T.C.

TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

ULUSAL SİBER GÜVENLİK STRATEJİSİ OLUŞTURMA SÜREÇ ANALİZİ VE TÜRKİYE İLE AFGANİSTAN'IN ULUSAL SİBER GÜVENLİK STRATEJİSİNİN DEĞERLENDİRİLMESİ

SAYED OSMAN SAYEDI

YÜKSEK LİSANS TEZİ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

Tez Danışmanı: Dr. Öğr. Üyesi Fatma BÜYÜKSARAÇOĞLU SAKALLI

EDİRNE – 2020

SAYED OSMAN SAYEDİ'nin hazırladığı **"ULUSAL SİBER GÜVENLİK STRATEJİSİ OLUŞTURMA SÜREÇ ANALİZİ VE TÜRKİYE İLE AFGANİSTAN'IN ULUSAL SİBER GÜVENLİK STRATEJİSİNİN DEĞERLENDİRİLMESİ"** başlıklı bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından Bilgisayar Mühendisliği Anabilim Dalında bir **Yüksek Lisan tezi** olarak kabul edilmiştir.

Jüri Üyeleri (Ünvan, Ad, Soyad): İmza

1. Dr. Öğr. Üyesi Fatma BÜYÜKSARAÇOĞLU SAKALLI
2. Dr. Öğr. Üyesi Özlem AYDIN
3. Dr. Öğr. Üyesi Mehmet Ali Aksoy TÜYSÜZ

Tez savunma Tarihi: 02/09/2020

Bu tezin Yüksek Lisan tezi olarak gerekli şartları sağladığını onaylarım.

İmza

Tez Danışmanı**:** Dr. Öğr. Üyesi Fatma BÜYÜKSARAÇOĞLU SAKALLI

Trakya Üniversitesi Fen Bilimler Enstitüsü onayı

Doç. Dr. H. R. Ferhat KARABULUT
Fen Bilimler Enstitüsü Müdürü

T. Ü. FEN BİLİMLER ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI YÜKSEK LİSAN PROGRAMI

DOĞRULUK BEYANI

Trakya Üniversitesi Fen Bilimleri Enstitüsü, tez kurallarına uygun olarak hazırladığım bu tez çalışmasında, tüm verilerin bilimsel ve akademik kurallar çerçevesinde elde edildiğini, kullanılan verilerde tahrifat yapılmadığını, tezin akademik ve etik kurallara uygun olarak yazıldığını, kullanılan tüm literatür bilgilerinin bilimsel normlara uygun bir şekilde kaynak gösterilerek ilgili tezde yer aldığını ve bu tezin tamamı ya da herhangi bir bölümünün daha önceden Trakya Üniversitesi ya da farklı bir Üniversite tez çalışması olarak sunulmadığını beyan ederim.

30/09/2020

Sayed Osman Sayedi

İmza

Yüksek Lisans Tezi

Ulusal Siber Güvenlik Stratejisi Oluşturma Süreç Analizi ve Türkiye ile Afganistan'ın Ulusal Siber Güvenlik Stratejisinin Değerlendirilmesi

T.Ü. Fen Bilimler Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

ÖZET

Son yıllarda, yeni teknolojiler, e-hizmetler ve internet bağlantılı yaşam olanakları günlük hayatımızın bir parçası olmuştur. Dolayısıyla bu nitelikteki hizmetlere erişim kadar edinilen bilgilerin doğruluğu ve gizliliği de önem arz etmektedir.

Toplumun bilgi teknolojilerine olan bağımlılığı kişisel kullanım kadar ulusal çapta da bilginin güvenliği kavramını etkilemektedir. Teknolojik altyapılarda meydana gelebilecek bozulmalar kişisel, toplumsal ve ülke çıkarları konularını etkileyecek bir hal almıştır. Dolayısıyla; siber güvenlik kavramı kişisel güvenlik alanını aşarak toplumsal çaplı bir politika halini almıştır. Bu kapsamda ülkeler siber güvenlik stratejileri oluşturarak siber alanı korumaya yönelik girişimlerde bulunmaktadır.

Bu tez çalışmasında ulusal siber güvenlik stratejisi için yapılması gerekenlerin planlanması ve Türkiye ile Afganistan'ın ulusal siber güvenlik stratejilerinin değerlendirilmesi hedeflenmektedir. Siber güvenlik kavramları, ulusal siber güvenlik stratejilerinin planlanma aşamaları, bu konuda öncü ve kabul edilen ülkelerin çalışmaları ile Türkiye ve Afganistan'ın siber güvenlik stratejileri incelenecektir.

Tüm bu incelemeler ışığında mevcut durum analizi karşılaştırılmalı olarak ortaya konarak alternatif çözüm üretme yolunda adım atılması düşünülmektedir.

Yıl : 2020

Sayfa Sayısı : 142

Anahtar Kelimeler: Siber Güvenlik, Güvenlik Stratejileri, Bilgi Gizliliği, Siber Savunma, Ülke Güvenlik Kriterleri

Master Thesis

National Cyber Security Strategy Development Process Analysis And Assesment Of Turkey And Afghanistan's National Cyber Security Strategy

Trakya Unıversıty Instıtute of Natural Science

Department Of Computer Engineering

ABSTRACT

In recent years, new technologies, e-services and Internet connected living facilities have become a part of our daily lives. Therefore, the accuracy and confidentiality of the information as much as access to such services has gained importance.

