Avrupa Birliği'nin Gelişen ve Değişen Tehdit Algısı: Siber Güvenlik

Ahmet Emre KÖKER*

Öz

Bu çalışmada Avrupa Birliği'nin ekonomik, siyasi, kültürel, sağlık ve güvenlik gibi birçok başlık altında etkilendiği dijitalleşme süreci ve buna bağlı olarak artan siber güvenlik tehditlerine "Avrupa Birliği'nin Gelişen ve Değişen Tehdit Algısı: Siber Güvenlik" sorusu ile cevap aranmaktadır. AB'nin siber güvenlik politikalarına yönelik odak noktası kurumlar ve gayri resmî (kurallar, prosedürler gibi) yapılar ekseninde kurumsalcılık ve bütünleşme kavramları çerçevesinde analiz edilmektedir. Bu maksatla örnek olay incelemesi araştırma deseni kullanılmıştır. Veri toplama aracı olarak belge (gazete, görsel medya, hükümet ve hükümet dışı raporlar vb.) incelemesi seçilmiştir. Belge taraması yapılarak elde edilen veriler literatür taraması ışığında belirli başlıklar altında tartışılmıştır. AB ve ona bağlı kurumlar özelinde hızlı dijitalleşme süreci siber güvenlik sorunlarının tartışılması için örnek olay niteliğinde ele alınmıştır.

Yapılan incelemeler sonrasında hızlanan dijitalleşmeyle aynı oranda siber güvenlik olaylarında artış olduğu tespit edilmiştir. Siber güvenlik tehditlerinin kâr amacı gütsün veya gütmesin tüm organizasyonların stratejik bir unsur olarak ele alması gereken bir olgu olduğu ortaya çıkmıştır. Ayrıca Avrupa Birliği'nin kurumsal tedbirlerinin de yeterli bir koruma sağlamayacağı anlaşılmıştır. Bu nedenle alınacak tedbirlerin tüm üye devletlerin ve hükümetlerin içinde olduğu bütüncül bir bakış açısıyla ele alınması gerektiği sonucuna varılmıştır. AB'deki mevcut kurumların tek başına bu süreci yönetemiyor olmasından dolayı

*Dr. Ahmet Emre KÖKER, PTT A.Ş. Genel Müdürlüğü, a.emrekoker@hotmail.com, ORCID No: 0000-0002-8032-4237

siber güvenlik konusunda farkındalık yaratılması ve gerekli yatırımların bir an önce yapılması tavsiye edilmiştir. Ancak bu yatırımlar stratejik yönetim bakış açısıyla yapılmalı ve üye devlet kurumlarının da içinde olduğu bir yönetişim ortamında gerçekleşmelidir.

Anahtar Kelimeler: Dijitalleşme, Avrupa Birliği, ENISA, JRC, Siber Güvenlik

The Evolvıng And Changıng Threat Perceptıon Of The European Unıon: Cyber Securıty

Abstract

In this study, an answer is sought to the digitalization process that the European Union is affected by under many titles such as economic, political, cultural, health and security , and the increasing cyber security threats, with the question "Evolving and Changing Threat Perception of the European Union: Cyber Security". The focus of the EU's cyber security policies is analyzed within the framework of the concepts of institutionalism and integration on the axis of institutions and informal structures (such as rules, procedures).

For this purpose, case study research design was used. Document (newspaper, visual media, governmental and non-governmental reports, etc.) review was chosen as the data collection tool. The data obtained by scanning documents were discussed under certain headings in the light of literature review. The rapid digitalization process in the EU and its affiliated institutions has been handled

as a case study for the discussion of cyber security problems.
After the examinations, it has been determined that there is an increase in cyber security incidents at the same rate as the accelerated digitalization. It has emerged that cyber security threats are a phenomenon that all organizations, whether for profit or not, should consider as a strategic element. It has also been understood that the institutional measures of the European Union will not provide sufficient protection. For this reason, it has been concluded that the measures to be taken should be addressed with a holistic perspective that includes all member states and governments. Since the existing institutions in the EU cannot manage this process alone, it is recommended to raise awareness about cyber security and make the necessary investments as soon as possible. However, these investments should be made from a strategic management perspective and should be realized in a governance environment that also includes member state institutions.

Keywords: Digitalization, European Union, ENISA, JRC, Cyber Security

Giriş

Avrupa Birliği 1950'li yılların ilk yarısından bu yana karşılaştığı krizleri teker teker atlatarak zamanın gerçeklerine de kendisini uydurarak başarıyla bütünleşmeyi sürdürmüş bu durumda kurumsallaşma sürecini güçlendirmiştir. Avrupa Birliği'nin özünde var olan küreselleşmeye ayak uydurma, kendini yenileme, geliştirme, büyüme gibi temel hedefler bütünleşmenin ve kurumsallaşmanın başarısını göstermektedir. Bu süreç günümüzde siber uzay özelinde de devam etmektedir.

Maddi ve manevi hasarlara yol açabilen siber saldırılar özellikle ağ ve bilgi teknolojilerinin gelişmesiyle birlikte siber uzayı daha önemli hale getirmektedir. Siber uzayda sıklıkla karşılaşılan tehditlerin ve ortaya çıkan güvenlik risklerinin Avrupa Birliği'ne ve üyelerine yönelik saldırı ihtimalini arttırdığı görülmektedir.

Artan saldırı ihtimalleri çerçevesinde günümüz yapısında Avrupa Birliği tarafından oluşturulmuş bilgi ve sistem güvenliğinden sorumlu birimler ve mekanizmalar ortaya çıkan yeni siber tehditlere karşı sistemleri korumayı sağlamakta zorluk çekmektedir. Çünkü bilgi güvenliği yöneticileri ve görevlilerinin yapacakları uygulamalar çok çeşitlidir. Avrupa Birliği'nin çok uluslu yapısı düşünüldüğünde OGSP kapsamında tüm ülkeler bir arada değerlendirilmelidir.

Bu çerçevede çalışmada odaklanılan temel kavramlar; Avrupa Birliği'nin güvenliğini sağlamak için geliştirdiği bütünleşme çabaları ve stratejiler ile kurumsal stratejiler ve politikalardır. Ayrıca siber saldırı örnekleriyle birlikte ortaya çıkan tehditler, algısal dönüşümleri tetikleyerek OGSP'nın yeniden ele alınması ihtiyacını doğurmuştur.

Çalışmanın ilk bölümünde, Avrupa Birliği'nin güvenliğini sağlama süreci ile siber güvenliğe ilişkin uygulamaları analiz edilmektedir. Ayrıca AB'nin siber güvenlik politikalarına yönelik geliştirilen bu analiz kronolojik olarak ortaya konulmuştur. Böylece makalenin teorik çerçevesini oluşturan kurumsalcılık teorisi ve bütünleşme yaklaşımına değinilmiştir. İkinci bölümde; ilk bölümde gerçekleştirilen analiz çerçevesinde ortaya konan veriler ışığında AB'nin siber güvenlik uygulamaları, politikaları, faaliyetleri ve stratejileri üzerinde durulmaktadır. Söz konusu incelemeler gerçekleştirilirken de Avrupa Birliği'nin otonom ve işbirliği altında uluslararası ilişkilerde yürüttüğü siber operasyonların bir bütünleşmeye mi gittiği sorusunu ortaya çıkarmaktadır. Bu doğrultuda AB'nin siber güvenliğe geçişinin açıklandığı bu bölümdeki yaklaşım, uygulama ve hedeflere yönelik tartışılmalar çerçevesinde çalışmaya adını veren "Avrupa Birliği›nin Gelişen ve Değişen Tehdit Algısı: Siber Güvenlik" sorusuna cevap aranmaktadır. Son kısımda Avrupa Birliği Siber Tehditlerle Nasıl Başa Çıkıyor? Sorusuna ENISA, JRC ve NIS özelindeki kurumsal güvenlik yaklaşımları ile cevap aranmaktadır.

Avrupa Birliği'nin Yeni Güvenlik Zorluğu Olarak Siber Güvenlik

Kavramsal ve Kuramsal Bakış

Dijitalleşme ve küreselleşmeyle birlikte artan ekonomik bağımlılık, teknoloji ve iletişimdeki değişiklikler, devletin devlete veya devletin kurumlara olan bağlılığını arttırmaktadır. Artan bağımlılık, uluslararası sınırların güvenliğini aşındırmakta devletlerin kendi ülkelerinin taleplerini her zaman karşılayamamasına yol açmaktadır. Bu durum güvenlik, adalet, refah ve insan hakları ihlallerini arttırmaktadır (Mccormick , 2005). Bu sebeple her aktör ilk olarak ulusal güvenlik sistemini kurmalı ve yakın çevresine yönelik stratejilerini belirlemelidir. İkinci aşamada küresel siber saldırılara karşı güvenlik stratejileri geliştirmelidir (Dedeoğlu, 2003). Bu kapsamda özellikle Avrupa özelinde uluslararası sistemde devletlerin egemenliğinin sarsılması fikrinden Avrupa Birliği fikri ortaya çıkmıştır. Geleneksel bu yargılar günümüzde sanal bir boyut üzerinde yaşanmaya başlamıştır. Dijitalleşmenin etkisinden dolayı artan bu dönüşüm sonucunda AB'nin güvenlik algısına yönelik kurumsal yapısının yeniden tanımlanarak siber uzaya kayması bir zorunluluk halini almıştır.

Robert Keohane ve Joseph Nye gibi Neoliberal düşünürlerin çatışma/işbirliği bakışı, ortak çıkarlar, güç dengesi ve barışçı ilişkiler üzerine kurulu bir uluslararası hukuk kodunun oluşturularak tehditlerin azaltılabileceği yönünde bir fikre dayanır. Robert Keohane'ye göre; hem sistemin hem de toplumun birbirinden ayrıldığı sınırların ve farklılığın üstesinden gelmek için bir tür dayanışma ve işbirliği modelinin gerekliliğinin altını çizmektedir. Bu kapsamda; Avrupa

Birliği'ne yönelik ilgili literatür analiz edildiğinde AB'nin çeşitli alanlarda işbirliğine yöneldiği görülmektedir (Nye & Welch, 2010). Ancak, siber güvenlik alanına yönelik literatürün kısır kaldığı ve önemli bir boşluk olduğu görülmektedir. Bu çerçevede artan üye sayısına paralel olarak sınırlarını genişleten Avrupa Birliği, siber sınırlar konusunda beklenen gelişmeyi sağlayamamıştır.

Bu anlatılandan yola çıktığımızda AB, siber uzayın önemli fırsatlar sunduğunu, ancak Ortak Dış ve Güvenlik Politikası da dâhil olmak üzere AB dış politikaları için sürekli gelişen zorluklar oluşturmasından dolayı siber tehditlerin ve risklerin azaltılması gerektiğini kabul etmektedir. Bu ön kabul çerçevesinde de AB'nin, üye devletlerinin ve vatandaşlarının bütünlüğünü ve güvenliğini korumaya yönelik artan ihtiyacı gidermek için siber faaliyetler gerçekleştirdiği görülmektedir.

Siber faaliyetlere yönelik ortaya çıkan güvenlik ihtiyacını sağlama sürecine kuramsal olarak baktığımızda Kopenhag Okulunun konuya yaklaşımı bize yardımcı olmaktadır. Buzan ve Waever'in başını çektiği Kopenhag Okuluna göre güvenlik kavramı, iletişim ve etkileşimler sonucu ortaya çıkar ve karşılıklı öznellik üzerinden açıklanabilir. Kopenhag Okulu temsilcilerine göre tehdidin gerçekte var olması gerekmemektedir. Yani bir durumun gerçekten tehdit olup olmadığı tecrübe edilmeden anlaşılamaz. Bu yüzden konunun aktörlerin tehdit olarak adlandırmalarıyla tehdide dönüştüğü anlaşılmaktadır (Baysal & Lüleci, 2011).

