Çankırı Karatekin Üniversitesi
İktisadi ve İdari Bilimler
Fakültesi Dergisi
Y. 2023, Cilt 13, Sayı 2, ss. 482-507

Cankırı Karatekin University
Journal of the Faculty of Economics
and Administrative Sciences
Y. 2023, Volume 13, Issue 2, pp. 482-507

Araştırma Makalesi

AB'nin Siber Güvenlik Alanındaki Politikalarının ve Uygulamalarının Etkinliği: Bir Siber Güvenlik Temsilcisi Olarak AB'nin Yeterliliği

Omca ALTIN
Kastamonu Üniversitesi, İİBF
oaltin@kastamonu.edu.tr, ORCID: 0000-0002-2529-4979

Öz

Bu çalışmada; AB'nin siber güvenlik alanındaki politikaları ve uygulamaları ele alınarak, bu politika ve uygulamaların ne kadar etkin olduğu ve bir siber güvenlik temsilcisi olarak nitelendirilen AB'nin bu alandaki yeterliliği değerlendirilmeye çalışılacaktır. Birlik ve Birlik üye ülkeleri arasındaki ortak vizyon eksikliği ve Birliğin hükûmetler arası karakteri siber güvenlik alanında Birliği sınırlayan iki ana faktör olarak karşımıza çıkmaktadır. Bunlar, Birliğin siber güvenlik stratejisinin uygulanmasını zorlaştırmakta ve bir siber güvenlik temsilcisi olarak siber tehditler karşısında etkili bir duruş sergileyememesine neden olmaktadır. Birliğin siber güvenlik tehditleri karşında etkili bir rol oynayabilmesi için öncelikle AB ekseninde ortak bir siber güvenlik anlayışı yaratması gerekmektedir. Aynı zamanda, üye devletlerin aynı güvenlik topluluğuna ait olmaları ve benzer çıkarlara sahip olmaları sebebiyle aralarında bir bölgesel iş birliği yaratılması ve siber güvenliğe ilişkin ulusal stratejilerinde bir koordinasyon sağlanması önemli olacaktır. Diğer yandan, uluslararası iş birliğini sağlayacak olan kurumsal düzenlemeler ve süreç planlamaları öncelikli hâle getirilmelidir.

Anahtar kelimeler: Avrupa birliği, AB'nin siber güvenlik politikaları ve uygulamaları, siber güvenlik, siber saldırı, siber tehdit.

Jel Sınıflandırma Kodları: D80, F50, K24, O33.

Effectiveness of EU Policies and Practices in the Field of Cyber Security: EU's Competence as a Cyber Security Representative[1]

Abstract

In this study, the EU's policies and practices in the field of cyber security will be discussed, and how effective these policies and practices are and the competence of the EU, which is described as a cyber security representative, in this field will be tried to be evaluated. The lack of a common vision between the Union and the Union's member states and the intergovernmental character of the Union appear as two main factors limiting the Union in the field of cyber security. This situation complicates the implementation of the Union's cyber security strategy, causes it fail to take an effective stance against cyber threats as a cyber security representative. In order for the Union to play an effective role in the face of cyber security threats, it must first create an understanding of cyber security on the axis of the EU. At the same time, since the member states belong to the same security community and have similar interests, it will be important to create a regional cooperation between them and to coordinate their national strategies on cyber security. On the other hand institutional arrangements and process planning that will ensure international cooperation should be prioritized.

Keywords: European union, EU's cyber security policies and practices, cyber security, cyber attack, cyber threat.

JEL Classification Codes: D80, F50, K24, O33

[1] Extended abstract is presented at the end of the article.

Geliş Tarihi (Received): 04.04.2023 – Kabul Edilme Tarihi (Accepted): 05.06.2023

Atıfta bulunmak için / Cite this paper:

Altın, O. (2023). AB'nin siber güvenlik alanındaki politikalarının ve uygulamalarının etkinliği: bir siber güvenlik temsilcisi olarak AB'nin yeterliliği. *Çankırı Karatekin Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *13* (2), 482-507. Doi: 10.18074/ckuiibfd.1276923

1.Giriş

Bilginin değerinin giderek artması ile birlikte içinde bulunduğumuz çağ, bilgi çağı olarak tavsif edilmekte olup, ihtiyaç duyulan bilgiye sürekli gelişim ve dönüşüm gösteren bilgi ve iletişim teknolojileri yardımıyla hızlı ve kolay bir biçimde erişilebilmekte ve bilgi paylaşılabilmektedir. Dolayısıyla, insanlık için tarihin başlangıcından günümüze kadar her dönem son derece önemli olan bilgiye, bilgi ve iletişim teknolojilerinin sağlamış olduğu olanaklarla etkin bir biçimde erişilmesi, bilginin iletilmesi, işlenmesi, muhafaza edilmesi ve kullanılması neticesinde ülkelerin ekonomik, siyasi ve askeri güçlerinin olumlu yönde yükselişi siber ortamın önemini daha fazla artırmaktadır.

Bilgi ve iletişim teknolojilerinde yaşanan gelişmeler doğrultusunda siber ortamın sağladığı olanak ve avantajlar yanında siber ortamın; saldırı, tehdit, zarar verme vb. amaçlarla kullanılması bireylerin, kurumların ve ülkelerin ciddi zarara uğramalarına sebep olmaktadır. Diğer bir ifade ile bilginin günümüzde elektronik bir ortamda bulunması ve saklanması, onu siber saldırılara açık bir hâle getirmekte, dolayısıyla bilgi ve iletişim teknolojilerinin faydalarından daha çok siber saldırılar üzerine odaklanılmaktadır. Dolayısıyla, bu durum siber güvenliği oldukça önemli bir konu hâline getirmekte, bilgi ve iletişim sistemlerinin siber saldırılardan korunmasının diğer deyişle siber güvenliğin sağlanmasının yolları aranmaktadır. Bu doğrultuda, ülkeler tarafından bilgi ve verilerin güvenliğinin sağlanması amacıyla etkin bir siber güvenlik stratejisi, politikası geliştirilmesi zorunlu bir hâle gelmektedir. Diğer taraftan, AB de siber güvenliğin sağlanması hususunda çeşitli stratejiler ve politikalar geliştirmeye çalışan bir aktördür.

AB, 1985'de Avrupa Komisyonu tarafından yaratılan, siber güvenlik politikasındaki çalışmalarının başlangıç noktası olan "Tek Pazar İnsiyatifi"nden günümüze kadar ekonomik açıdan faydanın sağlanması, temel hakların korunması, siber saldırıların engellenmesi, dijital sistemlere duyulan güvenin artırılması ve aktörler arasındaki iş birliğinin daha da güçlü bir hâle getirilmesi gibi hedefler kapsamında sosyo-ekonomik odaklı siber güvenlik stratejileri ve politikaları geliştirmektedir. Siber güvenliğin sağlanması noktasında çeşitli stratejiler ve politikalar geliştiren AB'nin bunun yanında siber güvenlik ile ilgili bütüncül dolayısıyla kolektif bir vizyonu içeren ortak bir tanıma sahip olmadığı görülmektedir. Diğer bir söylemle, AB, siber güvenlik kavramının ortak bir paydada tanımlanması ve aynı zamanda standartlaştırılmasında ciddi bir eksikliğe sahiptir. Birlik üyesi devletlerin siber güvenlik ile ilgili kendine özgü tanımlamaları ve stratejileri bulunmaktadır. Dolayısıyla, AB ve üye devletleri arasındaki ortak vizyon eksikliği ve Birliğin hükûmetler arası karakteri, siber güvenlik alanında Birliği sınırlayan iki ana faktör olarak karşımıza çıkmaktadır. Bu durum, Birliğin siber güvenlik stratejisinin uygulanmasını zorlaştırmakta, bir siber güvenlik temsilcisi olarak siber tehditler karşısında etkili bir duruş sergileyememesine neden

olmakta ve küresel rolüne zarar vermektedir. Böylece, Birliğin uluslararası alanda diğer güçlerle ilişkilerindeki başarısı da bundan olumsuz yönde etkilenmektedir.

Bu doğrultuda, Birliğin siber güvenlik tehditleri karşında etkili bir rol oynayabilmesi için öncelikle AB kapsamında siber güvenlik kavramının terminolojik açıdan ortak bir paydada tanımlanması ve standartlaştırılması, farklı bir söylemle AB ekseninde bir siber güvenlik anlayışı yaratılması gerekmektedir. Aynı zamanda, üye devletlerin aynı güvenlik topluluğuna ait olmaları ve benzer çıkarlara sahip olmaları sebebiyle aralarında bir bölgesel iş birliği yaratılması ve siber güvenliğe ilişkin ulusal stratejilerinde bir koordinasyon sağlanması önemli olacaktır. Bunun yanı sıra, siber güvenlik tehditlerinin sınır aşan bir niteliğe sahip olması sebebiyle bu tehditlerle baş edilebilmesi için Birliğin uluslararası alanda kilit ortaklarla da iş birliği yapması gerekmektedir. Bu çerçevede, uluslararası iş birliğini sağlayacak olan kurumsal düzenlemeler ve süreç planlamaları öncelikli hâle getirilmelidir.

Literatür analiz edildiğinde; siber güvenliğe, AB'nin siber güvenlik alanındaki stratejilerine ve politikalarına, AB'nin bu alandaki etkinlik ve yeterliliğine ilişkin çalışmaların kısıtlılığı nedeniyle bu alanda önemli bir boşluğun olduğu görülmektedir. Bu doğrultuda, söz konusu çalışma ile AB'nin siber güvenlik alanındaki politika ve uygulamalarının ne kadar etkin olduğu ve bir siber güvenlik temsilcisi olarak nitelendirilen Birliğin, bu alandaki yeterliliği değerlendirilmeye çalışılmaktadır. Bu kapsamda, öncelikle siber güvenlik ve ilgili kavramlara değinilmekte, ardından siber güvenlik kavramı, AB kapsamında ele alınmakta, hemen sonrasında AB'nin siber güvenlik alanındaki politikaları ve uygulamalarına yer verilerek, son kısımda AB'nin siber güvenlik alanındaki politika ve uygulamalarının etkinliği, bir siber güvenlik temsilcisi olarak AB'nin yeterliliği değerlendirilmektedir.

2. Siber Güvenlik ve İlgili Kavramlar

Bilginin öneminin her geçen gün artması ile birlikte içinde bulunduğumuz çağ, bilgi çağı olarak tavsif edilmekte olup, ihtiyaç duyulan bilgiye sürekli gelişim ve dönüşüm hâlinde olan bilgi ve iletişim teknolojileri aracılığıyla hızlı ve kolay bir şekilde erişilebilmektedir. Dijital dünya her ne kadar internet ile ilişkilendirilse de bilgisayarların arka planında yer alan bireyleri ve aynı zamanda onların bağlantılarının toplumları hangi yönde değiştirdiğini içeren bir siber uzay bulunmaktadır (Singer ve Friedman, 2014, s. 14).