The dependency of the society on information technologies affects the concept of information security at national level as well as on personal use. The distortions that may occur in technological infrastructures may affect the personal, social and country interests. In this context, countries are making efforts to protect cyber area by creating cyber security strategies.

In this thesis, the planning of national cyber security strategy in view of what needs to be done and the evaluation of national cyber security strategy of Turkey and Afghanistan is aimed. Cyber security concepts, planning stages of national cyber security strategies, the studies of the countries considered as pioneers, and cyber security strategies of Turkey and Afghanistan will be examined.

In the light of these examinations, it is thought to take steps to produce alternative solutions by presenting the situation analysis comparatively.

Year : 2020

Number of Pages : 142

Keywords : Cyber Security, Security Strategies, Information Confidentiality, Cyber Defense, Country Security Criteria

TEŞEKKÜR

Başta ailem olmak üzere, çalışmalarımda emeği geçen tüm hocalarıma, meslektaşlarıma, arkadaşlarıma şükranlarımı sunarım. Çalışmalarım boyunca değerli katkılarını, yardımlarını akademik ve insanı açıdan hiç esirgemeyen değerli tez danışmanım Dr. Öğr. Üyesi Fatma BÜYÜKSARAÇOĞLU SAKALLI hocama teşekkürü bir borç bilirim. Ayrıca tez düzenleme aşamasında sağladığı katkı ve yardımlarından dolayı Enstitümüz Müdürü sayın Doç. Dr. H. R. Ferhat KARABULUT'a çok teşekkür ederim. Son olarak bugüne kadar bana hep yürekten inanan, her türlü maddi ve manevi yardım ve fedakârlığı sağlayan ve her zaman yanımda olan Anne Babama minnettarım.

İÇİNDEKİLER

KISALTMALAR DİZİNİ

ABD	: Amerika Birleşik Devletleri
AFCERT	: Afganistan Cyber Emergency Response Team (Afganistan Siber Acil Müdahale Ekibi)
ANDC	: Afghanistan National Data Center (Afganistan Ulusal Veri Merkezi)
ANDS	: Afghan National Development Strategy (Afgan Ulusal Gelişme Stratejisi)
ANSC	: Afghanistan National Security Council (Afganistan Ulusal Güvenlik Konseyi)
APO	: Afghan Post Organizations (Afgan Post Organizasyonları)
ARCA	: Afghanistan Root Certification Authority(Afganistan Temel Sertifika Yetkilisi)
Ar-Ge	: Araştırma ve Geliştirme
ATRA	: Afghan Telecommunications Regulatory Authority Afgan (Telekomünikasyon Düzenleme Kurumu)
BGD	: Bilgi Güvenliği Derneği
BİT	: Bilgi ve İletişim Teknolojileri
CA	: Certification Authority (Özel Sertifika Yetkilisi)
CASA	: Central Asia-South Asia - CASA-1000Orta (Asya-Güney Asya enerji projesi)
CCD-COE	: Cooperative Cyber Defense Center of Excellence (Kooperatif Siber Savunma Mükemmeliyet Merkezi)
CDN	: Centralize Data Network (Merkezi Veri Ağı)
CERT	: Cyber Emergency Response Team (Siber Acil Müdahale Ekibi)
CERT/CC	: Computer Emergency Readiness Team Coordination Center (Bilgisayar Acil Durum Hazır Ekibi Koordinasyon Merkezi)
CIA	: Cetral Intelligence Agency (Merkezi İstihbarat Ajansı)
CII	: Critical Information Infrastructures (Kritik Bilgi Altyapıları)

CIO	: Chief Information Officer (Bilişim Kurulu Başkanı)
CNCI	: Comprehensive National Cybersecurity Initiative (Kapsamlı Ulusal Siber Güvenlik Girişimi)
CSO	: Chief Security Officer (Güvenlik Şefi)
CSRIR	: Cyber Security Regulations and Incentives Review (Siber Güvenlik Düzenlemesi ve Teşvikler İnceleme)
CSSUKS/SRCS	: Cyber Security Strategy Of The United Kingdom Safety, Security And Resilience İn Cyber Space (Siber Güvenlik Stratejisi Birleşik Krallık Güvenlik, Güvenlik ve Siber Alanda Dayanıklılık)
C4I	: Command, Control, Commonications, Computers, Intelligence (Komuta, Kontrol, Haberleşme, Bilgisayar ve İstihbarat)
DDOS	: Distributed Denial of Service (Dağıtılmış Hizmet Reddi)
DHS	: Department of Homeland (İç Güvenlik Bakanlığı)
DL	: Savunma Ligi (DefenceLeague)
DLP	: Data Loss Preventions Policies (Veri kaybı Önleme Politikaları)
DMZ	: Zemilitarized Zone (Arındırılmış Bölge)
DNC	: Democratic National Convention (Demokratik Ulusal Konvansiyonu)
DNS	: Domain Name Server (Alan Adı Sunucusu)
DOD	: Department of Defense (Savunma Departmanının)
DOS	: Denial Of Service (Servis Dışı Bırakma)
ENISA	: European Network and Information Security Agency (Avrupa Ağ ve Bilgi Güvenliği Ajansı)
ESET	: Enjoy Safer Technology (Daha Güvenli Teknoloji Keyfi)
FDE	: Full Disk Encryption (Tam disk şifrelemesi)
FSB	: Federal Security Service (Federal Güvenlik Servisi)
GCSA	: Global Cyber Security Agency (Küresel Siber Güvenlik Ajansı)
GRC	: Global Response Centre (Küresel Yanıt Merkezi)
GRU	: Main Intelligence Directorate (Ana İstihbarat Direktörlüğü)
GSM	: Global Systemfor Mobile Communications(Mobil iletişim küresel sistemi)
ICS/CERT	: Industrial Control Systems Cyber Emergency Response Team (Endüstriyel Kontrol Sistemleri Siber Acil Müdahale Ekibi)

