Türkiye'nin Siber Güvenlik Eylem Planlarının Değerlendirilmesi
Evaluation of Turkey's Action Plan for Cyber Security

Hüseyin ÇAKIR [*] Sündüs ARINMIŞ UZUN [**]

Makale Geliş Tarihi / Received :09.10.2021
Makale Kabul Tarihi / Accepted :19.11.2021

ÖZET

Bu çalışmanın amacı, Türkiye'nin 2013-2014, 2016-2019 ve 2020-2023 dönemlerini kapsayan eylem planlarının incelenmesi ve belirlenen on bir kriter açısından değerlendirilmesidir. Değerlendirme kriterlerinin siber güvenlik alanında yayımlanan tezlerden, Avrupa Birliği ülkelerinin siber güvenlik eylem planlarından ve Avrupa Birliği Siber Güvenlik Ajansı dokümanlarında yararlanılarak belirlenmiştir. Elde edilen sonuçlara göre Türkiye'nin siber güvenlik eylem planlarının pek çok kritere uyum sağladığı ancak özellikle eylem planlarının sürekliliği, eylem planlarına bütçe ayrılması, eylem planlarındaki hedeflerin takibi, insan kaynağının geliştirilmesi ve siber caydırıcılık konularında eksikliklerin olduğu tespit edilmiştir. Gelecek eylem planlarında sürekliliğin sağlanması, planlardaki hedeflere ulaşılması için belirli bir bütçe tahsis edilmesi, belirlenen hedeflere ne derece ulaşıldığının dönemsel olarak açıklanması, siber saldırıları başlamadan önce engellemek için özellikle caydırıcılık konusuna yatırım yapılması ve başarısının en önemli kriteri olan yetişmiş insan gücüne daha fazla ağırlık verilmesi önerilmektedir.

Anahtar Kavramlar: *Siber Güvenlik, Siber Güvenlik Eylem Planı, Türkiye'nin Siber Güvenlik Eylem Planı.*

ABSTRACT

The purpose of this study is to examine Turkey's action plans covering the 2013-2014, 2016-2019 and 2020-2023 periods and to evaluate them in terms of eleven criteria. The evaluation criteria are determined by using the theses published in the field of cyber security, the cyber security action plans of the European Union countries and the documents of the European Union Cyber Security Agency. According to the results, it has been determined that Turkey's cyber security action plans comply with many criteria, but there are deficiencies in the subjects of continuity of action plans, allocation of budget to action plans, tracking of targets in action plans, development of human resources and cyber deterrence. It is recommended to ensure continuity in future action plans, to allocate a certain budget to achieve the targets in the plans, to periodically explain the extent to which the specified targets have been achieved, to invest especially in deterrence to prevent cyber attacks before they start, and to focus more on trained manpower, which is the most important criterion of its success.

Keywords:. *Cyber Security, Cyber Security Action Plan, Turkey's Cyber Security Action Plan*

[*] *Doç. Dr., Gazi Üniversitesi Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı hcakir@gazi.edu.tr,* ***ORCID No:*** *0000-0001-9424-2323*

[**] *Yüksek Lisans Öğrencisi, Gazi Üniversitesi Bilişim Enstitüsü Adli Bilişim Anabilim Dalı sundus.arinmis@hotmail.com,* ***ORCID No:****0000-0001-9707-4791*

GİRİŞ

Siber güvenlik kavramı, son yirmi yılın en hızlı yükselen ve üzerinde çalışma yapılan konularından biri haline gelmiştir. Siber güvenlik olgusunun ilk incelenmesi gereken bileşeni güvenliktir. Güvenlik insanın en temel ihtiyaçlarından birisi olup tam anlamıyla karşılanmadığı zaman gelişme, araştırma ve ilerleme aşamalarına geçilemez. Bu açıdan siber güvenliğin sağlanması ile bilgi ve iletişim sağlıklı bir şekilde işleyebilir, altyapı tesisleri sorunsuz bir şekilde çalışabilir, ekonomik ve sosyal hayatın akışında herhangi bir kopma meydana gelmez.

Teknolojinin gelişmesi ve yaygın kullanımının bir sonucu olarak siber güvenlik ile birlikte siber uzay, siber suç, siber saldırı, siber terörizm, siber hacktivizm, siber sabotaj gibi pek çok kavram günlük kullanıma girmiştir. Bu kavramların kullanımı arttıkça aralarındaki ayrım ve farklılıklar unutulmakta ve kavram karmaşası ortaya çıkmaktadır. Bir suçun siber alana ait olup olmadığı veya siber terörizm ile siber saldırı arasında ayrımın nasıl yapılacağı sürekli bir tartışma konusu haline gelmiştir. Bunların yanı sıra kavramın yeni olması, literatürde çok farklı çalışmalara konu olması tam olarak anlamını ve tanımlamasını güçleştirmektedir.

Siber saldırılara, terörizme veya sabotajlar kurumlara, devletlere veya tesislere büyük zararlar verebilmekte, çalışamaz hale getirmekte, bilgilerin çalınmasına neden olabilmekte ve iletişimi sekteye uğratabilmektedir. Kurumların ve sistemlerin bağlantılı yapısından dolayı bir yerde meydana gelen bir zafiyeti kullanarak gerçekleşen saldırı tüm sisteme yayılabilmekte ve zarar verebilmektedir. İnsan unsuruna aşırı bağlılık siber açıklıkların sömürülmesini daha da artırmaktadır. Böyle durumlarla karşılaşmamak için güçlü siber güvenlik altyapısının kurulması, insan kaynağı farkındalığının yüksek olması, beşeri sermayenin gücü sürekli olarak artırılmalıdır. Bunun sağlanması için devletler planlar hazırlamakta ve bu planlara göre yeterlilik seviyelerini sürekli olarak yükseltmektedir.

Türkiye siber güvenlik alanındaki gelişmeleri inceleyerek 2013-2014, 2016-2019 ve 2020-2023 dönemlerini kapsayan strateji belgeleri eylem planları hazırlamıştır. Eylem planlarının takibi ve koordinasyonu için 2012 yılında Siber Güvenlik Kurulu oluşturulmuştur. Zamanla mevzuatın eski kalması ve yürütme modelinin değişmesi yapının değişmesine neden olmuştur. Bu çalışmanın amacı eylem planlarının belirlenen on bir kriter açısından değerlendirilmesidir.

Çalışmada giriş bölümünden sonraki ikinci kısmında güvenlik ve siber güvenlik kavramının tanımlanması yapılacak ve siber saldırı teknikleri incelenecektir. Değerleme kriterlerinin belirlenmesi Avrupa Birliği ve İngiltere'nin siber güvenlik eylem planları, dokümanları ve The European Union Agency for Cybersecurity (Avrupa Ağ ve Bilgi Güvenliği Ajansı/ ENISA) yayımlarından yararlanılmıştır. Çalışmanın üçüncü bölümünde Türkiye'nin Siber Güvenlik Kurulu, 2013-2014, 2016-2019 ve 2020-2023 dönemlerini kapsayan strateji belgeleri eylem planları detaylı bir şekilde ele alınmıştır. Daha sonra belirlenen kriterlere göre eylem planlarının analizi yapılmış ve sonuç bölümünde çalışmanın genel özeti ile öneriler açıklanmıştır.

2. GÜVENLİK VE SİBER GÜVENLİK KAVRAMI

Bu bölümde öncelikle güvenlik kavramı açıklanacak, daha sonra siber güvenlik kavramı ve siber güvenlik kavramının bileşenleri ele alınacaktır. Kavramın oldukça geniş bir anlamı olduğu için siber terör, siber savaş, siber espiyonaj gibi güncel tanılamalar da açıklanacaktır.

2.1. Güvenlik ve Ulusal Güvenlik

Güvenlik olgusu hayatın başlangıcı kadar eski olmasına rağmen bilimsel olarak ele alınması ve alanda özel olarak çalışma yapılması oldukça yenidir. İlk olarak uluslararası ilişkiler alanının çalışma konusu olan güvenlik kavramı zamanla diğer disiplinlerin de inceleme konularından birisi haline dönüşmüştür. (Güvenlik, 2003:11-12). Akademik olarak İkinci Dünya Savaşı'ndan sonra ortaya konulmaya başlanan çalışmalar zamanla daha spesifik alanlara yayılmış ve özündeki realist yaklaşımı sürekli olarak korumuştur. (Yılmaz, 2007:67-103). Bu kapsamda hem devletler hem de uluslararası organizasyonlar geniş anlamda güvenliği baz alan kamu politikaları oluşturmaktadır. (Terriff, Croft, vd., 1999)

Güvenlik olgusu dönemsel olarak çağın koşullarından etkilenerek farklı şekillerde tanımlanmıştır. Tanımı zamana, kişiden kişiye, gruptan gruba, devletten devlete farklı olup "*esası tartışılan*" bir kavram haline gelmiştir. (Barry, 1998). Güvenlik, yaşamın başlangıcında tek bir insandan başlayarak aile, kabile, toplum ve devlet gibi sosyal örgütlenme biçimlerine kadar genişlemiş bir kavramdır. Abraham Maslow'un insan ihtiyaç hiyerarşileri içerisinde güvenlik ihtiyacı hususu, yeme ve barınmadan sonra ikinci önemli basamak olarak görülmüştür. (Aydın, 2008:8-17).

Geleneksel güvenlik anlayışı, askeri bir yapıya sahip olup askeri güvenliği meşru bir gösterge olarak kabul etmektedir. Bu yüzden, klasik yaklaşıma göre güvenlik, ülkeler arası rekabet, çekişme ve en nihayetinde savaş durumuyla ile yakından ilgilidir. Askerî tehdit unsurları, sabotajlar, bilgi hırsızlıkları gibi konular klasik güvenlik yaklaşımının ana eksenini oluşturmaktadır. Doğrudan fiziksel güvenliğe vurgu yapılan geleneksel yani klasik güvenlik yaklaşımına göre, ulusal güvenliğin en belirgin unsuru ulusal devlet sınırlarının saldırgan ve genel olarak diğer devletlerin tecavüzünden korunmasıdır. Bu kapsamda, güvenliğe ilişkin geleneksel yaklaşımı, salt askerî kuvvetlerin kontrol edilmesi, doğrudan kullanılması ve tehdit unsuru olarak ele alınması çerçevesinde kullanılmaktadır. (Miller, 2001: 16-17).

Günümüzde güvenliğin boyutları değişime uğramış ve askerî boyutu da içine almasına rağmen onu oldukça aşan yeni bir güvenlik yaklaşımı ortaya çıkmıştır. (Krause, Wıllıams, 1996: 229-254). Küreselleşmenin, teknolojik ilerlemelerin ve insan, mal ve bilgi hareketliliğindeki büyük artışın getirdiği karşılıklı bağımlı ve bağlantılı uluslararası toplum, dünyanın işleyiş şeklini büyük oranda değişime uğratmıştır. Ulusal ve coğrafi sınırların giderek belirsizleştiği uluslararası ortamda güvenlik arayışları ve tehdit algılamaları da böylece büyük bir dönüşüm geçirmiştir. Ülke sınırlarının, sınır ötesi sorunların dışarısında tutulabilmesi giderek ortadan kalkmış ve bölgesel veya ulusal ölçekte yaşanan bir güvenlik sorunu diğer ülkelerin, global güçlerin veya uluslararası örgütlerin alanı haline dönüştürmektedir. Bu yüzen modern dünyada "*ülkesel tehditler*" tanımlanamaz bir hale gelmiş ve ülkeler ile güvenlik stratejilerini istikrarsız bir hale dönüştürmüştür. (Ağır, 2015:97-130).

Güvenlik, tanım olarak korku, tehlike ve tehditlerden kendini kurtarma veya özgür hissetme hali olarak tanımlanmıştır. Bu tanımdan güvenliğin fiziksel ve özellikle psikolojik boyutu olduğu, bunun yanı sıra gerek sübjektif gerekse objektif değerlendirmelere açık olduğu görülmektedir. Bu yönüyle kavram zihinsel ve fiziksel süreçlere vurgu yapılan kişiden kişiye değişmeye açık bir yapı olarak ortaya çıkmaktadır. (Ak, Duru, 2013). Güvenlik olgusu insanlığın gelişimini yönlendiren

stratejik bir yapıya sahiptir. Tarihin her bir döneminde güvenliğin sağlanması ve korunması konusu tartışılmış olup, toplumun ekonomik, sosyal ve aynı zamanda siyasal gelişim düzeyleriyle orantılı olarak değişim göstermiştir. Zamanla kavram evrim geçirmiş ve modern zamanlardaki biçimine kavuşmuştur. Güvenlik ve güvenlik örgütlerinin tarihi tüm milletlerin ve devletlerin geçtiği tarihsel gelişim yoluyla sıkı bir bağı bulunduğu gerçeğinden yola çıkılarak alanın öğrenilmesi tarih eğitiminin en önemli konularındandır.

