankaları, Blok-Zincir metoduyla kendi teknolojilerini geliştirmeye çalışmakta, masrafları azaltmak için kullanmanın yollarını araştırmaktadırlar (Çarkacıoğlu, 2016. 57).

Türkiye, Bitcoin hakkında 25 Kasım 2013'te Bankacılık Düzenleme ve Denetleme Kurumu tarafından bir basın açıklanması yapılmıştır. Açıklama da;

> *Herhangi bir resmi ya da özel kuruluş tarafından ihraç edilmeyen ve karşılığı için güvence verilmeyen bir sanal para birimi olarak bilinen Bitcoin, mevcut yapısı ve işleyişi itibarıyla Kanun kapsamında elektronik para olarak değerlendirilmemekte, bu nedenle de söz konusu Kanun çerçevesinde gözetim ve denetimi mümkün görülmemektedir. Diğer taraftan, Bitcoin ve benzeri sanal paralar ile gerçekleştirilen işlemlerde tarafların kimliklerinin bilinmemesi, söz konusu sanal paraların yasadışı faaliyetlerde kullanılması için uygun bir ortam yaratmaktadır. Ayrıca Bitcoin, piyasa değerinin aşırı oynak olabilmesi, dijital cüzdanların çalınabilmesi, kaybolabilmesi veya sahiplerinin bilgileri dışında usulsüz olarak kullanılabilmesi gibi risklerin yanı sıra yapılan işlemlerin geri döndürülemez olmasından dolayı operasyonel hatalardan ya da kötü niyetli satıcıların suiistimalinden kaynaklı risklere de açıktır* (Bankacılık Denetleme ve Düzenleme Kurumu, 2013: 32).

Türkiye de diğer ülkeler gibi Bitcoin'in yasal statüsü belirlenmediği için vergilendirme konusu muğlaklığını korumaktadır. Ancak bu konuda Avrasya Block Chain ve Dijital Para Araştırmaları Derneği'nin, Sermaye Piyasası Kurulu'nun, Türkiye Cumhuriyet Merkez Bankası Başkanlığı'nın bu konuda çalışmalar yaptıklarının sinyallerini vermektedir. Türkiye'de faaliyet gösteren Bitcoin borsaları BTCTurk ve Travelers Box gibi KKTC kaynaklı firmaların yanı sıra son zamanlarda Koinim, Koineks, Paribu gibi Bitcoin borsaları da faaliyet göstermektedir (Yazıcı, 2017,Haziran 6).

SONUÇ

Küreselleşen dünyada para, eski çağlardan bugüne evrimleşerek gelmiştir. Takas sistemiyle ortaya çıkan bu süreç bugün teknolojik devrimlerle yeni bir form kazanmıştır. Fiziki durumu ortadan kalkmaya başlayan paranın siber/dijital dünyada karşılığı sanal para birimlerinden en çok bilinirliğe sahip olan Bitcoin bu konuda öncü niteliğe sahip olması onu değerli kılan en önemli özelliklerden biridir. Regülasyona yani devlet tarafından işleme tabi olmayan bu para birimi, belli bir merkez tarafından kontrol edilememesi ve işlem görememesi bu para birimlerini küreselleşen dünyamızda daha cazip bir hale getirmektedir.

Bitcoin'den farklı olarak birçok sanal para birimi şu an işlem görmekteyse de bugün bu para birimlerinin altında yatan Block Chain teknolojisi dikkatleri üzerine çekmektedir. Bu teknolojide açık kaynak kodlu sistem olarak adlandırılan sistemin varlığı devrim niteliğinde görülmektedir. Merkez algısını ortadan kaldıran bu sistemle geliştirilen bu para birimleri ile

ticaret, alışveriş uygulamaları birçok ülke de hızla yaygınlaşmaya başlamıştır. Bitcoin'in kendi içerisinde kaynaklanan sorunlar (hızlı iniş çıkışlar, yaşanan güvenlik problemleri, yapılan siber saldırılara karşı ortaya çıkan sonuçlar gibi) hala bu para birimine yönelik ihtiyatlı tutum sergilendiği söylenebilir.

Devletlerin Bitcoin ve diğer altcoinler üzerinde düzenleme yetkilerinin bulunmaması, vergilendirilememesi, aracı kurumları ortadan kaldırması gibi birçok sebeple bugün her ülkenin bu sanal para birimlerine şüpheyle yaklaştığı söylenebilir. Birçok devlet bugün Bitcoin hakkında olumlu tutum içerisinde olabiliyorken, olumsuz tutuma sahip olan devletler de mevcuttur. Sanal para birimleri hakkında bugün bazı devletler tarafından yapılan birtakım düzenlemeler mevcut ise de dünya ekonomisine yön veren devletlerin, bu para birimlerini kabul edip etmeyecekleri, nasıl bir tutum içerisine girecekleri, nasıl yasal düzenlemeler yapacakları, önümüzdeki dönemde merakla beklenen konular arasındadır.

KAYNAKÇA

Ateş, B. A. (2016). Kripto Para Birimleri, Bitcoin ve Muhasebesi. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 349-366.

Atik, M., Köse, Y., Yılmaz, B., & Sağlam, F. (2015). Kripto Para: Bitcoin ve Döviz. *Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 6*(11), 247-261.

Avrasya BlockChain ve Dijital Para Araştırmaları Derneği. (2017, Nisan 18). *Bitcoin ve Dijital Paranın dünya ülkelerine göre yasal durumu* . BLASEA: http://www.blockchain.org.tr/bitcoin-ve-dijital-paranin-dunya-ulkelerine-gore-yasal-durumu/ adresinden alındı [Erişim Tarihi: 09.01.2018]

Bankacılık Denetleme ve Düzenleme Kurumu. (2013, Kasım 25). Basın Açıklaması. *Basın Açıklaması*. Ankara, Türkiye: Bankacılık Denetleme ve Düzenleme Kurumu.

BBC Türkçe . (2017, Aralık 15). *İngiltere'de Bitcoin yatırımcılarına uyarı: Tüm paranızı kaybetmeye hazır olun*. BBC Türkçe: http://www.bbc.com/turkce/haberler-dunya-42349256 adresinden alındı [Erişim Tarihi: 15.12.2017]

BirGün Ekonomi. (2017, Aralık 22). *5 senelik dönemde Bitcoin'in yaşadığı iniş-çıkışlar ve nedenleri*. BirGün.net: https://www.birgun.net adresinden alındı [Erişim Tarihi: 22.12.2017]

bitcoin. (2017, Ağustos 15). *Ödeme Olarak Bitcoin Kabul Eden Şirketler Listesi*. bitcoin: https://bitcoinlerim.com/odeme-olarak-bitcoin-kabul-eden-sirketler-listesi/ adresinden alındı [Erişim Tarihi:09.01.2018]

Bitcoin. (2018, Ocak 1). *Bitcoin Projesi*. Bitcoin: https://bitcoin.org/tr/sss#bitcoin-nedir adresinden alındı [Erişim Tarihi: 01.01.2018]

BITFINEX. (2017, Aralık 30). *BITFINEX*. BITFINEX: https://www.bitfinex.com/ adresinden alındı [Erişim Tarihi: 30.12.2017]

BTCTurk. (2017, Aralık 30). *BTCTurk*. BTCTurk: https://www.btcturk.com/ adresinden alındı [Erişim Tarihi: 30.12.2017]

Can, A. (2017, Temmuz 28). *Yasaklamıyorlar kullanıyorlar*. Hürriyet.com.tr: http://www.hurriyet.com.tr/yasaklamiyorlar-kullaniyorlar-40534266 adresinden alındı [Erişim Tarihi: 09.01.2018]

Cryptocurrency Market Capitalizations. (2017, Aralık 31). *Historical Snapshot - December 31, 2017*. Cryptocurrency Market Capitalizations: https://coinmarketcap.com/historical/20171231/ adresinden alındı [Erişim Tarihi: 09.01.2018]

Çarkacıoğlu, A. (2016). *KRİPTO-PARA BITCOIN*. Ankara: SERMAYE PİYASASI KURULU.

Demirkan, T. (2017, Ağustos 27). *Dünyada bir ilk: Estonya 'sanal para birimine' geçiyor*. Aralık 31, 2017 tarihinde BBC Türkçe : http://www.bbc.com/turkce/haberler-dunya-41066338 adresinden alındı [Erişim Tarihi: 09.01.2018]

DÜNYA. (2017, Kasım 16). *Rusya, Bitcoin kenti kuracak*. DÜNYA: https://www.dunya.com/dunya/rusya-bitcoin-kenti-kuracak-haberi-391024 adresinden alındı [Erişim Tarihi: 16.11.2017]

Ekonomi, Hürriyet. (2017, Eylül 9). *Çin yasakladı, Bitcoin'de sert düşüş*. Hürriyet.com.tr: http://www.hurriyet.com.tr/cin-yasakladi-bitcoinde-sert-dusus-40569405 adresinden alındı [Erişim Tarihi: 09.01.2018]

Ekonomi, Sputnik. (2017, Aralık 19). *BitcoinİKi ülkeden daha Bitcoin uyarısı: 'Bu ölümcül'*. Sputnik Türkiye: https://sptnkne.ws/gpSW adresinden alındı [Erişim Tarihi: 19.12.2017]

Epstein, J. (2017). *The Secret, Dangerous World of Venezuelan Bitcoin Mining*. Washington, DC: Reason; Free Minds And Free Markets. http://reason.com/archives/2016/11/28/the-secret-dangerous-world-of adresinden alındı [Erişim Tarihi: 09.01.2018]

European Central Bank. (2012). *Virtual Currency Shcemes*. Frankfurt: European Central Bank. Aralık, 2017 tarihinde

https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf adresinden alındı [Erişim Tarihi: 25.12.2017]

Gültekin, Y., & Bulut, Y. (2014). Bitcoin Ekonomisi: Bitcoin Eko-Sisteminden Doğan Yeni Sektörler ve Analizi. *Adnan Menderes Üniversitesi, Sosyal Bilimler Enstitüsü Dergisi, 3*(3), 82-92.

HaberTürk Ekonomi. (2017, Nisan 7). *Bitcoin artık Japonya'da Yasal*. HaberTürk.com.tr: http://www.haberturk.com/ekonomi/teknoloji/haber/1453992-bitcoin-artik-japonyada-yasal adresinden alındı [Erişim Tarihi: 31.12.2017]

Hern, A. (2013, Kasım 13). *Missing: hard drive containing Bitcoins worth £4m in Newport landfill site*. The Guardian: https://www.theguardian.com/technology/2013/nov/27/hard-drive-bitcoin-landfill-site adresinden alındı [Erişim Tarihi:01.01.2018]

Khalilov, M. C., Gündebahar, M., & Kurtulmuşlar, İ. (2017). Bitcoin ile Dünya ve Türkiye'deki Dijital Para Çalışmaları Üzerine Bir İnceleme. *19. Akademik Bilişim Konferansı* (s. 1-8). Aksaray: Aksaray Üniversitesi. http://ab.org.tr/ab17/ adresinden alındı

Koçoğlu, Ş., Çevik, Y. E., & Tanrıöven, C. (2016). Bitcoin Piyasalarının Etkinliği, Likiditesi ve Oynaklığı. *Journal of Business Research-Türk*, 77-97.

Mainelli, M., & Gunten, C. v. (2014). *Chain of Lifetime: How BlockChain Technology Might Transform Personal Insurance.* London: Z/Yen Group .

Milliyet Teknoloji. (2017, Ekim 10). *Kripto Ruble geliyor! Rusya kendi kripto parasını üretecek*. Milliyet.com.tr: http://www.milliyet.com.tr/kripto-ruble-geliyor-rusya-kendi-teknoloji-haber-2538804/ adresinden alındı [Erişim Tarihi: 29.12.2017]

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Satoshi Nakamoto Institute*, 1-9. 12 29, 2017 tarihinde http://nakamotoinstitute.org/ adresinden alındı [Erişim Tarihi: 09.01.2018]

SABAH . (2017, Ekim 30). *Rusya'dan Bitcoin açıklaması*. sabah.com.tr: https://www.sabah.com.tr/ekonomi/2017/10/30/rusyadan-bitcoin-aciklamasi adresinden alındı [Erişim Tarihi: 25.12.2017]

Sakmar, Ö. (2017, Temuz 24). *Bitcoin ATM'leri Çoğalıyor!* Koin Bülteni: https://koinbulteni.com/bitcoin-atmleri-cogaliyor-1364.html adresinden alındı [Erişim Tarihi: 31.12.2017]

Sönmez, A. (2014). Sanal Para Bitcoin. *The Turkish Online Journal of Design, Art and Communication, 4*(3), 1-14.

Taşdemir, F. (2017, Temmuz 22). *Güney Kore Resmi Olarak Bitcoin'i Yasallaştırdı*. Koin Bülteni: https://koinbulteni.com/guney-kore-resmi-olarak-bitcoini-yasallastirdi-1326.html adresinden alındı [Erişim Tarihi: 29.12.2017]

Teknoloji, NTV. (2017, Aralık 13). *Japon şirket, çalışanların maaşlarını Bitcoin ile ödeyecek*. ntv.com.tr: https://www.ntv.com.tr/galeri/teknoloji/japon-sirket-calisanlarin-maaslarini-bitcoin-ile-odeyecek,21e50bN1EkmVb_U0gDjVZw/tcwRqoK9xEKVxJ5ZOTHK6w adresinden alındı [Erişim Tarihi: 27.12.2017]

Üzer, B. (2017). *Sanal Para Birimleri.* Ankara: Türkiye Cumhuriyet Merkez Bankası.

Voice of America. (2017, Aralık 28). *Güney Kore'den Bitcoin'e Düzenleme*. Voice of America: https://www.amerikaninsesi.com/a/guney-kore-den-bitcoin-a-duzenleme/4182897.html adresinden alındı [Erişim Tarihi: 29.12.2017]

Yaşar GÜLTEKİN, Y. B. (2014). Bitcoin Ekonomisi: Bitcoin Eko-Sisteminden Doğan Yeni Sektörler ve Analizi. *Adnan Menderes Üniversitesi, Sosyal Bilimler Enstitüsü Dergisi*, 82-92.

Yazıcı, H. (2017, Haziran 6). *Türkiye Merkezli Bitcoin Borsaları*. Bitbaba: https://www.bitbaba.xyz/turkiye-merkezli-bitcoin-borsalari/ adresinden alındı [Erişim Tarihi: 04.01.2018]

DEEP WEB VE DARK WEB: İNTERNET'İN DERİN DÜNYASI

Emine ÇELİK[*]

Özet

İnternet şüphesiz insanlık tarihinde devrim niteliğinde bir buluş ve gelişimi de halen devam etmektedir. İnsanların birçoğu iletişim, sosyal medya, alışveriş, siyasi ve sosyal gündem takibi ve daha fazlası için interneti kullanmaktadır. İnternetin devletlerin uluslararası arenada, kamu kuruluşlarında ve insan hayatındaki yeri itibariyle Deep Web ve Dark Web kavramlarının yalnızca bilgisayar, yazılım mühendislerince ele alınmasının eksikliğinden yola çıkarak sosyal bilimler içerisinde incelenmesi büyük önem arz etmektedir. Buradan hareketle çalışma içerisinde Deep Web ve onun karanlık yanı olarak isimlendirilen Dark Web'in ortaya çıkardığı potansiyel tehlikelere değinilmiştir. İki kavramın nasıl ortaya çıktığı ve gelişimi, Deep Web'e erişimin nasıl sağlandığı, iki kavramın birbirinden ince bir çizgiyle ayrıldığı yerler, Dark Web'deki yasadışı faaliyet alanlarının getirmiş olduğu sorunların önemine vurgu yapılmıştır. Akabinde, Dark Web karşısında devletlerin nasıl bir politika izlemesi gerektiğine dair analizler yapılmaya çalışılmıştır.

