YENİ NESİL GADDARE
Teknoloji ve Güvenlik İlişkisi

Doç. Dr. Cenay BABAOĞLU
Selçuk Üniversitesi

Toplumsal bir ihtiyaç olarak güvenlik her daim insanların öncelikli sorun alanlarından birisi olmuştur. İnsanların birlikte hareket etmesinden, kentlerin kuruluşuna kadar güvenlik gereksinimi temel güdüleyicilerden birisidir. Öte yandan insanlığın ilerlemesindeki temel etkenlerden birisi olan teknik/teknoloji de genellikle güvenlik gerekçeleriyle türetilmiştir. Bu açıdan güvenlik ve teknoloji ilişkisi, üzerinde durulması gereken başlıklardan birisidir.

Teknik/teknolojik gelişmeler insanlık tarihi boyunca değişimi tetiklemiştir. Sabanın keşfi tarımı, pusulanın keşfi ticareti, barutun keşfi askeri hareketleri değiştirmiştir. Sanayi devrimi ise yeni bir çağa geçişi işaret eder. Tüm dünyada toplumsal yaşamlar değişmiş, ülkelerin rekabeti yeni boyutlar kazanmıştır. 1980'lerde yayılmaya başlayan bilgi ve iletişim teknolojileri de günümüzde toplumların yeni üretim, iletişim, yönetim ve yaşam biçimlerine sahip olmasının aracı olmuştur. Başlangıçta askeri faaliyetlerin bir

Güvenlik teması yeni teknolojilerden ve uygulamalardan iki yönlü olarak etkilenen alanlardandır. Bir yandan teknolojilerin getirileriyle birlikte daha gelişmiş teknolojik denetim mekanizmaları kurulabilmekte, diğer taraftan yeni güvenlik riskleri ortaya çıkmaktadır.

ürünü olan ağ teknolojileri, 1990'lı yıllardan itibaren sivil alanlara doğru hızla yayılım göstermiştir.

Bu yayılımlar değişimleri ve dönüşümleri de tetiklemektedir. Her bir yeni teknolojinin olumlu kullanımları ve riskleri bulunmaktadır. Günümüzde yapay zekâ, bulut bilişim, büyük veri, blokzincir, nesnelerin interneti, otonom araçlar, robotik teknolojiler, arttırılmış gerçeklik yeni başlıklar halinde gündelik hayatı ve yönetim pratiklerini değiştirmektedir. Her bir yeni teknoloji bir veya daha fazla alanda yönetime dair katkılar sunarken, diğer taraftan yeni sorun alanlarına neden olmaktadır.

Güvenlik teması da yeni teknolojilerden ve uygulamalardan iki yönlü olarak etkilenen alanlardandır. Bir yandan teknolojilerin getirileriyle birlikte daha gelişmiş teknolojik denetim mekanizmaları kurulabilmekte, diğer taraftan yeni güvenlik riskleri ortaya çıkmaktadır. Örneğin pek çok ülkede yaygınlaşan kapalı devre kamera sistemleri (KDKS/CCTV), toplumsal güvenliğin sağlanmasında, önleyici faaliyetlerde, tespit süreçlerinde, takip süreçlerinde önemli kazanımlar sağlamaktadır. Diğer taraftan bu kameraların topladığı verilerin terörist gruplarca ele geçirilmesi ya da düşmancıl amaçlarla kullanılması büyük zararlar doğurabilecek bir tehlikeyi barındırmaktadır. Dolayısıyla güvenlik – teknoloji ilişkisinde iki boyut öne çıkmaktadır. Birinci boyut, teknolojinin güvenliğin farklı boyutlarında kullanılması ve kamu güvenliğinin sağlanmasında bir araç olarak teknolojilerden faydalanılmasıdır. İkinci boyut ise yeni teknolojilerden doğan güvenlik risklerinin asgarileştirilmesi ve teknolojinin güvenliğinin sağlanmasıdır.

