KARADENİZ TEKNİK ÜNİVERSİTESİ * SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI

ULUSLARARASI İLİŞKİLER PROGRAMI

SİBER GÜVENLİK KAVRAMININ GELİŞİMİ VE TÜRKİYE ÖZELİNDE BİR DEĞERLENDİRME

YÜKSEK LİSANS TEZİ

Barış ÇELİKTAŞ

MAYIS - 2016

TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ * SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI

ULUSLARARASI İLİŞKİLER PROGRAMI

SİBER GÜVENLİK KAVRAMININ GELİŞİMİ VE TÜRKİYE ÖZELİNDE BİR DEĞERLENDİRME

YÜKSEK LİSANS TEZİ

Barış ÇELİKTAŞ

Tez Danışmanı: Prof. Dr. Hayati AKTAŞ

MAYIS - 2016

TRABZON

ONAY

Barış ÇELİKTAŞ tarafından hazırlanan "Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme" adlı bu çalışma 30.05.2016 tarihinde yapılan savunma sınavı sonucunda *oy birliği* ile başarılı bulunarak jürimiz tarafından *Uluslararası İlişkiler Anabilim* dalında **yüksek lisans tezi** olarak kabul edilmiştir.

Prof. Dr. Hayati AKTAŞ (Başkan/Danışman)

Prof. Dr. Mohammad ARAFAT

Doç. Dr. Ertan EROL

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduklarını onaylarım. … /… / 2016

Prof. Dr. Ahmet ULUSOY
Enstitü Müdürü

BİLDİRİM

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını, aksinin ortaya çıkması durumunda her tür yasal sonucu kabul ettiğimi beyan ediyorum.

Barış ÇELİKTAŞ

27/04/2016

ÖNSÖZ

İnternete bağlı olmayan sistemlerin neredeyse hiç kalmadığı günümüzde, kişi, kurum, kuruluş ve ülkeler için siber güvenlik kavramı, hayati öneme haiz bir hal almakla birlikte teknolojik gelişimlere paralel olarak, çok hızlı bir şekilde değişerek gelişmektedir. Bu kavramın gelecekte, ülkelerin milli güçlerinin vazgeçilmez ve en belirleyici unsuru olacağı aşikârdır. Tarih boyunca gücü elinde tutarak sınırlarını koruyan ve varlıklarını sürdüren devletler, yavaş yavaş milli güçlerinin merkezinde yer almaya başlayan siber güvenlik güç ve kapasitelerini artırma eğilimi içerisine girmişlerdir. Burada önemli olan, her geçen gün konrolü daha da zorlaşan siber uzaya, kimlerin daha iyi ayak uyduracağı ve bu ortamda daha iyi hareket kabiliyetine erişeceğidir. Türkiye'de konu hakkında oldukça sınırlı kaynağın bulunması sebebiyle, araştırma ve akademik çalışmaların yapılmasının teşvik edilmesi ve insanların siber güvenlik konusunda yeterli seviyede farkındalık ve bilinç seviyesine ulaştırılması amacıyla "Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme" adlı tez çalışmamız hazırlanmıştır. Ayrıca, ulu önder Gazi Mustafa Kemal Atatürk'ün Onuncu Yıl Nutkunda belirttiği "Millî kültürümüzü, muasır medeniyet seviyesinin üstüne çıkaracağız" amacına ulaşılabilmenin yolunun en kısa sürede, siber uzaya ülke olarak adapte olabilmek ve siber uzayı kendi ulusal menfaatlerimiz uğruna kullanabilmek için ileri seviyede milli, bilgi ve iletişim teknolojilerine sahip olabilmekten geçmektedir.

Yüksek lisans tez danışmanlığımı üstlenerek, çalışmam esnasında ilgi ve desteğini esirgemeyen, engin bilgi ve tecrübelerinden yararlandığım değerli hocam Prof. Dr. Hayati AKTAŞ'a, tezimin yazımı esnasında her soruma içtenlikle cevap veren ve beni yönlendiren hocam Arş. Gör. Vahit GÜNTAY'a, tezin imla ve yazım kuralları bakımından gerekli kontrolleri ve düzeltmeleri yapan değerli eşim Dr. M. Melis ÇELİKTAŞ'a sonsuz teşekkürlerimi borç bilirim. Tezimi bu topraklar için gözünü hiç kırpmadan canını feda eden şehitlerimize ithaf ediyorum.

Trabzon, Mayıs, 2016 Barış ÇELİKTAŞ

İÇİNDEKİLER

İKİNCİ BÖLÜM

ÜÇÜNCÜ BÖLÜM

DÖRDÜNCÜ BÖLÜM

ÖZET

Günümüzde ülkeler, teknolojik imkân ve kabiliyetlerini geliştirerek siber uzayda hak sahibi olabilmek ve bu alanda nüfuzlarını artırmak istemektedirler. Teknolojiye ve internete daha çok bağımlı hale gelen ülkeler, siber saldırıların vazgeçilmez bir unsuru olan internet üzerinden, çok daha rahat bir şekilde siber saldırılara maruz kalabilmektedir. Bu siber saldırıların, genellikle ülkeler için hayati öneme haiz olan ulaşım, enerji, su, finans ve haberleşme gibi kritik altyapı sektörlerine yapıldığını düşünürsek, sonuçları itibariyle, çok büyük maddi zararlar, can ve mal kayıpları yaşanabilecek ve bu sektörlerden bir süre hizmet alınamaz hale gelinebilecektir. Kendi savunma mekanizmalarını oluşturarak, belirsizliklerle dolu siber uzayı, yeni huzursuzluklar doğurmadan, kontrol altına alabilecek siber güvenlik çalışmaları ve politikalarını belirlemek zorunda olan devletler, dünyada yaşanmış siber saldırı örneklerinin sebeplerini, sonuçlarını ve uluslararası ilişkilerdeki rolünü göz ardı etmeden incelemeli ve muhtemel siber saldırılara karşı ulusal farkındalık, hazırlık ve güvenlik seviyelerini artırmalıdır. Ayrıca siber güvenlik kavramının temel bileşenlerinin özümsenerek anlaşılması, kavram karmaşasını ortadan kaldıracak, siber güvenlik kavramının daha iyi bir şekilde anlaşılmasını sağlayacak, uluslararası ilişkiler boyutunda etkileri daha iyi görülecek ve vuku bulan siber olayların sebepleri ve sonuçları daha iyi değerlendirilecektir.

Sonuç olarak, siber güvenlik kavramının bileşenlerini çok iyi bir şekilde idrak etmek, yaşanmış siber saldırı örneklerinden ders çıkararak yeterli seviyede bilinç ve farkındalık seviyesine ulaşmak, uluslararası örgütler ve devletler nezdinde yürütülen siber güvenlik çalışmaları ve politikalarını çok iyi anlayarak ulusal siber güvenlik politika ve eylem planlarını oluşturmak, devletlerin siber güvenlik ile ilgili yürütmek zorunda olduğu asıl amaçları arasında olmalıdır.

Anahtar Kelimeler: Kritik Altyapı Sektörleri, Siber Güvenlik, Siber Saldırı, Siber Uzay, Teknoloji.

ABSTRACT

In today's world, countries strive to be in a favorable position in the cyber space and improve their influence by enhancing technological adequacy and capabilities. Countries which are deeply dependent on technology and internet can be exposed to cyber-attacks more over the internet, an indispensable element of cyber-attacks. Considering that these cyber-attacks usually target the critical infrastructure sectors such as transportation, energy, water, finance, and telecommunications, which one of utmost importance for the countries. It is not hard to imagine the possibility of immense financial losses, loss of life and property and drastic reductions in services that can be experienced if such attacks occur. Therefore, countries, by creating their own defense mechanisms, should develop their own cyber security studies and policies to take control of cyberspace filled with uncertainties without new unrest occurred. The causes, the effects and the role in international relations of cyber-attacks should not be ignored, but examined and the level of national awareness, preparation and security against possible cyber-attacks should be increased by all countries. Thus, understanding the basic components of cyber security will also eliminate the confusion surrounding the concept and provide a better discernment on the subject. It will also reveal its effects in the area of international relations by making it possible to better assess the causes and the effects of cyber incidents.

Consequently, achieving an adequate level of consciousness and awareness by identifying lessons from the examples of experienced cyber-attacks, by recognizing the components of the concept of cyber security better, and creating their national cyber security policy and action plans by understanding very well of cyber security studies and policy conducted by international organizations and states should be among the main goals about cyber security which the states have to conduct.

Key Words: Critical Infrastructure Sectors, Cyber-Attacks, Cyber Security, Cyber Space, Technology.

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

GRAFİKLER LİSTESİ

RESİMLER LİSTESİ

KISALTMALAR LİSTESİ

AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
AFAD	: Afet ve Acil Durum Yönetim Başkanlığı
AGİT	: Avrupa Güvenlik ve İşbirliği Teşkilatı
APT	: Advanced Persistent Threats, Gelişmiş Siber Tehditler
AR-GE	: Araştırma Geliştirme
ASELSAN	: Askeri Elektronik Sanayii
BGP	: Border Gateway Protocol, Sınır Geçit Protokolü
BİLGEM	: Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BM	: Birleşmiş Milletler
BİT	: Bilgi ve İletişim Teknolojileri
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
C4ISR	:Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance, Komuta, Kontrol, Haberleşme, Bilgisayar, İstihbarat, Keşif ve Gözetleme Sistemleri
CCD CoE	:Cooperative Cyber Defence Enter of Exellence, Müşterek Siber Savunma Mükemmeliyet Merkezi
CERT	: Computer Emergency Response Teams
CNAP	:Cybersecurity National Action Plan, Siber Güvenlik Ulusal Eylem Planı
CSSL	: Siber Güvenlik Hizmet Hattı
CTF	: Siber Güvenlik Simülasyon ve Yarışma Ortamı
DARPA	:The Defense Advanced Research Projects Agency, Savunma İleri Araştırma Projeleri Ajansı
DCS	: Distributed Control System, Dağıtık Kontrol Sistemi
DDoS	: Distributed Denial of Service, Dağıtık Hizmet Dışı Bırakma
DHS	: Department of Homeland Security, ABD İç Güvenlik Bakanlığı
DNS	: Domain Name System, Alan Adı Sistemi

DoD	: U.S. Department of Defence, ABD Savunma Bakanlığı
DoS	: Denial of Service, Hizmet Dışı Bırakma
EFTA	: Avrupa Serbest Ticaret Birliği
ENISA	:European Union Agency for Network and Information Security, Ağ ve Bilgi Güvenliği Teşkilatı
FAPSI	:Federal Agency for Government Communications and Information, Devlet İletişim ve Bilişim Federal Teşkilatı
FBI	: Federal Bureau of Investigation, Federal Araştırma Bürosu
FİLTRE	: İnternet Erişim Kontrolü ve Raporlama Sistemi
FSB	:Federal'naya Sluzhba Bezopasnosti, Federal Security Service, Federal Güvenlik Servisi
FTP	: File Transfer Protocol, Dosya Transfer Protokolü
GCI	: The Global Cybersecurity Index, Dünya Siber Güvenlik İndeksi
GSMH	: Gayri Safi Milli Hasıla
HARMAN	: Harici Medya Yönetim Analiz Sistemi
HAVELSAN	: Hava Elektronik Sanayii
http	: Hyper-Text Transfer Protocol, Hiper-Metin Transfer Protokolü
ICS	: Industrial Control Systems, Endüstriyel Kontrol Sistemleri
IDS	: Saldırı Tespit Sistemi, Intrusion Detection System
IPS	: Saldırı Önleme Sistemi, Intrusion Prevention System
IPv4	:Internet Protocol Version 4
IPv6	:Internet Protocol Version 6
ISC	:International Conference on Information Security and Cryptology, Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı
ITU	: Dünya Telekomünikasyon Birliği
JSF	: Joint Strike Fighter
KGB	:Komitet Gosudarstvennoy Bezopasnosti, Committee for State Security, Devlet Güvenlik Komitesi.
MASAK	: Mali Suçları Araştırma Kurumu
MEBS	: Genelkurmay Muhabere, Elektronik ve Bilgi Sistemleri
MGK	: Milli Güvenlik Kurulu
MISP	:Malware Information Sharing Platform, Zararlı Yazılım Bilgi Paylaşımı Platformu

MİT	: Milli İstihbarat Teşkilatı
MN CD E&T	:Multinational Cyber Defence Education and Training, Çok Uluslu Siber Savunma Eğitim ve Öğretim
MN CD2	:Smart Defence Multinational Cyber Defence Capability Development, Akıllı Savunma Çok Uluslu Siber Savunma Yetenek Geliştirme Projesi
NAC	: Network Access Control, Ağ Erişim Kontrol Sistemi
NATO	: Kuzey Atlantik Antlaşması Örgütü
NCIA	: NATO Haberleşme ve Bilgi Sistemleri Ajansı
NCIRC	: NATO Computer Incident Response Capability, NATO Bilgisayar Olaylarına Müdahale Yeteneği
NCISS	:Communications and Information Systems School, NATO Muhabere ve Bilgi Sistemleri Okulu
NDPP	: Defence Planning Process, Savunma Planlama Süreci
NICP	: NATO Industry Cyber Partnership, Sanayi Siber Ortaklığı
NSA	: National Security Agency, Milli Güvenlik Teşkilatı
PLA	: Chinese People's Liberation Army, Çin Halk Kurtuluş Ordusu
RAT	: Remote Administration Tool
s.	: Sayfa
SAHAB	: Sanal Hava Boşluğu Sistemi
SCADA	:Supervisory Control and Data Acquisition, Merkezi Denetleme Kontrol ve Veri Toplama Sistemi
SGE	: Siber Güvenlik Enstitüsü
SİSATEM	: Siber Savunma Teknoloji Merkezi
SMTP	:Simple Mail Transfer Protocol, Elektronik posta gönderme protokolü
SOME	: Siber Olaylara Müdahale Ekipleri
SORT	: Siber Ortam Tuzak Sistemi
STAMP	: Siber Tehditleri Algılama Sistemi
STK	: Sivil Toplum Kuruluşu
STM	: Savunma Teknolojileri Mühendislik ve Ticaret A.Ş.
TCP/IP	:Transmission Control Protocol and Internet Protocol, İletim Kontrol Protokolü ve Internet Protokolü

TİB	: Telekomünikasyon İletişim Başkanlığı
TÜBİTAK	: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TÜİK	: Türkiye İstatistik Kurumu
TBMM	: Türkiye Büyük Millet Meclisi
UDHB	: Ulaştırma, Denizcilik ve Haberleşme Bakanlığı
UEKAE	: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
USAF	: U.S. Air Force, ABD Hava Kuvvetleri
US-CERT	:Computer Emergency Readiness Team, Bilgisayar Olaylarına Müdahale Ekibi
USCYBERCOM	: U.S. Cyber Command, ABD Siber Komutanlığı
USOM	: Ulusal Siber Olaylara Müdahale Merkezi
vb.	: Ve benzeri
VKÖS	: Veri Kaçağı Önleme Sistemi

GİRİŞ

İçinde bulunduğumuz bilgi çağında, bilgi ve iletişim teknolojilerinin çok hızlı bir şekilde gelişmesi, bu teknolojiler tarafından sunulan hizmetlerin her alanda yaygınlaşmasına ve birçok kişi, kurum ve kuruluş tarafından tüm faaliyetlerin ayrılmaz bir parçası haline gelmesine sebep olmuştur. Bütün bu gelişmeler ışığında da bilgi ve iletişim teknolojileri, ülkelerin önemli kritik altyapı sektörleri için yaşamsal hale gelmiştir. Başlangıçta çok büyük yararlar sağlayacağı düşünülse de zaman içerisinde bu bağımlılığın kötü niyetli kişi, grup veya örgütlerce menfaatleri uğruna kullanılması sonucunda, masum kişi, kurum veya devletler çok büyük zararlara uğramıştır.

Siber uzay, bu gelişimler ile birlikte siber saldırı ve tehditlere açık bir hale gelmiş ve organize suç ve terör örgütleri için bir eylem merkezi haline dönüşmüştür. Oluşan saldırı ve tehditler neticesinde de siber güvenlik ve savunma faaliyetleri, kişi, kurum, devlet ve uluslararası alanda önemini artırmıştır.

Geleneksel güvenlik anlayışını terk etmek zorunda kalan kurum, kuruluş, uluslararası örgüt ve devletler, kendi kritik altyapı sektörleri ile bilgi ve iletişim teknolojilerini bu tehditlere karşı koruyabilmek için siber güvenlik ve savunma konusundaki faaliyetlerini hızlandırmak durumunda kalmışlardır. Siber uzaya yönelik saldırıların etkilerini en aza indirebilmek maksadıyla, kritik altyapı sektörlerinin tespit edilmesi, güvenliklerinin sağlanması, alınan teknolojik ve hukuki tedbirlerin geliştirilmesi hususları hâsıl olmuştur.

Siber güvenlik kavramı, bilgi ve iletişim teknolojilerinin çok hızlı bir şekilde geliştiği günümüzde, kişi, kurum, uluslararası örgüt ve devletlerin en önemli gündem maddelerinden biri hâline gelmiştir. Günümüzde önemi tartışılmaz olan siber güvenlik kavramı, gelecekte de önemini sürdürecek konulardan biri olacaktır. Bilgi ve iletişim

teknolojilerine olan bağımlılığımız sürdükçe veya artarak devam ettikçe de, siber güvenlik, öncelikli güvenlik alanlarından biri olmaya devam edecektir.

Çalışmamızın birinci bölümünde, siber güvenlik kavramının temel bileşenlerini oluşturan siber uzay, siber saldırı, siber tehdit, siber suç, siber terör, siber caydırıcılık, siber istihbarat, siber casusluk, siber savaş tanımları ile siber güvenlik kavramının ortaya çıkışı ve uluslararası ilişkilerdeki yeri ve öneminden bahsedilecektir.

Çalışmamızın ikinci bölümünde, yeni bir güvenlik anlayışı olarak ortaya çıkmış olan siber güvenlik algısının gelişimini sağlayan siber uzayın vazgeçilmez aktörleri arasında yer alan siber silahlar hakkında genel bir bilgi verilmesini müteakip, siber saldırı türleri, bu saldırı ve tehditlere karşı korunma ve savunma yöntemleri ile son zamanlarda uluslararası ilişkilerde önemli yer işgal etmiş siber saldırı örneklerinden bahsedilecektir.

Çalışmamızın üçüncü bölümünde, siber saldırı ve tehditlerin boyutlarının her geçen gün arttığı, güvenlik kaygılarının endişe yaratacak boyuta ulaştığı günümüzde, siber güvenlikle ilgili Türkiye adına örnek teşkil edebileceğini düşündüğümüz ABD, Rusya, Çin ve İsrail gibi ülkeler ile AB ve NATO gibi uluslararası örgütlerin hâlihazırdaki durumları ve Türkiye'de siber güvenlik politikaları ve kurumların çalışmalarının son durumu hakkında bilgi verilecektir.

Çalışmamızın son bölümünde ise, açık kaynak verileri ve araştırma şirketleri tarafından yapılan istatistiki çalışmaların derlenmesi sonucunda, bazı dünya ülkelerinin siber savunma, siber saldırı güçlerinin yanında bir de siber uzaya olan bağımlılıklarının da hesaba katılarak Siber Güvenlik Güç ve Kapasiteleri Sıralaması oluşturulacaktır. Oluşturulacak Siber Güvenlik Güç ve Kapasiteleri Sıralaması sonucunda Türkiye'nin siber güvenlik güç ve kapasiteleri ile dünyadaki konumu belirlenmeye çalışılacak ve bu konuda bizden daha önde olan, farklı siber güvenlik stratejileri, politikaları, yaklaşımları ve tedbirleri uygulayan ülkeler hakkında ön bilgi sahibi olunacak ve bu sayede ulusal siber güvenlik farkındalık ve bilinç seviyesi yükseltilmeye çalışılacaktır.

Bu çalışmamızda, bilimsel makale, dergi ve kitapların yanı sıra AB, NATO gibi uluslararası örgütler ile ABD, Rusya ve Çin gibi ülkelerin yayınladığı raporlardan

faydalanılmıştır. Çalışmamızın son bölümüne kaynak oluşturması adına istatistiksel analiz ve siber güvenlik şirketlerinin verilerine de başvurulmuştur. Ayrıca çalışmamızın güncel gelişmeleri kapsaması sebebiyle de internet odaklı açık kaynaklardan, gazete haberlerinden, üst düzey yetkililerin demeç ve söylemlerinden de faydalanılmıştır.

Bu çalışmamızın amaçlarından biri, siber güvenlik kavramının ne olduğunu, uluslararası ilişkilerde önemini anlatabilmek ve bu konu ile ilgili yüksek farkındalık ve bilinç seviyesine ulaştırabilmektir. Siber saldırıların ne oldukları ve bu saldırıların uluslararası ilişkilerde ne derecede etkili olduklarını anlayabilmek için dünyada yaşanmış siber saldırı örneklerinin iyi anlaşılması gerekmektedir. Yaşanmış siber saldırı örnekleri ile oluşturulacak yüksek farkındalık ve bilinç seviyesi ile Türkiye için gelecekte karşılaşılabilecek siber olaylar öncesinde gerekli tedbirlerin en azından kullanıcı seviyesinde alınması amaçlanmıştır. Türkiye adına örnek teşkil edeceğini düşündüğümüz bazı ülke ve uluslararası örgütlerin siber güvenlik ile ilgili yapmış oldukları çalışmalar ile almış oldukları tedbirlerin bilincinde olmak, Türkiye'nin durumunu görmek bağlamında önemlidir. Ayrıca çalışmamızda oluşturulacak Dünya Siber Güvenlik Güç ve Kapasiteleri ile Türkiye'den daha iyi durumda bulunan ülkelerin siber güvenlik ile ilgili çalışmalarının ileride yapılacak akademik çalışmalar veya araştırmalarda ayrıntılı olarak incelenerek, Türkiye açısından çok olumlu katkılar sağlaması amaçlanmıştır.

BİRİNCİ BÖLÜM

1. SİBER GÜVENLİK KAVRAMININ TEMEL BİLEŞENLERİ

Türk Dil Kurumu sözlüğünde "toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet" olarak tanımlanan güvenlik, insan ile birlikte var olmuş, var oldukça da önemini korumuş ve çağlar boyunca yaşanılan tüm gelişim süreçlerinde etkisini sürekli artırarak karşımıza çıkmış ve çıkacak olan bir kavramdır (güvenlik (t.y.), http://www.tdk.gov.tr/index. php?option=com_bts &arama=kelime&guid=TDK.GTS.56a24cd989cae5.35079550).

Şekil 1: Maslow'un İhtiyaçlar Hiyerarşisi

Kaynak: Jerome, 2013: 39-45.

Güvenlik kavramının insan için önemi, ABD'li psikolog Abraham Maslow'un ihtiyaçlar hiyerarşisi teorisi ile açıklanabilir. Maslow'un ihtiyaçlar hiyerarşisinin temelini yemek yeme, su içme ve uyuma gibi fizyolojik ihtiyaçlar oluşturmaktadır (Jerome, 2013: 39-45). Bu temel ihtiyaçlarını karşılayan insan, müteakiben kendini korumak, kendisine yönelik oluşabilecek tehlikelere karşı tedbirler almak, varlığını sürdürebilmek, kısacası 0güvenliğini sağlamak istemektedir. Başka bir deyişle insanın sevgi, aidiyet, saygınlık ve

kendini gerçekleştirme gibi ihtiyaçlarını gidermeden önce güvenliğini sağlama isteği ve zorunluluğu güvenlik kavramının vazgeçilmez olduğunun ispatıdır. Bu itibarla, güvende olma ihtiyacı uğruna insan, tarih boyunca pek çok defa temel hak ve hürriyetlerinden feragat etmiş olup, hiçbir surette vazgeçemeyeceği bir ihtiyaç hâline gelmiştir (Ünver ve Canbay, 2010: 94). Tüm bunlar gerçekleşirken insan, kendi güvenliğini sağlamak için geleneksel güvenlik anlayışı çerçevesinde ordu, polis teşkilatı gibi silahlı unsurlar kurmuştur. Ancak içinde bulunduğumuz bilişim çağında, politik, ekonomik, sosyal, kültürel ve teknolojik alanlardaki çok hızlı değişimler geleneksel güvenlik anlayışını yetersiz kılmıştır.

1990'ların ortasında bilgi ve iletişim teknolojilerinin gelişmeye başlaması ve 2000'li yıllarda ise tüm dünyada çok hızlı bir şekilde yayılması sonucu kritik altyapı sektörlerinin uygulamaları sayısal ortam dediğimiz siber uzaya aktarılmış, bu da hayatımızı bilgi ve iletişim teknolojilerine daha çok bâğımlı hale getirmiştir. Başlangıçta çok büyük yararlar sağlayacağı düşünülse de zaman içerisinde bu bağımlılığın kötü niyetli kişi, grup veya örgütlerce menfaatleri uğruna kullanılması sonucunda, masum kişi, kurum veya devletler çok büyük zararlara uğramıştır. Siber uzay, bu gelişimler ile birlikte siber saldırı ve tehditlere açık bir hale gelmiş ve bu da insanın geleneksel güvenlik anlayışında değişimi zorunlu hale getirmiştir (Ünver ve Canbay, 2010: 94). Bu değişimin tam ortasında da siber güvenlik anlayışı ve kavramındaki değişim yer almaktadır. Sonuç olarak, siber güvenlik kavramı, bilgi ve iletişim teknolojilerinin çok hızlı bir şekilde geliştiği günümüzde, kişi, kurum, uluslararası örgüt ve devletlerin en önemli gündem maddelerinden biri haline gelmiştir.

Çalışmamızın bu bölümünde siber güvenlik kavramının temel bileşenlerini oluşturan siber uzay, siber saldırı, siber tehdit, siber suç, siber terör, siber caydırıcılık, siber istihbarat, siber casusluk, siber savaş tanımları ile siber güvenlik kavramının ortaya çıkışı ve uluslararası ilişkilerdeki yeri ve öneminden bahsedilecektir.

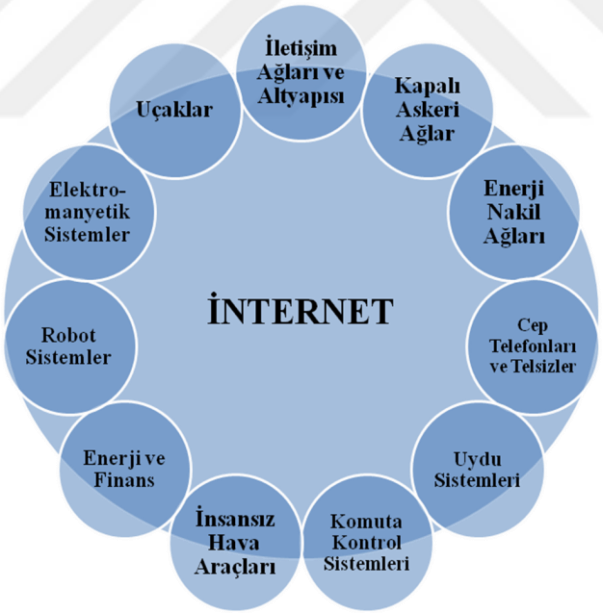
1.1. Siber Uzay (Siber Ortam, Siber Alan)

İngilizcede "cyberspace" olarak anılan bu kavram dilimizde siber uzay, siber alan, siber ortam olarak kullanılmaktadır (cyberspace (t.y.), http://tureng.com/tr/turkce-

ingilizce/cyberspace). Siber uzay, iletişim ağları, bilgisayar sistemleri ve kontrol birimlerini içeren bilgi ve iletişim teknolojileri altyapılarından meydana gelen ve birbirine bağımlı ağların oluşturduğu, herhangi bir coğrafi sınırlamaya bağlı olmayan küresel bir bilgi ortamıdır. 2016-2019 Ulusal Siber Güvenlik Stratejisi (2016: 7)'ye göre siber uzay, tüm dünyaya ve uzaya yayılmış durumda bulunan bilgi ve iletişim teknolojilerini ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal bir ortamdır.

En temel elemanı olan internetin yanı sıra birbirlerine elektronik olarak bağlı bilgisayarlar, enerji nakil ağları, cep telefonları, telsizler, uydu sistemleri, robot sistemler, insansız hava araçları, ağ sistemi bileşenleri, elektromanyetik sistemler ve bütün bunların birbirlerine bağlandığı iletişim altyapısı ve yazılımları dâhil tüm bilgi sistemleri, siber uzayı oluşturan elemanlardır (Akyazı, 2012: 56; Çifçi, 2013: 5).

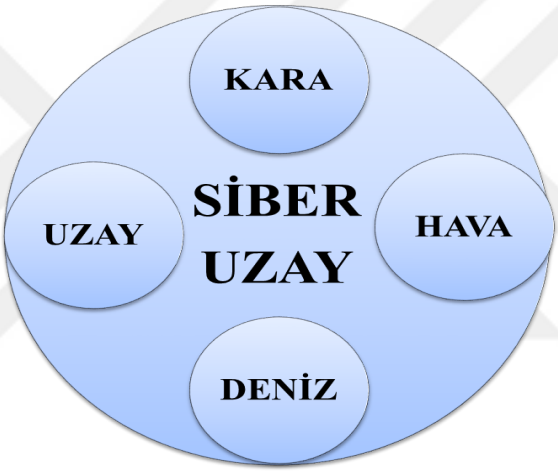
Şekil 2: Siber Uzay Elemanları



Siber uzayın başlıca aktörleri, bireysel veya grup halindeki suçlular, kötü niyetli kişiler, teröristler, kurumlar, kuruluşlar, uluslararası örgütler, sanayi casusluğu yapmak veya rakiplerini bertaraf etmek isteyen ticari kuruluşlar, siber uzayı casusluk, ekonomik avantaj veya savaş aracı olarak kullanmak isteyen ülkeler, ülkelerin silahlı kuvvetleri ve istihbarat örgütleridir (Hundley ve Anderson, 1995: 232; Çifçi, 2013: 5).

Teknolojinin çok yüksek devinim ile ilerlediği, coğrafi sınırların büyük ölçüde anlamının kalmadığı günümüzde, savunma ve güvenlik sektöründen finans ve bankacılık sektörüne, enerji sektöründen bilişim sektörüne kadar tüm sektörlerdeki sistemlerin fiziksel ve sanal varlıklarının birbirleri ile bütünleştiği görülmektedir. Böyle bir ortamda da ülkenin bekasında hayati önemi haiz bir kritik altyapı sektörlerine çok uzak mesafeden yeterli bilgiye sahip kötü niyetli herhangi bir kişi tarafından saldırı gerçekleştirilebilir. Başlangıçta tek bir sisteme yapılan kötü niyetli bir saldırı sistemlerin bütünleşik yapısından dolayı diğer sektörlerdeki sistemleri de aşırı seviyede etkilemektedir (Gürkaynak ve İren, 2011: 264-266).

Şekil 3: Harekât Alanları



Sonuç olarak, günümüzde bilgi iletişim sistemleri ve teknolojilerinin hızla gelişmesi kara, deniz, hava ve uzay harekât alanına siber uzay harekât alanını eklemiş, diğer tüm harekât alanları siber uzayda hareket eder hale gelmiştir. Dünyanın güçlü, etkin ülkeleri ve orduları tarafından siber uzay, harekât ortamının beşinci boyutu olarak kabul edilmeye başlanmıştır. Böylece siber uzay, 21'inci yüzyılda devletlerin iç veya dış politikalarını belirleyen temel araçlardan biri haline gelmesinin yanı sıra muharebe sahasına da önemli bir kuvvet çarpanı olarak iştirak edecek askerî bir dinamik haline gelmiştir.

1.2. Siber Saldırı

Kritik altyapı sektörlerine saldırma, hizmet dışı bırakma, yemleme, kötücül yazılımlarla zarar verme, sosyal mühendislik, iletişim ağını dinleme, veri çalma ve değiştirme gibi yöntemler ile devlet veya ticari kuruluşların internet sayfalarını bozma, sistemdeki gizli bilgileri çalma, silme, ifşa etme veya değiştirme amacıyla hedef kişi, şirket veya kurumun iletişim altyapılarına veya bilgi sistemlerine siber uzayda yapılan genellikle planlı ve koordineli saldırılara siber saldırı denir (Çakmak ve Demir, 2009: 29-30).

2016-2019 Ulusal Siber Güvenlik Stratejisi (2016: 7)'ye göre siber saldırı, ulusal siber uzayda bulunan bilgi ve iletişim teknolojilerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kişi veya sistemler tarafından kasıtlı olarak yapılan işlemlerdir.

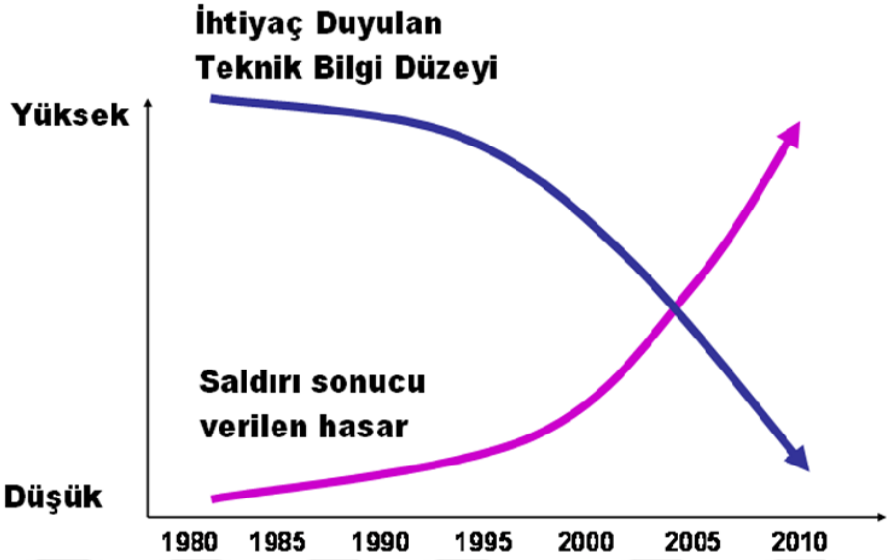
Siber saldırılar, bireysel bilgisayar korsanları, organize suç örgütleri, casusluk faaliyeti yapan kişiler, teröristler, dış istihbarat örgütleri veya hasım ülke tarafından planlı ve koordineli olarak yapılabildiği gibi sistem içerisindeki bilinçsiz kullanıcılar tarafından farkında olmadan da yapılabilmektedir.

Şekil 4: Siber Saldırı Kaynakları

Günümüzde bilgi, hızlı bir şekilde yayılmakta, siber uzayı oluşturan elemanların kullanımı hızla yaygınlaşmakta, bunların sonucu olarak da bilgiye, bilgi ve iletişim

teknolojilerine, kritik altyapı sektörlerine yapılan saldırılar da artmaktadır. Ayrıca son zamanlarda, saldırganların ihtiyaç duyduğu teknik bilgi her geçen gün azalırken siber saldırı tekniklerinin karmaşıklığı ve zararları da artmaktadır. Grafik 1'de bu ilişki ortaya konmuştur.

Grafik 1: Siber Saldırıların Gelişim Süreci



Kaynak: Sağıroğlu, 2013.

1.3. Siber Tehdit

Siber uzaya yönelik her türlü yıkıcı, bozucu, engelleyici ve ele geçirici özelliklere sahip girişimler ile siber saldırıların çeşitli araçlar ve yöntemler ile siber uzayda kullanılmasına siber tehdit denir. Siber tehditler ayrıca hem klasik suçların siber uzaya uyarlanmış hallerini hem de bilgi ve iletişim teknolojilerinden faydalanılarak türetilmiş, tamamen yeni suç tanımlarını da kapsamaktadır (Bilgi Teknolojileri ve İletişim Kurumu [BTK], 2009: 8).

Siber tehditler kaynağı ve geliş yönüne göre ikiye ayrılmaktadır (Şekil 5). Kurum içinden küskün ve art niyetli insanlardan kaynaklanan tehditlerin kurum dışı hasım kuvvetlerden kaynaklanan tehditlere göre çok daha başarılı ve tehlikeli olduğu da bilinmektedir. Siber tehditler, siber saldırılarda olduğu gibi bireysel bilgisayar korsanları, casusluk faaliyeti yapanlar, organize suç örgütleri, terörist organizasyonlar, dış istihbarat örgütleri, hasım ülke tarafından planlı ve koordineli olarak yapılabildiği gibi bilinçsiz

kullanıcılar tarafından farkında olmadan da yapılmaktadır. Siber tehditlerde kullanılan yöntemler ile hedefler, siber saldırıların yöntemleri ve hedefleri ile benzerlik göstermektedir.

Şekil 5: Siber Tehdit Kaynakları

Kaynak: Mehmet Bertan Kılıç, 2012.

Siber tehditlerin genel amaçlarını, sisteme yetkisiz erişim, bilgilerin değiştirilmesi, yok edilmesi, bilgilerin çalınması, ifşa edilmesi, sistemin bozulması ve hizmetlerin sekteye uğratılması olarak sıralayabiliriz (Atalay, 2012: 42).

Siber tehditleri, siber suç, siber terör, siber caydırıcılık, siber istihbarat ve siber casusluk ile siber savaş olarak beş ana başlık altında toplamak mümkündür.

1.3.1. Siber Suç

İçinde bulunduğumuz bilişim çağında teknolojinin çok hızlı şekilde ilerlemesinden dolayı sınırlarını net olarak çizemediğimiz siber suçu diğer suçlardan ayıran en temel fark, bilgisayar, bilgisayar sistemleri ve bilgisayar ağlarının suçların işlenmesinde kullanılmasıdır. Ortak bir görüş olarak bilgisayarların suçlarda araç olarak kullanılması ve bilgisayarsız da bu suçların işlenebilmesi gerçeği siber suçlar ile geleneksel suçların farklılığının temelini oluşturmaktadır (Çakmak ve Demir, 2009: 34).

Sistemin sahibinin rızası olmadan bilişim sistemine girilmesi, bu sistemin verilerine yetkisiz erişimde bulunulması, verilerin değiştirilmesi, silinmesi, sistemin kullanılmasının engellenmesi, iletişimin izinsiz izlenmesi, kayıt edilmesi gibi hukuka aykırı eylemler siber suçlara örnektir. Sonuç olarak siber suç, sayısal verinin veya bilgi akışının kasıtlı olarak yanlış amaçlar doğrultusunda kullanılmasıdır ve ağ sistemleri içerisinde veya ağ sistemlerine karşı işlenebilir (Corell, 2000: 8).

1.3.2. Siber Terörizm

Genel olarak kabul edilen net bir tanımının olmamasına rağmen terörizmi; sınırlı insan kaynağı ile en ucuz şekilde yapılan, pek çok hedefi aynı anda etkileyebilmekle birlikte; iletişim olanaklarının gelişmişliğine paralel olarak, büyük organizasyonlar gerektirmeyen, yüksek mobilite ve hızlı reaksiyon yeteneğine sahip, asimetrik olması sebebiyle kaynağında yok edilmesi son derece zor; bağlantılarının kanıtlanmaması ve gizliliği açısından bir devlet ile ilişkilendirilmesi neredeyse imkânsız, ulusal ve uluslararası hukuktaki boşluklardan faydalanan modern savaş tekniği olarak tanımlayabiliriz (Çitlioğlu, 2008: 14-15). Ayrıca terörizm, zaman ve mekân kısıtlaması olmayan, hedefinin genelde politik ve ilk amacının psikolojik ağırlıklı olarak korku yaratmak olduğu, içinde genellikle şiddet barındıran, insanlığın ayrılmaz bir parçası ve hayatımızın bir gerçeği haline gelmiş şiddet ve tedhiş hareketleridir.

Siber terörizmi ise terörizmin tanımından da yola çıkarak, organize suç örgütleri, gizli ajanlar, terörist gruplar veya bireylerin kasten ve siyasi bir amaç doğrultusunda, belirli bir toplum içerisinde belirsizlik ve karışıklık yaratarak günlük yaşamın gidişatını bozmak amacıyla, hükümet ve toplumları belirli bir politika veya ideolojiye uymaya zorlayarak, milyonların davranışını etkileyerek, sivil, kamu veya askeri hedeflere karşı şiddete, yıkıma ve/veya hizmetlerin sekteye uğramasına yol açan bilgisayar, bilgisayar ağları ve/veya iletişim altyapısını da kullanarak işledikleri suçlar olarak tanımlayabiliriz (Colarik, 2006: 45-47).

Teröristler için internet; merkezi kontrolden uzak olması, ulaşımının kolay ve ucuz olması, herhangi bir sınırlamasının olmaması, anonim olması ve medyanın yoğun ilgisi sebepleriyle iki temel amaç için kullanılmaktadır. Teröristler için birinci amaç, etkin bir

eğitim ve iletişim ortamı sağlamasıdır. İkinci amaç ise internetin, bilgisayar ve ağ yapılarının gerçekleştirecekleri siber terör faaliyetleri için siber uzayı oluşturmasıdır (Çakmak ve Demir, 2009: 38). Weimann (2004: 4)'e göre siber uzay ve terörizmin kesiştiği noktada siber terörizm doğmuştur.

Siber terörizm eylemleri, bilgisayarları, sanal ağları, bilgi, iletişim ve depolama sistemlerini hedef alan yasa dışı eylemler olup, bu eylemleri gerçekleştirenlerin temel amacı politik, sosyal, dini ve ideolojik amaçlarını kabule zorlamak ve bu amaçla birlikte korku ve panik havası oluşturmaktır (Güneştaş ve diğerleri, 2015: 88,89). Dolayısıyla, siber terörizm, sadece insanların can ve mal güvenliğini tehdit etmekle kalmayıp, hedef kitle üstünde sosyal, siyasi, dini, ideolojik ve özellikle psikolojik etki yaratmak amacıyla bilgisayar, bilgisayar ağları ve iletişim altyapısına yapılan terör eylemleridir (Çifçi, 2013: 6).

Bu konuda unutulmaması gereken nokta, siber saldırı ile siber terörizm arasında çok ince bir çizgi olduğudur. Çünkü klasik terörizmin yarattığı korku ve endişe bilgisayar ve internet aracılığıyla yaratılıyorsa ve hedef kişi, grup veya devlet ekonomik veya maddi olarak zarara uğratılıyorsa siber saldırı, siber terörizm olarak tanımlanabilmektedir (Altunok ve Kaya, 2009: 153,154).

1.3.3. Siber Caydırıcılık

Caydırıcılığı bir devlet veya topluluğun başka bir devlet veya topluluk tarafından kendi aleyhine yapılabilecek askeri kuvvet kullanımına değin uzanan hareketlerden sakınması için gerekli tedbirleri alması olarak tanımlayabiliriz (İduğ ve diğerleri, 2013: 287).

Caydırıcılık stratejisini uygulamada olmazsa olmaz iki temel unsur bulunmaktadır. Bunlardan ilki, olası saldırı ve tehditlere karşı güçlü bir savunmaya sahip olmak, ikincisi ise herhangi bir durumda herhangi bir kaynaktan gelen herhangi bir saldırıya karşı misilleme yapma kapasitesi ve yeteneğine sahip olmaktır (Haley, 2013).

Devlet ve toplumların şiddet oranlarına göre başvurdukları caydırıcılık yöntemleri Şekil 6'da görülmektedir. Prof. Dr. Martin C. Libicki'ye (2009: 29-30) göre tek başına

kullanıldığında siber gücün şiddeti diplomatik ve ekonomik yaptırımlardan daha yüksek iken, geleneksel (konvansiyonel) ve nükleer gücün şiddetinden daha düşüktür. Sonuç olarak, siber caydırıcılık tek başına etkili olmasının yanı sıra, diplomatik ve ekonomik yaptırımlar, konvansiyonel ve nükleer kabiliyetler ile birlikte müştereken kullanıldığında daha etkili hale gelmektedir.

Şekil 6: Şiddet Oranlarına Göre Caydırıcılık Yöntemleri

Kaynak: Libicki, 2009: 29.

Soğuk Savaş döneminde konvansiyonel silahların caydırıcılığı yerini nükleer caydırıcılığa bırakmıştır. Soğuk Savaş döneminin uzun soluklu olması ve caydırıcılık politikalarının fazlalığı sebebiyle caydırıcılık ile nükleer caydırıcılık kavramları birbirinin yerine kullanılmaya başlanmıştır. Bunun yanı sıra olası bir nükleer saldırı sonucu dünyadaki yaşamın yok olacağı düşüncesi, nükleer caydırıcılığın çok etkili olmasına sebep olmuştur. Ancak siber silahların, nükleer silahların kitlesel imha gibi geniş coğrafyaya yayılan etkisi olmadığından, siber caydırıcılığın önemi hususunda halen fikir birliğine varılamamıştır.

Nükleer silaha sahip olmak başka devlet veya topluluk üzerinde caydırıcılık etkisi yaratmaktadır. Siber silahlara sahip olmak ise düşman devlet veya toplulukların bu teknolojiyi elde etmelerine ve/veya bu silahlara karşı savunma kabiliyetlerini geliştirerek siber saldırılarını boşa çıkartmalarını sağlamaktadır. Ayrıca nükleer caydırıcılık daha çok misilleme odaklı iken, siber caydırıcılık siber saldırıların nereden geldiği tam olarak tespit edilemediği için ise savunma odaklıdır. Bu sebeple siber caydırıcılıkta, güçlü savunmadan

dolayı potansiyel saldırganların hedeflerine ulaşmadan, başarısız olacakları konusunda ikna edilerek harekete geçmelerinin engellenmesi amaçlanır (Lupovici, 2011: 51). Siber savunma kabiliyetleri yüksek olduğu müddetçe, siber saldırı kaynakları yapacakları siber saldırılarının boşa çıkacağını düşünerek bu yola başvurmayacak ve siber savunma yalnız başına caydırıcılık sağlamış olacaktır (İduğ ve diğerleri, 2013: 288). Ancak şunu da unutmamak gerekir ki, siber saldırı maliyeti siber savunma ve siber güvenlik maliyetinden çok daha düşük olduğundan bazı devletler, kritik altyapı sektörlerinin savunmalarını daha güvenli hale getirmek yerine, siber saldırganları misilleme veya cezalandırma ile bertaraf etmeye çalışmaktadır.

1.3.4. Siber İstihbarat ve Siber Casusluk

İstihbarat ve casusluk, insanın tarih boyunca hasım ülke, devlet veya topluluklar üzerinde avantaj ve üstünlük sağlamak amacıyla yürütmüş oldukları faaliyetlerdendir. Bu iki kavramın önemi hiç değişmese de, uygulanma yöntemi teknolojik gelişmeler ile doğru orantılı bir şekilde farklılaşmıştır (Çifçi, 2013: 289).

Siber saldırı ve siber tehdit tanımları ile yakın ilişkili olan siber istihbarat, dijital olarak sistemin siber saldırı ve tehdit analizlerini yapmak ve karşı siber saldırılar yaparak sistem hakkında istihbarat elde etmektir (Keleştemur, 2015*:* 90). Siber saldırılar düzenleyerek devletin bekası adına ehemmiyet teşkil eden bilgilerin elde edilmesi hususu siber istihbaratın en temel özelliğidir.

Önceleri casusluk ve istihbarat yolu ile düşmana karşı avantaj ve üstünlük sağlayacak bilgiyi elde etmek daha zor, daha maliyetli ve daha çok tehlikeli iken elde edilebilecek bilgi de fiziksel olarak yer işgal etmekteydi. Teknolojinin gelişmesi ile birlikte içinde bulunduğumuz bilişim çağında ise siber casusluk ve siber istihbarat faaliyetleri, daha kolay, daha ucuz, daha az tehlikelidir ve bu yolla elde edilen bilgi de hayal edilemeyecek kadar büyüktür (Clarke ve Knake, 2010: 120-127).

Çeşitli bilgisayar korsanlığı yöntemleri kullanılarak hedef kişi, şirket, kurum veya devletten bilgi sızdırmak amacıyla özellikle istihbarat teşkilatlarının çok sık başvurdukları yöntemlerden biri de siber casusluktur.

Siber casusluk, düşman üzerinde ekonomik, politik veya askeri üstünlük sağlamak amacıyla, iletişim ağları veya bilişim sistemlerine yasa dışı yollar ile sızarak, rızaları olmadan kişi, grup ya da devletin bekası için çok kritik bilgilerin elde edilmesi faaliyetidir (Çifçi, 2013: 291). Siber istihbarat ve siber casusluk sonucu elde edilen kritik bilgiler gelecekte karşılaşılabilecek konvansiyonel veya siber savaş öncesi düşmana karşı bilgi üstünlüğü ve avantaj sağlayacaktır (Singer ve Friedman, 2015: 130,131). Dolayısıyla, siber istihbarat ve siber casusluk, devletlerin bekaları adına konvansiyonel veya siber savaş öncesi ve esnasında kullanılması şart olan oldukça önemli kavramlardır (Keleştemur, 2015: 162).