IC/IRC	: Intelligence Community Incident Response Center (İstihbarat Topluluğu Olay Tepki Merkezi)
ICT	: Information and Communications Technology (Bilgi ve İletişim Teknolojisi)
ICTI	: Information And Communications Technology Institute (Bilgi ve İletişim Teknolojileri Enstitüsü)
IMEI	: International Mobile Equipment Identity (Uluslararası Mobil Cihaz Kimliği)
IMPACT	: International Multilateral Partnership Against Cyber Threats (Siber Tehditlere Karşı Uluslararası Çok Taraflı Ortaklık)
ISMS	: Information Security Management System (Bilgi Güvenliği Yönetim Sistemi)
INCB	: Israel National Cyber Bureau (İsrail Ulusal Siber Bürosu)
IOS	: International Organization for Standardization (Uluslararası Standartlar Örgütü)
IP	: İnternet Protokol
IP IPv4	: Internet Protocol version4 (Internet Protokolü Sürüm4)
IPv6	: Internet Protocol version6 (Internet Protokolü Sürüm6)
IROA	: Islamic Republic Of Afghanistan (Afganistan İslam Cumhuriyeti)
ISDRF	: Information Security Doctrine of the Russian Federation (Rusya Federasyonu Bilgi Güvenliği Doktrini)
ISP	: Internet Service Provider (İnternet Servis Sağlayıcıları)
ISSD	: Information Systems Security Directorate (Bilgi Sistemleri Güvenlik Müdürlüğü)
IŞİD	: Irak ve Şam İslam Devletleri
IT	: Information Technology (Bilgi Teknolojisi)
ITRC	: Information Technology Research Center (Bilgi Teknolojileri Araştırma Merkezi)
ITU	: International Telecommunication Union (Uluslararası Telekomünikasyon Birliği)
JPG	: Joint Photographic Experts Group (Birleşmiş Fotoğraf Uzmanları Grubu)

JTFGN	: Joint Task Force Global Network (Birleşik İş Gücü Evrensel Ağı)
LAN	: Local Area Network (Yerel Ağ Bağlantısı)
MAC	: Media Access Control (Medya Erişim Denetimi)
MCIT	: Ministry of Communications and Information Technology (İletişim ve Bilgi Teknolojileri Bakanlığı)
MoHE	: Ministry of Higher Education (Yüksek Öğretim Bakanlığı)
MoJ	: Ministry of Justice (Adalet Bakanlığı)
MPS	: Ministry of Public Security (Kamu Güvenliği Bakanlığı)
MR	: Manyetik Rezonans Görüntüleme
NATO	: North Atlantic Treaty Organization(Kuzey Atlantik Antlaşması Örgütü)
NCRCG	: National Cyber Response Coordination Group (Ulusal Siber Tepki Koordinasyon Grubu)
NCSA	: National Cybersecurity Strategy of Afghanistan (Afganistan Ulusal Siber Güvenlik Stratejisi)
NCSC	: National Cyber Security Center (Ulusal Siber Güvenlik Merkezi)
NCSD	: National Cyber Security Division (Ulusal Siber Güvenlik Birimi)
NHS	: National Health System (Ulusal Sağlık Sistemi)
NOC	: Network Operation Center (Ağ Operasyon Merkezi)
NSA	: National Security Agency (Ulusal Güvenlik Ajansı)
NSA/NTOC	: National Security Agency/Threat Operations Center (Ulusal Güvenlik Kuruluşu Tehdit Operasyonları Merkezi)
NSCRF	: National Security Conceptof Russian Federation (Rusya Federasyonu Ulusal Güvenlik Konsepti)
OS	: Operating System (İşletim Sistemi)
OSI	: Open Systems Interconnection (Açık Sistem Ara bağlantısı)
PLA	: Peoples Liberation Army (Halk Kurtuluş Ordusu)
PLC	: Programmable Logic Controller (Programlanabilir Mantıksal Denetleyici)
RPC	: Remote Procedure Call (Uzaktan Yordam Çağrısı)
RSK	: Rus Silahlı Kuvvetleri

