Centre for Economics and Foreign Policy Studies

edam

EDAM Siber Politikalar Kağıtları Serisi
2017/1

Siber Güvenlik: Beşinci Boyutu Anlamak

Haziran 2017

Can Kasapoğlu
Savunma Analisti, EDAM

Robert Bosch Stiftung
tarafından desteklenmiştir.

GİRİŞ

Bu kağıt, Siber güvenlik alanında bir giriş ve temel yaklaşımlara ilişkin referans olması amacıyla kaleme alınmıştır. Siber-uzay, uluslararası ilişkilerde güncel meselelerin yer aldığı dört fiziksel boyuta (kara – hava – deniz – uzay) eklenen, insanlar tarafından üretilmiş beşinci bir boyuttur. Nitekim 2016 Varşova Zirvesi'nde NATO tarafından operasyonel bir alan olarak resmen tanınmış bulunmaktadır[1].

Öte yandan siber-uzay, hem diğer boyutlardan radikal biçimde farklılaşan karakteristik nitelikler göstermektedir, hem de dört fiziksel boyut ile karmaşık ilişkiler ağına sahiptir. Toplumlar, dijitalize bilgi odaklı yaşadıkları ölçüde siber tehditlere karşı daha hassas hale gelmektedir. Özellikle enformasyon ağları ve sistemlerine bağımlı olan toplumlar için siber alandaki riskler çok daha fazladır. Dolayısıyla gelişmişlik düzeyi, ironik bir biçimde, ülkeleri siber risk ve tehditlere daha açık hale getirmektedir.

Keza bu yönüyle siber güvenliğin kendi özgün jeopolitiğinin hızla şekillendiğini söylemek mümkündür. Örneğin, bu raporun kaleme alındığı dönemde, ABD'nin Güney Kore topraklarına gelişmiş hava ve füze savunma sistemleri – THAAD – yerleştirmesi, Çin Halk Cumhuriyeti'nin ciddi siyasi tepkisi ile karşılaşmıştır. Bu noktaya kadar konu, Çin, Kuzey Kore, Güney Kore ve ABD'nin bölgedeki kuvvetleri açısından, hava ve füze savunmasına ilişkin bir askeri stratejik denge değiştirici sorunu olarak görülebilir. Ancak bahse konu kriz sürerken, önce THAAD sistemlerine yönelik Çin bağlantılı espiyonaj amaçlı siber saldırı haberlerinin çıkması[2] ve müteakiben ABD'nin THAAD sistemleri ile birlikte siber güvenlik unsurlarını da bölgeye konuşlandıracağının belirtilmesi[3], siber güvenlik konularının güncel siyasi ve askeri meseleler ile nasıl iç içe geçtiğini gösterir niteliktedir. Daha çarpıcı bir örnek, hem siber terörizm ile mücadele hem de bu eksende siber-uzayın jeopolitiğine ilişkin detayları gözler önüne sermektedir: 2016 yılında ABD yönetimi IŞİD'in siber faaliyetler ve propaganda amaçlı kullandığı unsurlara yönelik kapsamlı bir operasyon icra etme kararı almıştır. Operation Glowing Symphony adı verilen siber güvenlik faaliyetine ilişkin kritik bir detayın ABD yönetiminde görüş ayrılıklarına neden olduğu bugün basın kaynaklarınca bildirilmektedir. Görüş ayrılığının temel nedeni ise, siber saldırı düzenlenecek IŞİD hedeflerinin konuşlu bulunduğu ülkelere, ki bunların içinde ABD'nin müttefikleri ve partnerlerinin de bulunduğu söylenmektedir, istihbarat işbirliği kanalları üzerinden haber verilmesinin gerekip gerekmediği olmuştur[4]. Gerçekten de üçüncü ülke topraklarında kinetik etkiye neden olmayacak ancak üçüncü ülkelerde bulunan siber terörizm unsurlarını, siber-uzayın imkanlarını kullanarak akamete uğratacak bir terörle mücadele faaliyetinin 'coğrafi ve jeopolitik mahiyeti' nasıl algılanmalıdır? Siber terörizm ile ilişkilendirilen hedeflere yönelik siber saldırı düzenlemek ile bu hedeflere yönelik klasik terörle mücadele ope-

1 Varşova Zirvesi sonuç bildirgesi için bkz. http://www.nato.int/cps/en/natohq/official_texts_133169.htm, Erişim Tarihi: 4 Haziran 2017.

2 CNN, http://edition.cnn.com/2017/04/27/asia/china-south-korea-thaad-hack/index.html, Erişim tarihi: 10 Haziran

3 IISS, Cyber Report 1 to 7 June, https://www.iiss.org/iiss%20voices/blogsections/iiss-voices-2017-adeb/june-f086/cyber-report-1-to-7-june-1817, Erişim tarihi: 10 Haziran 2017.

4 The Washington Post, https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html?utm_term=.4dc4def5c91b, Erişim tarihi: 10 Haziran 2017.

rasyonları düzenlemek arasında bir bağlam farkı var mıdır ya da olmalı mıdır?

Siber güvenlik, içerdiği risk ve tehditler ile geniş spektrumdaki aktörlerin etkileşimleri bakımından da kompleks bir araştırma ve pratik alanına karşılık gelmektedir. Örneğin, Mart 2017'de İsrail ve Japonya arasında imzalanan siber güvenlik işbirliği anlaşmasını[5] jeopolitik ve uluslararası ilişkiler bağlamında nasıl değerlendirmek, hangi ortak tehdit algımalarının bir ürünü olarak kabul etmek gerekecektir? Bu yönüyle, siber güvenlik meselelerinin isabetli biçimde kavramsallaştırılmasında, doğru değerlendirilmesinde, geçerli parametrelerinin anlaşılmasında ve geleceğe ilişkin projeksiyon yapılmasında ciddi zorluklar barındırmaktadır. Öte yandan, sayılan tüm analitik faaliyetler aynı zamanda siber güvenlik kapasitesinin geliştirilmesi bağlamında birer zarurettir. Zira, siber alanda yaşanan gelişmelerin baş döndürücü hızı, aynı süratte adaptasyon yeteneklerine duyulan gereksinimi de beraberinde getirmektedir. Daha açık bir anlatımla, siber güvenlikte belirleyici trendlere yönelik güçlü bir paradigma üretmeksizin adaptasyon göstermek ve siber alanı yönetmek mümkün görünmemektedir.

Günümüzde, EDAM da dahil olmak üzere, savunma alanında çalışan birçok düşünce kuruluşu, bilgiye ulaşım imkanları ve teknik kapasiteleri ölçüsünde, çeşitli aktörler arasında askeri stratejik dengeyi analiz etmekte ve senaryo çalışmaları yapabilmektedir. Böylelikle bir ülkenin, söz gelimi, stratejik hava ve füze savunma yetenekleri, savunma ekonomisinin ve endüstrisinin askeri hedeflerini destekleme kapasitesi ya da güç projeksiyonu imkan ve kabiliyetleri gibi konular hakkında açık-kaynaklı analizler üretebilmekteyiz ve aktörleri bu sahalardaki performanslarına göre kategorize edebilmekteyiz. Öte yandan bir devletin siber güvenlik yeteneklerini ya da ne kadar 'caydırıcı bir siber aktör' olduğunu değerlendirmek kolay değildir. Buradaki zorluk salt güvenilir bilgiye ulaşma aşamasında değil, bilgiyi anlamlandıracak kavramsal altyapıdaki eksikliklerden de kaynaklanmaktadır.

