KAMU YÖNETİMİ VE SİBER GÜVENLİĞİN ARTAN ÖNEMİ

Mehmet KOCA
İl Planlama Uzmanı-AREM

Teknolojik gelişmelerdeki baş döndürücü gelişmeler ve yenilikler hem vatandaşların kamu hizmet sunumlarına yönelik beklentilerini değiştirerek dijitalleşme lehine bir baskı yaratırken hem de hizmet sunumunun güvenliğinin sağlanması gerektiği gerçeğini gözler önüne sermiştir.

GİRİŞ

İçinde bulunduğumuz küreselleşme çağında baş döndürücü bir hızla ortaya çıkan teknolojik gelişmeler ve yenilikler, sürekli bir dönüşüm ve gelişim deseni içerisinde olan toplumsal süreçlere de sirayet etmiş ve bireylerin yanı sıra kamusal hayatın da vazgeçilmez bir bileşeni olmuştur.

Günümüzün modern dünyasında teknoloji, artık bireylerin günlük yaşamlarından tutun da özel sektöre ve kamusal hayata dair olan genel ve milli güvenliği ilgilendiren tüm alanları kapsayacak şekilde hayatımızın içine kadar işlemiştir (USOM, 2014: 3).

Ülkelerin teknolojik gelişmelerle birlikte bilişim teknolojilerine ve özellikle de internete olan bağımlılıkları gün geçtikçe artmış (Hekim ve Başıbüyük, 2013: 136) ve Covid-19 pandemisi gibi olağanüstü

durumlar bir taraftan dijital araçlara ve proseslere olan ihtiyacı önemli ölçüde artırırken, diğer taraftan da ortaya çıkan yeni çalışma sistemleri, bireylerin ve kurumların dijitalleşme boyutunu giderek arttırmıştır (Çubuk ve Zeren, 2022: ty).

Teknolojik gelişmelerdeki bu baş döndürücü gelişmeler ve yenilikler hem vatandaşların kamu hizmet sunumlarına yönelik beklentilerini değiştirerek dijitalleşme lehine bir baskı yaratırken (Akmeşe, 2020: 109) hem de hizmet sunumunun güvenliğinin sağlanması gerektiği gerçeğini gözler önüne sermiştir.

Bu bağlamda artan dijitalleşme ve teknoloji tabanlı uygulamaların kullanımındaki artış hem bireylerin hem de devletlerin karşı karşıya olduğu risklerin artmasına neden olmuş (Bıçakçı vd., 2015: 3) ve siber alan olarak da adlandırılan bu yeni ortamda güvenliğin sağlanması ciddiye alınması gereken bir durum olarak ortaya çıkmıştır.

Bu çalışmada literatür taramasına dayalı nitel bir araştırma yöntemi takip edilmiş olup, kamusal hayatta dahil olmak üzere hayatın her alanında siber güvenliğin artan öneminin vurgulanması ve buna yönelik farkındalığın artırılması amaçlanmıştır. Çalışmanın en önemli hipotezini ise teknolojinin gelişmesine dayalı olarak artan dijitalleşme neticesinde siber güvenlik kavramının giderek önemli bir hale geleceği olmuştur.

Çalışma üç bölüm üzerinden yapılandırılacak olup, ilk bölümde konuya ilişkin kavramsal bir çerçeve sunulacak, ikinci bölümde siber güvenliğin neden önemli olduğuna ilişkin açıklamalar yapılmaya çalışılacaktır. Üçüncü bölümde Türkiye'deki siber güvenlik çalışmalarına kısaca yer verilirken, çalışma sonuç bölümüyle nihayete erdirilecektir.

1. Kavramsal Çerçeve

Teknolojinin sürekli kendini güncelleyerek gelişimini devam ettirmesi ve hayatın her alanına girmesi bireylerden devletlere kadar yapılan iş ve işlemlerde bilişim sistemlerinin etkisinin artmasına neden olmuştur. Günümüzde artık birçok kamusal hizmet e-devlet gibi dijital platformlar üzerinden verilmektedir.

Küreselleşmenin de etkisiyle dijitalleşmenin artan etkisi kamusal hayatta dahil olmak üzere hayatın her alanında vatandaşlara ve devletlere bir taraftan kolaylaştırıcı ve hızlandırıcı bir işlev sunarken diğer taraftan da ciddi riskleri bünyesinde barındırmaktadır.

Kamu yönetimi ve siber güvenliğin artan önemine ilişkin kaleme alınan bu makalede konunun daha iyi anlaşılabilmesi adına kamu yönetimi, kamu hizmetleri, güvenlik, siber güvenlik gibi kavramların tanıtılmasının önemli olduğu değerlendirilmektedir.

Toplumların, büyüklüğü ve ilişkilerindeki yoğunluk artmaya başladıkça devletlerin de yapı ve işlevleri dönüşüm göstermeye başlamış ve kurumların büyümesiyle uzmanlaşma ve farklılaşma ortaya çıkmaya başlamıştır. Bu nedenle yönetim faaliyetlerinin asli unsurlarından olan kamu kurumları da yapısal ve işlevsel bir dönüşüm geçirerek karmaşık ve teknik bir hale gelmiştir. Kamu yönetimi ile ilgili artan faaliyetler, bu faaliyetlerin karmaşıklaşması ve teknik bir hale gelmesi kamu yönetimi kavramının da farklı tanımlarının ortaya çıkmasına neden olmuştur (Eryılmaz, 2019: 6).

