**ORGANİZASYON ve YÖNETİM BİLİMLERİ DERGİSİ**
**Cilt:** 16 **No:** 1 **Yıl:** 2024 **ISSN:** 1309-8039 (Online) (**ss.** 23-47)
**Makale Geliş Tarihi:** 14.03.2024 **Makale Kabul Tarihi:** 19.04.2024 **Çevrimiçi Yayın Tarihi:** 26.04.2024

**-ARAŞTIRMA MAKALESİ-**

# TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKASININ EYLEM PLANLARI ÜZERİNDEN ANALİZİ*

**Arzu YILDIRIM**[1]
Doç.Dr.
Şırnak Üniversitesi, Sağlık Bilimleri Fakültesi
E-mail: a.ucar@sirnak.edu.tr
ORCID ID: 0000-0002-8543-278X

## *Öz*

*İnsanların var oldukları andan itibaren ihtiyaç duydukları en temel gereksinimleri güvenlik olmuştur. Güvenlik, ilk zamanlarda sadece askeri kurumların yerine getirmeleri gereken konular arasında sayılmaktayken; günümüzde ulusal ve uluslararası düzeyde faaliyet gösteren bütün kurum ya da kuruluşların temel ilgi alanları olmuştur. Bunda hiç şüphesiz hızla gelişen teknoloji ve bilgi toplumunun giderek gelişmesi, bilişim dönemine geçilmesinin etkisi olduğu söylenebilir. Günümüzde ulusal güvenliğin sağlanmasında temel koşul olarak siber güvenlik konusu öne çıkmaktadır. Bu nedenle ülkeler kendi ülkelerinin koşullarına ve şartlarına göre, sahip oldukları niteliklere göre kendi alanlarında siber saldırılardan korunması, verilerin ve bilgilerin güvenliğinin sağlanması amacıyla farklı siber güvenlik politikaları geliştirmektedirler. Türkiye bu noktada özellikle 2010 yıllarından sonra siber güvenlik konusunun önemini anlamış, bu dönemde yapılan çalışmalar ağırlık kazanmıştır. Türkiye'de siber güvenlik konusuna yönelik mücadele çalışmalarının yeni olduğunu söylemek mümkündür. Bu çalışmanın temel amacı, Türkiye'de günümüze kadar geliştirilen siber güvenlik konusundaki stratejileri, politikaları, bu konuda faaliyet gösteren kurum ve kuruluşları inceleyerek, genel işleyişini ortaya koymaktır. Araştırmada nitel araştırma yöntemlerinden biri olan içerik analizi yöntemi uygulanmıştır. Bu*

* Bu makalede bilimsel araştırma ve yayın etiği ilkelerine uyulmuştur.

[1] **Sorumlu Yazar:** a.ucar@sirnak.edu.tr

**Atıf (APA):** Yıldırım, A., (2024), Türkiye'nin Siber Güvenlik Politikasının Eylem Planları üzerinden Analizi, Organizasyon ve Yönetim Bilimleri Dergisi, 16 (1): 23-47.

*araştırmada ulaşılan sonuç, siber güvenliğin sağlanması konusunda Türkiye'nin gerçekleştirdikleri faaliyetlerin küresel alanda küçümsenmeyecek düzeyde olduğudur. Siber güvenliğin sağlanması amacıyla önemli sayılacak gelişimlerin yaşandığını söylemek mümkündür. Ancak siber güvenlik konusunda farkındalık çalışmalarının nitelik ve nicelik olarak arttırılması, bu alanda yapılan çalışmaların sonuçlarının da kamuoyu ile paylaşıması yerinde olacaktır.*

***Anahtar Kelimeler:*** *Güvenlik, Siber Güvenlik, Strateji Belgesi, Siber Saldırı, Teknoloji*

***Alan Tanımı:*** *Kamu Yönetimi, Kamu Politikası, Siber Güvenlik*

## ANALYSIS OF TURKEY'S CYBER SECURITY POLICY THROUGH ACTION PLANS

***Abstract***

*Security has been the most basic requirement that people need from the moment they exist. While the issue of security was among the subjects that only military institutions focused on in the early days; today, it has been the main interest of all institutions national and international level. Undoubtedly, the main reason for these developments is the development of technology. Today, cyber security is the basic condition for ensuring national security. For this reason, countries develop different cyber security policies according to the conditions and conditions of their own countries. At this point, Turkey understood the importance of cyber security, especially after 2010, and the studies carried out in this period gained weight. It can be said that the issue of cyber security in Turkey is new. The main purpose of this study is to examine the policies on cyber security developed in Turkey until today. Content analysis method, which is qualitative research methods, was used in the research. The conclusion reached in this research is that Turkey's activities in providing cyber security are at a level that cannot be underestimated in the global arena. It is possible to say that important developments have been experienced in order to ensure cyber security. However, it would be appropriate to increase awareness of cyber security in terms of quality and quantity, and to share the results of the studies in this field with the public.*

***Key Words:*** *Security, Cyber Security, Strategy Document, Cyber Attack, Technology*

***JEL Codes:*** F52, G38, H56, H58

## 1.GİRİŞ

Son zamanlarda, yaşanılan sorunların evrenselleşmesi, ortaya çıkan tehdit unsurlarının ülkeleri kısa zamanda etkilemesi, sektörler üzerinde olumsuz etki ortaya çıkmıştır. Güvenlik konusuna yönelik yapılan araştırmalar askeri konular üzerine yoğunlaşsa da içinde bulunduğumuz zamanda sosyal ve beşeri alanlarda da güvenlik konusu öne çıkmaya başlamıştır (İnce, 2021).

Güvenlik, insanların çok eski zamanlardan itibaren gereksinim duydukları temel gereksinimlerden biridir. İnsanlar, sürekli olarak yaşadıkları ülkelerde, bölgelerde, mahallede güvenlik sorunları ile karşılaşmamaları için gerekli önlemleri alma gayreti içine girmişlerdir. İnsanlar tarafından alınan güvenlik önlemleri, içinde bulunulan çağa göre değişiklik göstermektedir. Teknolojinin gelişmesi, iletişim alanında yaşanan gelişmeler ülkeleri, toplumları sürekli yeni tedbirler alınması konusunda zorunlu kılmıştır. Özellikle de internetin kullanılmasının yaygın hale gelmesi, akıllı telefonların, bilgisayar kullanım oranlarının yükselmesi ile insanlar, toplumlar, ülkeler yaşanan değişimlere bağlı olarak yeni güvenlik önlemleri geliştirmek durumunda kalmışlardır. Çünkü internet yardımı ile kurumların, insanların, ülkelerin en önemli bilgilerine, adeta milli sır niteliğini taşıyan bilgilere erişme ve kullanma daha kolay hale gelmiştir. Teknolojinin bize sunduğu kolaylıkların yanı sıra bazı sorunları da beraberinde getirdiği görülmektedir. Özellikle güvenlik konusu son dönemde ülkelerin, kurumların, insanların en önemli sorunlarından biri haline gelmiştir. Siber güvenlik ve siber güvenliğin sağlanması, siber saldırılara karşı mücadele konuları ülkelerin en önemli gündem maddeleri durumundadır. Ülkeler siber güvenlik sorunu ile etkili bir şekilde mücadele edebilmek için siber güvenliğin sağlanması konusuna ayrı bir önem vermektedir. Siber güvenlik konusunda stratejiler, eylem planları, politikalar geliştirme gayreti içerisine girmişlerdir. Kritik altyapı hizmetlerinin korunması, ulusal güvenliğin dolayısıyla siber güvenliğin sağlanması, herkese açık hâle gelen bilgilerin güvenliğinin sağlanması konusu ülkeler için hayati önem taşımaktadır. Bu noktadan hareketle çalışmada Türkiye'de siber güvenlik konusu üzerinde durulması ihtiyacı doğmuştur. Çalışmada Türkiye'nin siber güvenliğin sağlanması ve korunması hususunda günümüze kadar izlenen politikalar, stratejiler değerlendirilmiştir.

1980'li yılların başından beri ABD'de bireysel bilgisayarların üretilmeye başlamasıyla, özellikle Soğuk Savaş sonrasında interneti sivil insanların kullanmaya başlaması küresel düzeyde gelişimin ilk habercisi olmuştur. İnternetin sivil kullanımının arttırılması, cep telefonu kullanımının yaygınlaşması ile beraber

gittikçe yaygınlık kazanan akıllı telefon kullanım oranının artması hayatın her alanını etkilemiştir. Devletler sonraki süreçte kritik altyapılar şeklindeki ağ teknolojileri ile kamu hizmetlerini sunmaya çalışmışlardır. Bu gelişmelerin bir sonucu olarak kritik altyapıların korunması devletlerin en önemli sorumlulukları arasında yer almıştır (Darıcılı, 2019). Bunun sağlanması için kurumlardaki teknoloji yöneticilerinin iş devamlılığını sağlamak amacıyla ekosisteme uygun kararlar almaları ve yeni sistemde en verimli yöntemleri kurum kültürü olarak yaklaşmaları önemlidir (Korucu, 2021).