Yukarıda aktarılan sorunsala ilişkin kesin yanıtlar bulmak için olmasa da, en azından farklı yaklaşımlar sergilemek amacıyla, bu çalışma öncelikle siber-uzaya ilişkin kavramsallaştırma hususlarını değerlendirmektedir. Müteakip olarak, siber-uzayın özgün nitelikleri ve siber güvenlik ortamında temel fonksiyonlara ilişkin mülahazalar aktarılacaktır. Daha sonra, siber risk ve tehdit paternleri ile siber güç ve milli güvenlik arasındaki sistematik ilişkiyi inceleyen alt başlıklar bulunmaktadır. Son olarak, konuya ilişkin değerlendirmeler okuyucunun dikkatine sunulacaktır.

SİBER-UZAY VE KAVRAMSALLAŞTIRMA SORUNSALI

Siber-uzay modern yaşamı tanımlayan en önemli unsurların başında gelmektedir. Bireyler ve toplumlar arasındaki etkileşimin olağanüstü düzeyde artması, siber-uzayın en önemli etkileri arasındadır; nitekim, 2000 ile 2010 yılı arasında geçen on yıllık süreçte internet kullanımı 360 milyon insandan 2 milyar insana çıkmıştır. Siber-uzay, ticaret, finans, girişimcilik, yeni fikirlerin gelişmesi, sosyal ağların genişlemesi ve teknolojik ilerlemeler bakımından kritik bir rol oynamaktadır[6]. Bu nedenle siber-uzaya ilişkin tüm gelişmeler uluslararası ilişkileri güvenlikten ekonomiye, uluslararası hukuktan politik psikolojiye, savunma konularından teknolojik inovasyona kadar tüm boyutlarıyla etkilemektedir.

Siber-uzay kavramını internete indirgeyen yaklaşımlar

5 The Jerusalem Post, http://m.jpost.com/app/article/489647, Erişim tarihi: 10 Haziran 2017.

6 The US Department of Defense, Strategy for Operating in Cyberspace, 2011, p.1.

isabetli değildir. Zira siber-uzay interneti kapsamakla birlikte, donanım, yazılım, enformasyon sistemleri, bu unsurlarla ilgili kişiler ve ağlar arasındaki etkileşimin tamamını da içermektedir. Birçok devletin ulusal siber güvenlik prosedürleri ve protokolleri, bilgi güvencesi, bilgisayar güvenliği ve bilgi güvenliği gibi kavramların önemine atıf yaparak başlamaktadır[7]. Öte yandan bahse konu terminolojinin birbirinin yerine kullanılması da gözden kaçmamaktadır. Bilgi güvenliği, hangi formda olduğuna bakılmaksızın – örn. elektronik bilgi ya da basılmış doküman – tüm verilerin korunmasını esas almaktadır. Bilgisayar güvenliği ise enformasyonun korunması perspektifinden çok bilgisayar sistemlerinin işleyişlerinin akamete uğramaması ile ilgilenmektedir. Bilgi güvencesi ise bilgi güvenliğinin bir üst kümesi niteliğindedir ve hangi bilgilerin korunacağına ilişkin analizler yapılmasını ve vizyon teşkil edilmesini içermektedir[8].

Bilgi güvenliği, enformasyon ve telekomünikasyon sistemlerinin güvenliği, siber güvenlik, ağ güvenliği, internet güvenliği ve kritik enformasyon altyapısının güvenliği birbiri ile sıkı sıkıya ilişkili bir yapıya karşılık gelmektedir[9].

Bu noktada internet güvenliğine ilişkin teknik ve siyasi içerikli nüanslardan da kısaca söz etmekte yarar vardır. Teknik tanımı ile internet güvenliği internete bağlı servislerin ve ilgili enformasyon ve telekomünikasyon olanaklarının aksamaması olarak algılanırken, politik kontekst, internet içeriğinin yasal niteliklerini de dikkate almaktadır. İkinci bakış açısı, doğal olarak, ülkeler arasında sistem farklılıklarının ürünü olan siyasal mülahazaları da içermektedir[10]. Örneğin, Ruanda'da Ağustos 2017'de yapılacak olan, esasen mevcut devlet başkanı Paul Kagame ve Ruanda Yurtsever Cephesi gölgesi altında yürütülen seçim sürecinde, başkan adaylarının sosyal medya paylaşımlarının internette yer almadan önce seçim komisyonu onayına tabi olmasını öngören bir hukuki düzenleme yapılmıştır[11]. Her ne kadar bu düzenlemenin nefret suçlarını önlemek amacıyla yapıldığı belirtilse de, özellikle seçim sürecinde ifade özgürlüğünü kısıtladığı düşünülmektedir. Bununla birlikte, Ruanda yönetimine göre bu düzenleme 'internet güvenliğinin' bir parçasıdır. Kanımızca, bahse konu olay, internet güvenliğine ilişkin politik mülahazaların ön plana çıktığı yaklaşıma iyi bir örnek teşkil etmektedir.

Ağ güvenliği, bilgi güvenliğini sağlayacak ağların dizaynı ve işletilmesine odaklanırken; kritik enformasyon altyapısının güvenliği ise kritik altyapı tedarikçilerinin (enerji, telekomünikasyon, su yönetimi vb.) işlettiği ya da sağladığı sistemlerin güvenliği ile ilgilenmektedir. Dolayısıyla kritik enformasyon altyapısının bilgi güvenliği risklerine, ağ güvenliği risklerine, internet güvenliği risklerine ve siber güvenlik risklerine karşı korunmasından sorumlu durumdadır[12].

Siber güvenliği küresel ölçekte etkileyen en önemli parametrelerden biri de, siber harbe ilişkin teknoloji ve hukuki normları düzenleyen uluslararası geniş çaplı bir uzlaşının ya da bu uzlaşı zeminini denetleyecek kurumun bulunmayışıdır. Bu durum, teknolojik gelişmelerin baş döndürücü hızı da göz önünde bulundurulduğunda, hem güncel hem de yakın geleceğe ilişkin

7 Melissa E. Hathaway and Alexander Klimburg, "Preliminary Considerations: On National Cyber Security", National Cyber Security Framework Manual, Alexander Klimburg [ed.], NATO CCDCOE, Tallinn, 2012, p.9.

8 Ibid.

9 Ibid. pp. 10 – 11.

10 Ibid.

11 Daily Monitor, http://www.monitor.co.ug/News/World/Diplomats-concerned-over-Rwanda-social-media-controls/688340-3949076-format-xhtml-ohyc1s/index.html, Erişim tarihi: 10 Haziran 2017.

12 Melissa E. Hathaway and Alexander Klimburg, "Preliminary Considerations: On National Cyber Security", National Cyber Security Framework Manual, Alexander Klimburg [ed.], NATO CCDCOE, Tallinn, 2012, pp.10-11.

ciddi belirsizlikleri beraberinde getirmektedir[13]. Ayrıca bu noktada belirtilmelidir ki, siber dünyaya ilişkin yeterli kavramsallaştırma çalışması olmamasından dolayı, siber-uzayda icra edilen hemen her düşmanca aktivite, spekülatif biçimde, 'siber harp' kategorisinde değerlendirilebilmektedir. Oysa ki, siber suçlardan siber espiyonaja kadar uzanan geniş bir spektrum söz konusudur ve bu sahalar en az siber harp kadar kritiktir. Zira bahse konu faaliyetler devletlere ve devlet dışı gruplara hem hassas bilgilere erişim sağlamakta hem de geleceğin siber harp ortamında kullanılacak yetenekler için bir 'laboratuvar' niteliği taşımaktadır[14].

