T.C.
Dicle Üniversitesi Sosyal Bilimler Enstitüsü
Kamu Yönetimi Anabilim Dalı

Yüksek Lisans Tezi

SİBER TEKNOLOJİLERE DAYALI YENİ ULUSLARARASI GÜVENLİK KONSEPTİ BAĞLAMINDA TÜRKİYE'NİN SİBER GÜVENLİK STRATEJİSİ

İdris YIKICI
17919003

Danışman
Doç. Dr. Yılmaz DEMİRHAN

Diyarbakır 2020

T.C.
Dicle Üniversitesi Sosyal Bilimler Enstitüsü
Kamu Yönetimi Anabilim Dalı

Yüksek Lisans Tezi

SİBER TEKNOLOJİLERE DAYALI YENİ ULUSLARARASI GÜVENLİK KONSEPTİ BAĞLAMINDA TÜRKİYE'NİN SİBER GÜVENLİK STRATEJİSİ

İdris YIKICI
17919003

Danışman
Doç. Dr. Yılmaz DEMİRHAN

Diyarbakır 2020

TAAHHÜTNAME

SOSYAL BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Dicle Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmelik'ine göre hazırlamış olduğum "Siber Teknolojilere Dayalı Yeni Uluslararası Güvenlik Konsepti Bağlamında Türkiye'nin Siber Güvenlik Stratejisi" adlı tezin tamamen kendi çalışmam olduğunu ve her alıntıya kaynak gösterdiğimi ve tez yazım kılavuzuna uygun olarak hazırladığımı taahhüt eder, tezimin kâğıt ve elektronik kopyalarının Dicle Üniversitesi Sosyal Bilimler Enstitüsü arşivlerinde saklanmasına izin verdiğimi onaylarım. Lisansüstü Eğitim-Öğretim yönetmeliğinin ilgili maddeleri uyarınca gereğinin yapılmasını arz ederim.

29/01/2020

İdris YIKICI

T.C

DİCLE UNİVERSİTESİ

SOSYAL BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ

DİYARBAKIR

İdris Yıkıcı tarafından yapılan "Siber Teknolojilere Dayalı Yeni Uluslararası Güvenlik Konsepti Bağlamında Türkiye'nin Siber Güvenlik Stratejisi" konulu bu çalışma, jürimiz tarafından Kamu Yönetimi Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir

Jüri Üyesinin

Ünvanı Adı Soyadı

Başkan: Prof. Dr. Nezir AKYEŞİLMEN

Üye: Prof. Dr. Seyfettin ASLAN

Üye: Doç. Dr. Yılmaz DEMİRHAN

Tez Savunma Sınavı Tarihi: 20/01/2020

Yukarıdaki bilgilerin doğruluğunu onaylarım.

.../…/2020

Prof. Dr. Nazım HASIRCI

ENSTİTÜ MÜDÜRÜ

ÖN SÖZ

Günümüzde bilgi teknolojilerine dayalı siber güvenlik uygulamaları yaşamın bir gerçeği haline gelmiştir. Bununla birlikte, çok yakın zamana kadar devletler internet vasıtası ile yapılabileceklerin yeterince farkında olmayıp, onu özel sektörün yoğunlukla kullandığı bir araç olarak görmekteydiler ya da internetin potansiyel yararlarını ve sakıncalarını birinci derecede önemli görmemekteydiler. Fakat bugün devletler de internetin bütün yararlarını fark etmiş ve bu nedenle interneti bir ulusal güvenlik sorunu olarak görmeye başlamışlardır.

Toplumsal yaşamın neredeyse her bir alanını kapsayan duruma gelmiş olan internet, faydalı yeniliklerinin yanında çok sayıda problemi de beraberinde getirmiştir. İlk başlarda iletişimsel bir buluş olarak ele alınan internet; zamanla kendisine kattığı sayısız teknik, sosyal ve siyasal yönlerle birlikte "siber uzay" olarak isimlendirilen bir alana dönüşmüştür. Şimdilerde ise interneti, sadece tohumu veya çekirdeği olarak düşünebileceğimiz "siber uzay"; sanılanın aksine sadece sanal, teknik, kod, program ve internetten oluşan bir dünya olmayıp oldukça gerçek, fiziki, sosyal, siyasal ve kişisel yönleri de olan çok karmaşık, çok boyutlu, her saniye büyüyen, genişleyen bir alan ve gerçek bir uzaydır.

Siber uzay, uluslararası sistemdeki devletlerin işleyişinde son zamanlara kadar dahi önemsiz olan rutin kararları/süreçleri ve arka plan politikaları ifade eden "ikinci dereceden politikalar"ın meselesi olarak görülmekteydi. Siber uzay şimdilerde ise devlet işleyişinde ulusal güvenliği, asli kurumları, kritik olan karar sistemlerini, temel değerleri ve çıkarları ifade eden "yüksek dereceden politika" meselesi olarak görülmesinin yanı sıra siber uzayın "yüksek dereceden politika"nın alanını şekillendirdiği ve "yüksek dereceden politika"nın da siber uzayın geleceğini şekillendirdiği kabul edilmektedir.

Bu yeni sanal uzayda, çoğu kez bilinmeyen çeşitli kaynaklardan tanımlaması zor olan bir dizi tehdit ve saldırıyla yüz yüzeyiz. Çünkü saldırının kaynağını, onları yönlendiren nedenleri ve bir saldırı yayıldıkça seyrini öngörmeyi belirlemek zordur. Siber tehditlerin oldukça karmaşık olan kimliğini kamu ve özel menfaatler, ulusal ve uluslararası aktörler yönünden saptamak oldukça zordur. Çünkü siber uzaydaki tehditler doğasında küreseldir ve hızlı teknolojik gelişmeleri içerir, onlarla mücadele oldukça zordur çünkü durmadan değişiyor ve sürekli karmaşıklaşıyorlar. Üst düzey eğitim, gelişmiş bir yasal çerçeve, etkin örgütsel işbirliği ve önemli kaynakların tahsis edilmesini gerektirir.

Son yıllara bakıldığında siber uzayın, siber saldırıların ve siber savaşların insanlığa olan etkilerinin fazlasıyla ölümcül ve yıkıcı bir seviyeye vardığı, siber saldırıların yalnızca birey veya özel şirketleri değil, toplumsal hizmet sağlayan sektörlerin altyapılarını da hedef haline getirdiği görülmektedir. İnternet icatçılarının asıl amacı iletişimi sağlamaktı. Bu yüzden var etme evresinde göz ardı ettikleri güvenlik prensibi şu anda her geçen gün gelişen, büyüyen, karmaşıklaşan ve daha fazla yaşam alanımızı işgal eden "siber uzay"da esaslı bir konu olarak karşımızda durmaktadır. Ülkemizde siber teknolojiler ve siber güvenlik konularında oldukça sınırlı kaynağın bulunması ve son birkaç yılda yeni yeni ele alınmaya başlayan bir konu olması nedeniyle; bu çalışmada siber uzayın gelişimi, siber teknolojik silahların birey, kurum ve devletlere karşı kullanılması sonucunda yaşanan ulusal ve uluslararası çatışmaların seyri, bunlara karşılık siber güvenliğin sağlanması için yapılması gerekenler ve son olarak da Türkiye'nin bu alanda yaptığı tüm çalışmaların kronolojik olarak sunulmasına ihtiyaç bulunmaktadır. Bu kapsamda bireylerin siber ön ekli konular hakkında farkındalığa/bilinç seviyesine sahip olmasının sağlanması, akademik çalışma ve araştırmaların teşvik edilmesi amacıyla siber uzay/savaş/güvenlik konularında yaşanan önemli gelişmelerin tümünün kronolojik olarak ele alındığı bu çalışma hazırlanmıştır. Söz konusu bu çalışma ihtiyacı gidermeye dönük mütevazi bir girişimdir.

Bu tez çalışmasının gerçekleştirilmesinde benden yardımlarını esirgemeyen, bilgi ve tecrübeleriyle bana yol gösteren danışman hocam Doç. Dr. Yılmaz Demirhan'a, ayrıca uzun ve yorucu tez yazım sürecinde beni sürekli destekleyen,

manevi olarak her daim yanımda olan annem ve aileme sonsuz teşekkürlerimi sunarım.

İdris YIKICI

Diyarbakır, 2020

ÖZET

Siber uzay ekonomiden ticarete, eğlenceden sağlığa, iletişimden ulaşıma, siyasetten savunmaya, bireysel işlemlerden küresel işlemlere, işletmelere ait süreçlerden devlete düzeyindeki hizmetlere kadar her alanı baştan başa etkileyen bir hal almıştır. Nerdeyse tüm işlem ve süreçlerin transfer edildiği bir alan halini alan bu uzayın ve bu uzayın siber teknolojilerinin güvenliğinin sağlanması elzemdir. Son zamanlarda siber silahların gelişiminde yaşanan artışlar ve bu silahların bireylerden devletlere kadar oldukça geniş bir yelpazeye karşı kullanılması, siber uzayın güvenliğinin bireyler ve devletler düzeyinde sağlanması gerekliliğini dayatmaktadır. Siber saldırıların bıraktığı tahribatlar hem birey hem de devlet düzeyinde önemli problemlere neden olmaktadır. Buna istinaden siber güvenliğin en zayıf halkası olan bireyin farkındalığının arttırılması, siber güvenliğe devletler düzeyinde önem verilmesi ve siber uzayın devletler tarafından savunulması gereken bir alan olması durumları öne çıkmıştır. Dünya genelinde devletler kendi politikalarına siber güvenliğin önemini, kendi siber uzaylarını savunma tedbirlerini ve siber güvenlik strateji belgelerini dâhil etmeye başlamışlardır. Önümüzdeki yıllarda teknolojik gelişmelere bağlı olarak siber saldırıların ve siber savaşların daha da artacağı göz önüne alınacak olursa, her devletin kendisini savunabilecek gerekli bilgi ve donanıma sahip siber savunma birimlerini, siber güvenlik strateji belgelerini ve yeterli insan farkındalığını oluşturmasının önemi net bir şekilde görülmektedir.

Bu bağlamda, küreselleşme ve teknolojinin bu döneminde yeni bir alan olarak ortaya çıkan, Siber Uzay, Siber Saldırılar, Siber Çatışmalar, Dünyada Siber Güvenlik Sorunu ve Siber Güvenlik Stratejileri ve son olarak da Türkiye'nin Ulusal Siber Güvenlik Stratejileri/Politikaları çalışmanın önemli ve kilit noktasını teşkil edecektir.

Anahtar Sözcükler

Siber Güvenlik, Siber Uzay, Siber Saldırı, Siber Savaş, Ulusal Siber Güvenlik, Siber Strateji, Bilgi Güvenliği, Eylem Planı.

ABSTRACT

Cyber space has become an all-encompassing impact, from economics to trade, from fun to health, from communication to transportation, from politics to defense, from individual transaction to global transaction, from business processes to state-level services. It inevitably essential to ensure the security of this space and the cyber tecnologies of this space, which become a space where almost all processes and prodecure are transferred. The recent increase in the development of cyber weapons and use of this weapons against the wide range of from individuals to states, has imposed the necessity of ensuring the security of cyber space at the level of indviduals and states. The damage caused by cyber attacks causes significant problems at both the individual and state level. Therefore, it is important to increase awareness of the individual, which is the weakest link of the cyber security, give importance to cyber security at the level of states and defended by states. Goverments around the World have begun the include the importance of cyber security, their own ccyber security strategy documents to their policies. Considering that in the coming years, cyber attacks and cyber wars will increase due to technological developments, the importance of the cyber defense units, cyber security strategy documents and adequate human awareness is celarly seen.

In this context, Cyber Space, Cyber Attacks, Cyber Conflicts, Cyber Security Problem and Cyber Security Strategies in the World, and finally Turkey's National Cyber Security Strategies/Policies which are emerging as new field in this period of globalization and technology, are the subjects of this study.

Keywords

Cybersecurity, Cyber Space, Cyber Attack, Cyber Warfare, National Cybersecurity, Cyber Strategy, Action Plan.

İÇİNDEKİLER

Sayfa No.

ÖN SÖZ ..... **I**
ÖZET ..... **IV**
ABSTRACT ..... **V**
İÇİNDEKİLER ..... **VI**
KISALTMALAR ..... **X**
GİRİŞ **1**

BİRİNCİ BÖLÜM
KAVRAMSAL ÇERÇEVE

1.1. SİBER UZAY **6**
1.2. SİBER SALDIRILAR **11**
1.2.1. Teknik Tabanlı Saldırılar 14
1.2.1.1. Virüsler (Viruses) 14
1.2.1.2. Kurtçuklar (Worms) 14
1.2.1.3. Truva Atı (Trojan Horse) 15
1.2.1.4. Bot, Botnet, Zombie (Robot, Köle Bilgisayarlar) 16
1.2.1.5. DoS ve DDoS (Hizmet Engelleme-Distributed Denial of Service Attacks) 18
1.2.1.6. Casus Yazılımları (Spyware) 20
1.2.2. Sosyal Tabanlı Saldırılar (Sosyal Mühendislik) 21
1.3. SİBER ÇATIŞMALAR **22**
1.3.1. Moonlight Maze (1989-2003) 23
1.3.2. Çin'in Siber İstihbarat Faaliyetleri (2005-2013) 23
1.3.3. Estonya'ya DDoS Saldırıları (2007) 27
1.3.4. Gürcistan Hibrit Savaşı (2008) 30

1.3.5. Stuxnet (2010) 32
1.3.6. Wikileaks (2011) 34
1.3.7. Snowden Olayı (2013) 35
İKİNCİ BÖLÜM
DÜNYADA SİBER GÜVENLİK SORUNU VE SİBER GÜVENLİK STRATEJİLERİ
2.1. SİBER GÜVENLİK KAVRAMI VE SİBER GÜVENLİĞİN GELİŞİMİ 37
2.2. SİBER UZAYDA ETKİN BAZI ÜLKELERİN VE KURUMLARIN SİBER GÜVENLİK STRATEJİLERİ 39
2.2.1. ABD 39
2.2.2. Estonya 44
2.2.3. İngiltere 51
2.2.4. Almanya 56
2.2.5. G. Kore 58
2.2.6. Rusya 59
2.2.7. Çin 61
2.2.8. NATO 62
2.2.9. Avrupa Birliği 64
2.2.10. Küresel Siber Güvenlik Endeksi 68
2.3. ÜLKELERİN SİBER GÜVENLİK STRATEJİLERİ UYGULAMALARINDAN ÖNE ÇIKAN HUSUSLAR 69
ÜÇÜNCÜ BÖLÜM
TÜRKİYE'NİN ULUSAL SİBER GÜVENLİK STRATEJİLERİ
3.1. TÜRKİYE İÇİN SİBER GÜVENLİK STRATEJİLERİNİN ÖNEMİ VE İHTİYACI 72
3.2. SİBER GÜVENLİK ALANINDA YAPILAN YASAL DÜZENLEMELER 78
3.2.1. Ulusal Yasal Düzenlemeler 78
3.2.1.1. 2003/10 Sayılı Başbakanlık Genelgesinin Yayımlanması 78
3.2.1.2. 5070 Sayılı Elektronik İmza Kanunu (2004) 79

3.2.1.3. Telekomünikasyon Yoluyla İletişimin Denetlenmesi Kanunu (2005) 79
3.2.1.4. 5651 Sayılı İnternetle İlgili Kanun (2007) 80
3.2.1.5. İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik (2007) 81
3.2.1.6. 5809 Sayılı Elektronik Haberleşme Kanunu (2008) 81
3.2.1.7. 5846 Sayılı Fikir ve Sanat Eserleri Kanunu 83
3.2.1.8. Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı (2012) 83
3.2.1.9. Kişisel Verilerin Korunması Kanunu (2016) 84
3.2.2. Uluslararası Yasal Düzenlemeler (Siber Suçlar Sözleşmesi) 84
3.3. SİBER GÜVENLİK ALANINDA ATILAN ÖNEMLİ ADIMLAR. 85
3.3.1. Politika Belgeleri 85
3.3.1.1. E-Dönüşüm Türkiye Projesi (2003) 85
3.3.1.2. Bilgi Toplumu Stratejisi Eylem Planı (2006) 86
3.3.1.3. Ulusal Sanal Ortam Güvenlik Politikası (2009) 87
3.3.1.4. Ulusal Bilgi Güvenliği Programı 90
3.3.1.5. MGK Bildirisi (2010) 90
3.3.1.6. Ulusal Siber Güvenlik Strateji Çalıştayı (2012) 91
3.3.1.7. 2013-2014 Ulusal Siber Güvenlik Stratejisinin Yayımlanması 93
3.3.2. Siber Güvenlik Alanında Faaliyet Gösteren Kurumlar 97
3.3.2.1. Kamu Kurumları 97
3.3.2.1.1. Türkiye Bilgisayar Olayları Müdahale Ekibi (TR-BOME) 97
3.3.2.1.2. Ulusal Siber Olaylara Müdahale Merkezi ve Müdahale Ekipleri 98
3.3.2.1.3. Ulusal Bilgi Güvenliği Kapısı 99
3.3.2.1.4. Siber Suçlarla Mücadele Daire Başkanlığı (2011) 99
3.3.2.1.5. Siber Güvenlik (Koordinasyon) Kurulu (SGK) (2012) 100
3.3.2.1.6. TÜBİTAK- Siber Güvenlik Enstitüsü (SGE) (2012) 101
3.3.2.1.7. TSK Siber Savunma Komutanlığı (2013) 102
3.3.2.2. Özel Kurumlar (Bilgi Güvenliği Derneği-2007) 103
3.3.3. Siber Güvenlik Alanında Yapılan Tatbikatlar 104

3.3.3.1. Bilgisayar Olayları Müdahale Ekibi 2008 Tatbikatı 104
3.3.3.2. Ulusal Siber Güvenlik 2011 Tatbikatı..... 105
3.3.3.3. Siber Kalkan 2012 Tatbikatı 106
3.3.3.4. Ulusal Siber Güvenlik 2013 Tatbikatı..... 107
3.3.3.5. Uluslararası Siber Kalkan 2014 Tatbikatı 108
3.3.3.6. Ulusal Siber Savunma 2017 Tatbikatı..... 109
3.3.3.7. Uluslararası Siber Kalkan 2019 Tatbikatı 110
SONUÇ 112
KAYNAKÇA 118

KISALTMALAR

AB	Avrupa Birliği
ARPA	Advanced Research Projects Agency-İleri Araştırma Projeleri Ajansı
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojileri Araştırma Merkezi
BOME	Bilgisayar Olaylarına Müdahale Ekibi
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CCD COE	Cooperative Cyber Defence Centre of Excellence-Müşterek Siber Güvenlik Mükemmeliyet Merkezi
CERT/CC	Computer Emergency Response Team/Coordination Center-Bilgisayar Olayları Müdahale Ekibi Koordinasyon Merkezi
CERT	Computer Emergency Response Team-Bilgisayar Olayları Müdahale Ekibi
CI	Critical İnfrastructure- Kritik Altyapı
CIA	Central Intelligence Agency-Merkezi Haberalma Teşkilatı
CIIP	Critical Information Infrastructure Protection-Kritik Bilgi Altyapısı Koruması-
CMF	Cyber Mission Force-Siber Görev Gücü
CYBERCOM	Cyber Command-Siber Komutanlık
DDoS	Distributed Denial of Service Attacks-Dağıtık Hizmet Aksatma Saldırısı
DHS	Department for Homeland Security-Ulusal Güvenlik Bakanlığı
DoD	Department of Defence-Savunma Bakanlığı
DoS	Denial of Service-Hizmet Dışı Bırakma
DPT	Devlet Planlama Teşkilatı
GCI	Global Cybersecurity Index-Küresel Siber Güvenlik Endeksi
ICT	İnformation And Communication Technology-Bilgi ve İletişim Teknolojileri
IT	Information Technologies-Bilgi Teknolojileri
ITU	International Telecommunication Union- Uluslararası Telekomünikasyon Birliği
KGB	Komitet Gosudarstvennoy Bezopasnosti-Devlet Güvenlik Komitesi
NCIRC	NATO Computer Incident Response Capability-NATO Bilgisayar Olaylarına Müdahale Yeteneği
NSA	National Security Agency-Ulusal Güvenlik Teşkilatı
OECD	Organisation for Economic Co-operation-Ekonomik İş birliği ve Gelişme Teşkilatı

OSCE	Organization for Security and Co-operation in Europe-Avrupa Güvenlik ve İşbirliği Teşkilatı
PLA	People's Liberation Army-Halk Kurtuluş Ordusu
PLC	Programmable Logic Controller-Programlanabilir Mantık Denetleyicileri
RIA	Estonian Information System Authority-Estonya Bilgi Sistemi Kurumu
SCADA	Supervisory Control And Data Acquisition-Merkezi Denetim ve Veri Toplama
SGK	Siber Güvenlik Kurulu
SOME	Siber Olaylara Müdahale Ekipleri
TİB	Telekomünikasyon İletişim Başkanlığı
TUENA	Türkiye Ulusal Enformasyon Altyapısı Ana Planı
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
USGSEP	Ulusal Siber Güvenlik Stratejisi Eylem Planı
USOM	Ulusal Siber Olaylara Müdahale Merkezi
USSTRATCOM	U.S. Strategic Command- ABD Stratejik Komutanlığı

GİRİŞ

İnternet, insanların yaşamı ve sosyoekonomik faaliyetleri için temel ve vazgeçilmez bir gereklilik olarak gelişimini sürdürmektedir. İşleri kolaylaştırmakla birlikte, ortaya çıkan yeni riskleri de beraberinde getirmiştir. Hiç durmayan ve asla durmayacak olan, bunun yerine katlanarak artan siber saldırılar nedeniyle her ülkenin istikrarlı, güvenilir ve esnek bir Bilgi ve İletişim Teknolojileri (İnformation and Communication Technology-ICT) altyapısı gereksinimi bulunmaktadır. Zayıf bir ICT altyapısı yüksek riskli olabilir. Siber istihbarat konusuyla ilgilenen herhangi bir parti uzmanı IT'yi kullanarak hükümet ve endüstriler hakkındaki gizli bilgileri ileri teknolojilerle kötüye kullanabilir (Sarker ve diğ. 2019, s. 1).

Bireysel olarak zarar verebilme riski barındıran siber saldırılar, aynı zamanda kurumsal olarak devletlere de zarar vermektedir. 2007'de Estonya'daki ilk devlet düzeyli siber savaştan bu yana, Rusya-Gürcistan siber savaşı, Çin'in siber faaliyetleri, İran'ın nükleer tesislerine yönelik Stuxnet saldırısı ve son olarak da 30.000 Suudi Aramco iş istasyonuna zarar veren Shamoon virüsü gibi bir dizi siber savaş olayı yaşanmıştır.

Bu saldırılar, siber savaşın zaman içinde tehlikesini artıracağını kanıtlayarak 21. yüzyılda siber alanın güvenliğini sağlamanın kritik önemini ortaya koymaktadır. Aslında, İngiltere'de Bakanlar Kurulu tarafından Haziran 2009'da hazırlanan "İngiltere'nin Siber Güvenlik Stratejisi", "Ulusal güvenlik ve refah için nasıl ki 19. yüzyılda denizlerde ve 20. yüzyılda havada güvenliği sağlamak zorunda kaldıysak, aynı şekilde 21. yüzyılda da siber uzaydaki avantajımızı sağlamalıyız" vurgusuyla dikkatleri siber uzayın önemine çekmektedir. Siber güvenlik alanındaki bu son gelişmeler göz önüne alındığında, ulusların siber uzay alanında hem savunma hem de saldırgan önlemler açısından şiddetli bir rekabet içinde olduklarını iddia etmek mümkündür (Çil ve diğ, 2012, s. 112-113).

Siber uzayda meydana gelen gelişmelerin ardından, son zamanlarda, dünyadaki ülkelerin çoğu, ulusal siber güvenlik stratejilerinin kabul edilmesine veya güncellenmesine, yeni yasaların ve diğer belgelerin hazırlanmasına, onaylanmış ve etkili ulusal siber güvenlik strateji belgeleri oluşturulmasına odaklanmışlardır. Siber güvenlik stratejilerinin Avrupa Birliği üyesi ülkeler ve dünyanın dört bir yanındaki ülkeler tarafından benimsenmesi özellikle 2011 sonrasında gerçekleşmiştir. Bazı ülkeler stratejilerini geliştirme ve uygulamada büyük ilerleme kaydetmiş ve stratejilerinin ikinci versiyonuna yani, siber güvenlik alanındaki yeteneklerin gelişimine, kurumsal sorumlulukların stratejilerine ve iyileştirilmesine geçmişlerdir (Estonya, Hollanda, Çek Cumhuriyeti, vb.) (Štitilis ve diğ. 2017, s. 357-358).

Özellikle ülkelerinin kritik altyapısına (critical infrastructure-CI) ve ekonomik yapılarına yönelik gerçekleşen siber saldırılar nedeniyle siber güvenlik kavramının ciddi şekilde değerlendirilmesine ve bu alandaki ilk adımların ABD, Japonya, Rusya, Almanya, İngiltere gibi ülkeler tarafından atıldığına tanık olunmuştur. Bu ülkeler önce vizyonu, kapsamı ve metodolojisi olan stratejiler hazırlamış, ardından onları uygulamaya koymuş bu stratejiler sayesinde de siber güvenlik/uzay konusunda rehberlik eden ülkeler konumuna gelmişlerdir (Ataç ve Akleylek, 2018, s. 603).

Dünyanın dört bir yanında hayata geçirilmekte olan siber güvenlikçi politikalara/stratejilere paralel olarak Türkiye de 1990'lı yıllarda siber suçla mücadeleye yönelik yaptığı düzenlemeler ile siber güvenliği sağlamaya ve siber uzayda söz söyleyebilme mücadelesini başlatmıştır. 2010'dan sonraki yıllarda, Ekim 2012'de Siber Güvenlik Konseyi (SGK)'nin kurulması ile, Ocak 2013'te "2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2013-2014 USGSEP)"nın yayımlanmasıyla, Eylül 2016'da "2016-2019 USGSEP"sinin uygulanmasıyla Türkiye'deki siber güvenlik düzeyi daha profesyonel kurumsal yapılanmalara ve politika geliştirme süreçlerine dönüşmeye başlamıştır. Böylelikle de Türkiye'de siber uzay/güvenlik konusunda faaliyet gösteren kurumsal yapılanmalar hızla şekillenmeye başlamıştır.

Ülkelerin siber uzaya ilişkin ulaştıkları bu gelişmeler, uluslararası sistemdeki devletler için yeni zorluklar demektir. Devletler, siber uzayı, askeri yeteneklerini

kalkındırmaktan ve dış politikada sorunlu oldukları ülkelere karşı bir baskı aracı olarak kullanmaktan imtina etmemektedirler. Siber uzayda vuku bulan bunca çekişme ve siber savaş hali, uluslararası düzeni hiç olmadığı kadar belirsizliğe ve anarşiye itebilecek bir potansiyele sahiptir. Böylesine karmaşık olan uluslararası sistemde Türkiye'nin siber güvenlik stratejilerine, politikalarına, kurumlarına, savunmasına ve saldırı yeteneklerine yatırım yapmada tereddütsüz bir bilince sahip olduğu da aşikardır. Bu bağlamda Türkiye'nin yapması gereken şey, ulusal ve uluslararası siber güvenlik stratejilerinin güvenliğini olanaklı kılması ve ileri seviyede planlama ve organizasyon yapılanmasına gitmesi gerekmektedir.

Kısaca özetlenen bu bulgular bağlamında;

Tezin Sorunsalı: Türkiye'nin siber güvenlik stratejileri ve bu stratejilerin ulusal güvenlikle ilişkisidir. Bu çerçevede tezin ana sorusu ve yardımcı soruları aşağıdaki gibi formüle edilebilir.

- Türkiye'nin ulusal siber güvenlik stratejilerinin/politikalarının ulusal güvenliğe etkileri nelerdir?

Bu ana sorunun yanında şu yardımcı soruları da sormak mümkündür:

- Siber güvenlik neden önemlidir?
- Siber güvenliğin uluslararası güvenliğe etkileri nelerdir?
- Siber güvenliğin bileşenleri nelerdir?
- Ulusal siber güvenlik stratejilerinin koordinasyonu nasıl sağlanmaktadır?
- Seçilmiş ülkelerde siber güvenlik politika oluşturma süreci ve yönetimi nasıl düzenlenmiştir?
- Hangi aktörler siber güvenliğe dâhil olmaktadır ve siber güvenliğin sorumlulukları bunlar arasında nasıl dağılmaktadır?
- Siber güvenliğin sorumlulukları kanunla ve diğer düzenleme türleriyle nasıl düzenlenir?

Tezin Önemi: Siber güvenlik son yıllarda özellikle 11 Eylül saldırıları sonrası dönemde ulusal ve uluslararası güvenliğin önemli bir bileşeni haline geldi. Bu alanda

ulusal ve uluslararası literatür sürekli gelişirken, mevcut literatür daha çok teknik boyutlar ve teknik saldırılarla sınırlı kalmaktadır. Bu çalışma teknik boyutun yanında politik/stratejik boyutuna ağırlık vermektedir. Bu çerçevede, özellikle Türkçe literatürdeki bu boşluğun doldurulmasına mütevazi bir katkı sağlayacaktır.

Tezin Sınırlılıkları: Bu tez siber saldırılar ve siber güvenlikle ilgili bütün konulara değinmek yerine, Türkiye'nin siber güvenlik stratejileri çerçevesinde ihtiyaç duyulan bölümlerle sınırlı olacaktır. Bu çerçevede, Türkiye'nin siber güvenlik stratejilerini/politikalarını daha sağlıklı analiz edebilmek amacıyla siber alanda önemli aktörler olan ülkelerin siber güvenlik stratejilerine de değinilecektir.

Bu tez zaman ve kaynaklarla sınırlıdır ve bu nedenle genel bir değerlendirme niteliği taşımaktadır. Sonuç olarak, bu tez yalnızca son derece karmaşık ve dinamik bir alan olmalarından dolayı siber uzay/güvenlik/saldırılar/çatışmalar ve siber güvenlik strateji politikalarının/belgelerinin yüzeyine dokunabilecektir. Bununla birlikte, bu tezin sınırlı kapsamı dâhilinde, farklı ülkelerdeki farklı vakaları/uygulamaları, ülkelerin bu zorlukları nasıl ele aldıklarını ve siber güvenliğin/politikaların/stratejilerin sağlanmasının zorluklarına değinilecektir.

Tezin Yöntemi: Bu tez çalışmasında bilginin kaynağı ve bilgiye ulaşım yöntemi olarak öncelikle literatür taramasına ağırlık verilmiştir. Bu alanda etkin olan ülkelerin ulusal siber güvenlik strateji/politika belgeleri, anlaşmalar ve kurumların görüşleri gibi birincil kaynaklar da kullanılmıştır. Bunun yanında, ihtiyaç duyulduğunda güncel istatistikler, ülke karşılaştırmaları ve güncel yorumlara da başvurulmuştur. Birinci ve ikinci el kaynaklardan derlenen literatür taraması, çalışmanın bilimsel-akademik biçimini oluşturmuştur.

Bu çerçevede hazırlanan bu çalışma üç ana bölüm, giriş ve sonuç bölümlerinden oluşmaktadır.

Birinci bölümde, kavramsal çerçeve, siber uzay, siber saldırılar ve siber çatışmalar üzerinde durulmaktadır.

İkinci bölümde, dünyada siber güvenlik sorunu ve siber güvenlik stratejileri, siber güvenlik kavramı ve siber güvenliğin gelişimi, siber uzayda etkin bazı ülkelerin

ve kurumların siber güvenlik stratejileri ve bu kapsamda da Amerika Birleşik Devletleri (ABD), Estonya, İngiltere, Almanya, G. Kore, Rusya, Çin, NATO ve Avrupa Birliği'nin siber güvenlik politikaları/stratejileri ve kurumları üzerinde durulmaktadır.

Üçüncü bölümde, Türkiye'nin ulusal siber güvenlik stratejileri, neden Türkiye siber güvenlik stratejilerine önem vermeli ve strateji geliştirmeli? Siber güvenlik alanında yapılan yasal düzenlemeler, siber güvenlik alanında atılan önemli adımlar, politika belgeleri, kurumlar ve tatbikatlar üzerinde durulmaktadır.

Sonuç bölümünde incelenen tüm politika belgeleri ve stratejilerine yönelik genel bir değerlendirme ve öneriler üzerinde durulmaktadır.

BİRİNCİ BÖLÜM

KAVRAMSAL ÇERÇEVE

1.1. SİBER UZAY

Ekranlarımızın hemen ardındaki dünya olarak tanımlanan siber uzayın (Çakır, 2016, s. 140) önemi her geçen gün artmaktadır. Bu da günümüz sosyal bilimleri perspektifiyle daha yeni yeni ele alınmakta olan siber uzay konusuna daha fazla dikkat kesilmeyi zorunlu kılmıştır. Her yıl yayınlanan raporlar da bu zorunluluğu arttırmaktadır. Öyle ki "Digital in 2018" Raporuna göre günümüz dünyasında interneti kullanan insan sayısı 4 milyarı aşmış ve bu sayı bir önceki yıla göre de 250 milyon artmıştır (Türkay, 2018).

"We Are Social"ın 2018'de dünyada kullanılmakta olan sosyal medya, internet ve mobil cihazları kullanıcılarının yer aldığı istatistiklerinin sonuçlarına göre, 7 milyar 593 milyonluk dünya nüfusunun (Bayrak, 2018);

- ✓ 4 milyar 2 milyon kişi interneti kullanmaktadır. Bu oran dünyadaki nüfusun %53 kadarını oluşturmaktadır.
- ✓ Aynı rapora göre sosyal medyayı kullananların sayısı 3 milyar 19 milyon kişiye ulaşmıştır. Bu oran dünyadaki nüfusun %42 kadarını oluşturuyor.
- ✓ Mobil cihazları kullananların sayısı 5 milyar 13 milyon kişiye ulaşmıştır. Bu oran dünyadaki nüfusun %68 kadarına denk gelmektedir.
- ✓ Son olarak mobil cihazları ile sosyal medya kullananların sayısı 2 milyar 95 milyon kişiye ulaşmıştır. Bu oran dünyadaki nüfusun %39 kadarına denk gelmektedir.

Günümüzdeki internet kullanıcı sayısı ve trafiğinin böylesine milyarlarla ifade edilebildiği bir zaman diliminde siber uzayı tanımlayıp anlamak fazlasıyla önem kazanmaktadır.

Literatüre bilimsel bir kavram olarak değil de aksine edebiyat yoluyla giren siber kelimesi etimolojik olarak; gemiyi yöneten kişi, yönetim sanatı, yönetici, dümenci gibi anlamlara sahiptir (Akyeşilmen, 2018, s. 54). Siber sözcüğünün gerçekte yakın zamanda kazandığı semantiğinden farklı bir semantiğe sahip olduğu ve farklı bir alandan türetildiği görülür. Eski Yunan medeniyetleri döneminde Kübernetes telaffuzuna sahip olan sözcük, 1948 yılında Norbert Wiener'ın ele aldığı makinalar ile hayvanların aralarındaki kontrolü/iletişimi araştıran sibernetik kavramı olarak yeniden ortaya çıkmıştır (Kurnaz, 2016, s. 62). Siber uzay sözcüğünün ilk kullanımını ise bilim-kurgu yazarlığı yapan Kanadalı William Gibson 1984'te yazdığı Neuromancer isimli romanında yer almıştır. Burada siber uzayı "kabul görmüş halüsinasyon" şeklinde ele almıştır (Çakır, 2016, s. 141). Yine Gibson, kavramı aşağıdaki yönleri ile de tanımlamıştır. Buna göre siber uzayı "her ulustan milyarlarca yasal kullanıcı tarafından uzlaşmalı olarak, çocukken öğrenilen matematiksel kavramlar aracılığıyla görülen ve her gün tecrübe edilen bir halüsinasyondur. İnsan sistemindeki her bir bilgisayarın kayıtlarından yansıtılan verilerin grafiksel sunumudur. Kavranamayacak bir karmaşıklıktır. Zihnin uzaysızlığında, ışık çizgileri; öbekler ve takımyıldızlar şeklinde düzenlenen verilerdir. Tıpkı şehrin ışıkları gibi, gitgide uzaklaşan… aklın boş olmayan yerlerinde uzanan ışık hüzmeleri, veri küme ve topluluklarıdır." (Gibson, 1984, s. 69).

Başka bir tanıma göre siber uzay; dijital verilerin oluşturulduğu, depolandığı ve en önemlisi de paylaşımının yapıldığı bir bilgi ekosistemidir. Bu sadece bilgiden oluşan değil aynı zamanda bu bilgiyi depolayan bilgisayarlardan ve bu bilgileri paylaşmaya yarayan sistem ve altyapılardan oluşur. Buradaki sistem ve altyapıları ise bilgisayarları birbirine bağlayan internet, kapalı ağlar, mobil teknolojiler, uydu temelli iletişimler ve fiber optik kablolar oluşturur. Buradaki internet dijital bir dünyayı içine alırken, siber uzay ise burada sözü geçen dijital dünyanın arkasındaki insanı da içine almaktadır (Akyeşilmen, 2018, s. 53).

Siber gücün kullanılabilmesi, siber uzayın kullanılabilme kabiliyetine bağlıdır. Siber uzayın tanımını siber güç tanımı üzerinden de yapmak mümkündür. Buna göre siber güç, tüm harekât alanları ve güç unsurları (uzay, hava, kara, deniz) üzerindeki olaylara etki ederek avantaj sağlamaya yönelik siber uzayı kullanma kabiliyetidir. Tanımda da görülebildiği üzere siber alan şu anda birçok devlet tarafından tıpkı karada, denizde, havada ve uzayda yaşanan savaşlara benzer bir savaş sahası haline gelmiştir. Siber uzayın, aynı zamanda birer çatışma alanı olan ulusal güç unsurlarından (uzay, hava, kara, deniz) ayrılan yanı ise diğer ulusal güç unsurlarının her birisi üzerinde sağladığı etkinliğidir. ABD Hava Kuvvetleri Temel Doktrininde hava gücünün tanımında, siber uzayı görmek mümkündür. Bu tanımda siber uzay; önemli, işlevsel ya da taktiksel amaçlara erişmek maksadıyla hava kuvvetlerinden, uzaydan ve siber uzaydan faydalanılması ve kontrolünün sağlanması vasıtasıyla askeri etkiyi/gücü idare etme kabiliyeti şeklinde geçmekte olup burada daha çok bir çatışma alanına indirgenmektedir (Akyazı, 2013, 216).

Tümü insan eliyle yapılmış ve fazlasıyla karmaşık olan siber uzay, sadece internete bağlı olan bilgisayar sistemlerinden değil, aynı zamanda yerel ağlardan, mobil teknolojilerinden, optik lif kablolarından, dış dünyaya açık olmayan askeri ağlardan, program tabanlı telsizlerden, elektronik kontrol sistemlerinden, uzaktan kumandalı pilotsuz araçları ile uzay kaynaklı bilişim dizgelerinin tümünden meydana gelmektedir (Meral, 2015, s. 6).

Sanal âlem sözü internet ortamını çağrıştırmaktadır. Bu noktadan hareketle bir üst kavram olarak siber uzay internet ortamını da kapsamaktadır. Bilgisayar, internet ve cep telefonlarının kullanımının yanında; bilgi işlem teknolojileri aracılığıyla elde edilen hizmetlerin dünyanın her bir tarafına ve uzaya yayılmış olması, dahası tüm bunlara tümünü birbirine bağlayan mevcut ağların varlığının da eklenmesi siber ortamı oluşturmuştur. Böylelikle uzaya yayılmış olan siber ortam kendisiyle siber uzayı da var etmiştir (Daban, 2016, s. 87). Bu değerlendirme sonucunda, siber ortam tanımının siber uzay tanımına nasıl evrildiği ve aslında her iki kavramsallaştırmanın da uzaya yayılmış olan bir ağ teknolojisinden ileri geldiği ortaya çıkmaktadır. Bu tanımlama ışığında aynı zamanda siber ortamın siber uzay olduğu söylenebilir.

Her gün/saat/saniye büyüyen, sadece internet üzerinden günde beş milyar GB'i geçen bir bilginin üretildiği, bütün bilgisayar ve ağ sistemlerini, bütün dijital veri ve onları işleyen kullanıcıları kapsayan, internette ulaşılamayan diğer dijital üretimi de göz önüne alındığında siber uzayın muazzam bir büyüklüğü karşımıza çıkmaktadır. Böylesine karmaşık, dinamik ve geniş bir alanı anlayıp, tanımlayıp, analiz edebilmek zordur. Siber uzayın, bireysel düzeyden küresel düzeye, ekonomiden ticarete, iletişimden çatışmalara her alanı etkileyen, değiştiren ve dönüştüren gücüyle her geçen gün etkinliğini artırdığı görülmektedir. Bu nedenle, her geçen gün büyümesini bu hızla sürdüren bir siber uzayın sosyal etkilerini analiz etme çalışmalarının hızı, siber uzayın hızına yetişmesi zor olabilir, fakat siber alandaki çalışmalar arttıkça onu anlayıp yararlanabilme olanağı da artacaktır (Yeşilmen, 2018, s. 64).

Choucri (2013) siber uzayı, sosyal bilimler perspektifinden yaptığı tanımlamayla "etkileşimin yeni alanı ve oluşturulmuş bağlamı" şeklinde ele almaktadır. Choucri, bu tanımlama çerçevesinde daha derinlemesine ele alarak kendi deyimiyle "özünde (çekirdeğinde) internet olan" siber uzay:

- ✓ Milyonlarca bilgisayarın küresel bir ağ (internet) ile birbirine bağlanması yoluyla oluşturulmuştur.
- ✓ Fiziksel öğelerin mantıklı bir ara bağlantı (dâhili bağlantı) çerçevesinde bilgilerin işlenmesine, idare edilmesine, kullanılmasına, çoğaltılmasına ve insan ile bilgilerin birbiriyle etkileşimine olanak tanıyan katmanlı bir yapı olarak inşa edilmiştir.
- ✓ Kurumsal aracılık ve organizasyonlar tarafından etkinleştirilen (sağlanan), merkeziyetsizleştirme ile karakterize edilen ve bu aktörler, müşteriler (aboneler) ve çıkar grupları arasındaki karşılıklı etkileşimdir.

Küresel bilgi altyapısı genel olarak iletişim ağlarından, bilgi donanımı ve yazılımlarından, uygulamalardan ve içerik oluşturan, içerik kullanan, katma değer ve yeni iletişim tabanlı aktivitelerin oluşturulmasını sağlayan insanlardan oluşur (Spinello, 2002, s. 3). Bu genel açıklama, geniş kapsamlı bir rol ve işlev yelpazesini çağrıştıran karmaşık bir düzenlemeye işaret etmektedir. David D. Clark ise bu

tanımlamayı genişleterek, siber etki alanını sistematik olarak düzenler ve katmanlı bir siber model önerir (Choucri, 2012, s. 8).

Clark (2010)'ın katmanlı modeline göre siber uzay 4 katmandan oluşur:

1. Fiziksel Katman: Fiziksel iletişim altyapısıdır. Siber oyun alanını olanaklı kılan temel altyapılardır. Siber uzay, birbirine bağlı bilgi işlem aygıtlarının bir uzayıdır; bu nedenle temelleri bilgisayarlar, sunucular, süper bilgisayarlar, iletişim şebekeleri, sensörler, transdüserler (dönüştürücüler), internet ve diğer ağ ve iletişim kanallarıdır. İletişim, teller veya fiberler üzerinden, ya da radyo iletişimi yoluyla veya bilgisayar ve depolama aygıtlarının bir yerden başka bir yere fiziksel olarak taşınmasıyla oluşabilir.
2. Mantıksal Katman: siber uzay, siber mantıksal düzeyde, her biri yeni yeteneklerin inşa edildiği ve bir sonraki yenilik için bir platform haline gelen bir dizi platformdur. Mantıksal yapı taşları, siber uzayın fiziksel platformlu yapısını destekleyen, hizmetleri oluşturan ve etkinleştiren yazılımlardır.
3. Bilgi Katmanı: Siber uzayda depolanan, iletilen ve dönüştürülen bilgilerdir. Bilgi katmanı video, müzik, işletme kayıtları, işlem kayıtları, meta-veri (tanımlayıcı veri), statik ve dinamik olarak oluşturulan bilgiler vb. çok sayıda bilgi formundan oluşur.
4. Üst katman – İnsanlar: Bu alanda çeşitli rollerde yer alan, çeşitli ilgi alanlarına sahip aktörler, kuruluşlar ve kullanıcılardır. İnsanlar siber deneyime katılarak yani iletişim kurarak, bilgi ile çalışarak, karar verip ve planlayarak, siber uzayın bileşen hizmetleri ve yetenekleriyle çalışarak siber alanın doğasını kendileri dönüştürür.

Önceki sayfalarda verilen bilgiler ışığında siber uzay, ülkelerin kendi egemenliklerine alamadığı, askeri olarak korunmasının olanaklı olmadığı, ulusal sınırların geçerli olmadığı ve kimi zaman da "tüm internet"i karşılayan bir kullanım şeklinde karşımıza çıkan bir kavramdır. Siber uzay kavramını, "olmayan yer (no place)" ve mükemmel şeklinde tanımlayanlar da vardır. Bu tanımlamada sayısal evrenin fiziki evreni geçtiği anlamı vardır. Veri ile veriyi yönlendiren/işleten mevcutlar, atomun negatif yüklü parçacıkları misali "her yerde ve hiçbir yerdedir" (Rakhmanova, 2018, s. 51).

