Kamu Yönetiminde Siber Güvenliğe Yönelik Düzenlemeler ve Uygulamalar: Türkiye Örneği Üzerinden Bir Değerlendirme[1]

Regulations and Practices on Cybersecurity in Public Administration: An Evaluation Based on the Case of Turkey

Hasibe CEYHAN * Mustafa KOCAOĞLU **

Makale Geliş Tarihi / Received : 23.09.2025
Makale Kabul Tarihi / Accepted : 04.12.2025

ÖZET

Gündelik hayatın vazgeçilmezi haline gelen bilgi ve iletişim teknolojileri, vatandaşlara sunulan hizmet kalitesini arttırabilmek amacıyla, kurum ve kuruluşlar tarafından da en üst düzeyde kullanılmaktadır. Dünya ülkelerinin kalkınmasında önemli bir rol oynayan bu teknolojiler gerek kamu kurumlarında gerekse özel sektörde en yaygın şekliyle kullanılmaktadır. Devletlerin, kurum ve kuruluşların siber ortamdaki varlıklarını sürdürmeleri için, gelişmiş teknolojileri ne düzeyde kullandıkları son derece önemli bir hale gelmiştir. Bütün dünyada ve özelde Türkiye'de de kullanılan teknoloji sistemleri, yaşamı kolaylaştırmak için hayati bir rol oymakla birlikte, siber güvenlikle ilgili gereksinimleri de ortaya çıkarmıştır. Bu çerçevede teknolojik sistemler kamu kurum ve kuruluşları bünyesinde sağlık, çevre, haberleşme, enerji, finansal hizmetler gibi önemli sektörlerde kullanılmaktadır. Faaliyet alanının hızla artış gösterdiği teknolojik sistemlerin siber tehditlere karşı korunması, Türkiye için de ulusal bir ihtiyaç olmasının yanında stratejik bir alan olarak da kendisini göstermektedir. Türkiye'de kamu yönetiminin ve devlet mekanizmasının işleyişinin güvenli bir ortamda sağlanabilmesi için siber güvenlik alanında gerekli mücadeleler, ortaya konulan mevzuat değişiklikleri, hazırlanan programlar uluslararası ihtiyaçlar çerçevesinde ortaya konulmuştur. Bu minvalde çalışmanın amacı dijital çağın en önemli sorunlarından birisi olan siber güvenlik alanında Türkiye'nin yapmış olduğu yasal ve kurumsal düzenlemeleri tarihsel sürece bağlı kalarak incelemek ve üretmiş olduğu siber güvenlik politikalarını, uygulamaları ve aldığı önlemleri elde edilen bilgiler ışığında değerlendirmektir. Çalışmanın ilk bölümünde konu ile ilgili kavramsal çerçeve ele alınacaktır. İkinci bölümde Türkiye'nin uygulamış olduğu politikalar incelenecek, sonuç bölümde ise söz konusu alanda gerekli olan düzenlemelere dair değerlendirme yapılacaktır.

Anahtar Kavramlar: *Siber Güvenlik, Türk Kamu Yönetimi, Siber Güvenlik Politikaları.*

ABSTRACT

Information and communication technologies, which have become indispensable to daily life, are being utilized at the highest level by institutions and organizations to enhance the quality of services provided to citizens. These technologies, which play a significant role in the development of global countries, are widely used in both public institutions and the private sector. The extent to which states, institutions, and organizations utilize advanced technologies to maintain their presence in cyberspace has become extremely important. Technological systems used worldwide, and particularly in Türkiye, play a vital role in making life easier and have also raised cybersecurity requirements. Protecting technological systems used in key sectors such as healthcare, environment, communications, energy, and financial services, where public institutions and organizations are rapidly expanding their scope of activity, against cyber threats, is not only a national need but also a strategic area for Türkiye. The necessary efforts, legislative amendments, and programs in the field of cybersecurity to ensure the secure operation of public administration and the state machinery in Türkiye have been developed within the framework of international requirements. In this context, this study aims to examine Türkiye's legal and institutional regulations regarding cybersecurity, one of the most critical challenges of the digital age, within a historical framework, and to evaluate its cybersecurity policies, practices, and measures in light of the information obtained. The first section of the study will address the relevant conceptual framework. The second section will examine Türkiye's policies, and the concluding section will assess the necessary regulations in this area.

