Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Stratejileri[1]

Salim KURNAZ[*],
S. Mustafa ÖNEN[**]

Öz

Her ülke, kendi bilişim sistemlerini siber saldırılardan korumak ve sahip olduğu bilgi ve verileri güvenliğini sağlamak için etkin ve sürdürülebilir bir siber güvenlik stratejisi geliştirmek ve uygulamak zorundadır. Günümüzde siber güvenlik olgusu, artık her ülkenin ulusal güvenliğinin birer parçası halini almıştır. Yaşadığı siber saldırılar sonrası AB; siber güvenliğe yönelik stratejilerini ve yasal düzenlemelerini 2000'li yıllar itibari ile oluşturmuştur. Ayrıca AB, siber güvenlik stratejilerini uygulamak üzere gerekli kurumlarını da hayata geçirmiştir. Buna karşılık Türkiye'deki siber güvenlik stratejilerinin belirlenmesi ve iyileştirilmesi konusunun AB'nin siber güvenlik stratejileri ile karşılaştırıldığında; Türkiye'deki yapının henüz oluşum safhasında olduğu fark edilmektedir. Bu noktada Türkiye'nin AB uyum sürecinde AB'nin siber güvenlik stratejileri ile ilgili yasal ve kurumsal düzenlemelerini öncelikle gözden geçirmesi gerekmektedir. Bu çalışmanın esas amacı, AB tarafından hayata geçirilen siber güvenlik stratejilerinin yasal ve kurumsal boyutunu inceleyerek Türkiye'deki siber güvenlik stratejilerinin oluşturulmasına ve geliştirilmesine belli ölçüde katkı sağlamaktır. Çalışmada ilk olarak siber güvenlik kavramı ve türleri ele alınacaktır. Ardından Avrupa Birliği tarafından uygulanan siber güvenlik stratejileri ile Türkiye'de uygulamaya konan belli başlı siber güvenlik stratejileri kapsamında başlıca yasal ve kurumsal düzenlemeleri incelenecektir. Çalışmanın sonunda ise, ulusal siber güvenlik stratejilerinin oluşturulması ve iyileştirilmesi kapsamında mevcut düzenlemeler kısaca değerlendirilerek birtakım öneriler geliştirilecektir.

Anahtar Kelimeler: *Siber Uzay, Siber Güvenlik, Siber Güvenlik Stratejisi, Siber Güvenlik Yönetimi.*

Turkey's Cyber Security Strategies In The Adaptation Process To European Union

Abstract

Each country had to develop and implement an effective and sustainable cyber security strategy to protect its information systems from cyber attacks and to secure the information and data it has. Today, the cyber security phenomenon has become a part of the national security of every country. After the cyber attacks, the strategies and legal arrangements of the EU for cyber security were formed by the years 2000s. In addition, the EU has generated the necessary institutions to implement cyber security strategies. In contrast, in comparison with the EU's cyber security strategy, the structure in Turkey is yet to be realized as in the formation stage. At this point Turkey, in EU accession process, should revise "the EU Cyber Security Strategies" primarily related to legal and institutional arrangements. The main purpose of this study is to provide a certain degree of contribution to the creation and development of Turkey's cyber security strategy by examining the legal and institutional aspects of cyber security strategy implemented by EU. Firstly, cyber security concept and its types will be discussed. Then the main legal and institutional arrangements will be examined within the scope of major cyber security strategies implemented in Turkey and in the European Union. Finally, some proposals will be developed

[1] 18-20 Nisan 2019 tarihinde Gaziantep'te "13. Uluslararası Kamu Yönetimi Sempozyumu"nda sunulan ve tam metin olarak yayınlanmamış bildirinin geliştirilmiş halidir.

[*] Dr., Kara Kuvvetleri Komutanlığı, salimkurnaz@hotmail.com
[**] Prof. Dr., İnönü Üniversitesi İİBF Siyaset Bilimi ve Kamu Yönetimi Bölümü, mustafa.onen@inonu.edu.tr

by briefly evaluating the existing regulations within the scope of the creation and improvement of national cyber security strategies.

Key Words: *Cyber Space, Cyber Security, Cyber Security Strategy, Cyber Security Management.*

1. Giriş

Bilgi teknolojilerinin kullanımı her geçen gün artmaktadır. Günümüzde internetin sağladığı kolaylıklar, teknolojik ve elektronik aletler aracılığıyla yaygın bir şekilde gerçekleştirilmektedir. Geçmişte devletten bir belge almak veya vermek için kamu kurum ve kuruluşlarına bizzat başvurmak gerekir iken; artık işlemler, bilgi teknolojileri yardımıyla daha rahat ve pratik olarak yapılmaktadır. Kamusal hizmetlerin bilişim teknolojileri aracılığıyla fiziki ortamlardan kurtularak siber uzay olarak adlandırılan sanal ortama taşınması, hizmetlerin daha hızlı ve kolay sunulmasına yol açmaktadır. İnternetin hayatımıza sağladığı kuşkusuz birtakım yararlar kadar, birçok yeni tehlikenin de hayatımıza girmesi söz konusu olmuştur. Elektronik ortamda bulunan veya saklanan kişisel bilgiler, teknolojik gelişmelerle birlikte siber saldırılara daha açık hale gelmiştir. Hizmet kalitesi ve müşteri memnuniyeti gibi nedenlerle kamu kurum ve kuruluşlarınca kullanımı yaygınlaşan bilgi teknolojileri kapsamında veri tabanları ve e-hizmetler aracılığıyla saklanılan kişisel bilgiler, bu gelişmeler doğrultusunda daha çok siber saldırılara maruz kalmıştır.

Avrupa Birliği (AB), üye veya aday ülkelere birçok alanda önderlik ve yol gösterici özelliğe sahip bir kuruluştur. Bu alanlardan birisi de son dönemde giderek yoğunlaşan siber saldırılara karşı geliştirilmesi gereken bazı hareket tarzları ve ulusal siber güvenliğin sağlanmasına yönelik tedbirler olmuştur. AB üyelik sürecinde bulunan Türkiye, siber güvenliğine yönelik çalışmalarına son dönemde yoğunlaşmasına rağmen; Türkiye'nin bu konuda yeterli güvenlik seviyesini sağladığını söylemek güçtür. Türkiye; vatandaşlarının temel hak ve hürriyetlerini sağlamak, güvenli hizmet sunabilmek için hızlı bir şekilde kamusal hizmet ve faaliyetlere entegre ettiği bilişim teknolojilerini siber güvenliğe uygun hale getirecek gerekli tedbirleri biran önce hayata geçirmesi esastır. Bu kapsamda AB tarafından hayata geçirilen siber güvenlik stratejileri ve buna ilişkin düzenlemeler, Türkiye'deki çalışmalara belli ölçüde yol gösterici olabilir.

AB genel yasal düzenlemeler ve siber güvenlik kapsamında üye ülkelere öncülük etme özelliğine sahip olduğundan almış olduğu kararların incelenmesinde fayda vardır. Aslında üye

ülkelerin temsilcilerinden oluşan Avrupa Komisyonunun aldığı kararlar, bütün üye ülkelerin uyma ve uygulama zorunluluğu olan bağlayıcı nitelikte düzenlemelerdir. Bu kapsamda Avrupa Komisyonu güncel hayattan ekonomik ve sosyal hayata kadar birçok düzenlemeye imza atmaktadır. Avrupa Komisyonu 2013 yılında yayınladığı son siber güvenlik stratejisini yaşanan teknolojik gelişmeler, siber saldırı ve risk analizleri kapsamında 2017 yılında güncellemiştir. Güncellenmiş strateji, özellikle kritik altyapıların güvenliği ve bölgesel siber güvenliğin sağlanmasına odaklanan geniş kapsamlı yenilikler içermektedir. Bu güncelleme kapsamında hayata geçirilen yeniliklerin Türkiye tarafından uygulanan siber güvenlik tedbirleri, yasal düzenleme ve kurumsal yapılanmaya entegre edilmesiyle vatandaşlara sunulan hizmetlerin güvenlik ve kalitesi de artmış olacaktır.