Anahtar Kelimeler: Deep Web, Dark Web, Tor, Siber Suçlar, Siber Uzay

Abstract

The Internet is undoubtedly still a revolutionary breakthrough in the history of humanity. Many people use the internet for communication, social media, shopping, political and social agenda, and more. Deep Web and Dark Web concepts not only handled by computer, software engineers but also handled by social siciensists because of the role of internet for the States in international arenas, public institutions and human life. By the moving point that very important

[*] Doktora Öğrencisi, Necmettin Erbakan Üniversitesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, E-mail: eminegvenilir@gmail.com

role of internet for social sicientists, the potential hazards of Deep Web and its dark side referred to Dark Web have been put forth. The emergence and development of deep web and dark web concepts and the acsees of them were handled in the paper. The diffrences between the two concepts which are crucial point of the topic, and the Dark web significance of market are impressed on the paper. Additionally; In the face of Dark Web, an attempt has been made to analyze what kind of policy the states need to follow.
Key Words: Deep Web, Dark Net. Tor, Cybercrime, Cyberspace.

GİRİŞ

İnternet, tasarlanışı itibariyle bilgi paylaşımı ve şeffaflık üzerine inşa edilmiştir. Bu bağlamda da günümüze değin insanlar şeffaflık, bilgiye hızlı ve mekân sınırı olmadan erişim gibi olumlamalar üzerine internet ile olan ilişkilerini geliştirmişlerdir. 21. yüzyılda internetin insan hayatı içerisinde vazgeçilmez bir konuma ulaşması ise çeşitli tartışma alanlarının ortaya çıkmasına neden olmuştur. Sınırları hakkında bilgiye sahip olunmayan internetin ve dolayısıyla siber uzayın insan güvenliği açısından bazı tehlikeler barındırdığı 21. yüzyılda yaşanılan teknolojik gelişmelerin hızlı bir ivme sergilemesi sonucunda fark edilmiştir. Teknoloji dünyasında yaşanılan bu hızlı gelişim internetin bilmediğimiz katmanlarının ulaşılabilir olmasına sebep olmakla birlikte çeşitli güvenlik zafiyetlerinin de ortaya çıkmasına neden olmuştur. 2013 yılında internetin derin dünyası olarak adlandırılan Deep Web ve Dark Web üzerinde faaliyet gösteren Silk Road adı altında yasa dışı ürünlerin satıldığı siteye FBI tarafından gerçekleştirilen bir operasyon sonucunda internetin bazı katmanlarının ne kadar tehlikeli olduğu gözler önüne serilmiştir. Başta devletlerin, güvenlik güçlerinin, akademisyenlerin, düşünce kuruluşlarının ve kamuoyunun dikkatini çeken Silk Road operasyonun akabinde Deep Web ve Dark Web hakkında çeşitli tanımlamalar yapılmaya çalışılsa bile akademik manada doyurucu bir tanım yahut sınır çizilememiştir. Çeşitli parametrelerle izah edilebilecek bu durumun başlıca nedenin ise teknolojik gelişimin sürekli olması, günümüzde internet ve onun derinliği hakkında sağlıklı verilere ulaşılabilecek donanımsal materyallere sahip olunamaması şeklinde ifade edilebilmektedir.

İnternet Kavramı ve Gelişimi

İnternet sözcüğü 20. yüzyılın ikinci yarısı ile ABD ordusunun geliştirme kolu olan İleri Araştırma Projeleri Ajansı tarafından 1960'ların sonlarında yürütülen ve desteklenen küçük bir

bilim projesi olarak hayatımıza girmiş(Barttlet, 2016:15) ve günümüz dünyasında da bireysel olarak yaşamımızın her anında kullandığımız vazgeçilmez bir nesne olmuştur.

İnterneti kullanan 4,8 milyar kişinin varlığının yanı sıra yüzey interneti o1arak adlandırılan kısımda 1,2 milyardan fazla web sitesi bulunmaktadır. Bununla birlikte günde 3,5 milyar Google aramasından söz edilmektedir. Ayrıca "sıradan" bir gün içerisinde ortalama 157 milyar e-mail gönderildiği, 2 milyardan fazla aktif Facebook kullanıcısının olduğu, 500 milyon tweet atıldığı, 4 milyardan fazla YouTube'dan video izlendiği, 47 milyona yakın fotoğrafın Instagram'a yüklendiği araştırmalar sonucunda elde edilmiştir(Internetlivestats, 2018). Rakamsal bu verilerin yanı sıra internet devletler nezdinde ve kamu kuruluşlarında da işleyişin temel aktörlerinden biri haline gelmiştir.

İnternet aslında iletişim ve işbirliğine izin veren açık bir ağ mimari olarak tasarlanmıştır.[12] Tanımlaması yapılacak olur ise ilk başta tasarlandığı gibi birçok kümülatif ağ yapısının bir araya gelmesiyle ortaya çıkan ağ sarmalı olmasıyla birlikte özel standart protokoller kullanarak enformasyon iletmek üzere tasarlanmış devasa bir desantralize bilgisayar ağ şeklinde kavramsallaştırılmaya çalışılmıştır (Schmidt ve Cohen, 2015: 95).

Uzun ve karmaşık tanımlamanın akabinde şu sorular ortaya çıkmaktadır: İnternet sözcüğünü duyduğumuzda zihnimizde ilk olarak ne canlanır? İnternet yalnızca sosyal medya üzerinden etkileşim sağladığımız ağ ya da Google, Bing, Yandex, Yahoo gibi arama motorları ile hayatı kolaylaştıran bilgi kaynağı mıdır?

İnternetin tüm katmanları ele alındığında bilinmezlik ve güvenlik kaygısı taşıyan mimarisi, anonimlik, isnat ve tespitte yaşanan zorluklar -günümüzde devletlerin alt yapılarını oluşturan temel argümanların ağlar üzerinden yönetildiği düşünüldüğünde (Ermiş, 2014) - başta devletlerin olmak üzere, şirketlerin ve bireylerin de yaşamlarını tehdit eder seviyeye gelmiştir. Gelişiminden günümüze kadar uzanan internet yapısı incelendiğinde karşımızda geniş bir alanın olduğu görülmektedir. Düşünülenden fazlasını mevcut ağ yapısının içerisinde barındıran

[12] Deep Web'in spesifikliği ve alanın genişliği bağlamında konuyu karmaşıklaştırmamak adına İnternet yapısının ortaya çıkışı hakkında çalışmada detaylı olarak yer verilmemiştir. İnternetin ortaya çıkışı ve çalışma prensibi hakkında geniş bir bilgiye ulaşmak için bknz: Barry M. Leiner vd. (1997)"Brief History of the Internet ", Internet Society.

internetin ne olduğu aslında insanoğlunun uzay hakkındaki bilgisi kadar olmakla birlikte "Siber Uzay" kavramının karmaşıklığının da ortaya çıkmasıyla sonuçlanmıştır.

Deep Web ve Dark Web Kavramsal Tanımlanması ve Gelişimi

Günümüzde dünyadaki birçok kişi günlük yaşantısında kullandığı internetle siber uzay dünyasında var olan bilgilerin hepsine bahsi geçen arama motorları ile ulaşabileceğini düşünmektedir. Bilinen arama motorların ulaşabildiği bilgilerin çok daha fazlasıysa internetin ağ yapısı incelendiğinde "Deep Web" yani "Derin İnternet" olarak ifade edilen alanda karşımıza çıkmaktadır.

Detaylandıracak olursak; internet olarak adlandırdığımız şey kabaca üç katmana ayrılabilir: yüzey ağ, derin ağ ve karanlık ağ (Santos, 2017). Peki insanların birçoğunun yüzey interneti kullandığı düşünülürse kalan insanların kullanmış olduğu Deep Web neyi ifade etmektedir?

Amerikalı bir akademisyen ve girişimci olan Micheal Bergman "*Deep Web*" ifadesini ilk ortaya atan kişi ve bu konuda önde gelen otoritelerinden biri olarak 90'lı yılların sonlarında derinliğini ölçmek için yaptığı ölçek araştırmasının sonucunda çalışanlarına yüzey internetinin iki yada üç katı büyüklükte olduğunu ifade etmiş ve araştırmanın ilerleyen süreçlerinde tahmin edilen derinliğin daha fazla olduğunu vurgulamıştır. Ayrıca Bergman, Deep Web'i internette bilgilerin en hızlı büyüdüğü alan olarak ifade etmiştir (Beckett, 2009). Deep Web internetin karmaşık ve gizemli bölümü olarak kavramsallaştırılabilmektedir. Deep Web aynı zamanda Hidden Web (Gizli Web) ya da Invisible Web (Görünmeyen Web) olarak da isimlendirilmektedir (Hawkins, 2016: 5-7).

Günümüzdeyse yukarıda bahsi geçtiği gibi kavramsal olarak internetin yer altı olarak tabir edilen Deep Web, var olan yüzey ağının 400-500 katından fazlasının olduğu tahmin edilmektedir. Yüzey interneti olarak adlandırılan (%4 ile %10 aralığını temsil etmektedir) bölüm dışındaki Deep Web'e girmek için ise özel olarak tasarlanmış yazılımsal ürünler, browserler kullanılmaktadır (Epstein, 2014).

Deep Web'in kavramsallaştırılması ve fiziksel olarak ifade edilmesinde popüler olarak kullanılan buzdağı temsilinin yanı sıra yer altı maden işletmeciliği örneği de kullanılmaktadır. Zemin üzerindeki görünür ve bulunabilir her şey yüzey internetini temsil ederken yüzey

altındaki her şey Deep Web'in doğal olarak gizlenmiş, ulaşılması zor ve kolayca görülmeyen yanına atıf yapmaktadır (Cincaglini, vd., 2015:5).

Deep Web dünya çapındaki internetin büyük bir bölümü olmakla birlikte standart arama motorları tarafından indekslenemezler (NCA, 2016:49). Daha açık bir ifade ile Deep Web arama motorlarının ve dizinlerinin doğrudan veri tabanlarına erişimi olmayan geniş bilgi havuzunu ifade etmektedir (Lifewire,2017). Normal şartlarda sınırlı erişim ağları yahut standart bir ağ yapısıyla erişilemeyen Deep Web içerikleri ve barındırılan hizmetler bağlamında kötü amaçlı aktörlerin (terörist gruplar, uyuşturucu satıcıları, eski istihbarat elemanları, çocuk istismarcıları vb…) yasa uygulayıcı aktörler tarafından kısmen ya da tamamen algılanmamasına, görülememesine zemin hazırlamaktadır (Cincaglini, vd., 2015:5). Derin internetin indekslenmemiş bu katmanı ifade etmesiyse güvenlik kaygılarının temelini oluşturmaktadır.

Buraya kadar sorun teşkil etmeyen Deep Web ve Tor benzeri (FreeNet, IP2) yazılımsal sistemlerin kullanımının ortaya çıkardığı asıl sorun ise yasa dışı faaliyetlerin sürdürüldüğü ve bireysel ve devletler nezdinde tehlikeli hala gelen Deep Web'in bir parçası olan ve karanlık katman olarak ifade edilen Dark Web'in kullanımı olmuştur. Deep Web'in tanımlanmasındaki güçlükten yola çıkarak Dark Web'in tam bir akademik tanımının varlığından söz edilememektedir.

Araştırma sonucunda, Dark Web için: Google gibi standart bir web tarayıcısı kullanarak arama motorları tarafından dizine eklenmeyen ve yönlendirilmeyen internette bir bölüm olduğu ve veriye ulaşabilmek için uzman bilgi birikimi ve yazılımsal araçları gerekliliğinden bahsedilmektedir. Ayrıca unutulmamalıdır ki Dark Web, Deep Web değildir, Deep Web içerisinde yasadışı faaliyetlerin yürütüldüğü bir alan olarak belirtilmiştir (Cincaglini, vd., 2015:6). Bu bağlamda da Dark Web genel çerçevede yasadışı faaliyetlerle ilişkilendirilmektedir (Charlton, 2014).

İnternet'in 1990'ların ortasında hemen hemen tüm dünyada popüler hale gelmesinden bu yana var olan "Deep Web" ve onun karanlık yanı olarak nitelendirilen "Dark Web" kavramı uzunca bir süre kamuoyunun dikkatini çekmemiştir. Dark Web'in kamuoyunun tüm dikkatleri üzerine çekmesi ise Ross William Ulbricht'ın tutuklanmasıyla olmuştur. Ulbricht'ın kurmuş olduğu İpek Yolu (Silk Road) sitesi, 2011 yılında faaliyete geçmiş ve bu web sitesi aracılığıyla

satıcıların ve alıcıların internet üzerinden anonim şekilde alışveriş yapabileceği bir platform olması üzerine dizayn edilmiştir (Christin, 2012:3).

Ulbricht'in kurmuş olduğu İpek Yolu'ndaki işlemleri anonimleştirmek için iki türlü yola başvurduğu ortaya çıkmıştır. İlk olarak müşterilerinin anonim olması için Tor ağını kullanmış, ikincisi ise tüm yasa dışı alışverişleri –ilgili bölümde sınıflandırılmasında da bahsedildiği gibi- Bitcoin olarak bilinen ve internette kullanılan, bugün itibariyle herhangi bir yerde fiziksel formda var olmayan, merkezi olmayan elektronik para birimi üzerinden gerçekleştirmiştir. İpek Yolu sayesinde kullanıcılar anonim olarak uyuşturucu ve yasa dışı malların alım ve satımını gerçekleştirilmesini sağlanmıştır. Silk Road yani İpek Yolu Dark Web'de gelişen ilk başarılı anonim pazar olmakla birlikte Amazon tarzında bir yapı benimsediği de görülmüştür(Hawkins, 2016:13). FBI'ın iddiasına göre Ulbright'in bilgisayarına el konulduğunda 150 milyon dolar değerinde 144.000 Bitcoin ele geçirilmiştir. İnternet üzerinden gerçekleştirilen yasa dışı bu faaliyetin FBI tarafından ortaya çıkarılması tüm dünyanın merakını arttırmış ve Deep Web'e ve onun karanlık yönü olan Dark Web'in birçok alanda incelenme ihtiyacını ortaya çıkarmıştır.[13]

Çeşitli güvenlik departmanları ve akademisyenlerce yapılan araştırmalar derinleştikçe İpek Yolu'nun Dark Web'deki en büyük pazar olduğu ancak tek olmadığı anlaşılmıştır. Dark Web'de tamamen yasa dışı faaliyet gösteren bu sitelerin varlığının güvenlik güçleri tarafından takip edilmesi ve akabinde de kapatılmasına rağmen üzerinden çok zaman geçmeden yenilerinin faaliyet göstermeye başlaması ise Dark Web'in işlevselliğini gözler önüne sermektedir (Barttlet, 2016: 152-154).

Tor ve Free Net: Deep Web'in Araçları

Deep Web ve Dark Web hakkında yüzey internet protokollerinden farklı bir çalışma prensipleri kullanması haricinde ilk nasıl kullanılmaya başlandığına dair sağlıklı ve kesin bilgilere ulaşmak zordur. Bunun nedeni ise yukarıda bahsi geçen eylemlerin gerçekleştirildiği platform olmasından ve devletler nezdinde gizlilik arz etmesinden kaynaklandığını söylemek makul bir yaklaşım olabilmektedir. Bunun yanı sıra Deep Web'e giriş için gerekli olan yazılımsal

[13] FBI, "Manhattan U.S. Attorney Announces Seizure of Additional 28$ Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of "Silk Road" Website". https://archives.fbi.gov/, Cadie Thompson, (2015)."Beyond Google: Everything You Need to Know About the Hidden Internet", Business Insider, http://www.businessinsider.com/difference-between-dark-web-and-deep-web-2015-11.

araçlardan bahsedecek olur isek en popüler ve bilinenleri Tor ve FreeNet olarak sıralanabilmektedir.