1.3.5. Siber Savaş ve Bilgi Savaşı

Uluslararası alanda siber savaşın kabul görmüş bir tanımı olmamakla birlikte en çok rağbet gören yaklaşım Richard A. Clarke ve Robert K. Knake'e aittir. Onlara göre siber savaş, bir devletin, başka bir devletin bilgisayar veya iletişim ağlarına hasar vermek ya da kesinti yaratmak üzere gerçekleştirdiği sızma faaliyetleridir (Clarke ve Knake, 2010: 8). Carr, (2011: 2)'e göre ise siber savaş, kavga etmeden savaşma ve hasmın kanını dökmeden onu mağlup etme sanat ve bilimi olarak tanımlanmıştır.

Siber savaş, ülkedeki sivil, askeri ve hükümete ait bilgi ve iletişim teknolojilerinin hasmın siber saldırılarına karşı savunulması ile ekonomik, politik veya askeri nedenlerle hedef seçilen ülkeye, bilgi ve iletişim teknolojileri üzerinden organize saldırı faaliyetleri gerçekleştirilmesi olarak da tanımlanmıştır (Yazıcı, 2011).

Bilgi savaşı ise bilgisayarlar, bilgisayar ağları veya bilgisayar sistemlerini de içine alan siber savaştan daha kapsamlı bir tanıma sahiptir (Denning, 1999: 9-12). Bilgi savaşları her türlü bilgi ile ilgilenirken, siber savaşın ilgi alanı ise siber uzaydır (Çakmak ve Demir, 2009: 45). Libicki (1995: 18) bilgi savaşını; komuta kontrol savaşı, istihbarat merkezli savaş, elektronik savaş, psikolojik savaş, hacker savaşı, ekonomik bilgi savaşı ve siber savaş olarak yedi bölüme ayırmıştır. Bu sebeplerle, bilgi savaşı ile siber savaş kavramlarını birbiri ile karıştırmamak gerekmektedir.

1. Komuta Kontrol Savaşı: Bilgi savaşını muharebe sahasında uygulayan ve fiziksel yıkıma sebep olan askeri bir stratejidir. Amacı, hasmın komuta kontrol merkezi ile muharebe sahası unsurları arasındaki irtibatı koparmak veya kesmektir (Libicki, 1995: 9).

2. İstihbarat Merkezli Savaş: Operasyonların icrasında istihbaratın özellikle hasar tespiti ve hedefin durumu gibi hususlarda kullanılmasıdır (Libicki, 1995: 19).

3. Elektronik Savaş: Elektromanyetik yayınların izlenmesi ve teşhis edilmesiyle düşman tarafından kullanılmasının engellenmesi veya etkisinin azaltılması, dost kuvvetlerin etkin olarak yararlanmasının sağlanması için elektromanyetik sistemler ve yönlendirilmiş enerjinin askeri amaçlar için kullanılmasıdır (Ünal, 2015b: 119).

4. Psikolojik Savaş: Siber uzay bileşenleri yardımıyla, özellikle bireysel bilgilerin değerlendirilmesiyle kişiler, kurumlar hatta toplumlar üzerinde gerçekleştirilen algı operasyonlarıdır (Ünal, 2015b: 119).

5. Hacker Savaşı: Siber uzayda, virüsler, mantık bombaları, truva atları, köle bilgisayar gibi siber silahlar kullanılarak şantaj yapma, hırsızlık, verilerin silinmesi veya başka bir amaca ulaşmak için sivil veya askeri hedeflere yapılan siber güvenlik ihlalleridir (Libicki, 1995: 19).

6. Ekonomik Bilgi Savaşı: Siber uzayı etkinlikle kullanan finans, bankacılık, e-ticaret gibi sektörlerin verilerine yönelik gerçekleştirilen manipülasyon faaliyetleridir (Ünal, 2015b: 119).

7. Siber Savaş: Bilgi savaşı kavramı bölümlerinden en kapsamlı olanıdır. Sayısal ortam/siber uzay içerisinde, savunma ya da taarruz amaçlı, bilgi ve iletişim teknolojilerinin yok edilmesi, zarara uğratılması ya da manipüle edilmesi eylemlerini kapsar (Çakmak ve Demir, 2009: 48; Libicki, 1995: 19).

Ayrıca Libicki siber savaşı, stratejik ve operasyonel olarak iki gruba ayırmıştır. Stratejik siber savaş, bir devlete ve onu oluşturan topluma karşı özellikle de devletin tutumunu değiştirmek amacıyla gerçekleştirilen siber saldırı harekâtı, operasyonel siber savaş ise konvansiyonel bir savaş esnasında düşmanın askeri hedeflerine ve silahlı kuvvetleri ile bağlantılı sivil hedeflerine karşı gerçekleştirilen siber saldırı harekâtı olarak tanımlanmıştır (Libicki, 2009: 117,139).

Tablo 1: Konvansiyonel Savaş ile Siber Savaş Arasındaki Farklar

DEĞİŞKENLER	KONVANSİYONEL SAVAŞ	SİBER SAVAŞ
SALDIRININ KAYNAĞININ TESPİTİ	Kolaydır.	Zordur. Bazen de imkânsızdır.
SALDIRININ HIZI	En hızlı muharebe silahı hızındadır.	İnternet hızındadır.
SALDIRININ ETKİSİ	Coğrafi sınırlar içerisindedir.	Siber uzay içerisindedir.
SAVAŞÇILARI	İki veya daha fazla ülke orduları savaşmaktadır.	Tek bir kişi, bir grup, bir örgüt veya devletler savaşmaktadır.
MALİYETİ	Genellikle oldukça pahalıdır.	Ucuzdur.
KULLANILAN SİLAHLAR	Tank, top, tüfek, füze, bomba vb. kullanılır.	Bilgisayarlar, bilgi sistemleri vb. kullanılır.
İLERİ TEKNOLOJİ İHTİYACI	Vardır.	Yoktur. Mevcut teknoloji genellikle yeterlidir.
SALDIRININ BELİRTİLERİ	Tespit edilebilir.	Tespit edilemeyebilir.
HASAR TESPİTİ	Kolaydır.	Zordur.

Kaynak: Keleştemur, 2015: 164-165; Çifçi, 2013: 20.

Tablo 1'de konvansiyonel savaş ile siber savaş arasında bulunan temel farklar listelenmiştir. Siber savaşı konvansiyonel savaştan ayıran en belirgin farklar arasında saldırıların kaynağını belirlemenin neredeyse imkânsız olduğu, saldırıların asimetrik olduğu ve sınırlardan bağımsızlığı yer almaktadır. Bunlara ilaveten, siber savaşın caydırıcılık gücü nispeten daha az olduğundan tek başına kullanıldığında düşmanı silahsızlandırmak ve zararsız hale getirmek mümkün değildir. Ayrıca tek başına kullanıldığında düşman topraklarını işgal etmek için yeterli olmadığı için konvansiyonel savaş ile birlikte, müşterek ve doğru yer ve zamanda operasyonel savaş şeklinde uygulanması çok daha etkili olacaktır (Keleştemur, 2015: 163-164; Çifçi, 2013: 15).

Şu ana kadar tanımlarını yapmaya çalıştığımız siber saldırı, siber suç ve siber savaş kavramları sıklıkla birbirleri yerine kullanılmakta ve karıştırılmaktadır. Tablo 2, bu kavramlar arasındaki farklılık ve benzerlikleri göstermesi adına önem ihtiva etmektedir.

Tablo 2: Siber Saldırı, Siber Suç ve Siber Savaş Kavramları Arası İlişki

Siber Eylemin Niteliği	Siber Eylemin Türü		
	Siber Saldırı	Siber Suç	Siber Savaş
Sadece devlet dışı aktörlerin iştiraki		+	
Bilişim sistemleri aracılığıyla işlenen, ceza hukuku normlarının ihlalinin varlığı		+	
Bilişim sistemlerinin işlevini engelleme amacı	+		+
Politik ve ulusal güvenliğin sağlanması amacı	+		+
Etkilerin silahlı saldırıya eşdeğerliği veya eylemin silahlı çatışma bağlamında icra edilmesi			+

Kaynak: Hathaway ve Crootof, 2012: 833.

Dolayısıyla siber suç, sadece devlet dışı aktörler tarafından yapılan siber eylemlerinin yanı sıra ceza hukuku ihlallerini kapsamaktadır. Siber saldırılar, hem devlet dışı aktörler hem de devlet eli ile yapılabildiği gibi, bilişim sistemlerine yönelik olacak şekilde, ulusal ve politik güvenliğin sağlanmasını amaçlamaktadır. Siber savaş ise siber saldırıların nitelikleri haricinde eylemin etkilerinin silahlı saldırıya eşdeğer olması veya herhangi bir silahlı çatışma bağlamında icra edilmesi niteliğine sahip olması gerekmektedir.

1.4. Siber Güvenlik ve Siber Savunma

Siber güvenlik kavramının birçok tanımı bulunmaktadır. Birleşmiş Milletlerin (BM) haberleşme, bilgi ve iletişim teknolojileri alanındaki yetkili organı olan Dünya Telekomünikasyon Birliği (ITU) tarafından siber güvenlik, "siber uzayda organizasyon ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavram ve önlemleri, kurallar, risk yönetimi yaklaşımları, eylemler, eğitimler, uygulamalar

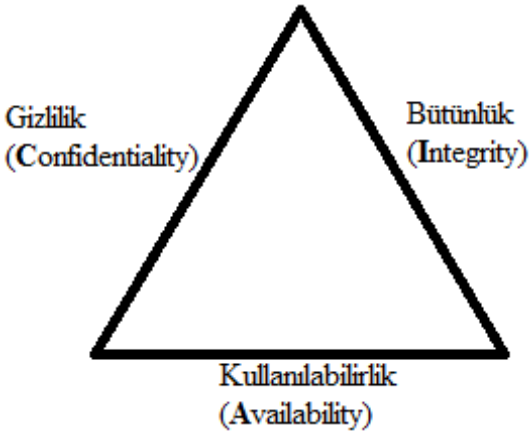
ve teknolojilerin bütünü" olarak tanımlanmıştır. Siber uzayda organizasyon ve kullanıcıların varlıklarını, bireyler, bilgi işlem donanımları, altyapılar, uygulamalar, hizmetler, haberleşme sistemleri ve siber uzayda iletilen ve/veya saklanan bilgiler oluşturmaktadır (ITU, 2008: 2).

Bilgi sistemlerini ve ağlarını işlemez kılan veya işlevine yönelik çalışmasını engelleyen her türlü tehdit, saldırı ve tehlikelere karşı ilgili sanal sistemleri korumaya da siber güvenlik denilmektedir (Akleylek ve Tok, 2011).

Siber güvenlik ayrıca siber uzaydaki güvenlik riskleri ve zafiyetlerinin belirlenerek, kurum, kuruluş ve kullanıcıların varlıklarının istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılarak önlemlerinin alınmasıdır. 2016-2019 Ulusal Siber Güvenlik Stratejisi (2016: 7)'ne göre siber güvenlik, siber uzayı oluşturan bilgi ve iletişim teknolojilerinin siber saldırılardan korunması, bu sayısal ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin sağlanması, saldırıların ve siber güvenlik olaylarının tespit edilmesi, bu tespitlere karşı tepki mekanizmalarının çalıştırılması ve sonrasında ise sistemlerin önceki durumlarına geri döndürülmesi süreçlerini kapsamaktadır.

Bilgi sistemleri içerisinde işlenen, depolanan ve transfer edilen bilginin gizliliği ve mahremiyetinin korunması, veri bütünlüğünün ve bilgiye erişimin, erişim hız ve kalitesinin muhafazası ve korunması ile sistemin sürekliliği ve devamlılığının sağlanması bilgi güvenliğinin temel amaçlarıdır ve siber güvenliğin de temel prensipleri olarak kabul görmüşlerdir (Sağıroğlu, 2011; Atalay, 2012: 43). Gizlilik, erişilebilirlik ve bütünlük kavramları "CIA üçlüsü" olarak da anılmaktadır (**C**onfidentially, **I**ntegrity, **A**vailability) (Singer ve Friedman, 2015: 57).

Şekil 7: CIA Üçlüsü



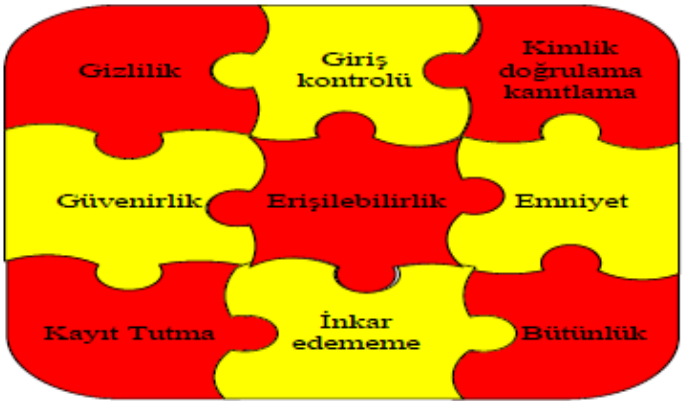
Kaynak: Tony ve Justin, 2011: 35.

1. Gizlilik: Bilgiye **i**zinsiz veya yetkisiz erişimin engellenmesi, bilginin mahremiyet ve gizliliğinin korunmasıdır. Verinin özel olarak muhafazasını ifade eder (Singer ve Friedman, 2015: 57). Başka bir ifade ile mesajın sadece gönderici ve alıcı kişiler tarafından görülebilmesidir (Yılmaz ve Salcan, 2008: 85).

2. Erişilebilirlik: Bilgiye erişim hız ve kalitesinin korunması, veri ya da kaynaklara kesintisiz bir şekilde erişilebilmesi veya erişim kayıplarının önlenmesidir.

3. Bütünlük: Sistem içerisindeki veri ya da kaynakların izinsiz bir şekilde değiştirilmesinin önlenmesi ve bütünlüğünün sağlanmasıdır. Verinin kaynaktan hedefe doğru giderken doğruluğunun, tutarlılığının, içeriğinin, sırasının vb. etkenlerin sadece yetkili kişiler tarafından yapılabilmesidir (Newman, t.y., 4).

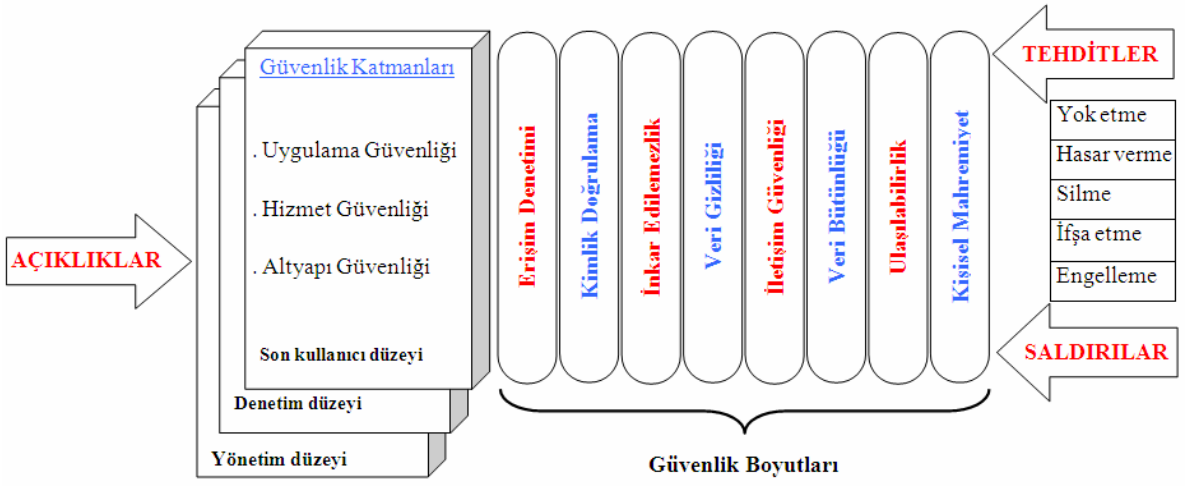
Şekil 8: Siber Güvenlik Prensipleri



Kaynak: Sağıroğlu, 2011.

Siber güvenliğin üç temel prensibinin yanında bilgi güvenliği için de önem arz eden, hesap verilebilirlik, inkâr edilemezlik, kimlik doğrulama, güvenirlik, kayıt tutma, giriş kontrolü, emniyet ve esneklik gibi ilave güvenlik prensipleri de bulunmaktadır. Hesap verilebilirlik, tüm eylemlerin kullanıcıya yani eylemi yapan kişiye kadar takip edilebilirliğidir (Yeşilyurt, 2015: 170-172). İnkâr edilemezlik, herhangi bir iş ve işlemin gerçekleştirilmiş olduğunun ispatlanması ve reddedilememesidir. Başka bir ifade ile mesajı gönderen kişinin mesajı gönderdiğini inkâr edememesidir (Yılmaz ve Salcan, 2008: 86). Kimlik doğrulama ise bilgi sistemlerini kullanan gerçek veya tüzel kişiler tarafından beyan edilen mesajın gönderen veya alıcı tarafından kimlik bilgilerinin teyit edilmesidir (Kurose ve Ross, 2013: 699; A.N. Ünal, 2015b: 111,112).

Şekil 9: Siber Güvenlik



Kaynak: BTK, 2009: 3 ve ITU, 2008: 11.

Siber güvenlik, kurum içi veya kurum dışından gelebilecek her türlü siber tehditler veya siber saldırılar ile mücadelenin yanı sıra, bilgi ve iletişim teknolojilerinde yer alan, sistem yöneticileri, kullanıcı veya üretici hatalarından kaynaklanan açıklıkları ve zafiyetleri yani güvenlik risklerini en aza indirmeyi amaçlamaktadır (BTK, 2009: 3 ve ITU, 2008: 11).

Siber savunma ise, hasmın herhangi bir taarruzu esnasında muhabere, elektronik ve bilgi sistemlerine siber uzayda yapılacak saldırılar ve tehditlerin olumsuz etkilerinin önlenmesi ve sistemlerin bekasının sağlanması için alınması gereken tedbirlerin bütünü olarak tanımlanmaktadır (Keleştemur, 2015: 315,316).

Siber savunmada, sistemleri oluşturan yazılım ve donanımların devamlı olarak güncellemelerinin ve bakımlarının aksatılmadan yapılması, sistemdeki güvenlik açıklarının tespiti, bu açıkların kapatılması için çok hızlı reaksiyon gösterilmesi, sistemin savunulmasını sağlayacak kişi veya kişilerin bilgi seviyelerinin yeterli, güvenlik ve arşiv araştırmalarının müspet, ketum ve sır saklama yetenekleri yüksek kişilerden seçilmeleri hayati önemi haiz hususlar arasındadır.

Tanımlardan da anlaşılacağı üzere siber güvenlik ile siber savunma arasındaki en temel fark, siber güvenliğin hasmın herhangi bir taarruzu vuku bulmadan, barış şartlarında alınan tedbirler bütünü, siber savunmanın ise hasmın taarruzu esnasında yani savaş durumunda alınan tedbirler bütünü olduğudur.

1.4.1. Siber Güvenlik Kavramının Ortaya Çıkışı

Bilginin hayatımızdaki yerinin vazgeçilmez ve aynı zamanda da hayati olduğu konusu tartışılmazdır. İçinde bulunduğumuz bilişim çağında teknolojinin çok hızlı bir ivme ile gelişmesi, hayatımıza sağladığı kolaylık ve yeniliklerinin etkilerini bir o kadar da zor gözlemleyebilmemize sebep olmuştur. Teknolojiye bağımlılığımız arttıkça da teknolojinin ortaya çıkaracağı zafiyetleri, açıklıkları ve dezavantajları da bir o kadar da artacaktır (Cavelty, 2008: 12,13). Bilgi ve iletişim teknolojilerinde yaşanan hızlı gelişim ile bu sistemler ve teknolojiler tarafından sunulan hizmetlerin her alanda yaygınlaşması sonucunda bilgi ve iletişim teknolojilerinin siyasi, sosyal, ekonomik ve askerî alandaki rolü artmıştır. Bütün bu gelişmeler ışığında birçok kişi, kurum ve kuruluş, bilgi ve iletişim teknolojilerini en üst seviyede kullanmaya başlamış, tüm faaliyetlerinin ayrılmaz bir parçası haline getirmiştir. Bunun sonucunda da bilgi ve iletişim teknolojileri ülkelerin kritik altyapı sektörleri için yaşamsal hale gelmiştir.

Son zamanlarda, organize suç ve terör örgütleri eylemlerini planlama, eğitim, bilgi paylaşma ve propaganda faaliyetlerini siber uzaya kaydırmakta, bilgi ve iletişim teknolojilerini hedeflerine ulaşmak için kullanmaktadırlar. Oluşan saldırı ve tehditler nedeniyle de siber güvenlik ve savunma faaliyetleri, kişi, kurum, kuruluş ve devletler nezdinde önemini artırmıştır.

Siber saldırı ve tehditlerin hedefinde, zarar görmesi ve/veya yok olması halinde, vatandaşların mal ve can güvenliğine, sağlığına ve ekonomik refahına veya kamu hizmetlerinin sağlanmasında olumsuz etki doğuracak, hayati önemi haiz tesisler, şebekeler, hizmetler ve varlıklar bulunmaktadır. Bunlar ülkeden ülkeye değişmekle birlikte, çoğunlukla savunma, finans, enerji, ulaşım, elektronik haberleşme, sağlık, eğitim, nükleer tesisler ve temel kamu hizmetlerine yönelik altyapılardır ve tüm bu unsurlar kritik altyapı olarak tanımlanmaktadır (Cavelty, 2008: 91-121).

Tablo 3: Türkiye'de Kritik Altyapı Sektörleri

1. Ulaştırma	**5.** Su Yönetimi	**9.** Tarım ve Gıda
2. Elektronik Haberleşme	**6.** Kritik Kamu Hizmetleri	**10.** Kültür ve Turizm
3. Bankacılık ve Finans	**7.** Kritik Üretim Ticari Servisleri	
4. Enerji	**8.** Sağlık	

Kaynak: Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2013: 4890; 2016-2019 Ulusal Siber Güvenlik Stratejisi, 2016: 8; T.C. Başbakanlık AFAD, 2014: 34.

Türkiye'nin 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ile 2016-2019 Ulusal Siber Güvenlik Stratejisi kritik altyapıları, "işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda; can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar" olarak tanımlamıştır. 20 Haziran 2013 tarihli Siber Güvenlik Kurulu Kararı uyarınca kritik altyapı sektörleri, Ulaştırma, Enerji, Bankacılık ve Finans, Elektronik Haberleşme, Kritik Kamu Hizmetleri ve Su Yönetimi olarak belirlenmiş, kritik altyapı sektörlerinin tespiti ve koordinesi için görevlendirilmiş T.C. Başbakanlık Afet ve Acil Durum Yönetim Başkanlığı (AFAD) tarafından da kapsamı daha sonra genişletilmiştir (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2013: 4890; 2016-2019 Ulusal Siber Güvenlik Stratejisi, 2016: s.8; T.C. Başbakanlık AFAD, 2014: s.34).

AB ve ABD'nin belirlemiş olduğu kritik altyapı sektörleri Tablo 4 ve Tablo 5'te gösterilmiştir.

Tablo 4: AB'ye Göre Kritik Altyapı Sektörleri

1. Enerji	**5.** Sağlık	**9.** Ulaşım
2. Bilgi ve İletişim Teknolojileri	**6.** Finans	**10**. Kimyasal ve Nükleer Endüstri
3. Su	**7.** Nakliye	**11.** Uzay ve Araştırmalar
4. Gıda ve Tarım	**8.** Kamu-Hukuk Düzeni ve Emniyeti	

Kaynak: Alcaraz ve Sherali, 2015: 53.

Tablo 5: ABD İç Güvenlik Bakanlığına (DHS) Göre Kritik Altyapı Sektörleri

1. Enerji	**7.** Nakliye	**13.** Ticari Tesisler
2. Bilgi ve İletişim Teknolojileri	**8.** Kamu-Hukuk Düzeni ve Emniyeti	**14.** Kritik Üretim
3. Su	**9.** Ulaşım	**15.** Savunma Sanayi
4. Gıda ve Tarım	**10.** Kimyasal ve Nükleer Endüstri	**16.** Barajlar
5. Sağlık	**11.** Uzay ve Araştırmalar	**17.** Acil Servisler
6. Bankacılık ve Finans	**12.** Milli Heykel ve Semboller	**18.** Sivil Yönetim

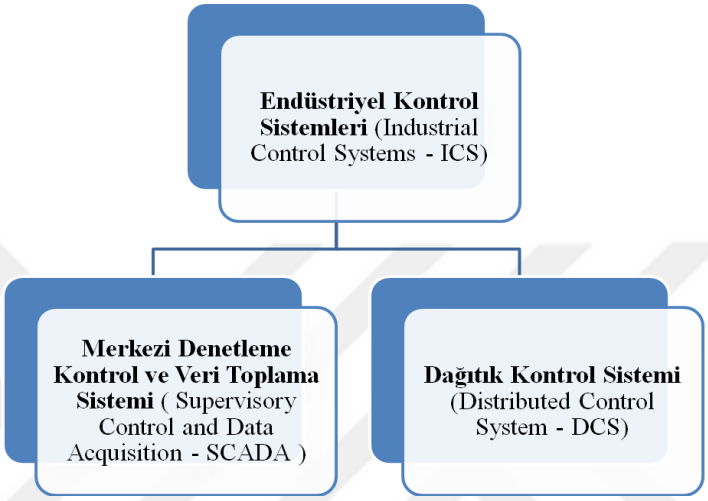
Kaynak: Alcaraz ve Sherali, 2015: 54.

Görüldüğü üzere, kritik altyapı sektörlerinin seçiminde devletler veya uluslararası örgütler nezdinde küçük farklılıklar olmasına karşın, değişmeyen tek özellikleri neredeyse hepsinin siber uzayla irtibatının olması ve bilişim sistemleri tarafından kontrol edilmeleridir.

Kritik altyapı sektörlerinin karmaşık ve dağıtıklığının çözülebilmesi için, bu sektörlerin operatörler tarafından uzaktan gözlenmeleri, kontrol ve kumanda edilmeleri gerekmektedir. Günümüz ağ sistemleri, operatörlere veya yetkililere kritik altyapı sektörlerini uzaktan denetleme, izleme ve yönetme olanağı sağlamaktadır. Günümüz teknolojisinde bu sistemler "Merkezi Denetleme Kontrol ve Veri Toplama Sistemi" (SCADA - Supervisory Control and Data Acquisition) ve "Dağıtık Kontrol Sistemi" (Distributed Control System - DCS) olarak ikiye ayrılmaktadır. Bu sistemler ile genel olarak, elektrik üretim ve dağıtım sistemleri, barajlar, sulama sistemleri, fabrikalar, doğal gaz sistemleri, petrol rafinerileri gibi endüstriyel, altyapı veya tesis tabanlı süreçleri izleyen

ve kontrol eden Endüstriyel Kontrol Sistemleri (Industrial Control Systems - ICS) ifade edilmektedir (Karabacak, 2011). SCADA sistemleri ile DCS arasındaki temel fark, SCADA sistemlerinin DCS'ye göre daha geniş coğrafi alana yayılmış olmalarıdır (Peterson, 2013: 120).

Şekil 10: Endüstriyel Kontrol Sistemleri



ICS'ler, tek bir merkezden bilgisayar, cep telefonu veya tablet gibi cihazlarla kritik altyapı sektörlerinin izlenmesini sağlamaktadır. Tek bir cihazdan kullanılabileceği gibi ağ bağlantıları marifetiyle birden fazla bilgisayar ve taşınabilir cihazla kontrol ve izleme yapılabilmektedir. Bu bağlanma özelliği, sitemlerin kontrolünü, denetlenmesini ve yönetimini kolaylaştırmış olsa da ciddi boyutta güvenlik problemlerini de beraberinde getirmiştir (Karakuş, 2013: 6). Çünkü bağlı olduğu ağdaki ICS'lere yapılabilecek saldırılar, yazılım, donanım veya insan kaynaklı hatalar tüm ağdaki sistemleri de etkileyecektir. Kritik altyapı sektörleri ile ICS'lerin karşı karşıya kaldığı bu tehditlerle ancak dikkatli tasarlanmış ve iyi uygulanan korunma ve savunma stratejileri ile baş edilebilir (Alcaraz ve Sherali, 2015: 54, 55).

Son dönemlerde dünyada kurum, kuruluş, uluslararası örgüt ve devletler kendi kritik altyapı sektörleri ve ICS'leri bu tehditlere karşı koruyabilmek için siber güvenlik ve savunma konusundaki faaliyetlerini hızlandırmışlardır. Siber güvenlik ve savunmanın sağlanması maksadıyla milli ölçekte idari, teknik ve hukuki kapasitenin geliştirilmesi, milli yazılım ve donanımların üretimi, kritik altyapı sektörlerinde mümkün olduğunca milli kaynaklı güvenlik ürünlerinin kullanılması önem kazanmıştır. Siber uzaya yönelik

saldırıların etkilerini en aza indirebilmek maksadıyla, kritik altyapı sektörlerinin tespit edilmesi, güvenliklerinin sağlanması, alınan teknolojik ve hukuki tedbirlerin geliştirilmesi hususları gerekli olmuştur.

Günümüzde önemi aşikâr olan siber güvenlik kavramı, gelecekte de en revaçta olacak konulardan biridir. Bilgi ve iletişim teknolojilerine olan bağımlılığımız sürdükçe ve artarak devam ettikçe siber güvenlik, kişi, kurum, uluslararası örgüt ve devletlerin öncelikli güvenlik alanlarından biri halinde kalmaya da devam edecektir.

1.4.2. Uluslararası İlişkilerde Siber Güvenliğin Yeri ve Önemi

Uluslararası ilişkiler başlangıçta, egemen ve eşit statüde sayılan devletler arasında gerçekleşmekteydi ve devletlerin sadece sahip oldukları sınırlar içerisinde yaptırım gücü bulunmaktaydı. Günümüzde ise sınırlarının belli olmadığı ve herhangi bir fiziksel kısıtlamanın olmadığı siber uzay içerisinde, egemenliğin ve yaptırım gücünün kimde olacağı konusu tartışma konusu haline gelmiştir. Artık devletler, fiziksel sınırları içerisindeki emniyetini sağlamak dışında, sınırları belli olmayan siber uzayda da yapılan siber saldırılara karşı savunma mekanizmalarını kurmaları gerekmektedir.

İçinde bulunduğumuz bilişim çağındaki teknolojinin çok hızlı bir şekilde gelişmesi, ülkelerin fiziksel olarak sınırlarının muğlaklaşması, siber saldırı ve tehditler ile bunların doğurduğu sorunlar, devletlerin güvenlik kaygılarına bir yenisini daha eklemiş ve klasik güvenlik anlayışlarını değiştirmelerine sebep olmuştur (Güntay, 2015: 477). Ayrıca siber saldırı ve tehditlerin, bunlara maruz kalan coğrafya dışında başka bir coğrafyada bulunan ülkeleri de etkileyebilmesi hususu, siber uzay sınırlarının belirlenmesini daha da zorlaştırmaktadır (Gürkaynak ve İren, 2011: 275-276).

Ülkelerin siber saldırı ve tehditlerine karşı bakış açıları çok farklılık göstermektedir. Bazı ülkeler siber uzayı az sıklıkla veya hiç kullanmazken, bazıları ise kendi menfaat ve çıkarları uğruna çok sıklıkla kullanmaktadır. Siber faaliyetleri çok sık kullanan ülkeler, teknolojik olarak daha gelişmiş olup, bu faaliyetlerden menfaat sağladıkları için küresel boyutta bir siber güvenlik oluşumuna genellikle sıcak bakmamaktadır. Ancak siber saldırıların az bir bilgiye sahip kötü niyetli kişi ve örgütlerce

kullanılabiliyor olması ve bundan büyük devletlerin daha çok zarara uğraması, siber uzayda yaşanan gelişmelerin klasik uluslararası ilişkiler çalışmaları içerisine alınmasını gerekli kılmıştır. Çünkü siber uzayda yaşanan gelişmeler, uluslararası ilişkilerde yeni aktörlerin doğmasını sağlamış ve yeni güvenlik risklerini ortaya çıkarmıştır (Gürkaynak ve İren, 2011: 265). Özellikle ülkeler için hayati önemi haiz, siber saldırı ve tehditlerin hedefi olan kritik altyapı sektörleri, izlenecek diplomasi ve politikada önemli bir yer işgal etmektedir. Siber uzayın aktörleri, artık uluslararası gündemi meşgul edip, direkt olarak etkileyebilecek siber saldırı, siber tehdit, siber terörizm, siber caydırıcılık ve siber savaş gibi mekanizmaları ellerinde tutmaktadırlar.

Küreselleşmenin son yıllarda insanlık tarihinde eşi benzeri olmayan bir şekilde hız kazanması ile birlikte uydu, cep telefonları, bilgisayarlar, internet ağı, bilgi ve iletişim teknolojileri de hayal bile edilemeyecek ölçüde gelişmiş, dünya ülkelerini birbirine yaklaştırmış ve adeta dünyayı elektronik otoyollarla birbirine bağlamıştır (Henderson, 2010: 20,21). Bu sebeple uluslararası alanda gerçekleştirilen ticareti, ekonomik, siyasi, kültürel ilişkiler, uluslararası suçlar, doğa olayları, sağlık sorunları, siber saldırılar, siber suçlar dâhil daha birçok olaylarda küresel işbirliği kaçınılmaz kılınmış ve uluslararası toplumun birlikte hareket etmekten başka da çaresi kalmamıştır (Aksar, 2013: 34,35).

Bu sebeplerle de devletler, artık dünya sahnesindeki tek önemli aktör olmaktan çıkmış, ulus ötesi şirketler, hükümet dışı örgütler, uluslararası örgütler ve birçok devlet dışı yapılanmalar da artık dünya siyasetinde söz sahibi olmaya başlayan yeni aktörler olarak yerlerini almışlardır (Heywood, 2014: 28-31). Burada önemli olan husus, bugüne kadar siber saldırılar konusunda sınırlı sayıda anlaşma imzalamış olan tüm bu aktörlerin birlikte hareket etme isteğini artırarak devam ettirmesidir.

Uluslararası ilişkiler nezdinde, siber güvenlik kavramının yeri ve önemi her geçen gün arttığı düşünülürse, dünya barış ve güvenliğinin sağlanabilmesi için, siber suç, siber saldırı, siber tehdit, siber terörizm ve siber savaş gibi kavramların tanımlanması, üzerinde anlaşma sağlanması, uluslararası hukuk kuralları içerisindeki yerlerinin netleştirilmesi önem ihtiva etmektedir (Gürkaynak ve İren, 2011: 275,276). Hâlihazırda uluslararası toplum bu tanımlar hakkında herhangi bir uzlaşıya varamamış ve yakın gelecekte de varması zor görünmektedir.

İKİNCİ BÖLÜM

2. SİBER GÜVENLİK ALGISININ GELİŞİMİ

2.1. Siber Silahlar

Hemen hemen her ülke konvansiyonel silahların kullanılmasına, sınıflandırılmasına ve satışına yönelik yasalarında iç düzenlemeler yapmıştır ve yapmaya da devam etmektedir. Günümüz uluslararası düzenlemeler ve yasalarında, siber silahın net bir tanımına yer verilmemiş olup, sadece genel bir kavram olarak silahın tanımı yapılmıştır.

Genel olarak silah, insanlara, suni yapılara veya sistemlere zarar vermek veya hasara uğratmak kastıyla kullanılan her türlü araç olarak tanımlanır. Silahlar, öldürme, sakatlama veya hasmı mağlup etme ve hasma karşı üstünlük sağlamak maksadıyla kullanılmaktadır (Brown ve Metcalf, 2014: 131). Silah, savunma ve saldırı amacıyla, insanları öldürmek, zarar vermek veya sakatlamak ile malları yıkmak veya yok etmek amacıyla kullanılan araç olarak da tanımlanmaktadır (Intoccia ve Moore, 2006: 480).

Kara, hava, deniz ve uzay harekât alanlarını da kapsayan ve beşinci harekât alanı olarak ortaya çıkan siber uzayda, ülkelerin veya şirketlerin kritik altyapı sektörlerindeki küçük bir güvenlik açığı sonucu uğradıkları ekonomik zararları düşünürsek, siber silahın tanımında uluslararası bir uzlaşıya varmanın önemi aşikârdır. Çünkü siber saldırılarda kullanılan siber silahların uluslararası hukuk kurallarına ve insani standartlara uygunluğunun denetlenebilmesi açısından siber silah tanımının daha özele indirgenerek yapılması gerekir (Brown ve Metcalf, 2014: 137).

Bugüne kadar tanımı ile ilgili uluslararası bir anlaşmaya varılamasa da, genel olarak siber silah, konvansiyonel silahların bir parçası olmakla birlikte kritik altyapı sektörleri, bilgi ve iletişim teknolojileri veya insanları fiziksel, işlevsel veya zihinsel olarak

etkilemek, bozmak, tehdit veya tahrip etmek amacıyla kullanılan veya geliştirilen bilgisayar kodudur diye tanımlanmaktadır (Rid ve McBurney, 2012: 7).

Çifçi (2013: 150)'ye göre siber silah, hasmın bilişim sistemlerinin veya içerisindeki bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini hedef alan, bilgi ve iletişim teknolojileri ile sayısal sistemleri etkisiz hale getirmek, bozmak, sekteye uğratmak veya tahrip etmek için kullanılan yazılım veya yöntemlerdir.

Siber silahların tanımı kapsam, amaç ve yöntem bakımından aşağıda bulunan üç özelliği de taşıması gerekmektedir (Mele, 2013: 10).

1. Kapsam: Siber silahların, stratejik, operatif veya taktik avantajı sağlamak, korumak veya sürdürmek amacıyla bilişim sistemlerinin, devlet veya devlet dışı aktörler tarafından siber savaş içerisindeki bir siber saldırıda kullanılması gerekmektedir.

2. Amaç: Siber silahların, bilişim sistemlerini sabote etme, hasara uğratma ile insanlara, aygıtlara veya cihazlara fark edilebilir, somut bir fiziksel zarar verme amacıyla kullanılması ve bilişim sistemlerinin işlemez veya kullanılamaz hale getirmesi yanında bu sistemlerin içerisine nüfuz etmesi gerekmektedir.

3. Yöntem: Siber silahların, interneti de içeren bilişim sistemlerine karşı kullanılıyor olması gerekmektedir.

Siber silah, doğrudan olmasa bile bir şekilde insanlara, aygıtlara veya cihazlara fiziksel bir zarar verme veya saldırılan hassas hedefin bilişim sistemlerine doğrudan zarar verme, sabote etme amaçlarıyla devlet veya devlet dışı aktörler tarafından siber savaş içerisindeki siber saldırılarda kullanılan cihaz, aygıt veya bilgisayar yazılımıdır (Mele, 2013: 7-10).

Burada dikkat edilmesi gereken en önemli husus, kullanılan zararlı yazılımın veya hizmet dışı bırakma saldırılarının hangi şartlarda siber silah olarak tanımlandığının yasal çerçevesinin belirlenmesi gereğidir. Örnek olarak, bilgi ve iletişim teknolojilerinin geçici olarak hizmet verememesine sebep olan dağıtık hizmet dışı bırakma saldırısı (Distributed Denial of Service - DDoS) ile bir internet sitesinin kullanılamaz hale getiren saldırı amaçlı kullanılan zararlı yazılım, hedefte önemli, fark edilebilir ve somut bir fiziksel hasara sebep

olmadı ise siber silah olarak düşünülmemelidir (Mele, 2013: 13). Ayrıca sadece suç işlemek veya casusluk faaliyeti yapmak amacıyla bilgi ve iletişim teknolojilerinde zararlı yazılımların kullanılmalarını siber silah kategorisi içerisine almamak gerekmektedir.

Konvansiyonel silahlar ile kıyaslandığında siber silahlar, üretilmeleri için daha az zamana ve daha az paraya ihtiyaç duymaktadır ve hedef üzerinde uygulanması da daha kolaydır. Bu özellikleri ile siber silahlar, devlet dışı aktörler tarafından çok daha yaygın şekilde kullanılmaktadır. Ayrıca, konvansiyonel silahların aksine, siber silahlar düşük maliyetler ile yeniden üretilebilmekte, bilgi ve iletişim teknolojilerine çok kısa sürede yayılabilmekte ve fiziksel bir risk olmadan uzun süre saklanabilmektedir. Bu avantajlarının aksine siber silahların, bir kez hedef üzerinde kullanıldığında, hasmın o silaha karşı savunma mekanizmalarını geliştirdikten ve gerekli güvenlik tedbirlerini aldıktan sonra aynı hedefte tekrar başarılı olma ihtimali çok zayıftır. Bu sebeple özel bir hedef için üretilen siber silahlar, tek kullanımlıktır, sonraki siber saldırılarda yetersizdir ve sonraki hedefleri aynı şekilde ve yoğunlukla etkilemesi aşırı derecede zordur. Bu sebeple siber silahların kullanılacağı yer ve zaman seçimi saldırının başarıya ulaşmasında çok önem ihtiva etmektedir (Mele, 2013: 17).

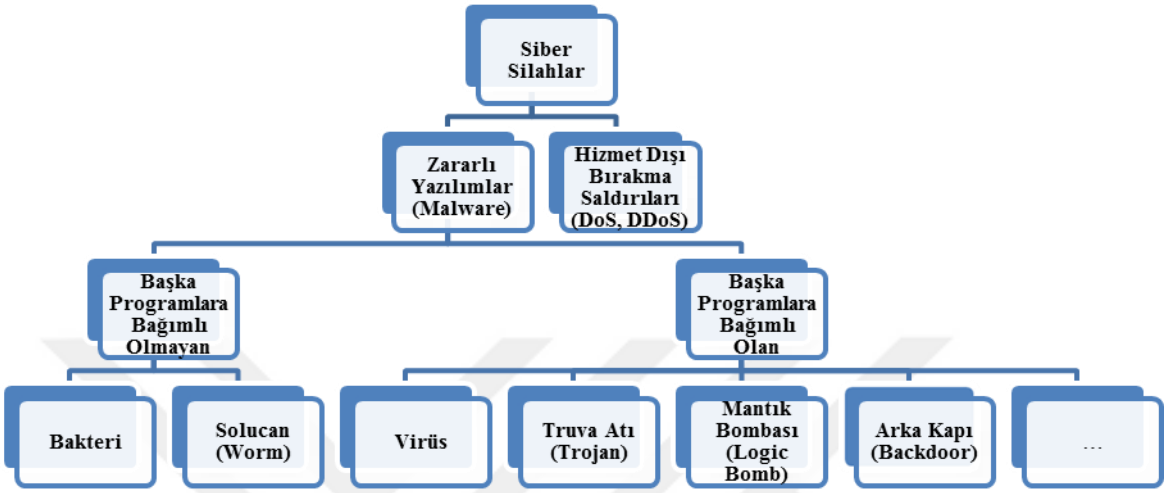
Siber silahların çok büyük bir kısmı devlet eli ile üretilmesine rağmen, devlet dışı aktörlerin de yoğun üretim faaliyetleri bulunmaktadır. Devlet eli ile ve devlet dışı aktörler tarafından üretilen ve kullanılan siber silahların hacmi göz önüne alındığında da siber silahların geliştirilmesi, yayılması ve kullanımı ile ilgili devletler veya uluslararası örgütler nezdinde bir anlaşmaya varılabilmesi de çok zordur (Arimatsu, 2012: 100).

Hedefte yüksek hasar potansiyeline sahip siber silahların devlet veya devlet dışı aktörler tarafından üretilmesi aşamasında, hedef odaklı, özel bir çalışmaya, kayda değer seviyede maddi güce, zamana ve istihbarat bilgilerine ihtiyaç duyulduğu ve siber silah geliştiricilerin son derece uzmanlaşmış, teknik bilgi kapasitelerinin çok yüksek olan kişilerden seçilmesi gerektiği çok iyi bilinmelidir.

Günümüzde konvansiyonel silahların yerine kullanılmaya başlanan siber silahlara örnek olarak, bakteri, solucan, virüs, truva atı, mantık bombası, arka kapı, kök kullanıcı

takımı, casus yazılımlar gibi zararlı yazılımlar ile hizmet dışı bırakma saldırıları (Denial of Service – DoS) verilebilir.

Şekil 11: Siber Silah Türleri



Kaynak: Çifçi, 2013: 150.

2.1.1. Zararlı Yazılım (Malware - Malicious Software)

Bilişim sistemlerine zarar verme, işleyişini bozma, çalışmasını sekteye uğratma ve bilgi çalma amaçları için özel olarak üretilmiş olan virüs, solucan, truva atı, arka kapı, casus yazılım gibi siber silahlara genel olarak zararlı yazılım denilmektedir (Malware Definition (t.y.), http://techterms. com/ definition/malware).

2.1.2. Bakteri

Bakteriler, başka programlara bağımlı olmadan, bağımsız olarak, kendi kendine çoğalabilen ve sonucunda işlemci gücü, hafıza ve disk alanı gibi sistem kaynaklarını meşgul ederek, kullanıcının bilgisayarında performans düşüklüğüne yol açan yazılımlardır. Bu tarz bir sınıflandırma genellikle tercih edilmemekle birlikte, yapı itibarı ile solucana, çalışma mantığı bakımından virüse benzemektedir (Çifçi, 2013: 150).

2.1.3. Solucan (Worm)

Kullanıcının müdahalesi olmadan, bağımsız olarak, kendi kendine çoğalabilen, ağ içerisindeki diğer bilgisayarlara çok kısa sürede yayılabilen, en çok bilinen ve kullanılan zararlı yazılımlardan biridir. Kendisini yayabilmek için ise ya hedef sistem içerisindeki güvenlik açıklarından faydalanmakta ya da sosyal mühendislik yöntemlerini kullanmaktadırlar (What is the Difference… (t.y.), http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html). Çok hızlı ve büyük sayılarda çoğalabilen solucanlar, e-postalar veya dosyalar ile diğer bilgisayarlara bulaşmakta ve hedef bilgisayarların kilitlenmesine ve internet sayfaları açılırken de uzun süre beklemesine neden olmaktadır (Ulaşanoğlu, 2010: 24).

2.1.4. Virüs

Virüsler, bir programın içerisinde gömülü olarak bulunan, mevcut sistem içerisinde çoğalabilen, bir dosyadan veya programdan diğerine yayılabilen, dosyalar kopyalandığı ve paylaşıldığı zaman diğer bir bilgisayara da bulaşabilen, yazılım veya dosyalara zarar veren bilgisayar programıdır (Çifçi, 2013: 152; Keleştemur, 2015: 222).

Virüsler genellikle içine gizlendiği programın insan eli ile çalıştırılması sonucu yayılmaya başlamakta ve bilgisayardaki program veya dosyalara zarar verebilmektedir. Elektronik posta, virüslerin yayılması için kullanılan temel yöntem iken, CD, USB bellek, hard disk gibi harici depolama araçları ile internetten dosya indirme, dosya transferi veya uzak kullanıcı bağlantıları da kullanılan diğer yöntemler arasındadır.