Bu çalışmada öncelikle siber güvenliğe yönelik kavramlara değinilmiş; ardından ise, Türkiye'deki siber güvenliğe yönelik mevcut durum analiz edilmiştir. Çalışmada Türkiye'de yapılacak düzenlemelere yol gösterici olabileceği değerlendirilen AB tarafından uygulanan siber güvenlik stratejilerine temel oluşturan yasal ve kurumsal düzenlemeler incelendikten sonra, çalışmanın sonunda konuya ilişkin birtakım değerlendirme ve önerilere yer verilmiştir.

2. Siber Güvenlik Kavramı

Sınırsız ve çok katmanlı internet ve bilişim teknolojilerinin kullanımı devlet gözetimi ve denetimi olmadan küresel ilerlemenin güçlü bir aracı haline gelmiştir. Özel sektör internetin yapımında ve günlük yönetiminde lider bir rol oynamaya devam etse de, şeffaflık, hesap verebilirlik ve güvenlik gereksinimlerine olan ihtiyaç gittikçe daha fazla önem kazanmaya başlamıştır. Bu kapsamda devletlerin ve uluslararası kuruluşların siber güvenlik politikasına rehberlik etmesi gereken ilke ve yasal düzenlemelerin biran önce belirlenmesi gerekmektedir.

Siber uzay; dünyada ve uzayda yer alan bilişim sistemlerinin ve ilgili ağların oluşturduğu ya da bağımsız bilgi sistemlerinde bulunan sayısal ortama denilmektedir[2]. Buna göre internete bağlanabilen her türlü elektronik cihaz, bilgisayar ve teknolojik alet siber uzayın bir parçası olarak tanımlanmaktadır. Siber güvenlik ise, siber uzayda oluşan bilişime yönelik saldırılardan korumak, bilişim sistemindeki bilgiyi/verinin gizliliğini, bütünlük ve erişilebilirliği güvenceye almak, saldırıları ve siber güvenlik olaylarını tespit etmek ve bununla

[2] Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (UDHB), "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a. pdf, 2013, s. 8, (04.01.2019).

ilgili mekanizmaları devreye almak ve sistemleri siber saldırı öncesine döndürmektir[3]. Birçok çalışmada siber güvenliğe yönelik tanımlamalar yapılmıştır. Bu çalışmada siber güvenlik genel olarak siber alanlara, birbirleriyle bağlantılı ağlara ve bilgi altyapısına zarar verebilecek tehditlere karşı korumak için sivil ve askeri alanlarda atılması gerekli adımları ifade etmektedir. Diğer bir deyişle siber güvenlik, ağların ve altyapının kullanılabilirliğini ve bütünlüğünü ve içerdiği bilgilerin gizliliğini korumak için çaba göstermektir[4]. AB ve ülkemizde oluşturulan siber uzay ve siber güvenlik tanımları birbirlerine büyük ölçüde benzerlik göstermektedir.

Siber tehdit kavramı ise; siber alanda bireysel veya kurumsal verilere dönük olarak güvenliği ortadan kaldırılacak her tür siber saldırıdır[5]. Bu tanım ile siber tehditleri klasik tehditlerden ayıran temel özelliklerin başında tehditlerin siber uzayda karşımıza çıkması gelmektedir. Siber uzayda ortaya çıkan tehditlerin önceden tahmin edilmesi ve önlem alınması son derece zordur. Siber alanda gerçekleştirilecek bir saldırı her hangi bir zaman ve yerden gerçekleştirilebilmektedir.

Siber suç, genellikle bilgisayarların ve bilgi sistemlerinin birincil bir araç veya hedef olarak yer aldığı çok çeşitli suç faaliyetlerini kapsamaktadır. Siber suçlara aldatma, sahtekarlık veya kimlik bilgilerini çalma gibi "geleneksel suçlar"; çocuk pornografisinin dağıtımı ve ırkçılıkla ilgili nefreti yayma gibi "içerikle ilgili suçlar" ve bilgi sistemlerine yönelik saldırılar, kötü niyetli bilgisayar yazılımları ise "bilgi sistemlerine özgü suçlar" olarak örnek gösterilebilir[6]. AB tarafından oluşturulan siber suç tanımı siber uzayda işlenebilecek suçları detaylı olarak ele almıştır. Ülkemizde ise, siber suçun kapsam ve sonuçları üzerine daha detaylı bir çalışmaya ihtiyaç vardır.

Siber caydırıcılık, sanal ortamda karşı karşıya kalınacak tehdit ve tehlikeleri önlemek veya engellemek için birtakım önlemlerin alınması durumudur. Diğer bir deyişle siber caydırıcılık, saldırıyı yapanları saldırıdan vazgeçirme, korkutma ile cesaretini kırma veya

[3] Age, s. 8.
[4] European Commission, "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", https://eeas.europa.eu/archives/docs/ policies/eu-cyber security/cybsec_ comm_en.pdf, (20.01.2019).
[5] Kamil Tahran, "Uluslararası Güvenliğin Bir Bileşeni Olarak Siber Güvenlik", (Yayımlanmamış Yüksek Lisans Tezi, Selçuk Üniversitesi, 2018).
[6] European Commission, "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", (20.01.2019).

vazgeçirme amacıyla yapılan girişimler şeklinde tanımlanabilir[7]. Kamu kurumları dikkate alındığında siber caydırıcılık, kamu kurumları tarafından atılması gerekli koruyucu ve engelleyici tedbirleri içermektedir. Bu tedbirlerin vatandaşların kullanım düzeylerini etkilemeyecek, ama kötü amaçlı kullanım ve saldırıları vazgeçirecek seviyede olması öngörülmektedir. Aşırı güvenlik tedbirleri vatandaşların hizmet alımlarını, dolayısıyla sistemin etkinliğini olumsuz yönde etkiler iken; buna karşılık yetersiz güvenlik tedbirleri ise, kötü amaçlı kullanım ve saldırıların artmasına neden olmaktadır.

Siber saldırılara maruz kalan sistemler, TÜBİTAK tarafından şu şekilde ortaya konmuştur[8]:

- *Bilgi Sistemleri,* bir kuruma ve paydaşlarına hizmet veren bilgisayar sistemleridir.
- *İletişim Sistemleri,* coğrafi olarak çok geniş bir alana yayılmış bileşenlerden oluşan, pek çok kurum ve kuruluşa iletişim hizmeti sağlayan sistemlerdir.
- *Merkezi Denetleme Kontrol ve Veri Toplama Sistemleri,* coğrafi olarak çok geniş bir alana yayılmış bir sistemin bileşenlerini merkezi olarak izlemek ve kontrol etmek için kullanılan sistemlerdir.
- *Dağıtık Kontrol Sistemleri,* belli bir tesis ve konumla sınırlı bir endüstriyel süreci izlemek ve kontrol etmek için, tesisin tümüne yayılmış kontrol bileşenleri bulunan sistemlerdir.

3. Türkiye'nin Siber Güvenlik Stratejileri

Türkiye'deki siber güvenliğe yönelik çalışmaların ve yasal düzenlemelerin çok yeni olduğunu söylemek yanlış olmayacaktır. Siber güvenlik kapsamındaki çalışmalar 2012 yılına kadar Bilim Teknoloji ve İletişim Kurumu (BTK) tarafından yürütülmüştür. 2012 yılında siber güvenlik faaliyetlerini yürütme ve koordinasyon görevi, Bakanlar Kurulu'nun 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Kararı" (USGÇYYKİK) ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na (UDHB)

[7] Şeref Sağıroğlu, "Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler", *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık* içinde, ed. Şeref Sağıroğlu ve Mustafa Alkan, (2018), 26.
[8] TÜBİTAK, "Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı", http://hgm.ubak.gov.tr/Content/UploadedFile/Kritik%20Bilgi%20Sistem%20Altyapıları%20İçin%20Asgari%2 Güvenlik%20Önlemleri&&6445b90e-b2ad-4e5e-9c13-6ae19ba 10e37.pdf, 2019, s. 6-7, (04.01.2019).

devredilmiş ve Siber Güvenlik Kurulu oluşturulmuştur[9]. 2012 yılından itibaren UDHB tarafından atılan adımlar ile Türkiye'nin siber güvenlik faaliyetlerine ise önemli ölçüde yön vermiştir.