Güvenlik kavramının bir yansıması olan "*ulusal güvenlik*" olgusunun kökeni tarihin en derinliklerine kadar uzanmaktadır. İlk kez tanımlanması ise ABD Başkanı Ruzvelt'in ABD Kongresine göndermiş olduğu 1904 tarihli resmi mektupta geçmektedir. Ancak, bununla birlikte tarihten bellidir ki, güvenliğin sağlanması ve özelinde ulusal güvenlik meselesi sistematik bir görev olarak ilk kez Asya kıtasında ortaya çıkmıştır. (Oğuzlu, 2007:1-35). Ulusal güvenliğin geçmişi siber güvenlik kavramının ortaya çıkmasından çok daha önce ele alınmış ve incelenmiştir. Siber güvenliğin bir yansıması olarak bilgi güvenliği ve iletişim güvenliği konuları ise güvenlik veya ulusal güvenlik ile yakın bir ilişkiye ve geçmişe sahiptir. Ulusal siber güvenlik stratejisinin geliştirilmesine etki eden en önemli gerekçe ulusal varlıkları, ekonomiyi ve toplumsal değerleri güvence altına alma ve koruma yaklaşımıdır.(Waltz, 2010:19).

Bir ülkenin ve yurttaşlarının her türlü güvenliğinin sağlanması anlamına gelen ulusal güvenlik kavramı, bu tanımlamadan ötürü basitliği aldatıcı olmamalıdır. Çünkü ulusal güvenlik kavramının, birçok bilimsel disiplin ile sıkı bir ilişkisinin olması ve uluslararası ilişkiler, siyaset, ekonomi, strateji, hukuk, savaş gibi bilim dallarını içinde barındırması kavramın çok daha zor anlaşılır olmasına neden olmaktadır. Ulusal güvenlik; "*Devletin bekasının ve refahının sağlanması, bunlara yönelik tehdit ve risklere karşı gerekli tedbirlerin alınması, ortak kimlik ve değerlerin korunması suretiyle ulusal çıkarların gerçekleştirilmesi halidir*" şeklinde tanımlanabilir. (Varlık, 2015:15-17).

Genel olarak ulusal güvenlik; devletlerin zararlı veya yıkıcı tehditlerden uzak kalmaya çalışma özgürlüğü olarak değerlendirilebilir. Bu yönüyle ulusal güvenlik kavramı ulus devletlerinin güvenlik endişelerini açıklamak için kullanılmaktadır. Devletin yararına veya çıkarına olan bir unsur güvenliği artırıcı özelliğe sahipken devletin güvenliğini tehlikeye atan her bir unsur istenmeyen bir yapı arz etmektedir. Ulusal güvenlik kavramı ekonomik, askeri, politik, sosyal, teknolojik unsurlarının tamamını bünyesinde barındırmaktadır. Her ne kadar ulusal güvenlik unsurları birbirlerinden ayrı tehditler olarak ele alınıp incelense de birbirilerinden bağımsız olmayan unsurlardır. (Erhan, 2002).

Özellikle II. Dünya Savaşından sonra başlayan ve büyük ilerlemesini 20. yüzyılının sonlarına doğru gösteren iletişim teknolojisi hem devletleri ve örgütleri hem de insanları pek çok alanda birbirine yakınlaştırarak tarafların karşılıklı olarak birbirlerine bağlı hale gelmesine neden olmuştur. Böylece adına küreselleşme denilen durum diğer pek çok alanda olduğu gibi güvenlik alanında da değişim rüzgarını hissettirmiştir. Söz konusu yeni dönemde ulusal güvenlikle diğer güvenlik alanları arasındaki ayrım büyük oranda ortadan kalkmıştır. Ayrıca değişen ve çeşitlenen tehdit unsurları güvenlik kavramının içeriğini değiştirmiş ve sınırlarını hem genişletmiş hem de muğlaklaştırmıştır. Çevre sorunları, insan hakları, kitlesel göçler, mikro milliyetçilik, etnik çatışmalar, köktendincilik, uluslararası terörizm, ekonomik sorunlar, uyuşturucu ve silâh kaçakçılığı, bulaşıcı hastalıklar, insan ticareti, siber saldırılar gibi tehdit unsurları uluslararası güvenliğin ilgi alanına dâhil olmuştur.(Koçer, 2004:101-122).

2.2. Siber Güvenlik ve Bileşenleri

Siber kelimesi, dil bilimsel açıdan bilgisayar veya bilgisayar ağlarıyla ilişkili bir kavram olup sanal varlıkları tanımlamak için kullanılan bir terimdir. Literatürde çoğunlukla kullanılan siber uzay (cyber space) kelimesi de birbiriyle bağlantılı donanım, yazılım, sistem ve insanların iletişim veya etkileşimde bulundukları soyut veya somut alanı tanımlamak için kullanılmaktadır. (Klimburg, 2012). Bu açıdan benzer durum ve konuları tanımlamak için kullanıldığını söylemek mümkündür.

Dil bilimi açısından siber olarak ifade edilen kelime İngilizcedeki anlamı "*cyber*" kelimesine referans gösterilerek "*bilgisayar ağlarına ait olan*", "*internete ait olan*", "*sanal gerçeklik*" manalarında da kullanılmaktadır. Modern dünyada bilişim ve iletişim ağlarının oluşturduğu uzayı tanımlamakta olan siber kavramı oldukça karmaşık bir yapıya sahiptir. (Kahn, McConnell, 2011). Ayrıca, sibernetik kelimesi siber kelimesinden türeyerek, ilk olarak Norbert Wiener'in "*Sibernetik*" isimli eserinde, "*hayvanlarda ve makinelerde kontrol ve iletişim*" olarak tarif edilmiştir. (Wiener, 1965). Böylece kavramların iç içe geçtiği ve birbirlerinin yerine kullanıldığı daha net bir şekilde anlaşılmaktadır.

Siber güvenlik kavramı üzerinde literatürde geniş bir fikir birliğine varılamamıştır. Genel olarak kavram daha çok bilgi güvenliği (*information security*) veya bilgisayar güvenliği (*computer security*) kavramlarıyla tanımlansa da bundan daha büyük bir yapıyı ifade etmektedir. Bilgi güvenliği olgusu kişisel, kurumsal veya devletin sahip olduğu verilerin korunması ile ilişkili bir kavramken bilgisayar güvenliği olgusu daha çok kullanılan bilişim sistemlerinin güvenliğini içine alan bir yapıyı ifade etmektedir. Siber güvenlik olgusunun tanımı bilişim sistemlerinin temeli olarak kabul edilen bilgi ve bilginin korunması kapsamında yapılmaktadır. Bu açıdan siber uzayın veya siber hayatın güvenli bir şekilde akıp gidebilmesi bilgiye dair üç temel kriterin sağlanmasıyla mümkündür. Bilginin gizliliği (*confidentiality*), bütünlüğü (*integrity*) ve erişilebilirliği (*availability*) siber güvenlik kavramının ana unsurları olarak öne çıkmaktadır (Goodrich, Tamassia, 2011). Bu üç unsuru siber güvenliğin ana amaçları ve değişkenleri olarak ele almak mümkündür.

Siber güvenlik; kurum, kuruluş ve kullanıcıların özellikle bilgileri dahil tüm varlıklarına karşı siber uzayda yer alan güvenlik tehditlerine karşı korumak amacıyla kullanılacak araçlar, güvenlik teminatları, politikalar, kılavuzlar, risk yönetim yaklaşımları, eğitim ve teknolojiler ile bu kapsamdaki faaliyetlerin bütününü kapsayan bir kavram olarak tanımlanabilir. (Ünver, Canbay, vd., 2018). Bu açıdan kavram, 2000 yılından sonra yaygınlaşan ve tehditleri azaltma konusunda stratejik bir bakış açısına sahip olan yeni bir terimdir. Bilgi devriminde ilk olarak ele alınan güvenlik kavramı olarak kabul edilmektedir. Ancak zamanla daha kapsamlı bir kavram olan bilgi güvenliği terimi yaygınlık kazanmıştır. Siber güvenlik aşağıdaki gibi açıklanabilir: (Evans, 2011: 1-11).

- Bilgi ve iletişim sistemleri ile her türlü bilgiyi içeren veya işleyen süreçlerin herhangi bir zarar, anormal işlem, sömürüden korunma önlemleri, faaliyetleri, süreçleri, yetenekleri veya diğer durumları ifade eder. Bu, siber güvenliğin teknik kaynağı ile ilişkilidir.

- Siber alanın güvenliğini artıran strateji, politika, ilkeler, standartlar ve mevzuatı ifade eder. Çeşitli araçların uygulanması ile tehdit ve kırılganlığın azaltılması, caydırıcılık, uluslararası katılım, esneklik konularını içeren; güvenli bir küresel bilgi ve iletişim altyapısı için

diplomasi, askeri ve istihbarat faaliyetlerini bu alan ile ilişkilidir. Bu stratejik güvenliğin mükemmelleştirilmesini amaçlayan bir yaklaşımdır.

- Kullanılan önlemler, faaliyetler ve politikaların bir sonucu olarak kişi, şirket veya devletin her türlü tehditten koruması anlamına gelir.
- Profesyonellik, araştırma ve geliştirme kavramlarını içeren bir araştırma ve inceleme alanına vurgu yapılarak sürekli gelişim içinde olunmasını ifade eder.

Siber güvenlik çok boyutlu olmasına rağmen temel olarak yedi prensipten oluştuğu söylenebilir. Siber güvenliğini en üst seviyede sağlamak maksadıyla, uygulanan söz konusu prensipler aşağıdaki gibi tanımlanabilir: (DALI, 2018).

- **Gizlilik:** Sanal dünyada oluşturulan verilere izin verilen kişi veya bağlı sistemler tarafından ulaşılabilmesini ifade etmektedir.
- **Bütünlük:** Oluşturulan verinin, kaynaktan çıktığı haliyle bir dış etkiye maruz kalmadan, bozulmadan veya değiştirilmeden alıcıya ulaşmasıdır.
- **Erişilebilirlik:** Oluşturulan veriye izin verilen yetkili kişilerin ve sistemlerin ihtiyaç duyulduğu zamanda ve yerde, hedeflenen kalitede erişebilmesi anlamına gelmektedir.
- **İzlenebilirlik:** Oluşturulan sistemde meydana gelen her bir olayın kayıt altına alınması ve istenildiği zaman analiz edilmek üzere kaydedilmesini ifade etmektedir.
- **Kimlik Doğrulama:** Oluşturulan verinin kaynağı olan alıcının, gönderici tarafından ifade edilen kişi olduğunun şüphe götürmeyecek bir şekilde bilinmesidir.
- **Güvenilirlik:** Oluşturulan sistemin hedeflendiği gibi çalışması, dış müdahalelere maruz kalmaması ve elde edilen sonuçların beklentilerle tutarlı olması anlamına gelmektedir.
- **İnkâr Edememe:** Gönderici olan kaynağın alıcı olan hedefe iletilen mesajın ispat edilebilir olmasıdır.

Siber güvenliğin bir yansıması olan bilgi güvenliği kavramı, içerisinde gizlilik, bütünlük, erişilebilirlik gibi üç ana unsuru barındırmaktadır. (Saltzer, Schroeder, 1975:1278-1308). Bu unsurlara ek olarak kayıt tutma, kimlik tespiti, güvenirlik, inkâr edememe gibi yan unsurları da bünyesinde barındırmaktadır. (Tekerek, 2008:132-137). Terimin temel üç ana unsuru aşağıdaki gibi özetlenebilir. (Aldemir, Kaya, 2020:6-27).

Şekil-1. Siber Güvenlik Kavramının Unsurları

Gizlilik	**•Bütünlük**	**•Erişebilirlik**
•Oluşturulan bilginin depolanması, işlenmesi, iletilmesi ve kabul edilmesi süreçlerindeki tüm adımlarda söz konusu bilgiye yetkili olan kişi veya sistemler tarafından oluşturulan yetki çerçevesinde ulaşılmasıdır.	•Oluşturulan bilginin kaynaktan hedefe iletilmesinde değiştirilmemiş, yeni veriler eklenmemiş, silinmemiş, bozulmamış veya dış etkilere maruz kalmamış bir şekilde iletilmesidir.	•Oluşturulan bilgiye sadece yetki tanımlanmış kişi veya sistemler tarafından ulaşılabilir olmasıdır. •Erişebilirlik kriteri aynı zamanda iletilen bilginin dış etki ve müdahalelere karşı korunmasını ifade etmektedir.