Güvenlik stratejisinde hedef, risk, tehdit gibi kavramlar önemlidir. Güvenlik ve tehdit kavramları devamlı birbirlerini etkileyen bir özellik taşıdığı için tehditlerin belirlenmesi, güvenlik stratejisi oluşturmada önemli bir unsurdur. Çünkü devletlerin alacakları güvenlik tedbirleri bir başka devlet tarafından tehdit olarak algılanabilecektir. Bu bakımdan karşılıklı etkileşim sonucunda tespit edilen tehditlerin belirlenmesi, alınabilecek tedbirlerin özelliği ve harekete geçmesini sağlayan unsurlar ülke stratejisinin belirlenmesinde kritik unsurlardır (Küçükşahin vd., 2008).

Siber güvenlik, insanın güvenlik sürecindeki rolünü dikkate alırken, önceleri bunu ek bir boyut olarak kabul etmiş ve ayrıca odak kişinin potansiyel bir hedefi olduğu bilgi güvenliği için birbirinin yerine kullanılmıştır. Bununla birlikte, siber güvenlikle ilgili bu tür bir tartışma, bir bütün olarak toplumun etik kısmına odaklandığından önemli bir çıkarımı vardır. Siber güvenlik kavramının güvenli paylaşım, gizlilik ve bilgiye erişim gibi çeşitli yönleriyle çeşitli tanımları bulunmaktadır. Ancak yine de tanımlar netlikten ve fikir birliğinden yoksundur (Thakur vd., 2015). Günümüzde siber güvenlik alanı, belirli alanların, disiplinlerin, uluslararası ilişkiler uzmanlarının çalışma alanları olmaktan çıkması gerekir. Siber güvenlik politikaları, farklı disiplinlerin çalışmasını gerektirmektedir. Devletin dijital yapıya geçmesi, kamu hizmetlerinin kritik altyapılar aracılığıyla sunulması siber güvenlik konusunun kapsamının genişlemesine katkıda bulunmaktadır. Sunulacak kamusal hizmetlerin, uygulanacak politikaların ve alınması gereken bütün kararların siber güvenlik kapsamında değerlendirilmesi zorunluluktan ziyade hayati bir unsur durumuna gelmiştir (Kutlu, Kahraman ve Dinçer, 2020). Aynı zamanda internet ortamındaki mevcut bilgilerin güvenliğinin sağlanması konusundaki sorunların çözüme kavuşturulması siber güvenlik alanlarının genişlemesine neden olmuştur (Özalp ve Asker, 2017).

2000'li yıllar ile birlikte siber tehditler için kullanılan yöntemler hem daha da karmaşık hale gelmiş hem de çoğu zaman büyük şirketlerin ve kamu kurumlarının internet siteleri hedef alınmıştır. Daha sonraki yıllarda siber saldırılara karşı ulusal seviyede tedbirlerin alınmasının önemini kavrayan ülkeler kendi güvenlik politikalarını uygulamaya başlamışlardır (Güngör, 2015).

Dünyadaki her ulusun kendi varlığını devam ettirmek için bir plan, bir tür ulusal güvenlik stratejisi vardır. Resmi olarak kamuya açık bir belgede ifade edilmiş olsun ya da hükümet liderleri tarafından dolaylı olarak konuşmalar yoluyla iletilmiş olsun, hem genel belirsizlik hem de iyi tanımlanmış tehditler karşısında uzun vadeli bir ulusal güvenlik stratejisinin temel amacı, gelecekteki zorluklarla ilişkili riskleri yönetme konusunda rehberlik sağlamak ve böylece ulusun kalıcı güvenliğini sağlamaktır (Kazel, 2021).

## 2.TÜRKİYE'NİN SİBER GÜVENLİK STRATEJİSİ

Güvenlik, güvenliğe bağlı küresel bir fikirdir; bir kişinin hayatına, mülkiyetine veya haklarına zarar vermeden hayatına devam edebileceğinin güvencesidir. Siber güvenlik , bilişim sistemlerine, veri alışveriş kanallarına ve işledikleri bilgilere odaklanan ve ihlalleri ceza hukuku kapsamında yaptırıma tabi tutulabilecek bir alt kümedir (Elmaghraby ve Losavio, 2014). Nesnelerin interneti teknolojileri, telekomünikasyon, ulaşım, imalat, su ve enerji yönetimi, sağlık, eğitim, finans, devlet ve hatta eğlence gibi birçok sektörde geniş çapta kullanılmaktadır. Çeşitli bilgi ve iletişim teknolojisi araçlarının kullanılması, işlevlerini ve hizmetlerini kullanıcıları yeni seviyelere çıkarmıştır. BİT, son on yılda sistem tasarımı, ağ mimarisi ve akıllı cihazlar açısından dikkate değer bir gelişmeye tanık olmuştur (Nguyen ve Reddi, 2022).

Siber güvenlik, içinde bulunduğumuz süreçte ulusal güvenlik stratejilerinde üzerinde durulan konular arasında yer almaktadır. Özellikle son yıllarda Türk şirketlerinin ve devlet görevlilerinin de devamlı siber casusların hedeflerinde olmaları bu konudaki sorunu ortaya çıkarmakta ve bu alana daha fazla yatırımın yapılmasını zorunlu kılmaktadır. Teknolojik alanda yaşanan gelişmeler ile beraber siber güvenlik alanında yaşanan gelişme çok hızlı gelişmektedir ki, alınan tedbirler ve uygulamaya konulan mevzuat yetersiz kalabilmektedir. Olabilecek riskler ve gereksinimler kapsamında alınan kararlar geleceğe dönük güvenliğin sağlanmasında yeterli olamamaktadır. Çok farklı sayıda ve türde siber saldırı yöntemleri bulunmakta ve bunların çoğu bireysel düzeyde bilinmemektedir. Siber güvensizliğin meydana getireceği maliyetlerin bu alana yapılabilecek maliyetten

daha fazla olacağına dikkat edilerek siber savunma alanına gereken hassasiyetin gösterilmesi gerekir (Aslay, 2017).

Siber güvenliğin ayırt edici yönlerini; (Craigen vd., 2014) disiplinlerarası sosyo-teknik karakteri, ağ aktörlerinin yeteneklerinin potansiyel olarak büyük ölçüde benzer olduğu, ölçeksiz bir ağ olmak, yüksek derecede değişim, bağlılık ve etkileşim hızı olarak belirlemiştir. Siber savaş alanında ortaya çıkan etkileşim, ekonomik bakımdan fazla maliyetli olmayan yazılımların ortaya çıkmasını ve nitelikli personel ihtiyacı konusunu öne çıkarmıştır. Uluslararası güvenlik ortamında siber tehditler, güvenlikleştirme modeli bakımından iç politikanın oluşturulmasında göz önünde bulundurulmaya başlamıştır (Güntay, 2017).

Siber güvenlik, bir kişinin/kuruluşun sadece bilgilerinin veya bilgi sistemlerinin korunmasından daha fazlasını korumakla ilgili olmalıdır. Siber güvenlik aynı zamanda siber bir ortamda kaynakları kullanan kişilerin korunması ve siber ortamdan kaynaklanan zafiyetler sonucunda riske maruz kalan toplumun geneline ait olanlar da dahil olmak üzere diğer varlıkların korunması ile ilgilidir (Solms ve Niekerk, 2013).

Özellikle COVID-19 salgını, siber suçlular tarafından kullanılan dikkate değer ve benzersiz toplumsal ve ekonomik koşullar yaratmıştır (Lallie vd., 2021). Pandemi sürecinde daha önceden kabul edilen bilginin güvenliği ve siber güvenlik kavramları pandemiyle birlikte artan dijital faaliyetler, siber güvenlik konusunda güncel yaklaşımlar ve işlerin devamlılığının sağlanması ikilemi yaşanmıştır. Pandemi döneminde iş devamlılığının sağlanması, ekonomik sistemin çalışması, arz ve talep dengesinin korunması için öncelikli koşul olan uzaktan çalışma yöntemi siber saldırılara adeta bir davetiye özelliği taşımıştır. Bilişim altyapısı ve bilgi güvenliği bakımından uzaktan çalışma altyapısına sahip olamayan birçok kurum, hızlı bir şekilde uzaktan çalışma sistemine geçmiş, siber güvenlik alanındaki zorlukları bir kez daha ortaya çıkarmıştır. Sanal alanda özel ağları bulunmayan kurum çalışanları tarafından güvenli olmayan yöntemler ile kritik verilerin kullanılması, mevcut tehditlerin azaltılması yaklaşımlarına karşı tutarsız bir yaklaışm ortaya çıkmıştır. Ortaya çıkan siber olaylar, kurumların siber güvenliğin sağlanması, iletişim ve bilgi teknolojisi alanlarında uzaktan çalışma sistemlerini güvenilir bir duruma getirebilmeleri için daha fazla çaba göstermelerine neden olmuş, kurumların teknolojinin yönetimi konusundaki zaafiyetleri ortaya çıkmıştır. Kurum çalışanlarının internete bağlanabilen bütün cihazlar ya da verileri kullanabilmeleri için kurumsal güvenlik kriterlerinin kriz süreçlerine uygun şekilde altyapının oluşturulması ihtiyacını ortaya çıkarmıştır

(Korucu, 2021). Kritik altyapının (örneğin elektrik gücü, ulaşım) bulunmaması, doğrudan ve fiziksel hasara neden olan sistemlerin çok ötesinde ekonomik etkiye sahip olabilir. Bu etkiler yerel, bölgesel, ulusal veya muhtemelen küresel ekonomiyi olumsuz etkileyebilir (Maglaras vd., 2018).