Türkiye'de de yaygın olarak kullanılan ve artık girişi yasaklanan (Aydoğan, 2017) The Onion Router yani Tor 2002 yılında bütünüyle ABD Donanma Araştırma Laboratuarı ile kar gütmeyen kuruluş olan Free Haven Projesi arasında ortak bir proje olarak ortaya çıkmıştır. Projenin temel amacı ise ihtiyaç duyanlar tarafından kullanılmak üzere dağıtılmış, isimsiz yani anonim ve kolayca konuşlandırılabilir, şifrelenmiş bir ağ oluşturmak şeklinde açıklanmıştır (Moore and Rid, 2016:11). Bir diğer deyişle Tor'un amacı iletilen verilerin adsız kalmasını sağlayacak bir ağ platformu oluşturmasıdır.[14]

Tor mimarisi tek bir yazılım aracılığıyla anonim tarama ve anonim bilgi alışverişlerinin barındırılması için iki temel hizmet sunmaktadır (Moore and Rid, 2016:9). Tor bağlantısı ile giriş yapılan Deep Web ve Dark Web'de aranılan argümanları bulmak kolay bir iş olarak gözükmemektedir. Bunun temel nedeniyse; Tor ile giriş yaptığınız Deep Web ve Dark Web'de internetin yüzey kısmında bulunan sitelerle buralardaki sitelerin benzerlik göstermesidir. Ancak herhangi bir başka siteyle bağlantısı olmamakla birlikte Tor ile giriş yapılan sitelerde URL adreslerinin anlamsız numaralar ve harflerden oluştuğu görülmektedir. Yüzey internetinde bilinen, sonu "com", "org" ve "com. tr" gibi adreslerin yerine "hy352qdvb21.onion" gibi adreslerle bu platformlarda gezinti yapmak mümkündür. URL farklılığının yanı sıra söz konusu sitelerin adresleri Tor Gizli Servisleri tarafından her gün düzenli şekilde değiştirilmektedir. Ancak Deep Web ve Dark Web kullanıcılarına kolaylık sağlayabilmesi açısından güncel sayfaların indekslendiği bazı siteler yer almaktadır. En popüler olanlarından Hidden Wiki'de Wikipedia mantığı ile çalışarak güncel sitelerin adresleri sıralı şekilde yer aldığı bilinmektedir (Bartlett, 2016:119).

Deep Web ile bağlantılı olarak FreeNet ise Edinburg Üniversitesi'nde Ian Clarke adında bir genç tarafından 1995'te insanların internette anonim olarak yani takip edilmeden kullanması için devrim niteliğinden yeni bir yol haritası öneren bilgisayar bilimi dersi için "Dağıtılmış, Merkezi Olmayan Bilgi Depolama ve Alma Sistemi" adında bir tez olarak hazırlanmıştır. Clarke tezinden yola çıkarak 2000 yılında FreeNet adlı yazılımı yayınlamıştır. Bu yazılım sayesinde anonim bir şekilde internetin yüzey katmanının altına inerek Deep Web'e erişim

[14] Hawking, B. a.g.e. p.15.

sağlanabilmiştir. Tor mantığı ile aynı şekilde anonimliği ön planda tutan Freenet'te standart adres uzantılarına -com, org, gov, gibi bilinen uzantılar yerine rakamlardan oluşan bir uzantı vermişlerdir- sahip olmadıkları ve çalışma prensiplerinin normal internetten farklı olması sebebiyle tamamen bir gizlilik sunmaktadır (Labovitz, 2009:11).

Dark Web'deki Potansiyel Tehlikeler

Klasik yüzey internetinin daha gelişmişi olarak birçok kişinin bazı parametrelerden sıyrılarak edinmeye çalıştıkları bilgi alış verişi olarak ele alınan Deep Web'in kullanımın tamamen yasa dışı olduğundan bahsetmek yanlış bir söylemdir. Birçok siyasi düşünür, gazeteci, bilim adamı, akademisyen ve hatta özel hayat gizliliğine önem veren sıradan vatandaşlar bile Deep Web'i kullanmaktadır.[15]

Arap Baharı sürecinde mevcut hükümetlerce internet kullanımın yasaklanmasına rağmen Twitter ve Facebook üzerinden organize olarak gösteri düzenleyen kitlelerin VPN'in yanı sıra, Tor ile birlikte Deep Web'i aktif şekilde kullandığı bilinmektedir. Deep Web'in güvenli kullanıma dair ABD başta olmak üzere Batı'da birçok bilişim şirketi bu yönde hizmet vermektedir.[16] Lakin kullanımı yasal ya da yasal olmasın Deep Web'e erişim kısıtlı ve kullananlar tarafından kasıtlı bir eylem olduğu belirtilmiştir (Hawkins, 2016:7). Buraya kadar birçok ülkede sorun teşkil etmeyen Deep Web'in temel problematiği; Dark Web'deki kişiler tarafından gerçekleştirilen paylaşımların anonim olması(diğer bir ifadeyle IP adresleri herkese açık olarak paylaşılmadığı için) olarak ifade edilmiştir. Bu bağlamda da bu kişilerin devletler veya şirketlerin müdahalesinden çekinmeden iletişim kurup yasadışı faaliyetlerde özgürce bulunmasıysa Dark Web'in potansiyel tehlikesinin temel argümanı şeklinde ifade edilmektedir (Digital Citizens Alliance, 2017:4). Bu argümandan yola çıkılarak vurgulamak gerekirse internet ortamında yani Dark Web'de bir düğümle diğer düğüm arasında Tor gibi yeterince kimlik gizleyici katmanlar söz konusu ise veri paketlerini kaynağına kadar izlemek kesinlikle olanaksızdır. Geniş bir çerçeve içerisinde bahsedilecek olursa da Dark Web platformunda karşıdaki kişiyi tespit etmek bugün neredeyse imkânsızdır(Smidt ve Cohen, 2015:134).

[15] Bu parametreye örnek olması açısından bknz: Marco, C., "Access The Deep Web And Protect Your Privacy Online With The Anonabox", 29.04.2016. https://www.forbes.com/sites/marcochiappetta/2016/04/29/access-the-deep-web-and-protect-your-privacy-online-with-the-anonabox/#6a922a6440c2

[16] Örnek olması açısından bknz: https://brightplanet.com

Deep Web ve Dark Web arasında ayrım yapılamamasının ve yasa dışılık ve yasalara aykırı olamama tartışmaları olmakla birlikte yasal yargı alanları arasındaki karışıklık ve karışıklıklar nedeniyle siteleri, yasal ya da yasa dışı olarak sınıflandırmanın zor olduğu ifade edilmiştir (Owen ve Savage, 2015:4). Sınıflandırmanın zorluğu üzerine Lüksemburg Üniversitesi'nde Deep Web içerisindeki 40.000 adet sitede yapılan analizin akabinde, sitelerin büyük çoğunluğunun İngilizce olduğu, %17'sinin yetişkin içerikli çocuk pornosu, uyuşturucuların %15'ini, sahte ürünlerin %8'ini, hackleme bilgilerinin %3'ünü, siyasi içerikli sitelerin %9'u, yazılım ve donanım üzerine %7 ve sanat üzerine de %2'lik bir oranın tespit edildiği anlaşılmıştır (Bartlett, 2016:280). Buradan yola çıkarak genel kabul gören sınıflandırma:

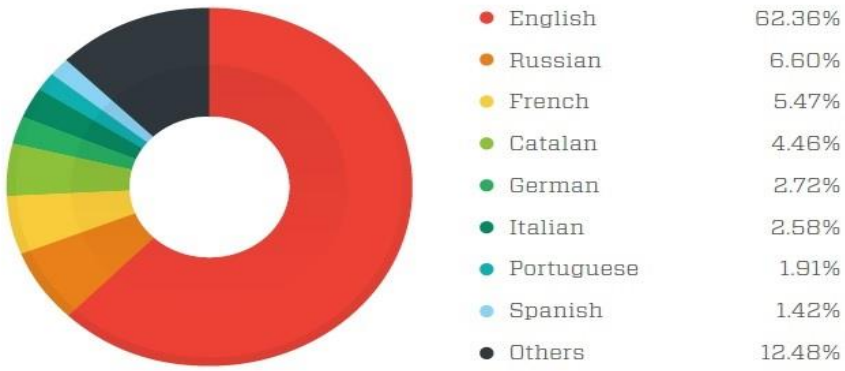
- Kötüye Kullanım: Bu başlıkta altında genel olarak cinsel istismarı gösteren(özellikle küçük çocuklar) ve Batı'da ve dünyanın neredeyse tamamında yasak olan siteler,
- Anonimlik(İsimsizlik): Anonim araçların yahut anonim kültürün tanıtımını veya öğretmeyi amaçlayan siteler,
- Bitcoin: Sanal para birimiyle para vs alış-verişi olarak isimlendirilse bile genel itibariyle kara para aklama hizmetleri,
- Blog: Kişisel yahut toplu blog ve genel itibariyle siyasi, etnik, dini saldırı içerikli,
- Kitaplar: Telif haklarıyla korunan kitapların ücretsiz olarak kullanımına izin verilmesinin yanı sıra yasaklı kitapların paylaşımı,
- Sohbet: Web tabanlı sohbet servisleri,
- Sahtekarlık: Sahte ürünler sunan siteler: Pasaport, kimlik kartları, sahte paralar… vs.
- Dizin: Dark Net içerisinde diğer sitelere bağlantı kuran siteler(genellikle anonim olan alan adlarının bulunmasının yardımcı olması için kullanılmaktadır.),
- Uyuşturucular: Uyuşturucu alışı veya satışı; genel itibariyle alıcılarla satıcıları birbirine bağlayan pazarlar,
- Forum: Birincil amacı başka bir kategoriye sığmayan web tabanlı formlar,
- Dolandırıcılık: Aldatmadan maddi bir amaç sağlayabilen siteler
- Kumar: Kumarı teşvik yada destekleyen siteler,
- Silahlar: Silah satma amaçlı siteler,
- Hacking: Yasa dışı bilgisayar eğitimleri/öğrenimleri sağlayan siteler,
- Hosting: Kullanıcıların başka bir Dark Net sitesine ev sahipliği yapmasına izin veren Dark Net'in barındırma hizmetleri,
- Mail: Dark Net web tabanlı e-posta ve mesajlaşma servisleri (Mail2Tor ve artık kullanımda olmayan TorMail)

- Pazar: Uyuşturucu, silahlar haricinde kalan hizmetleri satan aracı pazar siteleri,
- Haberler: Güncel olaylar ve Dark Net'e özgü haberler,
- Pornografi: Dünya'daki ve özellikle Batı'daki bölgelerdeki yasalarla uyuşmaması,
- Wiki: Gizli Wiki gibi düzenlenebilir içerik (Owen ve Savage, 2015:4-5), şeklinde ifade edilebilmektedir.

Sınıflandırmalara bakıldığında fiziksel dünyada hukuken ağır suç unsurları olan birçok öğenin yer aldığı görülmektedir. Bunun akabindeyse zihinlerde şu soru canlanmaktadır: Bunca yasal olmayan parametreye rağmen peki Dark Web'de kimler bulunmaktadır?

Yapılan araştırmaların neticesinde Dark Web'de kimlerin bulunduğunu söylemek gerçek manada bir durum tespitidir. Ancak Dark Web'in kullanıcılara sunduğu anonimlik seviyesi birçok güvenlik araştırmacısı ve istihbarat servislerinin bile kendi profilini oluşturmalarını zorlaştırmaktadır. Dolayısıyla da elde edilen veriler yalnızca site içeriği ve popülerliğine bakılarak kullanıcı tabanını ölçmeye yaramaktadır. Forward Looking Threat Research Team olarak kendilerini isimlendiren Vincenzo Ciancaglini, Marco Balduzzi, Robert McArdle ve Martin Rösler'in iki yıl içerisinde Dark Web'de birçok web sayfasını taramış, analiz etmiş ve kullandıkları dillere göre sayfaları kategorize etmişlerdir.

Tablo 1.1. :Drk Web'de en çok kullanılan diller :



Bu analiz ise Dark Web kullanıcılarının olabileceği olası bölgelerin açığa çıkmasını sağlamıştır (Cincaglini, vd., 2015:9).

Dark Web İçerisindeki Pazarlar

Silk Road baskının akabinde Dark Web içerisinde yapılan araştırmalar neticesinde,2011 yılında kurulan Black Market Reloaded'ın varlığı tespit edilmiş ve Silk Road'un (satabileceği ürünler sınırlı) aksine her türlü yasa dışı ürünün satışının gerçekleştirildiği tespit edilmiştir. Bu alanda tek olmayan bu iki pazarın yanı sıra: Russian Anonymous Market Place (2012), Sheep Market (Şubat 2013) ve Atlantis Online'ın varlığı açığa çıkmıştır (Bartlett, 2016:280). Silk Road'un satıcılar ve alıcılar arasında daha popüler ve güvenlik güçlerine karşı daha anonim olmasından dolayı Silk Road 2.0 yeniden aktive edilmiştir.

Marketplaces (Today)	Drug Listings	Total Listings	Weapons
Silk Road 2.0	13,648	17,192	No
Agora	7,400	9,158	Yes
Pandora Openmarket	5,249	5,812	No
Evolution	2,623	5,523	Yes
BlueSky Marketplace	1,740	1,833	No
New Markets			
Dark Bay	292	329	No
The Pirate Market	247	367	Yes
Outlaw Market	230	246	No
Tor Bazaar Alpha	205	252	Yes
Black Bank Market	201	239	No
White Rabbit Anonymous MarketPlace	194	256	Yes
TOTAL LISTINGS	32,029	41,207	

Tablo 1.2. Dark Web Markets

Tablo incelendiğinde Dark Web'de anonimlik sayesinde eskisi kapatılmış olsa bile her gün yeni bir pazarın aktif edildiği anlaşılmaktadır. Özellikle bahsi geçen ve birçoğunun varlığı tespit edilemeyen bu pazarları kullanan kişilerin Dark Web üzerinde yasadışı malları alıp satarken anonim kalmasını sağlayan üç temel yapı taşından söz edilmektedir. Bunlar: Tor Network, Bitcoin ve her market tarafından idare edilen pazar forumları (Digital Citizens aliance, 2017:3). Tor ve Bitcoin'in yanı sıra temel olarak ele alınan market forumlarında alıcılar ve satıcılar anonimliği ön planda tutarak satın alacakları yahut satacakları malların elde edilmesine yönelik çeşitli yöntemler geliştirmektedirler.

Genel çerçeve ile bakıldığında Deep Web'de: Kişisel bilgilerin deşifre edilmesi yahut izinsiz olarak ikinci şahıslara satılması, devletlerarası gizli anlaşmaların ifşa edilmesi, devlet politikalarına dair bilgilerin ifşa edilmesi, kara para aklama işlemlerinin gerçekleştirilmesi, çocuk pornografisi, uyuşturucu ve silah ticareti gibi yasa dışı her türlü faaliyetin gerçekleştirilmesi Dark Web üzerinden yapılmaktadır. Tehlikeli ve devletler tarafından- Tor kullanımın Türkiye'de yasaklanması da bu bağlamda değerlendirilmedir- şüpheyle yaklaşılan erişim alanı olan Dark Web ile birlikte başta Bitcoin olmak üzere sanal para birimi ile işlem yapılması ise birçok yasadışı faaliyetin izinin takip edilememesiyle sonuçlanmaktadır. Nca'ın raporunda da belirttiği üzere anonim ödeme sistemleri karanlık web ticaretinin tetikleyici durumundadır (NCA, 2016:7).

SONUÇ

Demokratik olan tüm toplumlarda aşırılık yanlısı terörizm, şiddetin teşvik edilmesi, çocukların istismarı, çocuk pornografisi, dolandırıcılık, kara para aklama, uyuşturucu ve sınırsız silah ticareti başta ahlaki değerler olmak üzere hukuk devletlerinin hepsinde yasalara aykırıdır. Bu bağlamda, internet ve ona bağlı yeni teknolojiler bu ahlaki değerleri ve yasaları yerle bir eden mimariler olarak –Dark Web'in- gayri meşruluğu teşvik edebilir mi? (Moore and Rid, 2016:9) Bu sorudan yola çıkarak gelecekte belki de en önemli sorun, bir toplumun internet kullanıp kullanmadığı değil, hangi versiyonunu kullandığı olacaktır (Erik ve Jared, 2015:96). Bu bağlamda da devletlerin, politikacıların ve karar verici kişilerin Deep Web'in güvenli bilgi sahası dışında kalan Dark Web ile mücadelesi büyük bir önem arz etmektedir. Uzaya insanoğlunun müdahalesinin zorluğu ne kadar ise Siber uzayda da aynı şartların var olduğu gerçekliğinden yola çıkarak devletler, özel sektör ve vatandaşlar arasında sağduyulu iş birliğinin önemi ve temel ahlaki, insan hakları ve evrensel prensiplerin oluşturulması ve geliştirilmesi, bu mücadele de temel yapı taşı görevindedir.