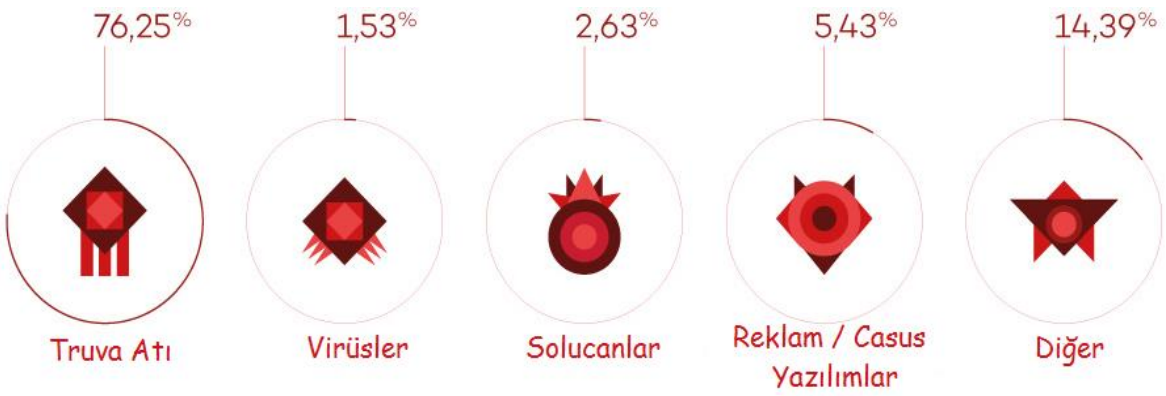
Zararlı yazılımların en yaygın kullanılan türleri olan solucanlar ve virüsler genellikle birbirleri ile karıştırılmaktadır. Solucanlar diğer dosya veya programlardan bağımsız olarak çalışırken, virüsler ise kendisini yayabilmek için bir programa veya insan müdahalesine ihtiyaç duymaktadır (What is the Difference… (t.y.), http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html).

2.1.5. Truva Atı (Trojan)

Truva atı, başlangıçta kullanıcıya iyi niyetli ve zararsızmış gibi gözüken ancak gizli bir şekilde yerleştiği bilgisayarın arka planında zarar vermeye yönelik faaliyetler icra eden programlardır (Altunok ve Katman, 2009: 73). Virüsün aksine, bir başka bilgisayara kendi kendini kopyalamazlar. Truva atı, kullanıcı tarafından çalıştırılmayı bekleyen, kullanıcıların dosyalarının, verilerinin kaybolması, değiştirilmesi hatta çalınması gibi ani istenmeyen sonuçlar doğurabilen, zararlı ve kötü amaçlı çalıştırılabilir bir kod içeren program veya program parçasıdır (Çifçi, 2013: 153; Keleştemur, 2015: 223).

Dolayısıyla virüsler çalışmaları için başka bir dosya, program veya insan müdahalesine (dosya kopyalama vb.) ihtiyaç duyarken, solucanlar bir ağa bağlı bilgisayarlara kendi kendini kopyalarken böyle bir şeye ihtiyaç duymamaktadır. Truva atları ise virüsler gibi kendilerini kopyalayamamalarının yanı sıra yararlı bir program gibi gözükür ve kullanıcı için faydalı işler yaparken, arka planda da zararlı işleri yapan casus yazılımlardır (Çifçi, 2013: 154).

Şekil 12: 2015 Yılı İkinci Yarısında Zararlı Yazılımların Kullanım Sıklıkları



Kaynak: Panda Security, 2015.

2.1.6. Mantık Bombası (Logic Bomb)

Belirli bir zamanda, belirli şartların ve durumların oluşmasıyla çalışan yazılımın içerisine kasıtlı olarak monte edilmiş olan kod parçası veya programdır. Dolayısıyla mantık bombası, sistem içerisinde gizli bir şekilde çalışacağı zaman gelene kadar kuluçka

döneminde beklemekte ve bu dönem sonunda ise harekete geçerek sisteme zarar verebilmektedirler (Çifçi, 2013: 154; Keleştemur, 2015: 229).

2.1.7. Arka Kapı (Back Door – Trap Door)

Sadece saldırgan tarafından bilinen ve normal kimlik doğrulama yöntemlerini kullanmaksızın genellikle gizli yollarla bilgisayar veya şifreli sistemlere girebilmek için oluşturulan yöntem veya giriş noktalarıdır (Çifçi, 2013: 154; Keleştemur, 2015: 225).

2.1.8. Kök kullanıcı takımı (Rootkit)

Bilişim sistemlerinde bulunan zararlı yazılım, program veya kod parçasının kullanıcıdan gizlenerek, tespit edilmelerinin engellenmesi için işletim sisteminde değişiklikler yapan yazılım paketlerine denilmektedir. Kök kullanıcı takımı bilgisayara sızmış olan zararlı yazılımların rahat bir şekilde tespit edilmeden çalışabilmelerini sağlamaktadır (Çifçi, 2013: 155; Keleştemur, 2015: 225,226).

2.1.9. Casus Yazılım (Spyware - Adware)

Kullanıcının bilgisi ve rızası olmadan bilgisayar üzerinde kontrol sağlayarak, kişi, kurum veya kuruluş hakkında bilgi toplamak amacı taşıyan yazılımların genel adıdır. Casus yazılımlar genellikle kullanıcıların internet üzerindeki hareketlerini izleyen, kayıt altına alan yazılımlar ile istem dışı olarak gönderilen ticari tanıtım yazılımlarını kapsamaktadır (Jonasson ve Sigholm, 2005:1).

2.1.10. Köle Bilgisayarlar (Botnet, Zombie)

Kullanıcının haberi dahi olmadan daha önce yüklenen bir program vasıtasıyla uzaktan kontrol edilebilen ve hedef bilgisayara saldırmak amaçlı kullanılan bilgisayarlara köle bilgisayar denilmektedir. Köle bilgisayarlar asıl saldırıyı yapanlar tarafından her an kullanılmaya hazır beklemekte, özel yazılımlarla uzaktan yönetilebilmekte ve büyük çaplı saldırılarında kullanılabilmektedir (Güngör, 2015: 45).

2.1.11. Gelişmiş Siber Tehditler (Advanced Persistent Threats - APT)

Belirli bir hedefe yönelik ısrarlı bir çalışma sonucunda üretilmiş ve çok etkili bir siber saldırı gerçekleştirme kapasitesine sahip siber tehditlere verilen isimdir. Hedeflere sızmak için gelişmiş tehditler ve özel geliştirilmiş saldırı teknikleri kullanmakta, bulaştıkları sistemlerde uzun süre fark edilmeden çalışabilmektedir. APT'ler genellikle bir grup veya devlet desteği ile belirli sistem veya kişileri hedef almaktadır (Bircan, 2012).

2.1.12. Saldırı Kitleri (Attack Kits)

Ücretsiz olarak internetten indirilebilen, az bir para karşılığı özel olarak yazdırılabilen, kolay kullanımı ve erişilebilmesi sebebiyle siber suçların hızlı bir şekilde artmasına yol açan, saldırıyı gerçekleştirebilmek için gerekli tüm programları içerisinde barındıran ve sıradan bir kullanıcının dahi etkili bir siber saldırgan olmasını sağlayan saldırı araçları topluluğuna denilmektedir (Symantec, 2011: 4-6).

Resim 1: Fidye Virüsü Görüntüsü

Kaynak: Öcüt, 2016.

2.1.13. Fidye Virüsü (Ransomware)

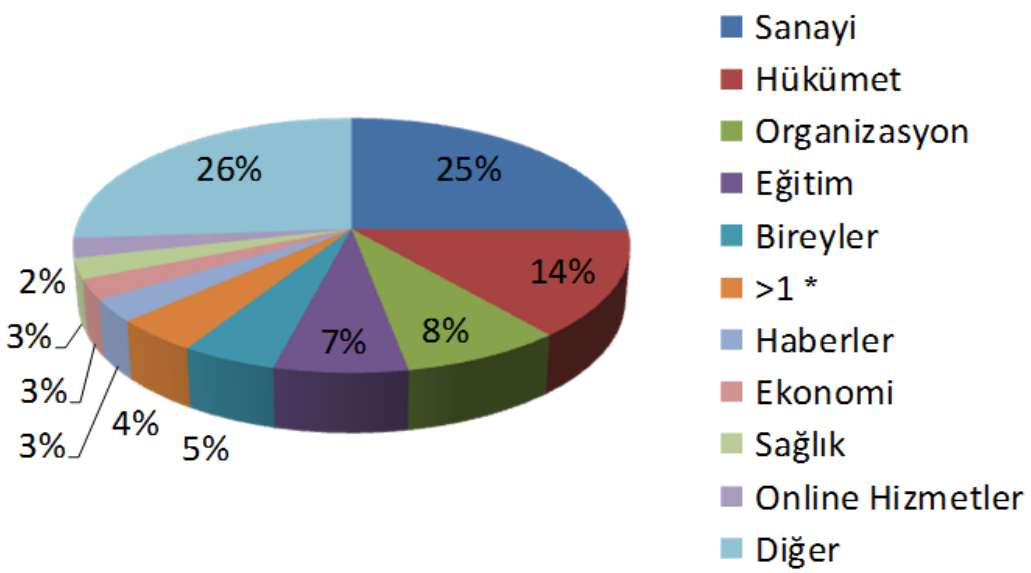
Bilişim sistemleri üzerindeki güvenlik açıklıklarından faydalanarak veya bilgisayara indirilen truva atı programı içeren bir dosyanın çalıştırılması sonucu aktif hale

gelen fidye virüslerinden bazıları işletim sistemine bulaşarak bilgisayarı açılmaz hale getirebilmekte, bazıları ise bulaşmış olduğu bilgisayar içerisindeki dosya ve verileri çözülmesi zor şifreleme algoritmalarını kullanarak şifrelemektedir. Bu zararlı yazılım daha sonra kullanılamaz hale gelen dosya ve verilerin şifrelerinin çözülmesi için kullanıcıdan belli bir süre içerisinde ödenmesi şartıyla fidye talep etmekte, belirtilen süre içerisinde ödemenin yapılmaması durumunda ise dosyaları silmektedir. 2007 yılı itibarı ile siber uzayda ortaya çıkan bu zararlı yazılım türü, 2015 yılı itibarı ile de oldukça yaygınlaşmıştır (Symantec, 2015: 3-28).

2.2. Siber Saldırı Türleri

Siber saldırganlar, kişi, şirket veya kuruma ait bilgisayar, bilişim sistemleri, kritik altyapı sektörleri, bilgisayar ağları veya kişisel bilgisayar cihazlarına zarar vermek amacıyla siber uzayda siber saldırı türlerine başvurmaktadır (Keleştemur, 2015: 288,289; Çifçi, 2013: 139). Siber saldırganların siber uzayda seçtikleri hedefler ve saldırılarının arkasında yatan sebepler Grafik 2 ve Grafik 3'te belirtilmiştir.

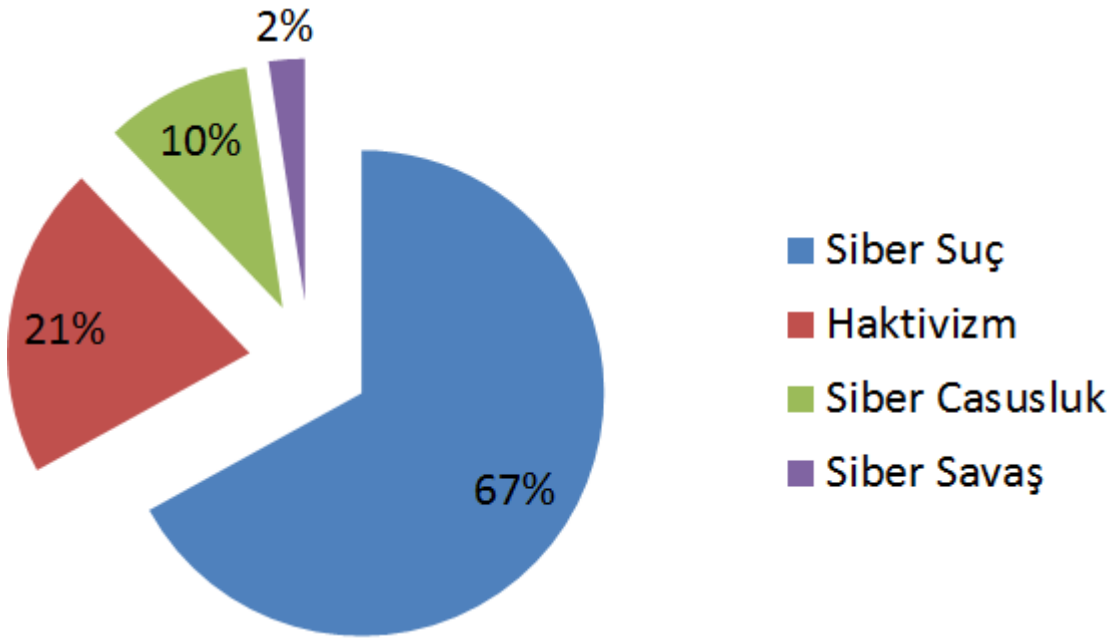
Grafik 2: 2015 Yılı Meydana Gelmiş Siber Saldırıların Hedeflerinin Dağılımı



*Siber saldırıların en az bir sektörü hedef aldığı durumları göstermektedir.

Kaynak: Passeri, 2016.

Grafik 3: Siber Saldırıların Arkasında Yatan Sebepler ve Güdüler



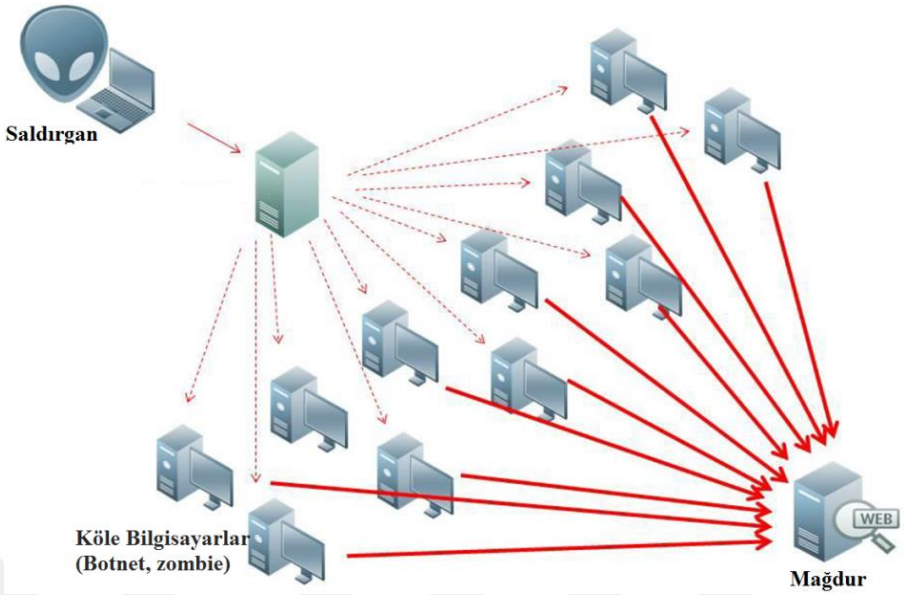
Kaynak: Passeri, 2016.

2.2.1. DoS ve DDoS Saldırıları

Bir sunucu bilgisayara eş zamanlı ve mümkün olduğunca fazla paket göndererek, bu bilgisayarın kullanıcılarının hizmet veremez ve iş göremez hale gelmesi durumuna "DoS" saldırıları denilmektedir. Bunun yanında, bu saldırılar güvenlik açıklıklarından faydalanılarak ele geçirilmiş ve kullanıcıların bilgisi dışında uzaktan yönetilen köle bilgisayarlar (zombi, bot) kullanılarak yapıldığında ise "DDos" adını almaktadır (Şekil 13) (Yazıcı, 2012: 38; Keleştemur, 2015: 307).

DDoS saldırılarının gücü, DoS saldırılarının gücünden köle bilgisayar sayısı ile çarpılması kadar büyük olacağından günümüzde çok daha sıklıkla kullanılmaktadır (Ünal, 2015a: 16). DDoS hedef bilgisayar ve bağlı olduğu sistemin saniyeler içerisinde on binlerce bilgisayarın saldırısına maruz kalarak hizmet dışı kalmasına sebep olacak kadar etkilidir.

Şekil 13: Köle Bilgisayarlar (Botnet, Zombie)



Kaynak: Ağyol, 2015.

2.2.2. Sosyal Mühendislik (Social Engineering)

Teknolojinin kullanılmasından ziyade insan tabiatındaki birtakım zafiyetlerinden (güven duyma ihtiyacı, aceleci davranma, korku, merak vb.) faydalanarak, insanları etkileme ve ikna etme yöntemlerini kullanarak veya hile ile kandırarak, kurbandan bilgi alma ya da istenen işleri yapmasını sağlamak olarak tanımlanmaktadır (Tombul, 2015: 141). En çok kullanılan sosyal mühendislik yöntemleri ise şunlardır (Tatar**,** 2011: 9-14; Çifçi, 2013: 147; Keleştemur, 2015: 307):

1. Güvenilir bilgi karşılığında para, hediye vb. önermek,

2. Güvenilir bir kaynak olduğuna karşı tarafı ikna etmek,

3. Genel olarak sahte senaryolar uydurmak,

4. Özellikle sosyal paylaşım sitelerinde, ortak tanıdıklar üzerinden yakınlık kurarak, bilgi, para vb. elde etmek,

5. Başka bir kişiyi taklit ederek, telefon veya e-posta yolu ile sanki bu kişiymiş gibi iletişim kurmak,

6. Karşı tarafın zor durumda olduğunu ve bu sebeple yardım ediyormuş izlenimi vermektir.

2.2.3. Yemleme - Oltalama (Phishing) Saldırıları

Genellikle güvenilir bir web sayfasının birebir kopyası veya sahte bir e-posta ile kurbanda sanki orijinal bir siteyi ziyaret ediyormuş hissi yaratarak, yasa dışı yollarla kurbanın kredi kartı bilgileri, kullanıcı adı ve parola gibi kişisel bilgilerini çalma eylemlerine oltalama veya yemleme saldırıları denilmektedir. Bu saldırı türünde, kötü niyetli kişiler, genelde e-posta vb. yollarla hedeflerine ulaşmakta, kurbanın kişisel bilgilerini sanki resmi bir kurum veya kuruluşmuş gibi istemekte ve buna karşılık veren kullanıcıların ise kişisel bilgileri çalınmaktadır (Ulaşanoğlu ve diğerleri, 2010: 28; Çifçi, 2013: 149). Yemleme saldırıları genellikle hedef sisteme girebilmek için insan tabiatındaki bir takım zayıflıkların kullanılması olarak tanımlanan sosyal mühendislik saldırısı içerisinde düşünülmektedir (Hekim, 2015: 58).

2.2.4. İstem Dışı Yığın İleti (E-posta) Gönderme (Spam - Bulk - Junk Mail)

İnternet üzerinde aynı tür iletinin çok sayıda kopyasının, bu tip bir iletiyi alma talebinde bulunmamış kişilere gönderilmesi şeklinde yapılan saldırı türüdür. Çoğunlukla bu iletiler, pazarlama, reklam veya sosyal içerikli olmaktadır ve daha çok bilgisayara zarar vermek veya yemleme yolu ile kullanıcıları dolandırmak için kullanılmaktadır (Ulaşanoğlu ve diğerleri, 2010: 21; Çifçi, 2013: 147).

2.2.5. Şebeke Trafiğinin Dinlenmesi (Sniffing - Monitoring)

Ağ üzerinde sunucu ve kullanıcılar arasındaki bilgi alışverişi ortamının dinlenmesine "monitoring", yapılan bu bilgi alışverişinde kullanılan bilgilerin içeriklerinin değiştirilerek başka bankacılık işlemlerinde kullanılan şifreler ve kredi kartı bilgileri gibi önemli bilgilerin elde edilmesine de "sniffing" denilmektedir (Ulaşanoğlu ve diğerleri, 2010: 21; Yazıcı, 2012: 39; Çifçi, 2013: 147).

2.2.6. Zararlı Yazılım Kullanımı (Virüs - Solucan - Truva atı vb.)

Zararlı yazılımlar, işletim sistemindeki veya üzerinde çalıştırılan çeşitli programlarda bulunan güvenlik açıklarını kullanarak, güncelleme veya program yükleme sitelerinin taklidi sonucunda bilgisayara yükletilerek veya kullanıcının e-posta, sohbet yazılımları gibi harici bir kaynaktan gelen eklentilerin kontrolsüz şekilde çalıştırılması sonucunda hedef sistemde etkili olmaktadırlar. Zararlı yazılımlar, hedef sistemde sorunlar yaratmasının yanında da yarattıkları yoğun bant genişliği ve trafiği sonucu sistem kaynaklarını boşa harcadıklarından, iletişim hattının devre dışı kalmasına dahi yol açabilmektedirler (Karaarslan ve diğerleri, 2008: 1).

2.2.7. Kriptografik Saldırılar

Şifrelenmiş bilgilerin şifresini kırmak veya çözmek için yapılan saldırılardır (Keleştemur, 2015: 304). Kripto analiz yöntemleri ile gerçekleştirilen bu saldırılar arasında, ortadaki adam saldırısı (man in the middle attack), sadece şifreli metin (chipertext only), kaba kuvvet saldırısı (brute forcing), sözlük saldırısı (dictionary attack), bilinen düz metin (known plaintext), uyarlanır seçili düz metin (adaptive chosen plaintext), seçilen düz metin veya şifreli metin (chosen plaintext, chipertext) ve ilişkili anahtar (related key attack) saldırıları bulunmaktadır (Canbek ve Sağıroğlu, 2007: 10).

2.2.8. Arka Kapı Kullanımı (Backdoor - Trapdoor)

Genellikle gizli yollarla, bilgi ve iletişim teknolojilerine uzaktan erişebilmeyi sağlayan arka kapılar, sistem içerisinde kurulu ve hazır bir program şeklinde olabileceği gibi aynı zamanda da var olan meşru bir programın içerisine kasıtlı olarak bırakılmış şekilde de olabilir (Canbek ve Sağıroğlu, 2007: 8). Kimi zaman sistemlerde "güvenlik açığı" olarak bildirilen siber olayların aslında saldırgan tarafından daha önceden sistem içerisine bir şekilde yerleştirilmiş bir arka kapı olması muhtemel bir durumdur (Çifçi, 2013: 140).

2.2.9. IP Aldatmacası - Gizlenmesi (IP Spoofing)

IP aldatmacası ile siber korsanlar güvenli bir sitenin IP adresini kullanarak gerçek kimliklerini gizlemekte, kişi ve kurumların önemli bilgilerine ulaşılabilmektedir (Gürkaynak ve İren, 2011: 272). Bir web sayfası ziyaretçisi girmek istediği adres yerine korsan tarafından oluşturulan web sayfasına yönlendirilmekte ve ziyaretçi bu sayfa ile dinamik bir etkileşime geçtiğinde ise siber korsan önemli bilgilere, bilgisayar veya ağ kaynaklarına erişebilir hale gelmektedir. (Türkay, 2013: 1189) Dolayısıyla, IP aldatmacası, siber saldırganlar tarafından hizmet veren sunucular ya da sistemlere gönderilen paketlerin başlık bilgilerindeki kaynak IP kısmında değişiklik yapılarak, saldırının kaynağının olduğundan başka gösterilerek gerçek kaynak adresinin gizlenmesi faaliyetidir (Ünal, 2011a: 27). Günümüzde özellikle değiştirilmiş IP numaraları kullanılarak yapılan DoS veya DDoS saldırılarında büyük oranda artış görülmektedir (Aydın, 2013: 39).

2.2.10. Dijital Manipülasyon (Digital Manipulation)

Özellikle istihbarat veya güvenlik birimlerinin kullandığı, kamuoyunu yanlış bilgilendirmeyi veya kandırmayı amaçlayan, herhangi bir görüntü, video veya imajı bilgisayar program araç ve yazılımları yardımıyla değiştirerek yeni anlam kazandırmayı hedefleyen siber saldırı türüdür (Gürkaynak ve İren, 2011: 274,275; Türkay, 2013: 1189).

2.2.11. Açık Mikrofon Dinleme

Casus bir yazılım kullanılarak, bilgisayar kullanıcısının haberi olmadan, bilgisayar mikrofonunun veya kamerasının açılarak ortamın dinlenmesi veya anlık görüntüsünün alınması amacıyla yapılan siber saldırı türüdür. Günümüzde yaygınlaşan akıllı telefonlar da ortam dinlemesi yapabilen birer mikrofon haline gelmişlerdir (Çifçi, 2013: 147; Keleştemur, 2015: 290,291).

2.2.12. Oturum Çalma (Session Hijacking)

Uzaktaki bilgisayarın oturum açma bilgilerini, şebeke trafiğinin dinlenmesi (sniffing), kaba kuvvet saldırısı (brute forcing), ortadaki adam (man in the middle), çapraz

site betikleme (cross-site scripting) gibi çeşitli yöntemlerle, web sayfasındaki açıklıklardan faydalanarak, bilgisayar sistemi servislerine veya bilgiye yetkisiz giriş yapma hakkının kazanılmasıdır (Kapoor, t.y.: 2).

2.2.13. Kabloya Saplama Yapma (Wire Tapping)

Emniyeti yeteri kadar alınmamış iletişim ağı kablolarına (telefon trafiği dâhil) özel teçhizatlar yardımı ile fiziksel olarak saplama yapılması sonucu, iki taraf arasındaki tüm trafiğin ele geçirilmesi faaliyetine yönelik siber saldırı türüdür (Yıldız, 2014: 31; Çifçi, 2013: 139).

2.2.14. İnternet Servis Saldırıları

Siber saldırganların bilgisayar sistemlerinin kendi aralarında haberleşmelerini sağlayan İletim Kontrol Protokolü ve İnternet Protokolü (TCP/IP), Dosya Transfer Protokolü (FTP), Hiper-Metin Transfer Protokolü (HTTP), Elektronik Posta Gönderme Protokolü (SMTP), Alan Adı Sistemi (DNS), Sınır Geçit Protokolü (BGP) gibi internet protokol ve servislerinin zayıf noktaları ve açıklıklarından faydalanarak yaptıkları saldırı türüdür (Keleştemur, 2015: 301; Çifçi, 2013: 143,144).

2.3. Siber Saldırı ve Tehditlere Karşı Savunma, Korunma Yöntem ve Sistemleri

Son zamanlarda teknolojide yaşanan gelişmeler ve internetin yaygınlaşması sonucunda kötü niyetli kişiler de bunlara paralel olarak, kullandıkları siber saldırı tekniklerini geliştirmiş, sistem ve teknolojilerin açıklıklarından daha fazla faydalanarak hedef sistemlere daha büyük zararlar vermeye başlamıştır. Hedef sistemlerin içerisinde, kurum, kuruluş veya ülkeler için hayati önemi haiz kritik altyapı sektörlerinin olduğunu düşünürsek, ortadaki zararın boyutunun ne kadar büyük olduğu anlaşılacaktır. Siber saldırı ve tehditlerin artması ve bunların sebep olduğu büyük mali kayıplarla birlikte kamu düzeni ve güvenliğini etkileyerek tehlikeye sokacak noktaya gelmeleri sebebiyle siber saldırılara karşı topyekûn olarak bireyler, sivil toplum kuruluşları, kamu kurumları ve ulusal boyutta korunma yöntemleri geliştirilmeli ve uygulanmalıdır (Ünver ve Canbay, 2010: 99).

Siber güvenliğin sağlanması konusunda ulusal boyutta yapılması gereken çalışmalar aşağıda belirtilen adımlardan oluşmaktadır:

Şekil 14:**Siber Güvenliğin Unsurları**

Kaynak: Alkan, 2012: 71.

1. Ulusal politika ve stratejinin geliştirilmesi: Siber güvenlik konusunda başarılı olunabilmesi için en başta bireyler, sivil toplum kuruluşları, kamu kurumlarına yol gösterici nitelikte bir ulusal politika ve stratejinin geliştirilmesi gerekmektedir (Ünver ve Canbay, 2010: 99).

2. Yasal çerçevenin oluşturulması: Cana veya mala etki eden siber saldırı veya tehditlerin suç olarak tanımlanması ve cezalandırılması, özellikle siber saldırganların caydırılması konusunda büyük önem teşkil etmektedir. Bu bağlamda, yasal mevzuatın gelişen teknolojilere, siber saldırı araç ve yöntemlerine göre eksikliklerinin giderilmesi ve güncellenmesi gerekmektedir (Ünver ve Canbay, 2010: 99).

3. Teknik tedbirlerin geliştirilmesi: Yasal çerçevenin oluşturulmasının yanında başta kişisel olmak üzere kamu kurum ve kuruluşların sahip oldukları bilgi ve iletişim teknolojilerinin yazılım ve donanım parçalarının da güvenliğinin sağlanması gerekmektedir. Bunun için de cihazların güvenlik standartlarının, teknik rehber ve kılavuzlarının geliştirilmesi, uygulanması ve kullanılması gerekmektedir (Ünver ve Canbay, 2010: 99).

4. Kurumsal yapılanmanın belirlenmesi: Bireyler, sivil toplum kuruluşları, özel sektör ve kamu kurum ve kuruluşlarının hepsinin görev ve sorumluğu olan siber güvenliğin başarıya ulaşabilmesi için asıl görevi ve vazifesi siber güvenlik olacak bir kamu kurumunun seçilerek, onun koordinatörlüğünde bilgisayar olaylarına müdahale ekibinin oluşturulması önem arz etmektedir. Bilgisayar olaylarına müdahale ekibi, bilgisayar güvenlik olaylarını tespit ederek, sorunları çözmek ve gelecekte olabilecek olayları önlemek için alınacak tedbirleri belirlerken internet kullanıcıları ile müşterek çalışan yapıya sahip aynı zamanda da bir koordinasyon merkezidir (Yılmaz ve Salcan, 2008: 95; Ünver ve Canbay, 2010: 99).

5. Ulusal işbirliği ve koordinasyonun sağlanması: Farklı kurum, kuruluşlarca kullanılan sistemler, şebekeler ve altyapıların neredeyse tamamı birbirine bağlı ve bağımlı olmakla birlikte sadece birindeki zafiyet veya açıklık tüm sisteme zarar vermektedir. Topyekûn bir güvenliğin sağlanabilmesi için ise tüm kurum ve kuruluşlar arası sıkı bir işbirliği ve koordinasyon sağlanmalıdır (Ünver ve Canbay, 2010: 99).

6. Kapasitenin geliştirilmesi: Teknolojide yaşanan gelişmeler, siber saldırı ve tehditlerin araç ve yöntemlerini de değiştirmiş ve geliştirmiştir. Buna karşılık, sistemlerin güvenliğini sağlama konusunda uygulanacak politikalar, yasalar, standartlar, ürünler ve çözümler de bu değişim ve gelişime uygun olarak oluşturulmalıdır. Bu sebeple politika belirleyiciler, hukukçular, yazılım, donanım ve uygulama geliştiriciler, kolluk görevlileri de teknik ve idari kapasitelerini geliştirmelidir (Ünver ve Canbay, 2010: 99).

7. Farkındalık Oluşturma: Eğitim kuruluşları ve kitle iletişim araçları kullanılarak, son kullanıcılara kadar kişiler, değişen siber saldırı araç ve yöntemleri konusunda bilgilendirilmeli, farkındalık ve bilgi düzeyleri yükseltilmelidir. Siber saldırılara karşı oluşturulmuş olan güvenlik politikalarının kullanıcılar tarafından içselleştirilerek bu anlamda bir kültürün oluşturulması çok önem arz etmektedir (Tombul, 2015: 163; Ünver ve Canbay, 2010: 99).

8. Uluslararası işbirliği ve uyumun sağlanması: Günümüzde bireysel, kurumsal ve ulusal tüm altyapı ve sistemler küresel bir ağ olan internet üzerinden birbirlerine bağlı ve bağımlıdır. Bu ağın güvenliği ise ancak uluslararası işbirliği ve koordinasyon ile sağlanabilir. Bu işbirliği çerçevesinde ortak bir mevzuatın oluşturulması, suç soruşturma ve kovuşturma usul ve yöntemlerinin uyumlu hale getirilerek, bilgi paylaşım mekanizmalarının oluşturulması gerekmektedir (Ünver ve Canbay, 2010: 99).

Bilişim sistemleri, kritik altyapı sektörleri gibi siber uzay elemanlarının güvenliğini sağlamak maksadıyla kurum ve kuruluş bazında alınması gereken genel siber savunma ve korunma yöntemleri aşağıdaki maddeleri kapsamaktadır (Çifçi, 2013: 191,192; Keleştemur, 2015: 318,319; Yılmaz ve Salcan, 2008: 71,72):

1. Güvenlik önlemlerinin artırılması, mevcut açıklık ve zafiyetlerin belirlenmesi ve çözüm getirilmesi,

2. Siber saldırı ve tehditlerin tespiti ve analizi sonucu gerekli önlemlerin alınması,

3. Siber saldırı ve tehditlerin gerçek zamanlı olarak izlenerek, haritalanması ve merkezi olay yönetimi desteğinin sağlanması,

4. Bilgi ve iletişim teknolojilerine yetkisiz veya izinsiz girişlerin tespit edilmesi ve engellenmesi,

5. Bilgi ve iletişim teknolojilerinde olabilecek zararlı yazılım veya yetkisiz işlemlerin devamlı olarak izlenmesi ve analiz edilmesi,

6. Bilgi ve iletişim teknolojileri altyapılarının, fiziksel saldırılara karşı da güvenlik sağlayacak şekilde tesis edilmesi,

7. Sadece içinde bulunduğu sistemin değil, siber uzay içerisindeki tüm açıklık ve zafiyetlerin izlenmesi ve değerlendirmelerinin yapılması,

8. Bilgi ve iletişim teknolojilerinin elektronik ve yönlendirilmiş enerji saldırılarından korunması,

9. Veri sızıntılarının izlenmesi, tespit edilmesi ve önlenmesi,

10. Zararlı yazılımların detaylı bir şekilde analiz edilmesi, bu yazılımların hareketlerinin tespit edilmesi ve muhtemel tehditlerin değerlendirilmesi,

11. Bilgisayar adli analiz işlemlerinin yapılması,

12. Bilgi ve iletişim teknolojilerinin güvenlik değerlendirmelerinin yapılması ve bu değerlendirme sonucuna göre önlemlerin alınması ve takibi,

13. Güvenlik konusunda bilinç, farkındalık ve eğitim seviyelerinin artırılması,

14. Elde edilen tüm bu değerli bilgilerin diğer kurum ve kuruluşlar ile paylaşılarak, gerekli işbirliği ve koordinasyonun sağlanmasıdır.

Ayrıca, ABD Milli Güvenlik Teşkilatı'nın (National Security Agency - NSA), kurumlarda güvenlik konusunda standartlarının olmamasının büyük bir problem teşkil ettiğini bildirmesi üzerine, ABD Savunma Bakanlığı tarafından yürütülen çalışmalar neticesinde ve Escal Institute of Advanced Technologies (SANS Institute) koordinesinde kurum, kuruluş ve firmaların kendi güvenliğini sağlayabilmeleri ve siber saldırılara karşı güçlü bir savunma mekanizmasını oluşturulabilmeleri için 20 kritik güvenlik kontrolü belirlenmiştir. Kurumlarda siber güvenliğin tesis edilmesi ve saldırılara karşı aktif bir siber savunmanın uygulanabilmesi için çok önemli olan 20 kritik güvenlik kontrolü aşağıda belirtilmiştir (The CIS Critical Security…(15.10.2015), https://www.sans.org/ critical-security-controls; Çifçi, 2013: 247-255; Keleştemur, 2015: 333,351):

1. Yetkili ve Yetkisiz Donanım Envanterinin Kontrolü,

2. Yetkili ve Yetkisiz Yazılım Envanterinin Kontrolü,

3. Mobil Cihazlar, Dizüstü Bilgisayarlar, İş İstasyonları ve Sunucu Bilgisayarların Yazılım ve Donanımlarının Güvenli Bir Şekilde Yapılandırılması,

4. Sürekli Olarak Açıklık Tespiti ve İyileştirmesi,

5. Sistem Yöneticisi Yetkilerinin Kontrolü,

6. Güvenlik Kayıtlarının Bakımı, İzlenmesi ve Analiz Edilmesi,

7. E-Posta (E-mail) ve İnternet Tarayıcısı (Web Browser) Önlemleri,

8. Zararlı Yazılımlara Karşı Savunma Mekanizması,

9. Ağ Portları, Protokoller ve Hizmetlerin Sınırlandırılması ve Kontrolü,

10. Veri Kurtarma Yeterliliği,

11. Güvenlik Duvarı (Firewall), Yönlendirici (Router) ve Anahtar (Switch) Gibi Ağ Cihazlarının Güvenli Bir Şekilde Yapılandırılması,

12. Sınır Savunması,

13. Veri Güvenliğini Sağlama,

14. Bilmesi Gereken Prensibine Göre Hareket Edilmesi,

15. Kablosuz Erişim Kontrolü,

16. Kullanıcı Hesabı Denetimi ve Kontrolü,

17. Güvenlik Beceri ve Bilgilerinin Değerlendirilmesi ve Açıklıkların Giderilmesi İçin Uygun Eğitimin Verilmesi,

18. Uygulama Yazılımları Güvenliği,

19. Bilgisayar Olaylarına Müdahale Edilmesi ve Yönetimi,

20. Güvenlik Analizi ve Sızma (Penetration) Testleri,

Siber savunma ve güvenlik önlemlerinin yanında kurumlar ayrıca mevcut veya muhtemel riskleri yorumlayan, ortaya çıkan sonuca, kurumun güvenlik ihtiyaçlarına ve maliyetlerine göre riskleri kontrol altına almayı hedefleyen ve alt süreçlerini risk analizi ve risk kontrolünün oluşturduğu risk yönetimi mekanizmalarını belirli aralıklarla işletmelidirler. Çünkü bilgi ve iletişim teknolojilerinin gelişen ve değişen doğasına paralel olarak, varlıklar, zafiyetler, açıklıklar, tehditler, karşı tedbirler ile güvenlik ihtiyaçları da değişiklik gösterecektir. Bu değişikliklerin de sistemler için teknolojik ve mali etkileri bulunmaktadır. Risk yönetimi sürecinin içerisinde yer alan risk analizi, sisteme yönelik riskleri çıkartıp, yorumlamaktadır. Risk kontrolü ise, risk analizi sonucundan çıkarılan risklere, kurumun güvenlik ihtiyaçlarına ve maliyete göre karşı tedbirleri almakta ve risk kontrollerini yapmaktadır. Sonuçta risk analizi ve risk kontrolü bir defa yapılıp bitirilen süreçler değil, aksine birbirini takip eden süreçler olup, bilgi ve iletişim teknolojilerinin güvenliğinin sağlanmasının temellerini oluşturmaktadırlar (Yılmaz ve Salcan, 2008: 78).

Siber saldırı ve tehditler ile mücadele ederken ve kullandığımız siber savunma yöntemlerini uygularken siber savunma sistemlerinin efektif ve doğru bir şekilde kullanılması gerekmektedir. Ancak o zaman sistemler içerisinde etkin bir savunma ve koruma mekanizması sağlanabilir. Etkin bir savunma ve korunma mekanizmasının oluşmasını sağlayan siber savunma ve korunma sistemleri de aşağıda açıklanmıştır (Çifçi, 2013: 196-212; Keleştemur, 2015: 320-332).

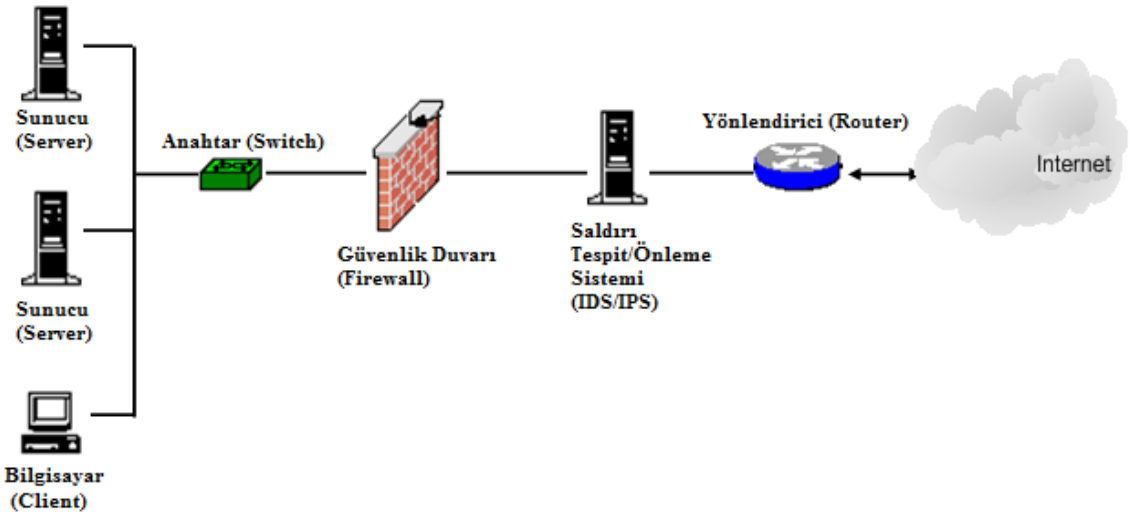
2.3.1. Zafiyet Tarayıcı (Vulnerability Scanner)

Bilgisayarlar, ağ sistemleri, işletim sistemleri ve yazılım uygulamaları dâhil bilişim sistemleri ve uygulamaları üzerinde muhtemel güvenlik açıklıklarını bularak sonuçlarını sunan bir yazılımdır (Government of the HKSAR, 2008a: 2).

2.3.2. Güvenlik Duvarı (Firewall)

Ağ veya bilgisayar sistemlerine, bağlı oldukları internet ortamından gelen bilgiden sadece izin verilenlerin geçmesini sağlayan yazılım veya donanım parçasıdır. Güvenlik duvarı, sadece internetten bilgisayara değil, aynı zamanda bilgisayardan internete giden trafik akışını da izlemekte ve paketler üzerinde filtreleme mekanizmasını kullanmaktadır (MS-ISAC ve US-CERT, 2006: 3).

Şekil 15: Saldırı Tespit / Önleme Sistemi



2.3.3. Saldırı Tespit / Önleme Sistemi (Intrusion Detection - Prevention System - IDS/IDP)

Bilgisayar veya ağın güvenliğini sağlamak adına ağ trafiğini sürekli olarak izleyen, zararlı davranışları veya yazılımları tespit eden ve şüpheli paketleri belirleyen bir yazılımdır. Saldırı tespit sistemleri, olası bir güvenlik ihlalini kaydedip, bir uyarı sinyali gönderen pasif sistemler iken, saldırı önleme sistemleri ise ağ içerisinde şüpheli bir hareket tespit ettiğinde güvenlik duvarını yeniden programlayarak ağ trafiğini engelleyen ve saldırıyı durduran aktif sistemlerdir (Martin, t.y.: 3).

2.3.4. Antivirüs

Solucanlar, virüsler, casus yazılımlar, klavye dinleme yazılımları, truva atları, arka kapı tuzakları ve rootkitler gibi zararlı yazılımları sisteme girmeden tespit eden, engelleyen ve yok eden, sisteme girmiş olanları ise tespit edip, temizleyen yazılımlara genel olarak antivirüs yazılımı adı verilmektedir (Çifçi, 2013: 200; Keleştemur, 2015: 320).

2.3.5. Veri Kaçağı Önleme Sistemi (Data Loss Prevention - DLP)

Sistem içerisindeki bilgilerin ağ üzerinden dışarıya kaçırılması veya sızdırılmasının önlenmesi amacıyla hem izleme hem de önleme yöntemiyle çalışabilen yazılım ve donanımdan oluşan bir güvenlik sistemidir (Kanagasingham, 2008: 4, 5).

2.3.6. Yığın İleti Engelleme Sistemi (Anti Spam)

Genellikle çok sayıda kullanıcıya zarar vermek ya da reklam amaçlı olarak gönderilen e-postaların, kullanıcı e-posta kutularına girmesini engelleyen sistemlere denilmektedir (Çifçi, 2013: 201; Keleştemur, 2015: 326).

2.3.7. İçerik Filtreleme Sistemi (Content Filter)

İletişim ağı içerisindeki tüm trafiği izleyerek, belirli kelimeler, resimler, web sayfaları ile sohbet programları gibi istenmeyen içeriğe sahip trafiği filtreleyen sistemlerdir (Çifçi, 2013: 203).

2.3.8. Bal Küpü (Honeypot)

Bilişim sistemlerine yetkisiz erişimleri, sistemin bir parçası gibi görünen, aslında saldırganı tespit edebilmek için tasarlanmış tuzak sistemler ile tespit eden güvenlik sistemleridir. Bal küpü sistemleri doğru kullanıldığında, iletişim ağını izleme aracı ve erken uyarı sistemi olarak hareket ettiğinden, bilgi ve iletişim teknolojileri ve ağlarına yapılabilecek saldırıları azaltmaktadır. Ayrıca saldırganın değerli bilgilerinin bulunduğu sistem açıklıklarına hangi yöntemler ile ulaşabildiğini ortaya çıkararak, müteakip

saldırılara karşı sistemlerin korunabilmelerini sağlamaktadır (Government of the HKSAR, 2008b: 2; Soysal ve Bektaş, 2009).

2.3.9. Hava Boşluğu Sistemi (Air Gap, Air Wall)

Seviyesi daha düşük bir ağdan gizlilik seviyesi daha yüksek bir ağa gerçek zamanlı güvenli iletişim sağlamak amacıyla denetimsiz veya doğrudan fiziksel bağlantıya izin vermeyen, iki ağ arasında yerleştirilen hava boşluğu sistemi ile veri aktarımının yapıldığı güvenlik sistemleridir (Yazıcı, 2011).

2.3.10. Ağ Erişim Kontrol Sistemi (Network Access Control - NAC)

Bir bilgisayarın ağa veya ağdaki çeşitli kaynaklara erişiminin gerçekleşmesinden önce bilgisayarın gerekli konfigürasyon ve güvenlik politikalarını sağlayıp, sağlamadığını kontrol eden eğer sağlıyorsa ağa bağlanmasına izin veren, sağlamıyorsa gerekli güncelleme ve ayarların yapılabilmesi için ilgili sunuculara yönlendiren sistemlerdir (Çifçi, 2013: 203; Keleştemur, 2015: 324).

2.3.11. Adli Bilişim Sistemleri (Computer Forensic Systems)

Bilgisayar ve ağ sistemleri, kablosuz iletişim ve veri depolama elemanları üzerinde bulunan bilginin mahkeme önünde delil olarak kullanılabilmesi için hukuk ve bilgisayar bilimleri çerçevesinde toplanabilmesi ve analiz edilebilmesini sağlayan sistemlerdir (US-CERT, 2008: 1).

2.3.12. Uç Nokta Güvenliği Sistemi (Endpoint Security)

Güvenlik duvarı, antivirüs, saldırı tespit/önleme, ağ erişim kontrol, veri kaçağı önleme gibi çok sayıda güvenlik yazılımlarını içerisinde barındıran, bilgi ve iletişim teknolojilerinin kurum içerisinde tek bir merkezden kontrol edilmesini sağlayan, yönetilebilirliği kolaylaştıran bütünleşik güvenlik sistemleridir (Çifçi, 2013: 204; Keleştemur, 2015: 321).

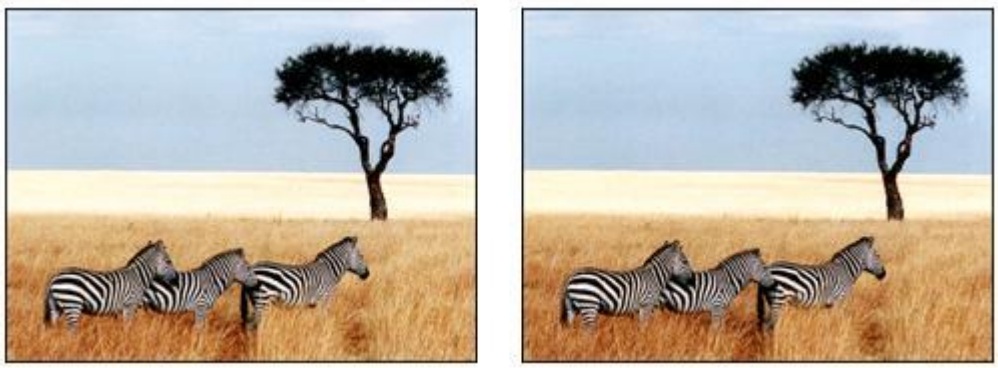
2.3.13. Şifreleme (Kriptografi)

İletişim esnasında iletilen mesajı aktif veya pasif saldırılara karşı korumak amacıyla, mesajın içeriğinin, mesajı gönderen ve alıcısı da dâhil olmak üzere şifrelenerek yetkisiz kişilerce okunmasının engellenmesi amacıyla kullanılan tekniklerdir. Kazemi (2011: 185)'ye göre şifreleme, bilgi güvenliğinin tüm prensiplerini sağlayabilmek için kullanılan matematiksel tekniklerin bütünüdür.