Keywords:. *Cyber Security, Turkish Public Administration, Cyber Security Policies.*

[1]*Bu makale 24-26 Nisan 2025 tarihleri arasında Karadeniz Teknik Üniversitesi tarafından düzenlenen 26. Uluslararası Kamu Yönetimi Forumu'nda (KAYFOR 26) sözlü olarak sunulan "Kamu Yönetiminde Siber Güvenliğe Yönelik Düzenlemeler ve Uygulamalar: Türkiye Örneği Üzerinden Bir Değerlendirme" başlıklı bildirilinin gözden geçirilmiş ve genişletilmiş halidir.*

* *Dr. Öğr. Üyesi, Karamanoğlu Mehmetbey Üniversitesi, Sosyal Bilimler MYO, Sosyal Güvenlik Programı, hcceyhan@hotmail.com, hasibeceyhan@kmu.edu.tr Orcid No: 0000-0002-6551-0787*

** *Prof. Dr. Mustafa KOCAOĞLU Necmettin Erbakan Üniversitesi, Uygulamalı Bilimler Fakültesi, Yönetim Bilişim Sistemleri Anabilim Dalı, kocaoglumustafa@gmail.com, Orcid No: 0000-0002-9341-6341*

GİRİŞ

Toplumların gündelik yaşamlarını sürdürebilmeleri adına kullanmak zorunda oldukları teknoloji, ülkeler için sürdürülebilir büyüme ve kalkınmanın vazgeçilmez bir unsuru olarak yerini almıştır. Türkiye de teknolojiyi yalnızca kullanan değil, aynı zaman da üreten bir ülke olmanın gerekliliğini her geçen gün daha yoğun şekilde yerine getirmekte; siber güvenlik alanında dünyayla rekabet edecek teknik çalışmalar, politikalar üretmektedir.

Vatandaşa sunulan kamusal hizmetlerin, ortaya konulan politikaların ve devletin karar mekanizması içerisindeki bütün faaliyetlerin siber güvenlik kapsamı ekseninde değerlendirilmesi hayati bir unsur haline gelmiştir (Kutlu vd., 2020). 2023 yılında internetin dünya genelinde 5 milyarın üzerinde kullanıcısının olduğu, üretilen veri miktarının çok büyük boyutlara ulaştığı, Türkiye özelinde ise günlük ortalama 7,5 saat internette zaman geçirilmekte olduğu ve bunun yaklaşık 3 saatini sosyal medya üzerinde harcandığı yapılan araştırmalarda ortaya çıkmıştır (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2024-2028).

Yukarıda verilen sayısal verilerden hareketle gün geçtikçe artan kamu ve özel sektöre ait hizmetlerin en üst seviyede halka sunulması hedeflenirken diğer taraftan da söz konusu hizmetlerin siber risk ve tehditlerden korunması için faaliyetler yürütmek devletin önceliği haline gelmiştir. Türkiye ulusal güvenliğini korumanın yanı sıra dünya tarafından kabul görmüş birtakım çalışmalar ortaya koyarak siber güvenlik alanında gerek yurt içinde gerek yurt dışındaki paydaşları ile iş birliği sağlayarak, ulusal çıkarları gözeten politikalar geliştirmiştir.

Bu çerçevede çalışmada ülkemizde siber güvenlik konusunda yapılan çalışmalar ve üretilen politikalar incelenmiştir. Çalışmamızda ortaya konan politikalar değerlendirilirken yıllar itibariyle yayımlanan eylem planları, ulusal düzeyde uygulamaya konan planlamaların stratejik yaklaşımlarının yanı sıra uygulamalardan sorumlu kurumların çalışmalarına yer verilmiştir.

1. SİBER GÜVENLİK

Dünyada gittikçe artan dijitalleşme sürecine bağlı olarak değişen uluslararası sistemlerde güç ve güvenlik algısı da değişmiştir. Bilhassa I. ve II. Dünya Savaşları'ndan sonra savaşlarda kullanılan silahların sanayi harcamalarını artırması nedeniyle devletler mali açıdan zorlanmışlardır ve bu durum yeni dünya düzeninin oluşmasının yanı sıra ülkelerin farklı savaş yöntemlerini benimsemelerine yol açmıştır (Arslan, 2023:28). Gerek teknolojinin gelişmesine bağlı olarak ihtiyaçların dijital ortamdan karşılanması, gerekse devletlerin birbirleri ile olan savaşları siber ortamda gerçekleştirme çabaları siber güvenlik arayışına yol açmıştır. Siber güvenlik alanının hızlı bir şekilde yaygınlaşması ve siber güvenlikle ilgili kavramların tanımlanma ihtiyacı gerekli politikaları üretebilmek için zorunlu hale gelmiştir. Söz konusu kavramların tanımlanması ihtiyaç duyulan siber güvenliği sağlayacak mevzuatın temelini oluşturmuştur. Siber güvenlik kavramı hayati önem taşıyan sistemleri ve ağları dijital saldırılara karşı koruyan, sınırsız verilere rağmen stratejik ve teknolojik çözümler sunan, artan saldırılar karşısında yeni yöntemler geliştiren sistemdir (Cyberarts, 2024). Klimburg, siber uzay içerisinde hareket alanı bulan ve bilişim sistemlerini her türlü tehdit ve saldırılardan korumak, söz konusu tehditlerin özelliklerini tespit etmek ve gerekli önlemleri alarak birtakım yaptırımları oluşturmak, bu alan içerisinde bulunan bilgilerin gizliliğine dikkat etmek şeklindeki çalışmalara ek olarak, insan haklarına uygun bir şekilde ortaya konan ulusal ve uluslararası hukuk çerçevesinde hareket alanı bulan her çeşit oluşumu siber güvenlik olarak tanımlamaktadır (Klimburg 2017). Bugün

geldiğimiz noktada birçok tanımı yapılan siber güvenlik kavramı, siber alanda kurumlar ve bireylerin bilgileri ışığında ihtiyaç duyulan politika ve prosedürlerin hayata geçirilmesi, olası problemlerin azaltılması ve gerekli verilerin varlıklarını korumak için kullanılabilecek güvenlik araçlarının izlenmesi ve gözden geçirilmesi olarak ifade edilmektedir (https://www.itu.int/, 2021).

