Güv. Str. Derg. 2020, 16(35): 635-674
DOI: 10.17752/guvenlikstrtj.807014

Araştırma Makalesi
Research Article

Avrupa Birliği'nin Siber Güvenlik Politikası: Kurumsalcılık mı Tutarlılık mı?

The Cyber Security Policy of European Union: Institutionalism or Coherence?

Fulya KÖKSOY*

Öz

Bilgi ve iletişim teknolojilerinin özellikle son dönemde hayatımıza yoğunluklu olarak entegre olduğu görülmektedir. Dijital çağın önüne geçilemez bir hızla değişim ve dönüşüm geçirmesi, pek çok avantaja neden olsa da beraberinde risk ve tehditleri getirmektedir. Öyle ki siber saldırılar bireylere, kurumlara ve devletlere yönelik önemli bir tehdit oluşturmaktadır. Bu bağlamda, son derece kırılgan bir dünya kompozisyonu ile karşılaşılmakta ve siber güvenlik kavramı ön plana çıkmaktadır. Siber güvenliğin sağlanması hususunun son derece önemli olması çerçevesinde Avrupa Birliği (AB) de dijitalleşen dünyadan kaynaklanan tehditleri kabul eden ve siber alanın güvenliğini sağlamaya dönük stratejiler ve politikalar geliştirmeye çalışan bir aktördür. Bu minvalden hareketle çalışmada, uluslararası sistemde kendine münhasır bir muhtevaya sahip olan ve 1 Aralık 2009 tarihinde yürürlüğe giren Lizbon Antlaşması ile beraber tüzel kişilik kazanan Avrupa Birliği'nin siber güvenlik politikaları analiz edilmekte, AB ile siber güvenlik olgusu bağlamında nasıl bir denklem ortaya çıkmaktadır? sorusuna cevap aranmakta ve bu denklemin, resmî (kurumlar) ve gayri resmî (kurallar, prosedürler gibi) yapılar ekseninde AB'nin siber güvenlik politikasının analiz edilmesini sağlayan kurumsalcılık mı yoksa tutarlılık bağlamında mı kurulduğuna odaklanılmaktadır.

* Dr. Öğr. Üyesi, Batman Üniversitesi, İktisadi ve İdari Bilimler Fakültesi Uluslararası İlişkiler Bölümü, ORCID: 0000-0002-6915-5620, e-posta: fulya.koksoy@batman.edu.tr.

Geliş Tarihi / Submitted: 18.05.2020
Kabul Tarihi / Accepted: 31.05.2020

Anahtar Kelimeler: *Avrupa Birliği, Siber Güvenlik, Tarihsel Kurumsalcılık, Tutarlılık, Avrupa Birliği'nin Siber Güvenlik Politikası.*

Abstract

It is seen that information and communication technologies have been intensely integrated into our lives especially in the recent period. The digital age has been changed and transformed at an unavoidable rate, despite it causes many advantages, but it also brings risks and threats. In fact, cyber-attacks pose an important threat to individuals, institutions and states. In this context, an extremely fragile world composition is encountered and the concept of cyber security comes to the fore. As the issue of ensuring cyber security is extremely important, the European Union (EU) is an actor that accepts threats arising from the digital world and tries to develop strategies and policies to ensure the security of the cyber space. Concordantly, the cyber security policies of the European Union, which has sui-generis content in the international system and gained legal status by Lisbon treaty entered into force on 1 December 2009, are analyzed. In addition to this, the equation arises between the European Union and the cyber security phenomenon has been examined for finding out whether the equation is built on institutionalism, which enables the analysis of the EU's cyber security policy on the basis of formal (institutions) and informal (such as rules, procedures) structures, or consistency.

Keywords: *European Union, Cyber Security, Historical Institutionalism, Coherence, European Union's Cyber Security Policy.*

Giriş

Çağdaş güvenlik yaklaşımları içerisinde kendine yer edinen iki önemli kavram söz konusudur: siber ve bu doğrultuda siber güvenlik. Güvenliğe ilişkin literatür analiz edildiği takdirde, özellikle son birkaç yıldır siber olgusu üzerine odaklanıldığı görülmektedir. Bilgi ve iletişim teknolojilerinin çığır açan bir boyutta gelişim göstermesini takiben, güvenlik ve siber alan ortak bir payda da buluşmakta ve son dönemde söz konusu alana yönelik ilgi peyderpey artmaktadır. Bu kapsamda günümüzde uluslararası sistemde yer alan

irili ufaklı birçok devletin yanı sıra, Kuzey Atlantik Anlaşması Örgütü (*North Atlantic Treaty Organization*/NATO) veya ve ya AB gibi uluslararası örgütlerin de kendi siber güvenlik strateji planlamalarını hazırlamaya başlamışlardır. Bununla birlikte NATO'ya kıyasla AB'nin siber güvenlik politikasına ilişkin yapılan çalışmalar ise bugüne kadar sınırlı düzeyde kalmıştır.[1] Bir diğer ifadeyle, ilgili literatür analiz edildiğinde AB'nin ekonomi, dış politika, savunma, güvenlik, çevre ve finans gibi çeşitli alanlardaki politikalarına yönelik birçok çalışmanın olduğu fakat siber güvenlik alanındaki politikalarına ilişkin literatürün kısır kaldığı ve önemli bir boşluk olduğu gözlemlenmektedir. Mevzubahis boşluğun analiz edilmesi amacıyla ortaya konan bu çalışmanın özünde AB'nin siber güvenlik politikası incelenmekte, Tarihsel Kurumsalcılık kuramı ve Tutarlılık yaklaşımı/modeli çerçevesinde söz konusu politikanın ne yönde bir gelişim gösterdiği (kurumsallaşma ve/veya tutarlılık) sorunsallaştırılmaktadır.

Yeni Kurumsalcılık kuramı altında yer alan Tarihsel Kurumsalcılık teorisi ekseninde, AB'nin siber güvenlik alanına hangi açıdan -askerî, sosyal, ekonomik vb- yaklaştığı ve zaman kavramına odaklanan kuram bağlamında söz konusu yaklaşımda herhangi bir değişim yaşanıp yaşanmadığı, siber güvenlik alanında faaliyet gösteren kurumların, kurumsal düzenlemelerin ve siber güvenlik politikasıyla ulaşılmak istenen hedeflerin geçmişten günümüze nasıl bir gelişim gösterdiği analiz edilmektedir. Bu noktada, kronolojik bir düzlemde AB'nin bilgi ve iletişim teknolojilerine yönelik ilgisinin başlangıç noktasını oluşturan 1985 yılındaki "Beyaz Kitap'tan" 2019 yılında yürürlüğe giren "Siber Güvenlik Yasası'na" kadar geçen 34 yılda ortaya konan ilgili dokümanlar içerik analizine tabi tutulmaktadır. 2013 yılında Avrupa Komisyonu tarafından yayımlanan "Siber Güvenlik Strateji Belgesi", AB'nin siber güvenlik politikasının somut bir zemine oturmasında önem arz ettiği için öncelikle söz konusu belge ayrıntılı olarak incelenerek, diğer

[1] Ali B. Darıcılı, "Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Siber Güvenlik Modeli için Öneriler", *TESAM Akademi Dergisi*, 2019, Cilt 6, Sayı 2, 11-33, s. 14.

belgelerin içerik analizinde kullanılacak kodlar elde edilmiştir. AB'nin yaklaşımı bağlamında sosyo-ekonomi kavramı, hedefleri ekseninde ise ekonomi, güven, dijital, temel haklar, siber suçların önlenmesi ve iş birliği kavramları ekseninde bir kodlama listesi oluşturularak söz konusu analiz pratik boyuta taşınmıştır.

Öte yandan, geniş bir politika spektrumu içerisinde yer alan AB'nin, siber güvenlik alanında hem üzerine inşa edildiği statik yapıya rağmen değişim ve dönüşüm odaklı yaptığı retorik vurgu hem de siber güvenlik alanında rol oynayan oyuncular ve enstrümanlar çerçevesinde karmaşık bir aktör portresi çizdiği görülmektedir. Söz konusu bu karmaşık yapı ise bir bütün olarak güvenlik özel de ise siber güvenlik alanında tutarlılığın olması gerekliliğinin altını çizmektedir. Bu doğrultuda, AB siber güvenlik alanında tutarlı bir aktör olarak değerlendirilebilir mi? sorusuna cevap aranmaktadır. Bir diğer ifadeyle, AB'nin tutarlılığının analiz edilmesi ve bunu siber güvenlik alanına yansıtma amacı söz konusudur.

Ortaya konan bu şablon ekseninde çalışmanın ilgili bölümleri gün yüzüne çıkmaktadır. Bu noktada ilk bölümde, AB bağlamında siber güvenliğe ilişkin ortak bir kavramsallaştırma olup olmadığı analiz edilmektedir. Daha sonra çalışmanın üzerine inşa edildiği tarihsel kurumsalcılık teorisine ve tutarlılık yaklaşımına ilişkin teorik çerçeve çizilmektedir. Üçüncü bölümde; yaklaşım, uygulama ve hedefler bağlamında AB'nin siber güvenlik politikalarının kronolojik bir düzlemde analizi sonrası, son kısımda ise söz konusu politika tarihsel kurumsalcılık ve tutarlık yaklaşımı çerçevesinde analiz edilerek, çalışmaya adını veren "AB'nin Siber Güvenlik Politikaları: Kurumsalcılık mı Tutarlılık mı?" sorusuna cevap aranmaktadır.

1. Avrupa Birliği Ekseninde Siber Güvenliğin Kavramsallaştırılması: Ortak Bir Siber Güvenlik Tanımı Var mı?

Siber uzay; yeni, karmaşık, çok boyutlu ve tam anlamıyla keşfedilemeyen bir alanı teşkil etmektedir. Bir bütün olarak siberin çok boyutlu ve küresel doğası çerçevesinde siberden doğan terimlere ilişkin

somut manada kabul gören bir tanımlama bulunmamaktadır.[2] Bu noktada, siber uzay terimini kavramsallaştırma çabası, benzer şekilde siber güvenlik terimi bağlamında da devam etmektedir.

İlgili literatür analiz edildiği takdirde; devletler, uluslararası örgütler, bölgesel örgütler gibi çeşitli aktörlerin siber güvenliğe ilişkin bir tanımlama yapmaya çalıştıkları görülmektedir.[3] AB ekseninde ise siber güvenliğe yönelik bütüncül bir anlayış ve kolektif bir vizyonu içeren, ortak bir tanım yapılmamıştır. Nitekim AB'nin siber güvenlikle ilişkili temel belgesi olan ve 7 Şubat 2013 tarihinde Komisyon tarafından yayımlanan "Avrupa Birliği'nin Siber Güvenlik Strateji" (*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*) belgesinde, söz konusu stratejinin 2017 yılında revize edilmiş versiyonunda (*Resillience, Deterrence and Defence:Building Strong Cybersecurity for the EU*) ve 11 Mart 2019 tarihinde Avrupa Parlamentosu'nda onaylanan ve 27 Haziran 2019 tarihinde yürürlüğe giren "Siber Güvenlik Yasası" (*Cyber Security Act*) içinde siber güvenlik tanımı bulunmamaktadır. Ancak AB'ye bağlı, ağ ve bilgi güvenliğinden sorumlu olan Avrupa Ağ ve Bilgi Güvenliği Ajansı, (*European Network and Information Security Agency*-ENISA) siber güvenliği tanımlamıştır. Söz konusu tanım çerçevesinde siber güvenlik; " bilgi, bilgi sistemleri, altyapılar ve uygulanmaların siber tehdit ve saldırılardan korunmasıdır".[4] Ayrıca şekil 1'de görüldüğü gibi ENISA tarafından siber güvenliğin korunmasına yönelik katmanlara ayrılan bir piramit ortaya konmaktadır.

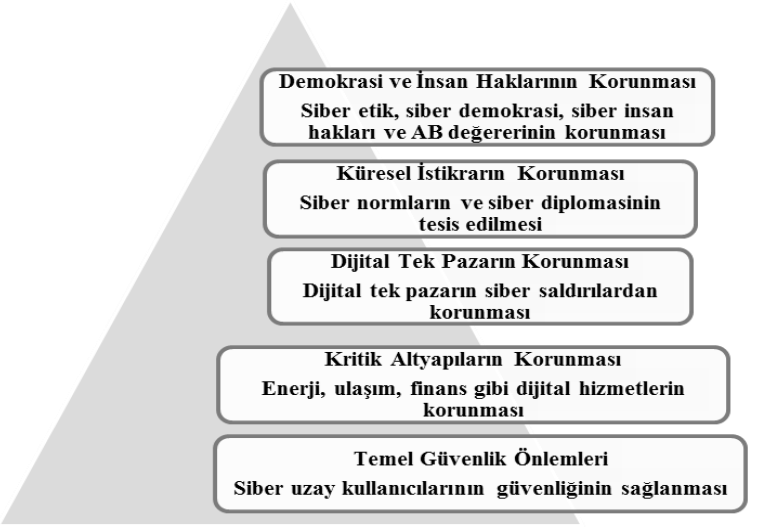
---

[2] Dan Craigen vd., "Defining Cybersecurity", *Technology Innovation Management Review*, 2014, p.1, https://timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf, (Erişim Tarihi: 18.02.2020).

