ACADEMIC REVIEW OF HUMANITIES AND SOCIAL SCIENCES
Vol.: 1 Issue: 2 Year: 2018, pp. 110-119

ARHUSS
ISSN: 2636-7645

SİBER UZAY VE SİBER GÜVENLİĞE MULTİDİSİPLİNER BİR YAKLAŞIM

Soner ÇELİK [1]

Received Date (Başvuru Tarihi): 01/08/2018
Accepted Date (Kabul Tarihi): 13/08/2018
Published Date (Yayın Tarihi): 25/08/2018

ÖZ

Güvenlik olgusu, geçmişten günümüze kadar üzerinde sürekli tartışılan bir kavram olmuştur. Özellikle ulus devlet yapılarının meydana çıkması ile güvenlik kavramı sürekli bir değişim içerisine girmiştir. Günümüzde, her alandaki değişimin hızlı bir şekilde artması ve özellikle yirminci yüzyılda küreselleşme, bilim ve teknoloji alanındaki gelişmeler, akademi literatüründe yer alan diğer kavramlarda olduğu gibi, güvenlik kavramı tanımında da değişime yol açmıştır.

Özellikle Soğuk Savaş sonrası dönemde, "tehdit" tanımlaması, düşman tanımlamasından çok daha önemli hale gelmiştir. Önceki dönemlerin aksine, klasik "düşman" nitelendirmesi büyük oranda geçerliliğini yitirmiş, güvenliğe yönelik algılamalar ve politikalar açısından tehdit tanımı ve tehditler ile mücadele yaklaşımı ön plana çıkmıştır. Tüm bu gelişmelerin sonucu olarak; terörizm, organize suç örgütleri, siber saldırılar, konvansiyonel ve kitle imha silahlarının yaygınlaşması, çevresel tehditler, kitlesel göç gibi tehditler; ulusal ve uluslararası güvenliğe yönelmiş tehditler arasında gösterilmektedir. Bu kapsamda, makalede siber uzay ve siber güvenlik sorunları, uluslararası ilişkiler disiplini ve güvenlik yaklaşımları çerçevesinde değerlendirilecek ve multidisipliner bir bakış açısı ile siber güvenlik sorunlarını ele almanın önemi ve çözüm önerileri analiz edilecektir.

Anahtar Kelimeler

Güvenlik,
Siber Uzay,
Siber Güvenlik,
Tehdit,
Siber Saldırılar

MULTIDISCIPLINARY APPROACH TO CYBERSPACE AND CYBERSECURITY

ABSTRACT

The term of security, has been consistently discussed as a case of human beings until today. Especially with the formation of nation-state structures, the concept of security has undergone a constant change. The rapid change in all parts of the world today has led to a change in the definition of security as well as in the concepts of globalization, science and technological developments in the twentieth century, as well as in all the concepts of the academia literature.

Especially in the post-Cold War period, the concept of "threat" became more important than the concept of the enemy. Contrary to the previous periods, the concept of classical "enemy" has lost its effectiveness in large scale and the approach to combat threat definitions and threats has come to the forefront in terms of security. As a result of these events; international terrorism, organized crime organizations, cyber attacks, the spread of conventional and weapons of mass destruction, environmental threats and mass migration; threatened national and international security threats. In this context, the cyber space and cyber security problems will be evaluated in terms of international relations discipline and security approaches in the paper, and the importance of handling cyber security problems from a multidisciplinary point of view and solution proposals will be analyzed.