## 3.TÜRKİYE'DE SİBER GÜVENLİK YAPILANMASI

Türkiye'de siber güvenlik konusunda organizasyon üç temel yapılanma üzerine oluşturulmuştur. Birinci grupta, siber suçlar konusunda faaliyet alanları kapsamında siber suçlar ile mücadele edecek kurumlar yer almaktadır. İkinci grupta kritik altyapının korunması, kamu kurumlarının siber güvenliklerinin korunması ve geliştirilmesi, Türkiye'nin siber güvenlik kapasitesinin oluşturulması alanlarına yoğunlaşan kurumlar bulunmaktadır. Üçüncü grupta ise, devlet destekli özel girişim özelliğini taşıyan kurumlar bulunmaktadır. Türkiye'nin siber güvenlik politikalarının oluşturulmasından, yönetilmesinden sorumlu olan üst kurul ise Siber Güvenlik Kurulu'dur. Siber suçlarla kendi faaliyet alanına yönelik mücadele eden kuruluşlar; Emniyet Genel Müdürlüğü'ne bağlı Siber Suçlarla Mücadele Daire Başkanlığı, Jandarma Genel Komutanlığı Bilişim ve Teknik İstihbarat Başkanlığı, Sahil Güvenlik Komutanlığı İstihbarat Daire Başkanlığı Siber Suçlarla Mücadele Şube Müdürlüğü bulunmaktadır. Ayrıca, 2009 yılında yapılan bir düzenleme ile Türkiye'de afet durumlarında acil durum görevi AFAD'ın sorumluluğuna verilmiştir. Bu düzenlemede afetler teknolojik ve doğal afet olmak üzere ikiye ayrılmıştır. Bu düzenlemeye göre Türkiye'de olası bir topyekün siber saldırı ile karşılaşılması ve bunun afet düzeyine ulaşması durumunda kriz yönetimi AFAD tarafından yönetileceği belirtilmiştir (Darıcılı, 2019). 2012 yılında kabul edilen Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar'a göre Siber Güvenlik Kurulu oluşturulmuştur. Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na siber güvenlik konusunda görev verilmiştir. 2014 yılında kabul edilen karar ile Bilgi Teknolojileri ve İletişim Kurumu'na siber güvenlik alanında yeni sorumluluklar yüklenmiştir (BTK, 2022).

Türkiye'de siber alanda mücadele edebilmesi amacıyla günümüze kadar çok sayıda kurum ve kuruluş yetkili kılınmıştır. Bu kurumlardan bazıları ülkenin savunma alanının nasıl korunacağı alanında fikir üretme, bazı kurumlar bu fikirler kapsamında yeni teknolojiler geliştirme, bazı kurumlar ise siber güvenliğin sağlanması amacıyla savaş alanında çarpışarak siber saldırılar ile mücadele edecektir. Bu kuruluşlardan öne çıkanlar; TÜBİTAK ve Alt Kuruluşları, Bilgi Teknolojileri ve İletişim Kurumu (BTK), Afet ve Acil Durum Yönetimi

Başkanlığı (AFAD), Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Ulaştırma ve Altyapı Bakanlığı şeklinde açıklanabilir (Karasoy ve Babaoğlu, 2021).

Siber Güvenlik Kurulu; 2012 yılında yapılan bir düzenleme ile Bakanlar Kurulu'nun almış olduğu Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar kapsamında Siber Güvenlik Kurulu oluşturulmuştur. Ayrıca Ulaştırma ve Altyapı Bakanlığı'na siber güvenliğin sağlanması konusunda yeni görevler tanımlanmıştır.

TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM): Türkiye'nin en yetkin araştırma ve geliştirme merkezi niteliğine sahiptir. Türkiye'de bilgi güvenliği ve bilişim alanlarında teknolojik alanda bağımsızlığı sağlayabilmek amacıyla gerek askeri gerekse de sivil bilginin güvenliğinin sağlanması, korunması ve iletilmesini sağlayan araştırma ve geliştirme çalışmaları yapmaktadır. Aynı zamanda ülkemizdeki bilişim ve bilgi güvenliğini tek tip çözümler ile değil işbirliği çalışmaları ile giderebilecek bir yaklaşımla çalışmaktadır. Bu özelliğinden dolayı BİLGEM'in geliştirdiği teknolojiler ulusal sınırları geçerek birçok ülke tarafından faydalanılmaktadır. BİLGEM'in sundukları bu fırsatlar ile Türkiye bilgi güvenliği ve bilişim alanında çözümler üreten, birçok ülke ile rekabet edebilir duruma gelmiştir (Biz Kimiz, 2022).

Afet ve Acil Durum Yönetimi Başkanlığı (AFAD): Afetler konusunda 2009 yılında yapılan düzenleme ile afetler konusunda yetkili olan diğer kurumların sorumlu olmaları durumu ortadan kaldırılmış, afet konusundaki sorumluluklar tek bir kurum altında toplanmak istenmiştir. 2018 yılında kabul edilen 4 Nolu Cumhurbaşkanlığı Kararnamesi ile Afet ve Acil Durum Yönetimi Başkanlığı İçişleri Bakanlığı'na bağlanmıştır (AFAD Hakkında, 2022). 2014 yılında AFAD tarafından hazırlanan 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi'nde ulusal düzeyde kritik altyapıların korunması sorumluluğu AFAD'ın da sorumlu kılındığı belirtilmiştir. Bu belgeye göre AFAD'ın siber güvenlik konusunda; teknolojik afet alanında sivil korunmanın sağlanması konusunda faaliyetler yürütecek şekilde hukuksal, kurumsal ve teknik alanlarda çalışmalar yapmak, bu düzenlemenin uygulanması için sorumlu olan diğer kurum ya da kuruluşlar ile işbirliği yapmak şeklinde görevler yüklenmiştir (2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi, 2014).

Bilgi Teknolojileri ve İletişim Kurumu (BTK), ülkemizde telekomünikasyon alanında düzenleyici ve denetleyici kurum özelliğine sahiptir. Türkiye'de ilk

düzenleyici kurum olma vasfını taşımaktadır. 2000 yılında Telekomünikasyon Kurumu oluşturulmuştur. 2008 yılında yapılan düzenleme ile kurumun adı Bilgi Teknolojileri ve İletişim Kurumu şeklinde yeniden oluşturulmuştur (BTK, 2022). Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2018 yılında yapılan düzenleme ile Dijital Dönüşüm Ofisi Başkanlığı'nın görev ve sorumlulukları; Cumhurbaşkanı tarafından belirlenen amaç ve politikalara uygun bir şekilde kamu kurumlarında dijital dönüşümün sağlanmasına katkıda bulunmak, kamu dijital dönüşüm kapsamında uygulanacak yol haritasını belirlemek, dijital kamu hizmetlerinin sunulmasını sağlamak amacıyla diğer kurum ve kuruluşlar ile işbirliği yapmak, bilginin güvenliğini ve siber güvenliği sağlayacak ve artıracak politikalar geliştirmek, kamu kurumlarında büyük veri analizi ve gelişmiş analizlerin çözümlerinin etkili kullanılmasına ilişkin stratejiler geliştirmek, kamu kurumlarında yerli dijital teknolojilerin kullanılması için projeler geliştirip farkındalık oluşturmak, kamuda yapay zeka kullanılmasına ilişkin projelere öncelik vermektir (1 Sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, 2021).

Siber Güvenlik Dairesi Başkanlığı'nın görev ve sorumlulukları; ulusal düzeyde siber güvenlik ve bilgi güvenliğini sağlayacak projelerin geliştirilmesi, siber güvenlik alanlarında politika, strateji ve eylem planlarının ulusal ortamda uygulanmasını sağlayacak tedbirleri almak ve süreci takip etmektir (1 Sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, 2021).

