TESAM Akademi Dergisi - Turkish Journal of TESAM Academy
Temmuz - July 2019. 6(2). 11-33
ISSN: 2148 - 2462 E-ISSN: 2458 - 9217

TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKALARININ ANALİZİ; TÜRKİYE'NİN POTANSİYEL SİBER GÜVENLİK STRATEJİSİ[1]

Ali Burak DARICILI[2]

Öz

Siber uzay denilen alanın ortaya çıkışı Amerika Birleşik Devletleri (ABD) ve Rusya Federasyonu (RF) arasında Soğuk Savaş döneminde yaşanan askeri rekabet kapsamında geliştirilen ağ teknolojileri temelli yeniliklerin 1990'lar ile birlikte sivil kullanıma açılmasıyla başlamıştır. Soğuk Savaş'ın bitimi ile birlikte internetin sivilleşmesi ve ticarileşmesi, 2010 yılı sonrası dönemde akıllı telefonların ve sosyal medya uygulamalarının hayatın her alanına yayılması siber uzayın kara, deniz, hava ve uzaydan sonra insanlığın ulaştığı beşinci boyut olarak adlandırılmasına neden olmuştur. Türkiye de 1990'lı yıllar ile birlikte, güvenliğini sağlamak amacıyla siber güvenlik politikaları geliştirmeye başlamıştır. Bu süreçler ise dünyadaki gelişmelere bağlı olarak 2010 yılı sonrasında hızlandırılmıştır. Bu kapsamda çalışmada Türkiye'nin siber güvenlik politikaları, bu alandaki kurumsal yapılanmaların irdelenmesi temel alınmak suretiyle değerlendirilecektir. Böylelikle de Türkiye'nin en etkili siber savunma ve saldırı kapasitesine sahip olması amacı kapsamında, dünyadaki diğer devletlerin siber güvenlik temelli planlamaları analiz edilmek suretiyle ve reel politik güvenlik paradigmalarına uygun şekilde, devlet merkezli bir yaklaşımla öneriler ortaya konmaya çalışılacaktır.

Anahtar Kelimeler: Türkiye, Siber Uzay, Siber Güvenlik, Siber Savunma, Siber Saldırı

---

1 Makalenin Geliş Tarihi: 29.11.2018 Makalenin Kabul Tarihi: 04.01.2019
2 Dr. Öğretim Üyesi, Bursa Teknik Üniversitesi İnsan ve Toplum Bilimleri Fakültesi Uluslararası İlişkiler Bölümü. e-mail: ali.daricili@btu.edu.tr

Atıf: Darıcılı, A. B. (2019). Türkiye'nin siber güvenlik politikalarının analizi; Türkiye'nin siber güvenlik modeli için öneriler. *Tesam Akademi Dergisi, 6*(2), 11-33. http://dx.doi.org/10.30626/tesamakademi.613517

Analysis of Turkey's Cyber Security Policies; the Potential Cyber Security Strategy of Turkey

Abstract

The emergence of the so-called cyberspace began in the 1990s with the introduction of civilian technologies in the context of military technologies developed during the Cold War period between the United States (US) and the Russian Federation (RF). The civilization and commercialization of the internet together with the end of the Cold War, the spread of smart phones and social media applications to all areas of life after 2010, cyber space has been accepted as the fifth dimension reached by humanity after land, sea, air and space. Turkey has begun to develop cyber security strategies and policies to ensure its security. These processes have been accelerated after 2010 due to the developments in the world. In this article, Turkish policies in the area of cyber security will be evaluated by particularly analysing organizational structures in this field. Thus, Turkey will also be demonstrated effective cyber defence and cyber-attacks in the world other states in order to have the capacity to analyse security-based planning and realpolitik security paradigms appropriate recommendations with a state-centred approach.

Keywords: Turkey, Cyber Space, Cyber Security, Cyber Defence, Cyber Attacks

Giriş

Reelpolitik paradigmanın güvenlik yaklaşımları, devleti uluslararası ilişkilerin temel aktörü olarak kabul ederek, uluslararası ilişkileri ve uluslararası politikayı devletlerarasındaki mücadele süreci olarak ele alır. Bahse konu yaklaşımda devletler anahtar analiz düzeyini temsil eder. Diğer devlet dışı aktörlerin varlığı yadsınamazsa da bu aktörler devletlere göre ikincildir (Arı, 2010, s. 164-167). Reelpolitik paradigmaya göre devletin temel amacı, bekasının ve güvenliğinin sağlanması, çıkarının yerine getirilmesi şeklinde tanımlanmaktadır. Realizmin güvenlik anlayışı devletlerin sahip oldukları güç unsurları (askeri kapasite) ve bu unsurların uluslararası ilişkileri güç mücadelesi üzerinden şekillendirmesine dayanmaktadır (Kegley, 1995, s. 1-24).

Bununla birlikte siber uzay alanındaki gelişmelere bağlı olarak gücün dağılımı noktasında yeniden analiz edilmesi gereken gelişmelerin söz konusu olduğu açıktır. Bunlardan en önemlisi, gücün yayılması (diffusion of power) ile ilgilidir. Joseph S. Nye'a göre, siber uzaydaki gelişmeler kapsamında gücün büyük devletlerden diğer görece daha küçük devletlere, daha da önemlisi devlet dışı aktörlere doğru evrilmektedir (Nye, 2004, s.16-20). Bununla birlikte Nye, siber uzay alanı kaynaklı yeni gelişmelerin ortaya çıkardığı bu güç yayılması olgusunun, nihai olarak asla devletlerin uluslararası sistemdeki başat rolünü değiştirmeyeceğini iddia etmektedir. Nye açısından bu duruma, bir devletin kritik altyapılarını tamamen çökertmeye yönelik bir saldırının düzenlenmesine hedefleyen sofistike planlamaların ve bu planlamalara ait maliyetlerin günümüzde sadece devletlerin bilgi birikimi, tecrübeleri ve bütçeleri ile karşılanabiliyor olması hali oldukça etkili bir örnektir (Nye, 2010).

Devletin uluslararası sistemdeki rolü sağlamlaştırmasına neden olan bir başka faktör ise siber uzayı oluşturan önemli etmenlerden olan servis donanımlarının ve fiber optik kabloların hala devletlerin egemenlik alanları içerisinde olması ilgilidir. Bu kapsamda Nye, bir devletin bu imkânların kullanılmasına engel olarak yeni bir baskı aracı yöntemi geliştirebileceğini savunmaktadır. Örneğin Google dünyanın önde gelen şirketlerinden birisi olmasına rağmen Almanya'nın baskısıyla bu ülkeden yapılması olası nefret söylemli arama taleplerini engellemek zorunda kalmış ve Almanya'daki faaliyetlerini Alman yasalarına uygun sürdüreceğini ilan etmiştir (Nye, 2011).

Öte yandan 1980'lerin başlarından itibaren ABD'de ilk kişisel bilgisayarların üretilmesi ile başlayan ağ teknolojileri merkezli ticari

ivme, Soğuk Savaş sonrası dönemde, internetin sivil kullanıma açılması ile birlikte küresel ölçekte büyük bir gelişimin ilk habercisi olmuştur. Bu itibarla internetin sivilleşmesi ve ticarileşmesi, akabinde 2000'li yıllar ile birlikte cep telefonu teknolojisindeki gelişmeler ile birlikte giderek yaygınlaşan akıllı telefon kullanımı günümüzde hayatın her alanını etkilemektedir. Bu gelişime paralel olarak devletler de "kritik altyapılar" şeklimde tanımlanan kamu hizmetlerini gerçekleştirdikleri sistemleri ağ teknolojileri temelli yenilikler ile kontrol etmeye başlamışlardır. Bahse konu gelişmenin bir sonucu olarak da kritik altyapıların siber güvenliklerinin sağlanması devletlerin en önemli önceliklerinden biri haline gelmiştir.