2.3.14. Steganografi

Özellikle kriptografi tekniklerinin bilginin güvenliğini sağlama konusunda yetersiz olduğu durumlarda kullanılmaktadır. Bilgiyi başka bir bilgi içerisinde saklayarak, iletişim içerisinde yer alan gerçeğin saklanması sanatıdır. Kriptografi tekniklerinde mesajın içeriğindeki bilgi şifrelenirken, steganografide mesaj gizlenmekte ve böylece saldırganlar bu mesajın önemli bir bilgi olduğunu fark edememektedirler (Morkel, 2005: 2).

Resim 2: **Steganografi Örneği***



Kaynak: Mataracıoğlu, 2009. *Solda, Orijinal Resim, Sağda, Bilgi Gömülü Resim

2.3.15. Elektronik İmza - Sayısal İmza (Electronic - Digital Signature)

Elektronik imza, elektronik ortam içerisinde yasal kimlik doğrulama sistemi olarak imza yerine kullanılan, üretilmiş belgelerin imzalanması yöntemlerine verilen genel isimdir. Günümüzde kullanılan çeşitli elektronik imza türleri bulunmaktadır. Örneğin, imza dosyaları, biyometri tekniği ile oluşturulan imzalar ve sayısal imzalar en çok bilinen elektronik imza çeşitleridir (Ermiş, 2006: 122-123). Asimetrik şifreleme yöntemini

kullanan elektronik imzalar, mesajın sonuna eklenerek, gönderici ve alıcının kimliğinin doğrulanmasına, mesajın inkâr edilememesine ve bütünlüğüne katkı sağlamaktadır (Yılmaz ve Salcan, 2008: 90).

2.3.16. Elektromanyetik Güvenlik (TEMPEST Karşı Tedbirleri)

Elektromanyetik yakalama veya kuvvetlendirme yoluyla bilgi ve iletişim teknolojilerinden yayılan veri sinyallerinin düşmanca niyetlerle yakalanmasına ve hasmın yönlendirilmiş enerji saldırılarına karşı alınan güvenlik tedbirleri bütününe elektromanyetik güvenlik veya TEMPEST karşı tedbirleri denilmektedir (Çifçi, 2013: 211-212). Başka bir ifade ile TEMPEST karşı tedbirleri, gizlilik dereceli bilgi işleyen bilgi ve iletişim teknolojilerinden yayılan istem dışı elektromanyetik enerji yayılımlarının araştırılmasını, yakalanmasını, analiz edilmesini ve kontrol altına alınmasını ifade eden bir terimdir (Akses, t.y.).

2.4. Yakın Geçmişte Yaşanmış Siber Saldırı Örnekleri

Kara, hava, deniz ve uzaydan sonra beşinci boyut olan siber uzay artık günümüzde siber saldırılar ile birlikte çok sık kullanılmaya başlanmıştır. Bilgi ve iletişim teknolojileri ve internetin yaygınlaşması ile birlikte, sistemlerden olumlu olarak istifade edilmesinin yanı sıra, sistemlerin açıklık ve zafiyetlerini kullanarak çalışmasını engelleyecek karşı girişimler de yoğunlaşmıştır. Özellikle kritik altyapı sektörlerine siber uzay üzerinden yapılan bu saldırılar devletlerin önemsemesi gereken tehditler arasında yerlerini almıştır. Son zamanlarda dünyada yaşanmış önemli siber saldırıların sebepleri, sonuçları ve bunların uluslararası ilişkilerdeki rolünden bahsetmenin gelecekte yaşanacak muhtemel siber saldırılara karşı farkındalık, hazırlık ve güvenlik seviyelerinin artırılması adına çok faydalı olacağı aşikârdır.

2.4.1. Rus-Çeçen Bilgi Harbi (1994)

Rus birlikleri Çeçenistan Savaşı'nda ağır silahları ile Grozni'ye girdikleri zaman karşı direnişin çok kısa süreceğini umuyorlardı. Fakat Çeçenler, propaganda faaliyetleri ile çok iyi mesajlar verdiler ve özellikle internet olmak üzere tüm medya imkânlarını

kullanarak bilgi savaşının (Information War) ilk örneğini oluşturdular (Geers, t.y.:5). İnternet ortamına aktarılan ölü Rus askerlerinin resimleri Rusya'da çok fazla yankı uyandırmış ve asker annelerinin çocuklarını kurtarmak adına harekete geçmesine sebep olmuştur. İnternetin savaş alanında kullanıldığı ilk örneğini teşkil eden bu olaydan sonra uluslararası sistemin aktörleri internet merkezli muhtemel saldırılara karşı hazırlık yapmaya başlamıştır (Aydın, 2013: 30).

2.4.2. Kosova Siber Savaşı (1999)

Kosova Savaşı'nda Sırplar tarafından Müslümanlara karşı yapılan etnik temizliğe karşı dur demek için NATO, Mart 1999'da Birleşmiş Milletler Güvenlik Konseyi'nden müdahale kararı çıkmamasına rağmen hava operasyonlarına başlamıştır. Hava operasyonları esnasında Sırp hedeflerinin vurulmaya başlanması ile birlikte Sırpların Kara El (Black Hand) grubu NATO, ABD ve İngiltere askeri haberleşme sistemlerine yönelik siber saldırılara başlamıştır. Asıl amaçları NATO askeri operasyonlarını durdurmak olan siber korsanlar, ilk büyük siber savaşın mimarları olmuşlardır (Geers, t.y.:6). Hava operasyonları sırasında Belgrad'da bulunan Çin Büyükelçiliğinin de yanlışlıkla bombalanması sonucu Çinli siber korsanlar da siber saldırılarla ABD devlet web sitelerine saldırmışlardır. ABD Ordusu ve Hava Kuvvetleri, sistemlerine bulaşan virüsleri temizleyebilmek için birkaç gün boyunca sunucularını kapatmak zorunda kalmışlardır. Saldırılarda en çok kullanılan siber saldırı yöntemleri ise DDoS ve binlerce zararlı virüs içeren istem dışı yoğun iletilerdir. Saldırılar derinlemesine araştırıldıkça, Sırp ve Çinlilere ilaveten Rus siber korsanların da eylemlere katıldığı ortaya çıkmış ve bu da reel politikadaki siyasi ittifakların siber uzayda da devam ettiğini göstermiştir. Sonuç olarak Kosova örneği, siber uzayın uluslararası aktörler tarafından hukuki olarak düzenlenmesi gerektiği ihtiyacını gündeme getirmiştir (Aydın, 2013: 31,32; Yener, 2015a).

2.4.3. Hainan Adası Olayı (2001)

Güney Çin Denizi üzerinde bir ABD casus uçağıyla Çin uçağı çarpışınca, Çin uçağı düşmüş, ABD uçağı ise hasar alarak Hainan Adası'na inişe zorlanmış ve yaklaşık 80000 Çinli siber saldırgan da ABD hükümetine karşı "ABD saldırganlığına karşı kendini savunma harekâtı" başlatmıştır (Çifçi, 2013: 164). The New York Times gazetesi ise bu

olayı Birinci İnternet Savaşı (World Wide Web War I) olarak nitelendirmektedir (Smith, 2001).

2.4.4. İkinci Irak Savaşı (Körfez Harbi) (2003)

İkinci Irak Savaşı'nda ABD, konvansiyonel savaşa başlamadan önce Irak askeri ağına sızarak, Irak Savunma Bakanlığı sistemi üzerinden binlerce Iraklı subayın savaşa girmeden teslim olmalarını sağlayan e-posta göndermiştir. Konvansiyonel savaş öncesinde propaganda amaçlı yapılan bu saldırı ile düşmanın moralini bozmak için psikolojik savaş yürütülmüş ve düşmanın savunması zayıflatılmıştır. Kimi uzmanlarca bu olay yakın geçmişte yaşanmış bir siber savaş örneği olarak görülse de, bilgi ve iletişim teknolojilerinin yok edilmesi, zarara uğratılması ya da manipüle edilmesi eylemlerini ihtiva etmediğinden bu olay için bilgi savaşı içerisinde, psikolojik savaş kavramını kullanmak daha yerinde olacaktır (Clarke ve Knake, 2010: 11,12; Çifçi, 2013: 165).

2.4.5. Estonya Olayı (2007)

İkinci Dünya Savaşı'nda Alman askerlerine karşı savaşırken ölen Sovyet askerlerini simgeleyen heykelin şehir merkezinden kaldırılması kararının Estonya hükümeti tarafından alınması üzerine üç hafta süreyle internet altyapısı, basın, medya, kolluk hizmetleri, hükümet internet sayfaları ve bankacılık hizmetleri siber saldırılara maruz kalmıştır. Avrupa'da e-devlet uygulamasının öncülerinden olan, bilgi ve iletişim teknolojilerine bağlılığı ile bilinen, internet kullanım oranının çok yüksek olduğu, bankacılık hizmetlerinin hemen hemen hepsinin internet bankacılığı üzerinden yapıldığı Estonya'da, DDoS saldırıları bu sebeplerle etkisini ikiye katlamıştır. Bu saldırılar sonucunda ülkedeki en büyük iki banka, devlet başkanlığı ve parlamentosu, bütün bakanlık ve siyasi partiler, altı büyük haberleşme kuruluşundan üçü ve iki büyük iletişim kuruluşundaki bilgisayarlar saldırılar karşısında büyük zararlara uğramış ve çalışamaz duruma gelmiştir (Çakmak ve Soyoğlu, 2009: 121). Estonya'nın NATO'dan yardım talebi karşısında da Talin'de Siber Savunma İşbirliği Mükemmeliyet Merkezi kurulmuştur. Dünya kamuoyu günümüze değin hâlâ bu saldırıların arkasında Rusya hükümeti veya istihbarat servisleri olduğu ile ilgili kesin hükümlere ulaşamamıştır (Clarke ve Knake, 2010: 16). İnternetin devlet ve özel sektör nezdinde en fazla kullanıldığı ülkelerden biri olması, bilgi ve iletişim teknolojilerine

yüksek bağımlılığı sebepleriyle Estonya, saldırılardan çok fazla zarar görmüştür. Estonya olayı, siber uzayın, politik amaçlar uğruna kullanılmaya başlandığının ve bu ortamı artık devletlerin rekabet alanı olarak gördüklerinin bir miladı olmuştur (Çakmak ve Soyoğlu, 2009: 122). Ayrıca bu olay, siber saldırıların hangi durumlarda savaş sebebi sayılacağı, siber saldırılara karşı nasıl cevap verileceği gibi konularda tartışmaların başlamasına neden olmuştur (Aydın, 2013: 35,36).

2.4.6. İsrail'in Orchard Operasyonu (2007)

1970'li yıllarda tasarlanmış ve üretilmiş F-15 ve F-16 uçakları ile İsrail, Türkiye hava sahasını da kullandığı düşünülen Orchard Operasyonunda, Suriye'nin son teknoloji ürünü hava savunma sistemleri ve radarlarına yakalanmadan, Suriye hava sahası içerisinde bulunan Kuzey Kore ve Suriye ortak nükleer tesisini bombalamıştır. İsrail o gece Suriye hava savunma sistemlerini ele geçirmiş, içerisine istedikleri görüntüleri yüklemiş ve böylece saldırı esnasında da Rus yapımı hava savunma sistemleri ve radarlar hava sahasındaki İsrail uçaklarını görememiştir (Clarke ve Knake, 2010: 4-8). Uçakların hava savunma sistemlerine yakalanmadan saldırıyı başarılı bir şekilde gerçekleştirmesinin üzerine dünya kamuoyunda şu iddialar ortaya çıkmıştır (Clarke ve Knake, 2010: 9,10):

1. İsrail, Suriye hava sahası üzerine gönderdiği ve özel boya ile boyayarak radara yakalanmaz hale getirdiği Heron insansız hava aracı ile hava sistemlerinden sinyaller alıp, aynı frekansta sinyal göndererek hava savunma sistemlerini saf dışı bırakmıştır.

2. Suriye'nin kullandığı hava savunma sistemlerine, İsrail adına çalışan bir casus tarafından truva atı zararlı yazılımı yerleştirilmiş, Heronlar tarafından gönderilen sinyalleri alan hava savunma sistemleri de bu zararlı yazılımı aktif hale getirerek, ekranlarda bir şey görünmemesini sağlamıştır.

3. İsrail casusları tarafından Suriye'deki radarlardan komuta merkezlerine giden kablolara saplama yapılarak, hava savunma sistemlerine müdahale edilmiştir.

Bu olay son teknoloji ile üretilmiş ve çok yüksek güvenlilik sağladığı düşünülen savunma sistemlerinin bile siber saldırılar sonucunda nasıl çalışamaz duruma

getirilebildiğinin kanıtı olmakla birlikte, siber savaşın net bir örneği olma özelliği taşımaktadır.

Resim 3: Orchard Operasyonu Öncesi ve Sonrası

Kaynak: Kalman, 2012.

2.4.7. Gürcistan Olayı (2008)

Dünya kamuoyu nezdinde Gürcistan toprağı olarak bilinen, fakat Rusya mali desteği ve koruması altında varlığını sürdüren Güney Osetya bölgesi sebebiyle, Rusya ile Gürcistan arasında çatışmalar çıkmıştır. Rusya, 7 Ağustos 2008 akşam saatlerinde, Gürcistan bilgi ve iletişim teknolojileri ile kritik altyapı sektörlerine karşı siber saldırılara başlamıştır. Ertesi gün ise askeri operasyon ile Güney Osetya'ya girmiştir. Kullanılan siber saldırı yöntemleri arasında Estonya örneğinde olduğu gibi DDoS saldırıları bulunmaktadır. Bu saldırılar Moskova'daki ana bilgisayar ile Türkiye, Çin, Kanada ve Estonya'daki köle bilgisayarlar aracılığıyla yapılmıştır. (Çifçi, 2013: 168) Bu saldırılarda Gürcü medyası ve kamu internet sayfaları zarar görmüş ve sonucunda da Gürcistan'ın dış dünya ile bağlantısı kopartılmıştır. Enformasyon altyapısının çok gelişmiş olmaması ile bilgi ve iletişim teknolojilerinin internete aşırı bağımlılığı olmadığından Gürcistan, bu saldırılardan az zararla çıkmıştır. Gürcistan olayının en önemli özelliği, konvansiyonel savaş yöntemlerinin yanında siber silahların da kullanılması sebebiyle operasyonel siber savaş örneği teşkil etmesidir (Aydın, 2013: 38).

2.4.8. Stuxnet (2010)

Stuxnet olayı, siber uzayda gerçekleştirilmiş en büyük gelişme ve siber güvenlik tarihinde dönüm noktası olarak kabul görmektedir (Hagerott, 2014: 244). Tüm dünyada yayılmasına rağmen en çok İran'ı etkileyen Stuxnet solucanı, İran nükleer tesislerine sızarak, yaklaşık olarak 1000 santrifüjü çalışamaz duruma getirmiş, uranyum zenginleştirme programını yaklaşık 2 yıl sekteye uğratmıştır (Mueller ve Yadegari,2012: 10). Bu bilgisayar solucanı, Microsoft Windows sistemlerindeki sıfırıncı gün açığını (Zero Day Exploit) kullanarak yayılmış ve spesifik olarak bir ana kartı hedef alacak şekilde programlanmış, sıradan kullanıcı bilgisayarlarına zarar vermemiştir. Bu sebeple yayılma tarzı, etkileri ve politik olarak kullanış şekli bakımından diğer zararlı yazılımlardan çok farklıdır. İran nükleer tesislerinde çalışan birinin kasıtsız olarak veya Mossad için çalışan birinin kasıtlı olarak bilgisayara USB belleği takarak solucanı aktif hale getirdiği ve bu şekilde sistemde yayıldığı düşünülmektedir (Aydın, 2013: 40-42).

Stuxnet, sadece ağa bağlı bilgisayarların değil aynı zamanda dış dünyaya kapalı olan ICS'leri de hedef almış olması bakımından önemli bir yere sahip olup, siber saldırılara karşı farkındalık seviyesi gelişmemiş ve yeteri kadar hazırlığı bulunmayan ülkeler için bir uyarı niteliği taşımaktadır (Çifçi, 2013: 176).

Stuxnet solucanının kodunun büyüklüğünü, karmaşıklığını ve sadece spesifik sistemlere bulaştığını düşünürsek, arkasında en az bir devlet desteği olduğu aşikardır. Dünya kamuoyu halen asıl saldırganları bulamasa da, birçok güçlü kaynak ABD ve İsrail'in ortaklaşa bu solucanı ürettiğini düşünmektedir (Mueller ve Yadegari, 2012: 10).

Stuxnet olayının en önemli özelliği, ağa bağlı olmayan sistemlere insan müdahalesi ile zararlı yazılımların yerleştirilip aktif hale getirilmesi sonucunda, siber saldırının gerçekleştirilebildiği ve bu sebeple de siber güvenlik ve savunmanın sağlanabilmesi için insan farkındalığının sistem içerisindeki tüm çalışanları kapsayacak şekilde oluşturulması gerektiğini göstermesidir.

2.4.9. Shady RAT (2006 - 2011)

İlk defa 2011 yılında McAfee'nin hazırladığı bir raporla öğrenilen Shady RAT (Uzaktan Yönetim Aracı, Remote Administration Tool) saldırıları, 2006 ile 2011 yılları arasında yapılmış olan APT türündeki casusluk eylemidir. Bu saldırılar ile 70'den fazla şirket, kurum ve kuruluş hedef alınmıştır. Günümüzde uluslararası piyasalarda rekabet ve şirket sırlarının, plan ve stratejilerin ekonomik başarılar açısından son derece önemli olduğu düşünülürse, böyle bir eylemin dünya piyasası üzerinde son derece etkili olacağı aşikârdır. Etki çapı ve süresi bakımından değerlendirildiğinde Shady RAT, siber uzay içerisinde şu ana kadar yapılmış en geniş çaplı siber saldırı türüdür (McAfee, 2011; Yener, 2015b; Çifçi, 178).

2.4.10. BlackEnergy ve KillDisk Truva Atı (2014)

BlackEnergy truva atı, ilk olarak 2007 yılında basit bir DDoS hedefli saldırılarda tespit edilen, ilerleyen zamanlarda spam göndermek, bankacılık dolandırıcılığı gibi amaçlarla kullanılmaya başlanan, 2014 yılına gelindiğinde ise yerleştirildiği bilgisayarların sabit sürücülerinden veri toplama, ağ keşfi yapma ve bilgisayarın uzaktan yönetilmesini sağlayan arka kapı niteliğinde bir zararlı yazılımdır. Çoğu Ukrayna'da olmak üzere Polonya'daki birçok devlet kuruluşunun, özel kurumların ve sivil organizasyonların bilgisayarlarında da görülmüştür. Ayrıca 23 Aralık 2015 tarihinde Ukrayna'da yaklaşık 800 bin kişiyi elektriksiz bırakan enerji dağıtım şirketlerine yapılan siber saldırılarda da BlackEnergy ile birlikte KillDisk truva atının kullanıldığı belirtilmiştir (Ukrayna Elektriğine Siber Saldırı - Enerji Günlüğü (2016) http:// enerjigunlugu.net/ukrayna-elektrigine-siber-saldiri_16907.html#.VrYB1EqLTIU).

KillDisk truva atı, sistemin yeniden başlatılmasına engel olmak için sistem dosyalarını silmesinin yanı sıra tam bir yok edici olarak çalışmakta, özellikle ICS'leri sabote etmek için geliştirilmiş ve kritik sistemleri kapatabilme yeteneğine sahip bir zararlı yazılımdır (Ukrayna'da Elektrik Dağıtım Sistemi Siber Saldırıya Uğradı (2016) http://www.hurriyet.com.tr/ukraynada-elektrik-dagitim-sistemi-siber-saldiriya-ugradi-40043686; Lipovsky, Robert, 2014). BlackEnergy ve KillDisk zararlı yazılımlarının Moskova'nın politikalarına karşı olan ülke ve özel sektör kuruluşlarının bilgisayar ve

iletişim ağlarında görülmesi bu gelişmiş siber saldırıların Rusya tarafından yapıldığının bir işaretidir. Ayrıca bilgi ve iletişim teknolojileri güvenlik analizcilerine göre gelişmiş saldırı kabiliyetlerine sahip "Vatansever Doğu Avrupa Siber Korsanları" (Patriotic Eastern European Hackers) tarafından Rusya'nın jeopolitik amaçlarını gerçekleştirmek amacıyla bu siber saldırıların gerçekleştirildiği düşünülmektedir (Dean ve Herridge, 2016).

2.4.11. Rusya ve Türkiye Arası Siber Saldırılar (2015)

Türkiye, tarihinin en büyük siber saldırılarına 14 ve 24 Aralık 2015 tarihlerinde 6 ayrı "DNS Sunucusu" hedef alınarak maruz kalmıştır. DNS sunucularına DDoS saldırılarıyla internet hizmetinin engellenmesi amacıyla yapılan bu saldırılar neticesinde "edu.tr", "gov.tr" ve "com.tr" gibi "tr" uzantılı 400 bin siteye 1 hafta boyunca ya hiç girilememiş ya da sitelere girişlerde sorunlar yaşanmıştır. Hacker grubu Anonymous saldırıları üstlenmesine rağmen, bu çapta büyük bir saldırıyı tek başına yapamayacağını savunan uzmanlara göre ise bu saldırıların arkasında bir devlet desteğinin bulunması ihtimalinin çok yüksek olduğudur. Siber saldırıların 24 Kasım 2015 tarihinde Rusya ile yaşanan uçak krizi sonrası gerçekleşmiş olması sebebiyle saldırıların arkasında Rusya'nın olması ihtimalini doğurmaktadır (Siber Saldırı Değil Savaş! (2015), http://www. haberhergun.com/bilim-teknoloji/siber-saldiri-degil-savas-h41902.html; Arslan, 2015).

Ayrıca bu bölümde ifade ettiğimiz siber saldırı örnekleri dışında Titan Rain, Conficker, İsrail'in Cast Lead Harekâtı, JSF (Joint Strike Fighter veya F-35) verilerinin çalınması, Ghostnet, Operation Aurora, Night Dragon, Duqu, Flame ve Kızıl Ekim (Red October) Virüsü gibi yaşanmış diğer siber saldırı örnekleri bulunmaktadır.

Sonuç olarak, bütün bu siber saldırı örneklerinden, günümüzde artık siber savaşın gerçek bir hal aldığı, çok hızlı bir şekilde gerçekleşerek küresel dünyada etkilerinin olduğu, genellikle konvansiyonel savaş başlamadan önce veya devam ederken başvurulan bir yöntem olduğu görülmektedir. Ayrıca en gelişmiş siber silahların kullanıldığı tam ölçekli bir siber savaşın gerçekleşmesi durumunda, dünyadaki askeri, ekonomik ve politik dengelerin topyekûn değişebileceği öngörülmektedir (Clarke ve Knake, 2010: 24).

ÜÇÜNCÜ BÖLÜM

3. DÜNYA'DA VE TÜRKİYE'DE YAPILAN SİBER GÜVENLİK ÇALIŞMALARININ DURUMU

Günümüzde ülkeler, küresel bir güç olabilmek için eski imparatorlukların yaptığı gibi coğrafi sınırlarını genişletmek yerine, teknolojik imkân ve kabiliyetleri ile birlikte nüfuzunu artırmak istemektedirler. Nüfuzunu artırmak isteyen ülkelerin kritik altyapı sektörleri, ICS'leri ve ordularının bilgi ve iletişim teknolojilerine bağımlılığı her geçen gün artmakta ve bu ülkeler de siber saldırı ve tehditlere karşı daha açık bir hedef haline gelmektedir. Çünkü siber saldırganlar, artık ellerinde karmaşık ve gelişmiş siber silahlar olmadan da hedefte ekonomik ve siyasi sonuçlar doğuracak saldırılar gerçekleştirme imkânına sahiptirler. Özellikle teknolojiye bağımlı ülkelerin, daha az bağımlı ülkelere nazaran siber saldırılara maruz kalma ihtimalinin daha yüksek olması sebebiyle de siber savunma konusunda farkındalık seviyelerini artırmak, siber güvenlik kültürünü oluşturmak ve gerekli siber savunma, korunma yöntem ve sistemlerini daha etkin kullanmak konusunda hızlı davranmaları gerekmektedir. Buradan, bir ülke siber uzayı ne kadar az kullanıyor ve siber uzaya ne kadar az bağımlıysa, o ülkenin siber saldırı ve tehditlerden etkilenme oranı da o kadar az olacaktır sonucunu çıkartabiliriz (Çifçi, 2013: 21).

Teknolojinin hayatımızın bir parçası haline geldiği, kaçınılmaz bir değişim ve dönüşüm sürecinin içerisinde bulunduğumuz bilişim çağı ve küreselleşme sonucunda devletler, kendi savunma mekanizmalarını oluşturarak en uygun siber güvenlik politikalarını belirlemek zorundadırlar. Özellikle iş dünyası, akademik camia, araştırma kuruluşları, silahlı kuvvetler, kamu ve özel sektör kuruluşlarının siber uzaya daha bağlı hale gelmesi ve siber uzayı daha sık kullanmaya başlaması sonucu bu ortama dair kural ve politikaların oluşturulması şart olmuştur. Çünkü gerçek dünyanın yerini yavaş yavaş alan, belirsizliklerle dolu siber uzayı, yeni huzursuzluklar doğurmadan, kontrol altına alabilecek siber güvenlik çalışmaları ve politikalarına ihtiyaç vardır. Bu politika ve çalışmalar kapsamında siber uzayda belli bir güce sahip olmak ve bu ortamı kontrol altına almak

isteyen ülkeler de konvansiyonel ordularının yanında siber ordular kurma çalışmalarını hızlandırmışlardır.

Çalışmamızın bu bölümünde, siber saldırı ve tehditlerin boyutlarının her geçen gün arttığı, güvenlik kaygılarının endişe yaratacak boyuta ulaştığı günümüzde, siber güvenlikle ilgili Türkiye adına örnek teşkil edebileceğini düşündüğümüz, devletler ve uluslararası örgütlerin hâlihazırdaki durumları ile Türkiye'de siber güvenlik politikaları ve kurumların çalışmalarının durumu hakkında bilgi verilecektir.

3.1. Dünya'da Siber Güvenlik Hususunda Önde Gelen Ülkeler ve Uluslararası Örgütlerin Hâlihazırdaki Durumları ve Çalışmaları

3.1.1. ABD

1990'lı yıllar itibarıyla siber güvenlik kavramını milli güvenlik kapsamına yavaş yavaş dâhil etmeye başlayan ABD, internetin hızla yaygınlaştığı 2000'li yılların ortası itibariyle de artan ağ ve bilgisayar sistemlerinin güvensizlikleri sebebiyle siber güvenlik çalışmalarını hızlandırmıştır (Wedermyer, 2012). Bu kapsamda, günümüze kadar siber güvenlik, siber savunma ve siber savaş stratejilerini dile getiren ve stratejilere yön veren bir dizi rapor ve strateji belgeleri düzenlemiştir. Bunlardan bir tanesi olan Kapsamlı Milli Siber Güvenlik İnisiyatifi (The Comprehensive National Cybersecurity Initiative - 2008) belgesinde ABD Başkanı Barack Obama, hükümet veya ülke olarak yeteri kadar hazır olmadıkları siber güvenliği ABD'nin karşılaşmış olduğu en ciddi ekonomik ve milli güvenlik meselelerinden biri olarak tanımlamıştır (The White House, 2010). Siber uzay ve güvenliğinin sağlanması hususunun ilk defa "stratejik milli çıkar" olarak belirtildiği 2010 yılı Milli Güvenlik Stratejisi (National Security Strategy) ile siber uzayın geleceği, siber güvenliğin sağlanmasına yönelik politika öncelikleri, ileriye yönelik adımların belirtildiği 2011 yılı Siber Uzay İçin Uluslararası Strateji (International Strategy for Cyberspace) önem ihtiva eden diğer strateji belgeleridir (The White House, 2010b: 27; The White House, 2011).

Siber tehditlerle mücadele konusunda ABD'nin lider konumda olduğunun vurgulandığı 2015 Milli Güvenlik Stratejisi'nde (National Security Strategy) ise siber

saldırılar, ulusal güvenliğe yönelik en büyük tehditler arasında gösterilmektedir. Bu belgede ayrıca yıkıcı ve hatta yok edici siber saldırıların her geçen gün arttığını, kötü niyetli siber saldırganlarla şiddetli bir şekilde mücadele edileceği ve siber güvenliğin sağlanması için tüm dünya ülkelerinin uzun soluklu bir işbirliği ve koordinasyonuna ihtiyaç duyulduğu belirtilmiştir (The White House, 2015: 13,24).

Siber uzaydaki en önemli aktörlerden biri olarak görülen ABD, devlet olarak siber uzayın kurulmasına destek çıkan ve kullanımını teşvik eden, özellikle Avrupa ve Asya'daki ülkelere siber sorunlar ile başa çıkılması konusunda örnek teşkil eden bir rol model konumundadır. ABD, siber saldırı ve tehditlere karşı siber savunma ve güvenlik altyapısı açısından en güçlü ülkelerden biri olarak görülse de, değişen tehdit ve saldırı potansiyeli ve her geçen gün artan siber altyapılara bağımlılığı göz önüne alındığı zaman hâlihazırdaki altyapısı ilerisi için yeterli olmayacaktır (Yıldız, 2014: 77).

ABD, ülke içerisinde başta kritik altyapı sektörleri olmak üzere, önde gelen bankalarına, özel ve kamu sektör bilişim sistemlerine sızarak güvenlik zafiyeti doğuran siber saldırılara karşı siber savunmasını güçlendirmek, farkındalık seviyesini artırmak, özellikle özel sektör şirketlerinin vuku bulan siber tehdit ve saldırıların bilgilerini özel ve kamu sektörü ile paylaşmalarını kolaylaştıracak bir mekanizmayı sağlamak maksadıyla oluşturduğu Siber Güvenlik Ulusal Eylem Planını (Cybersecurity National Action Plan - CNAP) 2016 yılı içerisinde açıklaması beklenmektedir. CNAP ile siber güvenlik sistemlerinin etkinliğini yükseltme konusunda sıkıntı yaşayan kurumlara ayrılan bütçeden öncelik tanınması ve siber güvenlik uzmanlarının kalitesinin yükseltilmesi amacıyla programlardaki yatırımların artırılması öngörülmektedir. Ayrıca kurulması öngörülen Ulusal Siber Güvenlik Esneklik Merkezi (National Center for Cybersecurity Resilience) ile kişisel bilgisayarlar dâhil kamu veya özel sektör bilişim sistemlerine bağlanacak tüm cihazların güvenlik standartlarına uygunluğunu denetlenecektir (The White House: 2016).

ABD'nin, siber güvenliğin sağlanması boyutunda, politika ve stratejilerini gerçekleştirmek için görevlendirdiği en üst düzeyde dört kurum bulunmaktadır (Çifçi, 2013: 27, 28).

1. Siber Komutanlık (U.S.Cyber Command - USCYBERCOM)
2. Milli Güvenlik Teşkilatı (National Security Agency - NSA)
3. Federal Araştırma Bürosu (Federal Bureau of Investigation - FBI)
4. İç Güvenlik Bakanlığı (Department of Homeland Security - DHS)

2008 yılında ABD Savunma Bakanlığı (U.S. Department of Defence - DoD) tarafından silahlı çatışma durumunda siber uzayın yönetilmesi görevini Hava Kuvvetleri (USAF)'ne vermiştir. Hava Kuvvetleri de sorumluluğu olan hava ve uzay alanının yanına siber uzayı dâhil ederek görev tanımını yenilemiştir (U.S. Air Force Mission, Vision, (t.y.), https://www.airforce.com/mission/vision). Daha sonra kara, hava, deniz ve uzayı da kapsayan ve tüm silahlı kuvvetler unsurlarının müşterek hareketine ihtiyaç duyulduğu siber uzayın sorumluluğunun yeni kurulacak olan ABD Siber Komutanlığına verilmesi kararlaştırılmıştır (Wedermyer, 2012). 2009 yılında kurulan 2010 yılında da tam hareket kabiliyetine ulaşan Siber Komutanlığın görevleri ise Savunma Bakanlığı bilgi ağlarını savunmak, siber uzaydaki askeri harekâtın yönlendirilmesini sağlamak, ABD ve müttefiklerinin siber uzayda bağımsız bir şekilde çalışması ve harekât yürütmesi ile hasımlarının benzeri faaliyetlerinin engellenmesi amacıyla gereken faaliyetleri planlamak, koordine etmek ve yönetmek olarak belirlenmiştir (USSTRATCOM, 2010).

Tamamen teknolojinin egemen olduğu, 2015 yılı bütçesi 509 milyon dolar olan ABD Siber Komutanlığı, hasmı caydırma konusunda dünyadaki en büyük siber savunma organizasyonlarından biridir (Gould, 2015; Çifçi, 2013: 30). ABD yüksek rütbeli askeri yetkililerine göre güçlü bir siber saldırı caydırıcılığı kazanmanın ülke bekası adına çok önemli olduğu belirtilmiştir. Açık bir şekilde ABD Savunma Bakanlığı tarafından açıklanmasa da ABD'nin aktif bir siber savunmanın yanında aktif bir siber saldırı gerçekleştirme potansiyeli olduğu aşikârdır. Gelmiş olduğu konum itibarıyla, kendisine yapılacak bir siber saldırıya karşı ABD Siber Komutanlığı, kara, hava ve deniz kuvvetleri ile müştereken karşı saldırı yapabilecek potansiyele sahiptir. Ayrıca bünyesinde yüksek teknik kapasiteye sahip, hem saldırı hem de savunma amaçlı olarak 133 ekip ve yaklaşık 6000 kişi bulunmaktadır (European Parliamentary Research Service, 2014: 4,5; Pellerin, 2014).

Ülke sınırları dışındaki iletişim ve sinyal istihbaratından, ABD devlet bilgi ve iletişim teknolojilerinin korunmasından sorumlu birim olarak görev yapan Milli Güvenlik Teşkilatı ise yabancı ülkelerin iletişim ağlarını dinleyerek istihbarat toplayan, yeryüzündeki en fazla matematikçiyi barındırdığı düşünülen, en büyük süper bilgisayarlara sahip, kriptoloji üzerine uzman bir teşkilattır (NSA, 2011; Çifçi, 2013: 37).

FBI ise federal suçların araştırılması ve ülke içinde istihbarata karşı koymayla ilgili siber olayların araştırılması ve engellemesinin yanı sıra ülke içi siber tehdit istihbaratının en üst düzeydeki yetkili kurumudur (Keleştemur, 2015: 184,185; Çifçi, 2013: 41).

Federal devlet ağlarının, kritik altyapı sektörleri ile bilgi ve iletişim teknolojilerinin güvenlik önlemelerini alan, iç güvenliği tehdit eden yüksek öncelikli siber olayların koordinasyon yetkisini üzerinde tutan, özel sektöre siber güvenlik konularında yardım eden, siber olaylara karşı ulusal çeviklik ve hazırlık derecesinin geliştirilmesini amaçlayan kurum ise ABD İç Güvenlik Bakanlığı'dır (US-DHS, 2016b). Bu bakanlık bünyesinde, bilgisayar olaylarına müdahale etmek, teknik destek ve koordinasyon sağlamak maksadıyla Bilgisayar Olaylarına Müdahale Ekibi (US-CERT-Computer Emergency Readiness Team) kurulmuştur. USCERT tarafından federal devlet ağlarına, sistemlerine karşı yapılan saldırıların tespit edilmesi ve transfer edilen tüm veri paketlerinin izlenmesi ve kontrolünü sağlamak maksadıyla 2003 yılında EINSTEIN I ve 2008 yılında da EINSTEIN II projeleri yürütülmeye başlanmıştır. Bu projelerle geliştirilen sistemler, siber tehditleri tespit ederek alarm üretmesine rağmen saldırı ve tehditlere karşı otomatik reaksiyon gösterememektedir. Bu sebeple özel sektör ve devlete ait iletişim ağlarındaki siber saldırıları derinlemesine analiz yaparak tespit edebilen ve önleyebilen EINSTEIN III projesi gerçekleştirilmiştir. Bu projeler ile 2015 yılında federal ve sivil internet trafiğinin yaklaşık yüzde 90'ının izlendiği değerlendirilmektedir (Bradbury, 2011; US-DHS, 2016a). Fakat kişisel gizliliği ihlal ettiği düşünülen EINSTEIN III projesi ise halen kamuoyunda tartışılmaya devam edilmektedir (Radack, 2009).

ABD'nin bir diğer projesi olan Savunma İleri Araştırma Projeleri Ajansı (The Defense Advanced Research Projects Agency - DARPA) tarafından yürütülen 500 milyon dolardan fazla bütçeli "Milli Siber Saha" (National Cyber Range) ile ülke içi ve dış

kaynaklı siber saldırılar bilgisayar ortamında canlandırılarak siber savaş eğitimleri icra edilmekte ve siber savaş kabiliyetleri test edilmektedir (BBC News, 2011).

Ayrıca 2006 yılından itibaren kamu ve özel sektörün siber alanda hazırlıklarını güçlendirmek maksadıyla ABD Kongresi tarafından yapılması zorunlu tutulan Siber Fırtına (Cyber Storm) tatbikatları icra edilmektedir. NSA'nın sorumluluğu altında düzenlenen Siber Fırtına I, II, III, IV tatbikatlarının genel amaçları aşağıda belirtilmiştir (US-DHS, 2016c):

1. Siber saldırılara karşı koyma, korunma ve hazırlık durumlarını görmek,

2. Siber saldırı durumunda ulusal politika ve stratejileri ile uyumlu olarak, stratejik kararların verilebilmesi ve kurumlar arası uyumun değerlendirilmesini sağlamak,

3. Siber olay durumsal farkındalığı ile birlikte siber saldırılara müdahale ve siber saldırılardan kurtulma bilinç seviyelerini artırmak,

4. Ulusal güvenlik çıkarlarına zarar vermeden, sektörler ve eyaletler arasında hassas bilgi paylaşımı yapabileceği araç ve yöntemleri belirlemektir.

Ayrıca NSA tarafından kontrol edilen, ABD, İngiltere, Avusturalya, Kanada ve Yeni Zelanda arasındaki bir anlaşma ile faaliyete geçen sinyal istihbaratı toplama ve analiz sistemi olan ECHELON ile ABD, özel olarak belirlenmiş siyasi liderler, suçlular, teröristler ve uyuşturucu kaçakçılarının her dilde telefon görüşmesini, fax ve e-posta trafiğini gerçek zamanlı olarak takip edebilmektedir (O'Neill, 2005: 212; BBC News, 2001).

3.1.2. Rusya

Son zamanlarda siber uzay, Rusya için "Savaşın Yeni Alanı" olarak görülmekte ve askeri AR-GE çalışmalarındaki önceliği olmuştur. 2010 Askeri Doktrini, askeri ve askeri olmayan güç ve kabiliyetlerinin modern askeri çatışmalar içerisinde kullanılması ile bilgi savaşının bu çatışmalar içerisindeki rolünü tanımlamaktadır. Siber uzaydan gelecek tehditlere karşı ordunun hazırlık seviyelerini artırmak amacı ile Rusya Silahlı Kuvvetleri içerisinde siber birliklerin kurulması çalışmalarına hız vermiştir. Ayrıca Rusya milli çıkar

ve amaçlarını gerçekleştirmek için ileri ve karmaşık siber saldırı teknikleri kullanmaktadır (European Parliamentary Research Service, 2014: 5).

Rusya, bilgi ve iletişim teknolojileri sektöründeki uzmanlar ve akademisyenler ile birlikte çalışarak önemli siber silahları ile güçlü bir siber savaş doktrini benimsemiştir. Konvansiyonel silahlarla birlikte kullanılan siber silahların, askeri birliklerin savaşma etkinliğini artıracağı ve böylece askeri güce bir güç çarpanı olarak etki edeceği anlayışı benimsenmiştir. Rusya, düşmanın mali, askeri ve sivil iletişim ağlarını tahrip edebilecek, konvansiyonel savaş öncesinde veya esnasında düşmanın kritik altyapı sektörlerini kullanılamaz hale getirebilecek yeteneğe sahiptir (Billo ve Chang: 2004: 107; Schaap, 2009: 139).

2000'li yılların başları itibariyle ABD askeri ve istihbarat servislerinin yüksek bilgi ve iletişim teknolojilerine sahip olması Rusya'nın iki devlet arasında olabilecek bir siber savaşı kaybedebileceği korkusunu doğurmuş, bu sebeple de siber güvenlik ve savunma konularında çalışmalarını hızlandırmak durumunda kalmıştır (Billo ve Chang: 2004: 110).

Rusya'nın siber güvenlik politikaları ve çalışmalarını yürütmek üzere Devlet Güvenlik Komitesinin (Komitet Gosudarstvennoy Bezopasnosti - KGB, Commitee for State Security) devamı olarak nitelendirilen Federal Güvenlik Servisi (Federal'naya Sluzhba Bezopasnosti – FSB, Federal Security Service) ile tıpkı ABD'deki NSA gibi çalışan Devlet İletişim ve Bilişim Federal Teşkilatı (Federal Agency for Government Communications and Information - FAPSI) isimli teşkilatları bulunmaktadır. Rusya Federasyonu'nun iç güvenliğinden sorumlu teşkilatı olan FSB, internet ile haberleşme dâhil kritik altyapı sektörlerinin korunmasından sorumlu iken FAPSI, ülkeye karşı içeriden veya dışarıdan gerçekleşebilecek siber saldırıları önceden tespit ederek, gerekli önlemleri alabilecek istihbarat çalışmalarını yapmaktadır. FAPSI ve FSB'nin casusluk üzerine muhtemel girişimlerde bulunduğuna dair kuvvetli şüpheler uyandıran bilgi toplama programını yürüttüğü düşünülmektedir (Billo ve Chang 2004: 107).

Rusya siber savaş doktrini içerisinde siber silahlar büyük öneme sahiptir. Özellikle düşman keşif ve elektronik sistemleri üzerinde üstünlük sağlamak amacıyla çatışma başlamadan önce veya esnasında güç çarpanı olarak kullanılacak olan bu siber silahların,

FAPSI ve FSB tarafından uzun dönemli planlama ve istihbarat çalışmaları neticesinde siber savaşta kullanmak amacıyla hazırlanmış, siber hedefler listesi bulunmaktadır (Billo ve Chang: 2004: 111).

Sınırları içerisindeki kritik internet altyapısının kontrolünü elinde tutan Rusya hükümeti aynı zamanda çıkardığı kanunla da internet servis sağlayıcıların yabancı bir ülkenin yetkili birimlerine ağ trafiği ile ilgili bilgi vermesini de yasaklamış ve böylece devlet eli ile gerçekleştirmiş olduğu siber saldırılar hakkında bilgilerin ulaşılmasını engellemiştir.

Son yıllarda Rusya hükümetinin yakın işbirliği içerisine girdiği yer altı suç örgütleri marifetiyle, onlara araç, malzeme ve zımni destek sağlayarak siber casusluk ve diğer siber saldırı faaliyetlerini gerçekleştirdiği düşünülmektedir (Wedermyer, 2012: 13, 14). Siber saldırıları özellikle civarındaki ülkelerin kendi çıkarları doğrultusunda hareket etmeleri için bir baskı aracı olarak kullandığı ileri sürülmektedir. Bunun en somut örnekleri arasında yakın geçmişte yaşanmış olan 2007'de Estonya, 2008'de Gürcistan, 2009'da Kırgızistan, 2014-15'te Ukrayna ve 2015'te ise Türkiye siber saldırıları bulunmaktadır (Keleştemur, 2015: 187; Çifçi, 2013: 86).

3.1.3. Çin

Siber saldırı kapasitesine ve gelişmiş istihbarat alt yapısına sahip bir devlet olan Çin, 2050 yılına kadar "elektronik egemenliği" hedefleyen ve konvansiyonel askeri operasyonların öncesinde düşman kuvvetlerini finansal, askeri ve sivil altyapıları ile iletişim yeteneklerini etkisiz hale getirebilmeyi içeren bir siber savaş doktrini benimsemiştir (Ventre, 2010; Schaap, 2009: 132). Çin, uzun bir süredir, olası bir siber savaşa hazırlık amacıyla siber saldırı kapasitesi yüksek birimler kurma ve bilişim altyapısını güçlendirme çalışmaları içerisindedir (European Parliamentary Research Service, 2014: 5).

1999 yılında Çin Halk Kurtuluş Ordusu'na (People's Liberation Army - PLA) ait PLA Daily gazetesinde, Çin'in siber savaş kapasitesinin kara, hava ve deniz gücü ile eşit öneme sahip olduğu ve ayrı bir kuvvet olarak değerlendirilmesi gerektiğinden ve internet

tabanlı tehditlere karşı önlemleri alabilmek için gerekli yazılım teknolojilerini geliştirerek, tehditlere karşı saldırılar ile cevap verebilme yeteneğine kavuşabilme hedefi içerisinde olduğu belirtilmiştir. Bu hedef doğrultusunda, çeşitli askeri ve istihbarat kaynaklarına göre Çin, ABD başta olmak üzere kendisine tehdit olarak gördüğü ülkelerin ticari, askeri ve devlete ait ağlarına karşı siber saldırılarda bulunmak amacıyla detaylı planlamalar ve hazırlıklar yapmaktadır (Keith, 2007: 59).

Siyasi yapısı ve ideolojisi sebebiyle ülkenin güvenliğinin yanında siber güvenliği de büyük oranda ordunun denetimi ve sorumluluğu altında bırakmıştır. PLA bünyesindeki Genelkurmay 3. ve 4. Dairelerinin diğer kuvvetler ile koordineli bir şekilde ülke dışındaki sinyalin toplanması, ele geçirilmesi ve analizi, Çin sınırları içerisindeki iletişim ağlarının kontrolünün sağlanması, elektronik harp, bilgi harekâtı ve siber saldırıların uygulanması gibi görevleri bulunmaktadır (Raska, 2015). PLA bünyesindeki bir diğer birim ise 2006 yılında faaliyete geçtiği ve şu ana kadar birçok batılı üst düzey firma ve devlet kurumuna karşı siber saldırılar yaptığı düşünülen Birim 61398'dir (Raf Sanchez, 2014). Bunlar dışında da 2002 yılı itibariyle teşkil edildiği düşünülen, yetenekli siber korsanlardan ve akademisyenlerden oluşan "Gönüllü Bilgi Teknolojileri Milis Birimleri" başka bir ifadeyle "İnternet Milis Birlikleri" bulunmaktadır (European Parliamentary Research Service, 2014: 5; Çifci, 2015: 43).

PLA'nın "Entegre İletişim Ağı Elektronik Harbi" (Integrated Network Electronic Warfare - Çince: wangdian yitizhan) isimli stratejisi altında, gelecek savaşlarda yer alacağı ön görülmektedir. Bu strateji, düşman bilişim sistemlerini felç etmek için kullanılan siber saldırıları, elektronik harp ve konvansiyonel silahlarla saldırı görevlerinin müştereken kullanılmasını ihtiva etmektedir. Ayrıca bu strateji kapsamında PLA içerisinde, düşman Komuta, Kontrol, Haberleşme, Bilgisayar, İstihbarat, Keşif ve Gözetleme Sistemleri (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance - C4ISR) içerisinde kör noktalar oluşturan, ihtiyaç halinde bu kör noktaları istismar ederek bu sistemlere elektronik harp, karıştırma, uydular ile saldırı düzenleyen saldırı birimleri bulunmaktadır (Raska, 2015; US-DoD, 2009: 14). Bu birimler, 2011 yılında Çin Milli Savunma Bakanı sözcüsü tarafından siber saldırılara karşı ülkelerini korumak vazifesi olan "Online Mavi Ordu" olarak tanımlanmıştır (Beech, 2011).

Çin'in 2010 yılı Savunma Raporu'nda da milli güvenliğin sağlanması konusunda siber güvenliğin önemi açıkça vurgulanmış ve siber saldırıların askeri harekâta üç önemli şekilde katkı sağladığı belirtilmiştir (US-DoD, 2015).

1. Siber casusluk yolu ile başka ülkelerden veri çalınmasına olanak tanımaktadır.

2. Ağ tabanlı lojistik, iletişim ve ticari faaliyetleri hedef alarak, hasımlarının harekâtlarını kısıtlamakta ve reaksiyon sürelerini yavaşlatmaktadır.

3. Kriz, çatışma veya savaş durumunda konvansiyonel silahlar ile birlikte kullanıldığında ise kuvvet çarpanı olarak hizmet etmektedir.

