KRİTİK ALTYAPILARA YÖNELİK BİLİŞİM SUÇLARI, TÜRKİYE VE AB UYGULAMALARI

Cyber Crimes Against Critical Infrastructures, Turkey and EU Practices

Muhammet KARACA[*], **Ensar GÜL**[**]

Öz

Kritik altyapılar, işlediği bilgi/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılardır. Teknolojik gelişmeler birçok bakımdan büyük kolaylıklar sağlasa da çeşitli güvenlik sorunlarını da beraberinde getirmektedir. Siber uzayda işlenen suçların gün geçtikçe artması, devletlerin bu alanda güvenlik önlemlerini artırması gerektiğini ortaya koymaktadır. Türk Ceza Kanunu'nda, Avrupa Siber Suçlar Sözleşmesi'nde bu alanda farklı uygulamalar dikkat çekmektedir. Bu makalede, kritik altyapılara yönelik siber saldırılar incelenmiştir. Bu saldırılara

[*] Savunma İş Geliştirme Sorumlusu, TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi, muhammet.karaca@tubitak.gov.tr, ORCID: 0000-0003-2948-8727.

[**] Profesör Doktor, Maltepe Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Yazılım Mühendisliği Bölümü, ensargul@maltepe.edu.tr, ORCID: 0000-0001-8753-6075.

Makale Gönderim Tarihi/Received: 18.05.2020.

Makale Kabul Tarihi/Accepted: 08.05.2021.

Atıf/Citation: Karaca, Muhammet, ve Gül, Ensar. "Kritik Altyapılara Yönelik Bilişim Suçları, Türkiye ve AB Uygulamaları." *Bilişim Hukuku Dergisi* 3, no: 1 (2021): 1-30.

karşı yapılan çalışmalardan ve alınan tedbirlerden bahsedilerek gerekli önerilerde bulunulmuş ve sonuçlar değerlendirilmiştir.

Anahtar Kelimeler: Kritik Altyapılar, Bilişim Güvenliği, Siber Suçlar, İnternet Hukuku, Avrupa Siber Suçlar Sözleşmesi.

Abstract

Critical infrastructures describe the physical and cyber systems which cause loss of lives, large scaled-economical damage, national security flaw or public order breakdown when their info/data confidentiality, integrity or accessibility is compromised. Although technological advances provide great convenience in many ways, they also bring various security problems. The increasing number of crimes committed in cyberspace reveal that goverments need to increase their security measures in this field. The Turkish Criminal Law, European Cyber-Crimes Contract have different laws and practices in this field. In this article cyber attacks on critical infrastructures and the measures taken against these attacks are discussed.

Keywords: Critical infrastructures, Information Security, Cyber Crimes, Internet Law, European Cyber-Crimes Contract.

GİRİŞ

Kritik altyapı, ülkeden ülkeye ve ülke birliklerine göre farklı farklı şekillerde tanımlanabilmektedir. Türkiye için kritik altyapı, işlediği bilgi/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar olarak ifade edilmektedir.[1]

[1] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, *2016-2019 Ulusal Siber Güvenlik Stratejisi*, (Ankara: T.C. UDHB, 2016), 8, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf.

Bilişim sistemlerinin gün geçtikçe gelişmesi ve değişmesi, farklı şekillerde işlenen bilişim suç fiillerinin de artmasına neden olmaktadır. Her ne kadar teknoloji büyük bir kolaylık sunsa da hukuka aykırı olarak bu teknolojinin kullanıldığına ve siber saldırıların artarak devam ettiğine her geçen gün şahit olunmaktadır. Bu konuya hem Türk Ceza Kanunu'nda hem de Avrupa Konseyi tarafından hazırlanan Siber Suçlar Sözleşmesi'nde önemli bir yer ayrılmıştır.[2]

765 sayılı Mülga Türk Ceza Kanunu'nda, bilişim suçlarına yönelik hükümler oldukça kısıtlıyken, 5237 sayılı yeni yasanın yürürlüğe girmesi ile daha geniş çaplı hükümlere yer verilmiştir. 5237 sayılı yasanın 243-246. maddelerinde bilişim alanında işlenecek suçlarla ilgili yeni düzenlemeler yapılmıştır. Bu bağlamda hem bilişim sistemleri ile işlenen suçlar hem de bilişim sistemlerine karşı işlenen suçlar, TCK'nın ilgili maddelerinde yerini almıştır.

Avrupa Konseyi Siber Suçlar Sözleşmesi de küreselleşmenin kaçınılmaz bir sonucu olan bilişim suçlarının küreselleşmesi sorununa bir çözüm üretilebilmesi için ortaya konmuş, birçok ülke tarafından kabul gören ve imzalanan bir sözleşme olmuştur. Bugün bu sözleşme kapsamında birçok bilişim suçu ile ilgili hükme yer verilmektedir.

Gelişen teknoloji hem birey bazında hem de kurumlar bazında olumlu ve olumsuz etkiler barındırmaktadır. Teknolojinin ilerlemesi, zaman, maliyet ve kalite konusunda büyük avantajlar sağlarken, yeni saldırı tiplerini de beraberinde getirmektedir. Bu saldırılar artık doğrudan fiziki bir saldırı olmaktan çıkmış, dolaylı yollardan bilişim sistemleri kullanılarak ve fark edilmesi imkânsız ya da uzun zaman alan bir saldırı tipine dönüşmüştür.

---

[2] Ebru Altunok ve Ali Fatih Vural, "Bilişim Suçları," *Denetişim*, no. 8 (2016): 76.

Bu makale dört bölümden oluşmaktadır. İlk bölümde, kritik altyapılara yönelik gerçekleştirilen bilişim suçları ve şekilleri ele alınmış ve kritik altyapıların tanımı yapılarak ve yapılara yönelik siber saldırı örnekleri verilerek durum analizi yapılmıştır. İkinci bölümde konu ile ilgili yayımlanmış eserlerden bahsedilmiştir. Üçüncü bölümde kritik altyapılarla ilgili ülkemizde ve Avrupa Birliği'nde yapılan çalışmalar incelenmiş, bu alanlarda yapılan siber saldırılarla ilgili yasal ve kurumsal düzenlemelere yer verilmiştir. Dördüncü bölümde kritik altyapılara yönelik siber saldırı istatistikleri verilmiş ve değerlendirmeler yapılmıştır. Son bölüme gelindiğinde çalışmamız ile ilgili sonuç ve değerlendirmeler yapılacaktır.

I. KRİTİK ALTYAPILAR VE KRİTİK ALTYAPILARA YÖNELİK SİBER SALDIRILAR

Teknolojinin gelişimi ve farklılığı, kritik altyapı sayılan sektörlerin de çeşitliliğini artırmıştır. Bu çeşitlilikle siber saldırılar artarak yükselmiş ve sektörlere göre çeşitlilik göstermiştir. Öyle ki bu saldırıların sayısı yıllık bazda milyonların üzerine çıkmıştır.

Kritik altyapılara yönelik siber saldırılar ulusal güvenliği tehlikeye atmaktadır.[3] Önce hangi altyapıların kritik altyapı olarak tanımlandığına bakmamız faydalı olacaktır.