3.1. Siber Güvenlik Kurulu

Ulusal siber güvenliğin sadece tek bir kurum tarafından yürütülecek bir uygulamayla değil de bütün kamu kurumları ve özel sektör kuruluşlarının katılımı ve dayanışmasıyla yürütülmesi gerektiği anlaşılmıştır. Bu gerçeğin anlaşılması ile uluslararası düzenlemelere paralel olarak bir üst yönetim ve karar organının kurulması ihtiyacı ortaya çıkmıştır. Bakanlar Kurulunun 2012 yılındaki USGÇYYKİK ile Siber Güvenlik Kurulu oluşturulmuştur. Stratejik plan kapsamında tüm kamu kuruluşlarıyla bütün tarafların Siber Güvenlik Kurulu'nun belirlediği politikalara, stratejilere ve eylem planlarına uyması ve bununla ilgili yükümlülükleri[10] yerine getirmesi istenmiştir. 2016-2019 Ulusal Siber Güvenlik Stratejisi kapsamında bilişim teknolojileriyle güvenlik konusunda öncü kimi kamu ve özel sektör kuruluşları Siber Güvenlik Kurulu üyeleri olarak sayılmıştır.

3.2. Ulaştırma ve Altyapı Bakanlığı

Bakanlar Kurulunun 2012/3842 sayılı USGÇYYKİK ile siber güvenlik ile ilgili temel görevler ve eylem planlarının hazırlanması görevi UDHB'na verilmiştir. UHDB ulusal çapta yürütülen siber güvenlik çalışmalarına önderlik etmekte, yasal düzenlemeler oluşturmakta, ulusal siber güvenlik stratejisini belirlemekte ve tatbikatlar ile kurum ve kuruluşların siber saldırılara karşı hazırlıklı olma seviyeleri arttırmaya çalışılmaktadır. Siber güvenliğe yönelik ulusal çaptaki ilk tatbikat 25-28 Ocak 2011 tarihinde 41 kurum ve kuruluşun katılımı ile gerçekleştirilmiştir[11]. Bu tatbikat sonucunda tespit edilen hata ve eksiklikler giderilmeye çalışılmıştır.

2018 yılında gerçekleştirilen başkanlık sistemine geçiş ile birlikte UDHB'lığı Ulaştırma ve Altyapı Bakanlığı şeklinde tekrar düzenlenmiştir. Siber güvenlik faaliyetlerinin koordinasyon ve siber güvenlik kurulu başkanlık görevi aynen devam etmiştir. Siber güvenliğin

[9] Seda Yılmaz ve Şeref Sağıroğlu. "Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi", *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, (2013b):329.
[10] Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (UDHB), "2016-2019 Ulusal Siber Güvenlik Stratejisi", http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf, 2016, s. 6, (04.01.2019).
[11] Faruk Aydın, "Cyber Security in National Protection of Turkey", (Yayımlanmamış Yüksek Lisans Tezi, Çankaya Üniversitesi, 2012).

arttırılması kapsamında UDHB tarafından iki adet strateji ve eylem planı yayınlanmıştır.

3.3. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı

İlgili plan Bakanlar Kurulu'nun 2012/3842 sayılı kararı gereği hazırlanmıştır. Eylem planında öncelikle 2013-2014 yıllarında siber güvenliğin arttırılmasına yönelik alınması gerekli planlar ele alınmıştır. Daha sonra bu tarihleri aşan ve sürekli yürütülmesi gereken faaliyet, eğitim ve geliştirme çalışmalarına yer verilmiştir. Bundan dolayı eylem planı her ne kadar 2013-2014 yılları için hazırlanmış olsa da uzun süreli bir doküman haline gelmiştir.

İlgili Siber Güvenlik Stratejisi ve Eylem Planının amacı,[12] öncelikle kamusal bilgi teknolojilerinin ve sistemleri üzerinden sağlanan sistemlerin güvenliğinin sağlanması olarak belirlenmiştir. İkinci amaç olarak kamusal kritik altyapılar ve bunlara ilişkin sistemlerinin güvenliğinin sağlanması olarak tayin edilmiştir. Son olarak ise, siber saldırılar sonucu zarar gören sistemlerin normal çalışma düzenlerine döndürülmesi ve saldırıyı gerçekleştirenlere yönelik adli makam ve kolluk kuvvetlerince yürütülecek faaliyetlerin koordinesine yönelik altyapı çalışmaları oluşturmuştur.

İlgili Eylem Planı kapsamında kamu bilişim sistemleri, gerek kamuda gerekse özel sektörde gerçekleştirilen altyapılara ilişkin bilişim sistemleri şeklinde tespit edilmiştir. Eylem planı kapsamında yedi adet stratejik siber güvenlik eylemi tanımlanmıştır. Tespit edilen stratejik siber güvenlik eylem planları ise şunlardır[13]:

- Hukuki düzenlemelere yer verilmesi,
- Adliye süreçlerine destek olan faaliyetlerin yapılması,
- Ulusal siber olaylarını denetleyecek organizasyonların kurulması,
- Ulusal siber güvenlik altyapısını güçlendirmeye yer verilmesi,
- Siber güvenliğe ilişkin personel yetiştirilmesine ve bilinçlendirilmesine imkan tanınması,
- Siber güvenlikle ilgili yerli teknolojilerin daha çok kullanılması,
- Ulusal güvenlikle ilgili mekanizmaların yaygınlaştırılmasıdır.

İlgili strateji ve 2013-2014 Eylem Planı, değerlendirildiğinde öncelikle ülkemize özgü olmadığı ve kamu ve özel sektör kuruluşlarının görev ve sorumluluklarını açıklamadığı, eylem

[12] UDHB, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", s. 10.
[13] Age, s. 10.

planlarında belirtilen sürelerin aşıldığı, yasal altyapının yetersiz olduğu, eğitim ihtiyaçlarının tespit edilemediği, kritik altyapılara yeterli önemin verilmediği ve bütçelendirmenin yapılamadığı[14] gibi konularda çeşitli eleştiriler yöneltilmiştir.

3.4. 2016-2019 Ulusal Siber Güvenlik Stratejisi

2013-2014 Eylem Planındaki düzenlemelerin geçerliğini yitirmesi üzerine UDHB öncülüğünde bütün paydaşların katılımıyla yeni stratejik planın oluşturulması çalışmalarına daha hızlı ve bilinçli bir şekilde başlanmıştır. Öncelikle eski stratejik plandaki hedeflerin gerçekleşmesi üzerinde durulmuştur. Daha sonra geniş kapsamlı bir katılım ve uluslararası kuruluşlar ve gelişmiş ülke örnekleri de dikkate alınarak stratejik plana son hali verilmiştir.