Çin, siber güvenliğinin geliştirilmesi amacıyla önde gelen üniversitelerin desteği ile sürekli olarak araştırma ve geliştirme faaliyetleri yürütmekle birlikte tıpkı ABD gibi konvansiyonel savaşları desteklemek amacıyla da siber uzaydaki faaliyetlerini genişletmekte ve siber, elektronik harp ve uzay silahları başta olmak üzere imkân kabiliyetlerini artırarak personel eğitimine ağırlık vermektedir (Keleştemur, 2015: 186; Çifçi, 2013: 43). Siber güvenlik ve siber savaş alanlarında dünyada etkin bir güç haline gelmeyi hedefleyen Çin, ordu eğitim merkezlerinde de düşman bilgi ve iletişim teknolojileri ve bilgisayar ağlarına zarar verme konuları başta olmak üzere siber savaş eğitimleri vermektedir (Ventre, 2010). Personel ihtiyacını karşılamak adına askeri birlikler, yetenekli genç siber savaşçıları keşfetmek ve yetiştirmek amacıyla düzenli olarak bilgisayar korsanlığı yarışmaları düzenlemektedir (Wedermyer, 2012: 17).

Çin, hassas verilerin ülke dışına çıkması veya içeri girmesini engelleyen, ülke içerisindeki tüm internet trafiğini kontrol altına alan, batıda "Büyük Çin Güvenlik Duvarı" olarak bilinen "Altın Kalkan" projesini yürütmektedir. Projenin en büyük özelliği herhangi bir siber savaş tehdidi algılandığı zaman, Çin'i siber uzaydan bloke ederek, dünyanın geri kalanından tecrit edebilmesidir. Ayrıca Çin devleti tarafından 2009 yılı itibariyle de başlattığı zaman zaman yürürlüğe koysa da halen tam olarak uygulayamadığı Yeşil Baraj Gençlik Koruması (Green Dam Youth Escort) projesi yürütülmektedir. Bu proje ile internet trafiği akışı izlenmekte, yasaklı sitelere erişim engellenmekte ve en önemlisi de yabancı ülkeler tarafından bilgisayarlara yüklenmiş zararlı yazılımlar tespit

edilebilmektedir (Clarke ve Knake, 2010: 35; Çifçi, 2013: 84, 85). Bu iki projenin ileride gerçekleşecek bir siber savaş durumunda Çin'e büyük avantajlar sağlayacağı kesindir.

Bu önlemlere ilaveten Çin, Microsoft ve Cisco gibi yabancı üretim işletim sistemi ve elektronik cihazların güvenlik seviyeleri ile ilgili olarak içlerinde zararlı yazılımların bulunmasından şüphe duyduğundan kendi milli üretimleri Kylin işletim sistemini, Huawei marka ağ cihazlarını ve işlemcilerini çok yoğun bir şekilde özellikle de ordu içerisinde olmak üzere kullanmaya başlamıştır (Clarke ve Knake, 2010: 35).

Siber savunma konusunda sıkı bir şekilde aldığı önlemlerin yanı sıra ağ casus istasyonları ile propaganda dağıtım unsurları kurma, mantık bombalarının siber uzaya yerleştirilmesi, ağ verilerini değiştiren cihazların üretilmesi, yanlış bilgiler ile siber uzayın doldurulması, bilişim keşif unsurlarının geliştirilmesi gibi saldırıya yönelik eylemleri de bulunmaktadır (Clarke ve Knake, 2010: 35,36; Çifçi, 2013: 41).

Çin, Pentagon yetkilileri tarafından ABD'ye karşı en önemli tehdit unsuru oluşturan ülke olarak görülmekte ve dünya genelinde birçok ülkeye siber saldırılar düzenlemektedir. Araştırmacılara göre, Çin kaynaklı siber saldırılar teknolojik olarak az gelişmiş nitelikte olmasına rağmen, birçok noktadan eş zamanlı yapılabilme özelliği sonucu oluşan geniş hacimli yapısı sebebiyle hedefte oldukça etkili olabilmektedirler (European Parliamentary Research Service, 2014: 5).

3.1.4. İsrail

Dünyada en iyi siber güvenlik ve savunma stratejisine sahip ülkelerden biri olarak kabul edilen İsrail, siber saldırılarla mücadele konusunda askeri ve istihbarat kaynaklarının imkân ve kabiliyetlerini birleştirmiştir (European Parliamentary Research Service, 2014: 6). İsrail'in kritik hükümet sistemleri, herhangi bir siber tehditten etkilenmemesi için iç ağ (intranet) gibi, internetten bağımsız olarak çalışabilen ve genellikle hassas ve gizli bilgileri taşıyan ağlar üzerinde çalışmaktadır (Yıldız, 2014: 88). İnternet güvenlik şirketi McAfee (2012)'e göre İsrail, siber saldırılara karşı en hazırlıklı ülkelerden biridir.

Uzun süredir siber savaş kapasitesine sahip askeri birlikler yetiştiren İsrail, siber savaşçılarını sadece teknik bilgi düzeylerine bakarak değil, aynı zamanda fiziksel savaşma yeteneklerine bakarak seçmektedir. Seçilen siber komandolar, hedef ülke içerisine sızarak, gerektiğinde düşman teknolojisinin keşfini yapabilecek, doğru hedefleri bulup, fiziksel tahribat yaratabilecek şekilde yetiştirilmektedir (Strategy Page, 2010).

İsrail'in ülke içerisindeki siber güvenliği sağlamak, iç istihbarat kurumu olan Şin Bet'in (Israel Security Agency - İsrail Güvenlik Servisi) görevidir. Ordu içerisindeki subaylar, MOSSAD ajanları ve emekli askerlerden oluşan Birim 8200 (Unit 8200) ise İsrail'in siber saldırı gücünü oluşturmaktadır. İsrail Savunma Kuvvetleri'nin (Israel Defence Forces) yüksek teknolojiye sahip casusluk organı olan Birim 8200, istihbarat analistleri tarafından dünyada bu konuda türünün en iyisi olduğu düşünülmekle birlikte yapısal ve çalışma mantığı olarak da NSA'in muadili olarak görülmektedir (Reed, 2015). Aynı zamanda Birim 8200, yetişmiş donanımlı personel temini konusunda akademik bir rol üstlenmekte ve eğittiği personeli çeşitli birimlerde görevlendirmektedir (Recep Kılıç, 2014).

Birim 8200'ün projesi olduğu düşünülen ve dünyadaki en önemli ve güçlü istihbarat toplama alanlarından biri olan Negev çölündeki Urim Üssü (Urim Base), sahip olduğu ileri teknolojik teçhizat ve radarlar sayesinde tüm dünyadaki internet ve veri trafiğini sürekli olarak takip edebilmektedir. Çalışma mantığı ve teknik kapasitesi ABD'nin sinyal istihbaratı toplama ve analiz sistemi olan ECHELON'a benzemektedir. (Hager, 2010).

3.1.5. AB

2013 yılında AB'nin Ortak Dış Politika ve Güvenlik konularının ana yürütücüsü ve sözcüsü konumundaki AB Dışişleri ve Güvenlik Politikası Yüksek Temsilciliği ile kriz yönetiminin sivil ayağının ortak karar alıcısı ve yürütücüsü konumundaki AB Komisyonu tarafından yayınlanan Siber Güvenlik Stratejisi Belgesinde, AB'nin siber güvenlik vizyonu ve politikasının, dünyanın en güvenli internet altyapısına sahip olmak amacıyla, AB ülke vatandaşların haklarını korumak ve savunmak olduğu belirtilmiştir. Bu vizyon ve politikanın ancak birçok aktör arasında gerçek bir ortaklığın sağlanması, sorumluluğun

birlikte alınması ve mücadelenin birlikte yapılması ile sağlanabileceği de belirtilmiştir. Ayrıca siber güvenlik seviyelerini artırmak ve vatandaşların haklarını korumak ve güvenliklerini sağlamak için sadece kamu kurum ve kuruluşları değil, aynı zamanda özel sektör kurum ve kuruluşları ile sivil toplum kuruluşları tarafından güçlü destek ve taahhütlerin verilmesi ve topyekûn işbirliğinin sağlanması üzerine durulmuştur. Siber Güvenlik Stratejisi Belgesinde ayrıca AB'nin, Avrupa'nın ihtiyacı olan siber güvenliğin sağlanması için tüm aktörler ile sıkı bir işbirliği içerisinde ve çalışma kararlılığında olduğu da belirtilmiştir (European Union [EU], 2013: 19-20).

AB Siber Güvenlik Stratejisinin, siber güvenliğin sağlanması adına aşağıda belirtilmiş beş temel önceliği bulunmaktadır:

1. Siber esnekliğinin sağlanması,

2. Siber suçların büyük ölçüde azaltılması,

3. AB Ortak Güvenlik ve Savunma Politikası (Common Security and Defence Policy - CSDF) ile ilgili olarak siber savunma politika ve yeteneklerinin geliştirilmesi,

4. Siber savunma ile ilgili endüstriyel ve teknolojik kaynakların geliştirilmesi,

5. AB ile uyumlu bir uluslararası siber güvenlik politikası oluşturmak ve AB'nin temel değerlerini desteklemektir (EU, 2013: 4, 5).

Siber güvenlik olaylarını tespit etmek ve önlemek için kamu ve özel sektöre ait kapasite, kaynak ve yöntemleri geliştirmek adına önemli bir çaba ve mücadele olmadan, Avrupa'nın siber saldırı ve tehditlere karşı savunmasız kalacağının farkına varan Avrupa Parlamentosu ve Konseyi, 2004 yılında Ağ ve Bilgi Güvenliği Teşkilatını (European Union Agency for Network and Information Security - ENISA) kurmuştur (EU, 2013: 4-5; ENISA, 2016a). AB'nin ağ ve bilgi güvenliğinden sorumlu olan ENISA'nın aşağıda belirtilmiş beş temel vazifesi bulunmaktadır (ENISA, 2016a).

1. AB sınırları içerisinde, çok yüksek ve etkin bir ağ ve bilgi güvenliği seviyesine ulaşmak,

2. AB kurumları ve üye devletler ile birlikte, AB içerisindeki iş dünyası ve kamu sektörü kuruluşları ve vatandaşların ağ ve bilgi güvenliği kültürlerinin gelişmesini sağlamak,

3. Avrupa Komisyonu, üye devletler ve iş dünyasının ağ ve bilgi güvenliği problemlerini önlemek ve çözmek,

4. Bilgi güvenliği alanında özel, teknik ve bilimsel görevleri yerine getirebilen uzman bir kurum olabilmek,

5. Ağ ve bilgi güvenliği alanında AB mevzuatının geliştirilmesi ve güncellenmesi amacıyla yapılan teknik hazırlık çalışmalarında Avrupa Komisyonuna yardımcı olmaktır.

ENISA sorumluluğu altında, Siber Avrupa 2010, Siber Atlantik 2011, Siber Avrupa 2012 ve Siber Avrupa 2014 siber güvenlik tatbikatları icra edilmiştir. Siber Atlantik 2011 tatbikatı, AB ve ABD'nin ortaklaşa icra ettikleri ilk siber tatbikat olma özelliği taşımaktadır (ENISA, 2016d). AB ile Avrupa Serbest Ticaret Birliği (EFTA) devletleri, yüzlerce siber güvenlik uzmanı ve kuruluşun katıldığı Siber Avrupa 2014 (Cyber Europe 2014 - CE 2014) tatbikatı ise ilk defa siber kriz yönetiminin farklı seviyelerini ele almak amacıyla taktik, operatif ve stratejik seviye olmak üzere üç seviyede icra edilmiştir. Bu tatbikatların amacı, büyük ölçekli siber güvenlik olaylarının etkilerini azaltmak ve siber krizler esnasında işbirliği ve bilgi paylaşımı yapabilmek için üye devletlerin eğitilmelerini sağlamaktır. Bu tatbikatlar, kamu ve özel sektör kuruluşları dâhil üye devletlerin acil durum planlarını, yeteneklerini ve siber güvenlik seviyelerini test edebilme imkânı doğurması açısından önem ihtiva etmektedir (ENISA, 2015: 8,9).

Ayrıca ENISA tarafından 2012 ve 2013 yıllarında, siber kriz durumlarıyla nasıl mücadele edileceği, işbirliğinin nasıl sağlanacağı, acil durum planlarının ne zaman uygulanacağı gibi konuların uluslararası siber güvenlik uzmanlarınca tartışıldığı ve kararların verildiği Siber Kriz İşbirliği ve Tatbikatları Konferansları (International Conferences on Cyber Crisis Cooperation and Exercises) düzenlenmiştir (ENISA, 2016c).

3.1.6. NATO

NATO, siber savunma ve güvenlik konularında çalışmalarını 90'lı yılların sonunda hızlandırmıştır. 1999'da NATO'nun Kosova Savaşı'na müdahale etmesi sonucunda Sırp siber saldırganlar tarafından NATO askeri haberleşme sistemlerine yönelik siber saldırılar yapılmış, bu da NATO'nun farkındalık seviyesini artırmıştır. 2002 yılı Prag'da icra edilen NATO zirvesinde, ilk defa siber saldırılara karşı savunma kapasitelerinin güçlendirilmesi ile ilgili bir karar alınmıştır (NATO, 2002). Müttefik ülke liderleri nezdinde, 2006 yılı Riga Zirvesinde de bilişim sistemlerine yönelik ilave koruma tedbirlerine ihtiyaç olduğu konusunda görüş birliğine varılmıştır (NATO, 2006).

2007'de Estonya'nın kamu ve özel sektör kuruluşlarının maruz kaldığı siber saldırıların ardından NATO, ilk Siber Savunma Politikasını oluşturmuştur. Bu kapsamda da 2008 yılında Estonya Tallinn'de, Müşterek Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defence Enter of Exellence – CCD CoE) kurulmuştur. CCD CoE, siber güvenlik alanında eğitim, danışmanlık, araştırma ve geliştirme ile uğraşan saygın bir merkezdir. CCD CoE, her sene dünyanın önde gelen siber savunma tatbikatlarından Locked Shields'i düzenlemektedir. 26 ülkenin ve 550'den fazla kişinin katılımıyla 18-22 Nisan 2016 tarihleri arasında dünyadaki en büyük ve en ileri uluslararası silahlı siber savunma tatbikatı düzenlenmiştir. Ayrıca hükümetlere verdiği danışmanlık hizmetleri, disiplinler arası çalışmaları, üye devletlerin katıldığı ücretsiz eğitimler ve düzenlediği konferanslar (Uluslararası Siber Çatışma Konferansları, International Conference on Cyber Conflict) ile dikkat çekmektedir (CCD CoE, 2016a; CCD CoE, 2016b; CCD CoE, 2016c; CCD CoE, 2016e).

CCD CoE nezdinde yürütülen en önemli çalışmalardan bir diğeri de, 2013 yılında yayınlanan "Siber Savaşa Uygulanacak Uluslararası Hukuk Hakkında Tallinn El Kitabı"dır (The Tallinn Manual on the International Law Applicable to Cyber Warfare). Tallinn El Kitabı, bağımsız "Uluslararası Uzmanlar Grubu" (International Group of Experts) tarafından mevcut uluslararası hukuk kurallarının, savaşın yeni şekli olan siber savaşa nasıl uygulanacağını düzenleyen, 3 yıllık bir çalışmanın ürünüdür. Tallinn El Kitabı, savaş hukuku, silahlı çatışma hukuku, uluslararası insani hukuku, silahlı çatışmada uygun araç ve yöntemlerin kullanılması gibi savaş başladıktan sonraki kuralları düzenleyen uluslararası

hukuk kuralları (jus in bello) ve devletlerin ulusal politikalarının bir aracı olarak kuvvete başvurma ve savaş açma hakkı konularını düzenleyen uluslararası hukuk kuralları (jus ad bellum) konularını içermektedir (CCD CoE, 2016d).

Tallinn El Kitabı, sadece yıkıcı ve tahrip edici siber saldırıların sebep olduğu savaş ve çatışma hukuk kuralları ile ilgilenmektedir. Fakat ülkeler, savaş sebebi sayılacak derecede yıkıcı ve tahrip edici olmayan siber saldırılara barış dönemlerinde de maruz kalmaktadır. Bu siber saldırılar, devletlerin sorumluluğu hukuku, deniz hukuku, uluslararası haberleşme hukuku, hava ve uzay hukuku, diplomasi ve konsolosluk hukuku, insan hakları hukuku kuralları ile kişi hak ve hürriyetlerine saygı gibi konuları da içinde barındıran kapsamlı bir mücadeleyi gerektirmektedir. Bu sebeple uluslararası hukukun konvansiyonel savaşı düzenleyen kurallarının siber savaşa nasıl uyarlanacağı sorusuna cevap bulan Tallinn El Kitabı'nın yetersizliğinin farkında olan NATO bünyesindeki CCD CoE, savaş ve çatışma hukuku dışında kalan genel uluslararası hukuk kurallarının siber uzay içerisinde nasıl uygulanacağına dair düzenlemeleri de içerecek olan Tallinn 2.0'ı Lahey Süreci, Hollanda Dışişleri Bakanlığı ortak girişimi ile 2016 yılı içerisinde yayınlamak için çalışmalarını hızlandırmıştır (CCD CoE, 2016d). Tallinn El Kitabı'nın ikinci versiyonu, uluslararası hukuk kapsamında resmi bir hüviyeti bulunmasa da devletlere siber uzay içerisinde barış dönemi uluslararası hukuk kurallarının nasıl uygulanacağını ve devletlerin en sık karşılaştığı siber saldırılar ile nasıl mücadele edeceği konularında referans kaynak niteliği taşıyacaktır.

2012 yılında NATO'nun Muhabere ve Bilgi Teşkilatı (NCI Agency) bünyesinde Siber Güvenlik Hizmet Hattı (CSSL), siber güvenliğin sağlanması için gerekli tüm yaşamsal faaliyetlerin yürütülmesinden sorumlu olacak şekilde faaliyete başlamıştır (NATO, 2015).

NATO son yıllarda, siber savunma yeteneklerinin geliştirilmesi amacıyla çok önemli faaliyetleri de hayata geçirmeye başlamıştır. Bunlardan belki de en önemlisi, sürekli değişen tehdit ve teknoloji ortamının hızına ayak uydurarak, NATO merkezlerine, 7/24 kesintisiz bir siber savunma desteği sağlama amacı taşıyan, NATO'nun iletişim ağlarını koruma programı "NATO Bilgisayar Olaylarına Müdahale Yeteneği"dir (NATO Computer Incident Response Capability - NCIRC). Siber savunma yeteneği gelişim

sürecine NATO kapsamında ortak bir bakış açısı kazandırma amacı taşıyan "Savunma Planlama Süreci" (Defence Planning Process - NDPP) ise, müttefik ülkelerin ulusal siber savunma yeteneklerinin gelişim hedeflerini ortaya koymaktadır (NATO, 2015).

NATO siber savunma çalışmalarını Akıllı Savunma Projeleri ile de entegre etmektedir. Akıllı Savunma Projeleri müttefik ülkelere, tek başlarına temin edemedikleri veya geliştiremedikleri yeteneklerini geliştirmek için birlikte çalışma imkânı sunmasının yanında diğer yeteneklerini geliştirmek üzere ücretsiz kaynak desteği sağlamaktadır. Akıllı Savunma Projeleri bugüne kadar, "Zararlı Yazılım Bilgi Paylaşımı Platformu" (Information Sharing Platform - MISP), "Akıllı Savunma Çok Uluslu Siber Savunma Yetenek Geliştirme Projesi" (Smart Defence Multinational Cyber Defence Capability Development - MN CD2) ve "Çok Uluslu Siber Savunma Eğitim ve Öğretim" (Multinational Cyber Defence Education and Training - MN CD E&T) projelerini hayata geçirmiştir (NATO, 2015).

NATO'nun ileri seviye politika amaçlarını gerçekleştirebilmesi için siber uzayın en önemli aktörlerinden biri haline gelen özel sektör kuruluşları bünyesindeki teknolojik gelişimlerin NATO ve müttefik ülkelere uyarlanması ve özel sektör altyapılarının korunması gerekmektedir. Bu kapsamda, siber güvenlik alanında sanayicilerle ilişkileri güçlendirmek ve işbirliği sağlamak amacıyla NATO, 2014 Galler Zirvesinde NATO Sanayi Siber Ortaklığı (NATO Industry Cyber Partnership - NICP) bildirgesini yayınlamıştır. Bu bildirgeden yalnız iki hafta sonra da 1500'e yakın sanayi lideri ve politikacının katılımı ile Bilgi Güvenliği Sempozyumu (Information Assurance Symposium) icra edilmiştir. NATO Haberleşme ve Bilgi Sistemleri Ajansı (NCIA) yetkililerinin yanı sıra NATO üyesi ülkelerden yetkililer ve siber güvenlik çözümleri olan dünyaca ünlü firmalarının katıldığı sempozyumlar da her yıl düzenlenmektedir (NICP, 2016; NCIA, 2014).

Ayrıca İtalya'da bulunan ve yakın bir zamanda Portekiz'e taşınacak olan NATO Muhabere ve Bilgi Sistemleri Okulu (Communications and Information Systems School - NCISS) ise müttefik ülkelerin personeline NATO, haberleşme ve bilgi sistemlerinin işletme ve bakımı ile ilgili eğitimler vermektedir (NATO, 2015).

Bünyesinde siber savunma ile ilgili çalışmalarını çok hızlı ve başarılı bir şekilde sürdüren, siber saldırı ve tehditlerin ulusal ve uluslararası sınırlarını aşan yapısının bilincinde olan NATO, uluslararası güvenliğin artırılması için ilgili uluslararası kuruluşlarla da işbirliği ve koordinasyon içerisindedir. NATO'nun bu kapsamda birlikte çalıştığı uluslararası kuruluşlar arasında AB, BM, Avrupa Konseyi ve Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT) bulunmaktadır (NATO, 2015).

3.2. Türkiye'de Siber Güvenlik Çalışmalarının Durumu

Türkiye'de siber güvenlik çalışmalarının durumu hakkında bilgi sahibi olunabilmesi için ilk olarak, siber güvenlik ile ilgili ilk strateji belgesi olma özelliği taşıyan "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının" onaylanmasına kadar yapılan siber güvenlik ile ilgili çalışmalar kısaca açıklanacak, müteakiben Planın stratejik eylem başlıkları çerçevesinde siber güvenlik görev ve sorumlulukların dağılımı, kamu kurum ve kuruluşları, üniversiteler ve sivil teşebbüsler tarafından günümüze kadar yürütülen faaliyetler ve çalışmalar incelenecektir.

Yürütülen faaliyet ve çalışmaların açıklanmasından sonra, Türkiye'nin siber güvenlik ile ilgili en güncel strateji belgesi olma özelliği taşıyan, 2016 yılı Nisan ayı içerisinde Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB) tarafından yayınlanan, 2013-2014 Eylem Planındaki faaliyetlerin gerçekleşme dereceleri, karşılaşılan güçlükler ve ileriye yönelik değerlendirmeler göz önüne alınarak oluşturulan, Türkiye adına önem ihtiva eden, 2016-2019 Ulusal Siber Güvenlik Stratejisi incelenecektir.

3.2.1. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı Öncesi Yapılan Çalışmalar

Siber saldırı ve tehditlerin sayısındaki ve etki çaplarındaki artış ile dünya ülkelerinin ve uluslararası örgütlerin siber güvenlik güç ve kapasitelerini artırma çabaları, Türkiye'nin de bu konuda çalışmalarına hız vermesine sebep olmuştur. Bu sebeple 2009 yılında Türkiye'de siber güvenlik ile ilgili ilk resmi nitelikte belge olan "Ulusal Sanal Ortam Güvenlik Politikası" oluşturulmuştur. Bu politikanın ana başlıkları arasında tehditler, açıklıklar, temel ilkeler ve sanal ortam güvenlik adımları olmakla birlikte,

politika belgesinde yer alan hususların uygulama adımlarını belirleyen bir strateji veya eylem planı bulunmamaktadır (Kırdı, 2015).

Uzun bir süre siber saldırı ve tehditler Türkiye'de, siber suç ve terörle mücadele kapsamı içerisinde değerlendirilmiştir. Bu saldırı ve tehditlerin küresel olarak ulaştığı boyut ve milli güvenliği de etkilemesi üzerine Milli Güvenlik Kurulu (MGK) tarafından 27 Ekim 2010 tarihli olağan toplantısında, siber saldırı ve tehditlerin engellenebilmesi için milli düzeyde yürütülen çalışmalar kapsamlı bir şekilde değerlendirilmiş ve tartışılmıştır. Olağan toplantı sonrası yayınlanan basın bildirisinde ise siber saldırı ve tehditler, Türkiye'nin tehdit algılamaları arasına alınarak, kamuoyunda "Kırmızı Kitap" olarak adlandırılan Milli Güvenlik Siyaset Belgesi'ne girmesine karar verilmiştir. Böylece siber saldırı ve tehditlere karşı önlem almaya yönelik kararlılık ve irade ortaya konmuştur (Bıçakcı, 2014: 126; MGK Genel Sekreterliği: 2010).

2012 yılında Bakanlar Kurulu'nun "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin Kararı" ile de Türkiye'de siber güvenlik konusundaki çalışmalar resmen başlamıştır. Söz konusu Karar ile "Siber Güvenlik Kurulu kurulmuş olup, siber güvenlikle ilgili Siber Güvenlik Kurulunun ve UDHB'nin görev ve yetkileri" belirlenmiştir.

Bu Karar ile Siber Güvenlik Kurulu, Ulaştırma, Denizcilik ve Haberleşme Bakanının başkanlığı bünyesinde olacak şekilde, Ulaştırma Denizcilik ve Haberleşme Bakanı, Dışişleri Bakanlığı Müsteşarı, İçişleri Bakanlığı Müsteşarı, Milli Savunma Bakanlığı Müsteşarı, UDHB Müsteşarı, Genelkurmay Muhabere, Elektronik ve Bilgi Sistemleri (MEBS) Başkanı, Milli İstihbarat Teşkilatı (MİT) Müsteşarı, Kamu Düzeni ve Güvenliği Müsteşarı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) Başkanı, Bilgi Teknolojileri ve İletişim Kurumu (BTK) Başkanı, Mali Suçları Araştırma Kurumu (MASAK) Başkanı, Telekomünikasyon İletişim Başkanlığı Başkanı (TİB) ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşmasına karar verilmiştir (Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, 2012: 3842).

Türkiye'de yapılan siber güvenlik çalışmalarının yürütülmesi ve icrasından UDHB sorumlu iken, çalışmalarla ilgili kararların verilip onaylanmasından ise Siber Güvenlik Kurulu sorumludur (Uslu, 2015). Siber Güvenlik Kurulunun kurulma kararı, Türkiye'nin siber güvenlik konusunda günümüze kadar almış olduğu en önemli stratejik adımdır ve bu güne kadar 4 kez toplanmış olup, bir dizi kararlar alınmıştır. Bu kararlar içerisinde en önemlileri aşağıda belirtilmiştir.

1. Türkiye'nin ilk Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının oluşturulması,

2. Kritik alt yapı sektörlerinin belirlenmesi ve UDHB tarafından bu konudaki çalışmaların "Ulusal Siber Güvenlik Strateji Belgesi ve 2013-2014 Eylem Planı" çerçevesinde yürütülmesi,

3. Kamu kurumları arasında güvenli bir ağ üzerinden veri aktarımı için Kamu Net projesi çalışmalarının yürütülmesi,

4. Siber Güvenlik Kurulunun Görevleri, Çalışma Usul ve Esasları Yönergesinin kabul edilmesidir (Uslu, 2015; Altıntaş, 2014).

21 Aralık 2012'de yapılan birinci Siber Güvenlik Kurulu toplantısı sonrasında UDHB koordinasyonunda, kurum, kuruluşlar ve Sivil Toplum Kuruluşlarının (STK) katkılarıyla 20 Haziran 2013'de "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" Resmi Gazetede yayınlanarak yürürlüğe girmiştir.

3.2.2. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı Kapsamında Yapılan Çalışmalar

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, kurum ve kuruluşların hizmet ve veri depolayan ya da üreten bilişim sistemleri ile kamu ya da özel sektör tarafından işletilen kritik altyapı sektörlerine ait bilgi ve iletişim teknolojilerinin güvenliğinin sağlanması ve siber güvenlik olaylarının etkilerinin en aza indirilmesini amaçlarıyla farklı kurum ve kuruluşlara görevler paylaştırmaktadır.

Eylem Planı, 7 ana başlık altında, 29 eylem maddesi, 86 alt eylem maddesi ve 31 sorumlu, ilgili kurum, kuruluş ve organizasyonu kapsamaktadır. Plan, 7 ana stratejik eylem başlığı içermektedir.

1. Yasal Düzenlemelerin Yapılması,
2. Adli Süreçlere Yardımcı Olacak Çalışmaların Yürütülmesi,
3. Ulusal Siber Olaylara Müdahale Organizasyonunun Oluşturulması,
4. Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi,
5. Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi,
6. Siber Güvenlikte Yerli Teknolojilerin Geliştirilmesi,
7. Ulusal Güvenlik Mekanizmalarının Kapsamının Genişletilmesidir (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2013: 4890).

Eylem Planı, 2013-2014 döneminde gerçekleştirilmesi planlanan işleri tanımlarken, sürekli yürütülmesi gereken eğitim ve bilinçlendirme faaliyetlerini de kapsamaktadır. Eylem Planı içerisinde, değişen şartlar, gelişen teknoloji ve ihtiyaçlar göz önünde tutularak kamu ve özel sektörden gelecek talepler doğrultusunda güncellenmesi gerektiği belirtilmiştir. Nitekim 2016 Nisan ayında da 2016-2019 Ulusal Siber Güvenlik Strateji Belgesi UDHB tarafından yayınlanarak Türkiye'nin yeni Ulusal Siber Güvenlik Stratejisi oluşturulmuştur.

3.2.2.1. Yasal Düzenlemelerin Yapılması

Eylem Planında, ulusal siber güvenliğin sağlanması konusunda, hem kurum ve kuruluşların görev, yetki ve sorumluluklarını tanımlayan, hem de ihtiyaç duyulan alanlarda mevcut eksiklikleri gidermeyi amaçlayan mevzuatın oluşturulması çalışmalarına başlanması gerektiği belirtilmiştir.

Bu kapsamda, "Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun" ile "Siber Güvenlik Kurulunun kuruluşu ve görevleri ile UDHB'nin görev ve yetkileri" belirlenerek, çalışmalar yasal bir zemine dayandırılmıştır. Aynı kanunla BTK'ya da siber güvenlikle ilgili görev verilmiştir.

Bu kapsamda, Siber Güvenlik Kuruluna verilen görevler şu şekilde belirlenmiştir (Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun, 2014: 6518; BTK, 2015):

1. Siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak,

2. Kritik altyapı sektörlerinin belirlenmesine ilişkin teklifleri karara bağlamak,

3. Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek,

4. Kanunlarla verilen diğer görevleri yapmaktır.

UDHB'ye verilen temel görev ve yetkiler şu şekilde belirlenmiştir (Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun, 2014: 6518; BTK, 2015):

1. Ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek,

2. Siber güvenliğin sağlanmasına ilişkin usul ve esasları belirlemek,

3. Eylem planlarını hazırlamak,

4. Siber Güvenlik Kurulunun sekretaryasını yapmak,

5. Kritik altyapı sektörleri ile ait oldukları kurumları ve konumları belirlemek,

6. Siber olaylara müdahale merkezlerini kurmak, kurdurmak ve denetlemek,

7. Her türlü siber müdahale aracının ve millî çözümlerin üretilmesi ve geliştirilmesi amacı ile çalışmalar yapmak, yaptırmak ve bunları teşvik etmek,

8. Bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek ve yürüttürmek,

9. Teknoloji geliştirme ve AR-GE faaliyetleri yürütmek ve yürüttürmek,

10. Siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlamaktır.

Bu Kanun ile BTK'ya verilen görev ise "siber güvenlik ve internet alan adları konularında Bakanlar Kurulu, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri TİB veya diğer birimleri marifetiyle yerine getirmek" şeklindedir. (Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun, 2014: 6518; BTK, 2015)

Eylem Planı doğrultusunda yürütülen yasal çalışmalar içerisinde Adalet Bakanlığı koordinasyonunda, UDHB ve diğer kamu kurumlarının katkıları ile "Siber Güvenlik Kanun Taslağı" hazırlanmıştır. Siber Güvenlik Kanun Taslağı ile devletin bilgi güvenliği faaliyetlerinin geliştirilmesi, gerekli politikaların üretilmesi ve belirlenmesi, bunu gerçekleştirmeye yönelik planların hazırlanması, buna yönelik metodolojinin oluşturulması ve kamu kurumlarının ve kritik altyapılara sahip özel sektör bilişim sistemlerinin siber saldırılara karşı uluslararası standartlarda korunmasını amaçlanmaktadır (T.C. Adalet Bakanlığı, t.y.). Siber Güvenlik Kanun Taslağının kabul edilmesi ile birlikte siber güvenlik kapsamında yapılacak çalışmaların hızı, hassasiyeti ve etkinliği artacaktır. Ayrıca siber uzayda gelişen teknoloji ve artan tehditler göz önüne alındığında, bir an önce yürürlüğe girmesi Türkiye adına çok faydalı olacağı aşikârdır.

3.2.2.2. Adli Süreçlere Yardımcı Olacak Çalışmaların Yürütülmesi

Ulusal ve uluslararası alanda, siber saldırı ve tehditlere maruz kalan tarafların haklarının korunabilmesi adına saldırı kaynağının tespit edilmesi, saldırıların etkilerinin belirlenmesi gerekmektedir. Eylem Planında bunu sağlayabilmek için siber uzayın gelişen teknolojiye uygun ve güvenilir kayıt mekanizmaları ile donatılması gerektiği belirtilmiştir.

Bu kapsamda Türkiye'de siber uzayda işlenen suçlarla mücadele konusunda atılmış olan adımlardan belki de en önemlisi, internet ve bilgisayar ağları aracılığıyla işlenen suçlara yönelik uluslararası bağlayıcılığı olan ilk ve tek anlaşma niteliği taşıyan "Sanal Ortamda İşlenen Suçlar Sözleşmesi"dir. Bu sözleşme 2 Mayıs 2014 tarihinde bazı çekinceler ve beyanlar ile birlikte onaylanarak 1 Ocak 2015 tarihinde yürürlüğe girmiştir (6533 Sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun, 2014: 6533). Avrupa Konseyi bünyesinde hazırlanan Budapeşte

Sözleşmesi adıyla da anılan bu sözleşme ile sanal ortamda işlenen suçların ortak tanımlarının yapılması ve uluslararası iş birliği rejiminin oluşturulması amaçlanmaktadır. Bu sözleşme, telif haklarının ihlalleri, bilgisayar kanalıyla yapılan sahtekârlık eylemleri, çocuk pornografisi, ağ güvenliğine ilişkin suçların tanımları ve bunlarla mücadele etme konuları üzerine odaklanmaktadır. Bu sözleşme ile birlikte Türkiye, internet konusunda hazırlayacağı ulusal yasa ve tüm mevzuatı, bu sözleşme hükümlerine göre yeniden düzenleyecek, internet dünyası daha da yasal zemine kavuşacak, sanal ortamda işlenen suçlarla mücadele ve uluslararası işbirliği kolaylaşacaktır. Ayrıca sözleşmenin onaylanması, Türkiye'nin Avrupa Konseyi çerçevesinde oluşturulan ortak hukuk sistemine siber uzayda işlenen suçlarla mücadele alanında da dâhil olmasını sağlayarak uluslararası saygınlığına katkıda bulunmuştur (Nebil, 2014a; Nebil, 2014b; Siber Suç Sözleşmesine TBMM'den Onay (2014), http://www.bilisimdergisi.org/pdfindir/s166/pdf/36-37.pdf).

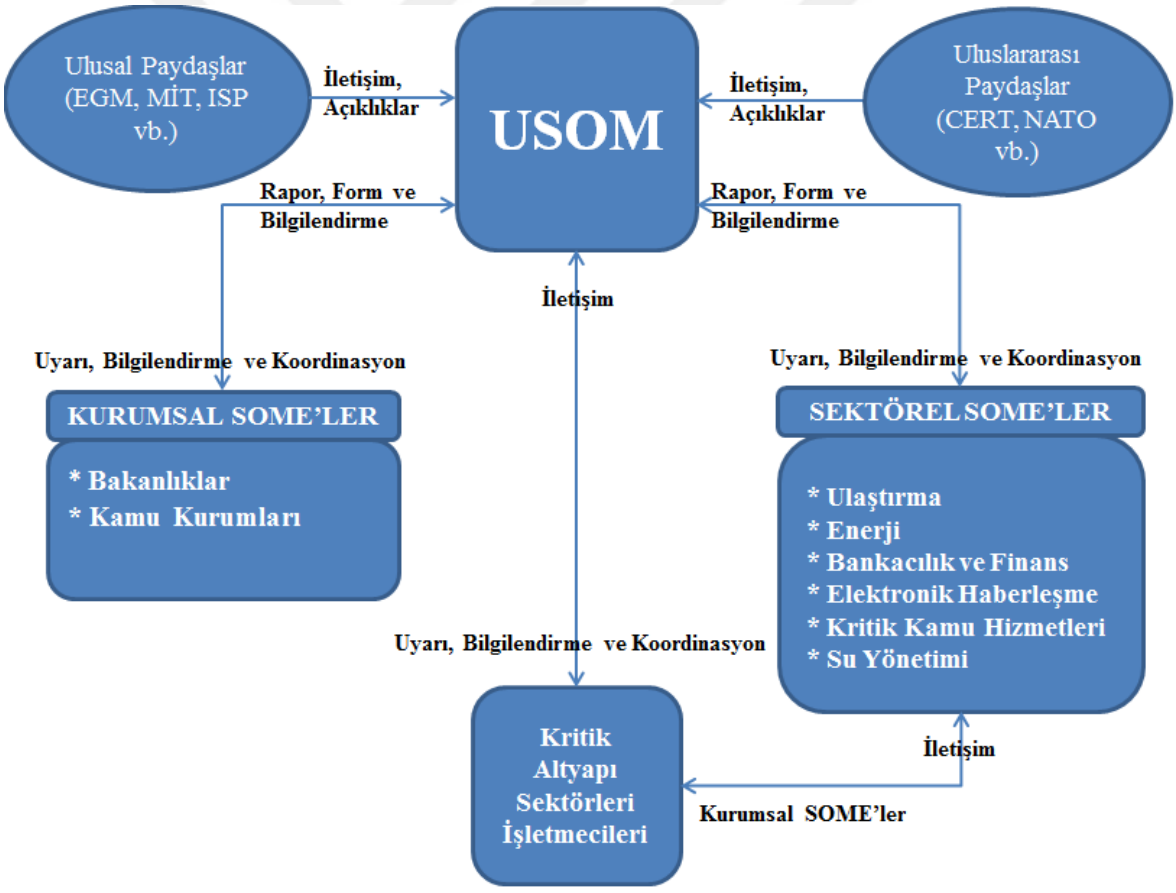
ABD ve İngiltere gibi ülkelerin Budapeşte Sözleşmenin bazı maddelerine şerhler koyması, kendilerine göre yorumlamaları, iç hukukuna uyarlamaları reddetmeleri, Rusya ve Çin gibi ülkelerin Sözleşmeyi imzalamamaları sebepleriyle Budapeşte Sözleşmesi, uluslararası siber anlaşma ihtiyaçlarını karşılamadığından tam olarak başarılı olamadığı düşünülmektedir. Ayrıca Türkiye'nin, sadece bilgi veren konumunda olmaması, gerektiği zaman da diğer ülke vatandaşlarının kişisel verilerini talep edebilen konumda olabilmesi için, Kişisel Verilerin Korunması Kanunu 24 Mart 2016 tarihinde TBMM tarafından onaylanarak, yürürlüğe girmiştir (Kişisel Verilerin Korunması Kanunu, 2016: 6698; Çifçi, 2013: 108).

3.2.2.3. Ulusal Siber Olaylara Müdahale Organizasyonunun Oluşturulması

Siber uzayda ortaya çıkan tehditlerin belirlenmesi, muhtemel saldırı ve olayların etkilerinin azaltılması veya ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi amacı güden Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT), 7/24 müdahale esasına göre çalışmak üzere 2013 yılında yayınlanan "Siber Olaylara Müdahale Ekiplerinin (SOME) Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ" ile TİB bünyesinde kurulmuş ve faaliyete geçmiştir (Altıntaş: 2014; Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, 2013).

USOM ulusal ve uluslararası siber uzayda meydana gelen siber güvenlik olaylarının tespit ve bertaraf edilmesine yönelik alarm, uyarı, duyuru faaliyetlerini yürütmekte olup, bu olaylar esnasında kamu ve özel kurumlarla koordinasyon ve gerektiğinde de onlara teknik destek sağlamaktadır (USOM, t.y.). Uluslararası alanda meydana gelen siber olaylarla ilgili tespit ettiği herhangi bir konu olduğunda ise diğer ülkelerin sahip olduğu eşdeğer bir kurum veya uluslararası kuruluşlarla işbirliği ve koordinasyon sağlamakla görevlidir (Yalçın, 2014). Bu koordinasyon ve işbirliğinin sağlanabilmesi amacıyla düzenleyici ve denetleyici kurumlar bünyesinde Sektörel SOME'lerin, kamu kurumları ve Sektörel SOME'lerin altında yer alan kritik altyapıya sahip kamu ve özel sektör bünyesinde ise Kurumsal SOME'lerin kurulması çalışmalarına başlanmıştır (USOM, t.y.).

Şekil 16: USOM ve SOME'ler Arası İlişki



Kaynak: Yalçın, 2014.

Son zamanlarda kritik altyapı sektörlerine karşı yapılan saldırıların kuvveti ve derecesinde meydana gelen artışlar sebebiyle SOME'lerin önemi de artmıştır. Bu

bağlamda, Siber Güvenlik Kurulunun belirlediği kritik altyapılar olan Enerji, Elektronik Haberleşme, Finans, Ulaşım, Su Yönetimi ve Kritik Kamu Hizmetleri sektörlerine ait düzenleyici ve denetleyici kuruluşlar varsa bu sektörlerin bünyesinde olmak üzere, eğer yoksa ilgili olduğu bakanlık bünyesinde Sektörel SOME'lerin kurulması faaliyetlerine başlanmıştır. Bir siber olay vuku bulduğunda Sektörel SOME'ler, Kurumsal SOME'ler ve USOM ile devamlı olarak iletişim halindedir ve Kurumsal SOME'lerde meydana gelen olayları da USOM'a en kısa sürede iletmekten sorumludur. Kurumsal SOME'ler de Sektörel SOME'ye bağlı kurulanlar ve kritikliklerine göre kamu kurum ve kuruluşlarında kurulanlar olarak ikiye ayrılmaktadır. Kurumsal SOME'ler, kurumların bilişim sistemlerinin siber tehdit ve saldırılara karşı korunmasını sağlamakta ve güvenlik adına alınması gereken önlemleri almaktadır. USOM ve Sektörel SOME'lerden gelen bilgiler doğrultusunda gerekli tedbirleri almakta ve tespit ettiği siber olayları da bünyesindeki Sektörel SOME'ler ile USOM'la paylaşmaktadır. Ayrıca Kurumsal ve Sektörel SOME'ler, içerisinde suç unsuru bulunan siber saldırı ve tehditlerle karşılaştığında direkt olarak kanunlarda belirtilmiş yetkili makamlara da bildirmektedir (Yalçın, 2014).

Bilgi sistemleri güvenliği ve siber savunma konusunda anında reaksiyon gösterebilmesi ve olası saldırıların etkilerinin azaltılması amacıyla TSK bünyesinde bir Siber Savunma Harekât Merkezi kurma çalışmaları başlatılmıştır. Bu kapsamda da modern savunma sanayiinin geliştirilmesi ve Türk Silahlı Kuvvetlerinin modernizasyonunun sağlanması amacıyla kurulan Savunma Sanayii Müsteşarlığı (SSM) tarafından TSK Siber Savunma Merkezi Projesi çalışmalarına hız verilmiştir. Değerlendirme aşamasında olan bu proje hayata geçer ise TSK, siber güvenliğin sağlanması, siber uzayın kontrol edilmesi ve saldırılara anında reaksiyon gösterebilmesi adına başarılı bir adım atmış olacaktır (SSM, 2015a; SSM, 2015b).

Ayrıca HAVELSAN (Hava Elektronik Sanayi) tarafından Türkiye'nin özel sektöre ait ilk siber güvenlik merkezi olan Siber Savunma Teknoloji Merkezi (SİSATEM) 24 Mart 2016 tarihinde açılmıştır (SİSATEM Açıldı (2016), http://www.havelsan.com.tr /a/Main/haber/3378/sisatem-acildi). Türkiye'nin Siber Güvenlik Mükemmeliyet Merkezi olma hedefiyle açılmış olan SİSATEM, siber güvenlik alanında AR-GE ürün ve teknolojiler geliştirecek ve geliştirilen ürünlerin testlerini ve doğrulamasını yapacaktır. Kamu veya özel sektördeki kurum ve kuruluşlara yerleştirilecek olan sensör cihazlar ile

muhtemel siber saldırılar anlık olarak takip edilecek, kurum ve kuruluşlara zarar vermesi önlenecektir (Ünal, 2016).

3.2.2.4. Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi

Eylem Planında kritik altyapılar, içerisindeki bilginin gizliliğinin, bütünlüğünün veya erişilebilirliğinin bozulması durumunda can kaybına, büyük ölçekte ekonomik zarara, kamu düzeninin veya ulusal güvenliğin bozulmasına sebep olan sistemler olarak tanımlanmış olup, tüm kurum ve kuruluşların başta kritik altyapılarına ait bilişim sistemleri olmak üzere siber güvenlik altyapılarını güçlendirmek adına çalışmalar yapması öngörülmektedir (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2013: 9). Bu sebeple özellikle Eylem Planının yürürlüğe girmesini müteakip kurum ve kuruluşlarda siber güvenlik altyapılarının güçlendirilmesi adına birçok çalışma yürütülmüştür.

Eylem Planının yürürlüğe girmesi öncesi de dünyada meydana gelen siber olaylar da bu konuda çalışmaların hızlandırılmasına sebep olmuştur. Estonya'nın 2007 yılında karşı karşıya kaldığı siber saldırılar, Rusya ile Gürcistan'ın 2008'deki kısa süreli savaşı, 2014 yılı içerisinde Ukrayna'nın yaşadığı siber saldırılar sonucu bu kritik altyapı sektörlerinin ülkeler için ne kadar önemli olduğunu ortaya çıkarmıştır. Özellikle 2007 Estonya olayları, NATO'nun, Estonya'da kurmuş olduğu Siber Savunma Mükemmeliyet Merkezine yeni sorumluluklar ve görevler yükleyerek siber güvenlik ile ilgili çalışmalarına hız kazandırmasına sebep olmuştur. Bu bağlamda Türkiye'de bu konudaki çalışmalara hız kazandıran 2010 yılı Milli Güvenlik Kurulu (MGK) Olağan Toplantısı sonucunda siber tehditlere karşı ulusal anlamda gerekli önlemlerin alınacağı vurgulanmış ve milli hedefler doğrultusunda gerekli çalışmalara başlanmıştır (Çatal, 2013; Çifçi, 2013).

TSK bu alanda başarılı çalışmalar yürüten Türkiye'deki en başta gelen kurumlardan bir tanesidir ve kara, deniz, hava ve uzay harekât alanlarını da kapsayan yeni bir harekât alanı haline gelen siber uzayda da yeteneklerini devamlı geliştirmektedir. 2010 yılı MGK Olağan Toplantısı sonucu alınacak ulusal boyuttaki önlemler ve yapılacak çalışmalar doğrultusunda 2012 yılı içerisinde Genelkurmay Başkanlığı nezdinde TSK Siber Savunma Merkezi Başkanlığı teşkil edilmiştir. 2013 yılında TSK MEBS ve Siber Savunma Komutanlığı olarak isim değiştiren komutanlığın amacı, TSK sistemlerinin siber

savunması ile sınırlı olmak şartıyla, siber tehditleri önleyen gelişmiş siber savunma ikaz ve tepki sistemlerine sahip, güçlü bir merkezi siber savunma yeteneği kazanmaktır (Çifçi, 2013: 356; Keleştemur, 2015:177; Çatal, 2014).