Siber, ister makinede olsun ister hayvanda olsun kontrol ve iletişim teorisi alanına atıfta bulunan sibernetik teriminden türetilen, siber uzayı ifade eden bir önektir ve elektronik iletişim ağları ve sanal gerçekliği ifade etmektedir (Craigen, Thibault ve Purse, 2014, s. 14; Oxford University Press, 2014). Siber uzay terimi ise William Gibson tarafından kaleme alınan, bilgisayar ve bilgisayar kümeleri arasında hareket eden ve saf bilgiden meydana gelen üç boyutlu bir uzay vizyonunun ele alındığı

1984 tarihli "Neuromancer" isimli roman aracılığıyla popüler hâle gelmiştir (Craigen, Thibault ve Purse, 2014, s. 14). Bu doğrultuda, siber uzay, bilgilerin çevrimiçi olarak depolandığı, paylaşıldığı ve iletildiği bilgisayar ağları (ve onların arkasındaki kullanıcılar) alanı şeklinde tanımlanmaktadır. Dolayısıyla, siber uzay her şeyden önce bir bilgi ortamıdır ve oluşturulan, saklanan ve en önemlisi de paylaşılan sayısal verilerden oluşmaktadır. Bu, onun yalnızca fiziksel bir yer olmadığı ve bu sebeple herhangi bir fiziksel boyutta ölçüme meydan okuduğu anlamına gelmektedir. Ancak siber uzay tamamen sanal değildir. Verileri depolayan bilgisayar ile onun akmasına izin veren sistemler ve altyapıdan oluşmakta olup, ağ bağlantılı bilgisayarların internetini, kapalı intranetleri, fiber optik kabloları, hücresel teknolojileri ve uzay tabanlı iletişimi de içermektedir (Singer ve Friedman, 2014, ss. 13-14).

Siber alanda yaşanan ilerlemeler, bilgiye erişimi, bilginin çoğaltılmasını ve paylaşılmasını çok daha kolay bir hâle getirmektedir. Birçok ülkede hizmetler siber alana taşınarak, hizmetlerin çok daha rahat ve hızlı sunulması sağlanmaktadır (Atakan, 2021, ss. 27-28; Kurnaz ve Önen, 2019, s. 83). Ancak bilginin günümüzde elektronik bir ortamda bulunması ve saklanması, maruz kaldığı riskleri artırmakta, onu siber saldırılara açık bir duruma getirmektedir (Kurnaz ve Önen, 2019, s. 83). Başka bir söylemle, siber alanın önemi her geçen gün artarken, siber alanda karşı tarafta yer alanların bilgilerini ve bilgi sistemlerini olumsuz bir şekilde etkileme isteği ve ihtiyacı olarak tanımlanan siber saldırılar ve dolayısıyla çoğunlukla dijital araçların suçlular tarafından çalmak ya da yasa dışı faaliyetlerde bulunmak için kullanılması olarak ifade edilen siber suçlar da aynı hızda artmaktadır (Singer ve Friedman, 2014, s. 85; Şenol, 2017, s. 1). Özellikle 2007 yılında Rus bilgisayar korsanları tarafından Estonya bilgi sistemlerine yönelik gerçekleştirilen saldırı neticesinde internet ve bankacılık hizmetlerinin durma noktasına getirilmesi ve ülkenin hem ekonomik hem de toplumsal açıdan zarara uğramış olması bir siber saldırı örneğidir. Bunun yanında 2008'de gerçekleşen Rusya-Gürcistan Savaşı'nda Gürcistan'a gerçekleştirilen siber saldırılar neticesinde haberleşme, finans ve elektrik sistemlerinde önemli ölçüde problemler ortaya çıkmıştır. 2010 yılında ise endüstriyel kontrol sistemlerini hedef alan ve en tehlikeli yazılım olarak ifade edilen "Stuxnet" yazılımı aracılığıyla İran nükleer zenginleştirme programına zarar verilmiştir. Diğer yandan, 2014'te yapımcı Sony Pictures Firması'na gerçekleştirilen siber saldırılar neticesinde Kuzey Kore lideri ile ilgili yaklaşık 44 milyon dolara mal olduğu belirtilen filmin gösterimden kaldırılması ve 2016 yılında ABD'nin doğu tarafına hizmette bulunan sistem altyapılarına yönelik yapılan siber saldırılar neticesinde ülkenin internet bağlantısının %90'nına engel olunması ve bu durumun çok ciddi ekonomik zararlara yol açması gibi örnekler de dünyada yaşanan ve medyaya yansıyan diğer siber saldırı örnekleridir (Şenol, 2016, ss. 11-12; Şenol, 2017, ss. 2-3). Özellikle bu siber saldırıların, 2009 yılında Amerika Birleşik Devletleri (ABD) Ulusal Araştırma Konseyi tarafından gerçekleştirilen bir araştırmada "bilgisayar sistemleri, ağlar ya da bilgiyi ve/veya bunlarda yerleşik olan ya da bunları taşıyan programları bozmak, aldatmak, küçük düşürmek veya yok

etmek için yapılan kasıtlı hareketler" şeklinde ifade edildiği görülmektedir (Singer ve Friedman, 2014, s. 68). Tüm bu olaylar da siber alanın bir takım hedefler doğrultusunda etik dışı kullanılabildiğini göstermekte (Nezgitli ve Benzer, 2020, s. 11), siber olay ve saldırıların ülkelerin, kurum ve kuruluşlarının güvenliğine yönelik ciddi tehlikelere neden olabileceği sonucuna varılmaktadır (Şenol, 2017, s. 3).

Tarihsel süreç içerisinde yaşanan siber saldırılar neticesinde kişilerin ve ülkelerin görmüş olduğu zararların ciddi boyutlara ulaşması, bilgi ve bilişim sistemlerinin kötü amaçlı saldırılara yönelik korunması ihtiyacını doğurmuş ve bu ihtiyaç siber güvenlik ve siber caydırıcılık kavramının ortaya çıkmasına neden olmuştur. Siber caydırıcılık, siber alanda bilişim sistem ve altyapılarına saldırı gerçekleştirmeyi planlayan saldırganı, saldırıdan vazgeçirme olarak ifade edilirken (Şenol, 2017, ss. 1,4), siber güvenlik ise gizlilik, bütünlük ve kullanılabilirliği sağlamak amacıyla ağları, bilgisayarları, programları ve verileri herhangi bir saldırı, hasar ve yetkisiz erişimden korumak için tasarlanmış teknolojiler, uygulamalar, süreçler, müdahaleler bütünüdür (Public Works and Government Services Canada. Translation Bureau, 2012, s. 24). Diğer bir ifade ile siber güvenlik, elektronik verilerin suça ya da yetkisiz kullanımına karşı korunma durumu ya da bunun için alınan tedbirlerdir (Oxford University Press, 2014). Özellikle giderek artan siber saldırılar, siber güvenlik konusunu bireylerin, ülkelerin, kurumların, NATO, AB gibi uluslararası kuruluşların en önemli konularından biri durumuna getirmektedir. (Ünver ve Canbay, 2010, s. 94). Özellikle AB siber alanın güvenliğini sağlamaya yönelik çeşitli stratejiler ve yasal düzenlemeler oluşturmakta, siber güvenlik stratejilerini uygulamak amacıyla ilgili kurumları faaliyete geçirmektedir (Kurnaz ve Önen, 2019, ss. 82-83). Kısaca siber alanın tehlikelerinin farkında olan bireyler, kurum, kuruluş ve ülkeler siber güvenlik konusunun üzerinde durmakta, siber saldırıları ulusal güvenliğe tehdit oluşturan faktörlerden biri olarak görmekte, birinci sırada elektronik haberleşme, su yönetimi, enerji, kritik kamu hizmetleri, bankacılık, ulaştırma ve finans alanları gibi önemli altyapılar olmak üzere bireyleri, kurum ve kuruluşları siber saldırılardan korumak amacıyla çeşitli çözümler üretmekte, politikalar ve stratejiler geliştirerek bunları uygulamaya koymaktadır. Diğer bir ifade ile bilgisayar ve iletişim teknolojilerinin sağladığı olanaklardan etkin bir biçimde faydalanabilmek için bilgi ve iletişim sistemleri ile altyapılarının, giderek artan ve çeşitlenerek devam eden siber saldırılara karşı korunmasının yolları aranmakta, siber güvenlik alanında stratejiler geliştirilmeye çalışılmaktadır (Şenol, 2017, ss. 3-4). Ancak büyük imkân ve avantajlarının yanı sıra bilinmedik riskleri de içinde barındıran, doğası gereği gizli, öngörülemez, zamansız ve sınırsız olan siber alanda tehditlere karşı yeni savaşma normları, teknikleri ve işbirlikçi ilişkiler geliştirmek de bir hayli zor olmaktadır (Akarçay ve Ak, 2018, ss. 195, 208-209).

3. AB Çerçevesinde Siber Güvenlik Kavramı: Kavramsal Netlik Eksikliği

Siber güvenlik kavramı AB çerçevesinde ele alındığında, AB kapsamında siber güvenliğe ilişkin bütüncül bir anlayışın ve kolektif bir vizyona sahip, ortak bir tanımın yapılmadığı görülmektedir. 7 Şubat 2013 tarihinde Avrupa Komisyonu'nca yayımlanan ve Birliğin siber güvenlik politikasının somut bir zemine oturması kapsamında son derece önemli bir belge olan "Siber Güvenlik Strateji Belgesi" açık, güvenli ve kesin bir siber güvenlik tanımı içermemektedir. Aynı zamanda, söz konusu strateji belgesinin 2017'de revize edilmiş hâlinde ve 11 Mart 2019'da Avrupa Parlamentosu tarafından onaylamış, 27 Haziran 2019'da da yürürlüğe girmiş "Siber Güvenlik Yasası"nda da siber güvenliğe ilişkin bir tanım bulunmamaktadır. Ancak Birliğin, Birlik üye devletlerinin ve iş dünyasının problemlerinin önüne geçme, çözüm üretme ve bu problemlere cevap verme yeteneğini geliştirmek amacıyla 13 Mart 2004 tarihinde tüzel bir kişilik olarak kurulan "Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA)" siber güvenliğin tanımına yer vermektedir. ENISA özellikle siber saldırılar esnasında koordinasyon yükümlülüğüne sahip olan, ulusal siber güvenlik stratejilerinin koordinasyonunu sağlayan, üye ülkelere, Birliğin kurum ve kuruluşlarına ve özel sektöre uzmanlık ve bilgi temin eden, ağ ve bilgi güvenliği ile bağlantılı Birlik politikalarının uygulanması ve gelişiminin sağlayan bir ajanstır. ENISA'da siber güvenlik; bilgi, bilgi sistemleri, altyapılar ve uygulamaların siber saldırılardan korunması şeklinde ifade edilmektedir (Akbaş, 2022, s. 22; ENISA, t.y.; Helmbrecht, Purser ve Klejnstrup, 2012, s. 13; Köksoy, 2020, s. 639; Sliwinski, 2014, s. 469). Ayrıca, ENISA, siber güvenliğin sağlanmasına yönelik katmanlardan meydana gelen bir piramite sahiptir. Bu çerçevede, piramitin katmanları; "Demokrasi ve İnsan Haklarının Korunması: Siber etik, siber demokrasi, siber insan hakları ve AB değerlerini korunması", "Küresel İstikrarın Korunması: Siber normların ve siber diplomasinin tesis edilmesi", "Dijital Tek Pazarın Korunması: Dijital tek pazarın siber saldırılardan korunması", "Kritik Altyapıların Korunması: Enerji, ulaşım, finans gibi dijital hizmetlerin korunması" ve "Temel Güvenlik Önlemleri: Siber uzay kullanıcılarının güvenliğinin sağlanması"ndan oluşmaktadır. ENISA'nın siber güvenliğin sağlanmasına yönelik yaratmış olduğu bu piramit çerçevesinde görülmektedir ki siber güvenlik şemsiye bir kavramı oluşturmakta ve bu kapsamda resmi ve aynı zamanda genel olarak kabul edilen bir tanımdan bahsedilememektedir. Buna karşın söz konusu yaklaşım, siber güvenlik kavramını tanımlamaya yönelik somut bir adım olarak değerlendirilmektedir (ENISA, 2017, s. 4; Köksoy, 2020, ss. 639-640). Tüm bunlardan da anlaşılacağı gibi AB ekseninde bir siber güvenlik anlayışı ortaya çıkarmak oldukça zor bir hususu teşkil etmektedir (Sliwinski, 2014, s. 469).