Şu ana kadar yapılmaya çalışılan tanımlardan da anlaşılacağı gibi, siber uzay ile ilgili hemfikir olunabilecek bir kavramsal tanımlamasının olmadığı dikkatlerden kaçmamaktadır. Bu durumu açığa çıkaran şey ise siber uzayın sürekli genişleyen doğasıdır. İletişim ve teknolojinin sürekli gelişmesi, siber uzayda yeni saldırıların, tehditlerin, suçların siber teknolojik silahların ve güvenlik kavramlarının boyutlarını da değiştirip genişletmektedir. Bu durum siber alana ve siber uzayın kavramlarına yönelik yapılacak tanımlamaların boyutlarının belirlenmesini zorlaştırmaktadır.

1.2. SİBER SALDIRILAR

Bilişim ve ağ teknolojilerinin sürekli artan gelişimlerine paralel olarak yeni teknolojilerin geliştirildiği bir zaman diliminde mevcudiyet bulan ve kendisiyle birlikte bu alandaki hâkimiyet mücadelelerini ve riskleri de getiren siber uzay kavramı; düşük maliyetli fakat büyük çaplı maddi ve manevi hasarlara olanak sunabilen siber saldırıları da beraberinde getirmiştir (Eren, 2017, s. 47). İnternetin gelişiminin ilk yıllarında küçük hackerlere itibar kazandırmak amacıyla gerçekleştirilen siber saldırılar, son yirmi yılda hızla gelişerek suçluların finansal kazanım elde etmek için, hacktivistlerin siyasi hedeflerini ilerletmek için, devletlerin ise güvenlik politikalarını gerçekleştirmek için kullanmaya başladıkları bir hal almıştır (Ünver, 2018, s. 28).

Siber saldırılara başvurulmayı çekici kılan birçok husus bulunmaktadır: Siber uzayın doğasından ve karmaşık yapısından ileri gelen bu hususların ilki (1) İlişkilendirme Sorunu dediğimiz hususdur. Burada saldırının hangi unsurla ve kimlerle bağlantılı olduğunu açığa çıkarma güçlüğü bulunmaktadır. Diğer bir husus ise (2) Coğrafi Mesafenin İlgisizliği (Dünyanın Her Bir Tarafından Saniyeler İçerisinde Yapılabilirliği) hususudur. Burada saldırının dünyanın her bir tarafından saniyeler içerisinde yapılabilirliği söz konusudur. Hususlardan bir diğeri ise nispeten (3) Düşük Maliyetlerle Gerçekleştirilebilirliğidir.

Almanya Bilgi Güvenliği Federal Ofisi, siber saldırıları, "siber uzayda bulunan araçlar, hizmetler veya uygulamalar aracılığıyla siber uzayda gerçekleştirilen ve bu süreçte, siber uzayın saldırının kaynağı, hedefi veya ortamı haline gelebildiği saldırılar" olarak tanımlamaktadır (Germany Federal Office for

Information Security-BSI). Yeni Zelanda'nın Siber Güvenlik Stratejisi'nde ise "bilgisayar tabanlı bir sistemin işlevini baltalama, tehlikeye atma, bilgiye erişme veya da bireylerin çevrim içi hareketlerini izinleri olmadan izleme girişimi" olarak tanımlamaktadır (New Zealand's Cyber Securıty Strategy 2011, s. 12).

Siber saldırı çeşitleri; küçük ölçekli e-posta dolandırıcılığı, verilerin bütünlüğünü veya altyapının işleyişini aksatma, kullanılabilirliklerini kısıtlama veya da kesintiye uğratma, bağlantılara veya sunucu servislerine aşırı yüklenme, yetkisiz (izinsiz) okuma, silme veya değiştirme aracılığıyla bilgilerin orijinalliğini ya da gizliliğini riske atma şeklinde olabilir (National Strategy for the Protection of Switzerland Against Cyber Risks, 2012, s. 9).

ICT'lere artan bağımlılık devletin ve vatandaşlarının siber saldırılara karşı savunmasızlığını artırmaktadır. Bu tür saldırılar yeni bir savaş türü olabileceği gibi, bir suçlunun ekonomik ya da herhangi bir nedenle toplumu istikrarsızlaştırmak için başlatmış olduğu bir saldırı türü de olabilir. Devlet kurumlarının stratejik kuruluşların ve devletin temel işlevlerini sağlayan şirketlerin ICT'lerine izinsiz girişler ve stratejik bilgi sızıntıları devletlerin stratejik çıkarlarını tehlikeye atabilir (Cyber Security Strategy of the Czech Republic for the 2011-2015 Period, 2011, s. 4). Siber güvenlik alanındaki gelişmelerin ne kadar hızlı olduklarını ve ne kadar çeşitliliğe sahip olduklarını gösteren çok sayıda örnek vardır. ICT yapılarına karşı yapılan saldırılar giderek daha sofistike ve daha kapsamlı hale gelmektedir. Farklı yöntemlerden faydalanır ve çeşitli hedefleri amaç edinirler. Saldırganların doğası ve motivasyonu de değişiklik gösterir. İyi organize olmuş saldırılar, devletin işleyişi için hayati öneme sahip olan CI unsurlarını hedef haline getirirler. ICT'ler günlük yaşamın birçok önemli alanına yerleştikçe kendileri bir CI unsuru halini almışlardır (Maurer ve Morgus, 2014, s. 69).

Siber saldırıların pratikteki boyutuna değinecek olursak burada devletlerin birbirlerine ciddi zararlar verebilme potansiyellerinin olduğunu görebiliriz. Stratejik ve Uluslararası Çalışmalar Merkezi'nin başkan yardımcı olan James Andrew Lewis'in yazdığı rapora göre, istihbarat ve askeri yönden gelişmiş askeri güçlere sahip birbirine düşman olan ülkeler birbirlerine zarar verebilme potansiyeline sahiptirler. Çok sayıda ülke askeri siber güç edinmiş durumdadır. Burada ABD ve

onun en tehlikeli rakipleri olarak da siber alandaki gelişmiş yeteneklerini ABD'ye göre "düşmanca" bir niyetle birleştirmiş olan Rusya ve Çin öne çıkmaktadır. Bu ülkeler ABD'nin siber alandaki açıklarını kullanarak askeri, ekonomik ve teknolojik hegemonyasını kısıtlamak için siber saldırıları askeri amaçla kullanabilecek kabiliyete ve hazırlığa sahip muhaliflerdendir (Rakhmanova, 2018, s. 56).

Siber saldırılar, önceki zamanlarda da yaşanmış olmalarına rağmen özellikle iletişim ve bilişim teknolojilerinin kullanıldığı 11 Eylül saldırıları ve ardından da 2007 Estonya saldırılarıyla birlikte uluslararası toplumda farkındalığı arttırmış ve devletlerin güvenlik politikalarının merkezinde kendine yer edinmiştir (Kurnaz, 2016, s. 69). 2010 yılında İran'a karşı gerçekleştirilen Stuxnet saldırıları; uluslararası organizasyonlar ve ülkeler açısından ciddi endişelerin ortaya çıkmasına, bunların siber güvenlik politikaları oluşturmaya başlayıp buna daha fazla ağırlık vermelerine ve siber ordular kurarak da savaş maliyetlerini düşürmeleri hedeflerinin ortaya çıkmasına sebebiyet vermiştir. Buna ek olarak Rusya tarafından Kırım'a yöneltilen Hibrit Savaş uygulamalarında kullanılan siber yöntemler; devletlerin karşı karşıya kaldıkları ve gittikçe de artan şekilde karşılaşabilecekleri bir durum olmasından dolayı incelenmesinin, yeni fikir ve güvenlik politikalarının ortaya çıkarılmasının gerekli olduğu bir alandır (Akyeşilmen, 2016, s. 9).

Küreselleşme ve teknolojik gelişmelerin artmasının sonucu olarak iletişim ve bağlantılılık yönünden meydana gelen sıkı ilişkiler iyi yönlerinin yanında, güvenlik alanında görülebileceği gibi tehlikeli durumları da ortaya çıkarmıştır. Çoğunlukla internet üzerinden yapılan saldırılar olarak gerçekleşen siber saldırıların (Yılmaz: 2017, s. 29) ne çeşit program ve donanımlarla yapılacağı, başka bir söylemle hangi tür enformasyon/veri işleme unsurlarının siber silahlar şeklinde nitelenebileceğiyle ilgili olarak; siber silahların çeşitlilik arz edebileceğini, Stuxnet örneğinde olduğu gibi spesifik bir hedefe odaklanan özel yazılımlar şeklinde de tasarlanabildiklerini görebiliriz. Siber uzayın silahlandırıldığı bir dönemde devletler de artık siber müdahale araçları olarak gelişmiş siber saldırı yöntemlerini ve silahlarını geliştirme yoluna gitmektedirler (Darıcılı, 2018, s. 320).

1.2.1. Teknik Tabanlı Saldırılar

1.2.1.1. Virüsler (Viruses)

Girdikleri sistemlerin klasörlerinde değişiklikler meydana getirerek işlemez duruma getirebilme, hoş karşılanmayan görüntülerin ekranlarda belirmesine sebep olabilme (Samet ve Aslan, 2018, s. 228) ya da veriler üzerinde değişiklikler yapabilme gibi özelliklere sahip belirli bir amaca yönelik olarak hazırlanmış olan kod parçalarına virüs denir (Aslay, 2017, s. 26). Başka programlara bağımlı olup yerleşebileceği bir programa ihtiyaç duyan ve kendi kendine çoğalabilen bir programdır. İçinde gizlendiği programın çalıştırılmasından ya da dizgede istenilen bir başka faaliyetin yapılmasının ardından farklı yazılımlara bulaşır. Genelde faydalı bir yük içeren virüslerin yararlı yüklerinin yanı sıra verilerin bozulması veya ortadan kaldırılması şeklinde hasar verici özellikleri saldırganlar tarafından programlanabilmektedir. Virüsün bağlı olduğu dosya veya program açılmadığı veya çalıştırılmadığı sürece bilgisayarda var olmasına rağmen ona zarar veremez (Türkay, 2013, s. 1188).

Bilgisayarı takip etme, reklam gösterme, şifre çalma ve sistemi çökertme gibi işlevleri olan virüsler, örneğin bir USB bellek üzerindeki bir dosyaya bulaşmışsa USB'nin çalıştırıldığı her bilgisayardaki dosyalara da bulaşır ve böylelikle çoğalır. Özetle virüsler kendiliğinden ağ üzerinden yayılmazlar, çoğalması için taşınmaları gerektir (Akyeşilmen, 2018, s. 77).

Virüslerin küçük gibi görünen zararları toplamda oldukça büyük zararlara neden olmuştur. Buna örnek olarak ise 3 Mayıs 2000'de oldukça kısa bir sürede 55 milyon bilgisayara ulaşan ve bunların yaklaşık 3 milyonuna bulaşan "I Love You" ya da "Love Bug" virüsü gösterilebilir. Bu virüs 8.7 milyar dolarlık bir zarara yol açmıştı (Turhan, 2006, s. 54).

1.2.1.2. Kurtçuklar (Worms)

Solucanlar, bilgisayar ağları arasında kullanıcı yardımına ihtiyaç duymaksızın virüslerde olduğu gibi hızlıca yayılabilen, en büyük özelliği olarak kendini sayısız defa kopyalayabilmesi kabiliyetiyle yüz binlerce kurtçuğun başka bilgisayarlara yayılmasına sebebiyet veren zararlı yazılımlardır (Gürkaynak ve İren, 2011, s. 273).

Kurtçuklar yayılmalarını virüslerin tersine herhangi bir kişinin yardımı olmaksızın gerçekleştirebilirler. Bunların riskli yönleri ise dizgelerde kendilerini kopyalayabilmeleridir. Böylelikle tek kurtçuk yollamaktansa yüzlercesini kopyalayıp yollayabilirler (Türkay, 2013, s. 1188). Bulaştıkları sistemlerde genelde izinsiz girişlere neden olan bu programlar, sistemlerde kendilerini gizleyebilmek için kendi dosyalarını silerler.

Solucanlar genellikle ağlara yönelik DoS saldırıları düzenlemek veya virüs yerleştirmek için back door (arka kapı) olarak bilinen sistem açıkları oluşturmada kullanılırlar (Çelik, 2013, s. 142).

Bilgisayar sistemlerine hem bir virüs gibi davranıp zarar verebilen hem de bir truva atı bırakabilen ağ solucanlarının (Turhan, 2006, s. 53) yaygın olarak bilinenleri Nimda, Code Red, Conficker, MyDoom ve Stuxnet'tir. Son zamanlarda solucan-virüs karışımı şeklinde olan programlar da gözükmeye başlamıştır (Samet ve Aslan, 2018, s. 229).

1.2.1.3. Truva Atı (Trojan Horse)

Yunan mitolojisinde bir hediye şeklinde gözüken fakat gerçekte Truva şehrini elde etmek için tasarlanan ve Odysseus'ın askerlerini içerisinde saklayan tahtadan yapılmış atın ismidir. Günümüzde ise adını siber saldırı ve siber suçların işlendiği, faydalıymış şeklinde gözüken ancak arkasında saklı kodların bulunması sebebiyle bilgi işlem emniyetini zedeleyen bilgisayar programları truva atı adını almışlardır (Turhan, 2006, s. 47).

Genellikle internet üzerinden yüklenen lisanssız ve ücretsiz yazılımlar; online oyun uygulamaları, ileti yazılımları ve e-posta yoluyla yayılan truva atı, kurtçuklardan değişik şekilde dizgeye bulaştığı vakit ne tür bir yazılımla bulaşmışsa o yazılımın çalıştırılmasını beklemeye koyulur ve o yazılım çalıştırılmayıncaya kadar da faal hale gelmez. Bunun yanında bir virüs olmayıp gerçek bir uygulamaya benzeyen zararlı bir programdır (Bozgeyik, 2018, s. 39).

Truva atı; kullanıcının çalıştırmak istediği program gibi davranan, mantık bombasına benzer bir sistemle çalışan (Çelik, 2013, s. 142), legal bir sağlayıcıdan

ulaşan bir klasör, zararsız bir program veya legal bir programmış şeklinde görünen bu türde bir truva atı alan kullanıcının bu truva atını açmasıyla birlikte tuzağa düşülen gerçekte ise içinde barındırdığı zararlı ya da kötü niyetli bir kod ile kendisinde var olan seçilmiş türdeki zararları gerçekleştiren yazılımdır. Truva atları, solucan ve virüslerin aksine, çoğalarak diğer dosyalara buluşmamakta ve kendisini kopyalayamamaktadır. Truva atları sistemdeki dosyaları silme ve bilgileri ortadan kaldırma gibi ciddi zararlara sebebiyet vermektedir (Türkay, 2013, s. 1188).

Bulaştıkları dizgeleri çoğunlukla ağırlaştırdıklarından dolayı truvaların varlıklarının tespit edilmesi ciddi çabalar gerektirmektedir. Truvalar, sistemlerde arka kapılar açma, girdiği sistemlere izinsiz bir şekilde uzaktan erişim imkânı sağlama, bilgisayarda depolanan kritik bilgileri karşı tarafa iletme (Samet ve Aslan, 2018, s. 229-230), sisteme truva atları sayesinde arka kapıdan ulaşan bilgisayar korsanlarına kullanıcıların kişisel bilgilerine/şifrelerine ulaşabilme imkânı sağlama (Aslay, 2017, s. 25), içinde bulundukları dosyaları kontrol edebilme, yerleştikleri bilgisayarların içinde farklı özel kelimeler arayarak o kelimelerin geçtiği dosyaları kopyalayıp başka bilgisayarlara otomatik olarak gönderebilme gibi kabiliyetlere sahiptirler (Gürkaynak ve İren, 2011, s. 273).

1.2.1.4. Bot, Botnet, Zombie (Robot, Köle Bilgisayarlar)

Robot sözcüğünün kısaltılmışı olan “bot” sözcüğünden ve İngilizcede ağ anlamına gelen “net” sözcüklerinin birleşiminden oluşmuş olan botnet (bot+net) sözcüğü, siber güvenlik literatüründe köleleştirilmiş, robotlaşmış veya da başkaları tarafından yönetilen bilişim ağlarına verilen addır. Kullanıcılarının bilgisi olmaksızın kötücül yazılımların yüklendiği, kontrolünün bilgisayar korsanlarının eline geçtiği ve yetkisiz kişilerce tertiplenen siber faaliyetleri gerçekleştirilen ve siber saldırıların olmasına rağmen gerçekleştirilen siber suçun içerisinde yer aldığından dahi bihaber olan donanımlara, sistemlere “zombi bilgisayar” ismi verilir. Siber faaliyet unsurlarının en önemlisi olan zombi bilgisayar ağı saldırıları, uzaktan yönetilebilen enfekte olmuş yüzbinlerce bilgisayar ile komuta ve kontrol sunucularından meydana gelir (Bozgeyik, 2018, s. 42).

Siber saldırı silahlarının en tehlikelisi olarak kabul edilen botnet veya zombi bilgisayar saldırılarındaki en önemli nokta, bilgisayar kullanıcısının bilgisayarının oldukça ciddi suçlarda kullanıldığının farkında olmamasıdır (Öğün ve Kaya, 2013, s. 155). Botnet saldırısı altında bulunan bilgisayar kullanıcısı genelde donanıma zararlı bir yazılım yüklendiğinin farkında değildir (Çelik, 2013, s. 141-142).

Firewall denilen güvenlik duvarlarına ve günümüzde artan bant genişliğiyle birlikte bilgisayarlar rahatlıkla botnetin zombi ordusunun bileşeni durumuna konulabilirler. Botnetler; bir bilgisayara, açık bırakılmış olan bir porttan (kapıdan), sonradan aktifleşecek şekilde bırakılan bir truva atıyla faaliyete geçirilebilirler. Botnetin bileşenleri durumuna getirilen bilgisayarların internetin bir sitesine eş zamanlı olarak yönlendirilmeleriyle botnet saldırısı başlamış olur. Saldırı, bu web sitesinin hizmet veremez hale gelmesiyle sonuçlanır (Öğün ve Kaya, 2013, s. 155).

Bir dizi robotlardan oluşan botnetler, zafiyetli sistem ve bilgisayarlara veriler gönderip onları sonradan yapacakları saldırılarda kullanırlar. Bunun sonucunda sistemler çalışamaz duruma sokulabilir, zombi şeklinde ele geçirilen donanımlardan ciddi veriler kaçırılabilir, ücret karşılığında başka şahıslara verilebilir. DDoS, spamming, sniffing traffic ve spreading new malware gibi saldırılar robotlar tarafından yaygın olarak yapılan saldırılardan bazılarıdır (Samet ve Aslan, 2018, s. 231).

Yasal ve güncel bir güvenlik yazılımı ve işletim sistemi bulunmayan, internette gezinirken kaynağı belirsiz sitelerdeki bağlantılara gelişi güzel tıklayıp buralardan indirmeler yapan, bilgisayarının belli bir sürenin sonunda yavaşladığından yakınan kişilerin bilgisayarının bir zombi bilgisayara dönüştüğü ihtimali yüksektir. Kötü niyetli bilgisayar korsanları, Siber suçun işlenmesi hizmetini bir ücret karşılığında kiraya veren (Cybercrime-As-A-Service) isimli suç hizmetinden illegal web siteleri aracılığıyla zombi bilgisayarlar kiralayabildikleri gibi, bunun yanında saldırı faaliyetlerini de tümüyle taşeron olarak gerçekleştirebilmektedirler. Bu suç hizmetinin 1 saatlik ücreti 2015 yılı rakamları itibariyle 20-40 $ arasında değişmektedir. Zombi bilgisayarları ile yapılan siber saldırıların saldırı kaynağı olarak kullanılan ülkelerin ilk 10'u; ABD, Ukrayna, Rusya, Hollanda, Almanya,

Türkiye, Fransa, Birleşik Krallık, Vietnam ve Romanya'dır (Bozgeyik, 2018, s. 42-43).

Botnet saldırısında kullanılan bir bilgisayar spam faaliyetlerinde, şahsi bilgilerin banka ve internet hesaplarının ele geçirilmesinde, suç unsuru sayılan görüntü ve dosyaların yayılmasında kullanılabilmektedir. Bilgileri ele geçirilen kişinin ismi ve parası kullanılarak oldukça ciddi suçların işlenmesinde kullanılabilir (Öğün ve Kaya, 2013, s. 156).

1.2.1.5. DoS ve DDoS (Hizmet Engelleme-Distributed Denial of Service Attacks)

DoS ve DDoS'un tanımını basit bir şekilde yapacak olursak, kullanıcıların bir sisteme olan erişimlerinin engellenmesi, sistemin hizmet veremez duruma getirilmesi veya da saldırılar sonucunda fiziksel olarak zarar görmüş olan sistemin hizmet sunamaz bir duruma getirilmesidir. Asıl mantığı, sistemin, gerçek hizmet isteklerine yanıt vermesini engelleyecek kadar çok sayıda sahte istek gönderimine maruz bırakılarak (Öğün ve Kaya, 2013, s. 156), sistemin bant genişliğinin işgal edilip devre dışı bırakılmasıdır. Günümüzde oldukça sık karşılaşılan bu saldırı türüne ilk kez 1998'de rastlanılmıştır (Çetin, Gundak ve Çetin, 2015, s. 229).

En fazla tercih edilen siber saldırı türlerinden biri olan Hizmet Dışı Bırakma (Denial of Service – DOS) saldırısının genel özellikleri bunlardır (Bozgeyik, 2018, s. 43):

- ✓ Çoğunlukla Botnet/Zombi Bilgisayar Ağları ile gerçekleştirilir.
- ✓ Yüzbinlerce ve daha fazla zombi bilgisayarlar kullanılabilir.
- ✓ Çoğunlukla itibarı zedeleyerek mali hasarlara uğratmak hedeflenir.
- ✓ Saldırıyı organize edenleri açığa çıkarmak hemen hemen olanaksızdır.

Bilgisayar ve bilgisayar ağlarının olabildiği kadar yavaşlatılmasının hedeflendiği DDoS (Dağıtık Hizmet Aksatma Saldırısı) saldırısının kabiliyetleri bunlardır (Yıldırım, 2018):

- ✓ Sitenin trafiği hedef alınarak siteye olan erişilebilirlik engellenebilir.
- ✓ Bant genişliği hedef alınarak ağda ciddi problemler oluşturulabilir.

- ✓ Programlar aracılığıyla hedef bilgisayarların faaliyetleri sonlandırılabilir.

DoS saldırısı, internete bağlı olan bir sunucunun hizmetlerine gereksiz taleplerle aşırı yüklenilerek geçici veya süresiz olarak aksatılması ve meşru taleplere doluluk gerekçesiyle yanıt verilememesiyken; DDoS saldırısı ise DoS saldırılarının zombi bilgisayarlar veya geniş bir kitle yardımıyla yapılması sonucunda oldukça tehlikeli bir boyuta ulaşmış olma durumunu ifade eder. Her geçen yıl daha kapsamlı bant genişliğini işgal ederek etkisini arttıran DDoS saldırılarının, siber korsanlar tarafından daha fazla kullanıldığı görülmektedir (Yalman, 2018, s. 263).

2015-2016 yıllarında gerçekleşen DoS faaliyetlerini baz alan Verisign 2016 İkinci Çeyrek Hizmet Dışı Bırakma Saldırı Eğilimleri Raporu DDoS saldırılarıyla ilgili birtakım vurgularda bulunmuştur (Bozgeyik, 2018, s. 44):

- ✓ Önceki yıllara göre daha büyük çapta ve daha sık aralıklarla yapıldığına,
- ✓ Ortalama saldırı boyutunun %214 daha büyük boyutta gerçekleştiğine,
- ✓ Saldırıların %64'ünün birden fazla saldırı yöntemi ve tekniği kullandığına,
- ✓ %45'inin bilişim teknolojileri ve bulut bilişim teknolojilerini,
- ✓ %23'ünün mali sistemleri,
- ✓ %14'ünün de resmî kurumları hedeflediğini vurgulamıştır.

DoS saldırısının özelliği, daha ileri teknolojili bir ağ veya bilgisayarlara karşı daha sınırlı kaynaklarla dahi düzenlenebilmesidir. Saldırganlar, eski ve yavaş bir bilgisayar ve modemle oldukça gelişmiş teknolojili ağı ya da bilgisayarı etkisiz bırakabilir. Bunun yanında bilgi akışı sisteminin çok sayıda mekân ve bilgisayardan kaynaklanmasından dolayı bir DDoS saldırısını durdurmak güçtür (Türkay, 2013, s. 1187). DDoS saldırılarının engellenebilmeleri için içerik filtrelerinin veya kurum içi güvenlik duvarlarının kullanılması gerekmektedir (Yıldırım, 2018).

DDoS saldırılarının en meşhuru 2007 Estonya saldırılarıdır. Rusya kaynaklı olan bu saldırılar dünyanın en dijitalleşmiş ülkesi olan Estonya'nın bankalarının, bazı devlet yayın organlarının ve devlet dairelerinin hizmet sağlayamaz hale gelmesine sebep oldu. Bununla birlikte Estonya saldırısının uluslararası ilişkilerde siber uzayın

bir güvenlik sorunu haline dönüşmesinde de önemli rolü olmuştur (Akyeşilmen, 2018, s. 78).

1.2.1.6. Casus Yazılımları (Spyware)

Casus (köstebek) yazılımların herkesçe kabul edilen bir tanımının bulunmamasıyla birlikte pratikteki eylemlerinden yola çıkılarak böyle bir tanımlama yapılabilir; kişinin onayı ve bilgisi olmaksızın bilgisayarının ayarlarını değiştiren, bilgisayarından veri toplayan, topladığı verileri kullanan ve başkasına ileten yazılımlardır. Bir başka ismi snoopware (burun sokan yazılım) olan casus yazılımların, solucan ve virüslerden ayrılan yönü bulaştıkları sistemlerde kendi kopyalarını oluşturmalarının dışında daha fazla yayılmaya ihtiyaç duymamalarıdır. Casus yazılımı saldırısı, kişisel gizliliğe yönelik düzenlenen kötü amaçlı yazılım saldırılarının en tehlikelisidir. Maksadı, hedef haline getirdiği dizgeye gizlenerek istenilen verileri toplamaktır (Bozgeyik, 2018, s. 40).

Ücretsiz paylaşılan yazılımlara veya da web sitelerine gömülerek yayılan casus yazılımlarına yaygın olarak bilinen örneklerinden Gator, Cydoor, CoolWebSearch ve BlazeFind gibileri gösterilebilir. Son zamanlarda hem sayı olarak artış gösteren hem de şekil değiştirerek karşımıza çıkan kötü amaçlı yazılımlar; siber saldırının şiddeti ve miktarı açısından da artışlar meydan getirmiş ve küresel boyutta kalıcı ve hedef odaklı siber saldırı yazılımlarının yapılmasına olanak sağlamıştır. Birden fazla zararlı yazılımın (arka kapı, truva atı, virüs, solucan gibi) bir arada kullanıldığı siber saldırı olayları ise bu türden saldırıların tespitini ve engellenmesini zorlaştırmış ve yeni savunma yazılımlarının geliştirilmesinde yeni nesil kötü amaçlı yazılımların göz önünde bulundurulmasını gerekli kılmıştır (Samet ve Aslan, 2018, s. 232).

Genellikle eş takip etme yazılımı, ebeveynler için çocuk izleme yazılımı gibi isimlendirmelerle piyasaya sürülen ve çoğu kez bedava deneme sürümlerine enjekte edilmiş halde bulunan casus yazılımlar, kullanıcıların bilgisayarlarına kurmalarıyla birlikte aktif hale gelmiş olurlar. Kurulmaları esnasında dikkatli okunmaları halinde çoğu kez gerekli uyarıların yapıldığı görülecektir. Fakat bu uyarılar, uzun kullanıcı sözleşmelerine sahip bu tür programların içerisinde bulunan hukuki terimler arasında

dikkatlerden kaçar ve sonuç olarak kullanıcının rızasıyla bilgisayarına kurulmuş olur. Bu tarz yazılımlar kurulma esnasında hızlı ve gelişmiş olmak üzere iki seçenek sunmaktadır. Fakat gelişmiş seçeneğin ayarlanmasının ve okunmasının zahmetli olacağından hareketle, kullanıcılar hızlı seçeneği tercih etmektedirler. Kullanıcılar tarafından gösterilecek dikkat ve özen ile birçok sorunun engellenebilmesi olanaklıyken, kullanıcının kişisel bilgileri kendi rızasıyla başkalarının eline geçmiştir (Öğün ve Kaya, 2013, s. 158-159).

Yapılan araştırmalara göre ABD'deki bilgisayarların %90'ının, şirket bilgisayarlarının %20-%50'sinin, dünya çapındaki PC'lerin ise %69'unun casus yazılımlara maruz kaldığı öne sürülmüştür. Bunlardan korunmak için ise (Yeşilmen, 2018, 79):

- ✓ Anti-virüs ve anti-spyware programları kullanılmalıdır.
- ✓ Kullanılan işletim sistemi, yazılım ve browserın güncelliğine ve güvenlik önlemlerinin ihmal edilmemesine dikkat edilmelidir.

1.2.2. Sosyal Tabanlı Saldırılar (Sosyal Mühendislik)

Yalan söyleyerek ve karşı tarafı ikna ederek kişilerin güvenini kazanma üzerine kurulan bilgi toplama sanatıdır (Aslay, 2017, s. 26). Kötücül uygulamaların cihazlara yüklenebilmesi için kullanıcıları kandırmaya odaklı sosyal mühendislik teknikleri kullanılmaktadır. Bu teknikler kısaltılmış hiper bağlantı, bir mesaj içerisindeki link ya da yasal bir uygulamanın değiştirildikten sonra tekrardan paketlenmesi şeklinde olabilmekteler. INTERPOL'ün yaptığı bir araştırma sonucuna göre dünyada en fazla kullanılan sahtekârlık yöntemi sosyal mühendislik yoluyla yapılan dolandırıcılıktır. İngiltere Ulusal Dolandırıcılıkla Mücadele Bürosu'nun araştırmasını göre ise Ocak 2014-Ocak 2015 tarihleri arasında sosyal mühendislik tarzı olaylarda %21'lik bir artışın olduğu görülmüştür (Alkan ve diğ., 2018, s. 319).

Bilgisayarların, ağların veya da sistemlerin suistimal edilmesi yerine insanların duygularını istismar ederek zayıflık ve zafiyetlerini kullanıp onları kandırmaya dayanan sosyal mühendislik, günümüzde bilinen dört önemli saldırı türlerinden biridir (Sağıroğlu, 2018, s. 32).

Farkındalık ve bilgi eksikliğinin bulunması halinde insanın bulunduğu etki alanı ve konum yönünde bilgi güvenliği problemleri açığa çıkaracağı aşikârdır. Bütün altyapı, teknoloji, kanun, politika, standartlar ve denetim alanlarının başarasının insan tarafından gerçekleştirilmesi günümüz insanını unsuru olduğu bilgi güvenliğinden çıkarmış güvenliğin esas bileşeni ve bütün unsurlarına tesir eden bir duruma getirmiştir. Dolayısıyla günümüzdeki saldırganların, teknolojik önlemleri aşmak yerine maliyetsiz ve daha kolay bir yöntem olan sosyal mühendislik yöntemini tercih ederek insan bileşenini zafiyete uğratması bu tezi doğrular niteliktedir (Erol ve Sağıroğlu, 2018, s. 112).

1.3. SİBER ÇATIŞMALAR

Siber uzaydaki gelişmeler neticesinde konvansiyonel istihbari faaliyetler gittikçe yerini özel istihbari faaliyetlere devrederken, savaş alanlarına da değişik bir perspektif kazandırmıştır. Siber savaş, ülkelerin kritik sektörlerinin bilgi altyapılarına zarar vermeyi amaç haline getirir. Bu bağlamda siber bağımlılıkları üst seviyede olan modern ülkelerin ulusal güvenliklerine yönelik gerçek bir tehdit oluşturmaktadır. Konvansiyonel silahlar kullanmaksızın görünmeyen saldırılar şeklinde gerçekleştirilebilmesi, az maliyetle büyük etkiler oluşturabilmesi ve asimetrik özelliği sebebiyle bireylerden karmaşık ulusal organizasyonlara kadar geniş bir yelpazede bulunan tehdit kaynağının tespit edilememesi gibi durumlar siber savaşın önemini daha da arttırmaktadır (Bayraktar, 2014, s. 119).

Siber savaşlar, insanoğlunun kara, deniz, hava ve uzay savaşlarının ardından beşinci harp sahası şeklinde kabul edilmişlerdir. Siber savaş, düşmanı ruhsal yönden çökertmek amacıyla bilişim teknolojilerine bağlı bulunan dizgelerine internet üzerinden görünmez ve izinsiz bir şekilde ulaşmak, denetimi elde ederek verileri yanlış yönlendirmek veya çalmaktır. Bir ülkenin, diğer bir ülkenin bilişim ağ ve sistemlerine girerek kesintiler ya da hasarlar oluşturmasıdır. İçerisinde çok sayıda teknik/yöntem bulunduran siber savaş, manipülasyon, casusluk, iletişimin kontrol altına alınması, propaganda, siber bombalarla sabotaj, dolandırıcılık gibi çok sayıda savaş enstrümanı ve yöntemine sahiptir (Ada, 2018, s. 28). Aşağıda bu saldırıların bazılarına yer verilmiştir.

1.3.1. Moonlight Maze (1989-2003)

1999'da ABD'de FBI'ın Moonlight Maze (Ayışığı Labirenti) isimli soruşturması, bilgisayar korsanlarının hükümet bilgisayarlarındaki gizli bilgilere ulaşma ve bazı siber casusluk durumlarında başarılı olma teşebbüslerinin ABD tarafından resmi olarak doğrulandığı birkaç durumdan bir tanesidir. FBI ve Pentagon yetkililerine göre Rus devleti destekli Rus bilgisayar korsanları tarafından yapılan ve ABD teknolojisini elde etme istihbarat kampanyası olarak tanımlanan bu olayda Savunma Bakanlığı bilgisayarlarına bir yıldan fazla bir süre boyunca nüfuz edilerek büyük miktarda kritik bilgileri çalınmış; NASA, askeriye müteşebbisleri ve askeriyeyle bağlantısı bulunan sivil üniversitelere saldırılar da amaçlanmıştır. Savunma Bakanlığı'na ait bilişim teknolojilerinde hiçbir hasarın raporlanmadığı bu olayda NASA'da Genel Denetmen olan Roberta Gross: "Zararın ne olduğunu anlatmak zor… Sistemi kapatmadılar. Dosyalardaki listeleri alıp, kişilerin yönetiminde nelerin olduğunu görmek istediler." şeklinde bir beyanat yapmıştır (Türkay, 2013, s. 1181-1193).

ABD'nin yapmış olduğu teknik takip sonucunda Moskova'ya iletildiği saptanan ve Rus bilgisayar korsanları tarafından çalındığı düşünülen bilgilerin değeri açık arttırmaya çıkartıldığında 100.000.000'larca dolarla ölçülebilir büyüklüktedir (Kara, 2013, s. 42-43). ABD, bu olayın izini eski Sovyet birliğine ait bir bilgisayara kadar takip edebilmiş, fakat Rusya ise bu olayla hiçbir ilgisinin olmadığını söylemiştir (Siberkuvvet, 2015).

Üç farklı ülkeden araştırmacının incelemeleri sonucunda Moonlight Maze'in evrimleşerek Rusça konuşan; Snake, Uroburos, Krypton ve Venomous Bear adlarıyla bilinen ve 2007'den beri faal olduğu düşünülen Turla isimli bir faile dönüştüğü tespiti yapılmıştır.

1.3.2. Çin'in Siber İstihbarat Faaliyetleri (2005-2013)

Çin İstihbarat Servisi, Merkezi Haberalma Teşkilatı (Central Intelligence Agency-CIA) veya Devlet Güvenlik Komitesi (Komitet Gosudarstvennoy Bezopasnosti-KGB)'ninki kadar bir popülariteye sahip olmasa da karşı istihbarat bağlamında en çok da siber istihbaratta fazlasıyla etkili ve başarılıdır. Coğrafi

sınırlılıkları ortadan kaldıran siber teknolojilerin kullanımıyla faaliyetlerde bulunan Çin İstihbaratı, ABD başta olmak üzere ülkelerin dikkatlerini üzerine çekmiştir. 2013'te PLA (Halk Kurtuluş Ordusu) başkanı Qi Jianguo'nun Çin Komünist Partisi Merkez Parti Okulunun haftalık resmî gazetesindeki yazısında siber güvenliğin ekonomik-toplumsal operasyonlarla ilişkili bir bağımsızlık meselesi olduğunu ve Batı'nın da gerçekte "internet özgürlüğü" mottosuyla yeni bir hegemonya inşa ettiğini söylemesinin ardından siber güvenlik konusunun artık teknik bir meseleden çok, stratejik bir öneme evrildiğini göstermiştir. PLA'nın New York Times'in bilgisayar sistemlerini 2012-2013 yılları boyunca hecklenmesinin dünyanın gündemine düşmesinin (Çelik, 2017, s. 69-70) ardından Amerika'nın başkanı Obama ile Çin Başkanı Xi Jinping'in bu konuda görüşmek üzere bir araya gelmelerinin ardından iki devletin iktisadi çıkarlar elde etmek için ticari sırlar dahil, fikri hakların sanal çevrede ele geçirilmesi faaliyetlerini onaylamayacakları üzerinde anlaştıkları açıklanmıştır. ABD iktisadi maksatlı siber casusluk saldırılarında bulunmadığını ileri sürerken, Batılı haber alma kuruluşları ise Çin'in uzun zamandır bu faaliyetlerde bulunduğunu ileri sürmektedirler (NTV, 2015)

İç/dış ve karşı istihbarat (kontrespiyonaj) konularında yetkili olan The Guojia Anquan Bu/Ministry of State Security (MSS) kurumunun siber kapasitesi bilinmemekle beraber, özellikle Çin'in düşman olarak tanımladığı ülkelerin ekonomik ve politik dokümanlarına/sırlarına vakıf olduğuna dair bir konsensüs söz konusudur (Çelik, 2017, s. 71). Çin, ABD'ye yönelik bir taraftan askeri diğer taraftan da ekonomik amaçlı istihbarat faaliyetleri yürütmektedir. Askeri alandaki çalışmaların başlıca amacı Amerika'nın ileri askeri teknolojisinin eksik yönlerini belirleyip buna yönelik önlemlere başvurmak ve Çin'in askeri modernizasyon sürecini hızlandırmaktır. Bunun yanında Çin, Amerika'yla askeri yönden yarışabilmek için teknoloji casusluğu faaliyetleri yaparak gerekli kilit teknolojileri ele geçirmeyi hedeflemektedir. Çin tarafından kendisi için "kırmızı bülten" ile arama çıkartılan karşıt iş adamı Guo Vıngui'in Amerika medyasında yankı bulan söylemlerine göre, teknoloji casusluğuna odaklanan 25.000 Çinli haber alma ajanı Amerika'da çalışmaktadır. Beyaz Saray Ticaret ve Üretim Politikaları Ofisi'nin haziran ayında yayımladığı "Çin'in Ekonomik Saldırılarının ABD ve Dünyanın Teknolojileri ve Fikri Mülkiyetini Nasıl Tehdit Ettiği" isimli raporunda Devlet

Güvenlik Bakanlığının Çin içerisinde 50.000'den çok Çin dışında ise 40.000 haber alma personelinin bulunduğunu; Çin'in sadece ticari hırsızlık alanında dünyaya olan maliyetinin ise senelik 180-540 milyar dolar civarlarında olduğu şeklinde beyanatlar yer almaktadır (Hürriyet, 2018).

Çin kaynaklı siber suç örneklerinden bazıları şöyledir: Çin Telekomünikasyon Şirketi Huawei, Avusturalya tarafından milli güvenliğe tehdit gerekçesiyle yasaklanmıştır ve 2012 yılında Economist tarafından yayınlanan raporda da Huawei'nin, Çin Hükümeti adına siber hırsızlık faaliyetlerinde bulunduğu ileri sürülmüştür (Çelik, 2017, s. 72). Bir diğer örnek ise 2001 Nisan'ında Çinli bir internet korsanı grubunun Çin ile Amerika hava yolu anlaşmazlığı sebebiyle ABD'nin 1200 web sayfasını hizmet dışı bırakması/saldırıya uğratması sonucunda Beyaz Saray, ABD Hava Kuvvetleri, enerji dairesi ve birçok şirketin bilgi teknolojileri hasara uğratılmıştır (Özalp ve Asker, 2017, s. 7).

Çin ile yapılan karşılıklı siber casusluk suçlamalarının başlıcaları aşağıdaki gibidir (Alagöz, 2013):

- ✓ Son zamanlarda New York Times, Washington Post, Microsoft, Coca-Cola, Apple, Facebook ve Twitter'a yapılan siber saldırıların Çin tarafından yapıldığına dair çok sayıda iddia bulunmaktadır. Siber casusluk olaylarını araştıran Virginia merkezli Mandiant firması, Çin ordusunun Ünite 61398 isimli gizli bir kolunun siber casuslukla ilgilenen bir birim olduğundan şüphe edildiğini ve tüm dünyada 141 terabaytlık veri çalmış olabileceğini belirtmiştir.
- ✓ Obama, son ulusa sesleniş konuşmasında finans kurumları, elektrik şebekesi, ve hava trafiği kontrol merkezine düzenlenecek saldırılara dikkatleri toplayarak siber tehditler üzerinde durmuş ve siber ajanları barındırıp onlara göz yuman Çin gibi ülkeleri uyararak ABD'nin neler yapabileceğinden bahsetmiştir.
- ✓ ABD Ulusal Güvenlik Ajansı (NSA)'ndan Joel Brenner'in iddiasına göre, Çin ordusu ABD'nin askeri/teknolojik sırlarını çalmak ve idari ve mali kurumlarına hasar vermek için 30.000 siber ajan ile 150.000 siber güvenlik uzmanı yetiştirmiştir.
- ✓ Çin'in Patriot füze sistemi, Black Hawk helikopteri ve F-35 taarruz uçağı gibi ABD'nin üst düzey silah sistemleri ve kurumsal sırlarını ele geçirmek için siber

saldırılar yaptığını, en az 10 silaha ait bilgilerin Çinli korsanlar tarafından çalındığı ve bunun da Çin silah teknolojisine 25 yıl kazandırdığı öne sürülmektedir. Sonrasında Guardian ve Washington Post gazeteleri Obama'nın Başkanlık Politika Direktifi 20 belgesini imzalayarak siber savaşa hazırlanma komutunu verdiğini açıklamışlardır.

- ✓ Pentagon'un 2013 yılı raporuna göre, 2012'de Amerikan hükümeti de dâhil olmak üzere dünya çapındaki çok sayıda bilgisayara, bazıları Çin hükümeti/ordusu tarafından gerçekleştirilen siber saldırılar yapılmıştır. ABD Savunma Bakanlığına göre Pentagon'un yayımladığı yıllık rapordaki siber casusluk olaylarının %90'ı Çin kaynaklıdır. ABD, Çin'i uzun süre siber casuslukla bağlantılı olduğu konusunda doğrudan suçlamamıştı.
- ✓ Rapora Göre Çin'in temel amacı, endüstriyel teknoloji sırlarını elde etmek; Amerikalı siyaset adamlarının düşüncelerini, Amerika'nın savunma sistemini, askeri kapasitesini ve lojistiğini öğrenmek; Amerikan uydularını etkisiz hale getirmek için elektronik savaş kabiliyetini artırarak aşamalı olarak Pasifik'teki Amerikan askeri varlığını Çin kıyılarından uzaklaştırmaktır.
- ✓ Bu iddialar üzerine Çin Dışişleri bakanlığı sözcüsü Hua Çunying tepkide bulunarak; Çin'in daima her türlü siber saldırının karşısında olduğunu, internet güvenliği konusunda ABD ile kapsamlı/yapıcı bir diyalog yürütmeyi arzu ettiklerini, zira taraflar arasındaki işbirliği çabalarını baltalayıcı bu tarz temelsiz suçlamalara/spekülasyonlara karşı olduklarını belirtmiştir.
- ✓ Mayıs 2011'de Çin, internet ağlarının ancak dış saldırılardan korunması için "süper elit siber savaşçı birliği"ne sahip olduğunu belirmiştir. ABD'nin ileri teknoloji silah sistemlerine yönelik siber casusluk olaylarıyla ilgili olarak, bu programları güvende tutmanın yolunun onların online erişime açılmaması ve gizli tutulması gereken şeylerin internetle bağlantılarının olmaması gerektiği vurgusunu yapmaktadır.

Çin'e yöneltilen diğer suçlamalar da başında çipler, çiplere yerleştirildiği öne sürülen casus yazılımlar ve tedarik zinciri sunucularına sızıldığıyla ilgilidir (Hürriyet, 2018):

- ✓ ABD'li yayın kuruluşu Bloomberg'in haberine göre, 2015'ten beri ABD'li şirketlerin bilgisayarlarına yerleştirilmiş "pirinç tanesi" boyutundaki çipler aracılığıyla Çin tarafından hacklenmişlerdir.
- ✓ Çinli ajanların, Apple ve Amazon'un da dahil olduğu 30 ABD şirketi sitesinin web sağlayıcılarına nüfuz ettiği de öne sürülmektedir.
- ✓ Çin'in, halihazırda üretim hatlarını Çin'e taşımış olan çip, işlemci ve ana kart üretici şirketlerinden hem ticari fayda sağladığı hem de bu ürünlerin içerisine yerleştirdiği casus programlarla tedarik zincirine müdahalede bulunduğu düşünülmektedir. Bu şekilde Çin'in, Çin'de üretilen ABD menşeli kartlar ve çiplerin ABD'nin stratejik kurumlarına sağlanması yöntemiyle hem teknoloji casusluğu yapmış oluyor hem de istihbarat faaliyetlerinin finanse edilmesini sağlamış oluyor.