TSK MEBS ve Siber Savunma Komutanlığının görevleri şu şekildedir (Çatal, 2013; Güven, 2013; Çifçi, 2013: 356):

1. TSK ağı içerisinde düzenli olarak siber güvenlik test ve denetlemeleri yaparak, güvenlik açıklıklarını tespit etmek,

2. Siber olaylara 7/24 esasına göre müdahale etmek,

3. Ulusal ve NATO kapsamında icra edilen siber savunmaya yönelik tatbikatlara iştirak etmek,

4. TSK bünyesinde bilinçlendirme ve farkındalık çalışmaları yapmak,

5. TSK Siber uzayı içerisinde bulunan tüm sistemlerin siber savunmasını yapmaktır.

TSK 2014 yılında MEBS ve Siber Savunma Komutanlığının ileri seviyede teknolojik ihtiyaçları için önemli adımlar atmıştır. "Siber Savunma Projesi" ile olası bir siber savaşta başarının sağlanabilmesi adına kullandığı sistemlerinin yüzde yüz milli donanım ve yazılımlardan oluşmasını şart koşmuştur. Milli Savunma Bakanı tarafından onaylanan bu proje ile TSK'nın aldığı ürün ve sistemler, NATO ile düzenlenecek tatbikatlarda kullanabileceği, güvenli milli yazılım ve donanımlardan oluşacaktır (Çatal, 2014). Ayrıca TSK MEBS ve Siber Savunma Komutanlığı, ulusal olarak UDHB, TÜBİTAK ve diğer kamu kurumları ile uluslararası alanda da NATO ile koordineli olarak faaliyetlerini icra etmektedir.

Siber uzayda meydana gelen gelişmeler sonrasında TSK, konvansiyonel savaş ile siber savaşın birlikte yürütüldüğü hibrit (karma) savaş ortamında mücadele edebilecek yeteneğe sahip olan bir silahlı kuvvetler olmayı hedeflemektedir. Bu sebeple kuvvet planlamalarında karma savaşa hazırlık durumunu göz önünde bulundurmaktadır. Bu doğrultuda Siber Savunma Filolarını da içerecek Hava Kuvvetleri Siber Komutanlığı 2018 yılında tam harekât kabiliyetine ulaşması planlanmıştır (Gürgen, 2015a; Gürgen 2015b).

Ayrıca siber tehditlerin algılanması, zararlı yazılım barındıran ve dağıtan web sayfaları ile köle bilgisayarların tespit edilmesi, ulusal siber tehdit istatistiklerinin yayınlanması ve bu tehditlere karşı geliştirilecek savunma önlemlerinin tüm ulusal siber uzayda etkin hale getirilmesi amacıyla "Bal Küpü Sistemi" UDHB tarafından TİB bünyesinde kurularak, Haziran 2013'te faaliyete geçmiştir (BTK, t.y.a: 125; Altıntaş, 2014). Türkiye çapında 200'e yakın bölgede kurulan Bal Küpü Sistemi ile de 2014 yılı başından itibaren 330 değişik zararlı yazılım türü ve 5 milyonun üzerinde bulaşma girişimi tespit edilmiştir (8. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (2015), http://www.haberler.com/8-uluslararasi-bilgi-guvenligi-ve-kriptoloji-7829357-haberi/).

Bal Küpü Sistemi ile tespit edilen zararlı yazılımların analiz edilmesi, kara listeye alınarak ağa erişiminin engellenmesi ve bulaştıkları sistem üzerinde yaptıkları değişiklik ve etkilerinin raporlanması amacıyla TÜBİTAK bünyesinde "Zararlı Yazılım Analiz ve Mücadele Merkezi" kurulmuştur (BTK, t.y.a: 125; Altıntaş, 2014). Bunlara ilaveten, Gelişmiş Siber Tehditler (APT) Analizi Siber Güvenlik Kurulu tarafından belirli kurumlarda düzenli aralıklarla yapılmaktadır (Altıntaş, 2014).

3.2.2.5. Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi

Günümüz siber uzayı içerisinde, siber saldırı ve tehditler ile baş edebilmek için teknolojinin tek başına yeterli olmadığı, bunun yanında kritik altyapı sektörlerini kullanan insan unsurunun da güvenliğin tesis ve idamesinde kritik role sahip olduğu aşikârdır ve bu sebeple insan kaynağı siber olaylara müdahale konusunda her daim eğitimli ve hazır tutulması gerekmektedir.

Eylem Planında insan kaynağı yetiştirilmesi ve bilinçlendirme faaliyetleri kapsamında orta ve uzun vadede yapılması gereken çalışmalar şu şekildedir (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2013: 4890; Altıntaş, 2014):

1. Bilgisayar kullanıcılarının siber güvenlik konusunda bilinçlendirilmesi,

2. İlk, orta, lise öğretimi ve yaygın eğitimde siber güvenlik eğitimlerinin yaygınlaştırılması,

3. Üniversitelerde siber güvenlik eğitimlerinin yaygınlaştırılması,

4. Siber güvenlik konusunda akademisyen yetiştirilmesi,
5. Ulusal ve uluslararası siber güvenlik etkinlikleri düzenlenmesi,
6. Siber güvenlik uzmanlığına yönlendirme programının yürütülmesidir.

Bu kapsamda özellikle üniversitelerde siber güvenlik ve bilgi güvenliği programı adı altında akademisyen yetiştirilmesi ve bilimsel çalışmaların yapılması amacıyla lisansüstü eğitim programları açılmıştır.

Tablo 6: Siber Güvenlik Kapsamında Açılan Lisansüstü Programlar

Üniversite	Enstitü	Program	YL DR	Tezli Tezsiz	Eğitim Dili
Gazi Üniversitesi	Fen Bilimleri Enstitüsü	Bilgi Güvenliği Mühendisliği	DR	-	Türkçe
İstanbul Ticaret Üniversitesi	Fen Bilimleri Enstitüsü	Siber Güvenlik	YL	Tezli-Tezsiz	Türkçe
Bahçeşehir Üniversitesi	Fen Bilimleri Enstitüsü	Siber Güvenlik	YL	Tezli-Tezsiz	İngilizce
Sakarya Üniversitesi	Fen Bilimleri Enstitüsü	Siber Güvenlik	YL	Tezli	Türkçe
Gazi Üniversitesi	Fen Bilimleri Enstitüsü	Bilgi Güvenliği Mühendisliği	YL	Tezli	Türkçe
İstanbul Şehir Üniversitesi	Fen Bilimleri Enstitüsü	Bilgi Güvenliği Mühendisliği	YL	Tezli-Tezsiz	Türkçe
TOBB Ekonomi ve Teknoloji Üniversitesi	Fen Bilimleri Enstitüsü	Bilgi Güvenliği	YL	Tezli-Tezsiz	Türkçe
Hacettepe Üniversitesi	Bilişim Enstitüsü	Bilgi Güvenliği	YL	Tezsiz	Türkçe
ODTÜ	Enformatik Enstitüsü	Siber Güvenlik	YL	Tezli-Tezsiz	İngilizce
Gebze Teknik Üniversitesi	Fen Bilimleri Enstitüsü	Siber Güvenlik	YL	Tezli	Türkçe
İstanbul Medipol Üniversitesi	Fen Bilimleri Enstitüsü	Elektik, Elektronik ve Siber Sistemler Yüksek Lisans Programı	YL	Tezli	Türkçe
Yaşar Üniversitesi	Fen Bilimleri Enstitüsü	Siber Güvenlik	YL	Tezli	Türkçe

Siber güvenlik konusunda farkındalığının artırılması, siber saldırılara karşı hazırlık derecelerini görme, saldırılara karşı kurum içi politikaları değerlendirme ve kurumların

siber saldırı öncesi, esnası ve sonrasında bilgi paylaşımını, haberleşmeyi ve koordinasyonu test etmek amacıyla da ulusal ve uluslararası alanda tatbikatlar icra edilmektedir. Yapılan tatbikatlar sonucunda kurum ve kuruluşların bilgi ve iletişim teknolojileri ile kritik altyapı sektörlerini korumak için aldıkları önlemlerin ne derece etkin ve yeterli olduğu görülmektedir.

Eylem Planının yürürlüğe girmesi öncesinde 2008 yılında, ilk bilgi sistemleri güvenliği tatbikatı özelliği taşıyan "BOME Tatbikatı" ile 2011 yılında "Ulusal Siber Güvenlik Tatbikatı", 2012 yılında "Siber Kalkan Tatbikatı" ve 2013 yılında da "Ulusal Siber Güvenlik Tatbikatı" başarılı bir şekilde gerçekleştirilmiştir. Ulusal nitelikte olan tatbikatlarda, başta kamu kurum ve kuruluşları olmak üzere, pek çok farklı sektörden ve çalışma alanından katılımcıların yer almasına özen gösterilmiştir (Siber Güvenlik Enstitüsü [SGE], 2015a). Bu tatbikatların kurum ve kuruluşların ulusal düzeyde siber saldırılara karşı hazırlık durumlarını göstermesi açısından olumlu katkıları olmasına rağmen sadece ulusal ölçekte düzenlenmiş olmaları en büyük olumsuz tarafıdır.

Eylem Planının 20 Haziran 2013 tarihinde yürürlüğe girmesi ile ve Sanal Ortamda İşlenen Suçlar Sözleşmesi'nin 2 Mayıs 2014 tarihinde çekinceler ve beyanlar ile birlikte yasalaşması sonucu uluslararası alanda bir tatbikatın yapılması hâsıl olmuştur. Bu tatbikat, 15-16 Mayıs 2014 tarihleri arasında İstanbul'da, UDHB desteğiyle, BTK ve ITU-IMPACT işbirliği ile gerçekleştirilen Uluslararası Siber Kalkan 2014 tatbikatıdır (International Cyber Shield Exercise). Etkinliğin ilk gününde Çocukların İnternetin Zararlı Etkilerinden Korunması, Mobil Güvenlik ile Adli Bilişim ve Siber Soruşturma konulu çalıştaylar gerçekleştirilmiş olup, ikinci gününde ise 19 ülkenin katılımıyla tatbikat icra edilmiştir. İcra edilen tatbikatın amaçları ise şu şekilde belirlenmiştir (BTK, t.y.b):

1. Siber güvenliğin sağlanması boyutunda uluslararası işbirliğinin önemi vurgulanarak, ITU-IMPACT ve katılımcı ülkeler ile söz konusu işbirliğinin artırılması,

2. Siber güvenlik hususunda Türkiye'nin adının duyurulması,

3. Ulusal çapta yapılmış tatbikatların uluslararası alana taşınmasıdır.

Türkiye'de bilgi ve iletişim teknolojileri güvenliği alanında, bireysel, kurumsal, ulusal ve uluslararası alanda, teknik, bilimsel, sosyal ve kültürel faaliyetler yürütmek,

üyelerinin mesleki gelişimini arttırmak, siber güvenlik kültürünün oluşturulmasına katkıda bulunmak, konferans, çalıştay, seminer, kurs ve benzeri etkinlikler düzenleyerek bilinçlendirme faaliyetleri yapmak gibi amaçlarla kurulmuş olan kamu yararına faaliyet gösteren Bilgi Güvenliği Derneği ve Siber Güvenlik Derneği gibi sivil toplum kuruluşları da bulunmaktadır. Hemen hemen her yıl olmak üzere, Bilgi Güvenliği Derneği tarafından Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (International Conference on Information Security and Cryptology - ISC), Siber Güvenlik Derneği tarafından da ulusal düzeyde "Siber Güvenlik Konferansı" düzenlenmektedir. Bu dernekler bünyesinde ayrıca siber güvenlik uzmanı yetiştirme kampları, siber güvenlik çalıştayları, raporları ve sempozyumları da düzenlenmektedir (Bilgi Güvenliği Derneği, 2016; Siber Güvenlik Derneği, t.y.; Çifçi, 2013: 377).

2013 ve 2014 yıllarında Ankara'da Savunma Sanayi Müsteşarlığı (SSM) tarafından Uluslararası Siber Savaş ve Güvenlik Konferansları (International Cyber Warfare and Security Conference-ICWC) düzenlenmiştir. Siber güvenlik kavramının her boyutuyla tartışıldığı bu konferanslar, ulusal ve uluslararası katılımcıların olduğu kadar, kamu ve özel sektörün de bakış açısını karşılaştırmalı olarak görebilmek adına oldukça faydalı olmuştur (ICWC, 2014).

Ayrıca kamu ve özel sektör kurum ve kuruluşlarının siber güvenlik ihtiyaçlarının karşılanması amacıyla hâlihazırda Türkiye'de 15 bin civarında siber güvenlik uzmanı ihtiyacı olduğu bilinmektedir (Ünal, 2016). Bilgi Güvenliği Akademisi tarafından ağ ve sistem güvenliği eğitimleri, sızma testleri uzmanlık eğitimleri, ileri seviye bilişim güvenliği eğitimleri, kurumsal bilgi güvenliği eğitimlerinin yanı sıra siber güvenlik kış ve yaz kampları düzenlenerek, Türkiye'nin ihtiyaç duyduğu siber güvenlik uzmanı eksikliğinin giderilmesine destek olunması ve kapasite geliştirilmesinin sağlanması amaçlanmaktadır (Bilgi Güvenliği Akademisi, t.y.). Bilgi Güvenliği Derneği de 2011 yılı itibariyle aynı amaçlar doğrultusunda düzenli olarak siber güvenlik uzmanı yetiştirme kampları düzenlemektedir (Bilgi Güvenliği Derneği, 2015). Amaçlarından bir tanesi siber güvenlik uzmanı yetiştirmek olan, HAVELSAN bünyesindeki SİSATEM'in bu alanda çalışmalara ön ayak olması gerektiğini düşünmekteyiz.

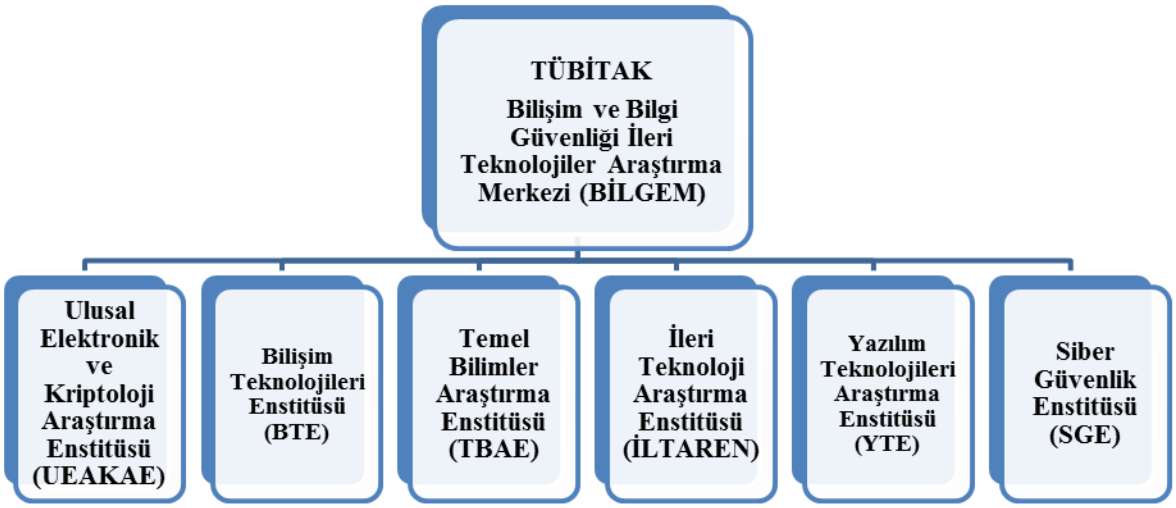
3.2.2.6. Siber Güvenlikte Yerli Teknolojilerin Geliştirilmesi

Eylem Planında özellikle, kamu ve özel sektör bilişim sistemlerinde yerli olarak üretilmiş ve geliştirilmiş ürünlerin kullanılması, yerli ürünlerin mevcut olmadığı takdirde ise güvenlik önlemleri alınmış sertifikalı ürünlerin tercih edilmesi gerektiği üzerine durulmuştur (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2013: 4890).

Bu kapsamda, UDHB koordinasyonunda, araştırma ve geliştirme faaliyetlerinin teşvik edilmesi, siber güvenlik konusunda araştırma ve geliştirme laboratuvarlarının kurulması, siber güvenlikte yerli ürün ve çözüm çalışmaları ve yerli ürünlerin teşvik edilmesi çalışmalarına hız verilmiştir (Uslu, 2015).

Siber güvenlikle ilgili yerli teknolojilerin geliştirilmesi hususunda önde gelen önemli kuruluşlardan biri olan TÜBİTAK'ın Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM), bilgi güvenliği, yazılım ve haberleşme alanlarında Türkiye'nin en yetkin araştırma ve geliştirme merkezi olma niteliği taşımaktadır. BİLGEM bünyesinde faaliyet gösteren altı adet enstitü bulunmaktadır (Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi [BİLGEM], 2015).

Şekil 17: TÜBİTAK BİLGEM Bünyesindeki Enstitüler



BİLGEM'e bağlı enstitülerden biri olan Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE), Türkiye'deki kamu kurumlarının ihtiyaç duyduğu bilgi güvenliği ve elektronik sistem projelerini geliştirmekte ve teknolojik dışa bağımlılığı azaltmak amacıyla

da kritik öneme haiz cihazların bileşenlerini üretmektedir Kriptoloji ve bilgi güvenliği konusunda Türkiye'nin en büyük kütüphanesine sahip UEKAE, siber güvenliğe yönelik teknolojiler, çözümler, projeler gerçekleştirmiş ve birçok ürün üretmiştir. Bunlar arasında, güvenli haberleşme sistemleri, kriptolojik anahtar yönetim sistemleri, akıllı kart ve kimlik doğrulama sistemleri, elektronik sertifika yönetim çözümleri, elektro-optik ve lazer çözümleri, TEMPEST ürünleri, radarlar, yazılım tabanlı telsizler ve daha birçok proje yer almaktadır. (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü [UEKAE], 2015).

BİLGEM'e bağlı enstitülerden bir diğeri ise, siber güvenlik alanında araştırma ve geliştirme faaliyetleri yürüten, askeri kurumlara, kamu kurum ve kuruluşlarına ve özel sektöre çözüme yönelik projeler gerçekleştiren ve Türkiye'de siber güvenlik bilgi birikimi oluşturulmasına önemli katkılar sağlayan Siber Güvenlik Enstitüsüdür (SGE). SGE bünyesinde, Sızma Testleri, Güvenli Yazılım Geliştirme, APT Analizi, Zararlı Yazılım Analizi, Dijital Adli Analiz, BT Ürün Güvenliği, Bilgi Güvenliği Eğitimleri, Bilgi Güvenliği Yönetim Sistemleri çözümleri ile Siber Ortam Tuzak Sistemi (SORT), Siber Tehditleri Algılama Sistemi (STAMP), Veri Kaçağı Önleme Sistemi (VKÖS), Harici Medya Yönetim Analiz Sistemi (HARMAN), İnternet Erişim Kontrolü ve Raporlama Sistemi (FİLTRE), Siber Güvenlik Simülasyon ve Yarışma Ortamı (Siber Meydan CTF) teknolojileri geliştirilmiştir (SGE, 2015b).

BİLGEM enstitüleri bünyesinde bugüne kadar gerçekleştirilen yüzlerce başarılı ürün, çözüm ve projeler birçok Avrupa ve Asya ülkesi ile NATO tarafından kullanılmaktadır. BİLGEM'in katkılarıyla teknolojik bağımsızlığını ilan eden ülkeler arasında yerini alan Türkiye, bilişim ve bilgi güvenliği alanlarında üretmiş olduğu bu gelişmiş teknolojileri dış pazara ihraç eden ve dünya devleri ile rekabet edebilen bir ülke konumuna gelmiştir (BİLGEM, 2015).

Ayrıca TSK'nın haberleşme cihaz ihtiyaçlarının karşılanması amacıyla 1975 yılında kurulan TSK Güçlendirme Vakfı kuruluşu olan ASELSAN (Askeri Elektronik Sanayii), "Kripto ve Bilgi Güvenliği Sistemleri" adı altında haberleşme ve iletişim sistemleri ile bilgi teknolojilerine yönelik, kriptografik ve bilgi güvenliği ürünlerinin proje, tasarım ve geliştirme faaliyetlerini yürütmektedir (ASELSAN, 2016a). Siber güvenlikle ilgili ASELSAN'ın ürettiği başlıca güvenlik sistemleri, Yeni nesil IP Ağ Kripto Cihazı, USB

Kripto Cihazı, Güvenli Disk Kriptolama Ürünleri, Sanal Hava Boşluğu Sistemi (SAHAB), Elektronik Anahtar Yönetim Sistemi, Güvenlik Yönetim Sistemleri, Tümleşik Tehdit Yönetim Sistemlerinden oluşmaktadır (ASELSAN, 2016b).

1982 yılında TSK'nın yazılım mühendisliği alanındaki ihtiyaçlarını karşılamak amacıyla ABD ortaklığıyla kurulan, 1985 yılında ise sermayesinin %98'i TSK Güçlendirme Vakfına ait bir kuruluş haline gelen HAVELSAN, Türkiye'nin kritik ve çok önemli Siber Güvenlik ve Bulut Bilişim Teknolojileri gereksinimlerini karşılamak amacıyla etkin, güçlü, kaliteli ve ulusal siber savunma sistemleri geliştirerek, ileri siber güvenlik hizmetleri vermektedir (HAVELSAN, 2015a; Çifçi, 2013: 376). Siber güvenlik hizmetleri arasında, Ağ Güvenliği, Olay, Kayıt Yönetimi ve İzleme, Varlık ve Zafiyet Yönetimi, Altyapı Güvenliği, Veri Güvenliği, Sistem Güvenliği, Güvenlik Testleri, Erişim Güvenliği, Son Kullanıcı Güvenliği ve Mobil Güvenlik hizmetleri bulunmaktadır (HAVELSAN, 2015b).

3.2.2.7. Ulusal Güvenlik Mekanizmalarının Kapsamının Genişletilmesi

Eylem Planında ulusal güvenlikten sorumlu kurumların görev alanlarına ulusal ve uluslararası siber uzayda meydan gelen zararlı faaliyetlere karşı savunmanın da ilave edilmesi gerektiği belirtilmiştir (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2013: 4890).

Ulusal güvenlik mekanizmalarının kapsamının geliştirilmesi boyutunda katkı sağlayan, özel sektör, kamu sektörü ve akademisyenlerin katkılarıyla, siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olduğu bilincinin tüm kesimler tarafından özümsenmesi amacı taşıyan 2016-2019 Ulusal Siber Güvenlik Stratejisi, 2016 yılı Nisan ayı içerisinde UDHB tarafından yayınlanmıştır.

3.2.3. 2016-2019 Ulusal Siber Güvenlik Stratejisi

Gelişen bilgi ve iletişim teknolojileri, artan internet kullanım oranları ile paralel olarak artan güvenlik gereksinimleri sonucu 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planının yeni şartlara uyarlanması hâsıl olmuştur. Bu sebeple UDHB'na bağlı Siber

Güvenlik Kurulu koordinesinde 2015 yılı içerisinde sorumlu veya ilgili kurumlarla birlikte 7 adet değerlendirme toplantısı yapılmış, toplantıların ardından kritik altyapı işletmecileri, bilişim sektörü, üniversiteler, kamu kurumları ve sivil toplum kurumlarını temsilen 73 kurum ve kuruluştan toplam 126 uzmanın katılımı ile Ortak Akıl Platformu gerçekleştirilmiştir. Bu platform çalışmaları bünyesinde, Türkiye'nin siber güvenlik boyutunda, stratejik amaçlar ve gerçekleştirmesi gereken eylemler belirlenmiştir. Yeni Siber Güvenlik Stratejisi oluşturulurken dünya ülkelerinin siber güvenlik stratejileri gözden geçirilmiş, bu ülkelerin siber güvenlik alanında hedefleri, öncelikleri, kuruluş yapıları, AR-GE çalışmaları, kaynak tahsisleri, kamu ve özel sektör kurum ve kuruluşları arası koordinasyon ve işbirliği ile eğitim durumları göz önüne alınmıştır (2016-2019 Ulusal Siber Güvenlik Stratejisi, 2016: 6).

Ulusal Siber Güvenlik Strateji Belgesi, kamu ve özel sektör nezdinde işletilen kritik altyapılara ait bilişim sistemleri yanında küçük ve orta ölçekli sanayi, özel ve tüzel kişiler de dâhil olmak üzere ulusal siber uzayı oluşturan Türkiye ölçeğinde bütün bileşenleri kapsamaktadır. Ayrıca siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olduğu bilincinin tüm kesimler tarafından özümsenmesi ve ulusal siber uzayı oluşturan tüm elemanların güvenliğini sağlamak amacıyla idari ve teknolojik önlemelerin alınmasını sağlayacak yeterliliğin kazanılması amacı taşımaktadır (2016-2019 Ulusal Siber Güvenlik Stratejisi, 2016: 9).

Diğer devletlerin strateji dokümanları da incelenerek oluşturulan Siber Güvenlik Stratejisi kapsamında, Türkiye açısından olası siber güvenlik riskleri ve riskleri ortadan kaldıracak eylemler uygulanırken, göz önünde bulundurulacak ilkeler belirlenmiş olup, aşağıda belirtilmiştir (2016-2019 Ulusal Siber Güvenlik Stratejisi, 2016: 11).

1. Risk yönetimi, teknik zafiyetlerin hızlı bir şekilde giderilmesini, siber saldırı ve tehditlerin önlenmesini, fark edilmesini, karşılık verilmesini ve muhtemel zararın minimum seviyeye indirilmesini içermektedir. Kritik altyapı sektörlerinin siber saldırı ve tehditlere karşı etkin ve sürekli bir risk yönetimi metotları geliştirilerek siber güvenliklerinin sağlanması gerekmektedir.

2. Ulusal siber uzayı oluşturan tüm paydaşların siber güvenlik risklerini bilmeleri, bu risklerin başka paydaşları da etkileyebileceği bilincinde olmaları, bu

farkındalık ve yetkinliğin sağlanması adına gerekli eğitim ve deneyimi kazanmalarının amaçlanması gerekmektedir. Siber güvenliğin sağlanması boyutunda teknik önlem ve tedbirlerin yanı sıra hukuki, ekonomik, idari, politik ve sosyal boyutları da içeren topyekûn bir yaklaşım benimsenmesi gerekmektedir.

3. Siber saldırı ve tehditler sonucu doğabilecek zararların minimum seviyede tutulması için siber olaylara karşı paydaşların hazırlık ve süreklilik planının bulunması ve uygulanması önem ihtiva etmektedir.

4. Siber uzay güvenliğinin sağlanabilmesi ve bu güvenliğin sürdürülebilmesi için, kamu, özel sektör, üniversiteler, STK'lar ve hatta bireyler arasındaki işbirliği ve koordinasyonu yanı sıra uluslararası işbirliği, koordinasyon ve bilgi paylaşımı çok önem arz etmektedir.

5. Siber güvenliğin sağlanması amacıyla atılan tüm bu adımlar çerçevesinde, hukukun üstünlüğü, temel insan hak ve hürriyetleri ile mahremiyetinin korunması ve ifade özgürlüğü kavramları sürekli olarak gözetilmesi gereken temel ilkelerdir.

6. Siber uzaydaki mevcut ve muhtemel risklerin yönetimi ile ilgili sorumluluklarını yerine getiren tüm paydaşlar, şeffaflık, hesap verilebilirlik ve etik değerleri devamlı göz önünde bulundurmaları gerekmektedir.

7. Siber uzaydaki mevcut ve muhtemel risklere karşı alınan siber güvenlik önlemlerinin orantılı olması, olumlu ve olumsuz sonuçlarının önceden değerlendirilmesi ve ona göre dengelenmesi gerekmektedir.

8. Siber güvenlik gereksinimlerinin karşılanmasına yönelik olarak yerli ürün ve hizmet kullanımı teşvik edilmeli ve bu kapsamda AR-GE projeleri desteklenmeli ve yenilikçi anlayış esas alınmalıdır.

2016-2019 Ulusal Siber Güvenlik Stratejisi oluşturulurken ulusal siber uzay içerisinde başlıca siber güvenlik riskleri ise şunlardır (2016-2019 Ulusal Siber Güvenlik Stratejisi, 2016: 12,13):

1. Kritik altyapı sektörlerinin bilişim sistemlerine karşı yapılabilecek DoS ve DDoS benzeri hedef odaklı saldırılar sonucu, ulaştırma, enerji, su vb. kritik hizmetlerin sekteye uğraması,

2. Siber saldırılar sonucu bireylere ait kişisel bilgilerin veya kamuya ait gizli bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi,

3. AR-GE ve üretim yapan kurum ve kuruluşların ticari sırlarının saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi,

4. Propaganda amacıyla yapılan haktivizm saldırıları sonucu hedef kurum ve kuruluşların itibarlarının zarar görmesi, hassas bilgi, verinin ifşa olması, değiştirilmesi veya yok edilmesi,

5. İnternet servis sağlayıcı konumunda bulunan kuruluşların, (e-ticaret yapan, sosyal medya hizmeti veren, e-posta hizmeti veren kuruluşlar) DoS, DDoS ve benzeri hedef odaklı saldırılar sonucunda maddi kayba uğraması, sahte işlem kaydı oluşturulması, gizli bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi,

6. Finans ve bankacılık sektörü, e-ticaret yapan kuruluşlar veya çevrimiçi ödeme ve para transferi yapan kuruluşların müşterilerine ait kritik ve gizli bilgilerin saldırganların eline geçmesi sonucu itibar kaybına uğraması, bilgileri ele geçirilen müşterilerin maddi kayıplara maruz kalmaları, toplum içerisinde çevrimiçi işlemlere yönelik güven kaybının oluşması,

7. Bilişim sistemlerindeki güvenlik önlemleri eksikliğinden veya kullanıcı hatalarından dolayı, küçük ve orta ölçekli sanayi, ticaret ve hizmet sektöründeki kuruluşların faaliyetlerinin kesintiye uğraması, hassas veya ticari değere sahip bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi,

8. Siber güvenlik alanı ile ilgili yeterli düzeyde bilinç ve farkındalık seviyesine sahip olunmaması, bilişim sistemlerinde yeterli kişisel güvenlik önlemelerinin alınmaması ve Türkiye'nin internete ve sosyal ağlara olan artan bağımlılığı gibi sebeplerle kötücül yazılım, oltalama, sosyal mühendislik, dolandırıcılık, kimlik hırsızlığı, kişisel verilerin ve cihazların saldırganlar tarafından ele geçirilmesi, değiştirilmesi veya yok edilmesi, sahte işlemlerin yapılması,

9. Her türlü kurum ve kuruluşta kötücül yazılım, yığın ileti ve benzeri saldırılar sonucu dolandırıcılık olayları ile karşı karşıya kalınması,

10. Her türlü kurum ve kuruluşta kullanıcı hataları veya doğal afetler sonucunda bilgi ve iletişim teknolojileri aracılığıyla verilen hizmet ve faaliyetlerin kesintiye uğraması.

2016-2019 döneminde, mevcut riskleri, belirlenen ilkeler ışığında asgari düzeye indirmeyi hedefleyen stratejik amaçlar da şunlardır (2016-2019 Ulusal Siber Güvenlik Stratejisi, 2016: 13,14):

1. Ulusal düzeyde kritik altyapı sektörlerin envanterinin oluşturulması, güvenlik gereksinimlerinin karşılanması ve düzenli aralıklarla güvenlik denetlemelerinin yapılması,

2. Uluslararası standartlara uygun bir siber güvenlik mevzuatının oluşturulması,

3. Sektör düzenleyici kurum ve kuruluşların siber güvenlik düzenleme ve denetleme farkındalıklarının ve yetkinliklerinin geliştirilmesi,

4. Kritik altyapı sektörlerinin sadece saldırganlardan değil, aynı zamanda kullanıcı hataları ve doğal afetlerden de korunması için düzenlemelerin yapılması,

5. Her kurum kendi bilgi güvenliği yönetim sürecini çalıştıracak yetkinliğe ve kapasiteye erişmesi,

6. Siber güvenlik konusunda kurum ve kuruluşların yöneticilerin farkındalık seviyelerinin artırılması,

7. Siber güvenlik alanında personel yetiştirilmesi ve bu alanda çalışmak isteyen personel, öğrenci ve araştırmacıların teşvik edilmesi,

8. Toplumun her kesimi ve seviyesinde siber güvenlik bilincinin oluşturulması, eğitim kurumlarının çalışmalarına ilaveten yazılı ve görsel medyada farkındalık çalışmalarının yapılması,

9. Kamu kurumlarında siber güvenlik uzmanı istihdam edilmesi için mevzuat desteği sağlanması ve personelin özlük haklarının iyileştirilmesi,

10. Kurumsal ve Sektörel SOME'lerin etkinliğinin arttırılması için mevzuat desteğinin sağlanması, mali düzenlemelerin yapılması, personel ihtiyacının karşılanması, bilişim altyapısının sağlanması ve bilgi paylaşımının geliştirilmesi,

11. Siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesi oluşturulması,

12. Kamu kurumları, özel sektör, STK'lar, denetleyici kurumlar, üniversiteler, geliştirici firmalar ve tüm diğer paydaşların katılım ve koordinasyonu ile ulusal siber güvenlik eko-sisteminin oluşturulması,

13. Ulusal Siber güvenlik eko-sistemi içinde danışmanlık hizmetlerinin verilmesi, açıklık, tehdit ve faydalı uygulamaların paylaşılması,

14. Kritik altyapıların kritik noktalarında kullanılan, yerli veya yabancı donanım ve yazılım ürünlerinin açıklıkların kötüye kullanılmasına engel olmak amacıyla sertifikasyon çalışmaları ve açıklık analizlerinin yapılması,

15. Güvenli yazılım geliştirme ve tedarik yönetimi kültürünün oluşturulması,

16. Siber güvenlikte dışa bağımlılığı azaltmak için AR-GE faaliyetlerine önem verilerek yerli ürünlerin geliştirilmesi,

17. Tehdit unsurlarının saldırı yapmadan önce de bertaraf edilememesi için ulusal proaktif siber savunma yeteneğinin geliştirilmesi,

18. Tehdit unsurlarının siber uzaydaki en büyük avantajı olan anonimliği ortadan kaldırmak için etkin kayıt yönetimi ve IPv6 teknolojilerinin yaygınlaştırılması.

Ulusal Siber Güvenlik Stratejik amaçlarına ulaşmak için 2016-2019 döneminde gerçekleştirilecek stratejik eylemler aşağıdaki beş stratejik eylem başlığı altında toplanmıştır (2016-2019 Ulusal Siber Güvenlik Stratejisi, 2016: 15):

1. Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması: Ulusal ekonomiyi, kritik altyapıları ve toplumu etkileyebilecek siber güvenlik risklerini azaltmaya yönelik eylemlerdir.

2. Siber Suçlarla Mücadele: Ağırlıklı olarak maddi zarara yol açan kurum, kuruluş ve bireyleri etkileyen siber güvenlik risklerini azaltmaya yönelik eylemlerdir.

3. Farkındalık ve İnsan Kaynağı Geliştirme: Kurum ve kuruluşların en üst düzey yöneticisinden kullanıcılara kadar tüm kesimler tarafından siber güvenlik kültürünün kazandırılması ve yeterli sayı ve yetkinlikte siber güvenlik uzmanı yetiştirilmesine yönelik eylemlerdir.

4. Siber Güvenlik Ekosisteminin Geliştirilmesi: Kamu, özel sektör, STK'lar, denetleyici kurumlar, üniversiteler, geliştirici firmalar ve tüm diğer paydaşların katılım ve koordinasyonu sonucu siber güvenlik ile ilgili mevzuat çalışmalarından, teknolojiye kadar gereksinimlerin belirlenmesine ve uygulamaya dökülmesine yönelik eylemlerdir

5. Siber Güvenliğin Milli Güvenliğe Entegrasyonu: Ulusal ekonomiyi, kritik altyapıları ve toplumu etkileyebilecek, milli güvenliği tehdit edebilecek, iyi organize olmuş hedef odaklı tehdit unsurları tarafından icra edilecek kasıtlı saldırıların verebileceği zararı azaltmaya yönelik eylemlerdir.

2016-2019 Ulusal Siber Güvenlik Stratejisi incelendiği zaman denetim, eğitim ve farkındalık amaçları ön planda tutulduğu görülmektedir. Siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesinin oluşturulması hususu ve siber saldırı ve tehditleri önceden bertaraf edebilmek adına ulusal proaktif siber savunma yeteneğinin geliştirilmesi Ulusal Siber Güvenlik Stratejisi amaçları arasında yer almıştır. Ayrıca siber saldırganların siber uzaydaki en büyük avantaj olarak kullandıkları anonim olma özelliğini ortadan kaldırmak için etkin kayıt yönetimi ve IPv6 teknolojilerinin ulusal siber uzay paydaşları bünyesinde yaygınlaştırılması amaçlanmıştır.

Sonuç olarak, güncel tehdit unsurları, günümüz bilgi ve iletişim teknolojilerindeki gelişimler, artan siber uzaya olan bağımlılık oranları göz önüne alınarak ve dünya ülkelerinin siber güvenlik konusunda yapmış olduğu çalışmalarının değerlendirilmesi sonucu oluşturulan 2016-2019 Ulusal Siber Güvenlik Stratejisi, Türkiye'nin ulusal güvenliğini de yakından ilgilendiren önemli bir belgesidir.

DÖRDÜNCÜ BÖLÜM

4. ÜLKELERİN SİBER GÜVENLİK GÜÇ VE KAPASİTELERİ İLE TÜRKİYE'NİN KONUMU

Birey, kurum ve kuruluşların birbiri ile ilişkilerinin siber uzayda yürütülmesini sağlayan bilgi ve iletişim teknolojileri günümüzde, toplumsal ve ekonomik gelişmenin en önemli sebebi olmakla birlikte, kamu ve özel sektörde sağladığı kolaylıklar sebebiyle de insan için vazgeçilmez bir hal almıştır. Güvenliği sağlanmış bilgi ve iletişim teknolojileri, birey, kurum, kuruluşlar ve devletler için siber uzayın ekonomik istikrarını sağlamasının yanı sıra, birey, kurum ve kuruluşların özgürce iletişim sağlaması ve faaliyetleri yürütmesi adına güvenilir bir ortam sağlamaktadır (ITU, 2015). Hayatımızın neredeyse her alanında kullanılan bilgi ve iletişim teknolojilerine olan ve günden güne artan bağımlılığımız sonucunda da siber uzay, suçlular için başarı oranının yükseldiği cazip bir suç işleme merkezi haline dönüşmüştür. Siber saldırganların siber uzay içerisinde kullandıkları siber saldırı yöntemlerinin şekli, kapsamı ve eğilimi de küçük ölçekli siber ihlal ve maddi zararlardan, büyük ölçekli organize olmuş devlet destekli ve büyük miktarda maddi zarara yol açan siber saldırılara kadar çeşitlilik göstermektedir (Narmeen ve Ashraf, 2016: 129). Ayrıca yüksek tehdit oranı ile karmaşıklığı ve niceliği günden güne artan APT'ler, yarattığı ekonomik zarar, bilgi ve iletişim teknolojileri açısından büyük bir engel ihtiva etmektedir. Kamu ve özel sektördeki yetkililerin görüşlerine göre günümüzde siber saldırılar, terör eylemlerinin sebep olduğundan daha fazla fiziksel ve ekonomik zarara sebep olmaktadır (World Economic Forum, 2013).

2007'de Rusya tarafından Estonya'nın internet altyapısına yapılan siber saldırılar, 2008'de Rusya ve Gürcistan arasındaki konvansiyonel savaşın siber savaşa dönüştüğü operasyonel siber savaş ve 2010'da İran nükleer santrallerine gerçekleştirilen siber saldırı olayı (Stuxnet), birçok ülkenin kritik altyapı sektörlerini oluşturan bilgi ve iletişim teknolojilerinin yüksek oranda siber saldırılara karşı hassas altyapılar olduklarını fark etmelerini sağlamıştır (Tatar ve diğerleri, 2014: 211). Bu siber saldırı örnekleri ile oluşan

farkındalık seviyeleri sonucu ülkeler ayrıca ulusal siber güvenlik güç ve kapasitelerini artırma çalışmalarını hızlandırmış ve özellikle siber güvenlik stratejileri ve planlarını hazırlamalarına veya güncellemelerine sebep olmuştur (Narmeen ve Ashraf, 2016: 129).

Bilginin değerinin her geçen gün arttığı içinde bulunduğumuz bilişim çağında, sürekli bir gelişim içerisinde olan bilgi ve iletişim teknolojileri ile ihtiyacımız olan bilgiye, daha hızlı ve daha kolay bir şekilde erişilebilmektedir. Enerji, haberleşme, su, tarım, sağlık, ulaşım, finans ve eğitim gibi kritik altyapı sektörlerinde de bilgi ve iletişim teknolojileri yoğun olarak kullanıldığından, bilgi ve iletişim teknolojileri ve kritik altyapı sektörlerinin güvenliğinin sağlanması hem hizmet veren kurum ve kuruluşların sağladığı hizmet ve kalitenin bekası, hem de hizmet alan bireylerin kişisel güvenliğinin sağlanması açısından çok önemlidir. Ayrıca kritik altyapı sektörlerinde meydana gelebilecek güvenlik zafiyetleri, birbirine sıkı sıkıya bağlı durumda bulunan siber uzay içerisinde, büyük ölçekte ekonomik zarara, kamu düzeninin bozulmasına, can kaybına, ulusal ve hatta uluslararası güvenliğin bozulmasına sebep olma riski taşıdığından, bilgi ve iletişim teknolojileri ile kritik altyapı sektörlerinin korunması hayati öneme haizdir (STM, 2016).

Türkiye İstatistik Kurumu (TÜİK)'nun 2013 yılında internetin çocuklar tarafından kullanılmasına yönelik yapmış olduğu araştırma sonuçlarına göre Türkiye'de bilgisayar kullanımına başlama yaşının 8, internet kullanımına başlama yaşının 9, cep telefonu kullanımına başlama yaşının ise 10 olduğu sonuçları çıkmıştır. 6-15 yaş grubunu kapsayan araştırmada çocukların %45,6'sı hemen hemen her gün internete girdiği, bu çocuklardan %84,5'inin interneti ödev yapma veya araştırma amaçlı kullandığı görülmektedir. Ayrıca TÜİK 2015 yılı verilerine göre, Türkiye'de bilgisayar kullanım oranı %54,8 iken, internet kullanım oranı ise %55,9'dur. Türkiye genelinde internete erişimi olan hanelerin oranı %69,5 iken, internet yolu ile bireylerin kişisel kullanım amacıyla mal ve hizmet siparişi verme veya satın alma oranı ise %33,1'dir. Araştırma sonucunda internetin kullanım oranı, ev ve iş yeri dışında internet kullanımı için taşınabilir cihaz kullanımı ile internetin düzenli kullanıcı sayısında önceki yıllara nazaran ciddi artışlar olduğu görülmüştür (TÜİK, 2013; TÜİK, 2015; STM, 2016). Türkiye'nin dünyanın en büyük ekonomileri olan G-20 arasında yer aldığını düşünürsek, internete bağımlılık ve kullanım oranının dünya genelinde de en az Türkiye'deki oranda artığı sonucuna ulaşabiliriz.

Yukarıda belirtilen TÜİK'in verilerinde görüldüğü üzere artan internet bağımlılığına ve gelişimine paralel olarak, aynı zamanda siber saldırı ve tehditlerin sayısı, yapılış şekli ve yöntemlerinde de değişimler ve gelişimler meydana gelmektedir. Gelişen teknoloji içerisinde siber güvenlik kavramının bu sürecin vazgeçilmez ve ayrılmaz bir parçası olduğu aşikârdır. Her ne kadar dünya genelinde siber güvenliğin önemi konusunda farkındalık seviyelerinde artış görülse de birçok ülkenin politika ve stratejilerinde siber güvenliğin sağlanması temel bir hedef olarak görülmemiştir. En kısa süre içerisinde siber güvenlik kavramının benimsenerek ülke politikalarının temel dinamiklerden biri haline getirilmesi ülkelerin daha güvenli ve sağlam temellere dayanan siber güvenlik politika ve altyapılarını geliştirmesi açısından oldukça önemlidir.

Bazı ülkelerin siber güvenlik kavramını içselleştirememesinin en temel sebepleri arasında, siber güvenlik kapasiteleri, seviyeleri ve siber güvenliğin hangi alanlarda geliştirilmeye ihtiyacı olduğu gibi konularda yeterli farkındalık seviyesine ulaşamamış olması ve bu konuda yeterli bilgiye sahip olmaması yatmaktadır.

4.1. Ülkelerin Siber Güvenlik Güç ve Kapasitelerinin Ölçülmesi

Ülkelerin herhangi bir konvansiyonel savaş veya siber savaş esnasında hasma karşı üstünlük sağlamasını sağlayacak olan husus ulusal milli güç unsurlarının toplamıdır. Özellikle milli güç unsurlarından askeri güç potansiyeli, ülkelerin iç ve dış tehditlere karşı caydırıcılık etkisi yarattığı devletin fiziki gücünü oluşturmaktadır. Günümüzde ülkelerin askeri birlikleri, kara, hava, deniz ve uzay muharebe alanları yanında siber uzay muharebe alanında da başarılı olabilmesi için siber güvenlik güç ve kapasitelerinin artırılması gerekmektedir. Siber güvenlik güç ve kapasitelerinin artırılmasını için ülkeler, siber savunma güçlerinin yanında siber saldırı güçlerini de artırmak zorundadır. Çünkü siber savaş esnasında siber savunma gücü yüksek olan ülkelerin eğer siber saldırı gücü düşük ise hasımları üzerinde yıkıcı etki bırakamayacağı ve başarı elde edemeyeceği aşikârdır. Ayrıca siber saldırı gücü düşük olan ülkeler, hasma karşı caydırıcılık sağlayamayacağından barış ve savaş şartlarında siber saldırılara hedef olma ihtimali de yüksektir.

Ülkelerin siber güvenlik güç ve kapasiteleri, ülkelerin yalnızca siber saldırı ve siber savunma güçleriyle de ölçülemez. Bunun için bilgi ve iletişim teknolojilerinin, kritik

altyapı sektörlerinin, ülke içerisindeki kurum ve kuruluşların siber uzaya ne kadar bağımlı oldukları hususunu da negatif yönde kuvvet çarpanı olarak hesaba katmak daha doğru olacaktır. Clarke ve Knake (2010: 74,75)'e göre siber savunma, bir ülkenin kendisine yapılan siber saldırıları durdurma çabası iken, siber bağımlılık ise ülkenin saldırıya açık sistemlere ve ağlara ne kadar gereksinim duyduğunun ölçüsüdür. Bir ülkenin kritik altyapı sektörleri ile kurum ve kuruluşları siber uzaya ne kadar çok bağımlı ise o ülke siber saldırılara karşı bir o kadar da savunmasızdır. Sonuçta, teknolojik olarak gelişmiş ve internete daha bağımlı olan ülkeler, siber saldırı güçleri yüksek olmasına rağmen, kritik altyapı sektörlerinde daha fazla açıklık bulunması kuvvetle muhtemel olduğundan kendisine yapılan siber saldırılardan daha fazla etkilenecek ve nihayetinde de siber güvenlik güç ve kapasitesi olumsuz etkilenecektir.

Bu bölümde, açık kaynak verilerinden ve araştırma şirketleri tarafından yapılan istatistiki çalışmaların derlenmesi sonucunda, bazı dünya ülkelerinin siber savunma, siber saldırı güçlerinin yanında bir de siber uzaya olan bağımlılıklarının da hesaba katılarak Siber Güvenlik Güç ve Kapasiteleri Sıralaması oluşturulmaya çalışılacaktır. Bu sıralamada Gayri Safi Milli Hasılası (GSMH) en yüksek ülkelerin oluşturduğu G8 ülkeleri ile son zamanlarda siber uzayda önemli yer işgal ettiğini düşündüğümüz ülkeler arasında olan Çin, Hindistan, Güney Kore, Kuzey Kore, İsrail, İran, Brezilya ve Türkiye yer alacaktır. Oluşturulacak Siber Güvenlik Güç ve Kapasiteleri Sıralaması sonucunda Türkiye'nin siber güvenlik güç ve kapasiteleri ile dünyadaki konumu belirlenmeye çalışılacak ve bu konuda Türkiye'den daha önde olan, farklı siber güvenlik stratejileri, politikaları, yaklaşımları ve tedbirleri uygulayan ülkeler hakkında ön bilgi sahibi olunacak ve bu sayede ulusal siber güvenlik farkındalık ve bilinç seviyesi yükseltilmeye çalışılacaktır.