AB üye ülkelerinin siber güvenliğe yönelik kendi stratejileri ve kavramsallaştırmaları mevcuttur (Sliwinski, 2014, s. 469). Birlik üyelerinin birçoğunun siber güvenliği kendilerince tanımladıkları görülmektedir. Örneğin Almanya siber güvenliği, siber uzayın kullanılabilirliğinin sağlanması, siber uzayda

yer alan verilerin bütünlüğü, özgünlüğü ve aynı zamanda gizliliğinin korunması şeklinde tanımlarken (Federal Ministry of the Interior, Building and Community, 2021, ss. 39, 125, 127), Polonya'nın ise siber güvenlik ile ilgili somut bir tanım yapmadığı görülmektedir. Aynı şekilde, 2018'de yeniden düzenlenen Çekya'nın kendi siber güvenlik strateji belgesinde de siber güvenlikle ilgili bir tanım bulunmamaktadır (Köksoy, 2020, s. 641; Ministry of Digital Affairs, 2017). AB üye devletlerinin siber güvenliğe yönelik kendi stratejilerinin ve kavramsallaştırmalarının olmaları ciddi problemlere yol açmaktadır. Ortak bir siber güvenlik tanımının, siber güvenlik kavramının neleri içermesi gerektiğine ilişkin tutarlı, ortak bir Avrupa anlayışının bulunmaması, siber güç, siber savunma ve siber güvenlik stratejisi gibi kavramlarda da kavramsal farklılıklar meydana getirmekte, Avrupa'nın siber tehditlere karşı tepkilerinin de zayıf kalmasına neden olmaktadır. Aynı zamanda, kavramsallaştırma farklılıkları farklı yaklaşımları da beraberinde getirmektedir (Köksoy, 2020, s. 640; Sliwinski, 2014, ss. 469-470,479). Diğer bir ifade ile AB üye devletlerinin siber güvenliğe ilişkin yaklaşımları da birbirlerinden farklılık göstermektedir. Fransa askeri ve istihbarat odaklı bir yaklaşım benimserken, Almanya ve Hollanda gibi devletlerin ise daha çok sivil ve hukuki temelli bir yaklaşım benimsedikleri görülmektedir. Bunun yanında, Estonya ise askeri ve istihbarat aynı zamanda da sivil ve hukuki odaklı bir yaklaşıma sahiptir. Dolayısıyla, AB çerçevesinde siber güvenlik kavramının terminolojik açıdan ortak bir paydada tanımlanmasında ve standart bir hâle getirilmesinde ciddi bir eksikliğin mevcut olduğu gözlemlenmekte (Köksoy, 2020, s. 641), bu konuda tam olarak net bir duruş sergilenememektedir (Sliwinski, 2014, s. 469).

4. AB'nin Siber Güvenlik Alanındaki Politikaları ve Uygulamaları

AB'nin siber güvenlik alanındaki politikaları, uygulamaları ve hedefleri çerçevesinde, 2013'de Avrupa Komisyonu'nca yayımlanmış olan "Avrupa Birliği'nin Siber Güvenlik Stratejisi" belgesi siber güvenlik alanındaki ilk somut adım olması yönünden oldukça önemlidir. Bu doğrultuda, AB'nin siber güvenlik politikalarının, bahsedilen belgeden öncesinde ve sonrasında atılan adımlar şeklinde ele alınması gerekmektedir. Dolayısıyla, öncelikle 2013'de yayımlanmış olan Siber Güvenlik Strateji Belgesi öncesindeki döneme yer verilecektir (Köksoy, 2020, ss. 644-645).

1985'de Avrupa Komisyonu tarafından yaratılan "Tek Pazar İnsiyatifi" AB'nin siber güvenlik politikasındaki çalışmalarının başlangıcı olarak kabul edilmektedir. Yine aynı sene Avrupa Komisyonu'nca yayımlanmış olan Beyaz Kitap'ta bilgi teknolojileri ve telekomünikasyon alanında ortaya çıkan gelişmeler ve bu gelişmelerin AB ortak pazarı üzerindeki etkisine değinilmiştir. Aynı zamanda, yeni bilgi teknolojilerinin kullanımının ekonomik büyümeyi de sağlayacağı ifade edilmiştir (European Commission, 1985, ss. 20,31).

1994'de kabul edilen "Bangemann Raporu" ile Birliğin siber güvenlik politikasının kapsamı oluşturulmaya başlanmıştır. Bu rapor çerçevesinde, Birliğin siber güvenlik

politikası çok daha görünür bir duruma gelmiş, aynı zamanda aktörler arasındaki iş birliğinin daha güçlü bir hâle gelmesine, fikri mülkiyet haklarının korunmasına, internet korsancılığı ile mücadele edilmesine ve Birliğin sosyo-ekonomik gelişimi sırasında bilgi ve iletişim teknolojilerinin oynadığı rolün önemine vurgu yapılmıştır (Bangemann, 1994; European Council, 1994).

Diğer taraftan, merkezi gerçek kişiler olan ve verilerin işlenmesi esnasında kişilerin haklarının ve özgürlüklerinin korunmasını kapsayan 25 Kasım 1995'deki "Verilerin Korunması Direktifi" (European Parliament and Council, 1995); bilgi güvenliği, ekonomik güvenlik, ulusal güvenlik, fikri mülkiyet, özel hayatın korunması faktörlerini kapsayan 16 Ekim 1996 tarihindeki "İnternetin Yasal Olmayan ve Zararlı İçeriğine İlişkin Belge" (Commission of the European Communities, 1996, s. 3); siber uzay kaynaklı tehditleri ilk defa kapsamlı bir şekilde ele alan (Commission of the European Communities, 2001, ss. 9-15), güvenliğin artırılmasına yönelik somut teknik önlemler yaratan (Commission of the European Communities, 2001, ss. 20-25), ağ ve bilgi güvenliğinin ilk defa tanımının yapıldığı, siber güvenlik ekseninde aktörler arasındaki iş birliğinin önemini ifade eden 2001'deki "Ağ ve Bilgi Güvenliğine İlişkin Öneri (NIS Proposal)" (Akbaş, 2022, s. 22; Commission of the European Communities, 2001, ss. 9, 26-27; Köksoy, 2020, s. 646); gerçek kişiler ile birlikte tüzel kişileri de kapsayan 31 Temmuz 2002'deki "Elektronik Haberleşme Sektöründe Gizliliğin Korunması Direktifi" (Official Journal of the European Communities, 2002, ss. 37-47); Birliğin siber güvenlik alanındaki politikalarının ve aynı zamanda mevzuatının uygulanması sürecine destek sağlayacak kurumlara duyulan ihtiyaç nedeniyle, Birliğin, Birlik üye ülkelerinin ve iş yaşamının problemlerinin önüne geçme, çözüm üretme ve bu problemlere cevap verme yeteneğini geliştirmek, siber saldırı esnasında koordinasyon yükümlülüğüne sahip olan, ulusal siber güvenlik stratejilerinin koordinasyonunu sağlayan üye ülkelere, Birliğin kurumlarına ve özel sektöre uzmanlık ve bilgi temin eden, ağ ve bilgi güvenliği ile bağlantılı Birlik politikalarının uygulanması ve gelişimini sağlamak üzere "Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA)" nın tüzel bir kişilik olarak 13 Mart 2004 tarihinde kurulması (Akbaş, 2022, s. 22; ENISA, t.y.); Birlik çerçevesinde meydana gelen siber saldırılara ilişkin cezai yaptırımların yükseltilmesi maksadıyla üye ülkeler ile iş birliğini amaçlayan 23 Şubat 2005'deki "Bilgi Sistemlerine Saldırılar Hakkında AB Konseyi Çerçeve Kararı" (Official Journal of the European Union: 2005, ss. 68-69); suçların saptanması ve araştırılması için üye ülkelerin yasal mevzuatlarında belirtilen telefon ve e-posta bilgilerinin saklanması yükümlülüğüne yer verilen 15 Mart 2006 tarihli "Verilerin Saklanması Direktifi" (Official Journal of the European Union, 2006); 31 Mayıs 2006'da ağ ve bilgi güvenliği politikasını faaliyete geçirme amacıyla yaratılan "Güvenli Bilgi Toplumu İçin Strateji Belgesi" (European Union, 2006) Birliğin siber güvenlik politikasının gelişimi noktasında son derece önemli rol oynamıştır. Bunun dışında, 2012'deki "AB Bilgisayar Acil Ekibi'nin (CERT-EU) ve 2013'de siber suçlara yönelik sınır aşan faaliyetlerin koordinasyonunu sağlayan, bu alana ilişkin teknik uzmanlık temin eden ve yetkileri git gide daha da

yükseltilen "Avrupa Siber Suç Merkezi"nin (European Cybercrime Centre-EC3) yaratılması da Birliğin siber güvenlik politikası açısından oldukça önemli olmuştur (Köksoy, 2020, s. 647).