Cumhurbaşkanlığı Savunma Sanayii Başkanlığı'nda ve Dijital Dönüşüm Ofisi'nin katkılarıyla 2018 yılında Türkiye Siber Güvenlik Kümelenmesi oluşturulmuştur. Bu projenin oluşturulmasının amacı; ulusal düzeyde siber güvenlik ekosistemini kurmak, yerel ve ulusal düzeyde siber güvenlik ürünlerinin geliştirilmesini sağlamak, siber güvenlik alanında dünyadaki diğer ülkeler ile rekabet edebilecek bir Türkiye hedeflenmektedir (Yanarışık, 2020).

1 sayılı Cumhurbaşkanlığı Kararnamesi ile Güvenlik ve Dış Politikalar Kurulu oluşturulmuştur. Bu Kurul'un görev ve sorumlulukları arasında siber güvenlik konusu da yer almaktadır. Bu düzenlemeye göre Kurul'a siber güvenlik konusunda politikaların oluşturulması, siber güvenliğin sağlanması için önerilerin geliştirilmesi sorumluluğu verilmiştir.

Ulaştırma ve Altyapı Bakanlığı, bu düzenlemeye göre ulusal düzeyde siber güvenliğin sağlanmasına yönelik politika, strateji geliştirmek, kamu kurum ve kuruluşlarının bilgi güvenliğinin sağlanması için yasal düzenlemeleri uygulamaya

koymak, ulusal siber güvenliğin gerçekleşmesi amacıyla ulusal kaynakların geliştirilmesine katkıda bulunmak ve desteklemek, ulusal siber güvenlik konusunda farkındalığın sağlanması için gerekli faaliyetleri yürütmek gibi yeni görev ve sorumluluklar Ulaştırma ve Altyapı Bakanlığı'na verilmiştir (Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı, 2022).

## 4.TÜRKİYE'DE SİBER GÜVENLİK STRATEJİSİNİN UYGULAMAYA YANSIMASI OLARAK EYLEM PLANLARI

2013 yılında kabul edilen Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının temelde siber güvenlik konusunda farkındalığın sağlanması, bu konuda kurum ve kuruluşların üzerlerine düşen görevleri yapmalarını sağlamak olduğu söylenebilir. Bütün kamu kurum ve kuruluşların bilgi teknolojisi kullanılarak yapılan bütün işlemlerin güvenliğinin sağlanması, kurumlarda kullanılan kritik altyapıların güvenliğinin tesis edilmesi, siber suçun ya da bir durumun ortaya çıkması durumunda kurumların izlemeleri gereken yöntemlerin belirlenmesi, belirlenen yol haritası kapsamında hareket edilmesini sağlamak genel amaçlar arasındadır. Kurumların siber güvenliğin sağlanması konusunda dikkat etmeleri gereken hususların olduğu belirtilen diğer konular arasındadır. Buna göre kurumlar siber güvenliğin sağlanması konusunda; hukuk kurallarına bağlılık ve kuralların üstün olması, temel hak ve hürriyetlerin korunması, mahremiyetin gizli tutulması hususlarına dikkat edilmesi gerektiği belirtilmiştir. Siber güvenlik konusunda sadece kamu kurumlarının değil özel kurumların da bu konuda ortak hareket etmeleri, kurumların siber güvenlik alanındaki güçlü ve zayıf yönleri, fırsatları ve tehditleri ortaya koymaları gerektiği, siber güvenlik alanında öncelikli olarak ulusal kaynakların kullanılması gerektiği hususları belirtilmiştir. Bu hedeflerin gerçekleştiirlmesine yönelik alt eylemler düzenlenmiştir. Aly eylemler olarak; Ulusal Siber Olaylara Müdahale Merkezi (USOM), Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) oluşturulması, Siber Güvenlik Kurulu'nun etkinliğinin sağlanması için ulusal düzeyde yasal düzenlemelerin yapılması, ulusal düzeyde siber güvenlik altyapılarının güçlendirilmesi konusunda çalışmaların yapılması, siber güvenlik alanında gelişmiş insan kaynaklarının geliştirilmesi, eğitilmesi, siber güvenlikte milli teknolojik unsurların geliştirilmesi çalışmalarına ağırlık verilmesi gerektiğine vurgu yapılmıştır.

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2013-2014 döneminde hazırlanan eylem planlarının sürelerinin dolmasından sonra Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından, dünyada yaşanan

değişime bağlı olarak teknolojinin gelişmesi, siber güvenlik konusunun zorunlu bir hâl almasından yola çıkılarak yeni bir eylem planı oluşturulmuştur. Eylem planının hazırlanması sürecinde diğer kurumlar ile işbirliği ve koordinasyon çalışmaları yürütülmüştür. Eylem planı hazırlanırken aynı zamanda diğer ülkelerin siber güvenlik konusundaki tecrübelerinden yararlanmak amacıyla ülkelerin siber güvenlik stratejileri, araştırma ve geliştirme çalışmaları ayrıntılı bir şekilde incelenmiş ve değerlendirilmiştir. 2016-2019 Ulusal Siber Güvenlik Stratejisinin temelde amacı; ulusal güvenliğin sağlanmasında siber güvenlik konusunun da artık önemli bir parçası olduğu, bu anlayışın bütün kurularda yerleşmesi gerektiği ve ulusal siber sistemde bulunan bütün kurumların, kuruluşların siber güvenliğin sağlanması konusunda her türlü tedbiri almak zorunda olduğu esasına dayanmıştır. Siber güvenliğin sağlanmasında kullanılan her türlü teknolojilerin korunması, gizliliğinin sağlanması, siber güvenlik saldırısı ile karşılaşılması durumunda saldırının etkisinin minimum seviyeye çıkarabilmek için gerekli stratejilerin geliştirilmesi, siber suç konularının gerekli adli kurumlar tarafından ayrıntılı olarak incelenmesi gerektiği hedefleri yer almaktadır. Belirtilen amaçlara ulaşılması konusunda stratejik eylemler geliştirilmiştir. Siber alanda savunmayı sağlamak ve kritik altyapıların korunması için devletin ve diğer birimlerin stratejik eylem geliştirmesi, siber suçlarla mücadele konusunda kurum ve kuruluşların yetkilendirilmesi, ülkedeki herkesin siber güvenlik konusunda bilgilendirilmeleri, bu konuda uzman kişilerin sayılarının arttırılması, siber güvenliğin sağlanması konusunda özel ve kamu kurumları ile diğer paydaşlar ile işbirliği çalışmalarının yoğunlaştırılması çalışmalarının yapılması gerektiği belirtilmiştir.

2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2020 yılında kabul edilen eylem planında daha önceki dönemlerin stratejik eylem planları gözden geçirilmiştir. 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nda diğer eylem planlarında belirtilen hususlara ek olarak, ülkenin ekonomisinin geliştirilmesinde ve korunmasında ulusal güvenliğin dolayısıyla siber güvenliğin önemi üzerinde durulmuştur. Siber güvenliğin ve kritik altyapıların korunması hususunda ulusal düzeydeki bütün kurum ve kuruluşların koordineli bir şekilde işbirliği çalışmalarının gerektiği belirtilmiştir. Ulusal düzeyde siber güvenliğin sağlanmasında kritik sektörler belirlenmiş, siber güvenlik alanında ulusal kapasitenin geliştirilmesi, siber saldırılara karşı birlikte mücade edebilmek için güvenli ağların oluşturulması, yerli ve ulusal teknolojilerin geliştirilmesi ve desteklenmesi, özellikle uluslararası alandaki tehditler ve riskler için uluslararası alanda işbirliği çalışmalarının geliştirilmesi konuları üzerinde durulmuştur.

2009 yılında TÜBİTAK UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) tarafından yürütülen "Ulusal Sanal Ortam Güvenlik Politikası" ile birlikte siber savunma ve siber güvenlik politikalarının sınırları belirlenmiştir. Bu faaliyetlere ek olarak 2012 yılından beri BİLGEM (Bilişim ve Bilgi Güvenliği İleri Teknolojileri Araştırma Merkezi) kapsamında faaliyet gösteren SGE (Siber Güvenlik Enstitüsü) siber güvenlik konusunda gerekli altyapının oluşması konusunda katkı sunmaktadır (Tamyapar, 2019).

## 5.TÜRKİYE'NİN SİBER GÜVENLİK STRATEJİSİNİN DEĞERLENDİRİLMESİ

İnternet günümüzde insanların yaşamlarının vazgeçilemez bir unsuru durumuna gelmiştir. Günlük hayatın ötesinde ekonomik, askeri, sosyal ve siyasi hayatta önemli bir güç unsuru, ekonomik bakımdan büyüyüp gelişebilmenin devamlılığı için hayati bir öneme sahip bir unsur haline gelmiştir. İnternetin oluşturduğu bu güç karşısında, internete bağımlı dünya ülkeleri, bu ülkelerin oluşturdukları organizasyonlar ve Türkiye önemli bir güvenlik alanı ile karşı karşıya kalmıştır: Siber güvenlik (Demircioğlu, 2014).