Ülkelerin karşılaştırmalı siber güvenlik analizini yapmak adına oluşturulacak Siber Güvenlik Güç ve Kapasiteleri Sıralaması için kullanacağımız son beş yıla ait araştırma ve istatistiksel veriler ile ülkelerin siber güvenlik güç ve kapasiteleri üzerine etki alanları Tablo 7'da gösterilmiştir.

Tablo 7: Siber Güvenlik Güç ve Kapasiteleri Sıralaması için Kullanılacak Veriler ve Etki Alanları

Sıra Nu.	Araştırma ve İstatistiksel Veriler	Etki Alanları
1	Verisign Firması Tarafından 2011 yılı Ülkelerin Siber Kabiliyetlerinin Sınıflandırılması	Siber Savunma Siber Saldırı Siber Bağımlılık
2	ABI Araştırma Şirketi ile ITU işbirliği ile yürütülen proje sonucu ortaya çıkan 2014 yılı Dünya Siber Güvenlik İndeksi (GCI)	Siber Savunma Siber Saldırı Siber Bağımlılık
3	Dünyanın en büyük güvenlik teknolojisi şirketi olan McAfee tarafından sunulan 2012 yılı Siber Savunma Raporu	Siber Savunma
4	2014 Yılı için Ülkelerin Silahlı Kuvvetlerine Ayırdığı Bütçe Miktarları	Siber Savunma Siber Saldırı
5	2015 Yılı için Ülkelerin Yazılım Sanayisinin Gelişmişlik Sıralaması	Siber Saldırı
6	2013 Yılı için Siber Saldırı Trafiğinin Kaynağı Olan Ülkeler Sıralaması	Siber Saldırı
7	2015-2016 yılları için Meydana Gelen Siber Saldırıların Kaynağı Olan Ülkeler Sıralaması	Siber Saldırı
8	2015 Yılı için Ülkelerin Teknolojik Olarak Gelişmişlik Sıralaması	Siber Saldırı Siber Bağımlılık
9	2016 Yılı için Ülkelerin Nüfuslarına Göre İnternet Kullanım Oranları	Siber Bağımlılık

Verilerin hazırlanış biçimi, kapsamı, doğruluğu, geçerliliği göz önüne alındığı zaman Verisign firmasının ülkelerin siber kabiliyetlerinin sınıflandırılması ve ABI araştırma şirketi ile ITU işbirliği ile yürütülen proje sonucu ortaya çıkan GCI raporu sonuçları, Siber Güvenlik Güç ve Kapasiteleri Sıralamasını belirlerken diğer veriler sonucu elde edilen sonuca direkt olarak etki edecektir. Ayrıca bu iki çalışma, ileride yapılacak çalışmalar adına örnek teşkil etmesi açısından önem ihtiva etmektedir.

Verisign firması tarafından 2011 yılında yapılan çalışma neticesinde, ülkeler siber güvenlik güç ve kapasiteleri açısından dört seviyeye ayrılmıştır. Aşağıdaki tablolarda hangi ülkelerin hangi seviyede olduğu, seviyelerin özellikleri, kurumsal kapsamları ve kabiliyetleri belirtilmiştir.

Tablo 8: Verisign Firması Tarafından 2011 Yılı Ülkelerin Siber Kabiliyetlerinin Sınıflandırılması

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

Kaynak: Dennesen, 2011: 31.

Tablo 9: Siber Güvenlik Güç ve Kabiliyetleri Seviyelerinin Özellikleri, Kapsamı ve Kabiliyetleri

Seviye	Özellikleri	Kurumsal Kapsamı	Kabiliyetleri
1	* Siber güvenlik ve savunma mekanizmalarını geliştirme konularında uluslararası politika belirleyebilmektedir. * Siber savunma konularına büyük destek vermekte ve siber güvenlik politikaları ve siber savunma çalışmalarına fazla bütçe ve insan desteği ayırmaktadır. * Diğer ülkelerin siber güvenlik kapasitelerini artırma çabalarına itici bir güç oluşturmaktadır.	* Çok sayıda, iyi tanımlanmış ve ihtisaslaşmış askeri ve istihbarat kurum ve kuruluşlarına sahiptir.	* Geleneksel savunma alanında siber kabiliyetleri kullanabilir. * Diğer ülkelere karşı kapsamlı, sürekli, karmaşık saldırı ve savunma eylemlerini kullanabilir.
2	* Birinci seviyedeki ülkeleri yakından takip etmektedirler. Daha kısıtlı altyapı ve daha az personele sahiptir.	* Birinci grup ülkelere nazaran daha az kaynak ayırmışlardır.	* Birinci grup ülkelere nazaran daha kısıtlı sayıda ülkelere karşı kabiliyetlerini kullanabilir.

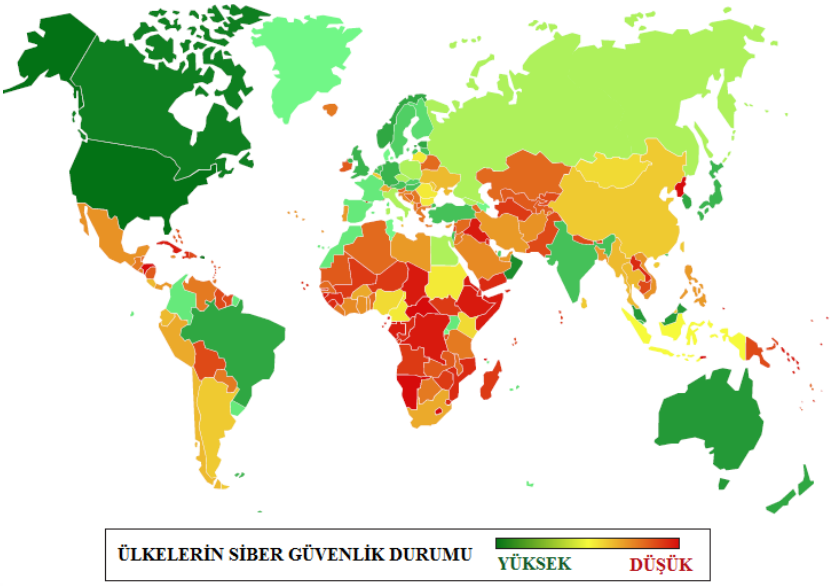
3	* Siber güvenlik ve savunma politikaları için önemli ölçüde kaynak tahsisi yapmaktadırlar. Çoğu durumda birinci seviyedeki ülkeleri taklit etmektedirler.	* Birkaç iyi tanımlanmış kurum ve kuruluşa sahip olsalar da kurumsallaşma açısından bunları geliştirme ihtiyaçları bulunmaktadır.	* Kapsamlı ve sürekli olarak siber savunma faaliyetleri yapabilirler fakat saldırıya yönelik faaliyetleri daha kısıtlıdır.
4	* Siber güvenlik ve savunma politikalarına yönelik kısıtlı kaynak tahsis etmektedirler.	* Az sayıda ve geliştirilmeye muhtaç kurum ve kuruluşlara sahiptir.	* Güçlü fakat yetersiz savunma kabiliyetleri ve kısıtlı saldırı faaliyetleri bulunmaktadır. Kendi iç kaynaklarını korumaya odaklanmış durumdadır.

Kaynak: Dennesen, 2011: 31-36.

Siber Güvenlik Güç ve Kapasiteleri Sıralamasını belirlerken sonuca direkt olarak etki edecek diğer bir araştırma ise GCI raporudur. Bu rapor, ülkelerin siber güvenlik gelişim seviyelerini, siber güvenlikle ilgili çalışmalarını, faaliyetlerini ve dünya genelindeki sıralamalarını göstermesi açısından önemlidir. Bu raporun hazırlanması için ülkelerin siber güvenlik ile ilgili hazırlanmış hukuksal mevzuatları, politikaları, ulusal stratejileri, standartları, sertifikasyon programları, BOME'lerin durumları, eğitim, farkındalık ve bilinçlendirme faaliyetleri, koordinasyon ve işbirliği çalışmaları üzerine bilgilerden yararlanılmıştır (ITU, 2015).

Raporun temel amaçları arasında, ulusal düzeyde siber güvenlik ile ilgili devlet politikalarının teşvik edilmesi, kritik altyapı sektörlerinin güvenliğinin sağlanması çabalarının sürdürülmesi, modern toplumların itici gücü haline gelen bilgi ve iletişim teknolojileri temelinde küresel siber güvenlik kültürünün oluşturulması ve idame ettirilmesi ile ülkeler nezdinde siber güvenlik farkındalık ve hazırlık seviyelerini artırmak yatmaktadır (ABI Research, 2014; ITU, 2015).

Şekil 18: Ülkelerin Siber Güvenlik Durumları Haritası



Kaynak: ABI Research, 2014; ITU, 2015.

GCI raporu, ülkelerin siber güvenlik güç ve kapasiteleri adına almış olduğu hukuki, teknik ve kurumsal önlemler ile kapasitenin gelişimi, ulusal, uluslararası işbirliği ve koordinasyon olmak üzere beş temel kategori verilerinin değerlendirilmesi sonucunda hazırlanmıştır (ABI Research, 2014; ITU, 2015).

Tablo 10: GCI Kategorileri ve Puanları

Kategori	Puan
1. Hukuki Önlemler	4
a. Ceza Hukuku ve Mevzuatı	2
b. Düzenleme ve Uyumluluk	2
2. Teknik Önlemler	6
a. BOME	2
b. Standartlar	2
c. Sertifikasyon	2
3. Kurumsal Önlemler	8
a. Politika	2
b. Hükümet Yol Haritası	2
c. Sorumlu Kuruluş Tespiti	2

d. Ulusal Değerlendirme Çalışmaları	2
4. Kapasite Artırımı	8
a. Standart Gelişimi	2
b. İşgücü Gelişimi	2
c. Uzmanlık Sertifikasyonu	2
d. Kurum Sertifikasyonu	2
5. İşbirliği ve Koordinasyon	8
a. Ülke İçi İşbirliği	2
b. Kurumlar İçi İşbirliği	2
c. Kamu ve Özel Sektör Ortaklıkları	2
d. Uluslararası İşbirliği	2

Kaynak: ABI Research, 2014; ITU, 2015.

GCI raporu, ülkelerin çeşitli alanlardaki siber güvenlik güç ve kapasitelerinin ölçülmesiyle, güvenilir bir siber güvenlik seviyesine ulaşabilmek adına gerçekleştirmeleri gereken adımların tespiti, nerelerde eksikleri oldukları ve kendi durumlarını değerlendirerek siber güvenlik güç ve kapasiteleri ile ilgili ön bilgi elde ederek yol gösterici bir rapor olma özelliği taşımaktadır (ABI Research, 2014; ITU, 2015).

Tablo 11: GCI Sıralaması

Sıra Nu.	Ülke	İndeks	Puan
1	ABD	0.824	**8,24**
2	Kanada	0.794	**7,94**
5	Brezilya	0.706	**7,06**
5	Almanya	0.706	**7,06**
5	Hindistan	0.706	**7,06**
5	Japonya	0.706	**7,06**
5	Güney Kore	0.706	**7,06**
5	İngiltere	0.706	**7,06**
6	İsrail	0.676	**6,76**
7	Türkiye	0.647	**6,47**

9	Fransa	0.588	**5,88**
10	İtalya	0.559	**5,59**
12	Rusya	0.500	**5**
14	Çin	0.441	**4,41**
19	İran	0.294	**2,94**
29	Kuzey Kore	0.000	**0**

Kaynak: ABI Research, 2014; ITU, 2015.

Bu sıralama, siber güvenlik boyutunda ülkelerin hukuksal olarak mevzuatlarında ne gibi değişiklikler ve çalışmalar yaptığı, aldığı teknik boyuttaki önlemleri, kurum ve kuruluşların hazırlık durumlarını, siber güvenlik kapasitelerinin geliştirilmesi için yaptıkları standardizasyon çalışmaları ve sertifika programları ile ulusal ve uluslararası alanda yapılan koordinasyon ve işbirliği faaliyetlerinin sonucunu göstermektedir. Başka bir ifadeyle bu sıralama, ülkelerin ulusal ve uluslararası alanda ülkelerin farkındalık seviyeleri ile yapması gerektiği çalışmaları hangi ciddiyetle ve özenle yaptığının görülmesi açısından önemlidir.

4.1.1. Ülkelerin Siber Savunma Güçleri

Ülkelerin Siber Savunma Güçleri ve Kapasitelerini belirlenirken, McAfee tarafından sunulan 2012 yılı Siber Savunma Raporundan faydalanılacaktır. Ayrıca dünya ülkelerinin silahlı kuvvetlerinin güçlendirilmesi adına ayırmış oldukları bütçelerin siber güvenlik güçleri ve kapasitelerini artırmak için ayırdıkları bütçe ile paralellik arz ettiğinden, ülke ordularının bütçelerinden de istifade edilecektir.

Tablo 12: McAfee 2012 Yılı Siber Savunma Raporu

Sıra Nu.	**Ülke**	**Puan**
1	İsrail	**10**
2	ABD, Fransa, Almanya, İngiltere	**9**
3	Kanada, Japonya	**8**
4	Çin, İtalya, Rusya, Güney Kore*	**7**

5	Brezilya, Hindistan, **Türkiye***	**6**
	İran*, Kuzey Kore*	**3**

Kaynak: McAfee, 2012. *McAfee Siber Savunma Raporunda değerlendirilmeye alınmamış ülkeler olan Güney Kore, Kuzey Kore, İran ve Türkiye'nin puanları Silahlı Kuvvetlerine Ayırdığı Bütçe Miktarlarına göre muadil ülkelerin puanları verilerek hesaplamaya dâhil edilmiştir.

Tablo 13: 2014 Yılı İçin Ülkelerin Silahlı Kuvvetlerine Ayırdığı Bütçe Miktarları

Sıra Nu.	**Ülke**	**Bütçe (Milyar $)**	**Puan***
1	ABD	612,5	**10**
2	Çin	126	**7,54**
3	Rusya	76,6	**6,76**
4	İngiltere	53,6	**6,2**
5	Japonya	49,1	**6,07**
6	Hindistan	46	**5,97**
7	Almanya	45	**5,93**
8	Fransa	43	**5,86**
9	İtalya	34	**5,49**
10	Güney Kore	33,7	**5,48**
11	Brezilya	33,142	**5,46**
12	**Türkiye**	18,185	**4,52**
13	Kanada	18	**4,5**
14	İsrail	15	**4,22**
15	Kuzey Kore	7,5	**3,14**
16	İran	6,3	**2,87**

Kaynak: Macias ve diğerleri, 2014. *Puan hesabı yapılırken, logaritmik dönüşüm yöntemi (z = log y) kullanılmış olup, verilerin 10 tabanına ($\log_{10}$ veya log diye ifade edilir) göre logaritmaları alınarak veri dönüşümleri yapılmıştır. Müteakip tüm puan hesaplamalarında da bu yöntem kullanılmıştır.

Tablo 14: Ülkelerin Siber Savunma Güçleri Sıralaması

Sıra Nu.	Ülke	Toplam Siber Savunma Gücü	Siber Savunma Gücü
1	ABD	19	**9,5**
2	İngiltere	15,2	**7,6**
3	Almanya	14,93	**7,47**
4	Fransa	14,86	**7,43**
5	Çin	14,54	**7,27**
6	İsrail	14,22	**7,11**
7	Japonya	14,07	**7,04**
8	Rusya	13,76	**6,88**
9	Kanada	12,5	**6,25**
10	İtalya	12,49	**6,25**
11	Güney Kore	12,48	**6,24**
12	Hindistan	11,97	**5,99**
13	Brezilya	11,46	**5,73**
14	**Türkiye**	10,52	**5,26**
15	Kuzey Kore	6,14	**3,07**
16	İran	5,87	**2,94**

4.1.2. Ülkelerin Siber Saldırı Güçleri

The Wall Street Journal gazetesi, açık kaynak, bilgisayar güvenliği uzmanları ve araştırmacılar yolu ile elde ettiği bilgiler neticesinde ülkelerin siber saldırı güçleri hakkında bazı sonuçlara ulaşmıştır. Bu sonuçlara göre, günümüzde 60'dan fazla ülkenin siber saldırı veya siber casusluk amacıyla kullanmak üzere siber silahlara veya bu silahları geliştirme gücüne sahip olduğu, 29 ülkenin resmi olarak askeri veya istihbarat birimlerini siber saldırı amaçlı kullandığını, 49 ülkenin kullanılmaya hazır siber saldırı yazılımları satın alarak bu saldırıları gerçekleştirdiği, 63 ülkenin ise siber silahları, ulusal veya uluslararası alanda keşif amaçlı olarak kullandığı ortaya çıkmıştır. Ayrıca ülkelerin siber silahları, keşif, tahrip etme ve yıkıma uğratma amaçlı kullandığı, siber saldırılar esnasında özel yetiştirdiği siber saldırı ekipleri, askeri birlikler veya istihbarat elemanlarından faydalandığı, siber

saldırıların devlet desteği altında veya devlet desteği olmadan yapıldığı görülmektedir (Valentino ve Yadron, 2015).

Ülkeler, küçük çaplı siber saldırı kabiliyetlerini, ekonomik kazanç elde etmek, hasım ülkenin açıklarını tespit etmek, olası siber savaşlara hazırlık yapmak gibi amaçlar için kullanırken, büyük çaplı siber saldırı kabiliyetlerini ise, siber saldırıların doğasındaki bir defa etkin kullanılabilmesi özelliği sebebiyle operasyonel siber savaş vuku bulduğu zaman uygun yer ve zamanı beklemektedir. Bu sebeple, devlet eli olmadan veya özellikle devlet eli ile yapılacak siber saldırılarda kullanılacak siber silahlar kullanılacağı ana kadar gizli tutulduğundan, ülkelerin siber saldırı güçlerini belirlemek oldukça zordur.

Ülkelerin siber saldırı güçlerinin belirlenmesi her ne kadar zor olsa da doğru veriler kullanılarak gerçeğe yakın sonuçlara ulaşmak mümkündür. Bu sebeple, siber saldırı gücü, ülkelerin teknoloji ve yazılım bakımından gelişmişlik sıralaması, siber saldırı trafiğinin kaynağı olan ülkelerin sıralaması ile silahlı kuvvetleri için ülke ekonomilerinden ayırmış oldukları bütçeler ile birlikte değerlendirilerek hesaplanacaktır.

Tablo 15: 2015 Yılı İçin Ülkelerin Yazılım Sanayisinin Gelişmişlik Sıralaması

Sıra Nu.	**Ülke**	**İndeks (Milyar $)**	**Puan***
1	ABD	160	**10**
2	İngiltere	31	**6,77**
3	Almanya	30	**6,7**
4	Çin	27	**6,49**
5	Fransa	22	**6,09**
6	Japonya	17	**5,58**
7	İtalya	14	**5,2**
8	Kanada	12	**4,9**
9	Hindistan	5	**3,17**
10	Brezilya, Güney Kore	4	**2,73**
11	İsrail, Rusya, Türkiye	1	**0,19**
12	İran, Kuzey Kore	<1	**0,02**

Kaynak: Ortner, 2015.

Tablo 16: 2015 Yılı İçin Ülkelerin Teknolojik Olarak Gelişmişlik Sıralaması

Sıra Nu.	**Ülke**	**Puan**
1	Japonya	**10**
2	ABD	**9**
3	Güney Kore	**8**
4	İsrail	**7**
5	Almanya	**7**
6	Rusya	**7**
8	İngiltere	**7**
9	Kanada	**6**
12	Çin	**6**
	Fransa*****	**5**
	İtalya*****	**4**
	Hindistan*, Brezilya*	3
	Türkiye*	**2,5**
	İran*****, Kuzey Kore*****	**1**

Kaynak: Richest Lifestyle, 2015. *****Fransa, Hindistan, İtalya, Brezilya, Türkiye, İran ve Kuzey Kore, Richest Lifestyle tarafından değerlendirmeye alınmadığından, bu ülkelerin sıralamadaki yerleri Çin'den sonra gelecek şekilde, yazılım sanayilerinin gelişmişlik durumuna göre belirlenmiştir.

ThreatCloud'un 1 ay süreli verilerine ve İngiltere bankacılık sektöründe önde gelen ticaret ortaklığı olan BBA'ya göre meydana gelen siber saldırıların kaynağı olan ülkeler sıralaması çıkarılmıştır. Listelerin farklılığını gidermek adına Tablo 17'de ülkelere verilen ek puanları Tablo 18'deki puanlara ilave ederek siber saldırı trafiğinin kaynağı olan ülkelerin nihai tablosu oluşturulmuştur. Siber saldırı trafiği ile ilgili toplanan veriler konusunda gözden kaçırılmaması gereken nokta, saldırı kaynağı olarak görülen ülkenin gerçekte saldırıyı yapan ülke olmaması durumudur. İstatistiksel verilerin içerisinde, özellikle köle bilgisayarlar kullanılarak yapılan siber saldırılarda, gerçekte saldırıyı yapan bilgisayar olmamasına rağmen saldırıyı yapanmış gibi hesaplamaya dâhil olduğu durumlar bulunmaktadır.

Tablo 17: 2015-2016 Yılları İçin Meydana Gelen Siber Saldırıların Kaynağı Olan Ülkeler Sıralaması

Sıra Nu.	ThreatCloud'e Göre	Ek Puan	BBA'ya Göre	Ek Puan
1	Rusya	5	ABD	5
2	Çin	4	Çin	4
3	Brezilya	3	Almanya	3
4	Güney Kore	2	Rusya	2
5	ABD	1	Japonya	1

Ülke	Toplam Ek Puan	Eklenecek Ek Puan
Çin	8	**4**
Rusya	7	**3,5**
ABD	6	**3**
Brezilya, Almanya	3	**1,5**
Güney Kore	2	**1**

Kaynak: Cybercrime Top 10 countries where attacks originate, 2015, https://www.bba.org.uk/wp-content/uploads/2015/02/red24+Cybercrime+Top+10+countries+where+attacks+originate+-++2015.pdf; ThreatCloud, 2016.

Tablo 18: 2013 Yılı İçin Siber Saldırı Trafiğinin Kaynağı Olan Ülkeler Sıralaması

Sıra Nu.	Ülke	Yüzde	Puan	Ek Puanlarla Birlikte	Nihai Puan
1	Çin	41	10	14	**10**
2	ABD	10	8	11	**7.85**
3	**Türkiye**	4.7	6	6	**4.28**
4	Rusya	4.3	6	9.5	**6.78**
6	Brezilya	3.3	5	6.5	**4.64**
8	Hindistan	2.3	4	4	**2.85**
9	İtalya	1.6	3	3	**2.14**
	Almanya		2	3.5	**2.5**

	Güney Kore		2	3	**2.14**
	Japonya		2	2.5	**1.79**
	Diğer Ülkeler		2	2	**1.43**

Kaynak: GovTech, 2013.

Cambridge ve Massachusetts üniversitelerinin bulut altyapı sağlayıcısı Akamai firması tarafından 2012 yılının son çeyreğinde sunulan dünya siber saldırı trafiği raporuna göre dünyada meydana gelen siber saldırı trafiğinin ülkelere göre dağılımı çıkarılmıştır. Buna göre Çin ve ABD dünya siber saldırı trafiğinin yarısını oluşturmaktadır (GovTech, 2013). 2014 yılının son çeyreğinde bazı istatistiksel çalışmalar neticesinde ise siber saldırıların kaynağı olan ülkeler sırasıyla Çin, ABD, Rusya ve Türkiye olmuştur (Juzenaite, 2015).

Tablo 19: Ülkelerin Siber Saldırı Güçleri Sıralaması

Sıra Nu.	**Ülke**	**Toplam Siber Saldırı Gücü**	**Siber Saldırı Gücü**
1	ABD	26,85	**8,95**
2	Çin	22,49	**7,5**
3	Japonya	17,37	**5,79**
4	Almanya	16,2	**5,4**
5	Rusya	13,97	**4,66**
6	İngiltere	13,77	**4,59**
7	Güney Kore	12,87	**4,29**
8	Fransa	12,52	**4,17**
9	Kanada	12,33	**4,11**
10	İtalya	11,34	**3,78**
11	Brezilya	10,37	**3,46**
12	Hindistan	9,02	**3**
13	İsrail	8,62	**2,87**
14	**Türkiye**	6,97	**2,32**
15	İran	2,45	**0,82**
16	Kuzey Kore	2,45	**0,82**

4.1.3. Ülkelerin Siber Uzaya Bağımlılık Güçleri

Günümüzde bilgi ve iletişim teknolojileri ile kritik altyapı sektörleri, küresel bir ağ ortamı olan internete bağımlı olduklarından, siber uzayın en önemli aktörü olan internetin, ülkelerin bekası açısından mutlaka emniyetinin alınması gerekmektedir. İnternetin sahip olduğu bu özel durum sebebiyle siber uzay, siber saldırganların saldırıları için kullandığı ve bilfiil yer işgal ettikleri cazip bir ortam haline gelmiştir. İlerleyen zamanlarda ülkelerin internete ve siber uzaya daha fazla bağımlı hale geleceğini düşünürsek, bu konunun önemini artırarak koruyacağı aşikârdır.

Bir ülkenin internete çıkış hizmetini sekteye uğratma, e-devlet uygulamalarını işlemez hale getirme, ülkelerin en üst düzey DNS sunucularını, merkezi yönlendirici cihazlarını ele geçirme, ulaşım, enerji, finans, haberleşme, kamu hizmetleri gibi kritik altyapı sektörlerinin çalışmalarını engelleme gibi siber saldırı faaliyetleri ABD, İngiltere ve Japonya gibi siber uzaya bağımlı ülkelerde daha kolay yapılabilmektedir. Kuzey Kore, İran ve Çin gibi herhangi bir siber tehdit vuku bulduğunda ulusal siber uzaylarını dış siber uzaydan koparabilen veya siber uzaya daha az bağımlı olan ülkeler üzerinde ise siber saldırılar daha zor yapılabilmektedir. Bu siber saldırılar yapılsa dahi bu ülkelerin siber uzaya bağımlılıkları az olduğundan saldırılardan diğer ülkelere nazaran daha az etkilenecektir.

Ülkelerin siber uzaya bağımlılık güçleri tespit edilirken, ülkelerin teknolojik gelişmişlik durumları ile ülke içerisinde nüfusa göre interneti kullanım oranları değerlendirmeye tabi tutulmuştur. Değerlendirme esnasında teknolojik gelişmişlik ve internet kullanım oranlarının, ülkelerin siber uzaya bağımlılık güç ve kapasitelerini negatif yönde etkilediği düşünülerek nihai puanlar hesaplanmıştır.

Tablo 20: 2016 Yılı İçin Ülkelerin Nüfuslarına Göre İnternet Kullanım Oranları

Sıra Nu.	Ülke	Oran (%)	Puan	Nihai Puan
1	İngiltere	92,6	9,3	**0,7**
2	Japonya	91,1	9,1	**0,9**
3	ABD, Kanada	88,5	8,9	**1,1**

4	Almanya	88	8,8	**1,2**
5	Fransa	86,4	8,6	**1,4**
6	Güney Kore	85,7	8,6	**1,4**
7	İsrail	72,5	7,3	**2,7**
8	Rusya	71,3	7,1	**2,9**
9	Brezilya	66,4	6,6	**3,4**
10	İtalya	65,6	6,6	**3,4**
11	**Türkiye**	58	5,8	**4,2**
12	Çin	52,2	5,2	**4,8**
13	İran	48,9	4,9	**5,1**
14	Hindistan	34,8	3,5	**6,5**
15	Kuzey Kore	= 0	0	**10**

Kaynak: InternetLiveStats, 2016.

Tablo 21: Ülkelerin Teknolojik Olarak Gelişmişlik Durumlarının Siber Uzaya Bağımlılık Sıralamasına Yansıması

Sıra Nu.	**Ülke**	**Puan**	**Nihai Puan**
1	Japonya	10	**0**
2	ABD	9	**1**
3	Güney Kore	8	**2**
4	İsrail, Almanya, Rusya, İngiltere	7	**3**
5	Kanada, Çin	6	**4**
6	Fransa	5	**5**
7	İtalya	4	**6**
8	Hindistan	3,5	**6,5**
9	Brezilya	3	**7**
10	**Türkiye**	2,5	**7,5**
11	İran, Kuzey Kore	1	**9**

Kaynak: Richest Lifestyle, 2015.

Tablo 22: Ülkelerin Siber Uzaya Bağımlılık Güçleri Sıralaması

Sıra Nu.	Ülke	Toplam Siber Uzaya Bağımlılık Gücü	Siber Uzaya Bağımlılık Gücü
1	Kuzey Kore	19	**9,5**
2	İran	14,1	**7,05**
3	Hindistan	13	**6,5**
4	**Türkiye**	11,7	**5,85**
5	Brezilya	10,4	**5,2**
6	İtalya	9,4	**4,7**
7	Çin	8,8	**4,4**
8	Fransa	6,4	**3,2**
9	Rusya	5,9	**2,95**
10	İsrail	5,7	**2,85**
11	Kanada	5,1	**2,55**
12	Almanya	4,2	**2,1**
13	Güney Kore	3,4	**1,7**
14	ABD	2,2	**1,1**
15	İngiltere	1	**0,5**
16	Japonya	0,9	**0,45**

Tablo 22'yi incelersek, İngiltere, Japonya ve ABD siber uzaya bağımlı ülke konumunda olmaları sebebiyle siber uzaya bağımlılık güçleri düşük iken, İran özellikle de Kuzey Kore internete bağımlılık oranları düşük olması veya dış siber uzaydan ulusal siber uzaylarını koparabildiklerinden siber uzaya bağımlılık güçleri diğer ülkelere nazaran daha yüksektir.

4.1.4. Ülkelerin Siber Güvenlik Güç ve Kapasiteleri

Tablo 23'de şu ana kadar hesaplamış olduğumuz, ülkelerin siber savunma, siber saldırı ve siber bağımlılık güçleri sonucunda, ülkelerin siber güvenlik güçleri bulunmuştur.

Tablo 23: Ülkelerin Siber Güvenlik Güçleri Sıralaması

Sıra Nu.	Ülke	Siber Savunma	Siber Saldırı	Siber Uzaya Bağımlılık	Toplam Siber Güvenlik Güçleri	Siber Güvenlik Güçleri
1	ABD	9,5	8,95	1,1	19,55	**6,52**
2	Çin	7,27	7,5	4,4	19,17	**6,39**
3	Hindistan	5,99	3	6,5	15,49	**5,16**
4	Almanya	7,47	5,4	2,1	14,97	**4,99**
5	Fransa	7,43	4,17	3,2	14,8	**4,93**
6	İtalya	6,25	3,78	4,7	14,73	**4,91**
7	Rusya	6,88	4,66	2,95	14,49	**4,83**
8	Brezilya	5,73	3,46	5,2	14,39	**4,8**
9	Türkiye	5,26	2,32	5,85	13,43	**4,48**
10	Kuzey Kore	3,07	0,82	9,5	13,39	**4,46**
11	Japonya	7,04	5,79	0,45	13,28	**4,43**
12	Kanada	6,25	4,11	2,55	12,91	**4,3**
13	İsrail	7,11	2,87	2,85	12,83	**4,28**
14	İngiltere	7,6	4,59	0,5	12,69	**4,23**
15	Güney Kore	6,24	4,29	1,7	12,23	**4,08**
16	İran	2,94	0,82	7,05	10,81	**3,6**

Tablo 24: Verisign Firması Seviyelere Göre Hesaplanmış Ülkelerin Puanları

Seviye	Ülke	Puan*
1	ABD, Çin, Rusya	**6,04**
2	Fransa, İngiltere, İsrail	**4,94**
3	Hindistan, Güney Kore, Kuzey Kore, Almanya, Türkiye	**4,6**
4	Brezilya, Kanada, İtalya, Japonya, İran	**4,1**

Kaynak: Dennesen, 2011: 31. * Puan hesabı yapılırken Tablo 23'de hesaplanan ortalama siber güvenlik gücü değerlerinden istifade edilmiştir. Birinci seviye ülkelerin puanları hesaplanırken ilk üç sırada bulunan ülkelerin siber güvenlik güçleri ortalaması,

ikinci seviye ülkelerin puanları hesaplanırken dört, beş ve altıncı sıradaki ülkelerin siber güvenlik güçleri ortalaması, üçüncü seviye ülkelerin puanları hesaplanırken yedi ile on birinci sıra dâhil ülkelerin siber güvenlik güçleri ortalaması, dördüncü seviye ülkelerin puanları hesaplanırken ise on iki ile on altıncı sıra dâhil ülkelerin siber güvenlik güçleri ortalaması kullanılmıştır.

Tablo 25: Ülkelerin Siber Güvenlik Güç ve Kapasiteleri Sıralaması

Sıra Nu.	Ülke	Ortalama Siber Güvenlik Gücü	Verisign Firması Verileri	GCI Raporu Verileri	Toplam Siber Güvenlik Güç ve Kapasiteleri	Siber Güvenlik Güç ve Kapasiteleri
1	ABD	6,52	6,04	8,24	20,8	**6,93**
2	Çin	6,39	6,04	4,41	16,84	**5,61**
3	Hindistan	5,16	4,6	7,06	16,82	**5,60**
4	Almanya	4,99	4,6	7,06	16,65	**5,55**
5	Kanada	4,3	4,1	7,94	16,34	**5,45**
6	İngiltere	4,23	4,94	7,06	16,23	**5,41**
7	İsrail	4,28	4,94	6,76	15,98	**5,33**
8	Brezilya	4,8	4,1	7,06	15,96	**5,32**
9	Rusya	4,83	6,04	5	15,87	**5,29**
10	Fransa	4,93	4,94	5,88	15,75	**5,25**
11	Güney Kore	4,08	4,6	7,06	15,74	**5,25**
12	Japonya	4,43	4,1	7,06	15,59	**5,2**
13	**Türkiye**	**4,48**	**4,6**	**6,47**	**15,55**	**5,18**
14	İtalya	4,91	4,1	5,59	14,6	**4,87**
15	İran	3,6	4,1	2,94	10,64	**3,55**
16	Kuzey Kore	4,46	4,6	0	9,06	**3,02**

Tablo 25 ise, şu ana kadar kullanmış olduğumuz 9 adet araştırma ve istatistiksel verinin sonucunda, belirlemiş olduğumuz 16 ülkenin, nihai olarak Siber Güvenlik Güç ve Kapasiteleri Sıralamasını göstermektedir.

4.2. Türkiye'nin Siber Güvenlik Güç ve Kapasiteleri Açısından Konumunun Değerlendirilmesi

Türkiye'nin siber güvenlik güç ve kapasiteleri bakımından dünya ülkeleri arasındaki yeri hiç de küçümsenebilecek yerde olamamakla birlikte, iyi konumda olduğu değerlendirilmektedir. Yapmış olduğumuz çalışmanın Türkiye'nin dünya ülkeleri arasındaki konumunu göstermesi açısından gerekli farkındalığı oluşturacağını değerlendirmekteyiz. Burada önemli olan husus, Türkiye'nin daha da ön sıralarda kendine yer bulabilmesi için gerekli çalışmalara kararlılıkla devam etmesi gerektiğidir.

Ülkelerin Siber Güvenlik Güç ve Kapasiteleri Sıralamasını oluştururken sıralamayı direkt olarak etkileyen GCI raporu, ülkelerin siber güvenlik ile ilgili almış oldukları hukuki, teknik ve kurumsal önlemlerin seviyeleri, siber güvenlik kapasitelerini artırma çalışmalarının durumları ile siber olay vuku bulduğu zaman işbirliği ve koordinasyon içerisinde olma durumlarını göstermesi açısından önem ihtiva etmektedir. Siber Güvenlik İndeksi raporunda Türkiye'nin son zamanlarda yapmış olduğu önemli çalışmalar yer almadığı için hukuksal mevzuat çalışmaları konusunda önde gelen Avrupa ülkelerinin gerisinde olduğu görülmektedir. Fakat hukuksal çalışmalar dışında diğer siber güvenlik güç ve kapasite kıstasları açısından değerlendirildiğinde Türkiye'nin, önde gelen Avrupa ülkeleri ortalamasının üzerinde olduğu görülmektedir (Tablo 26).

Tablo 26: Önde Gelen Avrupa Ülkeleri İçin Siber Güvenlik İndeks ve Sıralaması

Avrupa Ülkeleri	Hukuki Önlemler	Teknik Önlemler	Kurumsal Önlemler	Kapasite Gelişimi	İşbirliği ve Koordinasyon	İndeks	Bölgesel Sıralama
Norveç	1.0000	0.6667	0.7500	0.8750	0.5000	0.7353	1
Estonya	1.0000	0.6667	1.0000	0.5000	0.5000	0.7059	2
Almanya	1.0000	1.0000	0.6250	0.6250	0.5000	0.7059	2
İngiltere	1.0000	0.6667	0.7500	0.7500	0.5000	0.7059	2
Avusturya	1.0000	0.3333	0.8750	0.7500	0.5000	0.6765	3
Macaristan	1.0000	0.6667	0.7500	0.6250	0.5000	0.6765	3
İsrail	1.0000	0.6667	0.6250	0.7500	0.5000	0.6765	3
Hollanda	0.7500	0.5000	0.8750	0.6250	0.6250	0.6765	3
Litvanya	1.0000	0.6667	0.7500	0.5000	0.5000	0.6471	4
İsveç	0.7500	0.6667	0.6250	0.6250	0.6250	0.6471	4

Türkiye	**0.5000**	**0.6667**	**0.7500**	**0.7500**	**0.5000**	**0.6471**	**4**
Finlandiya	0.5000	0.6667	0.8750	0.5000	0.5000	0.6176	5
Slovakya	1.0000	0.6667	0.8750	0.2500	0.5000	0.6176	5
Danimarka	1.0000	0.6667	0.5000	0.5000	0.5000	0.5882	6
Fransa	1.0000	0.1667	0.5000	0.7500	0.6250	0.5882	6
İspanya	1.0000	0.6667	0.6250	0.6250	0.2500	0.5882	6
İtalya	0.7500	0.3333	0.6250	0.6250	0.5000	0.5588	7
Polonya	1.0000	0.3333	0.6250	0.6250	0.2500	0.5294	8
Çek Cumhuriyeti	0.7500	0.6667	0.6250	0.3750	0.2500	0.5000	9
Lüksemburg	0.7500	0.3333	0.5000	0.3750	0.5000	0.4706	10
ORTALAMA	**0.8875**	**0.58335**	**0.7063**	**0.6000**	**0.4813**	**0.6248**	

Kaynak: ABI Research, 2014; ITU, 2015.

Türkiye'de, GCI raporunu direkt olarak etkileyebileceğini düşündüğümüz çalışmalardan en başta geleni şüphesiz, 2016 Nisan ayı içerisinde açıklanan 2016-2019 Ulusal Siber Güvenlik Stratejisidir. Bu Strateji belgesi, 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planının, gelişen bilgi ve iletişim teknolojileri paralelinde artan güvenlik gereksinimleri ve dünya ülkelerinden başarılı örnekler çerçevesinde tekrardan güncelleyerek yeni şartlara uyarlanmasını sağlamıştır.

Türkiye'nin siber güvenlik ile ilgili yapmış olduğu diğer önemli bir çalışma ise internet ve bilgisayar ağları aracılığıyla işlenen suçlara yönelik uluslararası bağlayıcılığı olan ilk ve tek anlaşma niteliği taşıyan Sanal Ortamda İşlenen Suçlar Sözleşmesidir. Budapeşte Sözleşmesi olarak da bilinen bu sözleşme 1 Ocak 2015 tarihinde yürürlüğe girdiği için GCI raporu kapsamında değerlendirilememiştir. Ayrıca önem ihtiva eden Kişisel Verilerin Korunması Kanunu da 24 Mart 2016 tarihinde TBMM tarafından onaylanarak, yürürlüğe girmiştir (Kişisel Verilerin Korunması Kanunu, 2016: 6698).

Son zamanlarda Türkiye'nin, siber güvenlik güç ve kapasitesini artırmaya yönelik yapmış olduğu ulusal ve uluslararası hukuksal çalışmalar neticesinde, siber güvenlik konusunda önde gelen Avrupa ülkeleri ortalamasının üzerinde bir hukuksal önlemler seviyesine ulaşmış olduğu değerlendirilmektedir. Bunlara ilaveten 2016-2019 Ulusal Siber Güvenlik Stratejisi ile de teknik, kurumsal önlemler ve siber güvenlik kapasitelerinin

seviyeleri ile işbirliği ve koordinasyon bakımından önemli artışlar görüleceği aşikârdır. Sonuç olarak Türkiye, yapmış olduğu bu çalışmalar ile GCI raporunun dolayısıyla da bizim oluşturduğumuz Siber Güvenlik Güç ve Kapasiteleri Sıralamasının daha ön sıralarında olmayı hak eden bir konumdadır.

SONUÇ

Bilgi ve iletişim teknolojilerinin günümüzde geldiği nokta itibariyle ve internetin her alanda hayatımızın vazgeçilmez bir unsuru olarak yer alması sonucu artan internet bağımlılığı, yeni güvenlik sorunlarının doğmasına sebep olmuştur. Küreselleşme ile birlikte ülkeler arası sınırların ortadan kalkması, kara, hava, deniz ve uzayın yanında siber uzayı da kapsayacak şekilde çok boyutlu güvenlik anlayışının benimsenmesine yol açmıştır. Çok hızlı bir şekilde gelişen ve değişen dünyada, ülkeler, gelişimleri çok yakından takip ederek, analiz etmeli, ulusal güvenlikleri için doğru strateji ve politikaları izlemelidirler.

Günümüzde devletler, güvenliklerini sağlamanın yolunun ulusal siber uzaylarının güvenliğini sağlamaktan geçtiğinin farkındadırlar. Devletlerin milli güç unsurlarının içerisine siber güvenlik güç ve kapasitelerinin de dâhil edilmesi gerekmektedir. Bu sebeplerden dolayı dünya orduları da hareket kabiliyetlerini siber uzaya taşıyabilmek için siber ordular kurma çabaları içerisine girmişlerdir. Bu bağlamda, ülkelerin envanterinde yer alan konvansiyonel silahların yanında artık siber silahlar da savaş alanındaki yerini almıştır.

Siber uzayın kilit rolünü üstlenen internet, içinde bulunduğumuz bilişim çağının vazgeçilmez unsuru olan bilginin çok rahat ve hızlı bir şekilde paylaşılmasını sağlamaktadır. Fakat zaman içerisinde anonimleşen bilgi de daha büyük sorunları beraberinde getirmiştir. Kritik önemi haiz bir bilginin başkalarının eline geçmesinin engellenmesi, gizliliği, bütünlüğü ve erişilebilirliğinin sağlanabilmesi önemli bir konudur. Devletler için de bu konu ulusal güvenliklerinin sağlanması bakımından çok önemlidir. Bilginin kaynaktan hedefe giderken geçtiği sayısal ortam olarak bilinen siber uzayın emniyetinin ve güvenliğinin sağlanması siber güvenliğin sağlanmasının kritik rolünü oluşturmaktadır.

İçinde bulunduğumuz bilişim çağında, bireyler, kamu ve özel sektör kurum ve kuruluşları ile devletlerin sahip oldukları bilginin korunması bir zorunluluk haline gelmiştir. Ayrıca ülkeler için hayati öneme haiz kritik altyapı sektörlerinin güvenliği ülkelerin bekaları için çok önemlidir. Siber uzayı kötüye kullanmaya çalışan aktörler, kritik altyapı sektörlerini çalışamaz hale getirerek, can ve mal kaybına sebep olabilecekleri ve hizmetleri bir süreliğine sekteye uğratabilecekleri, yaşanmış siber saldırı örneklerinde görülmektedir. Kritik altyapı sektörlerine yapılan siber saldırılar neticesinde, nükleer santrallerde fiziksel tahribat yaratarak radyasyon sızıntısına sebep olabileceği, bankacılık ve finans sektörünün işlemez hale getirilebileceği, doğal gaz ve petrol boru hatlarının patlatılabileceği, enerji santrallerinin ve iletişim ağının devre dışı bırakılabileceği, uyduların bile yörüngelerinden çıkartılabileceği düşünüldüğünde, siber uzay güvenliğinin ulusal ve uluslararası alanda ne kadar önemli bir konu olduğu ortadadır.

Siber uzayın sunduğu sınırsız hareket kabiliyeti, internetin merkezi kontrolden uzak olması, anonim olma özelliği ve medyanın yoğun ilgisi sebepleriyle siber uzay, terör faaliyetleri için de cazibe merkezi haline gelmiştir. Bunun sonucunda siber terörizm, çağımızın yeni terör saldırısı şekline dönüşmüştür. Terörün tanımının tam olarak yapılamadığı ve terör noktasında fikir birliği oluşturamayan uluslararası alan, siber terörizm konusunda da ortak bir akıl ortaya koyamamıştır. Bir an önce, uluslararası alan içerisinde bu kavramların tanımlarının yapılarak, topyekûn terörün her şekli ile mücadele edilmesi, başarıya giden kilit yoldur.

Siber uzayın güvenliğinin sağlanması konusunda başarıya ulaşılabilmesi için, özellikle kritik altyapı sektörlerini internete bağlayan cihaz ve sistemlerde, yüzde yüz milli ürünlerin, başta işletim sistemleri olmak üzere, güvenlik duvarları, antivirüs programları kullanılması gerekmektedir. Milli üretim yazılım veya donanım ürünlerimiz olmadığı müddetçe siber uzayda başarılı olmamız mümkün değildir. Çünkü yurt dışı menşeli yazılım veya donanımlar, içerisine önceden yerleştirilmiş olan arka kapılar ve zararlı yazılımlar sebebiyle siber saldırıların açık bir hedefi haline gelmektedirler. Milli üretim yazılım ve donanımlarına sahip olabilmek adına çeşitli kurum ve kuruluşlar ile üniversiteler nezdinde AR-GE faaliyetleri yürütülerek bu alanda önemli adımlar atılmalıdır.

Bilgi ve iletişim teknolojileri çok büyük bir hızla geliştiği için, siber güvenlik stratejileri ve eylem planlarının şekillendirilmesinde bu gelişimi göz önünde bulundurmak bir zorunluluk haline gelmiştir. Özellikle ulusal ve uluslararası yasal mevzuatlara dayanan siber güvenlik anlayışına sahip olmak, mücadelenin başarısı için çok önemlidir. Bilindiği üzere, hukuksal bir düzenlemenin olmadığı zaman, ihlal ve suça doğal olarak zemin hazırlanmaktadır. Siber saldırıların kaynağını belirlemenin neredeyse imkânsız olduğu, saldırıların asimetrik olduğu ve sınırlardan bağımsızlığı uluslararası bir yapının ve yasaların olmasını zorunlu kılmaktadır. Çünkü siber uzayın doğası gereği bireysel olarak, bir ülkeye çok büyük maddi zararlar vermek mümkün olabilmektedir.

Şu ana kadar, siber savaş esnasındaki hukuk kurallarını düzenleyen, hiçbir bağlayıcılığı olmayan Tallinn El Kitabı dışında herhangi bir uluslararası çalışma mevcut değildir. 2016 yılının ikinci yarısında yayınlanması beklenen Tallinn El Kitabı'nın ikinci versiyonu, barış döneminde de devletlere siber uzay içerisinde uluslararası hukuk kurallarını nasıl uygulayacağını ve siber saldırılar ile nasıl mücadele edilmesi gerektiği ile ilgili referans kaynak niteliği taşıyacaktır. Bu El Kitabının da hiçbir bağlayıcılığı olmadığından caydırıcılık özelliği taşımayacak, siber saldırıların kontrol edilmesini ve önlenmesini sağlamayacaktır. Bu bakımdan, bir an önce barış ve savaş dönemlerini de kapsayan, siber saldırıların ve siber savaşın tam olarak ne zaman başladığı, devletlerin siber uzaydaki egemenliklerinin nereden başlayacağı, siber uzayda meydana gelen siber olayın ne zaman uluslararası bir sorun haline dönüşeceği, kişilerin siber uzayda nasıl ve kim tarafından temsil edileceği gibi sorulara cevap bulan, siber uzay içerisinde uluslararası hukuk kurallarını düzenleyen uluslararası bağlayıcılığı olan bir belgenin ortaya çıkarılması çok önemlidir. Fakat bütün bu soruların uluslararası alanda ortak bir irade altında cevaplanmasının çok zor olduğunu da vurgulamak gerekmektedir.