Yine söz konusu gelişmelere pareler olarak devletler, 1980'ler ile birlikte ağ teknolojilerini ordularının konvansiyonel imkanlarına adapte etmeye yönelik planlamalar yapmaya başlamışlardır. Bu çerçevede belirtilen dönemde Sovyetler Birliği Ordusu'nda görev yapan üst düzey görevli Nikolai Ogarkov tarafından tasarlanan Askeri Meselelerde Devrim (Revoluation in Military Affairs / RMA) önerisi, devletlerin ağ teknolojilerini askeri güçlerini artıma noktasında kullanmaya yönelik planlamalarının ilk örneğidir (Mowthorpe, 2005, s. 137-155). ABD ise Ogarkov'un gündeme getirdiği söz konusu öneriye karşılık olarak Yıldız Savaşları Projesi (Stratejik Savunma Girişimi)'ni planlamıştır (Başbaşoğlu, 2011, s. 75). Bu iki projede hiçbir zaman hayata geçmemiş olsa bile 1980'lerden itibaren dönemin süper güçleri olan ABD ve Sovyetler Birliği'nin ağ teknolojilerinin sağladığı imkanları askeri kapasitelerine dahil etmeye yönelik ilk çabaları göstermesi bakımdan çok önemlidir (Darıcılı, 2018, s. 313).

Söz konusu fikirsel devrim ile birlikte 1990'lardan itibaren devletler, siber uzayın sağladığı imkânları reelpolitik paradigmanın yaklaşımlarında ifade edildiği şekilde askeri kapasitelerini geliştirme noktasında yeni bir fırsat olarak okumaya başlamışlardır. Bu doğrultuda siber uzayda günümüzde ABD, RF, Çin Halk Cumhuriyeti (ÇHC), İran, İsrail, Almanya, İngiltere, Hindistan ve Kuzey Kore'nin etkili siber savunma ve saldırı kapasitesi sahip olukları iddia edilebilecektir. Bununla birlikte sadece belirtilen devletler değil, küresel sistemde yer alan irili ufaklı tüm devletler, hatta Kuzey Atlantik Örgütü (North Atlantic Treaty Organization / NATO) veya Avrupa Birliği (European Union / EU) gibi uluslararası örgütler, kendi siber güvenlik strateji planlamalarını yapmaya başlamışlardır.

Türkiye'de Siber Güvenlik Alanı Kapsamındaki Temel Gelişmelerin Değerlendirilmesi

Türkiye, 1990'lı yıllarda kabul etmeye başladığı yasalar ile birlikte siber güvenlik alanına kayıtsız kalmadığını göstermiştir. Bu doğrultuda siber suçlar ile ilgili olarak ilk kez 6 Haziran 1991 tarihli 3756 Sayılı Türk Ceza Kanununun Bazı Maddelerinin Değiştirilmesine Dair Kanun hazırlanmıştır (Bıçakçı vd., 2015, s. 4). Bu değişikliğin 20. maddesi ile "Bilişim Alanında Suçlar" başlığı altında; "*bir bilgisayardan programların, verilerin veya diğer unsurların hukuka aykırı olarak ele geçirilmesi veya bunların başkasına zarar vermek üzere kullanılması, nakledilmesi veya çoğaltılması yasayla ceza unsuru*" olarak kabul edilmiştir (TBMM, 1991). Daha sonrasında 2000'li yıllarda çıkartılan yasalar ve 2010 yılı sonrasında hazırlanan siber güvenlik strateji belgeleri ve kurumsal yapılanmalar ile birlikte Türkiye, siber savunma ve saldırı kapasitesini geliştirmek planlamalarda bulunmaya başlamıştır.

Dünyada olduğu gibi, Türkiye'de de siber güvenlik literatüründe farklı tanımlar yapılabilmektedir. Bu kapsamda Bilgi Teknolojileri Kurumu (BTK) siber güvenliği; "*siber ortamda 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 bütünüdür*." şeklinde tanımlamaktadır (BTK, 2018a). Bu kavram, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda; "*siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunması, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınması, saldırıların ve siber güvenlik olaylarının tespit edilmesi, bu tespitlere karşı tepki mekanizmalarının devreye alınması ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi*" şeklinde ele alınmaktadır (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2013).

Öte yandan, 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ise siber güvenliği; "*siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini*" belirterek tanımlar (T.C. Ulaştırma ve Altyapı Bakanlığı, 2016).

Öte yandan siber güvenlik kavramının tanımın yapıldığı gibi çalışmamız

açısından kritik altyapılar kavramının da irdelenmesinde bizce fayda bulunmaktadır. Bu kavram, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda; "*işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar*" şeklinde tanımlanmaktadır (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2013). 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ise kritik altyapıları benzer şekilde tanımlamaktadır (T.C. Ulaştırma ve Altyapı Bakanlığı, 2016).

Bununla birlikte 2012 Ekim ayı, Türkiye'nin siber güvenlik çalışmalarında somut bir adımın atıldığı önemli bir dönem noktasıdır. Bu tarihte Bakanlar Kurulu kararıyla Siber Güvenlik Kurulu (SGK) kurulmuştur. Ulaştırma, Denizcilik ve Haberleşme (UDH) Bakanı'nın başkanlığını yaptığı Kurul, Dışişleri, İçişleri, Milli Savunma, UDH Bakanlıkları ve müsteşarlarının yanı sıra, Kamu Düzeni ve Güvenliği Müsteşarı (Bu Müsteşarlık, 2018 yılı içinde kapatılmıştır.), Milli İstihbarat Teşkilatı Başkanı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri İletişim Kuurmu (BTK) Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) Başkanı, Mali Suçları Araştırma Kurulu (MASAK) Başkanı, Telekomünikasyon İletişim Başkanı (Bu kurum, 2016 yılında kapatılmıştır.) ve UDH tarafından belirlenen bakanlık ve kamu kurumu üst düzey yöneticilerinden oluşmaktadır (28447 Sayılı Resmî Gazete, 2012).

SGK'nın temel görevleri söz konusu Bakanlar Kurulu kararında detayları ile tespit edilmiştir. Bu görevler ise temelde Türkiye'nin siber güvenlik politikalarını belirlemek, yönetmek, konu kapsamındaki milli yazlım ve donanım sistemlerinin geliştirilmesini sağlamak, siber güvenlik hakkında toplumda farkındalık oluşturmak, siber güvenlik uzmanlarının geliştirilmesi noktasında çalışmalar yapmak, siber güvenlik alanında uluslararası işbirliği süreçleri geliştirmek şeklinde özetlenebilir (28447 Sayılı Resmî Gazete, 2012).

Öte yandan SGK'nın kurulduğu tarih sonrasında aldığı ilk önemli karar, 2013 Ocak ayında Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nı kabul etmesidir. 2013-2014 eylem planı oldukça iddialı toplam 29 eylemin gerçekleştirilmesini hedeflemiştir. Bu hedefler temelde, ülkenin kritik altyapılarının korunması ve güçlendirilmesi, bu konuda ilgili devlet kurumlarının inisiyatifler geliştirmesi, siber güvenlik farkındalığının artırılması, bilişim sistemleri uzmanları yetiştirilmesi, siber güvenlik tatbikatları ve etkinlikleri düzenlenmesi, konu üzerine verilen derslerin ve

bölümlerin artırılması, BTK'nın siber tehditlerin tespit edilmesi, izlenmesi ve önlenmesi için mekanizmalar geliştirmesi, bu tehditlerin tespit edilmesi amacıyla bir bal küpü sisteminin geliştirilmesi, üniversitelerde Ar-Ge laboratuvarları kurulması, proje teşviki sistemlerinde siber güvenliğin öncelikli konular arasına eklenmesi, kamu kurumları, özel kuruluşlar, devlet dışı kurumlar, üniversiteler ve bilişim uzmanları ile siber güvenlik alanında milli ürünler ve çözümler yaratılması için düzenli faaliyetlerde bulunulması gibi yöntemlerle siber güvenlik alanında milli teknolojilerin geliştirilmesi, Türk Dil Kurumu (TDK) siber güvenlik terimler sözlüğü yaratma görevinin verilmesi gibi oldukça detaylı bir şekilde sıralanmıştır (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2013)

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın kayda değer bir getirisi de siber tehditlerin tespit edilmesi ve gerekli tedbirlerin geliştirilmesi amacıyla Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT)'nin) kurulmasını sağlamasıdır (USOM, 2018). Daha sonra 2013 yılında yayınlanan bir tebliğ ile kamu kurumlarının kritik altyapılarını korumaları amacıyla USOM'a bağlı olarak Siber Olaylara Müdahale Ekipleri SOME)'ler kurmaları kararı alınmıştır (BTK, 2018b). Aynı tebliğ ile kritik altyapı işleten kamu ve özel kuruluşların sektörel SOME'ler altında çalışacak kurumsal SOME'ler açma yükümlülüğü getirilmiştir (BTK, 2018b).