2016-2019 siber güvenliğe ilişkin Strateji ve Eylem Planında öncelikli amaç olarak siber güvenliğin ulusal güvenliğin bir parçası kabul edilmesi ve ulusal siber uzaydaki sistemler ve paydaşların güvenliğinin sağlanması için gerekli tedbirlerin alınmasına ilişkin yetkinliklerin sağlanması esası benimsenmiştir[15]. Bu düşünce doğrultusunda oluşturulan stratejik planın kapsamı, ulusal siber uzayda yer alan tüm bileşenler şeklinde kamu ve özel sektörün bilişim sistemleriyle ilgili tüm taraflarını kapsamaktadır[16]. Bu amaç ve kapsam doğrultusunda hazırlanan stratejik plan kapsamında beş adet siber güvenlik stratejik eylemi tespit edilmiştir. Tespit edilen siber güvenlik stratejik eylemleri şunlar olmuştur[17]:

- Siber savunmayı güçlendirmek ve kritik altyapıları korumak,
- Siber suçlar ile mücadele etmek,
- Farkındalığı ve insan kaynağını geliştirmek,
- Siber güvenlikle ilgili ekosistemi geliştirmek,
- Siber güvenliği milli güvenlikle bütünleştirmektir.

Eylem planları genel olarak değerlendirildiğinde, öncelikle kritik altyapıların korunması kavramının eylem planlarına dahil edilmesi, konunun öneminin kavrandığını göstermektedir. Ayrıca siber güvenlik kapsamında personel eğitimine önem verilmesi de gelmektedir. Siber güvenliğe yönelik sorumlulukların tespit edilmemiş ve bütçe tahsis edilmemiş olması, stratejik

[14] Akın Aytekin, "Türkiye'nin Siber Güvenlik Stratejisi ve Eylem Planının Değerlendirmesi", (Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi, 2015)
[15] UDHB, "2016-2019 Ulusal Siber Güvenlik Stratejisi", s. 9.
[16] Age, s. 9.
[17] Age, s. 10.

plana yönelik getirilebilecek önemli eleştiriler arasında sayılabilir. Ayrıca genel olarak değerlendirildiğinde stratejik eylemlerin bir önceki stratejik planın tekrarı konumunda olduğu görülmektedir.

3.5. Kamu Güvenliği Ağı (Kamu-Net)

Kamu-Net'in projesi Ulaştırma ve Altyapı Bakanlığı tarafından; Ulusal Siber Güvenlik Stratejisinde ve 5809 sayılı Elektronik Haberleşme Kanunu'nda (md.5/1) belirtilen hükümler gereğince yürütülmeye başlanmıştır. Kamu-Net projesinin amacı olarak şunlar kabul edilmiştir:

- Vatandaşlara internet hizmetini kapalı ve güvenli bir sanal ağla sunmak,
- Siber güvenliği sanal ortamda belli standartlar altında sağlamak,
- Kamu kurumlarının uyumlu çalışabileceği alt yapıyı hazırlamaktır.

Sayılan amaçlara ulaşılabilmesi için birçok yasal düzenlemeye gidilmiştir. Kamu-Net'in kurulmasına ilişkin Protokolü UHDB ile Türk Telekomünikasyon arasında 2015 yılında imzalandıktan sonra; kamu kurumlarının Kamu-Net ağına girmesi için 2016 yılında 2016/28 sayılı Başbakanlık Genelgesi kabul edilmiştir. Ardından "Kamu-Net Ağına Bağlanmasına ve Denetimine İlişkin Tebliğ" 2017 yılında yayımlanmıştır. Bu tebliğle Aralık 2018 tarihi itibariyle 146 kamu kurumun daha Kamu-Net'e dâhil olması hedeflenmiştir.

4. Avrupa Birliğinin Siber Güvenlik Stratejileri

Avrupa Birliği'nin siber saldırılara karşı en önemli silahı hayata geçireceği yasal düzenlemelerdir. Çünkü AB'nin saldırılara karşı doğrudan operasyonel kapasitesi ve yasal kurumları mevcut bulunmamaktadır. Bu nedenle AB'nin yürürlüğe koyacağı yasal düzenlemeler ile üye ülkelerin siber güvenliğinin artırılması ve siber saldırılar karşısında hazırlıklı olması istenmektedir. AB üye ülkeleri, siber güvenlik yatırımlarını arttırmaya, personel eğitimine önem vermeye ve teknolojik yatırımlarını cesaretlendirmeye çalışmaktadır[18]. Bu sayede operasyonel kapasitesi veya yasal kurumları olmamasına rağmen hayata geçirdiği öncü danışma kurumları ve çıkardığı yasal düzenlemeler ile üye ülkelere öncülük etmesi amaçlanmaktadır.

Siber saldırıların sadece tek bir kişi ya da ülkeyi hedef alan bir tehdit olmamasından ve kişisel, kurumsal veya ulusal birçok siber saldırı yaşanmasından dolayı AB, kendi kurumlarını

[18] Camino M. Martinez, "Game Over? Europe's Cyber Problem", Centre for European Reform, https://www.cer.eu/publications/archive/policy-brief/2018/game-over-europes-cyber-problem, (20.01.2019).

ve üye ülkelere yol gösterici bir strateji izlemek amacıyla siber güvenlik politikalarını sürekli güncellemektedir. Bu kapsamda hayata geçirilen kurum ve yasal düzenlemelerin arasında başlıca; 2004 Avrupa Komitesi'nin Siber Suç Sözleşmesi, 2004'de Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA) [19], 2005'de Bilgi sistemlerinin Korunmasına Yönelik Düzenleme ve 2013'de Europol İçerisinde Siber Suçlar Merkezi'nin oluşturulması[20], 2013'de Avrupa Birliği Siber Güvenlik Stratejisi, 2015'de Avrupa Birliği Güvenlik Ajandası ve 2016'da ise, Avrupa Siber Güvenlik Kurumu (ECSO) sayılabilir.

Siber saldırılara karşı konulurken bilgi güvenliğine yönelik politikaların amaç, kapsam ve seviyesini en iyi açıklayan dokümanların başında yasal düzenlemeler gelmektedir. Aynı zamanda yasal düzenlemeler, kamu politikalarının resmi düzenlemelere yansıdığı ve üzerinde uzlaşı sağlandığı politik düzenlemeler olmaktadır. Bu tür düzenlemeler ile siber saldırılarda kullanılan yazılımların engellenmesi mümkün olmasa da bu zararlı yazılımların kullanılmasının nasıl değerlendirileceği baştan belirlenebilir. AB düzenleme, direktif ve yönetmelikler ile üye ülkelere yön gösterici düzenlemeleri hayata geçirirken; üye ülkeler ise, AB düzenlemeleri ve uluslararası sözleşmelere bağlı kalarak kendi iç hukuklarını saptayabilmektedirler[21]. Bu sayede ideal bir siber güvenlik seviyesi yakalanmaya çalışılmaktadır.

AB tarafından siber güvenliğe yönelik atılan ilk adımlardan birisi, 2001 yılında online dolandırıcılığa karşı hayata geçirilen düzenleme olmuştur[22]. Bu düzenleme ile AB bütün üye ülkelerin online dolandırıcılık faaliyetlerinde (online bilgi sistemlerine saldırı, bilgi hırsızlığı, izinsiz erişim, kişisel bilgilerin çalınması vb.) yasa dışı ilan etmelerini yasal yükümlülük altına almak istemiştir. Bu düzenleme aynı zamanda suç tanımına yeni kavramlar ekleyerek casus yazılımların üretilmesini, alımı ve satımı ve siber suçlar amacıyla kullanımını da yasaklamıştır. Bu suçları işleyenlere 5 yıla kadar hapis cezası öngörülmüş ve üye ülkelerin bu suçu kişisel bilgilere ulaşma ve çalma amacıyla kasıtlı olarak işleyenlere yüksek cezalar vermesi önerilmiştir[23]. Bu ilk düzenleme ile siber güvenliğin temelleri atılırken; aynı zamanda siber

[19] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe", https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from= EN, 2010:16, (20.01.2019).
[20] Helena Carrapico ve Aandre Barrinha. "European Union Cyber Security as an Emerging Research and Policy Field", *European Politics and Society* 19, no. 3, (2018): 299.
[21] Türkay Henkoğlu ve Bülent Yılmaz, "Avrupa Birliği (AB) Bilgi Güvenliği Politikaları", *Türk Kütüphaneciliği 27*, sy.3, (2003): 460.
[22] Camino M. Martinez, "Game Over? Europe's Cyber Problem", s. 4.
[23] Age, s. 4.

uzayda işlenen suçların cezalandırılması ve caydırıcılık seviyesinin arttırılması da amaçlanmaktadır.