7 Şubat 2013 tarihinde Avrupa Komisyonu'nca yayımlanmış olan "Siber Güvenlik Strateji Belgesi" Birliğin siber güvenlik politikası ile ilgili somut bir adım atılması ekseninde oldukça önemli bir belgedir. Bu strateji, AB'nin geleceği için öncelik olacak beş temel ilkeye dayanmaktadır. Bunlar; siber dayanıklılığa ulaşmak, siber suçları büyük ölçüde azaltmak, Ortak Güvenlik ve Savunma Politikası ile ilgili siber savunma politikaları ve yetenekleri geliştirmek, siber güvenlik için endüstriyel ve aynı zamanda teknolojik kaynaklar sağlamak ve Birlik için istikrarlı bir uluslararası siber uzay politikası yaratmak ve AB'nin temel değerlerini teşvik etmektir (European Commission, 2013, ss. 4-5; Kovacs, 2018, s. 17; Köksoy, 2020, s. 647). 2013'deki strateji belgesinin ardından Birlik, siber alandaki politikalarını daha da güçlendirmeye çalışmıştır. Bu hedef doğrultusunda, 2015'de siber suçlarla mücadele konusunu ön plana alarak "Güvenlik Üzerine Avrupa Gündemi" ve malların, hizmetlerin, sermayenin, kişilerin serbest dolaşımının mümkün olduğu; kişilerin, işletmelerin milliyetlerine ve ikamet yerlerine bakılmaksızın, adil bir rekabet ve verilerin korunması şartlarında çevrimiçi faaliyetlere problemsiz bir biçimde ulaşılabildiği ve bunları kullanabildiği, dijital ekonominin güçlendirilmesini temel alan "Dijital Tek Pazar"a yönelik strateji oluşturulmuştur. Dijital Tek Pazar'a ulaşmanın Avrupa'nın dijital ekonomide dünya lideri konumunu sürdürmesinde ve Avrupalı şirketlerin küresel olarak büyümesinde önemli bir rol oynayacağı belirtilmiştir (European Commission, 2015a, s. 2, European Commission, 2015b, s. 3; Köksoy,2020, ss. 647-648). Diğer taraftan 6 Temmuz 2016 yılında Avrupa Parlamentosu tarafından kabul edilmiş olan ağ ve bilgi sistemlerinin güvenliğini yükseltmeyi, siber güvenlik konusunda üye ülkeler arasında iş birliğini artırmayı hedefleyen ve ilk yasal düzenleme olarak kabul edilen NIS Direktifi 2016 Ağustos'ta yürürlüğe girmiştir (European Commission, t.y.; Köksoy, 2020, s. 648). Direktif; ENISA'ya da üye devletlere Direktifin uygulanabilmesi, ağ ve bilgi sistemlerinin güvenliği çerçevesinde destek sağlama gibi bazı yükümlülükler getirmiştir. Aynı zamanda, 7 Şubat 2013 tarihinde Avrupa Komisyonu'nca yayımlanmış olan "Siber Güvenlik Strateji Belgesi"nin 2017 yılında yeniden "Dayanıklılık, Caydırıcılık ve Savunma: AB İçin Güçlü Bir Siber Güvenlik Oluşturmak" ile revize edilmiş olması (Akbaş, 2022, s. 23), siber güvenlik politikasının güçlendirilmesi kapsamında son derece önemli bir adım olmuşken, 2017'den beri çalışılan ve 11 Mart 2019'da Avrupa Parlamentosu'nun onaylamış olduğu "Siber Güvenlik Yasası" ise bu alanın yasal bir seviyeye taşınması noktasında önemli bir adım olmuştur. Bu yasa, 27 Haziran 2019 tarihinde yürürlüğe girmiş ve yasa kapsamında özellikle siber güvenlik tehditleri ve saldırıları ile mücadelede üye ülkelere destek olma noktasında ENISA'nın yetki alanının daha da güçlendirilmesi (European Commission, 2017a; Köksoy, 2020, s. 648) ve bağımsızlığı, sağladığı öneri ve yardım kararlarının bilimsel ve teknik kalitesi hakkında siber güvenlikle alakalı bir uzmanlık merkezi hâline getirilmesi

hedeflenmiştir. Yasa ile Ajansın, üye devletlere siber güvenlik ile ilgili politikalarının geliştirilmesi ve uygulanmasında yardımcı olacağı ve aynı zamanda üye ülkelerin sınır dışı olaylarında, siber tehditlerin engellenmesi ve bunlara cevap verilmesi sırasındaki eylemlerinin tamamlanabilmesi için Birliğin siber güvenlik kapasitesinin yükseltilmesi noktasında önemli bir rol oynayacağı ifade edilmiştir (Nezgitli ve Benzer, 2020, s. 12). Diğer yandan Siber Güvenlik Yasası ile bütüncül bir yaklaşımla uygulanacak NIS 2 Direktifi teklifinin, Avrupa Komisyonu'nca Aralık 2020 tarihinde sunulması ile ENISA'ya tedarik zincirlerine yönelik risk değerlendirmesinde bulunmak, aktörler arasında iş birliğini artırmak, siber güvenlik alanına ilişkin belirli aralıklarda raporlar düzenlemek, gereken bilgi sistemlerini oluşturmak gibi birçok yükümlülük verilmesi de öngörülmüştür (Akbaş, 2022, s. 24). Siber Güvenlik Yasası'nda bilgi ve iletişim teknolojileri çerçevesinde bütün üye ülkelerde geçerliliği olacak bir siber güvenlik sertifikasının meydana getirilmesi gerektiği de belirtilmiştir. Bu doğrultuda, AB Siber Güvenlik Yasası, dijital ortamın daha da güvenli bir hâle getirilmesini hedefleyen Birliğin genel siber politikasının bir parçası olarak görülmüştür (European Commission, 2017a; Köksoy, 2020, ss. 648-649).

Aralık 2020 tarihinde Avrupa Komisyonu tarafından sunulan NIS 2 Direktifi, Aralık 2022'de Avrupa Birliği Resmi Gazetesi'nde resmi olarak yayınlanmış ve 16 Ocak 2023'de yürürlüğe girmiştir. NIS Direktifi'nin yerini alan NIS 2 Direktifi, ekonomik açıdan önemli hizmetler sağlayan ya da faaliyette bulunan kuruluşlara uygulanan siber güvenlik gereksinimlerinin, siber güvenlik türü, ayrıntı düzeyi ve denetim yöntemi bakımından üye devletlerde farklılık göstermesi nedeniyle üye devletlerin siber güvenlik düzenlemelerindeki ve siber güvenlik önlemlerinin uygulanmasındaki farklılıkları ortadan kaldırmayı ve daha fazla kurumu ve sektörü etkili bir şekilde önlem almaya zorlayarak, uzun vadede Avrupa'da siber güvenlik seviyesini artırmayı amaçlamıştır. Bu çerçevede, yasal dayanağı Avrupa Birliği'nin İşleyişine İlişkin Antlaşma'nın 114. maddesi olan NIS 2 Direktifi, AB'de siber güvenliği güçlendirme adına atılmış son derece önemli bir adım olmuştur (Akbaş, 2022, s. 24; Negreiro, 2013, ss. 1, 7; Kaya ve Aksöz, 2023; Lawels, 2022; Official Journal of the European Union, 2022a, ss. 81).

Enerji, sağlık, ulaşım ve dijital altyapı başta olmak üzere tüm sektörlerde siber güvenlik risk yönetimi önlemleri ve raporlama yükümlülükleri için asgari standartlar belirlemiş olan NIS 2 Direktifinde ön plana çıkan bazı düzenlemelere yer verilmiştir. Özellikle ekonomi ve toplum için önemli işlevleri yerine getiren iç pazardaki tüm kamu ve kuruluşların yeterli siber güvenlik önlemleri almasını sağlayan kurallar koyularak, ilgili tüm sektörlerde AB'de faaliyet gösteren bir dizi işletmenin siber dayanıklılık düzeyinin artırılması hedeflenmiştir. Telekomünikasyon, sosyal medya platformları ve kamu yönetimi gibi yeni sektörler de NIS 2 Direktifi kapsamına dâhil edilerek, mevcut NIS direktifinin kapsamı önemli ölçüde genişletilmiş, dolayısıyla NIS 2 kapsamındaki sektörlerde faaliyet gösteren ya da hizmet sağlayan tüm orta ve büyük ölçekli kuruluşların NIS 2

Direktifinde belirtilen kurallara uyması sağlanmaya çalışılmıştır. Çevrimiçi pazar yerleri, arama motorları ve bulut hizmet sağlayıcıları olarak üç kategoriye ayrılan dijital hizmet sağlayıcıları ve temel hizmet operatörleri arasında yapılan ayrımın ortadan kaldırılması gerektiği vurgulanmış ve temel bilgi ve iletişim teknolojisi için güçlendirilmiş tedarik zinciri siber güvenliğinin oluşturulması hedeflenmiştir (Negreiro, 2013, s. 7; Kaya ve Aksöz, 2023; Yeniyıldız, t.y.a, s. 2).

Aynı zamanda, direktifin kapsadığı sektörlerde iç pazar genelinde dayanıklılıktaki tutarsızlıkların, ulusal denetim ve yaptırımı düzenleyen hükümlerin, üye devletlerin yetkili makamlarının yeteneklerinin, güvenlik ve olay raporlama gerekliliklerinin, fiili kapsamın uyumlu hâle getirilmesi ile azaltılması amaçlanmıştır. Direktifte olay müdahalesi, tedarik zinciri güvenliği, şifreleme ve güvenlik açığı ifşası dâhil olmak üzere tüm şirketlerin aldıkları önlemlerin bir parçası olarak ele alması ve uygulaması gereken güvenlik önlemleri için bir listeye yer verilmiş, aynı zamanda bir siber tehdit durumu söz konusu olduğunda olay raporlamaya yönelik iki aşamalı bir yaklaşım önerilmiştir. Bu çerçevede, şirketlerin herhangi bir siber tehdit durumuyla karşılaştıklarını ilk fark ettikleri andan itibaren 24 saat içinde yetkili makamlara ilk raporlarını, bir ay sonra da nihai raporlarını sunmaları gerektiği belirtilmiştir. Direktifte aynı kuruluşların siber güvenlik risk yönetimine ilişkin kuralları ya da direktifte belirtilen raporlama yükümlülüklerini ihlal etmesi hâlinde kullanılabilecek yaptırım yetkilerinin asgari bir listesinin belirlenmesi ve bu tür bir uygulama için Birlik genelinde açık ve tutarlı bir çerçeve oluşturulması gerektiği de ifade edilmiştir. Bu doğrultuda, bağlayıcı talimatlar, bir güvenlik denetiminin tavsiyelerini uygulama emri, güvenlik önlemlerini direktifin gerekliliklerine uygun hâle getirme emri ve 10 milyon Euro ya da şirketin toplam küresel yıllık cirosunun %2'sine varan daha yüksek idari para cezaları gibi asgari bir idari yaptırım listesi öngörülmüştür (Negreiro, 2013, s. 7; Kaya ve Aksöz, 2023; Official Journal of the European Union, 2022a, ss. 105; Yeniyıldız, t.y.a, ss. 2-3).