Daha sonra 2016 Eylül ayında Türkiye, 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nı kabul etmiştir. Bu plan dahilinde 2013-2014 Eylem Planı ile benzer ve uyumlu hedefler gündeme getirilmiştir. Söz konusu plan, bir önceki stratejik planlamaya göre daha basit ve genel ifadeler ile hazırlanmıştır. Bu planda milli yazılım ve teknolojilerin geliştirilmesi konusu doğru bir yaklaşımla daha çok vurgu yapılmış ve bir siber güvenlik terimler sözlüğü hazırlanacağı belirtilmiştir. 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nında diğer devletlerin siber güvenlik stratejilerinin incelendiği ve bu strateji belgelerinde internet bağımlılığı, siber casusluk, siber güvenlik uzman personel eğitimi, siber güvenlik kurumları arası koordinasyon zaaflarının giderilmesi gibi ana başlıklarda hedeflemeler yapıldığı genel bir ifade ile gündeme getirilmiştir. Bunların dışında yine doğru bir yaklaşımla Türkiye'de siber ekosistemin geliştirilmesi gerektiği ve siber güvenliği milli güvenliğe entegre edilmesinin şart olduğu belirtilmiştir (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2013)

Bu noktada 2013-2014 Eylem Planı'nın gündeme gelen siber güvenlik terimler sözlüğü yaratılması konusundaki hedefin, ÇHC'nin siber

güvenlik sistematiği incelendiğinde dikkat çekici bir yaklaşım olduğu ifade edilebilecektir. Bu kapsamda Çin terminolojisinde siber güvenlik kavramı yerine ağırlıklı olarak "bilgi güvenliği" veya "ağ güvenliği" tanımlamaları kullanılmaktadır. Resmi, akademik ve askeri terminoloji de siber kelimesine karşılık olarak "ağ/network/wangluo" kelimelerinden istifade edilmekte, siber uzay kavramı ise "ağ uzayı/network uzayı/saibo kangjian" kavramlarıyla açıklanmaktadır. Siber savaş kavramına karşılık olarak da "ağ savaşı / network warfare/wanglua zhan" kavramları kullanılmaktadır. Batı terminolojisinde kullanılan "siber uzay" tanımı ise "ağ uzayı/network uzayı/saibo kangjian" tanımının bir alt kavramı olup, Çinli siber güvenlik uzman ve akademisyenler tarafından; "*insanlık bilgi işlem süreçlerini ve bilişsel uzayı da içeren dünya nüfusuna büyük bölümünün dahil olduğu bir iletişim alanı*" şeklinde açıklanmaktadır (Chang, 2014). Bir diğer farklı yaklaşım ise "siber savaş" tanımı ile ilgilidir. Çin terminolojisinde bu kavram sadece ve sadece başta ABD olmak üzere, Batı kaynaklı psikolojik savaş faaliyetlerini izahta kullanılmaktadır (NATO, 2016).

Terminoloji konusundaki bahse konu farklı yaklaşımların iki nedeni olduğu değerlendirilebilir. Bunlardan ilki ÇHC'nin sosyalist yönetim sistemidir. Bir diğer neden ise ÇHC'nin başta ABD olmak üzere Batı dünyasının siber uzay kavramı etrafında şekillendirdikleri literatüre karşı tepkisel bir tutum takınması ile ilgilidir. Görüldüğü üzere ÇHC gerek askeri, ekonomik, kültürel, siyasal ve sosyal alanda gerekse de siber uzay alanında ABD ve Batı hegemonyasına karşı kendi duruşunu ve özgün sistemini geliştirme gayreti içerisindedir. Bu itibarla da ÇHC'nin siber uzayda küresel bir alternatif olma hedefine sahip olduğu da ileri sürülebilecektir.

ÇHC örneği ile ilgili olarak detayları ile izah edildiği üzere, bir siber güvenlik sözlüğü hazırlanırken, Türkiye'nin milli siber güvenlik teknolojisine sahip olması hedefine de uygun şekilde, yerli siber güvenlik literatürünün geliştirilmesi amacının da gözetilmesinde bizce fayda görülmektedir. Bu kapsamda konu dahilinde araştırmalar yürüten akademisyenlerin, okuma yapan ilgililerin ve öğrencilerin daha anlaşılır bir kavramsal yapıyı takip etmeleri sağlanabilir, böylelikle de Türkiye'nin kendi milli siber güvenlik sistematiğinin geliştirilmesine katkı yapılabilir.

Bu bilgiler ışığında çalışmanın bu aşamasında, Türkiye'nin her iki strateji belgesinin, gerek 2000'li yılların başında buyana hazırladıkları strateji belgeleri, gerekse de 1980'lerden buyana ağ teknolojileri merkezli gelişmeleri askeri kapasitelerini geliştirme konusunda bir fırsat alanı

olarak görmeleri ve bu konuda oluşturdukları kurumsal yapılanmaları dahilinde siber uzayı domine etmeleri nedeniyle ABD ve RF'nin strateji belgeleri ile kıyaslamanın faydalı olacağı değerlendirilmektedir.

ABD'nin federal sistemi, bu sistemden kaynaklanan birbirinden bağımsız karar mekanizmalarının varlığı, siber güvenlik alanında faaliyet gösteren kurum ve kuruluş sayısının fazlalığı, iktidara gelen yönetimlerin yıllar içinde değişen politika öncelikleri, görece olarak daha açık yönetim yapısı nedenleriyle, ABD'nin RF'ye kıyasla 1990'ların ikinci yarısından itibaren siber güvenlik alanı ile ilgili olarak çok sayıda resmi plan, belge, strateji, doktrin ve başkanlık emri ortaya koyduğu görülmektedir. Bu karmaşık yapı nedeniyle sürekli olarak bahse konu resmi belgelerde ısrarla siber güvenliğin ABD kritik altyapılarının korunması noktasında çok önemli olduğu ve bu konuda ilgi kurumlar arasında koordinasyon zafiyetlerinin giderilmesi gerektiği gündeme getirilmiştir (Darıcılı, 2017, s. 244-245).

RF'de ise ABD'deki sistematikten farklı olarak, çok sayıda kurum ve kuruluş yerine belli bir standardizasyon içinde RF savunma-güvenlik-istihbarat bürokrasisi tarafından siber güvenlik resmi belge, doktrin ve dokümanlarının hazırlandığı görülmektedir. Tüm bu resmi dokümanlarda ise sürekli olarak siber güvenliğin önemi vurgulanmış, uluslararası işbirliğinin faydalarına atıfta bulunulmuş ancak hiçbir zaman detaya girilmemiştir. Bu standart yaklaşımın istisnası ise RF Genel Kurmay Başkanı Valery Gerasimov tarafından kaleme alınan, 2012 yılında "Military Industrial Kurier Dergisi'nde" yayınlanan "The Value of Science in Prediction" isimli makale ile gündeme gelen ve 2014-2015 Ukrayna müdahalesi esnasında etkili bir şekilde sahada tatbik edilen Gerasimov Doktrini (Hibrit Savaş Konsepti)'dir (Darıcılı, 2017, s. 247). Gerasimov Doktrini'ne göre, RF Ordusu planlı bir şekilde manipüle edilen ekonomik tedbirler, siber saldırı yöntemleri, özel piyade kuvvetlerinin destek verdiği yerel muhalif veya mikro milliyetçi gruplarla koordineli bir şekilde sürdürülen gerilla faaliyetleri ve enformasyon savaş yöntemlerini kullanmak suretiyle askeri operasyonlarını planlayacak bir imkan ve kabiliyete ulaşmayı hedeflemiştir (Gerasimov, 2013).