BİRİNCİ BOYUT: GÜVENLİĞİN SAĞLANMASINDA TEKNOLOJİ

Tarihin hemen her döneminde pek çok teknoloji, güvenlik gerekçeleriyle ya da askeri amaçlarla geliştirilmektedir. İnternetin atası kabul edilen ARPA.net dahi, konuya vakıf pek çok kişiye malum olduğu üzere Amerika Birleşik Devletleri (ABD), Savunma Bakanlığı tarafından geliştirilmiştir. Yapay zekâ, otonom araçlar, büyük veri, robotik teknolojiler, arttırılmış gerçeklik gibi uygulamalar da halihazırda askeri veya iç güvenlik amaçlarıyla kullanılmaktadır.[1]

Örneğin ABD/Boston'da kurulan veri analiz sistemiyle, şehirdeki asayiş sorunlarına gerçek zamanlı analiz ve hızlı müdahale imkânı getirilmiştir. Bu sistem sayesinde şehirdeki şiddet suçlarında %17, gasp suçlarında %19'luk bir düşüş sağlanmıştır. Söz konusu başarı dolayısıyla, New York Polis Teşkilatı da benzer bir sistem kurmuş ve beş yıl içerisinde hırsızlık ve cinayet suçları yarı yarıya düşüş göstermiştir. Benzer bir modelin kurulduğu Kolombiya/Bogota'da KDKS/CCTV üzerinden toplanan veriler, risk modellemeleri yoluyla analiz edilerek kentsel güvenlik sağlanmaya çalışılmaktadır (Rodríguez, Palomino ve Mondaca, 2017: 8-9). Bir tür veri toplama ve analiz sistemi haline gelen bu kamera sistemlerinin; kentsel güvenliğin sağlanmasında, güvenlik personeli ihtiyacının tespitinde, suçluların profilinin çıkartılmasında, güvenlik ihtiyacına dair dönemsel farklılıkların analizinde kullanılması mümkündür (Babaoğlu ve Çobanoğlu, 2019). Bu tarz bir sistem yoluyla Pakistan/Pencap'ta kurulan Pencap Güvenlik İdaresi tüm şehri gözetim altına almış, başarılı uygulamalar dolayısıyla uygulama Lahor, İslamabad gibi şehirlerde de yaygınlaştırılmıştır (Khan, 2018). Yine Pakistan'da kullanılan bir sistemde bu veriler analiz edilerek yangınlara karşı bir erken uyarı sistemi geliştirilmiş ve %90'ın üzerinde bir başarı gösterilmiştir. Bu erken yangın uyarı sistemi aynı zamanda New York İtfaiye İdaresi tarafından da kullanılmaktadır (Athey, 2017; Yu, Yang ve Li, 2018).

Aslında bu çalışmalar bir tür büyük veri analizidir. Farklı kaynaklardan elde edilen verilerin işlenmesi yoluyla güvenlik politikalarında başarı oranı arttırılmaktadır. Bu yöntem yalnızca yerel uygulamalarda değil, ulusal güvenlik gerekçesiyle de kullanılabilmektedir. Örneğin ABD'nin

1 Teknolojinin askeri gerekçelerle gelişmesi ve yönetimde kullanılmasına dair ayrıntılı bir araştırma için: Mete Yıldız, Uğur Sadioğlu ve Cenay Babaoğlu, "Adoption of communication technologies during the last century of the Ottoman Empire: 1823-1923"", 32nd EGPA Annual Conference, (Toulouse EGPA & IIAS), 2010; Mete Yıldız, Uğur Sadioğlu ve Cenay Babaoğlu, "Yönetsel tarih perspektifinden kamu yönetiminde teknoloji kullanımı: Osmanlı İmparatorluğu'nda ulaştırma teknolojileri kullanımı örneği (1823-1923)", iç. E-Devlet, (Edt: Mehmet Zahid Sobacı ve Mete Yıldız), (Ankara: Nobel, 2012), s: 65-85.