[3] Ibid.

[4] Udo Helmbrecht vd., "Cyber Security: Future Challenges and Oportunities", 2012, p.13, https://www.btg.org/wp-content/uploads/2012/01/ENISA-Cyber-Security-Report-2011.pdf, (Erişim Tarihi:03.05.2020).

Şekil 1: Siber Güvenlik Katmanları[5]



ENISA tarafından siber güvenliğin korunmasına ilişkin ortaya konulan bu piramit ekseninde belirtmek gerekir ki siber güvenlik şemsiye bir kavramı teşkil etmekte ve bu doğrultuda resmî ve genel kabul gören bir tanım ortaya konulamamaktadır. Ancak bu yaklaşımın, siber güvenliği tanımlamaya yönelik somut bir çabayı teşkil ettiği görülmektedir.

Öte yandan, AB üye devletlerinin siber güvenliğe ilişkin kendi stratejileri ve kavramsallaştırmaları bulunmaktadır.[6] Bir diğer ifadeyle, birçok AB üyesi siber güvenliği kendince tanımlamaktadır. Ancak söz konusu bu durum ekseninde sorun yaşanmaktadır. Örneğin, Almanya'ya göre siber güvenlik; siber uzayın kullanılabilirliğinin sağlanması, siber

[5] ENISA, "Overview of Cybersecurity and Related Terminology", 2017, https://www.enisa.europa.eu/publications/enisa-positionpapers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology, (Erişim Tarihi:03.05.2020).

[6] Feliks Sliwinski, "Moving beyond the European Union's Weakness as a Cyber Security Agent", *Contemporary Security Policy*, 2014, Vol 35, No 3, 468-486, p. 468.

uzaydaki verilerin bütünlüğü, özgünlüğü ve gizliliğinin korunması[7] anlamına gelirken Polonya somut bir tanım ortaya koymamıştır.[8] Diğer taraftan, çok daha yeni bir tarih olan 2018 yılında revize edilen Çekya'nın siber güvenlik strateji belgesinde de siber güvenliğe ilişkin bir tanımın söz konusu olmadığı görülmektedir (*Strategie Kybernetické Obrany ČR,* 2018).[9] Üstüne üstlük, siber güvenliğe ilişkin üye devletlerin yaklaşımlarında da farklılık gözlemlenmektedir. Öyle ki Fransa askerî ve istihbarat temelli bir yaklaşım sergilerken Almanya ve Hollanda sivil ve hukuki odaklıdır. Estonya ise hem askerî ve istihbarat hem de sivil ve hukuki bir yaklaşım ortaya koymaktadır.[10] Sonuç olarak, AB bağlamında terimin terminolojik olarak ortak bir payda da tanımlanması ve standartlaştırılmasında önemli bir boşluk olduğu görülmektedir.

2. Teorik Çerçeve

Avrupa Birliği ve siber güvenlik denkleminin analiz edilmesi noktasında bunun arka planındaki kurumsal dinamikleri ve AB'nin ne ölçüde tutarlılık gösterdiğini anlamak önem arz etmektedir. Bu noktada devreye, "Tarihsel Kurumsalcılık Teorisi" ve "Tutarlılık Yaklaşımı" girmektedir.

Çalışmanın üzerine inşa edildiği ana teori olan; kurumları resmî yapılar ve prosedürler, rutinler, normlar, sözleşmeler gibi gayri resmî yapılar ekseninde tanımlayan tarihsel kurumsalcılık,[11] teoriye yönelik

---

[7] Federal Ministry of the Interior, "Cyber Security Strategy for Germany", p.4, https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile, (Erişim Tarihi: 09.03.2020).

[8] Ministry of Digital Affairs, "National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022", 2017, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncssmap/strategies/govermental-program-for-protection-of-cyberspace-for-theyears-2011-2016-2013, (Erişim Tarihi:09.03.2020).

[9] Strategie Kybernetické Obrany ČR, 2018, http://www.acr.army.cz/assets/informacni-servis/zpravodajstvi/strategie-kyberneticke-obrany.pdf, (Erişim Tarihi:07.05.2020).

[10] Nezir Akyeşilmen, *Siber Politika ve Güvenlik*, Orion Yayınevi, Ankara, 2018, s. 135.

[11] Peter Hall and Charles Taylor, "Political Science and the Three New Institutionalisms", *Political Studies*, 1996, Vol 44, No 2, 936-957, p. 938.

birtakım mekanizmalar ortaya koymaktadır. Söz konusu teorinin ortaya koyduğu ilk mekanizma, içsel ve doğal çıkarlara ilişkin önemli soruları ele alması ve zaman kavramını odak noktası haline getirmesidir.[12] Bu noktada, kurumlar zaman içinde nasıl gelişmiştir?, kurumlar aktörlerin davranışları ve pozisyonlarını nasıl etkilemiştir?[13] gibi sorular devreye girmektedir.

Öte yandan teori, kurumlar ve aktörler arasındaki ilişkiyi yol bağımlılığı/izlek bağımlılığı (*path dependency*) ekseninde ele almakta ancak beklenmeyen sonuçlar bağlamında kesintiye uğramış denge/noktalanmış denge (*punctuated equlibrium*) kavramını da ortaya koymaktadır. Yol bağımlılığı çerçevesinde tarihsel kurumsalcılığın temel savı, siyasi ve sosyal bir süreçte başlangıçta alınan kararların -yolu yeni bir yöne kaydırmak için kritik dönemeçler oluşana kadar- daha sonra alınan kararlar üzerinde etkili olmaya devam etmesidir.[14] Bu noktada, belirli zamanlama ve sıralama kalıplarının önem arz ettiği ve önceki kararların ve seçimlerin sonrakilerden öncelikli olduğu belirtilmekte[15] ayrıca bir seçim yapıldıktan sonra, aktörlerin mevzubahis seçimleri değiştirmelerinin veya girdikleri yoldan sapmalarının zorlaştığı ifade edilmektedir.[16] Bunun nedeni ise ilgili tüm aktörlerin politika seçimlerini/kararlarını hüküm süren yapıya uyum sağlanması noktasında ortaya çıkan "kenetlenme (*lock-in*) etkisi'dir".[17] Bu bağlamda

---

[12] Paul Pierson and Theda Skocpol, "Historical Institutionalism in Contemporary Political Science", Ira Katznelson, Helen Milner and Ada Finifter (Edt.), *Political Science: The State of the Discipline*, Norton Press, NewYork, 2002, 693-721, p. 695; Mark Pollack, "The New Institutionalism and European Integration", Antje Wiener and Thomas Diez (Edt.), *European Integration Theory*, Oxford University Press, NewYork, 2009, 125-143, p. 127.

[13] Mette Eilstrupp-Sangiovanni, *Debates on European Integration*, Palgrave, Houndmilss, 2006, p. 198.

[14] Hall and Taylor, "Political Science", p. 941; Pollack, "The New Institutionalism", p. 127.

[15] Paul Pierson, "Increasing Returns, Path Dependence, and the Study of Politics", *American Political Science Association*, 2000, Vol 94, No 2, 251-267, p. 251.

[16] Mark Pollack, "The New Institutionalism and EU Governance: The Promise and Limits of Institutionalist Analysis", *Governance*, 1996, Vol 9, No 4, 429-458, pp. 437-438.

[17] Kathleen Thelen, "Historical Institutionalism in Comparative Politics", *Annual Review of Political Science*, 1999, Vol 2, pp. 369–404.

yol bağımlılığı, "politika eylemsizliği" veya "değişime karşı direnç" ile karakterize olsa da -bir diğer anlatımla, önceki kurumsal ve siyasa tercihlerinin kalıcılığı ve ısrarcılığı üzerine odaklansa da-[18] tarihsel kurumsalcılık nezdinde politika yollarının/kararlarının/tercihlerinin değişebileceği veya yeniden tanımlanabileceği bir mekanizma da bulunmaktadır. Söz konusu mekanizma kesintiye uğramış denge olarak tanımlanmaktadır ki[19] buradaki ana unsur bir politika yolundan giderken kritik dönemeçlerin/katalitik olayların meydana gelmesidir. Bu dönemeçler, seçimlerin yeniden değerlendirilmesine ve yeni politikalara gidilmesine neden olmaktadır.[20]

Teorinin ortaya koyduğu bir diğer kavram ise olumlu geri bildirim döngüsüdür (*positive feedback loop*). Kavram, bir kurumun faaliyetleri ekseninde olumlu geri bildirimler aldığını belirtmektedir. Söz konusu olumlu geri bildirim doğrultusunda, kurumun uzmanlık ve iş birliği merkezi olarak yetkilerinin artabileceği bir döngünün oluştuğu ifade edilmektedir. Diğer yandan yol bağımlılığı, olumlu geri bildirim sergileyen sosyal süreçler olarak tanımlanmaktadır. Bu bağlamda olumlu geri bildirimin, bir yolda gidilmesine yönelik alınan kararların -bir kurumun kurulması, bir politikanın uygulanması gibi- daha güçlü bir şekilde devam etmesinde etkili olduğu vurgulanmaktadır.[21]

Çalışmanın bir diğer odak noktası ise tutarlılık yaklaşımıdır. Tutarlılık, AB projesi yapımının merkezinde konumlandırılan, hem politika yapım süreçleri hem de akademik tartışmaların gündeminde

[18] Pierson, "Inreasing Returns", p. 259.
[19] Stephen D. Krasner,"Approaches to the State: Alternative Conceptions and Historical Dynamics", *Comparative Politics*, 1984, Vol 16, No 2, 223–246, p. 240.
[20] R. Berrins Collier and David Collier, "Framework: Critical Junctures and Historical Legacies", 1991, https://polisci.berkeley.edu/sites/default/files/people/u3827/Collier-Collier%20SPA%20Chap%201.pdf, (Erişim Tarihi: 10.04.2020).
[21] Paul Pierson, *Politics in Time: History, Institutions, and Social Analysis*, Princeton University Press, NJ., 2004, pp. 20-21; Matthew Lockwood vd., "Historical Institutionalism and the Politics of Sustainable Energy Transitions: A Research Agenda", 2016, https://core.ac.uk/download/pdf/43098859.pdf, (Erişim Tarihi: 19.02.2020).

yer alan önemli bir başlıktır.[22] AB Komisyonuna göre tutarlılık, daha iyi stratejik planlama yapılması, çok daha etkili olma, kurumlar ve aktörler arasında iş birliğinin oluştururulması ile eşit olan bir kavrama işaret etmektedir.[23] AB güvenlik stratejisi içerisinde ise tutarlılık, farklı enstrümanların ve kapasitelerin bir araya getirilmesi, AB ve üye devletler arasında koordinasyonun sağlanması ve uyum içinde olunması olarak tanımlanmaktadır. [24] Ancak, AB'nin tutarlı bir güvenlik aktörü olması beklentisi çerçevesinde teori ve pratikte önemli bir boşluk olduğu görülmektedir.

Bu çalışmada tutarlılık yaklaşımı, yatay (AB kurumları, üye devletler ve özel sektör bünyesindeki politikalar ekseninde tutarlılık) ve dikey (AB kurumları, üye devletler ve sektör arasındaki ilişkiler bağlamında tutarlılık) eksen çerçevesinde kurumsal koordinasyon ve ortak güvenlik anlayışı doğrultusunda analiz edilmektedir.

3. Avrupa Birliği'nin Siber Güvenliğe Yönelik Uygulamaları, Politikası ve Hedefleri

AB'nin siber güvenlik uygulamaları, politikaları ve hedefleri çerçevesinde 2013 yılında Avrupa Komisyonu tarafından yayımlanan "Avrupa Birliği'nin Siber Güvenlik Stratejisi" belgesi, bu alandaki ilk somut adımı teşkil etmesi nedeniyle son derece önemli bir mihenk taşını oluşturmaktadır. Bu noktada AB'nin siber güvenlik politikaları, söz konusu belgeden önce ve sonra atılan adımlar ekseninde ele alınmalıdır. Bu minvalden hareketle, öncelikle 2013 yılında yayımlanan

---

[22] Marise Cremona, "Coherence through Law: What Difference will the Treaty of Lisbon Make?", *Hamburg Review of Social Sciences*, 2008, Vol 3, No 1, pp. 11-36; Karolina Pomorska and Sophie Vanhoonacker, "Europe as a Global Actor: Searching for a New Strategic Approach", *JCMS*, 2016, Vol 52, No 1, pp. 216-229.

[23]European Commission$_a$, "Some Practical Proposals for Greater Coherence, Effectiveness and Visibility", 2006, https://ec.europa.eu/councils/bx20060615/euw_com06_278_en.pdf, (Erişim Tarihi: 03.04.2020).

