**AVRUPA BİRLİĞİ’NE UYUM SÜRECİNDE TÜRKİYE’NİN SİBER GÜVENLİK POLİTİKALARININ ANALİZİ**

***Önder KUTLU[[1]](#footnote-1)\****

***Selçuk KAHRAMAN[[2]](#footnote-2)\*\****

***Selçuk DİNÇER[[3]](#footnote-3)\*\*\****

**ÖZ**

Siber güvenlik nispeten yeni bir alan olarak sadece ulusal hükümetlerin değil, uluslararası kuruluşların da gündemine yoğun biçimde girdi. Bilgi iletişim teknolojilerindeki baş döndürücü gelişmeler bireylerin ve devletlerin hayatlarını kolaylaştırdıkları kadar, ciddi tehditler içerdiği de artık görülmeye başlandı. Avrupa düzeyinde siber güvenlik alanının tesisi Avrupa Konseyi aracılığıyla olmuş, genel manada Avrupa bu alana müdahalede geç kalmıştır. Ancak Avrupa Konseyi ve Avrupa Birliği eliyle uygulamaya konulan birtakım politikalar, Türkiye’nin AB sürecinde oldukça belirleyici olmuş, Türkiye Avrupa Konseyi tecrübesinden belli bir düzeyde yararlanmıştır. Ancak gelişmelerin birbirine yakın dönemlerde olması, Türkiye’nin güvenlik alanında diğer ilişkilerini daha fazla gündeme getirmiş, ABD mahreçli girişimlere karşı bir duyarlık oluşmuştur. Avrupa Birliği’nin Türkiye’nin siber güvenlik politikalarına etkisi başlangıç düzeyinden daha ziyade ilerleyen dönemlerde olmuş, özellikle bu amaçla kurulmuş olan AB kurumlarının izleme ve değerlendirme faaliyetlerine konu olmak durumunda kalmıştır. Avrupa ülkelerinde ortaya çıkan siber saldırılar Türkiye için uyarıcı olmuştur. Öte yandan, Gezi olayları ve 15 Temmuz darbe girişimi ile başlayan süreçte Türkiye siber alana farklı bir bakış açısıyla ilgilenmeye başlamıştır. Nitekim Cumhurbaşkanlığı Hükümet Sistemine geçiş sürecinde siber güvenlik alanına yönelik bütüncül bir bakış açısı içinde politika üretecek ve bu politikaların izlenmesini takip edecek bir birimin Cumhurbaşkanlığı bünyesinde tesis edilmekte olması Türkiye için bir şanstır. İyi bir şekilde planlanır, AB örneği yanı sıra ABD, Rusya ve Çin gibi ülkeler iyi bir şekilde analiz edilip, gerekli mekanizma kurulabilirse siber güvenlik alanı bir sorunlu alan olmaktan çıkar, düzenlenen ve kontrol edilen bir boyuta taşınabilir. Türkiye bu anlamda önemli bir yol ayrımındadır.

**Anahtar kelimeler**: Siber güvenlik, Avrupa Birliği, Uyum süreci, Ulusal güvenlik, AB–Türkiye ilişkileri.

**AN ANALYSIS OF TURKEY’S CYBER SECURITY POLICIES IN THE INTEGRATION PROCESS TO THE EUROPEAN UNION**

**ABSTRACT**

Cyber security, as a relatively new phenomenon, has been the subject matter of not only national governments but also international organisations. Breath-taking developments in ICT have been facilitating the lives of individuals and governments as well as posing incredible amount of threats to them. At Europe, cyber security was initiated by the Council of Europe (CE), though late. However, the policies formulated by the CE and the EU have been of good help for Turkey during the accession process. Therefore, it is fair to claim that Turkey has learnt from Europe at a certain level, especially in the policy formulation and establishing necessary organisational structure phases. Nonetheless, the close time period of formulation and implementation at European level and Turkey shows that Turkey has paid much attention to the US originated initiatives, rather than Europe. In addition, the European involvement in cyber security has been evident more not in the establishment term but in the following period, especially the observation and regulation procedures as a part of the accession agenda. Besides, the cyber-attacks in Estonia and Germany were the main motivating factors to drive policy makers in Turkey to take cautionary measures. The period starting with the Gezi events and eventually failed the 15 July coup attempt were inspiring and invoking the policy makers to establish an effective cyber security policy. Consequently, it is the right move in the right direction to initiate an Office formulating policies and implementing them for the sake of national security priorities as a part of the Presidential Government System uniquely designed for Turkey. If planned properly, learnt from the US, Russian and Chinese experiences, Turkey can sort out cyber security problems soon. Turkey is at crossroads in the cyber security issue.

**Keywords**: Cyber security, European Union, Integration process, National security, EU-Turkey relations.

**Giriş**

İlk Katılım Ortaklığı Belgesi’nin 8 Mart 2001 tarihinde Avrupa Birliği Konseyi tarafından onaylanması Türkiye-AB ilişkilerinde yeni bir dönüm noktası anlamına gelmektedir. Kırk yılı aşan AB macerası, bu tarihten itibaren Türkiye için yeni bir boyuta taşınmış, ülke reform çalışmaları kapsamında imzalanan Katılım Ortaklığı Belgelerine ve Kopenhag Kriterleri’ne daha uygun adımlar atmaya yönelik bir politika benimsemiştir. Bu çerçevede Avrupa Birliği kriterleri başat mesele haline gelmiş, belirlenen politikalarda AB kriter ve standartlarına uygun ekonomik, toplumsal, yönetsel, siyasal vb. alanlarda çeşitli reform ve yapılanma çalışmaları içerisine girilmiştir.

Bu politika alanları ve konuları arasından güvenlik politikaları önemli bir rol üstlenmiş, kendi bünyesinde oluşturmaya çalıştığı politikalar ile birlik içerisinde bütünlük oluşturma açısından üye ve adaylık sürecindeki ülkelere birtakım reformları yerine getirme yükümlülüğü getirmiştir. Bu süreçte, özellikle güvenlik politikalarının etkin olabilmesi adına birliğin bütünlüğünü ortaya koyan bir yaklaşım tercih edilmiştir.

Gelişen bilgi iletişim teknolojileri ile ülkelerin ekonomik, sosyal, yönetsel alanlar başta olmak üzere diğer tüm alanlardaki her türlü faaliyetlerin etkin ve hızlı hizmet sunma yaklaşımı içerisinde elektronik ortama aktarması ile siber güvenlik kavramının önemi daha da artmıştır. Siber güvenlik politikalarının artan önemine bağlı olarak Avrupa Birliği, üye ülke sistemlerinin birlikte çalışabilirliğini artırmak, birlik bünyesinde tutarlı politika belgeleri üretebilmek ve alanı koordine edebilmek için eu-LISA adlı sistemin dijital bir merkeze dönüştürülmesi ve yasal zorunluluklar getiren düzenlemelerin yaşama geçirilmesini hedeflemiştir.

Avrupa Birliği yaşadığı birtakım tecrübeleri takiben “Avrupa Birliği için Siber Güvenlik Stratejisi” belgesi çerçevesinde siber güvenlik hedeflerinin neleri kapsadığı, siber güvenliğin sağlanması adına hangi tür adımların atılması gerektiği, siber sorumluluğun kurumlar arasında nasıl paylaşılacağı ve siber yönetişim oluşturulmasında yol gösterici adımların atılmasına yönelik örnek teşkil edecek bir yapılanma içine girmiştir. Birliğe aday ülke konumunda bulunan, ilişkiler her ne kadar ‘iki ileri bir geri’ seyir gösterse de Türkiye’nin üyelikten sarf-ı nazar ettiğine dair resmi bir açıklama ve süreç başlatılmadığı için AB boyutu ülke açısından hala çok önemli bir tercih anlamına gelmektedir. Kaldı ki Türkiye AB ilişkilerini dondurmuş ya da bitirmiş olsa bile siber güvenlik açısından durumunu değerlendirme kriteri sunması hasebiyle bile olsa AB siber güvenlik politikaları bakımından değerlendirilmeyi hak eden bir boyutu ifade eder. Sonuç olarak; siber güvenlik politikaları noktasında Türkiye’nin mevcut durumunun tespit edilmesi ve gelecekte yaşanabilecek güvenlik sorunlarına tedbir alınması bakımından Avrupa Birliği’nde uygulanan mevcut siber güvenlik uygulama ve politika örneklerini analiz etmek oldukça faydalı olacaktır.