Diğer yandan, büyük ölçekli siber güvenlik konularını içeren vakalarda, yetkili makamlar arasında güven düzeyini artıracak önlemler alınarak, daha fazla bilgi paylaşılarak, kurallar ve prosedürler belirlenerek, ortak durumsal farkındalık düzeyinin, kolektif hazırlık ve yanıt verme kabiliyetinin geliştirilmesi hedeflenmiştir. Önerilen yeni kurallar; net sorumluluklar, uygun planlama ve daha fazla iş birliği getirerek, Birliğin, büyük ölçekli siber güvenlik olaylarını ve krizlerini önleme, ele alma ve bunlara yanıt verme şeklini geliştirmek amaçlı koyulmuştur. Aynı zamanda direktifle üye devletlerin bir plan benimsemesini, Birlik düzeyinde siber güvenlik olaylarına ve krizlerine müdahaleye katılmaktan sorumlu ulusal yetkili makamların atanmasını gerektiren bir AB kriz yönetimi çerçevesi oluşturulması öngörülmüştür. AB çapındaki siber güvenlik olaylarının koordineli yönetimini desteklemek ve düzenli bilgi alış verişini sağlamak için bir AB Kriz İrtibat Organizasyonu Ağı'nın ve ortak siber güvenlik düzeyinin yüksek bir seviyeye çıkmasını kolaylaştırmak için eşli öğrenme mekanizmasının kurulması

da öngörülen diğer hususlar olmuştur (Negreiro, 2013, ss. 7-8; Yeniyıldız, t.y.a, s. 2).

2017 yılında yeniden "Dayanıklılık, Caydırıcılık ve Savunma: AB İçin Güçlü Bir Siber Güvenlik Oluşturmak" ile revize edilen "Siber Güvenlik Strateji Belgesi", 2020 yılında "AB'nin Dijital On Yıl İçin Siber Güvenlik Stratejisi" ile son şeklini almıştır. "AB'nin Dijital Geleceğini Şekillendirmek", "Avrupa İçin İyileştirme Planı" ve "AB Güvenlik Birliği Stratejisi"nin ana öğesi olan ve 16 Aralık 2020'de yayımlanan "Yeni AB Siber Güvenlik Stratejisi" ile birlikte AB'nin siber güvenlik tehditlerine karşı kolektif direncinin artırılması, tüm vatandaşların ve işletmelerin güvenilir hizmetlerden ve dijital araçlardan faydalanmasının sağlanması hedeflenmiştir. Strateji, Birliğin siber uzayda uluslararası normlar ve standartlarla ilgili öncü rolünün artırılmasına, insan haklarına, hukukun üstünlüğüne, temel özgürlüklere ve demokratik değerlere dayalı olan küresel, açık, istikrarlı ve güvenli bir siber alanın teşviğini sağlamak için dünyanın birçok yerindeki ortaklarla iş birliğini geliştirmesine imkân sağlamıştır. Dolayısıyla, Strateji, "siber dayanıklılığın sağlanması", "siber suçların azaltılması", "siber savunma politikasının geliştirilmesi", "siber güvenlik sanayi ve teknolojileri için gerekli kaynağın tesisi" ve "AB için bütüncül uluslararası bir siber güvenlik politikasının yapılandırılması" gibi beş önceliği olan alana odaklanmıştır (Akbaş, 2022, s. 23; European Commission, 2020).

2022'de Avrupa Komisyonu tarafından 2020 tarihli AB'nin Dijital On Yıl İçin Siber Güvenlik Stratejisi doğrultusunda dijital bileşenli bir ürün ya da yazılım satın alan, kullanan tüketicileri ve işletmeleri korumak amacıyla dijital ürünler ve hizmetler için yeni siber güvenlik kuralları oluşturulmasını hedefleyen "Siber Dayanıklılık Yasası" (Cyber Resilience Act, CRA) başlıklı tüzük taslağı yayınlanmıştır. Yasa, yazılım ve dijital donanım ürünlerinin çok daha az güvenlik açığı ile piyasaya girişini ve dijital özelliklere sahip bir ürünün yaşam döngüsü boyunca siber güvenliği garanti etmesini sağlayarak güvenli ürünlerin ortaya çıkması için koşullar yaratmak ve aynı zamanda kullanıcıların dijital özellikler içeren ürünler seçerken ve kullanırken, siber güvenlik konusunu göz önünde bulunduracakları bir ortam oluşturmak olmak üzere iç pazarın düzgün bir biçimde işlemesine yönelik iki temel hedef ortaya koymuştur. Aynı zamanda, yazılım ve dijital donanım üreticilerinin siber güvenlik kurallarına uyumunu kolaylaştıran tutarlı bir güvenlik çerçevesi yaratmak, üreticilerin, tasarım ve geliştirme sürecinden itibaren dijital unsurlar içeren ürünlerin güvenliğini ve tüm yaşam döngüsü boyunca güvenliğini geliştirmelerini sağlamak, dijital unsurlar içeren ürünlerin güvenlik özelliklerinin şeffaflığını artırmak, işletmelerin ve vatandaşların, dijital unsurlar içeren ürünleri güvenli bir biçimde kullanmalarını sağlamak da yasanın özel hedeflerini oluşturmuştur (European Commission, 2022; Yeniyıldız, t.y.b).

2025 yılında yürürlüğe girmesi öngörülen "Dijital Operasyonel Dayanıklılık Yasası" (Digital Operational Resilience Act, DORA) da siber güvenlik alanında atılmış önemli bir adım olmuştur. Büyük miktarda kişisel ve finansal veriye sahip olan finans firmalarının her geçen gün dijital süreçlere, sistemlere daha fazla bağımlı bir hâle gelmesi ve buna bağlı olarak bilgi ve iletişim teknolojisi sistemlerine yönelik tehditlerin ciddi oranlarda artması neticesinde benimsenen DORA ile Avrupa'da yer alan tüm finans sektörünün bilgi ve iletişim teknolojisi kaynaklı olaylara karşı dayanıklılığının artırılması ve tüm finans sektörüne yönelik ortak standartlar getirilmesi hedeflenmiştir. Bu doğrultuda, ilgili sektörde operasyonel dayanıklılığın teşvik edilmesi, sağlanması ve daha da geliştirilmesi amacıyla DORA'da finansal kuruluşlara yönelik bazı düzenlemelere ve yükümlülüklere yer verilmiştir. Özellikle bilgi ve iletişim teknolojisi son yıllarda finansal hizmetlerin sağlanmasında hatta tüm finansal kuruluşların günlük işlerinin yürütülmesinde kritik bir öneme sahip olmuştur. Bu durum, finansal firmaların, bilgi ve iletişim teknolojisi kaynaklı olayları ve ardından gelebilecek mali ve itibari zararı önlemek için gelişmiş ve güncel iletişim ve teknoloji yetenekleri ile donatılmış olması gerekliliğini ön plana çıkartmıştır. DORA ayrıca finansal kuruluşlara bilgi ve iletişim teknolojisi ile ilgili hizmetler veren ve bulut platformları, veri analitiği ve denetim hizmetleri gibi son derece kritik konumlarda faaliyette bulunan bazı bilgi ve iletişim teknolojileri hizmet sağlayıcılarına ilişkin de özel yükümlülükler içermiştir. DORA'nın veri raporlama hizmet sağlayıcıları, yatırım firmaları ve sigorta aracıları gibi finansal kuruluşların dışında bilgi ve iletişim teknolojileri üçüncü taraf hizmet sağlayıcıları için de bir uygulama alanına sahip olacağı belirtilmiştir (Official Journal of the European Union, 2022b, ss. 1, 79; Özden, 2023; Pavlidis, 2021; 474).

DORA, Birlik yasal düzenlemelerinde ayrı ayrı ele alınmış olan operasyonel risk gerekliliklerinin bir unsuru olarak bilgi ve iletişim teknolojisi risk gerekliliklerini birleştirmeyi ve geliştirmeyi hedeflemiştir. Siber güvenlik ile ilgili diğer Birlik mevzuatlarından farklı olarak DORA ile daha önceki yasal düzenlemelerdeki eksikliklerin ve tutarsızlıkların giderilmesi için gerekli adımlar atılmış ve bilgi ve iletişim teknolojisi risk yönetimi yetkinlikleri, raporlama, operasyonel dayanıklılık testi ve bilgi ve iletişim teknolojisi üçüncü taraf risk denetimi ile ilgili öngörülmüş olan kurallar aracılığıyla bilgi ve iletişim teknolojisi riskine dikkat çekilmiştir. DORA, ileri seviyede bir ortak dijital operasyonel dayanıklılık düzeyine ulaşılabilmesi amacıyla finansal kuruluşlar için uygulanacak gereklilikleri, bilgi ve iletişim teknolojisi üçüncü taraf hizmet sağlayıcıları için gözetim çerçevesinin oluşturulması ve yürütülmesine ilişkin kuralları, yetkili makamlar arasında iş birliğine ve DORA çerçevesindeki tüm konularla ilgili olarak yetkili makamlar tarafından denetim ve uygulamaya yönelik kuralları belirlemiştir. DORA, finansal kuruluşların bilgi ve iletişim teknolojisi risk yönetimi, bilgi ve iletişim teknolojisi ile ilgili olay raporlama ve bildirim, operasyonel ya da güvenlik ödemesiyle ilgili olay raporlama, dijital operasyonel dayanıklılık testi, bilgi ve istihbarat paylaşımı ve bilgi ve iletişim teknolojisi üçüncü taraf risk yönetimi esaslarına dayanarak

operasyonların her aşamasında dijital dayanıklılığın sağlanmasını hedeflemiştir (Özden, 2023).

Tüm bu belgeler göz önünde bulundurulduğunda, Birliğin siber güvenlik ile ilgili çalışmalarının başlangıç noktası olan 1985'den günümüze kadar ekonomik açıdan faydanın sağlanması, temel hakların korunması, siber saldırıların önüne geçilmesi, dijital sistemlere duyulan güvenin artırılması ve aktörler arasındaki iş birliğinin daha da güçlendirilmesi gibi hedefler kapsamında siber güvenlik politikalarını geliştirmeye çalıştığı görülmektedir (Köksoy, 2020, s. 651).

5. AB'nin Siber Güvenlik Alanındaki Politikalarının ve Uygulamalarının Etkinliği: Bir Siber Güvenlik Temsilcisi Olarak AB'nin Zayıflığı

AB Soğuk Savaş sonrası ilk yıllarda önemli başarılara sahip olmasına rağmen, bugün gerçek ağırlığını ortaya koyma ve güçlü yönlerinden yararlanma noktasında başarısız olmaktadır. Yaygın olarak iki faktörün bunda etkili olduğu görülmektedir. Bunlardan birincisi, AB'nin etkisi ve nüfuzunun ortak bir küresel politika eksikliğinden muzdarip olmasıdır. Oysa ikili ya da çok taraflı düzeyler arasındaki daha fazla sinerji, daha tutarlı ve görünür bir küresel role katkıda bulunarak, AB'nin ortaklara daha kararlı ve tutarlı bir mesaj sunmasına olanak yaratacaktır. İkincisi ise Birliğin yükselen güçlerle olan ilişkilerinde üye devletler arasındaki mevcut farklılıklardır. AB'nin, yükselen güçlerle ilişkilerini geliştirmek için üye devletler arasındaki farklılıkları çözmesi gerekmektedir. AB birleştiğinde hem çok taraflı hem de ikili seviyelerde çok daha güçlü bir oyuncudur. AB'nin, Birleşmiş Milletler'de, NATO'da, Çin gibi partnerler ile ilişkilerinde başarılı olması ancak AB üye ülkelerinin kendi aralarında fikir birliğine varmasıyla mümkün olacaktır. Üye ülkeler arasında daha fazla fikir birliği için çalışmak, liderlik ve özenli bir diplomasi gerektirmektedir. Bu, AB'nin küresel rolünü güçlendirmesi açısından son derece önemli bir koşuldur. Bu ilk adım atıldığında, üye ülkeler AB çizgisine uymayan ikili anlaşmalara son verebilecek ve AB, Rusya, Çin ve diğer küresel güçlerin yanında ağılığını koyma güvenine sahip olacaktır. AB her ne kadar üye devletlerin yetenekleri aracılığıyla "Büyük Güç" statüsü adayı olarak kabul edilme potansiyeline sahip olsa da Birlik kendisini yeni bir küresel güç dengesi oluşturmaya aktif bir katılımcı olarak tasavvur etmemektedir (Stokes ve Whitman, 2013, ss. 1102-1103).