Kopenhag Okuluna özgü bakış açısıyla; karşılaşılan tehdit yaşamsal (beka) ile ilgilidir. Bu yüzden önlem almakta gecikilirse çok önemli sonuçları olabilir. Bu yüzden güvenlik kavramı hem fayda hem de zararı içinde barındırır. Kopenhag Okulu'nun güvenlik kavramını sektörlere ayırması da aslında siber güvenlik kavramının konuşulmasına büyük fayda sağlamaktadır. AB strateji belgesinin oluşturulması süreci de bu kavramsal çerçeve üzerine tasarlanmıştır (Köker, 2021).

AB strateji belgesinde belirtilen temel haklar, demokrasi ve hukukun üstünlüğü gibi kavramlar siber uzayda da korunması gereken temel ilkeler olarak belirtmiştir. Bir diğer önemli nokta internetin özgürlüğü ve refah seviyesini arttırmada pozitif etkisi bulunduğudur. Bu yüzden AB tarafından Avrupa dijital tek pazarının sağlanması ve dijitalleşme kapsamında hem vatandaşların güveninin sağlanması hem de refah seviyesinin artması hedeflenmektedir. Siber suçların önlenmesi ve ortak işbirliğinin sağlanması görevi de kurumlara düşmektedir.

Bu bağlamda Avrupa Birliği içerisinde kurumlar çok önemlidir. Kurumların bu önemi strateji belgelerinde de belirtilmektedir. Ayrıca strateji belgesinde endüstriyel ve teknolojik

ürün sunan birçok küresel liderin AB dışında bulunmasından dolayı AB ve üyelerinin bağımlılıklarından bahsedilmektedir. Bu bağlamda siber güvenlik ürünleri için bir tek pazar yaratılması, ortak arge geliştirilmesi, yenilik için teşviklerin oluşturulması gibi uygulamalar hedeflense de tam olarak sağlanamamıştır.

Bir diğer yandan AB siber güvenlik ilkeleri " AB'nin temel değerleri", " temel hakların, düşünce özgürlüğünün, kişisel bilgilerin ve gizliliğin korunması", " herkes için erişim" " demokratik ve etkili çok paydaşlı yönetişim" ve " güvenliği sağlamak için paylaşılmış sorumluk" olarak beş temel noktaya dayanmaktadır. Bu bağlamda yasaları, teamülleri ve normları içeren AB'nin temel değerlerinin sadece fiziksel dünyada değil dijital dünyada da geçerli olduğu belirtilmektedir.

Aslına bakılırsa Avrupa Birliği, normlarını yayıp, gücünü dünyanın çeşitli yerlerinde emperyal bir şekilde genişletmektedir. Fakat siber güvenliği sağlamaya yönelik Avrupa Birliği düzeyinde güçlü ve etkili yasaları temel alacak platformu işler hale getirememiştir. Örneğin; AB ve NATO'ya üye olan devletlerarasında izlenecek siber politikaların mükerrerliğinde ve farklılığında ne olacağı belli değildir.

Bu belirsizlik AB'nin çeşitli ekonomik ve siyasi egemenlik biçimleri ve hatta resmi ilhaklar yoluyla diğer aktörlere yerel kısıtlamalar getirmeye çalışmasına yol açmaktadır (Zıelonka, 2008). Söz konusu kısıtlamaların getirilmesinin bazı sebepleri bulunmaktadır.

Bu sebepler arasında AB kurumlarının web sitelerinin veya sistemlerinin yazılım bileşenlerinde, protokollerinde veya donanımlarında meydana gelen ve önemli sayıda kullanıcıyı ve/veya kritik altyapıyı etkileyebilecek güvenlik olayları ve açıklarının bildirilmesi ihtiyacı bulunmaktadır (Computer Emergency Response Team, 2020). Tüm bu açıkların bildirilmesi ve sürecin sağlıklı bir şekilde ilerleyebilmesi ihtiyacından dolayı Avrupa Konseyi birçok anlaşma gerçekleştirmiştir. Bu çerçevede AB, siber uzayın önemli fırsatlar sunduğunu, ancak Ortak Dış ve Güvenlik Politikası da dâhil olmak üzere AB dış politikaları için sürekli gelişen zorluklar oluşturduğunu kabul etmektedir. AB'nin bu kabulü, üye devletlerinin ve vatandaşlarının bütünlüğünü ve güvenliğini korumaya yönelik artan ihtiyacı teyit etmektedir (Council of Europe, 2001). Bu konuda Mai'a K. Davis Cross'un yaklaşımı önem kazanmaktadır.

Mai'a K. Davis Cross, AB'nin güvenliğinin sağlanması ve politika oluşturma süreci hakkında önemli tespitlerde bulunarak güvenlik entegrasyonunda hem dış hem de iç boyutları içeren ilerlemelerin gerçekleştiğinden bahsetmektedir (Cross, 2011). AB'nin siber uzaydaki bu teyidine yönelik içsel ve dışsal değişkenler birbirinden ayrılamaz derecede

bir öneme sahiptir. Örneğin; Tüm AB üye ülkeleri Schengen'in bir parçası değildir, diğerleri ise kapsam dışında kalma hakkına sahiptir.

Aynı zamanda, ortak serbest dolaşım alanı aynı zamanda birkaç AB üyesi olmayan ülkeyi de içine almaktadır. Schengen sisteminin çeşitli üyeliklerinin yanı sıra, onu yöneten iç kurallarda da farklılaşma gözlemlenebilir. Bu kurallar ve özellikle iç sınır kontrollerini yeniden uygulamaya koyma seçeneği, devletlere yüksek baskı durumlarında ulusal sınırlara dönme konusunda bir seçenek sunar(Somer, Tekin, & Meissner, 2020). Alternatif olarak sunulan bu haklar siber uzayda da bütünleşme sürecinde aynı yönde ilerlemektedir. Alternatif birçok seçenekler içerisinde varlığını sürdüren Avrupa Birliği üye ülkelerinin güvenliklerini sağlamaya yönelik oluşturulabilecek bir siber bütünleşmede dışsal değişkenlere ilişkin bir çalışma yapılması şarttır. Peter R. Neuman'a göre böyle bir yaklaşımın ne ölçüde içsel veya ne ölçüde dışsal değişkenlere yer vereceği baştan kararlaştırılmalıdır (Neuman, 2013). Çünkü siber uzayın yapısı belirsizdir. Bu kapsamda Waever 'in Avrupa tanımları içsel ve dışsal siber değişkenlerin tanımlanmasına fayda sağlayacaktır. (Çakır , 1996). Böylece içsel ve dışsal siber değişkenlerin neler olduğuna yönelik kriterin belirlenmesinin ardından Avrupa'nın siber sınırları kararlaştırılmalıdır.

Bu aşamada, siber güvenliği sağlamaya yönelik paydaşlarla koordinasyon ve işbirliği sağlanamaması AB'nin siber bütünleşme sürecini olumsuz etkilemektedir. Bu olumsuzluğu belirtmek için Thomas Schelling her koşulda işbirliğinin önemini ortaya koymuştur(Schelling, 1980). Bu yüzden makalemizde belirttiğimiz içsel veya dışsal bölümleme konusundaki karar verme zorunluluğumuz bir seçenek önermektedir. Siber uzayda bütünleşmeye yönelik iten bir etken olarak ortaya çıkan kurumlar özellikle ENISA özelinde belirlenen kurallar ve uygulamalar iten etken olarak gözükmektedir. ENISA özelinde bütünleşmeye karşı çıkan ülkeler ise kendini çeken etkenler olarak gözükmektedir. Bu karşıtlıklar içerisinde Avrupa bütünleşmesinden bahsedebilmemiz için siber konuları ayrı düşünemeyiz.

Geleneksel düzlemde Avrupa Birliği; Avrupa'daki ülkelerin hukuki, siyasi, ekonomik ve kimi durumlarda sosyal ve kültürel olarak bütünleşmesidir(Urgancı, 2014). Bu bütünleşme günümüzde de teknolojik alana kayarak siber alanda bir birlik nasıl olabilir şeklinde konuşulmasına yol açmıştır.

Avrupa bütünleşmesinin siber uzayda yaşanan gelişmeleri kuramsal çalışmaları ve tartışmaları beraberinde getirmiştir. Fakat bu tartışmaların ortaya koyduğu Avrupa bütünleşmesini tek bir kuram açıklayamamıştır. Dolayısıyla her bir kuram siber uzayın karmaşık ve çok kapsamlı halini göz önüne alarak bütünleşmenin sadece

bir kısmını ya da belli bir dönemini açıklayabilmektedir. Makale, bütünleşme ve kurumsallaşma kuramlarının AB'nin siber uzaydaki koordinasyon ve işbirliğini sağlama çabasına indirgemektedir. Çünkü mevcut koordinasyon ve işbirliği süreçleri siber uzaydaki entegrasyon sürecini açıklayamamaktadır. Bu çalışmada, AB'nin kurumlarının ve üye ülkelerinin siber uzaydaki ilişkileri analiz edilirken atıfta bulunulabilecek önemli hususların veya eksikliklerin olup olmadığı sonucuna ulaşmamıza fayda sağlanmaktadır.

Sonuç olarak; Avrupa Birliği'nin siber uzaya yönelik geliştirmiş olduğu yeni politika alanının merkezinde, Avrupa'nın şu anda karşı karşıya olduğu siber zorluklara etkili bir yanıt verme ihtiyacı bulunmaktadır (Carrapico & Barrinha, 2018). Bu ihtiyaç kurumsallaşma, bütünleşme ve politika tutarlılığı çabasından ayrı tutulamaz. Bu çaba çerçevesinde AB ilgisini ve politikalarını siber uzaya yönelik her geçen gün arttırmaktadır. Artan bu ilgi neticesinde gerçekleştirilebilecek en doğru yaklaşım AB'nin siber uzay sürecinin içinde birçok alt başlık barındırdığıdır.

AB'nin Siber Savunma ve Güvenlik Politikalarının Kurumsallaşmasının Tarihsel Gelişimi

1985 yılında yayınlanan "Beyaz Kitap'tan" Avrupa Birliği'nin bilgi teknolojileri ile iletişim teknolojilerine yönelik verdiği önemin kökenini oluşturmaktadır (Köksoy, 2020). Başlangıç noktası 1985'lere dayanan siber güvenlik olgusunun günümüzdeki karşılığı, ülkelerin ulusal güvenlik stratejilerinin önemli bir bölümünü oluşturmasıdır. Bu sebeple 2000'li yıllar itibari ile yaşanan siber saldırılar sonrasında AB; siber güvenliğe yönelik stratejilerini, yasal düzenlemelerini ve kurumsal dönüşümlerini gerçekleştirmiştir(Kurnaz & Önen, 2019).

2000'li yıllarda gerçekleştirilen yasal düzenlemeler çerçevesinde siber güvenlik stratejisi, ilkeleri ve eylemleri belirlenmeye başlamıştır. Bu bağlamda 2004 Yılında AB' de siber güvenliğin sağlanması konusunda koordinasyon oluşturması için kısa adı ENISA olan AB Ağ ve Bilgi Güvenliği Ajansı (European Union Agency for Network and İnformation Security) adıyla bir tüzel kişilik kurulmuştur. ENISA'nın kurulması siber güvenlik politikasının kurumsallaşmasında en önemli adımdır.

Ayrıca Ortak Güvenlik ve Savunma Politikası (OGSP) çerçevesinde siber güvenlik politikasını geliştirmek için 2013 yılında yayınlanan Cybersecurity Strategy for the European Union (AB için Siber Güvenlik Stratejisi) Strateji belgesinde siber güvenlik için siber savunmanın gerekli olduğu belirtilmiştir. OGSP misyonu çerçevesinde siber savunma stratejisi belirlemek, riskleri çıkarmak, gereklilikleri ve teknolojileri değerlendirerek geliştirmek, üyeler arasında diyalog ve koordinasyonu sağlamak, uluslara-

rası ortaklarla diyalog sağlamak gibi sorumluluklar siber güvenlik kriterlerinin belirlenmesinde önemli bir rol üstlenmektedir (European Commıssıon, 2013).