Çalışmada; Avrupa Birliği’nin siber güvenlik politikalarının temel bileşenleri, bu bileşenlerin gelişen teknoloji ve devletlerin-toplumların farklılaşan alışkanlık ve ihtiyaçları noktasında analizi yapılmak suretiyle bir taraftan siber güvenlik bağlamında AB’nin konumu ele alınacak, diğer taraftansa, etkin bir siber güvenlik politikası oluşturulması açısından Türkiye’nin mevcut durum analizinin yapılması, reform transferi kapsamında eksik noktalarının tespit edilmesi, etkin siber güvenlik politikalarının Türkiye’de uygulanabilmesi ve nihayetinde siber yönetişimin sağlanabilmesi için gerekli adımların neler olduğuna yönelik değerlendirme yapılacak, öneriler sunulacaktır.

1. **Teknoloji, Siber Güvenlik, Yönetişim ve Devletler**

Küresel düzeyde teknolojik gelişmelerin bireyleri, ülkeleri, yerel, bölgesel, ulusal ve uluslararası kuruluşları bilgi iletişim teknolojileri aracılığıyla hızlı bir şekilde etkilemekte olması ve 21. yüzyıl toplumlarına ‘bilgi toplumu’ nitelendirmesinin yapılması günümüz insanının teknolojiye ne kadar bağlı ve bağımlı hale geldiğini göstermesi noktasında ufuk açıcı bir durumdur. Bu değişim ve gelişim sürecinde üzerinde durulması gereken temel anahtar olguların başında bilgi, küreselleşme, temel haklar, demokrasi ve teknolojinin geldiği ifade edilebilir (Sevinç, 2006: 356). Bu kavramlardan bir kısmı salt teknoloji alanında teknik bir yönü ifade ediyor görünse de yine bir kısmı yönetim sistemini, insanı ve insana dair hukuksal boyutları yansıtmaktadır. Dolayısıyla, saf teknik ve teknolojik görünen mekanizmaların bile aslında insanı ve değerlerini ilgilendirdiğini hiçbir zaman unutmamak gerekmektedir.

Siber güvenlik alanı öyle bir alan haline gelmiştir, o kadar baş döndürücü bir ivme ile değişmektedir ki, son zamanlarda Endüstri 4.0 ya da 4. Sanayi Devrimi olarak nitelendirilen baş döndürücü gelişmelerden mülhem “Siber Güvenlik 4.0” teriminin kullanımı dahi gündeme gelmiştir. Bu benzetmenin bir bağı bulunduğu da aşikardır: Endüstri 4.0 pek çok modern otomasyon sistemini, veri alışverişini ve üretim teknolojisini içeren bir terimdir. Terim, siber-fiziksel sistemlerden oluşan bir değerler bütününü ifade etmektedir. Esasında Endüstri 3.0 sürecinde elektronik bilgi teknolojilerinin devreye girmesi ile başlayan kamusal hizmet üretim alanları ile bu alanların kritik altyapılarının oluşturulma ve korunma süreçlerinde devletler ve hükümetler geniş çaplı tedbirler almak zorunda kalmışlardır.

Kamusal aktörler siber güvenlik alanında karşılaştıkları yeni ve her geçen gün güncellenen risk tehditlerine karşın yeni ve alternatif strateji ve politikalar geliştirmeye çalışmaktadırlar. Bu bağlamda unutulmaması gereken şey siber uzay alanının güvenlik, terör, diplomasi, siyaset, ekonomi ve yönetim türünden konu başlıkları itibariyle etkin ve etkili faaliyetlerin yaşama geçirilmesinde yerel ortaklara ve paydaşlara ihtiyaç duyduğu kadar uluslararası işbirliğine de ihtiyaç duymakta olduğu hususudur. Bu açıdan siber yönetişim farklı sektörler ve farklı aktörler için farklı anlamlar ifade etmektedir (Akyeşilmen, 2018: 189). Bu noktada siber uzay alanının küresel bir olgu olması, siber yönetişimi küresel yönetişimin bir bileşeni olarak tanımlama konusunu gündeme getirmektedir.

**Şekil-1**: Siber Güvenlik Yönetişim Modeli

**Kaynak**: DTP, 2017: 8.

Şekil 1’de tanımlanan yönetişim modeli görevli kamu otoritesinin yanında mevcut bulunması gereken diğer bileşenleri de ihtiva etmektedir. Sürecin koordinasyonu, operasyonel süreçlerin yürütülme biçimi, ihtiyaç duyulan yapılanma sistemi ortaya konulmaktadır. Yukarıda ifade edildiği gibi, siber güvenlik alelade bir güvenlik meselesi olarak algılanırsa, eksik ve yanlış bir tanımlama olmuş olur. Konunun çok aktörlü, çok boyutlu, çok dereceli yapısı sağlıklı bir yapılanma dâhilinde başarılı bir mekanizmayı tanımlama imkânını ifade eder.

Kuşkusuz ülkeler kendi bilgi sistemlerini ve kritik altyapılarını teknolojik donanımlarıyla oluşturabilmektedirler. Bununla birlikte bu sistemlerin ve kritik altyapıların korunmasına yönelik sorunlar politika belirleyicileri, hükümetleri ya da devletleri çoğu kez karmaşık ve öngörülemeyen süreçlerle karşı karşıya bırakmakta, gerek politika belirleme gerekse uygulama safhasında hazırlıksız yakalanmalarına neden olmaktadır. Sorun tüm ülkelerin sorunudur. Teknolojik olarak iyi durumda olan ülkeler de geri durumda olanlar da benzer sorunlara muhatap olmaktadırlar. Bu nedenle, bir ülkenin özellikle kamusal hizmetlerini yürüten tüm elektronik ve teknolojik mekanizmaları üzerinde oluşabilecek siber saldırı tehditlerine karşı standartlar, politikalar ve stratejiler geliştirilmeye başlanmak zorunda kalınmıştır (Yılmaz vd., 2015: 133).

Siber güvenlik, genel manada ulusal güvenliğin bir parçası olarak değerlendirilmektedir. Örneğin Barrineau’ya göre (2004: 5), Amerikan ulusal güvenliği içerisinde siber güvenlik alanında kat edilmesi gerekenler yerine getirilmezse ‘elektronik Pearl Harbor’ ya da ‘siber 11 Eylül’ kaçınılmaz olacaktır. Siber güvenlik konusunun oluşturduğu güvenlik açığı son derece hayati ve son derece yıkıcı etkileri beraberinde getirmektedir. Bu amaca matuf olarak; Amerika Birleşik Devletleri’nde siber uzay alanında ülke genelinde bir sinerji oluşturma adına Aralık 2003’te toplanan Ulusal Siber Güvenlik Zirvesi’nin önemine dikkat çekilmektedir. Bu zirve sonrasında oluşturulan Ulusal Siber Güvenlik Stratejisi, ABD’de elektronik ortamdaki bilgi varlıklarının etkin bir şekilde korunması için atılması gerekli adımların ana hatlarını çizmektedir. Tüm bunların yanında Ulusal Siber Güvenlik Stratejisi’nde siber güvenlik alanının, kritik altyapıların çalışmasını sağlayan bilgisayarlardan servis sağlayıcılarına, fiber kablolardan elektronik mekanizmalara kadar pek çok unsuru bünyesinde barındıran ülkenin kontrol sistemini de anlatmaktadır (Yayla, 2013: 183).

Strateji belgesi ile çizilen genel sınırlarla yetinmek mümkün olamamaktadır. Zira siber güvenlik oldukça karmaşık ve oldukça hassas içerikli bir alan olması hasebiyle öncelikli stratejilerin başında ulusal siber güvenlik bilincinin artırılması ve eğitim programlarının gerçekleştirilmesi konularına özellikle önem vermek gerekmektedir. Mesuliyeti altında bulunan son derece hassas içerik ve kamu politikası ana aktörü olması nedeniyle özellikle devletin ve kurumlarının öğrenmesi gereken en önemli hususun bilgi güvenliği yönetişimine yönelik farkındalık olduğu belirtilmektedir (Conner ve Coviello, 2004: 11).