A. Kritik Altyapı Sistemleri

Ülkelerin gelişmişlik oranı, değer kavramları ve teknolojik donanımlarına göre kritik altyapı olarak nitelendirilen sistemleri

[3] Kenneth Geers, "The Cyber Threat to National Critical Infrastructures: Beyond Theory," *Information Security Journal: A Global Perspective*, no. 18 (2009): 1.

farklılaşmaktadır. Türkiye[4], AB[5] ve ABD[6] için belirlenen kritik altyapı sistemleri tablo şeklinde sunulmuştur:

Tablo 1: Türkiye, AB ve ABD' ye Göre Kritik Altyapılar

TÜRKİYE	AB	ABD
Enerji	Su ve Gıda	Ticari Tesisler
Su Yönetimi	Nakliye ve Ulaşım	Kimya Sektörü
Kritik Kamu Hizmetleri	Sağlık ve Finans	Kritik İmalat Sektörü
Ulaştırma	Kamu Düzeni ve Emniyet	İletişim Sektörü
Bankacılık ve Finans	Nükleer ve Kimyasal	Savunma Sanayi Baz Sektörü
Elektronik Haberleşme	Uzay ve Araştırmalar	Acil Servis Sektörü
	Bilgi ve İletişim Sektörü	Barajlar
		Enerji Sektörü
		Devlet Tesisleri
		Sağlık ve Halk Sağlığı
		Su ve Atık Su Sistemleri
		Bilgi Teknolojileri
		Ulaştırma Sektörü
		Nükleer Reaktörler, Malzemeler ve Atık Sektörü

Kritik altyapı sektörlerine ilişkin Tablo 1'e bakıldığında ABD'nin devlet endeksli ve ekonomik güvenliğe yönelik bir belirleme içinde olduğu görülmektedir. Kritik altyapı niteliğindeki işletmelerin birçoğunun özel şirketler tarafından yürütüldüğü ABD'de, devletin amaçlarından biri de bu şirketler arasında en yüksek seviyede iş birliğini sağlamaktır. Olası bir saldırıda ya da saldırı öncesinde bu şirketler arasında

---

4 T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. *2016-2019 Ulusal Siber Güvenlik Stratejisi*, 8.

5 "European Programme for Critical Infrastructure Protection-Summaries of EU Legislation", EUR-Lex, erişim tarihi: Aralık 26, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l33260&from=EN.

6 The White House, "Presidential Policy Directive," erişim tarihi: Aralık 2, 2018, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resilience.

koordinasyon sağlanması ve bilgi paylaşımı yapılması hedeflenmektedir.

AB açısından kritik altyapılar, ABD'nin aksine, sadece güvenlik ya da savunmaya yönelik altyapılar değildir. Kritik altyapıların belirlenmesinde daha sivil bir anlayışın olduğu söylenebilecektir. AB, bu kapsamda siber alanda teşvikler sunmakta ve tedbirlerin alınmasını kolaylaştırıcı önlemler almaktadır.

Türkiye'deki kritik altyapı sistemleri ise ekonomik ve kamu güvenliği endeksli belirlenmiştir. Ülkemizde bu alanın tanımlanması ABD ve AB'ye göre çok daha yeni olduğu için belirlenen sektörlerin çeşitliliği de değişmektedir. Örneğin, bilişim alanının kritikliği ülkemiz açısından sonraki yıllarda ortaya çıkan bir durum olmuştur. Ülkemizde, son dönemlerde gerek siber alan gerekse kritik altyapılara ilişkin çalışmalara hız verilmiş ve yeni birtakım düzenlemelerin yapılmasına başlanmıştır.

Türkiye'nin, kritik altyapı sistemi olarak tanımladığı alanları genişletmesi gerektiği Tablo 1'den anlaşılmaktadır. Teknolojinin hızlı gelişimi ve yaygın kullanımından dolayı Bilgi Teknolojilerini, Türkiye Uzay Ajansının kurulmasının akabinde Uzay Araştırmalarını ve Sinop ile Mersin'de yapılmakta olan nükleer santrallerden dolayı Nükleer Reaktörleri kritik altyapı sistemlerine dahil etmesi gerekmektedir.

B. Kritik Altyapılara Yapılan Siber Saldırı Vakaları

Teknolojik donanımları bünyesinde ağırlıklı olarak barındıran kritik altyapı sistemleri aynı zamanda üzerinde büyük bir risk taşımaktadır. Gerek ülkeler arasındaki rekabetler gerek düşmanlık duyguları gerekse kişisel menfaatler bu sistemlere saldırıları ön plana çıkarmıştır.

Kritik altyapı sistemlerini hedef alarak yapılan siber saldırılara örnek vermek gerekirse; 2000 yılında Avustralya'da, atık kontrol sistemine izinsiz erişen eski bir çalışan, birçok atık istasyonunun komutasını ele geçirerek bir milyon litrelik bir

atığın nehir ve deniz sularına karışmasına sebebiyet vermiştir.[7] Yine 2016 yılında Türkiye, tarihindeki en kapsamlı siber saldırıya maruz kalmıştır. Gerek internet trafiğini gerekse de ".tr" alan adlarını hedef alan bir DDOS (*distributed denial of service attack*) saldırısı gerçekleşmiştir. 2015 yılında Black Energy 3 adlı kötü amaçlı yazılım Ukrayna elektrik sistemini saatlerce devre dışı bırakmıştır. Bu saldırılara benzer birçok örnekler bulunmaktadır.

İnternete bağlı olmayan altyapılara bile siber saldırı yapmak mümkündür. Bu saldırılara örnek olarak 2010 yılında İran nükleer enerji altyapısını hedef alan bir siber saldırıyı gösterebiliriz. Daha sonra bu zararlı yazılımın adı *Stuxnet* olarak açıklanmıştır. Öyle ki bu saldırıda kullanılan zararlı yazılımlar sadece bu saldırı yapmak için geliştirilmiştir ve İran ciddi manada zarar görmüştür.[8]

Kritik altyapıların güvenliği için önlemler alınsa da bu tek başına yeterli olmamaktadır. Teknoloji hızlı bir gelişim içerisinde olduğundan aynı hızla saldırı çeşitleri de çoğalmaktadır. Bundan dolayı devletler ve şirketler bu önlemleri güncel tutmak zorundadırlar. Güncel durumun teyidi ve gerekli önlemlerin ne ölçüde olduğunu görebilmek için kurum ya da şirketler sızma testleri yaptırmaktadır. Bu testler, ihtiyaca göre

---

7 Kevin Curran, Kevin Concannon ve Sean McKeever, "Cyber Terrorism Attacks," iç. *Cyber Warfare and Cyber Terrorism*, ed. Lech J. Janczewski ve Andrew M. Colarik, (Hershey, PA: IGI Global, 2008): 2, http://doi:10.4018/978-1-59140-991-5.ch001.

8 Dünyada kritik altyapılara karşı yapılan çeşitli siber saldırılar hakkında bkz. Mutsuo Noguchı ve Hirofumi Ueda, "An Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures," *NEC Technical Journal* 12, no. 2 (2017), erişim tarihi: Kasım 16, 2020, https://www.nec.com/en/global/techrep/journal/g17/n02/pdf/170204.pdf.; Ana Kovacevic ve Dragana Nikolic, "Cyber Attacks on Critical Infrastructure: Review and Challenges," iç. *Handbook of Research on Digital Crime, Cyberspace Security and Information Assurance*, ed. Maria Manuela Cruz-Cunha ve Irene Maria Portela, (Hershey, PA: IGI Global, 2015): 6, http://doi:10.4018/978-1-4666-6324-4.ch001.

açık sızma testi ya da kapalı sızma testi olarak yapılmaktadır. Açık sızma testi yapılırken testi yapan firmaya şirketle ilgili maksimum oranda bilgi verilmektedir. Kapalı sızma testinde ise testi yapacak firmaya şirketle ilgili hiçbir bilgi verilmeden test yaptırılmaktadır. Bu testler sonucunda şirketin içeriden ya da dışarıdan gelebilecek saldırılara karşı hangi konumda olduğu belirlenmekte ve eksiklikler giderilmeye çalışılmaktadır.

II. İLGİLİ ÇALIŞMALAR

Aydın, bilişim suçları ile ilgili hukuki düzenleme yapılmadan önce bu konuya dikkat çekmiş ve bilişim suçlarının toplum düzenine aykırı davranışlar olarak kabul edildiğini, fakat yasaların ihlal edilmesi olarak tanımlanmadığını belirtmiştir.[9] Erdoğan tarafından adli bilişimin bir bilim dalı olarak kabul edilmesi ve adli tıp benzeri bir yapılanma kurulması önerilmiştir.[10] Böylece nesnelerin de internete bağlanmasıyla çok daha büyüyecek olan bilgisayar ağlarına yönelik saldırılar ve işlenecek suçların tespiti yapılabilecektir. Özsoy Yargıtay kararları ışığında doğrudan bilişim suçlarını incelemiş, TCK 243. ve 244. maddeleri üzerine yorumlar yapmıştır.[11] Bilişim suçlarına yönelik Yargıtay kararlarının incelenmesi neticesinde yerel mahkemelerin suçun vasfını belirlemek konusunda zorluk yaşadığı görülmüştür.[12] Bilişim suçlarının hızla yöntem değiştirdiği ve kanuni düzenlemelerin

---

9 Emin Aydın, "Bilişim Sistemlerinde Güvenlik, Güvenirlilik Mahremiyet ve Bilişim Suçları," *Marmara İletişim Dergisi* 1, no. 1 (1992): 113.