Yaşamlarımızın dijital enformasyon sistemleri ve buna bağlı olarak internet ile iç içe geçmesi arttıkça, her tıkla birlikte bireysel ve topumsal kırılganlıklarımız artmaktadır. Yakın gelecekte daha pek çok ülkenin ve insanın online yaşama katılmasıyla birlikte, bu kırılganlık genişleyecek ve şimdikinden daha karmaşık bir hal alacaktır (Erik ve Jared, 2015:118). Dolayısıyla, internet üzerinde gittikçe artan yasa dışı faaliyetlerin önüne geçmek adına atılan adımlar ülke vatandaşlarının internete olan erişimlerini kısıtlamak yerine bilişim sektörü ile karar vericilerin ortaklaşa geliştirecekleri yapıcı adımlar ve vatandaşların Dark Web ile Deep Web arasındaki

ayrım konusunda bilgilendirilmesi ve bilinç eğitimleri günümüz teknoloji şartları içerisinde yapılacak doğru bir hamle olacaktır.

Siber uzayda devletler, devlet dışı aktörler (özel şirketler) ve kişilerin ortak paydaş/aktör halinde bulunması yasal sınırlamaların etkin çözüm olmadığının/olamayacağının göstergesidir. Dolayısıyla, Deep Web ve Dark Web kavramlarının iç içe geçmesinden kaynaklanan çatışmanın önüne geçilmesi adına siber uzay güvenlik anlayışının etik ahlaki temellere oturtularak yasaklardan ziyade devlet politikası geliştirilerek güvenli hale getirilmesi bu soruna bir çözüm olarak düşünülmelidir. Siber uzayda fiziksel dünyanın dışındaki bir çatışma alanına dönüşen Dark Web'deki yasa dışı faaliyetler sürdüren kişilere karşı yalnızca Tor kullanımının yasaklanmasına dair yapılacak hamlelerin kısa sürede aşılabilir olması, etik ahlaki temellerin atılması vurgusunun en büyük makul argümanı şeklinde karşımıza çıkmaktadır.

Son söz olarak ifade edilmesi gerekir ise, çalışma boyunca karşılaşılan en büyük zorluklardan biri akademik manada beslenebilinecek kaynakların yoksunluğu olarak belirtmek mümkündür. Bunun temel nedenlerini üçe ayırabiliriz: İlk olarak Deep Web ve Dark Web hakkındaki bilgilerin birçoğunun internet ortamında asparagas haberlerden ibaret olması; ikinci olarak çalışma alanının genel itibariyle yazılım mühendisleri, bilgisayar mühendisleri ve veri analizcileri tarafından irdelenebileceği yanılgısının ortaya atılması neticesinde akademik olarak yazınsal ürünlerin ortaya koyulamaması ve son olarak ise devletlerin bu konuda gizlilik esasını gütmesi şeklinde sıralanabilmektedir.

KAYNAKÇA

Alistair Charlton (2014). "Snowden Files Reveal NSA had 'major problems' Tracking Tor Dark Web Users and Cracking Encryption", http://www.ibtimes.co.uk/snowden-files-reveal-nsa-had-major-problems-tracking-tor-dark-web-users-cracking-encryption-1481225, E.T: 11.10.2017.

Andy Beckett, (2009) "The Dark Side of the Internet", https://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet. E.T: 14.11.2017

Aydoğan, A. "Tor Network Türkiye'de Engellendi", http://www.webtekno.com/tor-network-turkiye-de-engellendi-h23134.html, E. T: 5.09.2017.

Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts and Stephen Wolff, (1997)"Brief History of the Internet ", Internet Society.

Jamie Bartlett, (2016). "Dark Net: İnternetin Yer Altı Dünyası", Konyalı, Y. (çev.). Timaş Yayınları, İstanbul. s. 15.

Brett Hawkins, (2016). "Under the Ocean of Internet", The Sans Institue

Cadie Thompson, (2015)."Beyond Google: Everything You Need to Know About the Hidden Internet", Business Insider, http://www.businessinsider.com/difference-between-dark-web-and-deep-web-2015-11. E.T: 11.11.2017.

Craig Labovitz, (2009). "The Dark Web Explained", https://witnessthis.wordpress.com/tag/craig-labovitz/. E.T: 23.11.2017.

Daniel Moore and Thomas Rid, "Cryptopolitik and The Dark Net.", Surival Vol.58 No.1 February-March, 2016.

Digital Citizens Alliance, "Busted, But No Broken The State of Silk Road And The DarkNet Market Places" Digital Citizens Alliance Investigative Report.

Eric Schmidt and Jared Cohen, (2015). "Yeni Dijital Çağ: İnsanların, Ulusların ve İş Dünyasının Geleceğini Yeni Baştan Şekillendirmek", Ü. Şensoy (çev).Optimist Yayın, İstanbul.

Ermiş, Uğur. "Saldırganın Geri Dönüşü: 1. Dünya Savaşı'ndan Siber Uzaya", 10.10.2014. ,https://siberbulten.com/makale-analiz/saldir-birinci-dunya-savasindan-siber-uzaya/, E.T: 2.09.2017.

FBI, “Manhattan U.S. Attorney Announces Seizure of Additional 28$ Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of “Silk Road” Website”. https://archives.fbi.gov/, E.T: 29.11.2017.

Internet Live States, (2018). Internet Usage & Social Media Statistics. http://www.internetlivestats.com. E.T. 01.01.2018.

Marco Chiappetta, (2016).“Access The Deep Web And Protect Your Privacy Online With The Anonabox”, https://www.forbes.com/sites/marcochiappetta/2016/04/29/access-the-deep-web-and-protect-your-privacy-online-with-the-anonabox/#6a922a6440c2, E.T: 9.12.2017.

NCA, ”National Strategic Assessment of Serious and OrganisedCrime 2016”, E.T: 20.11.2017.

Nicolas Christin, (2012). “Traveling the Silk Road: A Measurement Analysis of A Large Anonymous Online Marketplace”, Carnegie Mellon University Pittsburgh.

Gareth Owen and Nick Savage (2015). The Tor Dark Net”,Chatham House The Royal Institute of International Affairs, September.

Debiel Santos, (2017). “What The Dark Web Is And Isn’t”, Smart Data Collective, http://www.smartdatacollective.com/what-dark-web-and-isn-t/, E.T: 4.09.2017.

Vincenzo Ciancaglini, Marco Balduzzi, Robert McArdle, and Martin Rösler (2015). “Below the Sruface: Exploring the Deep Web”, Forward- Looking Treat Research Team, Trend Micro.

Zack Epstein, (2014). “How to Find the Invisible Internet”, BGR, http://bgr.com/2014/01/20/how-to-access-tor-silk-road-deep-web/.

CYBERSECURITY IN EDUCATIONAL SETTINGS

Ahmet YILDIRIM[*]

Abstract

Cyber security has gained currency recently since technology and internet started to play a pivotal role in our lives. Moreoever, as most of the organizations carry out their operations and store their work in cyber settings, the notion "cybersecurity" has become more significant. Educational settings are the places in which "cybersecurity" has gained importance as databases of educational settings involve the data about students, staff, parents, resources and budget. Furthermore, the fact that educational settings are the places in which new information is created and databases of educational settings include data about this new information renders educational settings more and more vulnerable to cyber threats. In addition to that, students as shareholders of educational settings may confront cyber threats such as cyber bullying more in their daily lives. In the present article, cyber security was defined, the aims of cyber threats were summarized. How vulnerable educational settings and students are to cyber threats was put forward. Lastly, what could be done so as to provide cybersecurity at the nation level and especially in educational setting was discussed.

Keywords: Cyber security, cyber threats, educational settings.

EĞİTİM ORTAMLARINDA SİBER GÜVENLİK

Özet

Teknolojinin ve internetin yaşamımızda daha fazla rol almaya başlaması ve pek çok kurumdaki işlerin siber ortamlarda yürütülmesi ve saklanmasıyla birlikte siber güvenlik, daha önemli bir konu haline gelmiştir. Siber güvenliğin önemli bir kavram haline geldiği yerlerden biri de eğitim ortamlarıdır. Eğitim ortamlarına ait veri tabanlarında; öğrenciler, personel, veliler, kaynaklar, bütçey ve bilginin üretildiği yer olarak üretilen bilgiyle ilgili pek çok verinin bulunması, eğitim ortamlarını siber tehditlerle karşı karşıya bırakmaktadır. Bununla birlikte, eğitim ortamlarının bir paydaşı olan öğrenciler siber tehditlerle, siber zorbalıkla gündelik yaşamda daha fazla karşılaşabilmektedirler. Bu yazıda, siber güvenlik kavramı tanımlanmış, siber tehditlerin amaçları ortaya konulmuş ve eğitim ortamları ile öğrencilerin siber tehditlere

[*] PhD, Ministry of National Education of Turkey. Can be accessed via yildirimahmat@yahoo.com.

karşı nasıl savunmasız oldukları tartışılmıştır. Son olarak da ülke genelinde ve özellikle eğitim ortamlarında siber güvenliğin sağlanması için yapılması gerekenlere kısaca değinilmiştir.
Anahtar Kelimeler: Siber güvenlik, siber tehditler, eğitim ortamları

Introduction

The information technology has developed recently and offered many opportunities and threats. Technology is everywhere and an integral part of life. However, information and computer technology is vulnerable to attacks. As a result, concerns about preserving information systems from cyber attacks have been addressed by many experts and policymakers (Fischer, 2016). According to Saluja, Bansal and Saluja (2012) we are getting more and more cyber generation. As a result, youth is getting more and more exposed to latest technology. This fact enables them to utilise the internet for different purposes. However, this also puts them at risk. With the onset of internet for personal purposes, there has emerged a new language. Computer pirates known as hackers investigated the mysterious world of the internet and demonstrated what could be done via the use of internet. The target of the hackers has sometimes been an individual internet user and sometimes corporates or pivotal institutions of the countries. The first hacking operations were conducted for personal interests. However, now hacking operations have posed a threat for countries' security and safety (Kara, 2013).

The principal elements of internet are computer, users and net. In the first years of development of internet, solely one computer could reach the main computer. The concept "net" emerged with the development of processors and communication protocols necessary for the access of two computers to the one computer simultaneously. With the development of "file transfer protocol" and "transmission control protocol", many users started to connect the main computer. With the development of wireless communication, net technology has gained much more importance (Bıçakcı, 2014).

Industrial age reigning 19th century was replaced with information age in the last quarter of 20th century. Capital, raw materials and workforce representing power in the industrial age were replaced with data and information in information age. As a result, information has become a factor of production and started to provide input for socioeconomic activities and facilities. Information age enables every kind of information (data, visuals, sounds etc.) to be expressed in numerical terms, stored and communicated in electronic spaces. Internet allowing numerical information to be communicated to various systems has been the dominant

technology in aforementioned technological facilities. Information age has led to many significant changes in many different parts of life and it rendered many critical infrastructures such as the fields of finance, electronic communication, transportation, energy, education and health dependent on itself (BTK, 2009). Critical infrastructures correspond to physical, technological services, systems that may influence the health, security and economic wealth if they are harmed. Information and communication are some of the critical infrastructures all around the world.

The fact that computers have been portable and access to internet has been common all around the world has been shaping the communication and exchange of information. Information technology makes people closer to each other, alters the communication habits. However, it may also cause unexpected problems (Bıçakcı, 2014). Organizations and institutions have become e-organizations and e-institutions with the use of network technologies. Schools and educational settings also provide many services on internet via internet pages (Çetin, Gundak and Çetin, 2015). The birth of cyber space has brought about many security risks for both individual users and national states. Those who organize cyber attacks may target financial institutions or they may capture national secrets and destroy the internet and national infrastructure (Bıçakcı, Ergun and Çelikpala, 2015).

Cyber Security and Cyber Crimes

The number of internet users has reached 2.3 billion. The number of internet users and the high dependence on internet have led to some security concerns. The first threats were about the physical infrastructure of internet. However, now the threats range from malicious codes and softwares to computer viruses. One of the problems faced within the framework of cyber security is the balance between freedom and cyber security. While trying to uphold cyber security, it is also necessary to keep the right to freely reach information and fight against cyber censorship (Öğün and Kaya, 2013). Cyber security refers to the all policies, security concepts, security instructions, approaches to risk management, training activities serving the aim of preserving the institutions in cyber spaces. The institutions, with the dependence on information technology, store the information about their personnel, infrastructure, practices and services in cyber space. Cyber security entails the formation of security properties in the way that resists security risks in cyber space. Moreover, the principal aim of cyber security is to ensure accessibility, integrity and confidentiality of information. Accessibility of information refers to

the reachability of information when the need arises even if the malicious cyber attacks occur. The integrity of information refers to the completeness and remaining of information unchanged. Especially for the sectors that are sensitive to the correctness of the information such as health and industrial design, the integrity of information is vital. The confidentiality of information corresponds to the prevention of the information from being captured by the unauthorized people (BTK, 2009).

Bardas and Ou (2013) assert that cyber security has become a priority for nations and organizations. Cyber security is a term that entered our lives in the post-cold war in a reaction to a mixture of technological developments and altering geographical conditions. Cyber security was first coined by computer scientists in the very beginning of 1990s so as to highlight a variety of insecurities relevant to networked computers (Hansen and Nissenbaum, 2009). Cyber security is the capacity to preserve and defend an institution's use of cyber space from a cyber attack committed via cyber space with the objective of "disrupting, disabling, destroying or malevolently controlling a computer environment/infrastructure; or destroying the integrity of the data or stealing controlled information" (IIROC, 2015).

Cyber crimes take place in Turkish Criminal Law under the heading of "Crimes in Information Technology". In the legislation, it is stated that the capture of computer programmes, data or other elements from a computer illegally or using, transferring or copying these data sources in contrary to law is a crime (Bıçakcı et al., 2015). In order for the precautions against cyber attacks to be successful, national policies and strategies should be developed (Yılmaz and Sağıroğlu, 2013).

The amount of data continues to increase without stopping. Businesses are getting basically more and more dependent on information technologies. Cyber criminals are aware of these susceptibilities. Cyber criminals are driven by lots of motivations to cyber attack such as obtaining financial gain, raising the profile of an ideology and terrorism. Individual cyber criminals, activists or organized hackers and states are attacking government and corporate networks with increasing frequency (KPMG, 2014).

Aims of Cyber Threats and Crimes

Cyber crimes include sexual crimes, child abuse and terrorism (New York State Office of Homeland Security and New York State Board of Education, 2004). Cyber threats consist of cyber attacks and cyber crimes committed in cyber space. Cyber threats could be categorized to five subgroups (BTK, 2009; Öğün and Kaya, 2013):

- Denial of service,
- Malicious software,
- Phishing,
- Spam e-mail,
- Monitoring the network traffic.

Denial of service attacks render information technologies busy via data traffic and make the provision of services impossible. Malicious software could be grouped as the following:

- Computer viruses,
- Worms,
- Trojans,
- Key logger software,
- Adware sent for commercial purposes,
- Spyware used for collecting information for the purpose of intelligence.

Computer viruses are software programs involving codes which are possible to give harm to the confidentiality, integrity and accessibility of data stored in computers. They can reach other computers and they are contagious.

The ultimate aims of cyber threats are the following (BTK, 2009):

- Unauthorized access to information and communication systems,
- Replacement, elimination and disclosure of data,
- Denial of the service.

Cyber threat is not only about a cyber attack, harm or an undeserved gain as a result of this attack. In addition to that, internet may be used by cyber terrorists as a means of communication and propaganda (Öğün and Kaya, 2013).

IIROC (2015) defines the risks of cyber threats as the following:

- Disclosure of confidential account or customer data- risking an institution's most valued relationships,
- Counterfeiting,
- Loss of cognitive and mental property,
- Destruction of central infrastructure,

- Financial loss,
- Devastation of financial organization's cyber assets,
- Causing embarrassment and reputation risks for organizations.

Both the accessibility and distribution of the numerical information available in information technologies and the increase in infrastructures and systems dependent on information technology has made information technology vulnerable to cyber risks and attacks. Dependence on information technologies has posed a threat for social, political, economic and military institutions. Therefore the magnitude of cyber attacks and risks has made the concepts "cyber security" and "protection of critical information and infrastructures" central issues in the field of information technology (BTK, 2009).