Özellikle siber suçlarla mücadelede uluslararası bir işbirliğine olan ihtiyaç, uluslararası ve ulus üstü birliklerinin de öncelikli gündem maddeleri arasında yerini almaya başlamıştır. Nitekim bunlardan birisi olan ve 1949 yılında kurulan Avrupa Konseyi tarafından hazırlanan Siber Suçlar Sözleşmesi, siber suçlarla mücadelede uluslararası işbirliğini öncelemiştir (Weber, 2003: 426-428). Avrupa düzeyinde işbirliği ve ortak çalışma platformu tesis edilmesi anlamında önemli bir adım olan bu Sözleşme ile sadece siber suçlar meselesini düzenlemekle kalmamakta, yani suç odaklı bir bakış açısı ortaya koymamakta, aynı zamanda siber güvenlik adına atılması gereken hayati adımları da sıralamaktadır. Devlet dışı bir mekanizma tarafından kabul edilen bu sözleşme ulusal hükümetler tarafından da benimsenmiş, başta üye ülkeler olmak üzere siber güvenliğin ulusal aktörlerine önemli bir çerçeve oluşturmuştur.

Türkiye Avrupa Siber Suç Sözleşmesi’ni 2010 yılında imzalamış ve 2014 yılında yürürlüğe koymuştur. Böylece Türkiye siber güvenlik politikaları alanında önemli bir adım atmış ve siber güvenliğe yönelik sınırlı ancak basit siber suçlarla ilgili uluslararası bir işbirliğini kabul ederek bu alandaki mücadelesini yürütmeye çalışmıştır. Türkiye’nin siber güvenlik alanına geç de olsa girmiş olması, sorunu önemsediği ve gereken adımları atmak üzere bir irade ortaya koyduğu ya da koyacağı anlamında yorumlanabilir. Ne var ki, Türkiye siber suçlara en fazla maruz kalan ülkeler sıralamasında başlarda yer almaya devam etmektedir. Bu bilgi siber güvenlik alanında atması gereken çok ciddi adımlar bulunduğu yönünde değerlendirilebilir.

Siber güvenlik alanı yalnızca teknoloji mühendislerinin ya da siber terör, siber savaş, siber diplomasi gibi temel konu başlıkları bağlamında uluslararası ilişkiler uzmanlarının ilgilendiği bir çalışma sahası olmaktan çıkmak durumundadır. Bu noktada siber güvenlik siyasetinin ve siber güvenlik politikalarının artık artan bir şekilde siyaset bilimi ve kamu yönetimi alt disiplinleriyle de çalışılmasını gerekli kılmaktadır. Devletin dijitalleşmesi ve temel tüm kamusal hizmet alanlarının aynı zamanda kritik altyapılardan oluşması, siber güvenlik konusunun kapsamını genişletmektedir. Kamu politikası genel başlığı zaten kamu politikası başlıkları itibariyle bu sorunu kamu yönetiminin gündemine getirmektedir. Sunulacak hizmetlerin, yürütülecek politikaların ve alınacak tüm kararların siber güvenlik bağlamında değerlendirmeye tabi tutulması bir zorunluluktan öte hayati bir mesele haline gelmiştir.

1. **Avrupa’da Siber Güvenlik Politikaları**

Avrupa düzleminde siber güvenlik politikalarının yasal alanda tartışılması 1990’lı yıllardan itibaren olmuştur. İlk olarak Avrupa Suç Sorunları Komitesi (CDPC) tarafından 1996 yılında siber suçlarla ilgilenecek bir Uzmanlar Komitesi kurulması kararı alınmıştır. Kararın temel gerekçesini ise bilgi teknolojileri alanındaki hızlı gelişmelere koşut olarak siber uzay adı verilen yeni bir alanın ortaya çıkması/çıkmakta olması gösterilmiştir. Bu alan aynı zamanda bilgisayar sistemlerinin ve telekomünikasyon ağlarının bütünlüğüne ve gizliliğine karşı muhtemel risk ve suç konularını içermektedir. Nihayet kararın uygulanması adına 4 Şubat 1997 tarihinde toplanan Avrupa Konseyi Bakanlar Komitesi’nin 583 sayılı Kararı ile ‘Siber Uzay Suçları Uzmanlar Komitesi (PC-CY)’ adı verilen yeni bir komite oluşturulmuştur. Komite çalışmaları ile hazırlanmaya başlayan sözleşme metninin imzaya açılması ise 23 Kasım 2001 tarihini bulmuştur. Budapeşte’de imzaya açılan sözleşmeyi Avrupa ülkeleri dışından ABD, Güney Afrika, Japonya ve Kanada gibi ülkeler de imzalamıştır (İçel, 2001: 4-6).

1 Temmuz 2004 tarihinde yürürlüğe giren Avrupa Siber Suç Sözleşmesi, bu alandaki ilk uluslararası antlaşma olarak kabul edilmektedir (Önok, 2013: 1241). Kuşkusuz Avrupa Siber Suç Sözleşmesi, Avrupa’da siber alanda etkili bir yasal mevzuat bulunmaması sonucunda ortaya çıkmıştır (Schell ve Martin, 2004: 104). Sözleşme ile siber suç konularında taraf devletlerin mevzuatlarını uyumlulaştırmayı ve etkin bir adli işbirliği mekanizmasını koordine etme amaçlanmıştır (Özbek, 2015: 73).

İşin doğrusu, Avrupa’da siber güvenliğin bir kamu politikası konusu olarak ciddi bir şekilde ele alınmaya ve tartışılmaya başlanması 2007 yılında Estonya’da devlet kurumlarına yönelik gerçekleştirilen siber saldırılar sonrasında vuku bulmuştur. Saldırıların boyutları, meselenin hassasiyeti ve AB üyesi bir ülkenin maruz kaldığı ulusal ve uluslararası durum Avrupa ülkeleri özelinde hükümetleri yeni tedbirler alma arayışlarına yöneltmiş, hatta Avrupa Birliği güvenlik politikalarının revize edilmesi sürecine bile girilmiştir (Yılmaz ve Sağıroğlu, 2013: 159). Ulusal hükümetler Estonya örneğinden ders çıkarma yoluyla kendi iç politikalarını gözden geçirme sürecini başlatmışlardır.

Elektronik devlet uygulamalarının kullanım sıklığı ve içeriği ile internet ağlarının ve altyapılarının yaygın ve yeterli oluşu doğrudan bağlantılı konular olması nedeniyle internet, Avrupa Birliği tarafından Kritik Bilgi Altyapısı (CII) olarak tanımlanmıştır. Ayrıca Avrupa Birliği Komisyonu’nun Kritik Bilgi Altyapısı Koruma (CIIP) Eylem Planı çerçevesinde 2010 yılında Siber Avrupa 2010 (Cyber Europe 2010) programı uygulanmıştır. Bu tatbikatlarda geniş çaplı siber saldırı tehditlerine karşı ön farkındalık hazırlıklarını sağlamak öncelikli hedef olmuştur. Nitekim 2010 yılında bu tatbikat çalışmalarında Avrupa düzeyinde ilk siber saldırı simülasyonu gerçekleştirilmiştir (Karaarslan, 2013: 1-2). Kuşkusuz Avrupa Birliği ülkelerinde siber güvenlik tehditlerine karşı yapılan bu çalışmalar, Avrupa’nın Dijital Ajansı’nda öngörülen hedefler bağlamında Avrupa Ağ ve Bilgi Güvenliği Kurumu’nun (ENISA) koordinasyonu ve Avrupa Komisyonu Ortak Araştırma Merkezi’nin (ECJRC) katkılarıyla düzenlenmiştir.

Avrupa Birliği açısından Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA), siber güvenlik politikalarının kurumsallaşmasının başarılı bir örneğidir. Ajans 5 Haziran 2003 tarihinde bir tüzel kişilik olarak oluşturulmuştur. 14 Mart 2014 tarihinden itibaren fiilen faaliyetlerine başlayan ENISA’nın temel misyonu AB’nin siber güvenliğinin korunmasında Avrupa genelinde üst düzey ağ ve bilgi güvenliği sağlamaktır. Bununla birlikte ENISA, üye devletlerin özellikle kritik altyapılara yönelik siber direnç kapasitelerini geliştirmek amacıyla 2013 yılında AB için Endüstriyel Kontrol Sistemleri – Bilgisayar Güvenliği Olaylarına Müdahale Ekibi’ni de oluşturmuş, siber güvenliğe yönelik eylemli bir koruma mekanizmasının kurulması için doğrudan müdahil olma görevini de üstlenmiştir (Eren, 2017: 73-74).