Bireysel veya bilgi sistemlerine yönelik saldırıların ardından 2004 yılında İspanya'nın başkenti Madrid'de gerçekleşen ve yolcu trenlerini hedef alan terörist saldırılar sonrasında Avrupa Komisyonu kritik altyapıların korunmasına yönelik olarak "Terörizmle Mücadele Kapsamında Kritik Altyapıların Korunması"na ilişkin tebliğini yayınlamıştır[24]. Bu tebliğ ile temelleri atılan kritik altyapıların korunmasına daha sonra hazırlanan Avrupa Komisyonunun 2005/576, 2006/786, 2006/787 ve 2008/676 sayılı komisyon çalışmaları sonucu hazırlanan 2008/114 sayılı direktifi oluşturulmuştur. Direktif enerji, ulaşım, bilgi teknolojileri ve iletişim sektörüne yönelik düzenlemeler içermiştir[25]. Kritik alt yapılara yönelik saldırılar toplumsal hayatı yakından etkilediği için bu kurumların siber güvenliğinin önemi artmıştır. Özellikle son dönemde AB ve Türkiye'de hazırlanan siber güvenlik stratejik planlarında kritik alt yapıların ağırlığı giderek ön plana çıkmıştır.

4.1. Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (European Union for Network and Information Security- ENISA)

AB Ağ ve Bilgi Güvenliği Ajansı (ENISA) 2004 yılında çıkarılan bir düzenleme (EC Regulation No 460/2004) ile kurulmuş olup, merkezi Yunanistan'ın başkenti Atina'dadır[26]. ENISA'nın ana görevi, AB içindeki ağ ve bilgi güvenliği sorunlarını önleme ve bunlara yanıt verme yeteneğini arttırmak için ulusal ve birlik kapasitesini geliştirmektir. ENISA ağ ve bilgi sistemlerinin güvenliği hakkında 2016/1148 sayılı Direktifin (NIS Direktifi) uygulanmasına destek olmak için özel ilave roller ve sorumluluklar üstlenmiştir[27]. Ajansın faaliyetleri, AB organları ve üye devletler tarafından bilinçlendirme ve işbirliğinin desteklenmesinin yanı sıra tavsiye ve önerilerde bulunma, veri analizi sağlamadan oluşmaktadır. Ulusal ve topluluk çabalarına dayanarak, ajans bu alanda bir uzmanlık merkezi konumundadır. ENISA uzmanlığı üye devletler arasında, kamu ve özel sektörden gelen eylemler arasındaki işbirliğini geliştirmek ve kapasite geliştirmeyi desteklemek için kullanılmaktadır. ENISA, stratejik hedeflere ulaşmak

[24] Mustafa Ünver vd. *Kritik Altyapıların Korunması*, (Bilgi Teknolojileri ve İletişim Kurumu, 2011b, s. 13).
[25] Age, s. 13-26.
[26] Mustafa Ünver vd. *Uluslararası Kuruluşların Siber Güvenlik Faaliyetleri*, (Bilgi Teknolojileri ve İletişim Kurumu, 2011a, s. 22).
[27] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on ENISA, the EU Cybersecurity Agency, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification. COM(2017)477 final.

için yönetmeliğe uygun olarak aşağıdaki dört temel görevi üstlenmektedir[28] [29] [30].

- Avrupa Komisyon'a ve üye devletlere bilgi güvenliği konusunda danışmanlık yapmak ve onlara yardım etmek,
- Avrupa'daki artan riskler ve saldırılar hakkında veri toplama ve analiz etmek,
- AB'nin bilgi güvenliği tehditlerine ilişkin risk değerlendirmesi ve risk yönetimi yöntemlerini teşvik etmek,
- Bilgi güvenliği alanındaki farkındalığın arttırılması ve işbirliğinin güçlendirilmesini sağlamaktır.

Bu kapsamda ENISA üye devletlerin katılımıyla gerçek zamanlı olay senaryolarının canlandırıldığı tatbikatları koordine etmektedir. Bu tatbikatlar sayesinde üye devletlerin ağ ve bilgi sistemlerinin güvenliği ile ilgili hazırlık ve işbirliği seviyeleri test edilmektedir. Bu tatbikatlar sonucu üye devletlere siber güvenlik düzeylerini geliştirebilmeleri için öneriler hazırlanmaktadır[31]. Her ne kadar operasyonel gücü ve kurumları olmasa da ENISA; üye ülkelerin siber güvenlik kurumlarının oluşturulmasında ve güvenlik seviyelerinin arttırılmasında aktif ve etkin bir rol oynamaktadır. Bu sayede birliğin siber güvenlik seviyesine önemli katkılar sağlanmaktadır.

4.2. Avrupa Siber Güvenlik Kurumu (European Cyber Security Organization ECS)

Kendi finans kaynakları olan ve kar amacı gütmeyen Avrupa Siber Güvenlik Kurumu (ECSO), 2016 yılında kurulmuştur. Kurumun amacı, AB içerisindeki siber faaliyetlere ilişkin güvenlik önlemlerini artırmak, güçlendirmek ve bu kapsamda atılacak her girişimi desteklemektir[32]. ECSO üyesi kuruluşlar; büyük şirketler, KOBİ'ler ve kuruluşlar, araştırma

[28] European Commission, "Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity certification "Cybersecurity Act", https://ec.europa.eu/transparency/regdoc/rep/ 1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF, , 2017b, s. 3, (20.01.2019).
[29] European Commission, "Study on the Evaluation of the European Union Agency for Network and Information Security", https://ec.europa.eu/digital-single-market/en/news/final-report-evaluation-european-union-agency-network-and-information-security-enisa, 2017e, s. 9-10, (20.01.2019).
[30] Mustafa Ünver, Cafer Canbay ve Ayşe G. Mirzaoğlu, *Uluslararası Kuruluşların Siber Güvenlik Faaliyetleri*, s. 22.
[31] European Union, "Directive (EU) 2016/1148 of The European Parliament and of The Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union", https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX :32016L1148&from= EN, 2016, s. 7, (20.01.2019).
[32] European Cyber Security Organization (ECSO), www.ecs-org.eu, (21.01.2019)

merkezleri, üniversiteler, son kullanıcılar, operatörler, kümeler ve derneğin yanı sıra AB üye devletlerinin yerel, bölgesel ve ulusal yönetimleri, ülkelerin bir parçası olan çok çeşitli menfaat sahipleri ve Avrupa Ekonomik Alanı (EEA), Avrupa Serbest Ticaret Birliği (EFTA) ve AB araştırma ve geliştirme programı olan Horizon 2020 ile ilişkili ülkeler oluşturmaktadır.

ECSO'nun temel amacı, Avrupa siber güvenliğini geliştirmeyi ve teşvik etmeyi amaçlayan her türlü girişim veya projeyi desteklemek ve özellikle kendisine verilen aşağıdaki görevleri yerine getirmektir[33]:

- Siber tehditlere karşı Avrupa Dijital Tek Pazarının büyümesini teşvik etmek ve korumak;
- Avrupa'daki siber güvenlik piyasasını geliştirmek ve artan pazar konumu ile rekabetçi bir siber güvenlik ve bilgi ve iletişim teknolojileri endüstrisinin gelişmesini sağlamak;
- Avrupa'nın lider olduğu sektörel uygulamalarda, güvenilir tedarik zincirlerinin kritik adımları için siber güvenlik çözümleri geliştirmek ve uygulamaktır.