Siber terörü barındıran tehdit potansiyeli günden güne artmaktadır. Günümüzde teknolojinin hızla ilerlemesi terörist gruplara yeni alanlar açmakta olup propaganda, eğitim, haberleşme, bilgi toplama gibi faaliyetlere katılımı yükseltmektedir. Siber terörizm kavramının ortaya çıkışı, 1990'lı yılların başlarında, internet teknolojilerinin hızla büyümeye başladığı döneme denk gelmektedir. Bu dönemde yoğun bir şekilde "*bilgi toplumu*" tartışması yapılmış, teknoloji ve bilgisayar ağlarına büyük oranda bağlı olan ülkelerin karşı karşıya kaldıkları gerçeğine vurgu yapılmıştır. (Collin, 1997). Terörün bir yansıması olan siber terör kavramı, belirli bir amacı olan terörist örgütlerin bilgisayar sistemlerini bir saldırı aracı olarak kullanmalarıdır. Siber terörizm, organize bir örgüt tarafından siber saldırı araçlarının, yazılımların, donanımsal araçların veya diğer her türlü elektronik ve bilişim sistemine ait araçlarla bir ülkenin sistemine zarar verilmesi, vatandaşlarının bilgilerinin ele geçirilmesi veya yasadışı yollarla söz konusu bilgilerin kullanılmasıdır. Bu eylem ve etkinlikler siber terörizmin konusunu oluşturmaktadır. (Denning, 2001).

Son yıllarda siyasi amaçlı olduğuna inanılan birçok siber güvenlik olayı yaşanmıştır. Bu olayların büyük çoğunluğunu; mağdurun zayıf yönleri kullanılarak gerçekleştiren istihbarat toplama faaliyetleri, fikri mülkiyet hırsızlığı ve teknolojik bilgi hırsızlığı gibi türlerde gerçekleşmiştir. Siber casusluk, düşmanın veya rakibin hassas bilgilerine erişmek ve düşmana karşı avantaj sağlamak için bilgisayarlar veya dijital iletişim faaliyetlerinin kasıtlı olarak kullanılması olarak tanımlanabilir. (O'Hara, 2012: 39). İngiliz hükümeti, çoğunlukla siber casusluk ve fikri mülkiyet hırsızlığından kaynaklı siber saldırılar neticesinde yıllık maliyetini yaklaşık 44 milyon dolar olduğunu tahmin etmektedir. (Özbay, 2015).

Siber suç, bilgisayar veya bilgi sistemini ilk araç ya da ilk hedef olarak kullanılması yoluyla geniş bir çerçevede işlenen suç faaliyetlerini ifade etmek için kullanılmaktadır. Siber suçlar; geleneksel suçları (dolandırıcılık, sahtecilik ve kimlik hırsızlığı), içermesinin yanı sıra bilgi sistemlerine özgü suçları (bilgi sistemlerine karşı yapılan saldırılar, hizmet dışı bırakma saldırısı ve kötücül yazılımlar) da içermektedir. (https://ec.europa.eu , 2020)

Siber alandaki faaliyetlerin hızlı, kolay ve iz bırakılmadan yapılabilmesinden dolayı terör örgütlerinin yanı sıra devletlerin de ilgisini çekmektedir. Hatta kimi ülkeler siber saldırı ve siber savaş yöntemlerini önemli stratejik savunma ve rakibe zarar verme yöntemi olarak kullanmaktadır (Ada, 2018:23). Eski ABD Başkanı Bush'un Siber güvenlik danışmanı Richard A. Clarke "Cyber War" adlı kitabında siber savaşı "*Siber savaş, bir devletin, diğer bir devletin bilgisayar sistemlerine*

veya ağlarına hasar vermek ya da bozmak amacıyla gerçekleştirdiği faaliyetlerdir." şeklinde tanımlamıştır (Knarke, Clarke, 2010: 11).

2.3. Siber Saldırı Teknikleri

İnternetin kullanıcı sayısının ulaştığı nokta siber güvenlik konusuna dikkat çekmektedir. Uluslararası Telekomünikasyon Birliği (ITU) verilerine göre 2019 yılı sonu itibarıyla dünya nüfusunun yaklaşık %53,6'sının (neredeyse 4,1 milyar kişi), internet teknolojilerinden yararlandığı tahmin edilmektedir. Türkiye'de ise Bilgi Teknolojileri ve İletişim Kurumunun (BTK) Türkiye Elektronik Haberleşme Sektörü 2020 yılı 2. Çeyrek Raporu'nda 2008 yılında yaklaşık 6 milyon internet sitesi kullanıcı sayısı 78,4 milyona yükselmiştir. Türkiye İstatistik Kurumu (TÜİK) verilerine göre ise 16-74 yaş arası bireylerin internet teknolojileri kullanım oranı %79'a kadar yükselmiştir (www.ab.gov.tr , 2020).

Siber dünyada, bireylerin, işletmelerin, devletlerin ve siber güvenlik uzmanlarının dahi kendilerini ve kendi bilgi işlem servislerini korumalarını zorunlu kılan pek çok yol ve yöntem bulunmaktadır. Siber saldırı tekniklerini kullanan kişilerin sızdıkları bilgisayar ve bilgisayar sistemlerini değiştirilebilir, sunulan hizmeti aksatabilir, verileri silebilir veya erişilemez hale getirebilir. Bu saldırılar sonunda zarar gören kişi, işletmelere veya kamu kurumuna maddi zararları olabileceği gibi itibarının azaltılması şeklinde manevi zararları da olmaktadır (Ada, 2018:9). Siber saldırı tekniklerini aşağıdaki gibi sıralamak mümkündür:

- **Oltalama Saldırıları (Phishing):** Oltalama saldırıları, sahte e-posta veya kopya web sitesi kullanılarak tanınmış ve güvenilir bir kurumu taklit ederek; sistemi kullanan kişilerin adını, parolasını, banka hesap numarasını veya kredi kartı numarasını ele geçirme faaliyetleridir. Bu bilgiler hassas bilgiler olarak değerlendirilir ve söz konusu eylemler adli olarak suç unsuru taşıyan aldatıcı hareketlerdir (Schreier, 2015:61). Phishing saldırısı, Türk Ceza Hukukunda tanımlanan bir suç türüdür.

- **Kötücül Yazılım (Malware):** Kötücül yazılım, bilgisayar kullanıcılarının haberi olmaksızın, kullandıkları bilgisayarlara sızmak ve bu bilgisayarlara zarar vermek amacıyla kodlanmış yazılımların genel adıdır. Bilişim ağlarına yetkisiz erişim sağlamak için ve kullanıcılarının iradesi dışında farklı işlerde kullanılmak üzere yerleştirilir (www.keepeek.com , 2020).

- **Truva Atı (Trojan):** Truva atı, internet kullanıcıları için faydalı gibi görünen ancak içinde barındırdığı zararlı kodlar sebebiyle bilişim güvenliğine zarar veren bir program türüdür (www.keepeek.com , 2020). Truva atları, bilgisayarları kullanıcıların isteğinin dışında yönetmek ve bilgisayarlara dışarıdan erişim sağlamak için arka kapı açan programlardır.

- **Virüs:** Virüsler, en eski ve en tehlikeli kötücül yazılım olarak bilinmektedir. Nitekim bilgisayar belleğine ulaşabilen, ulaştığı zaman ise kullanılan programlara zarar veren, programları değiştiren ve en önemlisi kendi kendileri çoğaltarak tüm sistemi ele geçiren zararlı yazılımlardır (Nickolov, 2008). Virüsler çoğaldıkları bilgisayarlarda her türlü verilere zarar vermenin yanı sıra sisteme zarar vererek tüm sistemin çökmesine de neden olabilmektedir (Canbek, Sağıroğlu, 2007:121-136).

- **Solucan:** Solucan, truva atına ve virüslere göre daha komplike olan zararlı yazılımdır. Solucanlar çoğunlukla e-posta yoluyla gönderilen mail ekleri, sahte internet siteleri veya doğrudan bağlı bulunan ağ ile paylaşılan dosyalarla bulaşmaktadır (Nickolov, 2008:85). Solucanlar, bir sisteme bulaştıklarında, kullanıcının başka hiçbir eylemine ihtiyaç duymadan, sistemdeki verilere ulaşır ve söz konusu verileri kullanır. Daha sonra solucanlar kendi dosyalarını hızlı bir şekilde diğer kullanıcılara ulaştırmaya çalışır. Ne kadar çok çoğalırsa o kadar tehlikeli hale gelir. Kullanıcıların ağ sistemini kullanan solucanlar kurumsal ağın çalışmasını engelleyebilir, ağı kilitleyebilir, e-posta sisteminin çökmesine neden olabilir veya web servislerinin hızının düşmesine neden olabilmektedir (www.keepeek.com , 2020).

- **Reklam İçerikli ve Casus Yazılımlar:** Reklam içerikli (adware) ve casus yazılımlar (spyware) bilgisayar kullanıcılarının istekleri dışında, sürekli reklam içerikli mail gelmesini ve bilgisayarlara yerleştirilen yazılımlar aracılığı ile kullanıcı bilgilerinin saldırganın eline geçmesini ifade etmektedir. Tarayıcısının varsayılan ayarları bilgisayara bulaşan reklam içerikli yazılım aracılığı ile değiştirilmektedir (www.commerce.senate.gov, 2021).

- **Botnet:** Botnet, kullanıcıların bilgisi dışında bilgisayarlarına yerleşen kötücül yazılımlar aracılığı ile merkezi bir yerden çok sayıda kötücül yazılım bulaştırılmış bilgisayarlar kümesini ifade etmektedir. Kullanıcısının iradesi dışında kötücül yazılım bulaşmış olan bilgisayarlar terminolojide zombi olarak da nitelendirilmektedir. Botnet tek bir komuta merkezinden genellikle bir kişi tarafından kontrol edilebilme yeteneği sağlamaktadır (www.enisa.europa.eu, 2020). Bir zombiye dönüşmüş olan bilgisayar komuta merkezinden gelecek komutlar doğrultusunda farklı amaçlara hizmet etmek için kullanılabilmektedirler.

- **Hizmeti Engelleme (DoS/DDoS) Saldırıları:** Hizmeti engelleme saldırıları günümüzde bilgi sistemlerinin erişilebilirliğine yönelik gerçekleştirilen yaygın saldırılardan biri olarak karşımıza çıkmaktadır. DoS/DDoS saldırılarının kullanıldığı birçok yöntemdeki temel amaç, gerçekleştirilen siber saldırılar ile resmi bir kuruluşun ya da şirketin bilgi iletişim ağlarını kilitlemek ve verdiği hizmeti engellemeye çalışmaktır. Günümüzde hizmet engelleme saldırılarının büyük çoğunluğu birden çok bilgisayar kullanılarak gerçekleştirilmektedir (Ada, 2018:10).

- **Sosyal Mühendislik Saldırıları:** Sosyal mühendislik (social engineering), insanlar arasındaki iletişimdeki ve davranışlardaki modelleri "*zafiyetler*" olarak tanımlayıp, bu zafiyetlerden faydalanılarak güvenlik süreçlerini atlatma yöntemine dayanan eylemlere verilen isimdir (www.bilgiguvenligi.gov.tr , 2020). Sosyal mühendislikte kullanılan yöntemler olarak karşımıza hedefe güvenilir bir kaynak olduğunu hissettirmek, ortak tanıdıklar üzerinden yakınlık kurmak, özellikle iletişim araçları ile başkasını taklit etmek, gizlice zor bir durum oluşturarak yardım ediyormuş izlenimi vermek, hedef sistemin çöp olarak attığı kişisel bilgileri karıştırmak örnek olarak verilebilir (http://online.securityfocus.com , 2020).

- **APT (Advanced Persistent Threat/Gelişmiş Kalıcı Tehdit) Saldırıları:** APT, yetkisiz bir ağa erişildikten sonra orada tespit edilmeden erişilen ağda uzun süre kalınan saldırı çeşididir. APT saldırılarında esas amaç verilerin çalınması ya da ele geçirilmesi değildir.

Buradaki asıl amaç erişilen ağda uzun süre kalınarak bu ağa veya kuruluşa zarar vermektir. APT saldırıları, ulusal savunma, imalat ve finans sektörü gibi bilgi değeri yüksek olan sektörler hedef alınarak gerçekleştirilir (Chen, Desmet, vd. 2014:63-72).

Kritik altyapılara yönelik siber saldırılar, bilgisayar altyapısının savunmasız hale geldiğini göstermektedir. Günümüzde özel kuruluşların, ülkelerin ve diğer sorumlu kuruluşların bile orduya, merkez bankalarına, savunmalara yönelik önemli siber saldırılardan istisna olduğunu söylemek mümkün değildir. Siber saldırı tehdidi hızla büyümekte olup karşılık vermek, saldırıyı tespit etme ve kaynağını bulma konusunda sorunlar bulunmaktadır. Yeterli karşı önlemler, yalnızca saldırılar meydana geldiklerinde engellemeye yardımcı olmakla kalmayacak, daha da önemlisi, dünya, bölge ve alt bölgedeki kolluk kuvvetleri için bir tatbikat düzenlenerek bilgisayar korsanlarını ilk etapta saldırmaktan caydıracaktır.

3. TÜRKİYE'NİN SİBER GÜVENLİK EYLEM PLANLARI

Bu bölümde ilk olarak Siber Güvenlik Kurulu ve görevleri incelenecektir. Daha sonra yayımlanan üç adet eylem planı hedefler temelinde özetlenecektir.