Siber saldırılar, kamu kurumlarının ve özel sektörün özel bilgilerine ulaşılması, askeri komuta-kontrol yapılarının sistem dışı bırakılması, merkez bankası gibi önemli altyapıların ele geçirilmesi, bazı temel hizmetlerden yoksun bırakılarak toplumların ayaklanma olaylarının desteklenmesi gibi çok sayıda olumsuz durumlara ve olaylara sebebiyet vermektedir. Bunun yanında sınır tanımayan, uygun mali kaynaklarla daha yüksek seviyede fiziki zarar verme gücüne ulaşan siber saldırılar, önemli noktaya geldiği durumlarda uluslararası güvenlik ve uzmanların yakından ilgi gösterdiği konular arasında sayılmaktadır. Günümüzde uluslararası gündemi yoğun bir şekilde meşgul eden siber güvenlik konusunun, kısa süre içerisinde ulusal gündemi yoğun olarak meşgul edebileceğini söylemek yanlış olmayacaktır (Güreşci, 2019). Dolayısıyla tüm dünyada ve ülkede bilgi toplumuna geçilmesi ile bireysel, siyasi ve teknik alanlarda zararlı yazılımların oranlarında büyük artış söz konusu olmuş, ülkeler ve kurumlar siber saldırıların hedefi olmuştur (Yılmaz vd., 2015).

Türkiye'de siber güvenlik konusu ile ilgili çalışmalar 2003 yılında kabul edilen Başbakanlık Genelgesi ile başladığı söylenebilir. Başbakanlık Genelgesi'nde güvenlik kültürünü oluşturmak, ülkelerin bilgi sistemlerine ve ağlarına ilişkin riskler karşısında, her seviyedeki kullanıcıların kabul edip kullanılmasının faydalı olacağı belirtilmiş, öncelikli olarak bütün kamu kurum ve kuruluşları olmak üzere,

bilgi sistemlerinin ve yapılarının korunması amacıyla yürütülecek uygulamalarda dikkate alınması gerektiği belirtilmiştir (Şenol, 2017).

Bu çalışmaların yanında Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında, siber güvenlik tehditleri ve dikkate alınması gereken hususlara yer verilmiştir. Eylem planlarında bulunan eylemler ve alt eylemlerin birkaçı için bitirilme tarihi belirtilmiş, sürekli olarak yapılması ve uygulanması gereken faaliyetlere ayrıca yer verilmiştir (Kılcı, 2020).

Küresel Siber Güvenlik Endeksi (GCI), ülkelerin siber güvenliğe olan bağlılığını küresel düzeyde ölçen, konunun önemi ve farklı boyutları hakkında farkındalık yaratmak için güvenilir bir referanstır. Siber güvenliğin birçok endüstriyi ve çeşitli sektörü kapsayan geniş bir uygulama alanına sahip olması nedeniyle, her ülkenin gelişme veya katılım düzeyi beş sütun üzerinden değerlendirilmektedir. Bunlar; Yasal Tedbirler, Teknik Tedbirler, Örgütsel Tedbirler, Kapasite Geliştirme ve İşbirliğidir (Global Cybersecurity Index, 2021).

**Tablo 1.** 2017 yılı küresel siber güvenlik endeksi

| Üye Ülkeler | Puan | Küresel Sıralama |
|---|---|---|
| Singapur | 0.925 | 1 |
| ABD | 0.919 | 2 |
| Malezya | 0.893 | 3 |
| Umman | 0.871 | 4 |
| Estonya | 0.846 | 5 |
| Moritus | 0.830 | 6 |
| Avustralya | 0.824 | 7 |
| Gürcistan | 0.819 | 8 |
| Fransa | 0.819 | 8 |
| Kanada | 0.818 | 9 |
| Rusya Federasyonu | 0.788 | 10 |
| Japonya | 0.786 | 11 |
| …… | …… | …… |
| Türkiye | 0.581 | 43 |
| …… | …… | …… |
| Yemen | 0.007 | 164 |
| Ekvator Ginesi | 0.000 | 165 |

**Kaynak:** Global Cybersecurity Index, 2017

2017 yılında yayınlanan Küresel Siber Güvenlik Endeksi incelendiğinde; Singapur 0.925 puan ile ilk sırada yer almaktadır, onu 0.919 puan ile ABD takip etmektedir. Türkiye yapılan bölge sıralamasında Avrupa bölgesinde 0.581 puan ile 22. Sırada bulunmaktadır. Küresel ölçekte yapılan sıralamada ise 165 ülke arasından 43. sırada bulunmaktadır. Bu sıralamada Türkiye'den sonra 122 ülke bulunmaktadır. En düşük sıralamada Yemen ve Ekvator Ginesi yer almaktadır. Küresel Siber Güvenlik Endeksinin 2017 raporunda Türkiye ile ilgili özel bir ifadeye rastlanmamaktadır.

2018 yılında yayınlanan Küresel Siber Güvenlik Endeksi incelendiğinde; Türkiye 0.853 puanla Avrupa bölgesinde 11. sıraya yükselmiş, küresel ölçekte yapılan sıralamada ise 175 ülke arasından 20.sıraya yükselmiştir. 2018 yılı Küresel Siber Güvenlik Endeksi raporunda Türkiye ile özel bir bölüm de bulunmaktadır.

**Tablo 2.** 2018 yılı küresel siber güvenlik endeksi

| **Üye Ülkeler** | **Puan** | **Küresel Sıralama** |
|---|---|---|
| Birleşik Krallık | 0.931 | 1 |
| ABD | 0.926 | 2 |
| Fransa | 0.918 | 3 |
| Litvanya | 0.908 | 4 |
| Estonya | 0.905 | 5 |
| Singapur | 0.898 | 6 |
| İspanya | 0.896 | 7 |
| Malezya | 0.893 | 8 |
| Kanada | 0.892 | 9 |
| …… | …… | …… |
| Türkiye | 0.853 | 20 |
| Danimarka | 0.852 | 21 |
| Almanya | 0.849 | 22 |
| …… | …… | …… |
| Maldivler | 0.004 | 175 |

**Kaynak:** Global Cybersecurity Index, 2018

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı siber güvenlik alanında yayımlanan ilk belge olması özelliğinden dolayı süreklilik bakımından değerlendirilmesi yerinde olmaz. Eylem planında siber güvenliğin sağlanması ve kritik altyapıların korunması için işbirliğinin geliştirilmesi amaçlar arasındadır. Araştırma ve geliştirme çalışmaları üzerinde durulmuş, temel hedefler arasında sayılmıştır. Eylem palnında hem ulusal düzeyde hem de uluslararası düzeyde işbirliğinin önemine vurgu yapılmış, siber güvenlik alanında tatbikatların yapılması gerektiği belirtilmiştir. Siber güvenlik konusunda yasal altyapının sağlanması, farkındalık çalışmalarının arttırılması gerektiği belirtilmiştir. Fakat eylem planının gerçekleştirilmesi konusunda herhangi bir bütçe belirtilmemiş ya da ayrılmamış, siber caydırıcılık konuları ile ilgili bir ifadeye rastlanılmamıştır. Eylem planlarının dönem içerisinde gerçekleşenleri ve eksiklikleri konusunda kamuoyuna açıklama yapılmamıştır (Çakır ve Arınmış-Uzun, 2021).

2016-2019 Ulusal Siber Güvenlik Stratejisi kamuoyu ile paylaşılmış ancak eylem planı hizmete özgü kabul edildiği için kamuoyu ile paylaşılmamıştır. Bu nedenle

strateji belgesinin değerlendirilmesini yapmak yerinde olacaktır. Süreklilik bakımından eylem planının gerçekleştirilmesi ile bir yıllık bir boşluk olduğundan dolayı süreklilik kısmını etkilediği söylenebilir. Bu belgede de milli teknolojik ürünlerin korunması, altyapıların korunması gerektiği belirtilmiştir. Araştırma ve geliştirme çalışmalarına ilişkin somut bir amaç bulunmamasına karşın belgede araştırma ve geliştirme çalışmalarının desteklenmesi gerektiği, araştırma ve geliştirme konuları üzerinde vurgu yapılmıştır. Siber güvelik konusunda yetişmiş insan kaynağının önemi üzerinde durulmuş, siber güvenlik eğitimlerinin yaygınlaştırılması gerektiği, farkındalık çalışmaları üzerinde durulmuştur. Bu belgede de bütçe konusuna değinilmemiş olup, siber caydırıcılık konusuna yine yer verilmemiştir. Strateji belgesinde hedeflerin gerçekleşip gerçekleşmeme durumları kamuoyu ile paylaşılmamıştır (Çakır ve Arınmış-Uzun, 2021).