Bu önem çerçevesinde AB'nin ağ ve bilgi güvenliği sistemine yönelik siber savunma sağlanması amacıyla AB Siber Güvenlik stratejisinin bir parçası olarak Avrupa Komisyonu, AB Ağı ve Bilgi Güvenliğini içeren NIS Direktifi (bkz. AB 2016/1148) ilan etmiştir. NIS Direktifi, AB çapında siber güvenlik mevzuatının ilk parçasıdır. Amaç, AB genelinde siber güvenliği artırmaktır (Christou, 2016, s. 119-142). Bu amaç doğrultusunda 9 Haziran 2016'da Konsey, siber uzaydaki suç faaliyetleriyle mücadele için sonraki adımlar üzerinde anlaştı. İşbirliğini geliştirmek için pratik önlemleri tanımlayan iki sonuç grubu ve daha fazla eylem için bir zaman çizelgesi benimsediler. Ayrıca Avrupa Siber Güvenlik Örgütü (ECSO), Haziran 2016'da kuruldu. ECSO'nun temel amacı, Avrupa Dijital Tek Pazarının korunmasını destekleyen Avrupa Siber Güvenlik Ekosisteminin gelişimini koordine etmek ve nihayetinde Avrupa dijital egemenliğinin ve stratejik özerkliğinin ilerlemesine katkıda bulunmaktır (European Cyber Security Organization, 2021). Ayrıca dijital tek pazar doğrultusunda AB, siber güvenlik ürünleri için tek pazarı oluşturmaya çalışmış ve Ar-Ge kapsamında yaklaşık 80 milyar Euro bütçeye sahip Horizon 2020 programını gerçekleştirmiştir(Amos, 2014).

24 Ekim 2017'de Konsey, AB siber güvenlik reformu için bir eylem planı hazırlamıştır. Hazırlanan bu eylem planlarında çevrimiçi güvenliğin Avrupa vatandaşları ve işletmeler için gerekli olduğu Bakanlar tarafından vurgulanmıştır. 20 Aralık 2017'de ise kurumlar arası bir düzenleme gerçekleştirilerek AB'nin tüm kurumlarını, organlarını ve ajanslarını kapsayan kalıcı bir Bilgisayar Acil Müdahale Ekibi (CERT-EU) kuruldu.

2018 yılına gelindiğinde Konsey, siber alanın küresel, açık, özgür, istikrarlı ve güvenli bir alan olduğu, bu alandaki uygulamalara yönelik hukukun üstünlüğünün baştan kabul edildiği ve insan hak ile özgürlüklerinin temel alındığı bir yapının önemini vurgulamıştır. Aynı zamanda 2018 yılında Konsey, "Siber Güvenlik Yasası" üzerinde bir anlaşmaya varılması amacıyla Avrupa Parlamentosu ile müzakerelere başladı. Ardından ENISA tarafından "Siber Güvenlik Yasası", BİT ürünleri, hizmetleri ve süreçleri için AB çapında bir sertifikasyon çerçevesi oluşturma çalışmaları başladı. Bu çalışmalardan sonra gerçekleşen 18 Ekim 2018'deki son toplantıda, AB'de güçlü siber güvenlik inşa etmek için önlemler alınması çağrısında bulunuldu.

9 Nisan 2019'da "Siber Güvenlik Yasası" yönetmeliği Konsey tarafından kabul edildi. Yönetmeliğin kabul edilmesine paralel olarak da mevcut ENISA'yı devralacak bir "Siber Güvenlik Ajans"ı planlandı. Ayrıca

Konsey'in, siber saldırılara karşı artık yaptırım uygulamasının gerektiği kararlaştırıldı. Zaten bu karar sonrasında da ilk uygulamalar gerçekleşti. Örneğin; 2018 yılında Kimyasal Silahların Yasaklanması Örgütüne (OPCW) "WannaCry", "NotPetya" ve "Operation Cloud Hopper" adı verilen siber saldırılar düzenlenmiştir. Söz konusu siber saldırılara yönelik AB Konseyinden yapılan açıklama ile aralarında Rus Askeri İstihbarat Servisinin (GRU)' nun da bulunduğu 3 kuruluş ile Rus ve Çinli 6 kişiye yaptırım kararı alındı(Hürriyet Gazetesi, 2020). Böylece AB'ye veya üye devletlerine dış tehdit oluşturan siber saldırıları caydırmak ve bunlara yanıt vermek için AB'nin hedefli kısıtlayıcı önlemler almaya başladı. 2019 yılının sonlarında da 5G teknolojisinin önemi ve güvenlik risklerini azaltma üzerine çalışmalar gerçekleştirildi.

2020 yılında Konsey, siber güvenlikle ilgili riskleri azaltmak ve güvenli bir 5G dağıtımını sağlamak için koordineli bir yaklaşım ihtiyacını ortaya koymuştur. Ayrıca Konsey ve Avrupa Parlamentosu, Avrupa Siber Güvenlik Sanayi, Teknoloji ve Araştırma Yeterlilik Merkezi ve bir ulusal koordinasyon merkezleri ağı kurma önerisi üzerinde geçici bir anlaşmaya vardı. Anlaşmaya varılan bu yapılar dijital tek pazarın güvenliğini sağlayarak siber güvenlik alanında AB'nin özerkliğini artırmayı hedeflemektedir.

2021 yılına gelindiğinde süreç özgür ve güvenli siber uzay olarak belirlenmiştir. Bu kapsamda; Konsey, AB'nin dijital on yıl için siber güvenlik stratejisini sağlamaya yönelik olarak AB vatandaşlarını ve işletmelerini siber tehditlerden korumak, güvenli bilgi sistemlerini teşvik etmek ve küresel, açık bir güvenliği korumak için AB eyleminin çerçevesini belirlemiştir. Bunun içinde Bükreş merkezli Siber Güvenlik Yetkinlik Merkezi kurulması yönünde çalışmalara başlandı. Böylece Ortak Dış ve Güvenlik Politikası (CFSP) hedefleri doğrultusunda üçüncü devletlere veya uluslararası kuruluşlara yönelik siber saldırılara yanıt olacak kısıtlayıcı önlemler uygulanabilmesinin kolaylaşması hedeflenmiştir (Eurupean Council, 2021).

Sonuç olarak; 2021 yılında yürürlüğe giren "Özgür ve Güvenli Siber Uzay" sürecine kadar geçen 36 yılda ortaya konan ilgili belgeler, raporlar ve dokümanlar özelinde kapsamlı bir içerik analizi gerçekleştirilmiştir. Bu analiz çerçevesinde bilişim suçlarının günümüzde istisnai bir suç işleme aracı olmaktan çıktığı görülmüştür. Bilişim sistemleri aracılığıyla işlenen suçlar arasında dolandırıcılık, hakaret, özel hayatın gizliliği, sahtecilik, ve kişisel verilere karşı suçlar gibi pek çok suç türü bulunmaktadır. Bu kapsamda; bilişim suçlarıyla mücadele edilebilmesi için ülkelerin aynı farkındalıkta ve hassasiyette olması gerekmektedir. Ayrıca ülkelerin uyguladıkları maddi ceza ve ceza muhakemesi hukuku mevzuatları arasında uyumluluk olması zorunluluktur(Aliusta & Benzer, 2018). Bu sebeple görünür kılınan

siber güvenlik zorluklarına yönelik bir aksiyon alınabilmesi için şuana kadarki Avrupa Birliği'nin gelişim süreci iyi yönde ilerlemektedir.

Siber Bütünleşmenin Fikri Temeli

Avrupa bütünleşmesi fikri uzun bir geçmişe dayanmaktadır. Bu fikrin temeli Avrupa toplumlarının ortaya koydukları normların, kuralların ve sosyal, kültürel değerlerin bir ürünü olarak ortaya çıkmasından gelmektedir (Çiftçi, 2005). Bu bağlamda bütünleşme fikri güvenlik ihtiyacından ayrı düşünülemez.

Avrupa güvenliği fikri hem ulus devlet hem de kolektif politika yapma fikriyle bir arada ilerlemiştir. Uzun yıllar süren Avrupa'daki düşmanlığın ve savaşların sonrasında güvenliği oluşturmak için sürekli arayışlar olmuştur. Fakat en olumlu sonuçlanan çözüm 2. Dünya Savaşından sonra gerçekleşmiştir.

9 Mayıs 1950 tarihinde dönemin Fransa Dışişleri Bakanı Robert Schuman ve Eski Milletler Cemiyeti Genel Sekreteri Jean Monnet'in tasarısı ile dönemin stratejik unsurları (kömür ve çelik) birleştirildi. Söz konusu pragmatik karar ile birlikte devam eden süreçte Avrupa bütünleşme projesi oluştu. Bu proje ile birlikte 1951 yılında Paris'te Fransa, Almanya, İtalya ile Belçika, Hollanda ve Lüksemburg (BENELÜKS) Avrupa Kömür ve Çelik Topluluğu (AKÇT) Antlaşmasını imzaladı (Canbolat, 2002, s. 109). Sürecin kömür ve çelikle başlamasının sebebi o dönemlerin ağır sanayinin en önemli iki maddesinin kömür ve çelik olmasından kaynaklanmaktadır. Böylece Avrupa'nın "büyük iç savaşının" biteceğine inanılıyordu. Bir başka açıdan bakarsak o günün stratejikleri kömür ve çelik bugünün siberiydi. Günümüzde ise en önemli madde dijitalleşme ve dolayısıyla da siber uzaya yönelik sektörlere güvenlik duvarlarının oluşturulmasıdır.

Bu inançla 1957'de imzalanan Roma Antlaşması ile süreç geliştirilerek, kömür ve çeliğin yanı sıra diğer sektörlerde eklenmeye başladı. Bu doğrultuda ilk olarak ekonomik birliği kurmak amacıyla, Avrupa Ekonomik Topluluğu (AET) bir yıl sonrada Avrupa Atom Enerjisi Topluluğu (EURATOM) kuruldu. 1965 yılında imzalan Füzyon Antlaşması çerçevesinde bu kurumların hepsi birleştirilerek Avrupa Topluluğu oluşturuldu. Avrupa Birliği ile sonuçlanan bu sürecin güvenlik ve istikrarla alakalı bütünleşme çabası ise 27 Mayıs 1952'de imzalanan Avrupa Savunma Topluluğu'nu Antlaşmasına ve Pleven Planına gitmektedir (Kaldor & Rangelov, 2014).

Avrupa Savunma Topluluğu'nun oluşturulması için ortaya atılan Pleven planında bazı noktalar ön plana çıkmıştır. Bunlardan ilki Avrupa ordusunun hangi temelde kurulacağı ve örgütlenme şeklinin nasıl olacağıdır. İkinci olarak Avrupa›nın siyasal kurumlarına bağlı tek bir siyasal ve

askeri otorite altında olan bir ordu örgütlenmesinin oluşturulmasıdır. Oluşturulacak bu ordu yapılanması Avrupanın maddi ve manevi tüm unsurlarının kaynaşmasıyla gerçekleşmelidir. (Gözkaman, 2014).

Avrupa Savunma Topluluğunun başarısızlığından sonra, Dönemin Fransa Başkanı Charles De Gaulle 1961'de ortak bir dış politika stratejisi ile ortak bir savunma politikasının oluşturulması hedefiyle siyasi entegrasyon için ikinci girişim olan Fouchet Planınıyla hükümetler arası bir temsili temsil eden yeni bir "Devletler Birliği" oluşturmasını önerdi. Fakat bu girişim de başarısız oldu.