Bu analizlerin neticesinde ABD'nin kurban, Çin'in saldırgan olduğu anlamı çıkarılabilirse de gerçek oldukça farklıdır. Bizler kamuoyuna açıklanan, tespit edilen saldırıları biliyoruz. Burada konu Çin'in siber istihbarat faaliyetleri olunca da ağırlık ona verilmiştir. Oysa hem savunma hem saldırı konularında en büyük siber gücün ABD ve siber istihbarat konularında da en aktif gücün yine ABD olduğu bilinmektedir. Edward Snowden olayı da yer kürenin en büyük kulağının NSA olduğunu ispatlamaktadır. ABD ve müttefikleri ile Çin arasında vuku bulan siber istihbarat faaliyetlerinin gelecekte güvenliği ve ekonomiyi daha da derinden etkileyecek siber saldırıların/operasyonların, daha da uzun süreye yayılacak olan siber istihbarat faaliyetleri sonucunda küresel çatışma eğilimlerinin büyük oranda etkileneceğinin ve bu çerçevede şiddet içermeyen çatışmaların artacağının habercisi gibidir (Yeşilmen, 2018, s. 235-236).

1.3.3. Estonya'ya DDoS Saldırıları (2007)

''Cyber Storm'' adlı CI elemanlarının hedef alındığı ilk tam ölçekli siber güvenlik tatbikatı 2006'nın Şubat'ında ABD'de yapılmıştı. Bu tatbikattaki senaryolar bu kez 2007'nin Nisan'ında Estonya'da gerçekleşti (Ada, 2018, s. 30). Siber savaşlar gittikçe artan bir şekilde devletlerin ilgi alanına girmiştir. Rusya, Çin, ABD, Fransa, İngiltere ve Almanya gibi devletler bu konuyu ciddi bir şekilde alarak araştırma ve geliştirme faaliyetlerini ilerletmektedirler (Alagöz, 2013).

İkinci Dünya Savaşının ardından Sovyetler tarafından Nazilerin işgalinden kurtarılmış olan Estonya, 1989'da Sovyetler Birliği'nin dağılmasıyla yeniden bağımsız bir devlet olmuştur. Estonyalılar 50 yıl boyunca Sovyetler Birliğinin baskısı altında kalmıştır. Estonya'nın başkentine Ruslar tarafından, Estonyalıların çoğunluğuna bu baskıcı 50 yılı anımsatan Bronz Kızıl Ordu Askeri Heykeli dikilmişti. Bu heykeli kaldırmak isteyen Estonyalılar ile etnik Ruslar arasında 26 Nisan 2007'de ismi tarihe "Bronz Gecesi" olarak geçen bir gerginlik yaşanmıştır. Sonraki günlerde en çok kullanılan web sayfaları çökmüş ulusal bilgi sistemlerine, web sağlayıcılarına ciddi hasarlar verdirilmiş, ticaret ve iletişim durma noktasına varmış, ülkenin en prestijli bankası olan Hansa Bank tümden etkisiz duruma getirilmiştir. Dahası, Estonya Meclisinin, tüm bakanlıkların, siyasi partilerin, altı tane büyük haber kuruluşunun iletişim konusunda uzmanlaşmış firmalar ile en büyük bankaların siteleri de saldırıya maruz kalmışlardır (Kara, 2013, s. 46-47), bilhassa bankacılık sistemi bundan etkilenmiştir (Göçoğlu, 2018, s. 82-83). Saldırıların yapıldığı üç haftalık süre zarfında, Estonya'daki sunucular ve yönlendiriciler de dâhil 178 ülkeden neredeyse 1 milyon bilgisayar hedef haline gelmişti. Estonya devleti web sitelerinin trafiği 400 katlık bir çoğalma göstermişti. Bu da faaliyetlerin tasarlanmış ve koordineli olduğunu göstermiştir (Ada, 2018, s. 30).

Saldırıya karşı anında pozisyon alan Estonya hükümeti, sistemlerini saatler içerisinde düzeltebilmiştir (Göçoğlu, 2018, s. 83). Bunun üzerine Savunma Bakanı Aaviksoo saldırıların, botnetler aracılığıyla yapılan ne ilk ne de en büyük saldırı olduğunu, ancak temel elektronik altyapının tamamına yakınının hedeflendiğini ve tüm halkı etkileyip ulusal güvenliği tehdit eden ilk botnet saldırısı olduğunu ifade etmiştir (Aytekin, 2015, s. 20-21). Sonuçta Estonya'nın DNS hizmetlerine müdahale edilerek ülkede kaosun baş göstermesine ortam hazırlanmıştır (Ada, 2018, s. 30).

Onbinlerce zombi bilgisayar tarafından saldırıya maruz bırakılan Estonya, DDoS saldırılarıyla karşı karşıyaydı. Uzman ekipler tarafından alınan tedbirlere karşın saldırıların yapıldığı zombi bilgisayarlar ana bilgisayarlar tarafından tekrardan programlanarak alınan yeni tedbirlere yeniden adapte edilmişlerdir. Tespitler sonucunda ana bilgisayarların Rusya'da olduğu, saldırıların dünyanın her tarafından yapılmasının yanında Rusya devlet sunucularının da saldırıların ev sahipliğini yaptığı

ve programın Kiril alfabesiyle yazıldığı açığa çıkarılmıştır. Estonya'yı siber hedef haline getiren şey internete dayalı bir çalışma sisteminin varlığı ve "e-devlet"in geliştirilmesinde öncü bir ülke olmasıdır (Kara, 2013, s. 47-48). E-devletin en etkin kullanıldığı, bankacılık hizmetleri ile devletin internet üzerinden yürütüldüğü, parlamento seçimlerinin bile internet üzerinden yapıldığı bir devlet olan Estonya, DDoS saldırıları için her ne kadar Rusya'yı sorumlu tutmuşsa da Rus hükümeti bunu reddetmiştir (Aytekin, 2015, s. 21). Şu ana kadar, dünya kamuoyunca Estonya saldırılarını Rusya hükümetinin/istihbaratının yaptığına dair kesin hükümlere ulaşılamamıştır (Çeliktaş, 2016, 54).

Rus korsanları tarafından DDoS saldırılarına maruz kalan Estonya, olayı NATO'nun gündemi haline getirmiş ve bu olaydan sonra NATO, bir siber savunma politikası oluşturmuştur (Yılmaz ve Sağıroğlu, 2013, s. 323) ve Talinn'de de Müşterek Siber Güvenlik Mükemmeliyet Merkezi (Cooperative Cyber Defence Centre of Excellence-CCD COE)'ni kurmuştur.

1999'daki Sırp bilgisayar korsanlarının saldırısı NATO'nun siber güvenliğe olan ilgisini artırdı. Ardından gelişen 2007 Estonya olayları ise Nato'nun siber güvenliğe olan bakışının şekillenmesini ve kendi birimindeki en iyi siber güvenlik uzmanlarının araştırmalarda bulunma ve ülkenin elektronik sistemlerini güçlendirme çalışmaları yapmaları için Talinn'e gönderdi. Bu durum, siber saldırıların önemli bir bölümünün NATO'nun üzerine çekilmesini sebebiyet verdi. Estonya olayı, Nato'nun müttefik devletlerle siber güvenlik çalışmalarında müşterek hareket etme girişimlerini başlatması yönünden önemlidir (Ada, 2018, s. 32).

Estonya saldırılarının bazı sonuçları olmuştur. Bu olay, devletlerin siber uzayı artık bir rekabet alanı olarak gördüklerinin miladını oluşturmuş ve siber uzayın politik hedefler uğruna kullanılmaya başlanmasını beraberinde getirmiştir (Çeliktaş, 2016, 55). Bilgisayar sistemlerine bağımlılık, aynı zamanda siber saldırılar karşısında savunmasızlığa yol açmaktadır. Bilişim sistemlerine karşı yapılan saldırı toplu tüfekli saldırıyla kıyaslandığında, bir devleti işgalini, boyunduruk altına alınmasını ve yok edilebilmesini kolaylaştırdığı görülebilir. Finans kurumları, bankalar, borsalar ve devlet dairelerinin çalışamaz duruma gelmesi, Estonya'da yaşamı da durma noktasına getirmiştir (Kara, 2013, s. 48).

1.3.4. Gürcistan Hibrit Savaşı (2008)

1991'de Sovyetler Birliği'nin dağılmasının ardından Gürcistan bağımsızlığını ilan etmiştir. Moskova'dan destek alan asiler 1993'te Gürcü ordusunu Abhazya ve Güney Osetya'dan çıkarmış ve Rus koruması altında olan bağımsız hükümetler kurmuşlardır. Asilerin 2008'de Gürcü köylerine yaptıkları füze saldırıları, Gürcistan'ın Güney Osetya'yı işgaliyle sonuçlanmıştır. Bunun ardından Rus ordusu 8 Ağustos 2008'de Gürcü ordusunu Güney Osetya'dan çıkartmıştır (Kara, 2013, s. 48). 2008'in Ağustos'unda Rusya, Gürcistan ile olan sıcak çatışmaları eş anlı olarak siber uzayda da desteklemiştir. Gürcistan siber saldırıları, siber güvenliğin ne kadar önemli olduğunun algılanması yönünden önem arz etmiş (Meral, 2015, s. 73) ve ikinci büyük siber savaş olarak kabul edilmiştir (Sınav, 2014, s. 54).

Güney Osetya Savaşı, Gürcistan'ın Güney Osetya'dan tümden çıkarılması ve Rusya'yla olan bütün ilişkilerini kesmesiyle sonuçlanmıştır. Bu savaşta eş anlı bir şekilde Gürcistan'ın siber sistemleri hedef alınmış (Bozgeyik, 2018, s. 57), yine siber dünya Gürcistan-Rusya Savaşı'nın önemli bir cephesi durumuna gelmiştir (Gurcan, 2012, s. 107-108).

Bu işgal harekâtında Rusya'nın siber saldırılar Estonya'daki saldırılarda da kullandığı DDoS saldırıları olmuştur. Saldırılar Moskova'da bulunan ana bilgisayarın yanında Çin, Kanada, Estonya ve Türkiye'de bulunan köle bilgisayarlar vasıtasıyla yapılmıştır. Saldırılar sonucunda Gürcü medyası ve kamu internet sitelerine hasarlar verilerek Gürcistan'ın dış dünyayla olan bağlantıları kesilmiştir (Çeliktaş, 2016, 56). Finans, medya ve siyasi alanda yayınlar yapan çok sayıda Azeri, Güney Osetya, Rus ve Gürcü internet sitelerinin maruz kaldığı siber saldırıların en dikkat çekici olanı, Gürcistan Devlet Başkanlığı resmî sitesindeki Mikhail Saakasvhili'nin resminin yerine Adolf Hitler'inkinin konulmasıdır (Gurcan, 2012, s. 107-108). Saldırılar sonucunda Gürcistan'ın web sitelerine, bu sitelerin sağladığı hizmetlere (Bozgeyik, 2018, s. 57), ve CNN ve BBC sitelerine girişi engellenmiştir. Gürcistan'a trafiği destekleyen bütün yönlendiricileri ele geçirmiş olan Rusya siber savaşçıları; Gürcistan'ı dışarıdan haber alamayıp dışarıya e-posta dahi gönderemeyen, kredi kartı ve cep telefonlarının kullanılamadığı bir pozisyona sokmuşlardır (Kara, 2013, s. 48).

Gürcistan'a ciddi zararlar veren 3 haftalık siber saldırılar, Estonya kadar siber güvenlik altyapısına sahip olmayan Gürcistan'daki etkilerini daha da artmıştır. Gürcistan, bu siber felakete karşı aşağıdaki önlemleri almıştır (Ada, 2018, 34):

- ✓ Gürcistan'daki akademik çevreler önlem alma faaliyetlerinde bulunarak ulusal Bilgisayar Olayları Müdahale Ekibi (Computer Emergency Response Team-CERT) rolünü üstlenmişlerdir.
- ✓ Ulusal internet trafiğini düşürüp bilgi güvenliğini sağlamak amacıyla Rus web sitelerine olan erişimler devlet eliyle engellenmiştir.
- ✓ Ana bilgisayarlar ile sunucuların ülke dışına taşınması suretiyle hizmet kesintisinin giderilmesi sağlanmıştır.
- ✓ Başka ülkelerdeki ulusal CERT makamlarından yardım talebinde bulunularak koordineli bir şekilde çalışılmıştır.

Medya kuruluşlarına ve devlet sitelerine erişimin engellendiği Gürcistan, siber uzayını korumaya çalışarak öncelikle Rusya kaynaklı internet trafiğini engellemiştir. Bunun üstüne Ruslar; Çin, Kanada, Estonya ve Türkiye üzerinden saldırmış ve öncelikle Gürcü Bankalarını ve onların üzerinden de tüm dünya bankalarını saldırılara maruz bırakmışlardır. Bu durum bankaların ağ bağlantılarını Gürcistan ile kapatmalarına neden olmuştur (Meral, 2015, s. 73).

Herhangi bir fiziksel zarar ve yaralanmanın meydana gelmediği Estonya ve Gürcistan siber saldırılarında; iktisadi faaliyetlerin kısmen kesilmesi sivil ve siyasal alandaki hak tecavüzüyle birleştiğinde oldukça büyük miktarlarda parasal hasarlar meydana gelmiştir (Türkay, 2013, s. 1193). ICT'lerin internete aşırı bağımlılıklarının olmaması ve enformasyon altyapısının çok gelişmemiş olması Gürcistan'ın bu saldırılardan düşük bir zararla çıkmasını sağlamıştır (Çeliktaş, 2016, 56). Fiziki saldırılarla eş anlı bir şekilde yapılan siber saldırılar, gerçek dünyadaki sorunların bir anda sanal dünyaya yansıtılabileceğini de göstermiştir. Hem Rusya hem de Gürcistan tarafından yapılan DoS saldırıları kamuoyunu şekillendirme ve yapılan sahte sitelerde yoğun propaganda faaliyetlerinde bulunma amaçları da taşımıştır (Sınav, 2014, s. 54). Yine Estonya olaylarındaki gibi Rus Hükümeti suçlamaları red edip inisiyatifi dışında geliştiğini belirtmiştir (Meral, 2015, s. 73). Rusya ile yaşadıkları gerginliklerin peşi sıra Estonya ile Gürcistan'ın her ikisinin de siber saldırılara

uğraması, saldırıyı yapabilecek tek ülkenin Rusya olduğu olasılığını güçlendirmektedir. Estonya olayında Rusya'nın kabul etmek zorunda olduğu, Estonya'nın 'saldırganların bulunması ve cezalandırılması şeklindeki diplomatik talebi'ni kabul etmemesi Rusya şüphesini güçlendirmektedir. Gürcistan olayında da saldırıların Rus istihbarat sitelerinden geldiği tespiti yapılmıştır. Buna rağmen kontrolünün dışında yapıldığını öne sürmüştür (Kara, 2013, s. 49).

Gürcistan'ın Rusya ile yaşadığı gerginliklerin arkasındaki neden, Gürcistan'ın Nato'ya tam üyelik hedefidir. Tam üyeliğinin henüz gerçekleşmemiş olmasından dolayı da Nato'nun güvenliğinden faydalanamamıştır. NATO yine de Siber Savunma Yönetimi Otoritesi'nden bir uzman ekibi Gürcistan'a göndererek incelemelerde bulunmuştur. Siber dünyadaki tehdit düzeylerinin artması, dahası siber araçlar ile oldukça küçük eğitimlerle bile saldırıların yapılabilir olması gerçeği NATO üyelerinin korkmasına neden olmaktadır (Ada, 2018, 54).

1.3.5. Stuxnet (2010)

Siber güvenlik tarihinde 2010'da ilk siber savaş silahı Stuxnet virüsü bulunarak bir ilke imza atılmıştır. Genel kanının aksine, Stuxnet'in bilgi çalmak, değiştirmek veya silmek gibi endüstriyel casusluğa dair amaçları yoktur. Amacı fiziki ve askeri hedefler belirleyip onlara zarar vermektir (Türkay, 2013, s. 1190).

Stuxnet olayı, siber uzayda gerçekleşen gelişmelerin en büyüğü ve siber güvenlik tarihinin de dönüm noktası olarak kabul edilmektedir (Çeliktaş, 2016, s. 57). Bilhassa Siemens üretimi uzaktan kumanda sistemlerine etki eden (Aytekin, 2015, s. 21) Stuxnet, İran nükleer programında, Merkezi Denetim ve Veri Toplama (Supervisory Control And Data Acquisition-SCADA) sistemlerince kullanılan santrifüjlerin patlamalarına ve zarar görmelerine yol açmak için bir silah olarak kullanılmıştır. SCADA sistemleri, çok sayıda fiziki sistemin operasyon işlevini yürüten; elektrik şebekeleri, akaryakıt boruları, su dağıtım ve toplama sistemleri, iletişim sistemleri, demiryolları vb. sistemlerdir. Dahası, Stuxnet, kendi kodunu kod blokları arasında saklayarak, PLC üzerindeki kodları inceleyen programcının da Stuxnet kodunu görebilmesine imkân vermemektedir. Stuxnet'in kodu PLC'ye entegre etmesinin ardından potansiyel olarak sistemi kontrol edip çalışma şeklini

değiştirebilmesi söz konusu olmaktadır (Aytekin, 2015, s. 21). Siber saldırılar hedef sistemdeki sistem açıkları kullanılarak yapılmaktadır. Stuxnet'te de, sistem açığı piyasalarındaki değeri 100.000'lerce dolarla ifade edilen "sıfırıncı gün" (zero day) adlı sistem açıkları oldukça çok kullanılmıştır. Bu da Stuxnet'in maliyetinin milyon dolarlık olduğunu göstermektedir. Konunun uzmanları açısından tüm bunlar Stuxnet'in teknik birikim ve devlet bütçesiyle tasarlandığının, amatör birey/gruplar tarafından gerçekleştirilemeyeceğinin yeterli verileridir (Ünal, 2015, s. 194).

Ancak Stuxnet'in asıl saldırısı SCADA yazılımı değil, endüstriyel denetleyicilerdir. Dahası Stuxnet saldırısı; uzaktan kumanda edilemeyen, tümüyle bağımsız ve internet bağlantısı gerektirmeyen bir saldırıdır (Türkay, 2013, s. 1190).

2010'un Kasım'ında İran'ın yüksek düzeyde güvenlikle korunan nükleer yakıt tesisine girmeyi başarabilen Stuxnet virüsünün amacı, uranyum zenginleştirmede kullanılan ve son derece hızlı dönen makineler olan santrifüjlerin kontrol edilmesinde kullanılan PLC kontrol devrelerini hedef alıp kontrolü ele geçirmektir. Sistemi ele geçirip içten içe, yavaş ve emin adımlarla zarar veren Stuxnet virüsünün korkunç olan yönü; merkez bilgisayarlarına her şeyin normalmiş gibi gösterilmesidir. Bundan dolayı verdiği zararlar uzun zaman sonra fark edilebilmiştir. Virüsün dünya çapındaki etkisinin %60'ı aşan bir oranla İran'da olmasının, virüsün bilhassa İran nükleer tesisini kontrol altına alıp çökertmek için yapıldığı düşüncesini güçlendirmektedir. Stuxnet, İran'daki Natanz uranyum zenginleştirme tesisine varıncaya dek 100 binin üzerinde sisteme bulaşmış (Kara, 2013, s. 34) ve nükleer tesise varınca da neredeyse tesisteki 1000 santrifüjü çalışamaz hale sokmuştur (Çeliktaş, 2016, s. 57). Bir diğer iddia ise solucanın fark edilmesinden önce 9000 civarında olan santrifüjlerden 3700 civarında santrifüjün kaldığıdır (Aytekin, 2015, s. 22).

Natanz'da bulunan nükleer yakıt tesisindeki SCADA sisteminin internet üzerinden herhangi bir ağ bağlantısına sahip bulunmadığı dikkate alınacak olursa Stuxnet virüsünün taşınabilir bir bilgisayar veya bir USB ünitesiyle Simatic WinCC Step7'ye bulaştırıldığı kesin gibi görünmektedir (Çelik, 2013, s. 148). Symantec firması, programı yazan şahısların kodlama stillerinin tıpkı insanların parmak izleri gibi birbirinden farklıdır. Bu nedenle en az otuz farklı şahsın programa katkıda

bulunduğu tahmin edilmektedir. Bir diğer uzman görüşü ise bu solucanın en az 6 aylık bir sürede yazıldığıdır (Aytekin, 2015, s. 22). Bu kadar ince detaylarla yazılan bir solucan, hedefteki donanımlarla ilgili önemli miktarda bilgiye sahip olma gerekliliğini akla getirmektedir. Bu yaklaşım da solucanı yazıp geliştirenlerin devlet gücüne (donanımı geliştiren devletler) ve politik bir motivasyona sahip oldukları düşüncesini destekler niteliktedir (Göçoğlu, 2018, s. 103). Sonuç olarak, İran'ın maruz kalmış olduğu bu saldırının ABD ve İsrail tarafından düzenlendiği düşünülmektedir (Ulutaş, 2018, s. 90).

Bir tek ağa bağlı olan bilgisayarları değil bunun yanında dış dünyaya kapalı olan Endüstriyel Kontrol Sistemleri (Industrial Control Systems) de hedeflemiş olması yönünden önemli bir yere sahip olan Stuxnet, siber saldırılar karşısında yeterli hazırlığı olmayan ve farkındalık seviyesi de gelişmemiş olan ülkeler için uyarı niteliğindedir (Çeliktaş, 2016, s. 57).

1.3.6. Wikileaks (2011)

2006'da internet sitesi ismini kaydettiren, Ocak 2007'de de yayınlanmak üzere 1,2 milyon belgeye sahip olduğunu bildiren Wikileaks, belgeleri yayınlayarak tüm dünyada büyük yankılar uyandırmış, siber casusluğun en çarpıcı örneklerinden birisini oluşturmuş (Yayla, 2013, 196) ve yayınladığı bir milyon civarındaki gizli yazışma belgeleriyle de diplomaside depremlere yol açmıştır (Şenol, 2018, s. 203). İsveç merkezli uluslararası bir organizasyon olan Wikileaks, hükümetlerin ve diğer organizasyonların hassas belgelerini yayınlamış fakat kaynaklarının gizliliğini korumuştur (Kaya, 2017, s. 18).

Irak operasyonu sırasında da görev almış olan ABD kıdemli eri Bradley Manning, ABD Dış İşleri Bakanlığının 1966-2010 yılları arasında yaptığı gizli yazışmaları, ordu veri tabanından indirdiği görüntü ve dokümanları Kasım 2010'da Wikileaks sitesine sızdırarak Cenevre Sözleşmesine göre sivil hedeflerin bombalanmasının yasaklılığı kuralının ihlal edildiğini deşifre etmiştir. Durumdan rahatsız olan Pentagon uluslararası arenadaki panik nedeniyle de Wikileaks sitesi ve kurucusu Julian Assange'in sansürlenmesi kararı üzerine Anonymous bilgisayar korsanları grubunun sokak protestolarıyla karşılaşmıştır. Bradley Manning kendisini

“Bilgi; kamuya aittir, hakkı olanlara bedava sunulmalıdır.” söylemiyle savunmuştur. Dokümanları gönderenlerin bilgileri Wikileaks tarafından daima gizli tutularak hem wikileaks hem de wikileaks çalışanları tarafından bir şeyler düzeltilmeye, haksızlıklara karşı gelinmeye çalışılmıştır (Kara, 2013 s. 17-18).

Wikileaks’in faaliyetlerinden bir diğeri de CIA’dan çalınmış olan 8761 adet dökümanın mevcut olduğu bir veri ambarının yayınlanmasıdır. Wikileaks’in “Vault 7” olarak adlandırdığı bu veri ambarında; çok sayıda hacking aracı, spying işlemelerinin dökümantasyonu, Ios ve Android zafiyetleri, bazı akıllı TV’leri birer dinleme cihazına dönüştürebilme yöntemleri ve Windows’daki böcekler ile ilgili dökümanlar mevcuttu (Ulutaş, 2018, s. 96).

Wikileaks olayı, “Wikileaks gazeteciliği” terimini ortaya çıkarmıştır. Dijital çağda gazetecilik tarihinde ortaya çıkmış en büyük fenomenlerden birine dönüşen Wikileaks’in açığa çıkardığı haberler; ABD başkanı Johnson’un Vietnam Savaşı’nın başlatılmasına dair yalanlarıyla karşılaştırılmasına, gazetecilik yöntemleri ve ülkelerin siber güvenliklerinin sorgulanmasına kapı aralamıştır (Sınav, 2014, s. 53).

1.3.7. Snowden Olayı (2013)

2013’ün Haziran’ında CIA personeli Edward Snowden Hong Kong’da basın açıklamaları yaparak ABD NSA’nın Prizma adlı izleme ve dinleme sistemini deşifre etti. Snowden’in raporlarına göre NSA; 1 milyarın üzerinde kullanıcısı olan üç GSM şirketine siber saldırılar yaparak sms veri tabanlarına sızıp sms takibi yapmayı ve istihbari bilgi elde etmeyi amaçladığı açığa çıkmıştır. Bunun yanı sıra Çin’in saygın ve büyük bir akademik enstitüsü olan Çin Eğitim ve Araştırma Enstitüsü’nün network altyapısını sağlayan Tsinghua Üniversitesine sızma girişimleri, Hong Kong merkezli deniz altı fiber kablo altyapısı Pacnet’e müdahale bulunulup teknik takip yapıldığı ve Türkiye’nin Washington Büyük Elçiliğinin de aralarında olduğu yabancı temsilciliklerin dinlenildiği şeklinde birtakım bilgiler açığa çıkmıştır (Özalp, 2014).

Tüm devletlerin güçlerini kötüye kullandıkları anlamına gelmese de devletlerin iyi niyetlerine olan güven bilhassa gizlilik ve insan hakları konularında, Snowden’in NSA ile alakalı yaptığı açıklamaların ardından büyük bir darbe almıştır. Snowden olayı dikkatleri, ulusal güvenlik adına yapılan kitlesel gözetimlerin insan

güvenliğine olan doğrudan etkileri gerçeğine çekmiştir. Gittikçe artan sayıda hükümet, vatandaşların internette neler yapabileceklerini/yapamayacaklarını kontrol etmektedirler (Ünal, 2015, s. 214).

ABD NSA Prizma Projesiyle; kişisel konuşma kayıtlarına, sosyal ağlarda kişisel konuşma kayıtlarına ve kişilere özel bilgilere, dosya aktarımına erişim sağlayabilmiştir. Bunlara ek olarak Prizma, aralarında PalTalk, AOL, Skype**,** YouTube, Apple, Microsoft, Yahoo, Google ve Facebook'un da bulunduğu dokuz tane büyük şirkete arka kapı girişi de sağlayabilmiştir (Ünal, 2015, s. 216-217).

Snowden ve Assange benzeri kişiler somut yöntemlerle ele geçirip siber uzaydan açıkladıkları bilgilerle ulus-devletlere olan sadakatin sorgudan geçirilmesine kapı aralamışlardır. Bu da 150 yıldır gittikçe güç kazanan merkezi devletler arasında yatay şekilde el değiştiren gücün siber uzay sayesinde yatay dağılmasının yanında devletten bireye uzanan spektrumda alt unsurlara dikey olarak dağılmasına da yol açmıştır. Bir devletin bir başka devlete siber saldırı yaptığını kanıtlayan argümanlar kamuoyuna ilk kez Snowden ve Sanger'ın katkılarıyla duyurulmuştur (Ermiş, 2018).

İKİNCİ BÖLÜM

DÜNYADA SİBER GÜVENLİK SORUNU VE SİBER GÜVENLİK STRATEJİLERİ

2.1. SİBER GÜVENLİK KAVRAMI VE SİBER GÜVENLİĞİN GELİŞİMİ

Güvenlik; günlük yaşamın öngörülebilirliğinin bir parçası olarak sabit bir gelir, sürekli konut, giyim ve yiyecek kaynakları, suçtan korunma ve psikolojik güvenlik dahil olmak üzere birçok şeyi temsil etmektedir (Bakrania ve Haider, 2016, s. 7). Güvenlik, adalet ve emniyet özellikle orta gelir seviyesi ve altındaki ülke vatandaşları için büyük bir endişe kaynağını teşkil etmekteyken ülkelerin düzgün işleyişlerinin de temel dayanaklarından biridir (Magrassi, 2016, s. 22). Buradan hareketle; günümüzdeki güvenlik kavramına, artık siber güvenliğin de dahil olduğunu gözlemleyebiliriz.

Siber güvenlik tartışması, 1970'lerde ABD'de ortaya çıkan ve ancak 1990'ların sonlarında diğer ülkelere yayılan teknolojik yeniliklere ve özellikle de "Soğuk Savaş" sonrası değişen jeopolitik koşullara bir cevap olarak ortaya çıkmıştır. Başlangıçta endişeler, hükümet bilgi sistemlerinde bulunan gizli bilgilere ilişkindi. Fakat bilgisayar ağlarının büyümesi ve günlük yaşama daha fazla girmesiyle birlikte odak noktası değişti. "Siber güvenlik" terimi ilk olarak bilgisayar bilimcileri tarafından 1990'ların başında kullanıldı. Ağ bağlantılı bilgisayarlarla ilgili bir dizi güvensizliği belirten odak noktası, sadece teknik bir bilgisayar güvenliği anlayışının ötesine geçerek tüm ulusun güvenliği, ekonomisi ve sosyal refahı üzerinde dijital tehditlerden kaynaklanan yıkıcı toplumsal etkilere sahip olabileceği noktasına kaydı (Adams ve diğ. 2015, s. 15-16). İnternetin siyaset, casusluk ve askeri faaliyetler için yeni bir araç ve iş dünyası için küresel bir altyapı olarak geliştirilmesiyle birlikte

siber güvenlik, ulusal ve uluslararası güvenlik için merkezi bir konu haline geldi (Cybersecurity and Cyberwarfare, 2011 s. 3). Siber güvenliğin, siber uzayın; iş, siyaset ve güvenlik için merkezi önemini yansıtan küresel bir sorun ve uluslararası güvenlik için de endişe verici bir konu haline gelmesi, en azından, Rusya Federasyonu'nun Birleşmiş Milletler Genel Kurulu (BMGK)nda siber çatışma riskini azaltmak için ilk kez bir antlaşma önerdiği 1998'den bu yana söz konusu oldu (The Cyber Index, 2013, s. 1). Rusya'nın BMGK İlk Komitesine sunduğu bu karar tasarısından bu yana bilgi güvenliği BM gündeminde yer almakta, bu konuda genel sekreter tarafından BM üye devletlerinin görüşlerini içeren yıllık raporlar Genel Kurula verilmekte ve ayrıca şimdiki ve gelecekteki siber tehditleri ve işbirlikçi önlemleri gözden geçiren üç Resmi Uzman Grubu da bulunmaktadır (Benoliel, 2015, s. 441-442).

Bilgi güvenliği, Rusya Federasyonu'nun 1998'de BM Genel Kurulu'nun ilk Komitesinde bir karar taslağını ilk kez başlatmasından bu yana BM gündeminde yer almaktadır. Mevcut ve gelecekteki siber tehditleri ve işbirliği önlemleri gözden geçiren üç Hükümet Uzmanı Grubu da var.

Bu on yılda, internet kullanıcı sayısı tüm dünyada katlanarak artmıştır. Azgelişmişten gelişmekte olan ve gelişmiş ülkelere kadar her ülke artık teknolojinin kutsaması ve laneti ile alt edilebilir durumdadır ve bu giderek artmaktadır. Bununla birlikte siber saldırılar da daha gelişmiş ve karmaşık hale gelmektedir. Bir de bunun üstüne, belirli bir ülke ile sınırlı olmayıp sınırın ötesinde olmaları, onlarla mücadelede uygun altyapı bulunmadığında tespit edilmeme olasılıklarını daha da yükseltmektedir (Sarker ve diğ. 2019, s. 2). 2007'de Estonya'nın internet altyapısına yönelik siber saldırılar, 2008'de Gürcistan ve Rusya arasındaki fiziksel savaşın bir siber savaşa dönüşmesi ve 2010'da Stuxnet solucanı ile İran'ın nükleer programına yapılan saldırı, çok sayıda ülkeye, her yerde bulunan ICT'lerin ulusal bilgi altyapılarını siber saldırılara karşı son derece savunmasız hale getirdiğini fark ettirdi. Ayrıca Snowden'in 2013'teki küresel güvenlik iletişiminde kitlesel bir gözetim yürüten Ulusal Güvenlik Ajansı'na (NSA) ilişkin açıklamaları; pek çok ülkeyi, dijital bilgilerini ve vatandaşlarının temel internet haklarını koruma konusunda temkinli hale getirdi (Shafqat ve Masood, 2016, s. 129).

Siber güvenlik, en genel şekilde ele alınacak olursa: “Siber güvenliğin, 21. yüzyılın küresel ekonomisine nüfuz eden ve onu harekete geçiren CI’lerin korunmasının yanı sıra hem devlet sırlarının korunması hem de ulusal savunmanın sağlanması için esas olduğudur (Klimburg ve Tirmaa-Klaar, 2011, s. 13).” Günümüzde olduğu gibi birbirine yakınlaşmış bir dünyada, ülkelerin karşılaştığı zorlukların daha da fazlalaştığı bir dönemde, ülkelerin gündeminde en yenilikçi teknolojilerden yararlanarak onları hükümetlerin hizmetine koyma eğilimi mevcuttur. Fakat bu yönüyle ilgili halen çözüm bekleyen ve test edilme aşamasında olan birçok gerilim bulunmaktadır. Bu durumda yapılabilecek tek şey; bir ülkenin, ulusal siber güvenlik gündemine (stratejisine) bir siber güvenlik programı dahil etmesidir. 1947'de Ulusal Güvenlik Stratejisi'nden ilk bahseden ve yalnızca 1986-2012 yılları arasında 15 program hazırlayan ülke, ABD’dir. Fakat 2007'de büyük bir değişiklik oldu: Çağdaş toplumların savunmasızlığını açıkça gösterdiğinden dolayı Estonya'ya yönelik siber saldırı gerçek bir dönüm noktasıydı. Bunun doğrudan bir sonucu olarak; ulusal güvenlik stratejilerinin küresel yayılımlarında ve detaylandırılmalarında bir artış oldu; ancak en önemli sonuç, ülkelerin Ulusal Güvenlik Stratejilerine siber güvenliğin dahil edilmesi oldu (Magrassi, 2016, s. 22-23).

2.2. SİBER UZAYDA ETKİN BAZI ÜLKELERİN VE KURUMLARIN SİBER GÜVENLİK STRATEJİLERİ

2.2.1. ABD

İnternetin kökenleri, Eylül 1969’da ABD’de Advanced Research Projects Agency (İleri Araştırma Projeleri Ajansı-ARPA) tarafından kurulan bir bilgisayar ağı olan ARPANET’e dayanır. ARPA, özellikle 1957'de Amerikan göklerini fetheden ilk uyduyu (Sputnik) fırlatan Sovyetler Birliği'nin ABD’yi geride bırakan bu teknolojik atılımının ardından, araştırmaları genişletmek ve geliştirmek amacıyla 1958’de ABD Savunma Bakanlığı (Department of Defence-DoD) tarafından kuruldu. NASA uzay programlarının yönetiminde başarılı olduğu vakit ARPA da ordudaki tüm uzun vadeli bilimsel araştırmaların kontrolünü ele geçirdi (Magrassi, 2016, s. 49).

ARPA’nın atılımıyla başlayan internet iletişimiyle birlikte “siber uzay”a ilişkin tehditlerin de ortaya çıkmasıyla beraber, ülkeler de siber güvenliğe yönelik

strateji ve politika çalışmalarına başlamışlardır. ABD, siber güvenliğe 1990'lardan bu yana odaklanmıştır. Özellikle ABD tarafından oldukça bilinen siber soruna, 1990'lardan bu yana siber güvenliğin sağlanmasına dönük çalışmalarla odaklanılmaya başlanmıştır (Cybersecurity and Cyberwarfare, 2011, s. 21). ABD yönetimi, yürütme yetkilerini kullanarak siber güvenliği sağlamaya, "2003 Siber Uzay'ın Güvenliği İçin Beyaz Saray Ulusal Stratejisi (2003 White House National Strategy to Secure Cyberspace)" ile katılmaya başlamıştır. Bu ilk adım, 11 Eylül saldırısından sonra daha kapsamlı bir boyutta yapılan Ulusal Güvenlik Bakanlığı (Department for Homeland Security-DHS) Ulusal Güvenlik İncelemesi (National Security Review)'nin ayrılmaz bir parçasıydı. ABD'deki siber güvenlik politikası, 2010 ABD Ulusal Güvenlik Stratejisi (2010 US National Security Strategy) ile birlikte devlet dışı terörizmden devlet aktörlerinin faaliyetlerine geçiş vurgusuyla gelişimine devam etmiştir (Robinson, 2013, s. 41).

Başkan Obama; siber güvenliği, ABD'nin yüzleşmesi gereken en ciddi ekonomik ve ulusal güvenlik sorunlarından biri olarak tanımladı ve aynı zamanda bir devlet ya da ülke olarak ABD'nin karşı koymaya yeterince hazırlıklı olmadığını belirtmiş ve bu nedenle göreve başladıktan kısa bir süre sonra ABD'nin bilgi ve iletişim altyapısını savunmak ve dijital altyapısını güvence altına almak için federal çabaların ve kapsamlı bir yaklaşımın geliştirilmesine yönelik ayrıntılı bir gözden geçirme emri vermişti (The Comprehensive National Cybersecurity Initiative). Bu doğrultuda, 2011 yılında tamamlanan Siber Uzay Gözden Geçirme Politikası (The Cyberspace Review Policy) ile siber altyapıyı güvence altına almak için federal kurumların rolleri özetlenmiştir. Bununla; kısa vadede, yürütme organının yeni siber güvenlik yetkilileri ataması ve federal hükümet içinde mevcut tehditlerle ilgili farkındalığı artırması beklenmiştir. Bu politikadaki noktaların çoğu, 2010 Ulusal Güvenlik Stratejisi'nde de bulunmaktadır (Cybersecurity and Cyberwarfare. 2011, s. 22). Mayıs 2011'de yayınlanan Uluslararası Siber Uzay Stratejisi (International Strategy for Cyberspace) ise ABD'nin "Ulusumuzu, müttefiklerimizi, ortaklarımızı ve çıkarlarımızı savunmak için gerekli tüm araçları (diplomatik, bilgilendirici, askeri ve ekonomik) uygun ve geçerli uluslararası hukuka uygun olarak kullanma hakkını saklı tutarız. Bunu yaparken elimizden geldiğince askeri güçten önce tüm seçenekleri

tüketeceğiz...” vurgusunu öne çıkarmıştır (International Strategy for Cyberspace, 2011. s. 14).

2013 ve 2017 yılları arasında ABD’de sırasıyla önce DoD yardımcılığı ve ardından da DoD görevlerinde bulunan Ashton Carter, 2015’te yayınlanan DoD Siber Stratejisi (The DoD Cyber Strategy)’nde birtakım açıklamalarda bulunmuştur. Ona göre; diğer birçok ülke gibi ABD’nin de çok sayıda kritik hizmet için internete, sistemlere ve siber uzayın verilerine bel bağlamış bir vaziyette bulunması hali, birçok kesimin (bireyleri, orduları, ticareti, okulları ve hükümetleri) gerçek ve tehlikeli siber tehditler karşısında savunmasız kalmasına, devlet ve devlet dışı aktörlerin CI ağları üzerinde yıkıcı siber saldırılar düzenlemesine ve teknolojik/askeri avantajlarını azaltmak için de ABD’nin fikri mülkiyetini çalma planlamaları yapmalarına yol açmıştır (The DoD Cyber Strategy, 2015). İnternete, siber uzayın sistemlerine ve verilerine olan bu bağlılık; bir siber saldırı halinde ülkenin esasında neden savunmasız olduğunun ve zamanında bir eylem olarak da uygun bir Ulusal Siber Güvenlik Stratejisi tarafından neden desteklenmesi gerektiğinin zorunlu ve hayati nedenidir.

Bu perspektifle; DoD, siber güçlerinin gelişimine rehberlik etmek ve siber savunma ve siber caydırıcılık duruşunu güçlendirmek amacıyla Nisan 2015’te dikkate değer bir belge olan “The DoD Cyber Strategy”i yayınlamıştır. Belge, DoD’nin üç siber görevi için siber yetenekler ve kurumlar oluşturmaya odaklanmıştır (Fact Sheet: The DoD Cyber Strategy, 2015). Bunlar:

- ✓ DoD’nin ağlarını, sistemlerini ve bilgilerini savunmak,
- ✓ Önemli sonuçları olan siber saldırılara karşı ABD’yi ve onun çıkarlarını korumak,
- ✓ ve Askeri operasyonları ve acil durum planlarını desteklemek için bütünsel siber yetenekler sağlamaktır.

Beş stratejik hedeften oluşan bu strateji, DoD’nin önümüzdeki beş yıl ve sonrası için ulaşması istenilen özel hedefleri belirler. Bu hedefler aşağıdaki gibidir (The DoD Cyber Strategy, 2015, s 7-8):

- ✓ Siber operasyonları yürütmek için hazır kuvvetler/yetenekler oluşturmak, sürdürmek,
- ✓ DoD bilgi ağını korumak, verilerini güvenceye almak ve misyonları için riskleri azaltmak,
- ✓ ABD anavatanını ve hayati çıkarlarını, önemli sonuçlara yol açan yıkıcı veya zararlı siber saldırılardan korumaya hazırlıklı olmak,
- ✓ Uygun siber seçenekler oluşturmak, sürdürmek ve bu seçenekleri çatışma tırmanışını kontrol etmek ve çatışma ortamını her aşamada şekillendirmek için kullanmayı planlamak,
- ✓ Ortak tehditleri caydırmak, uluslararası güvenliği ve istikrarı artırmak için güçlü uluslararası ittifaklar ve ortaklıklar kurup sürdürmektir.

Fakat DoD'yi yeni bir siber strateji geliştirmeye iten şey neydi? Burada esas olarak üç ana faktör öne sürülebilir (Fact Sheet: The DoD Cyber Strategy, 2015):

- ✓ Birincisi; DoD ağları, verileri ve sistemleri de dahil olmak üzere ABD menfaatlerine yönelik artan siber tehditlerin şiddeti ve ileri düzeyliliğidir. DoD'nin dünyadaki en büyük ağa sahip olduğu ve kendi ağlarını korumak, verilerini güvence altına almak ve misyonlarına yönelik riskleri azaltmak için agresif adımlar atması gerektiği bilinmektedir.
- ✓ İkincisi; daha önce de belirtildiği gibi, 2012 yılında Başkan Obama, DoD'ye diğer ABD devlet kurumları ile uyum içerisinde; ulusun, önemli sonuçları olan siber saldırılara karşı savunulması için bir planlamanın yapılması ve organize edilmesi emrini vermişti. Bu yeni misyon, yeni bir stratejik düşünmeyi gerektiriyordu.
- ✓ Son olarak da tehdide cevaben; DoD 2012 yılında, DoD'nin siber misyonlarını yerine getirmek için bakanlık içerisinde benzersiz bir role sahip olan bir Siber Görev Gücü (Cyber Mission Force-CMF)'nü kurmaya başladı. CMF, faaliyete tamamen geçtikten sonra bünyesinde askeri departmanlar ve savunma bileşenlerinden yaklaşık olarak 6.200 askeri, sivil ve müteahhit destek personeli içerecektir.

DoD ve ABD için bir bütün olarak büyük bir yatırımı temsil etmekte olan Siber Görev Gücü stratejisinin temel amacı, ABD ulusal çıkarlarını korumak ve

savunmak için CMF ile DoD'nin daha kapsamlı siber işgücü gelişimine rehberlik edecek özel hedefler ortaya koymaktır (The DoD Cyber Strategy, 2015, s 7-8).

Kapsamlı ve iddialı bir belge olan The DoD Cyber Strategy, amaçlarının gerçekleştirilmesi için aktarılması gereken kaynakların idare edilmesinde açıkça bir şekilde yüksek düzeyde bir uzmanlık gerektirmektedir. Gerçekte uygun kaynakların idare edilmesi; Amerika partnerleri-ABD kuruluşları, uluslararası müttefikler ve özel sektör arasında her zamankinden daha fazla sıkı bir işbirliği ile birlikte ilerlemeyi sağlamak için esastır. ABD, dijital çağın getirdiği zorluklara ancak bu şekilde ayak uydurarak çıkarlarını savunabilir (Magrassi, 2016, s. 52).

Önde Gelen Kuruluşlar

ABD'de siber güvenliğin sorumluluğu; DHS, FBI ve NSA'nın bileşenlerinden biri olan yeni ABD Siber Komutanlığı (Cyber Command-CYBERCOM)'nı da bünyesinde barındıran DoD arasında bölünmüştür. Saldırı operasyonları CYBERCOM'a ve CIA unsurlarına tahsis edilmiştir (Cybersecurity and Cyberwarfare, 2011, s. 21).

DoD; siber saldırılar dahil her türlü saldırının engellenmesinden, siber tehdit bilgilerinin toplanmasından, ulusal güvenlik ve askeri sistemlerin güvence altına alınmasından, siber suçların askeri yargı alanı altında soruşturulmasından ve ulusal çıkarlarına zarar vermeye çalışan her türlü düşmana karşı ABD'nin güvenliğinin sağlanmasından sorumludur. Bu amaçları gerçekleştirmek için de diplomatik, enformasyonel, askeri, ekonomik ve hukuki yaptırım araçlarıyla donatılmış çok sayıda yetenek geliştirmiş ve küresel bir stratejik istikrar sağlamanın yanı sıra aynı zamanda yeni ve daha güçlü ittifaklar kurmak için de uluslararası aktörler ve özel sektör ile birlikte bir dizi ortaklığa imza atmıştır (Magrassi, 2016, s. 141).