Kanımızca kavramsallaştırma alanında yaşanan eksikliklerin en önemli sonuçlarından biri de, konuya ilişkin analizlerde tanım ve terminoloji bütünlüğü sağlanamaması şeklinde tezahür etmektedir. Bu boşluk önemlidir, çünkü konunun entelektüel takibi ve gelişimi için ortak bir dil oluşturulması zorunludur.

Siber-uzaya ilişkin tanımlar değişiklik gösterse de, genel hatlarıyla siber-uzay, verilerin bilgisayarlar ve diğer elektronik cihazlar ile depolanabildiği, değiştirilebildiği ve iletilebildiği ağ tabanlı sistemler ve bu sistemler ile bağlantılı fiziksel altyapı olarak betimlenebilir. Siber-uzayın özgün niteliklerinin temelinde bilginin oluşturulması, saklanması, değiştirilmesi, iletimi ve kullanımı için elektronik imkanların ve elektromanyetik spektrumun kullanılması ile tüm bu işlemlerin enterkonekte enformasyon ve komünikasyon teknolojileri tabanlı sistemler ile gerçekleştirilmesi bulunmaktadır[15]. Bu nedenle verilerden bilgiye, bilgiden semantik süreçlere uzanan yol, siber-uzayda fiziksel katmandan kişi ve kurumlara doğru ilerleyen ilişkiler ağı hakkında da ciddi bir fikir vermektedir. Bahse konu hareketlerin takibi, siber-uzaydaki trendlerin daha doğru anlaşılmasını kolaylaştıracaktır.

Günümüz teknolojik gelişmeleri, barış durumunda olduğu gibi savaş ortamında da başarı gösterebilmek için siber-uzaya belirli oranda erişimin bir ön koşul haline geldiğini göstermektedir. Ağ – merkezli harp ve 'enformasyonize' harp sahası (informationalized battlespace) gibi konseptlerin siber-tabanlı sistemler ve yetenekler olmaksızın icra edilmesi neredeyse olanaksızdır[16]. Zira, uçuş yolu sırasında bir mühimmatın rota ve hedef bilgilerinin yeniden programlanması, GPS ve uydu teknolojilerinden gerçek-zamanlı bilgi erişimi sağlanması gibi tüm fonksiyonlar için siber-uzaya ilişkin imkan ve kabiliyetler zaruridir[17]. Ayrıca, siber ve elektronik harp imkanlarının birleşmesi, yakın gelecekte önemli kinetik sonuçlar doğurabilecektir. Nitekim, bu raporun yayıma hazırlanması aşamasında Hindistan Hava Kuvvetleri'ne ait Su-30 tipi bir savaş uçağının Çin sınırına yakın bir yerde düşmesi ve müteakip olarak Hint kaynaklarının, 'kazanın' Çin'in siber yeteneklerinden kaynaklandığını belirtmesi dikkat çekicidir[18].

Dolayısıyla siber yetenekler giderek sahip olunması avantaj oluşturan bir profilden çıkarak, sahip olunması zorunlu bir kimliğe bürünmektedir. Ayrıca, bahse konu sahadaki gelişmelerin artan bir ivme ile seyretmesi, siber yeteneklere ilişkin zorunlulukların ilerleyen yıllarda etkilerini daha da hissettireceğini göstermektedir. Ayrıca bazı aktörler siber yeteneklerini geliştirdikçe, arkadan gelen diğerlerinin açığı kapatmaları kümülatif olarak zorlaşacaktır. Bu nedenle 21. yüzyıl, siber teknolojilerde atılım yapanların yarışta ciddi avantaj

13 Fred, Schreier. On Cyberwarfare, DCAF Horizon 2015 Working Paper 7, pp.7-9.

14 Ibid.

15 Ibid. pp.9-13.

16 Ibid.

17 Ibid.

18 Indian Defence News, http://www.defencenews.in/article/Indias-Su-30MKI-likely-downed-by-Chinas-Cyber-Weapons-262280, Erişim tarihi: 10 Haziran 2017.

sağlayacakları bir döneme karşılık gelmektedir.

Siber-uzay üç katmandan oluşan bir yapıyı haizdir. İlk (fiziksel) katman, coğrafi ve fiziksel unsurları, iletim imkanlarını, platformları, elektronik cihazları ve bilgisayarları barındırmaktadır. Veriler buradaki araçlar ile iletilirler. İkinci katmanda (logical layer) internet protokolü ve URL (uniform resource locator) üzerinden bilgiye ulaşılabilir, sözdizimsel faaliyetlerde bulunulur. Üçüncü katman (cyber – persona) ise ağ üzerindeki – kişiler de dahil olmak – üzeri tüm aktörleri tanımlamaktadır. Semantik faaliyetler bu katmanda icra edilmektedir[19]. Bu üç katman arasındaki birçok yönde ilerleyen etkileşimler siber-uzaydaki trendleri ve temaları teşkil etmektedir.

Bu aşamadan itibaren, siber-uzayın karakteristik niteliklerinin analizine geçilecektir. Bu çalışma tarafından siber-uzayın jeopolitiği olarak da betimlenen özgün nitelikler manzumesinin doğru anlaşılması önemlidir. Zira, siber-uzayın farklı kuralları, siber ortamdaki aktörlerin angajman biçimlerinde de diğer fiziksel boyutlara kıyasla temel değişikliklere neden olmaktadır.

SİBER-UZAYIN KARAKTERİSTİK ÖZELLİKLERİ

Siber-uzay salt kara – deniz – uzay – hava gibi objektif gerçekliğin hakim olduğu boyutlarda değil, bilginin depolandığı, işlendiği ve iletildiği kognitif boyut ile de birlikte varlığını sürdürmektedir. Ancak siber-uzayı fiziksel boyutlardan farklı kılan belirleyici hususiyeti, bahse konu boyuta bizatihi oluşturmak için elektronik teknolojilerden ve elektromanyetik spektrumdan yararlanılması gerektiğidir. Bu karakteristik, siber-uzaya diğer boyutların ötesine geçen özgün bir nitelik kazandırmaktadır[20].

Elektromanyetik spektrum olmadan, enformasyon ve komünikasyon teknolojilerinden bahsetmenin imkanı yoktur. Bu denkleme en başta mikroelektronik aygıtlar ile fiberoptik kablolar dahildir. İkinci olarak, siber-uzay, var olabilmek için insan-yapımı şeylere gereksinim duyar. Oysa kara – deniz – hava – uzay boyutları, insan katkısına gereksinim duymadan 'var olabilmektedir'. Dolayısıyla siber-uzay, insanın elektromanyetik spektruma ilişkin inovatif aktivitelerine ve teknoloji geliştirme kapasitesine endekslidir[21]. Üçüncü belirleyici husus, siber-uzayın sürekli kopyalanabilmesidir. Kara – deniz – hava – uzay fiziksel boyutları 'üretilebilir' değildir; oysa ki siber-uzay üretilebilen bir nitelik arz etmektedir. Dördüncü olarak, siber-uzaya erişimin ilk aşamaları göreli olarak az maliyetlidir. Söz konusu maliyet uzaya erişim veya okyanuslarda sürekli donanma varlığı ile kıyaslanamayacak ölçüdedir[22]. Bu nedenle siber-uzayda stratejik etki oluşturmaya ilişkin faaliyetler milyarlarca dolarlık bütçeler, yüksek sayıda personel ihtiyacı ya da silah gerektirmemektedir. Dar bir uzman havuzu ve daha düşük finansman ile yeterli bilgisayar ağı siber-uzaya giriş ve stratejik etki oluşturmak için atılmış adımlar anlamına gelebilmektedir. Son olarak siber-uzay, taarruza yönelik stratejilerin müdafi stratejiler karşısında üstünlük sağladığı bir alandır[23].