[24] Antonio Missiroli, "Towards An Eu Global Strategy: Background, Process, References", 2015, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Towards_an_EU_Global_Strategy_0_0.pdf, (Erişim Tarihi: 12.03.2020).

siber güvenlik strateji belgesi öncesindeki dönem analiz edilmektedir.

AB'nin siber güvenlik politikasının ilk izlerinin başlangıç noktası, 1985 yılında Avrupa Komisyonu tarafından ortaya konan "Tek Pazar İnisiyatifine" uzanmaktadır. Nitekim 1985 yılında Avrupa Komisyonu'nun hazırladığı Beyaz Kitap'ta, bilgi teknolojileri ve telekomünikasyon sektörüne yönelik özel bir ilginin başladığı görülmektedir.[25] Ayrıca, yeni bilgi teknolojilerinin kullanımının ekonomik büyümeye neden olacağı vurgulanmaktadır.[26] AB'nin siber politikasının gelişiminde önem arz eden bir diğer belge, 1994 yılında kabul edilen "Bangemann Raporu'dur". Nitekim söz konusu rapor doğrultusunda, AB'nin siber güvenlik politikası daha görünür bir hale gelmekte ve aktörler arası iş birliğinin güçlendirilmesinin, fikri mülkiyet haklarının korunmasının, internet korsancılığıyla mücadelenin ve AB'nin sosyo-ekonomik gelişiminde bilgi ve iletişim teknolojilerinin önemine yapılan atıflar dikkati çekmektedir.[27] Öte yandan, odak noktası gerçek kişiler olan ve verilerin işlenmesi sırasında kişi hak ve özgürlüklerinin korunmasını içeren 25 Kasım 1995 tarihli "Verilerin Korunması Direktifi";[28] ulusal güvenlik, ekonomik güvenlik, bilgi güvenliği, fikri mülkiyet, özel yaşamın korunması gibi unsurları içeren 16 Ekim 1996 tarihli "İnternetin Yasal Olmayan ve Zararlı İçeriğine İlişkin Belge";[29] siber uzaydan kaynaklanan tehditlerin ilk kez detaylı

[25] European Commission, "Completing the Internal Market", 1985, p. 20, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51985DC0310&from=EN, (Erişim Tarihi: 09.02.2020).
[26] Ibid., p. 31.
[27] European Council, "European Council Conclusions Corfu", 1994, http://aei.pitt.edu/1444/1/corfu_june_1994.pdf, (Erişim Tarihi: 09.03.2020); Martin Bangemann, "Recommendations to the European Council Europe and the Global Information Society", 1994, http://www.channelingreality.com/Digital_Treason/Brussels_1995/Bangemann_report.pdf, (Erişim Tarihi: 13.03.2020).
[28] European Parliament and Council, "Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data", 1995, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046, (Erişim Tarihi: 10.03.2020).
[29] European Commission, "Illegal and Harmful Content on Internet", 1996, p. 3,

bir tipolojisini içeren,[30] güvenliğin güçlendirilmesine ilişkin somut teknik önlemleri ortaya koyan,[31] ilk kez ağ ve bilgi güvenliğini[32] tanımlayan, siber güvenlik çerçevesinde aktörler arası iş birliğini vurgulayan[33] 2001 yılındaki Ağ ve Bilgi Güvenliğine İlişkin Öneri (*NIS Proposal*); gerçek kişilerle beraber tüzel kişileri de içeren 31 Temmuz 2002 tarihli "Elektronik Haberleşme Sektöründe Gizliliğin Korunması Direktifi";[34] siber saldırı durumunda koordinasyon sorumluluğu bulunan, ulusal siber güvenlik stratejilerini koordine eden, üye devletlere, AB kurumlarına ve özel sektöre bilgi ve uzmanlık sağlayan, ağ ve bilgi güvenliğiyle ilişkili (NIS) AB politikalarının uygulanması ve gelişmesini yönlendiren ENISA'nın bir tüzel kişilik olarak 13 Mart 2004 'de kurulması;[35] AB ekseninde gerçekleştirilen siber saldırılara yönelik cezai yaptırımların artırılması için üye devletlerle iş birliğini hedefleyen 23 Şubat 2005 tarihli "Bilgi Sistemlerine Saldırılar Hakkında AB Konseyi Çerçeve Kararı;[36] suçların tespiti ve soruşturulması için üye devletlerin yasal mevzuatlarında tanımlanan telefon ve e-posta

---

http://aei.pitt.edu/5895/1/5895.pdf, (Erişim Tarihi: 10.03.2020).

[30] European Commission, "Network and Information Security: Proposal for A European Policy Approach", 2001, pp. 9-15, https://ec.europa.eu/transparency/regdoc/rep/1/2001/EN/1-2001-298-EN-F1-1.Pdf, (Erişim Tarihi: 11.03.2020).

[31] Ibid., pp. 20-25.

[32] Ağ ve bilgi güvenliği; bir ağın veya bir bilgi sisteminin, depolanan veya iletilen verilerin ve bu ağlar tarafından sunulan veya bunlara erişilebilen ilgili hizmetlerin kullanılabilirliğini, özgünlüğünü, bütünlüğünü ve gizliliğini tehlikeye atan olaylara veya kötü amaçlı eylemlere karşı direnme yeteneği ve sistemleri olarak tanımlanmaktadır. Ibid., p. 9.

[33] Ibid., pp. 26-27.

[34] European Parliament and Council, "Directive on the Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector", 2002, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN, (Erişim Tarihi: 11.03.2020).

[35] ENISA, "About ENISA", 2020, https://www.enisa.europa.eu/about-enisa, (Erişim Tarihi: 12.04.2020).

[36] European Council, "Council Framework Decision on Attacks against Information Systems", 2005, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN, (Erişim Tarihi: 11.03.2020).

verilerinin saklanması sorumluluğunu getiren 15 Mart 2006 tarihli "Verilerin Saklanması Direktifi";[37] ve ağ ve bilgi güvenliği politikasını canlandırma hedefi doğrultusunda kabul edilen 31 Mayıs 2006 tarihli "Güvenli Bilgi Toplumu İçin Strateji" belgesi[38] (*European Commission*, 2006) AB'nin siber güvenlik politikasının gelişiminde rol oynayan önemli mihenk taşlarıdır. Ayrıca, 2012 yılında AB Bilgisayar Acil Müdahale Ekibi'nin (*CERT-EU*) ve 2013 yılında siber suçlara ilişkin sınır ötesi faaliyetleri koordine eden, bu alanda teknik uzmanlık sağlayan ve yetkileri peyderpey arttırılan Avrupa Siber Suç Merkezi'nin (*European Cybercrime Centre-EC3*) kurulması AB'nin siber güvenlik politikası bağlamında önem arz etmektedir.

AB'nin siber güvenlik politikasının somut bir zemine oturması bağlamında ise 7 Şubat 2013 tarihinde Avrupa Komisyonu tarafından yayımlanan "Siber Güvenlik Strateji Belgesi" büyük bir rol oynamaktadır. Söz konusu belge çerçevesinde beş önemli hususa odaklanılmaktadır: siber direncin güçlendirilmesi, siber suçların azaltılması, ortak güvenlik ve savunma politikası (OGSP) doğrultusunda siber savunma politikasının ve kapasitesinin geliştirilmesi, AB için tutarlı bir uluslararası siber güvenlik politikasının oluşturulması, AB temel değerlerinin teşvik edilmesi ve siber güvenlik için endüstriyel ve teknolojik kaynakların geliştirilmesi.[39] 2013 yılındaki strateji belgesi sonrasında AB, siber alanda politikalarını güçlendirmeye devam etmektedir. Bu bağlamda, 2015 yılında siber suçlarla mücadeleyi ön plana alan "Güvenlik Üzerine

---

[37] European Parliament and Council, "Directive 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", 2006, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0024&from=GA, (Erişim Tarihi: 11.03.2020).

[38] European Commission$_b$, "Strategy for a Secure Information Society", 2006, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l24153a, (Erişim Tarihi: 03.04.2020).

[39] European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", 2013, pp. 4-5, http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf, (Erişim Tarihi: 15.03.2020).

Avrupa Gündemi" ve malların, kişilerin, hizmetlerin, sermayenin serbest dolaşımının sağlandığı; bireylerin, işletmelerin adil rekabet ve verilerin korunması koşulu altında çevrimiçi faaliyetlere sorunsuz bir şekilde erişebildiği ve dijital ekonominin güçlendirilmesi odaklı "Dijital Tek Pazar'a" ilişkin strateji kabul edilmiştir.[40] Öte yandan, ağ ve bilgi sistemlerinin güvenliğini artırmayı, siber güvenlik alanında üye devletler arasında iş birliğini güçlendirmeyi amaçlayan ve ilk yasal düzenleme olan NIS Direktifi 6 Temmuz 2016 tarihinde Avrupa Parlamentosu'nda kabul edilip, Ağustos 2016'da yürürlüğe girmiştir.[41] AB'nin siber güvenlik politikasının güçlendirilmesine ilişkin bir diğer adım 2013 yılında yayımlanan siber güvenlik strateji belgesinin 2017 yılında revize edilmesi iken[42] bu alanın yasal boyuta taşınması bağlamında son derece önemli olan bir diğer adım ise 2017 yılından itibaren üzerinde çalışılan ve 11 Mart 2019 tarihinde Avrupa Parlamentosu'nda onaylanıp, 27 Haziran 2019'da yürürlüğe giren "Siber Güvenlik Yasası'dır". Söz konusu yasa çerçevesinde temel olarak iki hedefe odaklanılmaktadır: i) siber güvenlik tehditleri ve saldırılarıyla mücadelede üye devletleri desteklemek konusunda ENISA'nın yetkilerinin güçlendirilmesi ve daimi bir AB siber güvenlik ajansına dönüşmesi, ii) bilgi ve iletişim teknolojileri bağlamında tüm üye devletlerde geçerli olacak siber güvenlik sertifikasının oluşturulması.[43] Bu bağlamda AB Siber Güvenlik Yasası, dijital ortamın güvenliğini artırmayı amaçlayan Avrupa Birliği'nin

---

[40] European Commission$_a$, "The European Agenda on Security", 2015, https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52015DC0185, (Erişim Tarihi: 17.03.2020); European Commission$_b$, "A Digital Single Market Strategy for Europe", 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192, (Erişim Tarihi: 18.03.2020).

[41] European Commission, "The Directive on Security of Network and Information Systems (NIS Directive)", 2020, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive, (Erişim Tarihi: 17.03.2020).

[42] European Commission$_a$, "Resillience, Detterence and Defence: Building Strong Cyber Secuirty for the EU", 2017, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450, (Erişim Tarihi: 14.04.2020).

[43] European Commission$_b$, "Cyber Security Act", 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0477&from=EN, (Erişim Tarihi: 19.04.2020).

genel siber politikasının önemli bir parçasıdır.

Tarihsel bir kronoloji ekseninde AB'nin siber güvenlik politikasının gelişimi doğrultusunda sosyo-ekonomik merkezli bir yaklaşım ön plandadır. Nitekim Avrupa Komisyonu'nun hazırladığı ve 1 Ocak 1993'e kadar tek pazar oluşturulması hedefini ortaya koyan 1985 yılındaki Beyaz Kitap, "iç pazar/tek pazar" terimini kurucu antlaşmaya dâhil eden ve 1 Temmuz 1987 tarihinde yürürlüğe giren Avrupa Tek Senedi (ATS), 1 Kasım 1993'de yürürlüğe girerek, Avrupa Birliğini kuran Maastricht Antlaşması[44] (AB Antlaşması-ABA) ile bu hususun daha belirgin hale geldiği görülmektedir.[45] Öte yandan, 1994 yılında yayımlanan Bangemann Raporu; istihdamın yaratılması, piyasa güçleri, fayda maksimizasyonu ve sosyal değişim gibi sosyo-ekonomik unsurların altını çizmekte ve bu unsurlar çerçevesinde politikalar belirlenmesi gerekliliğini vurgulamaktadır.[46] Bununla beraber, 1995 yılında yayımlanan "Verilerin Korunması Direktifi", ekonomik ve sosyal refahın güçlendirilmesi gerekliliğine vurgu yaparken 1996 yılında yayımlanan "İnternetin Yasal Olmayan ve Zararlı İçeriğine İlişkin Belge" ise büyüyen internet ekonomisi doğrultusunda ekonomik güvenliğe, internetin, ekonomik gelişimi güçlendirmesine, iç pazara yönelik yasal çerçeveye, rekabet kuralları doğrultusunda ağ ve bilgi sistemlerine ilişkin güvenliğin sağlanmasına odaklanmaktadır. Ayrıca söz konusu belgede internetin sosyal, kültürel ve eğitimsel alanlardaki güçlü etkisinin altı çizilmektedir.[47] Diğer

[44] ATS, güvenlik konseptinin ilk kez dile getirildiği ancak güvenliğe yönelik daha sembolik bir önemin vurgulandığı bir belge iken ABA ise ortaya koyduğu üç sütunlu yapıdan biri olan ve hükümetlerarası özellik taşıyan ortak dış ve güvenlik politikası çerçevesinde güvenlik konusunu daha somut bir zeminde ele almaktadır.