AB siber güvenlik politikalarının önem kazanmasında ilk kilometre taşı yukarıda zikredilen, 2007 yılında Estonya’nın uğradığı siber saldırılar etkili olurken ikinci ve potansiyel anlamda çok daha fazla etki kapasitesi içeren, Birliğin en büyük ülkesi Almanya’nın 2015 yılında uğradığı siber saldırılar etken olmuştur. 2007 yılında, yaklaşık 3 hafta boyunca süren saldırılar Estonya devlet kurumlarının işlemez hale gelmesine, kamu hizmetlerinin durmasına kadar varan etki meydana getirmiş, ülke yakın tarihin en büyük siber saldırılarından birine maruz kalmıştır (Erendor, 2016: 126; Güntay, 2016: 110).

Estonya tecrübesi, başta AB ve NATO düzeyinde olmak üzere siyasetçilerin, diplomatların ve politika yapıcıların siber güvenlik alanına daha fazla ilgi göstermesini sağlamaya yetmiştir. Hiçbir ülke hükümeti böyle hem yüz kızartıcı hem de kamu hizmetini ve dolayısıyla güvenliğini ihlal eden bir muameleye muhatap olmak istemez. Diğer yandan 7 Ocak 2015 tarihinde, Alman Federal Parlamentosu Bundestag ve Şansölye Angela Merkel’in web sayfalarına yönelik gerçekleştirilen siber saldırılar, bu sayfalara erişimi engellemiştir. Ardından zararlı yazılımlar aracılığıyla Alman parlamentosunun siber ağında yer alan yaklaşık 20 bin siyasetçi ve personelin bilgisayar sistemlerine erişim ve bu bilgisayarlardan veri akışı sağlanmıştır (Eren, 2017: 62). Hangi içeriğin ne şekilde zarar gördüğü kamuoyuna açıklanmayan bu saldırıların Almanya ulusal güvenliği açısından oluşturduğu risk sadece anılan ülkede değil, tüm AB ülkelerinde ciddi bir endişeye neden olmuştur.

Nitekim, Avrupa Birliği’nin siber güvenlik politikasını oluşturan temel belge, 7 Şubat 2013 tarihinde “Avrupa Birliği için Siber Güvenlik Stratejisi’’ (*Cyber security Strategy for the European Union*) başlığı ile Avrupa Birliği Komisyonu tarafından yayınlanmıştır. Strateji belgesinde siber güvenliğe yönelik temel ilkeler sıralanmıştır. Bunlar arasında Avrupa Birliği ortak temel değerleri, hak ve özgürlükler, kişisel verilerin korunması, demokratik ve etkili çok paydaşlı yönetişim ile paylaşılmış sorumluluk ilkeleri yer almıştır (EC, 2013: 3-4). Ayrıca Siber Güvenlik Stratejisi’nde ENISA’nın rolüne ve önemine dikkat çekilmiştir.

1. **Türkiye’de Siber Güvenlik Politikaları**

Türkiye’de siber güvenlik politikalarının gelişim serüveni genel olarak e-devlet uygulamalarının gelişimi ile doğru orantılı olmuştur. 2003 yılında kamuoyu ile paylaşılan E-Dönüşüm Türkiye Projesi ve devamında gelişen süreç siber güvenlik konularının kamu politikalarının bir parçası olarak değerlendirilmesine imkân sağlamıştır. Bununla birlikte, siber güvenlik alanın Amerika Birleşik Devletleri (ABD), Rusya Federasyonu ve Avrupa ülkeleri başta olmak üzere başka ülkeler tarafından daha önce keşfedilmesi ve temel politikaları belirleme noktasında daha ileri adımlar atmak suretiyle koruma kalkanı geliştirmeleri uluslararası sistemde Türkiye aleyhine bir durumun ortaya çıkmasına neden olmuştur. Küresel sistemi bir network olarak değerlendirdiğimiz zaman siber saldırıların networkun nispeten daha zayıf halkalarına karşı yöneltileceğini tahmin etmek zor olmasa gerektir.

Türkiye’de devletin tüm kurumları düzeyinde siber güvenlik konusu ilk kez 2010 yılı Ekim ayında toplanan Milli Güvenlik Kurulu’nda tartışılmıştır. 27 Ekim 2010 tarihli Milli Güvenlik Kurulu (MGK)’nun Bildirisi’nde şu ifadelere yer verilmiştir:

*“Siber tehdidin global düzeyde ulaştığı boyut ve bu tehdidin ulusal güvenliğe etkilerinin kapsamlı şekilde ele alındığı bildirilerek, bu bağlamda siber tehdidin engellenebilmesi açısından milli düzeyde yürütülen çalışmaların değerlendirildiği ifade edildi.”*

Meselenin güvenlik boyutuyla en üst düzeyde ilgilenen bir organı olan MGK’da tartışılması ve gerekli adımların atılmasına imkân sağlayacak olan sürecin başlatılmış olması önemli bir gelişme olarak değerlendirilebilir. Sonuçta Türkiye, temel hedefi siber suçlarla küresel düzeyde etkin bir şekilde mücadele edebilmek ve bu suç türleri ile mücadelede ortak bir işbirliği anlayışını benimsemek olan Avrupa Konseyi’nin 23 Kasım 2001 tarihinde imzaya açtığı 185 sayılı Siber Suç Sözleşmesi’ni 10 Kasım 2010 tarihinde Strasburg’da imzalamıştır. Türkiye Büyük Millet Meclisi (TBMM) Dışişleri Komisyonu söz konusu sözleşme ile ilgili raporunu 20 Aralık 2012 tarihinde Meclis Başkanlığı’na sunmuştur. Siber Suç Sözleşmesi, 22 Nisan 2014 tarih ve 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesi’nin Onaylanmasının Uygun Bulunduğuna Dair Kanun ile de onaylanmıştır. İlgili Kanun, 2 Mayıs 2014 tarihinde Resmi Gazete’de yayımlanmasıyla yürürlüğe girmiştir.

Türkiye’de “siber kriz yönetimi ve kritik altyapı koruması” görevi, 5902 sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanun ile AFAD’a verilmiştir. AFAD açısından afetler, doğal ve teknolojik afetler olmak üzere başlıca iki gruba ayrılmıştır. Kritik altyapıların korunması ve siber güvenlik konuları teknolojik afetler kategorisinde yerini almıştır. Bu çerçevede AFAD, Kritik Altyapı Koruma Planı içerisinde aralarında çeşitli bakanlıkların ve Hacettepe Üniversitesi’nin de bulunduğu 12 kurum ve kuruluşu kritik altyapı organizasyonları arasında belirlemiştir. AFAD, koruma sürecinin temel aşamaları için Eylül 2014’te “2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi”ni yayınlamıştır. Belge’de, kritik altyapı sektörleri ile ilgili Avrupa Birliği Direktifleri’nin dikkate alınması ve AB düzeyinde tüm ilgili paydaşlar arasında iletişim ve işbirliğinin güçlendirilmesi gerektiği ifade edilmiştir (Bıçakcı, Ergun ve Çelikpala, 2016: 43).

**Tablo 1: Türkiye’de Siber Güvenlik Politikalarının Gelişimi**

|  |  |
| --- | --- |
| **Yıl** | **Politika Kararları** |
| 2003 | Ulusal Sanal Ortam Güvenlik Politikası Belgesi |
| 2010 | Avrupa Siber Suç Sözleşmesi’nin İmzalanması |
| 2010 | Milli Güvenlik Siyaset Belgesinde Yer Alması |
| 2011 | I.Ulusal Siber Güvenlik Tatbikatının Düzenlenmesi |
| 2012 | 28447 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar |
| 2012 | 3842 sayılı Bakanlar Kurulu Kararı ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı’nın Yetkilendirilmesi |
| 2013 | II.Ulusal Siber Güvenlik Tatbikatının Düzenlenmesi |
| 2013 | Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı |
| 2013 | Siber Güvenlik Özel Komitesi’nin Kurulması |
| 2016 | 2016-2019 Ulusal Siber Güvenlik Stratejisi |
| 2016 | 2016-2019 Ulusal Siber Güvenlik Eylem Planı |
| 2018 | Devlet Denetleme Kurulu (DDK) Siber Güvenlik Raporu |

**Kaynak**: Kutlu, Sevinç ve Kahraman, 2018: 146; Kutlu, Kahraman ve Dinçer, 2019: 193-194.

Türkiye’de siber güvenlik politikalarını son dönemde yakından ilgilendiren iki hususa dikkat çekmek gerekir. İlki, 2016-2019 yıllarını kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı; ikincisi ise Kasım 2018’de DDK tarafından Cumhurbaşkanı’na sunulan Siber Güvenlik Raporu’dur.