10 Yavuz Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu," *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 12, (2010): 1427.

11 Nevzat Özsoy, "Yargıtay Kararları Işığında Doğrudan Bilişim Suçları," *Yaşar Hukuk Dergisi* 1, no. 2 (2019): 296.

12 Metin Turan ve Özgür Külcü, "Türkiye'de Bilişim Suçlarının Tanımlanması ve Yaşanan İhlallere Yönelik İçerik Analizi," *Türk Kütüphaneciliği* 28, no. 1 (2014): 19.

buna ayak uyduramadığı öne sürülmüştür.[13] Apiş, Bilişim Sistemlerine Girme Suçunu karşılaştırmalı hukuk açısından incelemiştir.[14] Erdağ, bu maddeler ile Alman Ceza Kanunu'nun ilgili düzenlemelerini incelemiş, Alman Ceza Kanunu'nda bilişim suçlarının Türk mevzuatında olduğu gibi ayrı bir başlıkta düzenlenmediği belirtmiştir.[15]

Kritik altyapılara yönelik Türkçe yayın sayısı yok denecek kadar azdır. Ak, iç güvenlik yönetimi açısından kritik yapıların korunmasına dair yeni bir iç güvenlik yaklaşımına ihtiyaç duyulduğunu belirtmiş, bu yapılara yönelik internet üzerinden de tehditlerin gelebileceğine dikkat çekmiştir.[16] Göçoğlu, akıllı şehirlerde kullanılan elektrik dağıtım sistemi, su ve atık su dağıtım sistemi ve ulaşım altyapısının, elektronik sistemlerle kontrol edildiğini, bu sistemlerin siber güvenliğinin sağlanması gerektiğini belirtmiştir.[17] Kritik altyapı operatörlerini kamera ile gözlemleyerek yorgunluk, uyku gibi davranışlar gösterdiklerinde uyarı veren bir sistem Osman Yeşil, Erdal Irmak ve Halil İbrahim Bülbül tarafından geliştirilmiştir.[18]

Von Solms, ülke içinde internete bağlı herhangi bir bilgisayarın kritik sistemler için risk oluşturabileceğini ve siber

---

13 Ercan Yılmaz, Serkan Gönen ve Halil İbrahim Ulus, "Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme," *Bilişim Teknolojileri Dergisi* 9, no. 3 (2016): 229.

14 Özge Apiş, "Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama," *Yasama Dergisi*, no. 37 (2018): 52.

15 Ali İhsan Erdağ, "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)," *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi* 14, no. 2 (2010): 285.

16 Tarık Ak, "İç Güvenlik Yönetimi Açısından Kritik Altyapıların Korunması," *ASSAM Uluslararası Hakemli Dergi* (2019): 46.

17 Volkan Göçoğlu, "Cyber Security of Critical Infrastructures in Smart Cities," *Uluslararası Yönetim Akademisi Dergisi* 2, no. 1 (2019): 56.

18 Osman Yeşil, Erdal Irmak ve Halil İbrahim Bülbül, "Kritik Altyapı Operatörleri İçin Görüntü İşleme Tabanlı Bir Yorgunluk Tespit ve Uyarı Sistemi," *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi* 6, no. 1 (2020): 39.

saldırılara karşı bütüncül bir yaklaşımla mücadele edilmesi gerektiğini söylemiştir.[19] Kozik ve Choras kritik altyapılara yönelik siber saldırıların fiziksel saldırılar kadar önemli olduğunu ve stratejik analizlere dâhil edilmesi gerektiğini belirtmiştir.[20] Kritik altyapılarda kullanılan endüstriyel kontrol sistemleri bilinen standartlara uygun parçalar kullandığından diğer bilgisayar sistemleri gibi siber saldırılara maruz kalabilecektir.[21]

Günümüzde enerji sistemleri sayısal sistemler tarafından kontrol edildiğinden siber saldırı tehdidi bu sistemler için de geçerlidir. Bu sistemleri siber saldırılara karşı korumak için bilişim teknolojisi ve operasyonel konularda uzmanlık gereklidir.[22] SCADA sistemleri ile kontrol edilen elektrik şebekesinin DOS, ortadaki adam ve kötücül yazılımlardan nasıl etkileneceği ve elektrik şebekesinin bu saldırılar sonucu kesintiye uğrayabileceği gösterilmiştir.[23] Malezya'da internet alt yapısının bir kritik altyapı olarak değerlendirilmesi ve siber terör

---

19 Sebastiaan von Solms, "Critical information infrastructure protection: How comprehensive should it be?," *2013 International Conference on Adaptive Science and Technology*, (Pretoria: IEEE, 2013): 1, https://doi.org/10.1109/ICASTech.2013.6707516.

20 Rafal Kozik ve Michal Choraś, "Current cyber security threats and challenges in critical infrastructures protection," *2013 Second International Conference on Informatics & Applications*, (Lodz: IEEE, 2013): 93, https://doi.org/10.1109/ICoIA.2013.6650236.

21 Kovacevic ve Nikolic, "Cyber Attacks on Critical Infrastructure: Review and Challenges," 5.

22 Chee Kiong Gary Ang ve Utomo Nugroho, "Cyber Security in the Energy World," *2017 Asian Conference on Energy, Power and Transportation Electrification*, (Singapore: IEEE, 2017): 3, https://doi.org/10.1109/ACEPT.2017.8168583.

23 Ester Ciancamerla, Michele Minichino ve Silvia Palmieri, "Modeling cyber attacks on a critical infrastructure scenario," *IISA 2013*, (Piraeus: IEEE, 2013): 2, https://doi.org/10.1109/IISA.2013.6623699.

saldırılarına karşı korunması gerektiği tavsiye edilmiştir.[24] İtalya'da, kritik bilişim altyapısını korumak üzere Napoli Futura isminde bir proje başlatılmış, büyük veri analitiği kullanarak siber saldırıların önlenmesi için öneriler getirilmiştir.[25] ABD'de, Başkanlık Ulusal Altyapılar Tavsiye Kurulu kritik altyapıların siber saldırılara karşı korunması ile ilgili bir rapor yazmıştır.[26] Taylor ve Sharif, kritik altyapıların siber-fiziksel sistemler olduğunu belirtmiş ve bu sistemlerin siber saldırılara karşı savunmasının zayıf olduğunu dile getirmiş, siber güvenliğin sağlanması için karmaşık olmayan ve kullanımı kolay siber savunmanın bu sistemlerde uygulanması gerektiğini belirtmiştir.[27]

---

24 Zahri Yunos et al., "Safeguarding Malaysia's critical national information infrastructure (CNII) against cyber terrorism: Towards development of a policy framework," *2010 Sixth International Conference on Information Assurance and Security*, (Atlanta, GA: IEEE, 2010): 25, https://doi.org/10.1109/ISIAS.2010.5604182.

25 Stefano Avallone et al., "Napoli Futura: Novel Approaches for Protecting Critical Infrastructures from Cyber Attacks," *2014 IEEE International Symposium on Software Reliability Engineering Workshops*, (Naples: IEEE, 2014): 35, https://doi.org/10.1109/ISSREW.2014.53.

26 The Cybersecurity and Infrastructure Security Agency, "National Infrastructure Advisory Council Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure Final Report," erişim tarihi: Aralık 6, 2020, https://www.cisa.gov/publication/niac-securing-cyber-assets-addressing-urgent-cyber-threats-critical-infrastructure-final.