[45] European Commission, "Completing the Internal Market"; Single European Act, 1987, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:11986U/TXT&from=EN, (Erişim Tarihi: 10.03.2020); Maastricht Treaty, 1992, https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_on_european_union_en.pdf, (Erişim Tarihi: 21.03.2020).

[46] European Council, "Conclusions Corfu"; Bangemann, "Global Information Society".

[47] European Commission, "Illegal and Harmful", p. 3, 5, 7, 19.

taraftan, 2001 yılındaki "NIS Önerisinde" ekonomik ve sosyal kalkınmada ağ ve bilgi sistemlerinin temel bir unsur olduğu belirtilmektedir.[48] 2002 tarihli "Elektronik ve Haberleşme Sektöründe Gizliliğin Korunması Direktifinde" ise devletlerin ekonomik refahının sağlanması (md.11), piyasanın gelişimi (md.4), internetin pazar yapısını bozmamasına (md.6) ve pazar yapısını bozabilecek dijital sistemlere yönelik önlemlere (md.8) ilişkin atıflar bulunduğu görülürken[49] 2006 tarihli " Güvenli Bilgi Toplumu İçin Strateji" belgesinde, Avrupa ekonomisi ve bir bütün olarak Avrupa toplumu için bilgi ve iletişim teknolojileri kaynaklı risklerin ciddiye alınması, ekonominin canlanması çerçevesinde büyüme ve istihdama yönelik bir "Avrupa Güvenlik Toplumu'nun" tesis edilmesi gerekliliği üzerinde durulmaktadır.[50] 2013 yılında yayımlanan "Siber Güvenlik Strateji" belgesinde ise bilgi ve iletişim teknolojilerinin sosyal etkileşim ve ekonomik büyüme için önemli bir belkemiği haline dönüştüğü ve finans, sağlık, enerji, ulaştırma gibi kilit sektörlerde önem arz ettiği ortaya konmaktadır.[51] Öte yandan, 2015 yılındaki "Dijital Tek Pazar Stratejisi'nde" küresel ekonominin büyük bir hızla dijitalleştiği, dijital ekonominin Avrupa pazarını güçlendiren yeni kaynaklar ve istihdam yaratan bir unsur olduğu, bilgi ve iletişim teknolojilerinin ekonomik ve sosyal yapıyı etkilediği ortaya konarken[52] 2016 yılında kabul edilen "NIS Direktifi'nde ise enerji, ulaşım, bankacılık, sağlık, finans ve dijital altyapı gibi sektörlerin bilgi ve iletişim teknolojisine dayanması bağlamında ekonomik ve sosyal yapının güvenliğinin sağlanmasının altı çizilmektedir.[53] Bununla beraber, 2013 yılındaki siber güvenlik strateji belgesinin 2017 yılında revize edilmiş versiyonunda

[48] European Commission, "Network and Information", p. 2, 16.
[49] European Parliament and Council, "Personal Data".
[50] European Commission, " Strategy for a Secure".
[51] European Commission, "Cybersecuriy Strategy", p. 2.
[52] European Commission, " A Digital Single".
[53] European Parliament and Council, "Directive on Network and Information Systems across the Union", 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC, (Erişim Tarihi: 15.04.2020).

ekonominin, dijital teknolojiye bağımlı olduğu ve siber güvenliğin sağlanmasında ekonomik ve sosyal yapı odaklı önlemler alınması gerekliliği ele alınırken[54] 2019 yılında yürürlüğe giren "Siber Güvenlik Yasası", diğer belgelerde olduğu gibi bir kez daha ağ ve bilgi sistemlerinin ekonomik büyüme ve sosyal refahın temeli olduğunu vurgulamaktadır.[55] Son kertede, analiz edilen tüm bu belgeler çerçevesinde AB'nin bilgi ve iletişim teknolojilerine yönelik yaklaşımı ve dolayısıyla siber güvenlik politikasının sosyo-ekonomik merkezli olduğu sonucuna ulaşılmaktadır.

Öte yandan, siber güvenliğe yönelik ilk izlerin görülmeye başlandığı 1985 yılından günümüze Birlik, beş temel hedef çerçevesinde siber güvenlik politikasını geliştirmeye yönelmektedir. Söz konusu bu beş temel hedef ise ekonomik fayda/maksimizasyonun sağlanması, temel hakların korunması, siber suçları/saldırıların önlenmesi, dijital sisteme yönelik güven unsurunun artırılması ve aktörler arasında iş birliğinin güçlendirilmesidir. Mevzubahis beş hedefe, çalışma boyunca incelenen dokümanların içerik analizine tabi tutulması çerçevesinde ulaşılmıştır. Elde edilen veriler ise şu şekildedir:

[54] European Commission, "Resillience".
[55] European Commission, "Regulation on ENISA and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (Cybersecurity Act)", 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN, (Erişim Tarihi:01.05.2020).

Tablo 1_a: 2013 Strateji Belgesi Öncesi Ekonomik Unsur[56]

1985 İç Pazarın Tamamlanmasına İlişkin İnisiyatif	1994 Bangemann Raporu	1995 Verilerin Korunması Direktifi	1996 İnternetin Yasal Olmayan Zararlı İçeriğine İlişkin Belge	2001 NIS Önerisi	2002 Gizliliğin Korunması Direktifi	2006 Güvenli Bilgi Toplumu İçin Strateji
Yeni bilgi teknolojileri, ekonomik büyümeye neden olacaktır.[57]	Bilgi toplumu, Avrupa vatandaşlarının yaşam kalitesini iyileştirme, sosyal ve ekonomik kalkınmayı güçlendirme ve uyumu artırma potansiyeline sahiptir.[58]	Ekonomik kalkınma ve refahın sağlanması gerekmektedir.	İnternet ekonomisi, bir dizi ekonomik sektörü kökten etkilemektedir. Aynı zamanda internet; sosyal, eğitimsel ve kültürel alanlarda da güçlü bir etkiye sahiptir.[59]	Bilgi ve iletişim güvenliği, ekonominin gelişiminde temel bir unsurdur.[60]	Internet, geleneksel pazar yapısını bozmamalıdır.	Avrupa ekonomisi bilgi ve iletişim teknolojileri kaynaklı riskleri ciddiye almalıdır.

Tablo 1_b: 2013 Strateji Belgesi ve Sonrası Ekonomik Unsur

2013 Siber Güvenlik Strateji Belgesi	2015 Dijital Tek Pazar Stratejisi	2016 NIS Direktifi	2017 Revize Edilmiş Siber Güvenlik Strateji Belgesi	2019 Siber Güvenlik Yasası
BIT ekonomik büyümenin belkemiğidir.[61]	Avrupa dijital ekonomisinin maksimize edilmesi temel hedeflerden biridir.	İç pazar bağlamında BIT güvenliğinin sağlanması gerekmektedir (md.1).	Ekonomik gelişim büyük oranda dijital teknolojilere bağımlıdır.	BIT ekonomik büyümeyi desteklemektedir (md.2).

[56] Tablo 1-5 arası yazarın kendisi tarafından oluşturulmuştur.
[57] European Commission, "Completing the Internal Market", p. 31.
[58] Bangemann, "Global Information Society", p. 11.
[59] European Commission, "Illegal and Harmful", p. 3.
[60] European Commission, "Network and Information", p. 18.
[61] European Commission, "Cybersecurity Strategy", p. 2.

Tablo 2_a: 2013 Strateji Belgesi Öncesi Güven Unsuru

1994 Bangemann Raporu	1995 Verilerin Korunması Direktifi	1996 İnternetin Yasal Olmayan Zararlı İçeriğine İlişkin Belge	2001 NIS Önerisi	2002 Gizliliğin Korunması Direktifi
Yeni teknolojilerin kullanımını sağlamak için toplumda bunların güvenliğine ilişkin genel bir kabulün sağlanmasında çaba sarf edilmelidir.[62]	BIT'ne yönelik güven artırıcı önlemler alınması gerekmektedir.	Üye devletler dijital sistemlere ilişkin güven artırıcı önlemleri takip etmelidir.[63]	Güvenlik tehditlerinden endişe duyan birçok kullanıcının e-ticaretten kaçınma riski vardır Dijital sistemlere yönelik güvenin güçlendirilmesi gerekmektedir.[64]	Dijital sistemlere karşı güven artırıcı önlemler alınmalıdır (md.20).

Tablo 2_b: 2013 Strateji Belgesi ve Sonrası Güven Unsuru

2013 Siber Güvenlik Strateji Belgesi	2015 Dijital Tek Pazar Stratejisi	2016 NIS Direktifi	2017 Revize Edilmiş Siber Güvenlik Strateji Belgesi	2019 Siber Güvenlik Yasası
Yeni teknolojilerle bağlanmak konusunda vatandaşların güvene ihtiyacı vardır. AB genelinde her 10 internet kullanıcısından biri siber saldırı kurbanıdır.[65]	Dijital risklere yönelik güvenin artırılması gelecek jenerasyon için önemlidir.	Güvenli servis sağlayıcıları için gereken adımlar atılmalıdır (md.7).	Gelişen teknolojilere yönelik güven tesis edilmelidir. Tüketiciler, yeni teknolojilere güvendiği için zarar görmektedir.	Sertifika kullanımı, dijital sistemlere güven artmasına yol açacaktır. BIT bağlamında güven tesis edilmelidir (md.4,7).

[62] Bangemann, "Global Information Society", p.12.
[63] European Commission, "Illegal and Harmful", pp. 15-16.
[64] European Commission, "Network and Information", p. 10, 15, 20-21.
[65] European Commission, "Cybersecurity Strategy", pp. 2-3.

Tablo 3_a: 2013 Strateji Belgesi Öncesi Temel Haklar Unsuru

1995 Verilerin Korunması Direktifi	1996 İnternetin Yasal Olmayan Zararlı İçeriğine İlişkin Belge	2001 NIS Önerisi	2002 Gizliliğin Korunması Direktifi	2005 Dijital Sistemler AB Konsey Çerçeve Kararı	2006 Verilerin Saklanması Direktifi
Temel hak ve özgürlükler korunmalı ve saygı gösterilmeli.	İfade ve düşünce özgürlüğüyle beraber bir bütün olarak kişi haklarının korunması gerekmektedir.[66]	Dijital dünyadan kaynaklanan tehditlere karşı bireysel hakların korunması temel önceliktir.[67]	Bireysel hak ve özgürlükler garanti altına alınmalıdır (md.1,2,3).	Temel haklara saygı gösterilmelidir (md.18)	Bireysel hak ve özgürlükler korunmalı ve buna yönelik yasal önlemler alınmalıdır (md.1,9,17).

Tablo 3_b: 2013 Strateji Belgesi ve Sonrası Temel Haklar Unsuru

2013 Siber Güvenlik Strateji Belgesi	2015 Dijital Tek Pazar Stratejisi	2016 NIS Direktifi	2017 Revize Edilmiş Siber Güvenlik Strateji Belgesi	2019 Siber Güvenlik Yasası
Bilgiye erişim ve ifade özgürlüğü dâhil olmak üzere temel hakların teşvik edilmesi ve korunası gerekmektedir.[68]	Siber tehditler vatandaşların temel hakarına sorun teşkil etmektedir. Görsel-işitsel sektördeki haklara saygı gösterilmesi, fikri mülkiyet haklarının, tüketicilerin gizlilik ve kişisel verilerin korunması önemlidir .	Temel haklara saygı gösterilmesi, tüketici ve firmaları siber tehditlerden korumak önemlidir (md.75).	Avrupa'nın refahını, toplumunu, değerlerini, hak ve özgürlüklerini korurken proaktif yaklaşım önemlidir. Dijital tek pazar, temel hakların korunmasına odaklanmıştır.	Fikri mülkiyet hakları korunmalıdır.

[66] European Commission, "Illegal and Harmful", pp. 10-11, 18.
[67] European Commission, "Network and Information", p. 22.
[68] European Commission, "Cybersecurity Strategy", p. 16.