Siber güvenlik sağlanırken, siber güvenliğin temel bileşenleri olan veri iletişimini gerçekleştiren ağ güvenliği, veri güvenliği, yazılım ve cihazları koruyan uygulama güvenliği, kimlik doğrulama ve yetkilendirme, güvenlik açıklarını düzeltebilmek için zafiyet yönetimi, insan zafiyetiyle mücadele eden eğitim ve farkındalık, olay izleme ve tepki, operasyonel ve fiziksel güvenlik, olağanüstü durum kurtarma ve iş sürekliliğinin en üst seviyede hizmet sunması son derece önemlidir (USOM, 2014).

Siber güvenliğin sağlanması kendi dönemi içinde kullanılan en ileri teknoloji, insan ve süreçlerin güvenliğine bağlıdır. Bu doğrultuda yeni nesil teknolojilerin güvenlik kriterleri, ülkelerin siber güvenlik planlamalarını da şekillendirecektir. Bütün dünyada artan siber tehditler karşısında, mücadele ederken kaynakların doğru planlanması, risklerin ve ihtiyaçların çok iyi değerlendirmeler sonucunda tespit edilmesi ve teknolojik gelişmelere bağlı olarak gerekli planlamaların yapılması öncelikli olmalıdır. Devletlerin en öncelikli konularından birisi haline gelen siber güvenlik konusu, ülkelerin milli çözümler üretmesine ek olarak, kendi aralarında da koordinasyonu sağlayacak politikalar için çaba sarfetmeleri halinde ülkeleri avantajlı hale getirmektedir.

2. TÜRKİYE'DE SİBER GÜVENLİK

Gündelik hayattan uluslararası zemine, ekonomiden sağlığa her alanda siber güvenliğin vazgeçilmez bir ihtiyaç halini aldığı günümüzde, güçlü devletler bu konuda geliştirdikleri stratejik politikalar sayesinde ulusal güvenliklerini sağlamaktadırlar. Jeopolitik konumu itibariyle stratejik bir alanda yer alan ve birçok Avrupa ülkesinden daha fazla nüfusa sahip olan Türkiye hem kamu kurumlarında hem de özel sektör alanında sunduğu hizmetlerde bilgi ve iletişim sistemlerini her geçen gün daha fazla kullanmaktadır. Bu sayede bilgi ve iletişim sistemleri aracılığıyla hem ulusal güvenliğimizi ihlal edecek her türlü zarardan ülkemizi korumakta, hem de dünya çapında oluşması muhtemel ekonomik zararlara engel olmak suretiyle rekabet gücümüzü arttırmaktadır.

1990'lı yıllardan itibaren bütün dünyada artan ağ teknolojilerinin kullanılmasıyla birlikte Türkiye' de siber güvenlik çalışmasına alt yapı oluşturacak birtakım mevzuat düzenlemeleri gerçekleştirmiştir. İlk düzenleme toplumsal düzeni korumak amacıyla 1991 yılında 765 Sayılı Türk Ceza Kanunu'na bilişim suçlarının dahil edilmesi ile gerçekleşmiştir ve "Özel hayatın gizliliği, mülkiyet hakkı, sırrın masumiyeti (dokunulmazlığı), haberleşme hürriyeti, ekonomik menfaatler, kamunun bilişim sistemlerine güveni, bilişim teknolojileri üzerinden yapılacak ekonomik işlemlerde güvenilirlik" şeklindeki değerler hukuken koruma altına alınmıştır (Eker, 2006: 111-116). Daha sonra 2004 yılında 5070 sayılı Elektronik İmza Kanunu (Mevzuat Bilgi Sistemi, erişim tarihi 04.04.2025), aynı yıl "temel hak ve hürriyetleri korumayı amaçlayan ayrıca kişinin güvenli bir toplumda yaşama hakkını sağlamayı hedefleyen" 5237 sayılı Türk Ceza Kanunu (Mevzuat Bilgi Sistemi, erişim tarihi 04.04.2025), 2007 yılında "İçerik, yer, erişim ve toplu kullanım sağlayıcılarının uyması gereken kuralları ve bunların sağladığı internet ortamında işlenebilecek suçlarla mücadeleyi düzenlenmesini" içeren 5651 sayılı kanun (Mevzuat Bilgi Sistemi, erişim tarihi 04.04.2025), 2008 yılında elektronik haberleşme sektörünü geliştirmeyi amaçlayan 5809 sayılı Elektronik Haberleşme Kanunu (Mevzuat