Aynı zamanda, AB'de ortak egemenlik varlığı söz konusudur. Ortak egemenlik ile kastedilen AB'nin ve ayrı ayrı üye devletlerin egemenlikleri değil toplam egemenliktir. Bu durumda hem Birlik hem de üye devletler egemendir. Yalnızca Birlik ve ulusal seviyedeki karar alma çerçevesinde düşünülmemesi gereken egemenlik, bölünen ve paylaşılan bir kavramdır. Böylece, AB'de gücün kullanılma şekli çeşitli düzeylerde ortaya çıkmaktadır. Yetkilerin bazıları ulusal karar alma mekanizmasından bir üst birim olarak nitelendirilen AB'ye aktarılırken, bazıları ise alt birimlere aktarılmaktadır. Bu nedenle Birliğin çok katmanlı bir yönetim yapısının olduğu söylenebilir (Tekin, 2002, ss. 81,85-86). Özellikle AB'de dış ve

güvenlik politikasının uygulanması sorunludur. Bunun nedeni bu alanın hükûmetler arası bir mantıkla çalışıyor olmasından kaynaklanmaktadır. Dolayısıyla, aynı genel zayıflıklar AB'nin siber güvenlik stratejisinde de bulunmaktadır. Bu durumun arkasında, AB'nin bir siber güvenlik temsilcisi olarak rolüne ilişkin hem belirli üye devletler hem de tüm kurum nezdinde gerçek bir Pan-Avrupa vizyonuna sahip olamaması yatmaktadır (Sliwinski, 2014, ss. 479-480). Bu doğrultuda, AB'yi bir siber güvenlik temsilcisi olarak sınırlayan iki temel faktör bulunmaktadır. Birincisi Birliğin hükûmetler arası yapısı, ikincisi ise siber güvenlik alanında AB ile üye ülkeler arasındaki ortak vizyon eksikliğidir (Sliwinski, 2014, s. 468). Her ne kadar her geçen gün ulusal makamlar, siber alanda daha yakın bir iş birliği kurma konusunda kararlı olduklarını dile getirseler de, gerçekte taahhütleri oldukça sınırlı kalmakta, daha çok siber güvenliğin ticaret ve iletişim ile ilgili yönlerine odaklanmaktadır (Sliwinski, 2014, s. 480).

AB'nin bilgi ve iletişim teknolojilerine ilgisinin başlangıç noktası olarak kabul edilen 1985'de yayımlanan Beyaz Kitap'tan 2019'da yürürlüğe giren Siber Güvenlik Yasası'na kadar geçen süre zarfında, Birliğin siber güvenlik yaklaşımı sosyo-ekonomik merkezli olmuştur. Avrupa Komisyonu'nun hazırlamış olduğu ve 1 Ocak 1993 tarihine kadar tek pazar yaratma amacını ortaya atan 1985'deki "Beyaz Kitap", "iç pazar/tek pazar" kavramının kurucu anlaşmada yer almasını sağlayan ve 1 Temmuz 1987'de yürürlüğe giren Avrupa Tek Senedi (ATS), 1 Kasım 1993 tarihinde yürürlüğe girerek, Avrupa Birliği'ni kuran Maastricht Antlaşması (AB Anlaşması-ABA) ile bu durumun çok daha kesin bir hâl almıştır (Köksoy, 2020, s. 649). Diğer yandan ekonomik ve sosyal kalkınmada ağ ve bilgi sistemlerinin ana faktörler olduğunun ifade edildiği 2001'deki "NİS Önerisi" (Commission of the European Communities, 2001, ss. 2, 16); bilgi ve iletişim teknolojilerinin sosyal etkileşim ve ekonomik büyüme açısından büyük önem taşıdığının ve finans, enerji, ulaştırma gibi alanlarda önemli bir role sahip olduğunun belirtildiği 2013'de yayımlanan "Siber Güvenlik Strateji Belgesi" (European Commission, 2013, s. 2); ekonominin dijital teknolojiye bağımlılığından ve siber güvenliğin sağlanmasında ekonomik ve sosyal yapı temelli önlemler alınmasının öneminden bahsedilen 2013'deki Siber Güvenlik Strateji Belgesinin 2017'de yeniden düzenlenmiş şekli (European Commission, 2017b, 2); yine diğer belgelerde de vurgulandığı gibi ağ ve bilgi sistemlerinin ekonomik büyüme ve sosyal refah için kilit bir role sahip olduğunun yinelendiği 2019'da yürürlüğe girmiş olan "Siber Güvenlik Yasası" (Official Journal of the European Union, 2019, s. 15) Birliğin bilgi ve iletişim teknolojilerine yaklaşımının, dolayısıyla siber güvenlik politikasının sosyo-ekonomik temelli olduğunu gösteren önemli örneklerden bazılarıdır (Köksoy, 2020, s. 651).

AB, siber güvenlik stratejisini uygularken, 5 temel sorunun çözülmesi gerekmektedir (Sliwinski, 2014, s. 480). Öncelikle, siber saldırılarda gerek saldırıya engel olma ve saldırı boyunca gerekse saldırının ardından devam eden adli süreç esnasında uluslararası iş birliği gerekli bir hâl almaktadır. Özellikle ulusal bilgi

güvenliği stratejilerinde siber tehditlerin sınır aşan bir niteliğinin olduğu ve bu sebeple uluslararası iş birliği olmadan bir devletin tek başına kendini sayısal bir ortamda güvende hissetmesinin mümkün olamayacağı belirtilmektedir. Siber güvenlik problemlerinin birey, kuruluş ve hatta ülkelerin sosyal ve iktisadi faaliyetleri için önemli bir tehdit olduğu günümüzde bu tehditlerle baş edilebilmesinde ulusal imkânlar tek başına yeterli olmayıp uluslararası iş birliği olanaklarından yararlanmak gerekmektedir (Güngör, 2015, ss. 57,69). Ancak buna rağmen, siber casusluk söz konusu olduğunda, uluslararası iş birliği, devletler arasındaki farklı çıkarlar ve rekabet gibi basit sebeplerle hayal kırıklığı yaratabilmektedir. Bu doğrultuda, üye ülkelerin siber güvenliğe ilişkin ulusal stratejilerinin koordinasyonu, Birliğin kısa vadede en büyük hedefi olacaktır. Ancak tüm Birlik üye ülkeleri aynı güvenlik topluluğuna ait olduğundan ve önemli bir çıkar yakınsaklığı paylaştığından, aralarında bölgesel bir iş birliği oluşturulması gerekmektedir. Aynı şekilde, uluslararası alanda Çin, ABD gibi kilit ortaklarla iş birliği kurmak da son derece önemli olacaktır. Aksi hâlde uluslararası iş birliği olmadan Birlik siber güvenlik tehditlerine karşı etkili bir duruş sergileyemeyecektir (Sliwinski, 2014, ss. 472, 480). Bu doğrultuda, uluslararası iş birliğinin sağlanmasında kurumsal düzenlemelere ve süreç planlamalarına ihtiyaç duyulacaktır (Güngör, 2015, s. 57). İkinci olarak, teknoloji devletler arasındaki ve içindeki güç dengesini değiştirme noktasında oldukça önemli bir faktördür. Bu açıdan internet, yönetenler üzerinde önemli bir baskı meydana getirerek bilgiye kolay ulaşılmasını sağlamaktadır. Teknolojik alanda ortaya çıkan gelişmeler ve iletişimin serbestleşmesi, devletlere siber suçlara karşı mücadelelerinde ya da kritik altyapının korunmasında "fazladan yardım" sağlayabilecek şekilde bireyleri ve özel kuruluşları güçlendirmektedir (Sliwinski, 2014, s. 480).

Öte yandan siber uzay, tüm teknolojik öncüllerinden farklı, bir iletişim aracı oluşturmanın dışında bilgi oluşturmanın, depolamanın, değiştirmenin ve kullanmanın da baskın bir şekli olarak nitelendirilmektedir (Sheldon, 2011, s. 101; Sliwinski, 2014, s. 480). Üçüncüsü, AB siber güvenlik stratejisinin gelecekte zorunludan kurumsala, yapısal ve üretkenliğe kadar farklı siber güç biçimlerini içermesi önemli olacaktır. Sadece dört formun dengeli bir kombinasyonu, gerçekten stratejik bir yaklaşıma izin verecektir. Diğer taraftan Avrupalıların, siber güvenliğe yönelik büyüyen tehditlerin yalnızca kendi devletlerinin güvenliğini değil, aynı zamanda, tüm AB'nin güvenliğini de etkilediğinin farkına varmaları gerekmektedir. Dördüncü olarak siber uzayın fiziksel altyapısının kontrolünün stratejik ve taktiksel açıdan son derece kritik bir öneme sahip olduğu görülmektedir (Deibert, Rohozinski ve Crete-Nishihata, 2012, s. 17). Söz konusu kontrolünse Avrupa devletleri açısından sağlanması serbest piyasa ekonomilerinde devletin rolünün ekonomiden ekonomiye değişmesi nedeniyle sınırlı kalmaktadır. Öte yandan, Colin Crouch modern Batı toplumlarının post-demokrasi olgusuyla karşı karşıya olduğunu belirtmektedir. Bu, devletin işlevlerinin çoğundan çekilmesi ve böylece güvenlik gibi kamu mallarının özel aktörlere açılması şeklinde ifade edilmektedir. Bu noktada, AB politika yapıcılarına hem devletlerin hem de AB'nin siber

güvenlikteki rolünü tanımlamaları için bazı sorumluluklar yüklemektedir. Devletin ve AB'nin siber güvenlikteki rolünün AB politika yapıcıları tarafından kararlı bir şekilde tanımlanması diğer taraftan özel işletmecilerin de güvenlik ihlalleri söz konusu olduğunda (özellikle kritik altyapı ve siber suç durumunda) hangi koşullarda ne derece yükümlülüklerinin olduğunu bilmelerini sağlayacak ve hatta onları sorumluluklarının yer aldığı daha ayrıntılı bir mevzuat takip etmek zorunda bırakacaktır. Birlik, siber güvenlik stratejisini uygularken, çözülmesi gereken temel sorunlar noktasında son olarak, siber güvenlik ya da siber güvenlik stratejisi ile gerçekte ne kastedildiğinin AB siber güvenlik stratejisinde açıklığa kavuşturulması gerekmektedir. Aynı zamanda, AB siber güvenlik stratejisi ulusal eylemlerin koordinasyonundan çok daha fazlasına ihtiyaç duymaktadır. İhtiyaç duyulan şey, zorlukların ve tehditlerin doğaüstü bir şekilde algılanması ve bunları ele alacak uygulanabilir araçlara sahip olunmasıdır. Böyle bir yaklaşım, belki de uzun süredir Avrupa entegrasyonunu karakterize eden yayılmanın yardımıyla, devlet güvenlik politikalarını daha da Avrupalılaştıracaktır (Sliwinski, 2014, s. 480-481).