Tablo 4_a: 2013 Strateji Belgesi Öncesi Siber Saldırıları Önleme Unsuru

1996 İnternetin Yasal Olmayan Zararlı İçeriğine İlişkin Belge	2001 NIS Önerisi	2002 Gizliliğin Korunması Direktifi	2005 Dijital Sistemler AB Konsey Çerçeve Kararı	2006 Verilerin Saklanması Direktifi	2006 Güvenli Bilgi Toplumu İçin Strateji
Diğer tüm iletişim teknolojileri gibi, internet potansiyel olarak zararlı veya yasadışı faaliyetler bağlamında kötüye kullanılabilir. Siberle bağlantılı suçlar önlenmelidir.[69]	Ağ ve bilgi güvenliği ile ilgili önerilen politika önlemleri sadece mevcut telekomünikasyon ve veri koruma mevzuatı bağlamında değil, aynı zamanda siber suç politikaları ile ilgilidir. Siber tehdit tipolojisi ekseninde önlemler alınmalıdır.[70]	İç pazarı olumsuz etkileyecek dijital kaynaklı saldırıların önüne geçilmelidir (md.8).	Dijital sistemlere yönelik saldırılarla mücadele edilmelidir (md.8).	İç pazarın bozulmasına neden olan dijital kaynaklı saldırılar önlenmelidir (md.6).	Kolluk kuvvetleri arasındaki iş birliğini iyileştirmek için önerilerde bulunmak ve internetten yararlanan ve kritik altyapıların işleyişini zayıflatan yeni suç faaliyetleri ele alınmalıdır.[71]

Tablo 4_b: 2013 Strateji Belgesi ve Sonrası Siber Saldırıları Önleme Unsuru

2013 Siber Güvenlik Strateji Belgesi	2015 Dijital Tek Pazar Stratejisi	2016 NIS Direktifi	2017 Revize Edilmiş Siber Güvenlik Strateji Belgesi	2019 Siber Güvenlik Yasası
AB ekonomisi özel sektöre ve bireylere yönelik siber suç faaliyetlerinden etkilenmiştir. Siber alanda ekonomik casusluk ve devlet destekli faaliyetlerin artması, AB hükümetleri ve şirketleri için yeni bir tehdit kategorisi oluşturmaktadır.[72]	Siber tehditlerin önüne geçilmesine yönelik politikalar takip edilmelidir.	BIT'ten kaynaklanan riskler önlenmelidir (md.7).	Üye devletler tarafından siber suçların etkileri minimize edilmelidir.	Siber saldırı risklerinin önlenmesi için ENISA'nın yetki ve kapasitesi artırılmalıdır (md.16).

[69] European Commission, "Illegal and Harmful", p. 3.
[70] European Commission, "Network and Information", p. 19.
[71] European Commission, "Strategy for a Secure", p. 5.
[72] European Commission, " Cybersecurity Strategy", p. 3.

Tablo 5_a: 2013 Strateji Belgesi Öncesi İşbirliği Unsuru

1995 Verilerin Korunması Direktifi	1996 İnternetin Yasal Olmayan Zararlı İçeriğine İlişkin Belge	2001 NIS Önerisi	2005 Dijital Sistemler AB Konsey Çerçeve Kararı	2006 Güvenli Bilgi Toplumu İçin Strateji
Aktörler arası küresel iş birliği gerekmektedir.	İnternetin zararlı ve yasal olmayan içeriğinden kaynaklanan sorunlarla mücadelede küresel iş birliği gerekmektedir.[73]	Bir ülkede ilk saldırı işaretleri hakkında anında bilgi alışverişi yoluyla Birlik genelinde erken uyarı sağlamak için iş birliği şarttır. Bu nedenle, Avrupa Birliği içindeki CERT sistemi ile iş birliği acil bir konu olarak güçlendirilmelidir.[74]	Aktörler arası iş birliği geliştirilmelidir (md.5).	Ağın ve bilgi güvenliğinin küresel boyutu, hem uluslararası düzeyde hem de üye devletler ile koordineli olarak NIS konusunda küresel iş birliğini geliştirme çabalarını artırmaya zorlamaktadır.

Tablo 5_b: 2013 Strateji Belgesi ve Sonrası İşbirliği Unsuru

2013 Siber Güvenlik Strateji Belgesi	2015 Dijital Tek Pazar Stratejisi	2016 NIS Direktifi	2017 Revize Edilmiş Siber Güvenlik Strateji Belgesi	2019 Siber Güvenlik Yasası
AB'de siber dayanıklılığı teşvik etmek için, hem kamu yetkilileri hem de özel sektör yeteneklerini geliştirmeli ve etkin bir şekilde iş birliği yapmalıdır. [75]	Etkin bir dijital tek pazar için aktörler arası iş birliği güçlendirilmelidir.	Siber krizlere yönelik etkin bir iş birliği grubu oluşturulmalıdır (md.4,5).	Siber güvenlik bağlamında uluslararası iş birliğinin tesisi önemlidir.	Üye devletler, AB kurumları ve ajansları arasında iş birliği güçlendirilmelidir (md.6).

Sonuç olarak, bilgi ve iletişim teknolojilerine yönelik ilgisinin başlangıç noktasını teşkil eden 1985 yılından günümüze AB, ortaya koyduğu önemli belgeler ve kurumsal yapıların oluşturulması bağlamında siber güvenlik politikasını geliştirip, güçlendirmeye odaklanmaktadır. Bu noktada AB'nin hem bu alandaki direktif, strateji, çerçeve kararları gibi dokümanları ekseninde siber güvenliğe sosyo-ekonomik odaklı

[73] European Commission, "Illegal and Harmful", p. 17, 25.
[74] European Commission, "Network and Information", p. 21.
[75] European Commission, "Cybersecurity Strategy", p. 5.

yaklaştığı hem de siber güvenlik politikasının temel olarak beş temel amaç üzerine inşa edildiği görülmektedir. Bir diğer ifadeyle, 1985 yılından günümüze kadar ortaya konan dokümanlar ve özelde siber güvenlikle ilişkili belgeler çerçevesinde siber güvenliğe ilişkin sosyo-ekonomik yaklaşım ve beş temel hedef devam etmektedir.

4. Tarihsel Kurumsalcılık Teorisi ve Tutarlılık Yaklaşımının/ Modelinin Avrupa Birliği ve Siber Güvenlik Denklemindeki Analizi

Avrupa Birliği sahip olduğu resmî ve resmî olmayan kurumları çerçevesinde bir bütün olarak kurumsalcılık teorisinin sunduğu önermelerin uygulanması açısından önemli bir test sahasını teşkil etmektedir.[76] AB politika yapımında büyük öneme sahip olan kurumlar, sadece fiziki yapılar değil, resmî kurallar, prosedürler, aktörlerin davranışlarını ve politika seçimleri etkileyen uygulamalardır.[77] Bu minvalden hareketle, siber güvenlik alanında kurulan kurumların ve ortaya konan belgelerin AB'nin siber güvenlik politikası üzerindeki etkisi incelenmiş ve bu doğrultuda tarihsel kurumsalcılığın altını çizdiği ve başta alınan kararların veya uygulanan politikaların daha sonraki kararlar/politikalar üzerinde etki ettiğini tanımlayan yol/izlek bağımlılığının doğrulandığı görülmüştür. Öyle ki analiz edildiği üzere, AB'nin bilgi ve iletişim teknolojilerine yönelik ilgisinin ilk kez görüldüğü 1985 yılında yayımlanan Beyaz Kitap'tan 2019 yılında yürürlüğe giren Siber Güvenlik Yasası'na kadar geçen 34 yıl içerisinde, AB'nin siber güvenliğe yönelik yaklaşımı sosyo-ekonomik merkezlidir ve siber güvenlik politikası; ekonomik maksimizasyonun sağlanması, temel hakların korunması, siber suçları/saldırıların önlenmesi, dijital sisteme yönelik güven unsurunun artırılması ve aktörler arasında iş birliğinin güçlendirilmesini içeren beş temel hedefe dayanmaktadır. Bir diğer ifadeyle, süreç içerisinde yapılan tercihlerin -sosyo-ekonomik yaklaşım sergileme ve beş ana hedef- daha sonraki zamanda da devam ettiği ve sonraki tercihler üzerinde etkili olduğu görülmektedir.

[76] Ben Rosamond, *Theories of European Integration*, London: Palgrave, 2000, p. 114.
[77] Hall and Taylor, "Political Science", pp. 939-940.

Dolayısıyla geçen 34 yıl zarfında AB'nin siber güvenlik politikasındaki kurumsal ve siyasa tercihleri, tarihsel kurumsalcılığın ortaya koyduğu yol bağımlılığı ve hâkim yapıya uyum sağlanması zarfındaki kenetlenme etkisi çerçevesinde değişmeyen ve kalıcı bir düzlemde devam etmiştir.

Teorinin ortaya koyduğu politika yollarının, kararların ve tercihlerin kritik dönemeçler zarfında değişebileceği ve hatta yeniden tanımlanabileceğini ele alan kesintiye uğramış denge mekanizması çerçevesinde AB, siber güvenlik politikalarına etki edecek iki önemli kritik dönemeç/katalitik olay yaşamıştır. Bunlardan ilki, 2007 yılında gerçekleşen ve Rusya kaynaklı olduğu düşünülen Estonya'nın bilgi ve iletişim altyapısına yönelik siber saldırılar iken[78] ikincisi ise 1 Aralık 2009 tarihinde yürürlüğe giren Lizbon Antlaşması'dır. Mevzubahis iki kritik dönemeç çerçevesinde AB'nin siber güvenliğe ilişkin sosyo-ekonomik odaklı yaklaşımında herhangi bir değişim yaşanmamıştır. İlk kritik dönemeçte, AB kesintili denge mekanizması çerçevesinde politika değiştirmek yerine ulusal güvenlik tehdidi ve bir savunma meselesi olarak tanımlanan bu şok krize, var olan politikası çerçevesinde cevap vermiş ve söz konusu olayı tek pazarın işleyişine yönelik bir risk algısı bağlamında yorumlamıştır. Öyle ki bu yaklaşımının değişmemesi durumu, Maastricht Antlaşması ile hayata geçen sütunlu yapı sistemine son veren ve AB'ye tüzel kişilik kazandıran ve dolayısıyla AB mimarisinde köklü değişimler yapan Lizbon Antlaşması çerçevesinde de devam etmiştir. AB'nin hangi politika alanına dâhil olabileceğini ve söz konusu alanlara ne ölçüde katılabileceğini yetki kataloğu çerçevesinde belirleyen Lizbon Antlaşması çerçevesinde üç ana ve iki spesifik kategorizasyon söz konusudur.[79] Bunlardan ilki; gümrük birliği, iç pazarın

---

[78] Mehmet, E., Erendor, "Risk Toplumu ve Refleksif Modernleşme Çerçevesinde Siber Terörizm: Tanımlama ve Tipoloji Sorunu", *Cyberpolitik Journal, 2016, Cilt* 1, Sayı 1, 114-133, s. 120.

[79] ABİHA, 2012, md.2, https://www.ab.gov.tr/files/pub/antlasmalar.pdf, (Erişim Tarihi: 30.04.2020); İlke Göçmen, *Avrupa Birliği Maddi Hukuku*, Seçkin Yayıncılık, Ankara, 2017, s. 120; Mehmet H. Bayram, *Avrupa Birliği Hukuku Dersleri*, Seçkin Yayıncılık, Ankara, 2015, s. 93; Sanem Baykal ve İlke Göçmen, *Avrupa Birliği Kurumsal Hukuku*, Seçkin Yayıncılık, Ankara, 2016, s. 128.

işleyişindeki rekabet kurallarının oluşturulması, avro alanına yönelik para politikası, ortak balıkçılık politikası çerçevesinde biyolojik deniz kaynaklarının koruma altına alınması, ortak ticaret politikası gibi alanları kapsayan ve sadece AB'nin bağlayıcı düzenleme yapıp, tasarrufları kabul ettiği münhasır yetkidir.[80] Diğeri, AB'nin yetkileri üye devletlerle paylaştığı; iç pazar, ekonomik, sosyal ve bölgesel uyum, çevre, tüketicinin korunması, taşımacılık, enerji gibi alanları içeren paylaşılan yetkidir.[81] Üye devletlerin eylemlerini desteklemek, koordine etmek ve tamamlamak amacıyla AB'nin eylemde bulunabildiği ancak tasarruf çıkaramadığı insan sağlığının korunması ve iyileştirilmesi, kültür, turizm, eğitim ve sanayi gibi alanları tazammun eden destekleyici, koordine edici ve tamamlayıcı yetki ise üçüncü ana kategori altında bulunmaktadır.[82] Öte yandan, spesifik kategorizasyon altında AB'nin üye devletlerin ekonomi ve istihdam politikalarını koordine edici eylemleri ve yetkilerinin oldukça sınırlı olduğu ortak dış ve güvenlik politikası yer almaktadır.[83] Sonuç olarak, bu kategorizasyon ekseninde AB yetkilerinin sosyo-ekonomik merkezli alanlarda olduğu görülmekte ve hem bu statik yapı hem de AB'nin içinde taşıdığı ve daha belirleyici özellik gösteren hükümetlerarası nitelik bağlamında AB'nin siber güvenlik alanında da sosyo-ekonomik bir yaklaşım sergilediği, kritik dönemeç ekseninde politika değişikliğine gidemediği ve bu noktada tarihsel kurumsalcılığın ortaya koyduğu kesintili denge mekanizmasıyla örtüşmediği görülmektedir.