Bilgi Sistemi, erişim tarihi 04.04.2025), 2009 yılında e-Devlet üzerinden vatandaşlara sunulacak hizmetleri denetlemek amacıyla oluşturulan ve e-Devlet politikalarını daha kurumsal hale getirmeyi hedefleyen e-Devlet ve Bilgi Toplumu Kanunu (https://www.sbb.gov.tr/wp-content/uploads/2020/04/e-DevletCalismaGrubuRaporu.pdf, erişim tarihi:04.04.20025) tasarısı yürürlüğe girmiştir.

Türkiye'de siber güvenlik konusunda politikaların üretilmesi 2012 yılında başlamış olsa da ilk olarak kamu kurumları, özel kuruluşlar, STK'ler ve akademik çevrenin katılımıyla, ülkemizin de dahil olduğu, sadece internetin değil, tüm bilişim teknolojilerinin sahip olduğu altyapı yeterliliğinin değerlendirildiği, "Türkiye Bilimsel ve Teknolojik Araştırma Kurumunun" (TÜBİTAK) sekretaryasını yaptığı "Türkiye Ulusal Enformasyon Altyapısı Anaplanı" (TUENA) 1999 yılında gerçekleştirilmiştir. Daha sonra bilhassa kamu kurumlarında "e- dönüşüm"ün gerçekleşmesi için "e-Türkiye Girişimi Eylem Planı", 2003-2004 ve 2005 Kısa Dönem Eylem Planları ve siber güvenliğin ulusal bir sorun olduğunu ortaya koyan "2006-2010 Bilgi Toplumu Stratejisi Eylem Planı" gerçekleştirilmiştir (Karasoy ve Babaoğlu, 2021:138- 139). Bu çalışmalardan sonraki süreçte teknolojinin kullanımıyla ilgili eğitim ve bilinçlendirme faaliyetleri yapılmış, siber güvenlikle ilgili alınacak önlemler belirlenmiş, yerli ve milli güvenlik yazılımları geliştirilmiştir. Türkiye'de 2012 yılında siber güvenlik alanında politikaların üretilmesi, bu konuda farkındalığın sağlanması, yerli güvenlik yazılımlarının geliştirilmesini sağlamak ve koordine etmek amacıyla Siber Güvenlik Kurulu oluşturulmuştur. Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesinde faaliyet göstermek üzere Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur ve ek olarak 2013 yılında "Ulusal Siber Güvenlik Stratejisi" ve eğitimden ticarete kadar birçok farklı alanının sanal ortamda varlık göstermesini hedefleyen "2013- 2014 Eylem Planı" hazırlanmıştır. Daha sonraki süreçlerde hukuki, idari ve teknik altyapının güçlendirilmesi hedefini önceleyen "2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" yayımlanmıştır. Ulaştırma ve Altyapı Bakanlığı tarafından 2020-2023 dönemlerini kapsayan "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" hazırlanmıştır. Hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Plan'larında genel olarak "araştırma ve geliştirme çalışmalarının artırılması, kritik altyapıların korunması, güvenlik konusunda farkındalık çalışmalarının yapılması, yetenekli insan kaynağının geliştirilmesi, güvenlik konusunda eğitim çalışmalarının yapılması, ulusal ve uluslararası alanda siber güvenliğin sağlanması amacıyla işbirliği ve koordinasyon çalışmalarının yapılması ve geliştirilmeleri, siber saldırıların önlenmesinde siber caydırıcılık" gibi konular ağırlıklı olarak üzerinde durulan konular arasındadır (Karasoy ve Babaoğlu, 2021:141-145). Bugün gelinen noktada ise "İnsan", "Savunma", "Caydırıcılık" ve "İş Birliği" şeklindeki ana temaların biçimlendirdiği, 6 stratejik amaç, 18 hedef ve 61 eylem maddesini içeren, siber güvenlik alanında uluslararası seviyede mücadeleyi hedefleyen, "İnsan", "Savunma", "Caydırıcılık" ve "İş Birliği" unsurlarını ön plana çıkaran Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) hazırlanmıştır (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2024-2028). Ek olarak 177 nolu Cumhurbaşkanlığı Kararnamesiyle 8 Ocak 2025 itibariyle Cumhurbaşkanlığına bağlı Siber Güvenlik Başkanlığı kurulmuştur (https://resmigazete.gov.tr/08.01.2025).

Yapılan tüm bu çalışmalar ışığında Türkiye'de Siber Güvenlik alanında "Global Siber Güvenlik Endeksi" verilerine göre Dünya genelinde 200'e yakın ülke arasında 2017 yılında 43'üncü ve 2018 yılında 20'nci sıraya yerleşirken, 2020 verilerine göre 11'inci sıraya yükselmiştir. Avrupa ülkeleri arasında 2017 yılında 22'nci ve 2018 yılında 11'inci sırada yer almaktayken 2020 verilerine göre 6'ncı sıraya yükselmiştir (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2024-2028).