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı’nın, kamu bilişim sistemlerin ve kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemleri ile küçük ve orta ölçekli sanayi, tüm özel ve tüzel kişiler de dâhil olmak üzere ulusal siber uzayın Türkiye ölçeğindeki tüm bileşenlerini kapsadığı belirtilmiştir (UDHB, 2016: 9). 2016-2019 yılları arasında Türkiye’nin siber güvenlik alanındaki yol haritasını belirleyen en geniş vadeli ve kapsamlı Strateji ve Eylem Planı, 5 ana eylem ve 41 alt eylemden oluşmaktadır. Ulusal Siber Güvenlik Eylem Planı’nın temel hedefleri arasında siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olduğu düşüncesinin tüm kesimlerde yerleştirilmesi, ulusal siber uzayda yer alan sistem ve aktörlerin tamamının güvenliğini sağlamak üzere yönetsel ve teknolojik tedbirlerin alınması yer almaktadır (Aslay, 2017: 26).

Diğer yandan 15 Temmuz 2016 tarihli meşum darbe girişiminin ardından hazırlanmaya başlayan ve Kasım 2018’de Cumhurbaşkanı’na sunulan DDK’nın Siber Güvenlik Raporu’nda kamu, özel sektör ve üniversiteler arasındaki işbirliğinin artırılması yoluyla siber güvenlik ekosistemlerinin oluşturulması ve hizmet entegrasyonun sağlanması hedeflenmektedir. Ayrıca siber güvenlik alanında “Ulusal Siber Güvenlik Teknoloji Yol Haritası”nın oluşturulması ve “Önceliklendirilmiş Sektör Alanları”nın belirlenmesi istenmektedir. Tüm bunlarla ilgili çalışmaların ise Cumhurbaşkanlığı Dijital Dönüşüm Ofisi koordinasyonunda yürütülmesi öngörülmüştür. Dijital Dönüşüm Ofisi ise, yeni cumhurbaşkanlığı hükümet sistemine geçişin ardından Cumhurbaşkanlığı’na bağlı, özel bütçeli, kamu tüzel kişiliğine haiz, idari ve mali özerkliğe sahip dört ofisten birisi olarak kurulmuştur. Bu açıdan siber güvenlik politikaları açısından gelecek yıllarda önemli politika üretim merkezlerinden birisi haline gelmesi beklenmektedir.

Türkiye’de siber güvenlik konusunun gelişiminde yer alan adımların sıralandığı Tablo 1’den de açıkça görüleceği gibi, siber güvenlik konusu oldukça yeni bir alandır. Çabaların daha çok 2010 yılı Ekim ayında yapılan MGK toplantısı sonrasına rast geldiği görülmektedir. Atılmış olan adımlarda ise Avrupa çerçevesinin, en azından süreci tetikleme ve çerçeve tesisine imkan sağlama boyutlarıyla da olsa, belirleyici olduğunu söylemek mümkün. Ayrıca 15 Temmuz süreci siber güvenlik açığı başta olmak üzere Türkiye’ye çok şey öğretmişe benzemektedir. Nitekim yukarıda bahsedilen Cumhurbaşkanlığı iradesi siber sorunlara yönelme bakımından önemli bir adım olarak değerlendirilebilir.

Meselenin Avrupa Birliği boyutuna tekrar dönersek, Birlik siber güvenlik politikalarında siber tehditlerin önlenmesinde karşılaşılacak sorunların tespiti oldukça önemsemiştir. Bununla birlikte AB’nin siber güvenliği sağlamaya yönelik geliştirdiği politikaların sonuçları ve AB’nin müşterek bir siber güvenlik politikası oluşturma çabaları, siber güvenlik alanında politika üretmeye çalışan Türkiye gibi AB’ye üyelik müzakeresi yürüten ülkeler açısından da oldukça önem arz etmektedir.

1. **AB ile Türkiye Siber Güvenlik Politikalarının Etkileşim Alanları**

Türkiye’de Haziran 2012’de düzenlenen Siber Güvenlik Strateji Çalıştayı’nın ardından Bilgi Güvenliği Derneği tarafından hazırlanan tavsiye belgesinde Ulusal Siber Güvenlik Strateji Belgesi’nin yayınlanması, Ulusal Siber Güvenlik Kurulu’nun oluşturulması ve Avrupa Birliği, Avrupa Konseyi ve ENISA benzeri uluslararası yapılarla işbirliğinin güçlendirilmesi gerektiği belirtilmiştir (Bıçakcı, Ergun ve Çelikpala, 2016: 36). Kuşkusuz Türkiye süreç içerisinde bu tür hedefleri yerine getirmeye başlamıştır. İlk olarak 2012 yılında Siber Güvenlik Kurulu oluşturulmuş ve 2013 yılında Ulusal Siber Güvenlik Strateji Belgesi yayınlanmıştır.

Diğer yandan Türkiye’nin Helsinki süreci ile yasal zemine taşınan Avrupa Birliği ile yeni dönem ilişkileri ve AB’nin güvenlik alanına ilişkin çeşitli endişeleri dikkate alındığında AB ile ortak ya da bireysel olarak yürütülecek siber güvenlik politikaları kaçınılmaz olarak karşımıza çıkacaktır. Avrupa’da ve Türkiye’de güvenlik konularına yönelik ilgi ve politika üretme motivasyonu devam ettikçe siber güvenlik politikaları alanında karşılıklı etkileşim ve işbirliği doğal olarak gelişmek durumundadır.

Siber güvenlik bağlamında, Avrupa’daki gelişmelerle Türkiye arasındaki etkileşim noktalarını esasen dört ana başlık altında toplamak mümkündür. İlki, Avrupa Konseyi Siber Suç Sözleşmesi; ikincisi Avrupa Komisyonu Siber Güvenlik Stratejisi; üçüncüsü, ENISA çalışmaları; dördüncüsü ise eu-LISA’nın operasyonel faaliyetleridir.

Siber güvenlik konularının değişen, gelişen ve bu arada karmaşıklaşan yapısı itibariyle uluslararası arenada mevcut bulunan birtakım işbirliği süreçlerine taraf olarak katılmak önem arz eden bir mevzudur. Türkiye açısından bu alandaki en önemli uluslararası dokümanların başında Avrupa Konseyi Siber Suç Sözleşmesi gelmektedir. Sözleşmede siber güvenlik alanını doğrudan ilgilendiren siber suçlar konusunda herhangi bir tanımlama yapılmamakla birlikte siber suçların, yetkisiz erişim, sisteme ve veriye müdahale, bilişim sistemleri aracılığıyla yapılan dolandırıcılık gibi suçlarla sınırlı tutulduğu belirtilmektedir (Marion, 2010: 702; Yayla, 2013: 193).

Yine aynı Sözleşme’de Avrupa siber suç politikalarının ana ilkeleri de belirlenmiştir (İçel, 2001: 6). Bu bağlamda ilk ilkenin ifade ve iletişim özgürlüğü gibi temel hak ve özgürlüklerin korunması olduğu ifade edilmiş (Wales, 2000: 7) ve Türkiye’nin Avrupa Birliği’ne uyum süreci de dikkate alındığında bu yasal düzenlemeye taraf olarak imzalamasının gerekliliğine vurgu yapılmıştır. İfade özgürlüğü pek çok düşünür tarafından diğer özgürlüklerin anası olarak kabul edilir. İletişim özgürlüğü ile beraber değerlendirildiğinde ifade özgürlüğü bireyin gelişim ve tercihlerinin çıkış noktası olarak değerlendirilebilir.

Avrupa Siber Suç Sözleşmesi’nin 23. maddesinde yer alan ‘adli işbirliği’ ile 35. maddesinde öngörülen ‘irtibat noktası kurulması’, devletler arası işbirliğine ve siber yönetişime doğrudan imkan veren örnekler olarak değerlendirilebilir. Örneğin 35. maddedeki yükümlülüğe uygun olarak Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı, taraf devletlerle sürekli iletişim halinde olacak şekilde irtibat noktası olarak belirlenmiştir (Erdem ve Özocak, 2017: 4). Siber suçların network üzerinden işleniyor olması, ülkeler arası ilişki ve desteği de zorunlu olarak gündeme getirmektedir. Dünyanın hangi ülkesinden olduğunu bilmediğimiz bir şahıs internet üzerinden pekala ülke ve bireyler için çok kritik bilgilere ulaşabilir, bu bilgileri dilediği gibi kullanmak suretiyle suç işleyebilir.