İlerleyen süreçte klasik düzenin değişmesi ve dijital bir yapının önem kazanmasıyla birlikte bu durum siber uzayda ne yapılacağı sorularının sorulmasına yol açmıştır. Çünkü siber uzayda karşılaşılan suç, terör, casusluk ve savaş dörtgeninde riskler ve tehditler artarak devam etmektedir. Deniz, hava, kara ve uzaydan sonra beşinci boyut olarak kabul edilen siber uzayda Avrupa Birliği'nin güçlü ve kritik ülkeleri kendi içlerinde siber ordu birimleri oluştururken siber alandaki güvenliklerini AB'ye bırakmamaktadır. Kısaca güvenlik söz konusu olduğunda hem coğrafi hem de politik açıdan siber alanın muğlaklığıyla "Avrupa" birliği kurulamamıştır.

1992 Maastricht Antlaşması uyarınca, güvenlik sadece bir politika alanı olarak görülerek Avrupa'nın entegrasyon projesine güvenlik ve savunma gibi kriterler belirli ölçütler dahilinde eklenmiştir. Avrupa Ordusu'nun hala kurulamamış olması sebebiyle de Avrupa Birliği siber uzayda, bölgesel olarak nüfuz sahibi olmak için askeri olmayan güç biçimlerine bel bağladı. Böylece; Avrupa güvenliğini sağlamak için siber suçlar, siber terör tehditleri ve siber güvenlik kapsamında sınırlandırmalara giderek Avrupa Polis Teşkilatı (EUROPOL) ve Avrupa Ağı ve Bilgi Güvenliği'nin oluşturulması Ajansı (ENISA) hakkında çok sayıda karar yayınladı. Çünkü günümüz dünyasında bilişim sektörüne yönelik gerçekleşen ilerleme ve gelişmelere bağlı olarak, mevcut fiziki alanda gerçekleşen iş ve eylemlerin sanal ortama taşınmasıyla birlikte tehdit algılamaları da değişmiştir.

Değişen bu tehdit algısıyla birlikte siber uzayda tarafların çıkarlarının örtüşmediği durumda meşru olmayan yöntemlerle kullanılan siber saldırılar ve bu saldırılara karşı geliştirilen politikalar ve araçlar siber uzayda güç mücadelesini ortaya çıkarmıştır. Bu çerçevede tanımlamaların daha net ortaya konulabilmesi amacıyla Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi imzalanmıştır.

Siber suçların ulus ötesi karakterini ele almak küresel bir çaba gerektir. Avrupa Konseyi bünyesinde siber suçlarla ilgili hazırlanan ilk resmi belge "Sanal Ortamda İşlenen Suçlar Sözleşmesi" dir. Bu belge, 2001

yılında Macaristan'da imzalanarak 2004 yılında yürürlüğe girmiştir. Söz konusu sözleşme Türkiye'de ise 10.11.2010 tarihinde imzalanmasına rağmen, 02.05.2014 tarihinde 28988 sayı numarası ile resmi gazetede yayınlanan "6533 Sayılı Uygun Bulma Kanunu" çerçevesinde yürürlüğe girmiştir (Bakanlar Kurulu, 2014).

Ayrıca Avrupa Birliği'nin siber güvenlik politikaları ve güvenlik stratejilerinin temeli kritik alt yapıların korunmasını sağlamaya dayanır. Bunu yaparken de Avrupa Birliği siber güvenlik hakkında yasal düzenlemeler gerçekleştirmektedir. Gerçekleştirilen bu yasal düzenlemelerden 2013 yılında yayınlanan Cybersecurity Strategy for the European Union (AB için Siber Güvenlik Stratejisi) en önemli belgedir. Bu belgeyle birlikte AB kritik alt yapı ve siber güvenlik bağlantısı vurgusu yapıp ortak siber savunma politikası oluşturulmasını hedeflemektedir. Ayrıca siber politikaların ve stratejilerin belirlenmesi ve kurumların siber uzaydaki güvenli faaliyetleri vurgulamaktadır. Uluslararası ortamda Avrupa Birliği'nin siber güvenlik hususuna önem vermesi uluslararası aktörler arasında siber güvenlik konusunun ne kadar önemsendiğinin göstergesidir (Eren, 2017, s. 80-90).

Bu doğrultuda AB strateji belgesi uluslararası düzeyde, koordinasyon ve işbirliği geliştirilmesine yönelik bir rehberdir. Bu rehber siber bütünleşmenin fikri temelini oluşturmaktadır. Fakat bütünleşmenin uygulama aşamasında siber güvenlik anlamında tam olarak karşılığını bulamamıştır. Bu yüzden konunun fikri düzeyde kalmaması amacıyla siber uzayda bütünleşmeye daha çok önem verilmesi, siyasi destek verilmesi ve yatırım yapılması gerekmektedir.

Bu ihtiyaçlar doğrultusunda özellikle son yıllarda AB içerisinde kurumsal düzeyde siber güvenlik stratejisi konusunda ciddi gelişmeler yaşanmıştır. Bu kapsamda Aralık 2020'de Avrupa Komisyonu ve Avrupa Dış Eylem Servisi (EEAS) yeni bir AB siber güvenlik stratejisi sundu. Bu stratejinin amacı, Avrupa'nın siber tehditlere karşı direncini güçlendirmek ve tüm vatandaşların ve işletmelerin güvenilir hizmetlerden ve dijital araçlardan tam olarak yararlanmasını sağlamaktı.

22 Mart 2021'de ise Konsey, siber güvenliğin dayanıklı, yeşil ve dijital bir Avrupa inşa etmek için gerekli olduğunu belirtti. Bu yaklaşım ile birlikte Avrupa bir bütün halinde değerlendirildi. Aslına bakılırsa bu vurgu AB'nin dijital liderliğini ve stratejik kapasitelerini güçlendirme hedefini temsil ediyordu.

Yukarıda ayrıntılı bir şekilde belirttiğimiz derinleşme ve genişleme yapısı üzerine kurulu olan Avrupa bütünleşme projesi, dijitalleşmenin yarattığı farklı dinamikler çerçevesinde tam olarak kendini geliştirememiş ve uluslararası sistemin değişen özellik-

lerine adapte olamamıştır(Akşemsettinoğlu, 2011). Bu adaptasyon sorunu siber uzaydaki genişleme ve derinleşme sürecinde de geçerlidir. Bu gelişim çizgisinin ortaya çıkarılması AB olgusunu daha iyi kavramak ve anlamak için önemlidir. Böylece daha bütüncül bir şekilde daha tutarlı analiz ve sonuçlara ulaşılabilir.

İçerisinde insan ve toplum olan her olgunun değişmesi ve evrimleşmesi kaçınılmazdır. İçerisinde birçok insan ve toplumu barındıran Avrupa bütünleşme projesi de zaman içinde değişikliğe uğramıştır. Zaman içerisinde ortaya çıkan siber uzaya yönelik projelerde bu değişikliğin en güzel göstergesidir.

Avrupa`nın yekpare olarak bir araya getirilmiş olması bütünleşmenin görünürdeki ilk başarısıdır. Fakat Birlik içinde dış politika hususlarında ortak bir refleks sağlanamamıştır. Zaten dijitalleşmenin etkisiyle az da olsa ortaya çıkan bu başarı da etkisini kaybetmeye başlamıştır.

Avrupa'nın siber uzayda bütünleşme sürecini olumsuz etkileyen örneklerin başında Estonya'nın uğradığı siber saldırılar gelmektedir. AB üyesi Estonya'nın başına gelen siber saldırılarda Avrupa Birliği bir destek verememiştir. İlerleyen süreçte Estonya gerek NATO'nun siber saldırılara karşı Estonya'yı koruma amacıyla Talinn Mükemmeliyet Merkezini Kurması gerekse kendi gerçekleştirdiği düzenlemeler çerçevesinde Estonya'nın siber kapasitesini ve gücünü geliştirdi(Estonia's e-Governance Academy, 2019). Dolayısıyla Estonya birliğe güvenmek yerine ulusal imkânlarına güvenmek zorunda kaldı.

Ulusallaşmayı ön plana çıkaran Estonya saldırısından sonra AB kurumsal anlamda düzenlemeleri gerçekleştirmeyi önceliğine aldı. AB'nin kurumsal olarak siber uzaya yönelik artan ilgisinde üye ülkelerin her alanda dijitalleşmesi, nüfusun internet kullanımındaki artışı ve kritik alanların dijitalleşmesi etkili olmuştur. Bu duruma en güzel örnek AB tarafından 2021 yılında gerçekleştirilen bir araştırmanın sonucudur. Bu araştırmaya göre 53 Avrupa ülkesinin nüfusunun internet kullanım oranı incelendiğinde bu ülkelerin toplam nüfusun yaklaşık %88'i internet kullanabiliyorken aynı durum tüm dünyada %55'lerdedir (Stats, 2021). Bu oranda Avrupa'nın dijitalleşme ve internet kullanımı alanında diğer kıtalardan önde olduğunu göstermektedir. Bu bağlamda siber tehditlerin uluslararası nitelikte olması ve devletlerinde dâhil olduğu kaotik bir ortamda ortaya çıkması konunun önemini arttırmaktadır. Zaten bilgi devrimiyle bağlantılı hem hükümetleri hem de uluslar ötesi aktörleri birleştiren siber savaş ve siber tehdit kavramları modern toplumlar için en büyük tehdittir.

Sonuç olarak; siber uzay olarak tanılandırılan bu yeni çatışma alanında ortaya çıkan çatışmaların temel silahları, belirli bir zaman ve verileri yok

etme veya yeniden yazma amacıyla yazılıma zarar vermek üzere programlanmış mantık bombaları ve bilgisayar virüsleridir. Mantık bombaları ve bilgisayar virüsleri çerçevesinde devletlerin, şirketlerin veya bireylerin sanal sınırlarının bütünlüğüne yönelik tehditler günümüzde siber sınırlar üzerinden gerçekleşmektedir. Bu siber tehditleri önlemek için AB tarafından da Nis işbirliği grubu, çok uluslu AB sistem yapısı, OGSP kapsamına alım süreci ve ENISA'nın yetkilendirilmesi gibi bütünleştirici uygulamalar gerçekleştirilmiştir. Gerçekleştirilen tüm bu uygulamalar siber bütünleşmenin fikri temelini oluşturmaktadır.

AB'nin Siber Güvenlik Stratejisi ve Politikaları

Avrupa Birliği'nin siber güvenlik stratejisi ve politikaları iki hat üzerinde değerlendirilebilir. İlk hat içeresinde Avrupa Birliği "Avrupa Güvenlik ve Savunma Politikası" (AGSP) ve "Ortak Güvenlik ve Savunma Politikası" (OGSP) kapsamında uluslararası ilişkilerde oynadığı rolü güçlendirme uygulamaları bulunmaktadır. İkinci hatta ise AB'nin içte güvenliği sağlamak üzere dış politikada kurguladığı ODGP kapsamındaki siber diplomasi uygulamaları bulunmaktadır.

"Avrupa Güvenlik ve Savunma Politikası" (AGSP) ve "Ortak Güvenlik ve Savunma Politikası" (OGSP) kavramları birliğin gerçeğini tam anlamıyla yansıtmamaktadır(Zhussipbek, 2009). Aynı durum hem otonom hem de işbirlikleri başlıkları çerçevesinde oluşturulan Avrupa Birliği'nin siber diplomasi süreçlerinin yürütülmesi amacıyla güvenlik stratejisi ve politikalarının belirlenmesi sürecinde de geçerlidir.

Sonuç olarak; AB bu iki sütun altında siber güvenliğini sağlama sürecinde birçok faaliyet yürütmüştür. Fakat siber uzaya yönelik geliştirilen politikalar veya hayata geçen uygulamalar tam anlamıyla AGSP ve OGSP kapsamına girecek şekilde üye ülkeler üzerinde kabul görmemiştir.