2.1. Siber Güvenlik: Yasal Düzenlemeler Bağlamında Tanımlar, İlkeler

Ulusal siber güvenliğin sağlanmasına ilişkin ortaya konan faaliyetlerin kapsamı ve ilkeleri belirlenirken kilit noktalardan en önemlisi ortak dilin konuşulmasıdır. Siber güvenlik alanında ortak tanımlamaların yapılması, paydaşlar arası koordinasyonun gelişmesine ve kolaylaşmasına katkı sağladığı gibi eylem planlarının doğru bir zemine oturtulması açısından son derece önem arz etmektedir.

Bilgi ve iletişim teknolojilerinin aracılığıyla halka sunulan her türlü hizmetin ve bu hizmetlerin sunumunda yer alan sistemlerin güvenliğini sağlamak adına başlıca şu kavramların tanımlanmasında fayda vardır: "Bilgi Güvenliği", "Siber Güvenlik", "Siber Risk", "Siber Uzay". Bilişim sistemlerinde yer alan "bilgilerin izinsiz ve yetkisiz kişilerce kullanılması, ifşa edilmesi, silinmesi, zarar verilmesini engellemek, için yürütülen her türlü faaliyet" bilgi güvenliği olarak tarif edilirken, siber güvenlik "Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin/verinin gizliliği, bütünlüğü ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber olayların tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber olay öncesi durumlarına geri döndürülmesini kapsayan faaliyetler bütünü" olarak ifade edilmektedir. Siber risk birçok bilginin var olduğu ortamda açıklığı kullanarak zarar yaratma potansiyelidir. Siber uzay ise doğrudan ya da dolaylı şekilde bilgisayar ağlarına bağlı olan tüm sistem ve hizmetleri içermektedir (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023). Belli başlı tanımların ele alındığı bu yaklaşımlar ışığında ulusal siber güvenliğin sağlanmasında, ekonomik ve toplumsal refahı geliştirecek eylem planlarında ortaya konan genel ilkeleri şu şekilde sıralamak mümkündür (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023 ve Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2024-2028):

i. Ulusal güvenliğin sağlanması siber güvenliğe bağlıdır ve ortaya konulacak hedefler ve programlarda kurumsallık, süreklilik esastır.

ii. Siber güvenlik politikaları uygulanırken paydaşların güçlü iletişimi ve koordinasyonu uygun metodolojilerle yürütülür; şeffaflık, hesap verebilirlik ve etik değerler göz önünde bulundurulur

iii. Siber güvenlik riskleri en etkin şekilde tespit edilerek, kritik altyapılar aracılığıyla halka verilen hizmetler kesintisiz bir şekilde sunulur.

iv. Tüm süreçlerde siber güvenlik kavramı esas alınarak, yürütülen işlemlerde bilginin "gizlilik-bütünlük-erişilebilirlik" prensiplerine sadık kalınmalıdır.

v. Güçlü hukuki temeller üzerine bina edilen siber güvenlik inşa anlayışı Ar-Ge, yenilikçi yaklaşımlarla güçlendirilerek yerli ve milli ürün ve hizmet kullanımı teşvik edilmelidir.

Yukarıda yer alan belli başlı tanımlar ve hedefler çerçevesinde, stratejik amaçlar doğrultusunda yapılacak faaliyetleri içeren eylem maddeleri ortaya konmuştur. Bu doğrultuda Ulaştırma ve Altyapı Bakanlığı tarafından yapılacak eylem maddelerinin gerçekleştirilmesine ilişkin politikalar sorumlu kurum ve kuruluşlarla birlikte yürütülmektedir.

2.2. Siber Güvenlik Riskleri

Geliştirilen politika ve ortaya konan hedeflere ulaşmak için siber güvenlik alanında insan kaynağının doğru bir biçimde kullanılması, süreçlerin kendini yenilemesi vazgeçilmez unsurlar olarak öne çıkmaktadır. Bütün dünyada olduğu gibi Türkiye'de güvenli bir siber ortam sağlayabilmek adına siber saldırılara karşı korunmaya yapılan saldırılara karşı gerekli müdahaleleri yapmaya ve cezalandırmaya, ihtiyaç duyulan yasal mevzuatı oluşturmaya ve siber ortama yönelik politikaları tesis etmeye çalışmaktadır (Çifci, 2013: 163-166).

Siber güvenliği risk altında tutan belli başlı tehlikeler dört kategoride incelenebilir. Kurum ya da devletlere yönelik olarak dijital ortamda yürütülen yasa dışı faaliyetler olarak nitelendirilen siber suçlar; direk olarak veri hırsızlığı, sistem çöküşü sonucunda dijital altyapıları hedef alan eylemleri içeren siber saldırı; iki devlet arasında dijital ortamda gerçekleşen siber savaş; siyasi veya ideolojik amaçla yapılan, sivilleri ve kamu düzenini hedef alan, politik talepleri kabul ettirmek için yapılan siber terör (Aydın, 2025: 13-14).