Ana hatlarıyla belirtildiği üzere RF ve ABD, siber güvenlik belgelerinde detaylara girmekten ve bu konudaki planlamalarını açıkça ifşa etmekten özenle kaçınmaktadırlar. Demokratik karar alma süreçleri konusunda iddialı olduğu düşünülen ABD'nin dahi bu konudaki tavrı, Türkiye içinde dikkat çekici olmalıdır. Bu kapsamda Türkiye, 2013-2014 Eylem Planı'nı bizce gereğinden fazla detaylı hazırlamış ve hedeflerini açıkça kamuoyuna ifşa etmiştir. Bu hedeflerin kayda değer bir kısmına da

ulaşılamamıştır. 2016-2019 Eylem Planı ise daha uygun bir yaklaşımla, yani genel ifadelerle hazırlanmıştır. Bu noktada yapılması gerekenin, söz konusu strateji belgelerinin daha çok kamuoyunda siber güvenlik alanında farkındalık yaratması hedefine uygun olarak hazırlanmasıdır. Bu bağlamda bizce Türkiye'nin siber güvenlik strateji belgeleri, kamuoyu ile devletin ilgi kurumları nezdinde farkındalık yaratacak şekilde, genel ifadelerle ve temel hedefleri ortaya koyacak şekilde hazırlanmalıdırlar. Ancak Türkiye, siber savunma ve saldırı kapasitesini geliştirecek kurumsal yapılanmalarını oluştururken hassasiyetle davranmalıdır. Bu yapılanmalar oluşturulurken de, genel hatlarıyla siber güvenlik strateji belgelerinde tespit edilen hedeflere ulaşma konusundaki planlamaların geliştirilmesine yönelik bir yönetim sistemi oluşturmalı, özellikle bahse konu kurumlar arasındaki koordinasyonun sağlanmasına özen göstermelidir.

Türkiye'nin Resmi Siber Güvenlik Kurumlarının Faaliyetlerinin ve Etkinliklerinin Değerlendirilmesi

Türkiye'nin resmi siber güvenlik kurumlarının organizasyon yapısı üç temel hedef kapsamında şekillendirilmiştir. İlk grupta yer alan kurumlar siber suçlar ile mücadele etmek ve faaliyet alanları dahilinde istihbari faaliyetlerde bulunmak amacıyla kurulmuşlardır. İkinci grupta yer alanlar kurumlar, kritik altyapıların ve kamunun siber güvenliğinin sağlanması ve Türkiye'nin siber savunma, saldırı ve espiyonaj kapasitesini oluşturması hedeflerine odaklanmışlardır. Üçüncü grupta yer alan kurumlar ise devlet destekli özel girişimlerdir. Tüm bu organizasyon yapısının Türkiye'nin siber güvenlik politikasının oluşturulması noktasındaki hedeflerinin tespit edilmesinden ve yönetilmesinden sorumlu üst kurul ise SGK'dır.

Siber suçla mücadele ve kendi faaliyet alanlarına dair istihbari faaliyet yürütme hedefine yönelen kuruluşlar, İçişleri Bakanlığı bünyesinde oluşturulan Emniyet Genel Müdürlüğü (EGM) Siber Suçlarla Mücadele Daire Başkanlığı, Jandarma Genel Komutanlığı (JGK) Bilişim ve Teknik İstihbarat Başkanlığı, Sahil Güvenlik Komutanlığı İstihbarat Daire Başkanlığı Siber Suçlarla Mücadele Şube Müdürlüğü'dür.

İkinci grupta yer alan kurumsal yapılanmalar ise BTK, Milli İstihbarat Teşkilatı (MİT) Başkanlığı, Afet ve Acil Durum Yönetimi Başkanlığı'na (AFAD), Türk Silahlı Kuvvetleri (TSK) Siber Savunma Komutanlığı, TUBİTAK'dır. Bu kapsamda 2008 ve 2014 yılında yapılan yasal düzenlemeler ile BTK, bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi, izinsiz erişime karşı şebeke güvenliğinin sağlanması,

elektronik haberleşme sektörüne yönelik olarak, millî güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirlerin alınması konuları kapsamında Türkiye'nin siber savunma kapasitesinin oluşturulmasında temel işlevleri sağlayan kurumu haline gelmiştir (BTK, 2018).

Diğer yandan 2009 yılında çıkarılan bir kanunla Türkiye'de afet hallerindeki acil durum yönetimi yetkisi AFAD'a verilmiştir. Yine aynı kanuna göre afetler, teknolojik ve doğal afetler olarak ikiye ayrılmıştır. Bu kapsamda Türkiye'nin topyekûn bir siber saldırıya karşı karşıya kalması ve bunun bir afet seviyesine ulaşması halindeki olası kriz süreci AFAD tarafından koordine edilecektir (27261 Sayılı Resmî Gazete, 2009). Ancak bu kriz yönetimin nasıl yapılacağı, hangi kurumsal yapılanmalar ve süreçler dahilinde sürdürüleceği konusu net olarak ortaya konmamıştır.

TÜBİTAK, 2012 Ekim ayına kadar siber güvenlikten sorumlu kurum olarak Türkiye'de temel işlevleri yerine getirmiştir. Bu yetkisini 2012 yılında UDH'ya devretmiştir. TÜBİTAK, günümüzde milli kripto çözümlerinin önemli bir kısmını sağlamaktadır. TÜBİTAK, halen UDH ve USOM ile birlikte, 81 ilde 164 farklı noktadan trafik toplayan ülkenin bal küpü (honey pot) siber tehdit tespit sistemini işletmektedir (Bıçakçı vd., 2015, s. 9)

MİT Elektronik ve Teknik İstihbarat (ETİ) Başkanlığı, 2937 sayılı MİT'in kuruluş kanununda yazan hedefleri kapsamında telekomünikasyon yoluyla elde edilen istihbaratı tespit etmek, bu şekilde tespit edilen istihbaratı analiz etmek, Görüntü İstihbaratı (Imagery Intelligence / IMINT) sağlamak ve analiz etmek, kriptolu haberleşmelere hulul etmek görevleri kapsamında faaliyet yürütmektedir. Sinyal İstihbaratı Başkanlığı (SİB) ise Sinyal İstihbaratı (Signal Intelligence / SIGINT) sağlamak, hedef unsurların haberleşme ve radar iletişimine hulul etmek ve derlenen ham istihbaratı analiz etmek şeklinde görevler icra etmektedir (MİT, 2018). SİB, daha önce Genelkurmay Elektronik Sistemler (GES) Komutanlığı olarak faaliyet gösteren birimin 2012 yılında MİT'e devri ile kurulmuştur (Sabah Gazetesi, 2012).

MİT'e devredilerek SİB adını alan GES Komutanlığı, NATO standartları kapsamında yıllarca TSK'nın sinyal istihbaratı ihtiyaçlarını karşılayan birimi olmuştur. Bu birim, 2012 yılında Fetullahçı Terör Örgütü (FETÖ) yapılanmalarının sızma girişimlerini engellemek amacıyla MİT'e devredilmiştir. GES Komutanlığı sahip olduğu imkan ve kabiliyetler bakımından ABD'nin Ulusal Güvenlik Ajansı (National Security Agency

/ NSA) ile kıyaslanabilir. NSA, ABD'nin küresel izleme, şifre çözme, veri toplama, veri analizi, sinyal toplama, çeviri ve yabancı istihbaratlara karşı istihbarat yapma amaçları için tesis ettiği müstakil bir istihbarat örgütüdür. NSA, ABD'nin haberleşme ve bilgi veri sistemlerinin korunmasından sorumludur. NSA, aynı zamanda ABD Silahlı Kuvvetleri ve diğer istihbarat servisleri için kriptanaliz desteği sağlamaktadır (NSA, 2018).

GES'in MİT'e devredilmesi dönemin şartları kapsamında bir zorunluluktan kaynaklanmış olmakla birlikte, böylesine geniş imkan ve kabiliyete sahip bir örgütlenmenin ABD örneğinde olduğu gibi asker-sivil personel yönetimi ile müstakil bir kanuna, örgütlenmeye ve bütçeye sahip olacak şekilde, Türkiye'nin siber güvenlik stratejisinde yer almasında bizce fayda mütalaa edilmektedir. MİT'in mevcut iş yoğunluğu, yeni yapılan yasal düzenlemeler ile giderek artan yetki alanı ve hacmi dikkate alındığında, SİB Türkiye'nin milli siber güvenlik ve espiyonaj ihtiyaçlarını karşılayacak şekilde NSA örneğinde olduğu gibi müstakil bir yapı şeklinde faaliyetlerine devam etmesi daha verimli bir yaklaşım olabilecektir.