Türkiye gibi çok önemi bir stratejik konumda bulunan bir ülkenin siber güvenlik uygulamaları ve izleyeceği politikaları hayati önem taşımaktadır. Özellikle de 11 Eylül saldırıları ile yeni bir sürece girdiğimiz küresel yapıda, ABD'nin Irak'ı işgal etmesine izin verilmeyen 2003 yılından sonraki dönemde başta ABD olmak üzere birçok ülkenin ve devletlerin saldırılarına daha açık duruma gelen Türkiye'nin bu alanda bağımsız olarak bir politika üretmesi zorunluluk durumuna gelmiştir. Bu politikaların, ülkenin ulusal sistemdeki öncelikleri ve yararları kapsamında ortaya koyacağı ilkeler çerçevesinde dünyadaki diğer ülkeler ile işbirliği ve ilişkileri gerçekleştirebilecek seviyede uygulanması gerekir. Ancak son zamanlarda dünya siyasetinde kullanılan ayrımcı ve ötekileştirici dil ve ülkeleri ulusal menfaatlerine yönelten birtakım nedenler Avrupa'nın karışmasına neden olmuş; ötekileştirici ve ayrıştırıcı dili kullanan kesimlerin ellerini güçlendirmiştir. Bu kapsamda Türkiye'nin siber güvenlik politikalarında önceliklerini ortaya koyması gerekir. Cumhurbaşkanlığı Hükümet Sistemi'nin benimsenmeye başlaması ile devletin birçok mekanizmasında güvenlik ve siber güvenlik alanlarında ciddi fırsatların sunulduğu bir süreç olmuştur. Küresel alanda siyasetin ana konularından olan ülkelerin siber güvenlik saldırılarına uğramaları, siber yöntemler ile işlenen suçlar gibi sanal ortamdaki suç unsurları topyekün bir mücadele ve önleyici bir mekanizmanın geliştirilmesi ile yok edilebilir. Siber suç örgütleri zayıf gördükleri sistemleri hedef aldıkları bilinen gerçektir. Türkiye'nin sistemini de ilişki içerisinde olduğu diğer ülkelere oranla ortalama ya da üzerine geçirebilecek bir noktaya getirilebilirse, bu tür yapılanmaların amaçları yok edilebilir (Kutlu, Kahraman ve Dinçer, 2020).

Güvenlik alanında dikkat edilmesi gereken bir başka husus, samimiyet ve daha gerçekçi politikaların uygulanması bu alanda önemli konular olarak karşımıza

çıkmaktadır. Değişen ve gelişen dünyada ortaya çıkan yenilikler, teknolojik alanda uluslararası aktörlerin saldırı ve savaş taktiklerinin de değişmesine etki etmiştir. Bu husus günümüzde o kadar gelişmiştir ki, siber saldırılar teknolojik ilerlemelere bağlı olarak kapasitesi gelişmiştir. Bu konuda tartşılan ve adının tam olarak konulamadığı husus ise, yaşanılanların tek taraflı bir saldırı mı yoksa savaş mı olduğudur. Bu nedenle ülkelerin siber güvenlik esasları kapsamında siber ortamda istihbarat alanında operasyon yapabilme, operasyonlara karşı koyma yeterliliklerini geliştirme konusunda çabaları artış göstermektedir. Siber güvenlik alanında ülkeler kritik altyapıların korunması konusunda bölge ülkeleri önemli adımlar atmıştır. Siber diplomasi masalarının oluşturulması çalışmaları ülkeler açısından ivme kazanmıştır. Türkiye'de ise ilgili birimler oluşturulmuş, siber tatbikatlar yapılmış. Sadece ülke düzeyinde değil uluslararası kuruluşların da siber güvenlik alanında stratejiler gerçekleştirdikleri görülmektedir (Güntay, 2015).

Türkiye'de 2009 yılında Milli Güvenlik Siyaset Belgesi'nde siber güvenliğe yapılan vurgu dikkat çekmektedir. Siber güvenliğin milli güvenlik unsuru olarak kabul edilmesi siber güvenliğin geliştirilmesi konusunun ne kadar önemli olduğunu ortaya koymuştur. Türkiye belirli süreler ile ulusal siber güvenlik stratejileri ile hazırladıkları belgelerde, hızlı bir şekilde değişen ve ilerleyen teknolojik gelişmelere uyum sağlayacak şekilde amaçlarını yeniden düzenlemektedir. İçinde bulunduğumuz zamanda siber güvensizliğin oluşturacağı karışıklık ve güvensizlik ortamının maliyetinin fazla olması siber savunmaya daha çok yatırım yapılması gerektiğini göstermektedir. Türkiye, siber güvenliği sağlamak için diğer kurum ve kuruluşlar ile multi-disipliner bir bakış açısı ile güvenliğin tesis edilmesi için gayret göstermelidir. Sonuç olarak Türkiye'nin siber güvenlik konusunda farkında olması ve bu konuda gayretlerinin olduğu bilinmektedir. Ancak bu alanda siber güvenlik altyapısının tesis edebilmesi amacıyla bu alanda uzman personellere, bu konuda ilgisi ve bilinci yüksek çalışanlara ihtiyaç duyulmaktadır. Bu konuda yapılan eğitimlerin ve farkındalık çalışmalarının sayıları ve nitelikleri arttırılmalıdır. Türkiye'de şartlara uygun bir şekilde etkili ve verimli internet altyapısının oluşturulması gerekir. Türkiye'de üniversitelerin siber güvenlik alanındaki çalışmaların arttırılması, nitelik bakımından geliştirilmesi gerekir (Turan ve Öcal, 2021).

2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, süreklilik bakımından 2020 yılının sonlarına doğru yayınlanmasından dolayı süreklilik ilkesini olumsuz etkilemiştir. Bu eylem planında kritik altyapılar, kritik kamu hizmetleri belirtilmiş ve bu kritik hizmetlerin korunmasına ilişkin amaçlara yer verilmiştir. Ayrıca diğer eylem planlarındaki gibi araştırma ve geliştirme çalışmalarına, milli teknolojik

unsurların korunup geliştirilmesi gerektiği, lider ülke olma amacına yer verilmiştir. Uluslararası alanda işbirliği çalışmalarına, siber güvenlik alanında işbirliği çalışmalarına, farkındalık çalışmalarına ilişkin amaçlar yer almaktadır. Bu eylem planında yasal altyapının sağlanmasına ilişkin bir amaç bulunmamaktadır. Bu eylem planında da bütçenin tahsis edilmesi konusuna yer verilmemiş, ilk defa siber suçların azaltılmasına yönelik siber caydırıcılığın arttırılması gerektiğinden bahsedilmiştir (Çakır ve Arınmış-Uzun, 2021).

Siber güvenliğin sağlanmasında öncelikli olarak yapılması gereken husus, kullanıcı bilincini artırmaktır. Kullanıcılar ise, bilgi sistemleri az ya da çok ilişkisi olan herkesi tanımlamaktadır. Bilinçlendirme sürekli yapılması gereken bir süreç olarak kabul edilmelidir. Bilinçlendirme faaliyetlerinin belli bir dönem içerisine sıkıştırılmadan yapılması, çalışanların niçin sorularının cevaplarını kendilerinin bulmaları sağlanmalıdır. Sayısal olarak savunmadan kritik altyapıların korunmasına kadar her konuda ulusal bilincin sağlanmasına yönelik ulusal platformlar kullanılarak bilinçlendirme çalışmaları yapılmalıdır (Karabacak, 2011).

Dijital teknolojilerin geniş çapta benimsenmesiyle birlikte, alışveriş ve sosyal etkileşimlerden iş dünyasına, endüstriye ve ne yazık ki suça kadar toplumun birçok yönü çevrimiçi ortama taşınmıştır (Lallie vd., 2021, s.2). Siber saldırılar karşısında alınacak, etkisini en aza indirebilecek yöntemlerden birisi de eğitim konusudur. Bu bağlamda kişisel olarak kendimizi ve kurumsal anlamda çalışanları siber güvenlik alanında eğitmek, güncel bilgiler ile eğitimlerin sağlanması önem kazanmıştır. Kurumlar ve çalışanlar aldıkları bu eğitimler doğrultusunda kurumlarının ve kendilerinin risk değerlendirmesini yapmaları gerekir. Muhtemel saldırılar ve aksaklıklar karşısında uygulanabilecek yedek planların belirlenmesi gerekir. Çünkü alınacak eğitim ve oluşturulabilecek altyapılar uzun dönemde siber saldırıların neden olabileceği zararlardan daha az olacağı muhtemeldir (Demir, 2021).