27 James M. Taylor ve Hamid R. Sharif, "Security challenges and methods for protecting critical infrastructure cyber-physical systems," *2017 International Conference on Selected Topics in Mobile and Wireless Networking*, (Avignon: IEEE, 2017): 5, https://doi.org/10.1109/MoWNet.2017.8045959.

III. TÜRKİYE VE AVRUPA'DA KRİTİK ALTYAPILARIN SİBER GÜVENLİĞİNE YÖNELİK GERÇEKLEŞTİRİLEN YASAL VE KURUMSAL DÜZENLEMELER

A. Türkiye Çalışmaları

Bilişim suçlarının niteliği ve kapsamı göz önüne alınarak bu suçlar için farklı düzenleme yapılması gerekliliği ortaya çıkmıştır.[28] Türkiye'de siber suçları da kapsayan bilişim alanındaki suçlarla ilgili ilk düzenleme 1991 yılında, 765 sayılı TCK'nın 20. maddesine eklenen "Bilişim Alanında Suçlar" başlığı ile yapılmıştır.[29] 2004 yılında yürürlüğe giren 5237 sayılı TCK ile "Bilişim Alanında Suçlar" tanımı teknolojinin gelişimine paralel olarak genişletilmiştir. Bu kanunun 243. maddesi ile bilişim sistemine girme, 244. maddesi ile girilen sisteme müdahale, 245. maddesi ile kredi kartlarının ve banka kartlarının kötüye kullanımı ve 246. maddesiyle 243-245. maddelerde belirtilen suçları işleyerek haksız kazanç sağlayan tüzel kişinin durumuyla ilgili suçlar tanımlanmıştır.

Bilişim kavramının geçtiği bir alanda akla ilk gelen kelime internettir. İnternetin varlığı ve yaygınlaşmasıyla bu alanda yasal düzenlemelere ihtiyaç duyulmaya başlanmıştır. Ülkemizde internet ile ilgili ilk kapsamlı düzenleme 23 Mayıs 2007 yılında, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun[30] ile yapılmıştır. Kanunla internet erişimlerinin kontrol altına alınması amaçlanmıştır.

5651 sayılı kanun tüm bu olumsuzlukları en düşük seviyeye indirmeyi amaçlayarak, hizmet veren kurumların, hizmet sundukları ve internette savunmasız bulunan kullanıcıları korumasını istemektedir. Bu sebeple, ücretli ya da ücretsiz

---

28 Berrin Bozdoğan Akbulut, "Bilişim Suçları," *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 8, no. 1-2 (2000): 551.

29 RG. 14.06.1991, S. 20901.

30 RG. 04.05.2007, S. 26530.

birden çok kişiye internet erişim hizmeti sunan tüm kurum ve kuruluşlardan henüz kara listeye alınmamış web sayfasında işlenebilecek suçları sonradan takip edebilmek ve kim/kimler tarafından nasıl gerçekleştirildiğinin öğrenilmesi amacıyla web sayfalarına erişen tüm kullanıcıların kayıtlarının (*log*) zaman ve tarih mührü ile tutulması ve saklanması istenmektedir. Buna göre, internet sağlayıcı konumunda bulunan kurumlar ve kuruluşlar kendi ağları içerisinde dağıtılan IP adreslerinin bilgilerini, kullanıma başlanıp bitirilme saatlerini ve kullanılan IP adresleriyle bağlantı kuran bilgisayarların MAC adreslerini elektronik ortamda kayıt altına almak zorundadır. Ayrıca, bu kayıtların doğruluk ve bütünlüğü için elde edilen verileri, dosyanın oluşturulduğu zaman bilgisini ve dosyaların "*hash*" bilgilerini günlük olarak kayıt altına almalıdır. Erişim kayıtlarının 1 yıl ilâ 2 yıl arasında saklanması istenmektedir.

5846 Sayılı Fikir ve Sanat Kanunu[31] (FSEK) madde 2'de, 7 Haziran 1995 tarihinde 4110 sayılı kanunun eklenmesi ile değişikliğe gidilmiş ve "eser" kavramının tanımlaması yapılırken bilişim programları da koruma altına alınmıştır. Madde 2'de bahsi geçen eserler, dil ve yazı ile ifade edilen eserler, bilgisayar programları ve bunların hazırlıkları olarak ifade edilebilir.

FSEK madde 6'da ise yeni eklenen kanun maddesi yer almaktadır. 10 numaralı bende şu ibareler eklenmiştir: "Bir bilgisayar programının uyarlanması, düzenlenmesi ya da program üzerinde değişim yapılması da fikir ve sanat eseri sayılmaktadır." Yapılan bu değişiklikle madde Avrupa Konseyi ilkelerine uygun hale getirilmiştir.[32]

TBMM tarafından 15 Ocak 2004 tarihinde kabul edilen ve bundan altı ay sonra yürürlüğe giren 5070 sayılı Elektronik İmza

---

31 RG. 05.12.1951, S. 7981.

32 Ali Karagülmez, *Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri*, (Ankara: Seçkin Yayıncılık, 2005), 154.

Kanunu[33], Avrupa Birliği direktifleri doğrultusunda hazırlanmıştır. Kanunda amaçlanan, elektronik imzanın hukuki ve teknik yönleri ile ilgili çeşitli yaptırımların sağlanabilmesidir. Bu madde ile elektronik araçlar kullanılarak oluşturulan rızasız, hukuka aykırı ve aynı zamanda da izinsiz şekilde düzenlenen elektronik imzaların yaptırımları net olarak ifade edilmektedir.

2006 yılında yapılan bir değişiklik ile 3713 sayılı Terörle Mücadele Kanunu[34]'nda siber suçların terör kapsamında değerlendirileceği durumlar belirtilmiştir. 2016 yılında, 6698 sayılı Kişisel Verilerin Korunması Kanunu[35] ile kişisel veriler kanun nezdinde koruma altına almıştır.

Ülkemizde siber saldırılarla ilgili en yüksek yetkili merci, Bilgi Teknolojileri ve İletişim Kurumudur. Kurumun amacı; Uluslararası sözleşmeler ile garanti altına alınan haberleşme ve mahremiyetin korunmasını sağlamak ve 2007 tarihli 5651 sayılı kanun gereği "… İnternet ortamında işlenen belirli suçlar ile içerik, yer ve erişim sağlayıcılar üzerinden mücadeleye ilişkin usul ve esaslar belirlemektir". Bilgi Teknolojileri ve İletişim Kurumu'nun yanında TÜBİTAK, Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve Siber Olaylara Müdahale Merkezi (SOME), Afet ve Acil Durum Yönetim Başkanlığı (AFAD), Türk Silahlı Kuvvetleri (TSK), Emniyet Genel Müdürlüğü ve Millî İstihbarat Teşkilâtı da siber saldırılara karşı ülkemizin korunmasında etkin rol almaktadırlar.

Ülkemizde özellikle 2000'li yılların başından itibaren siber güvenlik alanında çalışmalar ve düzenlemeler yapılmıştır. Bunlar[36]:

2003/10 Sayılı Başbakanlık Genelgesi (2003)

---

33 RG. 23.01.2004, S. 25355.

34 RG. 12.04.1991, S. 20843 Mükerrer.

35 RG. 24.03.2016, S. 29677.

36 Hasan Çiftçi, *Her Yönüyle Siber Savaş*, (Ankara: TÜBİTAK, 2017).

2003/12 Sayılı Başbakanlık Genelgesi (e-Dönüşüm Türkiye Projesi)

e-Dönüşüm Türkiye Projesi 2005 Yılı Eylem Planı

Bilgi Toplumu Stratejisi ve Eylem Planı (2006-2010)

Ulusal Bilgi Güvenliği Programı (2007)

BOME 2008 Tatbikatı (İlk Siber Tatbikatımız) (2008)

Ulusal Sanal Ortam Güvenlik Politikası (2009)

Ulusal Siber Güvenlik Tatbikatı (2011)

Siber Güvenlik Çalıştayı (2011)

Siber Güvenlik Hukuku Çalıştayı (2012)

Siber Kalkan Tatbikatı (2012)

Türkiye Siber Güvenlik Organizasyonu ve Yol Haritası (2012)