Bunlarla birlikte TSK'da 2012 Haziran ayında Siber Güvenlik Merkez Başkanlığı'nı kurmaya karar vermiştir. Bu yapı, ilk etapta daha çok TSK'nın SOME birimi şeklinde organize edilmiştir. TSK, 2013 yılında ise alay seviyesinde bir yapılanma ile Siber Savunma Komutanlığı'nın kuruluşunu ilan etmiştir. Bu birimin görevleri, TSK'nın kullandığı siber ortamda bulunan tüm sistemlerin siber savunması sağlamak, siber olaylara 7/24 esasına göre müdahale etmek, ulusal olarak ve NATO tarafından icra edilen tatbikatlara iştirak etmek, TSK çapında bilinçlendirme ve eğitim faaliyetleri yürütmek, TSK tarafından kullanılan ağlarda düzenli olarak siber güvenlik denetlemeleri ve testleri yapmak şeklindedir (Bıçakçı vd., 2015, s. 18).

Bu noktada, TSK bünyesindeki Siber Savunma Komutanlığı ile dünyanın en güçlü ordusuna sahip olan ABD'nin benzer yapılanması arasında bir kıyaslama yapmanın çalışmamız açısından önemli olacağı düşünülmektedir. ABD Savunma Bakanlığı (United States Department of Defense), ABD'nin siber güvenlik stratejisinin uygulanmasında etkin bir role sahiptir. Savunma Bakanlığı yapılanmasında siber güvenlik alanında en etkili rolü 2010 yılında kurulan CYBERCOM (Cyber Command) üstlenmektedir. CYBERCOM, ABD Ordusu'nun mevcut siber kaynaklarını düzenler, stratejik savunma ve saldırı planlarını hazırlar, ABD askeri bilgisayar ağları müdafaasını eşzamanlı bir hale getirir. Bünyesinde: "24. Hava Kuvvetleri, Ordu Siber Savaş Birimi, Donanma Siber Savaş Birimi, Deniz Kuvvetleri Siber Savaş Birimi" şeklinde yapılanmalar mevcuttur.

Söz konusu kuruluşların yanı sıra Savunma Bakanlığı bünyesindeki Kara, Deniz ve Hava Kuvvetleri Daireleri'nde her biri kendi görev ve sorumluluk alanı ile ilgili olarak faaliyet ve eşgüdüm görevi ifa eden birer Birleşik Siber Merkezi (Joint Cyber Center/ JCC) isimli organizasyonları da mevcuttur (Darıcılı, 2017, s. 88-90).

Görüldüğü üzere CYBERCOM, alt birimlere sahip, geniş ölçekli faaliyetler sürdüren bir yapılanmadır (Tirrell, 2012). NSA'nın başkanlığını yürüten NSA Direktörü, ayrıca CYBERCOM komutanıdır. TSK'nın siber savunma birimlerinin, CYBERCOM gibi henüz tam anlamıyla siber uzayda bir siber çatışma ortamında faaliyet gösterecek kapasiteden olduğunu söylemekte bu açıdan çok zordur. Bu nedenle TSK'nın süratle böyle bir imkan ve kabiliyeti sahip bir yapılanmaya gitmesi önemlidir.

Devlet destekli özel girişimler ise Savunma Teknolojileri Mühendislik (STM), Hava Elektronik Sanayii (HAVELSAN) ve Askerî Elektronik Sanayii (ASELSAN)'dır. Savunma Sanayii Müsteşarlığı (SSM) iştiraki olan STM, 2016 Mayıs ayında Siber Füzyon Merkezi (SFM)'ni kurmuştur. Bu kapsamda SFM, Türkiye'nin teknoloji ve bilgi varlıklarını koruyan koruyucu faaliyetleri sürdürmektedir. SFM, bilgi teknolojileri operasyonları ile tehdit istihbaratından gelen bilgi akışını ve güvenlik fonksiyonlarını yönetmekte ve koordine etmektedir. HAVELSAN, 2016 Mart Siber Savunma Teknoloji Merkezi (SİSATEM)'ni faaliyet geçirmiştir. Bu merkezin amacı siber alanda özgün ürün ve çözümler üretmek şeklinde belirlenmiştir. SİSATEM ayrıca Teknoloji, Ar-Ge, Test ve İzleme Merkezi olacak şekilde dizayn edilmiştir. Bunların yanı sıra ASELSAN ise siber güvenlik ve kriptoloji alanında milli çözümler oluşturarak, kamu, askeri ve sivil sektörler ile birlikte ihracat imkanlarını da araştıracak şekilde özgün projeler geliştirmeye çalışmaktadır (Ateş, 2018).

Türkiye'nin devlet destekli siber güvenlik sektöründe faaliyet gösteren girişimlerinin gelecek dönem planlamaları ile ilgili olarak bir perspektif oluşturulmak istenmesi halinde, İsrail'in 2010 yılından sonra ortaya koyduğu kamu ve özel sektör ile üniversite işbirliğini irdelemek oldukça faydalı olacaktır. İsrail'in siber güvenlik modelinde ulusal güvenlik stratejisi ile uyumlu bir şekilde faaliyet gösteren kamu ve özel sektör kurumları ile akademik çevrelerin sürdürdüğü inisiyatiflerin anahtar rolü bulunmaktadır. Bu kapsamda Birüssebi (Beerşeba)'da bulunan CyberSpark İnovasyon İnisiyatifi Projesi (CyberSpark Innovation Initiative Project) bahse konu siber güvenlik modelinin adeta pratik hayata yansımış ve somutlaşmış örneği olarak kabul edilebilir. Söz konusu proje, 2014 yılında INCB, Birüssebi Belediyesi, Ben Gurion Üniversitesi ve

EMC (RSA), Lockheed Martin, IBM, Deutsche Telekom, JVP Cyber Labs and Elbit isimli şirketlerin ortak inisiyatifi ile tesis edilmiştir. Bu kapsamda kurulduğu yıldan bu yana CyberSpark, hükümet, akademi, sanayi, yerel idare ve sivil toplumun paydaş olduğu bir siber eko-sistem yaratarak, İsrail'in siber güvenlik modelinin gelişimine önemli katkı sağlamaktadır (Cyberspark, 2018).

CyberSpark'ın kuruluş modeline benzer şekilde İsrail'in çeşitli bölgelerinde tesis edilen yirmiden fazla sayıda siber güvenlik Ar-Ge merkezi de İsrail'in siber güvenlik gelişim modelinde etkinlik göstermektedir. Söz konusu merkezlerin tesis ettiği global ekonomik ilişkiler kapsamında PayPal, IBM, VMWare, General Electric, Cisco, CA Technologies, McAfee, ve Ciscom gibi önemli teknoloji ve yazılım şirketleri bu merkezlerde temsilcilikler açmışlardır (Housen-Couriel, 2017, s. 15).

İsrail'in siber güvenlik modelinde ulusal güvenlik stratejileri uyumlu bir şekilde faaliyet göstermekte olan üniversitelerin ve çeşitli araştırma merkezlerinin de önemli etkinliği söz konusudur (Shkedi, 2015, s. 5). Söz konusu akademik ve araştırma kurumlarının sayısının İsrail genelinde 100 civarında olduğu ifade edilebilecektir. Bu tür kurumların gelişmesi noktasında Sanayi, Bilim ve Uzay Bakanlığı tarafından 2012 yılında geniş bütçeli bir teşvik programı yürürlüğe sokulmuştur (Housen-Couriel, 2017, s. 16).

Belirtilen şekilde yatırım teşvikleri ve diğer destekler ile birlikte İsrail'in kamu-özel sektör ve akademi işbirliği ile hızla geliştirdiği siber güvenlik modelinin, İsrail ekonomisi içindeki payı da hızla artmaktadır. Bu kapsamda siber güvenlik alanında faaliyet gösteren bahse konu şirketler ve akademik merkezler hem geliştirdikleri küresel ticari ve akademik ilişkiler ile İsrail'in ekonomisine ve sosyal hayatına katkı sağlamakta, hem de bu temasların oluşturduğu uygun zemin üzerinden İsrail'in diğer devletler ile olan diplomatik ilişkilerinin geliştirmesine yardımcı olmaktadırlar. Öte yandan kamu desteği ile hızla gelişen bahse konu şirketler ve akademik merkezler, İsrail'in siber uzay kaynaklı yeni teknolojilere ulusal ve yerli imkanlar ile sahip olmasına katkı sağlamakta, böylelikle de İsrail'in askeri kapasitesini (hard power) geliştirmesini de temin etmektedirler.