Kamu yönetimi kavramının çok farklı tanımları olmakla birlikte kavramı en basit haliyle devletin hedeflerini gerçekleştirecek şekilde bireylerin ve araçların örgütlenmesi ve yönetimi olarak tanımlayabilmek mümkündür. Bu bağlamda kavram en basit haliyle, devletin yürütme gücüne karşılık gelmektedir (Berkün, 2017: 640).

Kamu yönetimine ilişkin diğer birkaç tanımı ise "*halkın temel ihtiyaçlarını karşılamaya yönelik mal ve hizmetlerin üretimi, kamu politikalarının oluşturulması ve yürütülmesiyle ilgili tüm faaliyetler, kamu hizmetlerinin sunumuna ilişkin mevzuatın*

Siber güvenlik, bilgisayarların, ağların, verilerin ve programların izinsiz erişime karşı korunmasıyla ilgili bilgi güvenliğinin bir parçasıdır

öngördüğü işler ile idari kararları yerine getirmek üzere yönetim, siyaset ve hukuk teorilerinin ve prosedürlerin uygulanması, yasaları ve idari düzenlemeleri uygulamakla ilgili süreçler, organizasyonlar, kamu personelinin eylem ve işlemleri" olarak yapmak mümkündür. Yukarıdaki tanımlar ışığında kamu yönetimi yasaların öngördüğü işler ile kamu politikası kararlarını uygulamakla ilgili süreçleri ve faaliyetleri ifade etmektedir (Özer, ty: 23-25).

Günümüz dünyasında vatandaşların beklentilerindeki artış beraberinde talep edilen hizmetlerinde çeşitlenmesine neden olmuştur. Bu bağlamda kısaca kamu hizmetlerinin ne olduğuna ilişkin açıklamaların da faydalı olacağı değerlendirilmektedir.

Bireylere sunulan hizmetlerin büyük çoğunluğunun siber ortama taşınması, siber güvenliğin sağlanmasını devletler açısından günümüzün en önemli önceliklerinden ve aynı zamanda zorluklarından bir tanesi haline getirmiştir

Kamu hizmeti ya da kamusal hizmetler "*devlet veya diğer kamu tüzel kişilerince veya bunların yakın kontrolleri altında özel teşebbüs eliyle kamuya arz edilmiş olan, genel ve kolektif ihtiyaçları karşılamak ve kamu yararını sağlamak için uygulanan devamlı ve düzenli faaliyetler*" olarak tanımlanmaktadır (Altın, 2013: 103).

Süreklilik, düzenlilik, genellik ve tarafsızlık gibi özellikleri olan kamusal hizmetler organik, maddi ve şekli açıdan üçlü bir tanıma tabi tutulabilmektedir. Bu kapsamda organik açıdan kamu hizmeti "*belli bir görevin yürütülmesi için bir kamu tüzel kişisi tarafından tahsis edilmiş olan ajan ve vasıtaların bütünü*" olarak tanımlanırken, maddi açıdan "*kamu hizmeti "tatmininde kamu yararı olan toplumsal bir gereksinimi karşılayan faaliyetler*" olarak tanımlanmış, şekli açıdan kamu hizmetleri ise "*kamu hizmetleri hukuki rejimine, yani kamusal kamusal yönetim usullerine tabi hizmetler*" olarak tanımlanabilmektedir (Demir, 2019: 231).

İnsan yaşamının temel değerlerinden bir tanesini oluşturan güvenlik kavramının tarihsel kökenleri insanlık tarihi ile birlikte başlamaktadır. Bireyin yaşam bütünlüğü ile eşdeğer bir şekilde hareket eden güvenlik kavramı, toplu yaşama geçip devletlerin kurulmasıyla birlikte dönüşüm geçirmiş, son 30 yılda ise kavram hem genişlemiş hem de derinleşmiştir.

İnsanoğlu varlığını sürdürdüğü müddetçe güvenlik kavramı da mevcudiyetini farklı tanımlar altında devam ettirecektir. Sosyal bilimlerde her bir kavramın birden fazla tanımı olduğundan güvenlik kavramının da çok sayıda tanımı bulunmaktadır.

Güvenlik kavramına ilişkin birkaç tanıma bakılacak olursa; Wolfers'a göre güvenlik "*kazanılan mevcut değerlere yönelik herhangi bir tehdidin bulunmaması*" iken, Hermann güvenliği "*daha önce kabul görmüş değer çıktılarını engellerden arındırma ve geliştirme yeteneğini artırma beklentisi*" olarak tanımlamıştır.

Art ise güvenliği "*bir bireyin diğerlerinin verebileceği zararlardan uzak olduğunu hissettiği ruh hali*" olarak tanımlarken, Baldwin güvenliği "*sahip olunan kazanımlara gelebilecek bir zararın en düşük olduğu hal*" olarak tanımlamıştır (Koca, 2019: 8-9).