The cases of cyber threats occur as in the following (Öğün and Kaya, 2013):

- The deletion of main pages of internet sites which are accessible to public,
- Capturing the files available in the aforementioned internet sites and stealing them,
- Changing the available files,
- Making the internet sites unaccessible by cyber attacks,
- Loading viruses or malicious software to the personal or institutional computers,
- Conducting cyber propaganda or disclosing confidential information about institutions.

Cyber Security and Schools

As the significance of electronic information and network technologies improve, cyber security is increasingly getting more and more pivotal for the success of all institutions (Universities UK, 2013). Cyber security in internet use is a fact that emerged after the design of internet. Internet is a system that is based on the fact of accessibility. So, while internet was developed, the developers gave priority to user-friendliness, cost-effectiveness and universality. The developers of internet did not consider the fact that internet users may give harm to internet systems (Öğün and Kaya, 2013).

Security of data and information is exceptionally vital for all businesses. Many businesses keep the records of customer information, personal files, bank account details. Schools keep the records of students, their personnel, families of the students. If these records were captured by criminals or hackers, it could be have dangerous results.

Electronic data is in the heart of a university's facilities. As a result of this fact, protection and safety of this electronic data is pivotal for a number of reasons (Universities UK, 2013):

- Universities produce data as a core intellectual resource that is required to be kept, reached and utilised decently to understand its academic value,
- Universities depend on attainability to sensitive data from third-party organizations such as clinical data which is supplied by medical institutions,
- Universities collect data relevant to their work stuff such as data about students, budgets or personnel.

As a result of the fact that schools and universities are the producers and users of massive data sources, they are more vulnerable to cyber threats and attacks. That's why, it is necessary for them to develop cyber security facilities.

Saluja et al. (2012) recommend a curriculum of cyber security to be implemented at schools. The curriculum should include the following:

- Cyber threats,
- How users can preserve themselves and their computers,
- Cyber ethics,
- Cyber crimes.

Now in Turkey many schools have internet access, computer labs and multimedia learning centers. To be able to make learning and teaching more effective, most schools were provided with internet access services. However, there are many risks that cyber space brings about.

Cyber Security and Students

Cyber crimes have risen recently. Most of the students are unaware of the risks internet poses for them. As a result, the students are more vulnerable to cyber attacks and threats. They share lots of information, pictures in social media and other cyber spaces. However, they need to think before sharing. They need to use strong passwords and backup their data.

Given the fast and constant increase of cyber threats to schools; organizations and institutions urge the relevant people to develop security education and awareness programs that are persistent and compelling (Payne, 2003). Cyber security in the educational settings include many components. They include the privacy and security of personnel and student information and administrative information such as financial systems, grades of the students and confidential correspondence between school administration and other stakeholders (New York State Office of Homeland Security and New York State Board of Education, 2004).

Cyber-stalking, cyber bullies and sexual harassment in internet are also threats for students. The malicious people may create fake identities in internet. The students are susceptible to these threats. Moreover, cyberbullying is also a problem students confront in especially social media.

The anonymity of the internet causes the exploitation of the students (New York State Office of Homeland Security and New York State Board of Education, 2004).

The Provision of Cyber Security

The magnitude of dependence on cyber space and internet has made cyber security indispendable for institutions and nations. It is nearly impossible to detect those who conduct cyber attacks because the cyber attackers rarely leave traces behind them and even try to hide their own locations (Bıçakcı et al., 2015).

Cyber security is an immature field. There is a lack of trained personnel in this field. So, the first thing to do against cyber threats is to raise awareness in individual and institutional level. Moreover, cooperation of schools with other institutions may provide exchange of information about precautions about cyber security.

Erol, Şahin, Yılmaz and Haseski (2015) and IIROC (2015) recommend the following in order to keep cyber security high:

- Having an antivirus program,
- Keeping security software up to date,
- Having complex passwords,
- Making a backup of the files in the computers,
- Deleting insecure e-mails,
- Keeping away from sharing private pictures in social media,
- Keeping away from doing shopping based on the advertisements in social media sites,
- Appealing to the law in case of cyber threats.

As software-based precautions are not sufficient, the physical infrastructure of internet should be protected as well (Öğün and Kaya, 2013). To reach schools' information technology security purposes, it is necessary to take security precautions on the following different security controls (The Government of the Hksar, 2007):

- Physical security – preventing direct access from circumventing cyber security,
- Access control – preventing unauthorized reach to system resources.
- Data security – preventing data from destructive viruses, power failure, software failure and malicious software,
- Network and communication security – monitoring internet users at schools,
- User awareness and education – providing education and training for internet users.

Moreover, internet users should get training in the field of firewall and port. Web applications should be constructed in a very secure way that is out of reach for irrelevant users. Softwares

should be developed in a secure way and confidentiality of source codes shouldn't be violated. Private sector and public sector should cooperate to eliminate the risk of cyber threats. Schools or educational institutions should get technical support from private companies or competent institutions (Öğün and Kaya, 2013).

Training is one of the effective ways of fighting against cyber threats. The equipment of personnel, students and teachers with information about cyber security in both individual and institutional level may minimize cyber threats. Risk assessment and probable cyber attacks should be anticipated and possible action plans should be developed. Bardas and Ou (2013) argue that setting up a cyber security lab so as to give the students the possibility to realize various offensive cyber security activities is necessary. Moreover, they argue that cyber club could be set up and cyber defense courses might be planned. In the club, hands-on activities and tools could be used. Moreover, schools may prepare cyber security action plans, security programs aiming to preserve school or school-related internet pages from cyber threats or attacks. Furthermore, cyber security intervention teams may also be established. Limited information or data could be shared with the outsiders.

Tikk (2011) recommends ten rules for cyber security. They are listed as the following:

- *The territoriality rule*: Territoriality tenet makes institutions and nations more powerful to foist their dominance on information infrastructure taking place within their terrain.
- *The responsibility rule*: It refers to the fact that a cyber attack that has been performed from an information system taking place in a state's terrain is an evidence showing that the act could be attributed to that state or institution.
- *Cooperation rule*: It refers to the fact that a cyber attack which has been committed via information systems taking place in a state's terrain leads to the duty to collaborate with the victim state.
- *The self-defence rule*: Every nation and organization has the claim to self-defence.
- *The data preservation rule*: The data available in an internet site of an institution or an organization should be perceived as personal unless they are supplied for other people or organizations.
- *The mission of "care rule"*: Every organization has the charge to implement a reasonable level of cyber security in their organizational information infrastructure.
- *The early warning rule*: It is necessary to warn possible victims about unknown and probable cyber threats.

- *The attainability to information rule*: The public has the right to be made knowledgeable about the threats to their life and safety.
- *The delinquency rule*: Every nation has the duty to involve the most prevalent cyber crimes in their criminal and delinquency law.
- *The mandate rule*: Every institution has the duty to cooperate and coordinate in global cyber security.

If schools are designed as e-organizations, security systems should be established by taking into consideration the following (Çetin et al., 2015):

- The users should be identified,
- Access to the systems should be controlled,
- Alternative servers should be used,
- Users should be monitored,
- IP addresses of computers should be kept.

New York State Office of Homeland Security and New York State Board of Education (2004) recommends schools to pay attention to the following:

- Protect your user ID and password and change it constantly,
- Never share your password with anyone and don't write it down,
- Create a strong password that is difficult to guess,
- Don't reuse your previous passwords.

Conclusion

As educational settings have become more and more dependent on cyber space, they have accordingly become more and more susceptible to cyber threats. The magnitude of the data educational settings keep in their data base and the students of these educational settings who are vulnerable to cyber threats motivate cyber criminals to target educational settings. In order to protect educational settings and students from cyber criminals and not to short-circuit educational facilities, cyber precautions aforementioned should be taken.

REFERENCES

Bardas, A. G. and Ou, X. (2013). *Setting up and using a cyber security lab for education purposes*. Retrieved December 30, 2017, from http://people.cs.ksu.edu/~bardasag/publications/cdc2013.pdf

Bıçakcı, S. (2014). Nato'nun gelişen tehdit algısı: 21. yüzyılda siber güvenlik. *Uluslararası İlişkiler*, 10(40), 101-130.

Bıçakcı, S., Ergun, D., Çelikpala, M. (2015). *Türkiye'de siber güvenlik*. Ekonomi ve Dış Politika Araştırmalar Merkezi. Technical report.

BTK (2009). *Siber güvenliğin sağlanması: Türkiye'deki mevcut durum ve alınması gereken tedbirler*. Bilgi teknolojileri ve iletişim kurumu raporu.

Çetin, H., Gundak, İ. and Çetin H. H. (2015). E-işletme güvenliği ve siber saldırılar üzerine bir araştırma. *Çankırı Karatekin University Journal of Institute of Social Sciences*, 6(2, 223-240.

Erol, O., Şahin, Y. L., Yılmaz, E. and Haseski, H. İ. (2015). Personal cyber security provision scale development study. *International Journal of Human Sciences*, 12(2), 75-91.

Fischer, E. A. (2016). *Cybersecurity issues and challenges: in brief*. Congressional Research Service Report.

Hansen, L. and Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly*, 53, 1155-1175.

IIROC (2015). *Cybersecurity best practices guide for IIROC dealer members*. Technical report.

Kara, M. (2013). *Siber saldırılar – siber savaşlar ve etkileri*. (Unpublished master's thesis). İstanbul Bilgi University, İstanbul.

KPMG (2014). *Cyber security: it is not just about technology. The five most common mistakes*. Report. Sweden.

New York State Office of Homeland Security and New York State Board of Education (2004). *Best practices for school safety and security*.

Öğün, M. N. and Kaya, A. (2013). Siber güvenliğin milli güvenlik açısından önemi ve alınabilecek tedbirler. *Security Strategies*, 9(18), 145-181.

Payne, S. (2003). Developing security education and awareness programs. *Educause Quarterly*, 4, 49-53.

Saluja, S., Bansal, D. and Saluja, S. (2012). Cyber safety education in high schools. *International Conference on Computer Technology and Science*, 47, 107-112.

The Government of the HKSAR (2007). *Information technology in education project, IT security in schools*. Education Infrastructure Division Education Bureau.

Tikk, E. (2011). Ten rules for cyber security. *Survival*, 53(3), 119-132.

Universities UK (2013). *Cyber security and universities: managing the risk*. Retrieved December 31, 2017, from http://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2013/cyber-security-and-universities.pdf

Yılmaz, S. and Sağıroğlu, Ş. (2013). *Siber güvenlik risk analizi, tehdit ve hazırlık seviyeleri*. Paper presented at the 6th International Information Security and Cryptology Conference. Ankara, Turkey.

OPINIONS / YORUMLAR

RETHINKING CYBERSECURITY : A QUICK TRANSFORMATION

Nezir AKYEŞİLMEN[*]

Cybersecurity has been a popular concept and widely used in media and academy in recent years. It has both technological and social dimensions. It is so important that should not be left to the technicians alone. The individuals, politicians and decision-makers need to deal with it and take proper measures. Cyber failure is not only technical but much more political. Therefore, we need policies that aim to provide a safe cyberspace.

Transformation of International Conflict Trends

Even though there is no general consensus on the definition of conflict, it is widely accepted that the idea involves a wide range of things ranging from a simple ideas conflicts to wars. In this framework, conflicts can be classified into different forms. For instance, in a broad sense, violent and non-violent conflicts; or they can be examined in five categories: first two groups are latent/hidden (disputes) conflicts and manifest/conflicts (non-violent crisis). There is no physical violence in these two conflicts. The third group is crisis or violent crises. The fourth and fifth are limited wars (severe crisis) and wars. Another classification can be in the form of interstate and intra-state conflicts.

The trend of world conflicts changes from time to time according to technological, economic, cultural and political development at the global level. In general, the number of violent and non-violent conflicts in the world is close to each other. But from time to time this number has increased in favor of one. Especially during the post-Cold War period, the number of conflicts has declined in general (the number has fallen below 100 in the whole world in 1990s), especially in interstate conflicts. As of today, 189 of the 409 conflicts that exist in the world are non-violent, while 223 are violent ones. Of these, 180 are violent crises, i.e violent rarely appears. Only 71 of these conflicts are among the states, while 338 are within the states. 42 of them have intense violence that can be accepted as wars (both limited and full wars). And most importantly, none of these take place between the states. And yet none of the 42 conflicts occurs in democratic countries. All intense violent conflicts occur in non-democratic or semi-democratic countries. Only 10 out of 180 violent crises are among the states.

[*] Assoc. Prof. Dr., Department of International Relations, Selçuk University, Konya-Ankara. Can be accessed via nezmen@yaho.com

In summary, the trend of conflicts in the world is as follows. The number of conflicts is increasing. In the last 20 years the number has increased fourfold. Conflicts are increasingly being drawn into the state. More than 80% of the conflicts in the world are in the state. There is little or no violence in the conflicts between states. Likewise, in democratic countries conflicts either never exist or do not involve violence. In other words, democracy is a system with the ability to solve social and political conflicts without violence.

In recent years it has also been mentioned about cyber conflicts. This new type of conflict will affect the world's conflict trend. Before gong details, I would like to focus on the concept of "Cyber war", which is discussed extensively in the cyber policy literature. Some analysts both on the cyber-technical side and on the political side use this concept in an unreasonable and unnecessary way. If conflict management and international legal literature are taken into consideration, the concept of “cyber war” seems to be meaningless and unnecessary today. Why? Because, war is the most violent type of conflict that also contains high physical damages. However, there has not been any cyber attack from that have been made up to now, except for the Stuxnet (limited range), which causes physical damages. First of all, the concept of "cyber warfare" is a harmful concept that serves a security mindset that helps to securitize the cyberspace. It is a usage that gives the greatest damage to human rights and freedoms of the individuals. It is not innocent or ignorant. Then why do some people like to use the concept of "Cyber warfare"?

One reason is the effort to show that the area very important. Cyber space is already important, people feel it in their daily life. But they only damage the area by securitizing it. The second is to attract attention. The third is intended to serve relief, that is, securitization and ultimately from ignorance. Since, in international law and conflict management disciplines, such conflicts can not be defined as war on any criteria. If the nature of these attacks changes tomorrow, they can be accepted in the war category, but today there is no such conditions.

Technically cyber attacks are also cyber conflicts. Cyber conflicts are usually continuation of a kinetic conflict. There are too many types of cyber conflicts. But the ones that can be considered as cyber political conflicts are numerous. They are also quite effective on global politics and security policies. Unfortunately, globally, cyber conflicts have not been shown in world conflict maps or barometers yet. But they will be taken into consideration in the near future. Cyber conflicts will affect the world's conflict trend in a significant way. As can be seen in the statistics given above, the number of violent conflicts between states is very small in the world. This is

quite understandable, as states are avoiding it because a conflict involving interstate violence has a great deal of destructive power. I mean, there is some kind of deterrence in that sense. But since cyber conflicts do not involve physical violence as of today, the likelihood of such conflicts increasing at an international level is very high. The simplest example of cyber attacks alleged today for the US elections continued between the US and Russia. Similarly, cyber intelligence tensions between China and the US is on the agenda. Since these conflicts do not involve violence, as between states and non-state actors, the number of such conflicts will increase from day to day and unfortunately will often trigger other conflicts involving physical violence.

The world is heading towards a hybrid conflicts that have cyber and physical dimensions. Cyber conflicts are increasingly affecting our lives and continue to grow at a pace that will also impact international conflict and security trends.

Towards a Global Cybersecurity Question

Considering the effects of cyber conflicts on humanity, the concept of cybersecurity has become an important component of national and international security, targeting the infrastructures that have reached a rather deadly and destructive stage in recent years, not only individuals or private companies, but also social service sectors. A code can create a global chaos. How vulnerable is an environment such a fragile system? With a simple software program, planes can be prevented to fly. Digital machines can be controlled or taken out of control. Can not this all be a doomsday for people?

The concept of cyber security has become a very popular concept in recent years due to the hacking of big companies like Yahoo, BBC, Paypall, Amazon and recent discussions on US elections. Even though it was an important issue, people could not realize it before they were exposed to the cyber attack, and they regarded it as insignificant. But now, cyber security has become an important security question that includes national and international security beyond just a secure cyberspace. 2007 Estonia, 2008 Georgia, 2010 Stuxnet virus and 2011 Israeli attack on Syria are the clearest examples of this.