Bilgi güvenliğini, sistemlerin kurulmasından sonra gerçekleştirilecek basamaklar olarak değil; kurulması aşamasından beri dikkate alınacak önemli bir bileşen olarak değerlendirilmesi gerekir. Ortaya çıkan birçok güvenlik açıklarının nedeni; en baştan tasarlanmadığı ve daha sonradan ekleme çözümler mantığı ile daha sonradan gerçekleştirilmesidir. Güvenlik konusu, sonradan düşünülecek bir bileşen olarak görülmemelidir. Bilgi güvenliği ihlâlleri, yetkisi olmayan kişiler tarafından kullanılmasından kaynaklanmaktadır. Sadece yetkili olan çalışanların işlerini yürütebilecekleri kadar sınırlı düzeyde yetkilendirilmesi, bunun uzman

kişiler tarafından takibinin yapılması güvenliği sağlayacak diğer önemli konudur (Karabacak, 2011).

## YAZARIN BEYANI

**Katkı Oranı Beyanı:** Yazar çalışmaya tek başına katkı sağlamıştır.

**Destek ve Teşekkür Beyanı:** Çalışmada herhangi bir kurum ya da kuruluştan destek alınmamıştır.

**Çatışma Beyanı:** Çalışmada herhangi bir potansiyel çıkar çatışması söz konusu değildir.

## 6.SONUÇ

İnternetin 1990'lı yılların başlarında hızlı bir şekilde kullanılmasının yaygın hâle gelmesi güvenlik konusunu, bilgilerin güvenliğinin sağlanması konusunu öne çıkarmıştır. Uluslararası sitemde ağ teknolojileri konusu önemli bir rekabet ortamına dönüştürülmüştür. Her şeyin internete bağlı olduğu, internetin insanların, kurumların, ülkelerin en önemli unsurları haline gelmeleri bu noktada bazı çevreleri harekete geçirmiştir. Teknolojinin insanlara, ülkelere, kurumlara sınırsız sayıda sunduğu imkânların yanı sıra olumsuz durumda etkilenmelerini de beraberinde getirmiştir. Ülkeler için önemli olan ulusal güvenlik konusu siber güvenlik konusunu gündeme getirmiştir.

Siber güvenlik, teknolojinin kullanılmasıyla verilere kolayca erişilmesi, kullanılması, gizli bilgilere ulaşılması, kritik altyapılara ulaşılması gibi birçok unsuru içinde barındırmaktadır. Bu nedenle sadece bir insandan, bir kuruma, bir ülkeye etki edecek seviyeye ulaşmıştır. Son zamanlarda özellikle pandemi dönemini de içine katacak olursak teknolojinin gelişmesi ile esnek çalışma, uzaktan çalışma dönemlerinin de gündeme gelmesi ile kurumların bu konuya daha fazla önem vermelerini zorunlu hâle getirmiştir. Bu nedenle ülkeler siber saldırılarla mücadele edebilmek için farklı sayıda ve nitelikte politikalar üretmişler, strateji geliştirmişlerdir. Ülkemizde de bu konuda son zamanlarda çalışmaların yapıldığını söylemek mükündür.

Türkiye'de siber güvenlik konusunun kurumsallaşması, bu konuda politikaların üretilmesi 2010'lı yılların başına rastlamaktadır. Bu dönemden sonra siber

güvenlik alanında kurumsallaşmanın olduğu söylenebilir. 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. 2013 yılında Ulusal Siber Güvenlik Stratejisi ve 2013- 2014 Eylem Planı hazırlanmıştır. Daha sonraki süreçlerde 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ve 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 geliştirilmesi, 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.

Siber güvenlik konusunda kurumların desteklerinin alınması ve geliştirilmesi için araştırma ve geliştirme faaliyetlerine gerekli özenin gösterilmesi gerekir. Kurumların kendisinden beklenilen araştırma ve geliştirme faaliyetlerini etkili bir şekilde yerine getirebilmesi için ilgili kurumların bu alana yönelik ayrı bir bütçenin ayrılması gerekir, ayrılan bütçenin bu alanda kullanılması özendirilmelidir.

Siber güvenlik konusuna bütüncül bir bakış açısı ile yaklaşılmalıdır. Ulusal ve uluslararası düzeyde liderliğin sağlanması için etkili işbirliği ve koordinasyonun sağlanması gerekir. Ulusal düzeydeki bütün paydaşların katılımını sağlayacak şekilde takım çalışmaları yapılabilir.

Siber güvenlik konusunda yasal altyapının güçlendirilmesi gerekir. Özellikle siber saldırılara karşı etkili bir şekilde mücadele edebilmek için siber caydırıcılık konusu ele alınmalıdır. Siber güvenlik konusunda uygulanan bütün politikaların, stratejilerin uygulanma durumları hakkında kamuoyu ile paylaşılmalıdır. Gerekirse vatandaşların desteklerinin alınması gerekir. Siber güvenliğin sağlanmasında öncelikli koşul olan vatandaşların devlete ve kurumlarına olan güvenlerinin sağlanmasından hareket ederek etkili iletişim kanalları kurulmalıdır. Vatandaşların görüşlerini ve düşüncelerini paylaşabilecekleri bir ortam oluşturulmalıdır. Özelikle gençlerin bu konuda proje ve öneri geliştirmelerini destekleyecek yarışmalar, sempozyumlar, paneller düzenlenmelidir. Gençlerin bu

konuda geliştirecekleri projelerin önemli olacağı hususu göz önünde bulundurularak gençlere özgü projelerin geliştirilmesi gerekir.

Bilginin güvenliğinin sağlanması konusunda kurumların bilişim altyapılarının güçlendirilmesi, bu konuda alanında uzman kişilerin yetiştirilmesi, güvenlik konusunda bir kişinin sınırlı yetkilerle donatılması bilgi güvenliği konusunda açıkların oluşmasını engelleyecektir.

## KAYNAKÇA

Afad Hakkında, Afad ve tarihçesi, https://www.afad.gov.tr/afad-hakkinda [İndirme Tarihi: 24.02.2022].

Aldemir, C., & Kaya, M. "Bilgi Toplumu, Siber Güvenlik ve Türkiye Uygulamaları", Kamu Yönetimi ve Politikaları Dergisi, 1 (1), 2020, 6-27.

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

Atakan, M., "Siber Güvenlik Risklerinin Ve Covıd-19 Salgınının Uzaktan Denetim Üzerindeki Etkileri", Denetişim Dergisi, 11(2), 2021.

Berman, D. S.; Buczak, A. L.; Chavis, J. S & Corbett, C. L., "A Survey Of Deep Learning Methods For Cyber Security", Information 2019, 10, 2019, 122, Doi:10.3390/İnfo10040122.

Biz Kimiz?, Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (Tubitak.Gov.Tr), [İndirme Tarihi: 24.02.2022].

BTK, Mevzuat. https://www.btk.gov.tr/siber-guvenlik-mevzuat, [İndirme Tarihi: 17.03.2022].

Craigen, D.; Diakun-Thibault, N.& Purse, R. (2014). Defining cybersecurity. technology ınnovation management review, https://Www.Timreview.Ca/Sites/Default/Files/Article_Pdf/Craigen_Et_Al_Tımreview_October2014.Pdf, 2014, [İndirme Tarihi: 01.03.2022].

Çakır, H. & Arınmış Uzun, S., "Türkiye'nin Siber Güvenlik Eylem Planlarının Değerlendirilmesi", Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi, 7(2), 2021, 353-379.

Daban, C., "Siber Güvenlik ve Uluslararası Güvenlik İlişkisi", Cyberpolitik Journal, 1(1), Www.Cyberpolitikjournal.Org, 2016.

Darıcılı, A. B., "Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Potansiyel Siber Güvenlik Stratejisi", Tesam Akademi Dergisi, Temmuz, 6(2), 2019, 11-33 Issn: 2148 - 2462 E-Issn: 2458 – 9217.

Demir, Ü., "Uluslararası Güvenlik Açısından Ülkemizdeki Bilgi Güvenliği Ve Siber Güvenlik Eğitimlerinin Mevcut Durumunun İncelenmesi*",* İstanbul Rumeli Üniversitesi Uluslararası Güvenlik Sempozyumu Çevrimiçi/Online 25-26 Mart 2021, 2021, Isbn - 978-605-69205-5-4.

Demircioğlu, C., "Siber Uzayda Güç Ve Güvenlik", İdarecinin Sesi Dergisi, MartNisan,http://www.tid.web.tr/ortak_icerik/tid.web/160/8%20Cemalettin%20DEM%C4%B0RC%C4%B0O%C4%9ELU.pdf, 2014, [İndirme Tarihi: 09.03.2022].

Elmaghraby, A. S. & Losavio, M. M., "Cyber Security Challenges İn Smart Cities: Safety, Security and Privacy", Journal of Advanced Research, 5(4), 2014, 491-497

Global Cybersecurity Index, https://Www.İtu.İnt/En/Itu-D/Cybersecurity/Pages/Global-Cybersecurity-İndex.Aspx, 2021, [İndirme Tarihi: 25.02.2022].