Bu çalışmanın ana çatısını da oluşturan siber güvenlik kavramı ise son dönemlerde bilgisayar ve iletişim teknolojilerinin gelişimine ve bu teknolojilerin bireylerin sosyal hayat, iş hayatı ve kamusal hayat gibi yaşam alanlarının büyük bir çoğunluğunda kendisine yer edinmesine paralel bir şekilde sıklıkla kullanılan bir olgu olmuştur (Göçoğlu, 2018: 74).

Siber güvenlik kavramı kabaca siber ortamda faaliyette bulunan kurumların ve bu kurumlarda çalışanlarının mevcudiyetlerini korumak ve varlıklarının güvenliğini sağlamak için kullanılan bir kavram olup, siber ortamın misyonu; bireylerin, mal ve hizmetlerin, sermayenin ve fikirlerin özgürce dolaşımına dayanan küresel bir ekonomi oluşturmak şeklinde ifade edilebilmektedir (Karasoy ve Gezici, 2023: 175).

Siber güvenlik kavramının üzerinde genel olarak üzerinde uzlaşılmış bir tanımı bulunmamakla birlikte NICE (The National Initiative for Cybersecurity Education) siber güvenlik kavramını kısaca "*bilgi ve iletişim sistemleri ile bu sistemlerin içerisinde yer alan bilgilerin herhangi bir zarara, saldırıya ya da yok edilmeye karşı korunduğu, savunulduğu bir faaliyet ya da süreç olarak*" tanımlamaktadır (Göçoğlu, 2018: 77).

Siber güvenlik kavramı Ulusal Siber Olaylara Müdahale Merkezi tarafından "*Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi*" olarak tanımlanmaktadır (USOM, 2014:5).

2016-2019 "Siber Güvenlik Stratejisi" belgesinde ise siber güvenlik kavramı küçük nüanslarla bir önceki tanıma benzer bir şekilde "*siber uzayla ilgili bilişim sistemleri saldırılara maruz kalmaması, ilgili bilginin gizlilik, bütünlük ve erişilebilirliğinin korunması, saldırılar ile siber güvenlik saldırılarının saptanması, buna ilişkin ilgili tedbirlerin uygulanması, sorunun saptanması ve sonrasında sistemde yaşanan siber güvenlikle ilgili tehditlerin veya saldırıların öncesine dönülmesi durumu*" olarak tanımlanmıştır (Önen ve Kurnaz, 2017: 735).

Kavram "*siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi, yaklaşımlar, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünü*" olarak tanımlanırken, bir başka tanımda ise "*siber uzaydan ya da siber uzaya gelebilecek saldırılara/tehditlere, sabotajlara ve terör faaliyetlerine karşı kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan politikalar, oluşturulan güvenlik kavramları, risk yönetimi yaklaşımları gibi faaliyetlerin tamamı*" şeklinde tanımlanmıştır (Darıcılı, 2022: 178).

Ayrıca siber güvenlik kavramının "siber güvenlik, bilgisayarların, ağların, verilerin ve programların izinsiz erişime karşı korunmasıyla ilgili bilgi güvenliğinin bir parçasıdır" ve "siber güvenlik, ağları, cihazları ve verileri suç amaçlı kullanımdan ve yasa dışı erişimden koruma sanatı, [siber ortamdaki] bilgilerin bütünlüğünü, gizliliğini ve kullanılabilirliğini garanti etme uygulaması" gibi tanımları da bulunmaktadır (Karasoy ve Gezici, 2023: 175).

2. Siber Güvenliğin Artan Önemi

Siber güvenlik kavramı ilk defa 1990'lı yılların başında bilgisayar mühendislerince ağa bağlı bilgisayarlarla ilgili oluşabilecek güvenlik sorunlarını ifade etmek için dile getirilmiştir. Daha sonraları bu ağ tabanlı bu güvenlik sorunlarının yıkıcı sosyal sonuçlar doğurabileceği fark edilmiştir. Bu durum zamanla politikacılar, özel şirketler ve uluslararası medya tarafından Batı dünyasına yönelik büyük bir tehdit olarak algılanmış ve "Elektronik Pearl Harbor"lardan bahsedilmeye başlanmıştır (Öğün ve Kaya, 2013: 163).

Uluslararası düzlemde özellikle 2010 yılından sonra akıllı cep telefonlarının ve sosyal medya uygulamalarının kullanımının yaygınlaşması ile başta internet olmak üzere bilişim sistemleri gerek kamusal yaşamın gerekse de sıradan vatandaşların gündelik yaşantılarının temel bir parçası haline gelmiştir. Covid-19 pandemisi ise global ölçekte yaşamın her alanını büyük oranda değiştirmiş ve gündelik yaşamın kalıcı bir şekilde dijitalleşmesine neden olmuştur (Darıcılı, 2022: 196).

Bireylere sunulan hizmetlerin büyük çoğunluğunun siber ortama taşınması, siber güvenliğini sağlanmasını devletler açısından günümüzün en önemli önceliklerinden ve aynı zamanda zorluklarından bir tanesi haline getirmiştir (Ardielli ve Ardielli, 2017: 42).