Bu minvalde siber risklerin ortaya çıkmasında genel olarak, internet tasarımı sırasında adresleme sistemi, yönetim eksikliği, internetin çalışmasını sağlayan sistemlerin çoğunun açık ve şifresiz olması gibi zafiyetler, donanım ve yazılımlardaki hataların yanı sıra kritik sistemlere çevrim içi erişim imkanının olması gibi unsurları saymak mümkündür (Aslay, 2017: 25).

3.TÜRKİYE'DE SİBER GÜVENLİĞE YÖNELİK UYGULANAN POLİTİKALAR VE ORTAYA KONAN YOL HARİTASI

Ulusal güvenliği tesis etmenin en önemli unsurlarından birisi olan siber güvenlik, üst düzey milli güvenlik politikalarımızın en önemli parçalarından birisi haline gelmiştir. Söz konusu politikalarda kara, hava, deniz ve uzay güvenliğinin yanında siber güvenliğe ilişkin hususların da kayda değer bir şekilde dikkate alınması, ülkemize karşı oluşması muhtemel tehditlerin bertaraf edilmesi açısından son derece önemlidir. Uluslararası seviyede çalışmaların yürütüldüğü siber güvenlikte politika belirlenirken çok taraflı iş birliklerinin yanı sıra bilgi ve tecrübe alışverişi de yapılmaktadır (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020- 2023). Siber Güvenlik alanında geliştirilen politikalar incelendiğinde Türkiye'yi söz sahibi konuma getiren, bu konuda kapasitesini arttıran son dönemlerde ortaya koyduğu yol haritasını değerlendirmenin yanı sıra uluslararası ölçekte siber güç konusunda ön plana çıkmış ülkeleri de analiz etmek yerinde olacaktır.

Farklı jeopolitik, sosyal ve ekonomik özelliklere sahip olduğu için siber güvenlik ekosisteminde geliştirdikleri ulusal stratejilerle uluslararası siber politikaların şekillenmesinde öncü rol oynayan ilk ülke ABD'dir. Yaptırımı güçlü yasalarla siber saldırılardan korunma, bu saldırılar karşısında gerekli müdahalenin geliştirilmesi ve her düzeyde ortaya koyduğu iş birliği konularına öncelik veren ABD ürettiği politikalar çerçevesinde siber güvenlik alanında özel sektörle iş birliği yapmayı, bu alandaki araştırmaları ve siber güvenlik eğitimini teşvik etmeyi hedefleyen uygulamalar ortaya koymuştur. Siber tehditler karşısında savunmacı olduğu kadar saldırgan bir tavır belirleyen Rusya savunma stratejisi alanında ürettiği politikalarla kritik altyapıların güvenliğini sağlamış ve diğer ülkelerin siber uzaydaki faaliyetlerini engelleyerek Rusya kendi çıkarlarını ön planda tutmayı temel amaç edinmiştir. Son yıllarda ekonomik ve teknolojik hamleleri ile ön plana çıkan Çin kritik altyapıların korunması, kişisel veriler için en üst düzeyde sağladığı güvenlik ve kullandığı yapay zekâ teknolojileri sayesinde kapsamlı stratejilerin yanı sıra insan hakları ve özgürlükler açısından eleştirilen yasal düzenlemeler geliştirmiştir. Son olarak Estonya yapay zekâ ve otomasyon teknolojilerini siber güvenlik

stratejilerine entegre etmiş, yapay zekâ tabanlı çözümler geliştirmiş ve bu çözümleri siber tehditlerin önlenmesinde kullanılmıştır (Aydın, 2025:39-50).