Ulusal Siber Güvenlik Strateji Çalıştayı (2012)

TSK Siber Savunma Komutanlığı'nın Kurulması (2012)

TÜBİTAK Siber Güvenlik Enstitüsü'nün Kurulması (2012)

Siber Güvenlik Kurulu'nun Kurulması (2012)

Ulusal Siber Güvenlik Tatbikatı-2 (2013)

Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) (2013)

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı

Kurumsal SOME'lerin Kurulması (2013)

2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi (AFAD)

Siber Güvenlik Faaliyetlerinin Yasalaşması (2014)

Sanal Ortamda İşlenen Suçlar Sözleşmesi (Budapeşte Sözleşmesi) (2014)

Uluslararası Siber Kalkan Tatbikatı (2014)

Bilgi Toplumu Stratejisi ve Eylem Planı 2015-2018

Elektronik Ticaretin Düzenlenmesi

Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı

TSK Siber Savunma Merkezi Projesi (SİSAMER)(2016)

Kamu Kurum ve Kuruluşlarının KamuNet'e Dahil Edilmesi (2016)

Ulusal Siber Savunma 2017 Tatbikatı

"Bilgi ve İletişim Güvenliği" Başlıklı 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi[37],

Bilgi ve İletişim Güvenliği başlıklı Cumhurbaşkanlığı Genelgesinden bahsetmek faydalı olacaktır. Genelge, 6 Temmuz 2019 tarihli resmî gazetede yayınlanarak, kamu kurum ve kuruluşlarının bilgi ve iletişime yönelik uyması gereken birtakım kurallardan bahsetmiştir. Bu kurallardan özellikle bazıları çok önemli niteliktedir. Bu önemli maddeler incelenecek olursa;

* (Madde 1): *"Nüfus, sağlık ve iletişim kayıt bilgileri ile genetik ve biyometrik veriler gibi kritik bilgi ve veriler yurt içinde güvenli bir şekilde depolanacaktır***."** Söz konusu madde hayata geçirildiği takdirde; kritik bilgi ve verilerin yurt dışına çıkmasının ve yabancı devletlerin eline geçmesinin önünde büyük bir engel oluşturacaktır. Ülke içinde birçok kritik alanlara girişte güvenliğin genetik ve biyometrik verilerle sağlandığı göz önüne alınacak olursa bu maddenin hayata tez zamanda geçirilmesinin elzem olduğu da görülmektedir.

* (Madde 3): *" Kamu kurum ve kuruluşlarına ait veriler, kurumların kendi özel sistemleri ya da kurum kontrolündeki yerli hizmet sağlayıcılar hariç bulut depolama hizmetlerinde saklanmayacaktır."* Ülkemizde henüz yerli bulut depolama

[37] RG. 06.07.2019, S. 30823.

hizmeti verilmediği için bu madde ile kurum verilerinin yabancı menşeli bulut sağlayıcılarında tutulması engellenmiş olacaktır.

* (Madde 17): *"Milli güvenliği doğrudan etkileyen stratejik öneme haiz kurum ve kuruluşların üst yöneticileri ile kritik altyapı, tesis ve projelerde görev alacak… personellerin güvenlik ve arşiv araştırması yapılacaktır."* Ülkemizin son dönemde yaşadığı olağanüstü olaylardan, özellikle de 15 Temmuz 2016'da yaşanan darbe girişiminden sonra kritik yerlerde çalışan insanların güvenilirliği daha da önemli bir hale gelmiştir. Öyle ki kritik yerlerdeki bir kişi ülkenin kaderini etkileyebilecek birtakım hamleler yapabilmektedir. Dolayısıyla söz konusu maddenin hayata geçirilmesi çok önemlidir.

Yine bu genelge ile, Cumhurbaşkanlığı Dönüşüm Ofisi'nin koordinasyonu ve kamu kurum ve kuruluşlarının katkısı ile "Bilgi ve İletişim Güvenliği Rehberi" oluşturulması hedeflenmiştir. Bu rehber ile kamu kurum ve kuruluşları ile kritik öneme haiz işletmelerin uyması zorunlu kurallar getirilmesi hedeflenmekte ve kurulacak denetim mekanizması ile her sene en az 1 kere denetlenmesi amaçlanmaktadır. Söz konusu bu rehber söylemden ibaret kalmayıp hayata geçirildiği takdirde olumlu sonuçlar verecektir.

Yapılan bu çalışmalar ve düzenlemeler ile kritik altyapı tanımlamaları ve bu alanın siber güvenliğine yönelik birtakım düzenlemeler hayata geçirilmiştir. Ulusal Siber Güvenlik Stratejisi ve Eylem Planları ile birlikte artık ülkemiz için hangi sektörlerin kritik altyapı niteliğinde olduğu belirlenmiştir. Yine bu eylem planlarıyla birlikte siber alandaki mevzuat çalışmaları derinleşmiş ve siber güvenlik tatbikatlarından bahsedilmiştir.

Ülkemizde yapılan siber güvenlik tatbikatları ilk başlarda doğrudan kritik altyapılarla ilişkilendirilerek yapılmasa da 2011 yılında yapılan Ulusal Siber Güvenlik Tatbikatı ile birlikte doğrudan kritik altyapı sayılacak sektörleri içinde bulunduran tatbikatlar yapılmaya başlanmıştır. Yine, TSK Siber Savunma Komutanlığı'nın kurulması ve TÜBİTAK Siber Güvenlik

Enstitüsü'nün kurulması ile birlikte kritik alanlardaki siber savunma mekanizması güçlendirilmiştir.

SOME'lerin kurulmasıyla birlikte, kritik altyapılara yönelik yapılan siber saldırılara karşı USOM çatısı altında daha güçlü bir merkezi otorite oluşturulmaya çalışılmıştır. Kritik altyapı sektöründe de kurulan SOME'lerin birbirleriyle iletişimi artırılarak olası siber saldırılara karşı ortaklaşa önlem alınması amaçlanmıştır.

AFAD tarafından yayınlanan; 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi ile Türkiye'nin uzun vadede ulaşması gereken hedefler belirlenmiştir.[38] 2014 yılında Türkiye, Sanal Ortamda İşlenen Suçlar Sözleşmesi'ni (Budapeşte Sözleşmesi) imzalayarak uluslararası alandaki ilk siber anlaşmasını imzalamıştır.

B. Avrupa Çalışmaları

1. Avrupa Konseyi Siber Suç Sözleşmesi

Avrupa bilişim suçları ile mücadelede, bu alanda imzalanan ilk anlaşma olan Avrupa Konseyi Siber Suçlar Sözleşmesi'ni 23 Kasım 2001 tarihinde, Budapeşte'de imzaya açmış ve bu sözleşme 1 Temmuz 2004 tarihinde yürürlüğe girmiştir. Avrupa Konseyi'ne dâhil olmayan ülkelere de söz hakkı tanınan bu sözleşmeye bugüne kadar 46 tanesi Avrupa Konseyi üyesi olan toplamda 68 ülke sözleşmeye taraf olmuştur.[39] Sözleşme ülkemizde 10 Kasım 2010 tarihinde imzalanmış ve 2 Mayıs 2014'te yürürlüğe konmuştur. Sözleşme, Türkçe'ye "Sanal

[38] T.C. Başbakanlık Afet Acil Durum Yönetimi Başkanlığı, *2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi*, (Ankara: AFAD, 2014).

[39] İsa Başıbüyük, "Dijital Çağda Suçla Mücadele: Bir Avrupa Siber-Suç Merkezinin Kurulması," *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 15, (2013): 1585.