AB açısından, Avrupa Siber Suç Sözleşmesi’nin siber suçlara yönelik eksik tanımlama durumunu izale etme ve yeni gelişmeler çerçevesinde yeni prensipler geliştirme yönünde çabalar olsa da bu akamete uğramış bir girişim olarak kalmıştır. Avrupa düzeyinde ikinci bir sözleşme hazırlanmasında Avrupa Konseyi Siber Suç Sözleşmesi’nin küresel düzeyde katılıma da olanak tanıması ve Avrupa Birliği üyesi ülkelerin neredeyse tamamının sözleşmeye taraf olması nedeniyle Avrupa Birliği nezdinde de kabul gören bir sözleşme olmuştur. Bu nedenle Avrupa Birliği, Avrupa Konseyi Siber Suç Sözleşmesi’nin yerine yeni bir yasal mevzuat geliştirme yolunu tercih etmemiştir (Buono, 2010: 208).

Tablo 1’de tarihsel olarak sıralanan Türkiye’nin siber güvenlik geçmişi üzerinde Avrupa Birliği’nin etkili olduğunu söylemek oldukça zor görünmektedir. Avrupa Ağ ve Bilgi Güvenliği Ajansı’nın (ENISA) yayınladığı bir çalışmada üye devletlerin ulusal siber güvenlik politikalarını oluşturma yılları Almanya için 2011, Belçika için 2012, Avusturya ve İtalya için 2013, Danimarka ve Fransa için 2015 yılı tespit edilmiştir (ENISA, 2016). Bu bilgi ve değerlendirme ışığında Türkiye ile AB üyesi ülkelerin genel olarak siber güvenlik politikaları geliştirme serüvenleri yakın dönemlere dayandığı açıkça görülmektedir. Eğer bir etkileşim olmuş olsaydı ya AB ülkeleri ya da kurumları siber güvenlik alanına daha önce eğilmeleri gerekirdi ya da Türkiye bu alana daha sonra girmeli idi.

Öte yandan, ABD ve Rusya gibi ülkelerin siber güvenlik serüvenleri incelendiğinde, bu ülkelerin Avrupa’dan da Türkiye’den de çok önceleri bu alana girdikleri ve politikalarını geliştirdikleri söylenebilir. Muhtemelen Avrupa ve Türkiye bu dönem boyunca güvenlik konusunu genel manada NATO ve ABD’ye havale ettiği, kendi bağımsız güvenlik politikalarını geliştiremedikleri için siber güvenlik alanını da ihmal ettiler.

Diğer taraftan Avrupa Birliği için Siber Güvenlik Strateji Belgesi’nde de yer verilen ENISA, Türkiye için çeşitli tespitlerde bulunmakta ve Türkiye’de siber güvenlik politikalarının gelişimini yakından takip etmektedir. ENISA’nın Türkiye ile ilgili ilk takibi ulusal siber güvenlik stratejisini oluşturup oluşturmadığına yönelik olmuştur. Nitekim 1 Temmuz 2013 tarihinde Belçika’nın siber güvenlik stratejisini hala yayınlanmamasına karşın Türkiye’nin ulusal siber güvenlik stratejisini benimsediğine vurgu yapılmış, Türkiye’nin bu noktada kötü durumda olmadığının altı çizilmiştir.

Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA), 15 Kasım 2013 tarihinde Avrupa genelindeki 23 ülkede bulut bilişiminin kamu sektöründe başarıyla dağıtımına ilişkin mevcut durum analizi gerçekleştirmiştir. Raporda ülkeler belirli kriterlere göre sınıflandırılmış ve vatandaşların kişisel veri güvenliklerini daha ucuza ve güvenli koruma amacıyla “bulut bilişim güvenliği” (*govermental cloud computing security*) alanında öneriler getirilmiştir. Bu raporda yer alan önemli bir husus ise Avrupa ülkeleri arasındaki analizde 23 ülke içerisinde Türkiye’nin bulunmasıdır.[[4]](#footnote-4)

ENISA, 29 Eylül 2015 tarihinde ‘Siber güvenlik ortak bir sorumluluktur!’(‘*Cybersecurity is a shared responsibility!’*) sloganı ile 2015 yılının Ekim ayını “Avrupa Siber Güvenlik Ayı” (*European Cyber Security Month*) ilan etmiştir. Bu projenin temel amaçlarından ilki, teknolojilerde ve çevrim içi ağlarda siber güvenlik konusunda kamu-özel ortaklığının kurulmasını sağlamaktır. Nitekim ENISA, Avrupa Komisyonu ve 100’ün üzerinde paydaş (yerel otoriteler, hükümetler, üniversiteler, düşünce kuruluşları, sivil toplum kuruluşları, meslek örgütleri vb.) ile Avrupa genelinde bir ağa sahiptir.

**Tablo-2**: Avrupa Siber Güvenlik Ayı Projesi Çalışma Takvimi ve Konuları (Ekim 2015)

|  |  |
| --- | --- |
| **Çalışma Takvimi** | **Çalışma Konuları** |
| 1.Hafta / 1-4 Ekim | Çalışanlar için Siber Güvenlik Eğitimi  |
| 2.Hafta / 5-11 Ekim | İşyerinde Siber Güvenlik Kültürü Oluşturma |
| 3.Hafta /12-18 Ekim | Herkes için Kod Haftası |
| 4.Hafta / 19-25 Ekim | Herkes için Bulut Bilişim Çözümlerini Anlama |
| 5.Hafta / 26-31 Ekim | Herkes için Dijital Tek Pazar |

**Kaynak**: ENISA, 2015.

ENISA’nın Siber Güvenlik Ayı Projesi kapsamında Türkiye dahil ilk etapta 27 ülke yer almıştır. ENISA’nın, Avrupa’daki siber güvenlik strateji ve projelerine Türkiye’yi de dahil etmeye çalışması oldukça önemli bir değerlendirmedir. Tablo 2’de sıralanan etkinlikler bu ay boyunca siber güvenlik alanında eğitim seminerleri, strateji zirveleri vb. faaliyetler yoluyla yürütülmüştür. Bu bağlamda siber güvenlik alanında riskler ve tehditler hakkındaki farkındalık ve siber güvenliğin ortak bir sorumluluğa ihtiyaç duyduğu vurgulanmaya çalışılmıştır. Böylece politika yapıcılardan vatandaşlara ve sanayi kuruluşlarına kadar çeşitli paydaşların rolüne ve işbirliğine dikkat çekilmiştir.

**Şekil-2**: Avrupa Siber Güvenlik Ayı Projelerinde Yer Alan Ülkeler



**Kaynak**: ENISA, 2015.

2015 yılının Ekim ayındaki Avrupa Siber Güvenlik Ayı Kampanyaları çerçevesinde 32 ülkede kamu ve özel paydaşlardan oluşan 242 faaliyet kodlanmıştır. 14 Aralık 2015 tarihinde yayınlanan kampanyanın iki temel sonucu özetle şu şekilde sıralanabilir:

* AB üyesi devletler ile AB partneri ülkeler siber güvenlik eğitiminde işbirliği ile ilgilenmektedirler.
* Kampanya Avrupa’da kamu ve özel paydaşlar arasında iyi bir uluslararası işbirliği ortamı oluşturmuştur.

Öte yandan AB’nin siber güvenlik stratejilerinin etkili bir politikaya dönüşebilmesinin hem AB içinde işbirliği ve uyuma hem de uluslararası işbirliği ve koordinasyona ihtiyaç duyduğu belirtilmektedir (Eren, 2017: 6). Bu bağlamda Avrupa siber güvenlik politikaları açısından bir önemli husus da eu-LISA (*The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice*) isimli sistem ve kuruluştur (Chamon, 2016; Egeberg, Trondal ve Vestlund, 2014: 13). Avrupa Birliği’ne bağlı olarak 2011 yılında kurulan eu-LISA operasyonel faaliyetlerine 1 Aralık 2012 tarihinden itibaren başlamıştır. Ajans kendisini Avrupa güvenliğine yönelik mevcut ve ortaya çıkabilecek tehditlere karşı entegre yanıt üreten bir sistem olarak tanımlamaktadır. Böylece eu-LISA, üye ülkeler arasında hızlı veri alışverişine ve bilgi güvenliğine olanak vermektedir. Ajans’ın yasallaşması ise 21 Kasım 2018 tarihinde Avrupa Birliği Resmi Gazetesi’nde yayımlanarak gerçekleşmiştir. Schengen ve Vize Bilgi Sistemleri gibi Türkiye’yi de ilgilendiren sistem ağlarının dijital bir merkez altında yürütülmesine çalışılmaktadır.