Yukarıda son sayılan nitelik, yani siber-uzayın ofansif yöntemlere daha olumlu yanıt vermesi, büyük önem arz etmektedir. Zira bahse konu nitelik, siber alanda faaliyet gösteren aktörlerin yol haritalarını ve pers-

19 The United States Army War College, Strategic Cyber Operations Guide, 2016, p.7.

20 Fred, Schreier. On Cyberwarfare, DCAF Horizon 2015 Working Paper 7, pp.12-16.

21 Ibid.

22 Ibid.

23 Ibid.

pektiflerini de belirleyecektir. Daha açık bir anlatımla, sadece devletlerin ve devlet dışı aktörlerin yönetimlerindeki, ya da klasik realist bakış açısıyla insan doğasındaki, saldırganlık eğilimleri değil, ancak siber-uzayın mücadele parametreleri bu boyutta çatışma trendlerini de körükleyebilir. Kanımızca, ofansif siber faaliyetlere ilişkin gelişmişlik düzeyi, siber yarışın kazananlarını da belirleyecektir. Söz konusu gelişmişliğin salt teknolojik atılım ile değil, barış ve savaş durumu arasında muğlaklaşan alanlara dair yeni paradigma üretmeye yönelik entelektüel faaliyetleri de kapsadığı vurgulanmalıdır.

Öte yandan, siber güvenliğin ofansif faaliyetlerin egemenliğinde olduğu ileri sürülürken, strateji teorisi kapsamında taktik ve stratejik hedefler arasındaki ayrımı da iyi yapmak gerekmektedir. Belki de bu konudaki en önemli örnek, 2007 yılında Baltık ülkesi Estonya'ya karşı düzenlenen siber saldırılardır. Ülkedeki Rus azınlıkla Tallinn yönetimi arasında gerginliklerin devam ettiği dönemde gerçekleşen ve çoğunlukla Rusya'ya atfedilen sistematik siber saldırılar, Estonya'da birçok servisin ciddi şekilde durmasına neden olmuştur. Bu nedenle, yeterli ofansif siber kapasitenin kısa sürede ve taktik seviyede sonuç alıcı olduğunu göstermektedir. Öte yandan, bahse konu siber saldırılar, Tallinn yönetiminin dış politika ve kamu politikalarındaki yönelimlerini değiştiremediği gibi, Estonya'yı NATO'nun önemli siber merkezlerinden biri haline getiren süreci de beraberinde getirmiştir. Bu açıdan bakıldığında, siber yeteneklerin, mevcut haliyle bile tek başına uygulandığında, stratejik düzeyde ne denli sonuç alıcı olduğu da tartışmalı bir konudur[24].

SİBER GÜVENLİK ORTAMINDA BELİRLEYİCİ FONKSİYONLAR

Siber saldırı ve siber saldırı girişimleri, oldukça geniş bir alana karşılık gelmektedir ve çeşitli boyutlardaki yaygınlıkları giderek artmaktadır. Ülkelerin gelişmişlik seviyesi ve konjonktürel parametrelere bağlı olarak siber tehdit seviyesi olağanüstü düzeylere çıkabilir. Örneğin, sadece 2017 yılının ilk dokuz haftasında, Almanya Silahlı Kuvvetleri bilgisayar sistemlerine yönelik 284,000 siber saldırı girişimi olduğu resmi makamlarca ifade edilmiştir[25].

Siber tehditler, aktör, yöntem ve hedefleri bakımından kategorize edilmektedir. Kuşkusuz sayılanların arasında en yıkıcı etki potansiyeline sahip kategori, devlet düzeyinde aktörlerin milli askeri stratejilerinin bir parçası olarak icra edilen siber harp ve geniş kapsamlı siber espiyonaj fonksiyonlarıdır. Siber harp yetenekleri gerek elektronik harp kapasitesini desteklemesi, gerek kritik askeri ve sivil altyapıları hedef alabilmesi bakımından oldukça büyük tehlikeler arz edebilmektedir. Günümüzde birçok devlet düzeyindeki aktör ofansif siber yeteneklere büyük yatırımlar yapmakta, bahse konu sahayı ulusal güvenlik ve savunma stratejilerine ve doktrinlerine entegre etmekte ve bu görevler için özel ihtisas birimleri teşkil etmektedir[26]. İkinci olarak, siber terörizmin devlet-dışı terörist tehdit faktörleri arasında giderek önem ve yıkıcılık kazanan bir yere sahip olduğu görülmektedir. Son olarak, geniş bir spektrumda, siber alanda işlenen suçlar risk ve tehdit ortamını tamamlamaktadır. Bu noktada kritik olan husus, siber tehditlerin, tıpkı patojenlerin antibiyotik direnci geliştirerek evrimleştiği gibi daha dayanıklı ve tespitlerinin daha güç olacağı formlara evrildiğinin bilinmesidir[27].

24 Konuya ilişkin ayrıntılı bir inceleme için bkz. Sergei, A. Medvedev, Offense-Defense Analysis of Russian Cyber Capability, the US Naval Postgraduate School, 2015.

25 Politico, http://www.politico.eu/article/german-cybersecurity-chief-army-attacked-over-284000-times-this-year/, Erişim tarihi: 10 Haziran 2017.

26 Canada's Cyber Security Strategy: For a Stronger and more Prosperous Canada, 2010, p.5.

27 Ibid. P.6.

Siber terörizmin, dikkat çekici biçimde, hem klasik terör eyleminin hem de siber saldırıların karakteristik nitelikleri olan toplumda korku oluşturma ve belirsizliği bir kuvvet çarpanı haline getirme fonksiyonlarını bir arada kullandığı; ayrıca, terör eylemlerinin stratejik hedefleri arasında ilk sıralarda bulunan kamuoyu ve medya ilgisini çekme hususunda da ciddi bir kapasiteye sahip olduğu müşahede edilmektedir[28]. Elbette siber terörizm tehdidi ile ilgili en büyük endişelerden biri de, geniş çaplı, 'klasik' bir terör eylemine eşlik edecek ve kriz anında acil durum ve iletişim sistemlerini paralize edebilecek bir siber terör saldırısının gerçekleşmesidir. Bazı uzmanlar söz konusu tehdidi 'Siber Pearl Harbor' olarak betimlemektedir[29].

Kanımızca siber terörizmin en kritik ve yıkıcı hali de, yukarıda alıntılanan 'müşterek terör konsepti' çerçevesinde icra edildiği durumda ortaya çıkacaktır. Bu nedenle, bu çalışmanın giriş bölümünden itibaren vurgulanan analitik kapasite ve öngörü yetenekleri, siber güvenlik yönetiminde yaşamsal fonksiyonlardır. Bilhassa siber terör risk ve tehditleri ile mücadelede, önleyici bir yaklaşımın 'hayal gücü eksikliğini' de engelleyerek yaşama geçirilmesinde yarar görülmektedir.

Ofansif siber operasyonlar, özellikle ülke savunmasına ilişkin bir çerçevede icra edildiğinde, bir veya birkaç sisteme siber-uzay yoluyla saldırmak suretiyle ciddi nitelikli zarar vermeyi hedefleyen faaliyetlerdir. Teorik olarak böyle bir saldırı, sistemin software kontrolleri ile verilebilecek her türlü yıkıcılığa ulaşma yeteneğine sahiptir[30]. Bu noktada taarruza yönelik siber operasyonun seviyesine bağlı olmak üzere, saldırıya maruz kalan sistem üzerinde kontrolün tamamen kaybedilmesi ve / veya düşman unsurların sistem üzerindeki kontrolü bütünüyle ele geçirmesi de dahil olmak üzere, geniş spektrumda bir risk ve tehdit manzumesinden söz etmek mümkündür[31].