ODGP Çerçevesinde Siber Savunma Politikası Geliştirme Zorunluluğu

Ortak Dışişleri ve Güvenlik Politikası (ODGP) 1986 yılında Avrupa Tek Senedi'nin kurduğu Avrupa İş Birliği Kurumu'nun yerini almıştır. Avrupa Birliği'nin üç sütunundan biridir. 1992 yılında imzalanan Maastricht Anlaşması'yla resmileşmiştir. 1 Mayıs 1999 tarihinde imzalanan Amsterdam Anlaşması ile kapsam genişletilmiştir. 2007 yılında imzalanan Lizbon Antlaşması ile AB'nin ortak dış ve güvenlik politikası netleşmiştir. Böylece ortak bir savunmaya dönüşebilecek dış politikanın bütün alanlarını ve birliğin güvenliğine ilişkin tüm konuları kapsam altına alınmıştır. Genel olarak ODGP'nin amaçları şu şekildedir(Efe, 2008).

ODGP'nin amaçları;

• Birliğin bağımsızlığını, temel çıkarlarını, güvenliğini, değerlerini ve bütünlüğünü korumak,

• İnsan haklarını, hukukun üstünlüğünü, uluslararası hukuk ilkelerini ve demokrasiyi kuvvetlendirmek ve desteklemek,

• BM Antlaşması'nın amaç ve ilkelerine, Helsinki Nihai Senedi ilkelerine ve dış sınırlarla ilgili olanlarda dahil Paris Şartı'nın amaçlarına uygun olarak, barışı korumak, çatışmaları önlemek ve uluslararası güvenliği güçlendirmek,

• Öncelikli olarak yoksulluğun ortadan kaldırılması amacıyla, gelişmekte olan ülkelerin sürdürülebilir ekonomik, sosyal ve çevresel kalkınmasını desteklemek,

• Uluslararası ticaret üzerindeki kısıtlamaların kaldırılması da dâhil, tüm ülkelerin dünya ekonomisi ile bütünleşmesini teşvik etmek,

• Sürdürülebilir kalkınmayı sağlamak amacıyla, çevre kalitesinin ve küresel doğa kaynaklarının sürdürülebilir yönetiminin muhafaza edilmesi ve iyileştirilmesi için uluslararası tedbirlerin geliştirilmesine katkıda bulunmak,

• Doğal ve insan kaynaklı afetlere maruz kalan halklara, ülkelere ve bölgelere yardım etmek,

• Daha güçlü çok taraflı işbirliğine ve küresel iyi yönetişime dayanan bir uluslararası sistemi desteklemektir.

ODGP'nin yukarıda belirtilen amaçları siber uzayın öneminin ve kullanımının artmasıyla birlikte belli noktalarda başarısız olmuştur. Çünkü süreci yönetmek, risk ve tehditleri ölçebilmek, sorunlara çözüm getirebilmek geleneksel düzeydeki gibi olmamıştır. Beşinci boyut olarak ortaya çıkan siber uzay ile birlikte sanal sınırlar, sanal mülkiyet ve kullanım hakları, sanal yetkiler, kısıtlamalar, sanal alanın güvenliği, işbirliği gibi konuların muhatapsız kalmasına yol açmıştır.

Sonuç olarak; güvenlik teorileri kapsamında kurumsal zemine oturtulan Avrupa'nın güvenlik olgusu siber uzayda aynı şekilde şekillenmemektedir. Özellikle şuana kadar ilan edilen strateji belgelerinde belirtilen roller ve sorumluluklar ile ağ ve bilgi güvenliği hiyerarşik ve sıralı şekilde ilerleyememektedir. Bu yüzden ilan edilen strateji belgeleri rehber görevi görmekten başka bir işe yaramamaktadır.

Siber güvenlik konusunun çok önem verilmesi ve yatırım yapılması gereken bir alan olduğu açıktır. Çünkü siber saldırılar engellenememektedir. ODGP kapsamında siber güvenlik ve ENISA tek çatı altında tüm üye ülkelerin katılımıyla ortak politikalar geliştirirse güç kazanacaktır. Şuana kadar gerçekleştirilen uygulamalar siber uzayın güvenlik yapısının kurumsallaşmasında beklenen seviyeye ulaşılmasını engellemiştir. Çünkü tüm üye ülkeler arasında belirgin bir işbirliği yoktur. Kurumsal bir zemine oturtulamayan böyle bir durumda da

ENISA veya bir diğer kuruma sorumluluk yüklenememektedir.

Siber Diplomasi Örneği ve Avrupa Birliği

Uluslararası ilişkilerde dijital teknolojilerin kullanımının artmasıyla birlikte siber uzay önemli bir boyut olmaya başlamıştır. Bu boyutta işbirliği veya çatışmaya yönelik gelişen ilişkiler siber diplomasinin artan önemini ortaya koymaktadır. Bu çerçevede Avrupa'da siber uzayda diplomatik faaliyet göstermeye başlamıştır. Siber uzay ortamında başta Almanya, Fransa ve İngiltere olmak üzere bir dizi Avrupa ülkesi aktiftir. Aynı zamanda topluluk olarak 2013 tarihinde siber güvenlik stratejisini ilan etmiştir. 2015 yılında ise siber diplomasi adı altında bir kılavuz geliştirmiştir.

Avrupa Birliği yayınladığı bu kılavuzda beş ana eylem alanı tanımlanmıştır. Kılavuzda belirlenen bu beş eylem alanı şu şekildedir; siber uzayda insan haklarının geliştirilmesi ve korunması; uluslararası güvenlik alanında mevcut uluslararası hukukun davranış normları ve uygulaması; internet yönetişimi; rekabet gücünün ve refahın artırılması; kapasite oluşturma ve geliştirmedir. Bu hedeflere ulaşmak için Avrupa Birliği, özellikle siber konularda yapılandırılmış diyaloglar kurarak bir dizi ülkeyle işbirliğini derinleştirmiştir (Renard, 2015).

Ancak yapılan işbirliklerine rağmen, Avrupa Birliği'nin siber diplomasisi yeterince gelişmemiş ve yetersiz kalmaktadır. Rusya ve Çin'den gelen siber saldırı tehditlerine karşı Avrupa Birliği-ABD siber ortaklığı planlanmaktadır. Bu kapsamda, Avrupa Birliği'nin 2013 stratejisinde öne çıkan ortağı ABD'dir. İlerleyen yıllarda da siber uzayda stratejik ortaklık görüntüsü devam etmiştir.

ABD gibi birliğe üye olmayan ülkelerle siber alanda stratejik ortaklık faaliyetleri yürütmeye çalışan Avrupa Birliği, önemi ve kullanımı giderek artan siber ortama yönelik siber güvenlik politikaları geliştirmektedir. Fakat ulusal aktörlerden Avrupa Birliği'nin en büyük farkı siber casusluk geliştirememesi ve diplomatik ajanlarının olmamasıdır. Bu sebeple Avrupa Birliği'nin siber meselelerde dezavantajlarının bulunduğunu rahatlıkla söyleyebiliriz. Yine de, küresel siyasette siber meseleler giderek daha merkezi haline geldiğinden Avrupa Birliği bu alana odaklanmak zorundadır.

Bir diğer yandan Avrupa Birliği ülkesi olan Estonya'ya yönelik gerçekleşen siber saldırılarda Avrupa Birliği birlik olarak bir destek sağlayamamıştır. Bu doğrultuda verilen destekler diplomatik olarak sadece söylem niteliğinde kalmıştır. Üyelerinin uğradıkları siber saldırılara karşı teknolojik bir destek verememiş olması, oluşturulan Avrupa Birliği Siber Suçlar Sözleşmesinin tam anlamıyla işleyememesi, Rusya ve Çin arasında siber uzaya yönelik işbirliklerinin gelişmesi ve son olarak ABD-Çin siber anlaşmalarının imzalanması Avrupa Birliği'nin siber

dünyadaki geleceği için çok önemli tehditlerdir. Bu sebeple AB küresel sistemde kenarda kalmayı göze almayacaksa aktif bir siber güvenlik stratejisi geliştirmek zorundadır.

AB'nin aktif bir politika geliştirmek istemesinin en güzel örneği ise 8-9 Temmuz 2016'da Varşova'da düzenlenen NATO zirvesidir. Bu zirvede, İttifak'ın siber uzaydaki faaliyetlerine ilişkin konulara özel siber savunma taahhüdü oluşturuldu. Ayrıca Avrupa Konseyi Başkanı ve NATO Genel Sekreteri tarafından imzalanan ortak bildiri ile birlikte Avrupa Birliği ile siber savunmada işbirliğini genişletme kararı alındı (Karasev, 2016).

Tüm bu anlatılanlar ışığında rahatlıkla söylenebilecek en doğru şey Avrupa Birliği'nin gerçekleştirdiği siber güvenlik anlaşmaları ile birlikte oluşturduğu yasal süreçler bize AB'nin küresel düzen içerisinde iyi bir siber diplomasi örneği sergilediğini göstermektedir. Fakat bu yeterli düzeyde değildir. Bu yüzden Avrupa Birliği hem ikili hem de çok taraflı düzeylerde siber gündemi aktif bir şekilde şekillendirmeye çalışmalıdır.

Avrupa Birliği Siber Tehditlerle Nasıl Başa Çıkıyor?

ENISA'nın Siber Rolleri ve Sorumlulukları

Dijitalleşmenin hızla gelişmesiyle birlikte sadece devletler ve kurumlar değil AB gibi uluslar üstü yapılanmalarda siber saldırılarla profesyonel bir şekilde mücadele konusunda çalışmalar başlatmıştır. Bu mücadele çerçevesinde nitelikli insan geliştirmek için bütçeler oluşturmuş ve eğitim programları belirlemiştir. Bu doğrultuda tüm bu faaliyetleri gerçekleştirebilmek için ulusal düzeyde olduğu gibi AB düzeyinde de siber güvenlik ile ilgili birçok aktör oluşturulmuştur. ENISA, EUROPOL ve EDA gibi kolluk ve savunma ajansları arasında koordinasyon ve işbirliği siber güvenlik konusunda pratik çözümler sunmak için gereklidir. Çünkü sanal dünyayı analiz etmek için ülkelerin genel prensipleri, ulusal askeri stratejileri, ekonomik ve teknolojik yapıları, siber araç ve tekniklerin kullanılmasının izlenmesi gibi kriterler belirleyici rol oynamaktadır. ENISA da tam bu süreçte önem kazanmaktadır.

ENISA, ABD'nin en güçlü ve iyi finanse edilen siber ajansı olan CYBERCOM'a eşdeğerdir. ENISA'nın misyonu enerji endüstrisi, sigorta şirketi mühendisliği, havacılık, savunma ve uzay endüstrisi gibi temel konularda bir Ağ ve Bilgi kültürü geliştirmeyi hedeflemektedir. Bu doğrultuda AB üye devletlerinin desteğiyle Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) ve Ortak Araştırma Merkezi (JRC) tarafından Kritik Bilgi Altyapılarının Korunması amacıyla 2010 yılında ilk siber Avrupa raporu yayınlanmıştır (European Network and Information Security Agency, 2011).

2010 yılında gerçekleşen ilk siber Avrupa raporu ile birlikte Cyber Euro-

pe 2010 tatbikatı gerçekleştirilmiştir. Avrupa ülkelerinden bu tatbikat için gelen uzmanlar ve bilgisayar korsanları internet kullanılarak Avrupa çapında kritik çevrimiçi hizmetlerin felç edilme ihtimaline karşı simüle edilmiş araçlarla birlikte çalıştılar(SecurityWeek News, 2011). Simülasyon alıştırması hayali bir senaryoya dayanan bu tatbikatın amacı, Avrupa'daki ülkeler arasında büyük ölçekli saldırılara yanıt vermeye çalışmak, güvenlik risklerini azaltmak ve akıllı telefon kullanma fırsatlarını arttırmak için iletişim ve işbirliğini tetiklemekti. 2010 yılında başlayan bu tetikleme çabası hala devam etmekle birlikte tam anlamıyla bir sonuca ulaşamamıştır.