6. Sonuç

Bilginin değerinin git gide artması neticesinde içinde yer aldığımız çağ bilgi çağı olarak ifade edilmekte olup, ihtiyaç duyulan bilgiye sürekli gelişim ve dönüşüm hâlinde olan bilgi ve iletişim teknolojileri yardımıyla hızlı ve kolay bir biçimde ulaşılabilmekte ve aynı zamanda bilgi paylaşılabilmektedir. Bu durum, bilgi ve iletişim teknolojilerini günlük hayatımızın vazgeçilmez bir parçası hâline getirmektedir. Her dönem önemini koruyan bilgiye bilgi ve iletişim teknolojilerinin yaratmış olduğu imkânlarla erişilebilmesi, bilginin iletilmesi, saklanması ve kullanılması ile birlikte ülkelerin ekonomik, siyasi ve askeri güçlerinin olumlu bir yönde yükselişe geçmesi siber ortamın önemini daha da artırmaktadır. Ancak bilgi ve iletişim teknolojileri aracılığıyla siber ortamın sağlamış olduğu faydaların yanında bu ortamın tehdit, zarar verme, saldırı gibi amaçlarla kullanılması kişilere, kurumlara ve ülkelere ciddi zararlar vermektedir. Kısaca bilginin elektronik bir ortamda bulunması ve muhafaza edilmesi, onu siber saldırılara açık bir hâle getirmektedir. Bu durum da siber güvenlik konusuna ilginin yükselmesine neden olmaktadır. Dolayısıyla, siber tehditlerin ve saldırıların git gide artması ile beraber bilgi ve iletişim sistemlerinin bu tehdit ve saldırılardan korunmasının farklı bir söylemle siber güvenliğin sağlanmasının yolları aranmaktadır. Bu doğrultuda, bilgi ve iletişim sistemlerinin siber saldırılardan korunması diğer deyişle bilgi ve verilerin güvenliğinin sağlanması kapsamında siber güvenlik alanında etkili ve uygulanabilir stratejiler ve politikalar geliştirmek ülkeler için gerekli bir hususu teşkil etmektedir. Bu noktada, AB'nin de siber güvenliğin sağlanması kapsamında çeşitli stratejiler ve politikalar geliştirmeye çalışan bir aktör olduğu görülmektedir.

1985'de Avrupa Komisyonu tarafından yaratılan "Tek Pazar İnsiyatifi" AB'nin siber güvenlik politikasındaki çalışmalarının başlangıcını oluşturmaktadır. Birlik "Tek Pazar İnsiyatifi"'nden günümüze kadar ekonomik açıdan faydanın

sağlanması, temel hakların korunması, siber saldırıların engellenmesi, dijital sistemlere duyulan güvenin artırılması ve aktörler arasındaki iş birliğinin daha da güçlendirilmesi gibi hedefler doğrultusunda sosyo-ekonomik merkezli siber güvenlik stratejileri ve politikaları geliştirmeye çalışmaktadır. Dolayısıyla, siber güvenlik konusu AB tarafından üzerinde durulan son derece önemli bir konu hâline gelmiştir. Bu durumdan hareketle, AB'nin siber güvenlik alanındaki politikalarının ve uygulamalarının ne kadar etkin olduğunun ve bir siber güvenlik temsilcisi olarak nitelendirilen AB'nin bu alandaki yeterliliğinin değerlendirilmeye çalışıldığı bu çalışmada AB çerçevesinde siber güvenlik ile ilgili bütüncül aynı zamanda kolektif bir vizyona sahip ortak bir tanımın olmadığı görülmektedir. Birlik üye devletlerinin siber güvenlik ile ilgili kendine özgü tanımlamaları ve stratejileri bulunmaktadır. Bu durum, Avrupa'nın siber tehditlere karşı etkili bir duruş sergileyememesine neden olmaktadır. AB'nin siber tehditlere karşı etkili bir duruş sergileyebilmesi için öncelikle AB ekseninde bir siber güvenlik anlayışı yaratılması gerekmektedir.

AB'nin hükûmetler arası yapısı, Birlik ve üye ülkeler arasındaki ortak vizyon eksikliği, Birliği siber güvenlik alanında sınırlayan iki temel faktörü oluşturmaktadır. Dolayısıyla, bir siber güvenlik temsilcisi olarak nitelendirilen Birliğin hem üye devletler hem de kurum nezdinde Pan-Avrupa vizyonuna sahip olmadığı görülmektedir. Bu durum, Birliğin siber güvenlik stratejisinin uygulanmasını zorlaştırmakta, bir siber güvenlik temsilcisi olarak Birliğin küresel rolüne zarar vermekte ve uluslararası alanda diğer güçlerle ilişkilerindeki başarısını olumsuz yönde etkilemektedir. Birlik üyesi ülkeler her seferinde siber güvenlik alanında iş birliği konusundaki kararlılıklarını vurgulasalar da bu söylemlerinin oldukça sınırlı kaldığı ve gerçeği yansıtmadığı görülmektedir. Bu doğrultuda, üye devletlerin aynı güvenlik topluluğuna ait olmaları ve benzer çıkarlara sahip olmaları sebebiyle aralarında bir bölgesel iş birliği yaratılması ve siber güvenliğe ilişkin ulusal stratejilerinde bir koordinasyon sağlanması önemli olacaktır. Aynı zamanda, siber güvenlik tehditlerinin sınır aşan bir niteliğe sahip olduğu düşünüldüğünde tehditlere etkili bir yanıt verilebilmesi için Birlik uluslararası alanda kilit ortaklarla iş birliği yapması, bunun için de uluslararası iş birliğini sağlayacak olan kurumsal düzenlemelerin ve süreç planlamalarının öncelikli hâle getirilmesi gerekmektedir.

Kısaca, siber güvenliğin sağlanması çerçevesinde çeşitli stratejiler ve politikalar geliştiren ve geliştirmeye devam eden Birliğin, siber güvenlik tehditleri karşısında çok daha etkin bir duruş sergilemesi ve aynı zamanda strateji ve projelerinin siber güvenlik alanında etkili olabilmesi için AB düzeyinde ortak bir siber güvenlik anlayışı yaratılması, siber güvenlik ve siber güvenlik stratejisi ile tam olarak ne kastedildiğinin AB siber güvenlik stratejisinde açıkça ifade edilmesi, üye devletler arasında bölgesel bir iş birliğinin geliştirilmesi ve üye devletlerin siber güvenliğe ilişkin ulusal stratejilerinde koordinasyon sağlanması, Birliğin uluslararası alanda kilit ortaklarla iş birliği yapması ve dolayısıyla uluslararası iş birliğini sağlayacak düzenlemelere ve süreç planlamalarına öncelik verilmesi Birliğin kısa vadede gerçekleştirmesi gereken hedefleri arasında yer almalıdır.

Kaynakça

Akarçay, P. ve Ak, G. (2018). Rethinking cyber warfare: Timeless, normless and unconstrained. *IKSAD Journal*, 4(9), 195-214.

Akbaş, G., B. (2022). Avrupa Birliği siber güvenlik politikası ve ENISA. T.C. Sanayi ve Teknoloji Bakanlığı Stratejik Araştırmalar ve Verimlilik Genel Müdürlüğü, 34(398), 1-50. https://edergi.sanayi.gov.tr/File/Journal/2022/2/2_2022.pdf (Erişim Tarihi: 26 Şubat 2023)

Atakan, M. (2021). Siber güvenlik risklerinin ve Covid 19 salgınının uzaktan denetim üzerindeki etkileri. *Denetişim*, 11(22), 27-39.

Bangemann, M. (1994). Recommendations to the European Council. https://www.cyber-rights.org/documents/bangemann.htm (Erişim Tarihi: 06 Ocak 2023)

Commission of the European Communities. (1996). Illegal and harmful content on the internet. http://aei.pitt.edu/5895/1/5895.pdf (Erişim Tarihi: 8 Ocak 2023)

Commission of the European Communities. (2001). Network and information security: Proposal for a European policy approach. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298&from=EN (Erişim Tarihi: 8 Ocak 2023)

Craigen, D., Thibault, D. N. ve Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 13-21.

Deibert, J. R., Rohozinski, R. ve Crete-Nishihata, M. (2012). Cyclones in cyberspac: Information sharing and denial in the 2008 Russia-Georgia war. *Security Dialogue*, 43(1), 3-24.

ENISA. (t.y.). About ENISA. https://www.enisa.europa.eu/about-enisa (Erişim Tarihi: 8 Ocak 2023)

ENISA. (2017). ENISA overview of cybersecurity and related terminology. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology (Erişim Tarihi: 4 Ocak 2023)

European Commission. (1985). Completing the international market. https://eur-lex.europa.eu/legal-

content/EN/TXT/PDF/?uri=CELEX:51985DC0310&from=EN (Erişim Tarihi: 6 Ocak 2023)

European Commission. (2013). Cybersecurity strategy of the European Union: An open, safe and secure cyberspace. https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (Erişim Tarihi: 13 Ocak 2023)

European Commission. (2015a). The European agenda on security. https://www.europarl.europa.eu/cmsdata/125863/EU%20agenda%20on%20security.pdf (Erişim Tarihi: 13 Ocak 2023)

European Commission. (2015b). A digital single market strategy for Europe. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN (Erişim Tarihi: 8 Ocak 2023)

European Commission. (t.y.) NIS Directive. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (Erişim Tarihi: 13 Ocak 2023)

European Commission. (2017a). Proposal for a regulation of the European Parliament and of the Council on Enisa, the "EU cybersecurity agency", and repealing regulation (EU) 526/2013, and on information and communication technology cybersecurity certification ("Cybersecurity act"). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0477&from=EN (Erişim Tarihi: 14 Ocak 2023)

European Commission. (2017b). Joint communication to the European Parliament and the Council: Resilience, deterrence and defence: Building strong cybersecurity for the EU. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en (Erişim Tarihi: 25 Şubat 2023)

European Commission. (2020). New EU cybersecurity ctrategy and new rules to make physical and digital critical entities more resilient. New_EU_Cybersecurity_Strategy_and_new_rules_to_make_physical_and_digital_critical_entities_more_resilient.pdf (Erişim Tarihi: 14 Ocak 2023)

European Commission. (2022). Cyber Resilience Act. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act (Erişim Tarihi: 14 Mayıs 2023).