Günümüzde siber ortam; vatandaşların adli, sağlık ve kimlik bilgileri gibi önemli verilerinin saklandığı; sağlık, bankacılık, eğitim, enerji altyapıları gibi devletin sunduğu ve toplumun düzen ve huzurunun sağlanması için elzem olan birçok kamu hizmetinin gerçekleştirildiği bir ortam haline gelmiştir. Siber ortama artan bu bağlılık/bağımlılık devlet ve özel sektör için maliyetlerin ve kaynak israfının azalması ile hizmet performanslarının artması gibi birtakım avantajları öne çıkarırken, siber ortamdaki verilerin ve siber ortam aracılığıyla faaliyette bulunan kritik altyapıların güvenliğini de ön plana çıkarmıştır (Karasoy ve Gezici, 2023: 174).

Bu bağlamda ülkelerin milli güvenlikleri açısından önem arz eden ve saldırıya uğraması ya da zarar görmesi halinde hayati sonuçlar ortaya çıkarabilecek kritik altyapılar; barajlar, su tutma ve sulama sistemleri, elektrik üretme ve dağıtım sistemleri, petrol tesisleri, gaz sistemleri, ulusal enerji ve ulaşım sistemleri, e-devlet uygulamaları, telekomünikasyon ve finans sistemleri, savunma altyapıları, stratejik sanayi tesislerinin işletim sistemleri, sanayi ve teknoloji sırlarını barındıran sistemler olarak sayılabilmektedir (Öğün ve Kaya, 2013: 162).

Kamu hizmetlerinin ifa edilmesinde ve toplumsal yaşamın düzenli bir şekilde sağlanmasında önemli bir yer tutan kritik altyapılar büyük oranda ağ tabanlı teknolojilere bağlı olarak faaliyette bulunduğundan dolayı ülkelerin kritik altyapılarının siber güvenliğini sağlamak ulusal güvenlikle eş anlamlı hale gelmiştir (Darıcılı ve Çelik, 2022:260).

Çoğu siber alan ile entegre olan veya bir biçimde internet üzerinden ulaşılabilen bu sistemlerin, gelebilecek müdahale ve saldırılardan korunması hayati önem taşımakta-

Siber güvenlik olgusunun ne kadar önemli olduğuna yönelik küresel farkındalık ise ilk kez Estonya'ya karşı yapılan siber saldırılar neticesinde gerçekleşmiştir.

dır. Durumundan memnun olmayan bir çalışanın Avustralya'da nehir ve parklara bıraktığı atık sular, ABD'de 50 milyon kişiyi çaresiz bırakan ve 11 kişinin ölümüne sebep olan elektrik sistemi aksamasının sebebi olan yazılım, İran nükleer tesislerini hedef alan Stuxnet yazılımı siber güvenliğin önemine ilişkin akla gelen ilk örneklerdir. Yine ülkemizde Batman Hidroelektrik Santralinin faaliyetinin aksamasına sebebiyet veren milli olmayan yazılım, Atatürk Havalimanında aksamalara sebep olan virüs, 2011 yılında gümrük sistemlerinin çökmesi üzerine meydana gelen aksama ve uzun kuyruklarda siber güvenliğinin önemine ilişkin örnekler arasında sayılabilmektedir (Öğün ve Kaya, 2013: 162-163).

Siber güvenlik olgusunun ne kadar önemli olduğuna yönelik küresel farkındalık ise ilk kez Estonya'ya karşı yapılan siber saldırılar neticesinde gerçekleşmiştir. 2007 yılının Nisan ayında Estonya; bankalar, medya şirketleri, devlet kurumları gibi ülkenin temel taşı niteliğinde olan birçok kurum ve kuruluşu hedef alan çok büyük bir siber saldırıya maruz kalmış, hem kamuya hem de özel sektöre ait internet sitelerinin çökmesiyle Estonya'nın sahip olduğu iletişim ve e-devlet altyapısı kullanılamaz hale gelmiş, bunun yanı sıra ticaret alanında gerçekleşen birçok etkinlikte kesintiye uğramıştır (Aldemir ve Kaya, 2020: 13).

Siber güvenliğin sağlanması sadece kamusal hizmetlerin ya da kritik altyapıların güvenliğinin sağlanması ile sınırlı kalmamaktadır. Karasoy ve Gezici (2023: 179) siber güvenliğin yalnızca bir ülkenin kritik altyapılarını hedef almasıyla değil aynı zamanda ülkenin politik istikrarını, vatandaşları arasındaki uyumu, demokratik kurumlara ve sürece olan inancı baltalaması yönüyle de ulusal güvenliği tehdit ettiğini ifade etmişlerdir. Bu anlamda siber güvenliğin sağlanması kurumlara ve süreçlere yönelik güvenin sağlanmasında da kritik bir görev üstlenmektedir. Karasoy ve Gezici bu duruma örnek olarak ABD toplumunda kargaşa oluşturmak ve demokratik sürece olan inancı aşındırarak ABD liderliğindeki liberal demokratik düzeni baltalamak amacıyla Rusya'nın 2016 yılındaki ABD başkanlık seçimlerine müdahale etmesinin bizzat FBI eski direktörü James Comey'in ifadeleriyle teyit edildiğini söylemişlerdir. Ayrıca 2014 yılında Ukrayna'daki seçimlere de müdahale eden Rusya'nın, Ukrayna'daki oy sayma sistemlerini geçici olarak çalışamaz hale getirdiğini ve oy sayımını saatlerce geciktiren bir siber saldırı düzenlendiğini belirtmişlerdir.