Bir diğer yandan Avrupa Birliği, siber suçlar, siber tehditler ve siber güvenlik gibi kavramların kapsamında sınırlandırmalara giderek Avrupa Polis Teşkilatı (EUROPOL) ve Avrupa Ağı ve Bilgi Güvenliğinin oluşturulması Ajansı (ENISA) hakkında çok sayıda karar yayınladı.

Yayınlanan bu kararlar doğrultusunda ENISA; ağ ve bilgi güvenliğine yönelik ortaya çıkan problemleri önlemek, ele almak, yanıt vermek, farkındalık yaratmak, güvenli uygulamaları teşvik etmek, bölgesel CERT'lerle çalışmaları önermek ve bölgeye karşı kapsamlı bir savunma sağlamak gibi faaliyetler yürütmektedir.

ENISA'nın faaliyetlerinin çıkış noktasını ise kullanıcıların cihazlarla ilgili olası sorunlardaki farkındalık eksikliği, teknolojik ve güvenlik standartlarının yokluğu, operasyon eksikliği, endüstriyel tesisler ve BT altyapılarının güvensiz alt yapısı, artan bağlantı nedeniyle güvenlik sorunlarının farkında olunamama endişesi ve yeterli beceriye sahip olan figürlerin eksikliği gibi konular oluşturmaktadır.

Dolayısıyla Avrupa Birliği Siber Güvenlik Ajansı (ENISA), 2004'ten beri Avrupa'nın siber güvenliğini sağlamak, siber güvenlik yeteneklerini geliştirmek, üye devletlere tavsiye ve çözüm sunmak, diğer paydaşlarla yakın işbirliği içinde çalışmak gibi görevler üstlenmektedir. Ayrıca, yeni teknolojilerle siber saldırılara karşı daha savunmasız olunmasından dolayı büyük ölçekli sınır ötesi siber güvenlik olaylarına veya krizlerine işbirliğine dayalı bir uygulama geliştirmek amacıyla Mayıs 2019'dan beri siber güvenlik sertifikasyon programları hazırlamaktadır.

Gerekli işbirliklerini teşvik etmek ve ilgili tehdit ve risklerin farkındalığını arttırmak için Avrupa Birliği genelinde siber güvenliğe yatırım yapmanın önemi her geçen gün artmaktadır. Zaten sertifikasyon sürecinin oluşturulması da bu yüzdendir. Fakat süreç karmaşık bir şekilde ilerlemektedir. Bu karmaşıklık içinde ENISA Çekirdek Operasyonlar Bölüm Başkanı Steve Purser'ın sözleri süreci açıklayan güzel bir örnektir. Steve Purser'a göre "Endüstri 4.0 çerçevesinde öngörülen gelişmiş dijitalleşme, endüstrilerin fiziksel ve dijital dünya arasındaki sı-

nırları işleme ve bulanıklaştırma biçiminde bir paradigma değişikliğidir." (Enisa, 2018).

Şimdilerde de 5G ağlarının güvenliğindeki zorluklara genel bir bakış sunan ENISA, siber uzaydaki tehdit ortamı üzerine çalışmalarına devam etmektedir. Bu çalışmalar özelinde kapsamlı bir 5G mimarisinin oluşturulması için tehditler ve varlık haritalaması şeklinde gerçekleştirmektedir (Enisa, 2019).

Tüm bu anlatılanlardan da anlaşıldığı üzere siber güvenliğin işbirliği çerçevesinde oluşturulabilmesi için ortak güvenlik standartlarının oluşturulması gereklidir. Bu kapsamda ENISA siber güvenlik için teknik standartların mevcut parçalanmasını aşmada bir önceliktir(Enisa, 2009). ENISA'nın bu öncelikli konumu 2004'te Avrupa Konseyi'nin onayladığı tek bağlayıcı uluslararası mevzuat olan siber suçlar sözleşmesi çerçevesinde gerçekleşmektedir. Bu sözleşme, siber suçun suçluğunu tanımlar, kolluk kuvvetlerini görevlendirir. Sözleşmeyi desteklemek için Avrupa Konseyi, kolluk kuvvetlerinin eğitimi ve ulusal mevzuatın iyileştirilmesi şeklinde iki farklı eylem planı uygulamaktadır. Fakat bu uygulamalar üye devletler üzerinde bir baskı ya da zorunluluk yaratmamaktadır.

NIS İşbirliği Grubu

Avrupa Birliği direktifleri, üye ülkelerin mevcut organizasyon yapılarını yeniden kullanmanın veya mevcut ulusal mevzuata uyum sağlamanın gereğini belirtir. Bu kapsamda; AB'nin siber güvenliği sağlamaya yönelik ilk yasal düzenlemesi 2016 yılında kabul edilen NIS direktifidir.

2018 yılı itibariyle AB üye ülkeleri tarafından ulusal aktarımın tamamlandığı NIS işbirliği grubu, NIS direktifinin AB genelinde tutarlı bir şekilde nasıl uygulanacağı konusunda anlaştıkları stratejik işbirliği grubu haline gelmiştir. Bu işbirliği çerçevesinde AB CSIRT ağına stratejik yön vermeyi hedeflemektedir (European Union Agency For Cybersecurity, 2021).

Ayrıca, NIS direktifi kapsamındaki ENISA faaliyetleri büyük önem taşımaktadır. Örneğin; bu direktif çerçevesinde ENISA, AB üye ülkeleri ile birlikte üç yönerge geliştirmiştir. Bunlar; olay bildirimleri, DSP'ler için güvenlik gereksinimleri ve OES güvenlik gereksinimlerinin belirli sektörlerle eşleştirilmesidir. Ayrıca ENISA, ulusal siber güvenlik stratejileri, AB CSIRT ağı ve siber egzersizler konusunda da aktif görev almaktadır. NIS direktifinin bu üç bölümünü kısaca açıkladığımızda şu noktaları belirtmemiz gerekmektedir.

1. Ulusal yetenekler: AB üye devletleri ulusal siber güvenlik yeteneklerine sahip olmalı ve siber tatbikatlar gerçekleştirmelidir.
2. Sınır ötesi işbirliği: AB ülkeleri arasında operasyonel AB CSIRT ağı veya stratejik NIS işbirliği grubu şeklinde sınır ötesi işbirliği olmalıdır.

3. Kritik sektörlerin ulusal denetimi: AB üye devletleri, kritik sektörlerde (enerji, ulaşım, su, sağlık, dijital altyapı ve finans sektörü), ex-post denetim kritik dijital hizmet sağlayıcılar için denetim (çevrimiçi pazar yerleri, bulut ve çevrimiçi arama motorları) de kendi siber güvenliğini denetlemek zorundadır.

NIS direktifinin bu üç bölümünün düzgün işlemesi çok önemlidir. Çünkü COVID-19 pandemisinin patlak vermesi ve dijital araçların yaygın olarak kullanılmasının ardından, internet güvenliği ve siber suçların artmasıyla birlikte verilerin kötüye kullanılması veya dolandırıcılığın önlenmesi Avrupa özelinde büyük önem taşımıştır. Bu doğrultuda Kimlik avı ve pharming, yaşanan en yaygın güvenlikle ilgili sorunlardır. Bu sorunlar Avrupa'nın 28 Üye Devleti'nin dijital performansına ilişkin 24 veri seti kullanan Dijital Ekonomi ve Toplum Endeksi (DESI)'nde belirtilmiştir. Bu endekste de belirtildiği üzere 2019'da AB internet kullanıcılarının %30'u dolandırıcılık mesajları ile karşılaşmıştır. İnternet kullanan AB vatandaşlarının %39'u güvenlikle ilgili sorunlar yaşamıştır. Fakat yaşanan bu güvenlik sorunları üye devletlerarasında farklılık göstermektedir. Örneğin; o dönemde birliğe üye olan Birleşik Krallık'ta %50'den fazla iken Litvanya'da %10'dan daha azdır. (European Commission, 2020).

Sonuç olarak; bu çeşitlilik sürecin zorluğunu ortaya çıkarmaktadır. Bu zorluğun önüne geçilebilmesi içinde cezalar ve yaptırımlar ortaya konulmalıdır(Eurupean Council, 2021). Bu çerçevede Mayıs 2019'da Konsey, AB'ye veya üye devletlerine dış tehdit oluşturan siber saldırıları caydırmak ve bunlara yanıt vermek için AB'nin hedefli yaptırımlar uygulamasına izin veren bir çerçeve oluşturdu. Bu adım siber uzaya yönelik kurumsallaşma ve ortaklığı pekiştirme yönünde önemli bir dönemeç olmuştur. Çünkü AB; ilk kez siber saldırılardan veya siber saldırı teşebbüslerinden sorumlu olan, bu tür saldırılara mali, teknik veya maddi destek sağlayan veya başka şekillerde yer alan kişi veya kuruluşlara yaptırım uygulamasına izin vermiştir. Sonrasındaysa siber saldırılar için ilk yaptırımlar 30 Temmuz 2020'de uygulandı. Özellikle uygulama aşamasına geçen bu süreç NIS işbirliği sürecinin olumlu geliştiğini ama alınacak daha çok yolun olduğunu bize göstermektedir.

Çok Uluslu AB Siber Sistem Yapısı Bakımından Kurumsal Yenilikler ve JRC

Avrupa Birliği dünyadaki tek uluslar üstü topluluktur. Uluslararası ilişkilerde bu şekilde sembolik önemi olan Avrupa Birliği üzerine gerçekleştirilecek bir siber saldırı üye ülkelere ciddi zararlar verebilir. Bu yüzden Avrupa Birliği, üye ülkelerinin siber güvenliklerinin sağlanmasında teknolojiyi yaygınlaştırmaya yönelik ortak bir strateji geliştirmek istemektedir. Stratejik bu hedef doğrultusunda Ortak Araştırma Merkezi (JRC) ön plana

çıkmaktadır. Böylece ülkeye ve türe göre belirlenmiş siber güvenlik atlası yaratılarak ülkeler incelenmeye başlanmıştır. Aslına bakılırsa AB, ABD'den sonra siber güvenlik konusunda yayın yapılması konusunda bu alana öncülük etmektedir. AB özelinde gerçekleştirilen yayınların çoğu ise güvenlik yönetimi, ağ güvenliği, veri güvenliği ve gizliliği ile kriptoloji olmak üzere dört ana temel başlık özelinde yapılmaktadır.

Bu temel başlıklar altında Interpol, Europol ve Eurojust'ın çok önemli çalışmaları bulunmaktadır. Örneğin, EUROPOL tarafından Yüksek Teknolojili Suçlar Merkezi (High Tech Crime Centre) ve Avrupa Siber Suç Timi (European Cybercrime Task Force-EUCTF) adı altında çeşitli platformlar oluşturulmuştur. Bu platformların kurulmasındaki amaç, siber uzayda yaşanacak suçlarla mücadelede AB içinde işbirliğini arttırmak ve ortaya çıkan sorunlara çözüm bulmaktır (Europol Review, 2011).

Bu sorunlara cevap bulunması amacıyla Avrupa Komisyonu bünyesinde Ortak Araştırma Merkezi (JRC) oluşturulmuştur. JRC, AB politikalarının temelini oluşturacak fikirlerin üretilmesi, bu politikaların uygulanması, geliştirilmesi ve izlenmesi süreçlerine destek vermektedir. Özellikle telekomünikasyon, gaz, petrol ve yakıt tedariki gibi belirleyici ve kritik altyapı sistemleri bu ortak merkez tarafından siber uzayı içerecek şekilde bilim ve teknoloji konularında yeniden düzenlenmelidir (The European Commission's Science And Knowledge Service, 2016). Bu düzenlemeden sonra JRC birliğin tamamı için bir referans noktası görevi üstelenecektir.