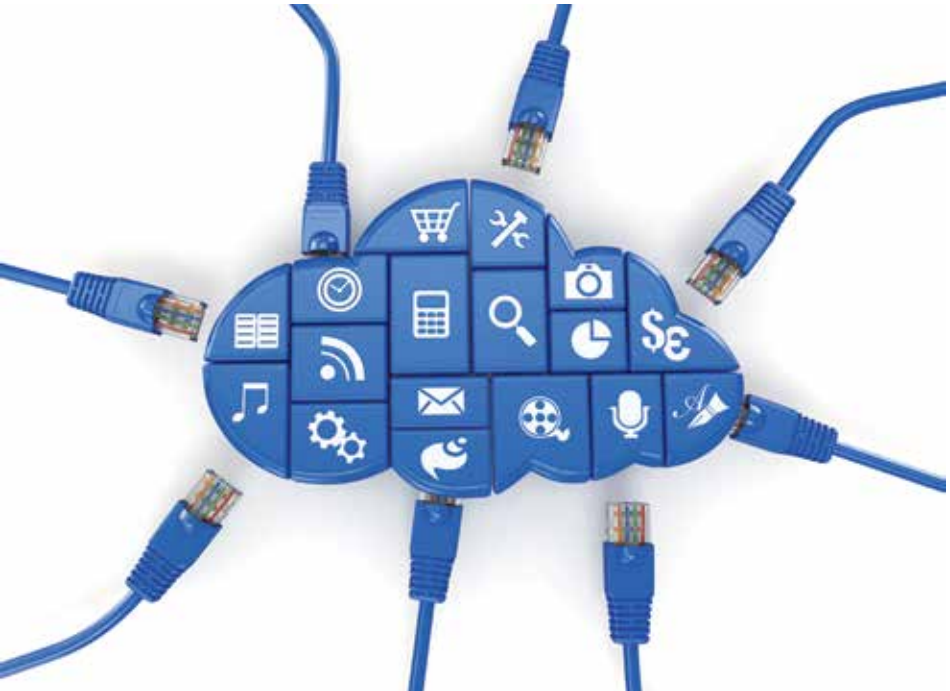
güvenlik teşkilatları NSA ve CIA tarafından da desteklenen Palantir isimli büyük veri analiz şirket; Usame bin Ladin'in yakalanması ve Sudan'daki iç savaşa müdahale edilmesi gibi olaylarda kullanılmıştır.

Mobil uygulamalar, sosyal medya platformları, uydu verileri, web site çerez analizleri, kamera kayıtları, sensörler, insansız hava araçlarının topladığı veriler gibi pek çok kaynaktan toplanan veriler işlenerek büyük veri analizleri yoluyla güvenlik stratejileri oluşturulabilmektedir. Büyük veri dışında da pek çok teknoloji askeri gerekçelerle kullanılmaktadır. Robotik teknolojiler, riskli bölgelerdeki müdahaleler için, arttırılmış gerçeklik uygulamaları askeri eğitimlerde kullanılmaktadır. Yapay zekâ yoluyla alternatif güvenlik modellemeleri ya da savaş stratejileri geliştirilmektedir. Öte yandan bu yeni teknolojiler aynı zamanda yeni güvenlik açıkları da doğurmaktadır. Teknoloji ve güvenlik ilişkisinin ikinci boyutu, teknolojinin güvenliği meseledir.

İKİNCİ BOYUT: TEKNOLOJİNİN GÜVENLİĞİ

Teknolojiyle birlikte doğan en önemli güvenlik risklerinden biri, teknolojilerin güvenliğinin sağlanmasıdır. Özellikle de elde edilen verilerin korunması ve başka gruplarca kullanılmasının önüne geçilmesidir. Yakın zamanda yemek servisi sağlayan özel bir firmada, sosyal medya ağlarında, bir belediyenin veri tabanında veri güvenliğiyle ilgili sorunlar yaşanmıştır. Kurum ve kuruluşlardaki bu güvenlik açıklarından elde edilen veriler, sonrasında karanlık internet ortamında satışa çıkarılmıştır. Sıralanan hususlar tekil örnekler değildir. Örneğin 2015 yılında ABD'de milyonlarca vatandaşın sağlık verileri bilgisayar korsanları tarafından ele geçirilmiş ve satışa konu edilmiştir (Whittaker, 2016). IBM tarafından yapılan bir araştırmaya göre veri ihlalleri nedeniyle kurumlar her yıl milyonlarca dolar zarara uğramaktadır (İBM, 2019).