**Genel Değerlendirme ve Sonuç**

Siber güvenliğin bir parçası olan ‘siber suçlarla mücadele’ başlığı, siber suçların sınır aşan boyutları nedeniyle teknik izleme ve cezai yargılamayı oldukça güçleştirmekte olduğundan ‘siber yönetişim’ konusunu gündeme getirmektedir. Böylece ülkeler siber suçlarla mücadelede ister devlet düzeyinde ihlal olsun, isterse bireyler ya da organize gruplar/örgütler aracılığıyla işlenen suçlara karşı olsun uluslararası ya da ulus üstü yasal bir zemine ve konunun mahiyeti itibariyle dinamik bir şekilde politika üretim sürecine ihtiyaç duymuştur.

Türkiye’nin siber güvenlik alanında taraf olduğu en önemli ve ilk uluslararası düzenlemenin başında Avrupa Konseyi Siber Suç Sözleşmesi (*Council of Europe: Convention on Cybercrime*) gelmektedir. Avrupa Siber Suç Sözleşmesi, Avrupa Birliği üyesi devletler arasındaki işbirliğinin yanı sıra uluslararası düzeyde diğer devletlerle de işbirliklerine temel vurgu yapmaktadır. Ancak Türkiye’de siber güvenlik politikalarının gelişiminde Avrupa Birliği’nden bağımsız olan Avrupa Konseyi Siber Suç Sözleşmesi de dâhil olmak üzere Avrupa Konseyi ve Avrupa Birliği’nin birincil referans kaynağı ya da itici gücün olduğunu söylemek güçtür.

AB, Avrupa Konseyi ve NATO benzeri uluslararası kuruluşların ülkelerin kendi ulusal siber güvenlik strateji ve tercihlerinin gelişimini zorlaştırabilecekleri de unutulmamalıdır. Teknolojinin karmaşık ve çok hızlı değişen yapısı, riskin mutlak olarak öngörülememesi ve siber sistemlerin belli bir ağ üzerinde yürütülmeye çalışılması özellikle ulus devletlerin kamusal menfaat ve milli siyasetleri açısından da sorgulanır hale gelmektedir. Bu noktada Türkiye özelinde AB’nin ya da başka bir taraf örgütlenmeye Türkiye’nin uyumu adına bağlayıcı ve itici bir unsur olması varsayılsa dahi, kendi ulusal çıkarlarını öncelemek durumundadır. Daha açık bir ifadeyle küresel siber yönetişim aktörleri ve ağları ile işbirliği, Türkiye’nin ulusal siber güvenliğini milli çıkarları ve öncelikleri ile koruması ve yürütmesine engel teşkil etmemelidir.

Öte yandan, Türkiye gibi son derece stratejik bir konumda olan bir ülkenin siber güvenlik politikaları ve uygulamaları da nitelik arz etmek durumundadır. 11 Eylül saldırıları ile yeni bir döneme girdiğimiz küresel sistemde, özellikle de ABD’nin Irak’ı işgaline karşı Türkiye’deki üsleri kullanmasına izin vermediğimiz 2003 sonrasındaki süreçte ABD başta olmak üzere her ülkeden ve devletten saldırılara karşı daha açık hale gelen ülkenin bağımsız bir politika üretmesi bir zorunluluk. Tabii ki bu politikalar ve ülkenin ulusal öncelikleri ve menfaatleri temelinde ortaya koyacağı ilkeler çerçevesince başta Avrupa ülkeleri olmak üzere tüm ülkelerle ilişki ve işbirliği alanları tesis edilebilir.

Bu bağlamda Avrupa Birliği ve Avrupa Konseyi Türkiye açısından oldukça öğretici, oldukça ufuk açıcı olmuştur. AB üyelik sürecinin hızlı ve dinamik olduğu dönemlerde siber güvenlik alanında atılmış olan adımları yadsımamak gerekmektedir. Her türlü önyargı ve ayrımcılık uygulamalarına karşın AB demokratik bir birlik olarak ilişki içinde olduğumuz, daha doğrusu olmak zorunda kaldığımız ulus üstü bir örgüttür. Sayıları 5-6 milyonu bulan Türk varlığı, büyük dış ticaret partnerlerimizin bulunması ve tarihsel bağlarımız Avrupa’yı önemsememizi gerektirmektedir.

Ancak, son dönemlerde dünya siyasetinde ortaya çıkan ayrımcı dil ve ülkeleri milli menfaatlerine yönelten siyasi, sosyal ve kültürel nedenler Avrupa’yı da karıştırmış, ötekileştirici, ayrıştırıcı dili kullanan çevrelerin ellerini daha da güçlendirmiştir. Sürekli dostluk ve sürekli düşmanlık düşüncesinin ortadan kalktığı günümüz siyasetinde Türkiye kendi siber güvenlik politika önceliklerini benimsemek durumundadır. 15 Temmuz Türkiye için son derece uyarıcı bir süreç olmuştur. Dost-düşman tanımlaması yeniden yapılmıştır. Bu süreçte Cumhurbaşkanlığı Hükümet Sistemi’nin tesis edilmeye çalışıldığı bugünlerde süreç birtakım imkânlar sunmakta, tüm devlet mekanizmasını olduğu gibi genel manada güvenlik ve özelde siber güvenlik alanında ciddi dönüşüm fırsatları bahşetmektedir.

Avrupa ve Avrupa Birliği Türkiye için ilk fitili ateşleme, siber güvenlik alanına yoğunlaşma ve hassasiyet oluşturma anlamında oldukça yararlı olmuştur. Ancak Türkiye sadece Avrupa ile ilişkili bir ülke değildir. Her şeye rağmen ABD ilişkileri, NATO boyutu, Rusya, Çin, Hindistan ve İran gibi ülkelerle ilişkileri olan Türk ve İslam dünyası ile olduğu kadar Afrika ile de tarihsel ve kültürel bağları olan bir ülke olması hasebiyle ulusal siber güvenlik politikalarını geliştirmek durumundadır.

Bu süreçte sınır aşan network yapılanması nedeniyle tüm politikalarını ve güvenlik odaklı uygulamalarını geliştirmek zorundadır. Türkiye’ye atfedilen ‘uyuşturucu güzergâhı’ ve ‘insan kaçakçılığı güzergâhı’ türünden yakıştırmalara da böylece bir cevap verilmiş olacaktır. Eğer varsa bu türden organizasyonlar bu yapılanmaların mutlaka parasal boyutu da mevcuttur. Değişim mutlaka bir bedel mukabilinde yürütülmektedir. Bu nedenle siber güvenlik aynı zamanda illegal para transferlerini de açığa çıkaracaktır.

Bütün bu sıralanan nedenlerle siber güvenlik alanı ulusal güvenliğin en önemli bileşeni durumundadır bugün. Küresel siyasetin temel konularından olan ülkelerin siber saldırılara maruz kalmaları, siber yolla işlenen suçlar vb. sanal âlemdeki suç örüntüleri topyekûn bir mücadele ve kayda değer bir önleyici mekanizmanın geliştirilmesi ile ortadan kaldırılabilir. Siber suç örgütlerinin en zayıf gördükleri sistemleri hedef aldıkları bir vakıadır. Türkiye sistemini en azından ilişkili olduğu ülkeler arasında ortalama veya üzerine bir noktaya taşıyabilirse bu türden yapılanmaların hedefi olmaktan kurtulabilir. Yok, bilerek ve isteyerek özellikle Türkiye’ye karşı bir saldırı planlanmışsa bu durumda yine bir politika bulunması gerekir.