Bir diğer yandan sembolik bir öneme sahip olan Ortak Araştırma Merkezi (JRC), siber saldırılara yönelik ciddi bir hedef olabilir. Bu doğrultuda 2020 yılında Avrupa Komisyonu'nun bilim ve bilgi hizmeti olan Ortak Araştırma Merkezi'nin (JRC) tarafından yayınlanan raporda son 40 yılda siber güvenliğin büyümesine dair çok boyutlu iç görüler sağlanmış, mevcut dijital evrimdeki zayıflıkları ve bunların Avrupa vatandaşları üzerindeki etkileri üzerinde durulmuştur (The Publication of Europen Commission, 2020).

Ayrıca Ortak Araştırma Merkezi (JRC), AB'de siber güvenliğe aktif olarak katkıda bulunmak amacıyla "Siber Güvenlik Sınıflandırması" geliştirmiştir (European Commission's Science And Knowledge Service, 2021). Böylece, siber güvenlikte kullanılan terminolojiyi uyumlu hale getirerek AB'deki siber güvenlik yeteneklerine daha net bir genel bakış oluşturmak hedeflenmiştir. Bu sebeple bu rapor aynı zamanda AB'nin siber güvenlik manzarasına yönelikte önemli bir manzara ortaya koymuştur.

Mevcut durumda siber güvenliği sağlamak üyelerin kendi sorumluluğundadır. AB Komisyonu, siber saldı-

rılara karşı ortak mücadele gerçekleştirmek amacıyla "Ortak Siber Birim" kurulmasını teklif etti (Şeker, 2021). Bu teklife göre, oluşturulacak yeni birim sayesinde kitlesel siber saldırı ve krizler etkili bir şekilde önlenebilecek, tehditler caydırılabilecek ve siber saldırılara yanıt verilebilecektir. Bunun sağlanması amacıyla da AB üye ülkelerinin mevcut kaynaklarının ve uzmanlıklarının bir araya getirilmesi planlanmaktadır. Böylece üye ülkeler birbirlerine yardım sağlayabilecektir. 2023 yılına kadar ortak siber birimin faaliyete geçmesi hedeflenmektedir. Fakat AB Komisyonun yapması gereken yatırımlar yerine getirilmemiştir. Ayrıca söz konusu birimin kurulması için AB üyeleri de onay vermemiştir.

Sonuç

Her yeni teknoloji uluslararası ilişkiler sisteminde rol oynayan tüm aktörler üzerinde ciddi etkiye sahiptir. Özellikle en önemli aktör olan devletler ve belirleyici rol görevi üstlenen kurumlar bu süreçten daha da fazla etkilenmektedir. Dijitalleşmenin öneminin hızla artmasıyla birlikte Avrupa Birliği'nin de kurumsal olarak siber uzaya yönelimi artmaktadır.

Avrupa Birliği'nin günümüzde siber uzaya yönelik artan eğilimi geçmiş güvenlik yaklaşımlarından ayrı tutulamaz. Bu yüzden Avrupa Birliği'nin şu anki kurumsal yapıya ulaşmasında Avrupa'nın geçmişinde yaşadığı güvenlik riskleri ve Avrupa'da gerçekleşen savaşlar etkili olmuştur. Özellikle var olan tehditlerin şekil değiştirmesi ve teknolojik değişimlerin yıkımlarının etkisini arttırması kurumsallaşma sürecini zorlamıştır.

Yukarıda da belirtildiği gibi Avrupa'nın birlik olmasında geçmiş güvenlik yaklaşımları çok önemlidir. Günümüzde de siber uzayda yaşanan risk ve tehditler bu birliğin siber uzayda da güçlenmesini zorunlu kılmaktadır. Bu doğrultuda Avrupa Birliğine üye tüm devletlerin ortak olarak yürütmeye çalıştıkları eğitim sistemi, sağlık, ulaşım, savunma vb. her alan gibi bütünleşme sürecine siber boyutta katılmıştır.

Bu bütünleşme süreci içerisinde Avrupa Birliği dijitalleşmenin ortaya çıkardığı siber risklere karşı şuana kadar birçok hukuki ve kurumsal düzenlemeler gerçekleştirmiş olsa da sorunlara yönelik bir çözüm getirememiştir. Avrupa Birliği'nin hem hukuki hem de kurumsal anlamda ortaya çıkan bu başarısızlığının devam etmesinden dolayı üye devletler kendi siber güvenliklerini sağlama ihtiyacına yönelmiştir. Bu durum kurumsal düzlemde olması gereken siber güvenlik risklerini azaltma ve bu risklerden korunma ihtiyacını bireysel olarak gerçekleştirmeyi ön plana çıkarmaktadır. Bu yüzden Avrupa Birliği'ne üye ülkelere yönelik gerçekleşen siber saldırılara karşı saldırıya uğrayan ülkeler kendi güvenliklerini sağlama amacıyla bireyselliğe yönelmektedir.

Artan bireysellik siber uzayda Avrupa'nın güvenliğini ortak olarak sağlamaya yönelik bütünleşme sürecini zayıflatmakta ve ODGP'den uzaklaştırmaktadır. Bu uzaklaşma birliğin güvenliği sağlama sürecini zayıflattığından üye ülkelere yönelik gerçekleşen siber casuslukları ve internet üzerinden gerçekleşen dolandırıcılıkları arttırdı.

Aynı zamanda hızlanan dijitalleşme süreci AB'ye üye tüm işletmeler ve kurumlar için siber risk ve tehditlere olan hassasiyeti arttırmaktadır. Bu konu bir var olma ve sürdürülebilirlik sorunu olduğu için stratejik planlama ve yönetim süreçlerinin en önemli konusu haline gelmelidir. AB tarafından kurumsal düzeyde siber uzaya yönelik oluşturulan kurumlar ve gerçekleştirilen düzenlemeler yeterli değildir. Bu sebeple ülkeler arasındaki siber bütünleşme arttırılmalı ve birliğin siber gücü arttırılmalıdır. Böylece siber uzayda güvenliğin sağlanması daha kolay hale gelecektir.

Ayrıca bilgi teknolojilerine ve güvenlik sistemlerine yatırımların arttığı 21. yüzyılda Avrupa Birliği uluslararası ilişkilerde sorunları çözücü, uluslar üstü bir otorite olarak faaliyet sürdürmek istiyorsa güvenlik ve savunma politikalarının merkezine siber uzayı almak zorundadır. Özellikle kurumlarını bu yönde dönüştürülmeli kanunlarını bu yönde oluşturulmalıdır.

Avrupa Konseyi, ulusal siber suçların ilerlemesi hakkında kanıt ortaya koymak için geniş bir veri tabanı tutarak nitel veriler sağlamaktadır. Böylece niceliksel analiz için gerekli istatistikleri sağlamaktadır. Ancak, siber ortamda nesnel olarak suçu belirlemek zordur. Uluslararası mevzuat da genellikle tepkisel olmakla birlikte genellikle teknolojik çabaların gerisindedir. Dolayısıyla, sözleşme hükümlerinin ulusal siber suç mevzuatının yasal çerçevesine uyarlanması belirsizliğini korumaktadır.

Sonuç olarak; uluslararası anarşik yapı içerisindeki rakipler arasındaki güç mücadelesinin savaşa dönüşmesi yerine işbirlikçi bir temelle çözülebilmesi için üyeler arasında bütünleşmenin siber uzayda da sağlanması gerekmektedir. Bütünleşmenin olumsuz etkilendiği durumlarda siber güvenlik alanında bilgi paylaşımının hızını arttırmak ve tehditleri bertaraf etmek için gerçekleştirilmesi beklenen kurumsal çabalardan bazıları şunlardır;

Büyük bir şemsiye ağ ile özerk kuruluşlar arasındaki tehditler için uyum sağlanmalı,

Siber tehditlere odaklanmak için tasarlanmış kar amacı gütmeyen kuruluşlar (CERT / CC, FIRST ve özel CERT'ler) arttırılmalı,

Gelişmiş devletlerarasındaki etkileşimleri yönetmek için AB çatısı altında kurulmuş bir dizi uluslararası kurumun çabaları bu süreci pekiştirir.

Bilgi teknolojisi potansiyelini ilerletmek için tasarlanmış uluslararası konferanslar küresel olarak siber sorunların siyasi profilini yükselterek sürdürülebilir kalkınmayı kolaylaştırır.

Ulusal düzeyde yaşanan karmaşık ve koordinasyonsuz yanıtlara rağmen, içyapılar aktörler daha fazla yetkilendirilmiştir. Belirli kurumlar siber suçlara yanıt vermekle daha fazla görev almalıdır (ENISA vb.).

AB üyelerini bağlayıcı uluslararası mevzuatın geliştirilmesi (Siber Suç Sözleşmesi) kırılganlık duygusunu, farkındalık düzeyini ve yanıtları koordine etme ihtiyacını artırır.

Daha resmi çerçeveli askeri ve istihbarat ağlarının savunmasına odaklanan siber stratejiler (ör. ODGP) geliştirilmelidir.

AB'nin siber uzayda bütünleşmesini sağlayarak kurumsal anlamda güvenliğini sağlama amacıyla ortaya koyacağı kurumsal çabalar bazı temel sonuçlar doğurur. Bunlar;

Bilgi teknolojisi uluslararası toplumun politika önceliklerinde olan ve sürdürülebilir kalkınma bağlantısının ayrılmaz bir parçasıdır.

Mevcut kurumsal manzara, tehditlere karşı kritik öneme sahip bir güvenliğin sağlanması için tüm siber kaynakları kapsayan bir şemsiye olmalıdır.

Birden fazla bağlam ve çeşitli kurumsal motivasyonlar göz önüne alındığında oluşabilecek siber krize karşı tepkiler koordineli ve proaktif yanıt yoluyla gerçekleşmelidir.

Tüm kalkınma düzeylerindeki karmaşık küresel gündem nedeniyle, uluslararası siber normların geliştirilmesinde devletler istekli değildir.

Kamu, özel ve gönüllü kuruluşlar arasında sektörler arası işbirliği mevcut savunma ağındaki delikleri kapatmak için geçici bir önlem olarak hizmet etmektedir.

Dijitalleşme ve İnternet'in kullanımı giderek arttıkça kurumsal bu modeldeki sonuçların aynı şekilde devam etmesi beklenemez.

Referanslar

Akşemsettinoğlu, G. (2011). Avrupa Bütünleşme Projesinin ve Genişleme Sürecinin Değişen Dinamikleri, Avrupa Çalışmaları Dergisi, 10(1), (ss.1-18).

Aliusta, C ve Benzer, R. (2018) Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 4(2), (ss.35-42)

Archick, K. (2006 5 28)"Cybercrime: The Council of Europe Convention", CRS Report for Congress

Akdemir, E. (2018). Avrupa Birliği'nin Dış İlişkileri ve Politikası: Avrupa Bir-

liği'nin Bütünleş(Eme)Mesi Üzerine Bir İnceleme, Ankara Avrupa Çalışmaları Dergisi, 17(2), (ss.181-218).

Amos, J.(2014) Horizon 2020: UK Launch forEU.2, BBC News, Shttps://www.bbc.com/news/science-environment-25961243 adresinden alındı.

Aliusta, C. ve Benzer, R. (2018). Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 4(2), (ss.35-42).

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

Bakan, S. ve Şahin, S. (2018). Uluslararası Güvenlik Yaklaşımlarının Tarihsel Dönüşümü ve Yeni Tehditler. The Journal of International Lingual Social and Educational Sciences, 4(2), (ss.135-152).

Bandyopadhyay, L. (2012). Cyber-Security Threats, Information Warfare and Critical Infrastructure Protection. Global İndia Foundation, 2(2464), (ss.1-14).