Türkiye diğer dünya ülkeleri ile karşılaştırıldığında siber güvenlik kavramı ile daha geç tanışmış olsa da bu alanda dijital dönüşümü gerçekleştirerek, teknolojik imkanlardan faydalanmak suretiyle, siber tehditlere karşı güçlü bir savunma mekanizması geliştirmeyi başarmıştır. Siber güvenliğin sağlanması için kamu, özel sektör, akademi ve STK temsilcilerinin fikirlerinin de alınarak oluşturulduğu amaç ve hedefler belirlenirken, ulusal ihtiyaçlar gözetilerek gerekli güncellemeler yapılmıştır. Bu çerçevede ulusal düzeyde siber güvenlik alanında en gelişmiş ülkelerin kullandığı son teknolojik imkânlara sahip olunması, kritik altyapılarımızın 7/24 korunması esas alınmıştır. Ayrıca kurumlar arası görev dağılımına bakıldığında siber güvenlik stratejisinin uygulanmasından sorumlu ana kurum olarak Ulaştırma ve Altyapı Bakanlığı, siber saldırıları önleme, caydırıcılık sağlama ve taraflara yaptırım uygulama yetkisine sahip olan Bilgi Teknolojileri ve İletişim Kurumu, bilgi güvenliği ve siber güvenliğin artırılmasına yönelik projeler geliştiren ve 28 Mart 2025 tarihli Resmi Gazete'de yayımlanan Cumhurbaşkanlığı Kararnamesi'yle kapatılan Dijital Dönüşüm Ofisi'nin önemli destek sağladıkları görülmektedir. Siber olaylara müdahale ekiplerinin yetkinliklerinin artırılmasının yanı sıra eğitim içeriklerinin zenginleştirilerek insan kaynağının güçlendirilmesi, yerli ve milli ürün kullanımıyla birlikte, düzenleme ve denetlemeye dayalı siber güvenlik anlayışının tercih edilmesi üretilen belli başlı politikalardır (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023). Ayrıca önümüzdeki zaman dilimine de damgasını vuracak politikalar "İnsan", "Savunma", "Caydırıcılık" ve "İş Birliği" argümanları çerçevesinde şekillenmiştir. Bu minvalde ihtiyaçlara cevap verebilecek siber güvenlik süreçlerinde yetkin insan kaynağının oluşturulması ve buna bağlı olarak hibrit tehditlere karşı siber savunmanın gerçekleştirilmesi sağlanmıştır. Riskler ve tehditler gerçekleşmeden önce veya erken aşamalarda tehditlerin önüne geçilmesine ilişkin durumlarda siber caydırıcılığın sağlanması esas alınmıştır. Sertifikasyon ve akreditasyon gibi mekanizmaların işletilerek millî ürün projelerinin oluşturulmasına ek olarak paydaşlarla iş birliği yapılarak mücadele edilmesi hedeflenmiştir (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2024-2028). 2024-2028 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, kritik altyapıların korunması, yerli ve milli teknolojilerin en üst seviyeye çıkarılması, insan odaklı yaklaşımların benimsenmesi ve uluslararası iş birliklerinin güçlendirilerek arttırılması gibi hedefler baz alınarak ülkemizin dijital geleceğini güvence altına almayı amaç edinen bir yol haritasıdır.

Sonuç olarak, Türkiye dışa bağımlılığı en aza indirgemek adına yerli ve milli çözümleri artırmalı, siber güvenlik alanında yetkin insan kaynağını desteklemeli yapay zekâ gibi yeni nesil tehditlerle mücadele etme noktasında savunma tekniklerini güncel tutmalı, siber güvenlik eğitimleri arttırılarak gerek ulusal gerekse uluslararası düzeyde koordinasyon ağı sağlamalıdır (Aydın,2025:62-63).

SONUÇ

Bilgi ve iletişim teknolojilerinin yaygın kullanımıyla birlikte siber uzaydaki tüm bileşenlerin birbiriyle bağlantılı olması ve siber güvenlik risklerinin gün geçtikçe artması ülkeleri her geçen gün yeni politikalar üretmeye zorunlu kılmıştır. Ulusal güvenliğin ihlaline neden olabilecek sorunları bünyesinde barındıran siber güvenliğin sağlanması konusu tüm dünyada gelişmiş ülkelerin en önemli mücadele alanıdır. Bu nedenle son zamanlarda siber tehditlerin cazibe alanı olan Türkiye için de siber güvenlik risklerinin yönetilebilir düzeylerde tutulması hedeflenmektedir.

Türkiye'de şu ana kadar siber güvenlik konusunda birçok hukuki çalışma yapılmış olmakla birlikte, ihtiyaç duyulduğu zaman mevzuatın güçlendirilmesi ve sürekli olarak güncellenmesine devam edilmelidir. Yine devam etmesi gereken bir başka önemli husus siber güvenlik konusunda ilgili paydaşların, kurumların desteklerinin alınması, iş birliği ve koordinasyon çalışmalarının yapılması ve eğitim çalışmalarının yetkin insan kaynağına ulaşana dek sürdürülmesi, ulusal ve uluslararası alanda siber güvenliğin sağlanması açısından önemlidir. Yapay zekâ destekli güvenlik çözümleri ışığında kamu-üniversite-sanayi iş birlikleriyle siber güvenlik Ar-Ge projeleri desteklenmeli ve kabul gören projeler hem iç piyasada hem de ihracatının yapılması yönünde desteklenerek uluslararası rekabet gücü artırılmalıdır.

Ulusal düzeydeki bütün paydaşların katılımını sağlayacak şekilde siber güvenlik konusuna bütüncül bir bakış açısı sağlanmalı ve uluslararası zeminde iyi uygulama örnekleri ışığında ulusal, kurumsal ve bireysel bazda, iş birliğine dair alınacak tedbirler tespit edilmelidir. Siber güvenlik hususunda karşılaşılan problemlerin %80'nin insan unsurundan kaynaklandığı görülmektedir (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2024-2028). Bu nedenle siber güvenlik riskleri ve siber olayların etkilerine dair bilgi düzeylerinin artırılmasına ve toplumun hemen her kesiminin bilgilenmesini sağlayacak çalışmalara hız verilmelidir. Ulusal siber güvenliğin sağlanmasında son süreçte ortaya koyduğu çalışmalar ile öne çıkan ülkemiz, millî siber güvenlik teknolojilerini geliştirerek, yurt içinde kullanımını yaygınlaştırmaktadır.