Yurt içi savunmasından öncelikli olarak DHS sorumludur. Bu bakanlığa bağlı Ulusal Siber Güvenlik Bölümü (National Cyber Security Division), sivil hükümet ağlarının federal (".gov" alan adı) alanını koruma ve kritik ağların güvenliğini artırmak için özel sektörle (".com" alan adı) işbirliği yapma çabalarına öncülük etmekte (National Cybersecurity Division) ve aynı zamanda siber altyapının

saldırılara karşı korunması için de bir dizi programa sahiplik yapmaktadır. Bu bölüm altında faaliyet gösteren Ulusal Siber Müdahale Koordinasyon Grubu (The National Cyber Response Coordination Group), 13 federal kurumdan oluşur ve ulusal olarak önemli bir siber olay olması durumunda federal müdahalenin koordinasyonundan sorumludur (Cybersecurity and Cyberwarfare. 2011, s. 21-22). DoD ve DHS, işbirliğini kolaylaştırmak ve bölümler arası işbirliğini artırmak için Ekim 2010'da siber güvenlik konusunda bir mutabakat zaptı da imzalamışlardır (Fredrick, 2018).

DoD'nin bünyesinde çalışan ABD Kuzey Komutanlığı (USNORTHCOM), Savunma Güvenliği İşbirliği Kurumu (Defence Security Cooperation Agency) operasyonları için kuvvetler koordine etmekten ve sağlamaktan sorumludur. ABD Stratejik Komutanlığı (USSTRATCOM); CYBERCOM aracılığıyla siber operasyonların senkronize edilmesinden, planlanmasından ve yürütülmesinden sorumludur. Belirli DoD ağlarının askeri siber uzay operasyonlarını ve savunmalarını bütün imkanları ile yürüten CYBERCOM (Robinson, 2013, s. 42), ABD STRATCOM bünyesinde askeri bir alt komut olarak varlığını sürdürmekte ve askeri siber altyapıya yönelik tehditlerle mücadele etmektedir (Fredrick, 2018).

2.2.2. Estonya

Estonya; 2007 yılında, oldukça olağan dışı bir olay olarak maruz kaldığı siber saldırılar nedeniyle uluslararası arenada önem kazanmıştır.

Sovyetlere ait II. Dünya Savaşı Anıtı'nın Estonyalılar tarafından yerinin değiştirilmesine bir tepki olarak yapılan saldırılar, genelde iki aşamaya yayılmış olarak düzenlendi. Saldırılardan ilki; düzenli DoS saldırılarıyla karakterize edilen, ikincisi ise daha büyük DDoS saldırılarıyla düzenlenen ve 85.000'den fazla bilgisayarın ele geçirilmesiyle sonuçlanan saldırılardır. Bu siber saldırılar; Estonya'nın devlet kurumlarını, medya kanallarını, özel web sitelerini hedef almasının yanı sıra Estonya'nın en büyük iki bankasının çevrimiçi hizmetlerini de çalışmaz hale getirebildi (Tikk ve Talihärm, 2010, s. 44-45).

Estonya; sadece 2007'de katlanmak durumunda kaldığı unutulmaz siber saldırılar nedeniyle değil, aynı zamanda Avrupa Birliği (AB)'nin "dijital devleti" olması nedeniyle de bugün, küresel siber savaşta en ileri referans noktasını temsil

etmektedir. Estonya'nın AB'nin dijital devleti olması ise halka açık binlerce Wi-Fi noktası, çevrimiçi politik danışmaları, banka işlemlerinin %90 oranında internet üzerinden gerçekleşmesi ve bilgi teknolojisi ve telekomünikasyon alanındaki binlerce yenilikçi girişiminden ileri gelmektedir. Ekonomi, politika, vatandaşlık hizmetleri ve buradaki her şey çevrimiçi olarak gerçekleşir ve ülkenin tümü fiber optik kabloludur. Gerçekten de devletin adı genellikle ironik bir şekilde "E stonia" olarak deformasyona uğratılır (Magrassi, 2016, s. 96). Estonya'ya yapılan saldırıların uluslararası güvenlik için bir tehdit oluşturduğunun kabul edilmesi, 2007'de Estonya'nın tümüne karşı ilk eşgüdümlü siber saldırı ve diğer birçok ülkede de bilgi sistemlerine yönelik gerçekleştirilen büyük ölçekli siber saldırılar nedeniyle yeni zirvelere ulaşmıştır. Bu gelişmelerin ardından Estonya; Savunma Bakanlığı'nın başkanlığında Dışişleri, İçişleri, Ekonomi, Adalet, Eğitim ve Araştırma bakanlıklarıyla işbirliği içinde Siber Güvenlik Strateji Komitesini (Cyber Security Strategy Committee) oluşturmuştur. Komite, 2008'de Siber Güvenlik Stratejisini yayınladı. Strateji, birtakım amaçlar ve bu amaçları gerçekleştirebilmek için de birtakım stratejik hedefler belirlemiştir (Estonia Cyber Security Strategy 2008-2013, s. 6-8-27-29). Stratejinin amacı;

- ✓ Siber alandaki güvenlik açıklarını azaltmak, siber saldırıları önlemek ve bir saldırı anında kritik bir altyapıyı mümkün olan en kısa sürede onarmaktır.

Stratejinin hedefleri ise;

- ✓ Çok düzeyli bir güvenlik önlemleri sisteminin oluşturulması,
- ✓ Bilgi güvenliği konusundaki uzmanlığın artırılması,
- ✓ Yasal reformların başlatılması ve uluslararası işbirliğinin teşvik edilmesi,
- ✓ Siber Güvenlik Stratejisinin amaçlarının uygulanması için Cumhuriyet Hükümeti Güvenlik Komitesi bünyesinde Siber Güvenlik Konseyinin kurulması,
- ✓ Devlet bilgi sistemlerinin güvenliğinden sorumlu olan Ekonomik İşler ve İletişim Bakanlığı bünyesindeki yapısal birimin görevlerinin belirlenmesi ve farklı düzeylerde (yani devletin yanı sıra, CI kurumları ve şirketler) risk analizlerini sağlaması için bu görevlerin yerine getirilmesidir.

Ancak her ne kadar güvenlik analistleri; diğer DoS ve DDoS saldırılarına kıyasla Estonya saldırılarının büyüklüğünün çığır açıcı düzeyde olmadığını savunmuşsa da benzer şekilde, Estonya hükümeti de siber saldırıların ülkenin normal günlük faaliyetlerini felç etmediği sonucuna varmış; fakat saldırıların, belirli koşullar altında önemli bir güvenlik riski oluşturduğu gerçeğinin bir kez ortaya çıktığı ve küresel olarak kayda değer bir politik ve sosyal motivasyon unsuru halini aldığı netlik kazanmıştır (Tikk ve Talihärm, 2010, s. 46). Bu olaydan sonra Estonya hükümeti; siber sorunu, daha sonra 2010'da parlamento tarafından kabul edilecek olan Estonya Ulusal Güvenlik Konsepti (National Security Concept of Estonia)'ne dahil etmek için ulusal politika (yasama, organizasyonel vb.) çerçevesini değiştirmiştir (National Security Concept of Estonia 2010). Bu geniş gözden geçirmenin bir parçası olarak, Konsept'te belirlenen amaçların yerine getirilmesi için 2009 yılında Acil Durum Yasası (Emergency Act) çıkarılmış ve bununla birçok yapı yeniden oluşturulurken diğer yapılar da düzenlenmiştir. Bu bağlamda; yeni örgütsel çerçeve kapsamında Estonya Bilişim Merkezi (Estonian Informatics Centre)'nin organizasyonu ve modernizasyonu, Ekonomik İşler ve İletişim Bakanlığı'na bağlı olan Estonya CERT'in rollerinin belirlenmesi, Kritik Bilgi Altyapısı Koruma (Critical Information Infrastructure Protection- CIIP) Departmanı'nın oluşturulması ve Siber Savunma Birliği (Cyber Defence League)'nin oluşturulması çalışmalarına gidildi (Magrassi, 2016, s. 44).

2009, siber güvenliği geliştirmek için birçok ilgili kararın alındığı bir yıl olduğundan dolayı Estonya için anlamlı bir yıl olarak kabul edilebilir. Bu amaca daha iyi hizmet edebilmek için siber güvenlik ilk olarak siber suç, ulusal savunma ve CI ve hayati hizmetler şeklinde üç kategoriye ayrılmıştır. İkinci olarak, siber güvenliğin geliştirilmesi için yasal alan ve uluslararası ilişkileri şekillendirerek insanları eğitmeye ve farkındalıklarını arttırmaya da dikkat edilmesi gerektiğine karar verilmiştir. Buna ek olarak, Ekonomik İşler ve İletişim Bakanlığı Genel Sekreteri'nin başkanlığında Siber Güvenlik Konseyi (Cyber Security Council) kurulmuştur (Republic of Estonia Ministry of Economic Affairs and Communication, 2019).

Estonya; 2008 Siber Güvenlik Stratejisi ile elde ettiği ilerlemesini, Estonya Siber Güvenlik Stratejisi 2014-2017 ile devam ettirmiştir. Bu stratejisi ile dört temel amaç ve alt başlıklarda da beş alt hedef ortaya koymuştur (Estonian Cyber Security Strategy 2014-2017). Belirlenen dört temel amaç aşağıdaki gibidir:

1. Ulusal düzeyde siber güvenliğin sağlanması için farklı seviyelerden oluşan kapsamlı bir güvenlik önlemleri sisteminin uygulanması gerekmektedir.
2. Estonya; çok yüksek düzeyde bilgi güvenliği, yetkinliği ve farkındalığı ile karakterize edilmiş bir ülke olarak görülmelidir.
3. Orantılı yasal düzenlemeler, bilgi sistemlerinin güvenli ve kapsamlı kullanımını desteklemek için hizmet vermektedir.
4. Estonya, siber güvenliği geliştirmek için uluslararası işbirliğinin önde gelen ülkelerinden biridir.

Bu amaçlardan ortaya çıkan vizyon; Estonya'nın ulusal güvenliği sağlayabilecek ve de açık, kapsayıcı ve güvenli bir toplumun işleyişini destekleyebilecek bir ülke olduğudur. Bu nedenle 2014-2017 Siber Güvenlik Stratejisinin dört yıllık ana hedefi; siber güvenlik yeteneklerini artırmak, nüfusun siber tehditlerle ilgili farkındalığını artırmak ve böylece siber uzaya sürekli güven sağlamaktır.

Bu temel amaç daha sonra aşağıdaki beş alt hedefte yapılandırılmıştır:

1. Önemli hizmetlerin altında yatan bilgi sistemlerinin korunmasını sağlamak: Estonya devletinin ve toplumunun işleyişi, her insanın ekonomik ve sosyal refahı, yaşamı ve sağlığı, sistem ve hizmetlerin güvenliğine gittikçe daha fazla bağlı hale gelmektedir. Stratejinin ana amaçlarından biri, hayati hizmetlerin kesintisiz çalışmasını ve esnekliğini sağlamak için yöntemler ve siber tehditlere karşı kritik bilgi altyapılarının korunmasını sağlamaktır.
2. Siber Suçlar ile Mücadelenin Geliştirilmesi: Siber suçtan kaynaklanan ekonomik hasar, dijital hizmetlere duyulan güveni azaltır ve en kötü senaryoda, can kaybına neden olabilir. Halk arasında siber güvenlik riskleri konusunda daha fazla farkındalık, siber suçların önlenmesine yardımcı olmaktadır. Daha fazla farkındalık, siber ilintili konuların eğitimin her seviyesinde ele alınmasıyla ve

insanların güvenli davranışlarının araştırılması ve analizine dayanarak bilgilendirilmesiyle başarılır.

3. Ulusal siber savunma yeteneklerinin geliştirilmesi: Devletin tasarrufundaki kaynaklara dayalı sivil, askeri ve uluslararası işbirliği de uyarı, caydırıcılık ve aktif savunma açısından siber alanda yeterince işlev görmelidir
4. Estonya gelişen siber güvenlik tehditlerini yönetir: Estonya, siber güvenlik kapasitesini korumak ve geliştirmek için araştırma, geliştirme, girişimcilik, güvenlik eğitimi ve eğitim olanaklarıyla desteklenen bağımsız siber güvenlik çözümlerini benimseyecektir.
5. Estonya sektörler arası faaliyetler geliştirir: Siber tehditlerle mücadelede gerekli olan yetenekleri geliştirmek için, bir dizi kapsamlı hedef ele alınmaktadır. Yasal çerçevenin ayarlanması ve siber dış politikanın geliştirilmesi hem kritik hizmetlerin korunması için hem de siber suçlarla mücadele ve siber uzayda ulusal savunmanın tasarımı için hayati önem taşımaktadır.

Estonya'nın Savunma Bakanı Hannes Hanso'nun verdiği röportaja göre Estonya; gerektiği takdirde her 4 yılda bir yenilenecek olan, sonuncusu 2016'da yaklaşık olarak 450 milyon Euro bütçeyle hazırlanan ve 2022'ye kadar sürecek olan 10 yıllık bir savunma planı üzerinde çalışmıştır. Uluslararası standartlara göre gösterişsiz olmasına rağmen yıllık olarak %7 oranında artışların uygulanacağı para; savunmaya harcanacak, orduya önemli miktarda yatırım yapılmasında, savunma altyapısının geliştirilmesinde ve siber direncin iyileştirilmesinde kullanılacaktır (DefenseNews). Bu kapsamda Estonya, son olarak 2019-2022 Siber Güvenlik Strateji belgesini yayınlamıştır. Son strateji belgesi, dört önemli amaç ve dört önemli ilkeyi hedeflemiştir (Republic of Estonia Ministry of Economic Affairs and Communication, 2019):

Dört önemli amaç şöyledir:

- ✓ Estonya, güçlü teknolojik esnekliğe ve acil duruma hazırlığa dayanan sürdürülebilir bir dijital topluluktur.
- ✓ Estonya siber güvenlik endüstrisi; Estonya'nın tüm kilit yeterliliklerini kapsayan güçlü, yenilikçi, araştırma odaklı ve küresel anlamda rekabetçidir.
- ✓ Estonya, uluslararası arenada güvenilir ve yetenekli bir ortaktır.

- ✓ Estonya, siber okuryazar bir toplumdur; yeterli ve ileriye dönük bir yetenek arzı sağlar.

Dört önemli ilke ise aşağıdaki gibidir;

- ✓ Temel hak ve özgürlüklerin, fiziksel çevrede olduğu kadar siber uzayda da korunmasını ve teşvik edilmesini önemli görmektedir.
- ✓ Siber güvenliği, Estonya'nın sosyoekonomik büyümesinin temeli olan Estonya'nın hızlı dijital gelişiminin bir etkinleştiricisi ve güçlendiricisi olarak görmektedir. Güvenlik, yenilikleri; yenilikler de güvenliği desteklemelidir.
- ✓ Dijital ekosistemin temeli olduğundan dolayı kriptografik çözümünün güvenlik teminatının, Estonya için benzersiz bir önem taşıdığı bilinmektedir.
- ✓ Dijital toplum için şeffaflığı ve kamu güvenini temel kabul etmekte ve bu nedenle, açık iletişim ilkesine bağlı kalma taahhüt edilmektedir.

Estonya siber güvenliğinin gerçek anahtarı, her bir Estonya e-Devlet ve IT altyapı sisteminin doğasında var olan emniyet ve güvenlikten kaynaklanmaktadır. Estonya vatandaşları ve işletmeleri, bilgilerinin ve işlemlerinin güvende olduğunu bilerek güvenle çalışırlar. Gerçekten de siber güvenliğin en iyi türü, insanların her gün hakkında düşünmek zorunda kalmadığı türdür (Magrassi, 2016, s. 96).

Önde Gelen Kuruluşlar

2008'de Estonya'nın stratejisinin yayınlanmasının ardından; Estonya'nın "IT front (IT cephesi)"ü, CCDCOE tarafından koordine edilmeye başlanmıştır. Karargâhı Tallinn'deki bir askeri üste bulunan ve uluslararası bir askeri organizasyon olan CCDCOE, savaş ve siber güvenlik temaları üzerine araştırma ve incelemelerde bulunur. Yıllar içerisinde ABD, İtalya, Almanya, Fransa, Hollanda ve İngiltere ile birlikte üye sayısı 15'i bulmuştur. Siber terör saldırılarını önleme, izleme ve muhtemel yanıt verme onun görevidir. Merkez, farklı ülkelerden yaklaşık kırk kişiyi istihdam etmekte ve dışarıdakilere erişimleri de NATO'nun güvenlik protokolleri çerçevesinde katı bir biçimde yasaklamaktadır (Magrassi, 2016, s. 96). Merkezin sponsor ülkeleri; Estonya, Almanya, Macaristan, İtalya, Letonya, Litvanya, Slovakya ve İspanya'dır (Cybersecurity and Cyberwarfare, 2011, s. 11). Ordu da özellikle

CCDCOE aracılığıyla NATO ile yürüttüğü işbirliği sayesinde siber savunmada kritik bir role sahiptir (Robinson ve diğ. 2013, s. 13)

2007 siber saldırılarından bu yana, siber güvenlik için merkezi bir otorite olan Estonya Bilgi Sistemi Kurumu (Estonian Information System Authority-RIA) kurulmuştur. RIA; devletin, siber ve ilgili departmanlardaki (CIIP Departmanı) girişim ve çabalarını koordine etmede yetkili olan kurumdur. RIA, olaylara müdahale etme ve kritik bilgi altyapılarını korumakla ilgilenmekte ve bunun yanı sıra çabaların bir entegrasyon ve işbirliği içinde yürütülmesinde bir platform işlevi görmektedir (Robinson ve diğ. 2013, s. 13). Estonya CERT, saldırılara müdahale için koordine edici bir kuruluş haline getirilmiş ve acil savunma programını yerel sağlayıcılar ve endüstri/hükümet alanındaki IT uzmanlarının gönüllü ağlarıyla işbirliği içinde koordine etmiştir. Ekip; derhal olayın ciddiyetini analiz etmeye, yurtdışındaki servis sağlayıcılarına kötüye kullanım raporları göndermeye ve etkilenen kuruluşlar ile servis sağlayıcıları arasında bilgi alışverişini kolaylaştırmaya çalıştı. Saldırıların etkisini bir dereceye kadar hafifletmeyi başarabilse de geçici, gayri resmi statü nedeniyle, tavsiyelerini tüm taraflara uygulatma yetkisine sahip değildi (Evron, 2008, s. 123).

Buna ek olarak; İçişleri Bakanlığı bünyesinde yer alan Kriminal Polis IT Suçları Bürosu (IT Crimes Office of the Criminal Police) ve Estonya'nın bilgi güvenliğini daha fazla koordine etmekten sorumlu olan kriz yönetimi, siber suçlar ve CI'nin korunmasına adanmış birimler de bulunmaktadır (Robinson ve diğ. 2013, s. 13). Çevrimiçi suç faaliyetlerini soruşturmak ve kovuşturmak için kendi Siber Suçlar Birimi (Cyber Crimes Unit)'ne sahip olan Estonya Polisi ve Sınır Muhafızları ofisleri de vardır (Magrassi, 2016, s. 96).

Estonya Bilişim Merkezi; devletin, IT yeteneklerini akıllıca uygulayarak vatandaşlara mümkün olan en iyi şekilde hizmet verebilmesi için devlet bilgi sisteminin geliştirilmesi ve yönetilmesinden sorumludur (Estonia Country Report, 2011, s. 21). Merkez, aralarında Estonya CERT ve CIIP Departmanı'nın da bulunduğu altı bölümden oluşur. Son zamanlarda modernize edilerek bakanlık tarafından idare edilen bir devlet kurumu olmaktan çıkartılıp özerk yürütme yetkilerine sahip bir devlet kurumuna yükseltilmiş olan Merkez, bilgi altyapısı ile

ilgilenen diğer resmî kurumları denetlemenin yanı sıra kritik bilgi altyapısına sahip olan ve işleten teşebbüsleri de izleyen ve düzenleyen bir konuma gelmiş oldu (Tikk ve Talihärm, 2010, s. 61-63). Bu yenilemenin amacı; Merkezi, Ulusal Siber Güvenlik Stratejisinde belirtilen prensiplerin yerine getirilmesinde ve etkin bir şekilde uygulanmasının garanti edilmesinde daha iyi hale getirmektir. 2009 Acil Durum Yasası'nın kabulünün bir sonucu olarak CIIP Departman'ı, Estonya'daki hem kamu hem de özel sektör IT sistemlerinin korunmasının hayati unsurlarıyla ilgilenecektir. Her hayati hizmetin sahibi, kendi sisteminin günlük savunmasıyla ilgili sorumluluğunu yerine getirmeye devam ederken CIIP genel koruyucu eylemleri koordine edecektir. CIIP, bilgi sistemlerinin savunulmasının iyileştirilmesi konusunda da tavsiyelerde bulunabilir (Information System Auhority, 2009).

2009 Acil Durum Yasası (2009 Emergency Act)'nın yürürlüğe girmesinden sonra kurulan bir diğer önemli organ, 1918'de kurulmuş gönüllü bir askeri ulusal savunma örgütü olan ve Savunma Birliği (Defence League)'nde faaliyet gösteren Siber Savunma Birliği (Cyber Defence League)'dir. Üç ana görevi vardır: Estonya sivil internetinin korunması, IT uzmanlarının eğitimi ve siber güvenlik ile ilgili bilgilerin kamuoyu ile paylaşılması (The Cyber Index, 2013, s. 32).

Siber Güvenlik Stratejisinin amaçlarının uygulanması için Cumhuriyet Hükümeti Güvenlik Komitesi bünyesinde Siber Güvenlik Konseyi kurulmuştur. Konseyin görevi, çeşitli kurumlar arasında işbirliğinin sorunsuz bir şekilde yapılmasına katkıda bulunmak ve Siber Güvenlik Stratejisi hedeflerinin uygulanması konusunda gözetim sağlamaktır (Republic of Estonia Ministry of Economic Affairs and Communication, 2019).

2.2.3. İngiltere

İngiltere, ilk stratejisini "Birleşik Krallık'ın Siber Güvenlik Stratejisi: Siber Uzayda Emniyet, Güvenlik ve Direnç (Cyber Security Strategy of The United Kingdom: Safety, Security and Resilience in Cyberspace)" ismiyle Haziran 2009'da yayınlamıştır (Robinson, 2013, s. 26). Bunun akabinde Haziran 2009'da Bakanlar Kurulu bünyesinde Siber Güvenlik ve Bilgi Güvenliği Ofisi (Office of Cyber Security and Information Assurance)'nin kurulmasının ardından (Intelligence and

Security Committee, 2011, s. 57) İngiltere'nin ulusal siber güvenlik programı, bu Ofis tarafından yönetilmeye başlanmıştır ve İngiltere siber saldırılara yönelik mücadelesini, 2010'dan bu yana Ulusal Güvenlik Stratejilerine dayanarak yapmaya başlamıştır. İkinci strateji belgesini Kasım 2011'de "Birleşik Krallık Siber Güvenlik Stratejisi: Dijital Dünyada İngiltere'yi Korumak ve Tanıtmak (The United Kingdom Cyber Security Strategy: Protecting and Promoting the UK in a Digital World)" ismiyle hayata geçirmiştir. Uygulanabilmesi için 650 milyon Sterlinlik bir yatırımın yapıldığı stratejinin dört ana hedefi bulunmaktadır (The UK Cyber Security Strategy 2011, s. 5-8). Bunlar sırası ile aşağıdaki gibidir:

1. Siber suçlarla mücadele etmek ve siber alanda iş yapmak için dünyanın en güvenli yerlerinden biri olmak,
2. Siber saldırılara karşı daha dayanıklı olmak ve siber alandaki çıkarlarını daha iyi koruyabilmek,
3. İngiliz halkının güvenle kullanabileceği açık toplumları destekleyen, istikrarlı, canlı ve açık bir siber ortamın şekillendirilmesine yardımcı olmak,
4. ve tüm siber güvenlik hedeflerini desteklemesi için ihtiyaç duyulan beceri ve yeteneğe sahip olmaktır.

Dönemin başbakanı David Cameron tarafından parlamentoya sunulan "Ulusal Güvenlik Stratejisi ve Stratejik Savunma ve Güvenlik İncelemesi 2015(National Security Strategy and Strategic Defence and Security Review 2015)" belgesi; İngiltere tarafından aynı madalyonun iki yüzü gibi görülen, ülkenin güvenlik sorunları ile mücadele etme ve ekonomik gücü sağlama yönündeki vizyonunu öne çıkarmaktadır. Bu belgeye göre; İngiltere, savunma ve denizaşırı kalkınma için önemli kaynaklara yatırım yapmayı seçmiştir. Belge, özellikle aşağıdaki önceliklere odaklanmaktadır (National Security Strategy and Strategic Defence and Security Review 2015, s. 9-10):

- ✓ Dünyada lider kurumlar olmaları için Silahlı Kuvvetler ile güvenlik ve istihbarat teşkilatlarımızı güçlendireceğiz (O kuruluşlar gücümüzü küresel olarak yansıtırlar ve rakiplerimizi caydırmak veya yenmek için yakın müttefiklerimizle birlikte savaşır ve çalışırlar).

- ✓ Değerlerimizi ve çıkarlarımızı küresel olarak destekleyen dünya standartlarındaki diplomasi servisimiz, denizaşırı kalkınmaya olan bağlılığımız, BBC Dünya Servisi ve British Council gibi kurumlarımızla dünyanın önde gelen yumuşak gücü konumumuzu daha da artıracağız.
- ✓ NATO dahil mevcut ittifaklarımıza daha fazla yatırım yapacağız, büyüyen güçlerle daha güçlü ilişkiler kuracağız ve geçmişteki rakipleri ittifaka dahil etmeye çalışacağız.
- ✓ Halkımızı, toplumlarımızı ve işlerimizi giderek daha fazla etkileyen küresel zorluklara karşı iç direncimizi ve hukuki yaptırım yeteneklerimizi güçlendireceğiz.
- ✓ Terörizmi yurtiçinde ve yurtdışında sert ve kapsamlı bir şekilde ele alıp, aşırılıkçılığa karşı koyup onu besleyen zehirli ideolojilere meydan okuyacağız. Siber güvenlik konusunda, dünya lideri olacağız. Devlet bazlı tehditleri caydıracağız. Krizlere hızlı ve etkin bir şekilde cevap vereceğiz, yurt içinde ve dışında direnci artıracağız.

Siber güvenlik, İngiltere için son derece önemli bir konudur. Ulusal Güvenlik Konseyi, "Ulusal Güvenlik Stratejisi ve Stratejik Savunma ve Güvenlik İncelemesi 2015" belgesinde İngiltere'nin baş etmesi gereken tüm yurtiçi ve yurtdışı riskleri olasılık ve etki kombinasyonunun hükümlerine dayanarak üç katmanlı bir sınıflandırmaya tabi tutmuş ve böylelikle siber saldırılar tarafından ortaya çıkarılan riskler de bu katmanda gözlemlenebilir duruma gelmiştir. Siber güvenlik sorununun; İngiltere için, terörizm veya uluslararası askeri çatışmaların da yer aldığı "Katman(seviye) 1" tehdidi olarak sınıflandırıldığı görülmektedir (Hammond, 2016).

İngiltere Maliye Bakanı Philip Hammond; 2016'daki "Ulusal Siber Güvenlik Stratejisinin Başlatılması" adlı konuşmasında, siber ulusal müdahalenin etkinliğini kanıtlamak için Bakanlar Kurulunun (Dışişleri, Savunma, İçişleri, Kültür Medya, Spor ve Sağlık bakanlıklarının katılımıyla) bir araya getirilmesiyle daimî bir Siber Komitenin kurulmasını ilan etti. Bu özel komitenin oluşturulması; askeri sırlara, finansal bilgilere, verilerin ihlaline ve belki de en önemlisi ulusal altyapıya yönelik siber tehditlerle başa çıkmada merkezi hükümetin (istihbarat ve güvenlik kurumları

da dahil) birlikte çalışma isteğini ifade ettiğinden dolayı bir dönüm noktası olmuştur (Magrassi, 2016, s. 36-37).

1,9 milyar sterlinlik dönüşümsel yatırımla desteklenen (Hammond, 2016) İngiltere'nin yeni Ulusal Siber Güvenlik Stratejisi 2016-2021; savunma, caydırma ve geliştirme olmak üzere üç temel konsepte dayanmaktadır (National Cyber Security Strategy 2016-2021):

- ✓ **Savunma:** İngiliz hükümeti bu konseptle; savunmaları, ulaştırma ve enerji gibi CI sektörlerini (ulaştırma ve enerji gibi) ve ekonomiyi güçlendirmeyi amaçlamaktadır.
- ✓ **Caydırma:** İngiliz hükümeti bu konseptle; İngiltere'nin siber alandaki çıkarlarını çalmayı, tehdit etmeyi veya zarar vermeyi hedefleyen her birey, grup veya terör örgütünü, özellikle de siber suçluları tespit edebilen, izleyebilen ve misilleme yapabilen saldırgan siber yeteneklerin geliştirilmesine yapılan büyük bir yatırımla caydırmayı amaçlamaktadır.
- ✓ **Geliştirme:** İngiliz hükümeti bu konseptle; İngiliz ekonomisinde ve toplumda gelecekte de tehditlere ayak uydurmak için ihtiyaç duyulan tüm bu yeteneklerin geliştirilmesini amaçlamaktadır. Bu gelişim; yeni nesil öğrencilere, uzmanlara ve şirketlere siber sorun hakkında en iyi araç ve bilgileri sağlayarak yüksek vasıflı uzmanların oluşturulması yoluyla gerçekleştirilebilir.

Önde Gelen Kuruluşlar

İngiltere, ilk siber güvenlik stratejisini 2009'da (Shafqat ve Massod, 2016, s. 131) yayınladıktan sonra Haziran 2009'da Bakanlar Kurulu'nda Siber güvenlik Ofisi (Office of Cyber Security)'ni kurmuş ve Ofis'i, Eylül 2010'da "siber güvenlik ve bilgi güvencesi için hükümet çapında bütünleşik ve tutarlı bir strateji ve politika liderliği sağlamak" amacıyla Siber Güvenlik ve Bilgi Güvencesi Ofisi (Office of Cyber Security and Information Assurance) olarak genişletmiştir. Ulusal Güvenlik Sekreteryası bünyesinde bulunan Ofis'in, çoğunluğu hükümetten ve az sayıda da özel sektörden olmak üzere 27 çalışanı bulunmaktadır (Intelligence and Security Committee, 2011, s. 57). Ofis'in; stratejik yön sağlama ve siber güvenlik politikasını Bakanlar Kurulu'ndan koordine etme, Ulusal Siber Güvenlik Programının

uygulanmasını sağlama ve 650 milyon sterlinlik bütçenin yönetilmesinden sorumlu olma gibi görevleri vardır (The Cyber Index, 2013, s. 63). Ofis; hükümetin siber güvenlik programının uygulanmasında, Siber Güvenlik Operasyon Merkezi ile beraber devletin önde gelen birçok kurumuyla [Devlet İletişim Merkezi (Government Communications Headquarters), Ulusal Altyapının Korunması Merkezi (Centre for the Protection of National Infrastructure), Siber Güvenlik Operasyon Merkezi (Cyber Security Operations Centre) vb.] çalışır (Robinson, 2013, s. 27).

Bahsi geçen Ulusal Altyapının Korunması Merkezi (The Centre for the Protection of National Infrastructure), İngiltere'deki kamu–özel ortaklığı çabalarını kolaylaştırmanın (Robinson, 2013, s. 27) yanı sıra; CI sahiplerine siber tehditler konusunda rehberlik sağlama, tehditler ve koruyucu önlemler hakkında kamu-özel bilgi paylaşımını kolaylaştırmak için bilgi alışverişinde bulunma gibi görevleri vardır (The Cyber Index, 2013, s. 63).

Siber Güvenlik Operasyon Merkezi (The Cyber Security Operations Centre), hem saldırgan hem de savunmacı siber yeteneklerin geliştirilmesinden sorumludur. Bunun yanı sıra başlıca görevleri; devlet IT sistemlerinin gelişimini ve sağlığını izlemek, eğilimleri analiz etmek ve siber olaylara verilen yanıtları iyileştirmektir. 2011 yılı başında 19 kişilik ilk personeliyle faaliyete geçmesi planlanan merkezin, 2009-2010 mali yılında bir bütçesi yoktu ve bu bütçe Hükümet İletişim Merkezi, Bakanlar Kurulu, güvenlik ve kolluk kuvvetleri tarafından karşılanmıştı (Cybersecurity and Cyberwarfare, 2011, s. 21).

İngiltere, siber güvenlik uzmanlarının kadrolarını artırmak için 2013 yılında Askeri Siber Rezervleri (Military Cyber Reserves)'ni hayata geçirmiştir. İngiltere, siber güvenlik bilinci ile ilgili olarak; kuruluşların ve küçük/orta ölçekli işletmelerin farkındalığını artırmak için Siber Gereklilikler ve Siber Streetwise (Cyber Essentials and Cyber Streetwise) gibi programlar başlatmış ve aynı şekilde vatandaşlarının siber eğitimi için İnternet Servis Sağlayıcıları (Internet Service Providers) ile birlikte çalışarak İnternet Servis Sağlayıcıları Rehber İlkeleri (Internet Service Providers Guiding Principle) yayınlarını da kullanmıştır (Sabillon ve diğ. 2016, s. 72).

2.2.4. Almanya

Almanya için siber güvenlik tehdidinin önceliklendirilmesi konusunda kamuya açık bir bilgi mevcut değildir. Bununla birlikte; tehdit aktörleri, savaş, terörizm ve suç gibi bağlamların yanı sıra doğal tehlikeler ve sistemlerin teknik arızası ile de karakterize edilir. Siber, Alman önleyici güvenlik stratejisinin kritik bir bileşenidir. Alman siber stratejisi, her ne kadar ABD ve İngiltere'deki benzer girişimlerin gerisinde kalsa da 2011 yılının başlarında Federal İçişleri Bakanlığı tarafından Almanya için federal bir Siber Güvenlik Stratejisi'nin yayınlanması ile bir adım öne çıkmıştır (Robinson, 2013, s. 18). Bu strateji, 2009 Federal Bilgi Teknolojisinin Güvenliğini Güçlendirme Yasası (2009 Act to Strengthen the Security of Federal Information Technology), 2009 CI Koruması Uygulama Planı (2009 Critical Infrastructure Protection Implementation Plan) ve Almanya'nın siber güvenliğe yönelik ilk kapsamlı çabası olarak öne çıkan 2005 Ulusal Bilgi Altyapısı Koruma Planı (2005 National Plan for Information Infrastructure Protection) üzerine kurulmuştur (The Cyber Index, 2013, s. 23-24). 2011 yılında yürürlüğe giren "Alman Ulusal Siber Güvenlik Stratejisi", aşağıdaki maddeler ile özetlenebilir (Cybersecurity Strategy for Germany, 2011):

- ✓ Kritik yapıların ve bilgi sistemlerinin korunması,
- ✓ IT sistemlerinin güvenilirliğini geliştirmek,
- ✓ Devlet kurumlarının IT konusunda güvenliğini ve emniyetini garanti etmek,
- ✓ Siber suçu kontrol etmekten emin olmak,
- ✓ Siber güvenliğin sağlanması için uluslararası işbirliğinin geliştirilmesi,
- ✓ Güvenilir teknoloji kullanımı,
- ✓ Kamu kurumlarında personel eğitimi,
- ✓ ve Etkili ve güvenli savunma araçları geliştirmektir.

Önleyici ve iş birlikçi siber güvenlik önlemlerini, savunma tekniklerini ve siber politikaları koordine etmeye odaklanacak olan Ulusal Siber Güvenlik Konseyi; Federal Şansölyeden, eyalet düzeyindeki temsilcilerden ve devlet sekreterlerinden (Dışişleri Bakanlığı, İçişleri Bakanlığı, Savunma Bakanlığı, Ekonomi ve Teknoloji Bakanlığı, Adalet Bakanlığı, Maliye Bakanlığı, Eğitim ve Araştırma Bakanlığı ve ayrıca eyalet düzeyindeki temsilciler) oluşmaktadır. Konseye, özel sektörün yanı sıra

akademi temsilcileri de ortak üye olarak davet edilmektedirler (The Cyber Index, 2013, s. 24).

Alman Bilgi Güvenliği Kurumu (German Information Security Agency), 2016'da "Almanya'da IT Güvenliği Durumu 2016" raporunu yayınlanmıştır. Raporda, IT güvenliği için mevcut riskler ve karşı önlemler hakkında bilgi verilmiştir. Mart 2015'te, Alman hükümeti IT güvenlik Ar-Ge'yi teşvik etmek için bir plan yayınlamış ve planda, özel şifreleme teknolojilerini teşvik etmek ve kişisel veri ve iletişim hizmetlerinin daha fazla korunmasını sağlamak amacıyla 2020 yılına kadar 180 milyon Euro (198 milyon $) bir bütçe tahsis etmiştir. Planın vurguladığı önemli alanlar aşağıdaki gibidir (Ataç ve Akleylek, 2018, s. 605-606):

- ✓ Son teknolojiler,
- ✓ Güvenli ve güvenilir bilgi ve bilişim güvenliği iletişim sistemleri uygulama alanları,
- ✓ Verilerin gizliliği ve korunması.

Önde Gelen Kuruluşlar

2011 stratejisi kapsamında; Ulusal Siber Savunma Merkezi (National Cyber Defence Centre) (Robinson, 2013, s. 18), İçişleri Bakanlığı'ndan bir devlet sekreteri başkanlığında Ulusal Siber Güvenlik Konseyi (National Cyber Security Council) ve Ulusal Siber Müdahale Merkezi (National Cyber Response Centre) kurulmuştur. İçişleri Bakanlığı, siber güvenliğin lideriydi ve bakanlık tarafından denetlenen Federal Bilgi Güvenliği Bürosu (Federal Office for Information Security), bilgi teknolojisinin güvenliğinin sağlanmasından sorumlu tutulmuştur (Strategy for Germany, 2011, s. 9-10).

Almanya'nın Ulusal Siber Müdahale Merkezi'nde; Federal Kriminal Polis Teşkilatı, Federal Polis, Gümrük Kriminolojik Bürosu, Federal İstihbarat Teşkilatı, silahlı kuvvetler ve CI yetkililerinden görevliler bulunmaktadır. Merkez, bilgi güvenliği için Federal Bilgi Güvenliği Ofisi'ne rapor verir; Federal Ofis'i, Anayasanın Korunması için ve Federal Sivil Savunma ve Afet Yardım Ofis'i için koordine eder. Merkez; saldırgan yetenekler geliştirmek yerine, operasyonel

işbirliğine ve güvenlik açığı koruması ve olay müdahalesi alanlarında bilgi paylaşımına odaklanmıştır (Cybersecurity Strategy for Germany, 2011, s. 8). Silahlı Kuvvetlerin Stratejik Keşif Birimi'nin Bilgi ve Bilgisayar Ağı Operasyonları departmanı, siber kapasitelerin geliştirilmesi ile görevlendirilmiştir. Bu kapsamda; 2009 yılında, 76 askeri personele silahlı kuvvetler tarafından verilen bilgisayar bilimleri eğitimi sonucunda bir birim oluşturuldu. Birim, saldırgan siber yetenekler konusunda eğitilmek üzere özel bir siber grup olarak tasarlanmıştır (Cybersecurity and Cyberwarfare, 2011, s. 13).

2.2.5. G. Kore

2008 Savunma Raporu (Defence White Paper)'nda siber güvenlik, ulusal savunmanın temel bir bileşeni olarak tanımlamıştır. 2010'daki Savunma Raporu'nda ise siber saldırı, geleneksel olmayan birkaç güvenlik tehdidinden biri olarak özetlenmiştir. Rapor, Savunma Bilgi Sistemleri'ni denetlemek için kurul seviyesinde CERT'in oluşturulmasını ve Savunma Bilgi Ağı (Defence Information Network) ve Savaş Alanı Yönetim Sistemi'ni (Battlefield Management System) korumak için de Millî Savunma Bakanlığı tarafından alınan güvenlik önlemlerinin detaylandırmasını yapmıştır (Cybersecurity and Cyberwarfare, 2011, s. 18). Rapor'un ardından Ağustos 2011'de, Kore İletişim Komisyonu (The Korea Communications Commission), 15 devlet kurumunun ortak çabası sonucunda geliştirilen ulusal siber güvenlik stratejisini açıklamış ve siber uzayın; kara, hava ve deniz gibi operasyonel bir etki alanı olarak kabul edileceğini ve bundan dolayı da devlet düzeyinde bir savunma sistemine ihtiyaç duyduğunu öne sürmüştür. Strateji, hanelerin yüzde 95'inden fazlasının internete erişebildiği ülkede siber saldırıların önlenmesine, tespit edilmesine, bunlara müdahale edilmesine, kamu ve özel sektörde şifreleme ve veri yedeklemesinin yanı sıra diğer güvenlik önlemlerinin sağlanmasına odaklanmıştır (The Cyber Index, 2013, s. 40-41).

Önde Gelen Kuruluşlar

Ulusal Siber Güvenlik Merkezi (National Cyber Security Center); siber saldırıların tanımlanmasından, önlenmesinden, güvenlik açıklarını analiz etmekten, siber acil müdahale faaliyetlerini koordine etmekten ve saldırılara yanıt vermekten

sorumludur. Merkez, bu çalışmaları yerine getirirken özel ve askeri sektörlerle de çalışmaktadır. Millî Savunma Bakanlığı, Ocak 2010'da başlıca amacı hükümet ve finansal bilgi ağlarının güvenliğini artırmak olan Siber Savaş Merkezi (Cyber War Centre)'ni ve bunun yanı sıra siber alanda savunma ve saldırı operasyonlarından sorumlu olan ve 200'den fazla personel istihdam eden bağımsız bir Siber Savaş Komutanlığı (Cyber Warfare Command)'nı da oluşturmuştur (Cybersecurity and Cyberwarfare, 2011, s. 18).

Kore İletişim Komisyonu'na göre siber konularda öncü rol oynayacak olan kurum, Ulusal İstihbarat Servisi'dir. Milli Savunma, Devlet İdaresi ve İçişleri Bakanlıkları ile birlikte sırasıyla özel sektör, ulusal savunma ve hükümet bilgisayar sistemlerinin güvenliğinden Kore İletişim Komisyonu sorumlu tutulmuştur. Kore Yüksek Bilim ve Teknoloji Enstitüsü (The Korea Advanced Institute of Science and Technology), siber saldırılara karşı tespit ve savunma konusunda yardımcı olan Siber Güvenlik Araştırma Merkezi (Cyber Security Research Center)'ni kurmuştur. Kore Cumhuriyeti ayrıca, saldırı ve savunma siber savaş silahları geliştirmeyi ve Siber Savaş Komutanlığı'nda insan gücünü artırmayı planlamaktadır; savunma planı personel sayısını 1000'e çıkarmayı tasarlamıştır (The Cyber Index, 2013, s. 41).

2.2.6. Rusya

Rusya, son yıllarda ulusal ve uluslararası ortamda siber güvenliğe ilişkin bir dizi üst düzey politika belgesini kabul etmiştir. Ancak politikayı desteklemek için yapılan risk değerlendirmesinin metodolojisi ve sonuçları halka açık değildir. Siber tehditlerin önceliklendirilme düzeylerine dair herhangi bir bulguya rastlamanın zor olduğu Rusya siber güvenlik stratejilerinde tehditler, genel olarak iç (suç ve yolsuzluk) ve dış (devlet, teröristler, yabancı rekabet) şeklinde nitelendirilmiştir. (Robinson, 2013, s. 24).

İnternet üzerinden yapılan düşman saldırıların, Rusya için ilk kez 1997'de ana tehdit olarak sayılmasıyla birlikte "Bilgi Savaşı" kavramı Rusya'da önemli bir boyut kazanmış ve kavramın dört bileşenden oluştuğu ileri sürülmüştür (Agentura.ru, 1997):

- ✓ Devlet ve askeri idare altyapı bileşenlerinin bastırılması (komuta kontrol merkezlerinin imhası); IT bileşenleri üzerinde elektromanyetik basınç (elektronik savaş),
- ✓ İletişim kanalları üzerinden iletilen bilgi akışlarını yakalayıp deşifre ederek istihbarat edinme,
- ✓ Bilgi kaynaklarına yetkisiz erişim,
- ✓ Bilgisayar sistemlerinin bozulması ve dezenformasyon.

Bu gelişmeden sonra Rusya, 2000 yılında Bilgi Güvenliği Doktrini'ni oluşturmuş ve bu çerçevede "Rusya'nın bilgi alanındaki ulusal çıkarlarına dayanarak devlet bilgi güvenliğini sağlamak için stratejik ve mevcut iç ve dış politika hedeflerini oluşturmuştur." (Information security doctrine of the Russian Federation, 2000).

Daha sonra, 2003 yılında, Federal Güvenlik Servisi, Federal Hükümet İletişim ve Bilgi Ajansı'nın kriptolojiden ve kod kırılmasından sorumlu olan bölümlerini kendi bünyesine katmıştır. 2010 yılına gelindiğinde ise Rusya ve müttefiklerinin ulusal çıkarlarını korumak için politik ve bilgi araçlarının kullanımını tartışan, askeri güç ve askeri olmayan yeteneklerin bütünleşik kullanımı da dahil olmak üzere modern askeri çatışmanın karakteristik özelliklerini tanımlayan yeni bir askeri doktrin yayınlanmıştır (Cybersecurity and Cyberwarfare, 2011, s. 19).

Temmuz 2012'de, Rusya Federasyonu Güvenlik Konseyi siber saldırıların tespit edilmesi ve önlenmesi, siber suçlarla mücadele edilmesi, ulusal bir sistemin oluşturulması ve ülke ağlarının 2020'ye kadar güvence altına alınması hedefleriyle sorumluluğu Federal Güvenlik Servisi'nde olan ulusal bir politika yayınlamıştır. Ocak 2012'de Savunma Bakanlığı, "Rusya Federasyonu Silahlı Kuvvetlerinin Bilgi Alanındaki Faaliyetlerine İlişkin Kavramsal Görüşlerini" yayınlamıştır. Bu stratejide, bilgi güvenliği ilkelerini ve bilgi sistemlerindeki müdahaleyi kontrol etmek için farklı önlemler tartışılmış ve 3. bölümünde; caydırıcılık, çatışmaların önlenmesi ve çözümü için farklı kurallar değerlendirilmiştir (The Cyber Index, 2013, s. 63).