4.3. Avrupa Komitesi Siber Suç Sözleşmesi 2004 (EU Cyber Security Act)

Avrupa Komitesi'nin Siber Suç Sözleşmesi (European Committee on Crime Problems-CDPC), 2001 yılında üye ülkelerin imzasına açılarak 2004 yılında yürürlüğe giren siber suçlara ilişkin ilk uluslararası antlaşma özelliğine sahiptir[34]. Siber ortamların güvenliği konusunda AB'nde kabul edilen en önemli hukuki metindir. Sözleşmeyi Türkiye, 10 Kasım 2010 tarihinde imzalamış; 2014 yılında ise, buna yönelik olarak 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesine İlişkin Kanun kabul edilmiştir[35]. Bu sözleşme ile siber alanın tamamen güvenli hale getirilmesi imkansız gibi gözükse de ilgili sözleşme, AB üyesi ülkelerin bir araya gelerek hazırladığı ve zamanının en kapsamlı düzenlemeleri arasındadır. Sözleşmeye taraf olmak, ülkemiz açısından siber güvenliğe verilen önemin bir göstergesi sayılabilir.

Avrupa'da bilgi güvenliği politikalarının oluşturulması kapsamında Avrupa Komisyonu tarafından Kasım-2005 tarihinde yayımlanan "Kritik Altyapıları Koruma Programına Yönelik

[33] European Cyber Security Organization (ECSO), "About ECSO–Mission& Objectives", http://ecs org.eu/about, (16.01.2019).
[34] Murat Önok, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslar Arası İşbirliği", *Marmara Üniversitesi Hukuk Araştırmaları Dergisi 19*, sy.2, (2013): 1241.
[35] Nusret O. Akpek, "Siber Suçlar Sözleşmesinin Getirdikleri ve İç Hukuk Açısından Konuya Yaklaşım", (Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, 2015)

Yeşil Kitap" diğer önemli bir belgedir[36]. Bu belgeyle kritik türden bilgi ve iletişim altyapısıyla olabilecek saldırılardan ve doğabilecek her türlü zarardan korunması öngörülmüş ve bireylerin bu tür felaketlerden korunmasını amaçlayan tedbirlere başvurulmuştur[37]. Siber saldırılarda yaşanan artışlar nedeniyle kısmi ya da kısıtlı kapsamlı çalışmalardan sonra daha kapsamlı bir stratejik plan yapılması ihtiyacı doğmuştur.

4.4. Avrupa Birliği'nin 2013 Siber Güvenlik Stratejisi

AB tarafından siber güvenliğe ve siber savunmaya yönelik hayata geçirilen birçok uygulama diğer ülke ve kuruluşlara örnek olmuştur. Özellikle 2013 yılında AB siber güvenlik politikasının temellerini oluşturacak olan ve Avrupa Ekonomik ve Sosyal Komite ve Bölgesel Komite tarafından hazırlanan "Avrupa Birliği Siber Güvenlik Stratejisi" raporu siber güvenlik kapsamında önemli bir adımdır. Raporda AB'nin siber güvenlik stratejisinin temeli "açık, emniyetli ve güvenli siber ortam" sloganı ile oluşturulması amaçlanmıştır. AB ve uluslararası siber güvenlik politikalarına rehberlik etmesi amacıyla oluşturulan raporda, siber güvenliğin etkin ve etkili bir şekilde sağlanması için siber güvenlik politikalarının temel hak ve özgürlükleri kısıtlamadan uygulanması gerektiği vurgulanmıştır. AB'nin siber güvenliğe ilişkin dayandığı temel ilkeler olarak şunlar belirlenmiştir[38] [39]:

- Fiziksel ortamda sağlanan Avrupa Birliği temel değerlerinin dijital ortamda da oluşturulması,
- Temel hak ve özgürlüklerin, ifade özgürlüğü ve kişisel bilgilerin ve mahremiyetin korunması,
- Herkese açık internet ortamının oluşturulması,
- Demokratik ve etkin katılımlı yönetimini oluşturulması,
- Sorumluluk paylaşımı ile güvenliğin sağlanmasıdır.

Bu ilkeler üzerine kurulan 2013 stratejisinde siber esnekliği sağlamak için, kamu otoriteleri ve özel sektör işbirliği, siber kapasite, kaynak ve verimliliğin geliştirilmesi

[36] European Commission, "Green Paper on a European Programme for Critical Infrastructure Protection", https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN, (16.01.2019).
[37] Türkay Henkoğlu ve Bülent Yılmaz, "Avrupa Birliği (AB) Bilgi Güvenliği Politikaları", s. 461.
[38] European Commission, "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", s. 3-4.
[39] European Commission, "EU Cybersecurity Initiatives- Working Towards a more Secure Online Environment. Factsheet", s. 2.

öngörülmüştür. Ancak, siber güvenlik olaylarının tespit edilmesi, önlenmesi ve yönetilmesi iyileştirilmeden ve AB düzeyinde koordine edilmeden bu hedeflere ulaşmak mümkün değildir. Bu nedenle 2013 stratejisi, üye devletlerdeki siber dayanıklılığı güçlendirmek amacıyla ENISA (Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı) için özel ve belirgin bir rol oynamıştır[40]. Bundan dolayı stratejik plan kapsamında ENISA'nın etkinliği arttırılarak siber güvenliğin sağlanması konusunda daha etkin ve öncü hale getirilmesinin gerekliliği dile getirilmiştir.

2013 ve 2017 yılları arasında yaşanan siber saldırıların Avrupa ekonomisine verdiği zararın beş katına çıktığı ve bu zararın 2019 yılına kadar üç kat daha artacağı değerlendirilmektedir[41]. Bu yüzden AB 2013 siber güvenlik stratejisi yaşanan teknolojik ve ekonomik gelişmeler ve risk algısındaki değişim nedeniyle Eylül 2017 tarihinde revize edilmiştir. Revize kapsamında yapılan değişikliklerde kritik altyapıların güvenliği ve bölgesel siber güvenlik kavramları ön plana çıkmıştır. Güncellenen siber güvenlik stratejisi beş temel reform hareketini içermiştir[42]. Bu reform hareketlerinden birincisi, Avrupa Siber Güvenlik Araştırma ve Yeterlilik Merkezi'nin kurulmasıdır. İkincisi, Avrupa çapında yaşanacak büyük çaplı saldırılara karşı koruyucu ve önleyici tedbirleri uygulayacak Avrupa çapında acil durum müdahale mekanizmasının sağlanmasıdır. Üçüncüsü, siber güvenlik acil durum fonunun oluşturulması; dördüncüsü, Avrupa savunma fonunun yardımıyla askeri siber güvenliğin bir parçası olacak ortak projelerin geliştirilmesidir. Son olarak ise, dünya çapında siber risklerin azaltılması için güven verici önlemlerin hayata geçirilmesi ve ülkesel sorumlulukların düzenlenmesidir. Bütün bu geliştirme önerileri AB'nin siber saldırılar karşısındaki esneklik, caydırıcılık ve güvenliğini arttırmayı amaçlamaktadır[43]. Bu reform hareketinin ortak noktaları, üye ülkelerini katılımı ile operasyonel kurumların oluşturulmaya çalışılması ve siber güvenlik faaliyetlerine yönelik ortak mali fonların kurulmak istenmesi olarak dikkat çekmektedir.

4.5. Avrupa Birliği Güvenlik Ajandası (2015) European Agenda on Security

AB komisyonu tarafından Nisan 2015 tarihinde kabul edilen AB Güvenlik Ajandası

[40] Laszlo Kovacs, , "Cyber Security Policy and Strategy in the European Union and NATO", *Military Art and Science*, 1(89), 2018, s. 17-18)
[41] European Commission, "Resilience, Deterrence and Defense: Building Strong Cyber Security for the EU", https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN, 2017a, s. 2, (20.01.2019).
[42] Annegret Bendiek vd. "*The EU's Revised Cybersecurity Strategy Half-Hearted Progress on Far-reaching Challenges*", *Stiftung Wissenschaft und Politik*, SWP Comments 47. İng. Cev. T.Genrich, 2017, s. 2.
[43] Age, s. 2.