Başaran, A. (2017). Yaklaşan felaketin habercileri Siber kıyamet. İstanbul: Arion Yayınları.

Bakanlar Kurulu, (2014 04 22). Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun, Resmi Gazete, http://www.resmigazete.gov.tr/eskiler/2014/05/20140502-12.htm adresinden alındı.

Baysal, B ve Lüleci, Ç. (2011). "Kopenhag Okulu ve Güvenlikleştirme Teorisi", Güvenlik Stratejileri, 22, (ss.61-90).

Bayraktar, G. (2015). Siber Savaş ve Ulusal Güvenlik Stratejisi. İstanbul: Yeyniyüzyıl Yayınları.

Canbolat, İ. S. (2002). Avrupa Birliği, Uluslar üstü Bir Sistemin Tarihsel Teorik Kurumsal Jeopolitik Analizi ve Genişleme Sürecinde Türkiye ile İlişkiler, 3. Baskı, Alfa Basım, (s.109).

Christou, G. (2016), Cybersecurity İn The European Union Resilience And Adaptability İn Governance Policy, Palgrave Macmillian, England, (ss.119-142).

CERT-EU, (2020). CERT-EU Responsible Disclosure Policy, CERT-EU, https://cert.europa.eu/cert/newsletter/en/latest_HallOfFame_.html#CERT-policy. adresinden alındı.

Council of Europe, (2001). Convention on Cybercrime, European TreatySeries,185(11), https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561. adresinden alındı.

Cross, M. K. D. (2011), Security İntegration In Europe How Knowledge Based Networks Are Transforming The

European Union, Michiagen University Press.

Cisco, Annual Cybersecurity Report, February 2018, https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf. adresinden alındı.

Çakır, A. E. (1996). The External Envıronment Of The European Polıtıcal Integratıon: Desıgnıng The Settıng Of The Play Odyssey. Öneri Dergisi, 1 (4) , (ss.169-176).

Çiftçi, S. (2005). "Treaties, Collective Responses and the Determinants of Aggregate Support for European Integration", European Union Politics, 6(4), (s.475).

Çifçi, H. (2013). Her Yönüyle Siber Savaş. Ankara: Tübitak Yayınları.

Dedeoğlu, B. (2005). Dünden Bugüne Avrupa Birliği, İstanbul, Boyut Yayınları.

Dedeoğlu, B. (2003). Uluslararası Güvenlik ve Strateji (İstanbul: Derin Yayınları.

Efe, H. (2008), Avrupa Birliği'nin Ortak Dış ve Güvenlik Politikası, Gaziantep Üniversitesi Sosyal Bilimler Dergisi Cilt 7 Sayı 1, (ss.66-78).

Enisa,(2009). Industry 4.0 Cybersecurıty: Challenges and Recommendatıons, The EU Agency For Cybersecurıty, https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations/at_download/fullReport

Enisa, (2019). Enisa Threat Landscape for 5G Networks, ENISA, https://www.enisa.europa.eu/publications/ adresinden alındı.

Enisa, (2020). Threat Landscape For 5G Networks, Europen Commission, The Report Cyber security Our digital anchor a european perspective, https://op.europa.eu/en/publication-detail/-/publication/a5e2b2af-dab3-11ea-adf7-01aa75ed71a1/language-en adresinden alındı.

Enisa, (2018 11 19). Cybersecurity Is A Key Enabler For Industry 4.0 Adoption, Enisa News, https://www.enisa.europa.eu/news/enisa-news/cybersecurity-is-a-key-enabler-for-industry-4-0-adoption adresinden alındı.

Eurupean Council, Council Of The European Union, Timeline Cybersecurity, https://www.consilium.europa.eu/en/policies/cybersecurity/timeline-cybersecurity/ adresinden alındı.

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

European Network and Information Security Agency, (2011). Cyber Europe 2010 Evalution Report, (ss.1-46).

European Commıssıon, (2013, 2 7). Cybersecurity Strategy Of The European Union: An Open, Safe And Secure Cyberspace, Brussels,https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf adresinden alındı

European Union Agency For Cybersecurity, NIS Directive, https://www.enisa.europa.eu/topics/nis-directive adresinden alındı.

European Commission, (2020). The Digital Economy and Society Index (DESI), (ss.95), https://digital-strategy.ec.europa.eu/en/policies/desi adresinden alındı.

European Commission, (2020). Cybersecurıty Our Dıgıtal Anchor A European Perspectıve, (ss.33-40)

Eurupean Council, Council Of The European Union, Cybersecurity: How The EU Tackles Cyber Threats, https://www.consilium.europa.eu/en/policies/cybersecurity/ adresinden alındı.

Europol Review, (2011). General Report on Europol Activities, European Police Office, (s.48). https://www.europol.europa.eu/sites/default/files/documents/en_europolreview.pdf adresinden alındı.

Eren, M. (2017). "Avrupa Birliği'nin Siber Güvenlik Politikası", İstanbul, Beta Yayınları.

Estonia's e-Governance Academy, (2019). 'National Cyber Security Index', https://ncsi.ega.ee. adresinden alındı

Gözkaman, A. (2015). Avrupa Savunma Topluluğu'nun Reddi Üzerine Bir Analiz, Beykent Üniversitesi Sosyal Bilimler Dergisi , 7 (2) , (ss.6-18).

Helena, C. ve Barrinha. A. (2018). "European Union Cyber Security as an Emerging Research and Policy Field", European Politics and Society 19(3) (ss.299-303).

Hiscox. (2019). The Hiscox Cyber Readiness Report 2019. London: Hiscox Insurance.

Hürriyet Gazetesi. (2020, 07 16). Pandemi Döneminde Siber Saldırı Sayısı Arttı. 06 10, 2021 tarihinde Hürriyet: https://www.hurriyet.com.tr/teknoloji/pandemi-doneminde-siber-saldiri-sayisi-artti-41566033 adresinden alındı.

Hürriyet Gazetesi, (2020,07 31) AB İlk Kez Siber Saldırılar Nedeniyle Yaptırım Uygulayacak, https://www.hurriyet.com.tr/teknoloji/ab-ilk-kez-siber-saldirilar-nedeniyle-yaptirim-uygulayacak-41577068, adresinden alındı.

Internet World Stats, Internet User Statistics 2021, Population for the 53 European countries andregions, https://www.internetworldstats.com/stats4.htm adresinden alındı.

Köker, A.E. (2021). Tehdit, Caydırıcılık ve Güvenlik: Çatışma ve Savaş İkileminde Siber Dünya, Urzeni Yayınları

Karasev, P. (2016, 10 13). NATO's Cyber Defense Evolution, Russian Council https://russiancouncil.ru/en/analytics-and-comments/analytics/evolyutsiya-kiberoborony-nato/ adresinden alındı.

Kurnaz, S. ve Önen, S.M. (2019) Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Stratejileri, International Journal of Politics and Security, 1(2), (ss.82-103).

Khan, N. A., Brohi, S. N. ve Zaman, N. (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. TechRxiv, (ss.1-7).

Köksoy, F. (2020). Avrupa Birliği'nin Siber Güvenlik Politikası: Kurumsalcılık mı Tutarlılık mı? Güvenlik Stratejileri Dergisi, 16(35): (ss.635-674).

Mccormıck, J. (2005). Understanding the European Union, A Concise Introduction, New York, Palgrave Macmillan, (ss.1-4)

Mercan, S. S. (2011). Siyasal Bütünleşme Kuramları Işığında AB Genişlemesi. Ankara Avrupa Çalışmaları Dergisi, 10 (1) , (ss.67-83).

Mor, H. (2010). Avrupa (Birliği Bütünleşme Süreci ve Sorunları, Gazi Üniversitesi Hukuk Fakültesi Dergisi, 14(1), (ss.499-541).

Neuman, P.R. (2013), The trouble with radicalization, International Affairs, 89(4), (ss.873-893).

Nicolas, E. S. (2020). Cybercrime Rises During Coronavirus Pandemic. Brussels: EU Observer.

Nye, J. ve Welch, D. Çeviren Akman, R. (2010). Küresel Çatışmayı ve İşbirliğini Anlamak, İstanbul, Türkiye İş Bankası Yayınları.

Ortahamamcilar, B. (2021). İrlanda Sağlık Sistemi Siber Saldırıya Uğradı: Kağıt Dosya Yöntemine Dönüldü, 27.06.2021 tarihinde euronews.: https://tr.euronews.com/2021/05/14/irlanda-sagl-k-sistemi-siber-sald-rya-ugrad-kag-t-dosya-yontemine-donuldu adresinden alındı

Pawlak, P., Tikk, E., ve Kerttunen, M. (2020). Cyber Conflict Uncoded The EU and Conflict Prevention İn Cyberspace. European Union İnstitute For Security Studies. 4(7), (ss.1-8) https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%207_Cyber.pdf. adresinden alındı.

Renard, T. (2015 10 30). US-China Cybersecurity Agreement: A Good Case Of Cyber Diplomacy, Reshaping Europe, http://reshaping-europe.boellblog.org/2015/09/30/us-china-cybersecurity-agreement-a-good-case-of-cyber-diplomacy/ adresinden alındı.

SecurityWeek News, (2011). ENISA Issues Report on 'Cyber Europe 2010' Cyber Security Exercise, https://www.securityweek.com/enisa-issues-report-cyber-europe-2010-cyber-security-exercise, adresinden alındı.

Sağıroğlu, Ş. ve Alkan, M. (2018) Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler, Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık içinde, Grafik Yayınları, (ss.21-45).

Somer, M.D. Tekin, F. ve Meissner, V. Schengen, (2020). Under Pressure: Differentiation or Disintegration? https://euidea.eu/wp-content/uploads/2020/09/euidea_pp_7.pdf adresinden alındı.

Şeker, A.U. AB Ortak Siber Birim Kurmaya Hazırlanıyor, Anadolu Ajansı, 23.06.2021, https://www.aa.com.tr/tr/dunya/ab-ortak-siber-birim-kurmaya-hazirlaniyor/2282716 adresinden alındı.

Şöhret, M. (2013). Avrupa Birliği'nin Güvenlik Yapılanmasının Tarihsel Gelişim Süreci ve Mevcut Durumu. Uşak Üniversitesi Sosyal Bilimler Dergisi, 6 (2), (ss.59-100).

The EU Cybersecurıty Agency, (December 2018). Cyber Europe 2018:After Actıon Report Findings From A Cyber Crisis Exercise İn Europe, (ss.1-14). https://www.enisa.europa.eu/publications/cyber-europe-2018-after-action-report adresinden alındı.

The European Commission's science and knowledge service, European Cybersecurity Taxonomy, https://ec.europa.eu/jrc/en/science-update/european-cybersecurity-taxonomy adresinden alındı.

The European Commission's science and knowledge service, The JRC in Seville, 07.07.2016, https://ec.europa.eu/jrc/en/about/jrc-site/seville adresinden alındı.

Turan, A. P. (2010). Avrupa Birliği Güvenlik Aktörü Olmaya Ne Kadar Yakın?, Bilge Strateji, 2(3): (ss.29-57). https://dergipark.org.tr/tr/pub/bs/issue/3807/51048 adresinden alındı.

Urgancı, B. Bütünleşme Entegrasyon, TUIC Akademi, 04.02.2014, https://www.tuicakademi.org/butunlesme-entegrasyon/ adresinden alındı.

Zıelonka, J. (2008). "Europe as a Global Actor: Empire by Example?", International Affairs, 84(3): (ss.471-484)

Zhussipbek, G. (2009), 2007 Lizbon Antlaşması, Avrupa Güvenlik ve Savunma Politikası Tanımı ve Özellikleri, Güvenlik Aktörü Olarak AB'nin Nitelikleri`, Ankara Avrupa Çalışmaları Dergisi, 8(1): (ss.139–165).