Keywords

Security,
Cyberspace,
Cybersecurity,
Threat,
Cyber Threats,

Citation: Çelik, S (2018), Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşim, ARHUSS, (2018), 1(2): 110-119

[1] *Doktora Öğrencisi, Süleyman Demirel Üniversitesi, İİBF-Uluslararası İlişkiler Bölümü, E-posta: sonercelik85@gmail.com*

1. GİRİŞ

Günümüz araştırmalarında siber güvenlik ve siber uzay olgusunun çalışma kapsamında ele alınış biçiminde, siber güvenliğin çoğunlukla bilgisayar odaklı enformasyon teknolojilerine ve uygulamalarına vurgu yapan "teknik boyutu" ile ulusal güvenlik kaygıları üzerinden siyasal ve hukuksal uygulamalara vurgu yapan "sosyal boyutu" arasında ciddi bir ayrım bulunmaktadır. Bu çerçevede, bir ülkenin ulusal güvenliğini bütüncül bir şekilde sağlamakla sorumlu olan üst seviye güvenlik karar alıcılarının; nasıl ki terörle mücadele kapsamında başvurulabilecek asimetrik çatışma ya da örtülü operasyon biçimleri konusunda uzmanlık seviyesinde teknik derinliğe sahip olmaları beklenilemez ise, bilgisayar ve enformasyon teknolojileri alanında da benzeri bir uzmanlık beklentisi içerisinde bulunulmaması gerekmektedir.

Ayrıca günümüzde devletlerin güvenliği teknolojik gelişmelere doğrudan bağlıdır. Bu kapsamda, siber uzay alanındaki teknolojilere sahip olamayan devletler ciddi güvenlik zafiyetleri ile karşı karşıyadırlar. Aynı şekilde devletlerin güvenliklerini sağlama noktasında, klasik güvenlik anlayışına göre planlanmış tüm kurum ve stratejilerini etkili bir siber saldırı ve siber savunma kapasitesi yaratmak adına yeniden organize etmesi de gerekmektedir (Darıcılı ve Özdal, Güz 2017: 34).

Bu kapsamda, siber güvenliğin teknik boyutunun çok daha derin ve karmaşık olmasının yanı sıra söz konusu boyut çoğu zaman akademik kuruluşların ve özel sektörde faaliyet gösteren firmalarının alanları ile de kesişmektedir. Dolayısıyla gerek tümüyle teknik mahiyette olması ve gözlem yapma yoluyla tam olarak kavranamayacak bir karakter taşıması, gerekse de kamu ve özel sektörün karma bir faaliyet alanı oluşturması nedeniyle; siber güvenliğin "teknik boyutu" bu makalenin kapsamı dışında bırakılmıştır.

2. SİBER GÜVENLİK'TE MULTİDİSİPLİNER YAKLAŞIM

Sosyal bilimler araştırmacıları ile mühendislik teknolojileri araştırmacılarının günümüzde üzerinde uzlaştığı bir husus vardır: Siber güvenlik ve siber uzay problem sahası sadece teknik çözümler gerektiren bir konu değildir.

Bilgi ve iletişim teknolojilerinin "sivilleşmesi" ile devletlerin, e-devlet, internet bankacılığı ile internet teknolojilerini yaygın şekilde kullandığı ve bu teknolojileri vatandaşların da kullanmasını teşvik ettiği gözlemlenmektedir. Enerji, ulaştırma gibi kritik altyapıların internetle olan tartışmasız bağları ve siber uzayın genişlemesi ile

beraber, aslında siber uzayda ortaya çıkacak problemlerin sadece bilgisayar, yazılım veya ağ mühendisleri tarafından çözülemeyeceği de anlaşılmıştır (Bıçakcı, 2014: s. 103). İtici gücü internet ve ağ teknolojileri temelli gelişmeler olan siber uzay, artık devletler tarafından yeni bir mücadele alanı olarak görülmeye başlanmıştır (Darıcılı, 2014: 19).

Bu noktada günümüzde ülkelerin, kurum ve kuruluşların siber güvenlik açısından zafiyetlerinin temellerini, farklı taraflar arasındaki iletişim zayıflığı (örneğin bir mühendis ve sosyal bilimci) ve paydaşlar arasındaki bilgi ve tecrübe paylaşımı eksikliği (akademi, sanayi ve iş dünyası) ve "bilgi kıskançlığı" gibi olumsuz unsurlarla açıklamak mümkün olup sorunların çözümü için multidisipliner yaklaşım (çok branşlı/disiplinli) gerektiği düşünülmektedir.