3.1. Siber Güvenlik Kurulu

2018 yılında Cumhurbaşkanlığı Hükümet Sistemine geçilmeden önce yürütmenin başı olan Bakanlar Kurulu'nun 11/06/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Kararı, 20/10/2012 tarihli ve 28447 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Söz konusu karar ile Siber Güvenlik Kurulu kurulmuştur. Kararla ayrıca Ulaştırma Denizcilik ve Haberleşme Bakanlığının (yeni adıyla Ulaştırma ve Altyapı Bakanlığının) siber güvenlik konusundaki yetki ve sorumlulukları tanımlanmış, siber güvenlik konusunda çalışma grupları ile geçici kurulların oluşturulabileceği hüküm altına alınmıştır.

5809 sayılı Elektronik ve Haberleşme Kanunu'na eklenen 1. ek madde ile birlikte Siber Güvenlik Kurulu'nun yapısı oluşturulmuş ve Bilgi Teknolojileri ve İletişim Kurumuna siber güvenlik ile ilgili yeni görevler yüklenmiştir. 5809 sayılı Kanun ile gelen yenilikler aşağıdaki gibidir:

- Siber güvenlik ulusal konusunda politika, strateji ve eylem planlarının onaylamak ve uygulanması için süreci koordine etmek,
- Ulusal kritik altyapı tesislerinin ve hizmetlerinin belirlenmesine yönelik gelen teklifleri karara bağlamak,
- Siber güvenlikle ilgili oluşturulan hedef ve yasal zorunluluklarının bir kısmından veya tamamından muaf tutulacak kurum ve kuruluşları belirmektir.

Siber Güvenlik Kurulu ilk düzenleme ile "*Dışişleri Bakanlığı Müsteşarı, İçişleri Bakanlığı Müsteşarı, Milli Savunma Bakanlığı Müsteşarı, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Müsteşarı, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı, Mali Suçları*

Araştırma Kurulu Başkanı ve Telekomünikasyon İletişim Başkanı"ndan oluşmaktadır. Ancak Cumhurbaşkanlığı Hükümet Sistemine geçiş ile birlikte müsteşarlıklar kaldırılmış, Telekomünikasyon İletişim Başkanlığı 2016 yılında Bakanlar Kurulu kararı ile kapatılarak görev, yetkileri Bilgi Teknolojileri ve İletişim Kurumuna aktarılmış ve bakanlıklar nezdinde birçok yeni düzenleme hayata geçirilmiştir. 02/07/2018 tarihli 703 sayılı Kanun Hükmünde Kararname'nin 205. maddesi ile yukarıdaki düzenleme mülga edilmiş olup yeni bir düzenleme 2020 yılı sonuna kadar yayımlanmamıştır.

1 sayılı Cumhurbaşkanlığı Kararnamesi'nin 26. maddesi ile Güvenlik ve Dış Politikalar Kurulu oluşturulmuş olup Kurula "*siber güvenlik ile ilgili politika ve strateji önerileri geliştirmek*" görevi tevdi edilmiştir. Bunun yanı sıra aynı Kararnamenin 527. maddesi ile kurulan Dijital Dönüşüm Ofisinin bir yetkisi de "*siber güvenlik ve bilgi güvenliğini artırıcı projeler geliştirmek*"tir. Aşağıdaki bölümlerde hazırlanan eylem planları ve eylem planlarında yer alan hedefler yer almaktadır.

3.2. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı

Eylem planı, bütün kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler, Siber Güvenlik Kurulu tarafından belirlenen politika, strateji ve eylem planları çerçevesinde kendilerine verilen görevleri yerine getirmek ve belirlenen usul, esas ve standartlara uymakla yükümlü olduğuna dair düzenlemeyle başlamaktadır. 2013-2014 döneminde gerçekleştirilmesi planlanan siber güvenlik temelli hedeflere ilave olarak dönem içini aşan farkındalığın artırılması ve eğitimin sürekli hale getirilmesi amaçlayan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı 20/06/2013 tarih, 28683 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının amacını aşağıdaki gibi özetlemek mümkündür:

- Tüm kamu kurum ve kuruluşlarının bilgi teknolojileri (BT) altyapılarıyla sunulan her türlü işlem, oluşturulan veri ve söz konusu verilerin kullanılmasındaki *sistemlerin güvenliğinin sağlanmasına,*

- Hem kamu kurum ve kuruluşlarının hem de özel sektörün sorumluluğunda olan *kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanmasına,*

- Siber uzayda ve bütünleşik dünyada siber saldırılardan tamamen korunmak mümkün değildir. Bu yüzden siber güvenlik saldırılarının etkilerinin en alt seviyede tutulmasını, saldırı sonrasında kullanılan tüm sistemlerin *en kısa sürede normal çalışmalarına dönmesine* yönelik stratejiler geliştirilmesi, eylem planı hazırlanması ve oluşan suçun adli makamlara bildirilmesi, araştırılması, soruşturulması ve cezalandırılması için yasal ve idari *altyapı oluşturmak*tır.

Bu amaçlarda dikkat çeken en önemli nokta kritik altyapılara yönelik güvenliğin sağlanması hedefidir. Söz konusu amaçlardan yola çıkılarak 13 adet ilke belirlenmiştir. Bu ilkelere tüm kamu kurumlarının uygulaması beklenmiş olup hukukun üstünlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması ilkeleri temel esas kabul edilmiştir. İlkeler aşağıda sıralanmıştır:

- Siber güvenliğin sağlanması için risk analizi ve yönetimi temelli *etkin ve sürekli iyileştirmeye* dayalı araçlarla sağlanır.

- Siber güvenliğin bilişim boyutuna ek olarak; *hukuki, idari, ekonomik, politik ve sosyal boyutlarda güçlü ve zayıf yönlerin, tehditlerin ve fırsatların belirlenmesi*ni bünyesinde barındıran bir model gereklidir.

- *Risk yönetimi*nde, teknolojik açıklıkların kapatılması, tehdit ve saldırıların engellenmesi ve ortaya çıkması olası zararların en aza indirilmesi esas alınır.

- Siber güvenlik tam anlamıyla sağlanmasında, *birey, kurum, toplum ve devletin tüm hukuki ve sosyal sorumlulukları*nı bilmesi ve bunları yerine getirilmesi önemlidir.

- *Kritik altyapıların güvenliğinin sağlanması* için, sadece kamu sektörünün değil aynı zamanda özel sektörün katılımının sağlanması, ortak projeler geliştirilmesi ve devletin yönlendirici gücünü göstermesi gerekir.

- Siber uzayda güvenilir bir şekilde var olmak ve varlığın sürdürülmesi için kamu, özel sektör, sivil toplum kuruluşları, üniversiteler arasındaki iş birliğinin yanında *uluslararası iş birliği ve bilgi paylaşımı* da gereklidir.

- Uluslararası siber güvenlik alanındaki iş birliği ve bilgi paylaşımının sağlanması için sürekli olarak *diplomatik, teknik ve kolluk iletişim kanalları*nın açık olması esas alınır.

- Siber güvenlik alanında *ihtiyaç duyulan mevzuat geliştirilirken uluslararası anlaşma ve düzenlemeler* temel alınır.

- *Hukukun üstünlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması* gibi ilkeler esas alınır.

- Siber uzayda şeffaflık*, hesap verilebilirlik, etik değerler ve ifade özgürlüğü* savunulur ve desteklenir.

- Güvenlik ile erişim arasında sağlam bir denge gereklidir.

- *Denetleyici ve düzenleyici kurumların* sorumluluğun olan alanlardaki siber güvenliğin korunması ve sağlanması esas alınır.

- Siber güvenlik alanındaki ihtiyaçların giderilmesinde *yerli ürün ve hizmet kullanımı teşvik* edilir, söz konusu ürün ve hizmetlerin üretilmesinde *araştırma ve geliştirme projeleri desteklenir*.

- Siber güvenlik gereksinimlerinin karşılanmasında, inovasyon anlayışı esas kabul edilir.

Yukarıda belirtilen ilkeler kendi içinde bir amacı ifade etmektedir. 2013- 2014 dönemini kapsayan eylem planında ulusal siber güvenliğin sağlanması ve korunmasına yönelik hedef ve stratejiler geliştirilmiştir. 2013- 2014 döneminde gerçekleştirilmesi planlanan ve 7 ana başlıkta toplanan stratejik eylemler ve alt eylemler şöyledir:

1. Yasal Düzenlemelerin Yapılması

- Kurulan Siber Güvenlik Kuruluna işlerlik kazandırılması

- Siber güvenlik alanının yasal altyapısının kurulması

2. Adli Süreçlere Yardımcı Olacak Çalışmaların Yürütülmesi

- Siber olayların kanıtlanabilir hale getirilmesi

3. Ulusal Siber Olaylara Müdahale Organizasyonunun oluşturulması

- Ulusal Siber Olaylara Müdahale Merkezinin (USOM) oluşturulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) kurulması

4. Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi

- Kritik Altyapılarda Bilgi Güvenliği Yönetimi Programının oluşturulması
- Kamu Bilgi Güvenliği Programının oluşturulması
- Siber güvenlik alanının eğitim yapısının sağlamlaştırılması
- Siber güvenlik tatbikatlarının düzenlenmesi
- Kamu güvenli iletişim kanallarının kurallarının tespit edilmesi
- Yazılım güvenliğinin sağlanmasına yönelik programının işletilmesi
- Siber tehditlerin ortaya çıkmadan önlenmesi projesinin oluşturulması
- Siber güvenlik alanındaki ürünlerin ve hizmet sağlayıcıların kayıt altına alınması ve akredite edilmesi
- Adli bilişim alanında hizmet sunanlara güvenlik belgesi verilmesine ilişkin standartların oluşturulması
- Hizmet sürekliliğinin sağlanması ve verilerin yedekleme altyapısının kurulması
- Kamu kurum ve kuruluşlarının internet sayfalarının tek bir merkeze taşınması
- Kamu kurumlarından ve özel sektörden veri sızıntılarının tespit edilmesi ve sistemlerin teste tabii tutulması ve otomatik uygulamalara alınması
- Kamu kurumlarının verilerin erişim yetki düzenlemesinin yapılması
- Açık kaynak kodlu ürünlerin kullanımının artırılması

5. Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi ve Bilinçlendirilme Faaliyetleri

- Siber güvenlik konusunda üniversitelerin desteklenmesi ve akademik personel yetiştirilmesi
- Akademik ortamlarda siber güvenlik eğitimlerinin yaygınlaştırılması
- Siber güvenlik konusunda uzmanlığın sağlanmasına yönelik programın uygulanması

- İlk, orta, lise öğretimi ve yaygın eğitimde yaygın bir şekilde siber güvenlik konusunun işlenmesi
- Bilgisayar kullanıcılarının siber güvenlik alanında farkındalığının artırılması
- Ulusal ve uluslararası siber güvenlik organizasyonlarının oluşturulması

6. Siber Güvenlikte Yerli Teknolojilerin Geliştirilmesi

- Ar-Ge faaliyetlerinin teşvik edilmesi
- Siber güvenlik konusunda Ar-Ge laboratuvarlarının oluşturulması
- Siber güvenlikte yerli ürünlerin ve sorunlara karşı yerli çözümlerinin teşvik edilmesi

7. Ulusal Güvenlik Mekanizmalarının Kapsamının Genişletilmesi her eylem için sorumlu ve ilgili kurum ve kuruluşlar belirtilmiştir.

- *Ulusal siber güvenliğin bir bütün olarak milli güvenliğe adapte edilmesi.*

Eylem planında, siber güvenliğe ilişkin eylemlerin uygulanabilmesi için siber güvenlik alanındaki risklerin belirlenmesi amaçlanmıştır. Siber Güvenlik Eylem Planı'nda bilgi ve iletişim sistemleri ile ilişkili 18 adet siber güvenlik riski belirlenmiştir. Bu riskler özetle, siber saldırıların hem maliyet hem de ürün gamı açısından oldukça kolaylaştığı, bilgi ve iletişim araçlarının birbirleriyle bağlantılı olmasının saldırıların çapını büyüttüğü, servis sunumunun bilişim altyapısına bağımlılığı, kritik altyapıların internet bağlantısı gerektirmesi, ulusal bilincin zayıflığı, koordinasyon eksikliği, saldırıların gizlenmesi, insan kaynağının zayıflığı, altyapının yetersiz olması, yeterli bilgi ve bilinç seviyesinin oluşmaması, kurumların siber güvenliğin sağlanmasını sadece BT birimlerine bırakması, denetimin yetersizliği, sadece ürün temelli siber güvenlik anlayışının hakimiyeti ve yerli ürünlerin yetersizliğidir.

Riskler ve eylemler ile ilgili tüm kurum ve kuruluşların, sorumlu kurum ve kuruluşların Siber Güvenlik Kurulu koordinatörlüğünde hareket etmesi hedeflenmiştir. Eylem planında yer alan hedeflerin bir kısmı için son tarih belirlenmiş ve birtakım hedeflerin periyodik olarak tekrar edilmesi ifade edilmiştir. 2013-2014 döneminde, gerçekleştirilmesi planlanan toplam 29 adet eylem maddesi oluşturulmuştur. Söz konusu eylem maddelerine stratejik eylem başlıkları belirlenerek toplulaştırma yapılmıştır. Ayrıca oluşturulan 29 adet eylem maddesine 86 adet alt eylem oluşturulmuştur. 2013-2014 Siber Güvenlik Eylem Planı'nda belirlenen söz konusu 86 alt eylemin sorumlu kurumlara göre dağılımını yine eylem planında belirlenmiştir.