Bir sisteme yönelik siber saldırının yıkıcı etkilerinin ne boyutta olacağını belirleyecek parametrelerden biri de ofansif aktörün hedef sisteme ve nasıl çalıştığına ilişkin bilgi kapasitesidir. Daha açık bir anlatımla, hedef sisteme ilişkin istihbari veriler ne kadar geniş ve kesin olur ise, siber taarruzun yıkıcı etkileri ve sonuçları da o denli ağır olacaktır. Dolayısıyla siber-espiyonaj, siber saldırıların boyutlarını ve etkilerini genişletmek bakımından önem arz etmektedir.

Siber saldırılara karşı koymanın iki temel yolu bulunmaktadır. Bunlardan ilki, yani saldırıyı engellemek, sisteme istenmeyen girişlerin engellenmesi, saldırganların istismar edecekleri açıkların kapatılması ve saldırganların sisteme ilişkin bilgi edinme kapasitelerinin kısıtlanmasıdır. Bu noktaya kadar bahsi geçen önlemler, siber espiyonaj faaliyetlerine karşı alınacak önlemler ile örtüşmektedir[32].

Elbette, siber espiyonaj faaliyetlerinin, daha geniş kapsamlı siber saldırılar için bir ön hazırlık olduğu da düşünülürse, yukarıda alıntılanan konseptin daha geniş bir siber savunma yaklaşımı için de bir gereklilik olduğu söylenebilir. Daha açık bir ifadeyle, tehdit unsurunun sisteme ilişkin bilgi toplamasını engellemek, müteakip siber saldırının yıkıcı etkilerini azaltacak ya da siber saldırının gerçekleşmesini engelleyecektir.

İkinci olarak, bir saldırı gerçekleştikten sonra sistemin kabul edilebilir fonksiyonellikte kalması, saldırıyı bir seviyede absorbe ederek toparlanması hedeflenmelidir.

28 Gabriel, Weimann. Cyberterrorism: How Real is the Threat, USIP, 2004.

29 Catherine, A. Theohary and John, W. Rollins. Cyber Warfare and Cyber Terrorism: In Brief, Congressional Research Service, 2015.

30 Don, Snyder. et.al. Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles, RAND, 2015, pp.3-5.

31 Ibid.

32 Don, Snyder. et.al. Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles, RAND, 2015, pp.3-5.

Bir sistemin siber saldırı sonrasında dahi kabul edilebilir ölçüde fonksiyonel olması sistemin kuvvetini (robustness); siber saldırıyı müteakip olarak yeniden fonksiyonel olma becerisi ise sistemin dayanıklılığını (resiliency) göstermektedir[33]. Dolayısıyla siber saldırılar karşısında siber güvenliğin sağlanmasına ilişkin önlemler bütünü çok katmanlıdır. Bu çerçevede ilk katman siber savunmadır. Ancak siber savunma katmanı geçilir ve siber saldırı icra edilirse, saldırının kuvvetli bir sistemle karşılaşması, bahse konu sistemin ayrıca yüksek dayanıklılık yetenekleri göstermesi beklenmektedir[34].

Bu noktaya kadar aktarılan hususlardan çıkarılan dersler, siber savunmada, aynı hava ve füze savunmasında olduğu gibi, çok katmanlı bir müdafi anlayış sergilenmesi gerektiğine işaret etmektedir. Ayrıca, potansiyel saldırganların hedef sistemlere ilişkin kritik bilgileri ele geçirmesi de önlenmelidir. Son olarak, özellikle siber güvenliğe ilişkin istihbarat analizinde, karşı karşıya kalınan siber espiyonaj faaliyetlerinin olası müteakip siber saldırılar ile birlikte değerlendirilmesi elzemdir.

SİBER RİSK VE TEHDİT PATERNLERİ

Siber ortamda devletlerden, sınır-aşan imkan ve kabiliyetlere sahip devlet-dışı gruplardan, suç örgütlerinden ve bireylerden veya küçük gruplardan müteşekkil radikal unsurlardan kaynaklanan risk ve tehditler bulunmaktadır. Bu tehditlerin boyutları saldırganın kaynakları, planlaması, hedefleri ve yetenekleri sonucu belirlenmektedir. Öte yandan siber-uzayda 'ayırıcı nitelikte olmayan ve imzasız' birçok tehdit bulunması, bir siber saldırıdan sonra gerçek saldırganın anlaşılması sorununu da (attribution problem) beraberinde getirmektedir[35].

Bu noktada 'attribution' sorunsalının salt teknik değil, politik nedenlerden de kaynaklandığı belirtilmelidir. Daha açık bir anlatımla, herhangi bir siber saldırıyı müteakip, faile ulaşmak kadar, uluslararası politikanın ve askeri – siyasi dengelerin inceliklerinden ötürü, elde olan bulguları diplomatik retoriğe dökmek de her durumda kolay olmayabilir. Özellikle siber saldırıya maruz kalan devlet eğer buna mukabele edemiyor ise, bu durumda siber saldırının failiyle birlikte açıklanması büsbütün bir zafiyet emaresi olarak anlaşılabilir.

Kimi uzmanlara göre siber güvenliğe ilişkin tehditler karmaşık bir problem niteliğindedir. Devletlerin, özel sektörün siber saldırılara ofansif olarak karşılık vermesini cesaretlendirmesi beklenmez, zira bu, devletin siber alan üzerindeki yönetsel kontrolünü kaybetmesine sebebiyet verebilecektir. Siber-saldırılara karşı kinetik yanıtlar verilmesi silahlı çatışmalar hukukunun limitlerini zorlayacağı gibi, 'kime yanıt verileceğinin bulunamayabileceği' (attribution problem) de ayrıca bir zorluk teşkil etmektedir. Dahası, mukabele edilecek hedef bulunsa dahi, ulusal kamuoyunu ve uluslararası toplumu hedefin meşruiyetine ikna etmek ayrıca bir uğraş gerektirmektedir. Öte yandan, salt müdafi unsurlara dayalı bir strateji, bir "Siber Maginot Hattı" ile neticelenecektir ki, bu da kabul edilemez bir durumdur. Dolayısıyla siber güvenliğe ilişkin sorunların çözümüne yönelik çabalar – kimi hallerde – başka sorunlara yol açabilmektedir[36].
Toplumlar, dijitalize bilgi odaklı yaşadıkları ölçüde siber tehditlere karşı daha hassas hale gelmektedir. Özellikle enformasyon ağları ve sistemlerine bağımlı

33 Ibid.

34 Ibid.

35 The US Joint Chiefs of Staff, Joint Publication 3-12, 2013, p.I – 6.

36 Benjamin, Runkle. "The Best Strategy for Cyber Conflict may not be a Cyber Strategy", 08 Kasım 2016, https://warontherocks.com/2016/11/the-best-strategy-for-cyber-conflict-may-not-be-a-cyber-strategy/, Erişim Tarihi: 04 Haziran 2017.

olan toplumlar için siber alandaki riskler çok daha fazladır. Dolayısıyla gelişmişlik düzeyi, ironik bir biçimde, ülkeleri siber risk ve tehditlere daha açık hale getirmektedir. Siber tehditler bireyleri, toplumları ve devletleri hedef aldıkları gibi; bireyler, devlet-dışı gruplar ve devletlerden kaynaklanan geniş bir spektrumdan kaynaklanmaktadırlar. Bu nedenle, siber güvenlik ortamı aktörler arasındaki ilişki bakımından kompleks bir yapıya sahiptir. Ayrıca siber alanda tehdit oluşturan aktörlerin yetenekleri her geçen gün artmaktadır[37].