21. yüzyılda bilim ve teknoloji alanındaki ilerlemeler güvenliğin yeni boyutlarının ortaya çıkmasına neden olmuştur. Düşmanın belli, tehditlerin açık olduğu, verilebilecek uygun karşılığın tahmin edilebildiği Soğuk Savaş döneminin ardından iyice ivme kazanan küreselleşmenin de etkisiyle uluslararası alanda ortaya çıkan belirsizlikler, güvenlik algısında bir dizi değişimi zorunlu kılmıştır (Erendor, 2017: 114). Yaşanan değişim süreci ile birlikte güvenlik kavramının anlaşılabilir, güvenilebilir ve devamlılık arz eden bir tarifini yapmak ya da herkesin üzerinde anlaşabileceği sınırlarını ve çerçevesini ortaya koymak gittikçe zorlaşmıştır (Yorulmaz, 2014: 14).

Siyaset bilimcilerin, siber güvenliğe ilişkin en çok ilgilendiği noktanın siber güvenliğin ulusal ve uluslararası güvenlikle örtüştüğü alan olduğunu söylemek mümkündür. Özellikle Soğuk Savaşın bitimini takiben, güvenlik algısının dönüşüme uğraması ve konvansiyonel güvenlik unsurlarının yerini asimetrik unsurların alması güvenliğe ilişkilerin tartışmaların boyutlarını arttırdı. Bununla beraber, gözlemlenebildiği kadarıyla neredeyse tüm politik ve askeri çatışmaların bir de siber boyutu oluşmuştur (Erendor, 2018: 59).

Enformasyon savaşları ve stratejik bilgiye erişim, aslında güvenlik ve uluslararası ilişkiler açısından yeni bir kavram değildir. Örneğin, İkinci Dünya Savaşı sırasında, Almanya'nın Enigma makinesinin şifrelerinin çözülmesiyle, Alman ordusuna yanlış bilgi akışı sağlanmış, savaşın kaderi Almanya'nın aleyhine dönmüş ve dünya tarihinin akışı değişmiştir (Geers, 2011: 12). Bilginin kadim gücüne rağmen, "siber güç" ve "siber uzay" kavramlarının görece yeni birer güç unsuru olarak karşımıza çıktığı söylenebilir.

Bilgisayarların ve internetin günlük hayatımızdaki rollerinin yadsınamayacak bir şekilde artması ile birlikte, feminizmden diplomasiye kadar, neredeyse her olgunun siber uzayda var olan ya da teknolojiden faydalanma esasına dayanan bir türevinin üretilmesi mümkün hale gelmiştir. İlişkilendirildiği kavram ve olguların günümüzün teknoloji odaklı dünyasındaki değerini arttırma kaygısını da içeren bu "siberleştirme" eğilimden, geleneksel biçimleri de kamuoyu için oldukça dikkat çekici olan "suç", "savaş", "terörizm" ve "güvenlik" gibi kavramlar da etkilenmiş ve hızlı bir şekilde bu kavramların siber türevleri üretilmiştir.

Bu çerçevede, yeni doğmuş bir olgunun nitelendirilmesi nedeniyle, "siber" kavramının kapsamına ilişkin açık ve net bir tanımlama bulunmamaktadır. Kimilerine göre, sadece kişisel bilgisayarlar veya internet ile kurulan ilişkileri niteleyen bu kavram, kimileri için ise tümüyle fiziksel dünyanın ötesindeki bir sanal ortamı temsil etmektedir. Söz konusu farklı yaklaşımların yanı sıra, kişisel bilgisayarların ve internetin yoğun olarak kullanıldıkları iletişim, hizmetler ve finans gibi pek çok alandaki isimlendirmeler de, "e-posta" veya "e-devlet" örneğinde olduğu gibi, "siber" olmalarına değil, "elektronik" tabanlı olmalarına vurgu yapmaktadırlar.