SDLC	: Software Development Life Cycle (Yazılım Geliştirme Yaşam Döngüsü)
SCADA	: Supervisory Control and Data Acquisition (Veri Tabanlı Kontrol ve Gözetleme Sistemi)
SCNPC	: Standing Committee of the National People's Congress (Kongresi Daimi Komitesi)
SIEM	: Security Information and Event Management (Güvenlik Bilgileri ve Etkinlik Yönetimi)
SIM	: Subscriber Identity Module (Abone Kimlik Modülü)
SOME	: Siber Olaylara Müdahale Ekibi
SP	: Solution Provider (Çözüm Sağlayıcıları)
SQL	: Structured Query Language (Yapılandırılmış Sorgu Dili)
SVR	: Foreign Intelligence Service (Dış İstihbarat Servisi)
TAO	: Tailored Access Operations (Özel Erişim İşlemleri)
TAPI	: Türkmenistan-Afganistan-Pakistan-Hindistan
TBD	: Türkiye Bilişim Derneği
TCP/IP	: Transmission Control Protocol/Internet Protocol (İletim Denetimi Protokolü/Internet Protokolü)
TUTAP	: Turkmenistan-Uzbekistan-Tajikistan-Afghanistan-Pakistan
UDHB	: Ulaştırma Denizcilik ve Haberleşme Bakanlığı
UK/CERT	: United Kingdom National Computer Emergency Response Team (İngiltere Ulusal Bilgisayar Acil Müdahale Ekibi)
UNCITRAL	: Unıted Natıons Commıssıon on Internatıonal Trade Law (Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu)
US/CERT	: United States Compute Emergency Readiness Team (ABD Siber Acil Müdahale Ekibi)
USB	: Universal Serial Bus (Evrensel Seri Veriyolu)
USOM	: Ulusal Siber Olaylara Müdahale Merkezi
VAS	: Value Added Services (Katma Değer Hizmetleri)
WAN	: Wide Area Network (Geniş Alan Ağı)
Wi-Fi	: Wireless Fidelity (Kablosuz Bağlantı Alanı)
WWW	: World Wide Web (Dünya Çapında Ağ)

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

BÖLÜM 1

GİRİŞ

Gün geçtikçe gelişen ve insan hayatının her noktasını etkileyen teknoloji, sunduğu imkânlar, sağladığı kolaylıklar ve yararları ile birlikte bazı risk ve siber saldırılarla karşılaşma olasılığı da oldukça artırmaktadır. Bilgisayar ve ağlardaki zafiyetlilerden faydalanarak sistemlerin faaliyetlerini durdurmak, bilgiler ve veriler üzerinde değişiklik yapmak, bilgilerin çalınmasına, silinmesine sebep olmak ve hatta maddi çıkar elde etmek amacıyla yapılan siber saldırılar günbegün çoğalmaktadır (Ercan, 2015).

Bilgi ve İletişim Teknolojilerinde (BİT) her geçen gün sayısı artan uygulamaların insan hayatında önemli roller oynaması, internetin yer ve zaman gibi engelleri aşarak anı haberleşme ve veri alışverişinin yapıldığı bir dünyada siber güvenliğe ihtiyaç duyulmuştur. Siber saldırganlar genellikle kurum ve şirketleri hedef almaktadır, bu saldırılar ve saldırı riskleri gittikçe artarak devam etmekte ve daha karmaşık bir hal almaktadır. Buna rağmen maalesef siber güvenlik kavramının kurumlar ve şirketler tarafından yeteri kadar ve tam olarak anlaşılamadığı gözlemlenmektedir. Siber saldırılara uğrayan kurum ve kuruluşlar bir yandan maddi zarara görürken diğer yandan ciddi şekilde müşteri ve itibar kaybı yaşamaktadırlar (Yaşar & Çakır, 2015).

İnternetin süratle gelişmesi, askeri, siyasi ve ticari alanlarında yaygın bir şekilde kullanılıyor olması, hükümetlerin milli ve milletler arası güvenlik bakımından siber güvenliğin ilk sırada yer vermesine sebep olmuştur. Bilgisayar ağlarında oluşan tehditler bireysel, kurumsal hatta küresel açıdan önemli neticelere sebep olmaktadır. Örneğin; İnternet bankacılığı kullanan bir kullanıcının banka hesabında işlenen bir siber suç olayı, yalnızca o şahısın maddi zarara uğramasına neden olmakta; fakat bir kurum veya şirket üzerinde gerçekleştirilen bir siber saldırı tüm personelin kimlik bilgilerinin

ele geçirilmesine neden olmaktadır. Bir ülkenin gizli verilerinin diğer ülkelerin bilmesi ya da ele geçirmesi, o ülkenin güçsüz yönlerinin ifşa olmasına bundan dolayı ülke itibarının zedelenmesine sebep olabilmektedir. Siber tehdit ve saldırıların artması, ülkeler için ulusal siber güvenlik önemlerini almak ve güvenlik stratejilerini uygulamak zorunlu hale gelmiştir (Ada & Çakır, 2017).