Mart 2012'de Rusya başkan yardımcısı Dmitry Rogozin, "silahlı kuvvetler ve ayrıca bir bütün olarak devlet altyapısı için bilgilerin güvence altına alınması ile

bağlantılı Siber Güvenlik Komutanlığı ve ABD'deki Savunma Gelişmiş Araştırma Projeleri Ajansına (Defense Advanced Research Projects Agency) benzeyen gelişmiş bir askeri araştırma kurumu kurulmasına ilişkin bir yasa tasarısı üzerinde çalıştıklarını" açıklamıştır (Atlantic Council, 2012).

2.2.7. Çin

2000'li yılların başında Çin'in Merkezi Askeri Komisyonu, "bilgilendirme" koşulları altında bir halk savaşı çalışmasının yapılması çağrısında bulundu. Bunun ardından Çin'in 2004 tarihli Ulusal Savunma Raporu, "bilgilendirilmenin silahlı kuvvetlerin savaşma kabiliyetini arttırmada kilit faktör haline geldiğini" ve Halk Kurtuluş Ordusu (PLA)'nun bilgilendirmeyi "kendi oryantasyon ve stratejik odak noktası" olarak ele aldığını belirtmiştir. Çin askeri doktrini; çatışmanın ilk aşamalarında, siber ve elektronik harp yeteneklerinin bir kombinasyonunu desteklemektedir (China's National Defense in 2004).

Rapor; PLA Hava Kuvvetlerini, bilgi işlem ve önlemlerinden sorumlu olarak tanımlamıştır. PLA Genelkurmay Başkanlığı'nın 4. Bölümü, elektronik karşı önlemlerin denetlenmesinden ve gelişen bilgi harp teknolojileri araştırma enstitülerinin siber kapasitelerinden; 3. Bölümü ise istihbarat sinyallerinden ve elektronik bilgilerin toplanması, analizi ve kullanılmasına odaklanmaktan sorumludur. PLA, yeteneklerini geliştirmek için doğrudan ticari firmalarla, araştırma üniversiteleriyle ve kamu sektörüyle bağlarını sürdürmektedir (Cybersecurity and Cyberwarfare, 2011, s. 8-9).

2012'de Çin Devlet Konseyi, ülkenin bilgi kaynaklarını korumak ve bilgi alışverişinde güvenliği sağlamak için işletmeler, kuruluşlar ve gerekli devlet kurumları tarafından veri toplanmasının sıkı bir şekilde düzenlenmesini istemiş ve bu kapsamda "bilgi aciliyetlerini" daha iyi tespit edip ele almak, internet suçunu azaltmak ve kişisel bilgileri daha iyi korumak için yoğunlaştırılmış çabalar çağrısında bulunan bir dizi yeni siber güvenlik politika yönergesini yayınlamıştır (Chinadaily, 2012). Bu çerçevede her ikisi de Devlet Konseyi tarafından denetlenen Kamu Güvenliği Bakanlığı, siber suçun araştırılmasından ve acil durumlara cevap verilmesinden, Sanayi ve Bilgi Teknolojileri Bakanlığı da düzenleme ve

geliştirmeden sorumlu (standartları belirlemek, tatbikat yapmak, ağ güvenliğine yönelik denetimler yapmak ve ulusal CERT'i işletmek gibi) tutulmuştur. Çin Devlet Konseyi Bilgi Ofisi; 2011 yılında, ulusal savunma hakkında, önceki belgelere de dayanarak orduya "uzayda, elektromanyetik uzayda ve siber uzayda güvenlik çıkarlarını sürdürmesi" görevini veren bir rapor yayınlamış ve strateji "bilgilendirme koşullarında yerel savaşları kazanmak için yeni bir savaş yeteneği türü" çağrısında bulunarak "Silahlı kuvvetlerin bilgi alma koşullarında savaşma yeteneklerinin önemli ölçüde arttırıldığını" belirtmiştir (The Cyber Index, 2013, s. 15-16). Mayıs 2011'de Savunma Bakanlığı ve eğitimin gereklerini göz önünde bulunduran PLA, Çinli birliklerin ağ koruma seviyesini arttırmak ve ağ güvenliğini korumak için "Çevrimiçi Mavi Ordu (Online Blue Army)"yu kurmuşlardır (Xin, 2011).

2.2.8. NATO

NATO, Sırbistan'a karşı askeri operasyonlar başlattığında, çok sayıda profesyonel Sırp korsan grubu NATO'nun savaşla mücadele kabiliyetlerini bozma hedefiyle NATO'nun İnternet altyapısına saldırılar düzenlemişti. NATO'nun 1990'ların sonlarında Balkanlar'daki operasyonlarının ardından kendisine yönelik gelişen DoS saldırılarına karşılık, 2002 yılında siber savunma programına başlamıştır (Nato And Cyber Defence, 2009, s. 9-10). NATO, tehditlerin yayılması ve çeşitlenmesine cevap olarak siber saldırılara yönelik mücadelesini güçlendirmiştir ve Şubat 2012'de, NATO Bilgisayar Olayı Müdahale Kabiliyeti (Computer Incident Response Capability)'ni güçlendirmek ve NATO bilgisayar ağlarına yönelik siber saldırılara cevap vermesi için Grumman ve Finmeccanica ekibiyle 58 milyon avroluk bir sözleşme imzalamıştır. Siber savunmaya olan bağlılığın artması, 1 Temmuz 2012'de NATO İletişim ve Bilgi Kurumunun (Communications and Information Agency) oluşturulması çabalarına kadar yansımıştır (Robinson ve diğ, 2013, s. 34).

2008'de Tallinn'de araştırma, eğitim ve öğretim faaliyetlerinde bulunmak ve yasal, doktriner ve teknik siber savaş konularında uygulamalı çalışmalara ev sahipliği yapmak amacıyla NATO CCDCOE kurulmuştur. Önemli odak noktası yasal çerçevenin oluşturulmasıydı. Bu kapsamda Merkez; uluslararası hukukun, normların ve uygulamaların siber savaşa nasıl uygulanabildiğini incelemek için uluslararası bağımsız bir uzman grubu davet etmiştir. Bundan üç yıl sonra da "Tallinn Manual"

adlı bir taslak versiyon yayınlanmıştır. Bunun yanı sıra Merkez'in; akademi, özel sektör ve ordu arasında bir arayüz görevi görme; eğitim etkinlikleri ve uygulamalı çalışmaları düzenleme ve AB ile işbirliği de dahil olmak üzere büyük bir sosyal yardım misyonu işlevleri vardır (The Cyber Index, 2013, s. 107-108).

NATO yetkilileri, NATO'nun siber savunma politikasının bir parçası olarak Siber Savunma Yönetim Makamı (Cyber Defence Management Authority)'nı da kurmuşlardır. Makam, adından da anlaşılacağı gibi "uygun olduğunda acil ve etkili bir siber savunma eylemini" başlatmak ve koordine etmekle görevlendirilmiş NATO bünyesinde bir otoritedir. Makam; eğer bir müttefik veya müttefikler, ulusal veya müttefik öneme sahip bir siber saldırıya maruz kalırsa uyumlu bir çaba içerisinde eşgüdüm ya da yardım sağlamaya hazırlıklıdır. Bunun ardından NATO; üye devletlerin siber saldırılara karşı koyabilmeleri için, kendilerine sunulacak Hızlı Tepki Ekipleri (Rapid Reaction Teams-RRTs)'nin geliştirildiğini de duyurmuştur (Nato And Cyber Defence, 2009, s. 11-12).

NATO; mevcut siber savunma düzenlemeleri kapsamında, müttefikleriyle Mutabakat Muhtıraları (Memoranda of Understanding) imzalamıştır. Buna göre müttefikler arasında danışma mekanizmalarının oluşturulması, erken uyarı ve durumsal farkındalığın kolaylaştırılması ve geliştirilmesi için bir çerçeve tanımlanmıştır. NATO; aynı zamanda, Akıllı Savunma (Smart Defence) konseptinin bir parçası olarak Trans-Atlantik Savunma Teknolojik ve Endüstriyel İşbirliği (Trans-Atlantic Defence Technological and Industrial Cooperation) kapsamında endüstriyel ortaklarıyla bir diyalog başlatmıştır. Siber endüstri ile işbirliği, çok sayıda amaç için gereklidir. Bunlar: NATO'nun siber güvenlik ihtiyaçlarını her teknolojik düzeyde (teller gibi fiziksel unsurlardan veri şifrelemeye kadar) daha iyi belirlemek; uygun güvenlik ve dirençlilik standartlarını belirlemek; Akıllı Savunma konseptinde tanımlanan paylaşma ve fon oluşturma hedefleriyle tutarlı, uygun maliyetli çözümler ve uyarlanabilir yetenekler geliştirmektir (Joubert, 2012, s. 6-7).

Kasım 2010'da Lizbon'da, Devlet ve Hükümet Başkanları tarafından NATO Üyelerinin Savunması ve Güvenliği için yeni bir Stratejik Konsept ilan edildi. NATO, bu Konsept kapsamında birtakım kararlar almıştır: "Siber saldırıları önleme, tespit etme, savunma ve kurtarma yeteneğimizi daha da geliştirmek, NATO planlama

sürecini kullanma da dahil olmak üzere ulusal siber savunma yeteneklerini geliştirmek ve koordine etmek, tüm NATO kurumlarını merkezi siber koruma altına almak ve NATO siber farkındalığını, uyarısını ve müdahalesini üye ülkelerle daha iyi bir şekilde bütünleştirmek"tir (North Atlantic Treaty Organization, 2012).

NATO'nun özellikle Kuzey Atlantik Antlaşması'nın 5. maddesinde belirtilen "bir ittifak üyesine/üyelerine karşı yapılan silahlı bir saldırının, tümüne karşı bir saldırı olarak değerlendirileceği" vurgusu kapsamında siber saldırıya nasıl tepki verilmesi gerektiği konusunda süren tartışmalar, aşağıdaki gibidir (The Cyber Index, 2013, s. 109):

- Birincisi; siber saldırılar yasal olarak bir "silahlı saldırı" niteliğinde mi ele alınacak? Bu hala belirsizdir. Yeni Stratejik Konsept'te; siber saldırıların "ulusal ve Avrupa-Atlantik refahını, güvenliğini ve istikrarını tehdit eden bir eşiğe ulaşabileceği", yalnızca "toplu savunmaya" atıf yapıldığı ve bununla birlikte bir silahlı saldırı olarak ele alınmadığı görülmektedir.
- İkincisi; NATO üyeleri böyle bir saldırıya cezayla mı, saldırgan siber misyonlarla mı yoksa konvansiyonel saldırılarla mı cevap verilmesi gerektiği konusunda da bölünmüş durumdalar. NATO, kendi bilgisayar ağlarını korumak için siber savunma politikasını iyileştirmeye ve üye devletleri sağlam ulusal siber sistemler kurmaya teşvik etmektedir.

Sivil siber güvenlik konularıyla ilgilenme yetkisi olmayan NATO, Avrupa–Atlantik toplumlarının siber zorluklarını karşılamak için AB, Avrupa Güvenlik ve İşbirliği Teşkilatı (Organization for Security and Co-operation in Europe-OSCE) ve Uluslararası Telekomünikasyon Birliği (International Telecommunication Union-ITU) gibi çok taraflı kuruluşlarla uluslararası işbirliği ve tamamlayıcılık faaliyetlerinde bulunmaktadır.

2.2.9. Avrupa Birliği

Avrupa Konseyi; siber tehditleri, 2008 Avrupa Güvenlik Stratejisini Uygulama Raporuna "Avrupa güvenliği için yeni bir risk olarak" dahil etmiştir.

AB'nin politikasını; kritik bilgi altyapısının korunması ile ilgili olarak AB Komisyonunun 2009'da yayınladığı "Avrupa'yı büyük siber saldırılara ve kesintilere karşı koruma: hazırlıklı olma, güvenlik ve dayanıklılığın arttırılması" başlıklı bildirisi yansıtmaktadır. Bildiri, Avrupa için yaklaşmakta olan zorlukların geniş anlamda dört yönlü olduğunu belirtmiştir. Birincisi, AB üye devletlerinin eşit ve eşgüdümlü olmayan ulusal yaklaşımlarının olduğunu; ikincisi, kritik bilgi altyapıları için yeni bir Avrupa yönetişim modeline ihtiyaç duyulduğu; üçüncüsü, Avrupa erken uyarı ve olay müdahale kabiliyetlerinin sınırlı olduğunu; son olarak da uygun uluslararası işbirliğine yönelik potansiyel bir ihtiyacın olduğunu belirtmiştir. Bu bildiri, Avrupa dışı ulusal siber güvenlik politikalarıyla işbirliği yapmanın verimliliğine ve Avrupa Komisyonunun İnternet direncinin geliştirilmesinde Avrupa'nın temel değerlerini yansıtan bir dizi ilkenin geliştirilmesi için küresel topluma katılma çağrısıdır (Benoliel, 2015, s. 453-454). AB, siber güvenlik politikalarını geliştirme yaklaşımını, yukarıdaki bildiride ele aldığı çerçeve kapsamında sürdürmüştür.

Avrupa Birliği içinde siber güvenlik alanında, siber savaşla ilgili özel bir önemi olan iki temel politika alanı vardır. Birincisi, siber saldırılarla (siber suç / siber terörizm de dahil olmak üzere) mücadele etmeye yönelik tedbirlerdir. İkincisi, CI Korumasını ve Ağ Güvenliğini desteklemeye yönelik tedbirlerdir. Buna karşılık; kısmen gizli ve kurumlar arası doğası nedeniyle ve de sıklıkla üye devletlere bırakılan bir konu olarak algılanması yaklaşımındaki zorluklar neticesinde Ortak Dış ve Güvenlik Politikası'nın rolü daha az gelişmiştir. Ekim 2010'da kabul edilen AB İç Güvenlik Stratejisi, siber uzaydaki vatandaşlar ve işletmeler için güvenlik seviyesini yükseltmeyi ve siber suç meseleleriyle başa çıkmayı amaçlamıştır. Strateji, üç özel öneri içermiştir: Birincisi 2013 yılına kadar bir AB Siber Suç Merkezi'nin kurulmasıdır. İkincisi 2012 yılına kadar tüm AB kurumlarında bir Bilgisayar Acil Müdahale Timi (Computer Emergency Response Teams-CERTs) ağının kurulmasıdır. Sonuncusu 2013 yılına kadar bir Avrupa Bilgi Paylaşımı ve Uyarı Sistemi (European information sharing and alert system-EISAS)'nin başlatılmasıdır (Klimburg ve Tirmaa-Klaar, 2011, s. 29-31).

Bunun ardından, 7 Şubat 2013'te "AB'nin Siber Güvenlik Stratejisi: Açık, Güvenilir ve Güvenli Bir Siber Uzay (Cybersecurity Strategy of The European Union: An Open, Safe and Secure Cyberspace)" Avrupa Komisyonu tarafından sunulmuştur. Strateji, planlarının gerçekleştirilmesi için dikkatleri birtakım kurumlara çekmiştir: Bu kurumlar Avrupa Komisyonu, Avrupa Ağ ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency-ENISA), Avrupa Siber Suçlar Merkezi (European Cybercrime Center) ve Dayanıklılık için Avrupa Kamu-Özel Ortaklığı (European Public-Private Partnership for Resilience)'dır (Min ve diğ. 2015, s. 17).

2004 yılında oluşturulan Avrupa Ağ ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency-ENISA), ENISA, Avrupa siber güvenlik politikasına aktif olarak katkıda bulunmakta ve AB üyesi ülkelere yönelik gerçekleşen büyük ölçekli siber olaylara yanıt verilmesine destek olmaktadır. Bunun yanı sıra, AB'nin ağ ve bilgi güvenliği ile ilgili konularda politika ve yasaların geliştirilmesini ve uygulanmasını desteklemek ve üye devletlere/AB kurumlarına, gönüllülük esasına dayalı olarak sistem açıklarını açığa çıkarma politikalarının oluşturulmasında ve uygulanmasında yardımcı olmak gibi görevleri de vardır. Bunların dışındaki görevleri de aşağıdaki gibidir (ENISA):

- ✓ Pan-Avrupa Siber Güvenlik Tatbikatlarını hazırlamak,
- ✓ Ulusal siber güvenlik stratejilerinin geliştirmek ve değerlendirmek,
- ✓ CERT'lerin işbirliği ve kapasitelerini geliştirmek,
- ✓ IoT ve akıllı altyapılar üzerine çalışmalar, veri koruma konularının ele alınması, gizlilik arttırıcı teknolojiler ve yeni ortaya çıkan teknolojilerdeki gizlilik, eID'ler ve güven hizmetleri, siber tehdit ortamını tanımlamaktır.

Avrupa Komisyonu (European Commission) ve Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA), sivil alanda siber politika için baş muhattaplardır ve Avrupa üye devletleri özellikle de Kritik Bilgi Altyapısının Korunması, siber suç (özellikle teknoloji suç birimleri) ve ulusal/resmi CERT'ler ile ilgili yetkili makamlarla yakın işbirliği içerisindedir.

Komisyon içerisinde, bir müdahale/yanıtın oluşturulmasından sorumlu üç ana kurum aşağıdaki gibidir (Robinson ve diğ. 2013, s. 38-39):

- ✓ İçişleri Genel Müdürlüğü (Directorate-General Home Affairs): Ortak bir AB yaklaşımı geliştirmeyi ve siber suçlarla mücadeleyi desteklemeyi ve kolaylaştırmayı amaçlamaktadır.
- ✓ İletişim Ağları, İçerik ve Teknoloji Genel Müdürlüğü [(Directorate-General for Communications Networks, Content and Technology-DG CNCT), (eski adıyla Bilgi Toplumu ve Medya Genel Müdürlüğü-DG Information Society and Media)]: Üye devletlerdeki gelişmiş uygulamalarla direnci, Kritik Bilgi Altyapısı Korumasını ve IT güvenliğini desteklemeyi amaçlamaktadır.
- ✓ Avrupa Birliği Dış İlişkiler Servisi (European External Action Service): AB'nin siber uzay ve siber güvenlik konusundaki dış politikasını geliştirmektedir.

Europol; 2013 yılında Avrupa Siber Suçlar Merkezini, AB'deki siber suçlara karşı kolluk kuvvetini güçlendirmek ve böylece Avrupalı vatandaşları, işletmeleri ve hükümetleri çevrimiçi suçlardan korumaya yardımcı olmak amacıyla kurmuştur. Kuruluşundan bu yana, siber suçlarla mücadeleye önemli bir katkı sağlamış, yüzlerce tutuklama ile sonuçlanan onlarca sansasyonel operasyona ve yüzlerce de yerinde operasyonel destek uygulamasına katılmıştır (Europol EC3, 2013).

AB'nin kamu-özel işbirliği için bilgi paylaşım ağı olarak ENISA'ya dayanan Dayanıklılık için Avrupa Kamu-Özel Ortaklığı (European Public-Private Partnership for Resilience) kuruldu. Ortaklık; hem hükümeti hem de özel sektörleri, CI koruması ve dayanıklılığının güçlendirilmesi için politika yapma ve stratejik karar alma süreçlerine katılmaya teşvik eden bir çerçevedir. Esasen, güvenilir işbirliği için ortamın inşasını amaçlamaktadır. Bunun için sadece sınırlı üyelerin katılımına izin veren Gönüllü Öz-düzenleme sistemi uygulanmaktadır. Bununla birlikte, siber güvenlik stratejisi ile Ağ ve Bilgi Güvenliği'nin uygulanmasının ardından Avrupa Kamu-Özel Ortaklığı yetkisinin güçlenmesi neticesinde AB'nin Zorunlu Öz-düzenlemeye geçmesi beklenmektedir (Min ve diğ. 2015, s. 17).

Avrupa Birliği, üye devletlerin desteklenmesi için normların oluşturulması ve tartışılmasında ve siber suçlara karşı dayanıklılık önlemlerinin tartışılmasında önemli

bir rol oynamaktadır. Bununla birlikte; teknik, yasal ve politik uyumlaştırılmış önlemler açısından bireysel üye devletler ile AB kurumları arasında hala önemli farklılıklar bulunmaktadır. Sivil yönelimine rağmen AB; ABD ve Avrupa içindeki NATO ve OSCE gibi güvenlik örgütleriyle bağlantılı olarak yine de önemli bir oyuncudur (The Cyber Index, 2013, s. 105).

2.2.10. Küresel Siber Güvenlik Endeksi

ITU tarafından yayımlanan Küresel Siber Güvenlik Endeksi (Global Cybersecurity Index-GCI), ülkelerin siber güvenlik alanındaki gelişmişlik düzeylerini bir endeks aracılığıyla göstermektedir. GCI raporları, temel olarak aşağıda gösterilen 5 kategoriye (kategorilerde yirmişbeş adet gösterge mevcuttur) dayanılarak oluşturulmaktadır (Global Cybersecurity Index, 2019, s.7-8):

1. Yasal Tedbirler (Legal Measures): Siber güvenlik ve siber suçlarla ilgili yasal kurumların ve çerçevelerin varlığına dayalı önlemler.

2. Teknik Tedbirler (Technical Measures): Siber güvenlikle ilgili teknik kurumların ve çerçevenin varlığına dayalı önlemler.

3. Organizasyonel Tedbirler (Organizational Measures): Politika koordinasyon kurumlarının varlığına ve ulusal düzeyde siber güvenlik geliştirme stratejilerine dayalı önlemler.

4. Kapasite Geliştirme (Capacity Building): Kapasite geliştirmeyi teşvik eden araştırma ve geliştirme, eğitim ve öğretim programları, sertifikalı uzmanlar ve kamu sektörü kurumlarının varlığına dayalı önlemler.

5. İşbirliği (Cooperation): Ortaklıkların, işbirlikçi çerçevelerin ve bilgi paylaşım ağlarının varlığına dayalı önlemler.

GCI 2018 raporu, 193 ITU üyesi ülkeyi ve Filistin Devleti'ni kapsayarak hazırlanmıştır. Yukarıdaki kategoriler dikkate alınarak hazırlanan GCI 2018 raporundaki ülke sıralamalarını çalışmamızda ele aldığımız ülkeler bazında inceleyecek olursak ortaya çıkan sıralamaya göre İngiltere 1. sırada, ABD 2. sırada,

Estonya 5. sırada, G. Kore 15. sırada, Türkiye 20. sırada, Almanya 22. sırada, Rusya: 26. sırada ve Çin 27. sırada yer almıştır (Global Cybersecurity Index, 2019, s.62-63).

2.3. ÜLKELERİN SİBER GÜVENLİK STRATEJİLERİ UYGULAMALARINDAN ÖNE ÇIKAN HUSUSLAR

ICT'nin gelişmesi ve akıllı topluma giriş, hayatımızı kesinlikle zenginleştirmekte ve aynı anda bizi çok fazla tehlikeyle de karşı karşıya bırakmaktadır. Her devlet bu konuda aynı görüşü paylaşmakta ve karşı önlemleri de çok benzemektedir (Min ve diğ, 2015, s. 18-19).

Bazı önde gelen ülkelerin ve hükümetlerarası kurumların ulusal siber güvenlik politikalarının oluşturulma, yapılandırılma, uygulanma ve sürdürülme konusundaki perspektiflerinin analiz edildiği yukarıdaki incelemelerden de anlaşıldığı gibi ulusal stratejilerin içeriği çok çeşitlidir ve her ülke stratejisini ilgili ihtiyaçlarına göre yapılandırmıştır (Sabillon ve diğ. 2016, s. 80).

Yukarıda tek tek anahatları ile incelenen ülkelerin siber güvenlik strarejilerinden aşağıdaki sonuçlar çıkarılabilir (Ataç ve Akleylek, 2018, s. 608):

- ✓ Ülkelerdeki siber güvenlik hizmetinin, ülkelerin refah ve güvenliğine eşdeğer olduğu ve durumun ciddiyeti ve öneminin farkında oldukları tespit edilmiştir.
- ✓ Ülkelerin kurumsal siber güvenlik yapılarında stratejik farklılıklar gösterebildikleri görülmüştür.
- ✓ Ülkelerden biri, stratejiyi daha dağınık bir mekanizma ile uygulamaya yönelirken diğeri merkezi bir yapı oluşturarak uygulamaya yönelmiştir
- ✓ Ulusal siber acil durum planlarını oluşturan bu ülkeler, CI'lerin korunmasına öncelik vermişlerdir.
- ✓ İnsan boyutunun siber güvenliğin en zayıf zinciri olduğunu kabul ederek siber güvenlik konusundaki araştırma ve geliştirme çalışmalarına özel önem vermektedirler.
- ✓ Ülkenin siber güvenliğini yerel çalışmalarla değil uluslararası işbirliği kurarak gerçekleştirilebileceklerinin farkındadırlar.
- ✓ Yasal boyutun siber suçun tanımlanmasında ve önlenmesinde etkili bir rol oynadığı ve strateji belgelerinde bu konuya dikkat çekildiği iyi bilinmektedir.

- ✓ Ulusal standartlara uyarlar; güncel teknoloji ve yazılımların kullanımı ve üretimine gerekli değeri verirler.

Ülkelerin siber güvenlik alanına yönelik gelecekteki normlarının, kurallarının ve düzenlemelerinin uluslararası kurallar çerçevesinde nasıl bir seyir izleyebileceğine yönelik bir değerlendirme yapılarsa bundan sonraki stratejilerin genel amacının barışçıl, güvenli, istikrarlı ve öngörülebilir bir siber uzayı korumak ve daha da geliştirmek olacağı söylenebilir. Bu, daha odaklı, çok taraflı bir işbirliği ve çok paydaşlı bir süreç dahilinde yapılacabilecektir. Siber güvenlik tartışmaları, henüz erken bir aşamadadır ve yapılacak çok iş vardır (The Cyber Index, 2013, s. 138).

ÜÇÜNCÜ BÖLÜM

TÜRKİYE'NİN ULUSAL SİBER GÜVENLİK STRATEJİLERİ

3.1. TÜRKİYE İÇİN SİBER GÜVENLİK STRATEJİLERİNİN ÖNEMİ VE İHTİYACI

Bilgisayar ve internetin birbirine paralel olarak devam eden gelişim seyirleri, devletlerin de kamu hizmetlerini internet ve bilgisayar aracılığıyla sunmasını ve e-devlet olarak isimlendirilen uygulamayı beraberinde getirmiştir. Böylelikle de içerisinde olduğumuz bilişim çağı IT'leri, devletlerin sunmak durumunda olduğu hizmetlerde yer almaya başlamıştır. Tüm dünyada görülen bu süreç, Türkiye'de 1985'ten itibaren yapılan politika ve bilişim yatırımları sonucunda internet ve bilgisayar kullanımını yaygınlaştırmıştır. 2000'li yıllardan itibaren ise çok sayıda devlet kurumu hizmetlerini e-devlet üzerinden vermeye başlamıştır (Çarıkçı, 2010, s. 96-97).

Türkiye'de bilgisayarın kullanıma girmesi, 1960 yılına kadar geri gitmektedir. 1960'ta 1 adet bilgisayar kullanımıyla başlayan süreç, 1975 yılına gelindiğinde 111 adete çıkmış bulunmaktadır (Kılan, 1976, s. 595). 1993 yılına gelindiğinde, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)-ODTÜ'nün ortak çalışması ve Devlet Planlama Teşkilatı (DPT) projesiyle Türkiye'ye global internete erişme olanağının getirilmesiyle (Parlak, 2005, s. 30) birlikte bilgisayarlaşma ve internet kullanımlarında artışlar artarak devam etmiştir. İlk yıllarda sahip olunan bilgisayar adediyle ifade edilen bilgisayarlaşma, ilerleyen zamanlarda nüfus oranı ile açıklanmaya başlanmıştır (nüfusun %17,65'i gibi) (Aktaş, 2006, s. 5). Günümüz koşullarında ise bilgisayar kullanımı internet kullanım verileriyle paralellik göstermektedir. Türkiye'de bilgisayar ve internet kullanımının 2019 yılı itibariyle 56 milyona ulaşacağı tahmin edilmektedir (Statista, 2018).

Bilginin oluşturulması, elde edilmesi, saklanması çoğaltılması ve gerektiğinde tekrar ulaşılıp kullanılmasında veya başka şekil ve bilgilere dönüştürülmesinde kullanılan teknolojilerin tümünü ifade eden ICT'nin önemli sonuçlarından birisi; e-devlet (Öztaş ve Yürük, 2017, s. 2154), diğeri ise e-devletleşme ile birlikte tüm CI'lerin siber uzayın birer bileşeni haline gelerek siber uzaydaki siber saldırılara açık hale gelmesi olmuştur. Buna en iyi örnek olarak da Estonya'nın aşırı derecede siber uzaya bağımlı hale gelmesi neticesinde karşı karşıya kaldığı saldırılar gösterilebilir. Estonya'ya yönelik siber saldırılar ile birlikte dünya gündeminde "devletler düzeyinde siber savaş" olarak yer edinmeye başlayan siber güvenlik sorunu, esasında Estonya'nın neredeyse her hizmetini e-devlet uygulamaları üzerinden vermesi ile gerçekleşmişti. Bu sürece varılmasının kapılarını e-devlet uygulamalarının yaygınlaşması aralamıştır.

Bu çerçevede Türkiye'nin bilgisayarlaşması ve internet kullanımının artmasına paralel olarak yaygınlaşan e-devlet uygulamalarının önemlilerine göz atmak Türkiye'nin de Estonya gibi e-devletleşmeye başladığını göstermesi açısından önemlidir. E-devlet politikasının oluşumuna öncülük eden çalışmaların başında Türkiye Ulusal Enformasyon Altyapısı Ana Planı (TUENA) gelmektedir. Bunun yanı sıra Türkiye'nin e-devletleşmesi sürecinde öne çıkan önemli uygulamalardan bazıları ise E-Dönüşüm Türkiye Projesi ve MERNİS (Merkezi Nüfus İdaresi Sistemi), VEDOP (Vergi Daireleri Otomasyon Projesi), GİMOP (Gümrük İdaresinin Modernizasyonu Projesi) gibi uygulamalardır.

Türkiye'nin, "TUENA" planı, Başbakanlığın 5 Şubat 1996 günlü direktifi gereğince, Ulaştırma Bakanlığı'nın koordinatörlüğünde ve aynı Bakanlığın Başkanlığını yaptığı, Genelkurmay Başkanlığı, MGK Genel Sekreterliği, DPT, Yükseköğretim Kurulu (YÖK), TTGV (Türkiye Teknoloji Geliştirme Vakfı), Türk Elektronik Sanayicileri Derneği (TESİD), Türkiye Bilişim Sanayicileri Derneği (TÜBİSAD) ve Türk Telekom temsilcilerinden oluşan bir kurulun denetiminde, TÜBİTAK tarafından 1999 başlarında tamamlanmış ve 11 Ocak 2000 yılında Çankaya Köşkü'nde düzenlenen bir törenle dönemin başbakanı olan Süleyman Demirel tarafından kamuoyuna duyurulmuştur (Göker, 2000, s. 1).

Ana Plan'ın hazırlanması ile ilgili olarak yapılan çalışmaların yer aldığı sonuç raporu incelendiğinde, kamu yönetiminde de bilgi ve iletişim teknolojilerinin kullanılması ile ilgili genel bir çerçeve ortaya koymaları amacıyla çalışma gruplarının oluşturulduğu, bunların rapor hazırladığı sunumlar gerçekleştirdiği görülmektedir. Ayrıca sonuç raporunda söz konusu gruplarının çalışmalarına dayanak olan pek çok başlığın (bilgi teknolojilerine erişim altyapısının geliştirilmesi, eğitim, sağlık gibi alanlardaki kamu hizmetlerinin elektronikleşmesi gibi) bulunduğu görülmektedir. Dolayısıyla TUENA kapsamındaki çalışmalar ve bu çalışmaları açıklayan sonuç raporu e-devlet politikasının oluşum sürecinde önemli bir belge niteliğindedir (Demirhan, 2011, s. 69-70).

TUENA planının hazırlanmasının ardından e-devlet projeleri, stratrejileri ve uygulamaları devlet yönetiminde ve toplumsal yaşamda daha fazla yer edinmeye başlamışlardır. Bu stratrejilerden E-Dönüşüm Türkiye Stratejisi; Vatandaşlara daha kaliteli ve hızlı kamu hizmeti sunabilmek amacıyla; katılımcı, şeffaf, etkin ve basit iş süreçlerine sahip olmayı ilke edinmiş bir devlet yapısı oluşturmak amacıyla 58. hükümet tarafından ortaya konulmuş bir projedir. Koordinasyonu, izlenmesi, değerlendirilmesi ve yönlendirilmesi ile ilgili olarak DPT görevlendirilmiştir. Bu strateji ile kısaca şunlar amaçlanmaktadır (Başbakanlık Genelgesi, 2003, s. 1):

- ✓ ICT politikaları ve mevzuatının Avrupa Birliği müktesebatı çerçevesinde gözden geçirilerek yeniden düzenlenmesi ve E-Avrupa+ kapsamında aday ülkeler için öngörülen eylem planının uyarlanması,
- ✓ Vatandaşın; ICT yardımıyla, kamusal alandaki karar alma süreçlerine katılımını sağlayacak mekanizmaların geliştirilmesi ve kamu idaresinin şeffaf ve hesap verebilir hale getirilmesine katkıda bulunulması,
- ✓ Kamu hizmetlerinin sunumunda ICT'lerden azami ölçüde yararlanılarak iyi yönetişim ilkelerinin hayata geçirilmesine katkıda bulunulması,
- ✓ ICT'lerin kullanımının yaygınlaştırılması,
- ✓ ve ICT alanında kaynak israfını azaltmak amacıyla, kamu kurumlarının örtüşen yatırım projelerinin bütünleştirilmesi, izlenmesi, değerlendirilmesi ve yatırımcı kamu kuruluşları arasında gerekli koordinasyonun sağlanmasıdır.

En önemli projelerden bir diğeri olarak karşımıza çıkan Mernis projesi; her vatandaşın bir kimlik numarası ile takibini esas alan ve 2002'de çevrimiçi olarak hizmet sunumuna geçen bir uygulamadır. VEDOP, vergi ile ilgili işlemlerin elektronik ortamda yapabilmesini amaçlayan projedir. GİMOP projesi ise 69 gümrük idaresindeki işlemlerin %99.5'inin elektronik ortamda yapılmasını sağlayarak gümrük işlemlerini kolaylaştırmaya dönük bir uygulama olarak karşımıza çıkmaktadır (Çukurçayır ve Çelebi, 2009, s. 73-74).

Türkiye'nin siber uzayın getirdiği avantajlardan aşırı yararlanma isteği; çok sayıda siber saldırıya maruz kalmasını da beraberinde getirmiştir. Bu bağlamda, ICT güvenliği yönünden Türkiye'nin diğer ülkelere göre konumu, farklı ölçütlere göre ele alındığında aşağıdaki sonuçlara ulaşılacak şekildedir:

- ✓ Amerikalı siber güvenlik firması olan FireEye bünyesindeki E-Posta ve Ağ koruması servisleri tarafından hazırlanan istihbarat raporuna göre; Türkiye'nin kısmen modern ama alarm verici seviyede güvensiz olan internet altyapısının adeta kötü amaçlı yazılım kaynadığını ve 2016 yılında Türkiye'de bütün Avrupa'da meydana gelenden daha fazla "kötücül yazılım" olduğunu tespit etti. FireEye sözcüsüne göre bu kategorideki sızmalar; muhtemelen devlet destekli, gelişmiş ve bilinen bilgisayar korsanları aktiviteleri ile aynı karakteristiklere sahiptir (Siberbülten, 2017).
- ✓ Symantec'in İnternet Güvenlik Tehdit Raporu'na göre Türkiye, 2016 yılında Avrupa, Ortadoğu ve Afrika'nın tüm zararlı yazılım tespitlerinin toplamının % 3.4 kadarını meydana getirmiştir (Siberbülten, 2017).
- ✓ Fortinet firması tarafından Ağustos 2016'da yayınlanan 2016 ikinci çeyrek siber tehdit analiz raporunda botnet, zararlı yazılım (malware) ve istismar kiti (exploit kit) tespit edilen ülke istatistiklerinde Türkiye'nin ilk 5 içerisinde yer aldığı ve bu raporla ülkemizdeki kontrol dışı bilgisayarlara yönelik soruna dikkat çekildiği görülmektedir (STM, 2016, s. 3).
- ✓ Trend Micro tarafından yayımlanan 2016 yılının ilk yarısına ait bir diğer güvenlik raporundaki veriler, tüm dünyada fidye yazılım saldırılarının yüzde 172 oranında arttığını, ülkemizin Avrupa bölgesinde fidye yazılım saldırılarını en

fazla yaşayan ülke olduğunu, dünyada ise ABD ve Brezilya'dan sonra üçüncü sırada yer aldığını ifade etmektedir (STM, 2016, s. 5).

- ✓ Trend Micro'nun araştırması, ülkemizde on-line bankacılığa yönelik tehditlerin de hız kesmeden devam ettiğini gözler önüne sermektedir. Tespitlere göre ülkemiz 11 bin 516 saldırı ile Avrupa bölgesinde en fazla on-line bankacılık saldırısı alan ülke olurken ülkemizi 4 bin 880 saldırı ile Almanya ve 3 bin 529 saldırı ile Fransa izlemektedir. (STM, 2016, s. 5).
- ✓ Küresel pazar araştırma şirketi Vanson Bourne'nun yaptığı araştırmaya göre dünya genelinde şirketler veri sızıntısını engellemek için aylık ortalama 4129 Euro harcama yaparken Türk şirketlerinin 3220 Euro harcadığı ifade edilmektedir (Aslay, 2017, s. 27).
- ✓ Cybersecurity Ventures firması tarafından en son yayımlanan 2016 üçüncü çeyrek siber güvenlik market raporuna göre önümüzdeki 5 yıl içerisinde siber suçların 2015'te 3 trilyon $ olan maliyetinin 2021'de 6 trilyon $ civarında olması beklenmektedir. Raporda dikkat çekici bir diğer husus da 2020'ye kadar günümüzdekinin 50 katı daha fazla veriyi siber tehditlerden korumak zorunda olacağımızdır. Siber suçlardaki bu artışlar, doğal olarak siber saldırılarla mücadele için ayrılan bütçeleri gittikçe çok daha yukarılara çekiyor. Kurumlar, bu tarz durumların yaşanmaması adına bilgi güvenliği hizmetleri sunan şirketlerden ürün ve danışmanlık satın almaktalar. Bu kapsamda, 2015'te 75 milyar $ olan siber güvenlik harcamalarının önümüzdeki 5 yıl içerisinde toplamda 1 trilyon $ olacağı öne sürülmektedir (STM, 2016, s. 5).

Yukarıdaki tespitlere ek olarak Türkiye'nin fiili olarak maruz kaldığı çok sayıda siber saldırıdan söz etmek de mümkündür. Türkiye'de de ABD ve İngiltere'dekine benzer birçok saldırı vuku bulmuştur.

Türkiye'ye yönelik saldırılardan bazıları aşağıdaki gibidir (Aytekin, 2015, s. 101):

- ✓ 2011 ve 2012 yılında, işbirliği içerisinde çalışan uluslararası siber korsan grubu Anonymus, internet özgürlüğü ve ifade hakkının korunmasına yönelik içerisinde Emniyet Genel Müdürlüğü, İçişleri, Dışişleri ve Adalet

Bakanlıklarının bulunduğu yirmiye yakın devlet sitesine internet erişimini engellemek amacıyla saldırmıştır.

- ✓ 2014 yılında ise HSBC Türkiye'ye yapılan siber saldırılar sonucunda 2,7 milyon müşterinin kredi kartı bilgilerinin alındığını, müşterilerin korunması maksadıyla banka tarafından bir takım önlemlerin alındığını ve ilgili kurumlarla ulusal ve uluslararası işbirliğinin devam ettiğini bir basın açıklaması ile bildirilmiştir.
- ✓ 31 Mart 2015'te de Türkiye'de sebebi halen belirlenemeyen uzun süreli bir elektrik kesintisi yaşanmıştır. Bu olayın nedenleri arasında bir siber saldırı olasılığının göz önünde tutulduğu bildirmiştir.

Bilgi Güvenliği Derneği Başkanı Prof. Dr. Mustafa Alkan, siber saldırılara en çok maruz kalan 10 ülkeden birinin Türkiye olduğunu; İngiltere, İsrail, İran, Rusya, ABD ve Çin'in ise gerçek manada siber ordulara sahip olmalarının yanında bir tek savunma amaçlı değil saldırı amaçlı siber timlere de sahip olduklarını belirtmiştir. Gazi Üniversitesi Bilgisayar Mühendisliği Bölüm Başkanı Şeref Sağıroğlu da Türkiye'nin günde ortalama 15.000 siber tehditle karşı karşıya kaldığını ve fiilen bir siber savaş halinde olduğunu vurgulamıştır. İnternet güvenlik şirketi McAfee'nin 2012'de açıkladığı güvenlik araştırması, siber saldırılar karşısında en hazırlıklı ülkelerin Finlandiya, İsveç ve İsrail olduğunu ortaya koymuştur (Ege, 2012). Dünyada, siber saldırılara maruz kalan ülkeler sıralamasında 2014 yılı itibariyle 4. sırada bulunan Türkiye'nin bunun yanında Milli Askeri Projeler alanında da ilerlemeler kat etmesi siber güvenliğe ağırlık vermesini beraberinde getirmiştir (Özalp, 2014).

Yukarıda örneklerini daha da çoğaltabileceğimiz siber saldırılar ve siber güvenlik risk raporları, Türkiye'nin siber güvenlik politikaları oluşturma sürecine dahil olmasını beraberinde getirmiştir. 2013 yılı itibariyle 100'den fazla devletin siber yeteneği bulunmaktayken bu devletlerden en az 50 tanesinin ise gelecekteki ekonomik ve ulusal güvenlik girişimlerinde siber güvenliğin önemine vurgu yapan yayınlanmış bir çeşit siber stratejileri bulunmaktadır (Akyazı, 2013). Bu devletler arasında Türkiye de siber güvenlik politika çalışmaları oluşturan bir devlet olarak yer almıştır.

Bu çerçevede siber güvenlik alanında Türkiye'de atılan önemli adımlar, 2003 yılından itibaren yapılmıştır. Kamu ağırlıklı olan bu çalışmalara özel sektör ve STK'ler tarafından da katkılar sunulmuştur (Erçağlar, 2017, s. 30). Siber güvenliğin dünya çapında devletler düzeyinde yakaladığı gündem, yaşanan siber saldırı ve siber olaylar, dünya devletlerinin konuya olan ilgisinin artmasını sağlamıştır. Bu çerçevede Türkiye de bu alanda çalışmalar yapmaya başlamıştır. Türkiye, siber güvenliğine ilişkin hukuki altyapı çalışmalarını 2000'li yılların başında oluşturmaya çalışsa da somut bir sonuç ortaya koyamamış; ülke, siber güvenlik alanındaki hukuki düzenlemelerini ancak 2012 yılı itibariyle oluşturulabilmiştir. Düzenlemeler kapsamında mevcut kurumlara siber güvenliğe ilişkin yeni görev tanımları getirilmiş ve siber güvenlik alanında yeni görevler üstlenecek yeni kurumlar kurulmuştur (Göçoğlu, 2018, s. 158).

3.2. SİBER GÜVENLİK ALANINDA YAPILAN YASAL DÜZENLEMELER

Siber güvenliği sağlamaya yönelik yapılan yasal düzenlemeler siber uzayın doğası gereği hem ulusal hem de uluslararası düzeyde olmak zorundadır. Bunun nedeni siber uzayın tüm ülke sınırlarının çok ötesinde olmasından kaynaklanmaktadır. Bu bağlamda Türkiye'de siber güvenliği sağlamaya yönelik yapılan yapılan yasal düzenlemeler de hem ulusal hem de uluslararası yasal düzenlemelerle sağlanmaya çalışılmıştır.

3.2.1. Ulusal Yasal Düzenlemeler

3.2.1.1. 2003/10 Sayılı Başbakanlık Genelgesinin Yayımlanması

Türkiye'de siber güvenliğe yönelik çalışmaların geçmişi, 2000'li yıllarda başlatılan Bilgi Sistem ve Ağ Güvenliği başlıklı çalışmalara dayanmaktadır. Ekonomik İş birliği ve Gelişme Teşkilatı'nın (Organisation for Economic Co-operation-OECD) ICT'lerin güvenli kullanılmasına yönelik tavsiye niteliğinde hazırladığı "Bilgi Sistemlerinin Güvenliğine İlişkin Rehber İlkeler"in "2003/10 sayılı Başbakanlık Genelgesi"yle bilhassa kamu kurum ve kuruluşları tarafından yürütülen çalışmalarda göz önünde bulundurulması istenmiştir (Meral, 2015, s.118).

Siber güvenlik alanında atılan adımların ilki olan “2003/10 sayılı Başbakanlık Genelgesi” ile güvenlik kültürünün oluşturulması ve bu konuda nelerin yapılabileceği konusunda önerilerin sunulması amaçlanmıştır. Bu genelge sonucunda siber güvenlik alanında yapılan çalışmalar hız kazanmış ve siber güvenliğe ilişkin bilinçlendirme eğitimlerinin, toplantıların ve kuruluşların gerekliliği fark edilmiştir (Erçağlar, 2017, s. 30).

3.2.1.2. 5070 Sayılı Elektronik İmza Kanunu (2004)

"Elektronik İmza Kanunu", Elektronik Sertifika Hizmet Sağlayıcılarının yetkilendirilmesi ve denetlenmesinin yanı sıra güvenli elektronik imzayla ilgili teknik kriterleri düzenler (Çil ve diğ. 2012, s. 117). 2004’te kabul edilen bu kanun ile elektronik imzanın geçerliliği kabul edilmiş ve sahte elektronik sertifikanın yapılması ve kullanılması da suç kapsamına alınmıştır (Sınav, 2014, s. 102).