2015-2020'nın üç hedefinden biri, siber suçlar ile daha etkin bir şekilde mücadele edilmesidir. Siber suçlarla birlik seviyesinde koordine edilmiş ortak tepki verilerek mücadele edilebileceği kabul edilmiştir. Bu kapsamda oluşturulan hareket tarzları ise şunlardır[44]:

- Mevcut siber güvenlik önlemlerine yeni bir bakış açısı getirilmesi,
- Yasal düzenlemelerin genişletilmesi ve güncellenmesi,
- Siber suçlara yönelik adli araştırmaları geliştirilmesi,
- Siber suçlar ile mücadele kapasitesinin uluslararası kuruluşlar yardımıyla iyileştirilmesidir.

4.6. Dijital Tek Pazar Stratejisi (2015) (Digital Single Market Strategy)

Dijital ekonominin temeli güven ve emniyettir. Bu yüzden AB, Mayıs 2015 tarihinde kamu ve özel sektör kuruluşlarında katılımı ile Dijital Tek Pazar Stratejisini hazırlamıştır. Bu stratejinin amacı, Avrupa'nın rekabetçiliğini teşvik etmek ve yenilikler yoluyla siber güvenlik pazarının parçalanmasını engellemek, üye devletler ile sanayi aktörleri arasında güven oluşturmak ve siber güvenlik ürünleri ve çözümleri için talep ve tedarik sektörlerinin eşitlenmesine yardımcı olmaktır. Ayrıca bu stratejinin, Avrupa'da dijital güvenlik endüstrisi kaynaklarını yapılandırmakta ve koordine etmekte etkili olması beklenmektedir. Strateji yenilikçi KOBİ'lerden bileşen ve ekipman üreticisine, kritik altyapı operatörlerine ve araştırma enstitülerine kadar çok çeşitli aktörleri içermektedir. Son olarak ortaklık, siber güvenliğe yapılan yatırımları artırmak için AB, ulusal, bölgesel ve özel kurum ve kaynaklardan (araştırma ve inovasyon fonları dahil) yararlanmaktadır[45]. Siber güvenliğin önemli etkenlerinden biri de kullanılan bilişim ve iletişim sistemlerinin üretiminden itibaren kontrol altına alınması ve dış bağımlılıktan kurtarılmasıdır. Siber güvenlik ile cihaz ve yazılımlarının üretiminden itibaren kontrol altında bulundurulması ve dış kaynaklı saldırıların azaltılması hedeflenmektedir. Bu yüzden AB iç kaynaklarda yapılacak her türlü yatırımı desteklemekte ve teşvik etmektedir.

5. Değerlendirme ve Öneriler

Teknoloji ve bilgi teknolojilerinin günlük hayatımızın ayrılmaz birer parçası haline gelmesinin yanında, kamu ve özel sektör tarafından sunulan hizmetlerin de büyük bir kısmı

[44] European Commission, "EU Cybersecurity Initiatives- Working Towards a more Secure Online Environment. Factsheet". http://ec.europa.eu/ information_society/newsroom/image/document/2017-3/factsheet_cyber security_update_january_2017_41543.pdf, 2017c, s. 2, (20.01.2019).
[45] Age, s. 3.

siber ortamlara taşınmış durumdadır. Bilginin erişim ve kullanılımının siber güvenlik ortamında ve emniyet ilkelerine riayet edilerek yapılması çok önemlidir. Bunun için özellikle siber güvenlik stratejileri kapsamında kişisel güvenlikten başlayarak ulusal güvenliğe kadar değişen seviye ve kapsamda detaylı planlama, uygulama, koordine ve denetlemeye ihtiyaç vardır. Ayrıca, bu çalışmaların uluslararası kurumlar ile işbirliği ve uyum içinde yapılması, kamu kurumları ve özel sektör kuruluşları arasında koordine edilecek bir tarzda yürütülmesi siber güvenlik stratejilerinin etkinliğini ve başarısını olumlu yönde etkileyecektir.

Son zamanlarda devletler ve kamu kurumları tarafından siber güvenliğin önemi daha çok kavrandığı, alınan güvenlik tedbirlerinin ve siber güvenliğe yönelik ilginin artmasından anlaşılmaktadır. Ancak günümüzde siber güvenlik tedbirlerinin tamamen yeterli seviyelerde olduğunu söylemek de pek mümkün gözükmemektedir. Siber tehdit, her geçen gün büyümekte; bireysel, kurumsal veya ulusal düzeylerde daha da belirgin hale gelmektedir. Bu kapsamda Türkiye'nin AB'nin siber güvenlik stratejilerini dikkate alarak mevcut stratejilerini gözden geçirmesi ve gelecekte karşılabileceği muhtemel siber saldırılara karşı daha dayanıklı, etkili ve uygulanabilir stratejilerini acilen hayata geçirmesi gerekmektedir.

Siber güvenlik stratejileri daha çok yasal düzenlemeler ve kurumsal yapıların oluşturulması şeklinde düşünüldüğünde, Türkiye'de siber güvenlik stratejilerine ilişkin temel unsurlar olarak öncelikle şu tedbirlerin uygulanması kaçınılmaz gözükmektedir[46] [47]:

- *Ulusal Politika ve Stratejinin Geliştirilmesi:* Öncelikle stratejik planların geliştirilerek, daha detaylı şekilde sorumlulukların tespit edilmesi, sektörel bazda özel eylem planlarının ve hareket tarzlarının belirlenmesi ve kritik altyapılara ilişkin rehber, standart ve çerçeve dokümanlarının hazırlanması gerekmektedir. Standart hareket tarzlarının ve çerçeve dokümanlarının hazırlanması yaşanabilecek saldırılara karşı alınacak tedbirlerin başarı olasılığını arttıracaktır.
- *Yasal Çerçevenin Oluşturulması:* Siber saldırılara yönelik hukuki ve yasal çerçevenin oluşturulması, uygulama ve denetimine ait kuralların belirlenmesi ve saldırılara karşı caydırıcılığı yüksek hukuki düzenlemelerin yapılmasını zorunlu hale getirmektedir.

[46] Seda Yılmaz ve Şeref Sağıroğlu, "Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri", *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, (2013a): 158-159.
[47] Seda Yılmaz ve Şeref Sağıroğlu, "Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi", *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, (2013b): 329-330.

- *Kurumsal Yapılanmanın Belirlenmesi:* 2016-2019 Ulusal Siber Güvenlik Strateji planında başlatılan kurumsal sorumlulukların belirlenmesinin yanında, ilgili tüm tarafların görev, sorumluluk ve yasal dayanaklarının en iyi şekilde belirlenmesi esastır.
- *Ulusal Teknoloji Kullanımı:* Siber saldırılar ile mücadelenin en önemli etmenlerinden biri de bütün yönetim ve düzenleme yetkileri kendimize ait olan ulusal teknolojilerin kullanımının ön plana çıkarılmasından geçmektedir.
- *Ulusal İşbirliğinin Arttırılması:* Ulusal siber güvenlik kapsamında bütün paydaşların işbirliği içinde çalışması ve kurumlar arası koordinasyonun tam sağlanması, siber saldırılara karşı verilecek tepkilerin etkinliğinin de artmasına yol açacaktır.
- *Personel Eğitimi:* Yaşanacak siber saldırılara karşı personelin bilinçlendirilmesi ve eğitilmesi de ayrı bir önem arz etmektedir. Özellikle siber saldırı tatbikatlarında personelin hazır bulunması siber saldırılara karşı başarı oranını yükseltecektir.
- *Uluslar Arası İşbirliği ve Uyumun Sağlanması:* Öncelikle gelişmiş ülkelerin siber güvenlik uygulamalarının ülkemize transferi kapsamında uluslararası işbirliğine gidilmelidir. Ayrıca siber saldırıların sadece ülke içerisinden değil, internet vasıtasıyla dünyanın herhangi bir yerinde yapılabileceği dikkate alındığında, diğer ülkeler ile işbirliği ve uyum bu açıdan önemli olmaktadır.