Her ne kadar günümüz itibariyle siber ön eki eklenmek suretiyle kastedilenler, genel olarak kişisel bilgisayarlar ve özellikle de internet ile bağlantılı olgulardır. Ancak benimsenen genel yaklaşım, özellikle "siber güvenlik" söz konusu olduğu zaman, çok daha büyük elektronik sistemlerin ve enformasyon sistemlerinin de siber güvenliğin kapsamına girdikleri yönündedir. Bu çerçevede, ister günlük hayatın akışı içerisinde özensizce ister uzmanlar tarafından büyük bir dikkatle kullanılmış olsunlar; "siber" ön ekini taşıyan kavramlara veya olgulara bu niteliği gerçek anlamda kazandıran şey, çeşitli teknolojiler ve ağlar üzerinden "siber uzay" ile kurmuş oldukları ilişkidir.

3. ULUSLARARASI İLİŞKİLER VE SİBER GÜVENLİK

Sosyal bilimcileri daha çok ilgilendiren konu siber uzay, siber alan ve uluslararası ilişkiler arasındaki köprü nasıl kurulabilir, siber güvenliğin uluslararası ilişkiler bakış açısına indirgenmesi ve bu disiplinin çalışılması nasıl mümkün olabilir? Nazli Choucri önderliğinde MIT (Massachusetts Institute of Technology)'in özellikle bu disiplinler arası çalışmada önemli yayınlar yapmaktadır. Uzmanlar ise her iki alandaki faaliyet de "insan odaklı" yürütülüyor olsa da, uluslararası ilişkiler ve siber alanın karakteristik özelliklerinin birbirinden oldukça farklı olduğu konusunda hem fikirdir.

Bu iki disiplin arasındaki başlıca farklılıklar, bir takım konu başlıklarıyla özetlenebilir (Chouchri, 2016: 11).

- Geçicilik (Temporality): Siber alandaki aktiviteler, uluslararası ilişkilerin klasik zaman anlayışını kırmıştır
- Fiziksellik (Physicality): Uluslararası ilişkilerin fiziksellik ve coğrafya anlayışını kırmıştır
- Nüfuz Etme (Permeation): Siber alandaki eylemler sınırların ve yargı süreçlerinin ötesindedir.
- Akışkanlık (Fluidity): Siber uzayın değişkenlik ve adaptasyon yeteneği yüksektir.
- Katılım (Participation)
- Atfedilebilirlik (Attribution): Siber alandaki herhangi bir eylemin kim tarafından yapıldığının tespiti zordur
- Hesap verme zorunluluğu (Accountability): Uluslararası mecrada, sorumluluk mekanizmaları siber alanda by-pass edilebilir.

Bu farklılıklara rağmen bir siber-uluslararası ilişkiler teorisi kurulurken, siber güvenliğin ulusal ve uluslararası güvenliğe etkisinin incelenmesinin günümüz dünyasında yaşanan siber saldırıları anlamak açısından önemli bir yer tutmasından yola çıkarak sosyal bilimciler tarafından bazı temel soruların cevapları aranmalıdır?

- Bu çerçevede aktörler kimlerdir? Siber güvenlik denilirken kimin güvenliği kastedilmektedir?
- Devletler siber uzayda yeni oyuncular mıdır? (new comers)
- Siber uzayın kapsamı nedir? Siber uzay anarşik yapıda mıdır? Siber uzay merkezi var mıdır?
- Siber uzayın yönetişim sorununun uluslararası-ulusal güvenlik boyutuna etkisi nedir? (Chochri, 2016: 15).

Zira " İlk olarak kimin güvenliği?" sorusuna verilen yanıt, salt alışılan ve otomatik hale gelen ulus devlet yerine, başta bireyin, devlet-üstü ya da devlet-altı başka toplulukların da olduğu süjeler kümelenmesine doğru evrilmiştir.