Vuku bulan siber saldırıların kim veya kimler tarafından yapıldığı ve çıkış noktası çoğu zaman tam olarak tespit edilememektedir. Bu sebeple, kurumsal ve sektörel SOME'ler ile ulusal ve uluslararası paydaşlar arasındaki uyarı, bilgilendirme, işbirliği ve koordinasyon faaliyetlerinin en kısa sürede USOM tarafından toplanması siber saldırılara karşı başarının ölçüsüdür. Reaksiyon süresinin kısa olması, kurum ve kuruluşlar arası işbirliği ve koordinasyonun eksiksiz yapılması, ulusal siber güvenliğin sağlanabilmesi açısından çok önemlidir.

Kamu ve özel sektör kurum ve kuruluşları, hizmetlerini genellikle kendi iç ağlarını oluşturarak gerçekleştirmekte ve herkesin kullanımına açık olan internet üzerinden gelebilecek siber saldırılardan kendilerini korumaktadırlar. İnternete bağlantısı bulunan e-devlet kapsamında yürütülen hizmetler, kamu hizmetleri kritik altyapı sektörünü, internet bankacılığı hizmetleri ise finans ve bankacılık kritik altyapı sektörünü tehdit etmektedir. Bilindiği üzere, siber saldırganlar, sistemler üzerindeki güvenlik açıklarından faydalanarak kritik bilgilere ulaşabilmekte ve hizmetleri sekteye uğratabilmektedir. Bu nedenle özellikle kamu sektörü hizmetleri mümkün olduğu kadar internete bağlı olmayan ağlar üzerinden yapılmalıdır.

Kurumların en üst düzey yöneticilerinden en alt seviyede çalışanına kadar bilmesi gereken prensibi ışığında siber güvenlik konuları ile ilgili bilinçlendirme ve farkındalık çalışmaları yapılmalıdır. Kurum ve kuruluşlarda en büyük tehdidin bilinçsiz kullanıcılar olduğu gerçeğiyle, eğitimli ve nitelikli personelin kilit role sahip olduğu düşüncesi akıllardan çıkarılmamalıdır. İlk, orta, lise öğretimi, üniversite ve yaygın eğitimde siber güvenlik eğitimleri verilmeli, üniversitelerde lisansüstü programlar yaygınlaştırılmalı ve bu konuda akademisyen yetiştirilmelidir. Özellikle kritik altyapı sektörlerinin işletmenlerinin eğitimine önem verilmeli, kurum ve kuruluşlarda yeteri kadar kadrolu siber güvenlik uzmanları iskân edilmeli ve bu doğrultuda yeterli maddi kaynak tahsisi yapılmalıdır.

Çalışmamızda, siber güvenlikle ilgili Türkiye adına örnek teşkil ettiğini düşündüğümüz devletler ve uluslararası örgütlerin hâlihazırdaki durumları, yapmış oldukları çalışmalar, tatbikatlar, siber güvenlik strateji belgeleri, eylem planları incelenmiş, bu sayede ulusal siber güvenlik bilinç ve farkındalık seviyelerinde artış olması amaçlanmıştır. Türkiye'nin siber güvenlik stratejileri, eylem planları, kurum ve kuruluşların çalışmalarının son durumu hakkında bilgi verilmesini müteakip, açık kaynak verilerinden ve araştırma şirketleri tarafından yapılan istatistiki çalışmaların derlenmesi sonucunda, bazı dünya ülkelerinin Siber Güvenlik Güç ve Kapasiteleri Sıralaması oluşturulmuştur. Bu sayede, Türkiye'nin siber güvenlik güç ve kapasiteleri ile dünyadaki konumu belirlenmiş olup, ileride yapılacak akademik çalışmalar veya araştırmalara zemin hazırlanmıştır.

Siber Siber Güvenlik Güç ve Kapasiteleri Sıralaması yapılırken ülkelerin siber savunma, siber saldırı ve siber uzaya bağımlılık güçleri birlikte değerlendirilmiştir. Teknolojik olarak daha gelişmiş ve e-devlet, e-finans, e-ticaret gibi alanlara daha bağımlı olan ülkelerin kritik altyapı sektörlerinde güvenlik açıklıkları kuvvetle muhtemel daha fazla olacağından siber saldırılara daha çok maruz kaldığı görülmüştür. Estonya örneğinde görüldüğü üzere, gerekli altyapıyı hazırlamadan ve gerekli güvenlik açıklıklarını kaldırmadan ülkelerin kritik altyapılarını internete bağımlı hale getirmeleri siber saldırılar neticesinde çok büyük zararlara sebep olacaktır. Ülkeler, siber güvenlik güç ve kapasitelerini artırmak adına attığı tüm adımlarda siber savunma, siber saldırı ve siber uzaya bağımlılık kavramlarını birlikte düşünerek hareket etmelidir.

Ayrıca geleceğin savaşlarının siber savaş şeklinde olacağı ve bilgiyi zamanından önce elde ederek, onu kontrol edenin üstünlük sağlayacağını bilerek, başta teknoloji ve yazılım sanayi olmak üzere, siber savunmanın yanında siber saldırı kapasitesimizi de artıracak savunma sanayi alanlarındaki çalışmalarımızı hızlandırmamız gerekmektedir.

Sonuç olarak, bilişim çağının getirmiş olduğu olumlu yanları kullanırken olumsuzluklarını da kullanmayı iyi bilen devletler, siber güvenlik mücadelesinden galip çıkacaktır. Siber güvenlik meselesini toplumsal ve devlet birlikteliği ile topyekûn bir yaklaşımla çözmek zorunluluktur. Toplumlar arası teknolojik farklılıkların hiç olmadığı kadar azaldığı günümüzde, bunu fırsata dönüştüren toplumlar, geleceğin öncü güçleri haline gelecektir. Biz de Türkiye olarak, önümüze gelen bu fırsatı çok iyi bir şekilde değerlendirerek, öncü bir güç haline gelebilmek için var gücümüz ile çalışmalıyız.

KAYNAKÇA

ABI Research (2014), "Global Cybersecurity Index", https://www.abiresearch.com/whitepapers/Global-Cybersecurity-Index/ (14.03.2016).

Ağyol, Ünlü (2015), "Dünden Bugüne DDoS", http://www.unluagyol.com/2015/03/dunden-bugune-ddos.html (01.02.2016).

Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun (2014), **T.C. Resmi Gazete**, 28918, 19 Şubat 2014.

Akleylek, Sedat, Tok, Zaliha Yüce (2011), "Siber Güvenlikte Kriptoloji", **Siber Güvenlik Çalıştayı**, Ankara.

Aksar, Yusuf (2013), **Teoride ve Uygulamada Uluslararası Hukuk-I**, Ankara: Seçkin Yayınları.

Akses, Aysam (t.y.), "TEMPEST", http://www.aysamakses.com/tr/bilgi-bankasi/tempest/ (14.02.2016).

Akyazı, Uğur (2012), **Siber Harekât Ortamının Siber Güvenlik Tatbikatları Kapsamında Değerlendirilmesi**, İstanbul: Harp Akademileri Basımevi.

Alcaraz, Cristina ve Zeadally, Sherali (2015), "Critical infrastructure protection: Requirements And Challenges For The 21st Century", **International Journal of Critical Infrastructure Protection**, 8, 53-66.

Alkan, Mustafa (2012), "Siber Güvenlik ve Siber Savaşlar", Bilgi Güvenliği Derneği,www.bilgiguvenligi.org.tr/index_files/sunumlar/siber_guvenlik_siber_savaslar_tbmm_internet_komisyonu_mayis_2012.pptx (21.01.2015).

Altıntaş, Emine Yazıcı (2014), "Ulusal Siber Güvenlik Çalışmaları", International Cyber Warfare and Security Conference, Ankara.

Altunok, Taner ve Katman, Filiz (2009), "Siber Tehdit Altyapısı ve Araçları", Haydar Çakmak ve Taner Altunok (Ed.), **Suç, Terör ve Savaş Üçgeninde Siber Dünya**, 1. Baskı *İçinde* (55-84), Ankara: Barış Platin Kitabevi.

Altunok, Taner ve Kaya, Zeynep (2009), "Siber Tehditlerle Mücadele", Haydar Çakmak ve Taner Altunok (Ed.), **Suç, Terör ve Savaş Üçgeninde Siber Dünya**, 1. Baskı *İçinde* (137-162), Ankara: Barış Platin Kitabevi.

Arimatsu, Louise (2012), "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations", 4th International Conference on Cyber Conflict, Talinn: NATO CCD COE Publications, 91-109.

Arslan, Rengin (2015), "Türkiye'ye Siber Saldırının 10 Günü: Ne Oldu?", BBC Türkçe, http://www.bbc.com/turkce/haberler/2015/12/151224_siber_saldiri_arslan (06.02.2016).

ASELSAN (2016a), "Hakkımızda, Tarihçe", http://www.aselsan.com.tr/tr-tr/hakkimizda/Sayfalar/Tarihce.aspx (13.02.2016).

ASELSAN (2016b), "Çözümlerimiz, Kripto ve Bilgi Güvenliği Sistemleri", http://www.aselsan.com.tr/tr-tr/cozumlerimiz/kripto-ve-bilgi-guvenligi-sistemleri (13.02.2016).

Atalay, Ahmet Hamdi (2012), Kurumsal Bilgi Güvenliği, **Siber Güvenlik, Mimar ve Mühendis Dergisi**, 68, 42-47.

Aydın, Mustafa (Ed.) (2013), **21.Yüzyılda Siber Güvenlik**, 1.Baskı, İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

BBC News (2001), "Q&A: What You Need to Know about Echelon" http://news.bbc.co.uk/2/hi/sci/tech/1357513.stm (07.02.2016).

BBC News (2011) "US Builds Net for Cyber War Games" http://www.bbc.com/news/technology-13807815 (05.02.2016).

Beech, Hannah (2011), "Meet China's Newest Soldiers: An Online Blue Army", Time, http://world.time.com/2011/05/27/meet-chinas-newest-soldiers-an-online-blue-army/ (07.02.2016).

Bıçakçı, Salih (2014), "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", **Uluslararası İlişkiler Akademik Dergisi**, 10(40), 101-130.

Bilgi Güvenliği Akademisi (t.y.), "Eğitimler", http://www.bga.com.tr/egitimler.html (16.02.2016).

Bilgi Güvenliği Derneği (2015), "Siber Güvenlik Uzmanı Yetiştirme Eğitim Kampı", http://www.bilgiguvenligi.org.tr/kategori/haberler/63210/siber-guvenlik-uzmani-yetistirme-egitim-kampi (16.02.2016).

Bilgi Güvenliği Derneği (2016), "Hakkımızda", http://www.bilgiguvenligi.org.tr/kategori/hakkimizda (14.02.2016).

Bilgi Teknolojileri ve İletişim Kurumu (2009), "Siber Güvenliğin Sağlanması: Türkiye'de Mevcut Durum ve Alınması Gereken Tedbirler", https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FSayfalar%2FSiberGuvenlik%2Fsg.pdf, Ankara (13.01.2015).

Bilgi Teknolojileri ve İletişim Kurumu (2015), "Siber Güvenlik Kurulu" https://www.btk.gov.tr/tr-TR/Sayfalar/SG-SIBER-GUVENLIK-KURULU (10.02.2016).

Bilgi Teknolojileri ve İletişim Kurumu (t.y.a), "2013 Faaliyet Raporu", http://www.btk.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fSayfalar%2fFaaliyet_Raporlari%2f2013_Faaliyet_Raporu.pdf (12.02.2016).

Bilgi Teknolojileri ve İletişim Kurumu (t.y.b), "Uluslararası Siber Kalkan Tatbikatı", http://www.btk.gov.tr/tr-TR/Sayfalar/SG-Uluslararasi-Siber-Kalkan-Tatbikati-2014 (12.02.2016).

Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (2015), "Kurumsal, BİLGEM", http://bilgem.tubitak.gov.tr/tr/kurumsal/bilgem (13.02.2016).

Billo, Charles ve Chang, Welton (2004), "Cyber Warfare, An Analysis of the Means and Motivations of Selected Nation States", U.S. Department of Homeland Security.

Bircan, Bahtiyar (2012), "Gelişmiş Siber Silahlar ve Tespit Yöntemleri", TÜBİTAK BİLGEM, http://docplayer.biz.tr/1142152-Gelismis-siber-silahlar-ve-tespit-yontemleri-bahtiyar-bircan-uzman-arastirmaci-siber-guvenlik-enstitusu.html (22.01.2016).

Bradbury, Steven G. (2011), "The Developing Legal Framework for Defensive and Offensive Cyber Operations", Keynote Address, Harvard National Security Journal Symposium, 2.

Brown, Gary D. ve Metcalf, Andrew O. (2014), "Easier Said Than Done: Legal Reviews of Cyber Weapons", **Journal of National Security Law and Policy**, 7(115), 115-138.

Canbek, Gürol ve Sağıroğlu, Şeref (2007), "Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme", **Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi** 23(1-2), 1-12.

Cavelty, Myriam Dunn (2008), **Cyber-Security and Threat Politics, US Efforts To Ensure The Information Age**, New York: Routledge.

CCD CoE (2016a), "About Cyber Defence Centre" https://ccdcoe.org/about-us.html" (08.02.2016).

CCD CoE (2016b), "History" https://ccdcoe.org/history.html" (08.02.2016).

CCD CoE (2016c), "Cyber Defence Exercises" https://ccdcoe.org/event/cyber-defence-exercises.html" (08.02.2016).

CCD CoE (2016d), "Tallinn Manual - Research", https://ccdcoe.org/research.html (08.02.2016).

CCD CoE (2016e), "World's Largest International Technical Cyber Defence Exercise Takes Place Next Week", https://ccdcoe.org/worlds-largest-international-technical-cyber-defence-exercise-takes-place-next-week.html (23.04.2016).

Cisco (t.y.), "What is the Difference: Viruses, Worms, Trojans, and Bots?", http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html (16.01.2016).

Clarke, Richard A. ve Knake, Robert K. (2010), **Cyber War – The Next Threat to National Security and What to Do About It**, New York DC: HarperCollins.

_____ (2010), **Siber Savaş, Ulusal Güvenliğe Yönelik Yeni Tehdit**, (Çev. Murat Erduran), İstanbul: İKÜ Yayınevi.

Colarik, Andrew M. (2006), **Cyber Terrorism: Political and Economic Implications**, Hershey and London: Idea Group Publishing.

Corell, Hans (2000), "The Challenge of Borderless Cyber-Crime", Syposium On The Occasion of The Signıing of The United Nations Convention Against Transnational Organized Crime, Palermo, http://legal.un.org/ola/media/info_from_lc/cybercrime.pdf. (23.01.2016).

Çakmak, Haydar ve Demir, Cenker Korhan (2009), "Siber Dünyadaki Tehdit ve Kavramlar", Haydar Çakmak ve Taner Altunok (Ed.), **Suç, Terör ve Savaş Üçgeninde Siber Dünya,** 1. Baskı *İçinde* **(**23-54), Ankara: Barış Platin Kitabevi.

Çakmak, Haydar ve Soyoğlu, İbrahim Kemal (2009), "Doğu Avrupa ve Asya'dan Siber Saldırı Örnekleri", Haydar Çakmak ve Taner Altunok (Ed.), **Suç, Terör ve Savaş Üçgeninde Siber Dünya,** 1. Baskı *İçinde* **(**111-136), Ankara: Barış Platin Kitabevi.

Çatal, Cengizhan (2013), "TSK'dan Siber Savunma Merkezi", http://www.hurriyet.com.tr/tskdan-siber-savunma-merkezi-22405874 (16.02.2016).

_____ (2014), "TSK'da Siber Ordu İçin Önemli Adım", http://www.hurriyet.com.tr/tskda-siber-ordu-icin-onemli-adim-26494181 (16.02.2016).

Çifçi, Hasan (2013), **Her Yönüyle Siber Savaş**, İstanbul: TÜBİTAK Popüler Bilim Kitapları.

Çitlioğlu, Ercan (2008), **Gri Tehdit Terörizm**, Ankara: Başak Matbaacılık ve Tanıtım Ltd.Şti.

Dean Matthew ve Herridge Catherine (2016), "Patriotic Hackers' Attacking on Behalf of Mother Russia", Fox News", http://www.foxnews.com/politics/2016/01/16/patriotic-hackers-attacking-on-behalf-mother-russia.html (06.02.2016).

Dennesen, Kristen (2011), "Cyber Warfare An Analysis of the Means and Motivations of Selected Nation States", http://www.cu.ipv6tf.org/lacnic15/LACNICV3.pdf (16.03.2016).

Denning, Dorothy E., (1999), **Information Warfare and Security**, New York: Addison-Wesley.

ENISA (2015), "Cyber Europe 2014 After Action Report", file:///C:/Users/HP/Downloads/Cyber%20Europe%202014%20After%20Action%20Report%20PUBLIC.pdf (08.02.2016).

ENISA (2016a), "About ENISA", https://www.enisa.europa.eu/about-enisa (07.02.2016).

ENISA (2016b), "ENISA Threat Landscape 2015", https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015 (07.02.2016).

ENISA (2016c), "International Conference", https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference (08.02.2016).

ENISA (2016d), "Cyber Atlantic 2011", https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-atlantic/cyber-atlantic-2011 (08.02.2016).

Ermiş, Kemal (2006), "Sayısal İmza ve Elektronik Belge Yönetimi", **Bilgi Dünyası**, 7(1), 121-146.

European Parliamentary Research Service (2014), Cyber defence in the EU Preparing for Cyber Warfare?, http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf (15.03.2016).

European Union (2013), European Commission, "Joint Communication to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", https://ccdcoe.org/strategies-policies.html (21.02.2016).

Flick, Tony ve Morehouse, Justin (2011), "Threats and Impacts: Utility Companies and Beyond", **Securing the Smart Grid Next Generation Power Grid Security** *içinde* (35-48), Science Direct, http://media.techtarget.com/searchSecurityChannel/downloads/Securing_ Smart_Grid_Chap3.pdf (12.01.2016).

Geers, Kenneth (t.y.), Cyberspace and the Changing Nature of Warfare, CCD COE, Tallinn, https://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/Black Hat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf (01.02.2016).

Gould, Joe (2015), Constructing a Cyber Superpower, Defense News, http://www.defensenews.com/story/defense/policy-budget/cyber/2015/06/27/us-cyber-command-budget-expand-fort-meade-offensive/28829321/ (03.02.2016).

GovTech (2013), "Top 10 Countries Where Cyber Attacks Originate", http://www.govtech.com/security/204318661.html (17.03.2016).

Güneştaş, Murat ve diğerleri (2015), "Siber Terörizm: Motivasyon ve Yöntem", Fatih Tombul ve diğerleri (Ed.), **Siber Suçlar, Tehditler, Farkındalık ve Mücadele** *içinde* (85-113), 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 (2015), "Uluslararası İlişkiler Bağlamında Güvenlik Algısı ve Siber Güvenlik; Akdeniz, Karadeniz ve Avrupa Bölgeleri Üzerine Bir Değerlendirme", **International Journal of Social Science**, 37, 477-489.

Gürgen, Murat (2015a), "Havada Hedef Uzay Gücü", http://www.haberturk.com/yazi-dizisi/haber/1072029-profesyonel-ordu-hudut-otesinde-savunma (16.02.2016).

_____ (2015b), "Kara Kuvvetleri'nde Hedef Hibrit Harekât", http://www. haberturk.com/yazi-dizisi/haber/1072029-profesyonel-ordu-hudut-otesinde-savunma (16.02.2016).

_____ (2015c), "Siber Mehmetçik Geliyor", http://www. haberturk.com/yazi-dizisi/haber/1072029-profesyonel-ordu-hudut-otesinde-savunma (16.02.2016).

Gürkaynak, Muharrem ve İren, Âdem Ali (2011), "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Dergisi**, 16(2), 263-279.

Güven, Buket (2013), "TSK'ya Siber Savunma Komutanlığı", http://www. haber7.com/guncel/haber/1102379-tskya-siber-savunma-komutanligi (16.02.2016).

Hager, Nicky (2010), Israel's Omniscient Ears, Le Monde Diplomatique, https://mondediplo.com/2010/09/04israelbase (04.02.2016).

Hagerott, Mark (2014), "Stuxnet and the vital role of critical infrastructure operators and engineers"**, International Journal of Critical Insfrastructure Protection,** 7, 244-246.

Haley, Christopher (2013), "A Theory of Cyber Deterrence", **Georgetown Journal of International Affairs**, 2013, http://journal.georgetown.edu/a-theory-of-cyber-deterrence-christopher-haley/ (24.04.2016).

Hathaway, Oona A. ve Crootof, Rebecca (2012), "The Law of Cyber-Attack", **California Law Review** içinde (817-886), 100, http://digitalcommons.law.yale.edu/fss_papers /3852 (24.04.2016).

HAVELSAN (2015a), "HAVELSAN", http://www.havelsan.com.tr/TR/Main/icerik/139/ havelsan (13.02.2016).

HAVELSAN (2015b), "Siber Güvenlik ve Bulut Bilişim Teknolojileri, Siber Güvenlik Hizmet ve Çözümleri", http://www.havelsan.com.tr/TR/Main/icerik/139/havelsan (13.02.2016).

Hekim, Hakan (2015), "Oltalama (Phishing) Saldırıları", Fatih Tombul ve diğerleri (Ed.), **Siber Suçlar, Tehditler, Farkındalık ve Mücadele** *içinde* (57-83), Ankara: Global Politika ve Strateji.

Henderson, Conway W. (2010), **Understanding International Law**, New Jersey: Wiley-Blackwell.

Heywood, Andrew (2014), **Küresel Siyaset**, 3. Baskı, Ankara: Liberte.

Hundley, Richard O. ve Anderson, Robert H.(1997), "Emerging Challenge: Security and Safety in Cyberspace", John Arquilla ve David Ronfeldt (Ed.), **In Athena's Camp, Preparing for Conflict in the Information Age** *içinde* (231-251), Santa Monica, CA: RAND Corporation.

ICWC (2014), "Home", http://www.icwcturkey.com/ (16.02.2016).

InternetLiveStats (2016), "Internet Users by Country 2016", http://www.internetlivestats. com/internet-users-by-country/ (18.03.2016).

Intoccia, F. Gregory ve Moore, Joe Wesley (2006), "Communications Technology, Warfare, And The Law: Is The Network A Weapon System?", **Houston Journal of International Law**, 28(2), 467-489.

ITU (2008), "Overview of Cybersecurity", ITU-T Recommendations, http://handle.itu.int/11. 1002/1000/9136-en?locatt=format:pdf&auth (15.01.2016).

ITU (2015), "Global Cybersecurity Index & Cyberwellness Profiles Report", https://www.itu.int/pub/D-STR-SECU-2015 (14.03.2016).

İduğ, Yavuz ve diğerleri (2013), "Siber Caydırıcılık ve Türkiye'nin İmkân ve Kabiliyeti", 6.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Bildiriler Kitabı, Ankara, 287-289.

Jeffrey, Carr (2011), **Mapping the Cyber Underworld – Inside Cyber Warfare**, 2nd Ed., California: O'Reilly Media.

Jerome, Nyameh (2013), "Application of the Maslow's hierarchy of need theory; impacts and implications on organizational culture, human resource and employee's performance", **International Journal of Business and Management Invention** 2(3), 39-45.

Jonasson, Daniel ve Sigholm, Johan (2005), "What is Spyware?", http://docplayer.net/8724618-What-is-spyware-daniel-jonasson-danjo620-student-liu-se-johan-sigholm-johsi264-student-liu-se-abstract-2-theory.html (23.01.2016).

Juzenaite, Rasa (2015), "The Most Hacker-Active Countries", http://resources.infosecinstitute.com/the-most-hacker-active-countries-part-i/ (17.03.2016).

Kalman, Aaron (2012), "Israel used 17 tons of explosives to destroy Syrian reactor in 2007, magazine says", http://www.timesofisrael.com/israel-uses-17-tons-of-explosives-to-destroy-syrian-reactor/ (01.02.2016).

Kanagasingham, Prathaben (2008), "Data Loss Prevention, SANS", https://www.sans.org/reading-room/whitepapers/dlp/data-loss-prevention-32883 (10.01.2016).

Kapoor, Shray (t.y.), "Session Hijacking Exploiting TCP, UDP and Http Sessions", http://www.infosecwriters.com/text_resources/pdf/SKapoor_SessionHijacking.pdf (23.01.2016).

Karaarslan, Enis ve diğerleri (2008), "Kurumsal Ağlarda Zararlı Yazılımlarla Mücadele Yöntemleri", X. Akademik Bilişim Konferansı.

Karabacak, Bilge (2011), "Kritik Bilgi Altyapıları ve Siber Güvenlik", Siber Güvenlik Konferansı, Ankara.

Karakuş, Cahit (t.y.), "Kritik Altyapılara Siber Saldırı", http://ckk.com.tr/bilimsel /siber.pdf, 6 (22.1.2016).

Kazemi, Manocheher ve diğerleri (2011), "On the Affine Ciphers in Cryptography", Azizah Abd Manaf ve diğerleri (Ed.), **Informatics Engineering and Information Science**, (185-199), Berlin: Springer.

Keith, B. Alexander (2007), "Warfighting in Cyberspace", **Joint Force Quarterly**, 46, 58-61.

Keleştemur, Atalay (2015), **Siber İstihbarat**,1. Baskı, İstanbul: Yazın Basın Yayınevi Matbaacılık Trz.Tic.Ltd.Şti.

Kılıç, Mehmet Bertan (2012), "Kurumsal Bilgi Güvenliği Yönetim Süreci", Bilgi Yönetimi Semineri, Antalya.

Kılıç, Recep (2014), "Siber Taarruz İcrası Muhtelif Gruplara Karşı Savunma ve Taarruz Teorilerin ve Çalışmaların İncelenmesi", Harp Akademileri Komutanlığı Harekât ve İstihbarat Ana Bilm Dalı, **Yüksek Lisans Tezi.**

Kırdı, Gökhan (2015), "Türkiye'de ve Dünya'da Siber Güvenlik Alanında Çalışmalar", http://sahipkiran.org/2015/01/14/siber-guvenlik/ (12.02.2016).

Kişisel Verilerin Korunması Kanunu (2016), **T.C. Resmi Gazete**, 6698, 24 Mart 2016.

Kurose, J.F., Ross, K.W. (2013), **Computer Networking, A Top-Down Approach**, 6th Ed., New Jersey: Pearson.

Libicki, Martin C. (2009), **Cyberdeterrence and Cyberwar,** Santa Monica, CA: RAND Cooperation.

_____ (1996), **What Is Information Warfare?**, 3th Ed., Washinghton, DC: U.S. Government Printing Office.

Lipovsky, Robert (2014), "Back in BlackEnergy: 2014 Targeted Attacks in Ukraine and Poland" http://www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014/ (06.02.2016).

Lupovici, A. (2011), "Cyber Warfare and Deterrence", **Military and Strategic Affairs**, 3(3), 49-62.

Macias Âmânda ve diğerleri (2014), "The 35 Most Powerful Militaries In The World", http://www.businessinsider.com/35-most-powerful-militaries-in-the-world-2014-7 (15.03.2016).

Martin, Chris (t.y.), "Intrusion Detection and Prevention Systems in the Industrial Automation and Control Systems Environment", Process Control Systems Industry Conference, https://ics-cert.us-cert.gov/sites/default/files/pcsf-arc/intrusion_ detection_prevention_ systems-martin.pdf (25.01.2016).

Mataracıoğlu, Tolga (2009), "Uygulamalarla Steganografi", TÜBİTAK BİLGEM, http://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/uygulamalarla-steganografi-3. Html (02.02.2016).

McAfee (2011), "Revealed: Operation Shady RAT", http://www.mcafee.com/us/resources/ white-papers/wp-operation-shady-rat.pdf (19.02.2016).

McAfee (2012), "57% Believe a Cyber Arms Race is Currently Taking Place, McAfee-Sponsored Cyber Defense Report", http://www.mcafee.com/us/about/news/2012 /q1/20120130-02.aspx (04.02.2016).

Mele, Stefano (2013), Cyber-Weapons: Legal and Strategic Aspects, Version 2.0, Machiavelli Editions, http://www.strategicstudies.it/wp-content/uploads/2013/07/ Machiavelli-Editions-Cyber-Weapons-Legal-and-Strategic-Aspects-V2.0.pdf (18.01.2016).

MGK Genel Sekreterliği (2010), "27 Ekim 2010 Tarihli Toplantı", http://www.mgk.gov.tr/ index.php/27-ekim-2010-tarihli-toplanti (10.02.2016).

Morkel, T. ve diğerleri (2005), "An Overview of Image Steganography", Proceedings of the Fifth Annual Information Security South Africa Conference, http://martinolivier. com/open/stegoverview.pdf (25.01.2016).

MS-ISAC ve US-CERT (2006), "Local Government Cyber Security: Beginners Guide to Firewalls", https://msisac.cisecurity.org/members/local-government/documents/firewall-guide.pdf (25.01.2016).

Mueller Paul ve Yadegari Babak (2012), "The Stuxnet Worm", http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report. pdf (01.02.2016).

Narmeen Shafqat ve Ashraf Masood (2016), "Comparative Analysis of Various National Cyber Security Strategies", **International Journal of Computer Science and Information Security**, 14 (1), 129-136.

NATO (2002), "NATO Press Release", Prague Summit Declaration, http://www.nato.int/docu/pr/2002/p02-127e.htm (08.02.2016).

NATO (2006), "Official Text: Riga Summit Declaration", http://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en (08.02.2016).

NATO (2015), "Cyber Security", http://www.nato.int/cps/en/natohq/topics_78170.htm (08.02.2016).

NCIA (2014), "NATO Industry Cyber Partnership", https://www.ncia.nato.int/NewsRoom/Pages/140911-NICP.aspx (08.02.2016).

Nebil, Fusun S. (2014a), "İnternet'te Yayınlanan Ses Kayıtları, 13 Yıllık Siber Suç Sözleşmesinin Onaylanmasını Sağladı", https://yenimedya.wordpress.com/tag/sanal-ortamda-islenen-suclar-sozlesmesinin-onaylanmasinin-uygun-bulunduguna-dair-kanun/ (11.02.2016).

_____ (2014b), "Uluslararası Siber Suç Sözleşmesinin Kabulü TBMM Gündeminde", http://www.turk-internet.com/portal/yazigoster.php?yaziid=45965 (11.02.2016).

Newman, R.E. (2000), "Computer and Network Security", http://www.cise.ufl.edu/~nemo/security/notes/network_security_standards.pdf (15.01.2016).

NICP (2016), "About the NATO Industry Cyber Partnership", http://www.nicp.nato.int/ (08.02.2016).

Nikiforakis ve diğerleri (2010), "SessionShield: Lightweight Protection Against Session Hijacking", https://www.securitee.org/files/sshield_essos2011.pdf (15.01.2016).

NSA (2011), "National Security Agency, Central Security Service Mission", https://www.nsa.gov/about/mission/index.shtml (03.02.2016).

O'Neill, Jack (2005), **Echelon: Somebody's Listening**, Pennsylvania: Word Association Publisher, https://books.google.com.tr/books?id=1x6Akzkxv5IC&printsec=frontcover&source=gbs_summary_r&redir_esc=y#v=onepage&q&f=false (06.02.2016).

Ortner, Michael (2015), "The World of Business Software: Which Countries to Serve?", http://blog.capterra.com/world-of-business-software/ (18.04.2016).

Öcüt, Adem (2016), "Mail ile gelen TTNET Faturalarına Dikkat Ediniz…", http://ademocut.com/mail-ile-gelen-ttnet-faturalarina-dikkat-ediniz/ (18.04.2016).

Panda Security (2015), "PandaLabs detected more than 21 million new threats during the second quarter of 2015, an increase of 43% compared to the same period in 2014", http:// www.pandasecurity.com/mediacenter/news/pandalabs-detected-more-than-21-million-new- threats/ (18.01.2016).

Passeri, Paolo (2016), "2015 Cyber Attacks Statistics", http://www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/ (18.01.2016).

Pellerin, Cheryl (2014), "Rogers: Cybercom Defending Networks, Nation", http://www.defense.gov/News-Article-View/Article/603083/rogers-cybercom-defending-networks-nation (03.02.2016).

Peterson, Dale (2013), "Offensive Cyber Weapons: Construction, Development, and Employment", **The Journal of Strategic Studies**, 36(1), 120-124.

Radack, Jesselyn (2009), "NSA's Cyber Overkill: A Project to Safeguard Governmental Computers, Run by the NSA, is too Big a Threat to Americans' Privacy", **Los Angeles Times**, http://articles.latimes.com/2009/jul/14/opinion/oe-radack14 (02.02.2016).

Raf Sanchez (2014), "China hacking charges: the Chinese army's Unit 61398", http://www.telegraph.co.uk/news/worldnews/asia/china/10842093/China-hacking-charges-the-Chinese-armys-Unit-61398.html (16.03.2016).

Raska, Michael (2015), "Revealed: The New Battleground in China's Future Wars", The National Interest, http://nationalinterest.org/feature/revealed-the-battleground-chinas-next-war-12387 (06.02.2016).

Reed, John (2015), "Unit 8200: Israel's cyber spy agency", FT Magazine, http://www.ft.com /intl/cms/s/2/69f150da-25b8-11e5-bd83-71cb60e8f08c.html (04.02.2016).

Richest Lifestyle (2015), 12 Most Technologically Advanced Countries, http://www.richestlifestyle.com/most-technologically-advanced-countries/6/ (15.03.2016).

Rid, Thomas ve McBurney, Peter (2012), "Cyber-Weapons", **The RUSI Journal**, 157(1), 6-13.

Sağıroğlu, Şeref (2011), "Siber Güvenlik ve Türkiye", Siber Güvenlik Çalıştayı, Ankara.

_____ (2013), "Siber Güvenlik ve Savunma", Harp Akademisi Geleceğin Harekât Ortamı ve Harp Teknolojileri Paneli, İstanbul.

SANS (2015), "The CIS Critical Security Controls for Effective Cyber Defense, Version 6", https://www.sans.org/critical-security-controls (10.01.2016).

Schaap, Arie J. (2009), "Cyber Warfare Operations: Development and Use Under International Law", **The Air Force Law Review,** 64, Cyberlaw Edition *içinde* (121-174), Washington DC: U.S. Government Printing Office.

Siber Güvenlik Derneği (t.y.), "Etkinliklerimiz", http://www.siberguvenlik.org.tr/p/etkinliklerimiz.html (14.02.2016).

Siber Güvenlik Enstitüsü (2015a), "Siber Güvenlik Tatbikatları", http://sge.bilgem.tubitak.gov.tr/tr/siber-guvenlik-tatbikatlari (12.02.2016).

Siber Güvenlik Enstitüsü (2015b), "Kurumsal, Siber Güvenlik Enstitüsü", http://sge.bilgem.tubitak. gov.tr/tr/kurumsal/sge-tarihcesi (13.02.2016).

Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ (2013), **T.C. Resmi Gazete**, 28818, 11 Kasım 2013.

Singer, P.W. ve Friedman, Allan (2015), **Siber Güvenlik ve Siber Savaş**, (Çev. Ali ATAV), 1.Baskı, Ankara: Buzdağı Yayınevi, 57.

Smith, Craig S. (2001), "6-12; The First World Hacker War", The New York Times, http://www.nytimes.com /2001 /05/13/weekinreview/may-6-12-the-first-world-hacker-war.html (01.02.2016).

Soysal, Murat ve Bektaş Onur (2009), "ULAKNET Balküpü Servisi", 3. ULAKNET Çalıştay ve Eğitimi, https://ulakbim.tubitak.gov.tr/sites/images/Ulakbim/didim_calistayi-balkupu.pdf (12.02.2016).

SSM (2015a), "Kurumsal", http://www.ssm.gov.tr/ANASAYFA/KURUMSAL/Sayfalar/default.aspx (16.02.2016).

SSM (2015b), "TSK Siber Savunma Merkezi Projesi", http://www.ssm.gov.tr/anasayfa/projeler/Sayfalar/proje.aspx?projeID=276 (16.02.2016).

STM (2016), "2016 Türkiye Siber Tehdit Durum Raporu", https://www.stm.com.tr/yayinlar/2016-SG/2016-turkiye-raporu.html (14.03.2016).

Symantec (2011), "Symantec Report on Attack Kits and Malicious Websites", http://www.symantec.com/content/en/us/enterprise/other_resources/b-symantec_report_on_attack_kits_and_malicious_websites_exec_summary_21169172_WP.en-us.pdf (14.01.2016).

Symantec (2015), "The Evolution Of Ransomware, Security Response", http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf (04.06.2016).

T.C. Adalet Bakanlığı (t.y.), "Siber Güvenlik Kanunu Tasarısı Taslağı", http://www.kgm.adalet.gov.tr/Tasariasamalari/Gorus/Gorus.htm (11.02.2016).

T.C. Başbakanlık AFAD (2014), "2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi", https://www.afad.gov.tr/Dokuman/TR/123-20141010111330-kritikaltyapi-son.pdf (14.03.2016).

Tatar ve diğerleri (2014), A Comparative Analysis of the National Cyber Security Strategies of Leading Nations, 9th International Conference on Cyber Warfare & Security, 211-218.

Tatar, Ünal (2011), "Sosyal Mühendislik Saldırıları", TÜBİTAK, BİLGEM, 4. Ağ ve Bilgi Güvenliği Sempozyumu, http://www.emo.org.tr/ekler/288230da37dbf3c_ek.pdf (10.01.2016).

TechTerms (t.y.), "Malware", http://techterms.com/definition/malware (24.01.2016).

The Government of the Hong Kong Special Administrative (2008a), "Region an Overview of Vulnerability Scanners", http://www.infosec.gov.hk/english/technical/files/vulnerability.pdf (25.01.2016).

The Government of the Hong Kong Special Administrative (2008b), "Honeypot Security", http://www.infosec.gov.hk/english/technical /files/honeypots.pdf (25.01.2016).

The White House (2010a) "The Comprehensive National Cybersecurity Initiative" https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (05.02.2016).

The White House (2010b) "National Security Strategy" https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (05.02.2016).

The White House (2011) "International Strategy for Cyberspace" https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (05.02.2016).

The White House (2015) "National Security Strategy" https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf (05.02.2016).

The White House (2016) "Fact Sheet: Cybersecurtiy National Action Plan" https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (19.02.2016).

ThreatCloud (2016), "Live Cyber Attack Threat Map", https://www.checkpoint.com/ThreatPortal/livemap.html (17.03.2016).

Tombul, Fatih (2015), "Kamu Yönetiminde Siber Suçlara Karşı Kullanıcılarda Farkındalık Oluşturulmasının ve Kurumsal Bilişim Güvenlik Politikalarının Oluşturulmasının Önemi", Fatih Tombul ve diğerleri (Ed.), **Siber Suçlar, Tehditler, Farkındalık ve Mücadele** *içinde* (141-164), Ankara: Global Politika ve Strateji.

TÜİK (2013), 06-15 Yaş Grubu Çocuklarda Bilişim Teknolojileri Kullanımı ve Medya, http://www.tuik.gov.tr/PreHaberBultenleri.do?id=15866 (14.03.2016).

TÜİK (2015), Hanehalkı Bilişim Teknolojileri Kullanım Araştırması, http://www.tuik.gov.tr/PreHaberBultenleri.do?id=18660 (14.03.2016).

Türk Dil Kurumu, Büyük Türkçe Sözlük (t.y.), "Güvenlik", http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.56a24cd989cae5.35079550 (10.01.2016).

Türkay, Şeyda (2013), "Siber Savaş Hukuku ve Uygulanma Sorunsalı", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, 71(1), 1177-1228.

Ulaşanoğlu, M. Emin ve diğerleri (2010), **Bilgi Güvenliği: Riskler ve Öneriler,** Bilgi Teknolojileri ve İletişim Kurumu, Ankara, http://docplayer.biz.tr/632957-Bilgi-guvenligi-riskler-ve-oneriler.html (12.01.2016).

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (2015), Kurumsal, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü http://uekae.bilgem.tubitak.gov.tr/tr/kurumsal/uekae (13.02.2016).

Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar (2012), **T.C. Resmi Gazete**, 28447, 20 Ekim 2012.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı (2013), **T.C. Resmi Gazete**, 28683, 20 Haziran 2013.

URL, "Cybercrime Top 10 affected countries" (2015), https://www.bba.org.uk/wp-content/uploads/2015/02/red24+Cybercrime+Top+10+affected+countries+-2015.pdf (17.03.2016).

URL, "Cybercrime Top 10 countries where attacks originate" (2015), https://www.bba.org.uk/wp-content/uploads/2015/02/red24+Cybercrime+Top+10+countries+where+attacks+originate+-++2015.pdf (17.03.2016).

URL, "Siber Saldırı Değil Savaş!" (2015), http://www.haberhergun.com/bilim-teknoloji/siber -saldiri-degil-savas-h41902.html (06.02.2016).

URL, “Siber Suç Sözleşmesine TBMM’den Onay”, **Bilişim**, 42(166), 36-37, http://www.bilisimdergisi.org/pdfindir/s166/pdf/36-37.pdf (11.02.2016).

URL, “SİSATEM Açıldı” (2016), http://www.havelsan.com.tr/a/Main/haber/3378/sisatem-acildi (15.04.2016).

URL, “U.S. Air Force Mission, Vision” (t.y.), https://www.airforce.com/mission/vision (03.02.2016).

URL, “Ukrayna Elektriğine Siber Saldırı - Enerji Günlüğü” (2016), http://enerjigunlugu.net/ukrayna-elektrigine-siber-saldiri_16907.html#.VrYB1EqLTIU (06.02.2016).

URL, “Ukrayna’da Elektrik Dağıtım Sistemi Siber Saldırıya Uğradı.” (2016), http://www.hurriyet.com.tr/ukraynada-elektrik-dagitim-sistemi-siber-saldiriya-ugradi-40043686 (06.02.2016).

URL, “8. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı” (2015), Ankara, http://www.haberler.com/8-uluslararasi-bilgi-guvenligi-ve-kriptoloji-7829357-haberi/ (12.02.2016).

US-CERT (2008), “Computer Forensics”, https://www.us-cert.gov/sites/default/files/publications/forensics.pdf (25.01.2016).

US-DHS (2016a), “Einstein”, http://www.dhs.gov/einstein (03.02.2016).

US-DHS (2016b), “Safeguard and Secure Cyberspace Mission”, http://www.dhs.gov/safeguard-and-secure-cyberspace (03.02.2016).

US-DHS (2016c), “Cyber Storm: Securing Cyber Space”, http://www.dhs.gov/cyber-storm (08.02.2016).

US-DoD (2009), “Military Power of the People’s Republic of China 2009: Annual Report to Congress”, http://www.defense.gov/Portals/1/Documents/pubs/China_Military_Power_ Report_2009.pdf (07.02.2016).

US-DoD (2015), “Military and Security Developments Involving the People’s Republic of China 2015”, Annual Report to Congress, http://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf (07.02.2016).

Uslu, Nurullah Celal (2015), "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı", 2015 Siber Güvenlik Çalıştayı, Bolu.

USOM, TR-CERT (t.y.), USOM Hakkında, https://www.usom.gov.tr/hakkimizda.html (11.02.2016).

USSTRATCOM (2010), "U.S. Department of Defense, Cyber Command Fact Sheet", http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf (02.02.2016).

Ünal, Ahmet (2015a), "Dağıtık Servis Dışı Bırakma (DDoS) Saldırıları: Güncel Yöntemler ve Mücadele", Fatih Tombul ve diğerleri (Ed.), **Siber Suçlar, Tehditler, Farkındalık ve Mücadele** *içinde* (11-36), Ankara: Global Politika ve Strateji.

Ünal, Ahmet Naci (2015b), **Siber Güvenlik ve Elektronik Bileşenleri,** 1.Baskı, Ankara: Nobel Akademik Yayıncılık Eğitim Danışmanlık Tic.Ltd.Şti.

Ünal, Arife Yıldız (2016), Türkiye'nin İlk Siber Güvenlik Merkezi Açılıyor, Bugün, http://www.bugun.com.tr/son-dakika/turkiyenin-ilk-siber-guvenlik-merkezi-2051486.html (16.02.2016).

Ünver, M. ve Canbay, C. (2010), "Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik", **Elektrik Mühendisliği Dergisi**, 48(438), 94-103.

Valentino, Devries Jennifer ve Yadron Danny (2015), Cataloging the World's Cyberforces, http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710 (16.03.2016).

Ventre, Daniel (2010), "China's Strategy for Information Warfare: A Focus on Energy", http://ensec.org/index.php?option=com_content&view=article&id=241:critical-energy-infrastructure-security-and-chinese-cyber-threats&catid=106:energysecuritycontent0510&Itemid=361 (03.02.2016).

Wedermyer, Landon J. (2012), "The Changing Face of War: The Stuxnet Virus and the Need for International Regulation of Cyber Conflict", http://www.law.msu.edu/king /2011-2012/Wedermyer.pdf (03.02.2016).

Weimann, Gabriel (2004), Cyberterrorism, How Real Is The Threat?, **United States Institute of Peace,** Special Report 119, Washinghton DC.

World Economic Forum (2013), "Global Risks 2013 Report Eight Edition", http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf (15.03.2016).

Yalçın, Esat (2014), "Türkiye'de Siber Güvenliğin Mevzuattaki Yeri ve Yapılan Çalışmalar", http://www.bilgiguvenligi.gov.tr/mevzuat/turkiye-de-siber-guvenligin-mevzuattaki-yeri-ve-yapilan-calismalar.html (11.02.2016).

Yazıcı, Ali (2011), "Siber Güvenlik ve SAHAB", http://www.emo.org.tr/ekler/fad64faae21db53_ek.pdf (22.01.2016).

_____ (2012), "Küresel Tehlike: Siber Savaş, Siber Güvenlik", **Mimar ve Mühendis Dergisi**, 68, 36-40.

Yener, Yavuz (2015a), "İlk Siber Savaş Örneği Olarak Kosova", https://siberbulten.com/makale-analiz/ilk-siber-savas-ornegi-olarak-kosova/ (19.02.2016).

_____ (2015b), "Gelmiş geçmiş en geniş çaplı siber saldırı: Shady RAT', https://siberbulten.com/makale-analiz/gelmis-gecmis-en-genis-capli-siber-saldiri-shady-rat/ (19.02.2016).

Yeşilyurt, Hamdi (2015), "Ulusal Güvenlik Perspektifinde Siber Güvenlik", Fatih Tombul ve diğerleri (Ed.), **Siber Suçlar, Tehditler, Farkındalık ve Mücadele** *içinde (*169-193), Ankara: Global Politika ve Strateji.

Yıldız, Mithat (2014), **Siber Suçlar ve Kurum Güvenliği**, Denizcilik Uzmanlık Tezi, T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Bilgi İşlem Dairesi Başkanlığı.

Yılmaz, Sait ve Salcan, Olcay (2008), **Siber Uzay'da Güvenlik ve Türkiye**, 1, İstanbul: Milenyum Yayınları.

2016-2019 Ulusal Siber Güvenlik Stratejisi (2016), T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf (18.04.2016).

6533 Sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun (2014), **T.C. Resmi Gazete**, 28988, 2 Mayıs 2014.

ÖZGEÇMİŞ

Barış ÇELİKTAŞ, 13.08.1986 İzmir doğumludur. İlköğretimini İzmir'de 1996-2000 yılları arasında Agâh Efendi İlköğretim Okulu'nda, ortaöğretimini ise 2000-2004 yılları arasında Maltepe Askeri Lisesi'nde tamamlamıştır. 2004 yılında Maltepe Askeri Lisesi'ni bitirmesini müteakip 2008 yılında, Kara Harp Okulu Komutanlığı'ndan Sistem Mühendisliği lisans diplomasıyla Teğmen rütbesiyle mezun olmuştur. Türk Silahlı Kuvvetleri bünyesinde İstanbul, Ankara, Diyarbakır, Hakkâri, Trabzon illerinde çeşitli birliklerde ve Avrupa Birliği Barış Gücü (EUFOR) bünyesinde Bosna Hersek'te görevlerde bulunmuştur. 2014 yılında Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Bölümü Tezli Yüksek Lisans Programı'na dâhil olmuş, bilimsel hazırlık ve ders yıllarını müteakiben "Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme" konulu yüksek lisans tezini hazırlamıştır. Hâlihazırda Bilgi Sistem Subay Temel Sertifikası eğitimi kapsamında Kara Harp Okulu Komutanlığı'nda görev yapmaktadır. Evli ve bir çocuk babası olup, iyi derecede İngilizce bilmektedir.