Ulusal güvenlik, ekonomi, insan hakları ve sivil özgürlükler dahil bir çok konu ile ilişkili olan siber güvenlik kavramı, teknoloji çağının yaşandığı şu günlerde politikacı ve akademisyenler için de en zorlu uğraşlar arasında yer almaktadır. Siber güvenliğin önemi, ilgili yasal düzenlemeler ve akademik çalışmalardan anlaşılsa da sorunun çözümüne yönelik arayışlar hala devam etmektedir. Özellikle siber güvenliğin sağlanmasında kritik altyapıların özelleştirilmiş olması, yani güvenliğin özel sektör tarafından işletiliyor olması, siber güvenlik alanında kamu ile özel sektör işbirliğini de kaçınılmaz hale getirmektedir[48].

Siber saldırı veya tehdit, aslında Türkiye'nin gelecekte karşılaşması muhtemel önemli riskler arasında yer almaktadır. Türkiye'nin şu anda siber tehditten tamamen korunması veya gelecekte yoğun bir siber saldırıyla karşılaşmayacağını şimdiden kestirmesi de mümkün değildir. Ancak Türkiye'nin siber güvenlik stratejilerini çeşitlendirmesi ve gelecekte maruz

[48] Madeline Carr, "Public-Private Partnerships in National Cyber-Security Strategies", *International Affairs 43*, no. 62, (2016): 43.

kalabileceği siber saldırılara karşı baştan hazırlıklı olması son derece önemlidir. Bunun için Türkiye, AB'nin siber güvenlik stratejilerinin temelini oluşturan yasal ve kurumsal düzenlemelerini özellikle ilgili antlaşmalarla iç hukuk haline dönüştürebilir veya mevcut düzenlemelerini bu şekilde güncelleyebilir. Dolayısıyla Türkiye'nin gelecekte karşılaşabileceği siber saldırılara kendi siber güvenlik stratejilerini AB'nin stratejileriyle yenileyerek güçlendirmesi veya muhtemel zararlarını bu şekilde en az düzeye düşürmesi mümkündür. Hatta Türkiye'nin siber güvenlik stratejilerini AB normları çerçevesinde sürekli olarak dinamik, yenilikçi ve hızlı hareket etme kabiliyetine sahip kılacak tarzda yeniden yapılandırması tamamen kendi yararına olacaktır.

Kaynakça

Akpek, Nusret O. "Siber Suçlar Sözleşmesinin Getirdikleri ve İç Hukuk Açısından Konuya Yaklaşım", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, 2015.

Aydın, Faruk. "Cyber Security in National Protection of Turkey", Yayımlanmamış Yüksek Lisans Tezi, Çankaya Üniversitesi, 2012.

Aytekin, Akın. "Türkiye'nin Siber Güvenlik Stratejisi ve Eylem Planının Değerlendirmesi", Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi, 2015.

Bendiek, Annegret, Raphael Bossong, ve Matthias Schulze. "*The EU's Revised Cybersecurity Strategy Half-Hearted Progress on Far-reaching Challenges*", *Stiftung Wissenschaft und Politik*, SWP Comments 47. İng. Cev. T.Genrich, 2017.

Carr, Madeline, "Public-Private Partnerships in National Cyber-Security Strategies", *International Affairs*, (2016): 43-62.

Carrapico, Helena ve Aandre Barrinha. "European Union Cyber Security as an Emerging Research and Policy Field", *European Politics and Society* 19, no. 3, (2018): 299-303.

European Commission, Green Paper on a European Programme for Critical Infrastructure Protection, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN, (16.01.2019).

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01) &from=EN, (20.01.2019).

European Commission, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", https://eeas.europa.eu/archives/docs/ policies/eu-cyber-security/cybsec_ comm_en.pdf, (20.01.2019).

European Commission, Resilience, Deterrence and Defense: Building Strong Cyber Security for the EU, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN, (20.01.2019).

European Commission, Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity certification "Cybersecurity Act", https://ec.europa.eu/transparency/regdoc/rep/ 1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF,(20.01.2019).

European Commission, EU Cybersecurity Initiatives- Working Towards a more Secure Online Environment. Factsheet. http://ec.europa.eu/ information_society/newsroom/image/document/2017-3/factsheet_cyber security_update_january_2017_41543.pdf, (20.01.2019).

European Commission, Proposal for a Regulation of the European Parliament and of the Council on ENISA, the EU Cybersecurity Agency, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification. COM(2017)477 final.

European Commission, Study on the Evaluation of the European Union Agency for Network and Information Security, https://ec.europa.eu/ digital-single-market/en/news/final-report-evaluation-european-union-agency-network-and-information-security-enisa, (20.01.2019).

European Cyber Security Organization (ECSO), www.ecs-org.eu, (21.01.2019)

European Cyber Security Organization (ECSO), "About ECSO–Mission& Objectives", http://ecs-org.eu/about, (16.01.2019).

European Union, Directive (EU) 2016/1148 of The European Parliament and of The Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union", https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX :32016L1148&from= EN, (20.01.2019).

Henkoğlu, Türkay ve Bülent Yılmaz, "Avrupa Birliği (AB) Bilgi Güvenliği Politikaları", *Türk Kütüphaneciliği 27*, sy.3, (2013): 451-471.

Kovacs, Laszlo, "Cyber Security Policy and Strategy in the European Union and NATO", *Military Art and Science*, 1(89), (2018): 16-24.

Martinez, Camino M., "Game Over? Europe's Cyber Problem", Centre for European Reform, https://www.cer.eu/publications/archive/policy-brief/2018/game-over-europes-cyber-problem (20.01.2019).

Önok, Murat, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslar Arası İşbirliği", *Marmara Üniversitesi Hukuk Araştırmaları Dergisi 19*, sy.2, (2013): 1229-1270.

Resmi Gazete (2017), Kamunet Ağına Bağlanma ve Kamunet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ, http://www.resmigazete. gov.tr/eskiler/2017/06/20170621-15.htm, (11.01.2019).

Sağıroğlu, Şeref. "Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler", *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık* içinde, Editör: Şeref Sağıroğlu ve Mustafa Alkan, 21-45, 2018.

Tahran, Kamil. "Uluslararası Güvenliğin Bir Bileşeni Olarak Siber Güvenlik", Yayımlanmamış Yüksek Lisans Tezi, Selçuk Üniversitesi, 2018.

TÜBİTAK, Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı, http://hgm.ubak.gov.tr/ Content/UploadedFile/Kritik%20Bilgi%20Sistem%20Altyapıları%20İçin%20Asgari%20Güvenlik%20Önlemleri&&6445b90e-b2ad-4e5e-9c13-6ae19ba10e37.pdf, (04.01.2019).

Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (UDHB), Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf, (04.01.2019).

Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (UDHB), 2016-2019 Ulusal Siber Güvenlik Stratejisi, http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf, (04.01.2019).

Ünver, Mustafa, Cafer Canbay ve Ayşe G. Mirzaoğlu. *Uluslararası Kuruluşların Siber Güvenlik Faaliyetleri*, (Bilgi Teknolojileri ve İletişim Kurumu, 2011a),

Ünver, Mustafa, Cafer Canbay ve Burhan H. Özkan. *Kritik Altyapıların Korunması*, (Bilgi Teknolojileri ve İletişim Kurumu, 2011b).

Yılmaz, Seda ve Şeref Sağıroğlu. "Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri", *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, (2013a): 158-166.

Yılmaz, Seda ve Şeref Sağıroğlu. "Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi", *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, (2013b): 323-331.