What is the cybersecurity? Is a full cybersecurity possible?

Everyone uses the concept of cybersecurity in different meaning and for different purposes. There is no globally accepted definition on the world, as there is no agreed agreement on this issue. The National Cyber Security Strategy and Action Plans of each country make different definitions. Naturally different definitions force each to take different measures, even though some are similar.

The problem is not just that everyone has different definitions. The problem is that no one question this concept. Everyone receives the concept of security of cyberspace as a given concept and accepts their definition as the most accurate one. But no one asks the question of who security? What types of security? and how to manage it? These are the questions that should be asked in national strategy action plans. In addition, academic studies continue with the same infertility.

The national action plans and literature heavily focus on the information and network security. However, the user is the most important component of cyberspace. Unfortunately, in the literature, the user in that sense, is generally ignored. While discussing the IP / TCP layers of the Internet the use, is constantly being emphasized as the most important layer or component of the internet, yet this element is kept out of sight in security debates.

For this reason, the vital question is the security for whom? If we proceed in this direction, a more healthy definition and series of measures can be developed. The measures that can be accepted by all cyberspace stakeholders. The stakeholders of cyber space are people, private companies and states. But today's global system, states alone can make decisions on behalf of other stakeholders. For this reason, they can not fully implement the decisions they make. Why? Because, unlike physical spaces, the dominant actors of cyberspace are not the states anymore. I.e. the cyberspace is not a state-centric environment. For this reason, if cyber is to be secured in the world, the states will not act on their own but will act jointly with other stakeholders. Such a strategy, taken into consideration all stakeholders' demands and requests, can only provide cybersecurity. In the world of cyberspace, national security is not possible without ensuring the safety and freedom of the individual. To shot down internet is not a cybersecurity measure. It's an indication of inadequacy. This is usually done by third world countries where the cyber Know-How is too weak or does not exit.

The main objective of cybersecurity is confidentiality, Integrity and accessibility (CIA) of information. The interruption of access means that there is no cybersecurity. Security, accessibility and privacy are at the same time human rights and freedoms. No cybersecurity

measure that does not target the protection of human rights and freedoms can provide real security. Just like in real life.

Evolution of Cybersecurity

The digital world or cyberspace with its most common name, continues to influence our daily life. Alongside the benefits and opportunities it has provided in recent years for the individual, institutional, national and global actors, it has brought threats and weaknesses, especially in security sector.

More than half of the world's population, 3.8 billion people use the internet today. Worldwide, the number of websites hits 1.3 billion today, despite the first was opened in 1991. More than 200 billion e-mails are sent on average per day. Again, five million smartphones are sold per day (source: internetlivestats.com). 1.2 billion machines are connected to the internet today and it is expected to reach 10 billion by 2020. Online trade volume has exceeded 10 trillion dollars. Smart houses, intelligent cars, intelligent home tools and devices, intelligent machines and robots are the benefits that facilitate, accelerate, and comfort people's lives.

But it should not be forgotten that every vehicle connected to the Internet creates a security vulnerability. Because everything is increasingly connected to the internet, and as a result everything becomes available for hacking. The number of daily malware or daily viruses in the world is over 500. The number of attacks is expressed in millions. An average of 50 thousand websites is hacked every day. These are pretty big and scary figures.

Cyber attacks can also adversely affect or prevent public services (attacks on critical infrastructures) and private services (especially attacks on finance and energy infrastructures), that also threaten the confidentiality, integrity and accessibility of information. In recent years, cybersecurity has become increasingly a national and global security problem. Cybersecurity has gradually become a global security issue today.

In the early days, cyberspace was seen as a low politics area such as entertainment, economy and communication, but in recent years this area has been seen by states as a high politics area such as security, strategy and military. One of the most important questions in cybersecurity as stressed above is whose security? Although the answer to this question has changed over time, it still has not found a healthy answer today.

The Internet was built on information sharing and transparency from 1969 until 1988 (the first virus appeared in 1982 though was not used in an attack that would cause harm). But in 1988, when Morris worm was produced and left on the Internet, it damaged thousands of computers in the United States. For this reason, cybersecurity in the 1990s was perceived more as a problem of personal information security. Then, in 2000, a 15-year-old student made DDoS attacks on global corporations such as CNN, Yahoo, e-Bay, and Amazon, destroying them and damaging billions of dollars after which, cybersecurity has become an important corporate security issue for private companies. However, in 2007, DDoS attacks on Estoya, Israel's control of the Syrian radar system, Russia's resorting to cyber attacks with physical attacks in Georgia in 2008, and finally, as the first cyber weapon the Stuxnet, produced for attacking Iran's nuclear facilities, the state has then begun to perceive cybersecurity as a national and international security problem.

Today, cybersecurity has become a crutial component of global security. For this reason, countries have been publishing National Cyber Security Strategy Documents in recent years and are making huge investments in cybersecurity. Defence units are set up in the face of cyber armies and cyber attacks (made up of hackers).

In the last National Security Strategy document of the United States, cyber space has been considered under the heading of international security and is described as a major threat. The document, which emphasizes that cyber conflicts have become an important issue of international security, mentioning of measures to be taken in for this purpose.

To sum up, cyber space, seen as a world of opportunities, has now become a space that also contains significant threats. This area, which generates security issues from the individual level to the global level, is also an important power tool at the same time. For this reason, nobody can give up on it. The most important measure for safe use of cyber space is personal consciousness and national cyber policies. Because the weakest link of cyber security is the user, the individual. Again, cyber security failure is far more political than being technical. That is, lack of appropriate and applicable policies. Perhaps the most important and crucial point is that cybersecurity can only guaranteed via morality or ethics. Just as morality is in the physical world, in the cyber world it is also the most important indicator and guardian of our humanity.

In short, cybersecurity is a relatively new issue, but has been very popular concept and effective at the global level. In order to catch up with social, economic and political measures need to be

taken along side with the technical and technological improvements. Policies are as important as technological innovations.

SİBER UZAY VE ULUSLAR ARASI İLİŞKİLER / TEORİSİ

Müberra ALTINER[*]

Fatma ÇAKIR[**]

Siber Uzay ve Uluslararası İlişkiler/ Teorisi Çalıştayı, Cyber Politik Journal, Orta Doğu Teknik Üniversitesi ve Selçuk Üniversitesi ortaklığı ile 11 Aralık 2017 tarihinde gerçekleştirilmiştir. Çalıştay iki oturumdan oluşmuş, ilk oturumda açılış konuşmasını Prof. Dr. Hüseyin Bağcı yapmıştır. Moderatör, Prof. Dr. Özlem Tür olurken, konuşmacılar ise, Dr. M. Emin Erendor (Çukurova Üniversitesi, Cyber Politik Journal) ve Doç. Dr. Nezir Akyeşilmen (Selçuk Üniversitesi, Cyber Politik Journal)'dir. Konuşmacıların sunum başlıkları ise, sırasıyla, 'Siber Uzayın Temel Kavramları' ve 'Siber Uzay ve Uluslararası İlişkiler/ Politika' dır.

Çalıştayın ikinci oturumunun moderatörlüğü ise Prof. Dr. Bilal Sambur (Yıldırım Beyazıt Üniversitesi, Cyber Politik Journal) tarafından yapılmıştır. Konuşmacılar sırasıyla, 'Siber Uzayın Felsefesi' konulu sunumu ile Prof. Dr. Mustafa Çevik (Ankara Sosyal Bilimler Üniversitesi) ve 'Teknoloji ve Uluslararası İlişkiler Teorisi' adlı sunumu ile Prof. Dr. Davut Ateş (Selçuk Üniversitesi) olmuştur.

'Siber Uzayın Temel Kavramları' adlı sunumunda Dr. M. Emin Erendor'a göre (Çukurova Üniversitesi, Cyber Politik Journal) siber kavramının tek başına bir anlam ifade etmemekte, literatürde yeni olan bu kavram, yanına aldığı eklerle anlamlı hale gelmektedir. Bunun yanında, antik Yunan kökenli bu kelime rehberlik etmek, kontrol etmek anlamları taşımaktadır. Siber kelimesi ilk kez 1958 yılında Louis Couffignal tarafından kullanılmış olmakla beraber, 1984 yılında William Gibson'ın Neuromancer adlı romanında siber uzay kavramını kullanımı ile kavramın kullanımı yaygınlık kazanmıştır. Siber Uzay kavramını tanımlayan Erendor; bilginin elektromanyetik formda oluşturulması ile başlayıp dünyanın dört bir yanını kuşatan çeşitli sistemler vasıtasıyla bilgiye erişimin sağlandığı sanal ortamın bütünü olarak tanımlamaktadır. Ancak bu tanımdan farklı olarak ABD Hava Kuvvetlerinin siber uzayı tanımlarken; ağ sistemleri ve fiziksel yapılar üzerinde veri depolamak, değiştirmek ve geliştirmek amacıyla

[*] Yüksek Lisans Öğrencisi, Selçuk Üniversitesi, İİBF Uluslar arası İlişkiler Bölümü.

[**] Arş. Gör., Selçuk Üniversitesi, İİBF Uluslar arası İlişkiler Bölümü.

elektronik ve elektromanyetik spektrumun kullanılması olarak tanımlama yoluna gittiğini de belirtmiştir.

Erendor, siber suçları siber uzayın bileşeni olan bilişim sistemleri ile bu bileşenlere karşı işlenmiş suçların bütünü olarak tanımlar. İnternete bağlı herhangi bir bilgisayar sisteminin ya da ağının diğer bilgisayar sistem/ağlarına karşı kötü maksatlı eylemler gerçekleştirmek amacıyla kullanılması, klasik suçların yeni teknolojik imkanlar kullanılarak işlenmesi de bu kapsamda değerlendirilmektedir.

Erendor, siber saldırıları; bir web sitesine, bilgisayar sistemine, bilgisayarların gizliliğini, bütünlüğünü, erişilebilirliğini veya içinde depolanan bilgiyi tehlikeye düşüren tek bir bilgisayara (toplu olarak bir bilgisayar) karşı yapılan saldırılar olarak tanımlamıştır. Siber saldırı çeşitlerini sıralayan Erendor; bir bilgisayar sistemine yetkisiz erişim kazanmaya çalışma, hizmetin bozulması veya reddi saldırıları (DDoS), bir web sitesini kesmek, virüs veya kötü amaçlı yazılım yüklemesi, verilerin işlenmesi için bir bilgisayarın yetkisiz kullanımı, bir şirketin çalışanları tarafından bilgisayarların/uygulamaların şirkete zarar verecek biçimde uygunsuz kullanılması örneklerini verir.

Siber terörizm konusunda Erendor; siber uzay ve terörizmin birleşimi şeklinde bir tanımlama yapar, siyasi/sosyal mercilere, kişilere gözdağı verip baskı oluşturmak maksadıyla, resmi birimlerin bilgisayarlarına, network sistemlerine, bilgi ve veri tabanlarına yapılan yasa dışı tehdit veya zarar verici saldırılar olarak belirtmiştir. Siber terör; ölümcül olan ya da fiziksel hasara yol açan, şiddetli ekonomik kayba neden olan saldırılar olarak örneklendirilebilir.

Siber savaş ise Erendor'a göre, bir devlet tarafından başka bir devletin bilgisayar sistemlerine veya ağlarına hasar vermek ya da kesinti yapmak üzere gerçekleştirilen sızma faaliyetleridir. Ayrıca ekonomik, politik, askeri veya psikolojik amaçlar için hedef seçilen ülkeye yönelik bilgi ve iletişim sistemleri üzerinden gerçekleştirilen organize saldırılar olarak tanımlanabilir.
Siber casusluk; kullanıcısının bilgisi dahilinde olmadan, bireysel kullanıcıların, firmaların, kurum ve kuruluşların bilgilerinin, internet veya internet üzerinden siber taarruz yöntemleri kullanılarak kişisel, askeri ve ekonomik amaçlar için elde edilmesidir.

Siber istihbarat; bir yandan bilgileri toplayıp analiz yaparak, karar vericilerin önünü aydınlatmak şeklinde tanımlanırken bir yandan da karar vericilerin belirlediği politikalar

doğrultusunda, psikolojik harekat, propaganda gibi yöntemler kullanarak toplumların algılarını yönetmek olarak ifade edilebilir.

Siber güvenlik; siber ortamda, devlet, kurum, kuruluş ve bireysel kullanıcılar tarafından güvenlik amaçlı kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik talimatları, klavuzlar, risk yönetim yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür. Kurum, kuruluş ve kullanıcıların varlıkları, bilgi-işlem donanımları, personeli, altyapı ve uygulamaları, hizmetleri, telekomünikasyon sistemleri ve siber ortamda iletilen veya saklanan bilgilerinin tümünü kapsamaktadır.

İlk oturumun ikinci sunumu 'Siber Uzay ve Uluslararası ilişkiler/Politika' konulu sunumu ile Doç. Dr. Nezir Akyeşilmen (Selçuk Üniversitesi, Cyber Politik Journal) tarafından yapılmıştır. Akyeşilmen'in verdiği bilgilere göre, günümüzde; internet kullanıcısı: 3.794 milyarken, ilk web-sitesi-1991 yılında oluşturulmuştur. İlk e-mail: 1971 yılında atılırken bugün günlük olarak 250 milyar e-mail atılmaktadır. Dünyanın en ünlü arama motoru Google'da günlük 5 milyar arama yapılmaktadır. Dünya üzerinde günlük blog yazısı: 5 milyonken, günümüzde toplam facebook kullanıcısı: 2,055 milyara ulaşmış durumdadır. Günlük olarak hacklenen web-sitesi sayısı 90 bini bulurken, dünya üzerinde günlük olarak satılan akıllı telefon sayısı 4 milyonu bulmaktadır. (Kaynakça; http://www.internetlivestats.com/)

Akyeşilmen sunumuna bir soruyla başladı: Siber uzay hayatımızın ne kadarını kapsıyor?
Siber küreselleşme kavramının tanımını yapan Akyeşilmen, küreselleşmenin dünyayı bir köy haline getirdiğini ancak bunun ötesinde siberin dünyayı bir apartman haline getirdiğini ifade etmiştir. Buna göre, artık herkes herkesle komşu, mesafe ve sınırlar ortadan kalkmış durumda. Siber uzay ve politika ilişkisini ifade eden Akyeşilmen, siber güven(siz)lik sorunu ya da siber başarısızlık teknik bir başarısızlık değildir. Politik başarısızlığın sonucudur. Yani fonksiyonel ve stratejik politikaların zayıflığıdır.(Lewis, 2013). Nedeni ise, siyasi ve bürokratik elitin ve karar alıcıların siber uzay konusunda az bilgi sahibi olmalarındandır. Siber güvenlikte en zayıf halka kullanıcıdır, yani bireydir ve bireylerin siber güvenlik konusundaki bilinç ve bilgi düzeyleri düşüktür.

Akyeşilmen, siber uzay ve uluslararası ilişkileri, literatür, çalışmalar ve konular üzerinden ele almıştır. Uluslararası İlişkilerde siber literatür; 2001-2010 tarihleri arasında 26, Uluslararası İlişkiler dergisinde Siber ile ilgili yayımlanan makale sayısı 49'a ulaşmıştır. (Reardon ve

Choucri, 2013). Bugün; Siber Çalışmalar, Oxford Uİ Siber Çalışmalar Programı, Charles Sturt University – Siber Çalışmalar ve Araştırmalar Master Programı, International Hellenic University – İletişim ve Siber Güvenlik YL programı, ABD Deniz Akademisi – Siber Güvenlik Çalışmaları Programı, The Centre for Strategic and International Studies(CSIS) – Güvenlik programı altında -Advanced Cyber Studies bulunurken Avrupa ve Amerika'da birçok üniversitede siber politika dersleri verilmektedir.