Sosyal medya konusu 2013 Gezi Olayları sürecinde popüler olmuş, bunun üzerinden ülke siyaseti dizayn edilmeye çalışılmıştı. Akabinde hiçbir kontrole tabi olmayan bu alana ilişkin birtakım düzenlemeler gündeme gelmişti. O dönemde başlayan saldırı ve manipülasyon kastı halen devam etmektedir. Milli savunma sistemlerini kurmak isteyen, silah sistemleri ve yazılımlarını geliştirmek için çabalayan bir ülke olan Türkiye’nin en temel sorun olan siber güvenlik alanına yönelme vaktinin çoktan geldiği ortadadır. Cumhurbaşkanlığı Hükümet Sistemine geçiş çabalarının fırsat oluşturduğu unutulmadan dönüşüm süreci hızlandırılmalıdır.

Bu meyanda siber güvenlik konusunun farklı disiplinleri, sektörleri, aktörleri ve bileşenleri bulunduğu hatırdan çıkarılmadan tüm bu değişkenleri aynı çatı altında buluşturabilecek bir yönetişim modelinin başarılı olabileceği de unutulmamalıdır. Resmi - gayri resmi, devlet – özel ayrımı olmadan ekonomik, sosyal, siyasal, teknik, kültürel ve hukuksal boyutları bulunan bir sorun yine bütün bu bileşenlerle beraber ele alındığı sürece başarıyla çözülebilir. Ayrıca, münhasıran Avrupa için üretilen çözümler veya ABD için bulunan yöntemlerin Türkiye özelinde başarılı olması mümkün olmayacaktır. Bütün bu nedenlerle Cumhurbaşkanlığı nezdindeki kurul Türkiye gerçeğine uygun bir yapılanma içine girmelidir.

**Kaynakça**

Akyeşilmen, N. (2018). Cyber Good Governance: A New Challenge in International Power Politics. *Siber Politikalar Dergisi*, 3 (6), 187-206.

Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye’nin Siber Güvenlik Mevcut Durum Analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies*, 1 (1), 24-28.

Barrineau, J. E. (2005). *Securing American Cyberspace: A Strategy Necessity*. USAWC Strategy Research Project. Pennsylvania: U.S. Army War College. <https://apps.dtic.mil/dtic/tr/fulltext/u2/a424249.pdf>, (Erişim Tarihi: 12.05.2019).

Bıçakcı, S., Ergun, F. D. ve Çelikpala, M. (2016). Türkiye’de Siber Güvenlik. Ed. S. Ülgen, *Türkiye’de Siber Güvenlik ve Nükleer Enerji*, 1. Baskı, İstanbul: İmak Ofset Basım Yayın, 28-73.

Buono, L. (2010). Investigating and Prosecuting Crimes in Cyberspace: European Training Schemes for Judges and Prosecutors. *ERA Forum*, 11 (2), 207-218.

Chamon, M. (2016). *EU Agencies: Legal and Political Limits to the Transformation of the EU Administration*. Oxford: Oxford University Press.

Conner, F. W. and Coviello, A. W. (2004). *Information Security Governance: A Call to Action*. Corporate Governance Task Force Report.

Dijital Türkiye Platformu (DTP) (2017). *Türkiye’nin Siber Güvenlik Stratejisine Yönelik Değerlendirmeler*. İstanbul.

Egeberg, M., Trondal, J. and Vestlund, N. M. (2014). *Situating EU Agencies in the Political-Administrative Space*. ARENA Working Paper 6, Oslo.

Erdem, M. ve Özocak, G. (2017). Sınıraşan Bir Suç Olarak Siber Suçlarla Mücadelede Uluslararası İşbirliği. 1-7, <https://ab.org.tr/ab17/bildiri/110.pdf>, (Erişim Tarihi: 12.05.2019).

Eren, M. (2017). *Avrupa Birliği’nin Siber Güvenlik Politikası*.1. Baskı, İstanbul: Beta Basım Yayım.

Erendor, M. E. (2016). Risk Toplumu ve Refleksif Modernleşme Çerçevesinde Siber Terörizm: Tanımlama ve Tipoloji Sorunu. *Siber Politikalar Dergisi*, 1 (1), 120-139.

European Commission (EC) (2013). <https://ec.europa.eu/info/law_en>, (Erişim Tarihi: 05.05.2019).

European Union Agency for Network and Information Security (ENISA) (2015). European Cyber Security Month: during October, find out how to be safe online. <https://www.enisa.europa.eu/news/enisa-news/european-cyber-security-month-during-october-find-out-how-to-be-safe-online>, (Erişim Tarihi: 21.05.2019).

European Union Agency for Network and Information Security (ENISA) (2016). CIIP Governance in the European Union Member States. <https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/ciip-governance-in-the-eu-annex>, (Erişim Tarihi:20.05.2019).

Güntay, V. (2016). Ulusal Güvenlik Çerçevesinde Siber Güvenlik Yaklaşımı Oluşturma Sorunu. *Siber Politikalar Dergisi*, 1 (1), 101-119.

İçel, K. (2001). Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 59 (1-2), 3-10.

Karaarslan, E. (2013). Siber Güvenlik Deneyleri için Ağ Benzetici ve Ağ Sınama Ortamlarının Kullanımına Dair Ön İnceleme. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisleri Dergisi*, 6 (1), 1-9.

Kutlu, Ö., Kahraman, S. ve Dinçer, S. (2019). Teknoloji Güvenliği ve Dijital Dönüşüm Kapsamında ABD, Rusya ve Türkiye’de Siber Güvenlik Politikaları. Ed. H. Acar, *Kamu Güvenliği Politikaları: Yerelden Küresele*. 1. Basım, Ankara: Nobel Akademik Yayıncılık, 169-200.

Kutlu, Ö., Sevinç, İ. ve Kahraman, S. (2018). Türkiye’de E-Devlet Uygulamalarında Güvenlik Risklerinin Analizi. *Turkish Studies*, 13 (21), 129-156.

Marion, N. (2010). The Council of Europe’s Cyber Crime Treaty: An Exercise in Symbolic Legislation. *International Journal of Cyber Criminology*, 4 (1-2), 699-712.

Önok, M. (2013). Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği. *Marmara Üniversitesi Hukuk Araştırmaları Dergisi*, 1229-1270.

Özbek, M. (2015). The Impacts of European Cybercrime Conventionon Turkish Criminal Law. *Articletter*, (Summer), 73-88.

Schell, B. H. and Martin, C. (2004). *Cyber Crime: A Reference Handbook*. California: ABC-CLIO.

Sevinç, İ. (2006). Türk Kamu Yönetiminde Bilgi Teknolojileri Kullanımı. *Selçuk Üniversitesi Sosyal Bilimler Meslek Yüksek Okulu Dergisi*, 9 (1-2), 355-372.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB) (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi. Ankara.

Wales, E. (2000). Draft Council of Europe Cyber Crime Convention Upsets Civil Rights Bodies. *Computer Fraud and Security Issue*, (12), 7-7.

Weber, A. M. (2003). The Council of Europe’s Convention on Cybercrime. *Berkeley Technology Law Journal*, 18 (1), 425-446.

Yayla, M. (2013). Hukuki Bir Terim Olarak Siber Savaş, *Türkiye Barolar Birliği Dergisi*, (104), 177-202.

Yılmaz, S. ve Sağıroğlu, Ş. (2013). Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri. 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Bildiriler Kitabı, 20-21 Eylül 2013, Ankara, 158-166.

Yılmaz, E. N., Ulus, H. İ. ve Gönen, S. (2015). Bilgi Toplumuna Geçiş ve Siber Güvenlik. *Bilişim Teknolojileri Dergisi*, 8 (3), 133-146.

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1726&from=EN>, (Erişim Tarihi: 21.05.2019).

1. \* Prof. Dr., NEÜ, Siyasal Bilgiler Fakültesi, Siyaset Bilimi ve Kamu Yönetimi, okutlu@erbakan.edu.tr [↑](#footnote-ref-1)
2. \*\* Araş. Gör., NEÜ, Siyasal Bilgiler Fakültesi, Siyaset Bilimi ve Kamu Yönetimi, skahraman@erbakan.edu.tr [↑](#footnote-ref-2)
3. \*\*\* Araş. Gör., NEÜ, Siyasal Bilgiler Fakültesi, Siyaset Bilimi ve Kamu Yönetimi, sdincer@erbakan.edu.tr [↑](#footnote-ref-3)
4. Bulut bilişim güvenliğini Avrupa Birliği ve Türkiye açısından inceleyen bir çalışma için bkz. Helvacıoğlu-Kuyucu, A. D. (2011). The Playground of Cloud Computing in Turkey. *Procedia Computer Science*, 3, 459-463. [↑](#footnote-ref-4)