Global Cybersecurity Index (2018), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf, 2018, [İndirme Tarihi: 22.03.2022].

Global Cybersecurity Index (2017), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf, 2017, [İndirme Tarihi: 23.03.2022].

Göçoğlu, V. & Aydın, M. D., "Siber Güvenlik Politikası: Abd, Rusya Ve Çin Üzerine Karşılaştırmalı Bir Analiz", Güvenlik Bilimleri Dergisi, 8(2), 2019, 229-252, Doı:10.28956/Gbd.646311.

Güleç, Ö. & Kişman, Z. A., "Uluslararası İlişkiler Açısından Siber Güvenlik Ve Nato'nun Siber Güvenlik Stratejileri", Akademik Açı, 1(1), 2021, 127-154,

Gündüz, M. Z. & Daş, R., "Akıllı şebekelerde iletişim altyapısı ve siber güvenlik", Iğdır Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 10(2), 2020, 970-984.

Güngör, M., "Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma", Bilgi Toplumu Dairesi Başkanlığı, Uzmanlık Tezi, Yayın No: 2919, 2015.

Güntay, V., "Uluslararası İlişkiler Bağlamında Güvenlik Algısı Ve Siber Güvenlik; Akdeniz, Karadeniz Ve Avrupa Bölgeleri Üzerine Bir Değerlendirme", The Journal Of Academic Social Science Studies, No 37, Autumn I, 2015.

Güntay, V., "Uluslararası Sistem Ve Güvenlik Açısından Değişen Savaş Kurgusu; Siber Savaş Örneği", Güvenlik Bilimleri Dergisi, 6 (2), 2017, 81-108.

Güreşci, R., "Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirmesi", The Journal of Defense Sciences, 18(1), 2019, ISSN (Basılı) : 1303-6831 ISSN (Online): 2148-1776.

International Telecommunications Union (Itu). (2008). Serıes X: Data Networks, Open System Communıcatıons And Securıty Telecommunication Security. Https://Www.İtu.İnt › Rec › Dologin_Pub › İd=T-R..., [İndirme Tarihi: 01.03.2022].

İnce, E., "Covid-19 Pandemisinin Türkiye Turizm Sektörüne Olan Etkilerinin Uluslararası Güvenlik Bağlamında Değerlendirilmesi", İstanbul Rumeli Üniversitesi Uluslararası Güvenlik Sempozyumu Çevrimiçi/Online 25-26 Mart 2021, 2021, Isbn - 978-605-69205-5-4.

Karabacak, B., "Kritik Altyapılara Yönelik Siber Tehditler Ve Türkiye İçin Siber Güvenlik Önerileri", Siber Güvenlik Çalıştayı, Bilgi Güvenliği Derneği, Ankara, 2011.

Karasoy, H. A. & Babaoğlu, P., "Türkiye'de Siber Güvenlik: Yasal Ve Kurumsal Altyapı", Yasama Dergisi, Sayı: 44, 2021.

Kazel, G. İ., "Soğuk Savaş Sonrasından Günümüze ABD Ulusal Güvenlik Strateji Belgelerinde Türkiye", İstanbul Rumeli Üniversitesi Uluslararası Güvenlik Sempozyumu Çevrimiçi/Online 25-26 Mart 2021 ,2021, Isbn - 978-605-69205-5-4

Kılcı, H. B., "Türkiye'nin Siber Güvenlik Politikaları", Cyberpolitik Journal, 5(9), 2020, www.cyberpolitikjournal.org.

Korucu, O., "Yeni Normal Dünya Düzeninin Siber Güvenlik Ve Bilgi Güvenliğine Etkileri", Yönetim Bilişim Sistemleri Dergisi, 7(1), 2021, 44-60, Issn: 2148-3752.

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

Küçükşahin, A. , Uyar, E. Ö. , Tahminciler, E. & Dinçer, D., "Türkiye'nin güvenlik strateji belgesi nasıl hazırlanmalıdır", Güvenlik Stratejileri Dergisi, 4(7), 2008, https://Dergipark.Org.Tr/Tr/Pub/Guvenlikstrtj/İssue/7536/99212.

Lallie, H. S.; Shepherd, Lynsay A. ; Nurse, J. R.C.; Erola, A.; Epiphaniou, G.; Maple, C. & Bellekens, X. (2021). Cyber Security İn The Age Of Covıd-19: A Timeline And Analysis Of Cyber-Crime And Cyber-Attacks During The

Pandemic, 2021, https://Doi.Org/10.1016/J.Cose.2021.102248, [İndirme Tarihi: 23.03.2022].

Maglaras, L. A., Kim K-H., Janicke, H., Amine, M. F., Rallis, S., Fragkou, P., Maglaras, A. & Cruz, T. J., "Cyber Security Of Critical İnfrastructures", CT Express, 4, 2018, 42–45.

Nguyen,T. T. & Reddi, V. J., "Deep Reinforcement Learning For Cyber Security" *IEEE Transactions On Neural Networks And Learning Systems,* 2021, doi: 10.1109/TNNLS.2021.3121870.

Özalp, A. N. & Asker, A., "Devletin Güvenlik Politikalarında Siber İstihbaratın Rolü Ve Önemi. Akademik Bilişim Konferansları", 2017, https://www.researchgate.net/publication/331998875_Devletin_Guvenlik_Politikalarinda_Siber_Istihbaratin_Rolu_ve_Onemi/citations#fullTextFileContent.

Özdemirci, F. & Torunlar, M., "Bilgi-Değişim-Siber Güvenlik-Bağımsızlık", Bilgi Yönetimi Dergisi, İnceleme Yazıları, 1(1), 2018.

Solms, R. V. & Niekerk, J. V., "From İnformation Security To Cyber Security", Computers & Security, Volume 38, 2013, 97-102.

Şenol, M., "Türkiye'de Siber Saldırılara Karşı Caydırıcılık", Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 3(2), 2017, 1-9.

Tamyapar, B., "Siber Güvenlik Ve Türkiye'de Yürütülen Siber Güvenlik Çalışmaları", Https://www.researchgate.net/profile/Berkay-Tamyapar, 2009, [İndirme Tarihi: 22.03.2022].

Thakur, K., Qiu, M., Gai, K. & Ali, M. L., "An Investigation On Cyber Security Threats And Security Models", IEEE 2nd International Conference on Cyber Security and Cloud Computing, 2015, 307-311, doi: 10.1109/CSCloud.2015.71.

Topcu, N., "Siber Güvenlik: Tehditler Ve Çözüm Yolları", Cyberpolitik Journal, 6(12), 2021, www.cyberpolitikjournal.org.

Turan, S. & Öcal, A., "Siber Güvenlik Perspektifinde Türkiye'nin Güvenlik Stratejileri", İstanbul Rumeli Üniversitesi Uluslararası Güvenlik Sempozyumu Çevrimiçi/Online 25-26 Mart 2021, Isbn - 978-605-69205-5-4.

Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi Ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı, 2021, https://Www.Resmigazete.Gov.Tr/Eskiler/2012/10/20121020-18.Htm, [İndirme Tarihi: 24.03.2022].

Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı, 2022,

https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf, [İndirme Tarihi: 22.03.2022].

Ünver, M.; Canbay, C. & Mirzaoğlu, A. G., "Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum Ve Alınması Gereken Tedbirler", Bilgi Teknolojileri ve İletişim Kurumu, 2011, ISBN: 978-9944-0189-6-8.

Ünver, M. & Canbay, C., "Ulusal Ve Uluslararası Boyutlarıyla Siber Güvenlik", Elektrik Mühendisliği Dergisi, Sayı 438, 2010.

Yanarışık, O., "İç Güvenlik Ve Siber Güvenlik. İç Güvenlik Yönetimi Ve Polislik", Derleyen, İbrahim İrdem, Polis Akademisi Yayınları: 111, 2020.

Yılmaz, S., "Türkiye'nin İç Güvenlik Yapılanmasında Değişim İhtiyacı", Ç.Ü. Sosyal Bilimler Enstitüsü Dergisi, 21(3), 2012, 17-40.

Yılmaz, E. N.; Ulus, H. İ. & Gönen, S., "Bilgi Toplumuna Geçiş Ve Siber Güvenlik", Bilişim Teknolojileri Dergisi, 8(3), 2015.

2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi, Https://Afyonluoglu.Org/Publicwebfiles/Reports-Tr-Sg/2014-2023-Afad-Kritik%20altyap%C4%B1larin%20korunmasi%20yol%20haritasi.Pdf, [İndirme Tarihi: 24.02.2022].

1 Sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, Https://Cbddo.Gov.Tr/Hizmet-Birimlerimiz/Siber-Guvenlik-Dairesi-Baskanligi/, [İndirme Tarihi: 24.02.2022].