Elektronik imza, elektronik ortamda hazırlanan dokümanları imzalamak için kullanılan bir elektronik koddur. Güvenilirliği şifrelenmiş olmasından kaynaklanır. Elektronik imza sistemi, şifrelenmiş verileri gönderen bilgisayar ile bu şifrelemeyi çözebilen alıcı bilgisayar arasında çalışır. Gönderenin şifreleme işlemi ile alıcının doğrulama işlemi, verinin güvenli bir kaynaktan geldiğini gösterir. Bu iki taraflı işlem elektronik imzayı tamamlar (T.C. Sağlık Bakanlığı EBYS, 2018).

3.2.1.3. Telekomünikasyon Yoluyla İletişimin Denetlenmesi Kanunu (2005)

“2003/10 Sayılı Başbakanlık Genelgesinin Yayımlanması” neticesinde açığa çıkan farkındalık ile 2005’in Kasım ayında önemli bir gelişme olarak “Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik” yayımlanmıştır.

Telekomünikasyon; her türlü işaret, sembol, ses ve görüntünün ve elektrik sinyallerine dönüştürülen her türlü verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri

vasıtasıyla iletilmesi, gönderilmesi ve alınmasını ifade etmektedir. Bu çerçevede yönetmelik, telekomünikasyon yoluyla yapılan iletişimin istihbarat veya suçun önlenmesi amacıyla denetlenebileceği gibi işlenmiş olan suçların soruşturma ve kovuşturmasında delil elde etmek amacıyla da denetlenebilme olanağını vermektedir (Şahin, 2007, s. 1095-1098).

Daha sonra, 2011'de yapılan bir değişiklikle telekomünikasyon yoluyla yapılan iletişim tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınması konularında teknik işleri yürüten teknik daire başkanlığı kaldırılarak yerine "Teknik İşletme" ve "Bilgi Sistemleri" daire başkanlıkları kuruldu. Teknik İşletme, güvenli iletişim altyapısının kurulmasından; Bilgi Sistemleri de yazılımları geliştirmeden sorumlu tutulmuşlardır (Dünya, 2011).

3.2.1.4. 5651 Sayılı İnternetle İlgili Kanun (2007)

Siber güvenlik alanındaki hukuki çalışmalar, siber suçların tespiti ve zararlı içeriklerin önüne geçilmesini önlemek şeklinde devam etmiştir. Bu kapsamda 2007'de "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"un yayımlanması gündeme gelmiştir.

Bu kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemektir. Bu yasa ile internet ortamında işlenen suçların önüne geçilmesi amaçlanmış fakat İnternet ortamında işlenen suçlarla ilgili her gün yeni bir haberin basına yansıması yasanın bu suçları önlemede yetersiz kaldığını düşündürmektedir (Demirhan, 2011, 188-189).

6 Şubat 2014 tarihinde kabul edilen 6518 sayılı torba yasası, "5651 Sayılı İnternetle İlgili Kanun"da bazı değişiklikler yapmıştır. Bu kapsamda ulusal siber güvenlik faaliyetleri kapsamında içerik, alan, hizmet sağlayıcıları, siber saldırıların tespit edilmesi ve önlenmesi konusunda diğer ilgili kurum ve kuruluşlar arasındaki koordinasyondan Telekomünikasyon İletişim Başkanlığı (TİB) sorumlu tutulmuştur (Çelikpala ve diğ. 2015, 36).

Günümüzde de güncellenerek geçerliliğini koruyan 5651 Sayılı İnternetle İlgili Kanun'un uygulanması kapsamında, 2008-2015 yılları arasında 80.062 tane siteye erişim engeli getirilmiştir (Ünal, 2015, s. 304).

3.2.1.5. İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik (2007)

2007 yılında çıkarılan "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"a dayanılarak Kasım 2017'de çıkarılan (İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik, 2017) bu yönetmelik ile siber saldırıların ve kötü niyetli içeriklerin yayınlanmasının engellenmesi amaçlanmıştır (Kaya, 2017, s. 22).

Yönetmelik, kişilere belirli bir yerde ve belirli bir süre boyunca internet ortamı kullanım olanağı sağlayan tüm gerçek ve tüzel kişilerin sorumluluklarını düzenlemektedir. Yani havalimanları, oteller, kafeler, işverenler vb. kısacası herhangi bir vasıtayla internet ortamına bağlanarak kullanım olanağı sunan tüm kişilerin ve kuruluşların mutlaka farkında olması gereken bazı konular bulunmaktadır. Bunların en önemli ve çarpıcıları, erişim kayıtlarını kendi sistemlerine kaydederek bunları iki yıl süreyle saklamak; suç teşkil eden içeriklere girişi engelleyen filtre mekanizmaları kullanmak, SMS ve benzeri yöntemlerle hizmet verilen kullanıcıları tanımlayabilecek sistemler kurmak, VPN ve sair tüm dolanıcıları devre dışı bırakacak sistemler kurmaktır. Görüldüğü üzere hem ticari olan hem de olmayan ciddi masraflar ve formaliteler öngören düzenlemeler söz konusudur (Kocasu, 2017).

3.2.1.6. 5809 Sayılı Elektronik Haberleşme Kanunu (2008)

5809 sayılı "Elektronik Haberleşme Kanunu", elektronik haberleşme sektörü için güvenlik ve hizmet kalitesi standartlarına ve şartnamelere uygunluk da dahil olmak üzere izinsiz erişime karşı ağların güvenliğini sağlamak için bilgi güvenliğini ve iletişimin gizliliğini düzenler. Mevzuatta öngörülen gerekli önlemleri alma görevi, Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yerine getirilmelidir (Çil ve diğ. 2012, s. 117).

6 Şubat 2014 tarihinde kabul edilen 6518 sayılı torba yasası, "5809 sayılı Elektronik Haberleşme Kanunu"nda da bazı değişiklikler yapmıştır. Bu değişikliklerle BTK, "Bakanlar Kurulu, UDHB (Ulaştırma, Denizcilik ve Haberleşme Bakanlığı) ve/veya Siber Güvenlik Kurulu (SGK) tarafından verilen siber güvenlik ve internet alanları ile ilgili görevleri TİB veya diğer birimlerinin kullanımı yoluyla yerine getirmekten sorumlu olmuştur." Torba yasasının 106. maddesiyle SGK'ye siber güvenlikle ilgili politikaları, stratejileri ve eylem planlarını onaylama görevi verilmiş ve SGK bu politikaların, stratejilerin ve eylem planlarının ülke genelinde etkin bir şekilde uygulanması konusunda gerekli kararları almaktan, CI'nin belirlenmesi için öneriler hakkındaki kararların kesinleştirilmesinden, siber güvenlik konusundaki düzenlemelerin tamamından veya bir kısmından muaf tutulacak kurum ve kuruluşların belirlenmesinden ve kanunla öngörülen diğer görevlerin yerine getirilmesinden sorumlu olmuştur. Yasa değişikliği, SGK çalışmalarına ilişkin kılavuz ilkelerin ve prosedürlerin Başbakanlık Ofisi tarafından yapılan düzenlemelere göre belirlenmesini önermiştir (Çelikpala ve diğ. 2015, 36).

Bu kanun, AB'ye uyum faaliyetleri kapsamında gelişen teknolojinin kendisiyle birlikte getirdiği sorunları çözmek amacıyla çıkartılmış bir yasadır (Sınav, 2014, s. 102). Bu düzenlemeden anlaşılan şey, siber güvenlik politikası üretim sürecinde alınacak olan politika kararlarının yürütme mekanizmasının Bilgi Teknolojileri ve İletişim Kurumu olarak belirlenmiş olduğudur. Söz konusu düzenlemeye benzer fakat daha kapsamlı bir şekilde yapılan bir diğer önemli düzenleme ise 5809 sayılı Elektronik Haberleşme Kanununun 5. maddesinin birinci fıkrasına eklenen "h" bendidir. Bu düzenlemeyle UDHB'ye siber güvenlik ile ilgili "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı (2012)" başlığında ele alınacak olan görevler verilmiştir. Böylelikle de bakanlığın görevleri arasına ilk kez siber güvenlik kavramına ilişkin fonksiyonlar eklenmiş, önceki yıllarda Millî Savunma Bakanlığı üzerinde düşünülen siber güvenlik fonksiyonları da bu bakanlığa devredilmiştir. Bu faaliyetler sonucunda da Türkiye'nin siber güvenlik politikalarında yetkili en üst merkezi aktörü UDHB olmuştur (Göçoğlu, 2018, s. 156-157-158).

3.2.1.7. 5846 Sayılı Fikir ve Sanat Eserleri Kanunu

İnsan ürünü olan şiir, roman, müzik, resim, fotoğraf, film gibi edebi ve güzel sanatların konusu olan eserler; bilimsel eserler ve bilgisayar yazılımlarını (Cebe ve Suçin, 2014, s. 120) kapsayan bu kanunun amacı, fikir ve sanat eserlerini meydana getiren eser sahipleri ile bu eserleri icra eden veya yorumlayan icracı sanatçıların, seslerin ilk tespitini yapan fonogram yapımcıları ile filmlerin ilk tespitini gerçekleştiren yapımcıların ve radyo-televizyon kuruluşlarının ürünleri üzerindeki manevi ve mali haklarını belirlemek, korumak, bu ürünlerden yararlanma şartlarını düzenlemek, öngörülen esas ve usullere aykırı yararlanma halinde yaptırımları tespit etmektir (5846 Sayılı Fikir ve Sanat Yapıtları Kanununun Bazı Maddelerinin Değiştirilmesine İlişkin Kanun, 1995).

3.2.1.8. Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı (2012)

Siber güvenlik alanında Türkiye'de atılan ciddi adımlardan bir diğeri, 2012'nin Ekim'inde yayımlanmış olan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı"dır. Böylelikle Türkiye siber güvenlik alanındaki çalışmalarına resmen başlamıştır. İlgili bakanlar kurulu kararınca; siber güvenlik konusunda Ulaştırma Denizcilik ve Haberleşme Bakanlığı (UDBH)'na sorumluluklar verilmiş, SGK oluşturulmuş ve siber güvenlikle ilgili geçici kurullar ve çalışma gruplarının oluşturulabileceği karara bağlanmıştır (Erçağlar, 2017, s. 31-32). Bu karar çerçevesinde SGK, UDBH'nin başkanlığında kurulmuştur (Ercan, 2015, s. 27).

Yukarıdaki kararla ulusal siber güvenliğin sağlanmasıyla ilgili politika, strateji ve eylem planlarının hazırlanması görevi TÜBİTAK'tan alınıp UDHB'ye verilmiştir. Bununla birlikte bu karar, siber güvenlik konusunda atılan en kapsamlı adım olması ve stratejik boyutta değerlendirilebilecek ilk somut adım olması yönünden de oldukça önemlidir. Yazılım ve donanım altyapılarında mümkün olduğu kadar milli kaynakların kullanılması esasının vurgulandığı bu kararda, kamu kurum ve kuruluşları tarafından siber güvenlik alanında yapılacak olan çalışmalar için gerekli maddi kaynak tahsisine öncelik verilmesi istenmiştir (Meral, 2015, s. 120-121).

3.2.1.9. Kişisel Verilerin Korunması Kanunu (2016)

Günümüzde bireylere ilişkin çeşitli veriler, gelişen teknolojinin de etkisiyle her gün farklı platformlarda kolaylıkla işlenebilmekte ve aktarılabilmektedir. Bu verilerin işlenmesi, kişiler ile mal ve hizmet sunanlar bakımından bazı kolaylıklar ve avantajlar sağlasa da verilerin istismar edilme riskini de beraberinde getirmiş ve bu nedenle de kişisel verileri koruyabilmek adına hukuki bir altyapının oluşturulması da zorunluluk halini almıştır. Bunun yanı sıra Avrupa Konseyi tarafından, tüm üye ülkelerde kişisel verilerin aynı standartlarda korunması ve sınır ötesi veri akışı ilkelerinin belirlenmesi amacıyla hazırlanan "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin 108 Sayılı Sözleşme", 1981 tarihinde imzaya açılmış ve ülkemiz tarafından da 2016'da imzalanarak iç hukukta da düzenleme yapılması gerekli hale gelmiştir (Bilir, 2018, 7-8-9).

Türkiye'nin 2016'ya kadar bir kişisel verilerin korunması kanununun bulunmaması, onu uluslararası alanda güç durumda bırakmaktaydı. Bununla birlikte, kişisel verilerin korunmasıyla ilgili mevcut bir çalışmanın olmamasından dolayı da çok sayıda ülke Türkiye'yle bilgi paylaşımına sıcak bakmamaktaydı. Böyle bir kanunun çıkarılması ve Kişisel Verileri Koruma Kurumunun kurulup faaliyete geçirilmesiyle birlikte diğer ülkelerle yapılacak ortak faaliyetlerin önü açılacaktı. Bunun üzerine TBMM, kanunu 24 Mart 2016'da onaylamıştır (Sanalp, 2016, s. 45-46).

Bu kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir (Kişisel Verilerin Korunması Kanunu 2016).

3.2.2. Uluslararası Yasal Düzenlemeler (Siber Suçlar Sözleşmesi)

Daha önceki başlıklarda ve çalışmamızın ilgili başlıklarında ele aldığımız kanun, yönetmelik ve uygulamalar ile Türkiye, siber güvenliğe ilişkin kendi içerisinde her ne kadar tedbirler almışsa da siber saldırıların sınır tanımamazlığı yüzünden ülkeler arasında da yapılması gereken birtakım çalışmalar ihtiyaç halini almıştır.

Siber güvenlik alanında uluslararası bir anlaşmanın hayata geçirilmesi, düzenli olarak gündeme getirilen bir konu olmuştur. Bugüne kadar bu çabaların gerçekleştirilmesine yönelik atılan en başarılı adım, Siber Suç Sözleşmesi'dir. Bu Sözleşme, siber suçlara dayanan ulusal yasaları uyumlulaştırmayı amaçlayan ve hem kamu hem de üye olmayan ülkeler tarafından bile onaylanan en kapsamlı uluslararası anlaşma metnidir. Siber riskler konusunda uluslararası düzenlemelerde en zorlu şey, milletlerin farklı otoritelere ve önceliklere sahip olmalarıdır. Bununla birlikte, belki de daha da önemlisi, bir siber suçu neyin tanımladığı ve bir siber ortamda neyin olmadığı konusunda fikir birliği olmamasıdır. Tüm bu zorluklar, doğalarının bir parçası olarak ortaya çıkan belirsizliği, riskleri ve tehditleri arttırır ve uluslararası işbirliği ve düzenleme çabalarını sorunlu hale getiren bir 'gri alanı' ortaya çıkarmaktadır (Han ve Çelikpala, 2015, s. 62).

Zorluklarına rağmen Siber Suçlar Sözleşmesi, çok sayıda ülkeyi ortak bir paydada buluşturabilmesiyle uluslararası siber güvenlik alanında önemli bir boşluğu doldurabilmiştir. 2001'de Budapeşte'de kabul edilen, 2010'da ise Avrupa Konseyi bünyesinde imzalanan ve bilgisayar ağları yoluyla yapılan kanunsuz davranışlara yönelik uluslararasında geçerliliği bulunan ilk ve tek antlaşma özelliğine sahip olan Siber Suçlar Sözleşmesi (Erçağlar, 2017, s. 31), Türkiye tarafından 10 Kasım 2010'da imzalanmış; fakat TBMM o tarihte onaylamadığı bu sözleşmeyi 2014'te onaylamıştır (Ercan, 2015, s. 30). Bu sözleşme kapsamında Türkiye'nin kendi iç yasalarını Avrupa Siber Suçlar Sözleşmesine paralel olarak uyarlaması gerekmektedir (Çil ve diğ. 2012, s. 121).

3.3. SİBER GÜVENLİK ALANINDA ATILAN ÖNEMLİ ADIMLAR

3.3.1. Politika Belgeleri

3.3.1.1. E-Dönüşüm Türkiye Projesi (2003)

58 ve 59. Hükümet Acil Eylem Planı'nda yer alan "e-Dönüşüm Türkiye Projesi" 2003 yılında başlatılmış, böylece ülkemizde yürütülmekte olan münferit çalışmalar tek proje çatısı altında toplanarak hızlandırılmıştır. e-Dönüşüm Türkiye Projesi; vatandaşlar, işletmeler ve kamu kesimi ile tüm toplumun bilgi toplumuna dönüşümünün uyum içinde ve bütünleşik bir yapıda yürütülmesini amaçlamaktadır

(Yeşilbaş, 2011, s. 5). Bu projenin hedefi, 2003'ün sonuna kadar daha güvenli, daha hızlı, daha ucuz internet kullanımının yaygınlaştırılması ve tüm hizmetlerin elektronik ortamda verilmesi olarak açıklanmıştır. Elektronik ortamda verilecek hizmetlerin başında, kamu hizmetlerinin e-devlet yaklaşımı çerçevesinde verilmesi gelmektedir (Göker, 2004).

E-dönüşüm Türkiye Projesi ile aşağıdakiler amaçlanmıştır (Bülbül, 2013, 10):

- ✓ Adalet, trafik, vergi, emniyet, sosyal güvenlik, nüfus, tapu, sağlık, eğitim gibi alanlardaki kurum ve kuruluşlara yapılacak müracaatlar bazı haklardan yararlanma ve belgelendirme hususlarının elektronik ortamda da gerçekleştirilmesi,
- ✓ Kamu kurumlarında iş akışı ve belgeleme başta olmak üzere hizmet üretme formatının birbiri ile uyumlu ve standart hale getirilmesi,
- ✓ Tüm kamu kurumlarının web sayfalarında, yasa ile açıklanması engellenmemiş tüm rapor, başvuru, inceleme vs.lerin yer alması,
- ✓ Her kamu kurumunun veri sistemini kurması, bütün bilgilerinin açık olması ve sistemin görünürlüğünün artırılması,
- ✓ E-Devleti en etkin kullanan ülkelerle yapılacak anlaşmalar ile "kıyaslama" yapılması,
- ✓ ve Türkiye'de e-dönüşüm politikası çerçevesinde, tüm e-uygulamalara tek merkezden erişimin sağlanması amaçlanmıştır. (Resmi olarak e-devlet portalı ya da e-devlet kapısı 18 Aralık 2008'de açılmıştır).

Siber güvenlik alanındaki çalışmalarına 2003'te başlayan Türkiye (Ercan, 2015 s. 30), aynı yıl Cenevre'de düzenlenen Dünya Bilgi Toplumu Zirvesi (World Summit on the Information Society-WSIS) çalışmalarına katılmış ve bu kapsamda 2004 yılında hukuk alanındaki çalışmalarını devam ettirmiştir (Ada, 2013, s. 49).

3.3.1.2. Bilgi Toplumu Stratejisi Eylem Planı (2006)

Ülkemizde siber güvenliğe yönelik faaliyetler, 2006-2010 Bilgi Toplumu Stratejisi Eylem Planı'na ve bu Plan'ın 88. maddesine dayanarak TÜBİTAK'ın yürüttüğü çalışmalarla büyük oranda hız kazanmıştır (Bozoklu ve Çil, 2017). Ülkemizde bu dönemde köklü bir dönüşümün meydana geldiği söylenebilir. Bu

dönüşüm ile devlet sırrı anlayışı elektronik güvenlik anlayışına dönüşmüş; fakat yasal düzenlemeler ve fiziki altyapıların hazır olmaması nedeniyle de çok sayıda güvenlik açığı ortaya çıkmıştır. Bunların sonucunda kamuoyunda günlerce sürecek olan tartışmalar yaşanmış ve işte bu nedenle de sürekli yeni arayışlara girilmiştir (Meral, 2015, s. 118).

Ülkemizde internete ilişkin düzenlemeler, 2001 yılına kadar gitse de siber uzama yönelik tehditlerden ilk kez 2006'da Devlet Planlama Teşkilatı'nın hazırladığı Bilgi Toplumu Eylem Planı Stratejisi'nde söz edilmiştir. Bu Eylem Planı kapsamında, TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'nün sorumluluğu altında, "Siber uzaydaki güvenlik tehditlerini sürekli olarak takip edecek, uyarılar yayınlayacak, bu risklere karşı tedbirlerin ne şekilde alınabileceğine dair bilgilendirme yapacak ve risklerin ortaya çıkması durumunda karşı tedbirlerin koordinesini yapabilecek bir Bilgisayar Olaylarına Acil Müdahale Merkezi (CERT)'nin" kurulması kararı alınmıştır (Ünal, 2015, s. 306).

Bilgi Toplumu Stratejisi Eylem Planı'nın Vatandaş Odaklı Hizmet Dönüşümü başlığı altında öngörülen eylemlerden en önemlileri şöyledir: Kamu internet sitelerinin görsel, içerik, güvenlik vb. yönlerden standart hale getirilmesi ve kamu internet sitelerini kullananların memnuniyeti endeksinin oluşturulması ve vatandaş görüşlerinin internet ortamında alınmasıdır. Bu hedefin hayata geçmesi farklı görsel yapılara, mükerrer içeriklere, güvenlik bakımından sorunlu olan kamu internet sitelerine olumlu bir katkı sağlayacaktır. Eylem çerçevesinde hedeflenen bu iki amaç da e-devlet politikasını hayata geçiren kamu kurumlarının en önemli eksiği görünümündeydi (Demirhan, 2011, s. 134). Bu eksiklikler tamamlanmaya çalışılarak aynı zamanda siber uzayla daha fazla iç içe olunmuş ve buna paralel olarak da siber güvenliği sağlamaya yönelik girişimlerde bulunulmuştur.

3.3.1.3. Ulusal Sanal Ortam Güvenlik Politikası (2009)

Gelişmiş ülkelerde son on yılda ICT, toplum ve ekonomi ile daha çok bütünleşmiştir. Bu gelişme ile beraber sayısal ortamda savaş kavramı, devletlerin ve hükümetlerin gündemi arasına girmiştir. Günümüzde gelişmiş ülkeler, devlet başkanı himayesinde ve bilgisinde hazırlanmış ulusal bilgi güvenliği politika belgesine

sahiptir. Bu kapsamda, politika belgesinin işlerlik kazanması için bu ülkelerde yeni yasalar çıkarılmış ve yürürlükte olan yasalarda değişiklikler hazırlanmıştır. Yapısal açıdan bakıldığı zaman da yeni kurumlar kurulmuş, koordinatörler belirlenmiş ve hâlihazırdaki kurumlarda gerekli yapısal değişiklikler yapılmıştır (Karabacak, 2010, s. 1). Bu anlayış çerçevesinde ülkemizde, siber savunma / sanal ortam güvenliği politika esaslarını belirlemek üzere TÜBİTAK UEKAE'nin koordinatörlüğünde çeşitli kamu kurum ve kuruluşlarının temsilcilerinden oluşan bir çalışma grubu oluşturulmuştur. Çalışma grubu, faaliyetlerini 30 Ocak 2009 tarihinde tamamlamış ve "Ulusal Sanal Ortam Güvenlik Politikası" belgesini hazırlamıştır. Söz konusu çalışma grubunda yer alan kurum ve kuruluşlar şunlardır (Mirzaoğlu ve diğ. 2009, s. 25-26): Cumhurbaşkanlığı, Başbakanlık, Genelkurmay Başkanlığı, Dışişleri Bakanlığı, Adalet Bakanlığı, Milli Savunma Bakanlığı, Maliye Bakanlığı, Ulaştırma Bakanlığı, İçişleri Bakanlığı, Devlet Planlama Teşkilatı Müsteşarlığı (Kalkınma Bakanlığı), Dış Ticaret Müsteşarlığı (Ekonomi Bakanlığı), Hazine Müsteşarlığı, Türkiye Cumhuriyet Merkez Bankası, Milli Güvenlik Kurulu Genel Sekreterliği, Milli İstihbarat Teşkilatı Müsteşarlığı, Bankacılık Düzenleme ve Denetleme Kurumu, Emniyet Genel Müdürlüğü, BTK ve TÜBİTAK-UEKAE.

Bu belgenin amacı: Türkiye'yi siber ortamdaki saldırılara karşı hazır hale getirecek ve siber ortamda yaşanacak problemlerin sonrasında hızlı bir şekilde toparlanmayı sağlayacak sanal ortam güvenlik adımlarını belirleme olarak verilmiştir. Bu politikada, Türkiye için bilgi ve iletişim sistemleri ile ilişkili tehditler ve açıklıklar genel hatları ile ortaya konulmuştur. Bu belgenin son bölümünde ise gelen tehditleri bertaraf etmek ve açıklıkları kapatmak için yapılması gereken güvenlik adımları verilmiştir. Bunlar (TBMM BİAK Raporu, 2012, s 777):

- ✓ Yasal düzenlemelerin oluşturulması,
- ✓ Ülke yeteneklerinin geliştirilmesi,
- ✓ Ulusal bilgisayar olaylarına müdahale organizasyonunun kurulması,
- ✓ Bilgilendirme ve bilinçlendirme çalışmaları yapılması,
- ✓ Ulusal Kritik Bilgi Sistem Altyapıları'nın güvenliğinin sağlanması,
- ✓ Uluslararası eşgüdümün sağlanması,
- ✓ Kurumsal bilgi ve iletişim sistemleri güvenliğinin sağlanması,

- ✓ Ulusal sanal ortam güvenlik stratejisinin hazırlanması olarak verilmiştir.

Politika belgesinde, ülkemizin bilgi ve iletişim sistemlerinde yer alan açıklıkların ortadan kaldırılması ve bu sistemlerin maruz kalabileceği tehditlerin bertaraf edilmesi amacıyla yapılacak çalışmalara dayanak oluşturacak temel ilkelere aşağıda yer verilmiştir (Karabacak, 2010, s. 3):

1. Yasal düzenleme ve faaliyetlerde kişisel bilgilerin mahremiyetine saygı prensibinin göz önünde bulundurulması,
2. Bilgi ve iletişim sistemlerinin güvenliği sağlanırken sistemlerde kullanılabilirlik ile güvenlik arasında denge kurulması,
3. Kurumların ihtiyaçlarını karşılayacak bilgi ve iletişim sistemleri güvenliği mekanizmalarının mümkün olduğunca milli kaynaklardan karşılanması,
4. Ulusal kritik bilgi ve iletişim sistem altyapılarının güvenliğinden sadece ilgili altyapıları işleten kurumlar değil ülke çapında belirlenecek olan denetleyici, düzenleyici kurumların da sorumlu olması,
5. Bilgi ve iletişim sistemlerinin sanal ortam güvenliğinin sağlanması hususunda, konunun teknik boyutları yanında hukuki, idari, ekonomik, politik ve sosyal boyutlarının da değerlendirilmesi gerektiği,
6. Faaliyetlerin gerçekleştirilmesi sırasında kamu kurumları, özel sektör ve sivil toplum örgütlerinin etkili bir iletişim içinde çalışması gerektiği,
7. ve sanal ortamda sınırlar kalktığı için olası bir tehdide veya saldırıya karşı etkili korunma ve müdahale mekanizmalarının oluşturulabilmesi için uluslararası işbirliğine önem verilmesidir.

Tehditler, Açıklıklar, Temel İlkeler ve Sanal Ortam Güvenlik Adımları gibi ana başlıklara sahip olan bu politika belgesinin içerisinde yer alan hususların uygulanma adımlarını belirleyen bir eylem planı veya stratejisi bulunmamaktaydı (Çeliktaş, 2016, s. 78). TÜBİTAK koordinatörlüğünde Cumhurbaşkanlığı, Başbakanlık, Genelkurmay Başkanlığı, ilgili bakanlık ve kamu kurumlarının katılımıyla siber güvenliğe yönelik Türkiye politikasının belirlenmesi maksadıyla hazırlanmış olan bu politika belgesi, onaylanmadan yarıda bırakılmıştır (Meral, 2015, s. 119).

3.3.1.4. Ulusal Bilgi Güvenliği Programı

2005'te oluşturulan Bilgi Toplumu Stratejisi'nin 88'inci maddesi kapsamında yürütme sorumluluğu TÜBİTAK-UEKAE'ye verilen Ulusal Güvenlik Programı'nın ana hedefleri ve yürüttüğü çalışmalar şunlardır (Sınav, 2014, s. 103-104):

Hedefler;

- ✓ Kamuda yer alan kurumların bilgi noksanlıklarının giderilmesi, bilgi güvenliği noktasında bilinçlenmelerinin sağlanması ve bu kurumlar için güncel olan bilgi güvenliği uyarılarının düzenli bir şekilde yayınlanması,
- ✓ "Bilgisayar Olayları Müdahale Ekibi (BOME)-Koordinasyon Merkezi"nin kurulup etkin olarak çalıştırılması,
- ✓ Kamu kurumlarında bilgi güvenliğinin sağlanması amacıyla gerekli olan tedbirlerin ortaya çıkarılması,
- ✓ Kamu alanında faaliyette bulunan kurumları hedef alan tehditlerin tespit edilmesi,

Çalışmalar;

- ✓ Örnek olarak belirlenen kamu kurumlarına "Bilgi Güvenliği Yönetim Sistemi" kurulumu danışmanlık hizmetinin verilmesi ve bilgi sistemlerinde yer alan güvenlik sorunlarının belirlenmesi,
- ✓ "BOME-Koordinasyon Merkezi"nin kurulması ve ardından kamu kuruluşlarına BOME'lerin kurulması için danışmanlık hizmetinin sunulması,
- ✓ Kamu kurumlarında bulunan bilgi sistemlerinin maruz kalacağı siber tehditlerin tespiti amacıyla "Sanal Ortam Savunma Sistemi"nin kurulması,
- ✓ Kamu kuruluşlarında bilgi güvenliğinin farklı boyutlarıyla ilgili uygulamalı eğitim hizmetinin verilmesi,
- ✓ Bilgi güvenliğiyle alakalı rehber doküman ve teknik makalelerin hazırlanması,
- ✓ ve Ulusal Bilgi Güvenliği Kapısı'nın kurulması ve işletilmesidir.

3.3.1.5. MGK Bildirisi (2010)

2008 yılında bildirilen Bakü-Tiflis-Ceyhan petrol boru hattı siber saldırısı, Türkiye'deki karar vericiler için paha biçilmez dersler vermişti. Bu saldırı ilk olarak,

düşman siber aktivitesinin kinetik etkilerini göstermesi; İkincisi, saldırının bölgesel güvenlik sorunları, enerji jeopolitiği ve siyasi/askeri rekabet arasındaki bağa işaret etmesi; Üçüncüsü, kritik ulusal altyapının beşinci savaş alanının ortaya çıkmakta olan tehditlerine karşı hassas olduğunu ortaya koyması açısından oldukça önemlidir. Saldırıya cevap olarak siber savunma yeteneklerini artırmaya karar veren Ankara, ilk olarak 2010'da Milli Güvenlik Kurulunu (MGK) toplamış ve 2012'de de Türk Silahlı Kuvvetleri (TSK) Siber Komutanlığı'nın kurulmasına karar vermiştir (Kasapoğlu, 2015, s. 15).

Daha öncesinde, siber saldırı ve tehditler, Türkiye'de uzun bir süre boyunca terörle mücadele ve siber suç kapsamında değerlendirilmekteydi. Bakü-Tiflis-Ceyhan saldırısında da görüldüğü üzere bu saldırı ve tehditlerin ulusal/küresel çapta ulaştıkları boyutların milli güvenliği de etkileyebilecek düzeyde olduklarını ortaya koymuştur.

Bunun üzerine MGK 27 Ekim 2010 tarihli olağan toplantısında, siber saldırı ve tehditlerin engellenebilmesi için milli düzeyde yürütülen çalışmaları kapsamlıca değerlendirip tartışmıştır. Toplantının ardından yayınlanan basın bildirisinde, siber saldırı ve tehditlerin Türkiye'nin tehdit algılamaları arasına alınmasına ve kamuoyunca "Kırmızı Kitap" olarak bilinen Milli Güvenlik Siyaset Belgesi'ne girmesine karar verilmiştir. Böylelikle de siber saldırı ve tehditlere karşı önlem almaya yönelik irade ve kararlılık ortaya koyulmuş (Çeliktaş, 2016, s. 78) ve farkındalığın artmasıyla da somut anlamda hız kazanan çalışmalarla beraber yeni çalışmaların da önü açılmıştır (Meral, 2015, s. 119).

3.3.1.6. Ulusal Siber Güvenlik Strateji Çalıştayı (2012)

2010'lu yıllar; Türkiye'de siber güvenlik konularının irdelendiği, tartışıldığı, çok sayıda çalıştayın, toplantının, konferansın ve seminerin yapıldığı bu çalışmalara paralel olarak rapor, makale ve kitap sayılarında da artışların yaşandığı yıllar olmuştur. Yapılan bunca çalışmanın en sonuç alıcı olanı ise 80'in üzerinde bilgi güvenliği uzmanının katılımı ile daha önce hazırlanarak ilgili kamu ve özel sektör kuruluşlarıyla paylaşılan strateji dokümanı taslağının değerlendirilmesini gerçekleştiren Siber Güvenlik Strateji Çalıştayı olmuştur (Meral, 2015, s. 122).

Bilgi Güvenliği Derneği'nin gerçekleştirdiği bu çalıştay, birtakım öneriler getirmiş ve öneriler neticesinde de "2013 Ulusal Siber Güvenlik Strateji Belgesi"nin yayımlanması gündeme gelmiştir. Çalıştayın ortaya çıkardığı bu sonuçlar, ne kadar önemli bir çalışma yapıldığını göstermesi açısından oldukça önemlidir.

Haziran 2012'de Bilgi Güvenliği Derneği tarafından gerçekleştirilen Siber Güvenlik Stratejisi Çalıştayının ardından Dernek tarafından oluşturulan bir öneri belgesi hazırlanmış ve belgede aşağıdaki adımların atılması çağrısında bulunulmuştur (Çelikpala ve diğ. 2015, s. 28):

- ✓ Ulusal Siber Güvenlik Strateji Belgesi'nin yayımlanması,
- ✓ Ulusal SGK'nin kurulması,
- ✓ Siber güvenlik konusunda farkındalığın arttırılması ve siber güvenlik kültürünün yaygınlaştırılması,
- ✓ Kişisel ve kurumsal verilerin korunması konusunda daha güçlü önlemler alınması,
- ✓ Uluslararası işbirliğinin güçlendirilmesi (belgede AB, ENISA, Avrupa Konseyi, BM, NATO ve OSCE sıralanmaktadır),
- ✓ Ulusal siber güvenlik Ar-Ge politikasının oluşturulması ve ulusal teknolojilerin geliştirilmesinin teşvik edilmesi,
- ✓ Üniversitelerde konuyla ilgili yürütülen bilimsel çalışmaların artırılması için adımlar atılması,
- ✓ İnsan kaynaklarını geliştirmek için adımlar atılması (diğer bir deyişle, ulusal siber güvenlik uzmanlarının eğitimi),
- ✓ Kurumların ve güvenlik güçlerinin siber güvenlik yeteneklerini artırmak için adımların atılması,
- ✓ Kurumlara siber güvenlik sızma testleri yapacak bağımsız merkezlerin kurulması,
- ✓ Yasama reformlarının yapılması,
- ✓ CI'lerdeki ve kamu ve özel kurumlardaki Siber Olaylara Müdahale Ekipleri (SOME) arasında koordinasyon sağlamak ve eğitim vermek için bir Türkiye Ulusal SOME'nin (TC-SOME) kurulması,

- ✓ Bir ulusal siber tehdit ve korunmasızlık inceleme laboratuvarının kurulması, bu laboratuvarda zararlı yazılımların incelenmesi, yerli ve yabancı donanımların tasnifi ve derecelendirilmesinin yapılması,
- ✓ İthal edilen donanımlarda bulunabilecek arka kapılara, yerleştirilmiş kötücül yazılımlara ve diğer güvenlik açıklarına değinilerek ulusal donanım, ulusal bir işletim sistemi (OS), arama motoru ve internet tarayıcılarının geliştirilmesi,
- ✓ ve savunma Sanayii Müsteşarlığı altında siber güvenlik alanında Ar-Ge yapmak ve koordinasyon sağlamak amacıyla bir Siber Güvenlik Mükemmeliyet Ağı'nın kurulması önerileri yer almaktadır.

3.3.1.7. 2013-2014 Ulusal Siber Güvenlik Stratejisinin Yayımlanması

Daha önceki konu başlığımızda ele alınan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı (2012)" ile "SGK" oluşturulmuştu. Oluşturulan SGK, 4 kez toplanmış ve siber güvenlik alanında ciddi kararlar almıştır. Alınan bu kararlardan bir tanesi; Bakanlar Kurulu Kararıyla 25 Ekim 2013'te 28683 sayılı Resmî Gazete'de "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" yayımlanması ve yürürlüğe girmesidir. Bu eylem planıyla bilhassa CI'lere (elektrik, su vb.) sahip kuruluşların karşı karşıya kalacakları olası siber saldırıların önüne geçilmesi planlanmıştır (Erçağlar, 2017, s. 32).

Siber suçlarla mücadele, 2012'ye kadar Bilim, Sanayi ve Teknoloji Bakanlığının koordinatörlüğünde BTK tarafından sivil toplum kuruluşları ve kurumlarıyla beraber yürütülmekteydi. Ancak 2012'de, 2013-2014 USGSEP'nin yürürlüğe girmesiyle birlikte UDHB'nin sorumluluğuna verilmiştir (Ada, 2018, s. 49).

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın amacı, başarıya ulaşmaya yönelik bir altyapı oluşturmaktır; bu çerçevede stratejinin amaçları ve yapılması kararlaştırılan eylem planları aşağıdaki gibidir (Turkey's National Cyber Security Strategy and 2013-2014 Action Plan, 2013):

Amaçları:

- ✓ Kamu kurum ve kuruluşları tarafından bilgi teknolojileri üzerinden sağlanan her türlü veri, hizmet ve işlem ile bunların sunumunda kullanılan sistemlerin güvenliğinin sağlanmasına,
- ✓ Kamu ya da özel sektörün işlettiği CI'lerin bilişim sistemlerinin güvenliğinin sağlanmasına,
- ✓ Siber güvenlik olaylarının etkilerinin en düşük seviyede kalmasına, olaylardan sonra sistemlerin en kısa sürede normal çalışmalarına dönmesine yönelik stratejik siber güvenlik eylemlerinin belirlenmesine ve oluşan suçun adli makam ve kolluk kuvvetleri tarafından daha etkin araştırılmasının ve soruşturulmasının sağlanmasına yönelik bir altyapı oluşturmaktır.

Eylem planları:

1. Yasal Düzenlemelerin Yapılması,
2. ve Adli Süreçlere Yardımcı Olacak Çalışmaların Yürütülmesi maddeleri ile siber saldırganların siber ortamda işledikleri suçlar nedeniyle cezalandırılmaları
3. USOM Organizasyonunun oluşturulması maddesi ile SOME'nin faaliyete başlayarak siber olayların tespitini, duyurulmasını, gerekli tedbirlerin alınarak saldırganlarla ilgili gerekli yasal işlemlerin de kısa sürede başlatılması,
4. Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi maddesi ile siber saldırıların başarılı olmasının zorlaştırılması ve daha masraflı hale getirilmesi,
5. Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi ve Bilinçlendirilme Faaliyetleri maddesi ile güvenlikte ihmallerin ve yanlışların azaltılması, bu konuyla ilgili strateji ve politikaların geliştirilmesi,
6. Siber Güvenlikte Yerli teknolojilerin Geliştirilmesi maddesi ile daha güvenli donanım ve yazılımların kullanılmaya başlanması,
7. ve Ulusal Güvenlik Mekanizmalarının Kapsamının Genişletilmesi maddesi ile de koordinasyon ve işbirliğinin artırılması amaçlanmıştır.

3.1.8. 2016-2019 Ulusal Siber Güvenlik Stratejisinin Yayımlanması

İlk siber savunma stratejisini 2013'te oluşturan Türkiye, bu stratejisinde aldığı kararların bir kısmını ciddi bir biçimde uygulamıştır. Fakat uygulama ve stratejiler, sürekli artan bir hızla gelişen teknolojiler ve bu sebeple de açılan yeni

sanal cephelere yetişmek için yeterli olamamıştır. Gerçekten de 2016 yılında oldukça ciddi DDoS siber saldırılarına maruz kalan Türkiye, bu saldırılar karşısında ciddi bir etkinlik gösterememiş ve bu saldırılar sayesinde Türkiye'nin siber güvenlik/savaş alanındaki eksikliği bir anlamda açığa çıkmıştır. Bu saldırılardan sonraki günlerde, 2016-2019 USGSEP belgesi çalışmalarının tamamlanmış olması ve siber alandaki hedeflerin 2019'a yılına kadar belirlenmesi, atılmış önemli bir adımdır (Sanalp, 2016, s. 46).

Yukarıdaki gelişmelerden sonra UDHB tarafından 2016-2019 dönemini kapsayacak eylemlerin belirlenmesi doğrultusunda ulusal siber güvenlik stratejisinin güncellenmesi gerekliliği ihtiyacı doğmuştur. Bu çerçevede eski eylem planında yer alan ilgili kurumlarla 10 Mart-7 Nisan 2015 tarihlerinde yedi adet değerlendirme toplantısı yapılarak eski eylem planında yer alan faaliyetlerin gerçekleşme dereceleri, karşılaşılan güçlükler, ileriye dönük değerlendirmeler ve siber güvenlik kapsamında gerçekleştirilmesi gereken faaliyetler, detaylı olarak belirlenmiştir. Toplantılardan sonra üniversiteler, sivil toplum kuruluşları, bilişim sektörü, CI işletmecileri ve kamu kurumları gibi 73 kurum ve kuruluşu temsilen 126 uzmanın katılımıyla iki gün süren Ortak Akıl Platformu çalışması gerçekleştirilmiş ve bunun sonucunda Türkiye'nin siber güvenliğinin güçlü ve zayıf yönlerinden hareketle stratejik amaçları ve gerçekleştirmesi gereken eylemleri belirlenmiştir (Ada, 2018, s. 54).

2016-2019 USGSEP Belgesi, kamu ve özel sektör nezdinde işletilen CI'lere ait bilişim sistemlerinin yanı sıra küçük ve orta ölçekli sanayi, özel ve tüzel kişiler de dâhil olmak üzere Türkiye ölçeğinde siber uzayı oluşturan bütün bileşenleri kapsamaktadır (Çeliktaş, 2016, s. 95). 2016-2019 USGSEP'sinin temel amacı; siber güvenliğin, ulusal güvenliğin ayrılmaz bir parçası olduğu anlayışının tüm kesimlerde yerleşmesinin sağlanması (Kaya, 2017, s. 24) ve ulusal siber uzayda bulunan tüm sistem ve paydaşların güvenliğinin sağlanması için idari ve teknolojik önlemlerin alınmasını destekleyecek yetkinliğin eksiksiz bir şekilde kazanılmasıdır (Ada, 2018, s. 55). Bu çerçevede 2016-2019 USGSEP, Türkiye'nin siber güvenliğinin sağlanmasında bundan sonra izleyeceği politikaları yansıtması bakımından dikkate değer ipuçları sunmaktadır. Bu kapsamda toplumun tüm kesimlerinde bilinç düzeyi ve farkındalığın arttırılarak hukuki, teknik ve diğer alanlarda gerekli hazırlıkların

tamamlanması ve altyapı ögelerinin güçlendirilmesi amaçlanmaktadır. Bu belgede ana hedeflerle birlikte ana hedefleri konsolide edecek destekleyici ve lojistik nitelikteki alt eylem maddeleri, ana hedeflerin ne şekilde hayata geçirileceği, icrası ve denetim yöntem ve usullerinin belirlenmesinin gereğine ilişkin hükümler sunulmuştur (Seren, 2016).

2016-2019 USGSEP oluşturulduğu vakit; diğer ülkelerin siber güvenlik stratejileri, siber güvenlik alanındaki hedefleri, AR-GE çalışmaları, kamu ve özel sektör kurum ve kuruluşları arası koordinasyon ve işbirliği, kaynak tahsisleri, eğitim durumları ile kuruluş yapıları gözden geçirilerek göz önünde bulundurulmuştur (Çeliktaş, 2016, s. 95).

2016-2019 USGSEP'sinin iki ana amacı vardır. Birincisi; tüm paydaşların siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olduğu anlayışını kabul etmeleri. İkincisi; ulusal ve siber alanda tüm sistemlerin ve paydaşların mutlak güvenliğini sağlamak için idari ve teknolojik önlemlerin alınmasına izin verecek yetkinliğin kazanılmasıdır. Bu amaçlar doğrultusunda 2016-2019 yılları arasında hayata geçirilmesi planlanan stratejik eylemler, aşağıdaki gibidir (Turkey's National Cyber Security Strategy 2016-2019, 2016):

1. Siber Savunmanın Güçlendirilmesi ve CI'lerin Korunması,
2. Siber Suçlarla Mücadele,
3. Farkındalık ve İnsan Kaynağı Geliştirme,
4. Siber Güvenlik Ekosisteminin Geliştirilmesi,
5. ve Siber Güvenliğin Milli Güvenliğe Entegrasyonudur.

2016-2019 USGSEP'sinde öngörülen dikkat çekici hususlardan biri, belgenin statik değil dinamik bir vizyonunun olmasıdır. Çünkü belgeye; sürekli gelişen teknolojiye, değişkenlik gösterip çeşitlenen risk ve tehditlerin oluşturduğu yeni ihtiyaç ve koşullara karşı kendisini güncelleme esnekliği tanınmıştır. Bu kapsamda, değişen ihtiyaçlar karşısında kamu ve özel sektörde beliren yeni taleplere hızlıca yanıt verilmesini ve bu konuda paydaşlar arasında ulusal düzeyde eşgüdümün sağlanmasını olanaklı hale getirecek güncellemelerin gerçekleştirilmesi hedeflenmiştir. Planın içerdiği amaçlara ulaşılabilmesi için nihai sürenin sonu, 2019

olarak belirlenmiştir. Bu vakte kadar tamamlanması öngörülen hedeflere ulaşılamaması durumunda ise eksik kalmış ya da gerçekleştirilmemiş eylemlerin bir sonraki eylem planına dahil edilmesi kararına varılmıştır (Seren, 2016).