Siber güvenlik eylem planının izlenmesine, sonuçların kamuoyuyla paylaşılmasına veya ilgili planın bütçesinin belirlenmesine yönelik herhangi bir açıklamaya rastlanılmamıştır. Planın uygulanmasına yönelik ise Siber Güvenlik Kurulu oluşturulmuş, bir takım yasal düzenlemeler hayata geçirilmiş, Siber Olaylara Müdahale Ekipleri (SOME) kurulmuş, eğitim ve farkındalık çalışmaları yürütülmüş, insan kaynağının güçlendirilmesine yönelik altyapılar oluşturulmuş, yerli teknolojiler teşvik edilmiştir. Ancak genel olarak hedeflerin çoğuna ulaşıldığını söylemek güçtür.

3.3. 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı

2013-2014 dönemini kapsayan Eylem Planının uygulama süresi dolduktan sonra yeni bir eylem planı hazırlıklarına girişilmiştir. Eski eylem planı kapsamındaki hedeflerin değişen dünya şartlarına uygun hale getirilmesi, siber güvenlik ihtiyacının yükselmesi, bilgi ve iletişim teknolojilerinin yapı değiştirmesi neticesinde yeni eylem planının hazırlandığı dönemdeki ismiyle Ulaştırma, Denizcilik ve Haberleşme Bakanlığı 2016-2019 dönemini kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planını hazırlamış ve yürürlüğe koymuştur. Eylem planının hazırlık döneminde 2013-2014 dönemi Eylem Planında yer alan amaç ve stratejilerden sorumlu veya ilgili kurumlarla 10 Mart-7 Nisan 2015 tarihleri arasında yedi toplantı yapılmıştır. Toplantılarda öncelikle 2013-2014 dönemini kapsayan Eylem Planındaki hedeflerin gerçekleşme seviyeleri analiz edilmiş, eylem planının uygulanmasında karşılaşılan güçlükler araştırılmış ve yeni dönemim stratejileri belirlenmiştir. Ortak Akıl Platformu olarak değerlendirilen bu çalışmalara kamu kurumları, kritik altyapı işletmecileri, bilişim sektörü, üniversiteler ve sivil toplum kurumlarını temsil eden 73 kurumdan 126 uzman katılmıştır. Toplam iki gün süren bu çalışmalar kapsamında Türkiye'nin siber güvenlik konusunda güçlü ve zayıf yönleri belirlenmiş ve eylem planının stratejik amaçları ve gerçekleştirmesi için atılması gereken adımlar ortaya koyulmuştur.

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı hazırlanırken yukarıdaki toplantıların yanı sıra geniş bir literatür taraması da yapılmıştır. Bu tarama Amerika, Avrupa ve Uzak Doğu'dan pek çok ülkenin siber güvenlik eylem planı, stratejileri ve faaliyetleri incelenerek ülkelerin siber güvenlik kapsamındaki hedefleri, eylemleri, öncelikler, örgütlenme yapıları, bütçe tahsisler, Ar-Ge (Araştırma ve Geliştirme) teşvikleri, kamu özel sektör işbirliği uygulamaları, insan kaynağı yatırımları, eğitim faaliyetleri gibi konulara odaklanılmıştır. Toplantılar ve kaynak taraması sonunda elde edilen bilgiler toplanmış, tasnif edilmiş, incelenmiş ve değerlendirilmiştir. Sonrasında ise "*2016-2019 Ulusal Siber Güvenlik Stratejisi*" ve "*2016-2019 Ulusal Siber Güvenlik Eylem Planı*" hazırlanmıştır. Eski eylem planında olduğu gibi sorumlu ve ilgili kuruluşların eylemlerden sorumlu tutulmuştur. 2016-2019 Siber Güvenlik Eylem Planı hizmete özel olduğu için kamuoyuyla paylaşılmamıştır.

2016-2019 Ulusal Siber Güvenlik Stratejisinin ana amacı; "*siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olduğu anlayışının tüm kesimlere yerleşmesi, ulusal siber uzayda bulunan sistem ve paydaşların tamamının güvenliğini sağlamak üzere idari ve teknolojik önlemlerin alınmasını sağlayacak yetkinliğin eksiksiz bir şekilde kazanılması*" olarak açıklanmıştır. Belirlenen ana amaç doğrultusunda:

- Türkiye'nin siber uzayın bir bütün olarak ele almak koşuluyla, bilgi ve iletişim teknolojileri kullanılarak sunulan her türlü hizmette, yapılan işlemde veya bilgi/ veri transferlerinde *kullanılan sistemlerin güvenliğinin, gizliliğinin ve mahremiyetinin sağlanması*na,

- Siber güvenlik saldırıları ve olaylarının *etkilerinin minimum seviyelerde tutulmasına*, *olaylardan sonra en kısa sürede çalışır hale getirilmesine* ve *normal çalışma düzeyine erişilmesinde* stratejiler geliştirilmesi,

- *Siber olaylar sonrası ortaya çıkan suç unsurlarının adli makam ve kolluk kuvvetleri tarafından etkili bir şekilde araştırılması ve kovuşturulmasının gerçekleştirilmesi,*

- Gizliliğin ve mahremiyetin korunmasında siber güvenliğin etkin şekilde kullanılması, bunun sağlanması için gerekli olan *kritik teknolojilerin ve ürünlerin ülke kaynaklarıyla üretilmesine,* üretilemiyorsa söz konusu teknolojilerin *yurtdışından amaca uygun ve güvenli bir şekilde tedarik edilmesine* yönelik bileşenler 2016-2019 Ulusal Siber Güvenlik Stratejisinin ve Eylem Planı'nda yer almaktadır.

Dünya çapında siber güvenlik stratejileri ve eylem planları incelenerek öne çıkan 8 adet ilke ve 10 adet risk tespit edilmiştir. Söz konusu ilkeler temel olarak etkin ve sürekli değerlendirmeye ve iyileştirmeye dayalı risk yönetiminin önemli olduğu, tüm paydaşların siber güvenlik risklerinin farkında olması gerektiği, tüm paydaşların hukuki, idari, ekonomik, politik ve sosyal boyutları bilmeleri için gerekli eğitim ve deneyimi kazanmalarının önemli olduğu, zararların asgari düzeyde tutulması için siber olaylara karşı bir hazırlıklı ve planlı olunması gerektiği, kamu, özel sektör, üniversiteler, sivil toplum kuruluşları ve bireyler dâhil tüm paydaşlar arasında işbirliğinin yanı sıra uluslararası işbirliği ve bilgi paylaşımının esas olduğu, hukukun üstünlüğü, ifade özgürlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunmasının çalışmaların ana dayanağı olduğu, şeffaflık, hesap verilebilirlik ve etik değerleri göz önünde bulundurulması, siber güvenlik önlemlerinin ilgili risklerle orantılı olması, olumlu ve olumsuz etkilerinin değerlendirilmesi ve dengelenmesi gerektiği ve yerli ürün ve hizmet kullanımının teşvik edilerek araştırma ve geliştirme projeleri desteklenmesi gerektiği şeklinde sıralanabilir.

Eylem planında sayılan riskler ise daha çok kritik altyapıların güvenliği, kişisel bilgilerin korunması, hassas ve ticari değere sahip Ar-Ge çıktılarının güvenliği, hacktivizm (propaganda amaçlı bilgisayar korsanlığı) faaliyetleri, Küçük ve orta ölçekli sanayi, ticaret ve hizmet sektöründeki kuruluşların zafiyetleri, bilgi ve farkındalık seviyelerinin düşüklüğü, dolandırıcılık faaliyetleri ile hizmet ve faaliyetlerin kesintiye uğraması konularına vurgu yapılmıştır.

2016-2019 dönemini kapsayan Eylem Planının stratejik amaçlarında ulusal kritik altyapılara, yasal mevzuata, farkındalık ve yetkinlik temelli faaliyetlere, kullanıcı hatalarından ve afetlerden korunmaya, yetkinliğin yükseltilmesine, farkındalığının artırılmasına, insan kaynağının geliştirilmesine, siber olaylara müdahale ekiplerine yatırım yapılmasına, koordinasyona, siber güvenlik ekosistemine (işbirliğine), uzman ve iyi uygulama desteklerine, ürün analizine, proaktif siber savunma yeteneğine (caydırıcılık), etkin kayıt yönetimine ve daha güçlü IPv6 (Internet Protokolü sürüm 6/ internet temelli ürünlerin birbirleriyle iletişim kurması için ihtiyaç duyulan IP adreslerinin daha güvenlikli olmasını sağlaması) teknolojilerine odaklanılmıştır. Planda belirlenen stratejik amaçlara ulaşmak için gerçekleştirilecek eylemler aşağıda belirtilen beş stratejik eylem başlığı altında toplanmaktadır.

- **Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması:** Bu eylem başlığı altında devletin ve ulusal ekonomik birimlerinin, kritik altyapıların ve toplumun tamamımın siber saldırı risklerini azaltmak için eylemler gerçekleştirilmesi planlanmıştır.

- **Siber Suçlarla Mücadele:** Kamu kurum ve kuruluşları, özel sektör örgütleri, bireyleri etkileme potansiyeline sahip, maddi kayba neden olan, manevi olarak olumsuz etkileyen siber saldırıların azaltılması ve engellenmesine yönelik eylemlerin gerçekleştirilmesi planlanmıştır.

- **Farkındalık ve İnsan Kaynağı Geliştirme:** İdarecilerden bilgi teknolojilerini kullanan bireylere kadar herkesin siber güvenlik kültürünü öğrenmeleri, siber saldırıların farkında olmaları, etkilerini tahmin edebilmelerine yönelik eylemlerin gerçekleştirilmesi ve doğrudan siber güvenlik uzmanı sayısının artırılması hedeflenmiştir.

- **Siber Güvenlik Ekosisteminin Geliştirilmesi:** Kamu, özel sektör, STK, üniversiteler ve diğer tüm paydaşların koordineli bir şekilde oluşturulan yasal altyapıdan teknolojik ürünlere kadar tüm ihtiyaçlarının belirlenmesine ve ihtiyaçların giderilmesine yönelik araçların uygulamaya dökülmesine yönelik eylemlerin gerçekleştirilmesi planlanmıştır.

- **Siber Güvenliğin Milli Güvenliğe Entegrasyonu:** Kamuyu, ekonomiyi, kamu ve özel sektörün sorumluluğunda olan kritik altyapıları, toplumun genelini veya özelini etkileme potansiyeline sahip, güçlü bir şekilde örgütlenmiş, bireysel veya organize bir şekilde saldıran tehdit unsurlarının saldırıları sonrası verebileceği zararları azaltmaya yönelik eylemlerin gerçekleştirilmesi planlanmıştır.

Eylem planında yer alan her bir eylem için sorumlu ve ilgili kurum ve kuruluşlar belirlenmiştir. Bu kapsamda ilgili kurum ve kuruluşlar eylemlerin tamamlanmasına destek sunarken yetkili kurum ve kuruluşlar doğrudan eylemin tamamlanmasından sorumludur. Sorumlu kurum ve kuruluşlar koordine görevini yerine getirirken sürecin yönetiminde aktif rol alması hedeflenmiştir. Oluşturulan eylemlerin bitirilme tarihi belirtilerek birtakım eylemlerin sürekli olarak tekrarlanması amaçlanmıştır. Bunun yanı sıra dönem içinde Afet ve Acil Durum Yönetimi Başkanlığı tarafından hazırlanan 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi ile kritik altyapıların korunmasına yönelik bir yasal düzenleme olmadığı ifade edilerek kritik altyapıların korunması uygulama çerçevesiyle birlikte kritik altyapılar sıralanmış ve daha sonra ülkenin ihtiyaç duyduğu düzenlemeler ve eylemler ele alınmıştır. Ancak eylem planı genel olarak değerlendirildiğinde hangi eylemlerin tamamlandığı, hangi eylemlerde eksiklik olduğu, tekrarlanan eylemlerde ne kadar ilerleme sağlandığı doğrudan bir rapor ile kamuoyuyla paylaşılmamıştır.

3.4. 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı

2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 29 Aralık 2020 tarihli ve 31349 sayılı Resmi Gazete'de yayımlanmıştır. Eylem planı toplam 12 bölümden oluşmakta olup hizmete özel kısmı tablolar şeklinde kamuoyuna açıklanmamıştır. Yönetici özetinde, ulusal siber güvenlikte gelişim seviyesinin çok yüksek olduğu, gelişmeleri yakalamak için ulusal stratejilerin güçlü olması gerektiği, eylem planının Türkiye'nin siber güvenlik alanındaki vizyonu ve misyonu doğrultusunda gelecek dört yıla ilişkin hedef, eylem ve politikaların konu aldığı ve daha önceki eylem planlarından elde edilen ilerlemenin daha öteye taşınması gerektiği ifade edilmiştir.