Görüldüğü üzere siber güvenliğe yönelik gerçekleştirilen siber saldırılar ulaşım sistemlerinin manipüle edilmesi, nükleer santrallerin veya elektrik şebekelerinin bozulması, bir ülkenin önemli bilgilerinin veya bir şirketin teknolojik verilerinin ele geçirilmesinin yanı sıra seçim müdahaleleri yoluyla demokratik düzene yapılan saldırılar gibi çok çeşitli amaçlarla gerçekleştirilebilmektedir (Koch vd., 2020: 275-276).

Siber güvenliğe ilişkin tehditler çok çeşitli olduğu gibi bunları gerçekleştirme yöntemleri de farklılık arz etmektedir. Fidye yazılımları, kötü amaçlı yazılımlar, sosyal mühendislik tehditleri, verilere yönelik tehditler, hizmet reddi saldırıları, internetin kullanılabilirliğine yönelik tehditler, dezenformasyon/yanıltıcı bilgilerin yayılması, tedarik zinciri saldırıları gibi farklı yöntemlerle gerçekleştirilen siber saldırılar siber güvenliğe yönelik tehditleri oluşturmaktadır (Karasoy ve Gezici, 2023: 178).

Görüldüğü üzere bilişim teknolojilerindeki ilerlemeler kamusal hizmetler başta olmak üzere gündelik yaşamdaki birçok faaliyetinde dijitalleşmesine neden olmuştur. Sağlıktan, eğitime, finans işlemlerinden ulaşım sektörüne kadar birçok hizmet günümüzde internet üzerinden gerçekleştirilebilmektedir.

Artan dijitalleşme sonucunda hizmetlerin birbirine bağlanması ve kritik altyapılarında online sistemler üzerinde entegre bir şekilde yönetilmesi bazı avantajlar getirmesinin yanı sıra dikkat edilmediğinde çok ciddi risk ve sınamaları da beraberinde getirmektedir.

Bu kapsamda Dünya genelinde yaşanan örnekler üzerinden düşünüldüğünde bireysel ve ulusal güvenliğin sağlanması adına artan dijitalleşmenin ortaya çıkarabileceği olumsuz sonuçla nedeniyle siber güvenliğe yönelik farkındalık seviyesinin artırılmasının ve tedbirler alınmasının elzem olduğu değerlendirilmektedir.

3. Türkiye'de Siber Güvenlik Alanında Yapılan Çalışmalar

Türkiye'de siber güvenlik alanında yapılan çalışmalara değinilecek olan bu bölümde 2024-2028 yıllarını kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planının ilgili bölümlerinden faydalanılmıştır.

Ülkemiz jeopolitik önemi, ekonomik yapısı ve son yıllardan gerçekleştir-

diği bilişim teknolojileri hamleleriyle siber tehdit aktörleri için cazibe alanı haline gelmiştir. Bu bilinçle ülkemiz, siber güvenlik alanında gerçekleştirdiği özverili çalışmalarla, geçmişten elde ettiği tecrübeleri günümüz teknolojik imkanlarıyla birlikte mümkün olan en üst seviyeye çıkararak, yurt içindeki ve yurt dışındaki paydaşları ile iş birliğini geliştirmiş ve siber uzay kaynaklı tüm olumsuz etkileri asgariye indirme yönünde önemli adımlar atmıştır.

Ülkemiz, ulusal siber güvenliğin sağlanması amacıyla erken dönemlerde aldığı tedbirler ve oluşturduğu ulusal siber güvenlik yapısı ile bu alanda öne çıkan ülkeler arasında yer almıştır. Bu kapsamda Türkiye 5809 sayılı Elektronik Haberleşme Kanunu kapsamında, ulusal siber güvenliğin sağlanması amacıyla politika ve stratejilerin geliştirilmesi ile eylem planlarının hazırlanması, bunlara ilişkin izleme ve değerlendirme faaliyetlerinin gerçekleştirilmesi, koordinasyonun sağlanması görev ve sorumlulukları Ulaştırma ve Altyapı Bakanlığına verilmiştir.

Ayrıca kanun kapsamında Bilgi Teknolojileri ve İletişim Kurumuna siber saldırıların engellenmesi ve caydırıcılığın sağlanması görevleri ile bu görevler kapsamında yükümlülüklerini yerine getirmeyen ilgili taraflara yaptırım uygulama yetkisi verilmiş, müteakiben 1 no'lu Cumhurbaşkanlığı Kararnamesi ile Dijital Dönüşüm Ofisine (CBDDO), bilgi güvenliğinin ve siber güvenliğin artırılmasına yönelik projelerin geliştirilmesine ilişkin görev ve sorumluluklar verilmiştir.