Yine, " Ne tür tehditler?" sorusunun yanıtı tek başına askeri nitelikli olma, sınır ötesinden kaynaklanma klasik konumundan çıkmış, kaynağı, zamanı ve şekli önceden tahmin edilmesi güç, hatta neredeyse imkânsız, yeni mücadele alanının bütün dünya olarak ortaya çıktığı, asimetrik ve çok boyutlu bir konuma yükselmiştir (Erdoğan, 2013: 265).

Siber güvenlik, siber uzay ve siber güç unsurları, uluslararası ilişkiler bağlamında özellikle geçtiğimiz yirmi yıla kadar "low politics" yani özellikle realist bakış açısına göre "ikincil derecede önemli" politikalar olarak yer buldu. Ancak, bir gecede sessizce açığa vurduğu kimi gizli belgelerle tüm dünyayı yerinden oynatan Wikileaks skandalı, , siber uzayın, ulusal güvenliğin ayrılamaz bir parçası olduğunu kanıtlamış ve karar alıcıları bu yeni alan karşısında pozisyon almaya itmiştir (Clark ve Choucri, 2013: 21).

Aynı şekilde Tunus'ta başlayan ve kısa bir sürede tüm bölgeyi etkisi altına alan Arap Baharı sürecinde, sosyal medyanın baskıcı rejimlerin devrilme sürecindeki rolü tüm dünyada kabul edilmiştir. Arap Baharı'nın kitlesel niteliğe dönüşmesinde ve diğer ülkelere hızla yayılmasında teknolojinin etkisi önemli olmuştur. Özellikle Tunus ve Mısır'da internet, siyasete ivme kazandıran işleviyle ön plana çıkmıştır (Korkmaz, 2013:2).

Facebook, Twitter, Youtube ve benzeri sosyal ağların kullanımının yaygınlaşması ile Arap toplumları daha fazla paylaşımda bulunmaya başlamış, halklar arasındaki fiziki sınırlar tüm etkisini kaybetmiştir. Arap Baharı sürecinde sürekli dile getirilen Domino etkisinin meydana gelmesinde, bu ortak bilincin, yani sosyal medya ile halkların ortak gündeme sahip olmalarının payı büyüktür. Örneğin, ABD Siber Komutanlığı, siber uzayı yeni bir savaş alanı olarak tanımlamış ve FBI en önemli üç önceliğini olarak, terörizm, casusluk ve siber saldırılar olarak belirlemiştir (Geers, 2011: 2). Siber-uzay, uluslararası ilişkilerde güncel meselelerin yer aldığı dört fiziksel boyuta (kara – hava – deniz – uzay) eklenen, insanlar tarafından üretilmiş beşinci bir boyuttur. Netice olarak siber uzay, 2016 Varşova Zirvesi'nde NATO tarafından da operasyonel bir alan olarak resmen tanınmış bulunmaktadır (NATO, 2016).

Siber uzayda ülkelere yönelik siber tehditlerin uluslararası ilişkiler düzleminde kullanılmaya başlaması, küresel politikaları ve geleneksel uluslararası ilişkiler anlayışını da derinden değiştirmeye başlamıştır. Örneğin uluslararası politika uzmanı Joseph Nye'a göre, siber tehditlerin devletler ya da devlet dışı aktörler tarafından kullanılmaya

başlanması, küresel güç dengelerini de değiştirmekte ve gücün küresel düzende yeniden dağılması konusundaki dinamiklerde önemli rol oynamaktadır (Nye, 2010: 1).