Analiz edildiği üzere, bir kurumun faaliyetleri ekseninde olumlu geri bildirimler alabildiği ve söz konusu olumlu geri bildirimler zarfında kurumun yetkilerinin arttığı olumlu geri bildirim döngüsü ise tarihsel kurumsalcılığın odaklandığı bir diğer mekanizmadır. AB'nin siber güvenlik politikaları çerçevesinde faaliyet gösteren Avrupa Siber Suç Merkezi'nin (EC3) ve Avrupa Ağ ve Bilgi Güvenliği Ajansı'nın (ENİSA)

[80] ABİHA, md. 2(3), 2(4).
[81] ABİHA, md. 2(2), 4(2).
[82] ABİHA, md. 2(5), 6.
[83] ABİHA, md. 2(3), 2(4).

yetkilerinin peyderpey artırılarak güçlendirilmesi ve 2019 yılında yürürlüğe giren Siber Güvenlik Yasası çerçevesinde ENİSA'nın daimi bir siber güvenlik ajansına dönüştürülmesi olumlu geri bildirim mekanizmasının işlerliğini doğrulamaktadır.

Öte yandan, tutarlılık yaklaşımının ana kurumsal prensiplerden biri haline dönüştüğü görülmektedir.[84] Nitekim Maastricht Antlaşması, söz konusu yaklaşımın altını çizmektedir. Buna göre: " Birlik; dış ilişkiler, güvenlik, ekonomi ve kalkınma politikaları çerçevesinde bir bütün olarak dışsal faaliyetlerin tutarlılığını garanti altına almalıdır".[85] Ayrıca, Maastricht Antlaşması'ndan itibaren Avrupa güvenliği ekseninde tutarlı bir yaklaşım geliştirmenin önemine değinilmektedir.[86] 2013 yılında Avrupa Komisyonu tarafından yayımlanan "AB Siber Güvenlik Strateji" belgesi ise tutarlılık yaklaşımının somut bir zemine oturtulmasına ilişkindir.[87] Ancak kritik bilgi altyapısının korunması, siber suçlar ve siber savunma şeklinde üç temel faaliyet alanını kapsayan belge çerçevesinde kademeli bir şekilde koordinasyonun geliştirilmesi amaçlansa da hala bu üç boyut birbirinden ayrı olarak ele alınmaktadır.[88] Diğer taraftan, Avrupa Güvenlik Gündemi'nde AB'nin iç güvenliği ve küresel güvenliğinin birbiriyle bağımlı ve bağlantılı olduğu, dolayısıyla AB'nin iç ve dış boyutlar çerçevesinde kapsamlı ve tutarlı faaliyetlere dayanması gerekliliğinin altı çizilmektedir.[89] 2016 yılında yayımlanan "Hibrit Tehditlere Karşı Ortak Çerçeve" içerisinde de tutarlılık yaklaşımının izleri görülmekte ve söz konusu belge doğrultusunda

[84] Cremona, "Coherence", p. 13.
[85] Maastricht Treaty, Article C.
[86] European Council, "Tampere Council Conclusions", 1999, https://www.europarl.europa.eu/summits/tam_en.htm#c, (Erişim Tarihi: 02.04.2020); European Commission, "Practical Proposals".
[87] Elaine Fahey, "EU'S Cybercrime and Cyber Security Rule-Making: Mapping the Internal and External Dimensions of EU Security", *European Journal of Risk Regulation*, Vol 5, No 1, 46-60, pp. 48-49.
[88] George Christou, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy*, Palgrave, London, 2016, pp. 27-32.
[89] European Commission, "The European Agenda".

hibrit tehditlere karşı ilgili tüm aktörler arasında sinerjinin ve koordinasyonun yaratılması gerekliliğine değinilmektedir.[90] 2017 yılında Avrupa Komisyonu tarafından yayımlanan revize edilmiş " Siber Güvenlik Strateji" belgesinde ise ENISA'nın daha güçlü bir danışmanlık rolü ifa edeceği ve bu bağlamda sektörel girişimler ve NIS Direktifi arasında tutarlılığı destekleyeceği ifade edilmektedir.[91] Son olarak, 27 Haziran 2019'da yürürlüğe giren "Siber Güvenlik Yasası" ekseninde ENISA'nın faaliyetlerinin ulusal ve AB düzlemindeki politikalarla tutarlı olması gerektiği ve AB bağlamında daha koordineli bir siber güvenlik yaklaşımına olan ihtiyaç ortaya konmaktadır.[92]

Görüldüğü üzere tutarlılık, AB'nin siber güvenliğe yönelik yaklaşım ve politikası zarfında ortaya konan önemli bir gerekliliği yansıtmaktadır. Mevzubahis gereklilik; üye devletlerin, kurumların ve uluslararası partnerlerin de dâhil olduğu tüm taraflar bağlamında bütüncül bir çabanın gösterilmesine ilişkin ortak bir yaklaşımı ifade etmektedir.[93] Nitekim siber güvenlik son derece hassas, kurumsal koordinasyon ve ortak yaklaşım tesis edilmesi gereken bir alandır. Ancak söz konusu alana ilişkin üye devletlerin yaklaşımlarındaki farklılık dikkati çekmektedir. Öyle ki üye devletlerden Almanya, Fransa, Hollanda ve İtalya mevcut AB siber güvenlik çerçevesinden daha öteye gitmek isterken birçok üye devlet, bölgesel iş birliğini tercih etmektedir. Öte yandan, Fransa siber güvenliğe askerî ve istihbarat odaklı yaklaşırken Almanya ve Hollanda sivil ve hukuk temelli yaklaşmakta, Estonya ise bu iki yaklaşım arasında denge kuran bir bakış açısı sergilemektedir.[94] Bununla beraber, eylemsel olarak da ortak adımların atılmadığı

[90] European Commission, "Joint Framework on Countering Hybrid Threats", 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018, (Erişim Tarihi: 22.04.2020).
[91] European Commission, "Resilliene".
[92] European Commission, "Cyber SecurityAct"; European Commission, "Regulation on ENISA".
[93] European Commission, "Cybersecurity Strategy".
[94] Akyeşilmen, "Siber Politika", s. 135.

görülmektedir. Nitekim Vişegrad devletleri[95] ve Avusturya özelinde kendi Bilgisayar ve Acil Müdahale Ekipleri (*CERT*) bağlamında iş birliğinin geliştirilmesi için 2013 yılında "Merkez Avrupa Siber Güvenlik Platformu" kurulmuştur.[96] Dolayısıyla, farklılaşan yaklaşımlar ve eylemler bağlamında tutarlılık ekseninde ortaya çıkan bu sorun, hem siyasi tercihler ve siber güvenlik ile ilgili faaliyetlerin yönetilmesindeki farklılık hem de diğer devletlerle bilgi paylaşımı için kurumsal bir çerçeve gerektiren mekanizma eksikliğiyle ilişkilidir ki bilginin toplanması ve paylaşımına ilişkin bir anlaşma da bulunmamaktadır. Ayrıca, devletler siber güvenlikte iş birliğinin sağlanması ekseninde farklı modellere sahiptir.[97] Üstüne üstlük, üye devletlerin mevcut ulusal siber güvenlik stratejileri incelendiğinde, bu alanın bir öncelik haline getirilmesi, gerekli altyapının sağlanmasına ilişkin finansal kapasite ekseninde de farklılıklar bulunduğu gözlemlenmektedir.

Diğer taraftan, siber güvenliğin sağlanmasında tutarlı olunmasına dair kurumsal koordinasyon ve ortak bir yaklaşımın geliştirilmesi için aktörler arasında iş birliği gerekliliğine ilişkin yapılan retorik vurgu göz önüne alındığında,[98] 2016 Ağustos ayında yürürlüğe giren NIS Direktifi'nde aktörler arası iş birliğini güçlendirmeye yönelik bir "İşbirliği Grubu (*Cooperation Group*)" önerisinin sunulması ve 2018 yılındaki Mutabakat Zaptı çerçevesinde ENISA, Avrupa Savunma Ajansı (EDA), EC3 ve CERT-EU'nun siber sorunların bertaraf edilmesine yönelik iş birliğini arttırma kararı almaları tutarlılık yaklaşımını yansıtmaktadır.[99]

---

[95] Vişegad devletleri; askerî, ekonomik ve enerji alanlarında iş birliğinin sürdürülmesi amacıyla oluşturulan Vişegrad grubundaki Çekya, Macaristan, Polonya ve Slovakya'yı içeren dört Orta Avrupa devletini kapsamaktadır.

[96] National Security Authority, "Central European Platform for Cybersecurity", 2018, https://www.nbu.gov.sk/en/cyber-security/partnership/central-european-platform-for-cybersecurity/index.html, (Erişim Tarihi: 25.04.2020).

[97] Charles Guitton,"Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK?", *European Security*, 2013, Vol 22, No 1, 21-35., p. 25, 27.

[98] European Commission, "Cybersecurity Strategy"; European Commission, "Resilliene"; European Commission, "Cyber Security Act".

[99] NIS Directive, 2016, https://eur-lex.europa.eu/eli/dir/2016/1148/oj, (Erişim Tarihi:

Öte yandan, kritik bilgi altyapılarının özel sektörün elinde olduğu düşünüldüğü zaman, özel sektörle geliştirilen/geliştirilmeye çalışılan iş birliği belirgin bir öneme sahiptir. Nitekim, üye devletlerin kapasitelerinin ve altyapılarının uyumlaştırılması ve söz konusu aktörlerin kamu ve özel sektörle iş birliği zemini oluşturmasına vurgu yapılmaktadır.[100] AB kurumları ve üye devletlerin partneri olarak, gündem belirleyici ve farkındalığı artırıcı özelliğiyle siber güvenlik alanında merkezî bir rol ifa eden özel sektör arasında iş birliğinin güçlendirilmesi, sektörden sektöre farklılık arz etmektedir. Örneğin, finans sektörü iş birliğine oldukça açıkken telekomünikasyon sektörü ise bilgi değişiminin rekabet avantajının aşınmasına yol açabileceği endişesiyle daha kapalıdır.[101] Bununla beraber, çıkarların farklılaşması nedeniyle özel ve kamusal sektör arasındaki iş birliği bağlamında da problemler söz konusudur. Bu noktada, kamusal sektör için güvenlik önceliklendirilirken özel sektör ise verimlilik ve kâr maksimizasyonuna yoğunlaşmaktadır.[102] Dolayısıyla çıkarların farklılaşması ve uyuşmazlığı durumu yaşanmakta ve bu husus siber güvenlik alanına da yansımaktadır.

Özetle, hem ortak bir güvenlik anlayışı hem de kurumsal koordinasyon ve iş birliği ekseninde tutarlılığın güçlendirilmesine yönelik teşebbüslerin tam anlamıyla somut bir sonuca ulaşmadığı görülmektedir. Bu noktada, kurumlar arasında açık bir şekilde belirlenmiş sorumluluk alanları, hesap verebilirlik eksikliği[103] ve

09.04.2020).

[100] Ibid.

[101] Giampiero Giacomello, "Introduction: Security In Cyberspace", Giampiero Giacomello (Edt.), *Security in Cyberspace- Targeting Nations, Infrastructures, Individuals*, Bloomsbury Academic, London, 2014, 1-20, p. 3.

[102] Myriam Dunn-Cavelty and Manuel Suter, "Public-Private Partnerships are no Silver Bullet: An Expanded Governance Model For Critical Infrastructure Protection", *International Journal of Critical Infrastructure Protection*, 2009, pp. 1-3, https://www.files.ethz.ch/isn/106323/PPP_no_silver_bullet.pdf, (Erişim Tarihi: 29.04.2020).

[103] Annegret Bendiek, "European Cyber Security Policy", 2012, https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2012_RP13_bdk.pdf, (Erişim Tarihi: 19.04.2020).

AB'nin uluslarüstü ve hükümetlerarası niteliği doğrultusunda parçalı bir mekanizma bulunduğu belirtilmektedir.[104] Öte yandan, kurumlar arası ve kurumların kendi içinde devam eden koordinasyon sorunu bulunmaktadır. Ek olarak, üye devletler ve AB kurumları arasında iş birliğinin güçlendirilememesine ilişkin ortaya çıkan sorun, üye devletler arasında yaşanan koordinasyon sorunu ile iç içe geçmekte ve daha da önemlisi üye devletler, AB'nin siber güvenlik alanında yetki gücünün güçlendirilmesi hususuna olumlu bakmamaktadır.[105] Ortak bir güvenlik anlayışının inşa edilmesine ilişkin çabaya ve retorik vurguya rağmen, AB'nin, üye devletleri bu alanda entegre olmanın önemi konusunda ikna etmekte yetersiz olduğu ve söz konusu alanda faaliyet göstermeye çalışan kurumların yetkilerinin ise oldukça kısır kaldığı görülmektedir. AB'nin siber güvenlik alanındaki tutarlılığına ilişkin ortaya çıkan durum ise tablo 6'da şematize edilmektedir.