Yine mezkûr kararname ile Sanayi ve Teknoloji Bakanlığına ileri teknolojiler ile büyük veri, yapay zekâ, siber güvenlik gibi kritik alanlarda bireylerin ve işletmelerin Ar-Ge ve üretim yetkinliklerinin artırılması amacıyla politika ve strateji öneri-

leri oluşturulması, girişimlerin desteklenmesi görev ve sorumlulukları verilmiş, 1 sayılı Cumhurbaşkanlığı Kararnamesinde; Cumhurbaşkanı'na bağlı çalışan Güvenlik ve Dış Politikalar Kuruluna "Siber güvenlik ile ilgili politika ve strateji önerileri geliştirmek" görevi verilmiştir.

"Siber güvenliğin sağlanması, bu alanda güçlü stratejiler oluşturulmasıyla mümkündür." anlayışıyla Ulaştırma ve Altyapı Bakanlığı tarafından 2012 yılından itibaren sürdürülen çalışmalar kapsamında hazırlanarak yayımlanan; 2013-2014, 2016-2019 ve 2020-2023 dönemlerini kapsayan "Ulusal Siber Güvenlik Stratejileri ve Eylem Planları" ile ülkemizde bu alanda stratejik yaklaşımın geliştirilmesi ve siber güvenlik çalışmalarının ulusal seviyede hazırlanan planlamalar doğrultusunda, süreklilik içerisinde yürütülmesi sağlanmıştır.

Bu politika belgeleriyle siber güvenlik mevzuatının geliştirilmesi, kritik altyapıların güvenliğinin sağlanması, toplumda siber güvenlik farkındalığının oluşturulması, siber tehditlerin tespiti ve önlenmesi konularında bu dönem içerisinde elde edilen kazanımlarla, stratejik seviyede ele alınan ulusal siber güvenlik çalışmalarının kazanımları elde edilmeye başlanmıştır.

Ayrıca 2013 yılında, BTK bünyesinde faaliyetlerini sürdüren Ulusal Siber Olaylara Müdahale Merkezi (USOM), ülkemizde siber güvenlik olaylarına müdahalede ulusal koordinasyonun sağlanması ve uluslararası temas noktası olarak görev yapması amacıyla kurulmuştur.

Bununla birlikte 11 Kasım 2013 tarihli ve 28818 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ" ile USOM koordinasyonunda 7/24 faaliyet gösterecek şekilde kritik altyapı sektörlerinde Sektörel Siber Olaylara Müdahale Ekiplerinin (Sektörel SOME) kurulması, kurumlar bünyesinde de Kurumsal SOME'lerin kurulması düzenlenmiş olup kurulacak olan SOME'lerin yapısı ve görevlerine yönelik düzenlemeler yapılmıştır. Böylece ülkemizde teknik seviyedeki siber güvenlik yapılanması USOM, Sektörel SOME'ler ve Kurumsal SOME'ler üzerinden şekillenmiştir.

2016-2019 dönemini kapsayan "2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" ile birlikte bu alandaki stratejik yaklaşımın sürekli hale getirilmesine yönelik yeni adımlar atılmıştır. Gerçekleştirilen çalışmalarla siber güvenlik risklerinin yönetilebilir ve kabul edilebilir düzeylerde tutulabilmesi için siber savunmanın güçlendirilmesi, kritik altyapıların korunması, siber suçlarla mücadele edilmesi, farkındalık ve insan kaynağı geliştirilmesi, siber güvenlik ekosisteminin geliştirilmesi ve siber güvenliğin millî güvenliğe entegrasyonu konularında önemli faaliyetler gerçekleştirilmiştir.

Bu kapsamda ulusal siber güvenlik kapasite inşası programı ile SOME'lerin insan kaynağının iyileştirilmesi ve siber olaylara hazırlık seviyesinin artırılması sağlanmış,

ülkemizin ihtiyaç duyduğu insan kaynağının yetiştirilmesine yönelik olarak eğitim, kamp ve yarışma gibi faaliyetler gerçekleştirilmiş, teknolojik önlemler programı kapsamında, yapay zekâ ve makine öğrenmesi imkânlarını kullanan AVCI, AZAD ve KASIRGA gibi hızlı tespit ve erken müdahale sistemleri geliştirilmiş, tehdit istihbaratı edinimi, üretimi ve paylaşımı programı kapsamında ulusal ve uluslararası paydaşlarla iki yönlü bilgi paylaşımı ve koordinasyon çalışmaları hayata geçirilmiş ve kritik altyapıların korunması programı kapsamında kritik altyapıların hizmet sürekliliğinin takibine yönelik izleme faaliyetleri, zafiyet tarama çalışmaları ve bilgi güvenliği açısından düzenleme ve denetleme çalışmaları yürütülmüştür.

2020-2023 dönemini kapsayan "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023" ile siber güvenliğe ilişkin 8 stratejik amaç belirlenmiştir. Eylem Planı çerçevesinde; kritik altyapıların korunması ve mukavemetin artırılması, ulusal kapasitenin geliştirilmesi, organik siber güvenlik ağı oluşturulması, yeni nesil teknolojilerin güvenliğinin sağlanması, siber suçlarla mücadelenin geliştirilmesi, yerli ve millî teknolojilerin geliştirilmesi ve desteklenmesi, siber güvenliğin millî güvenliğe entegrasyonu ve uluslararası iş birliğinin geliştirilmesi konularında önemli adımlar atılmıştır.