Tüm dünyada kurum ve şirketler daha iyi hizmet verebilmek için BİT sistemlerini gün geçtikçe daha çok kullanmaktadırlar, bunun yanı sıra, BİT sistemlerinin güvenliğinin sağlanması sadece kurum ve şirketlerin ulusal güvenliği için değil, aynı zamanda siber güç alanında önemli bir rol oynamaktadır. Kısacası toplumlar ve devletler BİT sistemlerine bağımlı duruma gelmektedir, buda siber saldırganlar için zemin hazırlamakladır. Bundan dolayı ülkeler kendi kritik altyapılarını ve bilgi sistemlerini harici ve dâhili tehditlere karşı kendi teknolojik imkânları ile güvenlik önlemleri almaktadır (Erkek, 2018).

Bu dinamiklerden yola çıkarak, siber güvenlik alanında gelişen yenilikler, değişen teknoloji, ticari olanakları ve toplumsal gelişimin destek olma yönden BİT sistemlerinin vazgeçilmez bir parçası olarak yerini almaktadır. Siber dünya gelişerek BİT sistemleri toplum üzerinde etkili olamaya devam ettikçe siber saldırılar ve risklerle beraber siber güvenlik önlemleri de daha fazla alınmalıdır. Tehdit ve saldırıların önüne geçebilmek için devlet kurumları ve özel sektörler iş birliği yaparak gerekli altyapıları geliştirmeleri zaruridir; böylelikle siber güvenlik çözümleri gelişen tehdit ortamının üstesinden gelinebilir ve yeniliklere yol açılabilir. Gelişen tehditlere karşı gereken önlemlerin alınmasının ciddi bir yöntemi ise hükümet kuruluşlarının ve özel sektörlerin sonuca yönelik çözüm ve gelişme sürecine yönlenmesidir. Yani riske dayalı bir güvenlik sistemi kurulmalıdır (Siber Tehdit, 2016).

Bu tezin amacı, günümüzde kurum ve şirketlerin BİT sistemleri üzerinden verdikleri hizmetlerin bir ayrıcalık olmaktan ziyade bu BİT sistemlerinin kullanımları bir zorunluluk olan siber ortamda uğradıkları siber tehdit ve saldırılara karşı kurumsal siber güvenliklerini sağlayabilmelerine ve sistemlerini siber saldırılardan koruyabilmelerine yardımcı olmaktır. Bu amaç doğrultusunda siber güvenlik, siber güvenlikle ilgili tehditler ve bu tehditlerden korunmak için kurumsal çapta yapılabilecek çalışmalar ele alınarak yanıtlar aranmıştır. Bu tez çalışmasının hedefi siber güvenlik

kavramının açık ve net bir şekilde anlaşılması, siber güvenlikle ilgili tehditler konusunda farkındalık bilinci yaratmak veya bu bilincin artırılmasını sağlamak siber tehditlere yönelik etkili ve faydalı mücadele yeteneği kazandırmaktır(Yaşar & Çakır, 2015). Saldırgan kişi veya grupların saldırıları neticesinde toplumun üzerindeki tesirleri ve verdiği hasarlar araştırılacaktır. Günümüze kadar yaşanan bazı önemli siber olaylar ve bu olayların etkilerinden bahsedilecektir. Çalışmanın ilerleyen bölümlerinde dünyanın bazı üncü ülkelerinde ve Afganistan ile Türkiye'de siber tehditlere karşı geliştirilen siber güvenlik stratejileri incelenecektir.

Son zamanlarda ortaya çıkan siber saldırılar güvenlik konusunun ne kadar mühim bir konu olduğunu bir kere daha göstermiştir. Bundan dolayı siber güvenlik nedir sorusuna cevap bulmaya çalışanların sayısı da oldukça çoğalmaktadır. Bu tez çalışmasında bu sorulara yanıt/yanıtlar verilmeye çalışılmıştır. Bu tez çalışması genel olarak 6 bölümden oluşmaktadır. Bu çerçevede birinci bölüm giriş bölümü olarak belirleniş ve çalışma ile ilgili genel bilgiler verilmiştir. İkinci bölümde ise siber güvenlik, siber güvenlik ilkeleri, siber güvenlik kavramları, siber güvenlik olayları, siber saldırılar ve siber saldırı türleri geniş bir şekilde incelenmiştir.

Üçüncü bölümde siber savunma, siber savunma stratejisi, siber savunma unsurları, siber savunmanın koruma adımları ve özelikleri gibi önemli konulara değinilmiştir. Dördüncü bölümde ise ulusal siber güvenlik, ulusal siber güvenlik stratejilerinin hazırlanması, öncü ülkelerin (ABD, Rusya, Çin, İngiltere, Almanya, İsrail) siber güvenlik ile ilgili çalışmaları incelenmiş ve aynı bölüm içerisinde Türkiye'nin ulusal siber güvenlik stratejilerine kısaca yer verilmiştir.

Beşinci bölüm Afganistan ulusal siber güvenlik stratejileri için ayrılmıştır, bu başlık altında Afganistan'ın siber güvenlik açısından mevcut durumu, 2014-2015 ulusal siber güvenlik stratejisi, Ülkenin maruz kaldığı siber saldırılar, Afganistan'ın güncel siber prosedür ve politikaları ve siber güvenlik için alınması gereken önlemler ayrıntılı bir şekilde incelenmiştir. Son olarak altıncı bölüm ise bu tez çalışması için sonuç ve tartışma bölümüdür.