Ortamda İşlenen Suçlar Sözleşmesi" biçiminde çevrilmiş olup, "Avrupa Siber Suçlar Sözleşmesi" ismiyle de anılmaktadır.[40]

Sözleşmede yer alan temel amaçlara, sözleşme açıklayıcı raporunda yer verilmektedir. Buna göre, bilişim suçları ile ilgili ulusal düzeyde bulunan yasal düzenlemeler ile bağlantılı hükümlerin uyumlu hale getirilmesi, bilişim suçları ve elektronik delillerin bulunduğu diğer klasik suçların soruşturması ve takibi ile ilgili olarak ulusal yetkilerin ve düzenlemelerin sağlanması, ayrıca uluslararası anlamda oluşturulacak iş birliğinin hızlı ve etkili olmasına çalışılması sözleşmenin temel amaçları olarak ifade edilmektedir. Sözleşme bazı yönlerden eleştiriler de almıştır, ancak yine de bilişim suçları ile mücadelede ciddi bir ilerleme sağladığı da inkâr edilemez bir durumdur.[41] Sözleşmede bu tür olumlu katkıların yanında, doğrudan kritik altyapılara yönelik bir hüküm bulunmaması ise bir eksiklik olarak nitelendirilmektedir. Sözleşmede belirsiz ifadelerin bulunması da yine bir eksiklik olarak tanımlanabilir. Örnek vermek gerekirse, Sözleşme'nin 14. maddesinde geçen "diğer suçlar" ifadesi açık değildir. Düzenlemeye göre, sözleşmeye taraf olan devletler bilgisayar aracılığıyla işlenen diğer suçlara uygulanacak usullere ve yetkilere ilişkin gerekli yasal ve diğer tedbirleri alacaklardır. Bu cümlede ve daha birçok maddede geçen ve tanımlanmayan

---

40 Türkiye Büyük Millet Meclisi, *Bilgi Toplumu Olma Yolunda Bilişim Sektöründeki Gelişmeler İle İnternet Kullanımının Başta Çocuklar, Gençler ve Aile Yapısı Üzerinde Olmak Üzere Sosyal Etkilerinin Araştırılması Amacıyla Kurulan Meclis Araştırma Komisyonu Raporu*, (Ankara: TBMM, 2012), https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss381.pdf.; Cahit Aliusta ve Recep Benzer, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci," *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi* 4, no. 2: (2018): 37.

41 Mücahid Özbek, "Avrupa Siber Suçlar Sözleşmesinin Türk Ceza Hukukuna Etkileri," (2015): 87, erişim tarihi: Ocak 12, 2019, https://www.goksusafiisik.av.tr/Articletter/2015_Summer/GSI_Articletter_2015_Summer_Article6.pdf.

"diğer" kavramının netleştirilmesi ve açık bir şekilde belirtilmesi gerekmektedir.

Avrupa Birliği tarafından bu alanda kapsamlı strateji geliştirme çalışmaları da devam ettirilmektedir. Avrupa Parlamentosu, internet altyapısına yönelik siber suçlarla mücadele için, üye ülkelerin kanun çıkarması ve mevcut kanunlara ek yapması için karar almıştır.[42] Buna ek olarak, Avrupa çapında bilişim suçlarının faillerinin takibi ve bilişim suçlarının soruşturması konusunda birtakım engeller bulunmaktadır. Yargı yetkisi, istihbaratın paylaşılması konusundaki yetersizlikler, bilişim suçlularının izlerinin sürülmesi önündeki teknik engeller, uzman personel sayısının az olması, hukuki imkânların uyumsuz olması bu engeller arasındadır. Bu gibi engeller, siber saldırganlara karşı caydırıcı cezalar verilmesine engel olmakla birlikte dolaylı yoldan saldırganlara açık kapı bırakmaktadır. Bu hususlar göz önüne alınarak Avrupa Komisyonu yeni kararlar almıştır. Avrupa Birliği ülkeleri mahkemeleri üye ülkelerden elektronik mesaj ve benzeri elektronik delilleri talep edebilecek, internet servis sağlayıcılardan ilgili verileri korumasını isteyebilecektir.[43]

III. KRİTİK ALTYAPILARA YÖNELİK GERÇEKLEŞEN SİBER SALDIRI İSTATİSTİKLERİ

Siber tehditlerin daha iyi gözlemlenmesi için birtakım istatistiki çalışmalar aşağıda sunulmuştur. 2017 yılında yapılan, endüstri ve organizasyon büyüklüğüyle ilgili bilişim

---

42 "Directive 2013/40/Eu Of The European Parliament And Of The Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA," EUR-Lex, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF.

43 European Commission, "e-evidence," erişim tarihi Aralık 7, 2020, https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime/e-evidence_en.

saldırılarını incelendiğinde aşağıdaki tablodaki veriler elde edilmiştir.[44]

Tablo 2: 2017 yılı Küresel Siber Güvenlik Olay Sayısı

	Büyük	Küçük	Belirsiz	Toplam
Konaklama	40	296	32	368
İdari	7	15	11	33
Tarım	1	0	4	5
İnşaat	2	11	10	23
Eğitim	42	26	224	292
Eğlence	6	19	7.163	7.188
Maliye	74	74	450	598
Sağlık hizmeti	165	152	433	750
Bilgi	54	76	910	1.040
Yönetim	1	0	1	2
İmalat	375	21	140	536
Madencilik	3	3	20	26
Diğer servisler	5	11	46	62

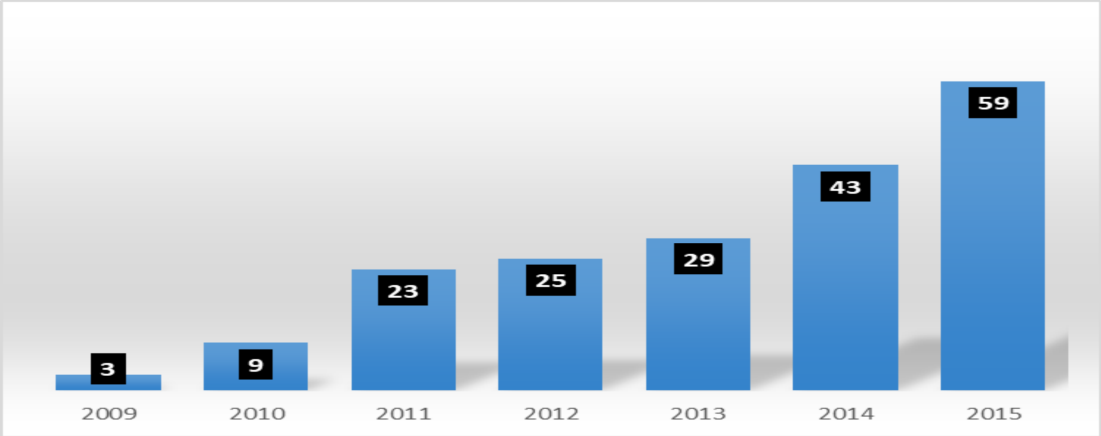
Saldırılar, konaklama sektöründe ağırlıklı olarak küçük sektörlere, imalatta ise büyük sektörlere karşı gerçekleşmiştir. Eğlence sektöründeki saldırıların ağırlığı ise büyüklük ya da küçüklük durumu belirlenemeyen sektörlere karşı yapılmıştır. Sektörler incelendiği zaman sağlık hizmeti, maliye ve bilgi teknolojileri gibi ülkeler için kritik altyapı niteliğindeki sektörlere de siber saldırılar yapıldığı ve toplam saldırı içindeki payının da yüksek olduğu gözlemlenmektedir.

Teknolojinin gelişimine paralel olarak kritik altyapı niteliğindeki bilgi teknolojileri alanına da siber saldırı sayısı

44 Statistica, "Global number of cyber security incidents in 2017, sorted by victim industry and organization size," erişim tarihi: Ekim 6, 2018, https://www.statista.com/statistics/194246/cyber-crime-incidents-victim-industry-size/.

artmıştır. Aşağıdaki grafikte 2009 yılından 2015 yılına kadarki siber saldırı sayısı ile ilgili istatistiki veri paylaşılmıştır[45]:

Grafik 1. Dünya Genelinde Bilişim Teknolojilerine Yapılan Saldırı Sayısı (Milyon)



Grafik incelendiği zaman Bilgi Teknolojileri alanında yapılan siber saldırı sayısındaki artışın teknoloji gelişimiyle paralellik gösterdiği gözlenmektedir. Bu artışa teknolojinin gelişimi kadar teknoloji kullanımının yaygınlaşması da etki etmektedir. Yaygınlaşmak, beraberinde tedbirsizliği de getirmektedir. Bu durum saldırganlar için bir fırsat niteliğinde sayılmaktadır. Nihayetinde grafikteki artış da bu durumun sonucunu ortaya koymaktadır.