Bu çerçevede aralarında kamu kurum ve kuruluşları arasındaki veri trafiğinin güvenli olarak sağlanmasına yönelik KamuNet (Kamu Sanal Ağı) ağının kullanımının sağlanması, kamu kurumlarınca bilgi güvenliği yönetim sisteminin (BGYS) uygulanmasının yaygınlaştırılması yönünde çalışmalar yapılması, TEKNOFEST kapsamında 2018 yılından bu yana düzenli olarak siber güvenlik yarışmaları düzenlenmesi ve 2023 yılında "HackMasters" adını alan yarışmalarda her yıl siber güvenliğin farklı konseptlerinin ele alınması, çevrim içi ve laboratuvar ortamında uygulamalı siber güvenlik eğitimleri ile ülkemizde yetişmiş insan kaynağının ve yetkinlik seviyelerinin artırılmasına katkı sağlanması, kuantum tabanlı güvenlik konularına ilişkin çalışmalar gerçekleştirilmesi, yapay zekâ, büyük veri, blok zincir gibi alanların siber güvenlikle etkileşimi incelenerek rehber dokümanlar oluşturulması, siber güvenlik alanında 4 üniversitenin araştırma odaklı misyon farklılaşması kapsamında ihtisas üniversitesi olarak belirlenmesi ve 2 üniversite de öncelikli alanlar arasında yer alan bilgi güvenliği alanında uzmanlaşan üniversite olarak belirlenmesi, siber güvenliğin mesleki ve teknik eğitim kapsamında değerlendirilmesi çerçevesinde; millî eğitimde siber güvenlik konularının yer aldığı mevcut eğitim müfredatının güncellenmesi gibi çok sayıda çalışma yapılmıştır.

Yapılan bu çalışmalar kapsamında son dönemlerde ülkemizde gerçekleştirilen siber güvenlik faaliyetlerinin bir sonucu olarak Uluslararası Telekomünikasyon Birliği (ITU) tarafından ülkelerin siber güvenlik konusundaki olgunluğunu ölçmekte kullanılan güncel "Global Siber Güvenlik Endeksi" verilerine göre Dünya genelinde 200'e yakın ülke arasında Türkiye 2017 yılında 43'üncü ve 2018 yılında 20'nci sıradayken 2020 verilerine göre 11'inci sıraya yükselme başarısını göstermiştir. Avrupa'da ise Türkiye 2017 yılında 22'nci ve 2018 yılında 11'inci sırada yer almaktayken 2020 verilerine göre 6'ncı sıraya yükselmiştir (Ulaştırma ve Altyapı Bakanlığı, 2023: 8-16).

SONUÇ

İçinde bulunduğumuz küreselleşme çağında baş döndürücü bir hızla ortaya çıkan teknolojik gelişmeler ve yenilikler, sürekli bir dönüşüm ve gelişim paterni içerisinde olan toplumsal süreçlere de sirayet etmiş ve bireylerin yanı sıra kamusal hayatın da vazgeçilmez bir bileşeni olmuştur.

Bu minvalde devletlerin teknolojik gelişmelerle birlikte bilişim teknolojilerine ve özellikle de internete olan bağımlılıkları gün geçtikçe artmış ve Covid-19 pandemisi gibi olağanüstü durumlar bir taraftan dijital araçlara ve proseslere olan ihtiyacı önemli ölçüde artırırken, diğer taraftan da ortaya çıkan yeni çalışma sistemleri,

bireylerin ve kurumların dijitalleşme boyutunu giderek arttırmıştır.

Artan dijitalleşme ve teknoloji tabanlı uygulamaların kullanımındaki artış ise hem bireylerin hem de devletlerin karşı karşıya olduğu risklerin artmasına neden olmuş ve siber alan olarak da adlandırılan bu yeni ortamda güvenliğin sağlanması ciddiye alınması gereken bir durum olarak ortaya çıkmıştır.

Günümüzde siber ortam; vatandaşların adli, sağlık ve kimlik bilgileri gibi önemli verilerinin saklandığı; sağlık, bankacılık, eğitim, enerji altyapıları gibi devletin sunduğu ve toplumun düzen ve huzurunun sağlanması için elzem olan birçok kamu hizmetinin gerçekleştirildiği bir ortam haline gelmiştir. Siber ortama artan bu bağlılık/bağımlılık devlet ve özel sektör için maliyetlerin ve kaynak israfının azalması ile hizmet performanslarının artması gibi birtakım avantajları öne çıkarırken, siber ortamdaki verilerin ve siber ortam aracılığıyla faaliyette bulunan kritik altyapıların güvenliğini de ön plana çıkarmıştır.

Bilişim teknolojilerindeki ilerlemeler kamusal hizmetler başta olmak üzere gündelik yaşamdaki birçok faaliyetinde dijitalleşmesine neden olmuştur. Sağlıktan, eğitime, finans işlemlerinden ulaşım sektörüne kadar birçok hizmet günümüzde internet üzerinden gerçekleştirilebilmektedir.