BÖLÜM 2

SİBER GÜVENLİK

Hiçbir zaman tam ve yüzde yüz bir güvenlik sistemi bulunmamaktadır, çok zayıf bir ihtimal olsa da güvenlik açıkları hep mevcuttur. Geçmişten günümüze yaşanan siber olaylar, siber güvenliğin ne kadar önemli bir konu olduğunu ve her geçen gün daha da önemli bir hal aldığını göstermektedir. Etkili bir siber güvenlik sistemi oluşturmak için, öncelikle siber olayları ve özellikle de siber tehditlerin farkında varmak ve siber güvenlik kavramının tanımını bilmek gerekmektedir (Sertçelik, 2015). Güvenlik kelimesinden önce Siber kelimesini bilmemize fayda vardır, Siber kelimesi dijital ağların tamamını içeren geniş bir terimdir. Bu ağların, mahremiyetinin korunması, bütünlük ve güvenliğinin sağlanması ise siber güvenliktir (Altun, 2017).

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na göre (2016)

> (…) Siber güvenlik, siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi olarak tanımlanıştır (s.8).

Siber güvenlik kavramını günümüzde sık sık duymaktayız. Siber güvenlik ve bilgi güvenliği kavramları birbiriyle karıştırılsa da siber güvenlik tüm bilişim sistemlerini kapsayan daha geniş kapsamlı bir kavramdır. Siber güvenliğin pek çok çalışma alanı bulunmaktadır. Bunlarından bazıları, yazılım güvenliği**,** web güvenliği**,** ağ güvenliği**,** donanım güvenliğidir (Kamis, 2017).

Siber güvenlik, bilgi güvenliği, bilgisayar sistemleri güvenliği gibi pek çok alanı içermektedir. Siber güvenlik herkes için başka bir anlam taşımaktadır. Örneğin; bireyler için güvende olmak, kişisel verileri ve gizliliği koruma altına almak anlamına gelirken kurumlar için iş hayatında önemli işlevlerin kullanılabilir olması ve gizli bilgilerin

saldırganların eline geçmesini engellemek demektir. Hükümetler açısından ise halkın, kuruluşların, kritik altyapının ve hükümetin bilgisayar sistemlerini siber tehditlere ya da bilgilerin etkisiz kişilerin eline geçmesine karşı korunması demektir. Siber güvenlik farklı şekillerde tanımlansa da bireylerin, kurumların ve devletlerin bilgi işlem amaçlarına güvenli bir biçimde ulaşmalarını sağlayan ortak faaliyetlerini ve etkinliklerini anlatmaktadır (Siber Tehdit, 2016).

Siber güvenliğin amacı, toplumun varlıklarının siber alanda güvenlik tehlikelerinin karşısında durabilecek biçimde korunmasını ve sürekliliğini sağlamaktır. Siber güvenliğin pek çok boyutu vardır ama asıl 7 ana ilkesi şekil 2.1'de gösterildiği gibidir (Ada & Çakır, 2017).

Şekil 2.1. Siber Güvenlik Prensipleri (Ada & Çakır, 2017).

2.1.1. Gizlilik

Gizlilik, bilginin yetkisiz kullanıcılar tarafından ele geçirilmesini önlemektir. Gizlilik, sadece kalıcı ortamlarda (disk, tape, vb.) değil aynı zamanda internet araçlığıyla iletilen gizli bilgiler içinde önem arz etmektedir. Buna ek olarak trafik analizinin, yani iki kullanıcı arasındaki iletişimin tespit edilmesine karşı alınan tedbirler de gizlilik hizmeti dâhilinde değerlendirmektedir (TurkHack Team, 2013).

2.1.2. Bütünlük

Veri bütünlüğü, veriyi bir kullanıcıdan gönderildiği gibi veriler üzerinde herhangi bir değişiklik yapılmadan bütünüyle diğer kullanıcıya iletilmesidir. Amaç veriyi bozulmadan, yeni veriler eklenmeden veya verilerin bazıları veya hepsi

silinmeden, tekrar edilmeden ve düzeni bozulmadan güvenli bir biçimde tutmak ve korumaktır (TurkHack Team, 2013).

2.1.3. Erişilebilirlik-Süreklilik

Erişilebilir prensibi bilgi veya veriye istenildiği zaman ulaşılabilir ve kullanılabilir olmasını sağlamaktadır. Süreklilik hizmetinin amacı, bilişim sistemlerini, dâhili ve harici her türlü tehditlere karşı korumaktır. Bu hizmet sayesinde, kullanıcılar, erişim yetkileri olan verilere, istedikleri zaman ve güvenli bir şekilde ulaşabilmektedirler. Sistem sürekliliği, sadece kötü niyetli bir saldırı sonucu zarar görmez. Aynı zamanda Bilgisayar yazılımlarının çökmesi gibi yazılım hataları sonucu veya donanım sorunları, sistemin yanlış, bilinçsiz ve eğitimsiz kişilerin kullanması, bazı doğal olumsuzluklar(ısı, nem, topraklama eksikliği, yıldırım düşmesi) gibi etkenler de sistem sürekliliğini bozabilmektedir (TurkHack Team, 2013).