Bir başka deyişle, kara ve denizde baskın güce sahip olan büyük aktörler, benzer şekilde siber uzayda yeterli kapasiteye sahip olamamakta ve bunun aksine daha küçük veya devlet dışı aktörler siber alanı asimetrik bir boyutla çok daha etkin şekilde kullanabilmektedir. Siber dünyanın, küçük aktörlere sağladığı en büyük avantaj siber silahların konvansiyonel silahlara göre çok daha ucuz olması, suçlunun kolayca tespit edilememesi ve siber uzayda yapılan bir eylemin gerçek dünyada yıkıcı etkiler doğurabilmesidir. Bununla beraber, geleneksel savunma anlayışında, ev sahibinin yani savunma yapanın mücadelede avantajlı konumda bulunmasının aksine, içinde bulunduğumuz siber uzayın şartları hackerlar ve siber suçlulardan yana olmaktadır. Bu sebeple, "iyi kovboylar" yani beyaz şapkalı hackerlar, devletler, ordular ve stratejik sektörlerde faaliyet gösteren kurumlar için paha biçilemez derecede önemli hale gelmiştir.

Estonya, Gürcistan ve İran'da yaşanan siber saldırıları uluslararası hukuk ve savaş hukuku açısından bir alt başlık haline getirmiştir. Geçmişte yaşanan siber unsurları saldırıların ciddi sonuçlarına rağmen bu saldırıların savaş nedeni olup olamayacağı konusunda ne akademik dünyada ne de uluslararası kamuoyunda fikir birliği mevcut değil. Yine de başka bir araştırmanın konusu olabilecek önemli soruları sormak mümkün:

- Siber saldırıların bir ülkeyi silahlı kuvvet kullanma eşiğine gelmesi söz konusu olabilir mi?
- Siber saldırılar, BM Antlaşması, 51. Madde kapsamında, meşru müdafaa hakkının doğmasına yol açar mı?
- Devletler, siber saldırılara karşı, uluslararası hukuk düzleminde ne gibi önlemler alabilirler? (Yayla, 2014: 189).

4. SİBER YÖNETİŞİM VE ULUSLARARASI İLİŞKİLER

Uluslararası ilişkilerde, "siber yönetişim" ve devletlerarasında işbirliği öne çıkan diğer konu başlıkları olarak karşımıza çıkmaktadır. Devletlerarasındaki işbirliği boyutuna bakıldığı zaman, uluslararası alanda, siber suçlara karşı imzalanmış ilk anlaşma, Avrupa Konseyi'nin 2001 tarihli, Siber Suç Sözleşmesidir (Önok, 2013: 1239).

Güvenlik ittifaklarına bakıldığı zaman ise, NATO'nun da değişen güvenlik ortamına uyum sağladığını görülmektedir. Örneğin, 2002 Prag zirvesinde organizasyon yeteneklerini siber saldırılara karşı geliştirme kararı alırken, özellikle Estonya ve Gürcistan'daki siber saldırılar psikolojik bir eşik olmuş ve ittifak içinde siber güvenlik tartışmalarını kuvvetlendirmiştir. Bu itibarla, 2008'de NATO Siber Savunma Politikası hazırlanmış ve netice olarak 2009'da ise «Rapid Reaction Teams» kurulmuştur. Son olarak, daha önce de belirtildiği üzere 2016 Varşova zirvesinde ise siber uzayın da bir savaş alanı olarak tanımlanmasına karar verilmiştir (Darıcılı, 2015: 413).

Birleşmiş Milletler (BM) ise siber güvenlik konusundaki çalışmalarını 1980'den beri sürdürmektedir. Siber güvenliğe ilişkin faaliyetler genel olarak büyük ölçüde BM Genel Kurulu kararları vasıtası ve bir BM Ajansı olan ITU (Uluslararası Telekomünikasyon Birliği) üzerinden yürütülmektedir. BM nezdinde ayrıca Siber Suçlara Dair Hükümetlerarası Uzmanlar Grubu çalışmakta ve bu girişim, diğer çalışmalara nazaran daha kapsayıcı olarak düşünülebileceği ve gelecekte siber uzayın barışçıl kullanımı konusunda uluslararası normların oluşumunun önünü açabileceği değerlendirilmektedir (Önok, 2013: 1239).