Artan dijitalleşme sonucunda hizmetlerin birbirine bağlanması ve kritik altyapılarında online sistemler üzerinde entegre bir şekilde yönetilmesi bazı avantajlar getirmesinin yanı sıra dikkat edilmediğinde çok ciddi risk ve sınamaları da beraberinde getirmektedir.

Bu kapsamda Dünya genelinde yaşanan örnekler üzerinden düşünüldüğünde bireysel ve ulusal güvenliğin sağlanması adına artan dijitalleşmenin ortaya çıkarabileceği olumsuz sonuçla nedeniyle siber güvenliğe yönelik farkındalık seviyesinin artırılmasının ve tedbirler alınmasının elzem olduğu değerlendirilmektedir.

KAYNAKÇA

Altın, A. (2013) *Kamu Hizmeti Anlayışında Değişim*, Muş Alpaslan Üniversitesi Sosyal Bilimler Dergisi, Cilt:1, Sayı:2.

Aldemir, C. ve Kaya, M. (2020) *Bilgi Toplumu, Siber Güvenlik ve Türkiye Uygulamaları*, Kamu Yönetimi ve Politikaları Dergisi, Cilt:1, Sayı:1.

Akmeşe, S. (2020) *Kamuda Dijital Dönüşümün Siber Güvenlik ve Dijital Güvence Boyutları ve İç Denetimin Rolü*, Denetişim Dergisi, Yıl: 10, Sayı: 20.

Ardielli, E. ve Ardielli, J. (2017) *Cyber Security in Public Administration of The Czech Republic*, Socıálno-Ekonomıcká Revue, 15 (4).

Berkün, S. (2017) Kamu Açısından Yönetim, Emek ve Toplum Dergisi, Cilt: 6 Yıl: 6 Sayı:16.

Bıçakçı, S., Ergun, D. ve Çelikpala, M. (2015) Türkiye'de Siber Güvenlik, EDAM Yayınları.

Çubuk, E. B. S. ve Zeren, H. E. (2022) Kamu Yönetiminde Siber Güvenlik: Yönetimsel Açıklar ve Çözüm Önerileri, https://www.researchgate.net/profile/Ecem-Buse-Sevinc-Cubuk/publication/382887643_Kamu_Sektorunde_Siber_Guvenlik_Yonetimsel_Aciklar_ve_Cozum_Onerileri/links/66b1cadd8f7e1236bc3dce18/Kamu-Sektoeruende-Siber-Guevenlik-Yoenetimsel-Aciklar-ve-Coezuem-Oenerileri.pdf, Erişim Tarihi: 14.10.2024.

Darıcılı, A. B. (2022) Siber Güvenlik ve Savunma, Ed. F. Pirinçci ve M. Yeşiltaş, içinde Savunma Politikaları (ss. 173-196), SETA Kitapları 86, İstanbul.

Darıcılı, A. B. ve Çelik, S. (2022), *National Security 2.0: The Cyber Security of Critical Infrastructure*, Perceptions: Journal of International Affairs, S.26(2).

Demir, L. (2019) *Kamu Hizmetleri*, https://www.muharrembalci.com/hukukdunyasi/makaleler/birikimlerI/67.pdf, Erişim Tarihi: 15.10.2024.

Eryılmaz, B. (2019) *Temel Kavramlar*, Ed S. Özen, içinde Kamu Yönetimi (ss.2-27), T.C. Anadolu Üniversitesi Yayını No: 3448, Eskişehir.

Göçoğlu, V. (2018) Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi, Doktora Tezi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Hekim, H. ve Başıbüyük, O. (2013) *Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları*, Uluslararası Güvenlik ve Terörizm Dergisi, 4 (2).

Karasoy, H.A. ve Gezici, H.S. (2023) *Bombalardan Baytlara: Siber Güvenliğin Ulusal Güvenlikteki Rolü ve Yapay Zekanın Siber Güvenlikteki Önemi*, Uluslararası Yönetim Akademisi Dergisi, Cilt:6, Sayı:1.

Koca, M. (2019) 15 Temmuz Sonrası Toplumsal Güvenlik ve Huzur, TİAV Yayınları, Ankara.

Koch, T., Moller, D. P. ve Deutschmann, A. (2020), *Smart Technologies as a Thread for Critical Infrastructures*", Ed. K. B. Akhilesh ve D. P. Möller, içinde Smart Technologies: Scope and Applications (ss. 275-289), Springer Publisher, Singapore,

Öğün, M., N. ve Kaya, A. (2013) Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınacak Tedbirler, Güvenlik Stratejileri Dergisi, Yıl: 9, Sayı: 18.

Önen, S. M. ve Kurnaz, S. (2017) Siber Güvenlik Politikalarının Kamu Yönetimine Yansıması, Turgut Özal Uluslararası Ekonomi ve Siyaset Kongresi IV, Malatya.

Özer, U. (ty) Kamu Yönetimi, https://web.hitit.edu.tr/dosyalar/duyurular/ugurozer@hititedutr170420176Y3K5T6V.pdf, Erişim Tarihi: 15.10.2024.

Ulaştırma ve Altyapı Bakanlığı (2023) Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2024-2028, Ankara.

USOM (2014) Siber Güvenliğe İlişkin Temel Bilgiler, Bilgi Teknolojileri ve İletişim Kurumu, Ankara.