2.1.4. İzlenebilirlik

Bu prensip sistemde gelişen olayları, daha sonra incelemek için kayıt edilmesini sağlamaktadır. Bir sistemde olabilecek tehditlere örnek olarak, kullanıcılar şifrelerini kullanarak sisteme girmesi, bir web sayfası üzerinden e-posta göndermek veya almak verilebilmektedir. Kaydedilen olaylar incelendikten sonra gerçekleştirilecek analiz neticesinde, herhangi bir saldırı türü görüntülenirse veya saldırı olasılığı yüksek bir tehdit görülürse yöneticilerini uyarmak için alarm mesajları kurulabilir (TurkHack Team, 2013).

2.1.5. Kimlik Doğrulaması

Ağ güvenliği bakımından kimlik doğrulaması; kullanıcının gerçekten iddia da bulunan kişiyle aynı olup olmadığından emin olmaktır. Aynı zamanda, bir yazılım sisteminden yaralanırken şifrelerin kullanılması da bir kimlik sınamasıdır. Günümüzde kimlik doğrulaması, bilgisayar ağ ve sistemlerinin yanı sıra, fiziki sistemlerde de oldukça mühim bir hizmettir. Akıllı kartlara veya biometrik teknolojilere yönelik doğrulama yöntemleri kullanılmaktadır (TurkHack Team, 2013).

2.1.6. Güvenilirlik

Sistemin öngörülen davranışıyla alınan sonuç arasındaki tutarlılığıdır. Diğer bir deyişle güvenilirlik, sistemin yapmasını beklediğimiz şeyi tam olarak ne eksik ne de fazla yapmış olması ve çalıştırılmak istendiği her defada da hiç değişiklik göstermeden aynen davranmasıdır (TurkHack Team, 2013).

2.1.7. İnkâr Edememe

Burada veriyi gönderen ile alan arasındaki iletişim mesajlaşmada çıkabilecek sorunları ne gönderici ne de alıcı inkâr edebilir. Yani iki kullanıcı arasında bir bilgi alışverişi gerçekleşmişse ne gönderen alana bir ileti ilettiğini ne de alan almış olduğu bu iletiyi inkâr edemez. Genellikle gerçekliği olan işlemlerde kullanılmakta ve kullanıcıların aralarında meydana gelebilecek sorunları minimum seviyeye indirmeyi amaçlamaktadır (TurkHack Team, 2013).

2.2. Siber Güvenlik Kavramları

Siber güvenlik kavramlarını açık ve net bir şekilde anlayabilmek için çalışmanın bu bölümünde, siber, siber ortam/uzay, siber saldırı, siber suç, siber terörizm, siber casusluk, siber savunma, gibi bazı siber güvenlik kavramlarına yer verilmiştir.

2.2.1. Siber

Siber kelimesi “Cybernetics” sözcüğünün ön ekidir. Siber kelimesinin ayni anda bu kelimenin kısaltması olarak da kullanıldığı görülmektedir. Türkçede siber kelimesinin yerinde “bilişim” kelimesi kullanılmaktadır (Ercan, 2015).

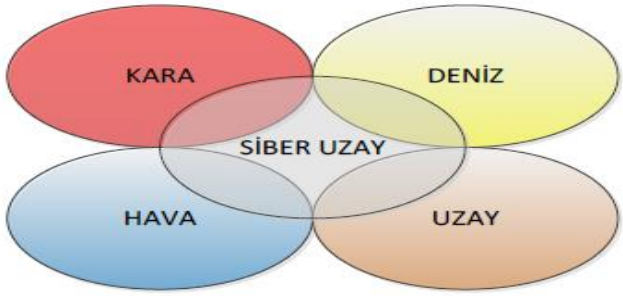
Türk Dil Kurumu ise bilişim kelimesini, “İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik” şeklinde tanımlamaktadır (TDK).

2.2.2. Siber Ortam/Uzay

Siber Uzay kelimesini ilk defa, bilimkurgu yazarı William Gibson 1980’li yılların başında kullanmıştır. Siber ortam, topluma yararlı pek çok hizmet vermektedir, kamu ve özel sektörler, daha iyi hizmet verebilmek için siber ortam kullanmaktadırlar.

Siber ortam sunduğu yararlı hizmetlerin yanı sıra bazı kötü amaçlar için de kullanılabilmektedir (Kara, 2013). T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı ise siber uzayı şöyle tanımlamaktadır. "Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortamdır" (T.C. UDHB, 2016).

5. boyut olarakta bilinen siber uzay, şekil 2.2'de gösterildiği gibi kara, hava, deniz ve uzaya bile bağımlı olmadan haberleşme altyapısın kullanan bir sanal ortamı ifade etmektedir.



Şekil 2.2. Siber Uzay Bileşenleri (Ada & Çakır, 2017).