2013-2014 dönemi ile 2016-2019 dönemlerini kapsayan eylem planı kapsamında uygulanan ve periyodik olarak yapılması gereken eylemler gözden geçirilmiştir. Böylece mevcut durum ve yapılan çalışmalar kapsamında yeni eylem planında eski eylem planlarının geliştirilmesi ve eksikliklerinin giderilmesi hedeflenmiştir. Stratejik amaçlar doğrultusunda planlanan kazanımların elde edilmesine yönelik eylemlerin belirlenmesi için ulusal paydaşların katılımıyla Hazırlık Çalıştayı düzenlenmiştir. Söz konusu çalıştaylara 67 kurumdan 127 katılımcı iştirak etmiştir. Eylem planının ikinci bölümünde kavramlar ile ilgili tanımlamalara yer verilmiştir. Üçüncü bölümde eylem planının giriş kısmı yer almakta olup dünya çapındaki gelişmeler değerlendirilmiştir.

Türkiye'de siber güvenlik başlığı altında çalışmalar ile risklerin azaltılmasının hedeflendiği ve 2013-2014 Eylem Planı ile mevzuat, kritik altyapılar, siber olaylara müdahale, farkındalık çalışmalarının yürütüldüğü, 2013 yılında Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuş olduğu, 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı eski plana ek olarak siber suçlarla mücadele edilmesi, insan kaynağı geliştirilmesi, siber güvenlik ekosisteminin kurulmasının hedeflendiği, Uluslararası Telekomünikasyon Birliği Global Siber Güvenlik Endeksinde gelişim gösterildiği, 2020-2023 dönemini kapsayan eylem planında ise benzer amaçların yer aldığı tespit ve değerlendirmelere yer verilmiştir:

Eylem planının vizyonu; "*Ülke ekonomisinin geliştirilmesini, toplumsal yaşamın korunmasını ve milli güvenliğin sağlanmasını desteklemek için; ülkemizde güvenli biçimde işleyen bir siber ortama sahip olmak ve siber güvenlikte uluslararası alanda marka haline gelmek.*" ve misyonu ise "*Siber güvenliğin milli güvenliğimizin ayrılmaz bir parçası olduğu bilinci ile kritik altyapılarımız başta olmak üzere siber uzaydaki varlıklarımızın tehditlerden korunmasına ve siber olayların muhtemel etkilerini azaltmaya yönelik çalışmaları ilgili tüm paydaşlarla koordineli olarak gerçekleştirmek.*" olarak belirlenmiştir.

2020-2023 Dönemi Eylem Planının ilkelerinde siber güvenlik ile ulusal güvenlik ilişkisi, proje yürütülmesinin sürekliliği, siber güvenliğin önemi, paydaşlar arasındaki iş birliği, şeffaflık, hesap verebilirlik ve etik değerler, kritik altyapılar, siber güvenlik temelli tasarımlar, gizlilik-bütünlük-erişilebilirlik konuları, yasal altyapı, Ar-Ge ve yerli ürün ve hizmetlerin kullanılması konularına dikkat çekilmiştir.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020- 2023) kapsamında belirlenecek ve gerçekleştirilecek hedeflerin, Türkiye'nin kısa, orta ve uzun vadede daha büyük ölçekli hedeflerine de katkı sağlayacağı değerlendirilmektedir. Eylem planında 22 adet hedef belirlenmiştir. 2020-2023 dönemi için bu temel hedefler kapsamında stratejik amaçlar oluşturulmuş olup belirlenen stratejik amaçlar aşağıda yer almaktadır:

I. KRİTİK ALTYAPILARIN KORUNMASI VE MUKAVEMETİN ARTIRILMASI

- **"Siber Uzayda Ulusal Güvenlik":** Türkiye'de "Elektronik Haberleşme", "Enerji" "Finans", "Ulaştırma", "Su Yönetimi" ve "Kritik Kamu Hizmetleri" olarak tanımlanan kritik altyapı sektörlerinin korunmasına yönelik faaliyetler gerçekleştirilecektir.

II. ULUSAL KAPASİTENİN GELİŞTİRİLMESİ

- **"İnsan Kaynağının Güçlendirilmesi":** İnsan kaynağı yetkinliklerinin daha da üst düzeylere çıkarılması amaçlanmaktadır.

- **"Toplumsal Farkındalığın Artırılması ve Çocukların Çevrimiçi Korunması":** Tüm toplum genelinde, farkındalığı artırıcı çalışmaların gerçekleştirilecektir.

II. ORGANİK SİBER GÜVENLİK AĞI

- **"İleri Seviye Tehditlerle Mücadele":** Siber tehditlere karşı ekiplerin olgunluklarının geliştirilmesine yatırım yapılacaktır.

- **"Birlikte Daha Güçlüyüz":** Ekipler ve paydaşlarla karşılıklı destek ve geri bildirim mekanizmaları ile ulusal siber güvenliğe katkı sağlanması amaçlanmaktadır.

III. YENİ NESİL TEKNOLOJİLERİN GÜVENLİĞİ

- **"Güvenle Gelen Yeni Nesil Teknolojiler":** Yapay zekânın ve blok zincir teknolojilerinin siber güvenlik temelli ele alınması ve yerli teknolojilere yatırım yapılması amaçlanmaktadır.

IV. SİBER SUÇLARLA MÜCADELE

- **"Güvenli Siber Ortam":** Ulusal kapasitenin ve teknolojik imkânların artırılması amaçlanmaktadır.

- **"Uluslararası Mücadele":** Siber suçlara yönelik bilgi paylaşımı ve uluslararası iş birliğinin daha da geliştirilmesi hedeflenmektedir.

V. YERLİ VE MİLLİ TEKNOLOJİLERİN GELİŞTİRİLMESİ VE DESTEKLENMESİ

- **"Türkiye'nin Teknolojisi":** Siber güvenlik alanında öncü olmak hedeftir.

- **"Teknoloji Geliştirmede İş Birliği ve Destek Mekanizmaları":** Özel sektörün desteklenmesi için mevcut mekanizmalardan faydalanmak ve yeni mekanizmalar ile bu desteğin artırılması amaçlanmaktadır.

- **Siber Güvenlik Test ve Sertifikasyon Sistemi":** Yerli ürün ve hizmetlerin uluslararası pazarda rekabet edebilecek seviyelere yükseltilmesi için çalışmalar yapılması amaçlanmaktadır.

VI. SİBER GÜVENLİĞİN MİLLİ GÜVENLİĞE ENTEGRASYONU

- **"Ulusal Güvenlik İçin Siber Güvenlik":** Üst düzey milli güvenlik politikaları ile siber savunmayı da içeren hibrit tehditlerden korunmak ve caydırıcılığın artırılması amaçlanmaktadır.

VII. ULUSLARARASI İŞ BİRLİĞİNİN GELİŞTİRİLMESİ

- **"Sınırı aşan Tehditlerle Mücadele":** Uluslararası siber güvenlik faaliyetlerine katılım ve katkı sağlanması amaçlanmaktadır.

Onuncu bölümde ise planının gerçekleştirme yaklaşımı ele alınmıştır. Eylem planının hazırlanmasında çalışmalara yer verilmiş, izleme ve ölçüm kriterlerinin belirlendiği ifade edilmiş, geniş bir paydaş grubunun olduğu, kapsamının oldukça geniş tutulduğu, ihtiyaç duyulursa güncelleneceği vurgulanmıştır. Ayrıca, Eylem maddelerinde yer alan faaliyetler sorumlu 14 farklı kamu kurumu ve iş birliği yapılacağı ve 34 farklı kamu kurumunun çalışmalarıyla eylem planının yürütüleceği ifade edilerek planın kapsamına dikkat çekilmiştir.

4. TÜRKİYE'NİN SİBER GÜVENLİK EYLEM PLANLARININ DEĞERLENDİRİLMESİ

Bu bölümde eylem planlarını değerlendirme kriterleri ele alınacaktır. Daha sonra eylem planları süreklilik, kritik altyapı güvenliği için yatırım, Ar-Ge çalışmaları, liderlik, iş birliği, insan kaynağının geliştirilmesi, eğitim, yasal önlemler, bütçe ayrılması, caydırıcılık ve sonuçların izlenmesi kriterleri açısından değerlendirilecektir.

4.1. Değerlendirme Kriterleri ve Seçimi

Değerleme kriterlerinin seçiminde AB ülkelerinin ve İngiltere'nin siber güvenlik eylem planlarından yararlanılmıştır. AB'ye bağlı ağ ve bilgi güvenliğinden sorumlu kurum ENISA 13 Mart 2004 tarihinde kurulmuş olup 1 Eylül 2005 tarihinde faaliyete geçmiştir. ENISA, AB Siber Güvenlik Yasası ile yapısını güçlendirmiş olup, AB'nin siber politikasına katkıda bulunur, siber güvenlik sertifika programları ile bilgi ve iletişim teknolojileri ürünlerinin, hizmetlerinin ve süreçlerinin güvenilirliğini artırır, üye devletler ve AB kurumlarıyla iş birliği yapar ve Avrupa'nın siber saldırılara, siber terörizme ve siber korsanlığa karşı hazırlanmasına yardımcı olmaktadır. Ajansın internet sitesindeki eylem planları, yasal dokümanlar ve raporlar incelenerek aşağıdaki değerlendirme kriterleri oluşturulmuştur.

- **Süreklilik:** Eylem planları belirli dönemleri kapsayacak şekilde hazırlanmaktadır. Örneğin Türkiye'nin eylem planları 2013-2014, 2016-2019 ve 2020-2023 dönemlerini kapsamaktadır. Her dönemin amaç, hedef ve beklentileri benzer olabildiği gibi farklı bir şekilde de belirlenebilmektedir. Genel olarak beklenti ise bir gelişim süreci içinde birbirlerini tamamlamalarıdır.
- **Kritik Altyapıların Korunması:** Kritik altyapı kavramı, ilk olarak 1997 Ekim tarihli Amerika Birleşik Devletleri Başkanlık Komisyonu'nun Kritik Altyapıların Korunması Hakkında Raporu'nda dile getirilmiştir. Bu açıdan kavram, toplum ve devlet düzeninin sağlıklı biçimde işletilebilmesi için gerekli, birbirleriyle bağı olan sistemler ve bu sistemlerin istenilen biçimde çalışmasını sağlayan altyapılar bütününü ifade etmektedir. 2013-2014 Eylem Planında kritik altyapılar kamu kurumlarına ilave olarak enerji, haberleşme, su kaynakları, tarım, sağlık, ulaşım, eğitim ve finansal hizmetler olarak sıralanmıştır. Kritik Altyapılarda Bilgi Güvenliği Yönetimi Programı başlıklı 5. eylem maddesinde ise kritik altyapıların belirlenmesi alt amacındaki görev Türkiye Bilimsel ve Teknolojik Araştırma Kurumuna

(TÜBİTAK) verilmiştir. Ancak günümüze kadar resmi olarak bu kurumların belirlendiği veya kamuoyuna duyurulduğu bir belgeye rastlanılmamıştır.