Bu kapsamda Ekonomik Kalkınma ve İşbirliği Örgütü (Organisation for Economic Co-operation and Development / OECD) verilerine göre İsrail son on yılda teknoloji sektörüne yönelik AR-GE harcamalarına GSMH'nın ortalama % 4 civarını (10 Milyar AVRO) ayırmak suretiyle, bu konuda

dünyanın önde gelen devletlerinden biri konumuna gelmiştir (OECD Data, 2018). İsrail, bilgi, komünikasyon ve teknoloji sektörü (ICT) hızla büyümektedir. Bu sektöre yönelik yabancı yatırımlar 2014 ve 2015 yıllarında % 20'lik bir oranla, 540 milyon ABD Doları'na yükselmiştir (Reuters, 2016). 2014 yılında İsrail'in global siber güvenlik sektöründeki payı ise %8 büyüyerek, 6 Milyar ABD Doları'na ulaşmıştır (Globes, 2016).

Yukarda belirtilen Türkiye'nin resmi siber güvenlik örgütlenmelerinin ve bu örgütlenmelerin organizasyon yapısı ile ilgili planlamaların yapılması noktasında koordinasyon görevinin ifade edilmesi oldukça önem arz etmektedir. Türkiye'deki mevcut sistemde bu görev kısmen SGK'ya verilmiştir. Güncel durum dikkate alındığında ise bahse konu resmi ve özel sektör kurumlarının kendi faaliyet alanlarına dair başarılı çalışmalar yaptıkları, ancak ortak bir siber güvenlik strateji doğrultusunda çalışma yapma noktasında bazı eksiklerin olduğu belirtilebilir. Bu koordinasyon yapısı ile ilgili olarak büyük nüfusu ve yüzölçümü kapsamında ortaya çıkabilecek potansiyel bürokratik gecikmelerin önüne geçmek adına **ÇHC'in** siber güvenlik alanında oluşturduğu sistem bizce yakından irdelenmelidir.

Bu kapsamda ÇHC, ulusal düzeyde bilgi teknolojileri konusundaki ilk resmi girişimini 1986 yılında "Devlet Ekonomik Bilgi Yönetimi Küçük Grubu / State Economic Information Management Leading Small Group" isimli yapılanmayı tesis etmesiyle başlamıştır. 1999 ve 2001 yıllarında alınan kararlarla ise "Devlet Bilgisayarlaştırma Lider Grubu / State Informatisation Leading Group (SILG)" kurulmuştur. Daha sonra 2003 yılında "Devlet Ağ ve Bilgi Güvenlik Koordinasyon Grubu / State Network and Information Security Coordination Small Group (SNISCSG)", SILG'nin bir alt çalışma yapılanması olarak göreve başlatılmıştır. Bu grupların temel amacı ise bilgi teknolojileri alanında ÇHC'nin gelişimin sağlanması olarak belirlenmiştir. SNISCSG, başarılı faaliyetleri sonrasında 2010 yılına doğru tasfiye edilmiştir. Söz konusu yapılanmalar doğrudan Çin Devlet Başkanlığı'nın şahsına bağlı olarak faaliyet göstermişlerdir. Bu nedenle de strateji belirleme süreçlerinde zaman kaybına uğramadan, etkili kararlara imza atabilmişlerdir. Bu itibarla, 2000'li yıllar ile birlikte ÇHC'nin bilgi ve ağ teknolojileri konusundaki hızlı gelişimi kayda değer olduğu açık bir şekilde ortadır (NATO-CCDCOE, 2016a). Türkiye'nin de ÇHC örneğinde olduğu gibi SGK'nın yapısında benzer yeni birimler ve işlevler organize edecek şekilde reorganizasyona gitmesinde bizce fayda mütalaa edilmektedir.

Yukarıda detayları ile ele alındığı üzere, Türkiye'nin siber güvelik

sistematiğinin sürdürülmesindeki ana omurga BTK'dır. Diğer güvenlik ve istihbarat kurumları ile özel girişimler ise kendi faaliyet alanları kapsamında siber güvenlik meselesine odaklanmaktadırlar. Halbuki bir devletin siber savunma ve saldırı kapasitesi geliştirilmesine yönelik tüm çabaları her şeyden önce o devletin ulusal ve uluslararası güvenliği ile doğrudan ilgilidir. Bu nedenle de bir devletin siber güvenlik sistematiğinin işletilmesi multi-disipliner bir yaklaşımla organizasyon yapısı belirlenmiş bir güvenlik örgütlenmesi tarafından yönetilmelidir. Bu noktada ABD İç Güvenlik Bakanlığı (United States Department of Homeland Security / DHS), Türkiye için uygun bir model olarak değerlendirilebilir. DHS, 11 Eylül 2001 saldırılarından sonra kurulan ve siber tehditler de başta ABD'nin iç güvenliğinin sağlanmasından sorumlu bir kurumdur. ABD Kongresi tarafından 2002 yılında çıkartılan "Kamu Güvenlik Yasası" ile kurulmuştur (Başa, 2018).

DHS, organizasyon şeması ele alındığında, ülke genelinde 7/24 esasına göre bir füzyon merkezi olarak görev ifa eden Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi (National Cybersecurity and Communications Integration Center / NICIC)'nin siber güvenlik alanındaki temel sorumlu birim olduğu görülmektedir. Bu merkez federal, eyalet ve diğer yerel birimler nezdinde ülke genelinde meydana gelen siber olayları izleyerek, bu olaylara anında cevap vermekten sorumludur. Ayrıca NICIC görevi kapsamında, ilgili güvenlik ve istihbarat birimleri ile özel sektör arasında eşgüdüm ve uyumu tesis eder (Tirrell, 2012).

Bu noktada ABD'de kamu-güvenlik-istihbarat örgütleri ve özel sektör arasında siber güvenlik alanındaki işbirliği yapısından da bahsetmek gerekmektedir. ABD'de kamu ve özel sektör arasındaki işbirliği, Avrupa Birliği (AB) sisteminin tersine özel sektör için zorunluluk ihtiva etmemektedir (NATO-CCDCOE, 2016b). Son yıllarda enerji, finans ve iletişim sektörleri başta olmak üzere Türkiye'nin kritik altyapılarına yatırım yapan şirketlerin yabancı ortaklı özel girişimler olduğu hatırlanmalı ve bu kapsamda siber güvenlik alanında bu girişimlere zorunluluklar getiren tedbirler ABD sistemine benzer şekilde alınmalıdır.

DHS, ABD siber savunma kapasitesinde önemli bir eşgüdüm merkezidir. Bu itibarla DHS, istihbarat ve güvenlik servisleriyle, ABD Savunma Bakanlığıyla ile ABD'nin ulusal siber güvenlik savunma planlamalarını hazırlamak, ABD Adalet Bakanlığı (United States Department of Justice) ile de ABD'ye yönelik siber saldırıların faillerinin tespit etmek şeklinde koordinasyon görevleri de mevcuttur Ayrıca Ulusal Siber Güvenlik Koruma Sistemi (National Cybersecurity Protection System / NCPS), DHS'nin ülke

genelinde siber güvenliğin sağlanması amacına yönelik olarak etkin bir şekilde kullandığı sistemdir. NCPS ise "EINSTEIN" adı verilen bir yazılım ile kullanılmaktadır (Department of Homeland Security, 2018).

Sonuç

İnternetin 1990'lı yıllar ile birlikte ticarileşmesi ve sivilleşmesi süreçleri siber uzay olarak adlandırdığımız alanın ortaya çıkmasını hızlandırmıştır. Siber uzay, ağ teknolojileri kapsamındaki yenilikleri devletlerin askeri kapasitelerini geliştirme adına yeni bir fırsat olarak görmeleri nedeniyle süratle uluslararası sistemde yeni bir rekabet alanı olarak karşımıza çıkmıştır.