2016-2019 USGSEP, 2013 yılındaki siber savunma belgesine göre çok daha vizyoner olmasıyla birlikte, belgede birtakım eksiklikler de bulunmaktadır. Belgede kritik yapıların güvenliğinin öneminin vurgulanmasından, siber güvenlik çalışmaları kapsamında üniversitelerle işbirliği yapılması planından ve siber savunmayla ilgili bir seferberlikten bahsedilmektedir. Diğer taraftan siber savunmadan sorumlu bir kamu otoritesinden bahsedilmekteyken bu otoritenin yetkileri, organizasyondaki yeri ve bu otoritenin nasıl bir konumda olacağına ilişkin herhangi bir bilgi bulunmamaktadır. Bu çerçevede, kamu otoritesinin detaylandırılması ve bu maksatla da ciddi adımların atılması gerekliliği vardır. Bunlara ilaveten siber güvenliğin, bir tek sivil kurumlar için incelenmiş olması ve ordunun da siber savunmadaki rolüne değinilmemiş olması, önemli eksikliklerdir. Veri koruma kanununu yasalaştırması, 2016-2019 USGSEP belgesini yayımlaması ve NATO CCD COE'ye sponsor üye olması; Türkiye'nin, siber güvenlik konusunda uluslararası arenada görünür olabilmesi adına attığı oldukça önemli adımlar olarak değerlendirilebilir (Sanalp, 2016, s. 48).

3.3.2. Siber Güvenlik Alanında Faaliyet Gösteren Kurumlar

3.3.2.1. Kamu Kurumları

3.3.2.1.1. Türkiye Bilgisayar Olayları Müdahale Ekibi (TR-BOME)

2007'de TÜBİTAK UEKAE bünyesinde ülkenin tamamında kurum ve kuruluşlara bilgisayar güvenlik olaylarına müdahale yeteneği ve görevi kazandırmak amacıyla Türkiye Bilgisayar Olayları Müdahale Ekibi (TR-BOME) ve Koordinasyon Merkezi kurulmuştur (Meral, 2015, s. 118-119).

Şu anda Türkiye'de resmen tanınmış iki tane Bilgisayar Acil Müdahale Ekibi (BOME/CERT) bulunmaktadır. Biri, hükümet tarafından işletilen (TR-BOME); diğeri ise araştırma ve eğitim amacıyla TÜBİTAK (ULAK-CSIRT) tarafından işletilen ve ona ait olandır. Uluslararası arenada da aktif olan TRBOME, 2007 yılında NATO Bilgisayar Olaylarına Müdahale Yeteneği (NATO Computer Incident

Response Capability-NCIRC) ile personel değişimi, NATO siber savunma tatbikatına katılım, ortak olaya müdahale, NCIRC ağına erişim, kötü niyetli kod analizi, güvenlik açığı veri tabanı, alarmlar, uyarılar ve olay ve zaafiyetlerin analiz ve değerlendirmelerine yönelik bilgi paylaşımı konularında destek olabilmesi amacıyla bir işbirliği anlaşması imzalamıştır. TRBOME, "Uluslararası Siber Savunma Atölyesi, Güz 09-ICDW09" tatbikatında Türkiye'yi temsil etmiş ve NATO Egzersiz Siber Koalisyonu (Exercise Cyber Coalition 2009)'na aktif olarak katılmıştır (Çil ve diğ. 2012, s. 118).

3.3.2.1.2. Ulusal Siber Olaylara Müdahale Merkezi ve Müdahale Ekipleri

Türkiye'nin 2013-2014 USGSEP'sinde, TİB'in denetimi altında ülkemizi etkileyebilecek tehditlere karşı 7/24 müdahale esasına göre çalışacak "Ulusal Siber Olaylara Müdahale Merkezi (USOM)'nin" ve USOM'un koordinasyonunda çalışacak sektörel "(SOME)'nin" kurulması çağrısında bulunulmuştur. Bu çağrı kapsamında kurulan USOM, CI sektörleri ve kamu kurumları için sektörel SOME'ler kurmakla ve bunlara eğitim ve koordinasyon sağlamakla görevlendirilmiştir. Bu çerçevede bakanlıklar, diğer tüm kamu kurumları, alt kuruluşlar, bakanlıkların ilgili birimleri, özel kurum ve kuruluşlar kendi kurumsal SOME'lerini ve alt birimlerini kurmaya başlamışlardır. SOME'lerin kurdurulmasındaki amaç; CI işleten firmaların, kendi bilişim teknolojileri birimleri olan bütün bakanlıkların ve diğer kamu kurumlarının birer kurumsal SOME'ye sahip olmalarıdır (Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, 2013).

Bütün SOME'lerin kanun dışı olabilecek her faaliyeti yargı birimlerine ve USOM'a anında haber vermesi, siber saldırılara karşı gerekli tedbirleri alması, müdahale ve olay kayıt sistemleri kurması ve kurumlarının bilgi güvenliğini sağlaması gibi yükümlülükleri bulunmaktadır. Eğer bir olay müdahale yeteneklerinin ötesindeyse sektörel SOME'lere (Bankacılık ve finans, ulaştırma, enerji, kritik kamu hizmetleri, su yönetimi ve elektronik haberleşme gibi kritik sektörlerin SOME'lerine verilen isimdir) ve/veya USOM'a yardım için başvurabilirler (Çelikpala ve diğ. 2015, s. 31).

3.3.2.1.3. Ulusal Bilgi Güvenliği Kapısı

Kurulması ve işletilmesi TÜBİTAK-UEKAE tarafından gerçekleştirilen ve Ulusal Bilgi Güvenliği Programı'nın bir alt projesi olan "Ulusal Bilgi Güvenliği Kapısı"nın amacı; bilgi güvenliği ile alakalı güncel uyarılar, bilgilendirici rehberler ve teknik yazılar yazmaktır. Ülkemizde ihtiyaç duyulan bilgi güvenliği konusunun bilgi birikimini oluşturmak adına çok önemli bir fonksiyonu gerçekleştirmesi umulan "Ulusal Bilgi Güvenliği Kapısı"na, içerik olarak her şahıs ve kurum katkı yapabilmektedir (Sınav, 2014, s. 104).

Ulusal Bilgi Güvenliği Kapısı'nın sitesinde; bilgi güvenliğiyle ilgili özel konularda okuyucuyu bilgilendirmeyi amaçlayan teknik yazılar, bilgi güvenliği ile ilgili kılavuzlar, ülkemizde yapılan etkinlik, toplantı, sempozyum vs. gibi organizasyonların duyuruları, önemli açıklıklarla ilgili güvenlik bildirisi sayfası bulunmaktadır. Bilgi birikimine katkının sadece TR-BOME tarafından değil, ülkemizde bilgi güvenliği alanında yetkinliğe sahip her türlü kurum veya kişi tarafından yapılmasına imkân sağlanmaktadır. Kişilerin siteye kayıt olduktan sonra bilgi güvenliği konularında oluşturduğu rehber, doküman veya makale, oluşturulacak değerlendirme komitesinin gözden geçirmesini takiben web kapısında yayınlanmaktadır (TBMM BİAK Raporu, 2012, s. 772).

3.3.2.1.4. Siber Suçlarla Mücadele Daire Başkanlığı (2011)

Siber güvenlik ile ilgili kavramlar diğer ülkelerde olduğu gibi Türkiye'de de 2010 yılından sonra daha fazla tartışılır ve bilinir hale gelmiştir. Neredeyse on yıldır kendi başına devam eden siber güvenlik çalışmalarının geç kalınmış olsa dahi bundan sonra ulusal siber güvenlik stratejileri kapsamında düzenlenme ve hızlandırılmaları ihtiyacının gündeme alınmaya başlanması, oldukça olumludur. 2010 yılından sonra daha sık gündeme gelmeye başlayan siber güvenlik konusuna paralel olarak 2011'de (Meral, 2015, s. 119-120), bilişim teknolojileri aracılığıyla yapılan suçların tahkiki, sayısal verilerin incelenebilmesi ve siber suçlara daha etkin karşı konulması amaçlarıyla Bilişim Suçlarıyla Mücadele Daire Başkanlığı kurulmuş ve son olarak da 2013'te ismi, Siber Suçlarla Mücadele Daire Başkanlığı olarak değiştirilmiştir (Hatipoğlu, 2017, s. 164).

Halihazırda 76 ilde faaliyet gösteren birimin merkezinde, bilişim ve materyal inceleme konusunda 562 uzman çalışırken Türkiye genelinde ise toplamda 2 bin 700 siber personeli görev yapmaktadır. Merkez, günde ortalama olarak 3.000 olmak üzere zaman zaman 30.000 civarına kadar ihbar aldığını ve haftalık olarak da 20.000 materyal incelemesiyle de dünyada birinci olduklarını belirtmektedir (Kızılkoyun, 2018).

Siber Suçlarla Mücadele Daire Başkanlığı sorumluluklarını şu şekilde sıralamaktadır (Siber Suçlarla Mücadele Daire Başkanlığı, 2019):

1. Siber suçlarla mücadele etmek,
2. Siber suçlar konusunda toplumda farkındalık oluşturmak,
3. Siber suçlarla mücadelede uluslararası iş birliklerini artırmak,
4. Ülkemize yönelik siber suç tehditlerini değerlendirmek, gerekli analizler yapmak ve bu tehditlerle mücadele etmek,
5. Siber suçlarla mücadelede alanında uzman soruşturmacı ve adli bilişim personelleri yetiştirmek,
6. ve Teknolojik gelişmeleri takip etmek ve bu teknolojiyi kullanmak suretiyle siber suçlarla mücadele kapasitesini artırmaktır.

3.3.2.1.5. Siber Güvenlik (Koordinasyon) Kurulu (SGK) (2012)

Daha önceki konu başlığımızda da ele alındığı üzere SGK "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı (2012)" ile siber güvenliğe ilişkin olarak alınacak önlemlerin belirlenmesi; hazırlanan plan, program, rapor, usul, esas ve standartların onaylanması, uygulanması ve koordinasyonunun sağlanması amacıyla UDHB'nin başkanlığında kurulmuştur. Böylelikle ulusal siber güvenliğin sağlanmasına yönelik her türlü eylem planı, strateji ve politika belirleme görevi UDHB'ye verilmiştir. Yine bu karar çerçevesinde, tüm kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler, SGK tarafından belirlenen eylem planı, strateji ve politika çerçevesinde kendilerine verilen görevleri yerine getirmek ve belirlenen usul ve esaslara uymakla yükümlü hale getirilmişlerdir (Ercan, 2015, s. 27-28). Siber güvenlik algısının SGK'da konumlandırılmasıyla daha özel bir platformda konumlandırıldığı, yetkinin

UDHB'ye bırakılmasıyla da daha spesifik bir uzmanlığa bırakıldığını söylemek mümkündür (Göçoğlu, 2018, s. 156)

Ulusal siber güvenliğin sağlanması maksadıyla bütün kamu kurum ve kuruluşlarında işbirliğini öngören karar kapsamında bakanlık tarafından yayımlanan plan, program, usul ve standartlara kamu kurum ve kuruluşlarının tümünün uyması esastır. Ulusal siber güvenliğin sağlanması noktasında önemli hususlardan biri, yapılacak çalışmalar sürecinde mümkün olduğu kadar milli çözümlerin üretilmesi ve milli kaynakların kullanılmasıdır. Çalışmaların önünü açacak ve gelişimini sağlayacak olan ilke ise maddi kaynak planlaması ve kaynak tahsisinde önceliğin ulusal siber güvenlik alanında yapılacak çalışmalara verilmesidir (Kara, 2013, s. 70).

Dört kez toplanan SGK, siber güvenlik alanında ciddi kararlar almıştır. Alınan kararlardan bir tanesi; Bakanlar Kurulu Kararıyla yürürlüğe giren 25 Ekim 2013 tarihli "2013-2014 USGSEP'dir (Erçağlar, 2017, s. 32).

3.3.2.1.6. TÜBİTAK- Siber Güvenlik Enstitüsü (SGE) (2012)

Siber güvenlik alanındaki teknik faaliyetlere TÜBİTAK öncülük etmektedir. 2010 yılında TÜBİTAK"ın bünyesinde Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) kurulmuş ve bilgi güvenliği, kriptoloji ve haberleşme teknolojileri alanında hizmet vermeye başlamıştır. Siber güvenlik faaliyetleri ağırlıklı olarak BİLGEM bünyesinde 2012 yılında kurulmuş olan Siber Güvenlik Enstitüsü (SGE) tarafından yürütülmektedir (Çelikpala ve diğ. 2015, s. 26). SGE'nin faaliyetlerini aşağıdaki gibi sıralanabilir (Kara, 2013, s. 70-71-72):

- ✓ Kamu kurum ve kuruluşlarına, özel sektöre ve askeri kurumlara bilgi güvenliği danışmanlığı yapmakta; bilgi güvenliğine ilişkin teknolojik çözümler sunar ve bu alanda araştırma ve geliştirme faaliyetleri yürütmektedir.
- ✓ Sunduğu birçok hizmetle siber güvenlik konusunda bilgi birikiminin oluşmasını sağlamaktadır.
- ✓ Kamu kurum ve kuruluşları ve özel sektör şirketlerine güvenlik denetlemeleri ve sızma testleri yapmaktadır.
- ✓ Kamu kurum ve kuruluşlarına ve özel sektöre güvenli yazılımların hazırlanması eğitimini vererek destek sunmaktadır.

- ✓ Bilgi sistemlerinin kurulumu, konfigürasyonu ve güvenli tasarımına ilişkin çalışmalarıyla eksik güvenlik önlemlerinin tespit edilmesini ve tasarlanmasını yaparak bilgi sistemlerinin güvenliğini sağlamaktadır.
- ✓ Kurum ve kuruluşlara Bilgi Güvenliği Yönetim Sistemi konusunda danışmanlık hizmeti sunmaktadır.
- ✓ IT Ürün Güvenliği Laboratuvarlarında akıllı kart okuyucuları, akıllı kart yongaları ve işletim sistemleri, kriptolu bellekler, donanım güvenlik modülleri, güvenlik uygulama ve yazılımları, güvenilir ortam modülleri ve ağ güvenliği ürünleri için sızma testi ve risk analizi çalışmaları yürütmektedir.
- ✓ Zararlı yazılımların analizlerini yapmaktadır.
- ✓ Adli olayların aydınlatılabilmesi için Dijital Adli Analiz Laboratuvarında adli bilişim teknik ve araçlarını kullanarak gerekli incelemeleri yapmaktadır.
- ✓ Siber saldırılarda saldırının kaynağı, sisteme nasıl sızıldığı ve sistemde nelerin yapıldığını belirleyerek detaylı incelemeler yapmaktadır.
- ✓ Ulusal geniş ölçekli ağ altyapılarında çalışacak siber tehdit gözetleme, tespit ve önleme teknolojileri/sistemleri geliştirme konusunda faaliyetler yürüterek milli bilişim altyapı ve hizmetlerinin korunmasına önemli katkılar yapmaktadır.
- ✓ TÜBİTAK BİLGEM SGE bünyesinde 2006-2010 Türkiye Bilgi Toplumu Stratejisi Eylem Planı çerçevesinde, bilgisayar güvenlik olaylarını ulusal ve uluslararası boyutta ele alan BOME'yi kurmuştur.
- ✓ Danışmanlık, AR-GE ve BOME çalışmaları kapsamında elde ettiği deneyimleri talepler doğrultusunda eğitimler aracılığıyla kurumlara aktararak bilinçlenmeye katkı sunmaktadır.

Ağustos 2012'de TÜBİTAK SGE tarafından UDHB'ye, siber güvenlik mevzuat, teknoloji ve eğitim ana konularında olacak şekilde Ulusal Siber Güvenlik Yönetim Danışmanlığı Projesi adı altında çalışmalar sunulmuş ve böylelikle Ulusal Siber Güvenlik Yönetim Danışmanlığı Projesi başlatılmıştır (Meral, 2015, 122).

3.3.2.1.7. TSK Siber Savunma Komutanlığı (2013)

2011'de, Genel Kurmay Başkanlığında CYBERCOM olarak faaliyet yürütecek 3 temel komutanlık kurulmuştur. Genelkurmay, büyük ölçüde ABD

CYBERCOM'u model almıştır. Bu çerçevede 8 bilgisayar mühendisinden (siber güvenlik eğitim uzmanı) oluşan bir takım kurulmuştur (Türkay, 2013, s. 1157)

Bunun ardından Haziran 2012'de, siber tehditleri önlemede gelişmiş siber savunma ikaz ve tepki sistemlerine ve güçlü/merkezi bir siber savunma yeteneğine sahip olunması amacıyla TSK Siber Savunma Merkezi Başkanlığı kurulmuştur. 2013 yılında ise siber olayların takibini, analizini ve değerlendirmesini yapmak; siber güvenliğin standartlarını oluşturmak, siber savunma faaliyetlerinin yönlendirmesini merkezi olarak yapmak ve TSK'de kullanılan sistemlerin zafiyet analizlerini yapmak üzere (Meral, 2015, 120) 2012 yılında kurulan TSK Siber Savunma Merkezi Başkanlığı, 30 Ağustos 2013'te TSK Siber Savunma Komutanlığı'na dönüştürüldü (Aykanat, 2017). TSK Siber Savunma Komutanlığı; TSK bünyesinde, NATO çerçevesinde kurulmuştur (Ünal, 2015, s. 307).

3.3.2.2. Özel Kurumlar (Bilgi Güvenliği Derneği-2007)

Ülkemizde kamu yararına faaliyet gösteren Bilgi Güvenliği Derneği ve Siber Güvenlik Derneği gibi sivil toplum kuruluşlarının amacı: ITC güvenliği konusunda bireysel, kurumsal, ulusal ve uluslararası alanda bilimsel, teknik, sosyal ve kültürel faaliyetler yürütmek; siber güvenlik kültürünün oluşturulmasına katkıda bulunmak; üyelerinin mesleki gelişimini arttırmak; seminer, kurs, çalıştay ve konferans benzeri etkinlikler düzenleyerek bilinçlendirme faaliyetlerinde bulunmaktır. Bu dernekler dahilinde neredeyse her yıl siber güvenlik konferansları, siber güvenlik çalıştayları, raporları, sempozyumları ve siber güvenlik uzmanı yetiştirme kampları da düzenlenmektedir (Çeliktaş, 2016, s. 90-91).

Bilgi Güvenliği Derneği'nin son yıllarda bu alana sunduğu önemli katkılardan biri de ilki Aralık 2018'de yayımlanan "BGD Siber Güvenlik ve Savunma Kitap Serisi"nin "Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık" kitabı olmuştur. Bahse konu seride siber güvenlik alanında uzman akademisyenler, kamu çalışanları ve üst düzey yetkililerin aynı amaç uğruna bir araya gelmesi de hayli merak uyandırmaktadır (Arar, 2019, s. 302).

Bilgi Gügvenliği Derneği'nin bu alana sunduğu katkılardan bir diğeri de Mayıs 2019'da yayımlanan "BGD Siber Güvenlik ve Savunma Kitap Serisi"nin ikincisi olan "Siber Güvenlik ve Savunma: Problemler ve Çözümler" kitabı olmuştur.

3.3.3. Siber Güvenlik Alanında Yapılan Tatbikatlar

Kamu kurum ve kuruluşlarının sahip oldukları bilgi ve bilişim güvenliği yeteneklerini ve aldıkları önlemlerin yeterliliklerinin ne derecede olduğunu test etmek (Ercan, 2015, s. 31), siber güvenlik konusundaki farkındalığı artırmak, kurumların siber saldırı öncesi, esnası ve sonrasındaki bilgi paylaşımı, haberleşme ve koordinasyonunu test etmek, saldırılara karşı kurum içi politikaları değerlendirmek, kurum ve kuruluşların CI sektörlerini korumak için aldıkları önlemlerin yeterliliğini ölçmek için ulusal ve uluslararası alanda tatbikatlar icra edilmektedir (Çeliktaş, 2016, s. 89-90). Tatbikatlardan sonra yayınlanan sonuç bildirgelerine bakıldığı vakit, başarılı sonuçlar alındığı görülmektedir (Özalp, 2014).

Siber güvenlik tatbikatlarının sağladığı bu kazanımlar çerçevesinde, Türkiye'de de bir takım siber güvenlik tatbikatları düzenlenmiştir

3.3.3.1. Bilgisayar Olayları Müdahale Ekibi 2008 Tatbikatı

Türkiye'nin düzenlediği ilk tatbikat olan "BOME 2008 Tatbikatı", 8 kamu kurumunun katılımıyla TÜBİTAK BİLGEM bünyesinde faaliyet gösteren TR-BOME tarafından 2008'in Kasım'ında düzenlenmiştir (Meral, 2015, s. 119). Cumhurbaşkanlığı, Başbakanlık, Adalet Bakanlığı, Sayıştay Başkanlığı, Hazine Müsteşarlığı, Merkez Bankası, Sermaye Piyasası Kurulu ve Tapu Kadastro Genel Müdürlüğü'nün katılımıyla icra edilen BOME 2008 tatbikatı (Kaya, 2017, s. 22), kurumsal Bome süreçleri ile kurumların dış kaynaklı bir siber saldırıya uğraması halinde TR-BOME ile işbirliği faaliyetlerinin kontrol edilmesi amacıyla gerçekleştirilmiştir (Ercan, 2015, s. 31).

Tatbikatta, gerçek saldırılarla kurumların eksikliklerinin yanı sıra sahip oldukları yeteneklerin görülmesi ve raporlanması amaçlanmıştır. Gerçek saldırılar kapsamında port taraması, dağıtık servis dışı bırakma saldırısı, web sayfası güvenlik denetimi ve kayıt dosyası analizi olmak üzere dört farklı faaliyet gerçekleştirilmiştir.

Yazılı ortamdaki senaryolarda ise elektrik kesintisi, kurum içinden veri sızdırılması, web sayfasının ele geçirilmesi, sosyal mühendislik saldırıları gibi olası saldırı senaryoları karşısında kurumların verdikleri tepkiler yazılı olarak değerlendirilmiştir. Bu saldırılar, kurumların işlettikleri bilgi sistemlerinin çalışmasına zarar vermeyecek ve işlenilen bilginin zarar görmemesi sağlanacak şekilde, katılımcı kurumlarla koordineli olarak gerçekleştirilmiştir (TÜBİTAK BİLGEM, 2011). Tatbikatın ardından kurumlara şu öneriler sıralanmıştır (TMMOB EMO, 2010):

- ✓ Kurum içi olay müdahale süreçleri açık ve yazılı hale getirilmeli,
- ✓ Birimler arası iletişim geliştirilmeli,
- ✓ Saldırı kayıtlarının saklama süreleri, inceleme yapmayı sağlayacak şekilde ayarlanmalı,
- ✓ ve Haberleşme için kullanılan altyapı; daha sık test edilmeli, bilgiler güncellenmelidir.

3.3.3.2. Ulusal Siber Güvenlik 2011 Tatbikatı

Gerçekleştirilmiş tatbikatların ikincisi olan Ulusal Siber Güvenlik 2011 Tatbikatı; 41 kamu kuruluşu, özel sektör ve sivil toplum kuruluşunun katılımıyla hem gerçek hem de simülasyon ve muhtemel senaryolarla gerçekleştirilmiştir. Ulusal Siber Güvenlik 2011 Tatbikatı; katılımcı kuruluşların bu alandaki yeteneklerinin test edilmesi, muhtemel saldırılara karşı müdahale etme yeteneğinin kazandırılması (Erçağlar, 2017, s. 33-34) ve ülke genelinde siber güvenlik bilincinin arttırılması maksadıyla idari ve hukuksal süreçlerin gözden geçirildiği bir tatbikat olmuştur (Meral, 2015, s. 119-120).

Bu tatbikatlar sonucunda kurumlara ilişkin olarak aşağıdaki sonuçlara ulaşılmıştır (Yaşar ve Çakır, 2015, s. 502):

- ✓ Bazı kurumlarda bilgi güvenliği politikalarının olmadığı, saldırı esnasında ve sonrasında ne tür faaliyetler icra edileceğine dair siber güvenlik kültürü oluşturulmadığı,
- ✓ Sistem yöneticilerinden birçoğunun yeterli teknik bilgiye sahip olmadığı,
- ✓ Bazılarında STS (Saldırı Tespit Sistemleri) olmadığı olanlarda ise saldırıların tespitinde sıkıntılar yaşandığı,

- ✓ Bazılarında teknik çözüm arayışına önem verilirken sosyal mühendislik saldırılarına karşı personelde farkındalık eksikliği bulunduğu,
- ✓ Antivirüs yazılımlarının düzenli olarak güncellenmediği,
- ✓ Bazılarında iletişim hususunda eksiklikler bulunduğu, saldırı anında gerekli adımların atılması konusunda sıkıntılar yaşandığı ve ilgili mercilerle temas kurmada problemler olduğu,
- ✓ Bazı personellerin kurumda (erişim izni olmadığı halde) kendisiyle ilgili olmayan hizmetlere erişebildiği, bazılarında sistem tasarım aşamasında güvenliğin temel bir tasarım ilkesi olarak ele alınmamasından dolayı güvenlik olayları yaşandığı ve bu olaylara etkin müdahalenin zorlaştığı,
- ✓ Bazılarının (yaşanan sistem kesintisine yol açan güvenlik olayı neticesinde) iş süreçlerinin devamlılığını sağlayacak iş sürekliliği planına sahip olmadıkları,
- ✓ DDoS saldırısı sonucunda bazı kurumların hizmetleri kesintiye uğrarken, internet servis sağlayıcılarından bu tür saldırılara karşı hizmet satın alanların sıkıntı yaşamadığının görülmesi sonucunda kurumlar arası iletişime, işbirliğine ve koordinasyona verilmesi gereken önemin yeterince anlaşılamadığı,
- ✓ Birçoğunun web uygulamalarında çeşitli açıklıklar bulunduğu, nispeten daha az güvenlik açığı bulunanların ise web uygulamalarını farklı kurumlara denetlettirdiği ya da web uygulamalarını geliştirirken güvenliğe dikkat ettikleri,
- ✓ Özel bir bilgi güvenliği birimlerine sahip olan kurumların yapılan saldırıları analiz etmede daha başarılı oldukları,
- ✓ Bazı kurumların da ulusal mevzuat hususunda yeterli bilgiye sahip olmamalarından dolayı yazılı senaryolarda siber suç olarak tanımlanan fiilleri adli mercilere bildirmedikleri tespit edilmiştir.

3.3.3.3. Siber Kalkan 2012 Tatbikatı

Türkiye'de internet erişim hizmeti sunan ve internete erişimi sağlayan haberleşme sektörünün %99,9'unu oluşturan 12 firmanın katılımıyla (Erçağlar, 2017, s. 34), siber saldırılara karşı önlem alma yeteneğinin kazandırılması (Kaya, 2017, s. 23) ve siber saldırıların bertaraf edilebilmesi için teknik yönlerin geliştirilmesi maksadıyla (Sanalp, 2016, s. 40) BTK tarafından 2012 yılında gerçekleştirilmiştir (Ercan, 2015, s. 33).

"Siber Kalkan Tatbikatı 2012" ile aşağıdaki sonuçlara ulaşılmıştır (Siber Kalkan Tatbikatı 2012 Sonuç Raporu):

- ✓ DDoS saldırılarında üretilen yasal olmayan trafiğin hedefe ulaşmadan erişim sağlayıcı seviyesinde engellenebilirliği test edilmiştir.
- ✓ Farklı DDoS saldırı türleri için en etkili önlemlerin neler olabileceği belirlenmiştir.
- ✓ Erişim sağlayıcıların mevcut teknolojik donanımları ve uzmanların deneyimlerinin DDoS saldırılarına karşı ne derece etkili olabildiğinin tespiti yapılmıştır.
- ✓ Erişim sağlayıcıların kendi içlerindeki ve bir üst erişim sağlayıcı ile koordinasyon kabiliyetinin belirlenmesi hususlarında başarı sağlayarak siber olaylara müdahalede ulusal düzeyde koordinasyon yeteneği ile bilgi ve tecrübe paylaşımının geliştirilmesi, bilinçlendirme ve farkındalık oluşturulması ve nihayetinde ulusal siber güvenlik kabiliyetlerimizin arttırılması konusunda atılan önemli bir adım olmuştur.
- ✓ Siber saldırıların gerçekleştiği mecra olan elektronik haberleşme altyapısının önemli aktörleri olan erişim sağlayıcıların ulusal siber güvenliğin sağlanmasındaki kritik rolüne vurgu yapılması açısından da başarı elde edilmiştir.
- ✓ Tatbikatın teknik açıdan en somut çıktısı ise DDoS saldırıları ile İnternet Servis Sağlayıcılar düzeyinde mücadele edebilme imkân ve kabiliyetlerinin geliştirilmesi olmuştur. Zira tatbikat sürecinde her bir erişim sağlayıcıya yapılan saldırılar sırasında saldırının tespit edilmesi ve DDoS ile mücadelede neler yapılması gerektiği canlı olarak tecrübe edilmiştir.
- ✓ Erişim sağlayıcılar kendi imkânları ve bir üst erişim sağlayıcı ile gerçekleştirdikleri işbirliğiyle saldırı trafiklerini engellemeye çalışmışlardır. Bu anlamda, "Siber Kalkan Tatbikatı 2012" ile elektronik haberleşme sektöründe faaliyet gösteren erişim sağlayıcılarla işbirliği sağlanarak siber saldırıların büyük oranda hedefine ulaşmadan altyapı seviyesinde önlenebileceği görülmüştür.

3.3.3.4. Ulusal Siber Güvenlik 2013 Tatbikatı

UDHB koordinesinde TÜBİTAK ve BTK tarafından yürütülen ikinci siber güvenlik tatbikatı olan Ulusal Siber Güvenlik 2013 Tatbikatı; enerji, sağlık, iletişim,

ulaştırma gibi CI'leri yöneten ve işleten kurumları da kapsayan ve bunun yanında adli ve kolluk birimlerinin katılımını da sağlayan, 41'i oyuncu, 20'si gözlemci olmak üzere toplamda 61 kurum ve kuruluşun katılımı ve toplamda da 194 personel ile birlikte 25 Aralık 2012 - 11 Ocak 2013 tarihleri arasında düzenlenmiştir (Ercan, 2015, s. 33). Bu tatbikat; kurumlar arası koordinasyonun artırılması, kurumların bilgi güvenliği sistemlerinin güçlendirilmesi ve siber saldırılara önlem alınması maksadıyla düzenlenmiştir (Erçağlar, 2017, s. 34).

3.3.3.5. Uluslararası Siber Kalkan 2014 Tatbikatı

2 Mayıs 2014'te Sanal Ortamda İşlenen Suçlar Sözleşmesi'nin çekinceler ve beyanlarla birlikte yasalaşması ve 2013-2014 USGSEP'nin 20 Haziran 2013'te yürürlüğe girmesi sonucunda uluslararası alanda 15-16 Mayıs 2014'te UDHB'nin desteği ve BTK ile ITU-IMPACT'ın işbirliğiyle İstanbul'da Uluslararası Siber Kalkan 2014 Tatbikatı (International Cyber Shield Exercise) düzenlenmiştir. Etkinliğin birinci gününde; Çocukların İnternetin Zararlı Etkilerinden Korunması, Mobil Güvenlik ile Adli Bilişim ve Siber Soruşturma konulu çalıştaylar, ikinci gününde ise 19 ülkenin katılımıyla tatbikat gerçekleştirilmiştir. Gerçekleştirilen tatbikatın amaçları ise aşağıdaki gibi belirlenmiştir (Çeliktaş, 2016, s. 90):

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.

Ulusal tatbikatların sonuçları incelenecek olursa bilhassa eksikliklerin objektif bir şekilde tespit edilmesinin gelecekte karşılaşılabilecek daha geniş saldırılar karşısında kurumların daha ciddi zararlar görmemesi noktasında büyük önem arz etmektedir. Bu da ulusal tatbikatların ne kadar faydalı olduğunu göstermektedir (Ercan, 2015, s. 33-34).

SGK oluşturulmadan önce de siber güvenliğin sağlanması noktasında çeşitli çalışmalar yapılmaktaydı. Bunlardan en önemlisi ise kurumların siber saldırılara karşı hazırlıklı olup olmadıklarının denetlenmesiydi. Bu çerçevede gerçekleştirilen

tatbikatlara, kamu sektörünün yanı sıra özel sektörden de çok sayıda firmanın katılım sağladığı görülmektedir. 2013'te gerçekleştirilen Ulusal Siber Güvenlik 2013 Tatbikatı'dan, 2011 yılında yapılan Ulusal Siber Güvenlik 2011 Tatbikatı'na göre daha başarılı sonuçlar elde edildiği söylenebilir. Bunun yanında 2012'de icra edilen Siber Kalkan 2012 Tatbikatı'nda DDoS saldırılarının engellenebilir olduğu tespitine varılmıştır. Bunlara ilaveten siber alanın düzenlenmesi hususunda da Türk Ceza Kanunu'nda bilişim alanına yönelik suçlar, elektronik ticaret kanunu, kişisel verilerin korunması kanunu gibi kanunlar çıkarılmış ve bununla bilişim sistemlerinde ortaya çıkabilecek hukuki uyuşmazlıkların çözümü amaçlanmıştır (Sarı, 2013, s. 68).

3.3.3.6. Ulusal Siber Savunma 2017 Tatbikatı

UDHB tarafından, 2016-2019 USGSEP'si çerçevesinde 29 Kasım 2017'de "Ulusal Siber Savunma 2017 Tatbikatı" düzenlenmiştir. Tatbikat'ın açılışında dönemin Ulaştırma, Denizcilik ve Haberleşme Bakanı Ahmet Arslan bir konuşma yapmıştır. Bakan Arslan, bugüne kadar 3'ü ulusal, 1'i uluslararası olmak üzere toplam 4 tatbikatın gerçekleştirildiğini ve 2017 Tatbikatı'nın gerçek ortam saldırıları, simülasyonlar, bulgu incelemeleri ve masa başı senaryolarının birlikte uygulandığı ilk Tatbikat olduğunu ve bu çerçevede diğer tatbikatlardan ayrıldığını belirtmiştir. Bunun yanı sıra Tatbikat'ın amacını kurumların kendi eksikliklerini gerçek ortamda ve simülasyon ortamında görmeleri ve alınan sonuçların ileride yapılacak çalışmalara ışık tutması olarak açıklamıştır (Sonhaberler, 2017).

Tatbikat iki faz halinde gerçekleştirilmiştir. Birinci faz 6-23 Kasım tarihi arasında kurumlara gerçek ortamda siber ataklar gönderilerek yapılmıştır. İkinci faz ise simülasyon ortamında ağ üzerinden gerçekleştirilmiştir. Birinci faz için gönüllü 41 kurumdan belirlenen 20 kuruma 7/24 esaslı olmak üzere gerçek ortamda ve her birine farklı IP adreslerinden saldırılar gerçekleştirilmiş ve toplam 60 adet test icra edilmiştir. İkinci faz için ise 32 kurumdan 145 oyuncu ve 26 kurumdan 60 gözlemci katılım sağlamıştır (Yenigaste, 2017). Tatbikat kapsamında yapılan siber saldırılar sadece gündüz mesai saatinin yoğunluğunun olduğu dönemde değil, gece de devam etmiştir. Tatbikat sonucunda; tatbikata katılan kurumların bir kısmının saldırıların tamamını tespit etme ve raporlama alanında eksiklerinin olduğu, bu eksikliklerin

kamu kurumlarının kendi imkanlarıyla giderilebilecek nitelikte olduğu ve saldırıların her an yapılabileceği görülmüştür (TIMETÜRK, 2017).

Gelecek yıllarda Türkiye'de siber güvenliğin gelişimi hakkında kapsamlı bir akademik çalışma yapılacak olursa, 29 Kasım günü Ankara'da gerçekleşen Ulusal Siber Güvenlik Tatbikatı bir dönüm noktası olarak bu çalışmada yerini alacaktır. Her ne kadar ulusal çaptaki beşinci tatbikat olarak kayıtlara geçse de son tatbikatın 'dönüm noktası' olarak nitelenmesine sebep olacak birçok farklı özellik bulunmaktadır. Bu özellikler aşağıdaki gibi sıralanabilir (Çelik, 2017):

- ✓ Otuzdan fazla kamu kurumundaki SOME görevlilerinin (yaklaşık 150 kişi) katıldığı tatbikatta, UDHB Bakanı Ahmet Arslan'ın açılışa katılarak konuşma yapmasının neden olduğu geniş medya ilgisi başlı başına bir farkındalık etkisi oluşturmuştur.
- ✓ Tatbikatın belki de en önemli ve en heyecan verici tarafı, özel sektörün ilk kez elini taşın altına koyması ve UDHB'nin düzenlediği böylesine kritik bir etkinliğin organizasyonu ve icrasında etkili olması olmuştur.
- ✓ Siber dünyanın getirdiği risk ve tehditleri devletlerin sadece kendi kaynaklarıyla göğüslemeye çalışmaları neticesi olmayan bir çabadan ibarettir. Bu yüzden özel sektör ne kadar işin içine girerse o kadar verimli ve başarılı bir çalışma ortaya konmuş olacaktır.
- ✓ Ulusal siber güvenlik stratejisinin eylem planında yer alan 'ulusal tatbikat' hedefinin gerçekleştirilmesi gelecek adına umut verici ve kesinlikle geliştirilmesi zorunlu bir adımdır. Sadece ulusal tatbikatlarda değil, uluslararası tatbikatlar da (NATO vb.) bile artık özel sektör damgası görünür şekilde kendini belli etmiştir.
- ✓ Tatbikatın bir başka özelliği ise simülasyon ortamında kamu kurumlarına gerçek saldırıların ilk kez yapılması olmuştur.

3.3.3.7. Uluslararası Siber Kalkan 2019 Tatbikatı

Türkiye'nin ulusal ve uluslararası alanda düzenlediği tatbikatların sonuncusu olan Uluslararası Siber Kalkan 2019 Tatbikatı, 19-20 Aralık 2019 tarihlerinde 17 ülkeden 87 katılımcıyla 19 takımın katılımıyla BTK tarafından düzenlenmiştir. Tatbikat, olay müdahale kabiliyetlerinin ve hazırlık seviyelerinin artırılması, siber

risklerin ve etkilerinin ortak anlayışla ele alınması ve siber tehditlerin azaltılması amacıyla düzenlenmiştir (Türksat, 2019).

Tatbikat'ın açılışında konuşan BTK Başkanı Ömer Abdullah Karagözoğlu, "Yaptığımız siber tatbikatların ülkeler arası deneyim paylaşımı ve işbirliği açısından önemli bir araç olduğunu vurgulamak isterim. Bunun için ülkelerin, uluslararası düzeyde koordinasyon, işbirliği, bilgi paylaşımı ve iletişim kabiliyetlerini eş zamanlı olarak ortaya koyması elzem hale geliyor. Ülkeler arasındaki ikili ve bölgesel anlaşmalar, siber güvenlik alanındaki işbirliğini güçlendiren önemli adımlar olarak öne çıkıyor." (TRTHABER, 2019) açıklamasında bulunmuş ve dikkatleri, tatbikatların uluslararası ölçekte ve işbirliği çerçevesinde olmasına çekmiştir.

Tatbikatın teknik altyapısı ve senaryoları tamamiyle USOM bünyesinde hazırlanmış ve hazırlanan bu senaryolar doğrultusunda kıyasıya rekabet ve zorlu mücadelelerden geçilmiştir. Sonuç olarak takımlar, siber olaylara müdahale kabiliyetlerini güçlendirmek ve hazırlık seviyelerini artırmak adına önemli tecrübeler edinmişlerdir (BTK, 2019). 17 ülkeden 19 takımın katılımıyla gerçekleşen tatbikatta, İspanya'dan gelen takım birinci, Litvanya'dan tatbikata katılan takım ikinci ve Türkmenistan'dan katılan takım ise üçüncü sırayı almıştır. Birinciliği elde eden İspanya takımı yarışmacılarına altın madalya, Litvanya takımı yarışmacılarına gümüş, Türkmenistan takımı yarışmacılarına bronz madalyalar ve katılım sağlayan diğer tüm takımlara da katılım sertifikaları verilmiştir (Memleket, 2019).

SONUÇ

İnternette ulaşılamayan diğer dijital üretimler hariç yalnızca internet üzerinden günlük 5 milyar GB'i aşan bir bilgi üretimi söz konusudur. Bu kapsamda siber uzay; sınırlarının insanlar tarafından tamamıyla bilinmediği, bütün bilgisayar ve ağ sistemlerini içerisinde barındıran, her saniye genişleyen bir alan olarak karşımıza çıkmaktadır. Bireyleri, küreselliği, ekonomiyi, ticareti, iletişimi, çatışmaları ve neredeyse her alanı etkileyen, değiştiren ve dönüşümünü sağlayan siber uzay, gün geçtikçe etkinliğini arttırmaktadır. Bu nedenle, siber uzayın sosyal etkilerini analiz etme çalışmaları, onun hızına ayak uydurmada güçlüklerle karşılaşabilir; fakat siber alandaki çalışmalar çoğaldıkça onu anlama oranı da artacaktır. Siber uzayı var eden insan, onu anlayabilecek birikime de sahiptir.

Siber saldırılar, kurtçuklar, Truva atları, virüsler, DDoS saldırıları ve fidye yazılımları olmak üzere teknik tabanlı olan siber saldırılar ile kandırma/ikna etme yöntemlerinden ileri gelen sosyal mühendislik şeklinde yapılan teknik olmayan siber saldırılar olarak vuku bulmaktadır. Her geçen gün bir yenisinin geliştirildiği bu siber saldırı tekniklerinin eğitim ve teknik tabanlı uygulamalar ile durdurulması yetersiz kalmaktadır. Buradan hareketle siber saldırıların engellenmesinin en mühim yöntemi olarak karşımıza güvenliğin en zayıf halkası olan kullanıcının bilinçlendirilmesi seçeneği belirmektedir.

Farklı amaçları ve teknik özellikleri olan, yeni, fakat bir o kadar tehlikeli olan, son 30 yıldır siyaseti fazlasıyla etkileyen, çeşitli boyutlarıyla iç ve dış politikada etkiler oluşturan siber saldırıların, dünyamızı gelecekte nasıl şekillendireceği bilinmezliklerle dolu bir gerçeklik olarak karşımıza çıkmaktadır. Belirsizliklerle dolu olan siber saldırılar konusunda şirketler, kurumlar ve devletler bilgiyi korumada ve sızıntıları önlemede yeni teknikler geliştireceklerdir.

Diplomatların, karar alıcıların ve liderlerin her söylediklerinin bir gün ortaya çıkma olasılığına karşı söyleyeceklerine fazlasıyla dikkat edip daha zor şartlarla karşılaşmamaya özen göstermesi gerekecektir. Buna ek olarak Ortadoğu'da demokrasi mücadelesi verdiğini öne süren büyük güçlerin işi oldukça zorlaşacaktır.

Fırsatlar dünyası olma özelliğiyle birlikte günümüzde bireysel düzeyden küresel düzeye güvenlik problemleri üreten siber uzay, ciddi bir güç aygıtına evrilmiş olmasından dolayı vazgeçilemeyen bir alan halini almıştır. Vazgeçilemeyen bu alanın güvenli kılınabilmesi için ise çok sayıda ülke; siber güvenlik stratejileri oluşturmaya, politikalar belirlemeye ve ülke ICT'lerinin de buna uygun pozisyon almasını sağlamaya odaklandıkları görülmektedir.

Bu çerçevede, Türkiye de siber güvenliğini sağlamak için siber uzay çağının gerekliliklerine ayak uydurmaya odaklanmıştır. Türkiye'nin siber güvenliğini sağlamasına yönelik gerçekleştirdiği faaliyetlerin ilki, "2003/10 Sayılı Başbakanlık Genelgesi"yle başlamıştır. Bu genelge ile OECD üyesi ülkeler tarafından güvenlik kültürünün oluşturulması amacıyla hazırlanmış olan "Bilgi Sistemlerinin Güvenliğine İlişkin Rehber İlkeler" kararlarının hem kamu kuruluşlarının hem de her düzeyden kullanıcının çalışmalarında dikkate alması ve benimseyip uygulamasının faydalı olacağı vurgulanarak ICT'lerin tehditlerden korunması amaçlanmıştır.

Bu gelişmenin ardından; MGK, Türkiye'nin "Kırmızı Kitap"ı olarak bilinen askeri stratejisine Ekim 2010'da diğer geleneksel olmayan tehditlerin yanı sıra siber tehditleri ekleyerek ilk kez siber güvenlik tehditlerini yeni ulusal stratejinin bir parçası haline getirdi. Siber güvenlik tehditlerinin Türkiye'nin en tepedeki ulusal güvenlik kurulunun bildirisine dahil olması, bu konudaki kararlılığın ortaya konması açısından bir ilk olmuştur.

MGK'nin bildirisine siber tehditleri dahil etmesinin ardından bilgi toplumu olma yolunda politika ve stratejilerin belirlenmesine yönelik atılan bir diğer önemli adım, Eylül 2011'de UDHB'nin teşkilat ve görevlerinin düzenlenmesi olmuştur. Bu çerçevede siber güvenlik faaliyetleri ve hizmetlerine ilişkin kamu kurum ve kuruluşlarıyla gerekli işbirliği ve koordinasyonun sağlanmasına ilişkin usul ve esasların belirlenmesi ve gerekli düzenlemelerin yapılması görevi, UDHB'ye

bırakılmıştır. Bu görev tahsisinin ardından ise bir çalıştay düzenlenmiş, tatbikatlar yapılmış, kamu kurumlarında yapılanmalar söz konusu olmuş ve böylelikle de Türkiye'nin siber güvenliğinin yol haritası yavaş yavaş ortaya çıkmaya başlamıştır.