5. SONUÇ VE TARTIŞMA

Günümüzde siber uzay ve siber güvenlik kavramlarını uluslararası ilişkiler disiplini kapsamında değerlendiren yaklaşımların önemi artmaktadır. Bunun temel nedeni ise devletlerin siber uzayı askeri kapasitelerini (hard power) geliştirme noktasında yeni bir fırsat mecrası olarak görmeleridir. Bu nedenle de siber uzay alanı üzerinde devletlerarasındaki mücadele artmakta, siber güvenlik meseleleri de hiç olmadığı kadar uluslararası ilişkiler disiplini ve güvenlik çalışmalarının analiz konusu olarak ele alınmaktadır.

Öte yandan tarihsel bir perspektif ile konuya yaklaşırsak Amerika Birleşik Devletleri (ABD) ve Sovyetler Birliği arasında Soğuk Savaş döneminde tecrübe edilen askeri rekabet ve uzay yarışı kapsamında ortaya konulan yenilikler günümüzde siber uzay temelli teknolojilerin temellerini teşkil ettiği ileri sürülebilecektir. Bununla birlikte Söz konusu rekabet 1990'lı yıllar boyunca da Rusya Federasyonu (RF) ve ABD arasında daha düşük profilli bir şekilde sürmüştür. Ancak 2000'li yıllar ile birlikte Çin Halk Cumhuriyeti'nin (ÇHC) de içinde bulunduğu teknolojik ilerleme ve ekonomik gelişim ile birlikte bu rekabete dâhil olmuştur. Bu kapsamda günümüzde siber uzay alanı merkezli

gelişmelerin ve teknolojilerin ABD, RF ve ÇHC tarafından domine iddia edilebilecektir. Bu domine etme sürecinin temel motivasyonu ise söz konusu devletlerin siber uzayı uluslararası sistemdeki güç mücadeleleri noktasında yeni bir fırsat olarak okumalarıdır.

Ayrıca siber savaş, siber terör, siber silahlar gibi tanımların üzerinde küresel bir uzlaşı zor olsa da, siber uzayın barışçıl kullanımı için uluslararası işbirliği, küresel standartlar ve normların oluşturulması hala söz konusu olamamıştır. Bunun temel nedeni ise bahse konu küresel güçlerin siber uzay alanı üzerindeki belirtilen rekabet süreçlerdir. Bu noktada söz konu tarzda bir uzlaşının sağlanması uluslararası sistemin barışçıl bir yönetimi için elzem hale gelmiş olmakla birlikte, kısa ve orta vadede böyle bir uzlaşın mümkün olamayacağı açıktır. Bahse konu bir uzlaşı tesisi edilmesi noktasında devletlerarası siber alana özgü geliştirilmiş bir sözlüğün ya da ortak ve teknik bir dilin kullanımı bir öneri olarak sunulabilir. Böyle bir uzlaşı, gelecek dönemler için siber uzay alanına dair başka uzlaşı alanların yaratılmasına da vesile olabilecektir.

Bunlarla birlikte tüm fikir ayrılıklarına rağmen küresel ölçekte siber sorunların tartışıldığı bir platform oluşturulması da siber uzay alanına dar tartışmaların giderilmesi noktasında önemli bir başlangıç adımı olabilir. Böyle bir platformun oluşturulması noktasında ise devlet dışı aktörlerin yani uluslararası örgütlerin ve hatta siber uzayda etkili bir aktör konumda olan bireylerin önemli rol oynayabileceği de düşünülebilir.

Yaşadığımız hayat ile siber dünya arasındaki bütünleşik durum, siber güvenliği yalnızca bilgi ve iletişim teknolojileri güvenliği çerçevesinden açıklanamayacak bir mücadele ve etki alanı olmasına sebep olmuştur. Gerek uluslararası ve ulusal, gerek kurumsal güvenlik açısından farklı disiplinleri içine alacak bütünleşik bir siber mücadele yaklaşımına ihtiyaç duyulmaktadır. Bu amaçla, multidisipliner siber mücadele kavramını geliştirip, bilimsel ve akademik literature katkıda bulunulmalıdır.