Verilerin korunması noktasında da bazı uygulamalar ve teknolojiler öne çıkmaktadır. Teknolojinin teknoloji eliyle korunmasında blokzincir öne çıkan araçlardandır. Blokzincir teknolojisi bir tür güvenlik protokolü sağlayıcısıdır. Adını söz konusu protokolü birbirleriyle bağlı ve tümleşik işlem yapabilen bloklardan oluşmasından almaktadır. Örneğin araç sicilleri, kaza, bakım kayıtları gibi bilgiler bu blokzincirler aracılığıyla tutulabilmektedir.



Teknolojiyle birlikte doğan en önemli güvenlik risklerinden biri, teknolojilerin güvenliğinin sağlanmasıdır. Özellikle de elde edilen verilerin korunması ve başka gruplarca kullanılmasının önüne geçilmesidir.

Bu şekilde oto hırsızlığının önlenmesi ya da azaltılması mümkündür. ABD'de sınır güvenliğinde kimlik kontrollerinin sağlanması gayesiyle blokzincir temelli bir sistem geliştirilmiştir. Güney Kore de sınır güvenliği ve gümrük kontrolleri için benzer bir modeli uygulamaya geçirmiştir (Tüfekçi ve Karahan, 2019; US DHS, 2016). Bu şekilde veriler güvenli şekilde işlenirken hem vatandaş hem devlet alanları güvenceye almaktadır.

Teknolojilerin korunmasında bir diğer boyut teknoloji geliştiricilerin kaynağı, amacı ve yönelimidir. Örneğin yukarıda ifade edilen Güney Kore örneğinde Samsung firmasından destek alınmıştır. Öte yandan Avustralya ve ABD gibi ülkelerde uygun olmayan veri protokolleri nedeniyle beşinci jenerasyon ağ (5G) teknolojilerinin kurulumunda Huawei firmasının çalışmaları kısıtlanmıştır (BBC, 2018; Whalen ve Nakashima, 2020). Bu nedenle teknolojik uygulamaların geliştirilmesi kadar, uygulanması süreçlerinde ulusal güvenliğe uygun seçeneklerin değerlendirilmesi bir öncelik olmalıdır.

NATO tarafından beşinci harekat sahası olarak tanımlanan siber uzay, ihmal edilmemesi ve devletin varlığını devam ettirmesi gereken bir alandır

SON SÖZ: GÜVENLİK NEREYE?

Teknoloji ve güvenlik ilişkisinde en önemli başlık aslında genel bir ifadeye tekabül eden siber güvenliktir. Çünkü teknolojinin güvenliğinin ve teknoloji eliyle güvenliğin sağlanmasındaki en önemli başlık siber tehditlere karşı yapılacak mücadeledir. Siber tehditler hem teknolojilerde hem teknoloji destekli uygulamalarda güvenlik sorunlarına yol açmaktadır. Bireylerin dijital ortamlardaki varlıkları olduğu kadar devletlerin dijital uygulamaları da bu tehditlerden nasibini almaktadır. Dolayısıyla burada da iki yönlü bir ihtiyaç doğmaktadır. Devlet bir yandan kendi varlığına, hizmetlerine, politikalarına yönelik olarak 'siber alanda' güvenliğini sağlamalı, öte yandan vatandaşların bu alanlardaki varlığını güvence altına almalıdır. Bu durum önemli bir başlık olarak pek çok ülke tarafından dikkate alınmaktadır. Ulusal politikalara yansımaktadır. NATO tarafından beşinci harekat sahası olarak tanımlanan siber uzay, ihmal edilmemesi ve devletin varlığını devam ettirmesi gereken bir alandır (Polat, 2020).