Siber Uzay ve Uluslararası İlişkiler/Politikalar noktasında ise Akyeşilmen, siber uzay çalışmalarının inter-disipliner olmakla birlikte sosyal bilimlerde daha çok Uluslararası İlişkiler'in alanına girdiğini ifade etmiştir. Uluslararası ilişkilerin belli başlı kavramları ve siber uzaya bakıldığında, siber uzayın anarşik doğası dikkat çekmekte ve siberin merkezi neresidir? sorusu gündeme gelmektedir. *Yine bu noktada belli başlı konu başlıkları ve bunlara yönelik bir takım soruların cevaplarının verilmesi gerektirmektedir. Bunlar genel manada şu şekilde sıralanabilir: Internet sistemi: Katman modeli: OSI-TCP/IP Modeli – Uİ'de Analiz düzeyi (Chouci ve Clark): Açıklayıcı bir model mi?Anonimlik siber uzayı daha bilinmez, belirsiz ve güvenliksiz kılmaktadır. Siberde kimlik ve güvenlik; Siber Yönetişim Sorunu (2014 Küresel Siber Yönetişim Programı – J. Nye)- Siber Uzayı kim yönetecek? Sorularının yanında Siber Güç - Siber Caydırıcılık var mıdır? Siber Güvenli derken Kimin güvenliğinden bahsediyoruz? Açık Diploması konusunda – diplomatik sızıntılar- Wikileaks ve Snowden olayları örnek teşkil etmektedir. Siber istihbarat: Kimin işidir? Nesnelerin Interneti (IoTs?nedir?; 1,2 milyar araç, 2020'de 40 milyar araç internete bağlanacaktır da bunlar ne kadar güvenlidir? Büyük Veri (Big Data)'den Uluslararası İlişkilerde teori ve analiz nasıl etkilenir? E-ticaret: 10 trilyon $: Küresel bölüşüm ve güç transferine etkisi?*

Aktörler (paydaşlar sistemi), Uluslararası Sınırlar, Egemenlik, Ulusal-Uluslararası Güvenlik, Küresel yönetişim, Dış Politika, Siber Çatışmalar, İnsan Hakları başlıkları da siber alanla birlikte tekrar gündeme gelmektedir. Siber uzayın Westfalyan Uluslararası İlişkiler düzenine etkileri; Yeni uluslararası aktörlerin ortaya çıkması, geleneksel güç ilişkileri değiştirmesi; güç transferini kolaylaştırması bağlamında, yeni tehdit türleri ve yeni ulusal güvenlik boyutu (siber güvenlik) oluşturması, siber çatışmalar; (güvenlikleştirme, kritik altyapılar ve siber istihbarat), siber uzay yönetişiminde özel sektörün gücü, geleneksel uluslararası yönetişim kurumlarının etkisinin siber uzayda az olması, Siber yönetişim için artan işbirliği ihtiyacı ve çabaları – küresel siber normlar sorusunu beraberinde getirmiştir.

Küresel Siber Saldırılar ve Uluslararası İlişkiler bağlamında; Estonya'ya DDoSsaldırları (2007) İsrail-Suriye radar kontrolü (2007), Stuxnet (2010), Wikileaks ve Snowden saldırıları ele alınmıştır.

İkinci oturumun birinci sunumu "Siber Uzayın Felsefesi" başlığıyla Prof.Dr. Mustafa Çevik (Ankara Sosyal Bilimler Üniversitesi) tarafından yapıldı. Siber uzaya felsefi bir yaklaşımla bakan Çevik, sanallık ve gerçeklik kavramlarını tartıştı. Var olma ve koşullarına değinilen tartışmada var olmak için fiziksel dünyada olmak ve üç boyutlu olmanın bir zorunluluk olup olmadığı tartışıldı. Siber uzayın farklı bilim dallarıyla ilişkisi ve gelecekte insan üzerindeki etkileri tartışıldı. Aynı sunumda yapay zeka ve insanlık kavramları da detaylı bir şekilde tartıldı.

İkinci oturumun ikinci sunumu, 'Teknoloji ve Uluslararası İlişkiler Teorisi' başlığı ile Prof. Dr. Davut Ateş (Selçuk Üniversitesi) tarafından yapılmıştır. Konvansiyonel teknoloji ile başlayan Ateş, modern uluslararası ilişkilerin ortaya çıkışında ve evriminde teknolojik gelişmelerin başat rol oynadığını ifade etmiştir. Sanayi devrimi-1 (buharlı makineler ve gemiler)... Denizaşırı taşımacılık ve ticaret...Sanayi devrimi-2 (içten yanmalı motorlar ve elektrik)... Fosil yakıtların ve doğal kaynakların önemi... Daha küçük ve hareketli makineler...Sanayi devrimi-3 (elektronik)... İşlevsel mini makinelerin yaygınlaşması... Uydular…

Konvansiyonel Teknoloji ve Uluslararası İlişkilerde Pratik Örnekleri; Savunma sanayi (yeni silahların gelişmesi) Ulusal güvenlik (istihbarat yöntemleri dahil) Uluslararası ticaret ve yatırımlar, Enerji kaynaklarının kontrolü, Ekonomik kalkınma politikaları, İletişim ve haberleşme, Nakliye araçları (deniz, hava, kara, demir), Diplomatik ilişkiler, Uluslararası örgütlenmeler, Yasal düzenlemeler (uluslararası hukuk) olarak belirtilmiştir.
Konvansiyonel Teknoloji ve Uluslararası İlişkilerde Teori Örnekleri; Teknolojik rekabet ve güvenlik (realist yorumlar), Karşılıklı bağımlılık, örgütler (liberal açılımlar), Hegemonya ve yeni sömürgecilik (neo-Marksist yaklaşımlar), Teknoloji / iktidar birliktelikliği, özgürlük özlemi (eleştirel yaklaşımlar), Alternatifleri keşfetme girişimleri (post-yapısal yaklaşımlar), Sosyal değişim ve evrim (konstrüktivistler)oolarak ifade edilmiştir.

Siber teknoloji 4. Sanayi Devriminin unsurlarından biri olarak görülmektedir. 4. Sanayi Devriminin başlıca unsurları: Akıllı makineler (yapay zeka), Üretimde robotların hakim konuma gelmesi, Mikro-çipleşme, İnternet ve siber dünya, İletişim ve nakliyede artan hız, Bilginin birincil sermaye haline gelmesi, İnsan-akıllı makine özdeşliği olarak ifade edilmiştir.

Siber teknoloji, reel hayatın siber ortama aktarılması ve sürdürülmesine yarayan araçlar bütünü olarak tanımlanabilir. Başlıca unsurları: İnternet, Sosyal medya, Bilgi ve iletişim teknolojileri, E-Ticaret, E-Finans, E-Suç olarak belirtilmiştir.

Konvansiyonel Teknoloji ve Uluslararası İlişkilerde Pratik Örnekleri; Günümüzde uluslararası alandaki bir kısım pratikler siber alana aktarılmaktadır. Bazı örnekler: Ülkeselliğin dönüşümü (post-territoriality), Siyasal alanın sibere kayması, Siber istihbarat ve siber saldırı, Siber güvenlik (ulusal, kurumsal ve kişisel), Siber savaşlar ve çatışmalar, terörizm, Yeni örgütlenmeler ve sosyal hareketler, E-devlet ve e-vatandaş (sanal devlet-vatandaş), Küresel toplum ve kamuoyu (mahşer), Uluslararası hukukun dönüşümü (siber hukuk) ele alınmıştır.

Konvansiyonel Teknoloji ve Uluslararası İlişkilerde Teori Örnekleri;Siber teknolojiler uluslararası ilişkilere yaklaşımları etkileyecektir sorusunu teoriler üzerinden ele alınmıştır. Realizm; Siber ilişkilerdeki gelişmeler ‘‘realizm’’i realist olarak bırakacak mı yoksa yeni bir tür realizme geçiş mi olacak? Savaş, güvenlik, ulusal çıkar ve güç gibi realist kavramlar siber dünyada nasıl incelenecek?Siber dünya gerçeklikten bir kopuş gibi algılanabileceği için realist perspektif bu konuya yabancı mı kalacak?Soruları cevaplanmıştır.

Liberalizm; Siber dünya bir ‘‘açık pazar ortamı’’ olarak kavramlaştırılabilecek mi? Kompleks karşılıklı bağımlılığın unsurları ve dinamikleri nasıl açığa çıkarılacak? Siber dünyada devlet dışı aktörlerin çoğalması ve etkinliklerinin artması mümkün olacak mı?Önceki dönemde bir seçenek gibi kavramlaştırılan uluslararası örgütlenmeler meselesi siber ilişkiler ağında artık geri döndürülemez bir zorunluluk olur mu?Siber dünya Kantçı idealin gerçeğe dönüşmesine imkan tanıyabilir mi? Soruları yanıtlanmıştır.

Yeni Marksist Yaklaşımlar; Siber dünyada sermaye, emek, artı değer, sömürü, emperyalizm, bağımlılık, dünya sistemi gibi olguların özünde bir kısım değişimler var mı, yoksa yalnızca şekil mi dönüşüyor?Yeni dönemde akıllı makineler insan için çalışacaksa, siber dünya Marksist ideal olan evrensel komünist toplum için bir altyapı teşkil edebilir mi?Sınıflar ve ülkeler arasındaki eşitsizlikler var olmaya devam edecek mi, yoksa siber dünya bunların giderilmesi konusunda bazı fırsatlar sunuyor mu? Uluslararası politik ekonomi? Olarak yanıtlanmıştır.

Konstrüktivizm; Siber dünya kimlik, çıkar ve normların şekillenmesi ve dönüşümü üzerinde nasıl bir etkiye sahip olacak? Uzay çalışmaları önümüzdeki dönemde olası yeni yerleşimler

konvansiyonel uluslararası ilişkileri nasıl etkiyecek?Kimliğin önemli bir unsuru olan dil farklılığının ortadan kalkması kimlik tanımları ve sınırları üzerinde nasıl bir etkide bulunacak? (otomatik simültane tercüme makinelerinin gelişimi)Siber dünya ve teknolojiler yeni değer oluşumlarını hangi yollarla destekleyecek? Olarak ifade edilmiştir.

Yeni Teorik Tartışma Başlıkları; Evrensel veya kozmopolitan toplum olgusu siber teknolojiler sayesinde zorunlu olarak ortaya çıkan yeni bir gerçeklik mi? Siber dünyada sınırlar olacak mı? Yoksa ülkeler arasındaki fiziki sınırlar zaman içerisinde anlamsızlaşacak mı?Savaş ve çatışmalar dahil pek çok iş, üretim ve faaliyet akıllı makineler tarafından yapılacağına göre siber dünyada insan faktörünün yeni rolleri nasıl olacak?Akıllı makineler güvenliğe katkı sağladığı kadar ne tür handikaplar taşımaktadır?Karşılıklı bağımlılığın ve entegrasyonun yoğun olacağı siber alanda devletlerin egemenliği ne ölçüde mutlaklığını koruyabilecek? Yoksa mutlak anarşiden tedrici biçimde bir hiyerarşiye dönüşüm olacak mı, olacaksa hangi yollarla gerçekleşecek? Siber teknolojiler küreselleşme olgusunu yeni bir evreye mi taşıyacak? Teknolojinin gelişimine bağlı olarak savaşlar meydan muharebesi, cephe savaşları, topyekunsavaş şekline dönüşmüştü. Yeni dönemde ne tür savaşlarla karşılaşacağız ve bunların icrasına ilişkin ortak kurallar nasıl belirlenecek? Olarak ifade edilmiştir.

Ontoloji Boyutunda; Bütün bu tartışma başlıkları özelde uluslararası ilişkilerle alakalıymış gibi görünse de, esasında sosyal teoriye ilişkindir. Siyaset, sosyoloji, iktisat, tarih, hukuk, felsefe gibi pek çok sosyal bilim dalı teknolojideki gelişmelere paralel biçimde dönüşen sosyal olguyu anlama, açıklama ve anlamlandırma konusunda yeni yaklaşımlar geliştirme yükümlülüğü altındadır.Bunlar arasında en fazla inter-disipliner özelliğe sahip uluslararası ilişkiler teorisi bu çerçevede kendisini güncelleyebilmek için öteki sosyal bilim dallarına daha fazla dayanmak zorunda kalacaktır. Aynı zamanda sosyal bilim dallarının her biri yeni sosyal gerçekliği açıklama uğraşı içerisinde siber ilişkiler ağı, küresel alan ve kozmopolitan toplum gibi olgulara daha fazla angajeolmak zorunda kalacaktır. Önceki dönemlerde daha özel bir alanmış gibi kavramlaştırılan uluslararası ilişkiler diğer sosyal bilim dallarının bir kesişim noktası haline gelecek, halka açılıp daha fazla şeffaflaşabileceği ifade edilmiştir.

Çalıştay boyunca sunum yapanlar ve katılımcılar siber uzay ve uluslararası ilişkiler disiplini arasındaki ilişkiyi irdelemek, anlamak ve anlamlandırmak için yoğun bir tartışma ve müzakere sürecine girdiler. Disiplinde yeni bir alan olması hasebiyle bağlantılar ve etkileşimleri tartışıldı.

ARTICLE AND BOOK REVIEWS / MAKALE VE KİTAP İNCELEMELERİ

CYBERDETERRENCE AND CYBERWAR

Fatma ÇAKIR[*]

[*] Research Assistant, Department of International Relations, Selcuk University-Konya-Turkey, can be accessed via fatmacakir021@gmail.com

Martin C. Libicki, Cyberdeterrence and Cyberwar, RAND Corporation, 2009.

Cyberspace that emerged as a new field parallel to technological developments has become an indispensable part of modern societies. Although conceptualizations in this new man-made area are similar to those in the physical world, it is actually difficult to transfer these concepts in the same way because of the nature of cyberspace.

In recent years, studies on cybersecurity have often included the concepts of cyberwarfare, cyberattack / defense and cyberdeterrence. However, it is argued that these concepts, like those in the physical world, can not fulfill the expected effect. At this point, Martin C. Libicki and his work *Cyberdeterrence and Cyberwar* have a prominent place in the literature. Libicki has a lot of work on cyberspace and cybersecurity and is a professor at the US Naval Academy in the field of Cyber Security Studies. Libicki also works as a leading scientist at RAND Corporation.

The aim of the *Cyberdeterrence and Cyberwar* is to guide US policymakers and Air Force leaders in preparing cyberwarfare and cyberdefense objectives, strategies, policies and operations. Focusing on the policy dimension of cyberwarfare, the study analyzes what the cyberwar means, what it requires, and whether it is possible to prevent others from resorting to it. (p.5)

The study consists of nine chapters and, in general terms, suggests the following basic arguments: Cyberspace is a separate field with its own rules. Conceptualizations in this area differ from those in other domains such as land, air, sea, space (p.11). For instance, cyber warfare is separate from wars in physical domains. Firstly, cyber attacks are enabled not through the generation of force but by the exploitation of the enemy's vulnerabilities. Secondly, there are ambiguities about who is attacking, what they have achieved, and whether they will do it again. Thirdly, a working attack today may not work tomorrow with changes in technology and security measures. In addition to these distinctions, Libicki also talks about the concepts of strategic cyberwarfare (p.117) and operational cyberwarfare (p.139). While he warns the US government and the Air Force not to consider strategic cyber warfare as a priority investment area due to unpredictable consequences, argues that operational cyber warfare should only be used under a support function.

On the other hand, Libicki points out the concept of cyberdeterrence and emphasizes that it is different from nuclear deterrence and other military deterrence in general. (p.39) These differences reveal the problematic aspects of cyberdeterrence. First of all, it is necessary to distinguish the purpose of an attack in order to be effective in cyberdeterrence. An attack may have been made by a certain intention or by mistake. Also, it is important to note that if a retaliatory attack occurs after an attack, the missile may be attacked against the wrong target, because it is hard to know exactly who launched the attack (p.41).

In his analysis of whether a state will consider retaliation, Libicki concludes that the state should consider whether they will win or lose by retaliating. States' actions can prevent more attacks, but they can also push the attacker to take the war further(p.53). In addition, whether the retaliation is open or hidden is a point that should be considered separately. Because of all these problems, Libicki states that the US administration and the Air Force should consume other options such as diplomatic, economic and prosecution before they go to the cyberwar.

In general, when examined, it seems that *Cyberdeterrence and Cyberwar* was written in a clear and understandable language and handled with a theoretical perspective. Therefore, this study can be read easily by the students of cyberpolitics, cyberspace and cybersecurity. Also, the author's section titles in the form of questions can be evaluated positive in terms of stimulating curiosity in the reader and having a general idea of which questions the author answered in the study. Finally, parallel to the purpose of it's preparing, the study is a good source of mind-opening for politicians and researchers interested in this subject.