Siber saldırılar politik ve ekonomik baskı enstrümanları olarak kullanılabilecekleri gibi, askeri güce eşlik edecek şekilde bir etki aracı olarak da karşımıza çıkabilir. Bununla birlikte siber alanı salt bir risk ve tehdit ortamı olarak tanımlamak da doğru olmayacaktır. Siber alan, kaynaklar ve fırsatlar da sunmaktadır. Örneğin güvenli bir siber ortamın ekonomik etkinlikler üzerinde çok olumlu etkileri vardır[38].

Siber ortamdaki tehditlerin kategorik nitelikleri ve boyutları tıpkı siber-uzay gibi olabildiğine geniş kapsamlıdır. Bu çerçevede kritik husus, siber alana ve siber fonksiyonlara bağımlı olan herşeyin siber saldırılar karşısında da çeşitli niteliklerdeki risk gruplarından birine dahil olduğunun iyi anlaşılmasıdır. Kritik ulusal altyapıyı akamete uğratabilecek, finansal sistemin işleyişini istikrarsızlaştırabilecek, milli güvenliğe ilişkin gizlilik derecesinde bilgiler ile özel sektörün ticari sır niteliğindeki bilgilerine kanunsuz erişimi olanaklı kılabilecek ve enformasyon ve telekomünikasyon teknolojileri sistemlerini aksatabilecek her türlü faaliyet siber risk ve tehditler kapsamında değerlendirilebilir[39]. Tüm bu sayılan potansiyel hedeflere bir arada ya da ayrı ayrı saldırı düzenlemek isteyen, devletlerden vekaleten savaş yürüten devlet dışı gruplara, teröristlere ve münferit olarak hareket eden kişilere kadar çok geniş spektrumda aktörler siber güvenlik ortamını daha da karmaşık hale getirmektedir. Siber ortamdaki tehditler, sistemlerin doğal açıklarından ya da kullanılan malware – zararlı yazılım / malicious software – unsurlarından kaynaklanacağı gibi, hiçbir zaman tamamen temizleneyebilir[40]. Dahası, 'siber küreselleşmenin' tersine çevirilmesi ve siber bağımlılık momentumunun azalması da mümkün görünmemektedir[41].

Bu noktada dikkat çeken husus, siber ortamda yaşanan gelişmelerin çok yüksek hızla seyretmesi, etkilerini tahmin etmenin ise oldukça zor olmasıdır. Enformasyon teknolojileri kapsamındaki yazılım için yaşam döngüsü kısadır. Benzer nitelikler siber ortamdaki ajan ve enstrümanlar için de geçerlidir. Dolayısıyla siber tehditler karşısında gerekli hazırlık seviyesine sahip olmak için ihtiyaç duyulan ön koşul, hızlı ve iyi koordine olmuş, birey-toplum-kamu düzeyinde aktörlerin işbirliğine dayanan bir sistemin varlığıdır[42].

Devlet, siber güvenlik yönetiminin en üst noktasını teşkil etmektedir. Zira görevi, siyasi ve stratejik yön gösterici çerçeveyi oluşturmak, karar almak ve kaynakları yönetmektir. Etkin bir siber güvenlik yönetimi devletin ve diğer ilgili aktörlerin siber güvenlik durumuna ilişkin gerçek-zamanlı ve güvenilir bilgiye ulaşımına dayanmaktadır. Her bir bakanlık ve idari birim, kendi çalışma sahasındaki siber güvenlik ile ilgili konulardan mesuldür. Bu nedenle siber ortam salt işbirliğini değil, etkin ve esnek bir koordinasyonu zaruri kılmaktadır[43]. Elbette böyle bir koordinasyonun

37 Finland's Cyber Security Strategy, 2013, pp.1 – 3.

38 Ibid.

39 Fred, Schreier. On Cyberwarfare, DCAF Horizon 2015 Working Paper 7, pp.32-34.

40 Ibid.

41 Ibid.

42 Finland's Cyber Security Strategy, 2013, pp.1 – 3.

43 Finland's Cyber Security Strategy, 2013, pp.1 – 3.

sağlanması için de, stratejik siber tehditlere ilişkin isabetli istihbarat yetenekleri gerekmektedir. Söz konusu istihbarata dayanmak suretiyle devletin her bir idari biriminin kendi mesuliyet sahasındaki faaliyet ve önlemleri şekillenecektir. Dolayısıyla ulusal siber dayanıklılık kapasitesinin iki temel dayanağı hazırlık seviyesi ile siber trend ve tehditlere ilişkin öngörü yetenekleridir[44].

Siber risk ve tehditlerin karakteristik nitelikleri kadar, fonksiyonel profilleri de önem taşımaktadır.

Hacker'ların niyetleri ne olursa olsun, teknik açıdan, üç ana tipte siber saldırıdan söz edilebilir. Birinci kategorideki saldırılar, bilginin gizliliğini hedef almaktadır. İlk tipteki saldırılar için saldırganların temel avantajı, halihazırda küresel bağlanabilirliğin – connectivity – küresel ve yerel ağ güvenliğinden daha gelişmiş olmasıdır. İkinci kategorideki saldırılar enformasyon bütünlüğünü hedef almaktadır. Bu kapsamda verilerin 'sabote edilmesi' yani kullanıcının iradesi dışında değiştirilmesi ya da kriptolanması da rastlanan saldırı paternleridir. Üçüncü tipteki saldırılar ise DoS (denial of service) olarak adlandırılmaktadır – kendi alt kategorileri de mevcuttur –, bilgisayarlara, veri tabanlarına ve ağlara yönelik ulaşımı engellemeyi hedefler[45].

Bu noktaya kadar aktarılanlar ışığında, siber yeteneklerin uluslararası ilişkilerde yeni bir milli güç unsurunu da kaçınılmaz olarak beraberinde getirdiği belirtilmelidir. Bununla birlikte, siber faktörler göz önünde bulundurularak milli güç kapasitesi nasıl yeniden kıymetlendirilecektir? Bir sonraki alt başlıkta bu sorunun yanıtını arayacağız.

SİBER GÜÇ VE MİLLİ GÜVENLİK

Uluslararası ilişkilerde güç kavramsallaştırması üzerine önde gelen teorisyenlerden biri olan Joseph Nye'a göre, güç bağlama dayanır ve siber alanın hızla büyümesi günümüz dünya siyasetinin en önemli bağlamlarından biridir[46]. Nitekim birçok ülkenin siber güvenlik konularını teşkilat yapılarına, milli güvenlik siyasetine ilişkin dokümanlarına ve doktrinlerine entegre ettiği müşahede edilmektedir. Söz konusu entegrasyon, elbette, standart bir yol haritası içermez. Ülkelerin stratejik kültürlerindeki, devlet – özel sektör ilişkilerindeki ve tehdit algılamalarındaki farklılaşmalar çeşitli siber güvenlik yönetimi modellerini de beraberinde getirmektedir[47].