Sonuç olarak, tarihsel kurumsalcılık teorisinin ortaya koyduğu mekanizmalarla büyük oranda örtüşen AB'nin siber güvenlik politikalarının, kurumsallaşma merkezli bir gelişim gösterdiği, ne var ki söz konusu politikanın bütüncül bir tutarlılığı yansıtmadığı görülmektedir. Aslında AB'nin siber güvenliğe ilişkin sosyo-ekonomik yaklaşımının ve beş temel hedefinin 34 yıldır devam etmesi, AB-siber güvenlik denklemindeki tutarlılığa ilişkin bir gösterge olarak kabul edilebilir. Ancak çalışmanın teorik kısmında ortaya konan Avrupa

---

[104] Alaxender Klimburg and Heli Tirmaa-Klaar,"Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU", 2011, p. 29, https://www.europarl.europa.eu/RegData/etudes/STUD/2011/433828/EXPO-SEDE_ET(2011)433828_EN.pdf, (Erişim Tarihi: 21.04.2020).

[105] Üye devletlerin, AB'nin siber güvenlik alanındaki yetkilerinin güçlenmesini istememelerinin altında, hükümetlerarası yapının etkisi ile yüksek ve alçak politika ayrımı bulunmaktadır. Alçak politika alanlarına giren ve daha işlevsel olan ekonomi, finans, maliye gibi alanlarda hem aktörler arası iş birliğinin sağlanması daha kolaydır hem de AB'nin bu alanda yetki sahibi olmasına yönelik üye devletlerden olumsuz sesler yükselmemektedir. Ancak güvenlik, savunma gibi daha siyasi ve hassas olan yüksek politika alanlarında hem iş birliğinin sağlanması daha zordur hem de çıkarları doğrultusunda üye devletler bu alanlarda AB'ye yetki devretmeyi istememektedir.

Komisyonu'nun "çok daha etkili olma ve aktörler arası iş birliğinin oluşturulmasını" merkeze koyan tutarlılık kavramsallaştırması perspektifinde bakıldığında, kurumsal koordinasyon ve ortak güvenlik anlayışı ekseninde yatay, dikey ilişkiler bağlamında çelişkiler ve sorunlar bulunduğu görülmektedir. Öte yandan, her ne kadar AB siber güvenlik alanında tutarlılık yaklaşımını ön plana alan bir duruş sergilese de ve bu alanda faaliyet gösteren kurumların yetkileri artırılsa da heterojen yaklaşımlar ve AB'nin üzerine inşa edildiği içsel dinamikler nedeniyle söz konusu tutarlılık, önemli oranda retorik ve üye devletlerin imtiyazı altında kalmaktadır.

Tablo 6: Siber Güvenlik Alanında Tutarlılık[106]

Tutarlılık	Yatay Eksen	Dikey Eksen
Kurumsal Koordinasyon	AB kurumları arasında iş birliğinin gelişmesine yönelik atıfta bulunan resmî belgelerin, niceliksel olarak arttığı ve siber güvenlik alanında faaliyetler gösteren kurumların kurulduğu görülmektedir. Yakın iş birliğine ilişkin söylemler, teorik kalmakta ve somut anlamda pratik boyuta taşınmamaktadır. Tutarlılık; finansal kaynaklar ve alana yönelik uzmanlardaki yetersizlik ve karmaşık işbölümü nedeniyle sınırlı kalmaktadır. Özel sektör arasındaki koordinasyonun büyük oranda sağlandığına ilişkin somut veriler bulunmamaktadır.	AB ve ulusal (üye devletler) düzleminde iş birliğinin geliştirilmesine ilişkin somut sorunlar bulunmaktadır. Siber güvenlik, üye devletlerin imtiyazı altında kalmaya devam etmektedir. Bölgesel ve bölge-altı işbirliklerinin geliştirilmesinde AB, parçalı bir yaklaşıma sahiptir. Siber güvenlik alanında ENISA ve EC3 yeni yetkiler kazanmıştır. Özel sektörün siber güvenlik alanında iş birliğinin sağlanmasına ilişkin istekliliği olmasına rağmen, bu durum sınırlı düzeyde sağlanmaktadır.

[106] Helena Carrapico and Andre Barrinha, "The EU as a Coherent Security Actor?", *JCMS*, 2017, Vol 55, No 6, 1254-1272, p. 1263.

Ortak Güvenlik Anlayışı	AB ve ulusal düzlemde ortaya konan resmî belgeler çerçevesinde siber tehditler ve güvenliğin sağlanmasına ilişkin teorik bazda ortak bir noktada buluşulmaktadır. Siber güvenliğe ilişkin ortak bir anlayış bağlamında üye devletlerin söylemleri ve taahhütleri belirgin değildir. Özel sektörün siber tehditlere ilişkin ortak bir anlayışa sahip olup olmadığına ilişkin somut veriler bulunmamaktadır. Önlem ve hazırlık faaliyetleri çerçevesinde benzer risk anlayışı bulunmamaktadır.	Siber güvenlikte merkezî bir rol oynamaları çerçevesinde üye devletlerin sorumlulukları artmaktadır. Ancak tüm üye devleler benzer tehdit ve sorunları yaşamamaktadır. Gelişim düzeyleri farklı olması nedeniyle üye devletler, siber tehditlere ilişkin benzer önlemler alamamakta ve bu tehditlere yönelik benzer karşılık verememektedir. Özel sektörün sadece bir bölümü, AB ve ulusal düzlemde ortaya çıkan kaygıları paylaşmaktadır.

Sonuç

AB; dış politika, savunma ve güvenlik merkezli oluşturulan bir proje olmasa da zaman içerisinde Birliğin, ekonomik entegrasyondan siyasi entegrasyona geçiş amacıyla hareket kabiliyetini güçlendirmeye çalıştığı ve özelde siber uzay kaynaklı tehditler bağlamında öne çıkan siber güvenliğin sağlanması konusunda politikalar takip ettiği ve bu alana ilişkin yoğun bir retorik vurgunun olduğu görülmektedir. Bu minvalden hareketle, özünde AB'nin siber güvenlik politikalarını tarihsel kurumsalcılık ve tutarlılık yaklaşımı çerçevesinde analiz ederek, bir kurumsallaşmanın mı yoksa tutarlılığının mı baskın geldiğini sorunsallaştırma amacıyla ortaya konan bu çalışma zarfında elde edilen ilk bulgu, hem AB ekseninde hem de ulusal düzlemde siber güvenliğe ilişin ortak bir kavramsallaştırma bulunmamasıdır. AB'nin bilgi ve iletişim teknolojilerine ilişkin ilgisinin ilk başlangıç noktasını oluşturulan 1985 yılında Avrupa Komisyonu'nun yayımladığı Beyaz Kitap'tan 2019 yılında yürürlüğe giren Siber Güvenlik Yasası'na kadar geçen süredeki siber güvenlikle ilgili dokümanların incelenmesi doğrultusunda, AB'nin siber güvenlik politikasının ve bu alandaki hedeflerinin gelişim serüveni analiz edilmiştir. İncelenen belgeler çerçevesinde AB siber

güvenliğe, sosyo-ekonomik ve beş nihai hedef merkezli yaklaşmaktadır. Bu doğrultuda ikinci bulgu, AB'nin siber güvenlik alanına sosyo-ekonomik merkezli yaklaşımının ve ekonomik fayda/maksimizasyonun sağlanması, temel hakların korunması, siber suçları/saldırıların önlenmesi, dijital sisteme yönelik güven unsurunun artırılması ve aktörler arasında iş birliğinin güçlendirilmesini içeren beş nihai hedefinin, 1985 yılından günümüze devam ettiğinin görülmesidir. Bu durum ise tarihsel kurumsalcılık teorisinin ortaya koyduğu ve başta alınan kararların, daha sonrakiler üzerinde etkili olacağını vurgulayan yol bağımlılığı mekanizmasıyla örtüşmektedir. Diğer taraftan AB, siber güvenlik politikalarına etki edecek iki önemli kritik dönemeçten geçmiştir. Söz konusu ilk dönemeç, Estonya'ya yapılan siber saldırılar ve ikinci dönemeç noktası ise AB'nin kurumsal mimarisine önemli değişiklikler getiren Lizbon Antlaşması'dır. Estonya saldırısı sonrası AB yaklaşımında herhangi bir değişime yönelmemiş, üstüne üstlük, kurumsal yapıda büyük dönüşümlere yol açan ve bu noktada AB'nin yetkilerinin kullanımı konusunda önemli bir mihenk taşı olan Lizbon Antlaşması'nın yetki kategorizasyonu ekseninde de AB yetkilerinin sosyo-ekonomik merkezli alanlarda olduğu görülmektedir. Dolayısıyla, AB'nin bu kritik dönemeçlere rağmen politika değişikliğine gitmeyerek siber güvenlik alanında sosyo-ekonomik odaklı yaklaşım sergilemeye devam etmesi ise teori bağlamında kritik dönemeçlerde politika değişikliğine gidebileceği savının temellendirildiği kesintiye uğramış denge mekanizmasının doğrulanmadığını göstermektedir ki bu da çalışma zarfında elde edilen üçüncü bulguyu teşkil etmektedir. Dolayısıyla, AB'nin siber güvenlik alanında savunma odaklı bir politikaya yönelmesi, hem statik yapı bağlamında yetkilerinin sınırlarının değişmemesinden hem de bu alanda hükümetlerarası özelliğin baskın olmasından ötürü yakın gelecekte beklenebilir bir durum değildir. Öte yandan, siber güvenlik alanında faaliyet gösteren EC3 ve ENISA'nın yetkilerinin güçlendirilmesi çerçevesinde teorinin sunduğu olumlu geri bildirim mekanizmasının işler olduğu sonucuna ulaşılması ise bir diğer bulguyu oluşturmaktadır.

Tutarlık yaklaşımı çerçevesinde ise gerek kurumsal koordinasyon ve iş birliği gerek ortak güvenlik anlayışı bağlamında hem AB ve ulusal düzlemde hem de özel sektör ekseninde sorunlar yaşandığı sonucuna

ulaşılmıştır. Aslında AB, siber güvenlik alanında tutarlılığı merkeze koyan bir yaklaşıma haizdir ve bu alanda faaliyet gösteren kurumların yetkileri peyderpey artırılmaktadır. Lakin üye devletlerin söz konusu alanda AB'nin kontrolüne ve yetkilerinin güçlendirilmesine ilişkin mukavemet göstermeleri, AB'nin üzerine kurulduğu dinamikler ve homojen olmayan yaklaşımlar doğrultusunda mevzubahis tutarlılık, retorik kalmakta ve imtiyaz büyük oranda üye devletlerin tekelinde bulunmaktadır. Bu noktada, neredeyse tamamen üye devletlerin imtiyazı altında bulunan siber güvenlik alanında Birlik yetkilerine ilişkin önemli bir değişim meydana gelmedikçe, Birliğin sosyo-ekonomik bir bağlamda hareket etmeye devam edeceği rahatlıkla öngörülebilmektedir. Ancak siber güvenlik alanı salt devletlerin yetkisi altına bırakılamayacak kadar karmaşık ve ulusötesidir.

Son kertede, AB'nin siber güvenlik politikaları tarihsel kurumsalcılık kuramının ortaya koyduğu çıktılarla büyük oranda uyuşması bağlamında kurumsallaşma merkezli bir gelişim göstermektedir. Fakat söz konusu politika ekseninde bütüncül bir tutarlılık söz konusu değildir. AB tutarlı olmaya çalışmakta ama bu husus, somut anlamda başarılmış gözükmemektedir. Bu noktada hem genel anlamda hem de siber güvenliğin sağlanması özelinde tutarlı bir AB'ne dönüşüm ihtiyacı bulunmaktadır.

Summary

Cyber security constitutes a new and popular area in contemporary security studies. Although the academic literature has not been focused on cyber security adequately for many years, it has been observed that security and cyberspace intersect at a common point following the development of information and communication technologies in a ground-breaking dimension and the interest in this field has increased recently. However, studies on the cyber security policy of the European Union (EU), which is an important actor in the international platform, has quite limited. Moving from this perspective, the cyber security policy of the European Union and the equation arises in the context of the cyber security phenomenon and the European

Union are analysed examined for finding out whether the equation is built on institutionalism or consistency.

Despite the contributions made by cyber space to human beings, it brings many problems because it includes all the actors which are related to the internet and communication technologies and its uncertain limit. In the context of these problems, the importance of the cyber security phenomenon for the European Union is increasing day by day and the policies regarding this field are carefully followed. On that note, it is seen that the EU approached cyber security with a socio-economic centre in the 34-year period started from the publication of the White Paper by the European Commission in 1985 to the Cyber Security Law which came into force in 2019. In addition, it was concluded that it tried to strengthen its mobility in cyber security field in line with five ultimate goals which includes ensuring economic benefits/maximization, protecting fundamental rights, preventing cyber-crime/attacks, increasing confidence in the digital system and strengthening cooperation among actors. This situation coincides with the concept of the "path dependency" of the historical institutionalism theory. On the other hand, the EU has gone through two important critical turns, one of which was the cyber-attack on Estonia in 2007 and the Lisbon Treaty, which came into force in 2009. However, despite these two important turning points, it is seen that the EU has not made a policy change and continues to approach the field of cyber security in a socio-economic manner. This does not match the theory's "punctuated equilibrium" mechanism. Additionally, increasing powers of ENISA and EC3 operating in the field of cyber security shows the functionality of the "positive feedback loop" of the theory.