KAYNAKÇA

Bıçakcı, S. (2014). NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik. Uluslararası İlişkiler, 10 (40) s.101-130.

Chochri, N. (2016). Explorations in Cyber International Relations: A Research Collaboration with MIT and Harward University, MIT Political Science Department Research Paper No. 2016-1. Available at SSRN: https://ssrn.com/abstract=2727414 or http://dx.doi.org/10.2139/ssrn.2727414

Clark, D. and Choucri, N. (2013). Who Controls the Cyberspace? Bulltein of the Atomic Scientists, 21.

Darıcılı, A. B. ve Özdal B. (Güz 2017). Rusya Federasyonu'nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi, Ahmet Yesevi Üniversitesi Türk Dünyası Sosyal Bilimler Dergisi (BİLİG), Avrasya'nın Siyasal İktisadı Özel Sayısı, ss. 121-146.

Darıcılı, A. B. ve Özdal, B. (Nisan 2017), Enformasyon Savaşı Bağlamında Rusya Federasyonu ve Türkiye İlişkilerinin Analizi, İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi, 4 (1), ss.19-40.

Darıcılı, A. B. (2014). Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırılar, Uludağ Üniversitesi Sosyal Bilimler Dergisi, 7 (2), ss.1-19.

Darıcılı, A. B. (2015). NATO'nun Siber Güvenlik Stratejisinin Analizi, VII. Uludağ Uluslararası İlişkiler Konferansı (Uluslararası Sistemde Yeni Düzen Arayışları), 21-22 Ekim 2015, ss. 407-417.

Erendor, M. E. (2017). Risk Toplumu ve Refleksif Modernleşme Çerçevesinde Siber Terörizm: Tanımlama ve Tipoloji Sorunu, Cyberpolitik Journal, 1 (1), ss. 114-133.

Erendor, M. E. ve Tamer, G. (2018), The New Face of the War: Cyber Warfare, Cyberpolitik Journal, 2 (4), ss. 57-74.

Erdoğan, İ. (2013). Küreselleşme Olgusu Bağlamında Yeni Güvenlik Algısı, Gazi Üniversitesi Akademik Bakış Dergisi, 6 (12), ss. 265-292

Geers, K. (2011). Strategic Cyber Security. NATO Cooperative Cyber Defense Center of Excellence.

Korkmaz, A. (2013). Arap Baharı Sürecinde İnternet ve Sosyal Medyanın Rolü. International Symposium on Language and Communication: Research Trends and Challenges (ISLC (s. 2). www.inlcs.org/online/Book14.pdf.

Önok, M.("Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararasi İşbirliği", Marmara Üniversitesi Hukuk Fakultesi Hukuk Araştırmaları Dergisi, Prof.Dr. Nur Centel'e Armağan Özel Sayısı, ss.1229-1269

NATO. (2016). Varşova Zirvesi Sonuç Bildirgesi. Brussel: NATO. 7 4, 2018 tarihinde, http://www.nato.int/cps/en/natohq/official_texts_133169.htm adresinden alındı

Nye, J. (2010). Cyber Power. Harward Kennedy School: Belfer Center for Science and International Relations, Harvard Kennedy School, Research paper, ss.1-24

Yayla, M. (2014). Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı. Hacettepe Üniversitesi, 4 (2), ss. 181-200.

Yorulmaz, M. (Temmuz 2014). Değişen Uluslararası Güvenlik Algılamaları Bağlamında Türkiye-Yunanistan İlişkilerinde Değişmeyen Güvenlik Paradoksu. Balkan Araştırma Enstitüsü, 3 (1) ss. 103-135.