Yakın geçmişe kadar, devletlerarası çatışmaların ve uluslararası ilişkilerin siber boyutuna ilişkin, daha doğrusu odak noktasında siber güvenliğin yer aldığı, pek az kuramsal modelleme çalışması bulunmakta idi. Siber harp ise son derece tartışmalı kavramsallaştırma çabalarına karşılık gelmektedir, zira özellikle liberal ve demokratik sisteme sahip devletler için 'savaş durumu' ile (siber) saldırıların ayrımı yaşamsal bir önemdedir. Daha açık bir anlatımla, belirtilen kriterlerdeki aktörler için 'barış dönemi' ve 'savaş dönemi' kesin uluslararası hukuki çizgilerle ayrışmaktadır. Öte yandan siber harbe ilişkin tüm yaklaşımlar böyle bir şeffaflık arayışında değildir. Örneğin Çin Halk Cumhuriyeti'nin enformasyon harbi konsepti, birçok demokrasinin doktrinlerinde yer veremeyeceği, oldukça muğlak (ya da esnek) bir anlayışa ve müphem uygulamalara karşılık gelmektedir[48]. Dolayısıyla şurası kesindir

44 Ibid.

45 Kenneth, Geers. Strategic Cyber Security, NATO CCDCOE, Tallinn, 2011, p.21.

46 Joseph, S. Nye, Jr. Cyber Power, Harvard Kennedy School Belfer Center, 2010, p.1.

47 Ayrıntılı bilgi için bkz. Keir, Giles and Kim Hartmann. Cyber Defense: An International View, US Army SSI, the Letort Papers, 2015.

48 Melissa E. Hathaway and Alexander Klimburg, "Preliminary Considerations: On National Cyber Security", National Cyber Security Framework Manual, Alexander Klimburg [ed.], NATO CCDCOE, Tallinn, 2012, pp. 27-28.

ki, demokrasinin temel prensiplerini zedelemeyecek, ancak enformasyonun yeni niteliklerini de doğru ve etkin karşılayabilecek bir paradigmaya gereksinim duyulmaktadır. Aynı şekilde kritik önemi haiz bir diğer sorunsal da, siber güvenliğe dair meseleler ile savaş ve barış dönemindeki (siber) işlevlerin geniş ufkunun, milli güç kapasitesinin çeşitli unsurlarını da kapsayacak şekilde, 'siber güç' kullanımına nasıl dahil edileceğidir[49].

Siber-uzayda 'güç' kavramını nelerin teşkil ettiğine dair geniş çerçeve halen doğru anlaşılmış değildir ve tartışma konusudur. Şurası kesindir ki, 'siber güç' yalnızca bir ulusun yetiştirdiği hacker havuzundan kaynaklanmamaktadır. Siber gücün kaynağı, bir ulusun siyasi ve iktisadi hedeflerine ulaşmak için kullanabileceği, bu arada kendi altyapısının dayanıklılığını da tahkim edecek yeteneklerin ve kaynakların tamamıdır[50]. Siber güce ilişkin kabul gören tanımlardan biri, siber gücü, siber-uzayı avantaj oluşturacak ve olayları etkileyecek şekilde tüm operasyonel çevrelerde ve diğer güç unsurları ile beraber kullanma becerisi olarak betimlemektedir. Kimi kaynaklar, yukarıda alıntılanan betimlemenin, ABD ve Avrupa'da siber-uzayı kara, hava, deniz ve uzaydan sonra yeni bir askeri operasyonel alan olarak gören siyasayı da tasvir ettiğini değerlendirmektedir[51]. Bu durum askeri konulardaki dış politika ve güvenlik siyasasına da direkt olarak yansımaktadır. Nitekim ABD ve Ürdün Silahlı Kuvvetlerinin 2011'den beri ortak icra ettikleri Eager Lion tatbikatlarının 2017 yılındaki ayağında siber savunma unsurlarının da olması dikkat çekicidir[52].

Nye'ın yaklaşımına göre, analojik olarak deniz gücü, okyanuslardaki (ya da denizlerdeki) kaynakların bu boyuttaki muharebelerin kazanılması ve kritik noktaların kontrol edilmesi kadar, karadaki çatışmalara, ekonomik aktivitelere ve kamuoyuna etki edecek şekilde kurgulanması ile de ilgilidir. Nitekim, Alfred Thayer Mahan'ın belirtilen çerçevedeki teorik çalışmaları, 20. Yüzyılın hemen başında, Theodore Roosvelt döneminde ABD donanmasının açık denizlerdeki yeteneklerini kuvvetlendirecek siyasasına dönüşmüştür. Benzer şekilde, kıtalararası balistik füzelerin ve uyduların geliştirildiği 1960'lı yıllarla birlikte, hava gücüne ilişkin teorik yaklaşımlar uzay gücüne doğru evrilmeye başlamıştır[53]. Bu kuramsal geçiş, Başkan Franklin Roosvelt'in İkinci Dünya Savaşı sırasında çok önemli bir askeri rol oynayan hava gücünü geliştirmeye yönelik yatırımlarından; Başkan John F. Kennedy döneminde başlayan uzay programına olan kaymayı da açıklamaktadır. Dolayısıyla, 2009 yılında Başkan Obama tarafından başlatılan siber inisiyatifin de, yukarıda betimlenen tarihsel akış içinde değerlendirilmesi isabetli olacaktır[54].

Bununla birlikte, belirtilmelidir ki, siber-uzay insan yapısı olması nedeniyle özgün nitelikleri haizdir ve teknolojik gelişmelere diğer (fiziksel) alanlara göre daha duyarlıdır. Daha farklı bir anlatımla, "siber-uzayın coğrafyası" diğer boyutlardan çok daha değişkendir, zira dağlar ve okyanusların hareketi zor iken, siber-uzayın bir bölümü kapatılabilir ve elektronların hareketi gemilerden daha hızlıdır. Ayrıca, uçak gemisi görev grupları ve denizaltı filoları oluşturarak deniz gücü teşkil etmek oldukça maliyetlidir. Dünyanın çeşitli yerlerinde korsanlık halen sürmekte olsa da, devlet dışı bir aktörün okyanusları ve açık denizi kont-

49 Ibid.

50 Ibid.

51 Ibid.

52 The Economic Times, http://economictimes.indiatimes.com/news/defence/jordan-us-launch-major-military-exercises-to-fight-terrorism-cyber-defence/articleshow/58563139.cms, Erişim tarihi: 10 Haziran 2017.

53 Joseph, S. Nye, Jr. Cyber Power, Harvard Kennedy School Belfer Center, 2010, p.4.

54 Ibid.

rol etmesi imkan ve kabiliyeti aşmaktadır[55]. Benzer şekilde, havacılık sektöründe özel birçok aktör olsa da, devletler halen beşinci nesil nesil savaş uçakları ve uydu ağlarıyla hava üstünlüğünden emin olabilirler, ancak bunun da yüksek bir maliyeti olacaktır. Oysa, siber-uzaya giriş ve etki oluşturma küçük devletler ve devlet dışı gruplar için çok daha az maliyetlidir. Büyük devletleri siber yetenekleri diğer aktörlere göre daha gelişmiş olsa da, siber-uzayda deniz gücü ya da hava gücünün oluşturabileceği türden bir dominasyonun sözünü etmek çok da isabetli olmayacaktır. Hatta, büyük ve gelişmiş devletlerin iktisadi ve askeri faaliyetlerini desteklemek için kompleks siber sistemlere daha çok bağımlı olması yeni savunmasızlıklara dahi yol açabilmektedir[56].