- **Ar-Ge Destekleri:** Siber güvenlik alanı sürekli gelişen ve bu gelişmeyle birlikte açıkların ve zafiyetlerin ortaya çıktığı bir alandır. Bunun yanı sıra saldırı tekniklerinin değişmesi, alanın kendini sürekli olarak hazır tutmasını ve geliştirmesini zorunlu hale getirmektedir. Siber güvenlik alanı Ar-Ge yoğun bir yapıya sahip olmasından dolayı kamu sektörünün ilgili alanı teşvik etmesi, desteklemesi ve doğrudan yatırım alanı olarak belirlemesi gerekmektedir.
- **Siber Uzayda Liderlik:** Siber güvenlik alanında lider olmak siber saldırılara karşı caydırıcılık sağlar, teknolojik ilerlemelerde yönlendirici olunur, kritik altyapılarının korunması sağlanır, yetişmiş insan gücünün beşerî sermayesi kullanılır gibi birçok fayda sağlayacaktır. İncelenen pek çok eylem planında ülkelerin siber güvenlik alanında lider olması, piyasayı yönlendirmeyi ve sağlam bir caydırıcılık sistemi oluşturmayı amaçlamaktadır.
- **Ulusal ve Uluslararası İş Birliği:** Siber güvenlik alanının çok geniş olması, sürekli gelişmesi, her gün yeni açık ve zafiyetlerin keşfedilmesi bir örgütü, kamu kurumu, doğrudan devleti aşan bir yapıya sahiptir. Bunun yanı sıra bir kurum veya kuruluştaki zafiyet diğer kurumların sağlam altyapıya sahip olmasına rağmen saldırılara açık hale getirmektedir. Bu yüzden tüm aktörler arasında koordinasyonun sağlanması ve uluslararası iş birliklerinin geliştirilmesi siber savunma ve siber caydırıcılık için son derece elzemdir.
- **İnsan Kaynağının Geliştirilmesi:** Siber güvenlik alanında pek çok teknolojik ürün otomatik ve yapay zeka temelli olmasına rağmen etkin bir yapı için yetişmiş insan gücü hayati bir öneme sahiptir. Bu yüzden hem beşeri sermayenin kurulması hem korunması hem de geliştirilmesi eylem planlarının ana dayanak noktalarındandır.
- **Eğitim Faaliyetleri:** Eğitim faaliyetlerinin iki sacayağı vardır. İlk olarak insan gücünün kalitesinin artırılmasıdır. Daha sonra ise kapsamı oldukça geniş olan farkındalık temelli tanıtım, bilgilendirme, hazır bulundurma faaliyetleridir. İnsan zafiyetine ve farkındalığına aşırı bağımlı olan siber güvenlik bu açıdan eylem planlarında sürekli olarak ana hedef ve alt amaç olarak yer almaktadır.
- **Yasal Önlemler:** Yasal altyapının kurulması, suç ve cezaların tanımlanması güncel gelişmelere karşı sürekli olarak uyumlu bir şekilde ilerlemesi toplumsal ve kurumsal gelişmişliğin bir göstergesidir. Yasal altyapısı oluşturulmuş bir siber güvenlik hem korunmanın hem de mücadelenin önemli göstergesidir.
- **Bütçe Tahsisi:** Her bir eylem planında ana hedefler, alt amaçlar, sorumlu kurumlar ve faaliyetler yer almaktadır. Bunların hepsi belirli bir parasal gidere sahip özelliklidir. Hatta teknolojik altyapının yenilenmesi, geliştirilmesi, güncellenmesi çok daha maliyetlidir. Bu yüzden her bir eylem planının bir bütçesi olmalı ve hedefler özelinde bütçe tahsisi yapılmalıdır.
- **Siber Caydırıcılık:** Her sistem, kurum veya devlet siber saldırı tehdidi altındadır. Ancak sağlam bir altyapı, yetişmiş insan gücü, farkındalığı yüksek bireyler siber

saldırıları başlamadan önleyebilir. Saldırıların karşılığı olacağını veya saldırıları etkilerinin zayıflığının farkında olan siber korsanlar hiçbir faaliyette bulunmamayı tercih ederek daha zayıf yapılara yönelecektir. Bu durum siber caydırıcılık olarak adlandırılmakta olup devletlere maliyet tasarrufu, zararların etkilerini azaltma, kendini geliştirme gibi faydaları vardır. Bunun yanı sıra siber caydırıcılık ile siber alanda liderlik eş bir yapıya sahiptir.

- **Eylem Planı Sonuçların İzlenmesi:** Her bir eylem planı belirli bir dönemi kapsar. Bu dönem için belirlene hedef ve faaliyetlerin ne kadarının gerçekleştirildiği, hangi faaliyetlerde eksiklikler olduğu, sorumlu ve ilgili kurumların ne kadar başarılı olduğu izlenmeli ve kamuoyuyla paylaşılmalıdır. Böylece hem gelecek eylem planına gerçekçi bir zemin oluşur hem de planların hayata geçirilmesi teşvik edilebilir.

Şüphesiz değerlendirme kriterlerinin çoğaltılması veya azaltılması mümkündür. Çalışmanın genel yapısının derli toplu olması açısından on bir adet kriter yeterli görülmüştür. Aşağıdaki bölümde Türkiye'nin üç eylem planının çalışma içinde belirlenen kriterler açısından değerlendirilmesi yapılacaktır.

4.2. Türkiye'nin Eylem Planlarının Değerlendirmesi

Siber güvenlik son yirmi yılın en çok tartışılan ve hakkında araştırma yapılan konularından bir tanesidir. Her gün mutlaka bir habere rastlamak mümkün olan bu konunun genişliği ve güncelliği uzun süre devam edecek gibi görünmektedir. Devletlerin daha güçlü bir şekilde konunun üzerine gitmeleri, teknolojilerini geliştirmeye çalışmaları ve sürekli olarak siber saldırı veya tehditlerle karşı karşıya kalmaları bunun bir göstergesidir. Bu yüzden ülkeler siber güvenlik konusunda daha sistemli hareket etmek için eylem planları, strateji belgeleri, rehber dokümanlar hazırlamakta ve kendilerini yükümlülük altına sokmaktadır. Önceki bölümde açıklanan 11 adet değerleme kriteri açısından Türkiye'nin 2013-2014, 2016-2019 ve 2020- 2023 dönemi eylem planları incelenecek ve son olarak tüm planlar toplu bir şekilde ele alındıktan sonra öneriler geliştirilecektir.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı ilk yayımlanan belge olduğu için süreklilik kriteri açısından değerlendirilmez. Eylem planında kritik altyapıların belirlenmesi ve güvenliğinin sağlanması, bunun için iş birliği geliştirilmesi ve bir program dahilinde bu sürecin yönetilmesi hedeflenmiştir. Dönem içinde kamuoyuna yansıyan belirleme veya program olmamıştır. Araştırma ve geliştirme faaliyetlerine plan içinde vurgu yapılmış ve ana hedeflerden biri olarak belirlenmiştir. Bunun yanı sıra Ar-Ge laboratuvarlarının kurulması ve yerli ürünlerin teşvik edilmesi hedeflenmiştir. Siber güvenlik alanında liderlik yerine Türkiye liderliğinde uluslararası siber güvenlik tatbikatlarının ilkinin düzenlenmesi amaçlanmıştır. Eylem planında hem yerel hem de uluslararası aktörlerle iş birliği hedeflerine özel önem verilmiştir. Ülke kaynaklarının optimum kullanılması için insan kaynağının geliştirilmesi ve eğitim faaliyetlerine yönelik amaçlar ile birlikte tüm sürecin yasal altyapının kurulması hedeflenmiştir. Ancak eylem planı için herhangi bir bütçe belirlenmemiş, tahsis edilmemiş olup siber caydırıcılık konusuna da değinilmemiştir. Eylem planındaki hedeflerin yıllık veya dönemsel gerçekleşmeleri, tamamlanmaları veya eksiklikleri kamuoyuna açıklanmamıştır.

2016-2019 Ulusal Siber Güvenlik Stratejisi kamuoyuna açıklanmasına rağmen eylem planı hizmete özel tutularak açıklanmamıştır. Bu açıdan değerlendirme strateji belgesi kapsamında

yapılmıştır. Süreklilik açısından eski eylem planıyla aralarında bir yıllık fark olduğu için belgenin eksik kaldığını söylemek mümkündür. Kritik altyapılar bu dokümanda da tanımlanmamış olmasına rağmen altyapıların korunması, yerli ürünlerle donatılması, tesislerin birbirleriyle entegre edilmesi hedeflenmiştir. Ar-Ge faaliyetlerine yönelik spesifik bir hedef yer almamasına rağmen metin içinde yerli ürün temelli Ar-Ge çalışmalarının desteklenmesine, Ar-Ge koordinasyonuna ve Ar-Ge çıktılarının korunmasına özel önem verilmiştir. Belge içinde liderlik temelli bir hedef ve ifade yer almamış, tüm paydaşlarla bilgi paylaşımı temelli iş birliği ve uluslararası siber olay yönetimi işbirliği hedeflenmiştir. Siber güvenlik alanında yetişmiş insan kaynağı gücünün yükseltilmesi, farkındalık eğitimleri ve siber güvenlik eğitimlerine yönelik hedefler dokümanda geniş yer tutmaktadır. Uluslararası standartlara uygun mevzuatın oluşturulması ise ana dayanak noktalarından birisidir. Bu planda da bütçe ile düzenleme yer almamakta olup siber caydırıcılık hedefine yer verilmemiştir. Strateji belgesindeki amaçların gerçekleşmeleri kamuoyuna açıklanmamıştır.

2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı sürekliliğe sahip olmasına rağmen 2020 yılının sonunda yayımlanması ile birlikte bir yıllık ara süreklilik ilkesine zarar vermiştir. Eylem planında kritik altyapılar, elektronik haberleşme, enerji, finans, ulaştırma, su yönetimi ve kritik kamu hizmetleri olarak belirlenmiş olup korunmasına yönelik ana hedefe yer verilmiştir. Diğer eylem planlarında olduğu gibi Ar-Ge ve yerli ürünlerin geliştirilmesi destekleneceği ve böylece lider ülke olma hedefi bu eylem planında yer almıştır. Uluslararası işbirliği eylem planında ana hedeflerden birisi olarak belirlenmiş olup teknoloji geliştirmede iş birliği ve destek mekanizmalarına özel önem verilmiştir. İnsan kaynağının güçlendirilmesi ve eğitim faaliyetleri diğer eylem planlarında olduğu gibi 2020-2023 eylem planında da yer almıştır. Bu eylem planında yasal altyapının geliştirilmesine yönelik herhangi bir hedefe yer verilmemiştir. Bütçe tahsisinin yapılmadığı bu eylem planında ilk kez caydırıcılığın artırılarak siber suçların azaltılması amaçlanmıştır. Eylem planının izlenmesine yönelik şu ana kadar herhangi bir doküman yayımlanmamıştır. Özetle kriterler ve eylem planlarının içeriği aşağıda tablo halinde sunulmuştur.

Tablo-1. Değerlendirme Kriterleri Açısından Türkiye'nin Siber Güvenlik Eylem Planları (1)

Eylem Planı Dönemi	Süreklilik	Kritik Altyapıların Korunması	Ar-Ge Destekleri	Siber Uzayda Liderlik	Ulusal ve Uluslararası İş Birliği
2013-2014 Dönemi	İlk plandır. **(✓)**	Kritik altyapılar tanımlanmamıştır olup korunması hedeflenmiştir. **(✓)**	Yerli teknolojiler özelinde hedeflenmiştir. **(✓)**	Uluslararası tatbikat yapılması hedeflenmiştir. **(✓)**	Hem yerel hem de uluslararası aktörlerle iş birliği hedeflenmiştir. **(✓)**
2016-2019 Dönemi	Arada 1 yıl ara vardır. **(X)**	Kritik altyapılar tanımlanmamıştır olup korunması hedeflenmiştir. **(✓)**	Yerli ürün Ar-Ge çalışmalarının desteklenmesi, koordinasyonu ve Ar-Ge çıktılarının korunmasına yer verilmiştir. **(✓)**	Belge içinde bu konuda herhangi bir ifade yer almamıştır. **(X)**	Tüm paydaşlarla bilgi paylaşımı temelli işbirliği ve uluslararası siber olay yönetimi işbirliği hedeflenmiştir. **(✓)**
2020-2023 Dönemi	Devamlılık vardır. Ancak 2020 yılının sonunda yayımlanmıştır. **(X)**	Kritik altyapılar; belirlenmiş olup korunmasına yönelik ana hedefe yer verilmiştir. **(✓)**	Ar-Ge ve yerli ürünlerin geliştirilmesi destekleneceği ifade edilmiştir. **(✓)**	Lider ülke olma hedefi bu eylem planında yer almıştır. **(✓)**	Uluslararası iş birliği hedef olarak belirlenmiştir. **(✓)**

Tablo-2. Değerlendirme Kriterleri Açısından Türkiye'nin Siber Güvenlik Eylem Planları (1)

Eylem Planı Dönemi	İnsan Kaynağının Geliştirilmesi	Eğitim Faaliyetleri	Yasal Önlemler	Bütçe Tahsisi	Siber Caydırıcılık	Sonuçların İzlenmesi
2013-2014 Dönemi	İnsan kaynağının geliştirilmesine yer verilmiştir. **(✓)**	Eğitim faaliyetlerine yer verilmiştir. **(✓)**	Yasal altyapının kurulması hedeflenmiştir. **(✓)**	Bütçe tahsisi yapılmamıştır. **(X)**	Siber caydırıcılık konusuna değinilmemiştir. **(X)**	Eylem planının sonuçları veya gerçekleşmeleri duyurulmamış. **(X)**
2016-2019 Dönemi	Yetişmiş insan kaynağı gücünün yükseltilmesi yer almıştır. **(✓)**	Farkındalık eğitimleri yer almıştır. **(✓)**	Uluslararası standartlara uygun mevzuatın oluşturulması hedeflenmiştir. **(✓)**	Bütçe tahsisi yapılmamıştır. **(X)**	Siber caydırıcılık konusuna değinilmemiştir. **(✓)**	Strateji belgesinin hedef gerçekleşmeleri açıklanmamış. **(X)**
2020-2023 Dönemi	İnsan kaynağının güçlendirilmesi amaçlanmıştır. **(✓)**	Eğitim faaliyetleri ve farkındalık eğitimleri amaçlanmıştır. **(✓)**	Yasal altyapının geliştirilmesine yönelik hedef oluşturulmamıştır. **(X)**	Bütçe tahsisi yapılmamıştır. **(X)**	Siber caydırıcılığın artırılması amaçlanmıştır.	Eylem planının geçekleşmeleri su ana kadar açıklanmamış. **(X)**

Eylem planları bir bütün olarak değerlendirildiğinde genel olarak kriterlerin çoğunu karşıladığı görülmektedir. Bütçe tahsisi yapılmamış olması, uzun bir süre siber caydırıcılığın amaçlanması ve bazı dönemlerde yasal altyapının, sürekliliğin ve planların izlenmesinin ihmal edilmesi olumsuz göstergelerdir.