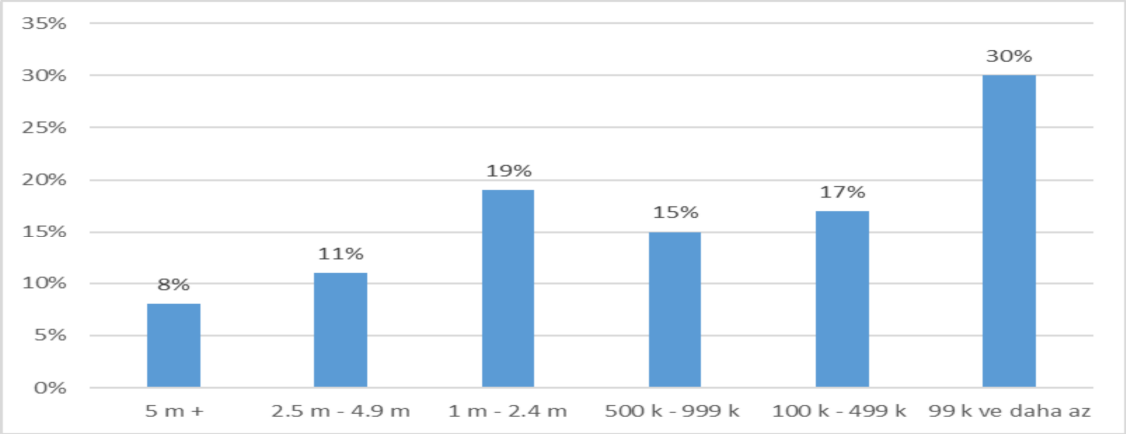
Nisan 2018'de yapılan istatistiki bir çalışmaya göre dünya çapındaki işletmelere yapılan siber saldırıların maliyetleri aşağıdaki gibi belirlenmiştir.[46]

---

45 Statistica, "Global number of cyber security incidents from 2009 to 2015," erişim tarihi: Şubat 16, 2019, https://www.statista.com/statistics/387857/number-cyber-security-incidents-worldwide/.

46 Statistica, "Average financial damages of cyber attacks caused to businesses worldwide as of 2018 (in U.S. dollars)," erişim tarihi: Şubat 19, 2019, https://www.statista.com/statistics/881158/average-financial-damages-via-cyber-attacks/.

Grafik 2. Siber Saldırıların Dünya Çapındaki İşletmelere Ortalama Finansal Zararı



Grafik incelendiği zaman, dünya çapında işlem gören işletmelere yönelik siber saldırıların %8'i 5 milyon doların üzerinde, %19'u 1 ilâ 2.4 milyon dolar arasında ve %30'unun ise 100 bin doların altında zarara sebep olduğu gözlenmektedir.

Bu grafiklerden görüldüğü üzere siber saldırılar ve bunun sonucunda ortaya çıkan zararlar eksponansiyel bir artış göstermektedir. Kritik altyapılara yönelik saldırılar ise sadece maddi zararlara değil toplum üzerinde psikolojik yıpranmaya da yol açabilecektir.

SONUÇ

Ülkemizde son yıllarda siber alanla ilgili birçok düzenleme, seminer ve çalıştay yapılmaktadır. Bu çalışmalar sonucunda bazı kararlar alınarak eksiklikler tespit edilmeye çalışılmıştır. Eksiklikler tespit edilmeye başlandığı halde gerek bürokratik engeller gerekse başka durumlardan ötürü yeterli düzeyde kanuni düzenlemeler yapılmamış ve yeterli önlemler alınmadığı tespit edilmiştir. Bu alanla ilgili düzenleme yalnızca 5237 sayılı TCK'nın 243-246. maddeleri ile genel çerçeveleri çizilerek belirtilmiştir. Bu maddelerin siber suçlara yönelik değil de doğrudan işlenen suçların bilişim alanına yansıması şeklinde düşünülerek hazırlanması bu alandaki ihtiyaca yeterince cevap verememektedir.

Bilişim suçları alanında TCK'da birçok yenilik yapılmış ve bu suçlar da çeşitli yaptırımlarla büyük oranda kontrol altına alınmıştır. Yeni Türk Ceza Kanunu aynı zamanda Avrupa Konseyi Siber Suçlar Sözleşmesi ile de büyük oranda uyum içinde geçerliliğini sürdürmektedir.

Belirtmek gerekir ki, bilişim alanında önlemler almış olsa da ne yazık ki ülkemizde henüz kritik altyapıları doğrudan ilgilendiren bir hukuki düzenleme yoktur. Kritik altyapılar için belirlenmiş strateji planı da henüz yoktur. Kanunlarımız siber saldırıların bireysel düzeyiyle ceza hukuku bazında ilgilenmiştir. Kurumları doğrudan ilgilendiren bir siber güvenlik yasası yoktur ve ihtiyaç duyulmaktadır. Bu yasa birtakım zorunluluklar getirmelidir. Kritik altyapıların herhangi birine yapılan siber saldırı hakkında diğer kritik altyapı işletmelerinin bilgilendirilmesi zorunlu hale getirilmelidir. Yasa kapsamında oluşturulan maddeler açık ve kesin olmalıdır. Kritik altyapılara yönelik siber saldırılar milyonlarca kişinin hayatını olumsuz yönde etkileyebilir hatta milli güvenliği tehlikeye düşürebilir. Bundan dolayı, kritik altyapılara yönelik saldırılara verilecek cezalar caydırıcı olmalıdır. Maddeler evrensel nitelikte lakin ülke menfaati ön planda tutulacak şekilde oluşturulmalı ve sürekli güncellenmelidir.

Ülkemizde eksikliği hissedilen durumlardan biri de ulusal bazda çıkarılan siber güvenlik strateji belgelerinin içinde belirtilen hususların çerçeve bir şekilde düzenlenmesidir. Örneğin, *2016- 2019 Ulusal Siber Güvenlik Strateji Belgesi* içinde belirlenen amaç ve eylemler başlığı altındaki 2. maddede belirtilen; *"Siber güvenlik alanında denetim yaklaşımını da içeren uluslararası standartlara uygun mevzuatın oluşturulması"* gerekliliği belirtilmiştir. Bu maddenin varlığına rağmen henüz böyle bir mevzuat oluşturulmamıştır. Belirlenen hedefler uygulamaya geçtiği takdirde ülkemiz açısından çok güvenli ve faydalı bir dijital alan oluşacaktır.

Her ne kadar bugün yaptırımlar ya da cezai hükümlerle ilgili birçok eleştiri ve eksik yön bulunuyor olsa da bu alanda

yapılan çalışmaların değişen dünya düzenine uyum sağlanması bakımından devam ettirildiği bilinmektedir. Bilişim suçlarına yönelik ceza hükümleri üzerinde gerekli olması halinde gerek ülke çapında gerekse Avrupa genelinde düzenlemeler ve kanunlarda yeniliklerin yapılacağı yahut yapılması gerektiği öngörülmektedir.

KAYNAKÇA

Ak, Tarık. "İç Güvenlik Yönetimi Açısından Kritik Altyapıların Korunması." *ASSAM Uluslararası Hakemli Dergi*, no. 1 (2019): 42-51.

Aliusta, Cahit ve Benzer, Recep. "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci." *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi* 4, no.2 (2018): 35-42.

Altunok, Ebru ve Vural, Ali Fatih. "Bilişim Suçları." *Denetişim*, no.8 (2016): 74-84.

Ang, Chee Kiong Gary ve Nugroho, Utomo. "Cyber Security in the Energy World." İç. *2017 Asian Conference on Energy, Power and Transportation Electrification (ACEPT)*. (Singapore: ACEPT, 2017):1-5. https://doi.org/10.1109/ACEPT.2017.8168583.