Son olarak belirtilmelidir ki, tehdit ve saldırıların anlamlandırılması (attribution) sorunu, 'siber gücün tanımlanması', 'siber-uzayın jeopolitiği' gibi karmaşık parametrelerin olduğu siber boyutta, uluslararası ilişkilerde 'güç' kavramına ilişkin teorik tartışmaların vazgeçilmez unsuru olan 'caydırıcılık' faktörü de karmaşık bir düzleme oturmaktadır. Siber-uzayda ve siber güvenlik çerçevesinde caydırıcılık ayrı bir çalışmanın konusu olsa da, bu aşamada, siber gelişmelerin caydırıcılığın temel teorik kabullerine ilişkin ciddi bir gözden geçirmeyi zaruri kıldığı not edilmelidir.

SONUÇ

Siber-uzay, kendi jeopolitiğini uluslararası sisteme dayatarak 'genişlemeyi' sürdürmektedir. Küreselleşme trendlerinde ciddi bir olumsuzluk yaşanmadığı sürece, sosyal, ekonomik ve siyasal faaliyetlerin giderek daha hızlı bir tempoda bu boyuta taşınacağı gibi; siber boyutun da fiziksel boyutlar ile etkileşiminin artacağı öngörülmektedir.

Yukarıda belirtilen şartlar altında, siber güvenliğin milli güvenlik portföyündeki rolünün artacağı ve siber güç olarak tanımlayabileceğimiz yetenekler ve kaynaklar manzumesinin milli güç kapasitesi içindeki yerinin giderek daha büyük önem kazanacağı değerlendirilmektedir. Gerek devlet düzeyinde gerek devlet dışı aktörlerin güç mücadelesine – ve işbirliğine – sahne olan siber-uzayda, adaptasyon kabiliyetinin ön plana çıktığı müşahede edilmektedir. Adaptasyon kabiliyetini belirleyen temel unsurlar ise analitik yetenekler ve siber alanın yönetilmesine ilişkin kapasitedir. Bahse konu fonksiyonlar, inovatif düşünceyi, bilimsel ve teknolojik ilerlemeyi ve tüm bu gerekliliklere yanıt verebilecek düzeyde uzmanlaşmayı zaruri kılmaktadır.

Siber-uzay giderek genişler ve karmaşıklaşırken, tıpkı bir yüzyıl öncesinde başlayan uzay yarışında olduğu gibi, uluslararası sistemde bu sürecin de kesin kaybeden ve kazananları olacağı açıktır. Öte yandan siber yarışın kaybedilmesi, diğer boyutlardaki yetenekleri de temelden etkileyeceği için, 'siber-gelişmişlik' makasının günümüzdeki diğer gelişmişlik indikatörlerinden 'daha acımasız' olacağını kestirmek de güç değildir.

55 Ibid.

56 Ibid.

TÜRKİYE VE SİBER GÜVENLİK

Türkiye'nin siber güvenlik teşkilatlanması ve stratejisi, EDAM'ın, siber araştırma programı kapsamında müteakip çalışmalarda detaylı olarak analiz edeceği bir konudur. Bununla birlikte, okuyucuya genel bir fikir verilmesi açısından bazı kritik hususlara değinmekte yarar görülmektedir.

Estonya'da 2007 yılında vuku bulan siber saldırıların ardından, 2008 yılında NATO Müşterek Siber Savunma Mükemmeliyet Merkezi, bahse konu Baltık ülkesinde kurulmuştur. Aynı yıl, Siber Savunma Mükemmeliyet Merkezi'nin kuruluşundan sadece birkaç ay sonra, bu kez NATO'nun güney kanadının en kritik ülkesi olan Türkiye'de, Bakü-Tiflis-Ceyhan boru hattına yönelik PKK terör örgütü tarafından bir saldırı düzenlenmiştir. Günümüzde, söz konusu saldırının konvansiyonel yöntemler ile değil, bizatihi kinetik etki oluşturmaya yönelik bir siber saldırı yoluyla icra edildiğine yönelik kuvvetli kuşkular ve yayımlanmış analizler mevcuttur. Özetle, Türkiye'nin, enerji güvenliğine ve bölgesel ittifaklarına yönelik kinetik etkili bir siber saldırı ile yaklaşık on yıl önce tanışmış olması muhtemeldir. Buna karşın siber güvenlik, Ankara'nın milli güvenlik stratejilerinde ancak son dönemde üst düzey bir yer bulabilmiştir.

Yine de, Türkiye'nin siber sahada önemli adımları hayata geçirdiğinin de belirtilmesi gerekmektedir. Türk devlet teşkilatı içinde, Ulaştırma Denizcilik ve Haberleşme Bakanlığı teknik düzeyde siber ulusal güvenlik stratejilerinin temel yönlendiricisi konumundadır. Ankara'nın, siber güvenliğin karakteristik niteliklerine ilişkin kurum ve doktrin çerçevesinde de doğru adımlar attığı söylenebilir. Öncelikle, geç de olsa, bir Siber Güvenlik Kurulu'nun teşkil edilmiş olması, siber güvenliğin ilk koşulu olan çeşitli bakanlıklar, istihbarat birimleri, sivil ve askeri bürokrasi paydaş çabalarının koordine edilmesi ve eşgüdüm sağlanması bakımından kritik bir eşiktir. Birçok kurumun katılımı ile siber tatbikatlar düzenlenmiş olması da öğrenilen-dersler bakımından olumlu bir gelişmedir. Ayrıca, siber harbe ilişkin konuların Türk Silahlı Kuvvetleri bünyesinde özel bir komutanlık tarafından deruhte edilmesi, 'harbin beşinci boyutu' paradigması kapsamında, konunun doğru anlaşıldığını gösteren önemli bir emaredir. Son olarak, 2013 – 2014 Eylem Planı'nı müteakiben yayımlanan 2016 – 2019 Ulusal Siber Güvenlik Stratejisi de dengeli ve modern bir risk analizi sunmakta, bu anlamda Türk Devleti'nin imkan ve kabiliyetlerine ilişkin iyimser bir fikir vermektedir.

Öte yandan, Türkiye'nin siber alanda, bu çalışmanın sonuç bölümünde aktarılan trendleri kaçırmaması için yapması gerekenler de bulunmaktadır ve en az başarıyla katedilen yol kadar, hatta daha fazla, önem arz etmektedir. Her şeyden önce siber güvenliğe ilişkin vizyon geliştirilmesi entelektüel ve analitik bir faaliyetler bütününe karşılık gelmektedir. Ülkemizde konuya ilişkin üst düzeyde çalışma yapan düşünce kuruluşu sayısı çok az olduğu gibi, üretilen yayınlarda da nicelik kadar nitelik eksiklikleri de göze çarpmaktadır. Bu bağlamda, Siber Güvenlik Kurulu'nun, Türk devlet kurumları arasında oluşturduğu eşgüdüm ve planlama yeteneklerinin bir benzerini, konuya ilişkin bilimsel ve analitik faaliyetler için teşkil edecek ve bahse konu entelektüel birikimi devletin milli güvenlik ihtiyaçlarına yönlendirecek bir ulusal siber güvenlik mükemmeliyet merkezine ihtiyaç duyulmaktadır. Ayrıca, siber güvenlik, yetişmiş insana ve bilgi birikimine en çok gereksinim duyulan alanların başında gelmektedir. Bu açıdan da Türkiye'nin önemli bir atılım yapması gerektiği değerlendirilmektedir.

Centre for Economics and Foreign Policy Studies

edam

EDAM Siber Politikalar Kağıtları Serisi 2017/1

Haziran 2017

Siber Güvenlik: Beşinci Boyutu Anlamak

Can Kasapoğlu
Savunma Analisti, EDAM