The EU tries to be a coherent actor in the field of cyber security within the framework of institutional coordination and common security understanding facility. However, there are problems in strengthening coordination and cooperation and establishing a common understanding of cyber security between and within the EU, national and private sector. The lack of accountability of EU institutions, the difference in financial capacity of member states, the different approaches of member states in this field and the resistance against strengthening the powers of the EU

and the dominance of intergovernmental quality as a whole put off its coherency. As the cyber space has a very complex and ambiguous structure, it is vital to construct a consistent, holistic and collaborative approach that covers all stakeholders in the EU context. However, coherence remains rhetorical and grant in the field of cyber security is largely monopolized by member states.

In the last instance, the EU's cyber security policies have progressed an institutionalization-centred in the context of a great deal of harmony with the outcomes of the historical institutionalism theory. However, there is no holistic coherence in this policy field. Although the EU wants to be coherent both in general and in cyber security, it has not succeeded in concrete terms yet.

Kaynakça

Kitap

AKYEŞILMEN, Nezir, *Siber Politika ve Güvenlik*, Orion Yayınevi, Ankara, 2018.

BAYKAL, Sanem ve Göçmen, İlke, *Avrupa Birliği Kurumsal Hukuku*, Seçkin Yayıncılık, Ankara, 2016.

BAYRAM, H. Mehmet, *Avrupa Birliği Hukuku Dersleri*, Seçkin Yayıncılık, Ankara, 2015.

CHRISTOU, George, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy*, Palgrave, London, 2016.

EILSTRUPP-SANGIOVANNI, Mette, *Debates on European Integration*, Palgrave, Houndmilss, 2006.

GÖÇMEN, İlke, *Avrupa Birliği Maddi Hukuku*, Seçkin Yayıncılık, Ankara, 2017.

PIERSON, Paul, *Politics in Time: History, Institutions, and Social Analysis*, Princeton University Press, NJ., 2004.

ROSAMOND, Ben, *Theories of European Integration*, Palgrave, London, 2000.

Makale

BULMER, Simon, "The Governance of the European Union: A New Institutionalist Approach", *Journal of Public Policy*, 1993, Vol 13, No 4, pp. 351-380.

CARRAPICO, Helena and Barrinha, Andre, "The EU as a Coherent Security Actor?", *JCMS*, 2017, Vol 55, No 6, pp. 1254-1272.

CREMONA, Marise, "Coherence through Law: What Difference will the Treaty of Lisbon Make?", *Hamburg Review of Social Sciences*, 2008, Vol 3, No 1, pp. 11-36.

DARICILI, B., Ali, "Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Siber Güvenlik Modeli için Öneriler", *TESAM Akademi Dergisi*, 2019, Cilt 6, Sayı 2, ss. 11-33.

ERENDOR, Mehmet, E., "Risk Toplumu ve Refleksif Modernleşme Çerçevesinde Siber Terörizm: Tanımlama ve Tipoloji Sorunu", *Cyberpolitik Journal, 2016,* Cilt 1, Sayı 1, ss. 114-133.

FAHEY, Elaine, "EU'S Cybercrime and Cyber Security Rule-Making: Mapping the Internal and External Dimensions of EU Security", *European Journal of Risk Regulation*, 2014, Vol 5, No 1, pp. 46-60.

GIACOMELLO, Giampiero, "Introduction: Security In Cyberspace", , Giampiero Giacomello (Edt.), *Security in Cyberspace- Targeting Nations, Infrastructures, Individuals,* Bloomsbury Academic, London, 2014, pp. 1-20.

GUITTON, Charles, "Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK?", *European Security*, 2013, Vol 22, No 1, ss. 21-35.

HALL, Peter and Taylor, Charles, "Political Science and the Three New Institutionalisms", *Political Studies*, 1996, Vol 44, No 2, pp.936-957.

KRASNER, Stephen D., "Approaches to the State: Alternative Conceptions and Historical Dynamics", *Comparative Politics*, 1984, Vol 16, No 2, pp. 223-246.

PIERSON, Paul, "Increasing Returns, Path Dependence, and the Study of Politics", *American Political Science Association*, 2000, Vol 94, No 2, pp. 251-267.

PIERSON, Paul and Skocpol, Theda, "Historical Institutionalism in Contemporary Political Science", Ira Katznelson , Helen Milner and Ada Finifter (Edt.), *Political Science: The State of the Discipline,* Norton Press, NewYork, 2002, pp. 693-721

POLLACK, Mark, "The New Institutionalism and EU Governance: The Promise and Limits of Institutionalist Analysis", *Governance*, 1996, Vol 9, No 4, pp. 429-458.

POLLACK, Mark, "The New Institutionalism and European Integration", Antje Wiener ve Thomas Diez (Edt.), *European Integration Theory*, Oxford University Press, NewYork, 2009, pp. 125-143.

POMORSKA, Karolina and Vanhoonacker, Sophie, "Europe as a Global Actor: Searching for a New Strategic Approach", *JCMS*, 2016, Vol 52, No 1, pp. 216-229.

SLIWINSKI, Feliks, "Moving beyond the European Union's Weakness as a Cyber Security Agent", *Contemporary Security Policy*, 2014, Vol 35, No 3, pp. 468-486.

THELEN, Kathleen, "Historical Institutionalism in Comparative Politics", *Annual Review of Political Science*, 1999, Vol 2, pp. 369–404.

İnternet Kaynakları

ABİHA, 2012, https://www.ab.gov.tr/files/pub/antlasmalar.pdf, (Erişim Tarihi: 30.04.2020).

BANGEMANN, Martin, "Recommendations to the European Council Europe and the Global Information Society", 1994, http://www.channelingreality.com/Digital_Treason/Brussels_1995/Bangemann_report.pdf, (Erişim Tarihi: 13.03.2020).

BENDIEK, Annegret, "European Cyber Security Policy", 2012, https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2012_RP13_bdk.pdf, (Erişim Tarihi: 19.04.2020).

COLLIER, R. Berrins and Collier, David, "Framework: Critical Junctures and Historical Legacies", 1991, https://polisci.berkeley.edu/sites/default/files/people/u3827/Collier-Collier%20SPA%20Chap%201.pdf, (Erişim Tarihi: 10.04.2020).

CRAIGEN, Dan, Diakun-Thibault, Nadia and Purse, Randy, "Defining Cybersecurity", *Technology Innovation Management Review*, 2014, https://timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf, (Erişim Tarihi: 18.02.2020).

DUNN-CAVELTY, Myriam and Suter, Manuel, "Public-Private Partnerships are no Silver Bullet: An Expanded Governance Model For Critical Infrastructure Protection", *International Journal of Critical Infrastructure Protection*, 2009, https://www.files.ethz.ch/isn/106323/PPP_no_silver_bullet.pdf, (Erişim Tarihi: 29.04.2020).

ENISA, "Overview of Cybersecurity and Related Terminology", 2017, https://www.enisa.europa.eu/publications/enisa-positionpapers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology, (Erişim Tarihi:03.05.2020).

ENISA, "About ENISA", 2020, https://www.enisa.europa.eu/about-enisa, (Erişim Tarihi: 12.04.2020).

European Commission, "Completing the Internal Market", 1985, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51985DC0310&from=EN, (Erişim Tarihi: 09.02.2020).

European Commission, "Illegal and Harmful Content on Internet", 1996, http://aei.pitt.edu/5895/1/5895.pdf, (Erişim Tarihi: 10.03.2020).

European Commission, "Network and Information Security: Proposal for A European Policy Approach", 2001, https://ec.europa.eu/transparency/regdoc/rep/1/2001/EN/1-2001-298-EN-F1-1.Pdf, (Erişim Tarihi: 11.03.2020).

European Commission$_a$, "Some Practical Proposals for Greater Coherence, Effectiveness and Visibility", 2006, https://ec.europa.eu/councils/bx20060615/euw_com06_278_en.pdf, (Erişim Tarihi: 03.04.2020).

European Commission$_b$, "Strategy for a Secure Information Society", 2006, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l24153a, (Erişim Tarihi: 03.04.2020).

European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", 2013, http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf, (Erişim Tarihi: 15.03.2020).

European Commission$_a$, "The European Agenda on Security", 2015, https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52015DC0185, (Erişim Tarihi: 17.03.2020).

European Commission$_b$,"A Digital Single Market Strategy for Europe", 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192, (Erişim Tarihi: 18.03.2020).

European Commission, "Joint Framework on Countering Hybrid Threats", 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018, (Erişim Tarihi: 22.04.2020).

European Commission$_a$, "Resillience, Detterence and Defence: Building Strong Cyber Secuirty for the EU", 2017, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450, (Erişim Tarihi: 14.04.2020).

European Commission$_b$, "Cyber Security Act", 2017, https://eur-lex.europa.eu/legal-

content/EN/TXT/HTML/?uri=CELEX:52017PC0477&from=EN, (Erişim Tarihi: 19.04.2020).
European Commission, "Regulation on ENISA and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (Cybersecurity Act)", 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN, (Erişim Tarihi:01.05.2020).
European Commission, "The Directive on Security of Network and Information Systems (NIS Directive)", 2020, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive, (Erişim Tarihi: 17.03.2020).
European Council, "European Council Conclusions Corfu", 1994, http://aei.pitt.edu/1444/1/corfu_june_1994.pdf, (Erişim Tarihi: 09.03.2020).
European Council, "Tampere Council Conclusions", 1999, https://www.europarl.europa.eu/summits/tam_en.htm#c, (Erişim Tarihi: 02.04.2020).
European Council, "Council Framework Decision on Attacks against Information Systems", 2005, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN, (Erişim Tarihi: 11.03.2020).
European Parliament and Council, "Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data", 1995, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046, (Erişim Tarihi: 10.03.2020).
European Parliament and Council, "Directive on the Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector", 2002, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN, (Erişim Tarihi: 11.03.2020).
European Parliament and Council, "Directive 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", 2006, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0024&from=GA, (Erişim Tarihi: 11.03.2020).
European Parliament and Council, "Directive on Network and Information Systems across the Union", 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC, (Erişim Tarihi:15.04.2020).
Federal Ministry of the Interior, "Cyber Security Strategy for Germany", https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile, (Erişim Tarihi: 09.03.2020).
HELMBRECHT, Udo, Purser, Steve and Ritter-Klejn, Maj, "Cyber Security: Future Challenges and Oportunities", 2012, https://www.btg.org/wp-content/uploads/2012/01/ENISA-Cyber-Security-Report-2011.pdf, (Erişim Tarihi:03.05.2020).
KLIMBURG, Alaxender and Tirmaa-Klaar, Heli, "Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU", 2011, https://www.europarl.europa.eu/RegData/etudes/STUD/2011/433828/EXPO-SEDE_ET(2011)433828_EN.pdf, (Erişim Tarihi: 21.04.2020).
LOCKWOOD, Matthew, Kuzemko, Caroline, Mitchell, Catherine and Hoggett,

Richard, "Historical Institutionalism and the Politics of Sustainable Energy Transitions: A Research Agenda", 2016, https://core.ac.uk/download/pdf/43098859.pdf, (Erişim Tarihi: 19.02.2020).
Maastricht Treaty, 1992, https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_on_european_union_en.pdf, (Erişim Tarihi: 21.03.2020).
Ministry of Digital Affairs, "National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022", 2017, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncssmap/strategies/govermental-program-for-protection-of-cyberspace-for-theyears-2011-2016-2013, (Erişim Tarihi:09.03.2020).
MISSIROLI, Antonio, "Towards An Eu Global Strategy: Background, Process, References", 2015, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Towards_an_EU_Global_Strategy_0_0.pdf, (Erişim Tarihi: 12.03.2020).
National Security Authority, "Central European Platform for Cybersecurity", 2018, https://www.nbu.gov.sk/en/cyber-security/partnership/central-european-platform-for-cybersecurity/index.html, (Erişim Tarihi: 25.04.2020).
NIS Directive, 2016, https://eur-lex.europa.eu/eli/dir/2016/1148/oj, (Erişim Tarihi: 09.04.2020).
Single European Act, 1987, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:11986U/TXT&from=EN, (Erişim Tarihi: 10.03.2020).
Strategie Kybernetické Obrany ČR, 2018, http://www.acr.army.cz/assets/informacni-servis/zpravodajstvi/strategie-kyberneticke-obrany.pdf, (Erişim Tarihi: 07.05.2020).
TRAUNER, Florian, "The Internal–external Security Nexus: More Coherence under Lisbon?", 2011, https://www.ies.be/files/op89_The_internal-external_security_nexus.pdf, (Erişim Tarihi: 12.03.2020).