Apiş, Özge. "Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama." *Yasama Dergisi*, no.37 (2018): 49-86.

Avallone, Stefano, Carrozza, Gabriella, Cinque, Marcello, Della Corte, Raffaele, Marotta, Antonio, Pecchia, Antonio ve Savignano, Agostino. "Napoli Futura: Novel Approaches for Protecting Critical Infrastructures from Cyber Attacks." *2014 IEEE International Symposium on Software Reliability Engineering Workshops*. (Naples: IEEE, 2014): 33-36. https://doi.org/10.1109/ISSREW.2014.53.

Aydın, Emin. "Bilişim Sistemlerinde Güvenlik, Güvenirlilik Mahremiyet ve Bilişim Suçları." *Marmara İletişim Dergisi* 1, no. 1 (1992): 109-138.

Başıbüyük, İsa. "Dijital Çağda Suçla Mücadele: Bir Avrupa Siber-Suç Merkezinin Kurulması." *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 15, (2013): 1583-1594.

Bozdoğan Akbulut, Berrin. "Bilişim Suçları." *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 8, no. 1-2 (2000): 545-550.

Ciancamerla, Ester, Minichino, Michele ve Palmieri, Silvia. "Modeling cyber attacks on a critical infrastructure

scenario." *IISA 2013*. (Piraeus: IEEE, 2013): 1-6. https://doi.org/10.1109/IISA.2013.6623699.

Curran, Kevin, Concannon, Kevin ve McKeever, Sean. "Cyber Terrorism Attacks." İç. *Cyber Warfare and Cyber Terrorism*. ed. Lech J. Janczewski ve Andrew M. Colarik. (Hershey, PA: IGI Global, 2008): 1-6. http://doi:10.4018/978-1-59140-991-5.ch001.

Çiftçi, Hasan. *Her Yönüyle Siber Savaş*. Ankara: TÜBİTAK, 2017.

Erdağ, Ali İhsan. "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)." *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi* 14, no. 2 (2010): 275-303.

Erdoğan, Yavuz. "Bilişim Sistemine Girme ve Kalma Suçu." *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 12, (2010): 1363-1433.

EUR-Lex. "Directive 2013/40/Eu Of The European Parliament And Of The Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA." https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF.

EUR-Lex. "European Programme for Critical Infrastructure Protection-Summaries of EU Legislation." Erişim Tarihi: Aralık 26, 2018. http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm#KeyTerms.

European Commission. "e-evidence." Erişim Tarihi: Aralık 7, 2020. https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime/e-evidence_en.

Geers, Kenneth. "The Cyber Threat to National Critical Infrastructures: Beyond Theory." *Information Security Journal: A Global Perspective*, no. 18 (2009): 1-7.

Göçoğlu, Volkan. "Cyber Security of Critical Infrastructures in Smart Cities." *Uluslararası Yönetim Akademisi Dergisi* 2, no.1 (2019): 51-63.

Karagülmez, Ali. *Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri*. Ankara: Seçkin Yayıncılık, 2005.

Kovacevic, Ana ve Nikolic, Dragana. "Cyber Attacks on Critical Infrastructure: Review and Challenges." İç. *Handbook of Research on Digital Crime, Cyberspace Security and Information Assurance*. ed. Maria Manuela Cruz-Cunha ve Irene Maria Portela. (Hershey, PA: IGI Global, 2015): 1-18. http://doi:10.4018/978-1-4666-6324-4.ch001.

Kozik, Rafal ve Choraś, Michal. "Current cyber security threats and challenges in critical infrastructures protection." *2013 Second International Conference on Informatics & Applications*. (Lodz: IEEE, 2013): 93-97. https://doi.org/10.1109/ICoIA.2013.6650236.

Noguchi, Mutsuo ve Ueda, Hirofumi. "An Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures." *Nec Technical Journal* 12, no. 2 (2017): 19-24. Erişim Tarihi: Kasım 16, 2020, https://www.nec.com/en/global/techrep/journal/g17/n02/pdf/170204.pdf.

Özbek, Mücahid. "Avrupa Siber Suçlar Sözleşmesinin Türk Ceza Hukukuna Etkileri," (2015): 73-88. Erişim Tarihi: Ocak 12, 2019. https://www.goksusafiisik.av.tr/Articletter/2015_Summer/GSI_Articletter_2015_Summer_Article6.pdf.

Özsoy, Nevzat. "Yargıtay Kararları Işığında Doğrudan Bilişim Suçları." *Yaşar Hukuk Dergisi* 1, no. 2 (2019): 295-352.

Statistica. "Average financial damages of cyber attacks caused to businesses worldwide as of 2018 (in U.S. dollars)." Erişim Tarihi: Şubat 19, 2019,

https://www.statista.com/statistics/881158/average-financial-damages-via-cyber-attacks/.

Statistica. "Global number of cyber security incidents from 2009 to 2015." Erişim Tarihi: Şubat 16, 2019. https://www.statista.com/statistics/387857/number-cyber-security-incidents-worldwide/.

Statistica. "Global number of cyber security incidents in 2017, sorted by victim industry and organization size." Erişim Tarihi: Ekim 6, 2018. https://www.statista.com/statistics/194246/cyber-crime-incidents-victim-industry-size/.

Taylor, James M. ve Sharif, Hamid R. "Security challenges and methods for protecting critical infrastructure cyber-physical systems." *2017 International Conference on Selected Topics in Mobile and Wireless Networking*. (Avignon: IEEE, 2017): 1-6. https://doi.org/10.1109/MoWNet.2017.8045959.

T.C. Başbakanlık Afet Acil Durum Yönetimi Başkanlığı. *2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi*. Ankara: AFAD, 2014.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. *2016-2019 Ulusal Siber Güvenlik Stratejisi*. Ankara: T.C. UDHB, 2019. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf.

The Cybersecurity and Infrastructure Security Agency. "National Infrastructure Advisory Council Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure Final Report." Erişim Tarihi: Aralık 6, 2020. https://www.cisa.gov/publication/niac-securing-cyber-assets-addressing-urgent-cyber-threats-critical-infrastructure-final.

The White House. "Presidential Policy Directive." Erişim Tarihi: Aralık 2, 2018. https://obamawhitehouse.archives.gov/the-

press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resilience.

Turan, Metin ve Külcü, Özgür. "Türkiye'de Bilişim Suçlarının Tanımlanması ve Yaşanan İhlallere Yönelik İçerik Analizi." *Türk Kütüphaneciliği* 28, no. 1 (2014): 18-46.

Türkiye Büyük Millet Meclisi, *Bilgi Toplumu Olma Yolunda Bilişim Sektöründeki Gelişmeler İle İnternet Kullanımının Başta Çocuklar, Gençler ve Aile Yapısı Üzerinde Olmak Üzere Sosyal Etkilerinin Araştırılması Amacıyla Kurulan Meclis Araştırma Komisyonu Raporu*. Ankara: TBMM, 2012. https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss381.pdf.

Von Solms, Sebastiaan. "Critical information infrastructure protection: How comprehensive should it be?." *2013 International Conference on Adaptive Science and Technology*. (Pretoria: IEEE, 2013): 1-5. https://doi.org/10.1109/ICASTech.2013.6707516.

Yeşil, Osman, Irmak, Erdal ve Bülbül, Halil İbrahim. "Kritik Altyapı Operatörleri İçin Görüntü İşleme Tabanlı Bir Yorgunluk Tespit ve Uyarı Sistemi." *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi* 6, no.1 (2020): 35-44.

Yılmaz, Ercan, Gönen, Serkan ve Ulus, Halil İbrahim. "Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme." *Bilişim Teknolojileri Dergisi* 9, no. 3 (2016): 229-236.

Yunos, Zahri, Ahmad, Rabiah, Suid, Syahrul Hafidz ve Ismail, Zuraini. "Safeguarding Malaysia's critical national information infrastructure (CNII) against cyber terrorism: Towards development of a policy framework." *2010 Sixth International Conference on Information Assurance and Security*. (Atlanta, GA: IEEE, 2010): 21-27. https://doi.org/10.1109/ISIAS.2010.5604182.