European Council. (1994). Presidency conclusions. https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/00150.EN4.htm (Erişim Tarihi: 6 Ocak 2023)

European Parliament and Council. (1995). Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046 (Erişim Tarihi: 8 Ocak 2023)

Negreiro, M. (2013). The NIS 2 Directive: A high common level of cybersecurity in the EU. European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf (Erişim Tarihi: 12 Mayıs 2023)

European Union. (2006). Strategy for a secure information society (2006 communication). https://eur-lex.europa.eu/EN/legal-content/summary/strategy-for-a-secure-information-society-2006-communication.html (Erişim Tarihi: 9 Ocak 2023)

Federal Ministry of the Interior, Building and Community. (2021). Cyber Security Strategy for Germany 2021. https://www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-security-strategy-node.html (Erişim Tarihi: 4 Şubat 2023)

Güngör, M. (2015). Ulusal bilgi güvenliği: Strateji ve kurumsal yapılanma, Uzmanlık Tezi, T.C. Kalkınma Bakanlığı Yönetim Hizmetleri Genel Müdürlüğü Bilgi ve Belge Yönetim Daire Başkanlığı, Yayın No:2919. http://www.bilgitoplumu.gov.tr/wp-content/uploads/2015/11/Ulusal_Bilgi_Guvenligi_Strateji_ve_Kurumsal_Yapilanma.pdf (Erişim Tarihi: 4 Şubat 2023)

Helmbrecht, U., Purser, S. ve Klejnstrup, R. M. (2012). Cyber security : Future challenges and opportunities. ENISA. https://www.btg.org/wp-content/uploads/2012/01/ENISA-Cyber-Security-Report-2011.pdf (Erişim Tarihi: 2 Şubat 2023)

Kaya, B. M. ve Aksöz, E. (2023). NIS 2 Direktifi: AB'de yeni siber güvenlik kuralları. Turkish Law Blog. https://turkishlawblog.com/insights/detail/nis2-direktifi-abde-yeni-siber-guvenlik-kurallari (Erişim Tarihi: 12 Mayıs 2023)

Kovacs, L. (2018). Cyber security policy and strategy in the European Union and NATO. Land Forces Academy Review, 23(1), 16-24. https://doi.org/10.2478/raft-2018-0002

Köksoy, F. (2020). Avrupa Birliği'nin siber güvenlik politikası: Kurumsalcılık mı tutarlılık mı?. *Güvenlik Stratejileri Dergisi*, 16(15), 635-674. doi:10.17752/guvenlikstrtj.807014

Kurnaz, S. ve Önen, M. S. (2019). Avrupa Birliği'ne uyum sürecinde Türkiye'nin siber güvenlik stratejileri. *International Journal of Politics and Security*, 1(2), 82-103.

Lawels. (2022). The NIS2 directive was officialy published in the official journal of the EU. https://lawels.com/en/2022/12/27/the-nis2-directive-was-officially-published-in-the-official-journal-of-the-eu/ (Erişim Tarihi: 2 Şubat 2023)

Nezgitli, S. ve Benzer, R. (2020). Avrupa Birliği siber güvenlik kanunu. *Bilişim Sistemleri ve Yönetim Araştırmaları Dergisi*, 2(1), 10-17.

Ministry of Digital Affairs. (2017). National framework of cybersecurity policy of the Republic of Poland for 2017-2022: Respecting the rights and freedoms in cyberspace comprehensive approach to security cybersecurity as an important element of the state policy. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Cybersecuritystrategy_PL.pdf (Erişim Tarihi: 2 Şubat 2023)

Official Journal of the European Communities. (2002). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002: Concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN (Erişim Tarihi: 8 Ocak 2023)

Official Journal of the European Union. (2005). Council framework decision 2005/222/JHA of 24 February 2005 on attacks against information systems. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN (Erişim Tarihi: 9 Ocak 2023)

Official Journal of The European Union. (2006). Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending directive 2002/58/E. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0024 (Erişim Tarihi: 9 Ocak 2023)

Official Journal of the European Union. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union agency for cybersecurity) and on information and communications technology cybersecurity certification and repealing regulation (EU) No 526/2013 (cybersecurity act). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN (Erişim Tarihi: 25 Şubat 2023)

Official Journal of the European Union. (2022a). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555 (Erişim Tarihi: 12 Mayıs 2023)

Official Journal of the European Union. (2022b). Regulations: Regulation (EU) 2022/2554 of the European Parliament and of the Councıl of 14 December 2022: On digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554 (Erişim Tarihi: 14 Mayıs 2023)

Oxford University Press. (2014). Oxford online dictionary. Oxford: Oxford University Press. http://www.oxforddictionaries.com/definition/english/Cybersecurity (Erişim Tarihi: 25 Şubat 2023)

Özden, Ü. S. (2023). AB finansal hizmetler sektörü aktörleri için operasyonel dayanıklılık yasası yürürlüğe girdi. Erdem&Erdem. https://www.erdem-erdem.av.tr/bilgi-bankasi/ab-finansal-hizmetler-sektoru-aktorleri-icin-dijital-operasyonel-dayaniklilik-yasasi-yururluge-girdi (Erişim Tarihi: 13 Mayıs 2023)

Pavlidis, G. (2021). Europe in the digital age: Regulating digital finance without suffocating innovation. *Law, Innovation and Technology*, 13(2), 464-477. DOI: 10.1080/17579961.2021.1977222

Public Works and Government Services Canada. Translation Bureau. (2012). Emergency management vocabulary: Terminology bulletin 281. Gatineau: Publıc Works and Government Services Canada. https://publications.gc.ca/site/eng/417764/publication.html (Erişim Tarihi: 25 Şubat 2023)

Sheldon, B. J. (2011). Deciphering cyberpower: Strategic purpose in peace and war. *Strategic Studies Quarterly*, 95-112.

Sliwinski, F. K. (2014). Moving beyond the European Union's weakness as a cyber security agent. *Contemporary Security Policy*, 35(3), 468-486. https://doi.org/10.1080/13523260.2014.959261

Singer, P. W. ve Friedman, A. (2014). Cyber security and cyber war: What everyone needs to know. New York: Oxford University Press.

Stokes, D. ve Whitman, G. R. (2013). Transatlantic triage? European and UK 'grand strategy' after the US rebalance to Asia. *International Affairs (Royal Institute of International Affairs 1944-)*, 89(5), 1087-1107.

Şenol, M. (2016). Siber güçle caydırıcılık ama nasıl?. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 2(10), 10-17.

Şenol, M. (2017). Türkiye'de siber saldırılara karşı caydırıcılık. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*. 3(2), 1-9.

Tekin, K. (2002). Avrupa Birliği ve egemenlik kavramı. *Türk İdare Dergisi*, 434, 71-87.

Ünver, M. ve Canbay, C. (2010). Ulusal ve uluslararası boyutlarıyla siber güvenlik. *Elektrik Mühendisliği*, 438, 103.

Yeniyıldız, N. S. (t.y.a). AP ve Konseyden siber güvenlik kurallarını güçlendirmeye yönelik yeni adımlar. İktisadi Kalkınma Vakfı. https://www.ikv.org.tr/images/files/Siber_Guvenlik_Kurallarinin_Guclendirilmesi_Bilgi_Notu.pdf (Erişim Tarihi: 12 Mayıs 2023)

Yeniyıldız, N. S. (t.y.b). Avrupa Komisyonundan Siber Dayanıklılık Yasası. İktisadi Kalkınma Vakfı. https://www.ikv.org.tr/images/files/Siber_Dayaniklilik_Yasasi_Bilgi_Notu(1).pdf (Erişim Tarihi: 14 Mayıs 2023)

Etik Beyanı: Yazarlar, bu çalışmanın tüm hazırlanma süreçlerinde etik kurallara uyulduğunu beyan etmektedir. Bilimsel etik konuları ile ilgili aksi bir durumun tespiti halinde tüm sorumluluk çalışmanın yazarlarına ait olup, Çankırı Karatekin Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi'nin hiçbir sorumluluğu bulunmamaktadır.

Effectiveness of EU Policies and Practices in the Field of Cyber Security: EU's Competence as a Cyber Security Representative

Extended Abstract

1. Introduction

With the increase in the value of information each passing day, information can be accessed quickly and easily through information and communication technologies, which show a very rapid transformation and development in the age we live in that is characterized as the information age. In other words, the positive rise of the economic, political and military powers of the countries as a result of being able to access, transmit, process, protect and use information with the opportunities provided by information and communication technologies, which have maintained their importance from the beginning of human history to this day, has made information and communication technologies indispensable elements of our lives, and therefore the importance of the cyber environment has increased even more.

In addition to the advantages of the cyber environment with the developments in information and communication technologies, the use of this environment for attack, threat, harm, etc. causes serious damage to individuals, institutions and countries. To put it in a different way, the fact that information is found and stored in an electronic environment today has made it vulnerable to cyber attacks, therefore focus has been more on cyber attacks, rather than the advantages of information and communication technologies. Since this situation has made cyber security a very important issue, ways of protecting information and communication technologies from cyber attacks and thus ensuring cyber security have been sought. Within this context, it has become necessary for countries to develop an effective cyber security strategy and policy to protect information and communication systems from cyber attacks and to ensure the security of information and data. EU, in particular, is an actor that strives to develop various strategies and policies for ensuring cybersecurity. In this regard, this study tries to evaluate how effective the EU's policies and practices in the field of cyber security are and the competence of EU which is described as a cyber security representative, in this field.

2. Evaluation and Discussion

The "Single Market Initiative", created by the European Commission in 1985, is the starting point for the EU's cybersecurity policy efforts. The EU has been working on developing socio-economic-based cybersecurity strategies and policies with the goal of achieving economic benefits, preventing cyberattacks, protecting fundamental rights, increasing trust in digital systems, and enhancing collaboration among actors from the beginning of the "Single Market Initiative" until the present day. It is seen that the Union, which has developed various strategies and policies to provide cyber security, does not have a common definition that includes a holistic, collective vision regarding cyber security. In other words, EU has an important deficiency in defining the cyber security concept on a common ground and in standardizing it at the same time. Each EU member state has its own unique definitions and strategies regarding cyber security. Thus, the lack of a common vision between the Union and its member states, as well as the intergovernmental structure of the Union, emerge as two main factors limiting the Union. This situation complicates the implementation of the Union's cyber security strategy, causes it fail to take an effective stance against threats as a cyber security representative and negatively affects its global role. Thus, the success of the EU in its relations with other powers in the international arena is also negatively affected by this situation.

3. Conclusion

In order for the EU to play an effective role in the face of cyber security threats, firstly, it is necessary to define and standardize the concept of cyber security in a common ground in terms of terminology, in other words, to create a cyber security understanding within the framework of the Union. Moreover, since the member states belong to the same security community and have similar interests, it will be important to create a regional cooperation between them and to coordinate their national strategies on cyber security. In other respects, because of the cross-border nature of cyber security threats, the Union should also cooperate with key partners in the international arena in order to deal with these threats. In this context, institutional arrangements and process planning that will ensure international cooperation should be prioritized.