STAYING AHEAD IN THE CYBER SECURITY GAME: WHAT MATTERS NOW

Mohammed ISHMEAL[*]

[*] PhD candidate at Selcuk University in the Department of International Relation, Konya, Turkey. Can e accessed via blkqatari@gmail.com

Erik van Ommeren, Martin Borrett an Marinus Kuivenhoven.(2014). Staying Ahead in the Cyber Security Game: What Matters Now: Sogeti and IBM.

The book as its title suggest stays ahead in the game of cyber politics tacitly and succinctly brings to bear concern issues relevant today and tomorrow. Although the authors of this work hinted the world in 2014, the expected challenges of cyber security in a complex cyber space world as information and computer technology evolutionalized, the solutions they provided in this premier book was quiet revealing and relevant to today's problems. In obvious expositions laid in a simple diction, the book analysis organizational security problems in the cyberspace taking into considerations management, usages and administration devoid of any form of technicalities detailed in the book. Thus, making cyber security a germane subject of enquiry in a capitalist world of business where security risk organizations profit is worthy of attention. The authors advocate states, organizations and individuals to transcend the technical area of information technology to consider social, economic, and ideological and the political dimensions. This is necessitated by the volume of increase in new computer devices, big data, software and the complex mobile usages by employees. In fact there is an imminent impact which poses security threats. In a 14 chapter discussion, the book presents each chapter independent of the other concentrating on the specific issue in relation to recent, relevance, solution and guiding principles.

The chapter one opens with a basic definition of Cyber security as "a set of people, process and technical practices aimed at protecting critical infrastructures, digital business and sensitive information from internal and external threats or negligence" (P, 15). Interestingly, despite the broad nature of the definition the authors discusses only a section of business organization. The emphasis of cyber security should rather be focused on protecting businesses and the society where interaction takes place. The credibility and sustenance of any business transaction hinges on how secured parties feel. Thus, the question of trust of people, the security of the organizations and benefit parties accrue occupies the central part of the three page discussion in this chapter. It is worthy to mention that the internet realm lacks any coordinated concerted effort which could normalize the maladjusted system of the internet virtual world. Security had not been part of the responsibilities of the designers of the internet. In a fast developing virtual world where users become more sophisticated in a very fast pace, out-maneuvering the available technology is a threat to the very purpose of the relevance of Information Technology (IT). Obviously, the concern of security executives over clouds and mobile security were discussed as a shift of conventional security of IT has assumed much more public debate today.

In fact recent activities where security experts such as John McAfee mobile and twitter account hacked[17] vindicate the authors of this book. The lesson is that no one is safe. As a result "pursuit of strategic advantage" (p. 17) in search of equilibrium between the hacker and the defender should be prioritized.

As they advocated for insightful and meaningful research to build a strong internet security structure, the chapter two, basically, advances the battle of the fitters in this unguarded cyber field of chaos where the "good" and "bad" guys compete for survival. Hacktivism from state to non-state actors and organized groups to individual criminals are scrambling for most lucrative element which is DATA, to advance their interest which could in blackmail, theft and conspiracy. In such a contested realm privacy and security becomes the *Janus* of the field of internet security.

The issue is that even when security officers possess the potential to protect and provide security to prospective victims their privacy remains an issue. This is so because, ethically, the security providers need the authorization of the individual before accessing his/her data. Thus, although privacy and security strive to protect, yet, it breaches on the confidentiality of the other. This issue of data ownership is well articulated at page 21 of the book. Fundamentally, the wishful list of cyber security officers from "securing end-to-end communication "developing "smarter system" and "a way to communicate to users about security" have improved not only the awareness of users but attempted to mitigate the level of attack. As is provided in the *Cyber Security Manifesto* "Keeping the flow of information running freely is an economic imperative". (P, 20).

Chapter three questions the difficulty in relation to employer-employee conflicting rights to usage and protection. How do we then restrict people's rights to using their preferred devices at work places at the expense of the organizations? Clearly, to protect the network system of institution there should be a choice of device provided by to people at the organization for the purposes of limiting the risk of being hacked. Chapter four therefore admonishes organizations not to limit security to technical or IT experts but should involve public relations officers, legal luminaries, human resource personnel, business expert, managers, political and economic

[17] Joe Pinkstone *Mailonline* , " 'I have haters I am a target' Cybersecurity guru John McAfee goes on Twitter rant after claiming his accounts was hacked to promote vital currencies". 29th Dec, 2017 http://www.dailymail.co.uk/sciencetech/article-5220579/Security-guru-John-McAfees-Twitter-account-hacked.html

experts. Cyber Security should therefore be a multi-facetted approach by all groups in relation to the business organization.

The chapter five argues that in designing software, apps and any form of internet device security should be incorporated to minimize insecurity and strengthen confidentiality and boost privacy. This approach is called security-by-design where the authors vividly provide carful explanations on the advantages and disadvantages to project. The authors argue that the "concept has far-reaching consequences and results"(P, 39). However, the chapter six identifies security measures through implementation convincing technologies as a way of default to regulate users' interaction with any form of technology in the virtual world. In the condition of realizing users anomaly behavior persuasion should be applied rather than force. This will enable organization to keep track of weaknesses of the new paths and stuffs which are insecure practices. When insecure practices are found settings could be change to help solve risk of users to hacktivism. The next chapter employs and discusses fear as a tool which may restrict users' adventurism in the internet and might save many from being victims of hack or path to attacking an organization. However, the challenge is that human mind can easily forget his fear being a victim and fall prey to hacking. Therefore organizations should always make a responsibility to minimize the risk of users. To do this, organizations must have the determinations and the commitment to interact with users.

Chapter eight further relates that hackers are often determined and committed to their course and even provide a very good communication when in group. Thus, there is the need for organization to provide a platform for dissemination of information to enhance communication since ignorance is also a major threat to security.

Out of this challenge followed the chapter nine which implore that hacking today should be viewed as a game which can be won at the same time lost. The most important thing is to understand and accept the possibility of a hack from hacktivists. The authors, however, provided measures which could help to ameliorate the risk from Advanced Persistent Threat (APT) from hacktivists. Equally important is the manner in which abnormalities are supposed to be detected in chapter 10 through observation, identification and analysis of data patterns to avoid hacking let alone risk the businesses of the organization. As done in the previous chapters, recommendations to face some of these complex cyber security challenges are well highlighted. (P, 62).

In chapter eleven, the authors explain the importance of setting up a response team to practice different possibility tactics and make efforts to tackle both past and new problems as a preparatory ground work to self-defense. Hackers are said to be fast lesson learners which demand equal measure of response to avoid repeating past mistakes. To be able to complete this task easily more experience needed to be shared among groups of different organizations, states and communities. However, security experts find it problematic in sharing experiences with each other since there is no trust among them. Chapter twelve briefly highlights encryptions as hidden weapon despite the fact that there still "computing power, computing parallel and new computing paradigm" (p, 67) which still threatens them in the virtual world. The competition to encrypt is parallel to arms race where parties employ to outwit the system. No matter the complexity of encryption it cannot be said to be hundred percent safe.

Thus, the final chapters 13 and 14 advocated for two things. First, the need to realize the importance of personal responsibility, by changing out attitude toward the use of the internet. Second, making cyber security the central theme in various organizations and the international community. These fundamental two issues are sure way to staying ahead away from hack risk in an attempt to win the cyber security crisis looming in the foreseeable future.

From the above discussion, it is patent that the book despite its brevity still provides a great insight into future of cyber world. Although much of the discussion was centered on business organization not much of cyber security and state role in the international system is discussed. In fact sates issues which mentioned were specific, general sketches and scattered international incident. However, the nature of conflict among organizations, lack of regulations governing the administration of the internet virtual world if extended into the domain of international politics will produce more chaotic hostility if not the same. As a result, it is palpable to conclude the book is more of handbook to understanding cybersecurity.

'GÜVENLİŞLEŞTİRME'Yİ YENİDEN GÖZDEN GEÇİRMEK: TEORİ VE VAKALAR

Cihan DABAN[*]

[*] Arş. Gör., Selçuk Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Bölümü, ,E-mail: dabancihan@gmail.com

Thierry Balzac, Sarah Leonard and Jan Rujicka.(2015). 'Securitization' Revisited: Theory and Cases, Sage Journal, 30(4), pp.494-531.

Makale üç yazar tarafından ele alınmıştır. Bu yazarlar, Thierry Balzacq, Sarah Leonard ve Jan Ruzicka'dır. Balzacq, doktorasını Cambridge Üniversitesi'nden almıştır. Doktora sonrası Harvard'da görev yapan Balzacq, ardından Edinburgh Üniversitesi'nde Onursal Profesörlük görevinde bulunmuştur. Ayrıca Beşeri Bilimler Enstitüsünde Yüksek Öğrenim Çalışmalarında "seçkin araştırma" konusunda görev de yapmıştır. 2015 yılında Diplomasi ve Uluslararası Güvenlikte Seviye 1, Kanada Araştırma Başkanı (yılda 200.000 ABD Doları değerinde) ödülüne layık görülmüştür. Balzacq, güvenlik, güvenlikleştirme teorisi, Uluslararası İlişkiler Teorisi ve Avrupa Birliği politikası üzerine 100'den fazla bildiri yayınlamıştır. 150'den fazla da sunum yapmıştır. Güvenlik üzerine çalışan Balzacq, 2015 yılında yayımlanan "Gözden Geçirilmiş Güvenlikleştirme: Teori ve Vakalar" konulu makalede diğer iki yazarla beraber siber güvenlik konusuna değinmiştir. Diğer yazarlardan Leonard, Birleşik Krallığa bağlı İskoçya Dundee Üniversitesi'nde çalışmaktadır. Yazarın çalışma alanları; dış politika ve güvenlik konularıdır. 2015 yılında Balzacq ile birlikte ele aldığı bu makalede, güvenlik konusunu siberle bağlantılı olarak ele almıştır. Üçüncü yazar olan Ruzicka, 2010 yılında güvenlikleştirme teorisine ilişkin teorik bir eleştiri ile Fransız ve Rus devrimlerinin tarihsel vaka incelemelerini konu alan teziyle doktorasını almıştır. Güvenlik üzerine çalışmalar yapan Ruzicka, öte yandan uluslararası ilişkiler teorisi ve Orta Avrupa bölgesi üzerine de çalışmalar yapmaktadır.

Gözden Geçirilmiş Güvenlikleştirme: Teori ve Vakalar başlıklı makalede en dikkat çekici durum güvenlik algısının siberle bağlantılı olduğu kısımdır. Bu kısım ikinci ana başlıkta ayrıntılı olarak değinilmiştir. Bu kapsamda makale, üç ana başlıktan oluşmaktadır. Birinci ana başlık *Güvenlikleştirmenin Kavramsal Boyutlarıdır*. Bu kısımda, güvenlikle ilgili olarak güç ilişkileri, uygulamalar ve araçlar ele alınmıştır. İkinci ana başlık, *Güvenlikleştirmenin Ampirik ve Teorik Etkileri'*dir. Bu kısımda kimlik ve göç, enerji ve çevre, küresel sağlık, din ve en önemli konulardan biri olan siber güvenlik alanlarına değinilmiştir. Üçüncü ana başlık ise; *Geleceğe Yönelik Kalkınma için Karşılaşılan Zorluklar ve Olası Yöntemler'dir*. Burada ele alınan konular ise, teori ve metodolojidir.

Üç ana başlıkta incelenen makalede ilgi çeken konu, siberden daha eski olan güvenlik konusunun siberle bağlantılı olarak ele alınmış olmasıdır. Güvenlikleştirme üzerine yapılan çalışmalarda, başlangıçta siber denilen bir alan olmadığı için siber alanın öneminden

bahsedilmemiştir. 196'lardan sonra yaygınlaşan internet, beraberinde siber alanı da ortaya çıkarmıştır. O günden bu yana, daha geniş teorik gelişmelere yol açan siber güvenlik ve güvenlikleştirme konusunda önemli çalışmalar yapılmaya başlanmıştır. Bu alanın önemi birbiriyle ilişkili iki eğilimden kaynaklanmaktadır. Birincisi, devletler, toplumlar, işletmeler ve bireyler giderek siber uzayda bulunan veri, sistem ve teknolojilere güvenmiş ve bu, bir dizi aktörün çeşitli tehditleri tanımlayan yeni güvenlikleştirme hareketlerini geliştirmesi için verimli bir zemin sunmuştur. İkincisi, siber güvenlik açıklarıyla meşgul olmaktır. Bu durum Soğuk Savaşın sona ermesinden bu yana güvenlik uzmanları ve bürokrasiler arasında sürmekte olan yeni tehditler ve risklerin araştırılmasına çok uygun bir dönem olmuştur.

Makale, bilgi teknolojilerinin (BT) yalnızca bilgisayarların güvenlik açığı başlangıçlarından beri bilindiği 1990'ların sonlarında güvenlikleştirmeyi incelemiştir. BT'nin güvenlik gündeminin bir parçası haline geldiğini anlamak için, "çerçeveleme" kavramını kullanmıştır. Bu kavramla başarılı bir güvenlikleştirme için kriterleri sunmuştur. Bunu ise yalnızca bir konunun siyasi gündeme yerleştirilmesi ile eşleştirmiştir. Buna ek olarak, BT'nin bir güvenlik sorunu olarak tanımlanmasının, geleneksel güvenlik uzmanlarının ötesine geçen, ayrı politika alanlarından aynı anda ortaya çıktığını da savunmuştur. Eriksson'un çalışması İsveç davasıyla sınırlı kalmıştır. Ancak uluslararası politika yayılımı konusunda daha geniş bir tartışmaya da yer verilmiştir.

Siber uzayın güvenlikleştirilmesi ile ilgili daha yeni çalışmalar Amerika Birleşik Devletleri'nde ortaya çıkmıştır. Bu anlamda makale, üç argüman üzerinde durmuştur. Bunlar; çerçeveleme özellikleri, bağlamsal koşullar ve çerçeveleyici aktörler olarak ileri sürülmüştür. Bu argümanları analizlerine dahil ederek gevenlikleştirme teorisinin ötesine geçmeye çalışmışlardır. 1990'lı yıllarda birçok güvenlikleştirme eylemine rağmen, Bush yönetimi, 2001 yılına kadar "güvenlikleştirme" üzerine çok az sayıda olağanüstü önlem çağrısı yapmıştır. Fakat bu dönemde siber güvenlik ve kritik altyapılar arasında kurulan bağlantı sayesinde, özellikle siber güvenlik alanına daha çok önem vermeye başlandığı görülmüştür. 11 Eylül saldırıları, daha sonra, devletlerarası siber çatışma açısından değil, siber terörizm açısından, siber tehditlerin çerçevesini güçlendiren bir "odaklanma olayı" olarak algılanmıştır. Bu döneme kadar siber tehditlere karşı (alınan istisnai önlemler dışında) çok az önlem alındığı görülmüştür. Bu durum güvenlikleştirme teorisine daha da çok odaklanmasına ve "tehdit politikası yaklaşımının" daha da çok geliştirilmesine olanak vermiştir.

Özetlemek gerekirse makale, ana hatlarıyla güvenlikleştirme teorisini siber güvenlikle bağdaştırmada önemli bir yol izlemiştir. Bu yönüyle literatüre önemli katkılar sunmuştur. Siber güvenlik açısından nasıl bir yol izlenmesi gerektiğini çok ayrıntılara girmeden ve karmaşık bir yöntem izlemeden, ana hatlarıyla ileri sürmüştür. Bu nedenle hem sade bir dil kullanılmış hem de teorik çerçeve iyi analiz edilmiştir. Bu durum okuyucunun makaleyi daha kolay anlamasını sağlamıştır. Öte yandan, güvenlikleştirme teorisi ile siber uzay arasındaki bağlantının incelenmesi, sadece siberle ilgili altyapıların incelenmesiyle değil, aynı zamanda sağlık, çevre, enerji, din, teori, kimlik ve göç gibi diğer alanlarda yapılan araştırmalar üzerinde de durmuştur. Bu yönüyle makale, okuyucuya önemli bilgiler kazandırmaya çalışmıştır/çalışmaktadır.

Notes For Authors / Yazarlar İçin Notlar

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.