UDHB'nin görev ve sorumluluklarının belirlenmesinin ardından bu kez Ekim 2012'de 'Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı' ile UDHB'nin başkanlığında ve ilgili kamu kuruluşlarından 12 kişilik üst düzey yönetici grubunun idaresinde SGK'nin kurulması gündeme gelmiştir. Böylelikle de siber güvenliğe ilişkin ilke, görev, sorumluluk ve teşkilat yapılanması resmi boyut kazanarak Türkiye'nin siber güvenliğini sağlama yolundaki en stratejik adımlardan biri atılmıştır.

SGK, stratejik bir adım olma durumunu "2013-2014 USGSEP"sini yayımlamasıyla göstermiştir. Bu stratejiyle aşağıdaki yol haritası dahilinde ulaşılmak istenen sonuçlar belirlenmiştir:

- ✓ Yasal Düzenlemelerin Yapılması ve Adli Süreçlere Yardımcı Olacak Çalışmaların Yürütülmesi,
- ✓ USOM Organizasyonunun Oluşturulması
- ✓ Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi
- ✓ Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi ve Bilinçlendirme Faaliyetleri
- ✓ Siber Güvenlikte Yerli Teknolojilerin Geliştirilmesi
- ✓ Ulusal Güvenlik Mekanizmalarının Kapsamının Genişletilmesi

Bundan sonra ise son olarak Eylül 2016'da '2016-2019 USGSEP'si yayımlanmıştır. Strateji dahilinde belirlenen yol haritası aşağıdaki gibidir:

- ✓ Siber Savunmanın Güçlendirilmesi ve CI'lerin Korunması,
- ✓ Siber Suçlarla Mücadele,
- ✓ Farkındalık ve İnsan Kaynağı Geliştirme,
- ✓ Siber Güvenlik Ekosisteminin Geliştirilmesi,
- ✓ Siber Güvenliğin Milli Güvenliğe Entegrasyonu

Türkiye'nin siber güvenlik stratejilerine yönelik yapılacak değerlendirmelerin ilki, 2013-2014 stratejisinin oldukça ayrıntılı bir şekilde hazırlanmış oluşu noktasındadır. Diğer ülke stratejilerinin incelenmesinde de görülebileceği üzere, özellikle de demokratik işleyişinin ileri düzeyde olduğu düşünülen ABD bile kendi stratejisini böylesine detaylı bir şekilde açıklamaktan imtina etmiştir. Aynı şekilde Rusya da stratejilerini detaylarıyla paylaşmaktan kaçınmıştır. Bu kadar detaylı paylaşılan 2013-2014 USGSEP'sindeki amaçların çoğuna ulaşılmadığı da görülmektedir. 2016-2019 USGSEP'sinin ise öncekine oranla daha makul ve genel hatlarıyla hazırlanıp paylaşıldığı görülebilmektedir. Bu konuda yapılması gereken şeyin siber güvenlik stratejilerinin detaylarına inilmesinden çok, stratejilerin hem toplumda hem de ilgili siber güvenlik kurumlarında bir siber güvenlik bilinci oluşturmasına, ana hatlarıyla hazırlanılmasına ve temel hedefler belirleyecek şekilde olmasına odaklanılmalıdır. Genel ifadelerle hazırlanmış ve belirlenen hedeflere ulaşmış stratejilere sahip olabilmek için de ilgili kurumların koordinasyonunu sağlayacak olan bir kurumsal yapılanmaya gidilmesi gerekliliği unutulmamalıdır.

Türkiye'de şu ana kadar biri, 2013-2014; diğeri ise 2016-2019 yıllarını kapsayan iki tane USGSEP hazırlanmış bulunmaktadır. Bu her iki stratejinin yürütülmesinin takibi, UDHB tarafından yapılmaktadır. UDHB bu stratejilerin yürütülmesinin takibini ise aldığı raporlar sonucunda düzenlediği çalıştaylar ile yapmaya çalışmaktadır. UDHB bu noktada yakın işbirliği, etkin veri paylaşımı, bürokratik güç, teknik ve hukuki altyapı yetersizlikleri gibi nedenlerden dolayı gerekli önlemleri almada yetersiz kalmaktadır. Yetersiz kaldığı noktada ise SGK'nin müdahil olması söz konusu olmaktadır. SGK ise böylesine hızlı gelişmelerin yaşandığı ve bazen neredeyse her gün toplanılıp karar alınması gerekliliğinin zorunlu olduğu bir siber uzayda, şu ana kadar 4 kez toplanmış bulunmaktadır. Oysa siber uzayda yetki makamları arasında çıkabilecek karmaşıklıkların çözümlenmesinde, son teknolojik gelişmelerin izlenerek buradaki yaklaşım farklılıklarının yasal düzenlemelere etkin bir şekilde yansıtılmasında, olabildiğince hızlı hareket edilmesi gereksinimi vardır. Çünkü siber uzay doğası gereği hızlıdır ve güvenliğinin sağlanması da o ölçütte olmalıdır. Bu durumda bunu sağlayacak merkezi bir otoritenin varlığı önem kazanmaktadır. Cumhurbaşkanlığına bağlı ya da özerk bir

yapıda olacak olan bu kurumun sıkı ve etkin işbirliği mekanizmasına engel oluşturamayacak bürokratik yapısının korunmasının önemi hayati derecededir.

Kamu kuruluşlarındaki durumu ele aldığımızda, buradaki siber güvenlik uygulamalarının bir ölçüye kadar yönlendirici rehber ilkeler eşliğinde yapıldıkları, fakat nihai olarak daha çok birbirinden bağımsız projeler şeklinde ve ulusal düzeyde bir denetim ve uygulama mekanizmalarından yoksun olarak uygulandıkları görülmektedir. Bunun yanı sıra; uzman bilişim personellerini istihdam etmede şartlarının yetersiz olduğu, güvenlik ürünü teminatlarında yeterli bilgiye sahip olmadıklarından ötürü siber güvenlik ürün ve hizmet tedariğinde bu tedariği yapan firmaların bilgileri ölçüsünde hareket ettikleri ve bu tedarikleri test etme olanağından yoksun oldukları, enerji/bankacılık/telekomünikasyon gibi CI sektörlerinde yönlendirici kuruluşların da etkisiyle siber güvenliğe yönelik bir ölçüye kadar düzenlemelerin yapıldığı, fakat bu CI sektörlerinin birbirleriyle olan bağımlılıklarını da kapsayan bütünlüklü bir korumadan yoksun oldukları, CI sektörlerinden olan bankacılık sektörünün bile bir elektrik kesintisi sırasında bu konuda gerekli önlemleri almaktan yoksun olduğu, CI'lerin siber güvenliğinin sağlanmasında kritiklik düzeylerine değil kuruluş yöneticilerinin konuya verdikleri önem ölçütünce önlem aldıkları gözlemlenmiştir. Yukarıda ele aldığımız bunca kurumsal sorunun siber güvenliğinin sağlanması; diğer ülke incelemelerinde de görüleceği üzere ancak üst düzey kanuni bir güce sahip, üst düzey uzmanlık bilgisi gerektiren ve kurumlar arası hiyerarşik yapıları da göz önünde bulundurarak tek bir merkez tarafından yönetilen merkezi bir yapılanmanın kurulması gereksinimidir. Böyle bir kurum; ulusal koordinasyonu sağlayabilir, siber güvenlik önlemleri alabilir, yasal düzenlemelerin tüm kurumlarda uygulanmasını sağlayabilir ve kurumlar arası etkin işbirliğini olanaklı kılabilir.

Türkiye'nin siber güvenliğinin değerlendirilmesinde göz önünde bulundurulması gereken bir diğer nokta ise TSK'nin 2013 yılında kurduğu Siber Savunma Komutanlığı'dır. Siber Savunma Komutanlığı'nı, ABD DoD'nin 2010 yılında kendi bünyesinde kurduğu CYBERCOM ile karşılaştırırsak Türkiye'nin bu konuda yapması gerekeni ortaya koymuş olabileceğiz. Bu bağlamda TSK'nin kurmuş olduğu Siber Savunma Komutanlığı'nın amaçlarını bu şekilde sıralayabiliriz:

TSK'nin kullandığı siber uzayın güvenliğini 7/24 esasına göre müdahalede bulunarak temin etmek, hem NATO'nun hem de kendi ülkesinin düzenlediği tatbikatlara katılım sağlamak, TSK bünyesinde yürütülen siber uzay farkındalığını/eğitimini yerine getirmek, TSK'nin kullandığı ağların denetimini ve sınamasını yapmaktır.

ABD'nin siber güvenlik stratejisinin yürütülmesinde 2010 yılına kadar "en etkin kurum" olan DoD, bu konumunu 2010'da kendi bünyesinde kurulan CYBERCOM'a devretmiştir. Bundan sonra siber uzay ile ilgili konularda en etkin kurum olarak ön plana çıkmış olan CYBERCOM, ABD ordusu için siber kaynakların teminini, stratejik savunma ve müdahale planlarının hazırlanmasını ve askeri IT ağlarının eşanlı savunmasını yapmaktadır. Kendi yapılanmasının içerisinde 24. Hava Kuvvetleri, Ordu/Donanma/Deniz Kuvvetleri Siber Savaş Birimlerine sahip olmanın yanında DoD'nin Kara/Deniz/Hava Kuvvetleri Daireleri'nin her birinde kendi görev ve sorumluluk alanlarına ilişkin koordinasyon faaliyetlerini yürüten birer Birleşik Siber Merkezi (Joint Cyber Center)'ne de sahiptir. Ayrıca NSA'nın başkanı olan NSA direktörü, aynı zamanda CYBERCOM'un komutanlığını da yapmaktadır. CYBERCOM, bu yapılanması ve çok sayıdaki alt birimiyle oldukça geniş bir yelpazede etkinlik göstermektedir (Darıcılı, 2019, s. 22-23).

Bu açıdan TSK'nin Siber Savunma Komutanlığı'nın, ABD'nin CYBERCOM'uyla kıyaslanmasının getireceği sonuçtan da anlaşılacağı üzere, Siber Savunma Komutanlığı'nın siber uzayda meydana gelecek olası bir savaş durumunda CYBERCOM'a oranla yeterlilikten yoksun olacağı görülebilecektir. Bu durumda TSK'nin Siber Savunma Komutanlığı'nın, CYBERCOM benzeri geniş yelpazeli organizasyon ve faaliyet ağlarına sahip olması, onu siber uzayda vuku bulacak bir siber savaş durumunda oldukça etkin bir kurum haline getirecektir.

KAYNAKÇA

Ada, M. (2018). NATO Üyesi Ülkelerin Siber Güvenlik Stratejileri Açısından İncelenmesi. Yayınlanmamış Yüksek Lisans Tezi. Ankara: Gazi Üniversitesi. Bilişim Enstitüsü.

Adams, S. A., Lorenzo M. B., Corte, D., Galič, M., Kala, K., Koops, Bert-Jaap., Leenes, R., Schellekens, M., Silva, K., Ivan Š. (2015). The governance of cybersecurity. (1. Baskı). Netherlands: Tilburg University.

Agentura.Ru. (1997). Cyber Wars. Erişim Tarihi: 3 Kasım 2019. http://www.agentura.ru/english/equipment/

Aktaş, C. (2006). Türkiye'de Bilgisayar ve İnternet Kullanımının Yaygınlaştırılmasında İnternet Kafelerin Rolü. İstanbul Üniversitesi İletişim Fakültesi Hakemli Dergisi. Sayı: 27. Yıl: 2006. 1-16.

Akyazı, U. (2013). Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler. 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiri Kitabı. Sayı: 6, Yıl: 2013, Cilt: 6. 216-220.

Akyeşilmen, N. (2016). Editorial. Cyberpolitic Journal. Sayı: 1&2, Yıl: 1, Cilt: 1. Erişim Tarihi: 20 Kasım 2018, http://cyberpolitikjournal.org/index.php/2016-volume-1-issues-1-2/

Akyeşilmen, N. (2018). Disiplinlerarası Bir Yaklaşımla Siber Politika & Siber Güvenlik. (1. Baskı). Ankara: Orion Kitabevi.

Alagöz A. E. (2013). Siber Güvenlik Ekseninde Obama-Şi Görüşmesi. Erişim Tarihi: 31 Aralık 2018, http://www.bilgesam.org/incele/608/-siber-guvenlik-ekseninde-obama-si-gorusmesi/#.XGRRSyfVLIW

Alkan, M., Doğru, İ. A., Dörterler, M., Urfalıoğlu, R., Sümer, Ç. (2018). Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık. Sağıroğlu, Ş ve Alkan, M (Ed.). Mobil Cihazlarda Siber Güvenlik (309-345). Ankara: Grafiker Yayınları.

Alp, Ö. (2018). Akıllı Şehirlerde Siber Güvenlik. Yayınlanmamış Yüksek Lisans Tezi. İstanbul: İstanbul Bilgi Üniversitesi. Sosyal Bilimler Enstitüsü.

Arar, D. (2019). Siber Güvenlık ve Savunma: Farkındalık ve Caydırıcılık. Cyberpolitik Journal. Sayı: 8, Yıl:2, Cilt: 4. Erişim Tarihi: 25 Ocak 2020, http://cyberpolitikjournal.org/wp-content/uploads/2020/01/CPJ_Volume4_no8.pdf

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

Ataç, C., Akleylek, S. (2018). An Overview for the National Cyber Security Strategy. International Conference on Advanced Technologies, Computer Engineering and Science (ICATCES'18), May 11-13, 2018 Safranbolu, Turkey. 603-609.

Atlantic Council. (2012). Russia Considering Establishing Cyber-Security Command. Erişim Tarihi: 10 Kasım 2019 https://cdn.atlanticcouncil.org/blogs/natosource/russia-considering-establishing-cybersecurity-command/

Aykanat, A. (2017). Türkiye'yi Çevrimiçi Koruyan Ordu: TSK Siber Savunma Komutanlığı. Erişim Tarihi: 12 Ocak 2019, https://www.webtekno.com/internet/tsk-siber-savunma-komutanligi-h17616.html

Aytekin, A. (2015). Türkiye'nin Siber Güvenlik Stratejisi ve Eylem Planının Değerlendirilmesi. Yayınlanmamış Yüksek Lisans Tezi. Ankara: Gazi Üniversitesi. Bilişim Enstitüsü.

Bakrania, S., Haider, H. (2016). Safety, Security and Justice: Topic Guide. GSDRC. (1. Baskı). UK: University of Birmingham.

Başbakanlık Genelgesi (2003). E-Dönüşüm Türkiye Projesi. T.C. Başbakanlık Personel ve Prensipler Genel Müdürlüğü.

Bayrak, H. (2018). 2018 İnternet Kullanımı ve Sosyal Medya İstatistikleri. Dijilopedi. Erişim Tarihi: 6 Kasım 2018, https://dijilopedi.com/2018-internet-kullanimi-ve-sosyal-medya-istatistikleri/

Bayraktar, G. (2014). Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat. Güvenlik Stratejileri Dergisi. Sayı: 20, Yıl: 10, Cilt: 10. 119-147.

Benoliel, D. (2015). Towards a Cybersecurıty Policy Model: Israel National Cyber Bureau Case Study. North Carolina Journal of Law & Technology. Sayı: 3, Yıl: 2015, Cilt: 16.

Bilir, F. (2018). 100 Soruda Kişisel Verilerin Korunması Kanunu. (1. Baskı). Ankara: KVKK Yayınları.

Bozgeyik, A. (2018). Gaziantep'te Faaliyet Gösteren Orta ve Büyük Ölçekli İşletmelerin Siber Güvenlik Yönetim Yaklaşımlarının Analizi.

Yayınlanmamış Doktora Tezi. Gaziantep: Hasan Kalyoncu Üniversitesi. Sosyal Bilimler Enstitüsü.

Bozoklu, O., Çil, C. Z. (2017). Yazılım Güvenlik Açığı Ekosistemi ve Türkiye'deki Durum Değerlendirmesi. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi. Sayı: 1, Yıl: 3, Cilt: 3. 6-26.

BTK (Bilgi Teknolojileri ve İletişim Kurumu). (2019). Siber Kalkan 2019 Başladı. Erişim Tarihi: 22 Aralık 2019, https://www.btk.gov.tr/haberler/siber-kalkan-2019-basladi

Bülbül, A. (2013). E-Devlet Uygulamalarının Bilgi ve Belge Yönetimi Açısından Analizi. Yayınlanmamış Yüksek Lisans Tezi. İstanbul: T.C. Marmara Üniversitesi. Türkiyat Araştırmaları Enstitüsü.

Cebe, R., Suçin, H,. (2014). Fikir ve Sanat Eserleri Kanununun Kısa Tarihçesi ve Eser Üreticileri Açısından Önemi. Rast Müzikoloji Dergisi. Sayı: 1, Yıl: 2014, Cilt: 2. 120-127.

Chinadaily. (2012). China Calls To Tighten İnformation Security. Erişim Tarihi: 6 Kasım 2019 http://www.chinadaily.com.cn/bizchina/2012-07/18/content_16048274.htm

China's National Defense in 2004, Information Office of The State Council of The People's Republic of China December 2004. Erişim Tarihi: 14 Ekim 2019, http://en.people.cn/whitepaper/defense2004/defense2004.html

Choucri, N. (2013). Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences (Report No. N00014-09-1-0597).

Cyber Security Strategy of the Czech Republic for the 2011-2015 Period. Erişim Tarihi 19 Eylül 2019, https://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF

Cybersecurity Strategy for Germany 2011, German Federal Ministry of the Interior. Erişim Tarihi: 11 Eylül 2019, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Germany_2011_Cyber_Security_Strategy_for_Germany.pdf

Çakır, F. (2016). Politik İdealizm ve Siber Uzay ile Dönüşen Uluslararası İlişkiler. Cyberpolitic Journal. Sayı: 1&2, Yıl: 1, Cilt: 1. 140-152.

Çarıkçı, O. (2010). Türkiye'de E-Devlet Uygulamaları Üzerine Bir Araştırma. Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi. Sayı:12, Yıl: 2010/2. 95-122.

Çelik, K. E. (2017). Çin İstihbaratı: Deskriptif Bir Bakış. Asya Araştırmaları Dergisi. Sayı: 1, Yıl: Cilt: 1. 67-74.

Çelik, M. (2017). Ulusal Siber Güvenlik Tatbikatı: Uzun Bir Yola Açılan Dönüm Noktası. Erişim Tarihi: 12 Aralık 2019, https://siberbulten.com/makale-analiz/ulusal-siber-guvenlik-tatbikati-uzun-bir-yola-acilan-donum-noktasi/

Çelik, Ş. (2013). Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme. Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi. Sayı: 1, Yıl: 11, Cilt: 15. 137-175.

Çelikpala, M., Ergun, D., Bıçakçı, S. (2015). A Primer on Cyber Security in Turkey and The Case of Nuclear Power. Ülgen, S ve Kim, G (Ed.). The Cyber Security Scene in Turkey (22-51). İstanbul: Edam (The Centre for Economics and Foreign Policy Studies).

Çeliktaş, B. (2016). Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme. Yayınlanmamış Yüksek Lisans Tezi. Trabzon: Karadeniz Teknik Üniversitesi. Sosyal Bilimler Enstitüsü.

Çetin, H., Gundak, İ., Çetin, H. H. (2015). E-İşletme Güvenliği ve Siber Saldırılar Üzerine Bir Araştırma. Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi. Sayı: 6, Yıl: 6. Cilt: 2. 223-240.

Çil, C. Z., Sağıroğlu, Ş., Şentürk, H. (2012). Cyber Security Analysis of Turkey. International Journal of Information Security Science. Sayı: 4, Yıl: 2012, Cilt: 1. 112-125.

Çukurçayır, M. A., Çelebi, E. (2009). Bilgi Toplumu ve E-Devletleşme Sürecinde Türkiye. ZKÜ Sosyal Bilimler Dergisi. Sayı: 9, Yıl: 2009, Cilt: 5. 59–82.

Daban, C. (2016). Siber Güvenlik ve Uluslararası Güvenlik İlişkisi. Cyberpolitic Journal. Sayı: 1&2, Yıl: 1, Cilt: 1. 84-100.

Daniel, L. (2012). Intelligence Leaders Urge Congress to Act on Cyber Laws. US: American Forces Press Service. Erişim Tarihi: 27 Eylül 2019, https://www.globalsecurity.org/intell/library/news/2012/intell-120202-afps01.htm

Darıcılı, A. B. (2018). Sosyal ve Beşerî Bilimlere Dair Araştırma Örnekleri. Acaravcı, A (Ed.). Askerileştirilen ve Silahlandırılan Siber Uzay (311-327). Ankara: Nobel Akademik Yayıncılık.

Darıcılı, A. B. (2019). Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Potansiyel Siber Güvenlik Stratejisi. TESAM Akademi Dergisi. Sayı: 2, Yıl: 2019, Cilt: 6. 11-33.

DefenseNews. Interview: Estonia's Defence Minister Hannes Hanso. Erişim Tarihi 25 Eylül 2019, https://www.defensenews.com/interviews/2016/02/03/interview-estonia-s-defence-minister-hannes-hanso/

Demirhan, Y. (2011). Türk Kamu Yönetiminde E-Devlet Politikası ve Yönetimi. Yayınlanmamış Doktora Tezi. Ankara: Ankara Üniversitesi. Sosyal Bilimler Enstitüsü.

Dünya. (2011). TİB'de Yeni Daire Başkanlıkları Kuruldu. Erişim Tarihi: 15 Kasım 2019, https://www.dunya.com/gundem/tib039de-yeni-daire-baskanliklari-kuruldu-haberi-153782

Ege, B. (2012). Bilişimin Karanlık Yüzü: Siber Savaşlar. Tübitak Bilim ve Teknik Dergisi. Sayı: 540, Yıl: 2012, Cilt: 540. 18-22.

ENISA. European Union Agency For Cybersecurity. About ENISA. Erişim Tarihi 27 Eylül 2019, https://www.enisa.europa.eu/about-enisa

Ercan, M. (2015). Kritik Altyapıların Korunmasına İlişkin Belirlenen Siber Güvenlik Stratejileri. Yayınlanmamış Yüksek Lisans Tezi. Gebze: Teknik Üniversitesi. Sosyal Bilimler Enstitüsü.

Erçağlar, E. (2017). Siber Güvenlik Operasyon Merkezi Gereksinimleri. Yayınlanmamış Uzmanlık Tezi. Ankara: T.C. Çevre ve Şehircilik Bakanlığı.

Eren, M. (2017). Avrupa Birliği'nin Siber Güvenlik Stratejisi İçin Kuramsal Çerçeve ve Strateji Belgesi Öncesi AB'nin Eylemleri. Cyberpolitic Journal. Sayı: 3, Yıl: 2, Cilt: 2. 25-58.

Ermiş, U. (2018). Bir Güvenlik Sorunu Olarak Siber Uzay. Erişim Tarihi: 7 Ocak 2019, http://www.tasam.org/tr-TR/Icerik/50249/bir_guvenlik_sorunu_olarak_siber_uzay

Erol, S. E., Sağıroğlu, Ş. (2018). Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık. Sağıroğlu, Ş ve Alkan, M (Ed.). Siber Güvenlik Farkındalığı, Farkındalık Ölçüm Yöntem ve Modelleri (103-141). Ankara: Grafiker Yayınları

Estonia Country Report. (2011). European Network and Information Security Agency (ENISA). Erişim Tarihi: 8 Eylül 2019, https://joinup.ec.europa.eu/sites/default/files/document/2014-12/Estonia%20Country%20Report.pdf

Estonia Cyber Security Strategy 2008-2013. Erişim Tarihi: 23 Eylül 2019, https://www.unodc.org/res/cld/lessons-learned/cyber-security-strategy_html/Cyber_Security_Strategy_Estonia.pdf

Estonian Cyber Security Strategy 2014-2017. Erişim Tarihi: 22 Eylül 2019, https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

Europol. (2013). European Cybercrıme Centre-EC3. Erişim Tarihi 27 Eylül 2019, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Evron, G. (2008). Battling Botnets And Onlıne Mobs. Estonia's Defense Efforts During The Internet War. Georgetown Journal of International Affairs. Cilt: 9, Sayı: 1 (Winter/Spring).

Fact Sheet: The Department of Defense (Dod) Cyber Strategy April 2015. Erişim Tarihi: 7 Eylül 2019, https://archive.defense.gov/home/features/2015/0415_cyber-strategy/department_of_defense_cyber_strategy_fact_sheet.pdf

Fredrick, I. (2018). Nigerian Cyber Crime Bill: An Imperative To The Nigerian Armed Forces. Erişim Tarihi 28 Eylül 2019, https://medium.com/@fredwave/nigerian-cyber-crime-bill-an-imperative-to-the-nigerian-armed-forces-8cd0365b9d13

Germany Federal Office for Information Security (Bundesmat fur Sicherheit in der Informationstechnik-BSI). Erişim Tarihi: 20 Eylül 2019, https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cybersicherheit_node.html

Gibson, W. (1984). Neuromancer. (1. Baskı). New York: Ace Books.

Global Cybersecurity Index. (2019). ITU Publications. Erişim Tarihi: 25 Ocak 2020. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Göçoğlu, V. (2018). Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi. Yayınlanmamış Doktora Lisans Tezi. Ankara: Hacettepe Üniversitesi. Sosyal Bilimler Enstitüsü.

Göker, A. (2000). Politik Bilim. "Türkiye Ulusal Enformasyon Altyapısı Ana Plânı". Erişim Tarihi: 22 Ocak 2020, http://www.inovasyon.org/html/cbt/AYK.CBT4.pdf

Göker, A. (2004). Politik Bilim. E-Dönüşüm Türkiye. Erişim Tarihi: 10 Ocak 2019, http://www.inovasyon.org/html/cbt/AYK.CBTD96.pdf

Gurcan, M. (2012). Teoriler Işığında Güvenlik, Savaş, Barış ve Çatışma Çözümleri. Sandıklı, A (Ed.). Savaşın Evrimi ve Teorik Yaklaşımlar (71-129). İstanbul: Ecem Basın Yayın Reklamcılık.

Gürkaynak, M., İren, A. A. (2011). Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler. Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi. Sayı: 2, Yıl: 16, Cilt: 16. 263-279.

Hammond, H. P. (2016). Chancellor Speech: Launching The National Cyber Security Strategy. Erişim Tarihi: 5 Kasım 2016, https://www.gov.uk/government/speeches/chancellor-speech-launching-the-national-cyber-security-strategy

Han, A., Çelikpala, M. (2015). A Primer on Cyber Security in Turkey and The Case of Nuclear Power. Ülgen, S ve Kim, G (Ed.). Cyber Security And Nuclear

Power Plants: International Framework (52-68). İstanbul: Edam (The Centre for Economics and Foreign Policy Studies).

Hatipoğlu, C. (2017). Teknolojik Savaşlar: Siber Terörizm Tehditleri. 3. Uluslararası Politik, Ekonomik ve Sosyal Araştırmalar Kongresi Bildiriler Kitabı. Sayı: 3 Yıl: 2017, Cilt: 3. 157-168.

Hürriyet. (2018). Çin'in dijital istihbarat savaşı hızla büyüyor!. Erişim Tarihi: 22 Aralık 2018, http://www.hurriyet.com.tr/teknoloji/cinin-dijital-istihbarat-savasi-40993198

Information Security Doctrine of The Russian Federation (2000). Erişim Tarihi: 4 Kasım 2019, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf

Information System Auhority. (2009). EIC Creates Unit For Defense Of Critical İnformation System. Erişim Tarihi: 20 Eylül 2019, https://www.ria.ee/en/news/eic-creates-unit-defense-critical-information-systems.html

Intelligence and Security Committee (2011). Annual Report 2010–2011. UK: Crown copyright. Erişim Tarihi: 1 Kasım 2019, https://www.ozelburoistihbarat.com/Content/images/archieve/intelligence-and-security-committee-cf197ef6-96e2-4f6b-8cbc-28466e8487fa.pdf

International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World May 2011. The White House. Erişim Tarihi: 6 Eylül 2019, https://info.publicintelligence.net/WH-InternationalCyberspace.pdf

İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik. (2017). T.C. Resmi Gazete, 30035, 11 Nisan 2017.

Joubert, V. (2012). Five Years After Estonia's Cyber Attacks: Lessons Learned for NATO?, Research Paper No. 76, NATO Defense College

Kara, M. (2013). Siber Saldırılar-Siber Savaşlar ve Etkileri. Yayınlanmamış Yüksek Lisans Tezi. İstanbul: İstanbul Bilgi Üniversitesi. Sosyal Bilimler Enstitüsü.

Karabacak, B. (2010). Ulusal Sanal Ortam Güvenlik Politikası. Presented at Cyber Defence Workshop 4th International Information Security & Cryptology Conference (ISCTurkey 2010), May 6-8, 2010, Ankara.

Kasapoğlu, C. (2015). A Primer on Cyber Security in Turkey and The Case of Nuclear Power. Ülgen, S ve Kim, G (Ed.). TURKEY'S FUTURE CYBER DEFENSE LANDSCAPE. 2-21. İstanbul: Edam (The Centre for Economics and Foreign Policy Studies).

Kaya, G. D. K. (2017). Bilgi Güvenliği ve Siber Güvenlik Kapsamında Bakanlık Uygulamaları İçin Güvenli Yazlılım Geliştirme Metodolojisi Önerisi. Yayınlanmamış Uzmanlık Tezi. Ankara: T.C. Çevre ve Şehircilik Bakanlığı.

Kılan, K. (1976). Bilgisayar ve Ülkemizde Kullanımı Paneli. Elektrik Mühsndisliĝî Dergisi. Sayı: 240. 595-596.

Kızılkoyun, F. (2018). 45 Milyon Sosyal Medya Hesabına Siber Göz. Erişim Tarihi: 17 Kasım 2019, http://www.hurriyet.com.tr/gundem/45-milyon-sosyal-medya-hesabina-siber-goz-40868004

Kişisel Verilerin Korunması Kanunu. (2016). T.C. Resmî Gazete, 29677, 24 Mart 2016.

Klimburg, A., Tirmaa-Klaar, H. (2011). Directorate-General for External Policies, Policy Department. Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU. (1. Baskı). Belgium: European Parliament.

Kocasu, A. N. (2017). Toplu internet kullanımı sağlayıcıları yönetmeliği ne getiriyor? Erişim Tarihi: 16 Kasım 2019, https://mediacat.com/toplu-internet-kullanimi-saglayicilari-yonetmeligi-ne-getiriyor/

Kurnaz, İ. (2016). Siber Güvenlik ve İlintili Kavramsal Çerçeve. Cyberpolitic Journal. Sayı: 1&2, Yıl: 1, Cilt: 1. 62-83.

Magrassi, C. (2016). The Cyber Security Challenge: A Comparative Analysis. (1. Baskı). Italy: Luiss University Press.

Maurer, T., Morgus, R. (2014). Compilation of Existing Cybersecurity and Information Security Related Definitions.

Memleket. (2019). Uluslararası Siber Kalkan 2019 Tatbikatı Tamamlandı. Erişim Tarihi: 20 Aralık 2019, https://www.memleket.com.tr/uluslararasi-siber-kalkan-2019-tatbikati-tamamlandi-1962189h.htm

Meral, M. (2015). Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi. Yayınlanmamış Yüksek Lisans Tezi. İstanbul: T.C. Harp Akademileri Stratejik Araştırmalar Enstitüsü.

Min, Kyoung-Sik., Chai, Seung-Woan., Han, M. (2015). An International Comparative Study on Cyber Security Strategy. International Journal of Security and Its Applications. Sayı: 5, Yıl: 2015, Cilt: 9. 13-20

Mirzaoğlu, A. G., Ünver, M., Canbay, C. (2009). Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler. Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı Mayıs 2009.

National Cyber Security Strategy 2016-2021, HM Government. Erişim Tarihi: 10 Eylül 2019,

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

National Security Concept Of Estonia 2010. Erişim Tarihi: 21 Eylül 2019, https://vm.ee/en/national-security-concept-estonia-2010

National Security Strategy and Strategic Defence and Security Review 2015, A Secure and Prosperous United Kingdom. Erişim Tarihi: 9 Eylül 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/555046/52309_Cm_9161_NSS_SD.pdf

National Strategy for the Protection of Switzerland Against Cyber Risks 2012. Erişim Tarihi: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf

NATO and Cyber Defence. (2009). NATO Parliamentary Assembly, Sub-Committee On Future Security and Defence Capabilities, NATO document 173 DSCFC 09 E bis, 2009.

New Zealand's Cyber Security Strategy 2011. Erişim Tarihi: 21 Eylül 2019, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/nzcybersecuritystrategyjune2011_0.pdf

North Atlantic Treaty Organization. (2012). Active Engagement, Modern Defence. Erişim Tarihi 15 Ekim 2019, https://www.nato.int/cps/en/natohq/official_texts_68580.htm?

NTV. (2015). "Çin'den ABD'ye siber saldırılar sürüyor". Erişim Tarihi: 24 Aralık 2018, https://www.ntv.com.tr/teknoloji/cinden-abdye-siber-saldirilar-suruyor,0dr6sHGcdUK4aj1BBZCqnw?_ref=infinite

Öğün, M. N., Kaya, A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. Güvenlik Stratejileri Dergisi. Sayı: 18, Yıl: 9, Cilt: 9. 145-181.

Özalp, A. N., Asker, Ali. (2017). Devletin Güvenlik Politikalarında Siber İstihbaratın Rolü ve Önemi.

Özalp, Y. (2014). Siber İstihbarat ve Güvenlik Politikaları.

Öztaş, N., Yürük, E. (2017). E-Devlet Ana Kapıları Üzerine İnceleme: Türkiye ve Seçilmiş Ülkeler. Süleyman Demirel Üniversitesi İİBF Dergisi. Sayı: 15, Yıl: 2017, Cilt: 22. 2133-2157

Parlak, A. (2005). İnternet ve Türkiyede İnternetin Gelişimi. Bitirme Ödevi. Elazığ: T.C Fırat Üniversitesi Mühendislik Fakültesi Elektrik-Elektronik Bölümü.

Piret, P., Jesse, W., Alexander, Verschoor-Kirss. (2016). National Cyber Security Organisation: United States. (1. Baskı). Tallinn: CCD COE publication.

Rakhmanova, U. (2018). Siber Uzayın Güvenlikleştirilmesi: ABD Örneği. Cyberpolitic Journal. Sayı: 5, Yıl: 2, Cilt: 3. 45-61.

Republic of Estonia Ministry of Economic Affairs and Communication. (2019). Cyber Security. Erişim Tarihi 21 Eylül 2019, https://www.mkm.ee/en/objectives-activities/information-society/cyber-security#cyber-crime1

Robinson, N., Gribbon, L,. Horvath, V,. Robertson, K. (2013). Cyber-Security Threat Characterisation A Rapid Comparative Analysis. (1. Baskı). United Kingdom: Rand Corporation.

Sabillon, R., Cavaller, V., Cano, J. (2016). National Cyber Security Strategies: Global Trends in Cyberspace. International Journal of Computer Science and Software Engineering. Sayı: 5, Yıl:2016, Cilt: 5. 67-81.

Sağıroğlu, Ş. (2018). Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık. Sağıroğlu, Ş ve Alkan, M (Ed.). Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler (19-45). Ankara: Grafiker Yayınları.

Samet, R., Aslan, Ö. (2018). Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık. Sağıroğlu, Ş ve Alkan, M (Ed.). Kötü Amaçlı Yazılımlar ve Analizi (223-255). Ankara: Grafiker Yayınları.

Sanalp, S. (2016). Çeşitli Ülkelerde USOM ve SOME Yapılandırılması ve Türkiye Modeli Önerisi. Yayınlanmamış Yüksek Lisans Tezi. İstanbul: İstanbul Bilgi Üniversitesi. Sosyal Bilimler Enstitüsü.

Sarı, O. Uluslararası Hukuk ve Türk Ceza Hukuku Bağlamında Siber Güvenlik ve Bilişim Sistemine Yönelik Suçlar. Yayınlanmamış Yüksek Lisans Tezi. İstanbul: T.C. Harp Akademileri Stratejik Araştırmalar Enstitüsü.

Sarker, K., Rahman, H., Rahman, K. F., Arman, S., Biswas, S., Bhuiyan, T. (2019). A Comparative Analysis of The Cyber Security Strategy of Bangladesh. International Journal on Cybernetics & Informatics (IJCI). Sayı: 2, Yıl: 2019, Cilt: 8. 1-21.

Seren, M. (2016). Siber Tehditlerle Mücadelede Farkındalık ve Hazırlık. SETA Siyaset, Ekonomi ve Toplum Araştırmaları Vakfı Dergisi. Sayı: 183, Yıl: 2016, Cilt: 193.

Sınav, A. (2014). Siber Suçlar ve Kurum Güvenliği. Yayınlanmamış Denizcilik Uzmanlık Tezi. Ankara: T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı

Siber Kalkan Tatbikatı 2012 Sonuç Raporu. (2012). Bilgi Teknolojileri ve İletişim Kurumu. Ankara. Erişim Tarihi: 21 Kasım 2019,

https://docplayer.biz.tr/19348923-Siber-kalkan-tatbikati-2012-sonuc-raporu-www-siberkalkan-gov-tr.html

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

Siber Suçlarla Mücadele Daire Başkanlığı. (2019). Erişim Tarihi: 19 Kasım 2019, https://www.egm.gov.tr/siber/hakkimizda2

SiberBulten. (2017). Kritik Rapor: Türkiye'nin Jeopolitik Durumu Siber Casusları Cezbediyor. Erişim Tarihi: 13 Kasım 2019, https://siberbulten.com/sektorel/trky/kritik-rapor-turkiyeninjeopolitik-durumu-siber-casuslari-cezbediyor/

Siberkuvvet. (2015). Siber Saldırılar ve Siber Terör. Erişim Tarihi: 23 Aralık 2018, https://siberkuvvet.com/kutuphane/oku/siber-saldirilar-ve-siber-teror

Sonhaberler. (2017). Ulusal Siber Savunma 2017 Tatbikatı. Erişim Tarihi: 10 Aralık 2019, https://www.sonhaberler.com/ekonomi/ulusal-siber-savunma-2017-tatbikati-h522991.html

Spinello, R. A. (2002). Regulating Cyberspace. (1. Baskı). London: Quorum Books.

Statista. (2019). Number of İnternet Users in Turkey From 2013 To 2019 (in Millions). Erişim Tarihi: 9 Kasım 2019, https://www.statista.com/statistics/369725/internet-users-turkey/

Štitilis, D., Pakutinskas, P., Laurinaitis, M., Castel, I. Malinauskaitė-van de. (2017). A Model For The National Cyber Security Strategy. The Lithuanian Case. Journal of Security and Sustainability Issues. Sayı: 3, Yıl: 2017, Cilt: 6 .357-372.

STM. 2016 Temmuz-Eylül Dönemi Siber Tehdit Durum Raporu. Mühendislik Teknoloji Danışmanlık. Erişim Tarihi: 16 Kasım 2019, https://www.stm.com.tr/tr/haberler/duyurular/siber-tehdit-durum-raporu-temmuz-eylul-2016-yayinlandi

Şenol, M. (2018). Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık. Sağıroğlu, Ş ve Alkan, M (Ed.). Hibrit Savaş Kapsamında Siber Savaş ve Siber Caydırıcılık (179-221). Ankara: Grafiker Yayınları.

T.C. Sağlık Bakanlığı. (2018). Elektronik Belge Yönetim Sistemi. Erişim Tarihi: 14 Kasım 2019, https://ebysportal.saglik.gov.tr/TR,1762/elektronik-imza-nedir.html

TBMM BİAK (Bilişim ve İnternet Araştırma Komisyonu) Raporu. (2012). Bilgi Toplumu Olma Yolunda Bilişim Sektöründeki Gelişmeler ile İnternet Kullanımının Başta Çocuklar, Gençler ve Aile Yapısı Üzerinde Olmak

Üzere Sosyal Etkilerinin Araştırılması Amacıyla Kurulan Meclis Araştırması Komisyonu Raporu.

The Comprehensive National Cybersecurity Initiative, The White House. Erişim tarihi 5 Eylül 2019, https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative

TIMETURK. (2017). "Ulusal Siber Güvenlik Tatbikatı" Gerçekleştirildi. Erişim Tarihi: 10 Aralık 2019, https://www.timeturk.com/ulusal-siber-guvenlik-tatbikati-gerceklestirildi/haber-790302

Tikk, E., Talihärm, Anna-Maria. (2010). International Cyber Security, Legal & Policy Proceedings 2010. (1. Baskı). Talin: CCD COE Publications.

TMMOB EMO (Türk Mühendis ve Mimar Odaları Birliği Elektrik Mühendisleri Odası). (2010). Siber Savaşın Tatbikatına Bile Hazır Değiliz. Erişim Tarihi: 20 Kasım 2019, http://www.emo.org.tr/genel/bizden_detay.php?kod=79264

TRTHABER. (2019). Uluslararası Siber Kalkan 2019 Tatbikatı Tamamlandı. Erişim Tarihi: 20 Aralık 2019, https://www.trthaber.com/haber/turkiye/uluslararasi-siber-kalkan-2019-tatbikati-tamamlandi-448154.html

Turhan, O. (2006). Bilgisayar Ağları ile İlgili Suçlar (Siber Suçlar). Yayınlanmamış Planlama Uzmanlığı Tezi. Ankara: T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği.

Turkey's National Cyber Security Strategy 2016-2019. Erişim Tarihi: 13 Aralık 2019, https://www.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf

Turkey's National Cyber Security Strategy and 2013-2014 Action Plan. Erişim Tarihi: 10 Aralık 2019, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/actionplan2013-2014.pdf

TÜBİTAK BİLGEM. (2011). Siber Güvenlik Tatbikatı. Erişim Tarihi: 20 Kasım 2019, https://bilgem.tubitak.gov.tr/en/node/198

Türkay, İ. (2018). "Digital in 2018" Raporunda Dünyada ve Türkiye'de Durum. Erişim Tarihi: 5 Kasım 2018, https://vergialgi.net/ekonomi-maliye/digital-in-2018-raporunda-dunyada-ve-turkiye-de-durum/

Türkay, Ş. (2013). Siber Savaş Hukuku ve Uygulanma Sorunsalı. İstanbul Üniversitesi Hukuk Fakültesi Mecmuası. Sayı: 1, Yıl:68, Cilt: 71. 1177-1228.

TÜRKSAT. (2019). Uluslararası Siber Kalkan 2019 Tatbikatı Yapıldı. Erişim Tarihi: 21 Aralık 2019, https://www.turksat.com.tr/tr/haberler/uluslararasi-siber-kalkan-2019-tatbikati-yapildi

Ulutaş, G. (2018). Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık. Sağıroğlu, Ş ve Alkan, M (Ed.). Siber Güvenlik (85-101). Ankara: Grafiker Yayınları.

Ünal, S. (2015). Siber Uzamın Güvenlikleştirilmesi Söylemi: Türkiye, ABD ve Avrupa Birliği Örnekleri. Yayınlanmamış Doktora Tezi. Ankara: Ankara Üniversitesi. Sosyal Bilimler Enstitüsü.

Ünver, G. N. (2018). Siber Çatışmaların Tanımlama Sorunu. Cyberpolitic Journal. Sayı: 5, Yıl: 2, Cilt: 3. 23-44.

Wikipedia. (2018). Fikir ve Sanat Eserleri Kanunu. Erişim Tarihi: 11 Şubat 2019, https://tr.wikipedia.org/wiki/Fikir_ve_Sanat_Eserleri_Kanunu

Xin, Y. (2011). PLA Establishes 'Online Blue Army' to Protect Network Security. Erişim Tarihi: 7 Kasım 2019 http://en.people.cn/90001/90776/90786/7392182.html

Yalman, Y. (2018). Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık. Sağıroğlu, Ş ve Alkan, M (Ed.). Siber Terör, Terörizm ve Mücadele (257-280). Ankara: Grafiker Yayınları.

Yaşar, H., Çakır, H. (2015). Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri. Düzce Üniversitesi Bilim ve Teknoloji Dergisi. Sayı: 2, Yıl: 2015, Cilt: 3. 488-507.

Yayla, M. (2013). Hukuki Bir Terim Olarak "Siber Savaş". Türkiye Barolar Birliği Dergisi. Sayı: 104, Yıl: 25, Cilt: 104. 177-202.

Yenigaste. (2017). "Ulusal Siber Güvenlik Tatbikatı" Gerçekleştirildi. Erişim Tarihi: 11 Aralık 2019, https://www.yenigaste.com/bilimteknoloji/ulusal-siber-guvenlik-tatbikati-gerceklestirildi-h2101.html

Yeşilbaş, M. (2011). Türkiye'de Elektronik Devletin İnşa Süreci ve Mevzuattaki Görünümü. Dicle Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi. Sayı: 2, Yıl: 1, Cilt: 1. 1-23.

Yıldırım, E. Y. (2018). Bilişim Sistemlerine Yönelik Siber Saldırılar ve Siber Güvenliğin Sağlanması. Mesleki Bilimler Dergisi. Sayı: 2, Yıl: 7, Cilt: 7. 24-33.

Yılmaz, O. (2017). Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik. Cyberpolitic Journal. Sayı: 4, Yıl: 1, Cilt: 2. 22-43.

Yılmaz, S., Sağıroğlu, Ş. (2013). Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi. 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiri Kitabı. Sayı: 6, Yıl: 2013, Cilt: 6. 323-331.

5846 Fikir ve Sanat Eserleri Kanunu. (1951). T.C. Resmî Gazete, 7981, 5 Aralık 1951.

5271 Sayılı Ceza Muhakemesi Kanunu (CMK) (Md. 134). (2004). T.C. Resmî Gazete, 22311, 17 Aralık 2004.