Ülkemizde Siber güvenlik alanında yapılan düzenlemeler dikkate alındığında söz konusu düzenlemelerin ülkemize ne kazandırdığı, ülkemizin hangi alanlarda eksik kaldığı ve geleceğe yönelik atması gereken adımlar bağlamında şunları söylemek mümkündür. Siber tehditlere karşı savunma kabiliyeti güçlendirilmiş olmakla birlikte, uygulama süreçlerinin çok daha etkin ve yaygın hale getirilmesi gerekmektedir. Gelecekte ise geliştirilen mevzuatın denetim ve izleme mekanizması ile desteklenerek siber güvenlik ekosisteminin sürdürülebilirliğini sağlamak temel hedef olmalıdır.

KAYNAKÇA

Arslan, S. F, (2023), 21. Yüzyılda Ulusal ve Uluslararası Siber Güvenlik: Türkiye'nin Siber Güvenlik Strateji ve Politikaları, Yüksek Lisans Tezi, İstanbul Yeni Yüzyıl Üniversitesi Sosyal Bilimler Enstitüsü, s:1-69.

Aslay,F. (2017), Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi, *International Journal of Multidisciplinary Studies and Innovative Technologies*,1(1),24-28.

Aydın,E. (2025), Siber Güvenlikte Öne Çıkan Ülkelerin Politikalarının İncelenmesi ve Türkiye'nin Siber

Güvenlik Stratejileri, Selçuk Üniversitesi, Fen Bilimleri Enstitüsü, s:1-135.

Cyberarts (2024). "2024 Cyberarts Siber Bülten.", https://www.cyberartspro.com/Erişim Tarihi: 31.08.2025.

Çifci, H. (2013). *Her Yönüyle Siber Savaş*, TÜBİTAK Popüler Bilim Kitapları, 3. Baskı, s:1-400, Ankara.

Eker, U. (2006), "Türk Ceza Hukuku'nda Bilişim Suçları" Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu", *Türkiye Barolar Birliği Dergisi*, S. 62, s. 111-116.

Karasoy, H. A. Babaoğlu, P. (2021), Türkiye'de Siber Güvenlik: Yasal Ve Kurumsal Altyapı, *Yasama Dergisi*, Sayı: 44 · (Temmuz-Aralık 2021), 123-155.

Klimburg, A. (2017), "*The Darkening Web: The War for Cyberspace*." ,Penguin Press, s:420.

Kutlu, Ö., Kahraman, S., Dinçer, S. (2020) "Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Politikalarının Analizi*", Assam Uluslararası Hakemli Dergi 13. Uluslararası Kamu Yönetimi Sempozyumu Bildirileri Özel Sayısı*.

https://www.mevzuat.gov.tr/mevzuat?MevzuatNo= 5070&MevzuatTur=1&Mevzuat, 5070 Sayılı Elektronik İmza Kanunu Erişim Tarihi: 04.04.2025

https://www.mevzuat.gov.tr/mevzuat?MevzuatNo= 5237&MevzuatTur=1&Mevzuat, 5237 Sayılı Türk Ceza Kanunu Erişim Tarihi:04.04.2025

https://www.mevzuat. gov.tr/mevzuat? Mevzuat No=5651&MevzuatTur=1&Mevzua, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun. Erişim Tarihi: 04.04.2025

https://www.itu.int/en/ITU-D/Conferences/WTDC/WTDC21/Pages/RPM/Digital-Trends-Reports-2021, Erişim tarihi: 04.04.2025

https://www.mevzuat.gov.tr/mevzuat Mevzua No=5809&MevzuatTur=1&Mevzuat, 5809 Sayılı Elektronik Haberleşme Kanunu Erişim Tarihi: 04. 04.2025

https://www.sbb.gov.tr/wp-content/uploads/2020/04/e-DevletCalismaGrubuRaporu.pdf, Erişim tarihi:04.04.2025)

https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf, Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2024-2028, s:1-34, Erişim Tarihi tarihi:05.04.2025

https://resmigazete.gov.tr/08.01.2025, 08 Ocak 2025 Tarihli ve 32776 Sayılı Resmî Gazete, Erişim Tarihi: 10.04.2025

https://cbddo.gov.tr/siber-guvenlik-stratejisi, Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023, Erişim Tarihi:10.04.2025.

USOM(2014),"Siber Güvenliğe İlişkin Temel Bilgiler." https://dsy.usom.gov.tr/usom/19/02/190211082958_siber_guvenlige_giris_ve_temel_kavramlar, Erişim Tarihi: 10.04.2025