Bu kapsamda, Soğuk Savaş döneminde ABD ve Sovyetler birliği arasında yaşanan askeri ve teknolojik rekabet süreçlerinin bir benzeri, özellikle 2000'li yıllardan sonra RF'nin siyasi ve ekonomik olarak yeniden toparlanması süreciyle birlikte hız kazanmıştır. Bu dönem ile birlikte RF ve ABD ortaya koydukları siber güvenlik stratejileri dahilinde siber uzayı şekillendiren önemli siber güçler olmuşlardır. Akabinde ÇHC de içinde bulunduğu teknoloji ve ekonomi merkezli gelişim süreci ile birlikte, siber uzayda söz sahibi olmaya başlayan bir diğer güç olmuştur. 2007 yılında Estonya'ya yönelik olarak RF merkezli planlandığı iddia edilen siber saldırılar ile birlikte, NATO kolektif bir savunma örgütü olarak siber güvenlik alanında planlamalar ve kurumsal yapılar geliştirmeye başlamıştır. Sonuç olarak 2010 yılı sonrasında uluslararası sistemdeki hemen hemen tüm devletlerin kendi ekonomik ve teknolojik güçleri kapsamında siber savunma ve saldırı kapasitesi geliştirmeyi hedef alan planlamaları gündeme gelmeye başlamıştır.

Çalışmada detayları ile irdelendiği üzere, Türkiye'de siber güvenlik alanında 1990'lı yıllar ile birlikte siber suçlarla mücadele kapsamında yasal düzenlemeler yapmak suretiyle girişimler başlatmıştır. Bu çalışmalar, 2010 yılı sonrası dönemde artarak daha profesyonel kurumsal yapılanmalara evirilmeye başlamıştır. Bu kapsamda 2012 Ekim ayında Siber Güvenlik Kurulu (SGK) kurulmuştur. SGK'nın görevleri ise Türkiye'nin siber güvenlik politikalarını belirlemek, yönetmek, konu kapsamındaki milli yazlım ve donanım sistemlerinin geliştirilmesini sağlamak, siber güvenlik hakkında toplumda farkındalık oluşturmak şeklinde tespit edilmiştir.

Daha sonra, 2013 Ocak ayında Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nı kabul edilmiştir. Siber güvenlik alnına ilişkin iddialı

toplam 29 eylemin gerçekleştirilmesini hedefleyen bu belgenin akabinde, 2016 Eylül ayında 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nı kabul etmiştir. Söz konusu plan, 2013-2014 Eylem Planı'na göre daha basit ve genel ifadeler ile hazırlanmıştır.

Türkiye'nin resmi siber güvenlik kurumlarının organizasyon yapısı üç temel amaç kapsamında örgütlendirilmiştir. İlk grupta yer alan kurumlar siber suçlar ile mücadele etmek ve faaliyet alanları dahilinde istihbari çalışmalarda bulunmak amacıyla kurulmuşlardır. Bu grupta yer alan kurumlar, İçişleri Bakanlığı bünyesinde oluşturulan EGM Siber Suçlarla Mücadele Daire Başkanlığı, JGK Bilişim ve Teknik İstihbarat Başkanlığı, Sahil Güvenlik Komutanlığı İstihbarat Daire Başkanlığı Siber Suçlarla Mücadele Şube Müdürlüğü'dür. İkinci grupta yer alanlar kurumlar BTK, MİT, AFAD, TSK Siber Savunma Komutanlığı, TUBİTAK gibi Türkiye'nin kritik altyapılarının siber güvenliğinin sağlanması, Türkiye'nin siber savunma, saldırı ve espiyonaj kapasitesini oluşturması hedeflerine odaklanmış kurumlardır. Üçüncü grupta yer alan ve devlet destekli özel girişimler ise STM, HAVELSAN ve ASELSAN bünyesinde alt birimler olarak faaliyete geçirilmiştir.

Türkiye'nin siber güvenlik politikaları ile ilgili olarak yapılacak ilk değerlendirme ise ortaya konulan her iki eylem planı kapsamındadır. Bu çerçevede, her iki eylem planında ortaya konan hedefler uyumlu olmakla birlikte, 2013-2014 Eylem Planı'nda ortaya kona hedeflerin kesin sonuçları tam olarak tespit edilememiştir. Bir diğer eleştirel değerlendirme ise AFAD'a verilen teknolojik afetler kapsamındaki kriz yönetiminin, nasıl yapılacağı, hangi kurumsal yapılanmalar ve süreçler dahilinde sürdürüleceği konusu henüz net olarak ortaya konmamış olması ile ilgilidir. Öte yandan TSK bünyesinde 2013 yılında alay seviyesinde bir yapılanma ile kurulan Siber Savunma Komutanlığı, henüz tam anlamıyla siber uzayda bir siber çatışma ortamında faaliyet gösterecek kapasiteden çok uzaktadır. Türkiye'nin siber savunma ve saldırı kapasitesinin etkinleştirilmesi açından bu birim süratle güçlendirilmelidir. Ayrıca İsrail'in siber güvenlik modelinde ulusal güvenlik stratejisi ile uyumlu bir şekilde faaliyet gösteren kamu ve özel sektör kurumları ile akademik çevrelerin sürdürdüğü inisiyatiflerin anahtar rolü bulunduğu dikkate alındığında, STM, HAVELSAN ve ASELSAN gibi devlet destekli özel girişimlerin siber güvenlik alanı kapsamındaki faaliyetlerinin benzer kriterler dahilinde planlanmasında bizce fayda bulunmaktadır

Bunlarla birlikte, Türkiye'deki mevcut sistemde siber güvenlik politikalarının belirlenmesi ve yönetilmesi görevi SGK'ya verilmiştir.

Güncel durum dikkate alındığında ise bahse konu resmi ve özel sektör kurumlarının kendi faaliyet alanlarına dair başarılı çalışmalar yaptıkları, ancak ortak bir siber güvenlik strateji doğrultusunda çalışma yapma noktasında bazı eksiklerin olduğu belirtilebilir. Türkiye'nin Cumhurbaşkanlığı Hükümet Model'ine geçmesiyle birlikte SGK'nın Cumhurbaşkanı'na bağlı olarak faaliyet göstermesinin siber güvenlik politikaları ile ilgili olarak süratli bir gelişim sürecini başlatacağı da ortadadır.

Belirtildiği üzere Türkiye'nin siber güvelik sistematiğinin sürdürülmesindeki ana omurga BTK'dır. Diğer güvenlik ve istihbarat kurumları ile özel girişimler ise kendi faaliyet alanları kapsamında siber güvenlik meselesine odaklanmaktadırlar. Halbuki bir devletin siber savunma ve saldırı kapasitesi geliştirilmesine yönelik tüm çabaları o devletin ulusal ve uluslararası güvenliği ile ilgilidir. Bu bağlamda da bizce devletin siber güvenlik sistematiğinin işletilmesi multi-disipliner bir yaklaşımla organizasyon yapısı belirlenmiş, müstakil bir güvenlik kurumu tarafından yönetilmelidir.

Sonuç olarak gelinen noktada Türkiye'nin devlet yönetiminde ülkenin siber güvenlik stratejisini geliştirme, siber savunma ve saldırı kapasitesine yatırım yapma konusunda bir farkındalık olduğu açıktır. Bu noktada yukarda belirtilen planlamalar ve kurumsal yapılanmalar dahilinde bugüne kadar iyi niyetli adımlar atılmıştır. Ancak bu adımların daha da geliştirilmesi gerekmektedir. Siber uzay, uluslararası sistemde devlet için yeni bir mücadele alanıdır. Bu alanı devletler askeri kapasitelerini geliştirmek adına bir fırsat olarak okumaktadırlar. Hatta siber saldırıları dış politikada sorun yaşadıkları ülkelere karşı bir baskı yöntemi olarak kullanmaktan da çekinmemektedirler. Tüm bu rekabet ve siber çatışma süreçleri de uluslararası sistemi eskisinden daha belirsiz ve anarşik hale getirmektedir. Bu kapsamda Türkiye'de, ulusal ve uluslararası güvenliğini sağlamak adına siber güvenlik stratejisini en sofistike planlama ve kurumsal yapılarla geliştirmek zorundadır.

Kaynakça / References

Arı, T. (2010). *Uluslararası ilişkiler teorileri: Çatışma, hegemonya işbirliği*. Bursa: MKM Yayınları.

Ateş, H. (2018). Türkiye'deki ateş, siber güvenlik istihbarat odaklı kurumsal aktörler. Erişim tarihi: 11.11.2018, https://www.academia.edu/36771509/T%C3%BCrkiyedeki_Siber_G%C3%BCvenlik_%C4%B0stihbarat_Odakl%C4%B1_Kurumsal_Akt%C3%B6rler.