Türkiye de 2020 yılının sonunda yayınlandığı Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ile konuya yönelik hassasiyetini tekrar vurgulamıştır. Son on yılda pek çok politika belgesine ve eylem planına konu alan siber güvenlik meselesi, genel bir çerçeveyle ulusal bir modele dönüştürülmüş durumdadır (Afyonluoğlu, 2020). Öte yandan, özellikle yeni teknolojilerin uyarlanması ve uygulanması noktasında dikkat edilmesi gereken önemli hususlar bulunmaktadır. Veri güvenliği bunların başında gelmektedir. Dijital Dönüşüm Ofisi, Sanayi ve Teknoloji Bakanlığı ve Bilim, Teknoloji ve Yenilik Politikaları Kurulu, TÜBİTAK ve TÜBA gibi kurumlar, teknoloji ve kullanım alanlarıyla ilgili çalışmalar yürütmektedir. Ancak bu konuda uygulamayı gerçekleştiren idarecilerin de konuya yönelik temel düzeyde bilgi sahibi olmaları, risklerin farkında olmaları, öte yandan kullanım imkânlarına yönelik de potansiyeli değerlendirmeleri önemlidir. Başlıkta belirtildiği üzere, teknoloji yeni nesil bir gaddaredir. İki ucu keskindir, ama dikkatli ve etkin kullanımda dosta güven, düşmana korku veren bir araçtır. Yeter ki hakkıyla kullanması biline…

KAYNAKÇA

Afyonluoğlu, Mustafa (2020). "Siber Güvenlik ve Kamu Politikaları", iç. *Teknoloji ve Kamu Politikaları* (Edt. M. Yıldız ve C. Babaoğlu) Ankara: Gazi Kitabevi, s. 379-411.

Athey, Susan (2017). "Beyond Prediction: Using Big Data for Policy Problems", *Science,* 355(6324), s. 483-485.

Babaoğlu, Cenay ve Çobanoğlu, Sedat (2019). "Akıllı Kentler ve Kentsel Güvenlik" iç. *Türkiye'de İç Güvenlik Yönetimi* (Edt. T. Avaner ve O. Zengin), Ankara: Gazi, s. 301-327.

BBC (2018). *Huawei and ZTE Handed 5G Network Ban in Australia,* (23 Ağustos 2018), Erişim: 16 Mayıs 2021, https://www.bbc.com/news/technology-45281495.

İBM (2019). *2018 Cost of a Data Breach*, Erişim: 20 Mayıs 2021, https://www.ibm.com/security/data-breach

Polat, Doğan Şafak (2020). "NATO'nun Yeni Operasyon Alanı: Siber uzay", *Güvenlik Bilimleri Dergisi*, Şubat 2020-UGK Özel Sayısı, s. 135-158.

Rodríguez, Patricio; Palomino, Norma ve Mondaca, Javier (2017). "Using Big Data And İts Analytical Techniques for Public Policy Design and Implementation in Latin America and the Caribbean", *Inter-American Development Bank (IADB),* (Eylül, 2017), Erişim: 3 Mayıs 2021, https://publications.iadb.org/publications/english/document/Using-Big-Data-and-its-Analytical-Techniques-for-Public-Policy-Design-and-Implementation-in-Latin-America-and-the-Caribbean.pdf.

Tüfekçi, Aslıhan ve Karahan, Çetin (2019). "Blokzincir Teknolojisi ve Kamu Kurumlarınca Verilen Hizmetlerde Blokzincirin Kullanım Durumu", *Verimlilik Dergisi*, 4, s. 157-193.

U.S. Department of Homeland Security (2016). *DHS S&T Awards $199K to Austin Based Factom Inc. for Internet of Things Systems Security*, (Haziran 17, 2016). Erişim: 20 Nisan 2021, https://www.dhs.gov/science-and-technology/news/2016/06/17/st-awards-199k-austin-based-factom-inc-iot-systems-security;

Whalen, Jeanne ve Nakashima, Ellen (2020). "U.S. Tightens restrictions on Huawei Yet Again, Underscoring the Difficulty of Closing Trade Routes", *Washington Post* (17 Ağustos 2020), Erişim: 16 Mayıs 2021, https://www.washingtonpost.com/business/2020/08/17/us-cracks-down-huawei-again/

Whittaker, Zack (2016). "A hacker is Advertising Millions of Stolen Health Records on the Dark Web", *ZDNET* (27 Haziran, 2016). Erişim: 20 Mayıs 2021, https://www.zdnet.com/article/hacker-advertising-huge-health-insurance-database/,

Yu, Manzhu; Yang, Chaowei ve Li, Yun (2018) "Big Data in Natural Disaster Management: A Review", *Geosciences*, 8(5), 165, s. 1-26.