BÖLÜM
18

ÜLKEMİZDE SİBER GÜVENLİK, SİBER SUÇLAR VE ADLİ YÖNÜ

Abdullah GENÇAY [1]
Nergis CANTÜRK [2]

GİRİŞ

Uluslararası Telekomünikasyon Birliği verilerine göre 2022 yılı itibariyle 8 milyar insanın yaşadığı dünyamızda, interneti insanların yaklaşık %66'sı (5.3 milyar insan) kullanmaktadır. 2015 yılında yapılan tahminlere göre 2025 yılında internet kullanıcısı sayısının 4 milyarı geçeceği öngörülmüş olsa da, henüz 2022 yılında 5.3 milyara kullanıcıya ulaşılmış olması internet dünyasının genişleme hızının tahminlerin ötesinde gerçekleştiğini göstermektedir (1, 2).

Bu oran Avrupa, Bağımsız Devletler Topluluğu (BDT[3]) ve Amerika'da nüfusun %80-%90'ına yükselmektedir. Ayrıca statista verilerine göre 2021 yılı itibariyle 11.28 milyar cihaz internete bağlı durumdadır. İnternete bağlı cihazlara bilgisayarlar, cep telefonları, tabletler, kol saatleri, beyaz eşyalar, güvenlik sistemleri, araçlar, kapı zilleri, endüstriyel robotlar, aydınlatma sistemleri, endüstriyel izleme sistemleri, ısıtıcılar, araçlar gibi birçok örnek verilebilmekte ve bu cihaz çeşitliliği gün geçtikçe artmaktadır.

Çok sayıda cihaz ve kişinin bağlı olduğu İnternet Platformunun yönetimi, kuralları, gizliliği, içerik önerim yapıları, suçlu takibine olanak sağlaması gibi tartışılagelen önemli ve hayatımızı etkileyen birçok yönü bulunmaktadır. Bu platformu kullanım

[1] Doktora Öğrencisi, Ankara Üniversitesi, Emniyet Genel M. abdullahgencay@gmail.com

[2] Prof. Dr., Ankara Üniversitesi Adli Bilimler Enstitüsü, nergiscanturk@yahoo.com

[3] BDT: 1991 yılında Sovyetler Birliği'nin dağılmasından sonra aynı yılın aralık ayında kurulan Bağımsız Devletler Topluluğu; Rusya, Ukrayna(2014te ayrıldı), Belarus, Azerbaycan, Ermenistan, Kazakistan, Kırgızistan, Moldova, Özbekistan, Tacikistan, Gürcistan(2009ta ayrıldı), Türkmenistan(2005te ayrıldı)'ın dahil olduğu birliğe verilen isimdir. Bugün itibariyle 9 üyesi bulunmaktadır.

kemiz ekonomisine destek sağladığı değerlendirilmektedir.

KAYNAKLAR

1. Yılmaz E, Halil U, Gönen S. Bilgi toplumuna geçiş ve siber güvenlik. Bilişim Teknolojileri Dergisi. 2015;8(3):133.
2. ITU. Facts and Figures. Geneva-Switerland: International Telecommunication Union; 2022 2022.
3. Bakanlığı UvA. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023. In: Kurulu SG, editor. Ankara: Siber Güvenlik Kurulu; 2020.
4. INTERPOL. Global Crime Trend Summary Report. France: INTERPOL General Secretariat; 2022.
5. Bakanlığı A. Adalet İstatistikleri 2021-2009. In: Müdürlüğü ASvİG, editor. Ankara: Adalet Bakanlığı; 2022.
6. Canada S. Police-reported cybercrime, . Canada: Statistics Canada; 2022.
7. Falliere N, Murchu LO, Chien E. W32. stuxnet dossier. White paper, symantec corp, security response. 2011;5(6):29.
8. Albright D, Brannan P, Walrond C. Did Stuxnet take out 1,000 centrifuges at the Natanz enrichment plant?: Institute for Science and International Security; 2010.
9. Military and Associated Terms. Washington DC2021. DOD Dictionary of Military and Associated Terms.
10. Çifci H. Her Yönüyle Siber Savaş (Birinci Baskı). Ankara: TUBİTAK Popüler Bilim Kitapları. 2013:3-184.
11. Janczewski L, Colarik A. Cyber warfare and cyber terrorism: IGI Global; 2007.
12. Clarke RA, Knake RK. Cyber war: Tantor Media, Incorporated Old Saybrook; 2014.
13. Jeffrey C. Mapping the Cyber Underworld–Inside Cyber Warfare. California: O'Reilly Media; 2011.
14. Lewis JA. Assessing the risks of cyber terrorism, cyber war and other cyber threats: Center for Strategic & International Studies Washington, DC; 2002.
15. AltyapıBakanlığı Uv. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı2020-2023. In: Kurulu SG, editor. Ankara: Siber Güvenlik Kurulu; 2020.
16. Goodman MD, Brenner SW. The emerging consensus on criminal conduct in cyberspace. International journal of law and information technology. 2002;10(2):139-223.
17. Moitra S. Developing policies for cybercrime. European Journal of Crime, Criminal Law and Criminal Justice. 2005;13(3):435-64.
18. Gazet A. Comparative analysis of various ransomware virii. Journal in computer virology. 2010;6:77-90.
19. Stallings W, Brown L, Bauer MD, Howard M. Computer security: principles and practice: Pearson Upper Saddle River; 2012.
20. Çakmak H, Altunok T. Suç, terör ve savaşüçgeninde siber dünya. Barış Platin Kitabevi, Ankara. 2009.
21. Fortinet. Type of Cyber Attacks 2023 [Available from: https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks.
22. Milliyet. THY 6 saatte 400 bin lira zarar etti 2012 [
23. Kurulu B. Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna-İlişkin Karar. Ankara: Bakanlar Kurulu; 2012.
24. Bakanlığı UvA. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. In: Kurulu SG, editor. Ankara: Siber Güvenlik Kurulu; 2013.

25. Çakır H, Uzun SA. Türkiye'nin Siber Güvenlik Eylem Planlarının Değerlendirilmesi. Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi. 2021;7(2):353-79.
26. USOM. Online Zararlı Bağlantı Veritabanı 2023 [Available from: https://www.usom.gov.tr/adres.
27. USOM. Siber Güvenlik Olayı Bildirim Veritabanı 2023 [Available from: https://www.usom.gov.tr/bildirim.
28. HaberTürk. Ulusal Siber Kalkan 2022 Tatbikatı" için düğmeye basıldı 2022 [Available from: https://www.haberturk.com/ulusal-siber-kalkan-tatbikati-icin-dugmeye-basildi-3528628-teknoloji?page=2.
29. Bakanlığı UvA. Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı. Ankara: Siber Güvenlik Kurulu; 2016.
30. Kurulu SG. Siber KümeÜyeleri Veritabanı Ankara2023 [Available from: https://www.siberkume.org.tr/Members.
31. Kurulu SG. Siber Küme Ürün ve Hizmet Veritabanı Ankara2023 [Available from: https://siberkume.org.tr/Katalog.
32. Cumhurbaşkanlığı. Bilgi ve İletişim Güvenliği Denetim Rehberi. Ankara: Türkiye Cumhuriyeti Cumhurbaşkanlığı; 2021.
33. SağlayıcılarıBirliği E. Erişim SağlayıcılarıBirliği Web Sitesi 2023 [Available from: https://www.esb.org.tr/.
34. TBMM. Türk Ceza Kanunu. Ankara: TBMM; 2004.