Başa, Ş. (2018). ABD iç güvenlik bakanlığı. Erişim tarihi: 11.11.2018, https://www.academia.edu/9830086/ABD_%C4%B0%C3%87_G%C3%9CVENL%C4%B0K_BAKANLI%C4%9EI_SUNUM_.

Başbaşoğlu, A. (2011). Füze savunma sistemi ve Türkiye. *Orta Doğu Analiz*, *3*(34), 74-79.

Bıçakçı, S., Ergun, D. ve Çelikpala, M. (2015). Türkiye'de siber güvenlik. *Ekonomi ve Dış Politika Araştırma Merkezi (EDAM) Siber Politika Kağıtları Serisi,* 2015/1, 1-35.

BTK. (2018). Mevzuat. Erişim tarihi: 13.11.2018, https://www.btk.gov.tr/siber-guvenlik-mevzuat.

BTK, (2018a). Genel Bilgi. Erişim tarihi: 06.11.2018, https://www.btk.gov.tr/siber-guvenlik-genel-bilgi.

BTK, (2018b). Kurumsal SOME. Erişim tarihi: 09.11.2018, https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi.

Chang, A. (2014). Warring state; China cybersecurity strategy. Report by Center For a American Security. Erişim tarihi: 11.11.2018, https://cryptome.org/2014/12/chinas-cybersecurity-strategy-china-file-14-1205.pdf.

Cyberspark. (2018). Erişim tarihi: 15.11.2018, http://cyberspark.org.il/.

Darıcılı A. B. (2017). *Siber uzay ve siber güvenlik; ABD ve Rusya Federasyonu'nun siber güvenlik stratejilerinin karşılaştırmalı analizi*. Bursa: Dora Yayıncılık.

Darıcılı, A. B. (2018). Askerileştirilen ve silahlandırılan siber uzay. A. Acaravcı (Ed.), *Sosyal ve Beşeri Bilimlere Dair Araştırma Örnekleri* kitabı içinde, (s. 311-327). Ankara: Nobel Yayıncılık.

Department of Homeland Security. (2018). Erişim tarihi: 20.11.2018, https://www.dhs.gov/national-cybersecurity-and-communications-integration-center.

Gerasimov, V. (2013). Tsennos' Nauki v Vredvidenii (Value of Applied Science). Voyenno Promyshlennyy Kuryer / Military Industrial Kurier. Erişim tarihi: 24.11.2018, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

Globes. (2016). Israeli cybersecurity grabs 8% global market share. Erişim tarihi: 30.07.2018, https://en.globes.co.il/en/article-israeli-cyber-industry-hits-the-big-time-1001114669.

Housen-Couriel, D. (2017). National cyber security organisation: ISRAEL. *NATO*

Cooperative Cyber Defence Centre of Excellence, 1-21.

Kegley, C. (1995). *Neoliberal challange to realist theories of world politics: An introduction*. New York: St. Martin's Press.

MİT. (2018). Mit'in görev, yetki ve sorumlulukları. Erişim tarihi: 15.11.2018, http://www.mit.gov.tr/gorev.html.

Mowthorpe, M. (2005). The Revolution in military affairs (RMA): The United States, Russian an Chinese views. *Journal of Social, Political and Economic Studies*, *10*(2), 137-153.

NATO Cooperative Cyber Defence Centre of Excellence / NATO-CCDCOE. (2016a). China and cyber attitudes, strategies, organizations. Erişim tarihi: 13.09.2018, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf.

NATO Cooperative Cyber Defense Centre of Excellence / NATO-CCDCOE. (2016b). National cyber security organisation in United States. Erişim tarihi: 19.09.2018, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf.

Nye, J. S. (2004). The Decline of America's soft power. *Foreign Affairs*, (3), 1-5.

Nye, J. S. (2010). Cyber power. Harvard Kennedy School, Belfer Center for Science and International Affairs, Erişim tarihi: 19.11.2018, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

Nye, J. S. (2011). The future of power. Erişim tarihi: 19.11.2018, https://amacad.org/publications/bulletin/spring2011/power.pdf.

Sabah Gazetesi. (2012). MİT'in derin kulağı GES üssü. Erişim tarihi: 24.11.2018, https://www.sabah.com.tr/gundem/2013/02/05/mitin-derin-kulagi-ges-ussu.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2013). Ulusal siber güvenlik stratejisi ve 2013-2014 eylem planı. Erişim Tarihi: 06.11.2018, https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf.

T.C. Ulaştırma ve Altyapı Bakanlığı. (2016). Erişim tarihi: 06.11.2018, http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf.

Tirrell, K. W. (2012). *United states cyber security strategy, policy and organization: Poorly Postured to Cope With a Post-9/11 Security Environment*. (Master Thesis, Washington University)

USOM, (2018). Hakkımızda. Erişim tarihi: 15.11.2018, https://www.usom.gov.tr/hakkimizda.html.

Summary

It can be claimed that the US, RF, People's Republic of China (PRC), Iran, Israel, Germany, the United Kingdom, India and North Korea have effective cyber defence and attack capacity in cyberspace. As a result, it is clear that cyberspace-based developments diversify and make asymmetric threats in the international system. With this development, it can be claimed that the international system is more uncertain when it is added to the increasing competition processes within the scope of cyber security strategies planned to improve the military capacity of the states.

In parallel with these developments, the adaptation of the network technologies to the conventional technologies of the armies, the priorities of the states to establish independent cyber war and intelligence units in the armed forces and intelligence services have resulted in the rapid militarization of cyberspace. In this context, states have begun to read network technologies as a new opportunity to develop their military power, and have begun to take measures to improve their cyber defence and attack capabilities.

Moreover, the civilization and commercialization of the internet together with the end of the Cold War, the spread of smart phones and social media applications to all areas of life after 2010, cyber space has been accepted as the fifth dimension reached by humanity after land, sea, air and space. The commercialization and civilization processes of the Internet in the 1990s have accelerated the emergence of so-called the cyberspace. Cyber space has emerged as a new field of competition in the international system as it sees innovations within the scope of network technologies as a new opportunity to improve the military capacity of states.

In this context, a similar period of military and technological competition between the US and the Soviet Union during the Cold War has gained momentum, especially after the 2000s, with the process of the political and economic recovery of the RF. In this period, RF and the United States have been the major cyber forces that have shaped the cyber space within the cyber security strategies they introduced. In the on-going process, PRC has become a force in cyber space, with its technology and economy-centred development process. In 2007, together with the alleged cyber-attacks planned for RF in Estonia, NATO has begun to develop cyber security schemes and institutional structures as a collective defence organization. As a result, after 2010, almost all states in the international system started to come up with plans to develop cyber defence and attack

capacity within the scope of their economic and technological forces.

In parallel with innovations in the field of network technologies, states have started to develop new policies and strategies in order to protect their critical infrastructures controlled mainly by network technologies. As a result of this process, ensuring the cyber security of critical infrastructures has become one of the most important priorities of the states. In this respect, it can be claimed that the USA, RF, PRC, Iran, Israel, Germany, England, India and North Korea have effective cyber defence and attack capacity in the cyberspace, However, not only the states mentioned above, but also the other regional strong states in the global system, and even international organizations such NATO or European Union (EU) have started to develop their plans and initiatives in the field of cyber security.

As discussed in detail in the study, together with Turkey in the field of cyber security in the 1990s for the fight against cybercrime has launched initiatives by making regulations. These studies started to evolve into more professional institutional structures in the post-2010 period. In this context, Cyber Security Council (SSI) was established in October 2012. Then, in January 2013, the National Cyber Security Strategy and the 2013-2014 Action Plan were adopted. 2016-2019 National Cyber Security Strategy and Action Plan were implemented in September 2016. Organizational structures operating in the field of cyber security in Turkey after this date quickly began to take shape.

As a result, this point in the development of the state administration, Turkey has begun to develop cyber security strategies and policies to ensure its security. These processes have been accelerated after 2010 due to the developments in the world. Turkey's cyber security strategy of the country, it is clear that a serious awareness to invest in cyber defence and attack capability. However, these steps need to be further developed. Cyberspace is a new challenge for the state in the international system. They read this area as an opportunity to improve their military capacity. They also do not hesitate to use cyber-attacks as a form of oppression against countries in which they face problems in foreign policy. All these competition and cyber conflict processes make the international system more vague and anarchic than before. In Turkey, in this context, to ensure the safety of national and international cyber security strategy is to develop the most sophisticated planning and organizational structure.