SONUÇ

Ulusal güvenlik kavramının bir yansıması olan siber güvenlik internet teknolojilerinin hayatımıza girmesiyle gündeme gelmiştir. Bilgisayar virüsleri, zafiyetler, saldırılar, terörist eylemler, bilgi hırsızlıkları, patent ihlalleri, sabotajlar, hizmet aksatma faaliyetleri gibi pek çok kavram ve uygulama insanların günlük hayatını etkilemiş, kurumların yapısına zarar vermiş ve devletlerin önlem almasını zorunlu kılmıştır.

Siber güvenlik alanının her türlü bilgi ve iletişim aracıyla ilişkili olması, insan kontrolü olmadan sistemleri işletilmesi, verilerin saklanması, gizli bilgilerin güvence altında tutulması ve kritik alt yapıların korunması gibi pek çok yansıması bulunmaktadır. Bu açıdan tek bir insandan bir kuruma ve hatta devletin tamamına etki edebilecek genişlikte bir kavramdır. Son yıllarda katlanarak artan siber saldırılar, hırsızlıklar, terörist faaliyetler, sabotajlar devletlerin ve kurumların önlem almasını zorunlu kılmıştır. Bu açıdan ülkeler altyapılarını korumak, farkındalığı yükseltmek, teknolojik gelişmeleri takip etmek ve sektörde yer almak için planlar hazırlamaktadır. Türkiye gelişmelerden etkilenerek 2013-2014, 2016-2019 ve 2020-2023 dönemlerini kapsayan siber güvenlik eylem planları ve stratejileri hazırlamıştır.

Ülkemizin siber güvenlik eylem planları belirlenen süreklilik, kritik altyapıların korunması, Ar-Ge destekleri, siber uzayda liderlik, ulusal ve uluslararası iş birliği, insan kaynağının geliştirilmesi, eğitim faaliyetleri, yasal önlemler, bütçe tahsisi, siber caydırıcılık, sonuçların izlenmesi kriterleri açısından değerlendirmeye tabii tutulmuştur.

Eylem planlarının süreklilik açısında birtakım eksikleri vardır. Bunun temel nedeni ana sorumlu kurumun belirlenmemesi, Siber Güvenlik Kurulunun işlevini yitirmesi ve koordinasyon güçlüğüdür. Bu açıdan merkezi bir idarenin oluşturulması ve Siber Güvenlik Kurulunun yeniden işlev kazanması önerilmektedir. Kritik altyapıların geçte olsa belirlenmesi olumlu bir gelişme olup altyapıların özeline yönelik eylem planları ve stratejiler geliştirilebilir. Yerli teknolojiler gelişmesi, mevcut teknolojilere uyumlu bir şekilde kullanılması ve sürekli ilerleme içinde olunması için Ar-Ge destekleri önemlidir. Bu açıdan belirli bir bütçe ile Ar-Ge desteklerinin verilmesi ve kamuoyuyla paylaşılması önerilmektedir. Böylece siber uzayda hedeflenen liderlik düzeyine erişim sağlanabilir.

Siber güvenliğin bir bütün olarak ele alınması ve tüm paydaşların aktif katılımın gerekmesi ulusal ve uluslararası iş birliğine ihtiyaç duymaktadır. Bu açıdan Türkiye'nin ENISA bünyesine katılması, ortak tatbikatlar düzenlemesi, uluslararası testler yapılması gibi bir takım iş birliği temelli faaliyetler önerilmektedir. Alanın özü itibarıyla insan kaynağına ve beşeri sermayeye aşırı bağımlı olması eğitim faaliyetlerinin ön planda tutulmasını zorunlu kılmıştır. Ayrıca tanıtım, bilgilendirme ve hatırlatma ile toplumsal farkındalığın yükseltilmesi siber güvenliğin ana destekleyici olacaktır.

Yasal altyapının kurulması güveni ve caydırıcılığı yükseltecektir. Alanın sürekli ilerlemesi ve her gün yeni yansımalarının ortaya çıkması mevzuat çalışmalarının süreklilik kazanmasını gerektirmektedir. Böyle bir hazırlık saldırı veya eyleme geçmeden önce kişi ve kurumlara karşı caydırıcılık kazandıracaktır. Asıl hedef bu açıdan ülke olarak siber caydırıcılığa ulaşmak olmalıdır. Tüm bu hedeflerin gerçekleştirilmesi için bütçeye ihtiyaç duyulacaktır. Bu yüzden eylem planlarındaki her hedef için bir bütçe tahsisinin yapılması önerilmektedir. Hedeflerin ne kadarına ulaşıldığı, hangi alanlarda eksik kalındığı ve ilerleme seviyesi eylem planlarının yıllık veya dönemsel izlenmesiyle sağlanabilir. Söz konusu izleme mekanizmalarının kurulması ve kamuoyuyla ilerlemenin paylaşılması önerilmektedir.

Gelecek çalışmaların değerleme kriterlerinin artırarak ve kurumsal planların da incelemeye dahil edilerek yapılması ülkenin seviyesini ölçmek için verimli olabilir. Bunun yanı sıra yapılacak çalışmaların araştırma yöntemlerinden anket, görüşme, vaka analizi gibi metotların kullanılması önerilmektedir.

KAYNAKÇA

Ada, M. (2018), NATO Üyesi ülkelerin siber güvenlik stratejileri açısından incelenmesi, T.C. Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim Anabilim Dalı, Yüksek Lisans Tezi.

Ağır, B. S. (2015), "Güvenlik kavramını yeniden düşünmek: Küreselleşme, kimlik ve değişen güvenlik anlayışı", Güvenlik Stratejileri Dergisi, 11 (22), s. 97-130.

Ak, T. Y., & Duru, B. T. D. (2013), Ulusal güvenlik-çevresel güvenlik ekseninde silahlı kuvvetler çevre ilişkisi, Doctoral dissertation, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Sosyal Çevre Bilimleri Anabilim Dalı.

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

Aydın, A. H., (2008), "Toplumsal Güvenlik ve Yerel Siyaset", Yerel Siyaset Dergisi, 28, s. 8-17.

Barry, B. (1998), Security: A new framework for analysis, UK: Lynne Rienner Publishers.

"Botnets: Detection, Measurement, Disinfection & Defence", ENISA, Erişim tarihi: Nisan 07, 2020, https://www.enisa.europa.eu/activities/Resilience-and-

CIIP/criticalapplications/botnets/botnets-measurement-detection-disinfection-anddefence/at_download/fullReport.

Canbek, G., & Sağıroğlu, Ş. (2007), "Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma", Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 22 (1), s. 121-136.

Chen, P., Desmet, L., vd. (2014, September), "A study on advanced persistent threats", 15th IFIP International Conference on Communications and Multimedia Security, s. 63-72.

Clarke, R. A. and Knake R., Cyber War, Harper Collins e-books.

Collin, B. C. (1997, March), "The future of cyberterrorism: Where the physical and virtual worlds converge", In 11th annual international symposium on criminal justice issues.

"Computer Viruses and Other Malicious Software: A Threat to the Internet Economy", OECD Publishing, Erişim tarihi: Mayıs 15, 2020, http://www.keepeek.com/Digital-Asset-Management/oecd/science-andtechnology/computer-viruses-and-other-malicious-software_9789264056510-en#page1

Dedeoğlu, B., (2003), Uluslararası Güvenlik ve Strateji, İstanbul: Derin Yayınları.

Denning, D. (2001), "Is Cyber Terror Next? New York: US Social Science Research Council" SSRC, Erişim Tarihi: Mayıs 05, 2020, http://www.ssrc.org/sept11/essays/denning.htm.2001.

Erhan, Ç., (2002), Soğuk Savaş Sonrası ABD'nin Güvenlik Algılamaları, Uluslararası Güvenlik Sorunları ve Türkiye, Ankara: Seçkin Yayıncılık.

Goodrıch, Michael and TAMASSİA, Roberto, Introduction to Computer Security. Essex: Pearson, 2010.

"Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması", TÜİK (TÜRKİYE İSTATİSTİK KURUMU), Erişim Tarihi: Aralık.28, 2020, https://www.ab.gov.tr/65.html.

Klımburg, A., National Cyber Security Framework Manual. Tallin: NATO CCD COE Publications, 2012.

Koçer, G., (2004), "Küreselleşme ve Uluslararası İlişkilerin Geleceği", Uluslararası İlişkiler, 1 (3), s.101-122.

Krause, K., Wıllıams M. C., (1996), "Broadening the Agenda of Security Studies: Politics and Methods", Mershon International Studies Review, 40 (2), s. 229-254.

"Law (Kanun)", European Commıssıon (EC), Erişim Tarihi: Mayıs 05, 2020, https://ec.europa.eu/info/law_en.

Lord, K. M., America's Cyber Future: Security and Prosperity in the Information Age (Volume II), 2011, Zurich: Center for New American Studies.

Miller B., (2001), "The Concept of Security: Should it be Redefined?", The Journal of Strategic Studies, 24 (2), s. 16-17.

"Modern Trends in the Cyber Attacks against the Critical Information Infrastructure", Modern Trends in the Cyber Attacks against the Critical Information Infrastructure s. 1-95. Erişim tarihi: Nisan 30, 2020, http://docplayer.net/756920-Modern-trends-in-the-cyber-attacksagainst- the-critical-information-infrastructure.html.

O'hara, C.. (2012), "Global Cyber Sleuth. The State Department's Chris Painter relishes his role as a cyber diplomat." Leadership Winter, s.36-43.

Oğuzlu, H. T.,(2007), "Dünya Düzenleri ve Güvenlik: Ulus-Devlet Güvenlik Anlayışı Aşılıyor Mu?", Güvenlik Stratejileri Dergisi, 3 (6), s. 1-35.

"On Cyberwarfare", DCAF Horizon, Working Paper No.7, 61, Erişim tarihi: Ekim 17, 2020, https://docplayer.net/4159538-Dcaf-horizon-2015-working-paper-no-7-on-cyberwarfare-fred-schreier.html

Özbay, R.,(2015), Aktif Siber Savunma Teknikleri ve Performans Analizi, Yayınlanmış Yüksek Lisans Tezi, İnternet ve Bilişim teknolojileri Yönetimi Anabilim Dalı, Fen Bilimleri Enstitüsü, Afyon Kocatepe Üniversitesi, Afyon.

Saltzer, J. H., Schroeder, M. D. (1975), "The Protection of Information in Computer Systems"Proceedings of the IEEE, 63 (9), s. 1278-1308.

"Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler", Bilgi Teknolojileri Üst Kurulu, Erişim tarihi: Mayıs 18, 2020, http://www.cybersecurity.gov.tr/publications/sg.pdf.

"Social Engineering Fundamental, Part I: Hacker Tactics", Security Focus Online, Erişim Tarihi: Nisan 06, 2020, http://online.securityfocus.com/infocus/1527

"Sosyal Mühendislik Saldırıları", Ulusal Bilgi Güvenliği Kapısı, Erişim Tarihi: Mayıs 05, 2020, http://www.bilgiguvenligi.gov.tr/sosyal-muhendislik/sosyal-muhendislik-saldirilari3.html.

Tekerek, M., (2008), "Bilgi Güvenliği Yönetimi", KSÜ Fen ve Mühendislik Dergisi, 11(1), s. 132-137.

"The Internet of Things. How the Next Evolution of the Internet Is Changing Everything", Cisco, Erişim Tarihi: Mayıs 12, 2020, http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Terriff, T. , Croft, S., vd. (1999), "Security Studies Today", Cambridge: Polity Press, USA,

"Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", Bilgi Teknolojileri ve İletişim Kurumu, Erişim tarihi: Ekim 17, 2020, https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf

"Ulusal Siber Güvenlik Stratejisi 2020 – 2023", İTU, Erişim tarihi: Ekim 17, 2020, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/NationalCybersecurityStrategyOfTURKEY.pdf

Varlık, A. B., (2015), Milli Güvenlik Teorisi, Ankara: Kripto Yayınları.

Yılmaz, S. (2007), "Güçsüz güç", Güvenlik Stratejileri Dergisi, 3 (5), s. 67-103.

Waltz, K. N. (2010), "Theory of international politics", Waveland Press.

Wiener, N. (2019), "Cybernetics or Control and Communication in the Animal and the Machine", MIT press.

"Written Comments of Dr. John R. Levine", Commerce Senate, Erişim tarihi: Ocak 15, 2021, http://www.commerce.senate.gov/pdf/levine032304.pdf

"2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı", Ulaştırma ve Altyapı Bakanlığı, Erişim tarihi: Ekim 17, 2020, https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf