T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİMDALI
YÖNETİM BİLİŞİM SİSTEMLERİ

SİBER GÜVENLİK POLİTİKALARI VE SİBER GÜVENLİK POLİTİKALARI HAKKINDA TÜRKİYE VE DİĞER ÜLKELER ÜZERİNDE İNCELEME

HASAN ALKAN

YÜKSEK LİSANS TEZİ

DANIŞMAN:

PROF. DR. MUHAMMET FATİH BİLAL ALODALI

KONYA-2023

T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİMDALI
YÖNETİM BİLİŞİM SİSTEMLERİ

SİBER GÜVENLİK POLİTİKALARI ve SİBER GÜVENLİK POLİTİKALARI HAKKINDA TÜRKİYE VE DİĞER ÜLKELER ÜZERİNDE İNCELEME

HASAN ALKAN

YÜKSEK LİSANS TEZİ

DANIŞMAN:

PROF. DR. MUHAMMET FATİH BİLAL ALODALI

KONYA-2023

T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ

Sosyal Bilimler Enstitüsü

Bilimsel Etik Sayfası

Öğrencinin	Adı Soyadı	HASAN ALKAN		
	Numarası	19081031022		
	Ana Bilim / Bilim Dalı	YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI		
	Programı	Tezli Yüksek Lisans	X	
		Doktora		
	Tezin Adı	SİBER GÜVENLİK POLİTİKALARI ve SİBER GÜVENLİK POLİTİKALARI HAKKINDA TÜRKİYE VE DİĞER ÜLKELER ÜZERİNDE İNCELEME		

Bu tezin hazırlanmasında bilimsel etiğe ve akademik kurallara özenle riayet edildiğini, tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada başkalarının eserlerinden yararlanılması durumunda bilimsel kurallara uygun olarak atıf yapıldığını bildiririm.

HASAN ALKAN

T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü

ÖZET

Öğrencinin	Adı Soyadı	HASAN ALKAN		
	Numarası	19081031022		
	Programı	YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI		
		Tezli Yüksek Lisans	X	
		Doktora		
	Tez Danışmanı	PROF. DR. MUHAMMET FATİH BİLAL ALODALI		
	Tezin Adı	SİBER GÜVENLİK POLİTİKALARI VE SİBER GÜVENLİK POLİTİKALARI HAKKINDA TÜRKİYE VE DİĞER ÜLKELER ÜZERİNDE İNCELEME		

Teknoloji tüm dünya üzerinde hızla gelişmeye devam etmektedir. Bu gelişmeler sayesinde küreselleşme, ülkelerin birbirleri ile etkileşimleri, birbirlerine karşı tutum ve davranışları da değişmektedir. Teknolojinin gelişmesi, internetin yaygın olarak kullanılması ile yeni kavramlar hayatımıza girmektedir. Siber kavramı, siber güvenlik kavramı bu kavramlardan bir tanesidir.

Ülkelerin gelişen teknolojiyi yakından takip etmesi ve buna yetişmek için yaptığı çalışmalar siber güvenlik, siber saldırı, siber politika kavramlarını doğurmuştur. Artık fiziki savaşlar yerini siber savaşlara bırakmıştır. Durum böyle olunca, ülkelerin sınırlarının kalkması, fiili savaşları siber savaşlara dönüştürmüştür. Siber savaşlar, ülkelerin siber güvenlik politikalarında çalışmalar yapmasını, bu alandaki çalışmalarını hızlandırmasına neden olmuştur. Askeri alandaki çalışmalara ek olarak siber alandaki çalışmalar için de aynı askeri alana ayrılan bütçe gibi siber alana da ek olarak bütçeler ayrılmaya başlanmıştır. Rusya, Çin ve ABD siber güvenlik alanında gelişim açısından en büyük ülkeler olurken Türkiye, Hindistan, Kuzey Kore, Almanya gibi ülkeler siber alanda gelişmekte olan ülkelere örnek olarak gösterilebilir. Ülkeler siber güvenlik politikalarını hazırlarken, birbirlerinden etkilenerek, ulusal olarak çeşitli tatbikatlar yaparak bu alandaki açıklarını tespit ederek bunları ortadan kaldıracak çalışmalar yapmaktadır.

Siber güvenlik politikaları hazırlanırken tüm unsurlar gözetilerek, diğer ülkelerin izlediği politikalar ve çalışmalar takip edilerek ülkenin şartlarına uygun siber güvenlik politikaları ve eylem planları hazırlanmalıdır.

T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü

ABSTRACT

Author's	Name and Surname	HASAN ALKAN		
	Student Number	19081031022		
		DEPARTMENT OF MANAGEMENT INFORMATIN SYSTEMS		
	Study Programme	Master's Degree (M.A.)	X	
		Doctoral Degree (Ph.D.)		
	Supervisor	PROF. DR. MUHAMMET FATİH BİLAL ALODALI		
	Title of the Thesis/Dissertation	CYBER SECURİTY POLİCES AND A REVİEW ON CYBER SECURİTY POLİCİES İN TÜRKİYE AND OTHER COUNTRİES		

Technology continues to develop rapidly all over the World. Thanks to these developments, globalization, the interactions of countires with each other, their attitudes and behaviors towards each other also change. With the development of technology and the widespread use of the internet, new concepts enter our lives. The concept of cyber, the concept of cyber security are some of these concepts.

The countries close follow up of the developing technology and efforts to keep up with it have given birth to the concepts of cyber security, cyber attack and cyber policy. Now physical wars have left their place to cyber wars. When this is the case, the removal of the borders of the countries has turned the actual wars into cyber wars. Cyber wars have caused countries to work on their cyber security policies and accelerate their work in this area. In addition to the works in the military field, budgets have begun to be allocated to the military field for the studies in the cyber field. While Russia, China and the USA are the biggest countries in terms of development in the field of cyber securtiy, countries such as Turkey, India, North Korea and Germany can be shown as examples of developing countries in the field of cyber security. While countries are preparing their cyber security policies, they are influenced by each other, conduct various exercises nationally, identify the gaps in this area and work to eliminate them.

Cyber security policies and action plans should be prepared in accodance with the conditions of the country by considering all the elements while preparing the cyber security policies, by following the policies and studies followed by other countries.

İÇİNDEKİLER

İKİNCİ BÖLÜM

TÜRKİYE'DE SİBER GÜVENLİK POLİTİKALARI

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

GRAFİKLER LİSTESİ

KISALTMALAR LİSTESİ

AB : Avrupa Birliği

ABD : Amerika Birleşik Devletleri

AFAD : Afet ve Acil Durum Yönetim Başkanlığı

APT : Gelişmiş Kalıcı Tehditler

AR-GE : Araştırma ve Geliştirme

ARPANET : Advanced Research Projects Authority Net

AUSSI : Fransız Ulusal Bilgi Güvenliği Ajansı

BİLGEM : Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi

BM : Birleşmiş Milletler

BSI : Federal Bilgi Güvenliği Ordusu

BTK : Bilgi Teknolojileri ve İletişim Kurumu

CCD COE : Siber Savunma Merkezi

CCIRC : Kanada Siber Olaylara Müdahale Merkezi

CDMA : Sanal Savunma Yönetimi Otoritesi

CERT-In : Computer Emergency Response Team Indian

CERT : Computer Emergency Response Team

CMK : Ceza Muhakemesi Kanunu

CMP : Kriz Yönetim Planı

CMS : Central Monitoring System

COMSEC : İletişim Güvenliği (Communications Security)

CS&C : Siber Güvenlik ve İletişim Departmanı

DCSSI : Bilgi Sistemleri Güvenlik Merkezi

DDK : Devlet Denetleme Kurulu

DHS : İç Güvenlik Bakanlığı (United States Department of Homeland Security)

DoD : Department of Defense

DoS : Disk İşletim Sistemi (Disk Operating System)

DDoS : Dağıtık Hizmet Reddi Saldırıları (Distributed Denial of Service attack)

DPT : Devlet Planlama Teşkilatı

DTC : Direction Technique du Chiffe

EGM : Emniyet Genel Müdürlüğü

E-İmza : Elektronik imza

ENİSA : European Network and Information Security

FBI : Federal Bureau of Investigation

GCI : Global Connectednes Index

GGE : Bilgi Güvenliği Devlet Uzmanları Grubu

GSES : Grid Security Expert System

HAVELSAN : Hava Elektronik Sanayi ve Ticaret A.Ş.

IoT : Internet of Things

IPA : AB Katılım Öncesi Mali Yardım Aracı

ISTF : Inter Departmental Information Security Task Force

ITU : International Telecommunication Union

KDEP : Kısa Dönem Eylem Planı

MİLNET : Militarynet

MEITY : Birlik Eletronik ve Bilgi Teknolojisi Bakanlığı

MGK : Milli Güvenlik Kurulu

NATO : Kuzey Atlantik Antlaşması Örgütü (North Atlantic Treaty Organization)

NCCC : Ulusal Siber Koordinasyon Merkezi

NCIIPC : Ulusal Kritik Bilgi Altyapı Koruma Merkezi

NeTRA : Network Traffic Analysis System

NIPC : Ulusal Altyapı Koruma Merkezi

NPC : Standing Committee of the National Peoples Congress

NSA : Ulusal Güvenlik Ajansı

NSD : National Security Database

ODTÜ : Orta Doğu Teknik Üniversitesi

OECD : Ekonomik Kalkınma ve İşbirliği Örgütü

OIP : Altyapı Koruması

OKTEM : Ortak Kriter Test Merkezi

RFBGD : Rusya Federasyonu Bilgi Güvenliği Doktorini

RSG : Rusya Siber Güvenlik Stratejisi

SGE : Siber Güvenlik Enstitüsü

SGK : Siber Güvenlik Kurulu

SİSATEM : Siber Savunma Teknoloji Merkezi

SOME : Siber Olaylara Müdahale Ekipleri

SSCB : Sovyet Sosyalist Cumhuriyetler Birliği

SSMP : Siber Savunma Merkezi Projesi

STC-CH : Service Central Technique du Chiffre

TBMM : Türkiye Büyük Millet Meclisi

TCK : Türk Ceza Kanunu

TİB : Telekomünikasyon İletişim Başlanlığı

TR-BOME : Türkiye Bilgisayar Olayları Müdahale Ekibi

TSK : Türk Silahlı Kuvvetleri

TÜBİTAK : Türkiye Bilimsel ve Teknik Araştırma Kurumu

TUENA : Türkiye Ulusal Enformasyon Altyapısı

UDH : Ulaştırma, Denizcilik ve Haberleşme Bakanlığı

UDHB : Ulaştırma ve Altyapı Bakanlığı

UEAKE : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

USGSEP : Ulusal Siber Güvenlik Stratejisi ve Eylem Planları

USOM : Ulusal Siber Olaylara Müdahale Merkezi

ÖNSÖZ

Gelişen teknoloji ile tüm dünya üzerine küresel olarak her alanda internet kullanılmaya başlanmıştır ve günden güne yaygınlaşmaktadır. Tüm kişi, kurum ve kuruluşlar internet üzerinden birçok işini halledebilmektedir. Durum böyle olunca siber alandaki güvenlik açıkları, tehditler söz konusu haline gelmiştir. Geçmişten günümüze değerlendirme yapıldığında gerçekleşen siber saldırılar her ülkenin kendi standartlarına ve şartlarına göre önlemler almasına neden olmuştur. Teknolojinin bu kadar hızlı gelişmesi ile siber alandaki savaşların, siber tehditlerin artışı da doğal olarak gerçekleşmiştir. Söz konusu gelişimler yeni tür saldırılara, yeni tür savaşlara, yeni savunma yöntemlerine yer açmıştır. Kişilerin, kurumların birçok işini internet üzerinden dijital ortamda halledebilmesi, kurum ve kuruluşların verilerinin tamamının internet ortamında saklanması siber güvenlik alanında yeterli düzeyde önlemler alınmasına sebep olmuştur. Türkiye ve diğer ülkeler göz önünde bulundurulduğunda her ülkenin kendisine göre siber güvenlik politikaları belirlediği, kendi şartlarına göre stratejiler uyguladığı tespit edilmiştir. Geçmişte yaşanılan saldırılar, tehditler karşısında kimi ülkeler siber güvenlik alanındaki çalışmalarına erkenden başlarken kimi ülkelerinde gündemine çok geç gelmiş ya da hiç gelmemiştir.

Tez dönemim boyunca bana yardımlarını esirgemeyen ve her sorduğuma hiç sıkılmadan cevap veren değerli danışmanım Prof. Dr. Muhammet Fatih Bilal ALODALI'ya, değerli hocam tezin düzenlenme aşamasında yardımcı olan Prof. Dr. Mustafa KOCAOĞLU'na, ders dönemindeki yardım ve desteklerinden ötürü Doç. Dr. Kazım KARABOĞA'ya, tüm eğitim hayatım boyunca bana maddi manevi desteklerini hiç esirgemeyen ve bugünlere gelmemdeki en büyük destekçim olan halam, değerli öğretmen Şerife ALKAN'a,

Tezi bitirmem ve yazmam için beni teşvik eden, sürekli destek olan ve yardımlarını hiç esirgemeyen, hiç sıkılmadan bana her gün tez ne durumda diye soran nişanlım Rabia'ya, benden desteklerini hiçbir zaman esirgemeyen babam Hüseyin ALKAN'a, annem Pınar ALKAN'a teşekkürü borç bilirim.

Hasan ALKAN-Konya 2023

GİRİŞ

Değişen dünya düzeni ve teknolojinin gelişmesi ile tüm dünyayı içine alan küreselleşme kavramı günden güne büyümektedir. Bu büyüme ile ülkelerin birbirleri arasındaki sınırların ortadan kalması, her ülkenin birbirinden haberdar olması, olası en ufak bir gelişmeyi dahi tüm dünya aynı anda öğrenebilmektedir. Bu küreselleşmenin bu kadar çabuk gelişmesi ve bu hızın sağlanması da internet üzerinden gerçekleşmektedir. İnternetin yaygın olarak her ülkede aktif olarak kullanılması, her geçen gün kullanım oranının artması, devletin kamu işlerinde, bireylerin kendi özel işlerinde kullanması ülkeler arasındaki sınırları kaldırmış, ülkeler arasındaki ulusal güvenlik politikalarını tehlikeye sokmuş ve yeni bir arayışa yöneltmiştir. Küreselleşme ile ülkelerin birbirlerine karşı olan güç dengeleri değişmiş, yeni güç ilişkilerini ortaya çıkarmış ve ulusal güvenlik kavramlarının yeniden daha kapsamlı ve farklı şekillerde tanımlanmasına neden olmuştur. Güçlerin dağılımı ve ülkelerin birbirlerine karşı güç dengelerinin değişimi de siber "siber güvenlik" kavramını ortaya çıkarmış ve yeni bir ulusal güvenlik politikası söz konusu olmuştur.

Gelişen teknoloji ile ülkeler birbirlerine karşı yeni güvenlik politikaları belirlemişlerdir. Siber alanda hükümetlerin internet üzerindeki verileri, kamu kurumlarına ait bilgiler, bireylerin şahıslarına ait kimlik bilgileri daima saldırılara açık hale gelmiştir. Bu saldırılara karşı engel olmak için, tehditlerin önüne geçebilmek ve devletin birliğini gizliliğini koruyabilmek adına yeni siber güvenlik politikalarını geliştirmek, siber güvenlik ve savunma alanlarında yapılan faaliyetlerin hızlandırılması ve geliştirilmesi hedeflenmiştir. Günümüzde ve gelecekte de siber güvenlik kavramı varlığını koruyacaktır ve gelişen teknoloji, artan küreselleşme ile günden güne önemini artıracaktır.

Standartlaşmış, alışılmış güvenlik önlemlerinin yanında siber alanda da güvenlik kavramının çok önemli olduğu bir anlayış ortaya çıkmıştır. Ülkelerin fiili savaşlarını, siber uzayda gerçekleştirme çabası, söz konusu saldırılara karşı korunma yerine göre bu saldırılara karşı güçlü şekilde cevap vermek amaçlanmıştır. Her ne kadar ülkeler kendi şartları ve koşulları doğrultusunda siber güvenlik politikaları

hazırlasalar da diğer ülkelerin güvenlik politikalarını da inceleyerek bunlara göre eylem planları ve stratejiler geliştirmektedir.

ABD, Rusya ve Çin siber güvenlik alanında listenin en başında yer almaktadır. Türkiye ise siber güç anlamında listenin altlarındadır. Bunun sebebi ise siber güvenlik alanındaki çalışmalara geç başlamasındandır. ABD, Rusya ve Çin'i gelişmiş ülkeler olarak sınıflandırırsak Türkiye'de siber güvenlik alanında gelişmekte olan ülkeler arasındadır diyebiliriz. Çalışmalar yaparak, ulusal olarak çeşitli tatbikatlar yaparak veya söz konusu tatbikatlara katılarak siber alandaki güvenlik açıklarının ya da oluşan zarara karşı nasıl önlem alınması gerektiği tespit edilmektedir.

Teknoloji geliştikçe siber güvenlik alanında her zaman yeni politikalara ihtiyaç duyulacaktır. Çünkü her yeni ortaya çıkan siber saldırı yöntemi, siber saldırılardan korunma yöntemleri ülkelerin üstüne düşmesi gereken en önemli kavramlar haline gelecektir.

Yapılan bu çalışma ile siber güvenlik kavramının ne olduğu, siber silahlarının, siber tehditlerin, siber uzay, siber saldırı türleri kavramları ile siber saldırılara karşı nasıl savunma oluşturulması gerektiği konuları incelenmiş, siber güvenlik sağlanırken hangi unsurlar üzerinde çalışmalar yapılacağı anlatılmıştır. Çalışmanın devamında Türkiye'nin siber alandaki faaliyetlerinin neler olduğu, siber güvenlik kavramı ile ne zaman tanıştığı, siber güvenlik politikalarını hazırlarken hangi unsurların dikkate alındığı, siber güvenlik alanında dünyadaki konumu değerlendirilmiştir. Bu değerlendirmeler yapılırken Türkiye'ye yakın seviyedeki ülkelerin politikaları incelenmiş, bu ülkelerin yanında listenin başında bulunan ABD, Çin, Rusya ve İngiltere gibi ülkelerin de siber güvenlik politikalarının hazırlanış aşamaları, strateji belgeleri, eylem planlarına da bakılmıştır. Bu incelemelerin yapılmasının ardından Türkiye'nin de siber alanda güçlü olan ülkelerden farkları, hangi alanda çalışmalar yapması gerektiği, söz konusu güvenlik açıklarının tespitlerinin nasıl yapılması gerektiği ve siber güvenlik alanında gelişmesi için çalışmalar yapılması amaçlanmıştır.

Çalışma hazırlanırken birçok kaynaktan yararlanılmıştır. Çeşitli doktora ve yüksek lisans tezleri, bilimsel dergiler ve makaleler, ülkelerin kendi bünyeleri kapsamında yayımladıkları eylem planları, NATO'nun siber alanda yayımladığı raporlardan, siber alanla ilgili yazılan kitaplardan faydalanılmıştır. Tüm bunların yanında siber güvenlik politikaları konusunda güncel bilgilerden faydalanmak adına internet üzerindeki açık kaynaklardan faydalanılmıştır.

Çalışma ile gelişen teknoloji karşısında siber kavramı güvenlik karamı hakkında detaylı olarak bilgi vermek, ülkelerin bu kavramdan ne kadar haberdar olduğu, siber güvenlik politikası kavramına ne kadar önem verdiği ve bu alanda güçlü olabilmek için ne gibi çalışmalar yaptığının tespiti, ülkemizin gelişen teknoloji kapsamında teknoloji ne kadar takip ettiği, söz konusu saldırılara, siber kavramına ne kadar hakim olduğu ve diğer ülkelerden farklı olarak ne tür çalışmalar yaptığının tespiti, Türkiye ve diğer ülkelerin siber alandaki güç potansiyellerinin karşılaştırılarak neler yapılması gerektiği, siber güç olarak listenin başındaki ülkelerden ne düzeyde geride olduğu ve neden listenin altlarında kaldığının tespitleri amaçlanmıştır.

BİRİNCİ BÖLÜM

SİBER GÜVENLİK ve SİBER GÜVENLİK İLE ALAKALI KAVRAMLAR

Bu bölümde siber güvenlik kavramının ne olduğu, siber güvenlik politikalarının nasıl hazırlandığı, hazırlanırken hangi hususların dikkate alındığı, siber silahların ne olduğu, siber savunma yöntemlerinin ne olduğu ne nasıl uygulandığı ele alınmıştır. Ülkelerin siber güvenlik politikalarını hazırlarken uyguladığı stratejilere de ayrıca yer verilmiştir.

1. Siber Güvenlik ve Siber Güvenlik ile Alakalı Kavramlar

Bu bölümde siber güvenlik ve siber güvenlik ile alakalı kavramların tanımı, siber güvenlik kavramının ortaya çıkışı, siber güvenlik politikalarının ülkelerdeki yeri ve önemi, siber silahların, siber saldırıların, siber saldırılara karşı alınan savunmaların ve önlemlerinden ve siber istihbarat kavramları tanımlanmıştır.

1.1. Siber Güvenlik

İnsanlık var olduğu günden hayatının devamlılığını sürdürebilmek için yemeye içmeye, güvenliğe, sevgiye, saygıya ihtiyaç duymuştur. Bu ihtiyaçlarını giderebilmesi için çeşitli arayışlara girmiştir ve sürekli olarak kendisini geliştirmiştir. Gelişen teknoloji ortaya çıkan sorunlar yeni kavram arayışlarına neden olmuştur. Gelişen teknoloji çağı ile ortaya çıkan güvenlik açıklarından, mevcut saldırılardan, verilen zararları en aza indirgemek için yeni güvenlik politikası arayışları söz konusu olmuştur. Siber güvenlik de bu arayışlar sonunda ortaya çıkmıştır. İnternet hayatının hemen hemen tüm dünya üzerinde kullanılması, herkesin erişebilir olması, kamu kurum ve kuruluşlarının, bireylerin interneti aktif olarak kullanması, kamu hizmetlerinin, bankacılık işlemlerinin dahi sanal alanda yapılması ciddi derecede güvenlik arayışına neden olmuştur. Siber alanın yaygınlaşması, ortaya çıkan saldırılar ile büyük zararlar vermiştir. Bu sebeplerle siber güvenlik konusu çok önemli bir hale gelmiş ve gündeme oturan bir kavram olmuştur.

Siber güvenlik kavramı hakkında kabul edilmiş ortak bir tanım bulunmamaktadır. Bu yüzden kavram hakkında birden fazla tanım söz konusudur. Siber güvenlik Korff'a göre; bilgi ve iletişim sistemleri arasında ve bu sistemlerin barındırdığı bilgilerin saldırılardan uzak tutulması, herhangi bir zarar verilmesinin

önüne geçilmesi yada yok edilmelerini engellemek için oluşturulan bir güvenlik sistem olarak tanımlamıştır (Göçoğlu ve Aydın, 2019: 230).

Siber güvenlik hakkında başka bir tanım ise Ulusal Telekomünikasyon Birliği tarafından yapılmıştır. Bu tanıma göre ise siber güvenlik; siber alanda kurumlar ve bireylerin bilgilerini, varlıklarını korumak için kullanılabilecek güvenlik araçları, politikaları, güvenlik talimatlarının tümüne verilen addır (https://www.itu.int/, 2021).

Şekil 1: Siber Güvenlik Araçları

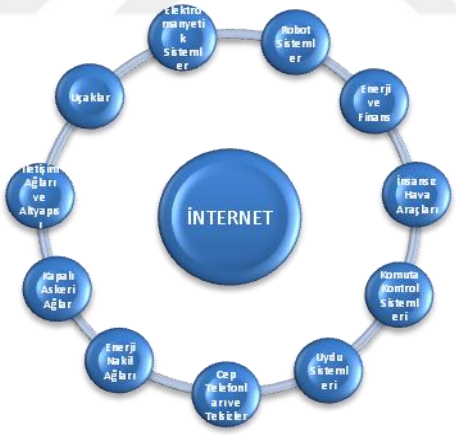
Siber güvenliğin araçları 3 kategoriye ayrılmıştır. Birinci kategori optimal tasarım. Optimal tasarım ile ağ kendisini yeniler, hasar meydana gelirse onarır ve restore eder. Optimal tasarım ile ağın kapasitesi ölçülür, kapasite arttıkça saldırılara ne kadar açık hale geldiği, bu saldırılar karşısında ne kadar güvenli olduğu tespit edilir. İkinci kategori ise sürekli ağ denetimidir. Bu kategori ile ağın sürekli olarak gözlemlenmesi, ortaya çıkan zayıflıklar ve sorunların o an tespit edilmesi ve ona göre çözümler üretmek hedeflenmektedir. Üçüncü kategori ise sonraki nesillerin güvenliğidir. Bu kategori ile siber uzayda birçok farklı saldırının söz konusu olduğu, bu saldırılara karşı şimdiden gerekli önlemlerin alınarak bu ağı kullanacak olan gelecek nesillerin güvenliği sağlamak amaçlanmaktadır (Yue, 2003: 565-569).

Siber güvenlik kavramının ardından bu kavramın nerede aktif olarak kullanıldığı, hangi alanda güvenliği sağladığına değinmek gerekmektedir.

1.2. Siber Uzay

Siber güvenlik kavramının ortaya çıkmasının en temel sebebi siber uzaydır. Yani siber alan. Bir diğer adı da siber ortam olarak geçmektedir. Siber alan, internetin olduğu ya da olmadığı tüm telefon, bilgisayar veya birbirinden farklı ağ sistemlerinin bir araya gelerek oluşturduğu alanlardır. Siber uzayı yazılımlar, bilgiler ve ağların yani birden fazla soyut olgunun bir araya gelerek oluşturduğu ortamlara da denebilir (Clark, Berson ve Lin 2014: 3). Siber uzayda herhangi bir coğrafi sınırlama yoktur. Bilgi ve iletişim teknolojilerinin alt yapılarından meydana gelen birbirine bağımlı olan, coğrafi kısıtlamalardan uzak olan küresel bilgi ve veri ortamıdır.

Siber uzayın en temel elemanı internettir. Bunun yanında bilgisayarlar, cep telefonları, uydular, telsizler, uydu sistemleri, robot sistemler, insansız hava araçları, ağ sistemi bileşenleri, yazılımlar, elektronik sistemler, iletişimin alt yapısını ve siber uzayı oluşturmaktadır (Çeliktaş, 2016: 6).



Şekil 2: Siber Uzay Elemanları

Siber güvenlik kavramı, siber uzay kavramı yanında yeni kavramları da getirmiştir. Bu kavramlardan birisi de siber saldırı kavramı olmuştur. Siber saldırı kavramı insan temeline dayanan, insanlar tarafından çıkarılan saldırılardır. Normal saldırılardan farkı ise; sanal ortama ve alana yapılan saldırılardır. Yapılan saldırı her ne kadar sanal ortam üzerinden olsa da sonucundan insanlar ve kurumlar etkilenmektedir. Yapılan her siber saldırının birer amacı vardır (Göçoğlu ve Aydın,

2019: 232). Siber saldırılar bireyleri, firmaları ve devlet kurumlarını hedef almaktadır. Bu saldırılar ise; bireyler veya grup halindeki suçlular, kötü niyetli insanlar, internet korsanları, hackerlar, kötü niyetli kurum ve kuruluşlar tarafından gerçekleştirilmektedir.

1.3. Siber Saldırılar

Siber saldırılar, siber uzay üzerinden gerçekleştirilen kamu kurum ve kuruluşlarını, hükümetleri, bireylerin kendilerini hedef alan sanal ortamda zarar vermeyi amaçlayan saldırılardır. Bu saldırılar ile bilgi barındıran sanal ağlara, bilgileri ve verileri çalmak ele geçirmek için, kimi zaman bu bilgileri değiştirmek ya da yok etmek için yapılmaktadır. Yapılan siber saldırılar daima planlı ve koordineli olarak şahıslar ya da sistemler tarafından gerçekleştirilir.

Siber saldırı, ulusal siber alanda bulunan bilgilerin, iletişim teknolojilerinin üzerindeki gizlilik, erişilebilirlik veya bütünlüğü bozacak ya da tehlikeye atacak, ortadan kaldıracak kişi veya siber alanda faaliyet halinde olan sistemler tarafından kasıtlı olarak yapılan saldırılardır (Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı, 2016: 8).

Siber saldırılar için kritik alt yapıya sahip olan her yer saldırıya açık hedefler halindedir. Bu kritik alt yapılar ise insanların hayati faaliyetlerini, sağlık açısından, emniyet ve güvenlik açısından, ekonomik ve toplumsal refah açısından doğrudan etkileyen, bu faaliyetlerin aksamı ile ciddi sorunlara neden olabilecek ciddi derecede etki yaratan ve olumsuz etkiler yaratan sistem parçaları olarak tanımlanmıştır (Göçoğlu ve Aydın, 2019: 232).

Siber saldırıları gerçekleştirecek belli başlı saldırı kaynakları söz konusudur.

Şekil 3: Siber Saldırı Kaynakları

Siber saldırılar, Tablo-3'de kaynaklar tarafından gerçekleştirilmektedir. Bu saldırıların büyük bir çoğunluğu dışardan yapılsa da bilinçsiz kullanıcıların farkında olmadan yaptığı saldırılar da söz konusudur. Gerçekleşen siber saldırılar ile bu saldırıları yapan teröristler, bilgisayarları, bilgisayar ağlarını, telefonları, mobil cihazların tamamını bu saldırılar için kullanabilmektedir. Bu saldırılar ile bireysel bilgilerin ele geçirilmesi, edinilen bilgilerin kötü amaçlar doğrultusunda kullanılması, hükümete yapılan saldırıların büyük ekonomik sorunlara yol açması, veri gizliliğinin korunamaması gibi sonuçlar doğurmaktadır. Bu amaçlarla siber saldırılar günden güne artmaktadır.

Hackerlar tarafından gerçekleştirilen siber saldırılar ile kişisel bilgisayarlar, mobil cihazlar, cep telefonları, kamu bilgisayar ve ağlarına izinsiz girmek hedeflenmiştir.

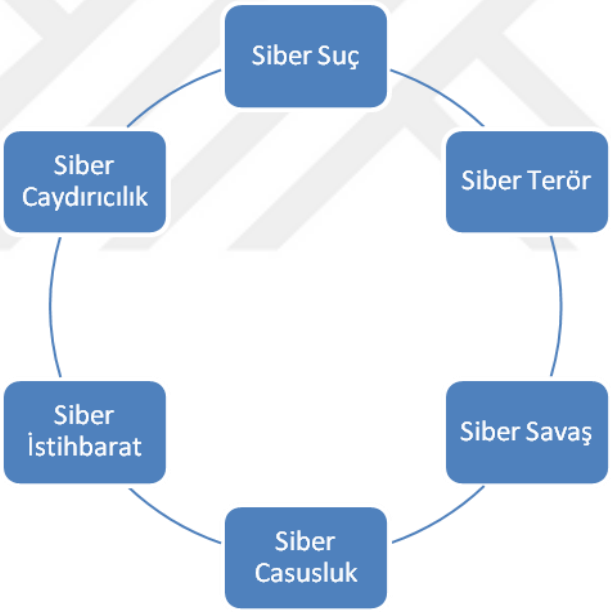
İç saldırganlar, belirli amaçlar için organize şekilde saldırı düzenleyen kurumsal kişilerdir.

Siber aktivistler, kendi dünya görüşlerinin dışında kendileri açısından yanlış veya uygunsuz gördükleri olaylara karşı toplumsal veya siyasi politik sorunları ortaya çıkarmak duyurmak amacı ile kamu veya özel alanda siber saldırı gerçekleştiren kişilerdir.

İstihbarat kurumları ise; uluslararası siber alanda ülkelerin birbirleri tehdit etmeleri sebebiyle hükümetlerin, ülkelerin verilerini ele geçirmeye çalışan, o ülkenin kritik alt yapısına saldırı düzenleyen kişilerdir.

1.4. Siber Tehditler

Siber alanda siber saldırı kaynakları tarafından karşı tarafa yönelik her türlü bozucu, yıkıcı, ele geçirici ve engelleyici girişimlerin kullanılmasına denir. Siber tehditler klasik suçların yanına eklenen yeni suç tiplerini oluşturmaktadır. Siber tehditleri de siber saldırıları gerçekleştiren hackerlar, bilgisayar korsanları, casusluk faaliyetleri yapanlar gerçekleştirmektedir. Aynı siber saldırılar gibi sistemlere yetkisiz giriş yapmak için, işleyişi bozmak ya da verilerin ele geçirilmesi için kullanılmaktadır. Siber tehditleri çeşitli başlıklar altında incelemek mümkündür.



Şekil 4: Siber Tehdit Unsurları

- **Siber suç**; bilgisayar, bilgisayar ağlarının ve sistemlerinin siber alanda yapılan saldırılar ve tehditler için doğrudan kullanılmasıdır. Bilgisayar sahibinin haberi ve bilgisi olmadan sistemine girilmesi, verilerinin ele geçirilmesi, değiştirilmesi ya da silinmesi, kişiye ait bilgilerin izinsiz olarak kullanılması siber suçu oluşturmaktadır.

- **Siber terörizm;** siber terörizm ile kaynağın tespit edilemeden, bağlantıların nereden geldiğinin tespitinin mümkün olmadığı, kim tarafından yapıldığının belli olmadığı ve tespit edilemediği, uluslararası hukuki boşluklardan faydalanan modern savaş tekniği olarak tanımlanmaktadır (Çitlioğlu, 2008: 14-15). Siber terörizm de herhangi bir zaman ve yer kısıtlaması yoktur. Amacı genellikle politik olarak dikkat çekmek ve korku yaratmaktır. Eylemleri genellikle bilgisayarları, sanal ağları ve depolama sistemlerini hedef alarak yasa dışı eylemler gerçekleştirerek politik, sosyal, dini, ideolojik ve psikolojik baskılar yaratarak tepki oluşturmayı amaçlamaktadır (Güneştaş ve Başıbüyük, 2015: 88-89).

- **Siber caydırıcılık;** yapılan siber saldırılara karşı cevap vermeye siber caydırıcılık denilebilir. Verilen cevapların karşıdan gelen saldırıya göre güçlü olması, o saldırıyı geri çevirebilme niteliğinin olması gerekir. Yapılan saldırıya karşı misilleme yaparak o saldırıdan vazgeçilmesini sağlamak amacıyla yapılır. Yapılan saldırılara karşı güçlü bir savunmaya sahip olmak da siber caydırıcılık kavramının içindedir.

- **Siber istihbarat ve casusluk;** İstihbarat ve casusluk kavramı geçmişten günümüze kadar daima hep birlikte kullanılmış ve aynı anlamları ifade etmiştir. Gelişen teknoloji ile bu kavramlar nitelik kazanmış ve etkilerini artırmıştır. Siber alan da oldukça etkili olan bu iki kavram gelişmeler ile değişmiştir.

Siber istihbarat, siber saldırı ve tehlikeler karşısında bu saldırıları analiz ederek ve karşı saldırı yaparak karşıdaki sistem hakkında bilgi edinilmesi sağlamaktadır (Keleştemur, 2015: 90).

Siber casusluk ise; karşı tarafın sistemlerine sızarak bu sistemler üzerinden politik, ekonomik, siyasi, askeri alanlarda üstünlük sağlamak için hükümete ya da kişilere ait bilgilerin ele geçirilmesi olarak tanımlanmaktadır (Çifçi, 2013: 291).

1.5. Siber Savaş

Bir devletin başka bir devlete ait olan bilgisayar veya iletişim ağlarına sızarak onlara hasar vermek, verilerini ele geçirmek, işlemleri üzerinde kopukluklar yaratmak ve kesintilerin yapılması siber savaş olarak tanımlanmıştır (Clarke ve Knake, 2010: 8). Siber savaş günümüzde kendini geliştiren ve değiştiren güncel bir

kavramdır. Silahların yanında hackerların siber ortam üzerinden yaptıkları saldırıları karşısında ayrıca bir savunma sistemlerinin geliştirilmesi gerektiğini gözler önüne seren bir kavramdır.

Siber savaş aynı zamanda ülkedeki bireylerin, askeri, ekonomik, politik ve hükümete ait bilgilerin ele geçirilmesi için organize olup saldırı yapılması olarak da tanımlanmaktadır. (Yazıcı, 2011: 1-32)

Siber savaşlar, mevcut askeri savaşlardan farklı olarak herhangi bir mesafeden başlamak yerine dünyanın bir ucundan diğer ucuna habersiz ve her an gerçekleştirilebilir saldırılar ile gerçekleşir. O ülkedeki ya da o hedefteki her teknolojik aletin ele geçirilmesi mümkündür. Aynı zamanda yapılan saldırının siber saldırı olup olmadığının tespit edilmesi gerekmektedir. Bu tespit ise; saldırının kaynağına, kim tarafından yapıldığına, verdiği zarara ve saldırının kapsamına göre değerlendirilir. Çünkü her siber saldırı bilinçli olarak yapıldığı gibi bilinçsiz kullanıcılar tarafından da farkında olmadan gerçekleşebilir.

Siber savaşlar, diğer savaşlar da olduğu gibi devletler arasında gerçekleşen birer çatışma örneğidir. Dünyadaki tüm ülkeler siber saldırılar karşısında kendi savunmalarını geliştirmek ve yapılan saldırılara cevap vermek için çalışmalarını artırmışlardır. Askeri siber güç alanında yatırımlar ve geliştirme çalışmaları yapmaktadır.

Devletlerin yanında bireylerin kendi başlarına yaptıkları bireysel siber saldırılar, devlet destekli değil ve bir devlet tarafından yönetilmiyorsa eğer siber savaş olarak kabul edilmemektedir. Siber saldırıların niteliği de siber savaş algısını değiştirmektedir. Herhangi birisinin banka hesabını ele geçirmek siber savaş olarak nitelendirilmezken, ülkenin hava üssüne karşı yapılan ya da devletin kamu sistemlerine yapılan saldırı siber savaş niteliği taşımaktadır. Siber savaşta yapılan saldırının niteliği ve verdiği zarar bu savaşın büyüklüğü konusunda ülkelere bilgi vermektedir.

Geçmişteki siber savaşlar sadece bilgilerin gözden geçirilmesi, bilgilerin toplanması veya bilgilerin çalınması için yapılırken günümüz gelişen teknolojisi ile teknolojik sistemlere sızarak, hedeflerden kişisel veya kurumsal bilgilerin çalınması

için, sistemlerin bozulması için, hasım devletler arasında zarar vermek veya yok etmek amacıyla gerçekleştirilen saldırılar haline bürünmüştür. Yapılan bu savaşlar ile hasım devletler karşıdaki devletin iletişim ağlarını, sağlık sistemini, ekonomik durumunu, güvenlik sistemini, ulaşım ağlarını, askeri ya da kritik alt yapı dediğimiz sistemlere saldırarak büyük zararlar vermeyi amaçlamaktadır.

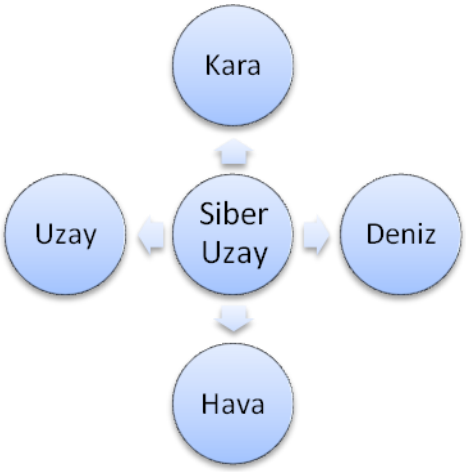
1.6. Siber Silahlar ve Siber Saldırı Türleri

Siber silah hakkında küresel anlamda kabul edilmiş sabit bir tanım söz konusu değildir. Bu yüzden birden fazla tanımı söz konusudur.

Siber savaşların gerçekleşmesi için birden fazla silah mevcuttur. Saldırıların yanında kendi bilgisayarlarını korumak için ayrıca koruma yazılımları vardır. Bu silahları, virüsler, Truva atları, kurtçuklar, botnet ve zombieler, istem dışı e-postalar (spam), klavye işlemlerini kaydeden programlar, casus yazılımlar, servis dışı bırakma, aldatma, şebeke trafiğinin dinlenmesi, yemlemeler ve propaganda olarak sınıflandırabilir.

Bu sınıflandırmaya dâhil olan siber saldırı silahları ile sızmış oldukları bilgisayar veya ağlara ciddi derecede yıkıcı, hizmetleri sınırlayıcı ya da verilen gizliliğini ihlal ederek çeşitli şekilde zarar verebilmektedir.

Siber silahların ortaya çıkması ile savaş mantığındaki hareket alanları değişmiştir. Kara, hava, deniz ve uzay alanlarının hepsini kapsayan siber uzay hareket alanı eklenmiştir. Böylece ülkelerin kritik alt yapılarının saldırıya açık halde olduğu, olası saldırılara karşısında ciddi sorunlar yaşamasına sebep olacak olan harekât alanı da günümüzde var olmuştur.



Şekil 5: Harekât Alanları

Siber silah, ülkelerin kritik alt yapı sektörlerine karşı, bilgi ve iletişim teknolojilerine karşı, bireylerin işlevsel, zihinsel veya fiziksel olarak zarar vermek amacıyla mevcut olan düzenlerini bozmak, tahrip etmek, ele geçirmek için kullanılan bilgisayar kodlarıdır (Rid ve McBurney, 2012: 7).

Siber silahların 3 temel özelliği vardır;

Siber silahlar kapsamı itibariyle, devlet içi veya devlet dışı olarak bilişim sistemlerine karşı korumak, devamlılığını sağlamak amacıyla siber savaşlar içinde siber saldırılarda kullanılması gerekmektedir.

Siber silahların amacı ise, bilişim sistemlerini kullanma, zarar verme, insanlara, aygıtlara, hükümetlere ve hükümetlerin sistemlerinin kullanılmasına engel olmak gibi amaçlar güder.

Siber silahların yöntemleri ise; tüm internet içeren teknolojik cihazlara karşı kullanılması gerekmektedir. Bu özelliklerin tamamına sahip olmayan silah siber silah olarak nitelendirilemez.

Siber silahlar diğer silahlara göre daha hızlı ve daha az maliyetli şekilde üretilmektedir. Bu sebeple devletlerin dışında da saldırılar düzenlemekte ve kullanılmaktadır. Siber saldırıların gerçekleştirilmesi karşısında karşı taraf bu saldırılara karşı daha ciddi önemler aldığından bir sonraki saldırılar zayıf kalacaktır. Bu yüzden yapılacak olan siber saldırıların başarıya ulaşması için saldırı zamanı ve miktarı çok önemlidir.

Birden fazla siber silah türü söz konusudur. Bunlar zararlı yazılımlar, hizmet dışı bırakma gibi kategoriler altında ayrılmaktadır.

1.6.1. Zararlı Yazılımlar (Malware)

Bilgisayar sistemlerini kötü amaçlı kullanarak verileri ele geçirmek için, bu verilerin kullanılarak karşıdaki devletlere şahıslara zarar vermek, bilgileri çalmak için kullanılan, sistemlere ciddi şekilde zarar veren bilgisayar programlarıdır. Zararlı yazılımlar ile bilişim sistemlerinin işleyişlerini bozma, çalışma düzenlerini bozma ve senkronizasyonlarını bozmaya yarayan yazılımlara denir (https://www.mcafee.com/, 2021)

1.6.2. Virüsler

Virüsler, bilgisayarların ortaya çıktığı zamandan beri mevcut olan ve bugüne kadar devamlılığını sağlayan yazılımlardır. Geçmişten günümüze kadar hep bilgisayarlara zarar veren yazılımlar olarak adlandırılmış olsa da virüslerin tamamı bilgisayar sistemlerine zarar vermez. Gerçek virüsler bir dosyadan diğer dosyalara geçerek tüm sisteme yayılan kötü yazılımlara denir (Graham ve Howard, 2010: 198-199).

Virüsler insan eliyle çalıştırılmaya ihtiyaç duyarlar. Çalıştırılmaları sonucu bilgisayardaki programlara ve yazılımlara yazılarak zarar vermeye başlarlar. İnternet üzerinden dosya indirme, e-postalar, CD'ler, USB bellekler virüslerin yayılmasında oldukça etkilidir.

1.6.3. Truva Atları

Truva atları (trojanlar) yararlı birer program gibi görünse de oldukça zararlı yazılımlardır. Ön planda bilgisayar için faydalı bir yazılım gibi görünürken arka planda bilgisayarın dosyalarının arasında zarar vermeye devam etmektedir. Kullanıcı tarafından çalıştırılan Truva atları, kullanıcı dosyalarının, verilerinin kaybolması hatta çalınmasına sebebiyet verir. Genellikle internet üzerinden ücretsiz olarak verilen programların yüklenmesi ile sisteme yerleşmektedir. Korunmanın tek yolu ise kaynağı bilinmeyen programların yüklenmemesidir. Truva atları kendilerini kopyalayamazlar, yararlı birer program gibi görünüp faydalı işler yaparken arka planda zararlı işleri yapan casus yazılımlardır (Çifçi, 2013: 54).

1.6.4. Solucanlar (Worms)

Solucanlar da virüsler gibi kendilerini bir bilgisayardan başka bir bilgisayara kopyalanması için tasarlanmışlardır. Yayılmaları dosya üzerinden ya da programlar üzerinden değil de doğrudan ağ sistemleri üzerinden gerçekleşmektedir. Bu yayılma ile bilgisayarın internetinin yavaşlaması, sayfaların yavaş açılması veya hiç açılmamasına sebep olmaktadır.

Solucanlar, kullanıcıların müdahalesi gerekmeden kendi başlarına çoğalıp çok kısa sürede yayılabilen zararlı yazılımlar olarak da adlandırılmaktadır. Bir başkasının, bulaştıklarını bilgisayar üzerinde tünel açarak bilgisayarın denetimini başka birinin eline geçirmesine olanak sağlayabilmektedirler (https://bidb.itu.edu.tr, 2021).

1.6.5. Zombi Ordular (Botnetler)

Zombi bilgisayarlar bu zararlı yazılımlar arasında en tehlikeli olan gruptur.

Kullanıcılarının haberi olmadan bilgisayarlara daha önce yüklenen programlar sonucunda uzaktan kontrol edilebilen bilgisayarlara denmektedir. Hedef bilgisayarlara saldırmak için bu zombi bilgisayarlar üzerinden hedefe doğru saldırılar gerçekleştirilmektedir. Köle bilgisayarlar, asıl saldırıyı yapan tarafından daima saldırı için hazır ve uzaktan yönetilmektedir (Güngör, 2015: 45).

Zombi bilgisayarların bu şekilde kullanılmalarının en temel sebebi sistemlerinde mevcut olan güvenlik duvarlarının aktif olarak çalışmaması ya da hiç olmamasıdır (Öğün ve Kaya, 2013: 155). Herhangi bir korumaya sahip olmayan ve saldırılara açık olan her bilgisayar botnet olarak kullanılabilmektedir. Botnetler yüzünden şahsi bilgisayarlar, kullanıcıların farkında olmadan kendi bilgilerini kullanarak ciddi suçların işlenmesine sebep olabilir.

1.6.6. Spamlar (İstem Dışı Elektronik Postalar)

İnternet üzerinde aynı içeriğe sahip maillerin, rastgele olarak birden fazla kullanıcıyı hedef olarak e-posta şeklinde gönderilerek hedefteki şahısların bilgilerine ulaşabilmek, onları dolandırmak amacıyla gönderilen maillerdir. Bu saldırı türünde hedefteki şahsın böyle bir maili talep etmediği, tamamen pazarlama, reklam veya

kampanya tarzındaki gönderiler ile kullanıcının dikkatini çekerek bilgilerini ele geçirmek hedeflenmiştir.

1.6.7. Keyloggers (Klavye İşlemlerini Kaydeden Programlar)

Klavyede yapılan her işin kaydedilmesini sağlayan programlara denmektedir. Bu kaydedilen işlemler ise, keyloggersları gönderen saldırganlara gönderilmesini sağlar. Bu tip saldırılar genellikle alışveriş sitelerinde, internet üzerinden gerçekleştirilen bankacılık hizmetlerinde bulunan açıklar sayesinde gerçekleşir ve kişilerin verileri böylece ele geçirilmektedir.

Bu tarz saldırıların ya da verilerin korunması için ekrandan tuşlama ile yapılan girişler, telefona sms gönderilerek sağlanan güvenlik çalışmaları devam etmektedir (Öğün ve Kaya, 2013: 157).

1.6.8. Spyware (Casus Yazılımlar)

Casus yazılımlar, bilgisayarlar üzerinden casusluk yapmak için üretilen yazılımlardır. Bu yazılımlar, karşı taraftaki kullanıcıların bilgilerinin, yaptığı işlemlerinin o kullanıcının haberi olmadan elde edilmesi ve bu bilgilerin kötü niyetli olarak kullanılmasına sebebiyet vermektedir. Casus yazılımlar virüsler, solucanlar gibi yayılma ihtiyacı duymazlar. Bulaştıkları sistemde gerekli olan bilgilerin ve verilen ele geçirilmesi için tasarlanmışlardır.

Casus yazılımlar bilgisayarlara genellikle ücretsiz olarak indirilen programların içine bütünleşmiş şekilde gelmektedir ve kullanıcılar kendi rızaları ile bu yazılımları bilgisayarlarına farkında olmadan yüklemektedirler (Jonasson ve Sigholm, 2005: 1).

1.6.9. DoS ve DDoS Saldırıları

Bir sisteme kullanıcıların erişimi engellemek amacıyla eş zamanlı ve birden fazla saldırı göndererek bu sistemdeki kullanıcıların kullanılamaz hale gelmesi ve sistemin erişiminin engellenmesi ve hizmet verememesi için yapılan saldırılardır. (Öğün ve Kaya, 2013: 158). Bu saldırılara DoS saldırıları adı verilmektedir.

DoS saldırılarının yanında mevcut olan güvenlik açıklıklarından faydalanarak ele geçirilen bilgisayarların botnet olarak kullanılması ve toplu halde yapılan saldırılara ise DDoS adı verilmektedir (Yazıcı, 2012: 38).

DDoS saldırılarının gücü ele geçirilen botnetlerin sayısı ne kadar fazla olursa o kadar etkili olmaktadır. Günümüzde bu tarz saldırılar oldukça fazladır. DDoS saldırılarının hedef bilgisayarı on binlerce bilgisayarın saldırısına maruz kalarak saniyeler içinde kullanılamaz hale gelebilmektedir (Çeliktaş, 2016: 37).

1.6.10. IP Spoofing (IP Aldatmacası)

Bilgisayarlar kendileri arasındaki bağlantıları çeşitli yollarla yapabilmektedir. Bu bağlantılar LAN sistemi, IP bilgileri ve buna benzer birçok bilgi ile birbirleri ile bağlantı kurabilmektedir. IP aldatmacası da bu bağlantılar sayesinde gerçekleşmektedir. Bilgisayar korsanları, herhangi güvenli bir IP adresini kullanarak gerçek kimliklerinin dışında kişilerin veya kurumların bilgilerini ele geçirebilmektedir (Gürkaynak ve İren, 2011: 272).

IP Aldatmacası ile siber saldırganlar, hizmet veren sunucular ve sistemlere yaptıkları saldırılar ile gerçek kimliklerini gizlemektedir ve sahte IP adresleri ile bu siteye giren kullanıcıların verilerini ele geçirmektedir.

Günümüzde IP Aldatmacası ile DoS ve DDoS saldırıları oldukça artmış durumdadır ve halen artmaktadır (Aydın, 2013: 39).

1.6.11. Sniffing (Şebeke Trafiğinin Dinlenmesi) Saldırıları

Sniffing, sabit bir ağ üzerindeki bilgisayarların arasındaki veri alışverişinin takip edilmesidir. İki bilgisayar arasındaki tüm verilerin yakalanarak saklanmasını sağlar. Korsanların kullandığı önemli yöntemlerden birisidir (Öğün ve Kaya, 2013: 160).

1.6.12. Phishing (Yemleme-Oltalama) Saldırıları

Bir web sitesinin sahtesinin yapılarak kullanıcılara bilgilerini girmelerini, güncelleme yapmalarını, ödül kazandıklarını söyleyerek kullanıcıların verilerinin ele geçirilmesine denir.

Saldırılar yapılırken genellikle orijinal sitenin birebir aynısını, sahte e-posta ile sitenin orijinalini ziyaret ediyormuş hissi vererek yasa dışı yollarla kullanıcıya ait kredi kartı bilgilerinin, kullanıcı adları veya parolaların ve kişisel bilgilerin çalınması hedeflenmektedir (https://www.isnet.net.tr/, 2021).

1.6.13. Logic Bomb (Mantık Bombası)

Mevcut olan çalışan yazılımların içine belirli zaman ve şartların oluşması durumunda programların içine bilinçli olarak yerleştirilen yazılımlardır. Yalnızca belirli bir olaydan sonra yazılımın içinde istenmeyen bir kod olarak kullanılmaktadır. İstendiği zaman çalışmaktadır ve çalıştığı andan itibaren zararlı olmaktadır (https://teknodestek.com.tr/, 2021).

1.6.14. Rootkit (Kök Kullanıcı Takımı)

Yapılan çalışmaları, dosyaları ya da sistem bilgilerini işletim sisteminden gizlemek için yazılım içinde bulunan ve varlığını sürdüren programlardır. Bu tarz saldırılarda amaç yayılmak değil gizli olarak varlıklarını sürdürmektir (Çalışkan, 2018: 22).

Bu yazılımların daha önceden kullanılma amaçları çok kullanıcıya sahip yönetim ve sistem bilgilerinin tüm kullanıcılar tarafından erişiminin sağlanmaması adına sistem bilgilerini gizlemek için geliştirilmiş olsa da kötü amaçla kullanımlarına rastlamak da söz konusudur. (https://www.kaspersky.com.tr, 2021).

Diğer virüslerde olduğu gibi sistemi yavaşlatmak veya yayılımı sağlamak gibi amaçları yoktur. Rootkitlerin amacı içinde bulunduğu sistemi ele geçirmek ve o sistemde varlığını korumaktır. (https://tr.wikipedia.org, 2021).

Rootkitlerin hangi dosyaları etkilediği, hangi yazılımları yüklediği, sistemin hangi dosyasında kayıtlı olduğu ve nasıl harekete geçtiğini tespit etmek oldukça zordur.

1.6.15. Trap Door (Arka Kapı) Açıkları

Arka kapı saldırıları, çeşitli yollar ve teknikler ile yazılım ve sistem üzerinde giriş çıkış noktalarında bilerek ya da istek dışında oluşturulup sisteme girişlerin ve çıkışların, aynı zamanda veri girişinin ve çıkışının yapıldığı açık noktalara verilen genel addır (https://lostar.com.tr, 2021).

Arka kapılar sisteme uzaktan erişim sağlamak ya da şifreleme sistemlerine erişimi sağlamak için kullanılır.

1.6.16. Attack Kits (Saldırı Kitleri)

İnternetten ücretsiz olarak indirilebilen, ücret karşılığında yazılımsal olarak yazdırılabilen herkesin kolayca elde edebileceği ve kolayca kullanabileceği, siber saldırıların rahatça yapılabileceği, profesyonel ve amatör olarak herkesin kullanabileceği yazılımlardır (Çeliktaş, 2016: 35).

1.6.17. Ransomware (Fidye Virüsü)

Sistemler üzerindeki güvenlik açıklarından ve sisteme indirilen Truva atı içeren programı içeren herhangi bir dosyanın çalışması sonucu aktif hale gelen virüslerdir. Fidye virüsleri genellikle şifreleyiciler ve kilityeciler olarak iki şekilde incelenmektedir.

Şifreleyici fidye virüsleri bilgisayara ya da sisteme bulaştıklarında sistem üzerinde bulunan tüm dosyaların şifrelenmesine sebep olur ve açılmaz hale gelir. Bu dosyaların içerisindeki verilere ulaşmak imkânsız hale gelir. Bu verilere erişmek için fidye virüsünün sahibi olan saldırganlar verilerin şifresini açmak için fidye istemektedirler.

Kilitleyici fidye virüsleri ise sisteme bulaştıktan o sistemin sadece dosyalarının değil tüm sisteme erişimi engellemektedir.

1.6.18. Social Engineering (Sosyal Mühendislik)

İnsanların duygularını, onların zayıf noktalarından faydalanmak suretiyle yapılan siber saldırılardır. Bu siber saldırılarda insanları ikna etmek, onlara menfaatleri karşılığında para ya da hediye vermek, hiç olmamış olaylardan bahsederek kandırmak, sahte hesaplar üzerinden yakınlık kurarak başkaları adına

paralar talep etmek yine birisinin adına açılan sahte hesap üzerinden o insanmış gibi davranarak insanların kandırılması, para ve bilgi elde etmek için yapılan saldırılardır.

1.6.19. Kriptografik Saldırılar

İnternet üzerinden siteler ve bireyler arasında paylaşılan bilgilerin üçüncü kişiler tarafından ele geçirilmesi için yapılan saldırılara denir. Şifrelenmiş bilgilerin, verilen şifrelerini çözmek için kullanılır (Keleştemur, 2015: 304).

Kritografik saldırılar kendi içerisinde de 9 alt başlıkta incelenmektedir. Bunlar; Duqu saldırıları, İlişkili Anahtar Saldırıları, İndirgeme Saldırısı, Tekrarlama Saldırısı, Gökkuşağı Tablosu, Güç Analizi, Kaba Kuvvet Saldırısı, Yalnız Şifreli Metin Saldırısı ve Yan Kanal Saldırısıdır (https://tr.wikipedia.org, 2021)

1.6.20. Dijital Manipulation (Dijital Manipülasyon)

İstihbarat ve güvenlik birimlerinin kullanmış olduğu, vatandaşları kandırmayı ve yanlış bilgilendirmeyi hedefleyen aslına uygun olmayan mevcut olan haberi, görüntüyü, videoyu değiştirerek yapılan saldırı türüdür (Gürkaynak ve İren, 2011: 274-275).

1.6.21. Açık Mikrofon Dinleme

Casus yazılımlar ile kullanıcının haberi olmadan, bilgisayarına erişerek bilgisayar mikrofonunun ya da kamerasının açılarak ortamın dinlenmesi veya anlık görüntüsünün alınması için yapılan saldırılardır. Günümüzde oldukça yaygınlaşmıştır (Çifçi, 2013: 147).

1.6.22. Wire Tapping (Kabloya Saplama)

Ağ ve telefon hatlarının uygun emniyeti yeteri kadar alınmamış iletişim ağı kablolarına özel teçhizatlar yardımı ile fiziksel olarak saplama yapılması sonucu iki taraf arasındaki tüm trafiğin ele geçirilmesi faaliyetine yönelik saldırılardır (Yıldız, 2014: 31).

1.6.23. Propaganda

İnternet ortamında ucuz ve etkili olmasından ötürü kullanılan siber ortamda gerçekleştirilebilecek en kolay ve en güçlü saldırıdır. Doğru ya da yanlış olan herhangi bir bilginin, görselin veya videonun bir anda tüm dünya üzerine yayılmaktadır (Öğün ve Kaya, 2013: 161).

1.7. Siber Saldırılar ve Tehditlere Karşı Savunma Yöntemleri ve Siber Güvenliğin Sağlanması

Siber güvenlik, siber uzayı oluşturan faktörlerin, bilgi ve iletişim sistemlerinin, bu sanal ortamda olan tüm bilgi, belge, verilerin çalınmasını engellemek, bütünlüğünü korumak için var olan sistemlerdir. Siber güvenlik ile yapılan saldırıların tespit edilmesi, bu saldırılara karşı tepki verilmesi, saldırı sonrasında zarar gören verilerin ve sistemlerin geri eski haline getirilmesi için geliştirilen sistemlerdir (Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı: 7).

Siber güvenlik, siber uzaydaki güvenlik risklerini ve zafiyetlerinin belirlenerek kurum, kuruluş ve kullanıcıların varlıklarının istenmeyen tehdit ve tehlikelere karşı korunmasını sağlamak için geliştirilen politikalardır.

Siber saldırı silahları, siber tehditler ile dünya üzerinde birden fazla milyonlarca hatta milyarlarca saldırılar gerçekleşmektedir. Bu saldırılar karşısında durabilmek, verilerin korunması, bilgilerin çalınmaması için savunma yöntemleri geliştirilmek zorundadır. Siber saldırıların günümüzde ne zaman yapılacağı, hangi oranda ve hangi araçlar kullanılarak yapılacağının tespiti mümkün değildir. Bu yüzden söz konusu saldırılara karşı daima hazırlıklı olmak gerekmektedir. Bu saldırılara karşı olarak da saldıranın tespit edilerek aynı kaynaklar üzerine karşı saldırılar düzenlenmesi gerekmektedir.

Gerçekleşen siber saldırılar hükümetlerin milli güvenlik birliğini, kritik alt yapılarına karşı gerçekleştiğinde ciddi boyutta ve geri dönülmez sonuçlara sebep olabilir. Bu saldırılar ile ulaşım, ülke genelindeki finansal faaliyetler, mobil iletişim ve ağlar, sağlık alanı, ulusal savunma alanları, sanayi ve teknolojik faaliyetleri

gerçekleştiren sistemlerin hepsi ele geçirilebilir ve çalışmaları durdurularak ciddi devletleri derecede zarara uğratabilmektedir.

Gelişen teknoloji ile siber saldırıların ve tehditlerinin artması ve bu saldırıların sonuçlarının ağır olması, kamu kurum ve kuruluşlarının zarara uğraması, hizmetlerinin aksaması, güvenliğinin azalması sonucunda bu saldırılara karşı ulusal düzeyde korunma ve savunma sistemlerinin geliştirilmesi gerekmiştir (Ünver ve Canbay, 2011: 96).

Günümüzde teknolojinin gelişmesi ile fiziki savaşlar aslında yerini siber savaşlara bırakmış haldedir. Siber saldırılar ile teröristler ya da kötü niyetli salgınların bir devletin kritik alt yapılarını, kamu kurum ve kuruluşlarını ya da tüm dünya ile iletişim ağlarına karşı saldırı gerçekleştirerek tüm bunları yok edebilme ihtimali söz konusudur. Siber güvenliğin sağlanması aslında milli güvenliğin sağlanmasına eş değerdir.

Siber güvenlik alanında yapılan çalışmalar, siber güvenliğin sağlanması için devletler bu alanda ciddi bütçe ayırmaya başlamışlardır. Bu alanda devletler ve özel sektörler oldukça büyük yatırımlar yapmaktadırlar. Saldırılar ve güvenlik açıklarından dolayı ortaya çıkacak olan zararlar ve itibar kayıpları dikkate alındığında devlet ve kurumlar bu maliyetlerden kaçınmayacak düzeyde çalışmalar gerçekleştirmektedir. Milli güvenlik açısından devlet eliyle yapılan saldırılar genellikle siber savaş ve ekonomik casusluk alanlarında gerçekleşirken, devletlerin dışından gelen saldırılar ise daha çok siber suç ve siber terörizm ile ilişkilendirilmektedir (Öğün ve Kaya, 2013: 165).

1.7.1. Siber Güvenlik Stratejileri

Ülkelerin siber güvenliğin ulusal boyutta sağlanması için belli başlı stratejilere ihtiyaçları söz konusudur. Ünver ve Canbay'a göre ulusal boyutta siber güvenlik stratejileri sekiz bölüme ayrılmaktadır (Ünver ve Canbay, 2011: 99).

Birinci olarak ulusal politika ve stratejilerin geliştirilmesi gerekmektedir. Bireylerin, sivil toplum kuruluşlarının, kamu kurumlarının ve özel sektörlerin siber saldırı alanında bilgi sahibi olması, bu saldırılar karşısında nasıl bir yol izleyeceklerine dair hazırlıklarının bulunması, belirli hedefler ve anlayış

doğrultusunda başarının sağlanması adına tüm hepsinin ulusal bir politika ve bu politikalar çerçevesinde stratejilerin hazırlanması gerekmektedir.

İkinci olarak yasal bir çerçeve oluşturulması gerekmektedir. Yapılan saldırıların, açtığı tahriplerin ve zararlar sonucunda saldırıyı gerçekleştirenler hakkında saldırının bir suç niteliğinde olması nedeniyle sonucunda bir cezai işlemin uygulanması ve bu fiilleri gerçekleştirenlerin caydırılması noktasında yaptırımların olması gerekmektedir. Bu sebeplerden ötürü mevzuatların, kanunların bu siber saldırıları gerçekleştirenlere karşı da düzenlenmesi şarttır.

Üçüncü olarak ise siber saldırılar karşısında teknik tedbirlerin geliştirilmesidir. Gelişen teknoloji ile yapılan saldırıların ve siber tehditlerin oluşturduğu zararlar ve etkiler büyümektedir. Hukuki tedbirlerin yanında da teknik tedbirlerin geliştirilerek, sağlam savunma mekanizmalarının geliştirilmesi, daha güçlü güvenlik uygulamalarının yapılması, ISO/IEC 15408 ve TS ISO/IEC 27001 gibi güvenlik standartlarının, yazılımların, donanımların ve işlerin daha güvenli kılınması da saldırılar karşısında caydırıcı nitelik taşıyacaktır.

Dördüncü olarak siber saldırılara karşı kurumsal olarak yapılanmanın belirlenmesidir. Bir ülkede siber güvenliğin sağlanması için, bireylerin, kurumların, özel sektör kurumlarının ve kamu kuruluşlarının hepsine ayrı ayrı şekilde sorumluluklar düşmektedir. Siber güvenliğin ulusal boyutta sağlanması için bu kurumları, bireylerin tamamının siber güvenlik kavramını benimsemesi gerekmektedir. Bunun için, siber güvenliğin tam anlamıyla sağlanması için idari, mali ve teknik imkânların sağlanması gerekmektedir.

Beşinci olarak ulusal olarak iş birliği yapmak ve koordinasyonun sağlanması gerekmektedir. Siber güvenlik alanında faaliyet gösteren kendilerine rol ve sorumluluk yüklenen bireyler ve kurumların birbirlerine bağlı ve koordineli olarak çalışmaları gerekmektedir. Çünkü birimlerin herhangi birisinde en ufak bir güvenlik açığının bulunması tüm birimleri tehlikeye sokmakta ve tüm sisteme zarar vermektedir. Ulusal olarak güvenliğin sağlanması için ilgili birimlerce ulusal politikalar ve stratejiler göz önünde bulundurularak iş birliği ve koordinasyon içinde çalışılmalıdır.

Altıncı olarak siber güvenlik alanında kapasitenin geliştirilmesi söz konusudur. Çünkü gelişen teknoloji ile yapılan saldırıların niteliği, boyutu, etkisi, türü her geçen gün değişmektedir. Bu saldırılara karşı güvenliğin sağlanması için uygulanacak olan politikalar, yasalar, standartlar, siber güvenliği sağlayan sistemlerde geliştirilebilir olmalı ve o zamanın şartlarına uyum sağlamalıdır.

Yedinci olarak siber güvenlik alanında farkındalıklar oluşturulmalıdır. Eğitim kuruluşları, kamu kurum ve kuruluşları, özel sektör alanında faaliyet gösteren bireyler kendilerini ve o kurumda çalışanları siber güvenlik alanında bilgilendirmeli, farkındalık ve siber güvenlik alanında bilgilerinin artırılması gerekmektedir.

Sekizinci olarak uluslararası iş birliği ve uyumun sağlanması gerekmektedir. Küreselleşme ile dünyanın hemen hemen her yerinde kullanılan internet ağları ile bireysel, kurumsal ve ulusal olarak tüm veriler sanal ortamda alt yapılar ve şebekeler üzerinden iletişim kurabilmeyi, veri alışverişi yapabilmeyi sağlamaktadır. Bu ağlar üzerindeki güvenliğin sağlanması adına tüm ülkelerin iş birliği içinde olup dışarıdan gelebilecek saldırılara karşı hazırlıklı olmalı ve yeterli düzeyde güvenliği sağlamaları gerekmektedir. Siber alanda ulusal düzeyde güvenliğin sağlanması için ortak bir mevzuat oluşturulmalı ve o mevzuata göre hareket edilmelidir.

Kamu kurum ve kuruluşlarının, özel sektördeki firmaların veya kurumların, hükümetlerin genel olarak siber alanda savunma ve korunmayı sağlamak adına birtakım yöntemleri uygulaması gerekmektedir (Çeliktaş, 2016: 44). Bu yöntemler;

-Bilişim sistemlerinin bulunduğu cihazlar için oluşan zararlara karşı yama yönetimin yapılması,

-Mevcut güvenlik önlemlerinin artırılması, zafiyet yöntemi ile güvenlik açıklıklarının ve zafiyetlerin tespit edilerek bunların kapatılması,

-Siber saldırı ve tehditlerin tespiti, yapılan saldırıların analiz edilerek sonuçlara göre gerekli önlemlerin alınması,

-Kurum ve kuruluşlarda zaman zaman taramalar yapılarak mevcut olan açıklıkların ve zafiyetlerin tespit edilmesi, raporlanması ve bunlara göre güvenlik önlemlerinin alınması,

-Yapılan siber saldırıların izlenmesi, takip edilerek harita düzenlenmesi ve bu saldırılara karşı merkezi olay yönetim desteğinin alınması,

-Sistemlere gerçekleşen izinsiz, kaçak ve yetkisiz girişlerin tespit edilerek bunların engellenmesi,

-Kanallar için erişim yönetim sistemlerinin oluşturulması,

-Sistemler üzerinde mevcut olan zararlı yazılımların, kaçak işlemlerin takip edilerek ve analizlerinin yapılarak güvenlik açıklarının yetkilerinin düzenlenmesi,

-Sistemlerin alt yapılarının, gerçekleşebilecek tüm saldırılara karşı güvenli olarak inşa edilmesi,

-Siber uzay alanındaki tüm saldırıları, güvenlik açıklarını, zafiyetlerin izlenerek bunlara karşı değerlendirmeler yapılması,

-Sistemlerin elektronik ve yönlendirilmiş saldırılardan korunması,

-Sistemden gerçekleşen veri sızıntılarının izlenmesi, tespit edilerek önlenmesinin sağlanması,

-Zararlı yazılımların sistemlere yüklenmesinin önlenmesi, bu kötü amaçlı yazılımların sistemler üzerindeki hareketlerinin ve zararların tespit edilerek önüne geçilmesi için çalışmalar yapılması,

-Bilgisayarlar üzerinde adli şekilde analizlerin yapılarak; güvenlik önlemlerinin değerlendirilmesi ve yeni önlemlerin alınması, bu önlemlerin takip edilmesi, siber güvenlik alanında farkındalık sağlamak için konu hakkında eğitimler düzenleyerek kurumların farkındalık düzeylerinin arttırılmasının sağlanması,

-Tüm bu önlemlerin ortak platform ile tüm kurumlarca değerlendirerek benimsenmesi ve kurumlar arasında iş birliği, koordinasyonun sağlanmasıdır.

Siber saldırılar ve tehditler ile mücadele ederken ve kullanılan siber saldırılara karşı savunma yöntemlerinin iyi öğrenilmesi ve savunma sistemlerinin doğru şekilde kullanılması gerekmektedir. Sistemler içinde yeterli ve etkin bir koruma ancak doğru savunma yönteminin kullanılması ile sağlanmaktadır (Çalışkan, 2018: 34).

1.7.2. Siber Savunma Yöntemleri

Sisteme karşı yapılan saldırılar karşısında bu saldırılara cevap vermek ya da saldırılar karşısında durabilmek, verilerin korunması, sisteme zarar vermesinin engellenmesi için çeşitli savunma yöntemleri vardır.

1.7.2.1. Zafiyet Tarayıcı (Vulnerability Scanner)

Zafiyet taraması mevcut sistem içerisindeki tüm açıkların tespit edilmesi için yapılan bir yöntemdir. Tarama sonucunda sistemin güvenlik durumunun tespit edilerek olası tehditlere ve saldırılara karşı savunmanın geliştirilmesi için planlar yapılabilir (https://www.mshowto.org/, 2021).

1.7.2.2. Güvenlik Duvarı (Firewall)

Güvenlik duvarları, sistem ve diğer dış ağlar arasında iletimin güvenliği sağlayan yazılımlardır. Güvenlik duvarı ile sistem üzerindeki güvenlik politikaları belirlenir. Tanımlanan politikalar ile hangi veri paketlerinin gönderileceği ya da sisteme alınacağı, hangi verilerin ya da sistemlerin engelleneceği, kimler iletişimde bulunulacağı şeklinde kontrolleri sağlar.

1.7.2.3. Saldırı Tespit ve Önleme Sistemi

Siber saldırıların artması kritik alanlara karşı yapılan saldırıları da doğal olarak artırmıştır. Böylece kritik alanlardaki güvenlik önlemlerin de artması gerekmiştir. İnsanların kendisinin bu alanlarda sürekli olarak güvenliği sağlaması mümkün değildir. Çünkü insan sürekli olarak neyin güvenli olduğu ya da güvenli olduğunu tespit edememektedir. Bu sebeple bu savunma sistemlerinin otomatik olarak doğrudan sistemin kendisi ile akıllı sistemler oluşturarak sağlamak daha faydalıdır. Bu sistemler ile tüm ağda saldırı tespitini yapma, sunucuya gelen talepler içerisinde tehlike oluşturabilecekler içinde tespit yaparak bu tespitler doğrultusunda karşı tepki vermek için çalışır (Of, 2019: 1-7).

1.7.2.4. Antivirüs

Antivirüs programları, virüslere karşı geliştirilmiş temizleme, kurtarma işlemlerini yapan koruyucu programlardır. Bu programlar virüsleri bulmak,

sistemlere girişlerini tespit etmek ve mevcut olan virüsleri silmek için yazılmışlardır (https://it.bilgi.edu.tr/tr, 2021)

Antivirüslerin birtakım amaçlar vardır;

-Bilgisayarları belirli zamanlarda tararlar.

-Sistemde bulunan zararlı yazılımları bulur ve siler.

-Sistem içerisindeki kişisel verileri korur.

-İnternet sitelerinden bulaşmak isteyen trojanlar, spy, worm ve zararlı yazılımları engeller.

-İşletim sisteminin stabil ve düzenli şekilde çalışmasını sağlar (https://ata.com.tr, 2021).

-Bilgisayara takılan CD, USB Bellek, harici HDD gibi birimler üzerinden bulaşabilecek tehlikelere karşı sizi korur.

1.7.2.5. Veri Kaçağı Önleme Sistemi (Data Loss Prevention)

Sistemler içindeki bilgilerin ağ üzerinden dışarıya kaçmasını ya da dışarıdan bu bilgilerin sızdırılmasının önlenmesi için hem izleme hem de önleme amacıyla yapılan ve çalışan yazılımlardan oluşan güvenlik sistemidir (Çeliktaş, 2016: 49).

Veri kaçağı önleme sistemleri son yıllarda trend haline gelmiştir ve kullanılmaya başlanmıştır. Bu sistemler ile verilerinizin sisteminizden çıkışını engelleyebilir ve belirlenen dosyaların kullanım şekilleri izlenebilmektedir (Çalışkan, 2018: 42).

1.7.2.6. Yığın İleti Engelleme Sistemi (Anti Spam)

İstek dışında mail hesabına gelen reklam içeren maillere spam denmektedir. Antispam sistemleri ile bu gelen spam maillerin önüne geçmek hedeflenmiştir. Bu sistemler kullanıcıların istenmeyen reklam amaçlı zararlı maillerin gelmesini engelleyerek kullanıcıların e-postalarını korumayı hedefler (https://www.atakdomain.com, 2021).

Anti spam yazılımlarını kullanarak mevcut olan spamlar engellenebilir, gelen spamlar karantinaya alınabilir, spamlar için filtrelemeler yaparak güncellemeler

yapılabilir, kullanılan birçok hesabı aynı anda takip ederek spamların hareketlerini takip edebilir ve söz konusu spamlar hakkında spam bildirimi yapabilmeyi sağlamaktadır.

1.7.2.7. İçerik Filtreleme (Content Filter)

İletişim ağları içinde belirli kurallar belirleyerek bu kurallara göre istenmeyen kelimeler, videolar, web siteleri, sohbet sitelerine erişimin engellenmesi için kullanılmaktadır. Bu filtreleme tamamen zararlı içerikleri filtreleyen bir sistemdir. Bu sistem ile herhangi bir zararlı yazılım, içerik tespit edildiğinde doğrudan engellenme sayfasına yönlendirir ve o sayfanın görüntülenmemesini sağlar (https://kurumsal.turktelekom.com.tr, 2021).

1.7.2.8. Bal Küpü (Honeypot)

Bal küpü adı casusluk alanından gelmektedir. Bir düşmanın gizliliğini çoğu zaman bal küpü tuzağı ile ortaya çıkarmak mümkündür. Bu sistem bilgisayar ve ağ üzerinde de siber saldırılar karşısında korsanlara karşı tuzak kurmak için kullanılmaktadır. Saldırıları kendi üstüne çekmek için kurban bilgisayar sistemlerine de bu ad verilmektedir. Korsanların hedeflerinin şaşırtılarak asıl hedefi taklit ederek mevcut olan saldırıyı asıl sistemler üzerinden uzaklaştırarak koruma sağlamaktadır (https://www.kaspersky.com.tr, 2021).

1.7.2.9. Adli Bilişim Sistemleri

Adli bilişim sistemleri ile bilgisayar sistemleri üzerinden, sanal ortamlardan, elektronik ortamlardan, bilgilerin ses, video, data olarak toplanması, yedeklenmesi, imajlarının alınarak ve analiz yapılacak şekilde standartlara uygun hale getirerek mahkemelerde yasal delil olarak sunulan çalışmalar olarak değerlendirilir (https://bilirkisiraporlari.com, 2021).

1.7.2.10. Uç Nokta Güvenliği Sistemi (Endpoint)

Uç nokta genel olarak kurumsal bir ağ üzerinde ve o ağ içerisinde sürekli olarak etkileşimlerde bulunan masaüstü bilgisayarlar, laptoplar, akıllı telefonlar, tabletler, yazıcılar olarak tanımlanmaktadır (https://tr.linkedin.com, 2021).

Uç nokta güvenlik sistemleri ile kullanıcıların dikkatinden kaçan zamanlarda özellikle kişisel cihazların güvenliğinin sağlanması, ağ üzerindeki tehditler ve siber saldırılar karşısında o cihazların korunmasını sağlamaktadır.

1.7.2.11. Şifreleme (Kriptografi)

Şifreleme yöntemi, bir bilginin, verinin iletimi, aktarımı sırasında yada sistemin içinde herhangi bir üçüncü kişi tarafından görünmemesi, ele geçirilmemesi için koruma amacıyla yapılan bir sistemdir (https://medium.com, 2021).

1.7.2.12. Elektronik İmza (E-İmza)

Elektronik imza, iletiyi, veriyi gönderenin kim olduğundan emin olmak için ve yasal olarak doğrulama yapmak için elektronik dokümanları imzalamak için kullanılan imza türüdür. Elektronik imza aynı zamanda ıslak imza yerine de geçmektedir. Şifrelemesi asimetriktir. Elektronik imzalar kamu kuruluşlarıyla yapılan işlemlerde, bankacılık sigortacılık işlemlerinde resmi yazışmalarda, hukuki işlerde de kullanılmaktadır (https://ebysweb.ogu.edu.tr, 2021).

1.8. Ulusal Olarak Siber Güvenliğin Sağlanması

Bilgi ve teknolojileri cihazlarının gelişmesi, internetin gelişmesi ve yaygınlaşması, kamu kurum ve kuruluşlarının da, hükümetin bir çok alanda interneti kullanması, teknolojiye bağımlılığın artması olası siber saldırıları da yanında getirmektedir ve bu saldırılara karşı ulusal olarak güvenlik önemlerinin alınması, siber alanda güvenlik politikaları oluşturularak bunların geliştirilmesi, eğitimlerin verilmesi ve bu alanın desteklenerek hükümete ait kritik alt yapıların, güvenlik alanlarının korunması hedeflenmelidir (Ünver ve Canbay, 2011: 100).

Ulusal olarak siber güvenliğin sağlanması ile gelebilecek siber saldırılara karşı, siber tehditlere karşı koyma, tüm teknolojik cihazlarda güvenliğin sağlanması, hükümete ait kritik alt yapı olarak adlandırılan kurumların verilerinin korunması hedeflenmektedir. Bu verilerin saldırıya uğraması, çalınması, oluşabilecek en küçük zarar ile oluşacak kayıplar o hükümetin bireysel veya kurumsal, ulusal çapta, ekonomik, siyasi ve sosyal alanların hepsinde ciddi derecede zarara uğramasına sebep olur. Bu zarar sonrasında ise kurumların, bireylerin hatta diğer hükümetlerin dahi saldırıya uğrayan hükümete olan güveninin sarsılmasına, yok olmasına

sebebiyet verebilir. Tüm bunlar göz önüne alındığında ulusal olarak siber güvenlik politikaları benimsenmelidir ve geliştirilmelidir (Ünver ve Canbay, 2011: 99).

Türkiye'de Bakanlar Kurulu'nun kararı ile siber olaylarla müdahale için çeşitli ekipler kurulmasına karar verilmiştir. Siber Olaylara Müdahale Ekipleri (SOME) ve Ulusal Siber Olaylara Müdahale Merkezi (USOM) bu ekiplerin başında gelmektedir. Bu ekipler ile olası saldırılar karşısında kurum veya kuruluşların siber saldırılardan zarar görmelerini engellemek adına gerekli çalışmalar yapıp tedbirleri almakla görevlendirilmişlerdir (Çalışkan, 2018: 46).

Ulusal ve uluslararası siber güvenliği sağlarken kurum ve kuruluşların dikkat etmesi gereken birtakım hususlar söz konusudur. Bu hususlar;

-Ölçülülük esası temel alınmalı,

-İçinde bulunduğu toplumun düzenine göre yapılmalı,

-Saldırılar için oluşturulan politikalar kısıtlayıcı nitelikte değil, koruma amacı olmalı,

-Kurum için oluşturulan politikalar o kurumun kültürüne ve ihtiyaçlarına göre yapılmalı,

-Politikalar hazırlanırken uluslararası mevzuatlara ve yasalara uygun olmalı,

-Hazırlanan politikaları uluslararası iş birliğine dayanarak yapılmalı,

-Politikalar hazırlanırken kişilerin, kurumların özel hayat gizliliğini esas alarak herhangi bir açık verilmeden hazırlanmalı,

-Siber saldırılar hakkında kişilerin, kurum çalışanların bilgilendirilmesi, bu konular hakkında eğitimler verilmeli,

-Kurumların kendi siber güvenlik ekipleri oluşturulmalı, sürekli olarak geliştirilmeli ve olası saldırılara karşı koruma için hazır olmalı, eğitim ve siber alan hakkında olan gündemi daima takip etmelidir (Ünver ve Canbay, 2011: 94).

Ulusal ve uluslararası siber güvenliğin tam olarak sağlanması adına uygulanacak olan politikaların yanında bir takım güvenlik analizlerinin yapılması da gerekmektedir. Bu yapılacak olan güvenlik analizleri ile mevcut olan saldırıların ne

oranda değiştiği, nasıl bir politika izlenmesi gerektiği, hangi yöntemlerle koruma sağlanıp verimli olanın tespitinin yapılması söz konusudur. Bu analizler sonrasında alt yapıların, sistemlerim uğrayacağı saldırıları engellemek için birtakım yöntemler vardır (İş, 2015: 10). Bu yöntemler;

-Saldırılar karşısında etkin olacak şekilde güvenlik politikalarını oluşturmak ve geliştirmek,

-Sistem ve ağ sistemini geliştirmek, siber güvenlik politikalarını uygulamak,

-Birinci derecede önem arz eden verilerin, sistemlerin, belgelerin sürekli olarak izlenmesi ve takip edilmesi,

-Kuruma uygun, kurum için uygulanabilir politikalar belirlenmesi,

-İleriye dönük veri analizi yapacak politikalar hazırlanması,

-Siber saldırı alanında eğitimler düzenlemek ve farkındalık oluşturulmalı,

-Kurum ve kuruluşların birincil verilerinin saklandığı sistemler için olabilecek saldırıları engellemek adına bu sistemlerin güvenliğinin en üst düzeyde sağlanması, sisteme giriş çıkışların sürekli olarak kontrol edilmesi gerekmektedir.

İKİNCİ BÖLÜM

TÜRKİYE'DE SİBER GÜVENLİK POLİTİKALARI

Türkiye siber güvenlik kavramı ile diğer dünya ülkeleri ile karşılaştırıldığında geç tanışmış ülkelerden birisidir. Her ne kadar geç tanışmış olsa da siber güvenlik alanında günümüzü yakalayacak düzeyde çalışmalar yapmıştır. Bu çalışmalar ile çeşitli siber güvenlik politikaları ve siber güvenlik stratejileri geliştirerek adından dünya gündeminde de söz ettirmeyi başarmıştır.

2. Türkiye'de Siber Güvenlik Politikaları

Türkiye'de daha önceden siber suçlarla mücadeleyi kaçakçılık ve organize suçlarla mücadele dairesi başkanlığı yürütürken günümüzde siber suçlar dairesi başkanlığı yürütmektedir. Türkiye'de en çok banka ve kredi kartı dolandırıcılığı yapılmaktadır. Gelişen teknoloji sebebiyle bilişim suçları her geçen zaman içinde artmaktadır.

Siber suçlara TCK'da ilk kez olarak 6 Haziran 1991 yılında 3756 sayılı kanunda bazı maddelerin değiştirilmesi ile yer almıştır. Bu alanda değişikliğin 20. maddesi "Bilişim Alanında Suçlar" başlığı altında madde eklenmiş, bu madde doğrultusunda bilgisayardan programların, verilerin, bilgilerin hukuk dışı faaliyetler sonrasında ele geçirilmesi ve bunları başkasına zarar verme amacıyla kullanılması, satılması ve nakledilmesi ceza olarak kabul edilmiştir (http://www.kanunum.com, 2022)

Bu gelişmelerin ardından Eylül 2004 yılında yürürlüğe giren 5837 sayılı TCK genişletilerek siber suç kavramı da TCK'ya eklenmiştir. Bilişim alanında suçlar kapsamında 3 bölüme ayrılarak; 243.madde bilişim sistemine göre, 244.madde sistemi engelleme, bozma verileri yok etme, değiştirme ve 245.madde; banka veya kredi kartlarının kötüye kullanımı olarak sınıflandırılmıştır (https://www.mevzuat.gov.tr, 2021)

Siber suçlar hakkında 2006 yılında yapılan değişiklikle siber suçlar terör faaliyeti olarak da ele alınmaya başlamıştır. Bu madde kapsamında "belirli amaçlar doğrultusunda, suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti kapsamında kalırsa, terör suçu sayılır." olarak kabul edilmiştir (https://tr.wikipedia.org, 2022)

Tüm bu gelişmelerin yanında Ankara'da siber uzay, siber güvenlik kavramlarının ulusal güvenlik unsuru kapsamında kabul edilmesi için çeşitli politika çalışmalarına başlanmıştır. Bu çalışmalar kapsamında 2011 senesinde Devlet Planlama Teşkilatı (DPT) bazı belgeler yayımlamıştır. Bu belgeler;

-"e-Türkiye İnisiyatif Eylem Planı (2003-2004)",

-"e-Dönüşüm Türkiye Projesi ve Kısa Dönem Eylem Planı (2003-2004)"

-"e-Dönüşüm Türkiye Projesi ve 2005 Eylem Planı" bu belgelerden bazılarıdır (Şentürk, 2012: 116). Bu belgelerin yanında DPT, 2006-2010 yılını kapsayan bir strateji belgesi ve eylem planı hazırlamıştır. Bu eylem planlarının ana temalarından güvenlik ve kişisel verilerin mahremiyetini korumaktır (http://www.resmigazete.gov.tr, 2022)

Eylem planlarının takip edilmesi, siber güvenlik tehditlerinin takip edilmesi, müdahale edilmesi, siber saldırıların tespiti halinde alınması gereken tedbirlerin belirlenmesi ve bu tedbirler hakkında bilgilendirmeler yapması, koordinasyon sağlanması için SOME'ler kurulmuştur (Darıcılı, 2019: 17).

Ülkede siber alanda politikaların geliştirilmesi sorumlu kurumların artırılması, yetkinleştirilmesi için adımlar atılmıştır. Bu adımlar ile ülkenin siber alandaki yetkinlikleri artırılmış ve geliştirilmiştir. Böylece siber güvenlik alanında güvenilir yerli yazılım ve donanımların geliştirilmesine odaklanılmıştır.

Siber güvenlik politikaları ve stratejileri hazırlanırken temel olarak bazı önemli alanlar vardır. İlk önemli alan askeri siber operasyonlardır. Böylece doğrudan etken yapıya sahip olduğu bilişim alt yapılarının korunması hedeflenmiştir. Bu alanların korunması için aktif ve pasif olarak siber savunma biçimleri olmalıdır ve uygulanmalıdır. Aktif savunma ile saldırganın saldırı maliyetlerinin artırılması ve saldırıdan vazgeçmesi amaçlanır. İkinci ise askeri alanda düşman unsurlarının bilişim alt yapılarına stratejik ve nitelikli şekilde operasyonlar gerçekleştirilmelidir. Bu operasyonların dışında düşmanın sahip olduğu alt yapılara karşı siber saldırılar yapılmalıdır. Son olarak saldırı ve savunma mekanizmalarının gelişen teknolojiye göre uyum sağlaması sağlanmalıdır (Hekim ve Başıbüyük, 2013: 153).

Siber alanda önemli olan ikinci alan ise siber suçlarla mücadele yapabilmek adına ilk olarak siber alanda ulusal ve uluslararası hukuki alt yapıların oluşturulması gerekmektedir. Hukuki alt yapılının oluşumunun sağlanması Adalet Bakanlığı tarafından yürütülmektedir. Siber alanın ulusal nitelikte olması sebebiyle ulusal olarak hukuk sistemlerinin gelişmesi, ulusal olarak iş birliği halinde çalışmalar yapılmalıdır. Ülkemizde siber suçlarla mücadele alanında en büyük görev polislerin üzerine düşmektedir. Bu sebeple adli bilişim uzmanlarının sayısının artırılması, mevcut personelin deneyimlerinin ve bilgilerinin artırılması hedeflenmiştir. Ulusal suçların dışında sınırı aşan suçlar içinde ve bu suçların soruşturmasının yapılabilmesi için diğer ülkelerin polisleri ile iletişim halinde olmalı, bilgi ve tecrübelerin paylaşılarak soruşturmanın seyrini hızlandırmak hedeflenmiştir (Hekim ve Başıbüyük, 2013: 153).

Siber alanda önemli olan üçüncü alan ise siber istihbarattır. Ulusal olarak siber alandaki güvenliği sağlamak için önemli unsurlardan birisidir. Sadece kendi alanında değil, karşı istihbarat bilgilerinin de güçlü olması, istihbarat operasyonu yapabilme ve buna karşı koyabilmelidir. Siber alanda önemli olan dördüncü alan ise kriz yönetimi ve ulusal olarak kritik alt yapıların korunmasını sağlamaktır. Kriz yönetimi becerileri ile siber saldırılar sonrasında oluşan zararlar ve hasarlar karşısında uygun adımlar atmak, saldırılara karşı saldırı ile cevap vermek, acil noktalara müdahale, hasar gören sistemlerin tekrardan ayağa kaldırılması amaçlanmıştır. Tüm bu işlemleri Ulusal CERT (Computer Emergency Response Team) gerçekleştirir. Ulusal olarak kritik alt yapıların korunması için tüm ülke kapsamında risk analizi yapılarak bu analiz doğrultusunda çalışmalar yapılmaktadır (Hekim ve Başıbüyük, 2013: 153-154).

Siber alanda önemli beşinci ve son alan olan; siber diplomasi ve internet yönetiminin kontrolünün sağlanmasıdır. Ulusal çıkarların korunması adına bu çıkarlar doğrultusunda siber diplomasiye yeterli düzeyde önem verilmelidir (Hekim ve Başıbüyük, 2013: 154).

2.1. Siber Güvenlik Politikalarında Hukuki Alt Yapı

Siber politikalar hazırlanırken hukuki olarak alt yapısının da hazırlanması gerekmektedir. Yapılan saldırılar karşısında bu saldırıların sonucunun bir yaptırımı olması gerekmektedir. Elektronik ortamdan yapılan saldırılan veya işlenen suçlar Nitelikli Dolandırıcılık olarak TCK'da yer almış ve ağırlaştırıcı sebep olarak kabul edilmiştir. İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun belirtilmiştir. Elektronik ağlar ile işlenen suçlar içinde TCK'da Bilişim Alanında Suçlar başlığına yer verilmiştir (Hekim ve Başıbüyük, 2013:149).

TCK'da genel olarak bilişim sistemleri üzerinden işlenen suçları, elektronik ortamdaki işlenen suçlar vb. tüm suçları kapsayan hükümler ve cezai yaptırımlar bulunmaktadır. Casusluk veya tehdit amacıyla saldırıyı düzenleyen kişi ve herhangi bir statü için siber saldırı düzenleyen kişi aynı şekilde değerlendirilecektir. Siber saldırının hangi alanda olduğu ya da saldırı yapılan sistemin küçük veya büyük olması fark etmeksizin yaptırımı aynıdır (Hekim ve Başıbüyük, 2013: 150).

TCK yönünden siber alanda başkaca önemli bir hukuki metin vardır. Avrupa Konseyi Siber Suçlar Sözleşmesi 2001 yılında kabul edilmiş 2004 yılında yürürlüğe girmiştir. Türkiye bu sözleşmeye 2010'da taraf olmuştur. TCK'ya nazaran daha detaylı bir sözleşmedir ve birçok siber alan ile ilgili tanımlara ve hükümlere yer verilmektedir (Önok, 2013: 1241).

Bilişim suçlarını ve siber alandaki suçları ilgilendiren başka bir kanun ise 5271 sayılı CMK'dır. Bu kanuna göre bilişim sistemlerindeki verilerin bilgisayar vb. unsurlar ile arama, kopyalama, el koyma sonucunda, bu verilerin muhafaza edilmesine dair hükümler bulunmaktadır (Hekim ve Başıbüyük, 2013: 151). Siber suçlarla mücadele hedefli başka bir kanunda 5651 sayılı internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkındaki kanundur. Kanun yürürlüğe girmesinden sonra uygulamayı düzenlemek ve geliştirmek adına çeşitli yönetmelikler çıkarılmıştır. Kanun internette mevcut olan hangi içeriğin yasa dışı olduğunu internet ve içerik sağlayıcılarının rol ve sorumluluklarını belirtmektedir. Yasa dışı içeriklerle mücadelede bu içeriği doğrudan

engelleyip ortadan kaldırma anlayışı benimsenmiştir (https://www.mevzuat.gov.tr, 2022).

Bilişim teknolojilerinin yaygınlaşması, internet kullanımının artması ile siber güvenlik kavramına ulusal güvenlik stratejilerinde yer verilmiştir. Bu sebepten ötürü gelişmiş ülkeler dâhil birçok AB ülkesi siber güvenlik alanında çeşitli stratejiler oluşturmuştur. Bu stratejilerin incelemesi sonucunda çeşitli ortak hedeflere varılmıştır. Stratejiler ile güvenli, saldırılar karşısında dayanıklı ve sağlam bir siber alan, siber alanın ve teknolojinin kullanılarak ekonomik büyümesinin sağlanması, refahın artırılması vb. bilişim sistemlerinin doğuracağı risklerin kontrol altına alınması ve bilişim alt yapılarının güçlendirilmesi hedeflenmiştir.

Ülkemizde siber güvenlik alanında geçmişte çok fazla çalışma yapılmamıştır. Önemli olarak iki temel çalışma vardır. İlki bilgi güvenliğine ilişkin yasal düzenlemelerin yapılması, ikincisi bilgisayar olaylarına acil müdahale merkezinin kurulması ve kamu kurumlarının bilişim güvenliğinin sağlanmasına yönelik faaliyetlerdir. Bu faaliyetlerin yanında Bilgisayar Olaylarına Müdahale Ekibi (TR-BOME), TUBİTAK ve BİLGEM bünyesinde kurulmuştur ve faaliyete geçmiştir (Karasoy ve Babaoğlu, 2021: 141).

Ülkemizde siber güvenlik alanında atılmış en somut adım "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar", Bakanlar Kurulu kararıyla Siber Güvenlik Kurulu'nun kurulmasıdır (https://www.resmigazete.gov.tr, 2021). Bu kurul Bakanlar Kurulu'nun doğrultusunda; ulusal bilgi teknolojilerinin ve iletişim alt yapısı ve sitemleri ile veri tabanlarının güvenliğini sağlamaya, kritik alt yapılarını belirleyecek bunlara yönelik siber tehdit ve saldırı izleme, müdahale ve önleme sistemlerini oluşturmaya, ilgili merkezleri kurmaya, korumaya, bu sistemlerin denetimi, işletimi ve sürekli güçlendirilmesine yönelik çalışmalar yapılmıştır. Bu çalışmalar kapsamında da Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekipleri (SOME)'ler kurulmuştur ve faaliyetleri beraber yürütmüşlerdir (https://www.btk.gov.tr, 2021).

2.2. Türkiye'nin Siber Güvenlik Politikalarının Gelişimi

Günümüz gelişen teknolojisi ile toplum ve devletlerin siber saldırılar karşısında kendisini geliştirmesi gerekmektedir. Çünkü tam anlamıyla bir korunma sağlanması, saldırılar karşısında yeterli düzeyde güvenlik önlemleri bulunmamaktadır. Siber alan tüm herkese açık bir alandır ve her alanda herkesin saldırı yapabileceği, güvenlik önlemlerindeki açıkların tam olarak giderilmemesi bu saldırılar sonucunda ciddi derecede zararlara sebep olmaktadır. Bu saldırıların temel kaynağı teknolojinin çok hızlı şekilde gelişmesi, ülkelerin ya da toplumların bu gelişimleri eş zamanlı takip edememesi ve saldırılar karşısında yeterli düzeyde önlemler almamasından kaynaklanmaktadır. Ülkeler ve toplumlar bu saldırılar karşısında çeşitli çalışmalar yaparak tam anlamıyla önlemek yerine, saldırılar karşısında izleyeceği adımları yönetebilmeli doğru hamlelerde bulunmalıdır.

Türkiye bu saldırılar karşısında bağımsız değildir. Siber güvenliği ulusal alanda sağlanması adına sorumluluğu Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na (UDHB) vermiştir. UDHB'nin yanında Emniyet Müdürlükleri, Milli İstihbarat Teşkilatı gibi güvenlikten sorumlu birimlerinde kendi alanlarında siber saldırılar karşısında sorumluluklarını ve görevlerini belirtmiştir. Öncelikle savunma sanayi ile ilgili olan alanlardaki verilerin korunması adına gerekli önlemlerin alınması için çalışmalar yapmaktadır. UDHB siber alanda, siber saldırıların karşısında güvenliğin sağlanması için birimler ve kurumlar arasındaki koordinasyonu sağlama, ulusal alanda yapılacak olan eylem planlarının hazırlamakla, bunların uygulanması ve takibi açısından en önemli sorumluluğa sahiptir (Seren, 2016: 21).

Türkiye'ye yapılan siber saldırılar sonrasında ilk ciddi atılım olarak 1997 yılında TÜBİTAK BİLGEM bünyesinde "Ağ Güvenliği Grubu" ile başlamıştır. Ağ Güvenliği grubu adını 2012 tarihi itibariyle "Siber Güvenlik Enstitüsü (SGE)" olarak değiştirilmiştir (https://sge.bilgem.tubitak.gov.tr/, 2022). Siber Güvenlik Enstitüsü ile Türkiye'de siber güvenliğin sağlanması adına yürütülen çalışmalar başlamış, güvenliğin sağlanması adına projeler geliştirilmeye başlanmıştır. 2001 yılında Genelkurmay Başkanlığı'nın desteği ile "Ortak Kriter Test Merkezi (OKTEM)" kurulmuş, ardından "Haberleşme Güvenliği (COMSEC)" testleri faaliyete girmiş, 2006 sonrasında ise "Yan Kanal Analizi" ve "Tersine Mühendislik" konularında

uzmanlaşmalar gerçekleşmiştir. Tüm bunların yanında Devlet Planlama Teşkilatı Bilgi Toplumu Dairesi Başkanlığı'nın 2005 yılında başlattığı "Bilgi Toplumu Stratejisi" projesi ile Türkiye adına önemli getirileri olmuştur. Bu proje ile Ağ Güvenliği Grubunun yürüteceği kamu kurum ve kuruluşlarının bilgi sistemleri üzerine güvenliği sağlamak, olası güvenlik problemlerine karşı önlem almak ve bu problemleri en aza indirgemek amaçlanmıştır ve "Bilgi Güvenliği Programı" oluşturulmuştur (Seren, 2016: 22). Bu adımlar ile Türkiye'nin sanal ortamda bilgi güvenliği sorunlarına karşı zamanında ve sağlıklı müdahale edebilmek amaçlanmıştır.

Siber güvenlik konusunda ilk ciddi adım ise 27 Ekim 2010 tarihinde Milli Güvenlik Kurulu'nda siber güvenlik sorunları ve konularının Milli Güvenlik Siyaset Belgesi'nde açıkça yer verilmiştir ve gerçekleştirilmiştir (Bıçakçı, Ergün ve Çelikpala, 2015: 10).

Bu adımla Milli Güvenlik Kurulu, siber güvenlik kavramını ve siber alanı ülke gündemine taşımıştır.

Siber güvenlik için gerçekleştirilen tatbikatlar önemlidir. 25-28 Ocak 2011 tarihleri arasında TUBİTAK ve BTK iş birliği ile 1. Ulusal Siber Güvenlik Tatbikatı yapılmıştır. Bu tatbikatta kamu ve özel sektör üzerinden 41 ülke katılmıştır. Tatbikat sonrasında yayımlanan rapora göre devlet kurumlarının siber alanda çok fazla yetkin olmadığı tespit edilmiştir. 2012 yılında Redhack tarafından gerçekleştirilen saldırılar e-devlet kurumları ve hizmetleri üzerinde tehdit algısını geliştirmiştir. Bunun üzerine 20 Ekim 2012'de Bakanlar Kurulu "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar"ı onaylamış ve 28447 sayılı Resmi Gazetede yayımlanmıştır. Yetki, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na verilmiştir (Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, 2012:3842). Bu gelişmenin ardından Siber Güvenlik Kurulu ilk toplantısını 21/12/2012 tarihinde Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nda gerçekleştirilmiştir. Siber Güvenlik Kurulu'nun temel görevleri arasında ise siber güvenlikle ilgili alınacak önlemlerin tespiti, Türkiye'nin siber güvenlik politikalarını belirlemek, söz konusu politikaları yönetmek, hazırlanan

plan, program, rapor, yöntem ve standartların onaylanarak uygulanması ve koordinasyonu sağlanmasına yer verilmiştir (Darıcılı, 2019: 27).

İkinci siber alanda tatbikat 2013 yılında tekrar yapılmıştır. Bu tatbikatta 61 adet kurum ve kuruluş katılmıştır. Olası tehditlere karşı alınacak olan tedbirler denenmiştir (Bıçakçı, Ergün ve Çelikpala, 2015: 9). Bu tatbikatın ardından ilk eylem planı olan 2013-2014 yıllarına ait eylem planı hazırlanmıştır. Bu eylem planı ile Türkiye'de alınan siber güvenlik faaliyetlerin yetersiz olduğu ve tehditlere karşı alınan tedbirlerin yetersiz olduğu vurgulanmıştır (Ceyhan, Demiryürek ve Kandemir, 2015: 7).

USOM ve SOME'ler bu eylem planı ile oluşturulmuştur. 2013-2014 eylem planı gereğince Türk Standartları Enstitüsü'nde Siber Güvenlik Özel Komitesi oluşturulmuştur. Bu komite ile siber güvenlik alanında inovasyon ve araştırma-geliştirme çalışmalarına başlanılmıştır (Akkaya, 2014: 51).

Ulusal düzeyde bilgi güvenliğinin ve siber savunma alanında yapılan çalışmalar kapsamında 2012 yılında TSK bünyesinde Siber Savunma Merkezi Başkanlığı kurulmuştur. Başkanlık 2013 yılında ise Siber Savunma Komutanlığı'na dönüştürülmüştür. Bu gelişmelerle birlikte siber alanda oluşabilecek tehditleri belirlemek adına, saldırıların oluşan zararların tespiti adına ve bu zararların etkilerin ortadan kaldırılması ya da en aza indirgenmesi amacıyla "Ulusal Siber Olaylara Müdahale Merkezi (USOM)" kurulmuştur (www.usom.gov.tr, 2022).

USOM'un arkasından siber saldırılar karşısında anında harekete geçebilmek, savunmayı ve yeterli düzeyde güvenliği sağlamak adına "TSK Siber Savunma Merkezi Projesi (SSMP)" geliştirilmiştir. Bu proje ile siber saldırılar karşısında aynı anda karşılık verebilmek amaçlanmıştır. SSMP'nin ardından HAVELSAN, siber alanda en iyi savunmayı geliştirmek ve saldırıları tam anlamıyla engellemek adına 2016 yılında "Siber Savunma Teknoloji Merkezi (SİSATEM)" kurulmuştur (https://www.savunmasanayiidergilik.com, 2022).

Bu süreç zarfında birçok ülkenin stratejik planları, siber güvenlik stratejileri, eylem planları incelenmiş elde edilen veriler hazırlanacak olan yeni eylem planında hepsi göz önünde bulundurularak "2016-2019 Eylem Planı" da hazırlanarak

yayımlanmıştır. Bu eylem planı ile siber güvenlik kavramının ulusal güvenlik, kamu güvenliğinin bir parçası olduğunun benimsenmesi hedeflenmiştir (Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı, 2016: 9)

2016-2019 Eylem planı ile iç ve dış güvenlik birimleri, savunma sanayi, eğitim, sağlık, ulaşım, enerji gibi kritik alt yapıların korunması devletlerin ve karar alıcıların öncelikli politikaları olarak öne alınmıştır. Diğer ülkeler ve Türkiye incelendiğinde de Türkiye'nin kritik alt yapılarla ilgili ulusal ve politika açısından diğer ülkelerden geri kaldığı, siber alanda yapılan çalışmaların 2010 yılına kadar yetersiz kaldığı söylenebilir.

Uluslararası Telekomünikasyon Birliği'nin 6 Temmuz 2017 tarihinde yayınladığı Siber Güvenlik Araştırması ve indeksi Türkiye açısından önemli bilgiler içermektedir. Bu rapora göre Türkiye siber güvenlik alanında yaptığı faaliyetleri ile 43.sırada yerini almıştır (Global Cybersecurity Index, 2017: 60)

Bu raporlar doğrultusunda Türkiye'de Kasım 2018'de Devlet Denetleme Kurulu'nun 10 bölüm ve 859 sayfadan oluşan siber güvenlik raporu 2 yıllık çalışma sonrasında Cumhurbaşkanlığı'na sunulmuş ve ilgili kurum ve kuruluşlara gönderilmiştir. Bu rapor 68 ana öneri, 179 alt öneriden oluşmaktadır ve 15 ülkenin siber alandaki çalışmaları dikkate alınarak hazırlanmıştır. Rapora göre siber güvenlik faaliyetleri Cumhurbaşkanlığı Dijital Dönüşüm Ofisi koordinasyonu ile yürütülmelidir.

Devlet Denetleme Kurulu'nun raporuna göre kritik alt yapıların önceliklerinin belirlenmesi, kurum ve kuruluşlardan siber güvenlik faaliyetlerinin sağlanması için yerli ve milli ürünlerin kullanılması ve geliştirilmesi, siber güvenlik ekosistemlerinin oluşturulması, nitelikli personel yetiştirilmesine dair maddelere yer vermiştir. Bu maddelerin dışında; siber güvenlik alanında farkındalık ve başlangıç eğitimi çerçevesinde; güvenli internet, yazılım, kodlama ve robotik alanda ilk ve orta okul düzeylerinde müfredatların yer alması; üniversitelerde ön lisans, lisans ve lisansüstü programların açılması, fiziki olarak engelli ancak zihinsel olarak üst düzey zekaya sahip kişilerin kamu ve kuruluşlarda istihdam edilmesi, bu kişilere siber güvenlik alanında eğitim programlarının hazırlanması önerilmiştir (Demirci, 2021: 55).

Türkiye bu raporların ardından siber güvenlik alanında eğitim ve farkındalığın artırılması için çalışmalar yapmıştır. Ekim 2018'de Zonguldak'ta düzenlenen "Türkiye Siber Güvenlik ve Eğitimi" başlıklı bir sempozyum yapmıştır.

Türkiye'de siber alanda mücadele 2012 yılına kadar Bilim, Sanayi ve Teknoloji Bakanlığı'nın önderliğinde Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yürütülmüştür. 2013 yılından itibaren oluşturulan "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" yürürlüğe girmiştir. 20 Ekim 2012 tarih ve 2012/3842 sayılı "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 eylem planında siber ortamı oluşturan sistemlerin saldırılardan korunması, siber ortamda işlenen bilgilerin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınması, saldırın ve güvenlik açıklarının tespit edilmesi amaçlanmıştır (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2012: 9-47).

Bu eylem planının ardından 9 Eylül 2016 tarihinde gerçekleşen bir toplantı ile Türkiye'nin her 4 yıllık süreçte siber alanda izleyeceği güvenlik politikalarını oluşturan 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı oluşturulmuştur. Bu planından ardından 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem planı takip etmiştir. BTK'nın ardından siber güvenlik çalışmalarının yürütülmesi için TSK'nın da bilgi sistemlerinin güvenliğini sağlaması ve olası saldırılar karşısında harekete geçebilmesi adına ve bu saldırıların etkilerinin en aza indirgenmesi hedeflenmiştir. "TSK Siber Savunma Merkezi Projesi (SSMP)" projesi geliştirilmiştir. Bu proje ile siber savunma merkezinin kurulması, bu savunma merkezinin gereksinimlerinin giderilmesi adına "Siber Savunma Harekât Merkezi" faaliyete geçirilmiştir. Siber Savunma Hareket Merkezi'nin faaliyete geçirilmesinin ardından HAVELSAN bünyesinde "Siber Savunma Teknoloji Merkezi (SİSATEM)" 23 Mart 2016 tarihinde faaliyete girmiştir (https://www.haberbilimteknoloji.com, 2021).

Tüm bu gelişmelerin ardından Ulusal Siber Güvenlik Stratejisi ve Eylem Planları (USGSEP) oluşturulmaya başlanmıştır. Bu eylem planları ile Türkiye'nin bu zamandan sonra siber güvenlik alanında izleyeceği politikalar benimsenerek; stratejik olarak hareket etme, siber güvenliğinde milli güvenlik gibi önemli bir unsur olduğunu, toplumun tüm kesimlerinin siber alanda farkındalıkların oluşturulması ve

bilgi sahibi olmaları açısından bilinç seviyelerinin artırılması, siber güvenlik alanında alt yapıların güçlendirilmesi ve saldırılar karşısında her an hazır olmak hedeflenmiştir.

USGSEP'ler ile; bilgi teknolojileri, kamu verileri, ülkenin güvenliğinin saklandığı, tüm bu verilerin akışını sağlayan, her türlü işlem ve hizmeti gerçekleştiren sistemlerin güvenliğinin sağlanması, siber alanda güvenlik açısından risk ve tehdit olarak belirlenen olayların, faaliyetlerin önlenmesi, saldırının gerçekleşmesi halinde söz konusu zararın en aza indirgenmesi, oluşan zararın en kısa sürede giderilmesi ve zarar gören sistemin eski haline döndürülerek çalışmasının devam etmesi, suçun hukuki ve idari kovuşturmaya ve soruşturmaların takip edilmesi amaçlanmıştır. Tüm bunlara ek olarak siber güvenlik alanında kullanılan teknolojilerin ve verilerin gizliliğinin sağlanabilmesi adına güvenliği sağlayan araçlarda yerli üretim teknolojilerin kullanılması amaçlanmıştır.

Yine USGSEP'ler ile; sürekli gelişen teknoloji ve sürekli olarak değişen sistemler karşısında eş zamanlı olarak gelişimin sağlanması ve sürekli olarak güncel sistemlere, güncel koruma ve güvenlik sistemlerine sahip olmak hedeflenmiştir. Ortaya çıkan yeni saldırılar karşısında güvenlik açısından eksik kalmamak, saldırılar karşısında hazır olmak ve aynı değerde onlara karşılık vermek hedeflenmiştir. Siber alandaki gelişmeler sonrasında özel ve kamu sektörlerinde meydana gelen açıklıkların kapatılması amaçlanmıştır (Seren, 2016: 24).

20 Ekim 2012 tarihli ve 28447 sayılı Resmi Gazete'de yayımlanan Bakanlar Kurulu'nun 2012/3842 sayılı kararı ile Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin kararın yürürlüğe girmesi ile Siber Güvenlik Kurulu (SGK) bir takım çalışmalara imza atmıştır. Bu çalışmalar doğrultusunda; kamu kurum ve kuruluşlarının olası fiziksel ve siber saldırılar karşısında güvenliğinin sağlanması adına kendi aralarında güvenli bir ağ üzerinden haberleşmeleri amacıyla, e-Devlet uygulamalarının ortak kullanırken daha güvenli olmasını sağlamak amacıyla "Kamu Sanal Ağı (KamuNet)" oluşturulmuştur. 3 Aralık 2016 tarih 29907 sayılı Resmi Gazete'de yayımlanarak tüm kamu kurum ve kuruluşları KamuNet'e dâhil edilmiştir (https://www.resmigazete.gov.tr, 2022).

Genel olarak değerlendirme yapıldığında Türkiye'nin siber politikalar alanında yaptığı; Siber Güvenlik Eylem Planları, Ulusal Bilgi Güvenliği Kapısı, Ulusal Bilgi Güvenliği Programı, yapılan yasal çalışmalar, Siber Güvenlik Müdahale Ekipleri ve Birimleri, Siber Güvenlik Tatbikatları, Konferanslar ve Çalıştaylar ve TSK'nın kendi kapsamında siber güvenlik alanında yaptığı projeler ile Türkiye'de siber güvenlik bilincinin ve farkındalığının artırılması hedeflenmiştir (Öğün ve Kaya 2013: 168).

2.3. USOM – Ulusal Siber Olaylara Müdahale Merkezi

USOM, 20 Haziran 2013 tarihinde Bakanlar Kurulu kararı ile kurulmuştur. 2013-2014 eylem planı içerisine dahil edilmiştir. Ülkemizde siber güvenliğin sağlanması için ortaya çıkan veya olası siber tehditlerin belirlenmesi, muhtemel olan saldırıların ve güvenlik açıklarından doğacak zararların en aza indirgenmesi amacıyla kurulmuştur. Söz konusu siber saldırılar hakkında gelen ihbarlar doğrultusunda bu olayların en başından çözüm aşamasına kadar takip ve kontrol eden resmi bir kurumdur. Ulusal ve uluslararasında siber güvenlik tatbikatları düzenleyerek tüm özel veya kamu kurumlarına siber saldırılar karşısında bilinçlendirmek ve farkındalığın artırılması hedeflenmektedir.

USOM, BTK bünyesinde kurulan bir kurumdur (https://berqnet.com, 2021).

Yurtiçi ve yurtdışı kaynaklı olarak gelişen siber suçları, saldırıları ve tehditleri tespit ederek bunları engellemek, saldırının gerçekleşeceği yerleri kurumları, verileri korumakla görevlidir. Ortaya çıkacak olan sorunları değerlendirerek söz konusu kurumları bilgilendirmesi, uyarılmasını gerçekleştirmektedir.

Tüm bunların yanında bünyesinde SOME isimli ekipleri barındırmaktadır. SOME'ler USOM'un altında Kurumsal SOME ve Sektörel SOME olarak ikiye ayrılmaktadır.

Kurumsal SOME'ler bakanlıklar ve müstakil kamu kurumları arasındaki koordinasyonu sağlamaktadır.

Sektörel SOME'ler ise; özel sektörler ve kritik seviyede iş yapan kurumlar arasındaki koordinasyon sağlamaktadır. Enerji, bankacılık ve finans sektörleri,

ulaştırma, kritik kamu hizmetleri, su yönetimi ve elektronik haberleşme konusunda koordinasyon sağlamaktadır.

USOM'lar kurumsal ve sektörel SOME'leri bünyesinde barındırdıkları için doğrudan ve dolaylı olarak gerçekleşebilecek siber saldırılar karşısında gerekli önlemlerin alınması, saldırılara müdahale edebilmesi ve müdahale ekiplerinin, sistemlerinin, mekanizmaların kurulmasında yardım etmekle yükümlüdürler. Bu sebeplerden ötürü çok önemli yere sahiptirler (https://it.bilgi.edu.tr, 2021).

USOM kurulduğundan bu yana 27.408 zararlı bağlantı, 8 bin 841 resmi güvenlik açığı, 878 güvenlik bildirimi tespit etmiştir. Uluslararası Telekomünikasyon Birliği Global Siber Güvenlik Endeksi'nde yükselip Dünya'da 11., Avrupa'da ise 6. Sırada yer almıştır (https://www.haber365.com.tr, 2022).

2.4. SOME – Siber Olaylara Müdahale Ekipleri

SOME'ler USOM'un kurulması ile USOM kapsamında kurulan ekiplerdir. 11 Kasım 2013 tarihli 28818 sayılı Resmi Gazetede ilk kez yayımlanmışlardır. SOME'ler hakkında yayımlanan resmi gazetede SOME'lerin siber olaylar karşısındaki kuruluş amaçları, görevleri ve çalışmaları belirlenmiştir. (https://www.resmigazete.gov.tr, 2022).

2.4.1. Kurumsal SOME

Bakanlık bünyesinde hizmet gereklerine göre bakanlık birimine bağlı ilgili ve ilişkili kurumları kapsayacak şekilde kurulur. Bakanlık koordinesinde bakanlık birimlerine bağlı, ilgili ve ilişkili kurum ve kuruluşları alt yapıların büyüklüğüne ve ihtiyaçlar doğrultusunda kendi bünyelerinde kurumsal some'ler kurulabilirler. Tüm kamu kurum ve kuruluşları kendi bünyeleri kapsamında kurumsal some kurabilirler (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014: 11).

Kurumsal SOME'ler bünyesi içinde bulundukları kurumlara doğrudan veya dolaylı olarak yapılan ve yapılacak olan saldırılar karşısında önlemleri alma, olası saldırılar karşısında bu saldırılara karşı müdahale merkezleri hazırlamak kurum veya kurumların bilgi ve veri güvenliğini sağlamakla görevlidir. Siber olayların önlenmesi, zararların en aza indirgenmesi, oluşan hasarların azaltılmasına yönelik

kurumların bilişim sistem güvenliğinin kurulması, işletilmesi ve geliştirilmesi hususunda katkı sağlar (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014: 7).

Kurumsal SOME'ler siber olayların önlenmesi veya zararların azaltılmasına yönelik faaliyetleri eğer varsa sektörel someler ile birlikte eş zamanlı olarak yürütürler ve bu durumu USOM'a bildirmek zorundadırlar. Kurumsal SOME'ler olası bir saldırı karşısında USOM ve birlikte çalıştığı sektörel SOME'ye bilgi verme koşulu ile mevcut saldırıyı engellemeye, bertaraf etmeye çalışır. Başa çıkamayacak düzeyde ise sektörel some ve USOM'dan yardım talep edebilirler (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014: 14).

Kurumsal SOME'ler siber olaylara müdahale ederken suç işlendiğine dair bir bulguya rastlarlarsa durumu yetkili kanuni merciiye ve USOM'a bildirir. Gelişen olaylara saldırılara karışı düzenlenen siber raporları vakit geçirmeden USOM'a ve Sektörel SOME'ye bildirirler. (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014: 14).

2.4.1.1. Kurumsal SOME Kuruluş Aşamaları

Kurumsal SOME'ler kurum içinde belli aşamalara göre kurulmaktadır. Bu aşamalar Kurumsal SOME'lerin kurum içerisindeki yeri ve kapasitesi, kurum içi ve kurum dışı paydaşlarla iletişim esasları, gerekli eğitimlerin alınması şeklinde gerçekleşmektedir (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014: 12)

Kurumsal SOME'ler bilgi işlem birini bünyesinde veya bilgi işlem birimi dışında kurulabilirler. Kurum içerisindeki bilgi güvenliği veya siber güvenlikten sorumlu birimler (şube müdürlükleri, daire başkanlıkları, başbakanlık vb.) kurulmuş ise Kurumsal SOME görevlerini bu birim yerine getirebilir ya da bu birim altında kurulurlar.

Kurumsal SOME'lerin temel sorumluluğu siber güvenlik olan bir amir yönetiminde; bir birim olarak kurulması tavsiye edilmektedir. Amirleri en az lisans derecesinde mezun olup, siber güvenlik alanında uzmanlıklarının olması gerekmektedir. Kurumsal SOME'lerin 5 temel fonksiyonu vardır (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014: 15). Bu fonksiyonlar:

-SOME biriminin yönetimi ve fonksiyonu,

-Olaya karşı müdahale yönetim ve koordinasyon fonksiyonu,

-Sistemin test ve denetimi fonksiyonu,

-Kurumsal olarak siber güvenlik bilinçlendirme fonksiyonu,

-İş kayıt analiz fonksiyonu.

Kurumsal SOME'ler, siber olay öncesinde, siber olay sırasında ve siber olay sonrasında olmak üzere 3 temel şekilde içinde bulunduğu kurumun bilgi işlem birimi, hukuk ve halkla ilişkiler birimleri birlikte çalışmaktadır (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014: 17).

Kurumsal SOME'ler; siber güvenlik alanında belirlenen politikalara uygun şekilde faaliyet göstermek, ihtiyaç halinde yetkili birimler ve makamlar ile iletişime geçmek, kayıtları, elde edilen verileri yetkili makamlara iletmekle ve bu olaylar karşısında gerekli müdahalelerde bulunmakla sorumludurlar.

Kurumsal SOME'lerin diğer kurumlar ile arasındaki iletişimi süreklidir ve USOM üzerinden gerçekleştirilmektedir. USOM'un yanında diğer Kurumsal SOME'ler de bilgi aktarımı, veri paylaşımı yapabilirler. Kurumlar arasındaki bu iletişimler şifreli ve sürekli olarak gerçekleşmektedir.

2.4.1.2. Kurumsal SOME'lerin Görev ve Sorumlulukları

Kurumsal SOME'ler kurumun içinde çalışırken siber olay öncesinde, siber olay sırasında ve siber olaydan sonra olmak üzere 3 ayrı görev ve sorumluluklara sahiptir (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014: 17).

- **Siber Olay Öncesi**

Kuruma karşı herhangi bir siber olayın yaşanmadığı veya gerçekleştirilmediği durumlarda Kurumsal SOME'ler kurum içinde farkındalık çalışmaları yapmaktadır. Kurumsal sistemler üzerinde sızma testleri gerçekleştirerek, olası saldırılar karşısında kurumun ne denli koruma altında olduğunun tespiti için inceleme çalışmaları yapılmaktadır (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014: 18).

Kurumsal SOME'ler farkındalık çalışmaları ile:

-Kurum içerisindeki personele düzenli aralıklarla siber alan ve siber güvenlik alanında sunumlar, eğitimler yapmaktadır.

-Siber güvenlik alanında kurum içinde çeşitli bültenler hazırlanmaktadır.

-İçinde bulunduğu kurumun çalışanlarına yönelik periyodik alarak siber güvenlik hakkında E-Postalar gönderilmektedir.

-Kurumun kullandığı sistemlerde siber güvenlik için çeşitli bakımlar yapar.

-İçinde bulundukları kurumun bilişim sistemleri içerisinde çeşitli güvenlik testleri yaparak açıkları tespit ederler.

-Kurumsal SOME'ler belirli zaman aralıkları ile bilişim sistemleri üzerinde gerekli güvenlik testlerini yaparlar.

-Yılda en az 1 kez olmak kaydıyla sistemler üzerinde test ve denetimler yaparlar. Bu test veya denetimleri kendileri dışında TSE (Türk Standartları Enstitüsü) tarafından belirlenen firmalar tarafından da gerçekleştirilir. Bu test ve denetimlerin hangi sınırlar, hangi kriterler çerçevesinde gerçekleştirileceği ise USOM tarafından belirlenmektedir. USOM'a göre bu kriterler:

-İç ağda yer alan bileşenler üzerindeki mevcut güvenlik zafiyetlerinin taranması,

-Dış ağda yer alan bileşenler üzerindeki mevcut güvenlik zafiyetlerinin taranması,

-Dışa açık internet uygulamaları içine olan, oluşabilecek sızmalarının tespitinin yapılması,

-Kuruma ait veri tabanlarının yapılandırılması,

-Kurumlar için özel olarak geliştirilen yazılımlar,

-Kuruma ait DNS sistemlerinin testleri,

-E-Postaların testleri,

-Sosyal mühendislik testleri,

-Sadece kurum içinden erişilebilen Web uygulamalarına sızma testleri gibi bir çok test ve denetimler söz konusudur. Bu testler sonrasında;

-Ortaya çıkan zafiyetlerin önem derecesi,

-Söz konusu zafiyetlerin oluşturduğu etkiler, zararlar,

-Zafiyetlerin bileşenleri,

-Zafiyetin açıklaması ve nasıl tespit edildiği,

-Zafiyetlere karşı alınan önemler hususlarında tespitler yapılarak Kurumsal SOME'ler bu zafiyetlerin tespit edildiği varlıklar hakkında test sonuçlarını açıklar. Bu test sonuçları ile risk değerleri hesaplanır ve "Kurumsal Siber Güvenlik Değerlendirme ve Risk Analiz Raporu" hazırlanır.

Bu raporun içeriğinde; varlık değeri, zafiyetin önemi, zafiyetin yer aldığı bileşenler, zafiyetin açılması ve tespiti, zafiyete karşı alınması gereken önlemler ve zafiyetin risk değeri belirlenir.

Tüm bu testler, tespitler ve denetimler sonrasında 6 ay içinde test adımları tekrardan gözden geçirilerek suç olabilecek iz, delil bulunması durumunda birim amiri ve kurumun hukuk müşavirliği ile görüşülecek kanunen soruşturma için Sektörel SOME ve USOM'a bildirilir.

Kurumsal SOME bunlardan sonra rapor üzerinde güncellemeler yapar. Kurum yönetimi ve bilgi işlem yönetimi düzenli olarak toplantılar yaparak gerçekleşen siber olayları, mevcut riskleri düzeltici veya engelleyici faaliyetleri gözden geçirirler.

Kurumsal SOME'ler testler ve denetimler sonrasında bulunan zafiyetler ile ilgili bilgi işlem personeli tarafından kapatılmasını koordine eder. Bu testler sonrasında zafiyetlerin giderilip giderilmediğinin tespiti açısından doğrulama testleri yapar.

Kurumsal SOMEler, siber olay öncesi, siber olay sırasında ve sonrasında olmak üzere görev ve sorumluluklara sahiptir. Bu aşamalarda kurumun diğer birimleri ile bağlantılarını düzenler. Siber olay yönetme talimatlarını belirler ve

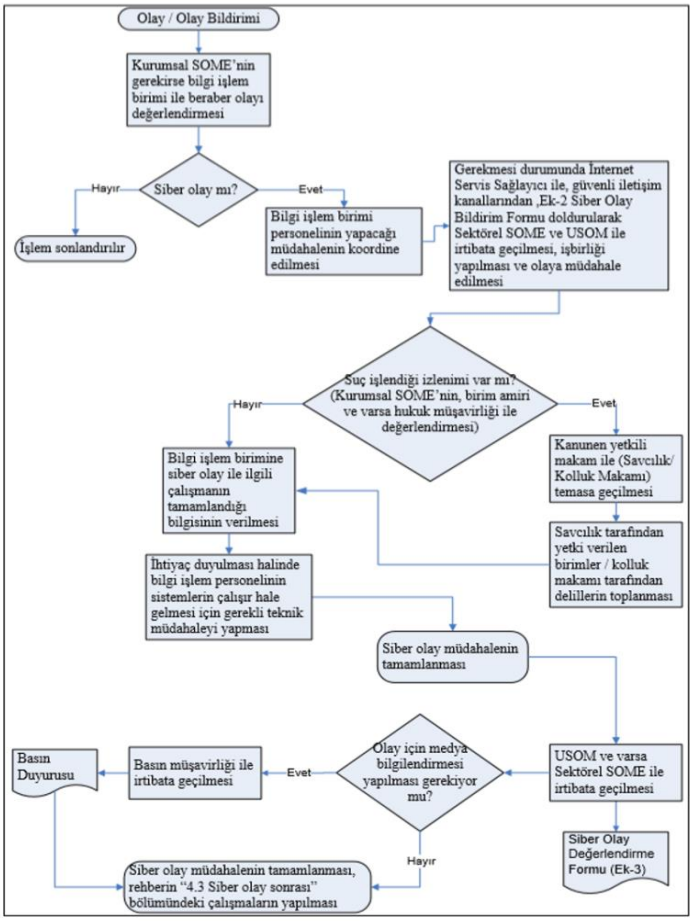
hazırlar, birimlere iletir. Bunların yanında ulusal siber güvenlik tatbikatlarına ve bu alandaki diğer tüm tatbikatlara hazırlanır ve katılım sağlarlar.

USOM'a bağlı Sektörel SOME'lerin gerçekleştireceği toplantılara hazırlanır ve katılırlar. Güvenliği sağlanması için siber saldırı tespit sistemi, güvenlik duvarının geliştirilmesi çalışmalarına destek verirler (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014: 20-22).

- **Siber Olay Esnası**

Kurumsal SOME'ler, siber saldırısı sırasında bilişim sistemlerine yetkisiz erişim sağlanmaması, sistemlere girilmemesi için gerekli tedbirleri alırlar. Siber olaya müdahale akışı içinde suç unsuruna rastlanması halinde bunu gerekli makamlara iletir. Öncelikle olay hakkında bildirim yapılması, olayın siber olay olup olmadığının tespiti yapılır. Siber olay ise bilgi işlem biriminin yapacağı müdahalenin belirlenmesi ve koordine edilmesi, müdahalenin yetersiz kalması durumunda Sektörel SOME ve USOM'a olayın bildirilir. Söz konusu saldırının suç unsuru içerip içermediğinin tespitinin yapılması, suç unsuru içermesi halinde kanunen yetkili makam ile iletişime geçilmesi ve soruşturmasının başlatılması şeklinde devam eder. Kurumsal SOMElerin siber olaylara müdahale şeması aşağıdaki şekilde gibi gerçekleşmektedir (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014: 22)

Tablo 1: Siber Olaya Müdahale Şeması



(Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014: 23)

- **Siber Olay Sonrası**

Kurumsal SOME'ler siber olay gerçekleştikten sonra ve olaya müdahale edildikten sonra; siber saldırıya neden güvenlik açığının tespiti yapılır. Söz konusu siber olay ile ilgili detaylı bilgileri USOM tarafından belirlenen kriterler doğrultusunda uygun şekilde USOM'a ve bağlı olduğu Sektörel SOME'ye gönderir ve kayıt altına alır. Söz konusu olayla ilgili olarak gerçekleştirilebilecek faaliyetlere ilişkin tespitler ve öneriler kurum yönetimine verilir. Yaşanan siber olay sonrasında verdiği zarar, miktarı, maliyetleri ve saldırının türü tespit edilir. Yaşanan bu siber olaya ilişkin tüm her şeyin detaylı olarak anlatıldığı siber olay müdahale raporu hazırlanır. Üst yönetim USOM'a ve Sektörel SOME'ye gönderilir (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014: 24).

2.4.1.3. Kurumsal SOME'ler için Gereksinim Listesi

Kurumsal SOME'lerin sorumlu olacağı bilişim varlıkları ve hizmet vereceği kurumlar net bir şekilde belirlenmelidir. Görev ve yetkileri SOME'nin temel hedeflerini içerek ve açık şekilde belirlenmelidir.

Kurumsal SOME'nin içinde kurulduğu kuruma ait organizasyon şemasındaki yeri belirlenmelidir. Amir ve personelin görev ve sorumlulukları ile kurumdaki yerleri detaylı olarak anlatılmalıdır. Tüm ekip çalışanları aynı birimde bulunmuyorsa bu durum Kurumsal SOME organizasyon şemasında belirtilmelidir.

Söz konusu bilginin somutlaştırılması ve korunması için hassas gizli veya halka açık şekilde sınıflandırılması, bu bilgilerin nasıl saklanacağı, korunacağı, nasıl aktarılacağı, nasıl erişileceği konularının açıklaması ve bunlar için özel politikalar belirlenmesi ve oluşturulması gerekmektedir.

Kurumsal SOME'ler de tutulan kayıtların sınıflandırılarak elektronik veya basılı olarak ne kadar saklanacağı, yedeklemelerin ne şekilde olacağı ve nasıl aktarılacağı, arşivlemelerin nasıl yapılacağı önceden belirlenmeli ve bunlara ilişkin politikalar belirlenmelidir.

Sayısal, basılı ve elektronik ortamdaki kayıtların sınıflarına göre nasıl ve kim tarafından yok edileceğinin belirlenmesi için ayrıca politikalar hazırlanmalıdır.

-Dağıtılabilecek bilginin türü, yöntemi, hangi bilgilerin kimler tarafından erişilebileceğine ilişkin politikalar belirlenmelidir.

-Kurumsal SOME sistemlerinin çalışanlarının ekipmanlarının günlük işlerinde nasıl kullanacakları, izin erişime karşı nasıl korunacağı, kişisel kullanılabilirlik açısından hangi sitelere erişimin olacağı, hangi sitelere erişimin engelleneceği, kişisel yazılımların indirilip indirilemeyeceği, virüs veya casus yazılımlardan nasıl korunacağı, virüs ve casus yazılımlara karşı ne sıklıkla taramalar yapılacağı sorularına cevap verecek politikalar belirlenmelidir.

-Kurumsal SOME sorumluluklarının detaylı olarak anlatıldığı, hangi durumda kolluk kuvvetlerine veya USOM ya da bağlı bulunduğu Sektörel SOME'lere haber

vereceği ve yardım isteyeceği durumların açık olarak belirlenmesine ilişkin politikalar belirlenmelidir.

-Kurumsal SOME birimlerine ait çalışanların çalışma yerlerindeki haberleşme alt yapısında bilgilerin korunmasına yönelik önlemler alınmalıdır.

-Kurumsal SOME ekibi depolanması gereken fiziksel varlıkları güvenli şekilde saklamalıdır. Bu varlıkların nasıl ve nerede saklanacağı, kimlerin erişimine açık olacağı önceden belirlenmelidir (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014: 38-41)

2.4.2. Sektörel SOME'ler

Sektörel SOME'ler kritik sektörü düzenleyici ve denetleyici kurumlar ile bu kurumlar kurulana kadar ilgili bakanlık hangisi ise o bakanlıklarda kurulmaktadır. Sektörel SOME'lerin genel olarak hizmet alanları kritik alt yapı sektörleridir. Kendisine bağlı Kurumsal SOME'lerin USOM ile olan iletişim faaliyetlerini düzenleyerek, sektör içinde kullanılacak iletişim yöntemlerini hakkındaki usul ve esasları belirler (Sektörel SOME Kurulum ve Yönetim Rehberi, 2014: 13)

Ülkemiz için geçerli olan temek kritik alt yapılar için ayrı ayrı Sektörel SOME'ler kurulmuştur. Sektörel SOME'ler sorumluluk alanlarındaki kritik alt yapı sektörlerindeki siber güvenliğin, siber güvenlik koordinasyonundan, düzenlemelerden ve denetlenmesinden sorumludur. Bunları gerçekleştirirken ayrı zamanda USOM ve Kurumsal SOME'ler ile koordinasyon ve iletişim halindedir (Sektörel SOME Kurulum ve Yönetim Rehberi, 2014: 15)

Sektörel SOME'ler bulundukları sektör içindeki siber güvenlik politikalarını ihtiyaçlar halinde USOM ile birlikte iş birliği yaparak bu belirlenen politikaların uygulanıp uygulanmayacağını denetler.

Siber Güvenlik Kurulu'nun aldığı kararların sektör açısından karşılığını Sektörel SOME'ler yerine getirir. Sorumluluk içindeki kurumlara siber alanda bilgilendirme yapar, siber sorunlar açısından çözümleri bulmak ve sağlamak adına hizmet verir. Olası gerçekleşebilecek siber saldırı uyarısı ve mevcut olan güvenlik açıkları durumunda kurumu bilgilendirmektedir (Sektörel SOME Kurulum ve Yönetim Rehberi, 2014: 15)

2.4.2.1. Sektörel SOME'lerin Kurulum Aşamaları

Sektörel SOME'lerin ilgili kurumların içinde kurulurken aynı Kurumsal SOME'ler gibi çeşitli kurulum aşamaları söz konusudur. Yine Sektörel SOME'ler de kurum içerisindeki yeri ve kapasite planlaması, sonrasında kurum içi ve kurum dışı paydaşlarla iletişim aşamalarından oluşturmaktadır.

- **Kurum İçerisindeki Yeri ve Kapasite Planlaması**

Sektörel SOME'ler kurulurken kurum içinde düzenleme veya denetleme fonksiyonlarını doğrudan yapan birimlerim altında kurulmalıdır. Kurum içindeki denetleme ve düzenleme fonksiyonları birden fazla ise bu birimlerde çalışan temsilcilerin oluşturduğu şekilde kurulur. SOME'nin amiri en az lisans mezunu olmalı sektör tecrübesine sahip, siber alanda bilgili ve tecrübeli olmalıdır. Kurum içindeki kurumsal SOME'ler ile koordinasyon halinde olmalıdır (Sektörel SOME Kurulum ve Yönetim Rehberi, 2014: 15)

Sektörel SOME'lerin uyum, düzenleme veya denetleme sektörel siber güvenlik bilinçlendirme ve sektör içi olay yönetim ve koordinasyon sağlama gibi fonksiyonları vardır. Bu fonksiyonlar dışında ayrı bir uzmanlık gerektiren her fonksiyon için en az bir kişilik uzman personel istihdamı yapılmalıdır (Sektörel SOME Kurulum ve Yönetim Rehberi, 2014: 15)

- **Kurum İçi Paydaşlarla İletişim**

Sektör içindeki siber güvenliği yönetirken varsa hukuk ve basın, halkla ilişkiler müşavirlikleri ile birlikte çalışır. İlgili sektördeki siber güvenlik çalışmaları incelenir, düzenlenir ve gerekli mevzuatlar hazırlanır. Gerekli uyarılar ve bilgilendirmeler yapılır. Sektör ile alakalı siber olaylarda koordinasyon görevini üstlenir, gerekli kurumlar ile ihtiyaç halinde iletişime geçer. Yıllık olarak "Sektörel Siber Güvenlik Faaliyet Raporu" hazırlanır ve bağlı bulunduğu kurum veya kuruluşun üst yönetim merciine sunar (Sektörel SOME Kurulum ve Yönetim Rehberi, 2014: 16)

2.4.2.2. Sektörel SOME'lerin Görev ve Sorumlulukları

Sektörel SOME'lerin kurum içerisinde belli başlı görev ve sorumlulukları vardır. Bu görev ve sorumluluklar, siber olay öncesinde, siber olay sırasında ve siber olay sırasında olmak üzere 3 bölüme ayrılmaktadır (Sektörel SOME Kurulum ve Yönetim Rehberi, 2014: 19)

- **Siber Olay Öncesi**

Sektörel SOMEler firmaların kurum ve kuruluşların temsilcilerinin ve USOM'un içinde bulunduğu mevzuat ve teknik çalışmalar için oluşturmaktadır. Çalışma gruplarıyla birlikte sektör içi siber güvenlik mevzuatlarını belirler. Sektörde bulunan kritik bilgi sistemlerinin belirlenmesi için kriterler belirlenir.

Sektörel çalışma grubu ile beraber sektör içi siber güvenlik mevzuatını hazırlar ya da hazırlanmış mevzuatı gözden geçirir. Sektörel çalışma grubu ile birlikte sektör içindeki asgari siber güvenlik kriterlerini belirler.

Sektörel çalışma grubuyla beraber bilgi güvenliği ve siber güvenliğe ilişkin çerçeve sözleşme hükümleri üretir ve yayınlar.

Kurumsal SOME'lerden yapmasını istediği risk analizlerinin metodunu, kapsamını, hazırlama periyodunu ve raporun formatını belirler.

Sektörel siber olay müdahale prosedürü oluşturur ve tatbikat yaparak test eder.

USOM tarafından yayımlanan duyuru ve bildirilerin sektöre aktarılmasını sağlar.

Sektörel SOME'ler 7/24 erişilebilir olan iletişim bilgilerini birlikte çalıştıkları Kurumsal SOME'lere ve USOM'a bildirirler ve aynı bilgileri alırlar.

Sorumluluk alanındaki faaliyet gösteren kurum ve kuruluşlara faydalı siber güvenlik pratikleri hakkında bilgi sağlama hizmeti verir.

Sektördeki kurumlara siber güvenlikle ilgili ve özellikle kendi sektörüne ilişkin bilgiler içeren bülten gönderir.

Sorumluluk alanını oluşturan kritik sektörü kapsayacak şekilde genel siber saldırı uyarısı ve güvenlik açığı duyurusunu yayınlar.

USOM'dan aldığı sektöre özel siber güvenlik önlemlerini kurumsal SOME'lere aktarır.

Siber güvenlik alanında eğitim ve konferanslar düzenler.

Kurumsal SOME'lere verilecek eğitimler ile ilgili ihtiyaçları tespit eder ve bu eğitimleri koordine eder.

Sektöre özel siber tehditlerin tespiti için sektörel çalışma grubu ile koordine içinde sektöre özgü bilgi sistemlerini kapsayan bal küpü sistemlerinin kurumsal SOME'lere kurulmasını tavsiye eder.

Kurumsal SOME'lerin kendi bünyeleri içinde gerçekleştirecekleri sızma testleri için kapsam, rapor formatı ve minimum ihtiyaçların belirlenmesi hususunda Kurumsal SOME ve USOM ile koordinasyon sağlar.

Kurumsal SOME'ler ile birlikte sektöre özgü bilgi sistemlerinin üreticilerini bir araya getirerek sistemlerde yapılabilecek iyileştirmelerin ve alınabilecek önlemler hususunda çalışmalar yapılmasını koordine eder (Sektörel SOME Kurulum ve Yönetim Rehberi, 2014: 19-22).

- **Siber Olay Sırasında**

Sektörel SOME'ler siber olay sırasında kurumsal SOME'ler de gözlemci bulundurabilir, imkanlar doğrultusunda gerekli desteği kendisine verir. Kendisine bağlı olan kurumsal some'ler ve USOM'a siber olaylarla ilgili bilgilendirme mesajları gönderir. Siber olaya karşı müdahale sırasında suç işlendiği izlenimi varsa eğer vakit geçirilmeden kurumsal somelerin yetkili makamlarına bildirmesi ve siber olay raporunun USOM'a iletilmesini sağlar.

Gerçekleşen siber olaylarda teknik arızalar, doğal afetlerle ve kullanıcı hataları ile ortaya çıkan durumlar kolluk kuvvetlerine bildirilmez. Kurumsal bilgi sistemlerine içeriden veya dışarıdan yapılan saldırılar Kurumsal SOME'ler ve kolluk kuvvetlerinin iş birliği ile çözülmesi gerekir.

Kurumsal bilgi sitemleri kullanılarak işlenen sahtekarlık, fikri mülkiyet hırsızlığı vb. suçların delillerin bilgisayar ortamında bulunduğu işgal, hırsızlık, fiziksel saldırı eylemlerinde görevin büyük ağırlığı kolluk kuvvetine düşer (Sektörel SOME Kurulum ve Yönetim Rehberi, 2014: 22-23)

- **Siber Olay Sonrası**

Sektörel SOME'ler sektörde yer alan bir kurumda bir siber olay sonrasında ve olaya müdahaleden sonra siber olay bildirim formunu kurumsallardan doldurmasını ve USOM'a iletmesini sağlar. Gerçekleşen siber saldırıyı kayıt altına alır.

Kurumsal SOME'lerin yaşadığı siber olay tecrübelerinden sonra yapılacak olan düzenlemelere esas teşkil edecek bilgileri işler ve kayıt altına alır.

Siber olay sonrasındaki tecrübelerini rekabet şartları ve ticari sınırlar çerçevesinde sektörlerdeki diğer kurumsal SOME'ler ile paylaşır.

Gerekli hallerde kurumsal SOME'ler ile iletişime geçerek koordine kurarak medya ile iletişime geçerek son durum bildirisi yapar.

Kritik kamu hizmetleri; vatandaşların gündelik hayatında sürekli olarak kullandığı nüfus, tapu, sağlık, gıda, güvenlik ve adli işlemlerin yapıldığı hizmetlerin tamamıdır. Bu hizmetler için bakanların hepsinde Sektörel SOME'ler kurulmalıdır (Sektörel SOME Kurulum ve Yönetim Rehberi, 2014: 23)

- **Siber Olaylara Müdahale Kabiliyeti**

BTK'nın 2009 yılında yayınladığı rapor ile ülkenin siber güvenlik alanındaki faaliyetlerin, mevzuatların geliştirilmesi belirtilmiştir. Bu rapor ile gerçekleşen siber saldırıların nasıl inceleneceği, saldırılar hakkında delillerin nasıl toplanması gerektiği, siber alanda yapılan çalışmaların, yetkin kişilerin yetersizliğinden bahsedilmiştir (Ünver, 2009: 28). Bu rapor sonrasında siber güvenlik kabiliyetlerini artırma, siber güvenliği artırma adına çalışmalar yapılmıştır.

Bu çalışmalara örnek olarak Ulusal Güvenlik Siyaset Belgesi, Emniyet Müdürlüklerinde bulunan Bilişim Suçlarıyla Mücadele Daire Başkanlıklarının, Siber Suçlarla Mücadele Daire Başkanlığı'na çevrilmesi gösterilebilir.

Haziran 2012'den sonra Siber Güvenlik Çalıştayı'ndan sonra Bilgi Güvenliği Derneği tavsiye belgesi yayımlamıştır (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2012). Bu tavsiye belgesi ile;

-Ulusal Siber Güvenlik Stratejik Belgesinin yayınlanması,

-Ulusal Siber Güvenlik Kurulu oluşturulması,

-Siber güvenlik alanında farkındalığın artırılması,

-Siber güvenlik kültürünün yaygınlaştırılması,

-Siber alanda uluslararası iş birliğinin güçlendirilmesi,

-Ulusal siber güvenlik Ar-ge çalışmalarının yapılması ve milli teknoloji yapımının özendirilmesi,

-Üniversitelerde siber güvenlik alanında çalışmalar yapılması,

-Siber güvenlik uzmanlarının yetiştirilmesi,

-Ulusal olarak tüm kurumlarda siber güvenlik kabiliyetlerinin sağlanması,

-Siber güvenlik alanında yasal mevzuatların düzenlenmesi,

-Kritik alt yapılarda, kamu ve özel kurumlar arasında SOME'lerin kurulması ve bu SOME'lerin koordinesinin sağlanması ve eğitimler verilmesi,

-Ulusal olarak siber güvenlik alanında ulusal bir donanım, işletim sistemi, arama motoru ve internet sağlayıcılarının geliştirilmesi gerektiği belirtilmiştir.

Bu belgeye göre kritik alt yapıların zarar görmesi, yok olması, toplumsal düzenin ve kamu hizmetlerinin devamlılığı sağlanması, güçlük oluşturacak; işlevlerini tamamen veya kısmen yerine getiremediğinde vatandaşın sağlığına, emniyetine, güvenliğine ve ekonomik faaliyetler veya hükümetin etkin ve verimli işleyişine olumsuz etki edecek yapılar olarak tanımlanmıştır.

2.5. Siber Güvenlik Kurulu

20 Ekim 2012'de Bakanlar Kurulu tarafından kurulmuştur. Siber Güvenlik Kurulu ile siber güvenlik alanında alınacak önlemleri belirlemek, hazırlanacak olan

planı, programı, rapor, usul ve esasları belirlemek, uygulamak ve koordine etmekle görevlidir.

Siber Güvenlik Kurulu; Dışişleri, İçişleri, Milli Savunma, Kamu Düzeni ve Güvenliği Müsteşarlığı, Genelkurmay Başkanlığı, Muhabere Elektronik ve Bilgi Sistemi Başkanı, BTK Başkanı, TUBİTAK Başkanı, Mali Suçları Araştırma Kurulu Başkanı, TİB Başkanı ve UDH tarafından belirlenen bakanlık ve üst düzey yöneticilerden oluşmaktadır.

Siber Güvenlik Kurulu'nun bir takım görevleri vardır;

-Ulusal siber güvenliğin sağlanması için politikalar, strateji ve eylem planı hazırlamak,

-Kamu kurum ve kuruluşlarına ait bilgi ve belgelerin güvenliğini sağlamak,

-Kamu kurum ve kuruluşlarında siber güvenlik için teknik alt yapının oluşturulması, uygun politikaların takibi ve doğruluklarının kontrolünün yapılması,

-Ulusal verilerin, veri tabanlarının güvenliğinin sağlanması, ulusal kritik aş yapıların belirlenerek oluşabilecek siber saldırıların, tehditlerin engellenmesi, bunları korumaya yönelik sistemlerin denetlenmesi, güçlendirilmesi ve iyileştirilmesine yönelik çalışmalar yapılması,

-Ulusal siber güvenliğin sağlanmasında milli siber güvenlik unsurlarının geliştirilmesi, üretilmesi, Ar-ge çalışmalarının yapılması,

-Ulusal siber güvenliğin sağlanması adına bu alanda uzman personel eğitimi, gelişimi için çalışmalar yapılması,

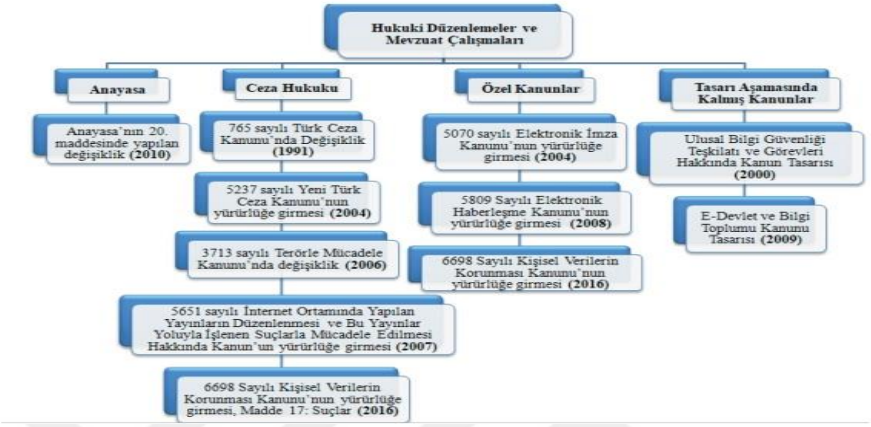
-Siber güvenlik alanında diğer ülkeler ile uluslararası antlaşmalar yapmak görevleri arasındadır.

Siber Güvenlik Kurulu, 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planını yayımlamıştır (https://www.btk.gov.tr, 2021).

2.6. Türkiye'de Siber Güvenlik Politikalarının Yasal Gelişimi Süreci

Siber güvenlik alanında hukuki düzenlemeler ve mevzuat çalışmaları tablodaki gibi gerçekleşmektedir:

Tablo 2: Türkiye'de Siber Güvenlik Politikalarının Gelişimi



(Karasoy ve Babaoğlu, 2021: 133)

2.6.1. Mülgan 765

Türkiye'nin ağ teknolojilerinin yaygınlaşmasına sivilleşmesine ilk tepkisi ceza hukuku anlamında olmuştur ve kamu düzeninin asayişinin bozulmaması adına gerçekleştirilebilecek siber saldırılara karşı cezalar belirtilmiştir.

Bu tepki Mülga 765 sayılı TCK'ya 1991'de Bilişim suçlarının dahil edilmesi ile gösterilmiştir. Bu kanun ile özel hayatın gizliliği, mülkiyet hakkı, sırrın masumiyeti, haberleşme hürriyeti, ekonomik faaliyetleri dikkate alınmıştır. (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2012: 11-12) Kanun bu haklar ile ceza hukuku kapsamında kanun koyucunun faaliyetleri o günün dışında günümüzü kapsayan tehditleri, olaylara karşı tedbirleri aldığı söylenebilir.

2.6.2. Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun

Milli Savunma Bakanlığının koordinatörlüğünde Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun'a yer verilmiştir **(**Bıçakcı, Ergün ve Çelikpala, 2016: 32). Bu tasarıda ulusal olarak siber güvenliğin sağlanması hedeflenmiş Ulusal Bilgi Güvenliği Kurumu Başkanlığı'nın oluşturulması hedeflenmiştir. Kanun tasarı olarak kalmış yürürlüğe girmemiştir.

2.6.3. 5070 Sayılı Elektronik İmza

2004 yılında TBMM'de kabul edilerek Ocak ayında resmi gazetede yayımlanmıştır. Bu kanun ile; elektronik imzanın hukuki ve teknik yönleri ile kullanıma ilişkin esasları düzenlemek amaçlanmıştır (https://www.mevzuat.gov.tr, 2022)

2.6.4. 5237 sayılı Yeni TCK

2004 yılında TBMM tarafında kabul edilerek aynı yıl yürürlüğe girmiştir. Bu anayasa ile temel hak ve hürriyetleri korumasını amaçlayan, kişi güvenliğinin sağlanması hedeflenir. Anayasa; hak ve hürriyetleri kararların siber alanda güvenliğini korumayı hedefler. Bilişim suçları kanunun 243. ve 246. Maddelerinde bilişim suçunu oluşturan fiiller ve cezaları belirtmiştir.

2.6.5. 3713 Sayılı Terörle Mücadele Kanunu

TCK'da 2006 yılında yapılan değişiklik ile "Terör amacı ile işlenen suçlar" kapsamına alınmıştır. 243. ve 246. Maddede gerçekleştirilen suçlar terör örgütünün faaliyeti ile gerçekleştirilmiş ise terör suçu sayılmıştır. Bu kanun ile Türkiye'de siber uzayın ilk kez terörizm sahası olabileceği kabul edilmiştir.

2.6.6. 5651 Sayılı Kanun

Bu kanunun internet ortamında işlenebilecek suçları düzenlemeyi hedefleyerek Mayıs 2007 yılında onaylayarak yürürlüğe girmiştir (https://www.mevzuat.gov.tr, 2022).

Kanun incelendiğinde; gerçek ya da tüzel kişilerin kişisel ya da ekonomik haklarını ihlal edecek içeriklerin engellenmesi, hakim kararına bağlanması öngörülmüştür. Kişilerin özel hayatın gizliliğini mülkiyet hakkı ve haberleşme hürriyetine yönelik olabilecek tehditlerin önlenmesi, saldırıların etkisinin giderilmesi amaçlanmıştır.

2.6.7. 5809 Sayılı Kanun

2008 yılında TBMM tarafından kabul edilmiştir. Kasım 2008'de resmi gazetede yayımlanmıştır. Bu kanun ile elektronik haberleşme sektörüne düzenleme ve denetleme yoluna gidilmesi, tüketici haklarının gözetilmesi, ülke genelinde tüm

faaliyetlerin artırılması ve kaynakların verimli kullanılması hedeflenmiştir. Haberleşme alt yapılarında yerli, yeni teknolojilerin ve yatırımların teşvik edilmesi amaçlanmıştır.

2.6.8. E-Devlet ve Bilgi Toplumu Kanun Tasarısı

2009 yılında meclise sunulmuştur. Bu tasarı ile e-Devlet üzerinden vatandaşlara sunulacak hizmetler belirlenmiştir. Bu yapılanma ile sağlıklı ve vatandaşın lehine çözümler sunacak, uygulanacak olan politikaların kurumsal olarak hazırlanası hedeflenmiştir (https://www.memurlar.net, 2022). Bu tasarıda daha çok ekonomik hükümlerin yer alması, hizmetlerin yürütüleceği bilişim sistemlerinin alt yapılarının korunmalarına yönelik ifadelerin yer alması, bu alt yapıların korunması görevinin hizmeti veren kuruma verilmesi hedeflenmiştir ancak Bilgi Toplumu Ajansı'nın hem denetim hem icraa merci olması amacın gerçekleşmesi için eksiklik olarak görüldüğünden tasarı olarak kalmıştır.

2.7. Siber Güvenlik Eylem Planları

Türkiye'de 1990'lı yılların başında siber uzay anlamındaki ilk tepkisini ceza hukuku alanında, 1990'lı yılların sonlarına doğru ise ulusal alanda tehlike olarak kabul edilmiştir (Afyonluoğlu, 2020: 49). Bu sebeple birçok eylem planı hazırlanmıştır.

Tablo 3: Türkiye'de Siber Güvenlik Eylem Planları

(Karasoy ve Babaoğlu, 2021: 138)

2.7.1. Türkiye Ulusal Enformasyon Altyapısı Ana Planı (TUENA)

Temelleri 1995 yılında atılan bu eylem planı Ulaştırma Bakanlığı'nın koordinatörlüğünde ve TUBİTAK destekleriyle hazırlanmıştır (http://www.bilgitoplumu.gov.tr, 2022). Kamu kurumlarının yanında; özel kuruluşlar, dernekler ve akademik çevre hazırlanması için katılmıştır. Sadece internet değil tüm bilişim sistemleri kontrol edilmiştir. Başka ülkelerin eylem planları ile karşılaştırmalar yapılmıştır. Bu karşılaştırmalar sonrasında yaparak eksiklikler belirlenmiş, fırsatlar araştırılarak yeni öneriler ve yeni çalışmalar yapılmıştır.

Bu çalışma ile siber güvenlik alanında tehditlerin ulusal nitelikte olduğu, bu tehditlere karşı savunma mekanizmalarının geliştirilmesinin eyleme geçirilmesi amaçlanmıştır.

2.7.2. E-Türkiye Girişimi Eylem Planı

Günümüzdeki eylem planlarının temelini oluşturan bu eylem planı Başbakanlık koordinatörlüğünde 2002 yılında hazırlanmıştır ve ağustos ayında yayımlanmıştır (http://www.bilgitoplumu.gov.tr, 2022) Bu çalışma kamu alanında ve sivil alanda "e-dönüşüm" gerçekleştirilmesi hedeflenmiştir. Bu hedef doğrultusunda teknik ve hukuki alt yapılar belirlenmiş ve eğitim, ulaşım, sağlık, ticaret, çevre vb. alanlarda e-dönüşüm adına çalışmalar yapılmıştır.

2.7.3. 2003-2004 ve 2005 Kısa Dönem Eylem Planları

İnternetin yaygınlaşmasına ve teknolojinin gelişimi ile Türkiye'de e-dönüşüm hız kazanmıştır. Bu hız ile birlikte siber alanda güvenliğin sağlanması adına 2003-2004 kısa dönem eylem planı (KDEP), Başbakanlık Genelgesi ile 2003 Aralık'ta Resmi Gazetede yayımlanmıştır (Afyonluoğlu, 2020: 52).

Bu eylem planı ile Teknik Altyapı ve Bilgi Güvenliği ekseni adı altında "ağ güvenliğinin test edilmesi ve sağlanmasına ilişkin pilot uygulamaların geliştirilmesi" isimli eylem planı için TUBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEAKE) görev verilmiştir (http://www.bilgitoplumu.gov.tr, 2022)

2005 yılında tamamlanan eylem planında hedeflenen politikaların %47'si tamamlanmıştır. 2005'de hazırlanan KEDP ile kritik ağlar üzerinde işlem yaptığı

kabul edilen 7 farklı kuruluş hakkında güvenlik risk raporu hazırlanmıştır (Afyonluoğlu, 2020: 56). Hazırlanan raporda her kuruluşun ayrı ayrı değerlendirilmesi yapılmıştır. Bu değerlendirmeler sonucunda kuruluşların siber güvenlik alanındaki güvenlik seviyelerin farklı farklı olduğu tespit edilmiştir. Tam anlamıyla oturmuş kabul edilen bir siber güvenlik anlayışının olmadığı anlaşılmıştır.

2.7.4. 2006-2010 Bilgi Toplumu Stratejisi Eylem Planı

Devlet Planlama Teşkilatı öncülüğünde 2006-2010 yılları arasını kapsayan Bilgi Toplumu Stratejisi Eylem Planı hazırlanmış ve 28 Temmuz 2006 yılında Resmi Gazetede yayımlanmıştır (Ünver, Canbay ve Özkan, 2011: 48). Önceki eylem planlarına nazaran daha kapsamlı olarak hazırlanmıştır. Bu kapsamın yanında belirlenen politikaların maliyetlerini ve ayrıntılı olarak belirlenmiştir. Siber güveliği genel bir sorun olarak ele alan bir eylem planıdır. Bu eylem planı ile hedeflenen politikalara "4. Kamu Yönetiminin Modernizasyonu" başlığı altında 87. ve 88. numaralı eylem planları içinde yer vermiştir (Karasoy ve Babaoğlu, 2021: 141)

87 numaralı eylem planı ile ülkenin güvenliğinin sağlanması için, devletin bilgi güvenliğinin sağlanması, sistemlerin geliştirilmesi, hukuki alt yapıların oluşturulması, kişisel verilerin korunması hakkında kanun tasarısının hazırlanması hedeflenmiştir.

88 numaralı eylem planı ile siber alandaki tehditler karşısında her zaman saldırı olacağı kabul edilerek hazırda bulunulması gerektiği, tehditlere karşı savunma halinde olunması hedeflenmiştir.

87-88 numaralı eylem planı ile kamu kurumları için gerekli güvenlik seviyelerinin artırılması, kurumların kullandığı sistemler üzerinde güvenlik seviyelerinin tespiti, mevcut eksikliklerin giderilmesi hedeflenmiş, hukuki alt yapı açısından 2010 yılı Anayasa değişikliği karşımıza çıkmaktadır. Bunların dışında siber tehditleri kontrol etmek, koordineyi sağlamak için Türkiye Bilgisayar Olaylarına Acil Müdahale Ekibi (TR-BOME) koordinatörlüğü kurulmuş olup, siber güvenlik tatbikatları gerçekleştirilmiş ve kriz planları yapılmıştır. BİLGEM'e bağlı olarak Siber Güvenlik Enstitüsü 2012 yılında kurulmuştur (Karasoy ve Babaoğlu, 2021: 144)

2.7.5. 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı

Türkiye'de bilgi ve iletişim teknolojilerinin kullanımı ve gelişimi her geçen hızla artmaktadır. Bu teknolojiler ise hayatımızın neredeyse her alanında mevcuttur ve aktif olarak yer almaktadır. Tüm kamu kurum ve kuruluşlarında, özel sektörlerde ulaşım, finansal, sağlık, su kaynakları gibi kritik alt yapı sektörlerinde faaliyet gösteren kurum ve kuruluşlarda bilgi ve iletişim sistemleri yoğun olarak kullanılmaktadır (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı: 1)

Gelişen teknoloji ile bilgi ve iletişim sistemlerinin kullanımı da paralel olarak artmaktadır. Toplumun yaşam standartlarının yükselmesi, bilgi ve iletişim sistemlerinin daha fazla kullanılması bu sistemlerin güvenliklerinin ulusal düzeyde sağlanması ihtiyacını ortaya çıkarmıştır. Bu sistemlerde bulunan güvenlik açıkları, hizmetlerin devre dışı kalmasına, kötü niyetli kişiler tarafından kötüye kullanıma, can ve mal kaybına, büyük oranda ekonomik olarak zararın oluşmasına ve mevcut düzenin bozulmasına ve ulusal güvenliğin tehlikeye girmesine sebep olacaktır.

2013-2014 yılı eylem planı siber alanda gerçekleştirilmesi beklenen işleri belirlemiş olup diğer yıllar içinde sürekli ve düzenli olarak yapılması gereken faaliyetleri de içermektedir.

Bu eylem planı içinde tanımlamalara, planın amacına, kapsamına, güncellemelere, çeşitli risklere, planın ilkelerine, stratejik olarak siber güvenlik eylemlerine ve 2013-2014 yılları kapsamında ulusal siber güvenlik eylem planı bulunmaktadır.

- **2013-2014 Eylem Planı için Tanımlar**

Bilişim sistemleri: Bilgi ve teknoloji aracılığıyla sağlanan hizmetlerin, işlemlerin ve verilen sunulmasında kullanılan sistemleri,

Siber ortam: Tüm dünya üzerinde geçerli olan bilişim sistemleri ve bunların arasındaki bağlantıları sağlayan ağlardan oluşan ortam,

Kamu bilişim sistemleri: Türkiye Cumhuriyeti kapsamında bulunan kamu kurum ve kuruşlarının kullandığı bilişim sistemleri,

Gerçek ve tüzel kişilere ait bilişim sistemleri; Türkiye Cumhuriyeti kapsamında kanunlara tabi gerçek veya tüzel kişilerin kullandığı bilişim sistemleri,

Ulusal siber ortam: Kamu bilişim sistemleri ve gerçek veya tüzel kişilerin kullandığı bilişim sistemlerinin tamamı,

Gizlilik: Bilişim sistemlerinde saklanan verilere sadece yetkili kişilerin ya da sistemlerin erişebilmesi, dışarıdan herhangi bir kişinin ya da sistemin bu verilere erişememesi,

Bütünlük: Bilişim sistemlerindeki verilerin sadece yetkili kişiler veya sistemler tarafından değiştirilebilmesi,

Erişilebilirlik: Yetkili kişilerin veya sistemlerin ihtiyaç duyulduğu zaman bilişim sistemlerine erişebilmesi,

Kritik alt yapılar: Bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğu can kaybına, büyük kapsamlı ekonomik zarara, ulusal güvenlik açıklarına ve kamu düzenin bozulmasına sebep olacak bilişim sistemlerini barındıran alt yapıları,

Siber güvenlik olayı: Bilişim sistemleri veya bu sistemler tarafından korunan verilerin gizlilik, güvenlik ve erişilebilirliğin ihlal edilmesi,

Siber güvenlik: Siber ortamın içerisindeki bilişim sistemlerinin olası siber saldırılar karşısında korunması, sistemdeki tüm verilerin gizlilik, bütünlük ve erişilebilirliğin güvence altına alınması, olası siber saldırıların ve siber güvenlik açıklarının tespiti ve bu tespitlere karşı koruma mekanizmalarının hazırlanması, saldırılara karşı savunma ve karşı saldırıların yapılması,

Ulusal siber güvenlik: Ulusal siber alanda bilgi ve iletişim teknolojileri ile sağlanan tüm hizmet, işlem ve verilerin korunması için yer alan sistemleri ifade eder. (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı: 3)

- **2013-2014 Eylem Planının Amacı**

Kamu kurum ve kuruluşları tarafından bilgi teknolojileri ve sistemleri tarafından sağlanan hizmet, işlem ve verilerin bulunduğu sistemlerin korunması,

Kamu kurum ve kuruluşlarının, özel sektörler tarafından işletilen kritik alt yapı olarak adlandırılan bilişim sistemlerinin güvenliğinin sağlanması,

Siber güvenlik olaylarının, saldırıların en düşük düzeyde kalması, oluşabilecek zararların en düşük düzeyde olması, zarara uğrayan sistemlerin en kısa sürede düzeltilmesi ve eskisi gibi çalışmasını sağlaması amaçlanmıştır. Mevcut saldırıların araştırılarak soruşturma veya kovuşturma işlemlerinin de takibinin yapılması hedeflenmiştir (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı: 4).

- **2013-2014 Eylem Planının Kapsamı**

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 eylem planı kapsamında bilişim sistemleri ve kamu ya da özel sektör tarafından işletilen kritik alt yapıların tamamının güvenliğini kapsar.

- **2013-2014 Eylem Planının Güncellenmesi**

Eylem planı, sürekli olarak gelişen teknoloji karşısında, değişen şartlar ve yeni ihtiyaçlar doğması da hesaplanarak kamu ve özel sektörden gelecek olan talepler doğrultusunda güncellemelere açık olarak hazırlanmıştır. Yılda en az bir kez olmak üzere ulusal olarak mevcut şartlar doğrultusunda güncellenmesi planlanarak hazırlanmıştır.

- **Siber Güvenlik Riskleri**

Eylem planının doğru ve düzgün şekilde hazırlanabilmesi için ülke sınırları içindeki mevcut koşulların değerlendirilerek, oluşabilecek siber saldırılar karşısında doğru politikaların belirlenebilmesi için öncelikle siber güvenlik risklerinin belirlenmesi gerekmektedir. Bu riskler;

-Siber ortamda yapılan saldırıların kim tarafından yapıldığının tespiti oldukça zordur. Bu saldırıların anonim olması ve inkâr edilebilir olması saldırı için gerekli araç ve bilginin çok ucuza mal edilebilmesi, dünyanın herhangi bir yerinde herhangi birisinin bu saldırıları gerçekleştirebilmesinin mümkün olması,

-Siber alanın daima saldırıya açık şekilde olması, siber alanda mevcut olan verilerin korumasız olması, olası tehditler durumunda sistemlerin birbirlerine zarar verebilmesi,

-Günümüz çağında ulusal alanda hizmet veren kamu kurum veya kuruluşlarının ve özel sektörlerin verdiği hizmetlerin teknolojinin gelişmesi ile bilişim sistemleri tarafından sağlanması,

-Kritik alt yapıların büyük bir çoğunluğunun internet alt yapısının olması verilerin sistemler üzerinde saklanması,

-Siber güvenlik, siber saldırı kavramlarının ulusal düzeyde bilinmemesi, vatandaşın ulusal düzeyde siber güvenlik alanında bilgisinin yetersiz olması,

-Siber güvenlik alanında kurumlar arasındaki koordinasyon eksikliği,

-Siber saldırılara maruz kalan kurumların, itibarlarının ve saygınlıklarının zedelenmemesi adına gelen saldırıları gizlemesi,

-Siber güvenlik saldırılarının araştırılması hususunda ulusal ve uluslararası mevzuat eksikliklerinin bulunması,

-Kritik alt hizmetlerinin ve servislerinin siber saldırıların dışında kendi hatalarından, kullanıcı hatalarından veya doğal afetlerden olumsuz etkilenerek bu tarz olaylara karşı tedbir açısından yeterli bulunmaması,

-Kurumlarda siber güvenlik alanında bilgi güvenliğini sağlaması açısından alt yapılarının yetersiz olması,

-Siber güvenlik alanında kurumsal ve kişisel olarak yeterli düzeyde bilgi sahibi olunmamış olması,

-Siber güvenlik alanında kurumların ve kurum yöneticilerinin bilgi sahibi olmaması, siber güvenlik kavramına karşı bir benimseme olmaması,

-Siber alanda kurumların yapılanmalarının yetersiz ve etkisiz kalması, siber güvenlikten sorumlu birimlerin yalnızca bilgi işlem birimlerinin sorumluluğunda sanılması,

-Bilgi işlem çalışanlarının siber güvenlik alanında yeterli düzeyde bilgi sahibi ve siber güvenlik alanında tecrübeye sahip olmamaları,

-Siber saldırılar sonrasında, saldırılar hakkında soruşturma yapılması için personel sayısının yeterli olmaması,

-Siber güvenlik alanında kurumlar içindeki denetimlerin gerçekleştirilmesi için ekibin ve sistemin olmaması, denetimlerin yeterli düzeyde yapılmaması,

-Siber güvenliği sağlayacak teknolojilerin, yazılımların ve donanımların yerli üretim olmamasıdır (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı: 4).

- **Siber Güvenlik İlkeleri**

Ulusal alanda siber güvenlik politikaları belirlenirken bir takım ilkeler etrafında hazırlanması gerekmektedir. Bu ilkeler;

-Siber güvenlik için risk alarak etkin ve sürekli devam eden geliştirmeler ve iyileştirmeye yönelik çalışılmalıdır.

-Siber güvenlik sağlanırken ekonomik, hukuki, idari, politik ve sosyal alanların güçlü ve zayıf yönlerinin, olası tehditlerin tamamının bütün olarak takip edilmesi gerekmektedir.

-Olası saldırılar karşısında oluşan zararın en aza indirgenmesi için çalışılmalı, saldırıların, teknik güvenlik açılarının tespit edilmesi gerekmektedir.

-Siber güvenlik alanında bireylerin, özel ve kamu kurumlarının, devletlerin, toplumların siber alanda sorumluluklarını yerine getirmeleri gerekmektedir.

-Hükümetlerin kritik alt yapılarının güvenliğinin sağlanması adına yeterli düzeyde önlem alınmalıdır.

-Siber alanda genel olarak güvenliğin sağlanması için sadece kamu kurumları, özel sektörler değil uluslararası işbirliği de bulunmalıdır.

-Uluslararası işbirliği sağlanırken diplomatik, teknik ve kolluk kanalları sürekli etkin kullanılmalıdır.

-Siber alanda geliştirilen plan, politikalar hazırlanırken uluslararası antlaşmalar ve düzenlemeler dikkate alınmalıdır.

-Siber güvenlik sağlanırken hukukun üstünlüğü ve insanın temel hak ve hürriyetlerinin korunması esas alınmalıdır.

-Siber alanda şeffaflık, hesap verebilirlik benimsenmelidir.

-Denetleyici ve düzenleyici kurumların sorumlu oldukları alanlar doğrultusunda siber güvenliğin sağlanması ve denetlenmesinin sağlamalıdır. (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı: 6)

- **Stratejik Siber Güvenlik Eylemleri**

2013-2014 Eylem planı ile belirlenen ilkeler çerçevesinde ulusal olarak siber güvenliğin sağlanması adına belli başlı stratejik eylemlerin gerçekleştirilmesi planlanmıştır (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı: 7)

- **Yasal Düzenlemeler**

Eylem planı ile ulusal olarak siber güvenliğin sağlanması adına kurum ve kuruluşların, görev, yetki ve sorumluluklarının belirlenerek ihtiyaç duyulan alanların tespit edilerek mevcut eksikliklerin giderilmesini amaçlayan mevcut çalışmaları yapılacaktır. Kavramların karışmasını engellemek adına siber güvenlik terimleri sözlüğü oluşturulacaktır. Yapılan yasal düzenlemeler, hukuka uygun şekilde siber alanda usul hükümlerinin düzenlenmesini sağlayacak şekilde hazırlanacaktır (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı: 7).

- **Adli Süreçlere Yardımcı Olacak Çalışmaların Yürütülmesi**

Uluslararası hukuk kuralları çerçevesinde saldırıya maruz kalanların haklarının korunabilmesi ve mağduriyetlerinin giderilmesi, saldırı kaynağının tespit edilerek söz konusu saldırı hakkında, saldırının kaynağının tespiti, saldırı sistemleri ve bu sistemleri satan tarafların cezalandırılmasına yönelik çalışmalar yapılmalıdır. Ulusal alanda güvenliğin sağlanması için o dönemin teknolojilerinden uygun ve güvenilir olanlarla çalışılmalıdır (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı: 7)

- **Ulusal Siber Olaylara Müdahale Organizasyonunun Oluşturulması**

Siber alanda ortaya çıkan tehditler ve saldırılar karşısında, ortaya çıkan bu tehditlerin belirlenmesi, saldırıların etkilerinin azaltılması ve etkilerinin ortadan

kaldırılmasına yönelik çalışmalar yapılmalıdır. Ulusal ve uluslararası alanda etkili bir şekilde çalışacak Siber Olaylara Müdahale Organizasyonu oluşturulmalıdır.

Ülkemize için olası tehditlere karşı "Ulusal Siber Olaylara Müdahale Merkezi (USOM)" kurulmuştur. USOM'un koordinasyonunda çalışacak şekilde ise "Siber Olaylara Müdahale Ekibi (SOME)" kurulmuştur. Kurulan bu kurumlar siber olaylara müdahale ederken suç soruşturmasına destek sağlayacak şekilde adli ve kolluk birimleri ile koordineli şekilde çalışacaktır. (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı: 7)

- **Ulusal Siber Güvenlik Altyapısının Geliştirilmesi**

Tüm kurumlar bilişim sistemlerinin siber güvenliğini sağlamak adına geniş kapsamlı çalışmalar yaparak alt yapıları güçlendirecek siber güvenliği destekleyecek çalışmalar yapılacaktır. Kritik alt yapıların sistemlerinin siber güvenliği teknolojik önlemler ile birlikte idari ve tedbirler ile de sağlanacaktır. Kurum içinde idari ve teknolojik açıdan eğitimler ile yöneticiler ve tüm çalışanların siber güvenliğin sağlanması bilgilerinin ve yetkilerinin artırılması hedeflenmiştir. (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı: 7)

- **Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi ve Bilinçlendirme Faaliyetleri**

Siber güvenlik alanında zaman içerisinde yeterli sayıda ve yetkin tecrübeli insan kaynağı oluşturulması hedeflenmiştir. Tüm okul düzeylerinde siber güvenlik alanında eğitim verilmesi için çalışmalar yapılmıştır. Bilişim sistemlerini denetleyenlerin, sistem yöneticilerinin siber alandaki tüm tarafların siber güvenlik hakkında bilincin artırılması için çeşitli etkinlikler eğitimler gerçekleştirilmiştir. Kurumlar içinde siber güvenlik alanında denetimlerin yeterli seviyede olması adına çalışmalar yapılmıştır. Tüm toplumun siber güvenlik alanında toplum bilincini oluşturmak ve geliştirmek için çalışmalar yapılmıştır (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı: 9)

- **Siber Güvenlikte Yerli Teknolojilerinin Geliştirilmesi**

Siber güvenlik alanında zaman geçtikçe teknik destek, teknik bilgi, siber güvenlik teknolojilerinin geliştirilmesi ve verilen desteğin artırılması hedeflenmiştir. Kamu ve özel sektör siber güvenlikte yerli teknolojilerinin kullanılması ve geliştirilmesi adına çalışmalar iş birliği halinde yürütülmesi planlanmıştır. (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı: 9)

- **Ulusal Olarak Güvenlik Mekanizmalarının Geliştirilmesi**

Ulusal ve uluslararası alanda siber güvenliğin sağlanması, olası saldırılara ve oluşacak zararlar karşısında bu zararın en aza indirgenmesi, oluşabilecek saldırılara karşı savunmayı sağlayacak çalışmalar yapılmıştır (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı: 9).

- **2013-2014 Ulusal Siber Güvenlik Eylem Planı**

Bu eylem planı ile ulusal olarak siber güvenliğin sağlanması adına eylemler bulunmaktadır. Eylem planlarında her eylem için bir kurum belirlenmiştir ve gruplandırmalar yapılmıştır. Bazı eylemler için kurumların ortak olarak çalışmaları gerekmektedir (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı: 9).

2.7.6. 2015-2018 Bilgi Toplumu Stratejisi Eylem Planı

2014 yılında mülga kalkınma bakanlığı tarafından hazırlanmıştır. Bu eylem planı Şubat 2015 tarihinde Resmi Gazetede yayımlanmıştır (2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı, 2015: 3). Bu döneme kadar olan bütün eylem olanlarını kapsayan "şemsiye" belge olarak karşımıza çıkmıştır (Afyonoğlu, 2020: 388). Eylem planı ile hedeflenen 72 adet eylem ve 8 eksen vardır. 5 numaralı eksende "Bilgi Güvenliği ve Kullanıcı Güveni" ele alınmıştır. Bu başlık temel siber güvenlikle alakalı olarak; (2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı, 2015: 12)

-Siber alanda nitelikli insan kaynağını artırmak ve güvenli internet kullanımı sağlamak, farkındalık için eğitim çalışmaları yapılması,

-Kurum ve kuruluşlar arasında koordinasyon sağlanması ve alt yapı denetimi yapılması,

-Hukuki alt yapı oluşturarak siber güvenlik için minimum standartların belirlenmesi ve siber suçlarla etken şekilde mücadele edilmesi hedeflenmiştir.

Bu eylem planında hem gerçekleşmiş hem de gerçekleşmemiş hedefler vardır;

-Siber güvenlik alanına özel bir siber güvenlik kanunu çıkarılması hedeflenmiş ancak çıkarılamamıştır.

-Kişisel Verilerin Korunması Kanunu yürürlüğe girmiştir.

-Ulusal Siber Suç Stratejisi hazırlanmış ve 2016-2019 ve 2020-2023 eylem plan amacı olarak yer almıştır.

2.7.7. 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı

Gelişen teknolojik imkânlar, teknolojik cihazlar ve bunlarla beraber artan güvenlik ihtiyaçları stratejik planlarda yeniliklere ve gelişmelere gitmek durumunda bırakmıştır. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın ulusal olarak stratejik planı güncellemesi ve yeni eylem planları bu doğrultuda gerçekleşmiştir. Eski eylem planında sorumlu olan kurumlar ile yapılan toplantılar sonrasında mevcut eylem planında olan açıklıkları, eksiklikleri, hedeflenen faaliyetlerin gerçekleşme durumları göz önünde bulundurularak yeni plan açısından ileriye dönük yeni hedefler belirleyerek ve siber alanda siber güvenlik eylemlerinin daha iyi ve sağlıklı olması için yeni faaliyetler belirlenmiştir.

Bu toplantılar ile kamu kurumlarındaki kritik alt yapıların, bilişim sektörü, sivil toplum kuruluşları, üniversitelerden bir araya gelen uzmanlar ile değerlendirmeler yapılarak Türkiye'nin siber güvenlik alanında güçlü ve zayıf yönleri tespit edilerek hangi strateji ve eylem planlarının uygulanacağı belirlenmiştir.

2016-2019 Yılı Eylem Planı hazırlanırken sadece Türkiye kapsamında inceleme yapılmamış; Avrupa Birliği Ülkeleri, NATO Ülkeleri, OECD Ülkeleri gibi uluslararası ülkelerinde siber güvenlik stratejileri takip edilmiştir. Bu ülkelerin siber güvenlik politikalarının kapsamı, hedefleri, öncelikleri, organizasyon yapıları, ARGE çalışmaları, kullanılan teknolojilerin özellikleri, kamu ve özel sektörün koordinesi, siber alanda eğitim durumları, farkındalık çalışmaları da dikkate alınarak

incelenmiştir. Tüm bu incelemeler sonrasında yeni eylem planı olan 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Güvenlik Eylem Planı hazırlanmıştır.

- **2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planının Amacı**

Bu eylem planı ile siber güvenlik kavramı ve ulusal güvenlik kavramlarının ayrı olarak düşünülemeyeceği, siber güvenliğin ulusal güvenliğin ayrılmaz bir parçasının olduğu kabul edilmiştir. Bu anlayışın ulusal olarak herkes tarafından benimsenmesi hedeflenmiştir. Ulusal olarak siber alanda bulunan tüm verilerin korunması adına idari ve teknolojik açıdan önlemlerin alınması için siber alanda yetkinliğin artırılması, herkesin bu konu hakkında yeterli düzeyde bilgi sahibi olması amaçlanmıştır. Eylem planı ile hedeflerin, alt eylem maddelerinin belirlenmesi bu hedeflerin ve maddelerin gerçekleştirilmesi amaçlanmıştır. Bu amaçlar doğrultusunda;

Ulusal siber alanın tamamında geçerli olmak üzere, bilgi teknolojilerinin üzerinden sağlanan hizmetlerin, işlemlerin, verilerin güvenliğinin, gizliliğinin ve mahremiyetinin sağlanması,

Siber güvenlik alanında gerçekleşen saldırıların etkilerinin en aza indirgenmesi, gerçekleşen saldırılar sonrasında çalışma düzeninin eski hale en kısa sürede getirilmesi, saldırıların geldiği yerin belirlenmesi ve oluşan suç hakkında adli makam ve kolluk tarafından soruşturma başlatılması için etkin şekilde araştırma yapılması,

Siber güvenliğin sağlanması için kullanılan teknolojilerin ülkemizde üretilmesi, yerli ve milli olması, dışarıdan alınan milli olmayan ürünler içinde güvenlik ve mahremiyetin sağlanması adına gerekli önlemlerin alınması amaçlanmıştır (Ulusal Siber Güvenlik Stratejisi 2016-2019: 9)

- **2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planının Güncellenmesi**

Eylem planı değişen teknolojik şartlar kapsamında, değişen koşullar ve gereksinimler dikkate alınarak güncellemeye açık şekilde hazırlanmıştır. Kamu ve özel sektörden gelecek talepler doğrultusunda ulusal düzeyde güncellemeler

yapılacaktır. Eylem planının geçerli olduğu yıllar içerisinde gerçekleşmeyen hedefler bir sonraki eylem planına aktarılacaktır (Ulusal Siber Güvenlik Stratejisi 2016-2019: 10)

- **Dünyada Siber Güvenlik Stratejileri ve Eylem Planları**

2016-2019 Eylem Planı'nda diğer ülkelerin stratejik belgeleri ve eylem planları incelenmiştir. Diğer ülkelerin eylem planlarında da 2016-2019 eylem planında olduğu gibi olası siber saldırılar karşısında, siber saldırılara karşı alınacak önlemler konusunda çeşitli ilkeler benimsenmiştir ve bu ilkelerin benzer oldukları saptanmıştır.

Bu incelemeler sonrasında en çok önemli olan ilkeler;

-Siber güvenliğin sağlanması adına bireyden başlayarak, kurum, toplum ve devletin tüm hukuki ve sosyal olarak sorumluluklarının yerine getirilmesi,

-Siber alanda kamu, özel sektör, üniversiteler ve sivil toplum örgütlerinin iş birliği içinde çalışarak bilgi paylaşımında bulunmaları,

-Uluslararası Siber Güvenlik Operasyon Merkezleri arasındaki siber olayların yönetiminde iş birliğinin sağlanması,

Bu incelemeler sonrasında dikkat çeken riskler;

-Tüm toplumların sosyal ağlara karşı çok bağımlı olmaları,

-Kritik alt yapıların ve kurumların siber alandaki konumları,

-Siber casusluk çalışmaları ve saldırılar,

-Siber alanda çalışacak olan personel ve bilgi yetersizliği,

-Kurumların kendi arasındaki iletişim kopukluğu ve koordinasyon eksikliğidir.

Tüm bu ilkeler ve riskler göz önüne alınarak ulusal olarak siber güvenlik ilkeleri, siber güvenlik amaçları ve eylem planları belirlenmiştir (Ulusal Siber Güvenlik Stratejisi 2016-2019: 10)

- **2016-2019 Stratejik Siber Güvenlik Amaçları ve Eylemleri**

Mevcut riskleri, olası saldırıları ve tehditleri en aza indirgemek adına belirlenen stratejik amaçlar belirlenmiştir. Bu amaçlar;

-Ulusal kritik altyapıların belirlenmesi ve envarter oluşturulması, bu kritik alt yapıların güvenliklerinin sağlanması ve denetlenmesi,

-Siber alanda denetim için uluslararası mevzuatın oluşturulması,

-Siber güvenlik kapsamında kamu kurum ve kuruluşlarının düzenleme, denetleme ve siber alanda yetkinliklerinin geliştirilmesi,

-Kurumların sistemlerinin sadece saldırılara karşı değil kullanıcılara, doğal afetlere karşı da korunması için düzenlemeler yapılması,

-Kurumların kendi içinde siber güvenlik alanında yetkinliklerinin sağlanması,

-Siber güvenlik kavramı hakkında kurum yöneticilerinin bilgilerinin artırılması,

-Siber güvenlik alanında bilgi sahibi ve yetkin personelin yetiştirilmesi, bu alanda uzmanlaşmak isteyen personeller, uzmanlar ve öğrenciler için teşvik ve destek sağlanması,

-Toplumun tamamında siber güvenlik alanında bilincin oluşturulması, eğitimlerin verilmesi ve farkındalıkların oluşturulması,

-Kamu kurumlarında siber güvenlik alanında uzman personellerin haklarının iyileştirilmesi,

-Kurumsal ve sektörel SOME'lerin etkinliklerinin artırılması, mevzuat desteğinin sağlanması, mali düzenlemelerin yapılması, yetkin ve bilgili tecrübeli personel istihdamının sağlanması, ulusal siber olaylara müdahale organizasyonu kapsamında bilgi paylaşımlarının geliştirilmesi,

-Siber güvenlik alanında koordinasyonu sağlayacak bir merkezi kamu otoritesi oluşturulması,

-Ulusal siber güvenlik ekosisteminin oluşturulması,

-Siber güvenlik alanında danışmanlık hizmetlerinin artırılması, faydalı uygulamaların paylaşılması, ekosistem içinde iyi örneklerin yaygınlaştırılması,

-Siber güvenlik alanında kullanılan bilişim sistemlerinde kullanılan yabancı donanımların açıklarının giderilmesi, tehdit oluşturabilecek unsurlara karşı önlemlerin alınması,

-Ar-Ge çalışmaları yaparak yerli teknolojilerin geliştirilmesi, yazılımların ve donanımların kullanılması

-Tehditlerin ortadan kaldırılması için, saldırı yapılmadan önce ulusal siber savunma yeteneğinin geliştirilmesi eylem planının amaçları olarak benimsenmiştir. Bu amaçların gerçekleştirilmesi beş adet stratejik eylem başlığı adı altında; Siber Savunmanın Güçlendirilmesi ve Kritik Alt Yapıların Korunması, Siber Suçlarla Mücadele, Farkındalık ve İnsan Kaynağı Geliştirme, Siber Güvenlik Ekosisteminin Geliştirilmesi ve Siber Güvenliğin Milli Güvenliğe Entegrasyonu olarak sınıflandırılmıştır (Ulusal Siber Güvenlik Stratejisi 2016-2019: 13)

2.7.8. 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı

Bilgi ve iletişim teknolojileri gün geçtikçe kendini geliştirmektedir. Bu gelişmelerin ortaya çıkardığı avantajlardan en üst düzeyde faydalanmak gerekmektedir. Ulusal siber güvenliğin geliştirilmesi, çalışmaların artırılması da bu gelişen teknoloji ile eş zamanlı olmalıdır (Karasoy ve Babaoğlu, 2021: 133).

Teknolojinin gelişmesi ile değişen, gelişen, karmaşık bir hale gelen, sayıları ise sürekli artan siber tehditler karşısında toplumun, kurumların, kritik alt yapıların güvenliklerinin artırılması gerekmektedir. Yani gelişen teknoloji sonrasında siber güvenlik alanında ilgili ihtiyaçlar günden güne artmaktadır (Ulusal Siber Güvenlik Stratejisi 2020-2023: 31)

2020-2023 eylem planı ile önceki eylem planlarındaki faaliyetlerin gerçekleşme düzeyleri, yapılan faaliyetler ve çalışmalar göz önünde bulundurularak bu planın geçerli olduğu süre zarfında öncesinde hayata geçirilen faaliyetlerin daha da güçlendirilmesi ve geliştirilmesi hedeflenmiştir. Eylem planı hazırlanırken ulusal olarak siber güvenliğin daha da geliştirilmesi, teknolojik gelişmelerin etkileri, siber tehditler sonrasında ortaya çıkan sonuçlar, siber tehditlerin neye yönelik olduğu,

ulusal olarak siber güvenlik alanındaki ihtiyaçlar dikkate alınmıştır. Tüm bunlar dikkate alınarak yapılan çalışmalar sonucunda bu eylem planı ile belirlenen stratejik amaçlar sekiz ana başlıkta toplanmıştır;

-Kritik altyapıların korunması,

-Ulusal kapasitenin artırılması ve geliştirilmesi,

-Organik siber güvenlik ağı,

-Yeni nesil teknolojilerin güvenliği,

-Siber suçlarla mücadele,

-Yerli ve milli teknolojilerin geliştirilmesi ve desteklenmesi,

-Siber güvenliğin milli güvenliğe adaptasyonu,

-Uluslararası iş birliğinin geliştirilmesidir (Ulusal Siber Güvenlik Stratejisi 2020-2023: 22)

Kritik alt yapıların korunmasına ilişkin düzenlenmelerin faaliyete geçirilmesi, siber tehdit ve riskler konusunda acil durum planlarının geliştirilmesi, kaynak ve hedeflerin sadece yurt içinde kalması, siber güvenliğin milli güvenlik kapsamında ele alınması gibi eylem planları belirlenmiştir. İlk ve orta dereceli okullarda siber güvenlik alanında eğitimlerin verilmesi, siber güvenlik açısından verilen eğitimin kalitesinin artırılması, içeriklerin geliştirilmesi ve yaygınlaştırılması, siber olaylara karşı müdahale ekiplerinin yetkinliklerinin ölçülmesi ve denetlenmesi, yetkin kurumların artırılması geliştirilmesi hedeflenmiştir. Oluşturulması planlanan organik siber güvenlik ağı çerçevesinde ileri düzey uzmanlık projelerinin hazırlanması ve geliştirilmesi, tüm ülke genelinde kullanılacak şekilde çalışmalar yapılması, bu çalışmaları yapacak kurumlar arasında ve Ulusal Siber Olaylara Mücadele Merkezi (USOM) arasında bilgi paylaşılması amaçlanmıştır (Ulusal Siber Güvenlik Stratejisi 2020-2023: 7)

Yerli ve milli güvenlik teknolojilerinin geliştirilmesi, teşvik ve desteğin artırılması, bu çalışmalara yönelik çalışmaların desteklenmesi amaçlanmıştır. Tüm bunlara ek olarak siber güvenliğin geliştirilmesi için ulusal faaliyetlerin yanında

uluslararası faaliyetlerde iş birliğinin geliştirilmesi, bilgi paylaşımın artırılmasına yönelik çalışmalar yapılması hedeflenmiştir.

Gelişen teknoloji ile internetin ve teknolojik cihazların kullanımı ülkemizde doğru orantılı şekilde artmıştır. Artan kullanım doğrultusunda da bilgi ve teknolojik cihazların güvenli kullanımı çok önemli bir ihtiyaç halini almıştır. Özellik kritik alt yapıların güvenliğinin sağlanması günden güne önemli bir ihtiyaç haline gelmiştir. Bu gelişmelerin doğrultusunda siber riskler ve tehditler de gelişime ayak uydurmakta, karmaşıklaşmakta ve artış göstermektedir. Bu saldırılar sonrasında tehditler, fiziki saldırılardan daha çok olumsuz sonuçlar ve ciddi derece zararlara sebep olmaktadır (Ulusal Siber Güvenlik Stratejisi 2020-2023: 26)

Siber güvenlik alanında tedbirlerin sağlanması, güvenliğin sağlanması COVİD 19 pandemisi ile kendisi daha da öne çıkarmıştır. Bu süreçte dijital ortamlardan sağlanan çalışmalar, çevrimiçi eğitimler siber güvenlik alanındaki ihtiyacı, olası saldırılar karşısında savunma yapabilmeyi daha çok önemli kılmıştır. Siber tehditler her geçen zamanda sayısal olarak artmakta ve nitelik olarak kendisini geliştirmekte bu gelişmeler sonrasında yarattığı etki de büyümektedir. Bu tehditler karşısında kaynakların planlanması ve kullanım şekli, risklerin ve ihtiyaçların saptanması, teknolojik gelişmeler karşısında kısa ya da uzun vadeli planlar yapılması gerekmektedir (Ulusal Siber Güvenlik Stratejisi 2020-2023: 12)

- **2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı İlkeleri**

2020-2023 eylem planı doğrultusunda siber güvenlik alanında belirli ilkeler benimsenmiştir. Bu ilkeler;

-Siber güvenlik, ulusal güvenliğin ayrılmaz bir parçasıdır ve bütün olarak kabul edilmelidir. Ulusal güvenliğim tam olarak sağlanması için siber güvenlik alanında belirlenen hedeflere ulaşılması gerekmektedir.

-Siber güvenlik ilgili çalışmalar geçmişten günümüze kadar elde edinilen bilgiler, hedefler, eylem ve planların tamamı gözetilerek hazırlanmaktadır.

-Dijitalleşmenin başarılı ve sürekli olabilmesi için siber güvenliğin ciddi derece önemli olduğunu kabul etmek gerekmektedir.

-Siber güvenlik politikalarının uygulanmasına yönelik tüm çalışmalar bu alanda çalışanların birbirleri ile etkin iletişimi ve koordineli iş birliği içerisinde yürütülmelidir.

-Siber güvenlik alanında çalışma yapan kurumlar, siber uzaydaki risklerin yönetimi ile ilgili sorumlulukları karşısında yeterli düzeyde şeffaf olarak çalışabilmeli, hesap verebilirlik ve etik kuralları çerçevesinde çalışmalıdır.

-Siber alandaki riskler etkin şekilde belirlenir ve yönetilmelidir.

-Kritik alt yapıların sağladığı hizmetlerin kesintisiz ve etkin şekilde sunulması esas alınmalıdır.

-Hizmetlerin ve ürünlerin ortaya çıkmasında, son kullanıcıya ulaşımına kadar olan tüm aşamalarda siber güvenlik kavramı esas alınmalıdır.

-Yapılan işlemlerin tümünde söz konusu işlemlerin ve bilgilerin gizliliğinin, bütünlüğünün ve erişilebilirlik prensiplerinin temel siber güvenlik prensibi olarak kabul edilmesi ve temel siber güvenlik prensiplerine sadık kalınmalıdır.

-Siber güvenlik güçlü hukuki temeller üzerine kurulmalıdır.

-Siber güvenlik için yenilikçi, güçlü ve kendini geliştirebilir teknolojilerin sağlanması, yerli ve milli ürün ve hizmet kullanımları için Ar-Ge çalışmalarına önem verilmelidir (Ulusal Siber Güvenlik Stratejisi 2020-2023: 18)

- **2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı Hedefleri**

Gelişen teknolojik şartlar ve politikalar doğrultusunda her eylem planı ile yeni hedefler belirlenmiştir. Bu hedeflere ulaşmak içinde faaliyetlerin süreklilik içinde yürütülmesi gerekmektedir. Tüm eylem planlarının asıl ve tek hedefi söz konusu siber tehditler karşısında, risklerin, oluşturacağı zararların ve saldırıların etkilerini en aza indirgenmesidir.

Siber güvenlik alanında insan kaynağının doğru ve etkin kullanımı, siber alandaki süreçlerin iyileştirilmesi ve teknolojik gelişim açısından hem istikrarlı büyümeyi, hem de kalkınmayı tamamlayan unsurlar olmuşlardır.

2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı kapsamında hedefler aşağıdaki şekilde listelenmiştir;

-Kritik alt yapıların siber alandaki güvenliklerinin 7/24 sağlanması,

-Ulusal seviyede siber güvenlik alanında gelişen teknoloji karşısında son teknolojilerin kullanılması,

-Siber alanda yerli ve milli teknolojilerin kullanılması ve geliştirilmesi,

-Siber olaylarda, müdahalenin olaya müdahale etmeden, müdahale etmenin ve müdahale sonrasının bir bütün olarak yapılması,

-Siber olaylara müdahale ekiplerinin yetkin kişiler olması ve sürekli olarak yetkinliklerinin artırılması,

-Kurum ve kuruluşlar arasında veri paylaşımlarının güvenli şekilde yapılması,

-Kurumsal, sektörel veya ulusal bazda siber olaylara karşı hazırlık seviyelerinin çeşitli planlamalar ve analizlere bağlı olarak artırılması,

-Çıkış kaynağı ve hedefi yurt içinde olan verinin sadece yurt içinde kalması,

-Kritik alt yapılarda düzenleme ve denetlemeler yaparak siber güvenlik alanında gelişimlerin sağlanması,

-Yeni nesil teknolojilerin güvenliğinin sağlanmasına yönelik ihtiyaçların belirlenmesi,

-Yenilikçi fikirler, yapılan Ar-Ge çalışmaları doğrultusunda yapılan faaliyetlerin desteklenmesi, yerli ve milli ürün ve hizmetlerin dönüşümün gerçekleştirilmesi,

-Toplumun tüm kesimleri tarafından siber alanın güvenle kullanılması,

-Siber güvenlik alanındaki farkındalıkların tüm toplumlarda en üst seviyede kullanılması, buna yönelik etkinliklerin sürdürülmesi,

-Kurum ve kuruluşlarda kurumsal bilgi güvenlik kültürünün yerleşmesi,

-Çocukların siber alanın zararlı kısımlarına karşı korunmasının sağlanması,

-Siber güvenlik alanında uzmanlaşmak isteyen ve bu alanda ilgili olan bireyler için çeşitli projeler gerçekleştirerek insan kaynağının güçlendirilmesi,

-Örgün ve yaygın eğitimde siber güvenlik hakkında dersler verilmesi, içeriklerin artırılması,

-Ulusal ve uluslararası alanda siber güvenlik alanında bilgi paylaşımlarının geliştirilmesi, iş birlikleri için çeşitli mekanizmaların oluşturulması,

-Siber alandaki suçların en aza indirgenmesi ve caydırıcılığın oluşması,

-İnternet ve sosyal medyada doğru ve güncel bilgi paylaşımlarının yapılması, buna uygun mekanizmaların geliştirilmesidir (Ulusal Siber Güvenlik Stratejisi 2020-2023: 20)

- **2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planının Stratejik Amaçları**

2020-2023 eylem planı ile hedeflerin yanında çeşitli stratejik amaçlar da belirlenmiştir. Bu amaçlar (Ulusal Siber Güvenlik Stratejisi 2020-2023: 22);

a. Kritik Altyapıların Korunması ve Mukavemetin Artırılması

Ülkemizde: elektronik haberleşme, enerji, finans, ulaştırma, su yönetimi ve kritik kamu hizmetleri kritik alt yapıların içinde bulunmaktadır. Bu kritik alt yapılar hem hükümet hem de toplum için en önemli unsurlardır. Verilerin gizliliğinin sağlanması, korunması adına birçok faaliyetler gerçekleştirilmiştir.

Kritik alt yapıların sürekli olarak korunması, gelişen teknoloji ile ortaya çıkan daha büyük tehditler, olası saldırılar karşısında ulusal olarak siber alandaki mukavemetin artırılması, tüm kamu ve özel sektörlerin korunması amaçlanmıştır.

Bu amaçlar doğrultusunda uluslararası bilgi güvenliğinin sağlanması, söz konusu bilgilerin ülke sınırları içerisinde kalması, yurt içinde üretilen verilerin yurt içinde kalması, sektörlerin ve kurumların siber güvenlik alanında düzenlemelerin yapılması ve denetim mekanizmalarının kurulması amaçlanmıştır.

Kısaca kritik alt yapıların, siber alandaki tüm verilerin korunması adına siber tehditlere karşı korunması ve siber olaylara müdahale kabiliyetlerinin

güçlendirilmesi, oluşabilecek zararların en aza indirgenmesi hedeflenmiştir (Ulusal Siber Güvenlik Stratejisi 2020-2023: 23)

b. Ulusal Kapasitenin Geliştirilmesi

Ulusal siber güvenliğin sağlanmasındaki en önemli unsurlardan birisi yetkin, uzman insan kaynağıdır. Bu kapsamda insan kaynağının geliştirilmesi, bilgi düzeyi ve tecrübesini artırmak amaç amaçlanmıştır. Aynı zamanda bu gelişim sağlanması için nitelikli olarak insan gücünün yetiştirilmesi hedeflenmiştir.

Siber olaylara karşı hazırlık seviyelerinin yükselmesi SOME'ler üzerinde gelişimler sağlanarak yetkinliklerinin artırılması, daha da üst seviyeye çıkarılması amaçlanmıştır. Tüm bunların yanında sektörel, ulusal ve uluslararası seviyede düzenli olarak siber güvenlik tatbikatları ve eğitimlerin yapılması hedeflenmiştir.

Siber güvenlik uzmanlığı kavramlarının geliştirilmesi, bu kavrama mesleki nitelik kazandırılması, üniversitelerde siber güvenlik ve bu alanlardaki programların geliştirilmesi ve yaygınlaştırılması, siber olaylarla mücadele eden birimlerin, personellerin uzmanlık düzeylerinin artırılmasına yönelik faaliyetlerin gerçekleştirilmesi, toplum içinde de siber güvenlik alanında uzmanlaşmak isteyen bireylerin de eğitim alabilmeleri amaçlanmıştır. Bu hususta çalışmalar yapılması ile siber güvenlik alanında çalışanların dışında da nitelikli insan kaynağı oluşturulması hedeflenmiştir.

Toplumun tüm kesimlerinde siber güvenlik kültürünün yerleşmesi de gelişen teknoloji ile çağın gereklerinden birisi haline gelmiştir. Bu kültürün sağlanması için de siber güvenlik alanında farkındalığın oluşturulması gerekmektedir. Tüm toplumda oluşturulan siber güvenlik alanındaki tehditler bilinçlendirmelerin sağlanması ile risklerin, tehditlerin olumsuz etkileri azalacaktır (Ulusal Siber Güvenlik Stratejisi 2020-2023: 24)

c. Organik Siber Güvenlik Ağı

Siber tehditler, gün geçtikçe ve teknolojik olarak gelişim sağlandıkça saldırıların tespitlerinin sağlanması ve ulusal olarak güvenliğin sağlanması zor bir hale gelmektedir. Zararlı yazılımlar, tehditler güvenlik açıklarından faydalanarak büyük ölçüde zararlar vermek isteyen saldırganlar bu açıkları kullanmaktadırlar.

Organik siber güvenlik ağı ile siber güvenlik alanında çalışan, siber alanla ilgilenen her insanın bilgi, birikim ve tecrübelerinin bir araya getirilerek iş birliği içinde çalışmaları amaçlanmıştır (Ulusal Siber Güvenlik Stratejisi 2020-2023: 25).

d. Yeni Nesil Teknolojilerin Güvenliği

Yapay zekânın, gelişen teknolojilerin siber güvenlik için kullanım alanlarının belirlenmesi, geliştirilecek olan yerli ve milli teknolojilerin kullanılmasına teşvik edilmelidir (Ulusal Siber Güvenlik Stratejisi 2020-2023: 27)

e. Siber Suçlarla Mücadele

Siber suçlarla mücadele kapsamında uluslararası seviyede iş birliği sağlanmalıdır ve ona göre çalışılmalıdır. Siber alanda yapılan saldırılarda yer ve mekân olmadığı, yapılan saldırıların boyutlarının uluslararası düzeyde olduğu, yapılan saldırının ulusal sınırların dışına çıkabileceği dikkate alınmalıdır (Ulusal Siber Güvenlik Stratejisi 2020-2023: 26)

f. Yerli ve Milli Teknolojilerin Geliştirilmesi ve Desteklenmesi

Yeni nesil teknolojilerin milli ve yerli teknolojiler ile entegre edilerek siber güvenlik alanında sayılarının artırılması ve kullanımının yaygınlaştırılması hedeflenmiştir. Siber güvenlik alanında kurumlar arasında sağlanacak olan iş birlikleri ile siber alandaki güvenlik önlemleri daha üst seviyeye taşınacak, iş birlikleri sayesinde de yerli ve milli teknolojik ürünlerin kullanımı ve gelişimi de artacaktır. Yerli ve milli teknolojik ürünlerin üretimi bu iş birliği sayesinde ihtiyaca yönelik olarak gerçekleşecektir. Siber güvenliğin yerli ve milli ürünlerin ile sağlanması, kritik alt yapıların yerli ve milli güvenlik ürünleri ile korunması en önemli amaçlardandır. Ulusal kaynaklar ile üretilen ürünlerin marka ve hizmet değerlerinin yükseltilerek küresel olarak kullanılması hedeflenmiştir (Ulusal Siber Güvenlik Stratejisi 2020-2023: 27)

g. Siber Güvenliğin Milli Güvenliğe Entegrasyonu

Siber güvenlik kavramı gelişen teknoloji ve değişen saldırı kavramları sebebiyle milli güvenlik kavramının en önemli ayrılmaz unsurlarından birisi haline gelmiştir. Ulusal olarak hazırlanan güvenlik politikalarından sadece fiziki tehditler

dışında da siber tehditleri göz önünde bulundurarak politikaların hazırlanması hedeflenmiştir. Kara, deniz ve havanın yanında da siber savunmanın da bulunması siber alanda oluşabilecek zararlar ve saldırılara karşı korumanın sağlanması amaçlanmıştır.

Söz konusu siber saldırılar gelen ihbarlar doğrultusunda bu olayların en başından çözüm aşamasında kadar takip eden ve kontrol eden resmi bir kurumdur. Ulusal ve uluslararasında siber güvenlik tatbikatları düzenleyerek tüm özel ve kamu kurumlarının siber saldırılar karşısında bilinçlendirmek ve farkındalığın artırılmasını hedeflemektedir (Ulusal Siber Güvenlik Stratejisi 2020-2023: 27)

h. Uluslararası İş Birliğinin Geliştirilmesi

Dünya ülkelerinin tamamı siber güvenlik politikalarını hazırlarken iş birliği ile hareket etmektedirler. Çünkü birbirlerinin güvenlik politikalarından esinlenerek siber alandaki güvenliklerini artırmaları için koruma yöntemleri ve siber saldırıların geliştirilmesi konusunda iş birliği yapmakta, bilgi ve tecrübelerini paylaşmaktadırlar.

Ortak stratejilerin hazırlanması, siber güvenlik alanındaki uzmanların fikir ve görüş alışverişleri, dünyada ve ülke genelinde siber olaylara karşı müdahalelerin güçlenmesini sağlamaktadır (Ulusal Siber Güvenlik Stratejisi 2020-2023: 28)

2.8. TSK'nın Siber Güvenlik Yapısı

Türkiye'de kamu kurum ve kuruluşlarına özel sektör kurumlarına karşı gerçekleştirilen siber saldırılar gün geçtik artmaya başlamıştır. Bu artışlar sonrasında siber alanda gerçekleşen saldırıların artık tehdit niteliğinde olduğu kabul edilmiştir ve çeşitli siber güvenlik mekanizmaları inşa edilme gereksinimi ortaya çıkmıştır. Bu dönemde Siber Savunma Komutanlığı oluşturulmuştur. Bu komutanlığın amacı ülkeyi siber saldırılara karşı korumaktır. Komutanlık, Savunma Bakanlığı, TUBİTAK, ODTÜ ve Genelkurmay Başkanlığı bünyesinde çalışacaktır (Bıçakçı, Ergün ve Çelikpala. 2016: 44)

Komutanlığın ardından Siber Güvenlik Kurulu, ardından TSK bünyesinde Siber Savunma Merkezi Başkanlığı kurulmuştur. Siber Savunma Komutanlığı'nın belli başlı görevleri vardır;

-TSK'nın kullandığı siber ortamındaki tüm sistem ve verilerin siber güvenliğini sağlamak,

-Gerçekleşen siber olaylara 7/24 sürekli olarak müdahale etmek,

-NATO tarafından gerçekleştirilen siber tatbikatlara katılmak,

-TSK bünyesinde farkındalık ve nitelik eğitimleri vermek,

-TSK'nın kullandığı sistemler üzerinde siber güvenlik denetimleri ve testleri yapmak olarak bahsedilebilir (Bıçakçı, Ergün ve Çelikpala, 2016: 44-46).

2.9. EGM'nin Siber Güvenlik Yapısı

Emniyet Genel Müdürlüğü, ilk olarak siber alanda "Bilgisayar Suçları ve Bilgi Güvenliği Kurulu"nu Nisan 1998'de kurmuştur. Bu kurul, bilişim suçlarının kapsamının belirlenmesi, ulusal ve uluslararası suç mevzuatının incelenmesi, bilişim teknolojileri ile işlenecek suçların incelenmesi ve EGM kapsamındaki birimlerin görevlendirilmesi için çalışılmıştır (Bıçakçı, Ergün ve Çelikpala, 2016: 46).

EGM'nin 2011 senesinde; siber suçlarla mücadeleyi baz alan Bilişim Suçlarıyla Mücadele Daire Başkanlığı'nı kurmuştur. 2013 yılında bu birim isim değiştirerek Siber Suçlarla Mücadele Daire Başkanlığı'na dönmüştür.

2.10. Siber İstihbarat

Siber istihbaratın asıl amacı, söz konusu siber güvenlik tehditlerine yanıt verebilmek, siber araçlarla bilgi toplamak hedeflenir. Siber saldırı gerçekleşmeden tehdidin neden geldiği, nereden geldiği, kim tarafından olduğunun tespit edilmesi amaçlanır. Türkiye'de MİT bu görevli üstlenmiştir. MİT'in görevleri ise; siber güvenlik konularında her türlü teknik istihbarat, insan istihbaratı, sistem ve araçları kullanarak bilgi, haber, belge, veri toplamak, kaydetmek ve bunların analizini yapmak, istihbaratı gerekli kuruluşlara göndermek (https://www.resmigazete.gov.tr, 2023).

2.11. Devlet Dışı Aktörler Yerli Hacker Grupları

Devletin resmi olarak siber alanda çalışmalarının yanında devlet dışında siber alanda bireysel veya grupsal olarak faaliyet gösteren aktörler vardır. Bu hacker veya hacker gruplarının iyi veya kötü niyetli olarak çalışmaları söz konusudur. Aşağıda söz konusu bu hacker gruplarından bazılarına değinilmiştir.

- **Ayyıldız Tim**

Verilerine göre bu grup 2002 yılında kurulmuştur. Grubun kendine göre bir takım amaçları vardır;

-Türkiye devletine karşı söz konusu tüm kamu ve kuruluşlarına karşı gelebilecek her türlü siber saldırıyı engellemek,

-Türkiye karşıtı uygun olmayan pornografik anayasal düzeni değiştirmeye çalışan satanist tüm yayınları engellemek,

-Faydalı ve verimli yayın yapan sitelere ve sistemlere teknik destek vermek,

-Türkiye devletini internette temsil eden sistemleri ve verileri korumak,

-Saldırılara karşı saldırı yapmak, cevap vermek ve Türkiye'yi hak ettiği, olması gereken yere getirmek,

-Gerekli hallerde ülkeye karşı yönelen saldırılara şiddetle cevap vermek,

-Kamuoyunu bilinçlendirmek adına faaliyetler yapmak (https://www.ayyildiztim.com.tr/, 2022).

- **RedHack**

Türkiye'de bilinen hacker gruplarından birisidir. Bu grubun 1977 yılında kurulduğu iddia edilmektedir. Amaçları ve ideolojileri eşit, adil ce sömürüsüz bir dünya sağlamak için hackleme yapmaktır. 2008'de Ankara Emniyet Müdürlüğü'ne, 2013 de ise Gezi Olayları'ndan sonra devlet kurumlarına ciddi derecede saldırılar yaparak isimlerini popülerleştirmişlerdir (https://www.milliyet.com.tr, 2022).

- **B3yaz Hacker**

Çevrimiçi sistemleri daha güvenilir hale getirmek için üreticilere, güvenlik açısından açıkları tespit ederek çalışmaktadırlar. Pentest hizmeti için hackleme kabiliyetine sahiptirler. İki tür saldırı gerçekleştirirler. Birincisi sistemlerdeki var olan güvenlik açıklarını bildirmek, ikincisi ise kendi değer yargılarına karşı aykırı olan içerikleri engellemek için yapılan saldırılardır (https://tr.wikipedia.org, 2022).

- **Türk Hack Team**

En teşekküllü ve en bilinen hacker grubudur. 2002'de kurulmuştur. İnternet siteleri diğer hacker gruplarına göre daha kapsamlı, detaylı ve öğretici niteliktedir. Kendilerini "Vatanını Seven Müslümanlar" olarak tanıtmaktadırlar. Bu hacker grubunun belli başlı hedefleri vardır;

-Dilimize, dinimize, ülke değer ve inançlarına örf ve adetlere aykırı sitelerin hayatına son vermek,

-Zevk için değil, misyon olarak hacklemek,

-Doğru, düzgün ve ahlaklı yayın yapan sitelere destek olmak, çıkar yönetmeden çalışmalar yapmak,

Türk Hack Team, ülke çapında en büyük botnetlerden birisini kontrol ettiği görülmektedir. Geçmiş dönemde yaptığı saldırılar ne kadar kapsamlı bir olduğunu, hükümet yanlısı olduğunu, Türkiye'ye karşı olası tehditlerde savunucu olduğu ortaya koymaktadır (https://www.turkhackteam.org, 2023).

- **Cyber Warrior (Akıncılar)**

Cyber Warrior, diğer adıyla akıncılar 1999'da illegal-part adıyla kurulan bir gruptur. Daha sonradan Cyber Warrior olarak tekrar yapılanmaya başlamışlardır. Hiyerarşi ordu ile aynıdır. Grup kendisini bir kardeşlik yolu olarak tanımlar. Grup üyelerinde örfi adetlerine sadık, Türk milliyetçisi, birlik arasında kardeş bağı sağlaması özellikleri aranmaktadır.

Cyber Warrior internet sitesi, Türkiye İnternet Yasası'nın hazırlanması sürecinde aktif olduğu iddiaları bulunmaktadır. Böylece karar vericilere, siyasilere yakınlıklarının olabileceği söz konusudur. Grup yeni çıkan bu yasaya göre görevlerini şekillendirmiştir:

-Ahlaki inanç ve değerlere saldırı yapan,

-Saf beyinleri bulandırmaya, karıştırmaya çalışan içerikleri yayınlayan,

-Satanist ve pornografik yayın yapan,

-Türkiye aleyhine yayınlar yapan, kamu vicdanını olumsuz şekilde etkileyen yayınlar yapan siteleri ve engellemeyi hedeflemiştir.

Cyber Warrior kendi internet sitelerinde kendilerine ait görevlerine yer vermiştir. Hiçbir dernek, kurum, örgüt be parti ile ilişkilerinin olmadığını, grup içindeki üyelerin uzmanlık ve bilgiye göre sorumluluklarının ve görevlerinin olduğunu belirtmişlerdir (https://spysecurity.net, 2022).

Günümüzde misyonlarını ve amaçlarını gerçekleştirdikleri için bu hacker grubu kapanmıştır.

2.12. Avrupa Birliği ve Türkiye'de Siber Politikalar

Avrupa Birliği, Türkiye'yi siber politikalar alanında olumlu şekilde etkilenmiştir. AB içinde kurulan kurumları izleme değerlendirme fırsatı elde etmiştir. Avrupa ülkelerinde meydana gelen siber saldırılar, Türkiye'yi tetiklemiş ve siber politikaları geliştirme açısından teşvik etmiştir. Uyarıcı nitelikte olan bu saldırılar Türkiye'yi siber alanda yeni politikalar için yönlendirmiştir (Kutlu, Kahraman ve Dinçer, 2019: 6)

Güncel olarak 15 temmuzda gerçekleşen darbe girişimi Türkiye'nin siber alana bakış açısını değiştirmiş ve daha çok ilginin gösterilmesine neden olmuştur. Türkiye'de siber güvenlik politikası e-devlet uygulamalarının kullanımı ve gelişimi bu olaylarla paralel olarak gerçekleşmiştir.

2003 yılında ortaya çıkan E-Dönüşüm Türkiye Projesi ve devamı Türkiye'de siber politikaların siber güvenlik kamu politikaları haline getirilmiştir. Türkiye'nin siber güvenlik kavramıyla geç tanışması, diğer ülkelerin daha önceden bu alanda çalışmalar yapması Türkiye'yi zayıf hale getirmiştir. Bu sebeplerden ötürü siber alanda daha farklı çalışmalar yapmak gerekmiştir. Türkiye'nin tüm kurumları siber güvenlik kavramı ile 27 Ekim 2010 yılında (MGK) Milli Güvenlik Kurumu Bildirisi'nde tanışmıştır. MGK'nin bu bildirisinde siber güvenlik konusuna değinmesi ilk aşamada önemli bir gelişme olarak ele alınabilir. Çünkü Türkiye AB'nin açtığı Siber Suç Sözleşmesi'ni 10 Kasım 2010'da imzalamıştır.

22 Nisan 2014 tarih ve 6533 sayılı "Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasına Uygun Bulunduğuna Dair Kanun ile Siber Suç

Sözleşmesi" onaylanmıştır. İlgili kanun 2 Kasım 2014'de Resmi Gazetede yayımlanmıştır **(**https://www.sibersan.com, 2022)

Türkiye'de ilk aşamada "Siber Kriz Yönetimi ve Kritik Altyapı Korunması" görevi 5902 sayılı yasa ile AFAD'a verilmiştir. AFAD bu kanun ile kendi içerisinde doğal ve teknolojik afetler olarak iki gruba ayrılmıştır. Ülkeye ait kritik alt yapıların siber güvenlik konuları teknolojik afetlere dahil edilmiştir. AFAD, kritik alt yapıları koruma planı içerisinde çeşitlik bakanlıkların ve Hacettepe Üniversitesi'nin içinde bulunduğu 12 adet kurumu kritik alt yapıların korunması için organizasyonlara dahil etmiştir. Siber saldırılara karşı korunmayı sağlamak için temel aşamaları bildirir Eylül 2014'de "2014-2023 Kritik Alt Yapıların Korunması Yol Haritası Belgesi"ni yayımlanmıştır. Bu belge ile kritik alt yapılar korunurken AB direktiflerinin dikkate alınması gerektiği ve AB düzeyinde iletişim ve iş birliği yapılması gerektiği belirtilmiştir (Bıçakçı, Ergün ve Çelikpala, 2016: 43).

Türkiye'de siber güvenlik politikaları hakkında 2016-2019 ve 2019-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı hazırlanmıştır. Bu stratejik eylem planlarının yanında siber güvenlik raporu da belirleyici olmuştur. Ulusal Siber Güvenlik Eylem Planlarının temel hedefleri arasında siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olduğu düşüncesinin tüm kesimlere yerleştirilmesi, ulusal siber uzayda yer alan sistem ve aktörlerin tamamının güvenliğini sağlamak üzere yönetsel ve teknolojik tedbirlerin alınması yer almaktadır (Aslay, 2017: 24).

Darbe girişimi olaylarından sonra 2018'de DDK'nın Siber Güvenlik Raporu doğrultusunda kamu özel sektör ve üniversiteler arasındaki iş birliğinin artırılması, siber güvenlik ekosistemleri oluşturulması ve hizmet entegrasyonunun sağlanması amaçlanmaktadır. DDK raporuna göre; ulusal siber güvenlik teknoloji yol hatırası ve öncelikli sektör alanlarının belirlenmesi amaçlanmıştır. Bu çalışmalar ise Dijital Dönüşüm Ofisi koordinasyonunda yürütülmesi hedeflenmiştir (Kutlu, Kahraman ve Dinçer, 2019: 7).

2.13. Türkiye'de Siber Güvenlik Tatbikatları

Türkiye siber alanda yaptığı çalışmalar sonrasında mevcut olan durumu kontrol edebilmek, olası saldırı durumunda neler olabileceğini test etmek amacıyla çeşitli tatbikatlar yapılmıştır ve bu tatbikatlar doğrultusunda çalışmalar gerçekleştirilmiştir.

2.13.1. BOME 2008 Tatbikatı

Bu tatbikat ile kurumsal BOME süreçlerinin takibinin yapılması ve kontrol edilmesi, TR-BOME iş birliği sürecinin takibi, siber olaylara müdahale ederken eksikliklerin ortaya çıkartılması hedeflenmiştir. Tatbikata Başbakanlık, Cumhurbaşkanlığı, Adalet Bakanlığı, Hazine Bakanlığı, Sayıştay, Merkez Bankası, Sermaye Piyasası Kurulu ve Tapu Kadastro Genel Müdürlüğü katılmıştır.

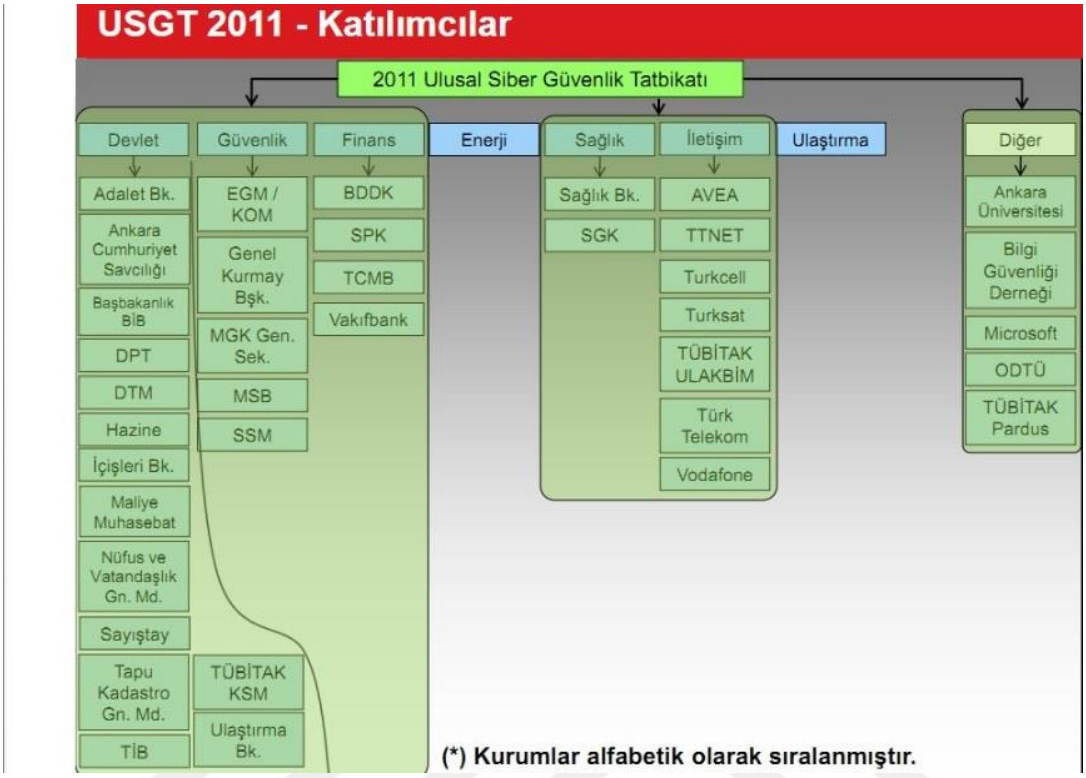
Tatbikatta alt konular ve asıl konular üzerinde durulmuş, yazı tabanlı ve gerçek saldırılar yapılmış kurum ve kuruluşların merkezi yapılarına gerçekleşmiş kurum içi ve kurumlar arasında gerçekleşmiştir. Tatbikat TUBİTAK, BİLGEM ve BTK iş birliği ve koordinasyonunda 30 kurum ve kuruluşun katılımı ile 25-28 Ocak 2011 tarihinde yapılmıştır (Tatar, 2011: 15-17)

2.13.2. I. Ulusal Siber Güvenlik Tatbikatı 2011

Bu tatbikat ile zaman geçtikçe daha ciddi tehlike oluşturan siber saldırılara karşı hazır olunması gerektiği, kurumların bilgi sistemlerinin güvenliği açısından siber olaylara müdahale ve kurumlar arasında koordinasyonların yapılması, kurumlar arasındaki iletişimin artırılması siber güvenlik alanında bilgi ve tecrübelerin paylaşımlarının artırılarak ulusal olarak siber güvenlik bilincinin artırılması amaçlanmıştır.

Bu tatbikat; TUBİTAK, BİLGEM ve BTK'nın yanında 39 farklı kurumun katılması ile toplam 42 kurum ile yapılmıştır.

Tablo 4: 2011 Ulusal Siber Güvenlik Tatbikatına Katılan Kurumlar



(Tatar, 2011: 21)

Yapılan tatbikat ile gerçek olarak yapılan siber saldırılar kurum ve kuruluşların gönüllülük esasına göre gerçekleştirilirken, tatbikat içeriğindeki yazılı senaryolar tüm kurumlara karşı gerçekleştirilmiştir.

Tatbikattaki yazılı senaryolar ile:

-Kuruma ait resmi web sitesindeki içeriklerin izinsizce değiştirilmesi,

-Kuruma ait IP adresinden başka bir kuruma DDoS saldırılarının yapılması,

-Kuruma ait IP adresinden başka bir kuruma spam mesajların gönderilmesi,

-Kurumdan ayrılan personelin ayrılmadan veri tabanına zarar vermesi

-Kuruma ait verilere sistemlerde gezen solucanların yayılması,

-Telefon yoluyla kurumda çalışan personelden bilgi çalmaya çalışılması,

-Kurum çalışanlarının erişimi engellenen sitelere giriş yapmaya çalışması,

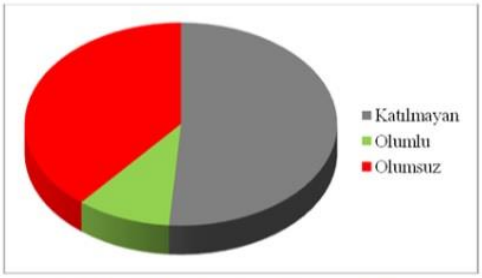
-İzinsiz kazı sebepleri ile interneti sağlayan fiber kabloların kopartılması,

-Sahte web sitesinden kuruma spam mesajlar gönderilmesi,

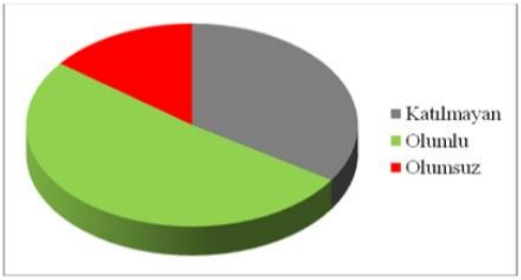
-Sistem odasında bulunan soğutma sistemlerinin arızalanması,

-Kurumun bulunduğu bölgede elektrik kesilmesi ve jeneratörlerin devreye girmemesi,

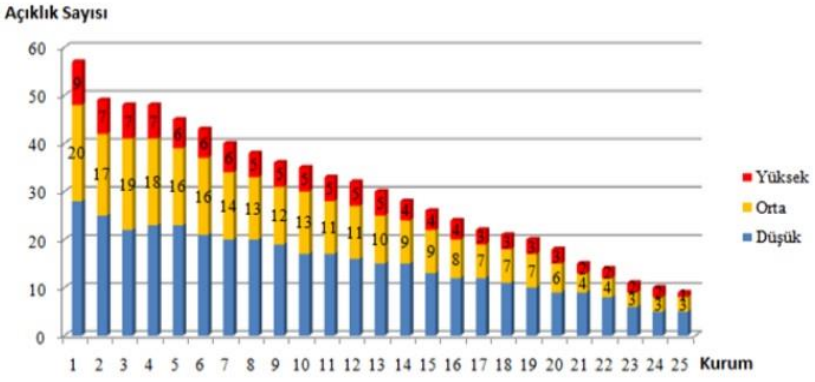
-Kurum içinde ismi kolaylıkla tespit edilecek bağlantı sağlanan kablosuz ağ erişim noktasının bulunması şeklinde saldırılar gerçekleştirilmiştir (Tatar, 2011: 19-25).



Dağıtık Servis Dışı Bırakma Saldırısının Sonuçları



Port Tarama Saldırısının Sonuçları



Grafik 1: 2011 Ulusal Siber Güvenlik Tatbikatı Sonuçları (Tatar, 2011: 25).

2.13.3. II.Ulusal Siber Güvenlik Tatbikatı 2013

25 Aralık 2012 tarihi ile 11 Ocak 2013 tarihleri arasında Ulaştırma, Denizcilik ve Haberleşme Bakanlığı kapsamında BTK ve TUBİTAK'ın katılımları ile gerçekleştirilmiştir.

Bu tatbikata 61 kurum ve kuruluşla birlikte 194 personel katılmıştır. 8 aşamadan oluşan tatbikatta 6 aşamada katılan kurumlara karşı gerçek saldırılar

yapılırken diğer 2 aşamada da yazılı senaryolar gerçekleştirilmiştir (https://www.bilisimdergisi.org.tr, 2023)**.**

2.13.4. Ulusal Siber Kalkan Tatbikatı 2021 ve 2022

Ulusal Siber Kalkan Tatbikatı 2021, 12-13 Ekim 2021 tarihlerinde gerçekleştirilmiştir. Bu tatbikata 36 kurum ve kuruluştan toplam 135 siber güvenlik uzmanı katılmıştır (https://www.btk.gov.tr, 2023).

Bu tatbikatın ardından Ulusal Siber Kalkan 2022 Tatbikatı 11-12 Ekim tarihlerinde 53 ekibin katılımı ile gerçekleştirilmiştir (https://www.cybermagonline.com, 2023).

Bu tatbikatlar da Ulaştırma Denizcilik ve Haberleşme Bakanlığı alt yapısında BTK çatısı altında USOM tarafından düzenlenmiştir. Tatbikatların sonucunda Türkiye'nin eskiye göre siber alanda daha başarılı ve güçlü olduğu anlaşılmıştır.

ÜÇÜNCÜ BÖLÜM

ÜLKELERİN SİBER GÜVENLİK POLİTİKALARI

Türkiye'de olduğu gibi diğer dünya ülkelerinde de siber güvenlik politikalarının gelişimi açısından çeşitli çalışmalar yapılmaktadır. Ülkeler birbirlerinin politikalarını inceleyerek, tatbikatlar ile siber güvenlik politikalarındaki açıkların tespitini yaparak yeni politika çalışmaları yapmaktadırlar. Bu bölümde siber güvenlik politikaları çalışmalarında Türkiye'ye yakın seviyede olan ve Türkiye'den daha güçlü politikalara sahip olan ülkeler incelenecektir.

3.1. Siber Güvenlik Açısından Ülkelerin Güç Sıralaması

Ülkelerin siber güvenliklerinin güç oranları ölçülürken tek bir etmen yerine yedi ayrı faktörü dikkate almak gerekir. Bu faktörler; yerel grupların incelenmesi, ulusal siber savunmaların geliştirilmesi, bilgi ortamının kontrolü ve yönetimi, ulusal siber güvenlik için istihbarat toplanması, siber alandan sağlanacak olan milli gelir, düşman siber saldırı gerçekleştiren birimlerin alt yapılarının ve sistemlerinin yok edilmesi veya devre dışı bırakılması, siber normların ve teknik standartların uluslararası tanımlanması faktörleri dikkate alınmalıdır.

Siber güç oranı yalnızca saldırı açısından değil, söz konusu siber saldırılara karşı savunma ve ona karşı gösterilen savunmanın güç oranı ile de ölçülmektedir. Çünkü gelebilecek saldırılar ne kadar çok engellenirse siber alandaki güç oranı daha yüksektir. Siber güvenliği geliştirirken siber güvenlik alanında ülkelerin kendi koydukları hedefler çok önemlidir.

Ülkelerin siber güç oranında sıralamasına bakıldığında; ABD siber güç olarak en başta yer almaktadır. Arkasından Çin ikinci sırada gelirken, İngiltere, Rusya, Hollanda, Fransa takip etmektedir. Türkiye dünya ülkeleri ile kıyaslandığında oldukça gerilerde yer almaktadır. Türkiye'nin gerisinde ise İran, Brezilya, Ukrayna ve Suudi Arabistan gibi ülkeler kalmaktadır.

3.2. Devletlerin Güncel Siber Güvenlik Politikaları

Dünya ülkelerinin güncel olarak siber güvenlik politikaları incelendiğinde ABD tüm dünya ülkelerine göre en güçlü siber güvenlik politikalarına sahip ülkedir.

Siber güvenlik politikalarının güç oranı, ülkelerin siber savunma ve siber saldırı oranlarına bakılarak belirlenmektedir.

3.2.1. ABD'nin Siber Güvenlik Politikaları

ABD, 2000'li yılların başına kadar siber güvenlik stratejisini kendi hegemonyasın devam ettirmek amaçlı olarak geliştirmiştir ancak 2000'li yıllardan sonra siber uzay doğrultusunda askeri güçlerin gelişmesi, Rusya'nın ve Çin'in siber alanda tehdit oluşturması, siber politikalarını geliştirmeleri ABD açısından tehdit oluşturduğu için ABD'de siber alanda askeri ve istihbari yeniliklere yönelmiştir.

ABD'nin siber güvenlik stratejilerinde ABD'nin hazırladığı sadece temel belgeler yoktur. Bu belgelerin yanında ABD'nin kendi kurumlarının kendi içlerinde yayımladıkları dokümanlar, askerlik ve güvenlik doktrinleri, bunlara ek olarak federal sistem sebebiyle her eyaletin kendi kurumlarına yönelik hazırladığı stratejiler, eyaletler için hazırlanan siber stratejik planlarda esas alınmıştır.

ABD siber güvenlik alanında stratejileri hazırlarken; kamu ve özel sektörün beraber hareket etmesini, siber uzay alanından gelebilecek saldırılara karşı kamu ve özel sektörün birlikte hareket etmesinin yanında; ortak kabiliyetlerin geliştirilmesi, ortak taktik ve planların yapılması ve uygulanması, siber uzay alanında özel sektörün görevlerini yerine getirme konusunda teşvik edilmesi, işveren, işçi kesimi ve toplumun siber saldırılar karşısında farkındalıklarının artırılması, eğitim ve oryantasyon faaliyetlerinin yapılması, Rusya ve Çin'in siber tehditleri karşısında ABD'nin bu tehditlere karşı engel olmak adına çalışmalar ve planlar yapılması, kritik alt yapıların belirlenmesi ve bunların dış siber saldırılara karşı korunması dikkate alınmıştır.

ABD siber güvenlik politikalarını oluştururken Ulusal Güvenlik Politikası ve Stratejisi, diğer stratejik belgeler, kanunlar, direktifler ve önerilen düzenlemeler siber güvenlik ile ilgili kurumlar ve son olarak düşünce üretim kuruluşlarının etkilerini dikkate almıştır (Göçoğlu ve Aydın, 2019: 238). Siber alanla ilgili olarak ilk çalışmalara 1930'lu yıllarda teknolojik hamleler yaparak başlamıştır. Bu yıllarda ENİGMA ismindeki kripto cihazına benzeyen SIGIBA isimli bir cihaz üretilmiş ve şifre çözmek adına çalışmalar yapılmıştır (Darıcılı, 2017: 3) Bir sonraki çalışma ise

1958 yılında kurulan İleri Araştırma Projeleri Ajansı'dır. Bu kuruluşun asıl amacı Sovyet Sosyalist Cumhuriyetler Birliği (SSCB) ile rekabet etmektir. Bu proje aynı zamanda internet tarihinin de başlangıcı olarak kabul edilmiştir ve ARPANET olarak adlandırılmıştır (Darıcılı, 2017: 4). ABD'nin internet sistemleri konusundaki güvenlik çalışmaları 1980'li yıllarda ARPANET'e yönelik virüs sızıntısı ile elektrik kesintisi olmuş ve bunun üzerine çalışmalara başlanmıştır. İlerleyen yıllarda tehditlerin artması ile askeri veri iletişimi için ABD Savunma Bakanlığı tarafından Militarynet (MİLNET) kurulmuştur.

ABD'ye karşı gerçekleştirilen ilk siber saldırı Soğuk Savaş yıllarında 1982'de gerçekleşmiştir. Rusya'nın, Kanada'dan doğal gaz boru hatlarının kontrolünü sağlayan yazılım çalma girişimi olmuştur. Bu girişim ABD tarafından fark edilerek yazılıma Truva atı yükleyerek tuzağa düşürülmüştür. Bu saldırı sonrasında yazılım bozulmuş ve doğalgaz akışı değiştiği için Sibirya Doğalgaz Boru Hattı üzerinde patlama meydana gelmiştir (Sertçelik, 2015: 31). Bu yıllarda siber savunma, siber saldırı, siber suç gibi kavramlardan çok bahsedilmezken gelişen teknoloji ve 11 Eylül saldırısı sonrası dikkate alınmaya başlamıştır. Soğuk savaş sonrasında ABD'de siber güvenlik konusunda kurumsallaşma, kurumsal alt yapı oluşmaya başlamıştır. Bu politikalar şekillenirken başkan direktifleri, siber stratejik planlar rol almıştır.

Siber güvenlik hakkında ilk resmi belge niteliğinde başkanlık direktifi 1995 yılında yayımlanmıştır. 1997'de ise yayımlanan ilk resmi doküman ile kritik alt yapıların tanımlamalarına yer verilmiştir.

1998'de siber saldırılara karşılık vererek ve alt yapıyı ilgilendiren tehditlerin bilgi koordinasyonu sağlaması amacıyla Ulusal Altyapı Koruma Merkezi (NIPC) kurulmuştur. Bu merkez FBI bünyesinde kurulduğu için ABD'nin siber tehdit algılamasının siber suçlara ve tehditlere yöneldiğini gösterir (Demirel, 2012: 91).

11 Eylül saldırısından sonra ABD'nin siber güvenlik algısında değişiklikler olmuştur. Bu saldırıdan sonra siber güvenlik ulusal güvenliğin bir parçası haline gelmiştir. ABD siber güvenlik konusunda üçlü bir yapıya sahiptir. Bu üçlü yapının içerisinde FBI ve DHS'de bulunmaktadır. Üçüncü yapı ise Savunma Bakanlığı'dır. Bu üçlü yapı ABD'nin siber güvenlik atılımlarını, uygulamalarını ve strateji

konusunda temel oluşturmakta ve kurumsal alt yapı özelliği taşımaktadır (Darıcılı, 2017: 7).

Savunma Bakanlığı bünyesinde siber güvenlik alanında faaliyet gösteren şifre çözme, veri analizi, karşı istihbarat gibi faaliyetlerde bulunan kurumlar vardır. Bunların yanında 1952 yılında kurulan Ulusal Güvenlik Ajansı (NSA) öne çıkmaktadır (Darıcılı, 2017: 8).

ABD'nin Savunma Bakanlığı siber uzayı bir savaş alanı olarak sınıflandırmış ve "Siber Uzay Hareketları için Ulusal Askeri Stratejisi" belgesi ile bunu resmi hale getirmiştir. Bu belgeye göre siber uzay elektromanyetik enerjinin kullanıldığı ağ sistemlerine meydana gelen fiziksel bir alandır. Bu alanda hareket serbestisi için ABD Hava Kuvvetleri Siber Komutanlığı, FBI siber güvenlik alanında faaliyet gösterirken istihbarat oluşturmak, casusluk faaliyetleri ile ilgilenmektedir. Görevlerini bu alan oluşturmaktadır. Siber güvenlik stratejileri oluşturulurken siber saldırılara karşı koyma görevi oluşturulmaktadır. FBI kapsamındaki birimler; "Siber Ulusal Güvenlik ve Siber Suç bölümleridir (Darıcılı, 2017: 10).

DHS ise terörle mücadele konusunda asıl yetkili kuruluştur. DHS'nin siber güvenlik konusundaki amaçları; siber güvenliğin ilerletilmesi, kritik alt yapıların korunması, kritik önemdeki kaynakların direncinin korunması, hükümetin iletişim gücünün sürdürülebilirliğini sağlamaktır. Bu birim 24 saat boyunca çalışmaktadır. DHS kapsamında siber güvenlik konusunda temel sorumluluğu geniş birim Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi'dir. Bunların yanında Ulusal Siber Güvenlik Koruma Sistemi de kullanılmaktadır (Darıcılı, 2017: 9).

ABD, siber güvenlik stratejisi bakımından ilk kapsamlı belge niteliği taşıyan 2003 tarihli Güvenli Siber Uzay belgesinin alt yapısını oluşturan Siber Uzay Güvenliği Ulusal Strateji Belgesi'dir. Bu belgede kritik alt yapılara olan saldırıların engellenmesi, saldırılara yönelik güvenlik açıklarının giderilmesi ve saldırıların yol açacağı zararların minimum hale getirilmesini amaçlamıştır (The National Cyber Space Strategy, 2003: 15). Beyaz Saray tarafından 2003 yılında çıkarılan "Secure Cyberspace" adına sahip olan bu belgede siber güvenlik kavramı sadece 3 kez geçmektedir. Siber güvenlik kavramının yerine genellikle siber uzay kavramı

kullanılmıştır. Bu belge siber uzayın korunmasında ulusal güvenliğin sağlanmasında önemli bir bileşen olarak görülmüş ve ulusal güvenliğin sağlanmasına yönelik ulusal strateji ile kritik alt yapıların ve değerli varlıkların fiziki olarak korunmasına yönelik ulusal strateji belgesinin uygulama bölümü olarak hazırlanmıştır.

Belge siber güvenlik konusuyla ilgili olan ulusal ve federal kurumların direktiflerin içermekte ve devlet ile yerel yönetim kurumlarının özel sektör firmalarının sivil toplum kuruşlarının ve vatandaşlarının kolektif siber güvenliği geliştirmekte üzere atacağı adımları belirlemektedir.

Secure Cyperspace belgesine göre; ulusal olarak siber güvenliğin sağlanmasında 5 adet öncelik bulunmaktadır. Bunlar;

-Ulusal bir siber uzay güvenliği karşılık sistemi,

-Ulusal bir siber uzay güvenliği tehdit ve güvenlik açığı savunma programı,

-Ulusal bir siber uzay güvenliği farkındalık ve geliştirme programı,

-Hükümetin siber uzayını güvenlik altında tutma,

-Ulusal güvenlik ve uluslararası siber uzay güvenliği iş birliğidir.

Siber Uzay Güvenliği Ulusal Strateji Belgesi ise ulusal olarak siber güvenliğin sağlanması saldırılara karşı cevap verilmesi için sekiz önemli eylem ve oluşabilecek siber saldırılara tehditlere karşı 8 önemli öncelik belirtmiştir (WH, 2003: 10). Söz konusu tehditlere karşı yapılacak eylemler;

-Kamu-özel iş birliği,

-Taktiksel ve stratejik analizler,

-Snaptik bir bakış açısı geliştirmek üzere özel sektör kapasite artırımı

Tablo 5: Siber Tehditlere Karşı Eylem ve Önlemler

Tehditlere Karşı Eylem	Tehditlere Karşı Önlem
Kamu-özel işbirliği.	Gerekli hukuki düzenlemeler.
Taktiksel ve stratejik analizler.	Güvenlik açıkları ve sonuç analizi.
Sinoptik bir bakış açısı geliştirmek üzere özel sektör kapasite artırımı.	internet mekanizmalarının güvenliğini sağlanması.
Siber uyarı ve bilgilendirme ağının genişletilmesi.	Güvenilir dijital kontrol ve veri güvenliği sistemlerinin kullanımının yaygınlaştırılması.
Ulusal olaylar yönetiminin geliştirilmesi.	Yazılım açıklarının önlenmesi.
Ulusal boyuttaki kamu-özel işbirliğinde gönüllü katılımı.	Siber ağlar ve iletişim sistemlerinin fiziksel güvenliklerini sağlamak.
Federal siber güvenlik planlarının yürütülmesi.	Federal siber güvenlik ar-ge kurumlarının önceliklendirilmesi.
Kamu-özel sektör arasındaki bilgi akışı ve paylaşımının geliştirilmesi.	Aciliyet sistemlerini değerlendirilmesi ve güvenliklerinin sağlanması.

(Göçoğlu ve Aydın, 2019: 239)

Bu belgede tablodaki önlem ve eylemlerin detaylandırmaları mevcuttur. Ulusal boyutta öne çıkan vurgu; kamu-özel sektör ve vatandaşlar siber alanlar hakkında yeterli bilgi ve donanıma sahip olması, koordineli şekilde güvenliğin sağlanması, iş birliği ve katılım, kritik alt yapıların korunmasına yönelik programların yapılması ve geliştirilmesidir.

Uluslararası boyutta Kuzey Amerika Güvenli Siber Uzayı'nı oluşturmak için Kanada ve Meksika ile yapılacak olan, siber tehdit ve risklere karşı ulaşım, enerji dağıtımı, iletişim, bankacılık gibi ortak kritik alt yapı korunmasına yönelik iş birliği yapmıştır. 2003 yılından sonra 2011, 2013 ve 2015 yıllarında da siber güvenliğe ilişkin belgeler yayımlamıştır.

2011 yılında yayımladığı siber güvenlik strateji belgesi 5 adet stratejik önceliklerden oluşmaktadır. Bu öncelikler;

-Savunma departmanının organizasyonel olarak geliştirilmesi,

-Yeni savunma içeriklerinin edinilmesi,

-Kamu-özel iş birliği,

-Diğer ülkelerle güçlü ilişkiler kurulması,

-Yaratıcılığın artırılmasıdır (DOD, 2011).

2013 yılında DOD, "Savunma departmanının ağları, sistemleri ve Bilgiyi Savunma Stratejisi" isimli bir belge yayımlamıştır. Bu belgede stratejinin asıl hedeflerine, 2011 yılındaki belgeye ek olarak savunmada esneklik, asimetrik, güvenlik tehditlerine karşı savunma ve bu amaca yönelik yeni savunma mekanizmalarının kurulması hedeflenmiştir. Aynı zamanda siber güvenlik sistemlerinin gelişmesi amacıyla kritik alt yapıların alt yapı şirketleri ile ve ortakları ile birlikte çalışarak belirlenen stratejileri izlemeleri konusunda talimat verilmiştir (Kara, 2013: 54).

2014 yılında ise Beyaz Saray Basın Ofisi ile AB arasında siber güvenlik iş birliği yapılmıştır (WHOPS, 2014). Bu iş birliği ile internet yönetişimi, internet özgürlüğü, siber uzayda insan haklarının korunmasına dair kanunlar işlenmiştir. İş birliği içeriği ise; uluslararası siber uzay gelişmeleri online insan hakları tanıtımı ve korunması, yürürlükteki uluslararası hukukun uygulanışı siber güvenlik ölçütlerini geliştirme, siber ortamdaki davranış normları gibi uluslararası güvenlik konuları, üçüncü taraf ülkelerde siber güvenlik kapasitesini geliştirmek gibi konuları barındırır.

2015 yılında Siber Strateji Belgesi yayımlanmıştır. Bu belgenin içeriğine göre yeni bir siber stratejinin yanında bu strateji için atılan adımlar belli olmuştur. Bu stratejiyi gerektiren 3 temel unsur vardır;

-ABD çıkarlarına, DOD ağlarına ve bilgi sistemlerine karşı devam eden kapsamlı saldırılar,

-Dönemin başkanı Obama'nın DoD'a diğer Birleşmiş Milletler (BM) ülkelerine birlikte hareket ederek siber saldırılar karşı savunma planları oluşturma düşüncesi,

-2012 yılından beri oluşturulan kurumun görevlerini yerine getirmek için operasyon yürütecek siber güvenlik güçlerinin oluşturulmasıdır.

Bu belge ile stratejik hedeflere ulaşılması için somut adımlar atıldığı ve siber saldırıları gerçekleştirenler haklarında hukuk yoluna başvurulması için emniyet güçlerine fazla yetkiler verilmesi için gelişmeler yaşanmış ve yeni tasarılar söz konusu olmuştur (https://www.bbc.com, 2023).

ABD yeni siber güvenlik stratejilerini hazırlarken oluşan yeni tehditleri göz önüne alarak hazırlamış, Rusya ve Çin'in siber casusluk faaliyetleri ABD için büyük bir tehdit haline gelmiştir (Darıcılı, 2017: 7).

2017 yılından itibaren Trump ile birlikte kritik altyapıların korunması için siber güvenlik alanına ciddi derecede yatırımlar yapılmıştır. Her bakanlık kendi siber güvenliğinden sorumludur (https://siberbulten.com, 2022).

2018 yılında imzalanan Ulusal Siber Güvenlik Stratejik Belgesi saldırgan nitelikte kabul edilmiştir. Çünkü söz konusu gerçekleşen saldırılara karşı daha güçlü saldırılar ile cevap verilmesi hedeflenmiştir. Siber suç işleyenlere karşı ihbar ve yaşsal işlemler bakımından daha etkili sistemler kurarak küresel üstünlük amaçlanmıştır. Bu belgede siber alanı; Amerikan halkı için ekonomi ve savunmadan ayrılmaz bir parça olarak kabul edilmiştir. Belge ile gelebilecek tehditleri en aza indirgemek, siber tehditlere karşı ulusal güvenliği sağlamak, ulusal saldırıları engellemek, kritik alt yapıları korumak, federal hükümetlerin bilgi sistemlerini korumak amaçlanmıştır (The Department of Homeland Security, 2018: 3).

Herhangi bir çatışma veya kriz anında bilgi toplamak ve askeri siber kapasiteyi artırmak için siber uzay operasyonları yapılacağından bu belgede bahsedilmiştir. Geleceğe yönelik plan ve stratejilerden güvenliğin şimdi ve gelecekte askeri siber kapasiteyi artırmak için sistemlerin ve ağın güçlendirilmesi hedeflenmiştir (The Department of Homeland Security, 2018: 1).

3.2.2. Rusya'nın Siber Güvenlik Politikaları

Soğuk Savaş dönemi ve sonrasında Rusya, 2000'li yılların sonrasında askeri alanda gücünü geliştirme çabalarına girmiştir. Sovyetler Birliği, soğuk savaş döneminde sahip olduğu teknoloji alt yapısı, nitelikli mühendislik gücünü Rusya'ya aktarmıştır. Bu da Rusya'nın kendisini askeri alanda geliştirmesini sağlamıştır. Tüm bunlar doğrultusunda Rusya'nın siber savunma ve saldırı alanında yaptığı yatırımlar,

istihbarat birimleri, bu birimlere bağlı olarak hareket eden siber suç örgütleri, ağ temelli askeri güçler hepsi bir arada değerlendirildiğinde Rusya küresel bir güç haline geldiği görülmektedir.

Rusya'nın siber güvenlik ana stratejilerini anlamak için Rusya'nın gayri resmi savaş doktrinini anlamak gerekmektedir. Bu doktrin "hibrit savaş" veya "bulanık savaş" olarak adlandırılan "Gerasimov Doktrini" ele alınmalıdır. Bu doktrine göre; askeri müdahale öncesinde devlete karşı siber saldırılar ile hedefin yıpratılması, psikolojik olarak etkileyecek ve düşürerek amaçlanan hedefe ulaşılır.

Rusya siber güvenlik alanında ABD'ye nazaran daha erken çalışmalara başlamıştır. Siber güvenlikle alakalı çalışmalar 2000 yılında başladığı Uluslararası İletişim Birliği ile belirtilmiştir. Bu belgeler (https://www.itu.int, 2023);

-Rusya Federasyonu Bilgi Güvenliği Doktorini, (Topçu, 2022: 22),

-Uluslararası Bilgi Güvenliğinde Rusya Federasyonu Devlet Politikası Temel Prensipler Belgesi (2013 ve 2020 için ayrı ayrı 2 adet) ve taslak halinde olan Rusya Siber Güvenlik Stratejisi (RSG, t,y) belgesidir.

2000 yılındaki ilk belge (RFBGD, 2000) bilginin toplanması, bilgi ve iletişim teknolojileri, internet siteleri, iletişim ağları, bilgi işlem aşamaları, teknolojilerin geliştirilmesi ve siber alanda güvenliklerin sağlanmasını konu almaktadır. Belgenin asıl amacı ülke çıkarlarını iç ve dış tehditlere karşı korumak ve sürekli olarak gelişimini sağlamaktır. Bilgi güvenliğini sağlarken, istihbarat bilim ve teknoloji, bilgi analizi, insani ve ekonomik kaynakların, bilgiye karşı tehditlerin tespiti, belirlenmesi ve önüne geçilmesi hedeflenerek zararlı sonuçların yok edilmesi amaçlanır. Bilgi güvenliğini sağlamak için devlet kurumları, özel kurumlar, askeri kurumlar eş zamanlı ve koordineli olarak çalışmaları sağlanacaktır (RSG, 2000: 21). Dışarıdan gelecek saldırılara karşı istihbarat ağının güçlendirilmesi ve güvenliğin artırılması hedeflenmiştir. Bu belgede yerli sistemlerin ve teknolojilerin geliştirilmesi konusunda yapılan çalışmaların insani kaynağının yeterli olmadığı saptanmıştır (RSG, 2000: 24). Ülkelerin bilgi teknolojilerinin kaydettikleri gelişmelerde siber uzaydaki hakimiyet artarak, bu alanda baskın olmak için çalışmalar artırılmalı, yerli

üretim teknolojiler kullanılmalıdır. Eksikliklerin tespit edilerek bu eksiklikler üzerine çalışmalar yapılmalıdır (Topçu, 2022: 25).

Uluslararası Bilgi Güvenliği'nde Rusya Federasyonu Devlet Politikası Temel Prensipler Belgesi ele alındığında siber güvenlik kapsamında daha yakın bir belge olduğu düşünülmektedir. Bu belge uluslararası hedefleri belirtmekte, temel prensiplere göre federal kurumlar ve ulusal anlamda gerçekleştirilen federe hükümetler ile Rusya'nın uluslararası bilgi güvenliğini sağlamak üzere hükümetler arası hedef planlarını, konuyla ilgili hukuki ve örgütsel fonksiyonlarını dâhil ederek daha sağlam uluslararası bilgi güvenliği sistemi oluşturulduğu tespit edilmiştir. Stratejik belgelerin etkili şekilde uygulanması için kurumlar arası iş birliği, reel ekonomide ve bilgi teknolojilerini ileri düzeyde kullanan devletler ile Rusya'nın eşitlenmesi hedeflenmiştir.

Rusya'nın siber güvenlik stratejisi olarak ortaya çıkan başka bir hedef ise ABD'nin sahip olduğu küresel hegemonyayı yıkmak için kendi ulusal yazılım ve donanımları geliştirmeye çalışmasıdır. Yerli teknolojiler ve yerli sosyal medya kullanımı teşviki bunlara örnektir. Ayrıca yoğun şekilde internet denetimi söz konusudur.

2000 yılındaki belgeye göre bilgi güvenliği açısından daha kapsamlıdır ve daha geniş tanımlamalara yer verilmiştir. Bu belgede uluslararası bilgi güvenliği kavramı; bireysel hakların gasp edilme ihtimali göz önüne alınarak; bireysel, toplumsal ve ülkesel bilgi alanına karşı tehditlerin kritik alt yapıların üzerindeki yıkıcı ve kanuni olmayan etkilerini önlemek adına çıkarılan durumdur. Bu belge ile hedefle ulaşmak için araç olarak kullanılan kurumlar federal yönetim organları olarak gösterilmiştir. Bu organlar kamu-özel iş birliği içinde çalışacaktır. Federasyonun güvenlik konseyi yönetim arasındaki koordinasyonu sağlayacak yönlendirici birim olarak görülmüştür. Rusya'nın siber güvenlik anlayışı savunmadan ziyade saldırı odaklıdır. Savunma anlayışı olarak yapılacak yatırımların daha dikkatli olarak yapılması ve rakiplerin düşman olarak görülmesi, saldırılara saldırı ile karşılık vermek üzere stratejiler benimsemişlerdir.

Rusya'nın siber güvenliğine karşı tutumunu belirleyen iki temel kavram vardır; Ulusal internet ve ülke egemenliğine karşı siber uzaydan gelecek herhangi bir tehdit potansiyeline karşı katı koruma olarak 2 ye ayrılmıştır (Göçoğlu ve Aydın, 2019: 245).

Rusya günümüzde siber espiyonaj, siber kontrespiyonaj, dezenformasyon, elektronik savaş, siber saldırı gibi faaliyetleri kapsayan geniş ve büyük bir siber güç olma yönünde ilerlemektedir. Böylece etken bir siber güce ulaşarak siber uzayın sağladığı imkân ve fırsatlardan dış politikalardaki baskınlıkla başa çıkmayı hedeflemektedir. Bu amaçlar doğrultusunda da Estonya'ya, Gürcistan'a, Litvanya'ya DDoS saldırıları gerçekleştirmiştir. Putin başkan olmasının ardından askeri ve ekonomik kapasitesini artırmayı hedeflemektedir. Bu hedefler doğrultusunda küresel düzeyde etkin olmak amacıyla yeni stratejiler geliştirmektedir.

3.2.3. Çin'in Siber Güvenlik Politikaları

Çin'in siber güvenlik alanındaki çalışmaları bilgi teknolojilerinin ilk ortaya çıkması ile başlamıştır. 1986 yılında ilk olarak ekonomik verilen yönetimine dair grup kurulmuştur. İlk sivil belge olan Belge 27 yayımlanmıştır. Bu belge ile kritik alt yapıların korunması, gelişimi destekleme, gözlemleme, devlet ve kurumların iş birliği içinde çalışarak siber güvenlik politikalarını yönlendirmeyi amaçlamıştır (Raud, 2016: 11). Siber güvenlik alanında yapılan kurumsal ve hukuki çalışmalar 2014 yılının biraz öncesinde yapılmaya başlamıştır. 2014 yılından önce yapılan düzenlemeler ile siber güvenliğe ve sistemsel alt yapıların önemine odaklanıp devlet tarafından bilgi güvenliği konseyi oluşturulmuştur.

2014 yılında Çin devlet başkanı Xi Jinping; siber güvenlik grubunu kurmuş ve yapılan çalışmalara hükümet raporda yer vermiştir.

2015 yılında Çin'in ulusal kongresi olan NPC'de (Standing Committee of the National Peoples Congress)'de halkın görüşü alınarak Siber Güvenlik Kanunu tasarısı oluşturulmuştur. Tasarı 2016 yılında yayımlanmıştır (Göçoğlu ve Aydın, 2019: 244).

Bu tasarı 2017 yılından itibaren yürürlüğe girmiş ve uygulanmaya başlamıştır. Kanun 7 bölüm ve 76 maddeden oluşmaktadır. İlk 2 bölümde siber

güvenlik hakkında temel prensipler ve stratejiler hakkında bilgi verilmektedir. 3. Bölümde ilgili kurum ve kuruluşların sağlaması gereken siber güvenlik şartları, 4. Bölümde bilgi güvenliği konuları, 5. Bölümde ağların izlenmesi ve tehlikeler karşısında neler yapılması gerektiği, 6. Bölümde ise kuralların ihlal edilmesi halindeki yaptırımlara yer verilmiştir. Son bölümde ise tanımlamalar ve ek bilgiler vardır.

Çin nüfusu sebebi ile dünyanın en geniş siber güvenlik uzman topluluğunu elinde bulundurmaktadır. ABD ve Rusya gibi siber uzay alanında söz sahibi, küresel siber güç konumunda bulunmaktadır. Çin sahip olduğu kapasitesini, iç güvenliğinin istikrarının korunması doğrultusunda öncelikle savunma ve ardından özellikle siber espiyonaj operasyonları dahilinde saldırı amacıyla dizayn etmeye çalışmaktadır. Bu kapsamda Çin'in siber güvenlik stratejisinin temelinde ekonomik, politik ve askeri hedefleri vardır.

Çin'in siber güvenlik alanında belirlediği hedefleri kısa şöyle maddelendirebiliriz;

-Ekonomik olarak büyüme ve istikrarın sürekli olarak sağlanabilmesi için yeni nesil teknolojilerin siber espiyonaj operasyonları kapsamında temin edilmesi,

-Çin Komünist Partisi'nin ülke yönetimindeki devamlılığın sağlanması için ülke içindeki internetin sürekli olarak denetlenmesi, toplumsal ayaklanmaların engellenmesi,

-Ağ teknolojileri merkezli savaş planlarına karşı tedbirler sağlanması, ülkelerin iç işlerine yönelik faaliyetlere karşı korunması,

-Yabancı istihbaratların Çin aleyhine yaptığı çalışmaları tespit edici çalışmalar yapılması,

-Yeni nesil siber teknoloji alanında askeri kapasitenin desteklenmesi, düşman birimlerin kritik alt yapılarına karşı planlar yapılması,

-Hedef bölgedeki ülkelere karşı siber stratejiler ve siber saldırıların faaliyetlerinin belirlenmesi,

-Çin'de Rusya gibi kendi hegemonyasını oluşturmaya çalışmakta, yerli ve milli uygulamaları, yazılımları ve teknolojileri geliştirme çabasındadır.

Gelişen teknoloji sebebiyle ülke genelinde internet, bilgi ve iletişim teknolojilerinin kullanımının artması ülkede siber suçlar ve internet ağına yapılan siber saldırılarda artmıştır. Bu ortam siber saldırılar sonrasında 350.000 üzerinde insan olumsuz olarak etkilenmiştir ve Çin bu sebeple siber güvenlik kavramına öncelik vermiştir (Symantec, 2018).

Çin'de diğer ülkeler gibi devlet açısından siber güvenliği önemli kılan konuları ele almıştır. Yapılan siber saldırılar ile ülkenin kritik alt yapılarına zarar verilmesi, internetin ve bilginin ve her türlü sanal dosyanın toplum düzenine, ekonomik gelişim sürecine bireysel mülkiyet hakkına, askeri yapıya zarar vermek amacıyla kullanılmaktadır (Swaine, 2013: 3). Çin'in uygulandığı siber güvenlik politikası bazı yönleri ile batı ülkelerinden ayrılmaktadır. Çin; kendisine ait bilişim teknolojilerini üretmektedir. Böylece diğer ülkelerden uzak durmaktadır. Politikası oluştururken bağımsız internet teknolojisini savunmuştur. Yerli üretim yapan teknoloji firmalarına yeterli miktarda destek olmalıdır. Buna örnek olarak Çin'in kendi ürettiği akıllı telefonlar ve bu telefonlar özel uygulamalar, indirme mağazaları örnek verilebilir.

Ülke içinde küresel boyutta dış ülkeler tarafından üretilen uygulamalara kullanım açısından sınırlar ve sansürler uygulanmaktadır. Bunların sebebi ise ülke içi ve dışına veri-bilgi sızdırılmasının önüne geçilmesi içindir. Tüm bu önlemlere rağmen Çin'in ülke kapsamında korsan yazılım kullanımı ve üretimin yaygınlığı çok fazladır. Bu da ülkenin siber güvenliğini tehdit etmektedir (Gierow, 2015: 5).

Çin'in siber güvenlik alanında geliştirdiği politikalar sadece savunmaya yönelik değildir. ABD'ye karşı yaptığı saldırılar ABD'de büyük sorunlara yol açmıştır. Bunun yanında Almanya ve Tayvan'ın da içinde olduğu 103 ülke saldırılara ciddi derecede etkilenmiştir.

3.2.4. Hindistan'ın Siber Güvenlik Politikaları

Hindistan siber güvenlik alanında Türkiye gibi gelişmekte olan ülkeler arasında yer almaktadır. Nüfusunun kalabalık olmasından ötürü ve dünyadaki yeri açısından stratejik olarak önemli bir konuma sahiptir. Durum böyle olunca da siber alanda tehditlere karşı açık bir ülke halindedir. Siber güvenlik alanında yaptığı çalışmaların yetersiz ve düzensiz olması sebebiyle siber alanda savunmasız bir haldedir.

Siber güvenlik alanında çalışmalar yapmaya 2000'li yılların başında başlamış ve Bilgi Teknoloji Yasası'nı çıkarmıştır ancak yetersiz kalmıştır. Bu gelişmenin ardından 2012 ve 2013 yıllarında iki ayrı Ulusal Siber Güvenlik Politikası yayımlamıştır.

Hindistan'ın siber güvenlik alanındaki sorumlusu Gulshan Rai'nin 2017 temmuz ayında yaptığı açıklamalarda siber tehditlerin 2000'li yıllarından başından bu zamana kadar değiştiğini, daha ciddi bir hal aldığını, söz konusu tehditler ile ağır saldırılar gerçekleştiği, bu saldırıların ilk ve ana hedeflerinin devlet olduğu, devletin unsurlarının, bankacılık hizmetlerinin, enerji hizmetlerinin, iletişim ve Telekominasyon hizmetlerinin, ülkenin savunma birimlerinin sürekli olarak hedef halinde olduğunu ve bu sebeple siber güvenlik alanında yeterli ve gelişmiş politikalar hazırlanması için ülke ekonomisinden ciddi derecede bütçeler ayrıldığını belirtmiştir.

2000 yılında Bilgi Teknolojisi Kanunu (Information Technology Act) çıkarılmıştır. Bu kanun ile ülkeye gerçekleşmesi muhtemel olan hacker saldırıları, bilişim ve veri sistemlerine karşı saldırılar, sistem açıkları, güvenlik ihlalleri karşısında mücadele etmek için siber savunma alt yapıları oluşturulmuştur. Ülkenin kritik alt yapılarını doğrudan ve dolaylı olarak etkileyen sistemlerin korunması hedeflenmiştir. Bu hedef doğrultusunda CERT-In siber savunma ve siber saldırılara karşı müdahale yapması için görevlendirilmiştir (Durna, 2012: 6).

Ülkenin bilişim sistemlerinin ve bilgi güvenliğinin sağlanması ve önlem alınması için Hindistan Devleti Bölümlerarası Bilgi Güvenliği Görev Gücü (Inter Departmental Information Security Task Force-ISTF) kurulmuştur. Bu kuruluş Ulusal Güvenlik Konseyi (National Security Council) ile birlikte çalışması

yetkilendirilmiştir (Alioğlu, 2019: 106). Bu yetkilendirme sonrasında Ulusal Siber Güvenlik Politikası oluşturulmuştur. Politikanın oluşturulmasının ardından ülkenin bilgi ve veri güvenliğinin sağlanması için mevzuatlar hazırlanarak siber güvenlik alanında bilgilendirmenin halkın bu alanda farkındalığının artırılması, siber güvenlik alanında çalışacak olan personellerin ve birimlerin yetkinliklerinin artırılması, Ar-Ge çalışmalarının yapılması istenmiştir. Bu kapsamda üniversiteler ve özel sektörler ortak çalışmalar yürütmüştür. Bilgi Güvenliği Çerçeve Politikası hazırlanarak; ülkenin ağları ve kritik altyapılarının korunması amaçlanmıştır (Lewis ve Timlin, 2011: 28).

Ülkenin, Savunma Bakanlığı bünyesinden siber güvenlikle alakalı güvenliği sağlamak için birçok birim bulunmaktadır. Bu birimler;

-Savunma Bilişim Savaş Ajansı (The Defence Information Warfare Agency); siber alandaki bilgi savaşlarını koordine eder.

-Savunma İstihbarat Ajansı (The Defence Intelligence Agency) ve Ulusal Teknik İstihbarat İletişim Merkezi (National Technical İntelligence Communication Centre) ise devleti olası siber alandaki oluşan güvenlik açıklarına karşı gerçekleşecek olan tehdit ve saldırılara karşı uyarma ile görevlidir (Darıcılı, 2017: 18).

Hint Ordusu tarafından 2005 yılında; ülkenin şebekelerinin bölünmesini engellemek ve bu şebekelerin denetimlerini sağlamak için Siber Güvenlik Kuruluşu (Cyber Security Establishment)'i kurmuştur. Yine ordu 2010 yılının Nisan ayında ise Siber Güvenlik Laboratuvarı'nı, Telekomünikasyon Mühendisliği Askeri Koleji'nde açmıştır (Lewis ve Timlin, 2011: 32).

Ocak 2004 yılında Hindistan Acil Bilgisayar Müdahale Ekibi (Indian Computer Emergency Responce Team – CERT-In), Bilgi Teknolojileri Departmanı bünyesinde kurulmuştur. Kurulan bu ekibin amacı ise bilgisayar içeriklerine karşı gerçekleşen saldırılara anında müdahale etmektir. Aynı zamanda bu ekip devlete ait kritik altyapıların korunmasından, verilerin çalınmasının önüne geçilmesinden, kısacası tüm siber güvenlik alanındaki faaliyetlerden sorumludur. Bu ekip 2010 yılında Siber Saldırılar ve Siber Terörizme Karşı Kriz Yönetimi Planı oluşturmuştur. Yapılan çalışmalar ile siber olay gerçekleşmeden belirli risk parametreleri ile siber

olay önceden tespit edilerek saldırı gerçekleşmeden ya da gerçekleşirken bu saldırı için korunma sistemleri ile siber saldırıyı engeller.

Hindistan tüm bu gelişmelerin yanında Ulusal Güvenlik Veri Tabanı (National Security Database-NSD) adıyla bir kuruluş kurmuş ve himayesinde siber güvenlik alanında çalışacak, kritik altyapıların ve hükümete ait bilişim sistemlerinin korunması için çalışacak siber güvenlik uzmanlarını belirlemiştir. Bu oluşum sayesinde siber güvenlik alanında yetkin, uzman personeller yetiştirmeyi hedefleyerek, insan tarafından oluşabilecek hataların en aza indirgenmesi hedeflenmiştir (Çeliktaş, 2018: 474).

2013 yılında yayımlanan Ulusal Siber Güvenlik Politikası (National Cyber Security Policy) isimli politika Hindistan'ın ilk ve tek ulusal strateji belgesidir. Bu strateji belgesi ile siber güvenlik ve devlet stratejileri birleştirilmiştir. Belge ile siber alanda çerçeve ve ilkeler belirlenmiştir. Belgenin amacı ülkede güvenli siber alanda güvenli bir eko sistem oluşturmaktır. Bu stratejik belge ile çeşitli uygulamalar yapılmıştır (Alioğlu, 2019: 164).

-2015 yılında Birlik Eletronik ve Bilgi Teknolojisi Bakanlığı (MEITY) kapsamında Hindistan Bilgisayar Olaylarına Acil Müdahale Timi (Indian Computer Emergency Response Team (CERT-In)'e bağlı olarak kurulmuş olup; siber güvenlik tehditlerinin tespiti ve ülkenin internetini tamamen taramaktır (Alioğlu, 2019: 166)

-Ulusal Siber Koordinasyon Merkezi (NCCC) ile ülke kapsamındaki hacker ve casus yazılımlar karşısında siber güvenliğin sağlanması hedeflenmiştir ve siber alanda gelişmiş olan ABD, Rusya ve Çin gibi ülkelerin siber güvenlik düzeylerine yaklaşmak hedeflenmiştir (Alioğlu, 2019: 166)

-Botnet Temizleme ve Kötü Amaçlı Yazılım Analiz Merkezi (Cyber Swachhta Kendra Projesi) ile internet ortamındaki botnetlerden tarafından oluşabilecek tehditler ve saldırıları engellemek amaçlanmıştır. Bu uygulama Dijital Hindistan girişiminin bir parçasını oluşturmaktadır (Alioğlu, 2019: 167). Bu belge kapsamında Merkezi İzleme Sistemi (Central Monitoring System-CMS) kurulmuştur.

-Ulusal Kritik Bilgi Altyapı Koruma Merkezi (NCIIPC) kurularak, kritik altyapı sektörlerini koruyan diğer güvenlik kurumları ile iş birliği içinde çalışarak siber güvenlik alanında önlemler alınması hedeflenmiştir (Alioğlu, 2019: 168).

-Ülke bünyesinde kurulan CERT'ler ile kendi idaresi kapsamındaki siber saldırıları önlemek ve saldırılar karşısında gerekli önlemleri almaları hedeflenmiştir.

-Şebeke Güvenliği Uzman Sistemi (Grid Security Expert System (GSES) kurulmuştur. Bu kuruluş ile otomatik savunma mekanizmaları geliştirilmiştir.

-Siber saldırılar ve siber teröre karşı Kriz Yönetim Planı (CMP) hazırlanmıştır. Gerçekleşen saldırılar sonrasında ulusal düzeyde etki oluşturan saldırıların sonuçları hafifletmek ve oluşan zararları iyileştirmek amaçlanmıştır.

-Ağ üzerindeki siber saldırıları ve siber faaliyetleri izlemek için Ağ Trafiği Analizi Sistemi (Network Traffic Analysis System-NeTRA) kurulmuştur (Alioğlu, 2019: 167-168).

3.2.5. İngiltere'nin Siber Güvenlik Politikaları

Siber güvenlik alanında dünya ülkelerinin başında yer alan ülkelerden birisi de İngiltere'dir. İngiltere siber güvenlik alanındaki çalışmalarına bilişim alanındaki 1990 yılında yaptığı hukuksal düzenleme ile çıkarılan "Bilgisayarların Kötüye Kullanılması Yasası" ile adım atmıştır. Söz konusu kanun ile bilgisayarlardaki yazılımların, verilerin kötüye kullanılması, böylece bilişim alanında suçların işlenmesi ve suç işlenmesinin kolaylaştırılması, bilgisayara izinsiz olarak erişim sağlama ve söz konusu verilerin çalınması ya da değiştirilmesi bu suçlara dâhil edilmiştir. 1990 yılından sonra 1998 yılında Veri Koruma Yasası çıkarılmıştır (Alioğlu, 2019: 105).

Tüm bu gelişmelerin ardından 2009 yılında ilk siber güvenlik stratejisi niteliğinde olan "Siber Güvenlik Stratejisi Birleşik Krallık Güvenlik, Güvenlik ve Siber Alandaki Dayanıklılık (Cyber Security Strategy Of The United Kingdom Safety, Security and Resilince İn Cyber Space) isimli belge, kraliçenin emri ile çıkarılmıştır (Cyber Security Strategy of The United Kingdom Safety, Security and Resilince İn Cyber Space, Cabinet Office, 2009). Suç örgütleri ile diğer düşman ülkelere karşı savunma planlarını içeren ilk belge niteliğindendir. Bu belge ile

hükümetin, şirketlerin ve kişilerin siber saldırılar karşısında risklerin söz konusu olduğunu, bu sebeple daha kapsamlı olarak hazırlanan Ulusal Siber Güvenlik stratejisi ile beraber yayımlanmıştır. Çıkarılan bu belge içeriğinde, siber uzay alanında güvenliliğin ve dayanıklılığının sağlanması, siber uzay alanındaki imkânlar, sadece hükümeti koruma amaçlı değil vatandaşlarında korunacağını, olası kimlik hırsızlığı ve siber alanda işlenen suçlara karşı korumanın nasıl yapılacağından bahsetmektedir. Teknolojinin gelişmesi, internetin yoğun olarak kullanılması ile siber saldırıların çeşitliliğinin artması hakkında uyarılar içermektedir. Belgenin yanında ek olarak siber alanın devlet veya terör gruplarının suç amaçlı kullanılabileceğinden tehditler söz konusu olacağı, bu sebeple siber Siber Suç Stratejisi yayımlanacağından bahsetmiştir (Kınıkoğlu, 2012: 29)

İngiltere 2010 yılında Ulusal Güvenlik Stratejisi (A Strong Britain in an Age of Uncertainty: The National Security Strategy) ve Stratejik Savunma ve Güvenlik Gözden Geçirmesi (The Strategic Defence and Security Britain İn A Age Of Uncertanity) isimli belgeleri ile 5 yıllık süre kapsamında stratejik planlardan, alınması gereken önlemlerden bahsetmiştir (The National Security Strategy, 2010). Bu belge ile siber alanda önlem alınması gereken, güvenliğin asıl önemli olduğu 4 temel ögeden bahsedilmiştir. Bu ögeler; devlet, organize suç örgütleri, terörist gruplar ve bu gruplar tarafından gerçekleştirilecek saldırılar olarak belirlenmiştir (The National Security Strategy, 2010). Ülkenin ulusal olarak siber güvenlik alanında risk kontrollerinin 2 yılda bir yapılması gerektiğini, yapılacak kontrollerin ise 3 kategori kapsamında toplamda 15 risk faktörü göz önünde bulundurularak yapılmasını belirtmiştir (Alioğlu, 2019: 107)

Birinci kategorideki risklerin ülkenin bilişim sistemlerine gelecek olan saldırıların tamamı olarak değerlendirilmiştir. Bu saldırıların gerçekleşme ve etki alanlarının büyüklüğü sebebi ile ulusal güvenliğin tehdit altında olabileceği, öncelik gösterilmesi gerektiği belirtilmiştir. Ülkeye karşı gerçekleşebilecek tüm siber saldırılar büyük risk grubuna dâhil edilmiştir.

İngiltere'nin yayımladığı Ulusal Güvenlik Strateji raporunda, ülkeye birçok ülkeden gerçekleşen siber saldırılar olduğunu, siber güvenlik meselesinin ülkenin en

büyük ulusal güvenlik meselesi haline geldiğini, ulusal güvenlik riskleri olarak değerlendirilmesi gerektiğini özellikle belirtmiştir (Kınıkoğlu, 2012: 30).

Yayınlanan raporun ardından siber güvenlik alanındaki çalışmaları, faaliyetleri koordine etmek, stratejilerin belirlenmesi, geliştirilmesi için Siber Güvenlik Ofisi kurulmuştur. Siber Güvenlik Ofisi kurulduktan sonra ülke genelinde siber alanda liderlik sağlamak ve ülkenin siber güvenlik stratejisinin dağılımını sağlamak için İç İşleri Bakanlığı ile ortak olarak çalışmalar yürütmeye başlamıştır (Cyber Crime Strategy, 2010: 27).

Siber Güvenlik Ofisi ile ülkenin stratejik planlar hazırlanırken değişen tehditlere karşı hazırlıklı olmak, siber suç stratejilerini geliştirmek, siber alanda sürekli gelişim içinde olmak amaçlanmıştır. Yapılan çalışmalar ise İç İşleri Bakanlığı'nın 6 ayda bir olmak gözetiminden geçeceği belirtilmiştir. Kurulan siber güvenlik ofisi ve hazırlanan stratejik belgeler ile İç İşleri Bakanlığı'nın siber olaylar karşısında ve siber güvenlik politikaları alanına ne kadar önem verdiği görülmektedir (Cyber Crime Strategy, 2010: 28).

2011 yılının Kasım ayında İngiltere yeni bir strateji belgesi yayımlamıştır. "Birleşik Krallık Siber Güvenlik Stratejisi: Dijitalleşen Dünya'ya Birleşik Krallığı Taşımak ve Korumak" isimli bu belge ile Ulusal Siber Güvenlik Programı, siber güvenlik stratejileri ve ayrıntıları belirtmiştir. Ulusal Siber Güvenlik Programı ile siber güvenlik alanında köklü değişikliklere gidilmiştir. Siber güvenlik için birçok yeni kurum oluşturulması hedeflenmiş, siber güvenlik için ayrılan bütçenin istihbarat ve güvenlik kurumlarına paylaştırılmıştır (Alioğlu, 2019: 109).

Yayımlanan strateji belgesi ile siber alandaki bağımlığın artması ile yeni tehditlerin ortaya çıkacağından bahsedilmiştir. Söz konusu tehditler ile kritik alt yapılara ve veri sistemlerine zarar vermek isteyenlerin açık hedefi haline geleceği, bu hedeflerin saldırılarından korunmak için nasıl savunma yapılacağından bahsedilmiştir.

Yayımlanan strateji belgesi ile 4 temel hedef belirlenmiş ve bu hedefler bahsedilmiştir. İlk hedef olarak siber suçlarla mücadele etmek ve siber alanında yapılan çalışmalar ile dünyanın en güvenli siber alanı oluşturmaktır. İkinci hedef,

siber saldırılara karşı dayanıklı olmak, karşı koymak ve siber alan karşısında görüşlerin değişmeden insanların ilgisini korumaktır. Üçüncü hedef ise ülke vatandaşlarının siber alanı güven içinde sağlıklı bir şekilde koruması, son hedef ise siber alandaki çalışmalar açısından yeterli düzeyde bilgi ve beceriye sahip olunmasıdır (Cyber Crime Strategy: 2010: 21).

Siber saldırılar karşısında ülkenin korunması gerekmektedir. Siber güvenliğin tam anlamıyla sağlanabilmesi için belirli koruma aşamaları söz konusudur. Ülkenin birlik ve beraberliğinin bozulmadan, kritik alt yapılara karşı saldırıların engellenmesi için siber saldırılar karşısında devlet ve devlet kurumları ilk olarak korunması gereken birimlerdir. Sonraki korunması gereken birim siber alanda içerisinde bulunan özel kurumlardır. Son olarak korunması gereken birim ise halktır.

İngiltere, Siber Güvenlik Stratejisi raporundan sonra internetin gelişimi, internetin kullanımının artması sonrası yaptığı incelemelerde; söz konusu siber tehditlerin değiştiğini, geliştiğini tespit etmiştir. Bu tehditleri 4 ayrı sınıfa ayırmıştır. İlk sınıfta bilişim ve bilgi sistemlerine yönelik tehditler, ikinci sınıfta devlete yönelik tehditler, üçüncü ve dördüncü sınıfı ise kamu kurumlarına ve özel kurumlara yönelik saldırıları gerçekleştiren Hacker gruplarına ayırmıştır (Kınıkoğlu, 2012: 30-32).

İngiltere'nin yayımladığı strateji belgesinde 4 temel hedeften bahsedilmiştir. Bu hedeflere ulaşabilmek için; halkın siber tehditler karşısında korunmayı bilmesi, şifrelerini koruması, kişisel verilerini güvenli şekilde aktarmasını bilmesi gerekmektedir. Özel sektörün; söz konusu tehditlerden haberdar olması, ticari bilgilerini, kişisel verilerini saklaması, siber alandaki tehditlere karşı yeterli düzeyde siber güvenlik önlemleri alması için çalışmalar yapması ve yatırımlar yapması gerekmektedir. Son olarak devletin üstüne düşen görev ise; yüksek derecedeki siber tehditlerin tespit edilebilmesi, kritik alt yapılarda ve devlete ait sistemlerdeki güvenlik önlemlerinin artırılması, siber alandaki kolluk kuvvetlerinin güçlendirilmesi ve bu siber tehditlerle mücadele edebilmesi gerekmektedir (The UK Cyber Security Strategy: Protecting and Promoting The UK in a Digital World, 2011: 22-23).

İngiltere, Savunma Strateji Belgesi ile askeri alanda çalışması planlanan iki temel merkez kurmayı hedeflemiştir. Silahlı kuvvetler bünyesinde siber savunma

alanında çalışan Küresel Operasyonlar ve Güvenlik Kontrol Merkezi (Global Operations and Security Control Centre) ve 2012 yılında faaliyet göstermeye başlayan Siber Operasyonlar Savunma Grubu (Defence Cyber Operations Group)'tur (Alioğlu, 2019: 113).

İngiltere strateji belgesi ile çeşitli öncelikler belirlemiştir. Bu öncelikler;

-Gelişmiş siber tehditleri belirleme ve analiz etme, siber tehditlere karşı cevap verme, yüksek derecedeki tehditlere karşı savunma, tehditleri caydırma ve devlet dışındaki aktörlerin bu tehditleri engellemek için üst düzey teknolojileri kullanabilmesi ve ülkeler arasında güven sağlama,

-Budapeşte Sözleşmesi'nin imzalanmış olması sebebiyle, siber suçluların sınır dışında yargılanması,

-Siber suçluların faaliyetlerinin engellenmesi ve vazgeçirilmesi, gerçekleşen siber saldırılar karşısında sorumluların etkili bir hukuki alanda yargılanabilmesi,

-Ülkenin kendi sınırları içerisinde siber güvenlik alanında en iyi uygulamaların kullanılması,

-Yetkin ve profesyonel siber güvenlik uzmanlarının yetiştirilmesi ve sürekli olarak siber alanda yenilikçi çalışmalar yapılması,

-Siber güvenliğin sağlanması için güvenlik uygulamalarının sürekli olarak güncellenmesi, sistemdeki açıkların engellenmesi,

-Geliştirilen siber güvenlik araçları ile dünya genelinde bir pazar oluşturulması şeklinde belirlenmiştir (The UK Cyber Security Strategy Protecting and promoting the UK in a digital World 2011: 26).

2012 yılında ENISA tarafından yayımlanan Ulusal Siber Güvenlik Stratejileri isimli rapor ile İngiltere siber güvenlik alanında yaptığı çalışmalar ile Bilişim ve Teknoloji alanında yenilikler, yatırımlar yaparak siber dünyadan tam olarak faydalanmak adına ve kullanmak için, siber güvenlik alanında kendine ulusal hedefler belirlemiş, siber güvenlik alanındaki stratejisini belirlerken öncelik olarak vatandaşların ve işletmelerin daha güvenilir halde olmasını önemsemiştir (National Cyber Security Strategies, 2012). Bu raporun ardından 2013 yılının Aralık ayında

Ulusal Siber Güvenlik Stratejisi 2013: Gelecekteki Planlar ve Başarılar (National Cyber Security Strategy 2013: Forward Plans and Achievements) isimli ilerleme raporu,

2014 yılında Ulusal Siber Güvenlik Stratejisi 2014: İlerleme ve İleriye Dönük Planlar (National Cyber Security Strategy 2014: Progress and Forward Plans) isimli ilerleme raporu ve 2015 yılında İngiltere 2010-2015 Hükümet Politikası: Siber Güvenlik (2010 to 2015 Goverment Policy: Cyber Security) isimli politika belgesi (https://www.gov.uk/, 2022) yayımlanmıştır.

Bu belgenin ardından da Ulusal Siber Güvenlik Strateji 2016-2021 (National Cyber Security Strategy 2016 to 2021) isimli strateji belgesi yayımlanmıştır (National Cyber Security Strategy 2016 to 2021, September 2017). Yayımlanan bu strateji belgesi ile İngiltere siber güvenlik alanında ciddi derecede önem vermiş ve yatırım yapmıştır. Bu belge ile 2016'ın Kasım ayından 2021 yılına kadar ülkenin genel olarak siber güvenlik vizyonu, hazırladığı siber güvenlik alanında politikaları, olası siber tehditlere karşı güvenlik önlemleri, saldırılar sonrasında toplanma aşamasında neler yapılacağı, hangi adımlar izleneceği, saldırılar karşısında korumalı şekilde durulması hedeflenmiştir.

İngiltere'nin yaptığı çalışmalar ile vatandaşlara, kurum ve kuruluşlara teknolojik gelişmeler ve yenilikler ile siber alanda gerçekleşecek olan saldırılara karşı korumak, büyük tehditleri engellemeyi amaçlamıştır. Ülke genelinde sivil toplum ve çalışan toplumun, kamu kurum ve kuruluşlarının siber güvenlik alanında bilgi sahibi olmalarını, hazırlanan güvenlik önlemleri ile gelebilecek saldırıları caydırmayı, yapılan saldırıların etkilerinin en aza indirgenmesi hedeflenmiştir. Yaptığı araştırmalar ve geliştirmeler ile siber güvenlik alanında sürekli olarak gelişmeyi amaçlamıştır.

3.2.6. Japonya'nın Siber Güvenlik Politikaları

Japonya, siber güvenlik alanındaki çalışmalarına diğer ülkelere göre geç başlamıştır. Japonya siber güvenlik stratejilerini hazırlarken; olası siber saldırılar karşısında hazırlıklı olmanın, saldırıya cevap vermek için planlamaların yapılması, siber saldırılar hakkında bilgi ve verilerin toplanması, bilgi güvenliğinin, kişisel

verilerin korunması için toplumu ve kurumların bilinçlendirilmesi ve siber güvenlik alanında teşviklerin yapılması için planlamalar yapmıştır. Tüm bunların yanında uluslararası anlaşmalar yaparak siber güvenlik alanında güvenliğin sağlanması için ittifaklar kurmayı hedeflemiştir.

Japonya siber güvenlik alanındaki ilk stratejisini 2010 yılında yayımlamıştır. Bu Bilgi Güvenliği Stratejisi (Information Security Strategy for Protecting the Nation) ile amaçlar belirlemiştir (https://www.nisc.go.jp, 2023).

Bu amaçları aşağıdaki maddeler halinde;

-Siber saldırılar karşısında politika açıklarının tespit edilerek bu açıkların kapatılması, güçlendirilmesi, bu saldırılara karşılık vermek için kurum oluşturulması,

-Gelişen teknoloji ile bilgi güvenliğinin sağlanması için değişen şartlar ortamında yeni politikalar hazırlanması ve değişen şartlar altında politikaların güncellenmesi,

-Aktif olmayan, işe yaramayan güvenlik önlemlerini almak yerine bunları engelleyip yerine aktif olarak koruma sağlayan güvenlik önlemlerinin alınması amaçlanmıştır.

Japonya hazırladığı strateji belgesi ile siber alandaki güvenliği artırmak adına çeşitli eylemlerden söz etmiştir. Bu eylemler ise;

-Siber alanda ulusal düzeyde güvenliğin sağlanması adına uzmanlığın artırılması,

-Siber güvenlik alanında uluslararası ittifaklar kurulması,

-Ekonomik büyüme sağlayacak siber güvenlik politikası sağlanması,

-Ulusal güvenlik, siber saldırı durumunda kriz yönetimi ve ulus/kullanıcı bakış açılarını kapsayan politikalar oluşturulması olarak belirtebiliriz.

Japonya, 2010 yılında hazırladığı strateji belgesi ile siber güvenlik alanında yapılması gereken faaliyetlerden bahsetmiş, ulaşılması gereken hedefleri belirlemiştir. Bilgi güvenliği sistemlerinin güvenliğinin sağlanması için önlemler alınmış ve 2020 yılını hedeflemiştir.

2012 yılında Japonya siber alanda bir girişime imza atmıştır. Savunma Bakanlığı tarafından yapılan bu girişimde ülkeye karşı gerçekleştirilen saldırılara karşı savunma amaçlı olarak bilgisayar virüsü geliştirmiştir. Bu virüs ile üst düzey saldırıların önüne geçilmesi, veri tabanında bulunan virüslerin temizlenmesi, gerçekleşen siber saldırıların kaynaklarının tespit edilmesi ve bu kaynakların takip edilmesi amaçlanmıştır. Bu virüse milli güvenlik virüsü olarak isimlendirmiştir (https://webrazzi.com, 2023).

2013 yılında Japonya'nın 2013 yılı Savunması başlıklı, Beyaz Kitap yayımlanmıştır. Bu belgede siber güvenlik konusuna özellikle yer verilmiştir. Bu Beyaz Kitap ile küresel olarak ülkelerin siber alanda gerçekleşebilecek saldırılara karşı risk altında olduğu, siber alanda mücadele edebilmek için çeşitli girişimlerde bulunduklarını, internet ve teknolojinin gün geçtikçe gelişmesi sebebiyle siber saldırıların ciddi derecede sorunlara yol açabileceğine değinilmiştir. Bu belgede siber saldırıların şu özelliklerinden bahsedilmiştir;

-Siber saldırıların çeşitliliği ile her saldırının kendisine göre amacı, yöntemi ve şartlarının farklıdır.

-Saldırıların kaynaklarının tespit edilememesi, kim tarafından yapıldığının bulunamaması sebebiyle anonim kalır.

-Saldırıların kimsenin fark etmeden gerçekleşmesi, oluşan zararların bilinememesine neden olur.

-Siber saldırı araçlarına kolaylıkla erişilmesi ve söz konusu açıkların kapatılması zor gerçekleşir.

-Gerçekleşen siber saldırılara karşı saldırılar ile cevap verilmesi, yeterli düzeyde savunma sağlayarak saldırıların caydırılmasıdır.

Japonya'nın 2013 yılında çıkardığı Ulusal Güvenlik Strateji belgesi ile siber alanda 10 yıllık süreçte siber güvenliğin nasıl sağlanacağı, ulusal güvenliğin nasıl sağlanacağı, güvenliğe ilişkin mevcut sorunlara değinilmiştir. Tüm bunların yanında uzay, siber uzay ve deniz gibi ortak kullanım alanlarındaki siber risklerin arttığı, gizli bilgilerin ele geçirilmesinin riskinin olduğu, kritik altyapılara gerçekleşen saldırılar ile işlevselliklerini kaybetme risklerinin olduğu, siber saldırılar ile askeri alanın

faaliyetlerinin engellenmesi gibi risklerden söz etmiştir. Japonya'nın bu belge ile siber güvenliğe bakış açısı değerlendirildiğinde; siber güvenlik alanındaki faaliyetlerin artırılmasını, gelebilecek siber saldırılara karşı cevap verilmesi için saldırıların güçlendirilmesini, ülkenin kritik altyapılarının siber saldırılara karşı sürekli olarak korunmasını, siber uzay alanının aktif olarak kullanılması için siber alanda alınan önlemlerin sürekli olarak güncellenmesi ve artırılmasını belirtmiştir. Tüm bunların yanında ABD ile siber alanda iş birliği yapmayı, bu iş birliği ile ortak siber tatbikatlar, siber gözetim ve keşifler yapılması gerektiği belirtilmiştir (Alioğlu, 2019: 145).

2015 yılının Ekim ayında yayımlanan Siber Güvenlik Stratejisi ile güvenli bir siber ortam sağlanması amaçlanmıştır. Bu siber ortamın tüm herkese eşit, adil ve serbest olması hedeflenmiştir. Söz konusu stratejinin amaçlarına ulaşmak 5 temel ilke belirlenmiştir. Bu ilkeler;

-Bilginin Serbest Akışının Güvencesi İlkesi: Bu ilke ile siber alanın sürekli olarak yenilenmesi, gelişmesi, siber ortamda aktarılan bilgilerin sansürlenmeden ya da zarar görmeden değiştirilmeden aktarılması için benimsenen bir ilkedir. Bu ilke ile bilginin tam anlamıyla siber alanda serbest dolaşımının sağlanması, kişisel gizliliğin korunması hedeflenmelidir (Alioğlu, 2019: 150).

-Hukuk Kuralı İlkesi: Japonya'da siber alanlar normlara ve kanunlara bağlıdır. Hukuk aktif, eşit ve adil olarak uygulanmalıdır. Siber alanda dışındaki alanlarda uygulanan tüm kanunlar, normlar ve kurallar siber alan içinde geçerlidir. Ülke içinde hukukun üstünlüğü kabul edildiği gibi uluslararası olarak da kurallar ve normlar geliştirilmesi gerekmektedir (Alioğlu, 2019: 150).

-Açıklık İlkesi: Ülke kapsamındaki siber alanın yalnızca belirli bir grup, belirli bir insan topluluğu tarafından değil ülkenin içinde bulunan, siber alanı kullanmak isteyen tüm insanlara açık halde olmalıdır (Alioğlu, 2019: 151).

-Özerklik İlkesi: Siber alanda faaliyet gösteren katılımcıların çok fazla olması sebebi ile bu ilke benimsenmiştir. Ülkenin kendi geliştirdiği yöntem ve sistemler ile gelişilmelidir (Alioğlu, 2019: 151).

-Çoklu Paydaşlar Arasında İş Birliği İlkesi: Siber alan; birden fazla kişi, kurum, ülke tarafından aynı anda aktif olarak kullanılmaktadır. Bu sebeple hükümet bu paydaşlar arasında koordine sağlayarak, paydaşlar arasındaki ilişkilerin geliştirilmesini, gerçek zamanlı bilgi paylaşımı yapılmasını hedeflemiştir (Alioğlu, 2019: 152).

Bu ilkeler ile insanların güvenliği, ulusal güvenliğin sağlanması, olası tehditlere veya terör eylemlerine karşı olabilecek tehditlere ve zararlara izin verilmeyeceği, aynı zamanda sadece siber alanda değil siber güvenlik politikaları hazırlanırken baz alınmalıdır. İlkeler doğrultusunda siber güvenlik politikaları hazırlanırken hedefe ulaşmak için bazı politika yaklaşımları belirlenmiştir. Bu yaklaşımlara göre;

-Güvenli IoT (Internet of Things) sistemleri oluşturularak, güvenlik zihniyetine sahip yönetim geliştirilmesi ve siber güvenlikteki iş ortamının iyileştirilmesi,

-Halkın ve toplumun verilerinin korunmasına yönelik tedbirler alınması, ülkenin kritik altyapılarının korunmasına yönelik tedbirler alınması,

-Siber alanda ulusal olarak güvenliğin sağlanması, ülkeler arasında uluslararası barış ve istikrar sağlanması, uluslararası iş birliklerinin yapılması,

-Ar-Ge çalışmaları yaparak siber güvenlik gücünün geliştirilmesi ve güvence altına alınması olarak belirlenmiştir.

Japonya hükümeti, 2017 yılında üç ayrı ulusal siber güvenlik stratejisi yayımlamıştır. Bunlar;

-Kritik Alt Yapı için 4. Uygulama Güvenlik Eylemi (4th Information Security Action Plan for Critical Infrastucture),

-Siber Güvenlik İnsan Kaynaklarının Geliştirilmesi Programı (Program for Cybersecurity Human Resources Development) ve Siber Güvenlik Araştırma ve Geliştirme Stratejisi'dir (Alioğlu, 2019: 153).

Japonya hazırladığı bu stratejiler ile işletme ve kurum yöneticilerinin siber güvenlik alanında aktif olarak yer almasının gerektiğini, stratejilerdeki söz konusu

riskleri bu yöneticilerin yöneteceğini söylemiştir. Kritik Alt Yapı 4. Uygulama Güvence Eylem Planı ile stratejiler hazırlanırken yönetimin daha fazla dâhil edilmesi, bilgi güvenliği sağlanırken aktif olarak çalışması gerekmektedir (http://afyonluoglu.org, 2022)

Siber Güvenlik İnsan Kaynaklarını Geliştirme isimli belgede diğer belge gibi yönetimin siber güvenlik politikalarında aktif olarak çalışması gerektiği, siber güvenlik önlemlerinin hızlandırılması hazırlanacak olan siber güvenlik politikalarında önemli derecede rol oynar (Alioğlu, 2019: 154)

Japonya, Nisan 2017'de Mükemmellik Sınai Siber Güvelik Merkezi'ni Ekonomi, Ticaret ve Endüstri Bakanlığı bünyesinde kariyer ve iş idarecisi yetiştirmek üzere IPA kapsamında kurulmuştur. Japonya tüm bunlardan sonra 2018 yılının Temmuz ayında Siber Güvenlik Stratejisi yayımlanmıştır (http://afyonluoglu.org, 2022). Bu strateji belgesi ile ülke kapsamında sosyo-ekonomik bir değişim, sürekliliği olan bir kalkınma süreci, halkın güvenli bir ortamda olması ve hissetmesi, ülke sınırları kapsamında ulusal güvenliğin ve barışın sağlanması için siber güvenlik yaklaşımları açıklanmıştır.

Strateji belgesi 2015 yılındaki belgeyi dikkate alarak 2018 yılına kadar olan tüm gelişmeleri göz önünde bulundurarak hazırlanmıştır. Kamu ve Özel Sektör Verilerinin Kullanımına İlişkin Temel Yasa ve Kişisel Bilgilerin Korunmasına İlişkin Değişiklik Yasası da dâhil edilerek bilgi verilerin kullanımı yasal bir temele bağlanmıştır. Siber alan hazırlanan strateji belgesi ile gerçek alanla bütünleşmesi, ekonomik ve sosyal olarak gelişme, insan merkezli toplumu gerçekleştirme politikası benimsenmiştir. Hazırlanan politikalar doğrultusunda gelişen teknoloji kullanılarak gerçek uzayda sensörler, cihazlar ile veriler toplanarak analizler yapılarak yeni ürünler ortaya çıkarılması ve geliştirilmesini benimsenmiştir. Tüm olumlu gelişmelerin yanında siber alanda oluşan birleşme sonrasında doğan riskler, güvenlik açıkları da artmış ve hızlanmıştır.

Japonya siber güvenlik alanında yaptığı çalışmalar, hazırladığı stratejiler ve attığı adımlar ile siber güvenlik kavramındaki faaliyetlerini sürekli olarak ileriye taşıdığı anlaşılmaktadır.

3.3. Uluslararası İlişkiler Açısından Siber Güvenlik

Uluslararası alanda siber güvenliğin korunabilmesi ve sağlanabilmesi açısından ülkelerin kendi içlerinde çeşitli güvenlik çalışmalarına ve iş birliklerine ihtiyaçları vardır. Ancak ülkeler açısından bu antlaşmalar oldukça az sayıdadır. Avrupa ülkelerine karşı yapılan siber saldırılar sonrasında; AB, G8 ülkeleri ve NATO'ya üye olan ülkeler harekete geçmiş ve gerçekleşen siber saldırılar karşısında iş birliği içinde hareket etmeyi hedeflemişlerdir (Gürkaynak ve İren, 2011: 275). Gerçekleşen siber saldırılar NATO'nun siber güvenlik stratejilerini oluştururken önemli bir yer edinmiştir.

Avrupa Konseyi, G8, BM ve NATO gibi uluslararası kuruluşlar, siber güvenlik alanında çeşitli stratejiler üreterek siber güvenlik alt yapısını oluşturmak ve güçlendirmek adına çalışmalar yapmaktadır. Avrupa Konseyi, siber güvenlikle alakalı 2004 yılında yürürlüğe giren uluslararası suç sözleşmesinde anlaşmaya varmıştır.

Avrupa Konseyi Siber Suçlar Konvansiyonu, siber suç konusunda ilk ve tek uluslararası sözleşmedir. Bu sözleşme uluslararası alanda ve siber suçlarla mücadele hususunda çok önemli bir yere sahiptir. Avrupa Konseyi'ne üye devletlerin 42'si bu sözleşmeyi imzalamış, 25'i ise kanunu onaylamıştır (Turhan, 2010: 71-72).

G8 ülkeleri, 1995'ten bu zamana kadar siber güvenlik, bilgi toplumu ve kritik alt yapıların korunması alanlarıyla ilgili sürekli olarak ilgilenmiş 1995'teki Halifa X Zirvesi ile mevcut uluslararası antlaşma ve örgütlere mücadeleleri incelemek için Kıdemli Uzmanlar Grubu atanmıştır. Bu zirveden sonra G8 Kıdemli Uzman Grubu tarafından birçok öneriler kabul edilmiştir. Bu grup ileri teknoloji suçları anlayan ilk uluslararası grup olarak nitelendirilmektedir (Turhan, 2010: 78).

Birleşmiş Milletler (BM), Bilgi Güvenliği Devlet Uzmanları Grubu'na (GGE) liderlik etmektedir. Bu grup siber alandaki anlaşmazlıkların önüne geçmeyi, istikrarı sağlamayı, siber alanda uluslararası normlar oluşturmayı temel amaçlar olarak benimsemiştir. Bu grup 2004 yılından beri faaliyet göstermektedir (Dijital Türkiye, 2017: 14).

Ülkelerin genel olarak siber alandaki yansımaları incelendiğinde; birbirinden farklılık gösteren yönleri varken genellikle benzer özellikler göstermektedir. Kimi ülkeler siber güvenlik alanında alt yapı çalışmalarını yaparken, yeni kurumlar kurarken kimi ülkeler görev alanlarını değiştirmeye, genişleterek yeni siber güvenlik kavramına alışmaya çalışmaktadır (Ada, 2018: 61). Yine ülkelerin siber saldırılara ve gerçekleşen siber olaylara karşı bakış açıları farklıdır. Bazı ülkeler siber alanı daha az kullanırken bazı ülkeler kendi çıkarları için daha sık kullanmaktadır. Siber etkinlikleri çok kullanan ülkeler teknolojik olarak daha ileri düzeydedirler ve küresel güvenliği desteklemezler. Çünkü kendi çıkarlarına uymamaktadır.

Günümüzde siber alanın uluslararası ilişkiler alanında görülmesi sebebiyle tüm ülkeler kapsamında siber politikalar adına çalışmalar yapılmaktadır ve ciddi oranda bir artış görülmektedir. Ülkelerin kendi çıkarları siber alanda da aynı zamanda devletleri sıcak çatışmalara sürükleyecek hale getirmiştir (Güntay, 2018: 80-81).

3.4. NATO ve Siber Güvenlik

Fiziki savaş sistemlerinin etkilerinin azalması ile gün geçtikte gelişen teknoloji ile ortaya çıkan siber tehditler ve savaşlar ülkelerin güvenlikleri açısından daha zararlı hale gelmeye başlamıştır. Böylece eski sistem savaşlar yerini hibrit savaşlara bırakmıştır. Hibrit savaşlar tarafların sadece birbirleri ile sahada çatışmadığı, tarafların zihinleri kazanma savaşı olarak yapılan çalışmalar olarak tanımlamışlardır (Güleç ve Kişman, 2021: 140). Bu savaşın hedefleri yalnızca halk değil, uluslararası aktörlerdir. Askeri avantajın yanında "manevi olarak güç ve zafer" kazanmak için hedefin ülkenin kritik internet noktalarını çökertmek amaçlanır (Altınışık, 2017). Siber savaş da aynı hibrit savaş gibi ülkelerin stratejik sayılabilecek hedeflerine yönelmektir.

NATO ortaya çıkan bu siber saldırılar karşısında çeşitli stratejiler ve yöntemler geliştirmiştir. Bu strateji ve yöntemlerin zeminini gerçekleşen siber krizler hazırlamıştır. NATO ülkeleri, geliştirilen siber saldırılara karşı kendi özellik ve alt yapılarına göre NATO tarafından geliştirilen stratejilere göre şekil almaktadır (Somuncu, 2018: 67).

3.4.1. NATO'nun Katıldığı Siber Kriz Örnekleri

NATO, siber krizlere karşı stratejiler geliştirirken; Kosova Saldırısı, Estonya'ya yönelik siber saldırılar, Gürcistan Saldırısı gibi saldırıları temel almıştır (Güleç ve Kişman, 2021: 141).

- **NATO-Kosova Krizi (1999)**

NATO uçaklarının yanlışlıkla Çin Elçiliği'ne çarpması sonucunda Çin Kırmızı Hacker İttifakı, NATO ve askeri web sitelerine saldırmıştır. Bu saldırı neticesinde NATO'nun sitesinde çeşitli kesintiler olmuştur. NATO'ya üye devletlerin e-posta hesapları erişim dışı kalmıştır.

Bu olay dünya tarihindeki ilk siber savaş olarak tanımlanmıştır. Bu olaydan sonra NATO ilk siber güvenlik adımını atmıştır. Saldırı sonrasında NATO yeni stratejik belge hazırlamıştır (Ada ve Çakır, 2017: 638).

- **Estonya Siber Savaşı (2007)**

Nisan ve Mayıs 2007'de Estonya'nın savunma sistemini durduran, kamu ve özel kuruluşların, bankaların, medyaların web sitelerini hedef alan büyük çaplı saldırılar gerçekleşmiştir. Bu saldırılar sonrasında siber tehdit algısı değişmiş, "21. Yy'da siyasi, ekonomik ve Bilgi teknolojileri güvenliğine zarar verecek öncelik risk" olarak kabul edilmiştir.

NATO, bu saldırı sonrasında politika kapsamında "Sanal Savunma Yönetim Otoritesi (CDMA)" ve Estonya merkezli Siber Savunma Merkezi'ni (CCD COE) kurmuştur (Seren, 2016: 16-17).

- **Gürcistan Siber Savaşı (2008)**

Gürcistan'da ayrılıkçı bir grubun provokasyonuna karşılık vermesi sonucunda olaylar büyümüş ve siber saldırılar devam ederek siber çatışmaya dönüşmüştür.

3.4.2. NATO Üyesi Ülkelerin Siber Güvenlik Çalışmaları

NATO üyesi ülkeler, siber güvenlik konusunda ciddi çalışmalar yürüten ve işbirliği içinde olan ülkelerdir. NATO'nun temel amacı, üye ülkelerin savunma ve

güvenliklerini korumak olduğundan, siber güvenlik de NATO'nun öncelikli konularından biridir.

NATO, üye ülkeler arasında siber tehditlerle mücadele etmek için bir dizi politika, strateji ve yönergeler geliştirmiştir. Bu kapsamda, NATO Siber Savunma Politikası ve Siber Savunma Eylem Planı gibi belgeler oluşturulmuştur. Bu belgeler, siber tehditlerle mücadele etmek, siber savunma kapasitelerini güçlendirmek ve NATO üyesi ülkeler arasında bilgi paylaşımını teşvik etmek için tasarlanmıştır.

- **ABD**

ABD, siber güvenlik ve siber uzay konusunda diğer ülkelere önderlik eder. Avrupa ve Asya'daki ülkelerin siber sorunlarla mücadele konusunda örnek alınmaktadır.

ABD 11 Eylül Saldırısı sonrasında siber güvenlik ve kritik alt yapıların korunması için siber alanda değişiklikler yapmıştır. Siber güvenli alanında güvenliğin sağlanması için DHS bünyesinde Altyapı Koruması (OIP) ve Siber Güvenlik ve İletişim Departmanı (CS&C) kurulmuştur.

OIP, ülkedeki mevcut alt yapıları korumak, söz konusu güvenlik açıklarını değerlendirerek önüne geçilmesinden, uluslararası alanda güvenlik kültürünün oluşması ve benimsenmesinden, siber güvenlik alanında uluslararası ilişkiler kurmak ve kritik alt yapıların korunmasından sorumludur.

CS&C ise, siber tehditler, risk yönetimi, acil durumlarda iletişim ve siber olaylara müdahale merkezlerinin kurulmasından sorumludur (Turhan, 2010: 103).

- **Almanya**

Almanya ilk ulusal siber güvenlik stratejisini 2011 yılında oluşturmuştur ama çalışmalarına başlamasının ardından kapsamlı ve hızlı bir şekilde büyümeye ve gelişmeye başlamıştır. 2015 yılındaki çalışmaları ile siber güvenlik stratejilerini günün şartlarına göre güncellemiştir. Bu güncellemeler yapılırken ülkenin kritik alt yapılarının korunmasına yönelik çalışmalar yapmıştır.

Almanya'nın stratejilerinde siber güvenlik ve siber savunma mekanizmalarının uluslararası olarak önemi ve iş birliğine değinilmiştir.

Almanya'nın kritik alt yapılarının korunması ve bu kanundaki çalışmaların koordinasyonundan sorumlu olan Federal Bilgi Güvenliği Ordusu'nun (BSI), 2011 yılında hazırlanan ve daha sonradan güncellenen stratejik planın ardından yetkileri artırılmıştır. Almanya tüm çalışmalarına rağmen ABD'nin geliştirdiği askeri yazılımlara bağlıdır (Sanalp, 2016: 28-30).

- **Estonya**

2007 yılındaki yapılan siber saldırılar ülkenin siber yeteneklerini sorgulamasına neden olmuştur. Böylece siber savunma faaliyetleri Savunma Bakanlığı tarafından yürütülmeye başlanmıştır. Aynı zamanda Savunma Birliği adı altında bir kuruluş siber savunma kuvvetlerini iyileştirmek adına çalışmalar yapmaktadır. Bu kuruluşun yanında Siber Güvenlik İttifakı görevlerini üç ana başlık altında toplamıştır;

-Estonya'nın elektronik hayatlarını korumak,

-Bilgi Teknoloji uzmanlarının eğitimi,

-Siber savunma ile ilgili kamuoyunu bilgilendirme çalışmalarıdır.

- **Birleşik Krallık**

Ekim 2010'da Ulusal Güvenlik Strateji Raporu'nu yayımlamıştır. Bu raporda Birleşik Krallık'ın karşılaşabileceği riskleri gruplar ayırmış ve siber saldırıları en yüksek risk grubuna dahil etmiştir. Raporun içeriğine göre diğer ülkelerin siber saldırıları ve terörist grupların örgütlü ağların saldırılarını da dahil etmiştir.

- **Kanada**

Siber güvenlikten sorumlu Kanada Siber Olaylara Müdahale Merkezi' (CCIRC) dir. Bu müdahale merkezi gerçek zamanlı olarak çalışarak gerçekleşen siber saldırılara anında müdahale etmektedir.

Bu merkez, aynı zamanda kritik alt yapı sektörlerine olayların müdahale, koordinasyon ve destek sağlama, izleme ve siber güvenlik tehditlerini analiz etme, bilgi ve teknoloji alanında danışmanlık sağlama farkındalık çalışmaları hususunda eğitimlerden de sorumludur (Turhan, 2010: 114-115).

- **Fransa**

Fransa'nın siber alandaki ulusal stratejisi siber güvenliği sağlamak ve bu alanda politikalar çizmek olarak belirlenmiştir.

Bu politika çizme durumu İkinci Dünya Savaşı dönemine kadar uzanmaktadır. 1943'te Fransız Ulusal Direnişi altındaki Fransız topraklarının çoğunluğu ile 1943'teki Fransız ulusal direnişi ile kurulan Direction Technique du Chiffe (DTC) savaş sırasında Alman'ların şifreli iletişimini önlemeye çalışarak direnişteki iletişimin gizliliğini sağlamıştır. Savaşın ardından 1953 yılında birim geliştirilebilecek Service Central Technique du Chiffre STC-CH dönüştürülmüştür.

1977 yılında kurulan İletişim Güvenliği ve Parola Hizmetleri Merkezi (Service Central Du Chiffre Et Securitdes Telecommunications) 1956 yılında Bilgi Sistemleri Güvenliği Merkezi'ne dönüştürülmüştür. Bu merkez daha sonra Bilgi Sistemleri Güvenlik Merkezi (DCSSI) haline gelmiştir.

Bilgi güvenliği politikalarının uygulamaları ve koordineli kontrol etmek amacıyla (DCSSI) yerini Fransız Ulusal Bilgi Güvenliği Ajansı (AUSSI)'a bırakmıştır.

Fransa'nın siber alandaki güvenliği artırmak amacıyla siber güvenli hakkında olan Ulusal Güvenlik ve Savunma Hakkında Beyaz Kitap çıkmıştır. Beyaz kitap, Fransa'nın ulusal güvenlik tehdidinin başında siber saldırıları başta görmekte ve riski en aza indirmek amaçlanmıştır.

3.5. Siber Güvenlik Gücünün Dünya Siyasetindeki Yeri ve Önemi

Siber güvenlik kavramı, bireylerin kuruluş ve kurumların siber alanla ilişkisini sağlayan, sosyal ve ekonomik kalkınmayı sağlarken bir yandan da kamu ve özel sektöre sağladığı kolaylıklar ile günümüz için vazgeçilmez bir kavram haline gelmiştir (Gül, 2009: 199-200). Günümüzde hayatın her alanında kullanılan bilgi ve iletişim teknolojilerine olan bağımlılık sonucunda siber alan suçlular açısından cazip bir alan haline gelmiştir. Siber saldırganlar tarafından siber alanda kullanılan siber saldırı yöntemlerinin araçları, kapsamı ve eğilimi de küçük ölçekli siber ihlallerden ve maddi zararlardan yüksek düzeyde maddi kayıplarla sonuçlanan organize ve devlet destekli büyük ölçekli siber saldırılara kadar çeşitlilik gösterir (Shafqat &

Masood, 2016: 129). Yüksek düzeyde tehdit oluşturan ve her geçen gün artan karmaşıklığa neden olan Gelişmiş Kalıcı Tehditler (APT) neden oldukları zarar nedeniyle bilgi ve iletişim teknolojileri için büyük bir engel oluşturmaktadır. Kamu ve özel yetkili görüşlerine göre siber saldırılar bugün terörist eylemlerinden çok daha fazla fiziksel ve ekonomik kayba yol açmaktadır (http://www3.weforum.org, 2023)

Gelişen teknoloji ile bilgi iletişim sistemleri ve günümüz teknolojisinin hızla gelişmesi kara, deniz, hava ve uzay alanında gelişmelere neden olmuştur. Bu harekât alanlarının yanına siber uzay hareket alanı eklenmiş ve diğer tüm harekât alanlarını da siber uzay da etkili hale gelmiştir. Bu gelişmeler doğrultusunda siber uzay alanı harekât alanlarının beşincisi olarak kabul edilmiş, siber uzay bütün devletlerin iç veya dış politikalarını belirlenirken etkili olmuş ve caydırıcı konuma gelmiştir.

Siber uzay gelişmeler doğrultusunda ülkelerin iç ve dış politikaları hazırlanırken temel araçlardan birisi olarak kabul edilmiştir. Günümüzde gelişen teknolojiler sayesinde ülkeler teknolojik imkân ve yeteneklerini geliştirerek siber uzayda ve siber alanda etkin olabilmek ve yeteneklerini artırabilmek için çalışmalar yapmaktadır. İnternet ve teknolojiye bağımlılığı artan ülkeler doğrudan siber saldırı alanında tehlikeli konuma düşmektedir. Söz konusu siber saldırıların ülkeler çapında hayati tehlikeyi riske atacak ulaşım, elektrik, sağlık, eğitim, nükleer tesisler, bankalar, su, tarım ve sanayi birimlerine, kritik alt yapılarına yapıldığı düşünüldüğünde ciddi derecede zararlara sebep olacağı ortadadır.

Rusya'nın 2007'de Estonya internet alt yapısını hedef almasıyla, Rusya ile Gürcistan arasındaki konvansiyonel savaş 2008'de siber savaşa dönüşmüştür ve İran nükleer santrallerinin 2010'da Stuxnet siber saldırısıyla kırılgan olduğu tespit edilmiştir (Çelik, 2013: 145). Bu tarz siber saldırı örneklerinin oluşturduğu farkındalıklar ile ülkeler ulusal siber güvenlik gücünü artırma çabalarını daha da hızlandırmış, özellikle siber güvenlik stratejileri ve planları hazırlamış veya mevcut olan silahları güncellemişlerdir (Shafqat ve Masood, 2016:129).

Ülkeler kapsamında tüm bunların önüne geçebilmek için ulusal olarak siber güvenlik güçlerini artırabilmek adına çalışmalar yapılmaktadır. Bilgi ve iletişim teknolojilerinin ilerleyen bilgi ortamı sayesinde teknoloji üzerinden verilen

hizmetlerinde artmasına sebep olmuştur. Bu sebeple birçok alanda kişi, kurum, kuruluş ve ülkeler tarafından vazgeçilmez bir faaliyet haline gelmiştir. Ülkelerin ulaşım, elektrik, eğitim, sağlık, tarım sanayi vb. kritik alt yapıları, bu teknolojilerin gelişmesi ile siber saldırılara açık hale gelmiştir.

Gelişen teknoloji ile siber alan, siber alandaki saldırılara ve tehditlere karşı savunmasız hale gelerek suç ve terör örgütlerinin saldırıları için açık bir hal almıştır (Solms, Niekerk ve Geers, 2013: 100). Saldırılara açık halde bulunması siber güvenlik ve savunma faaliyetleri, kişiler, kurum ve kuruluşlar arasında ve ülkeler çapında zaman geçtikçe önem kazanmıştır. Bu sebepler doğrultusunda alışılmış güvenlik anlayışlarından vazgeçilerek kritik alt yapı sektörlerinin yanında siber güvenlik alanındaki faaliyetlerin hızlandırılması ve geliştirilmesi için çalışmalar yapılmaya başlanmıştır (Ralston, Graham ve Hieb, 2007: 583-584). Böylece kritik alt yapı sektörlerinin korunması, tespit edilmesi ve güvenliklerin sağlanması, siber alanı hedef alan saldırıları engellemek ya da en aza indirgemek hedeflenmiştir.

Siber alanda kişisel verilerin güvenliğinin sağlanması, kritik alt yapı sektörlerinin yanında iletişim teknolojilerinin korunması da hayati önem taşımaktadır. Ülkelerin oldukça güvenli siber güvenlik politikası ve daha güvenli daha güçlü temellere dayanarak alt yapı çalışmaları yapmaları gerekmektedir. Siber güvenlik kavramının en kısa sürede benimsenmesi ülke politikalarının temel dinamikleri arasına alınması çok önemlidir. Ülkelerin siber güvenlik güçleri konusunda yeterli düzeyde farkındalığa sahip olamaması, siber güvenliğin hangi alanlarda iyileştirilmesi gerektiği konusunda yeterli bilgiye sahip olmaması siber güvenlik kavramının benimsenmemesinden kaynaklanır.

Bugün siber alan; güçlü etkili ülkeler ve dünyanın silahlı kuvvetleri tarafından kara, deniz, hava ve uzay alanında meydana gelebilecek savaşların yanında 5. Alan olarak kabul edilmektedir. Bilgi ve teknoloji sistemlerinin günümüzde hızla gelişmesi siber güvenlik alanında siber güvenlik kavramı, kurumlar, kişiler, kuruluşlar, ülkeler ve dünya gündeminde siyasi olarak çok önemli bir yere sahiptir (Ünal, 2016: 412). Teknolojinin sürekli olarak gelişmesi, internet kullanımının sürekli olarak artması güvenlik alanında siber güvenlik kavramının en başında yer alacaktır.

3.6. Siber Güvenlik Gücünün Ölçülmesi ve Ülkelere Göre Sıralama

Ulusal güç, ülkelerin herhangi bir konvansiyonel veya siber savaş sırasında ülkelere karşı üstünlük elde etmelerini sağlayacak ülkelerin ulusal güç unsurlarının toplamıdır.

Günümüzde kara, deniz, hava ve uzay güçlerinin yanında siber uzay alanında başarılı olunması adına siber güvenlik gücünün artırılması gerekmektedir. Siber güvenlik gücünü artırmak için ülkeler, siber savunma gücünün yanı sıra siber saldırı yeteneklerini de artırmakla görevlidir. Siber saldırı gücü düşük olan ülkelerin rakibe karşı caydırıcılık göstermemesi nedeniyle hem barış hem savaş koşullarında siber saldırıların hedefi konumundadır. Ülkelerin siber güvenlik gücünü sadece siber saldırı ve savunma kabiliyetleri ile ölçmek mümkün değildir. Bilgi ve iletişim teknolojilerinin yanında siber uzay alanına bağımlı yerli kurum ve kuruluşların ne kadar olduğu da önemlidir (Ralsten, Graham ve Hieb, 2007: 583-584).

Siber savunma bir devletin siber saldırıları durdurma çabasıdır. Siber bağımlılık ise bu tür saldırılara karşı savunmasız sistemlere ve ağlara ne kadar ihtiyaç duyduğunun göstergesidir (Clarke ve Knake, 2010: 74-75)

Ülkenin kritik alt yapılarını, kritik alt yapı sektörleri, kurumları siber alana ne kadar bağımsız olursa, siber saldırılara karşı o kadar savunmasız kalır. Yani internet alanında bağımlılığı yüksek olan teknolojik olan ülkeler siber saldırılardan daha çok etkilenmektedir. Çünkü kritik alt yapı sektörlerinde siber açıklar daha fazladır.

Tablo 6: Siber Güvenlik Güç Sıralaması için Kullanılan Veriler ve Etki Alanları

No	Araştırma ve İstatiksel Veriler	Etki Alanları
1	2011 Ülkelerin Siber Yeteneklerinin Verisign'a Göre Kategorizasyonu	Siber Savunma Siber Saldırı Siber Bağımlılık
2	AB Araştırma Şirketi tarafından yürütülen proje sonucunda 2014 Dünya Siber Güvenlik Endeksi (GCI) ve ITU	Siber Savunma Siber Saldırı

		Siber Bağımlılık
3	ITU tarafından yürütülen proje sonucunda 2017 Dünya Siber Güvenlik Endeksi (GCI)	Siber Savunma Siber Bağımlılık Siber Saldırı
4	Ülkeler tarafından Silahlı Kuvvetler için tahsis edilen bütçe 2014	Siber Savunma Siber Saldırı
5	Ülkelerin 2016 yılındaki Askeri harcamaları	Siber Savunma Siber Saldırı
6	2015 Ülkelerin Teknolojik Gelişim Sıralaması	Siber Saldırı Siber Bağımlılık
7	2012 Dünya'nın en büyük güvenlik teknoloji şirketi McAfee tarafından yayınlanan Siber Savunma Raporu	Siber Savunma
8	2015 Ülkelerin Yazılımlarının Kalkınma Sıralaması	Siber Saldırı
9	Siber Saldırı Trafiğini Kaynaklandıran Ülkelerin 2013 Sıralaması	Siber Saldırı
10	2015-2016 yılları arasında meydana gelen siber saldırıları kaynak kullanan ülkelerin sıralaması	Siber Saldırı
11	Ülkelerin 2016 yılındaki internet kullanımının nüfusa oranı	Siber Bağımlılık

(Çeliktaş, 2016: 105)

Data hazırlama araçları, kapsamı, doğruluğu ve geçerliliği göz önünde bulundurulduğunda ITÜ tarafından yürütülen projeler aracılığıyla ortaya konan GCI raporunun sonuçları ve ülkelerin sıralaması aşağıdaki tablodaki gibidir.

Tablo 7: Verisign şirketi tarafından yapılan ülkelere göre Siber Güvenlik Gücü Sıralaması

Seviye	Ülke
1	ABD, Çin, Rusya
2	Fransa, İngiltere, İsrail
3	Hindistan, Kuzey Kore, Almanya, Türkiye
4	Brezilya, Kanada, İtalya, Japonya, İran

(Dennesen, 2011:31)

Tablo 6 ve tablo 7 incelendiğinde belirtilen raporlar yani GCI raporları Siber Güvenlik Güç Sıralamasını belirlerken sonucu doğrudan etkileyecek ana araştırmadır. Bu raporlar ülkelerin siber güvenlik geliştirme seviyelerini ve siber güvenlikle çabaları, faaliyetleri ve dünya sıralamasını ortaya çıkarması açısından önemlidir. Ülkelerin mevzuatı, ulusal stratejiler, sertifika programları, siber güvenlik ekiplerinin durumu hakkında bilgi veren bu raporlar hazırlanırken eğitim, farkındalık, koordinasyon ve iş birliği çalışmalarından yararlanılmıştır (ITÜ, 2015: 1, ITÜ: 2017).

Ulusal düzeyde siber güvenlikle ilgili devlet politikalarını teşvik etmek, kritik alt yapı sektörlerinin güvenliğini sağlama çabalarının sürekliliğini sürdürmek, siber güvenlik kültürünü korumak ve sürdürmek raporun ana hedefleri arasında yer almaktadır. Hali hazırda modern toplumların itici gücü haline gelen bilgi ve iletişim teknolojilerinin temeli ve ülkeler adına siber güvenliğe yönelik farkındalık ve hazırlık düzeylerini yükselterek hedeflerin merkezindedir (ITÜ, 2015:1 AB1 Research, 2014, ITÜ, 2017).

Askeri güçlere ülkeler tarafından ayrılan bütçelerin ve harcamaların siber güvenlik güçlerini geliştirmek içinde aynı askeriyeye ayrılan bütçeler oranında bütçeler verilmiştir.

Wall Street Jamal'ın açık kaynak, bilgisayar güvenliği uzman araştırmacılar aracılığıyla yaptığı araştırmalar sonucunda, ülkelerin siber saldırıcı gücü hakkında bazı sonuçlar elde etmiştir. Bu sonuçlara göre;

-60'tan fazla ülkenin siber silahlara sahip olduğu,

-Siber silahları, siber saldırılar ve siber savunmada kullanma yeteneklerinin olduğu,

-29 ülkenin siber alanda istihbarat birimleri ordusunun resmi siber saldırı araç olarak kullandığı,

-49 ülkenin siber saldırı yazılımı tedarik ettiğini ve kullandığını ve 63 ülkenin siber saldırı silahlarını gözetim amacıyla kullandığını ortaya koymuştur. Ayrıca ülkelerin siber silahları gözetleme, zarar verme ve imha amaçlı olarak kullandıkları, buna bağlı olarak askeri veya istihbarat birimlerinden yararlandığı ve bu tür saldırıların devlet desteği olsun ya da olmasın gerçekleştirildiği görülmektedir (Valentine ve Yadron, 2015). Bu sonuçlar ülkelerin siber rekabet içinde olduklarını ve bu rekabette galip gelenlerin dünya siyasetinde daha aktif bir ol oynama olasılıklarının daha yüksek olduğunun farkında olduklarını göstermektedir.

Operasyonel bir savaş durumunda büyük ölçekli siber saldırı yeteneklerini kullanmak için doğru zamanı ve yeri beklerken, ekonomik fayda sağlamak, rakip ülkelerin zayıflıklarını tespit etmek ve olası siber savaşlara hazırlanmak için sınırlı siber saldırı gücünü ölçmek oldukça zordur. Çünkü bu siber saldırılar doğal olarak bir kez etkili bir şekilde kullanılabilir. Bu nedenle özellikle devlet desteği olmadan veya özellikle devlet desteğiyle olan saldırılar için kullanılacak siber silahların kullanılacağı ana kadar gizlilik altında tutulması sebebiyle ülkelerin siber saldırı güçlerini belirlemek zordur. Ülkelerin siber saldırı gücünü belirlemek zor olsa da doğru veriler kullanılarak gerçeğe yakın rakamlar elde etmek mümkündür.

Bilgi ve iletişim teknolojisinin günümüzde küresel bir ağ medyası sağlayan internete bağlı olması nedeniyle siber alanın en önemli aktörü olan ülkelerin hayatta kalması uğruna, internetin güvenliğini sağlamak gerektirmektedir. Sahip olduğu böyle özel bir statünün sonucu olarak internet siber saldırganlarının saldırıları ve aktif olarak işgal ettikleri yerler için çekici bir ortam haline gelmiştir. Ülkelerin

gelecekte internete ve siber uzaya daha bağımlı hale geleceği göz önünde bulundurulduğunda bu faktör daha fazla önem kazanacaktır. Siber alana bağımlı ülkelere siber saldırılar ile zarar vermek diğer ülkelere göre daha kolaydır. Bu ülkelerin arasında ABD, İngiltere ve Japonya gibi ülkeler bulunmaktadır. Siber alana daha az bağımlı olan veya bir siber tehdit durumunda ulusal siber alanları ortak siber alandan izole eden Kore, İran ve Çin gibi ülkelere yapmak daha zordur. Bu tür siber saldırılar gerçekleştirilirse bile söz konusu ülkeler sırf siber alana daha az bağımlı oldukları için diğer ülkelere kıyasla daha az etkilenecektir.

Ülkelerin siber alana bağımlılık gücü ölçülürken nüfusa göre internet kullanım oranı, ülkelerin teknolojik gelişme durumları değerlendirmeye alınmaktadır. Yapılan bu değerlendirmeler boyunca tekno-mantik geliştirme ve internet kullanımı düzeyinin siber uzay bağımlılığına yönelik güçleri üzerinde olumsuz bir etkisi olduğu düşünüldüğünde ülkeler için nihai puanlar değerlendirilir.

Aşağıda Tablo 8 incelendiğinde, ülkelerin siber güç ortalamaları belirlenirken siber savunma gücü, siber saldırıcı gücü, siber uzay bağımlılığı dikkate alınarak ortalama siber güvenlik güçleri belirlenmektedir. Tablo incelendiğinde dünya ülkeleri üzerinde ABD'nin siber güç olarak listenin başında yer aldığı, onun arkasından Çin ve Hindistan'ın geldiği görülmektedir. Türkiye bu listenin alt sıralarında yer almaktadır. Listenin başında olan ülkeler gelişmiş ülkeler olarak göz önünde bulundurulduğunda alt sıralarda yer alan ülkeler gelişmekte olan ülkeler diyebiliriz.

Tablo 8: Ülkelere Göre Ortalama Siber Güç Sıralaması

No	Ülke	Siber Savunma Gücü	Siber Saldırı Gücü	Siber Uzay Bağımlılığı	Toplam Siber Güvenlik Gücü	Ortalama Siber Güvenlik Gücü
1	ABD	9,5	8,95	1,1	19,55	6,52
2	Çin	7,06	7,67	4,4	19,13	6,38
3	Hindistan	6.06	3,06	6,5	15,62	5,21
4	Fransa	7,54	4,24	3,2	14,98	4,99
5	Almanya	7,43	5,32	2,1	18,85	4,95
6	İtalya	6,17	3,73	4,7	14,6	4,87
7	Rusya	6,84	4,63	2,95	14,42	4,81
8	Brezilya	5,56	3,37	5,2	14,13	4,71
9	Kuzey Kore	3,07	0,82	9,5	13,39	4,46
10	Türkiye	5,18	2,27	5,85	13,3	4,43
11	Japonya	7,01	5,77	0,45	13,23	4,41
12	İsrail	7,18	2,92	2,85	12,95	4,32
13	Kanada	6,18	4,01	2,55	12,74	4,25
14	İngiltere	7,56	4,56	0,5	12,62	4,21
15	Güney Kore	6,28	4,38	1,7	12,36	4,12
16	İran	3,21	1	7,05	11,26	3,75

(Çeliktaş, 2016: 120**)**

Yapılan araştırmaların sonuçlara göre listelerin üst sıralarındaki ülkeler dünya siyasetinde daha etkin oynayabilecek caydırıcı rolü çok daha iyi kullanabilecek ve gelecekteki hibrit savaşlarda galip gelebileceklerdir. Dünya genelinde değişen güvenlik anlayışı ile siber uzayın oynadığı rol ve gelecekte daha da önemlisi ülkeler siber alanda güvenlik güçlerini artıracak çalışmalar yürütmek zorundadır.

SONUÇ

Teknoloji sürekli olarak kendini geliştiren bir kavramdır. Teknolojinin gelişmesinin yanında ülkelerdeki internet kullanımının artışı, internete karşı bağımlılıkların artması, internetin aktif olarak kullanılması, vatandaşların ve hükümetlerin devlet işlerinde de bu teknoloji ve internetin aktif olarak kullanılmasını sağlamıştır. İnternetin ve teknolojinin bu denli aktif olarak kullanılması da beraberinde yeni güvenlik sorunlarına neden olmuştur. Teknolojinin gelişmesi, internet kullanımının artışı ve küreselleşme ülkeler arasındaki sınırları ortadan kaldırarak, kara, deniz, hava, uzayın yanında siber alanda da sınırların ortadan kalkmasına neden olmuştur. Ortaya çıkan yeni güvenlik sorunları sebebiyle ülkeler, birbirlerinin izlediği politikaları yakından takip ederek doğru politikalar hazırlamalı ve gelişen teknoloji karşısında da çağa ve teknolojiye ayak uydurmak zorundadırlar.

Ülkeler hava, kara, deniz, uzay alanlarında güvenliklerini sağlarken bunların yanında siber alanda da güvenliklerinin sağlanması gerektiğini fark etmişlerdir. Siber güvenlik kavramı da ulusal güç olarak benimsenmelidir. Bu sebeple siber savunma araçları, siber saldırı araçları için çalışmalar yapmalıdır. İnternetin gelişmesi ve bu denli çok kullanılması siber alanda ciddi derecede sorunlara neden olabilmektedir. Hükümet ve vatandaşlarının verilerinin internet ortamında saklanması, onların her an ele geçirilebileceğinin göstergesidir. Bunların ele geçirilmesinden ziyade ülkenin kendisine ait bilgileri, vatandaşların kişisel bilgilerinin ele geçirilmesi, gizliliğinin sağlanamaması hükümete karşı ciddi derecede güvensizlik oluşmasına neden olacaktır.

Her ülkenin kendisine ait kritik alt yapıları vardır. Bu kritik alt yapıların siber alanda sürekli tehdit altında olduğu açıktır. Kritik alt yapıların siber saldırılara karşı sürekli açık halde ve hedef halinde olması ciddi derecede sorunlara sebep olacaktır. Olası saldırılar karşısında oluşan zararlar, ele geçirilen bilgiler, siber saldırı sonrasında oluşan zararlar yeterli derecede önlem alınmazsa geri getirilemez sonuçlar doğuracaktır. Sanal alanın sürekli olarak açık halde olması hep bir hedef olarak görülmesine neden olmaktadır. Siber saldırıların kaynağının tespitinin zor olması, yapanların kimliğinin anonim olarak kalması da siber saldırı sonrasında kargaşaya sebep olmaktadır. Kimliği tespit edilemeyen kötü niyetli şahıslar tarafından

gerçekleştirilen saldırılar zaman zaman terörizm kaynaklı olarak gerçekleşmektedir ve siber terörizm kavramını da ortaya çıkarmıştır. Siber terörizm gün geçtikçe ülkeler üzerindeki yeni terör saldırısı olarak kabul edilmiştir.

Gelişen teknoloji her geçen gün yeni siber saldırı mekanizmaları, yeni siber saldırı türlerinin ortaya çıkmasına neden olmaktadır. Yapılan saldırıların, saldırı silahlarının gelişinin ülkeler açısından sürekli olarak takip edilmesi gerekmektedir. Saldırılar sonrasında ciddi derecede zararlar ortaya çıkabilmektedir. Bu sebeple ülkeler sürekli olarak siber alanda güvenliklerini sağlamak için yeni güvenlik önlemleri almalıdır. Yeterli düzeyde güvenlik önlemlerinin alınmaması ülke açısından çok büyük zararlara sebebiyet verecektir. Gerçekleşen saldırıların kaynağının tespitinin yapılamaması da hukuki alanda yaptırımlar için yetersiz kalmaktadır ve yargı alanında da yetersizliklerin olduğunu göstermektedir. Bu yetersizliklerin ortadan kaldırılması için siber güvenlik politikalarına özgü kanunlar oluşturulmalıdır.

Devlet içerisinde kamu kurumları ve kuruluşları, özel kurum ve kuruluşları kendi özel sistemleri üzerinden birçok hizmet vermektedirler. Bu hizmetlerin yanında internet üzerinden de hizmetleri yürütmektedirler. Kamu ve özel kurumların internet üzerinden verdikleri hizmetler, kritik alt yapıların siber saldırılar karşısında savunmasız olmasına neden olmaktadır. Olası siber saldırılar sonrasında tüm kamu ve özel kurumların verilerinin çalınabilme, yok edilme ihtimalleri söz konusudur. Bunların önüne geçebilmek adına ya internet kullanılmadan kendi içlerinde oluşturdukları sistemler üzerinden hizmet vermeli ya da bu hizmetlerin verildiği alanda ciddi derecede güvenlik önlemleri alınması gerekmektedir. Gelişen teknoloji sebebiyle her kurumun bünyesinde çalışan kişilerin siber güvenlik alanında bilgi sahibi ve uzmanlıklarının olması gerekmektedir.

Siber güvenlik kavramı, siber güvenlik politikaları günümüzde ülkelerin en önemli üzerinde durması gereken konulardan birisi haline gelmiştir. İnternetin aktif olarak kamu ve özel sektör hizmetlerinde kullanılması, verilerin internet ortamından aktarılması ve saklanması, kritik alt yapıların aktif olarak interneti ve gelişen teknolojiyi takip ederek bu siber saldırılara karşı savunma mekanizmaları oluşturmalıdır. Bu savunma mekanizmaları oluşturulurken yeterli düzeyde kurum

içinde yetkin ve uzman personeller çalıştırmalıdır. Aynı zamanda siber güvenlik ile alakalı eğitimler düzenleyerek çalışan personellerin siber güvenlik alanında bilgilendirmelidir.

Tüm bunların yanında siber güvenlik sağlanırken yetkin ve uzman personeller ile milli araçlar kullanılmalı, AR-GE çalışmaları yaparak ülkenin kendisine ait siber güvenlik araçları oluşturmalıdır.

Ülkemiz açısından değerlendirme yapıldığında Türkiye'de listenin altlarında yer almasından ötürü kendisini siber alanda geliştirerek olası siber saldırılar karşısında durabilmelidir ve bunun için sürekli olarak çalışmalıdır. Siber alanda diğer ülkeler gibi geniş kapsamlı çalışmalar yapmak zorundadır. Tüm bu çalışmaların yanında AR-GE çalışmalarını artırarak yerli ve milli siber güvenlik unsurlarının oluşturulması gerekmektedir. Politikalarını hazırlarken, listenin başında gelen ülkelerin politikalarının analizlerinin yapılarak politika hazırlama yoluna gidilmelidir. Kamu hizmetlerinin gerçekleştirilmesi adına yeni milli uygulamaların geliştirilmesi, veri tabanları yerli ve milli olarak hazırlanan platformlarda saklanabilmelidir.

Çalışma hazırlanırken incelenen tüm kaynaklar doğrultusunda ülkemizin siber güvenlik alanında kendini geliştirmeye çalıştığı saptanmıştır. Çalışma için yapılan literatür taramasında kaynak sayısının az olduğu, bu konuda sayılan doktora ve yüksek lisans tezlerinin sayısının az olduğu, yayımlanan makalelerin bu alandaki çalışmaların yapılması için teşvik edici olduğu tespit edilmiştir. Bu çalışma siber güvenlik politikalarını incelemek için örnek bir çalışma halinde hazırlanmıştır.

Sonuç olarak değerlendirdiğimizde bu çalışma ile siber güvenlik kavramının, siber tehditlerin, siber saldırı ve savunma araçlarının ne olduğu, siber güvenlik politikaları oluşturulurken nelerin dikkate alınması gerektiğine değinilmiştir. Ülkemiz açısından siber güvenlik alanında hangi çalışmaların yapıldığı, dünya üzerinde siber güvenlik konusunda yerinin, sırasının kaçıncı olduğu, diğer dünya ülkeleri ile kıyaslandığında siber güvenlik çalışmalarının benzer ya da farklı yönleri saptanmıştır. Gelişen teknoloji ile fiziki savaşlar yerini siber savaşlara bırakacaktır.

Bu sebeple ülkelerin siber alanda kendilerini geliştirmeleri, askeri alanda yaptıkları çalışmalar kadar siber güvenlik alanında da çalışmalar yapmak zorundadırlar.

Siber güvenlik konusu daima güncelliğini koruyabilecek bir konudur. Gelişen teknoloji ve dünya standartlarının artması insanların siber güvenlik politikalarına bağımlılığını, ihtiyacını artıracaktır. Bu çalışma ile siber güvenlik kavramı ve siber güvenlikle alakalı kavramların tamamı, Türkiye'nin ve dünyada siber güvenlikte güç olarak başta gelen ülkelerin politikaları incelenmiştir. Türkiye'nin bu çalışma ile dünya üzerindeki yeri saptanmış, ulusal olarak siber güvenlik politikaları hakkında farkındalığın, yetkinliğin artırılması gerektiği amaçlanmıştır. Hazırlanan eylem planları, birbirlerinden farkları, eksikleri belirlenmiş, bir sonraki eylem planında söz konusu eksikliklerin yapılmaması için çalışılmıştır. Hem Türkiye hem de belirli dünya ülkelerinin güç sıralaması belirlenmiş ve sonraki akademik çalışmalar açısından bir kaynak hazırlanmıştır.

KAYNAKÇA

ADA, Mehmet ve Hüseyin Çakır (2017). "Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi", **Düzce Üniversitesi Bilim ve Teknoloji Dergisi**, Cilt. 5, Sayı. 2, ss. 632-656.

ADA, Mehmet (2018). **NATO Üyesi Ülkelerin Siber Güvenlik Stratejileri Açısından İncelenmesi**, Ankara: Adli Bilişim Ana Bilim Dalı, Yüksek Lisans Tezi.

AFYONLUOĞLU, Mustafa (2020). **Teknoloji ve Kamu Politikaları Kitabı**, (Ed.: Mete Yıldız-Cenay Babaoğlu), Ankara, Gazi Kitabevi.

AKKAYA, Mariye Umay (2014). "Siber Güvenlik Standartları ve Belgelendirmeleri", **ICSG İstanbul 8/9 Mayıs**, 2014, ss. 48-51 .

ALİOĞLU, Su Dilara (2019). **Siber Saldırılar ve Ülkelerin Siber Güvenlik Politikaları**, İstanbul Bilgi Üniversitesi Lisanüstü Programlar Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, İstanbul.

ALTINIŞIK, Halim (2017). Hibrit Savaş ve Siber Saldırılar. http://webcache.googleusercontent.com/search?q=cache:bHvUyQuekg4J:www.siberteror.org/siberteror2017/files/HalimAltinisik.pdf+&cd=5&hl=tr&ct=clnk&gl=tr (Erişim Tarihi: 01.10.2021)

ALTINTAŞ, Emine (2014). **Ulusal Siber Güvenlik Çalışmaları**, International Cyber Warfare and Security Conference, https://slideplayer.biz.tr/slide/2785253/ (Erişim Tarihi: 02/06/2022)

ASLAY, Fulya (2017). "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi", **International Journal of Multidisciplinary Studies and Innovative Technologies**, Sayı:1, ss. 24-28.

AYDIN, Mustafa (Ed.) (2013). **21.Yüzyılda Siber Güvenlik**, 1.Baskı, İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

BAŞA, Şafak (2012). **ABD İç Güvenlik Bakanlığı**, https://www.academia.edu/9830086 (Erişim Tarihi: 05/02/2022)

BIÇAKCI, Salih (2013), **21. Yüzyılda Siber Güvenlik**, İstanbul Bilgi Üniversitesi Yayınları.

BIÇAKÇI Salih, F. Doruk Ergün ve Mithat Çelikapala (2015). "Türkiye'de Siber Güvenlik" **Edam Siber Politika Kağıtları Serisi** 2015/1, ss. 1-35

BIÇAKÇI, Salih, F. Doruk Ergün ve Mithat Çelikpala (2016). **Türkiye'de Siber Güvenlik ve Nükleer Enerji**, 1. Baskı, İstanbul: İmak Ofset Basım Yayın

CEYHAN, Eyüp Burak, Ebru Demiryürek ve Büşra Kandemir (2015). "Sosyal Ağlarda Güncel Güvenlik Riskleri ve Korunma Yöntemleri", **Uluslararası Bilgi Güvenliği Mühendisliği Dergisi**, Cilt. 1, Sayı. 1, ss:1-10

CLARK, David, Thomas Berson and Herbert S. Lin (2014). At the Nexus of Cybersecurity and Public Policy". **National Research Council** of **The Natinaonal Academies Press**, Washington DC, ss. 1-116

CLARKE, Richard A. and Robert K. Knake (2010). **Cyber War – The Next Threat to National Security and What to Do About It**, New York DC: HarperCollins. Ss. 1-36

ÇALIŞKAN, Bülent (2018). **Siber Güvenliğin Önemi ve Alınabilecek Tedbirler**, Yönetim Bilişim Sistemleri Yüksek Lisans Programı Dönem Ödevi

ÇELİK, Şener (2013). "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:15, Sayı 1.

ÇELİKTAŞ, Barış (2016). **Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme**, Yüksek Lisans Tezi.

ÇELİKTAŞ, Barış (2018). "Cyber Security Power Ranking By Country and Its Importance On World Politics", **The Journal of Academic Social Science Studies**, Sayı: 67, ss. 469-488

ÇİFÇİ, Hasan (2013). **Her Yönüyle Siber Savaş**, İstanbul: TÜBİTAK Popüler Bilim Kitapları

ÇİTLİOĞLU, Ercan (2008). **Gri Tehdit Terörizm**, Ankara, Başak Matbaacılık ve Tanıtım Ltd.Şti.

DARICILI, Ali Burak (2017). "Demokrat Parti Hack Skandalı Bağlamında ABD ve RF'nin Siber Güvenlik Stratejilerinin Analizi", **Uluslararası Çalışmalar Dergisi**, Cilt. 1, Sayı. 1, ss. 1-24

DARICILI, Ali Burak (2019). "Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Potansiyel Siber Güvenlik Stratejisi", **TESAM Akademi Dergisi**, Cilt.6 Sayı

DEMİRCİ, Kıvanç (2021). "Kritik Altyapılarda Siber Güvenlik ve AFAD Üzerinden Bir Değerlendirme", **Nazilli İktisadi ve İdari Bilimler Fakültesi Dergisi, Cilt.2 Sayı. 2**

DEMİREL, Murat (2012). **Asimetrik Tehdit Kavramı Bağlamında 11 Eylül 2001 Sonrası Dönemde Amerika Birleşik Devletleri'ndeki Siber Tehdit Algılamasının ve Geliştirilen Güvenlik Politikalarının İncelenmesi,** Kara Harp Okulu/Savunma Bilimleri Enstitüsü, Ankara

DENNESEN, Kristen (2011). **Cyber Warfare An Analysis of the Means and Motivations of Selected Nation States**, http://www.cu.ipv6tf.org/lacnic15/LACNICV3.pdf (Erişim Tarihi: 15/04/2022)

DİJİTAL TÜRKİYE PLATFORMU, (2017). Türkiye'nin Siber Güvenlik Stratejisine Yönelik Değerlendirmeler. İstanbul: Dijital Türkiye

DOD (2011). Department of Defense Strategy for Operating in Cyberspace. Department of Defense. Erişim tarihi: 17.04.2017, http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operatingin-Cyberspace.pdf

DURNA, İ. Deniz, (2012). **Siber Güvenlik Raporu 2012** https://docplayer.biz.tr/1001726-Siber-guvenlik-raporu.html (Erişim Tarihi: 04/04/2022)

GİEROW, Hauke Johannes (2015). "Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses" **Mercator Institute for China Studies**, Sayı:22, ss. 1-10.

GÖÇOĞLU, Volkan ve Mehmet Devrim AYDIN (2019). "Siber Güvenlik Politikası: ABD, Rusya ve Çin Üzerine Karşılaştırmalı Bir Analiz", **Güvenlik Bilimleri Dergisi,** Kasım 2019, Cilt. 8 Sayı. 2, ss. 229-252

GRAHAM, James ve Richard Howard (2010). **Cyber Security Essentials,** Boca Raton, Auerbach Publications.

GÜL, Murat (2009). "The Concept of Change and James N. Rosenau: Still International Relations?", **African Journal of Political Science and International Relations**, Vol. 3 (5), pp.199-207

GÜLEÇ, Özge, Zülfükar Aytaç Kişman (2021). "Uluslararası İlişkiler Açısından Siber Güvenlik ve NATO'nun Siber Güvenlik Stratejileri" **Akademik Açı Dergisi,** Cilt. 1, Sayı. 1 ss. 127-154

GÜNEŞTAŞ, Murat ve Oğuzhan Başıbüyük (2015). "Siber Terörizm: Motivasyon ve Yöntem", Ed. (Fatih Tombul) **Siber Suçlar, Tehditler, Farkındalık ve Mücadele İçinde**, Ankara: Global Politika ve Strateji.

GÜNGÖR, Murat (2015). **Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma**, Uzmanlık Tezi, T.C. Kalkınma Bakanlığı, Bilgi Toplumu Dairesi Başkanlığı.

GÜNTAY, Vahit (2018). "Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler", **Güvenlik Stratejileri,** Yıl. 14, Sayı. 27 ss.79-111

GÜRKAYNAK, Muharrem, Adem Ali İren (2011). "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Cilt. 16, Sayı. 2, ss.263-279

HANSEN, Lene ve Helen Nissenbaum (2009). "Digital Disaster, Cyber Security, And The Copenhagen School", **International Studies Quarterly**, Sayı:53, ss. 1155-1175.

HEKİM, Hakan ve Oğuzhan Başıbüyük (2013). "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", **Uluslararası Güvenlik Ve Terörizm Dergisi**, 4(2), 135-158.

IJEASS, Haziran 3, s; 33-44 https://www.gedik.edu.tr/wp-content/uploads/ijeass-cilt-3-sayi-1-2020.pdf (Erişim Tarihi: 05/06/2022)

İngilterenin 2016-2021 Ulusal Siber Güvenlik politikası (National Cyber Security Strategy 2016 to 2021). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (Erişim Tarihi:

İŞ, Hafzullah (2015) Kurumsal Siber Güvenlik Rehberi https://batman.edu.tr/images/files/%C4%B0dari%20Birimler/Bilgi_%C4%B0slem_DB/Kurumsal_Siber_Guvenlik_Rehberi.pdf s: 1-17 (Erişim Tarihi: 07/08/2021)

İTU (2015) Global Cybersecurity Index (GCI) 2015 https://www.itu.int/pub/D-STR-SECU-2015 (Erişim Tarihi: 07/08/2021)

İTU (2017). Global Cyber security Index (GCI) 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017- PDF-E.pdf (Erişim Tarihi: 10/10/2021)

JONASSON Daniel ve Johan Sigholm (2005). **"What is Spyware",** http://docplayer.net/8724618-What-is-spyware-daniel-jonasson-danjo620-studentliu-se-johan-sigholm-johsi264-studen-liu-se-abstract-2-theory.html (Erişim Tarihi: 07/10/2021)

KARA, Mahruze (2013). **Siber Saldırılar, Siber Savaşlar ve Etkileri,** İstanbul Bilgi Üniversitesi, İstanbul

KARASOY, Hasan Alpay ve Pelin Babaoğlu (2021). "Türkiye'de Siber Güvenlik: Yasal ve Kurumsal Alt Yapı", **Yasama Dergisi**, Temmuz-Aralık 2021, Sayı: 44, ss: 123-155

KAY, Sean (2004). "Globalization, Power and Security", **Security Dialogue**, Sayı:35, ss. 9-25.

KELEŞTEMUR, Atalay (2015). **Siber İstihbarat**,1. Baskı, İstanbul: Yazın Basın Yayınevi Matbaacılık Trz.Tic.Ltd.Şti.

KINIKOĞLU, B.Y. (2012). **Birleşik Krallık İncelemesi**, İstanbul Bilgi Üniversitesi, Bilişim ve Teknoloji Hukuku Enstitüsü ss.30

KIZILAY, Şeyma (2020). "Soğuk Savaş Sonrası ABD'nin Siber Güvenlik Politikası", **International Journal of Economics Administrative and Social Sciences,** Cilt:3, Sayı:1, ss.33-44.

KORFF, Douve (2020). Cyber Security Definitions. UK: Associate of the Oxford Martin School of the University of Oxford's Global Cybersecurity Capacity Centre.

KUTLU, Önder, Selçuk Kahraman ve Selçuk Dinçer (2019). "Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Politikalarının Analizi", **Assam Uluslararası Hakemli Dergi**, 13. Uluslararası Kamu Yönetim, Sempozyumu Bildirileri Özel Sayısı

LEWİS, James A. ve Katrina Timlin (2011). "Cybersecurity and Cyberwarfare**," Center For Strategic and International Studies**, (http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfarepreliminary-assessment-of-national-doctrine-and-organization-380.pdf)

OF, Mustafa (2019). "A Research on Cyber Security: Software Security" **Bayburt Üniversitesi Fen Bilimleri Dergisi,** c:2 s:2 ss: 1-7

ÖĞÜN, M.Nesip ve Adem Kaya (2013). "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", **Güvenlik Stratejileri Dergisi**, Yıl. 9, Sayı. 18 ss. 145-181

ÖNOK, Murat (2013)**. "**Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt.19, Sayı. 2

RALSTON, Patricia A.S ve James H. Graham, Jeffrey L. Hieb (2007). "Cyber Security Risk Assessment For SCADA And DCS Networks", **ISA Transactions**, Sayı:46, ss. 583-594

RAUD, Mikk (2016). "China and Cyber: Attitudes, Strategies, Organization", **Tallinn Universıty of Technology Department of Computer Scıence,** Sayı:18, ss. 12-15

RİD, Thomas ve Peter McBurney (2012). "Cyber-Weapons", **The RUSI Journal**, February/March Sayı: 157, ss. 6-13

SANALP, Sinem (2016). **Çeşitli Ülkelerde Usom ve Some Yapılandırılması ve Türkiye Modeli Önerisi**, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilgi Üniversitesi Doktora Tezi

SEREN, Merve (2016). **Stratejik İstihbaratın Güvenlik Stratejileri ve Politikaları Açısından Yeri ve Önemi**, Doktora Tezi, Ankara

SEREN, Merve (2016). "Siber Tehditlerle Mücadelede Farkındalık ve Hazırlık" **Siyaset, Ekonomi ve Toplum Araştırmaları Vakfı (SETA) Analiz**, Sayı. 183, ss. 6-27

SERTÇELİK, Aşır (2015). "Siber Olaylar Ekseninde Siber Güvenliği Anlamak", **Medeniyet Araştırmaları Dergisi**, Cilt. 2, Sayı. 3, ss. 25-42.

SHAFQAT, Narmeen ve Ashraf Masood (2016). "Comparative Analysis of Various National Cyber Security Strategies", **International Journal of Computer Science and Information Security**, Sayı: 14, Cilt: 1, ss. 129-136

SOLMS, Rossouw Van ve Niekerk, Johan (2013). "From Information Security To Cyber Security", **Computers & Security**, Sayı: 38, ss. 97- 102.

SOMUNCU, Gizem (2018). **NATO'nun Güvenlik Alanında Yeni Bir Boyut: Siber Güvenlik**, İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi.

SONALP, Sinem (2016). **Çeşitli Ülkelerde Usom ve Some Yapılandırılması ve Türkiye Modeli Önerisi**, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilgi Üniversitesi Doktora Tezi

SYMANTEC, (2018). **2017 Norton Cyber Security Insights Report Global Results**. "https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf" (Erişim Tarihi: 03/02/2022)

SWAİNE, Michael D. (2013). "Chinese Views on Cybersecurity in Foreign Relations", **China Leadership Monitor**, Sayı:42, ss. 1-27.

ŞENTÜRK, Hakan, C. Zaim Çil, Şeref Sağıroğlu (2012). "Cyber Security Analysis of Turkey" **International Journal of Information Security Science,** Cilt.1, Sayı. 4 ss.112-125

TATAR, Ünal (2011). **Dünyada ve Türkiye'de Siber Güvenlik Tatbikatları**, http://www.bilisimdergisi.org.tr/s134/pdf/108-109.pdf (Erişim Tarihi: 08/05/2022)

TBMM "3765 sayılı Türk Ceza Kanunun Bazı Maddelerinin Değiştirilmesine Dair Kanun", Kanun No. 3756 Kabul Tarihi 6.6.1991 (Resmi Gazete ile yayımı 14.6.1991,Sayı:20901) http://www.kanunum.com/files/kanun_tbmm_c074_03756.pdf (Erişim Tarihi: 08/07/2022)

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürlüğü, Kurumsal SOME Kurulum ve Yönetim Rehberi, Temmuz 2014

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürlüğü Sektörel SOME Kurulum ve Yönetim Rehberi, Temmuz 2014

T.C. Resmi Gazete, (2006, Temmuz 28) No: 26242, "Bilgi Toplumu Stratejisi Eylem Planı (2006-2010) http://www.resmigazete.gov.tr/eskiler/2006/07/20060728-7.html (Erişim Tarihi: 19/07/2022)

The White House (2003). The National Strategy to Secure Cyberspace https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf (Erişim Tarihi: 28/08/2022)

TOPÇU, Servet Habip (2022). "Rusya Federasyonu'nun Siber Güvenlik Stratejisi: Kırım Örneği", **Uluslararası İlişkiler Çalışmaları Dergisi**, Cilt:2 Sayı:1 19-35

TURHAN, Meltem (2010). **Siber Güvenliğin Sağlanması Dünya Uygulamaları ve Ülkemiz İçin Çözüm Önerileri**, Ankara: Bilgi Teknolojileri ve İletişim Kurumu Uzmanlık Tezi

UDHB 2012, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Ankara s: 9-47

Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, 2012:3842, https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf Erişim Tarihi: 06/07/2022)

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı

Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı

Ulusal Siber Güvenlik Stratejisi ve 2020-2023 Eylem Planı

ÜNAL, Sevda (2016). "Legitimization Of Surveillance And Control Through Securitization Discourse Of Cyber space: USA, Eu And Turkey Examples", **Jass StudiesThe Journal of Academic Social Science Studies**, Sayı: 42, ss. 409-430, Winter III 2016.

ÜNVER, Mustafa ve Cafer Canbay (2011). "Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik", **Elektrik Mühendisliği Dergisi**, ss. 94-103, 2011

ÜNVER, Mustafa, Cafer Canbay ve Ayşe Gül Mirzaoğlu (2009). **Siber Güvenliğin Sağlanması: Türkiye'de Mevcut Durum ve Alınması Gereken Tedbirler**, Bilgi ve Teknolojileri Kurumu, Ankara, 2009

ÜNVER, Mustafa, Cafer Canbay ve Hüseyin Burhan Özkan (2011). **Kritik Altyapıların Korunması,** 1. Baskı, Nisan 2011, Ankara: BTK

URL,https://www.sibersan.com/sanal-ortamda-islenen-suclar-sozlesmesi-6533-sayili-yasa/ (Erişim Tarihi: 12/07/2022)

URL, "Ayyıldız Tim Misyonu", https://www.ayyildiztim.com.tr/ (Erişim Tarihi: 06/06/2022)

URL,"RedHack Emniyeti hackledi mi?", http://www.milliyet.com.tr/RedHack-emniyet-i-hackledi-mi /gundem/detay/1759446/default.html (Erişim Tarihi: 18/05/2022)

URL,https://tr.wikipedia.org/wiki/Beyaz_%C5%9Fapkal%C4%B1_hacker (Erişim Tarihi: (16/05/2022)

URL, http://www.turkhackteam.org/misyon.html (Erişim Tarihi: 26/05/2022)

URL,https://spysecurity.net/cyber-warrior-misyonunu-tamamladi (Erişim Tarihi: 14/12/2022)

URL,https://tr.wikipedia.org/wiki/Siber_ter%C3%B6rizm (Erişim Tarihi: 09/10/2021)

URL,https://tr.wikipedia.org/wiki/Kategori:Kriptografik_saldırılar (Erişim Tarihi: 14/10/2021)

URL, https://it.bilgi.edu.tr/tr/guvenlik/antivirus (Erişim Tarihi: 15/10/2021)

URL,https://ata.com.tr/blog-detay/antivirus-nedir-virusten-koruma-programi-ne-ise-yarar-205 2020 (Erişim Tarihi: 16/10/2021)

URL,https://www.atakdomain.com/blog/anti-spam-nedir (Erişim Tarihi: 28/10/2021)

URL,https://kurumsal.turktelekom.com.tr/bilisim-teknolojileri/siber-guvenlik/siber-guvenlik-urunleri/icerik-filtreleme (Erişim Tarihi: 27/10/2021)

URL,https://www.kaspersky.com.tr/resource-center/threats/what-is-a-honeypot (Erişim Tarihi: 19/10/2021)

URL, https://bilirkisi

raporlari.com/adli-bilisim-nedir (Erişim Tarihi: 01/11/2021)

URL,https://tr.linkedin.com/pulse/u%C3%A7-noktaendpoint-g%C3%BCvenli%C4%9Fi-fevziye-tas 2019 (Erişim Tarihi: 25/10/2021)

URL,https://medium.com/clevelteam/%C5%9Fifreleme-kriptografi-nedir-%C5%9Fifreleme-tarihi-ve-gelece%C4%9Fi-22b4ffe0ea3d (Erişim Tarihi: 20/10/2021)

URL,https://ebysweb.ogu.edu.tr/Sayfa/Index/35/e-imza-nedir 2019 (Erişim Tarihi: 17/10/2021)

URL,https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/vir%C3%BCs-solucan-ve-truva-at%C4%B1 (Erişim Tarihi: 25/11/2021)

URL,https://www.kaspersky.com.tr/resource-center/definitions/what-is-rootkit (Erişim Tarihi 22/10/2021)

URL,https://tr.wikipedia.org/wiki/kök_kullanıcı_takımı (ErişimTarihi22/10/202)

URL,https://lostar.com.tr/2016/09/backdoor-arka-kapi.html (Erişim Tarihi 20/10/2021)

URL,https://www.isnet.net.tr/BlogIcerik/Phishing-Oltalama-Yemleme-Sald%C4%B1r%C4%B1s%C4%B1-Nedir-isnet-blog (Erişim Tarihi 01/10/2021)

URL,https://teknodestek.com.tr/logicmantik-bombasi-nedir (Erişim Tarihi 22/10/2021)

URL,"ABD Başkanı Obama'dan Siber Güvenlik Paketi", https://www.bbc.com/turkce/haberler/2015/01/150113_obama_siber_guvenlik (Erişim Tarihi: 06/04/2022)

URL,"Trump'tan devrim gibi karar: Her bakanlık kendi siber güvenliğinden sorumlu olacak.", https://siberbulten.com/uluslararasi-iliskiler/trumpdan-devrim-gibi-karar-her-bakanlik-kendisiber-guvenliginden-sorumlu/ (Erişim Tarihi: 15/05/2022)

URL,"US. Department of Homeland Security, Security Strategy.", https://afyonluoglu.org/siberguvenlik/world-css (Erişim Tarihi: 01/09/2022)

URL,http://haber.yasar.edu.tr/teknoloji/siber-guvenlikte-avrupada-6-dunyada-11-siradayiz.html (Erişim Tarihi: 10/10/2022)

URL,https://www.aa.com.tr/tr/analiz/devletlerin-guncel-siber-guvenlik-stratejileri/2062810 (Erişim Tarihi:13/10/2022)

URL,https://www.webtekno.com/siber-guvenlik-en-guclu-ulkeler-h100650.html (Erişim Tarihi: 12/10/2022)

URL, www.usom.gov.tr/index.html (Erişim Tarihi: 08/08/2021)

URL,https://www.savunmasanayiidergilik.com/tr/HaberDergilik/Turkiye-nin-siber-guvenlik-mukemmeliyet-merkezi-HAVELSAN-SiSATEM (Erişim Tarihi: 13/06/2021)

URL,https://www.haberbilimteknoloji.com/2016/03/27/siber-savunma-teknoloji-merkezi-sisatem-acildi (Erişim Tarihi: 30/12/2022)

URL,https://www.resmigazete.gov.tr/eskiler/2016/12/20161203-24.pdf (Erişim Tarihi: 04/03/2022)

URL, https://berqnet.com/blog/usom-nedir, (Erişim Tarihi: 10/10/2021)

URL, https://it.bilgi.edu.tr/tr/guvenlik/usom (Erişim Tarihi: 12/10/2021)

URL,https://www.haber365.com.tr/usom-nedir-h271273 (Erişim Tarihi: 15/07/2021)

URL,"5070 Sayılı Elektronik İmza Kanunu", https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5070.pdf (Erişim Tarihi: 01/03/2022)

URL,"5237 Sayılı Türk Ceza Kanunu", https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf (Erişim Tarihi: 05/04/2023)

URL,"5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf (Erişim Tarihi: 05/05/2021)

URL,"E-Devlet ve Bilgi Toplumu Kanunu Tasarısı", https://www.memurlar.net/haber/146427/e-devlet-ve-bilgi-toplumu-kanun-tasarisi.html (Erişim Tarihi: 11/07/2022)

URL,"Türkiye Ulusal Enformasyon Altyapısı Anaplanı: Sonuç Raporu", http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/991000_TuenaRapor.pdf (Erişim Tarihi: 11/11/2022)

URL,"E-Türkiye Girişimi Eylem Planı", http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/020800_E-TurkiyeEylemPlani.pdf (Erişim Tarihi: 01/09/2022)

URL,"e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı", http://www.lu.gov.tr/wp-content/uploads/2015/02/050000_E DonusunTurkiyeKDEP.doc (Erişim Tarihi: 05/12/2022)

URLhttps://www.bilisimdergisi.org.tr/s151/pdf/148-151.pdf (Erişim Tarihi: 15/12/2022)

URL,https://www.btk.gov.tr/haberler/ulusal-siber-kalkan-2021-tatbikati-basladi (Erişim Tarihi: 01/01/2023)

URL,https://www.cybermagonline.com/bilgi-teknolojileri-ve-iletisim-kurumu-tarafindan-duzenlenen-ulusal-siber-kalkan-tatbikati039nda-hazine-ve-maliye-bakanligi-1-oldu (Erişim Tarihi: 01/01/2023)

URL,https://www.btk.gov.tr/usom-vekurumsal-siber-olaylara-mudahale-ekibi

URL,"Global Cybersecurity Index, 2017: 60" https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (Erişim Tarihi: 01/02/2023)

URL,https://www.btk.gov.tr/siber-guvenlik-kurulu (Erişim Tarihi: 15/01/2023)

URL, https://sge.bilgem.tubitak.gov.tr/ (Erişim Tarihi: 15/03/2022)

URL,https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security (Erişim Tarihi: 08/02/2023)

URL,https://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf (Erişim Tarihi: 05/02/2023)

URL,https://webrazzi.com/2012/01/06/japonyadan-milli-guvenlik-virusu/ (Erişim Tarihi: 09/02/2023)

URL,http://afyonluoglu.org/PublicWebFiles/strategies/Asia/Japan%202018%20National%20Cyber%20Security%20Strategy-EN.pdf (Erişim Tarihi: 04/03/2023)

URL,http://www3.weforum.org/docs/WEF GlobalRisks_Report_2013.pdf**,** (Erişim Tarihi: 04/04/2023)

URL,https://www.uscert.gov/sites/default/files/publications/cyberspace_strategy.pdf (Erişim Tarihi: 04/04/2023)

URL, "Cyber Security Strategy of The United Kingdom Safety, Security and Resilince İn Cyber Space, Cabinet Office, 2009," https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf (Erişim Tarihi: 02/04/2023)

URL,"The National Security Strategy, 2010" https://www.ojp.gov/ncjrs/virtual-library/abstracts/national-security-strategy-may-2010 (Erişim Tarihi: 01/04/2023)

URL,"Cyber Crime Strategy, 2010)" https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf (Erişim Tarihi: 09/03/2023)

URL,"The UK Cyber Security Strategy: Protecting and Promoting The UK in a Digital World, 2011", https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (Erişim Tarihi: 01/02/2023)

URL,"National Cyber Security Strategies, 2012" https://www.enisa.europa.eu/publications/cyber-security-strategies-paper (Erişim Tarihi: 08/01/2023)

URL,https://www.mcafee.com/tr-tr/antivirus/malware.html (Erişim Tarihi: 03/04/2022)

VALENTİNO Jennifer ve Danny Yadron (2015). **Cataloging the World's Cyber Forces,** https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710 (Erişim Tarihi: 02/02/2023)

YAZICI, Ali (2011). **Siber Güvenlik ve SAHAB**, https://www.emo.org.tr/ekler/ad10c28377689d7_ek.pdf (Erişim Tarihi: 03/03/2023)

YAZICI, Ali (2012). "Küresel Tehlike: Siber Savaş, Siber Güvenlik", **Mimar ve Mühendis Dergisi**, Sayı: 68, ss. 36-40

YILDIZ, Mithat (2014). **Siber Suçlar ve Kurum Güvenliği**, T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı Bilgi İşlem Dairesi Başkanlığı

YUE, Oc (2003). "Cyber Security" **Technology İn Society**, Sayı: 25 ss. 565-569

YÜKSEKTEPELİ, Onur (2013). https://www.mshowto.org/bilgi-guvenliginde-vulnerability-assessment-ve-penetration-test-nedir-ne-amacla-kullanilir.html (Erişim Tarihi: 02/10/2021)