2.2.3. Siber Uzayı Oluşturan Katmanlar

Siber alan ile ilgili yukarıda verilen tüm tanımlar eksik kalmaktadır. Fakat bu alanı oluşturan katmanları ele almak tanımların eksikliğini giderecek ve alanın özelliklerini açık ve net olarak anlamamıza yardımcı olacaktır.

a) Fiziksel Katman

Siber uzayın oluşmasını sağlayan etkinler gerçek ve fiziksel dünyadaki donanım ile insanlar ve varlıklardır. Siber uzayın durumu fiziksel dünya ile ne kadar etkileşim içinde olduğuna göre değişiklik göstermektedir. Bu katmanın temel faktörünün oluşturulması kullanılan teknoloji sayesindedir. Siber uzayın fiziksel varlığı sadece teknoloji üzerinde değil aynı zamanda ülkelerin altyapılarının çalışması için lazım gelen kritik altyapı ile ülkeler arasında bağlantıyı sağlayan internet omurgası da bu iletişimin sürekliliği için önemlidir (Bıçakcı, 2014).

b) Kodlar Katmanı

Siber uzayın mevcudiyetinin fiziksel durumdan sanal duruma yakınlaştıran katmanlardan birisidir. Fiziksel katmanın tüm temelleri (Anakartlar, işlemciler,

RAM'lar, diskler) kodlar sayesinde kullanılabilmektedir. "Doğru ya da Yanlış" veya "1 ya da 0" şeklinde oluşturulan programlama dilleri yardımıyla işlemcilerin nasıl işleneceği mümkün olmaktadır. İnternetteki içeriklere ulaşmamızı sağlamak içi işletim sistemlerinden sonra kodlar gelmektedir. Ayrıca internetin temelini oluşturan web siteleri de kodlar araçlığıyla hazırlanmaktadır (Bıçakcı, 2014).

c) İçerik Katmanı

Fiziksel ve kodlar katmanı esasında bir çerçeve katman oluşturmaktadır. Bu katmanlar yoksa içeriklerin internet üzerinden sunulması imkânsızdır. Ancak içerikler ve içerdikleri bilgi yoksa internetin oluşmasına sebep olan başka katmanlarda anlamsız olacaktır. Bu katman mesaj gönderen bir iletişim ortamı olmakla beraber, finansal işlemlerin verilerini muhafıza ettiği, ülkelerin stratejik bilgilerinin sakladığı bir ortamdır (Bıçakcı, 2014).

d) Düzenleyici Katman

Bu katman sözü geçen içeriklerin kullanılmasını düzelten hukuki yaptırımlardır. Bu katmanın büyük bir sorunu, teknoloji ve bununla beraber içeriklerin gün geçtikçe hızlı bir şekilde gelişmesinin aynı hızla devlet yöneticilerinin izleyememesidir. Siber ortamdaki riskler ve yelpazelerin yükselişi ister istemez devletin yapılarını da etkilemektedir (Bıçakcı, 2014).

Siber suçlarla mücadele eden ülkeler birbirleri ile iş birliği içinde olup siber suçlar hakkında geniş bir değerlendirme yaparak düzenleyici katmanı bu yönde oluşturmaya çalışmaktadırlar. Fakat sürekli olarak yenileri ortaya çıkan siber suçlardan dolayı bu mümkün değildir.

2.2.4. Siber Olay

"Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilgi ve verinin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya teşebbüste bulunulmasını ifade etmektedir" (T.C. UDHB, 2016).

Siber olay, BİT sistemlerinden faydalananların, bu sistemler yardımıyla kazandıkları fayda ve yararların negatif yönde etki gördüğü, doğal afetler, elektrik

kesintileri, fiber optik hatlarında ortaya çıkan bozukluklar ve bunlar gibi olaylar "siber olay" olarak görülebilir.

2.2.5. Siber Suç

Teknolojinin sağladığı kolaylıklardan yararlanan kötü niyetli kişiler siber ortamı suç işleme açısından yeni bir ortam olarak görmektedirler. Siber suç bilgisayar sistemi ve ağları araçlığıyla yapılabildiği gibi kredi kart, cep telefon, çevrimiçi bankacılık gibi sıkça kullanılan araçlar üzerinden de gerçekleşebilmektedir (Ercan, 2015).

Siber suçlar, bilgisayar ve bilgi sistemlerini temel amaç olarak kullanan suç işlemleridir. Siber saldırılar hakkında sayımlama yapan "hackmageddon" internet sitesi Nisan 2016'da yaptığı araştırmaya göre dünyada meydana gelen siber saldırıların %71,1'i siber suç olarak belirlenmiştir. Siber suçlar; genel suçları (dolandırmak, sahtecilik yapmak ve kimlik bilgilerini çalmak), içeriğe bağlı suçları (internet araçlığıyla çocuk istismarı, ırkçılıkla alakalı suçlar) ve bilgi sistemleri ile ilgili suçlar (sistem siber saldırıları, DOS saldırısı ve zararlı yazılımları) kapsamaktadır (Ada, 2018).

2.2.6. Siber Savaş

Siber savaş pek çok şekilde tanımlanmaktadır, en çok kullanılan tanımı, ise ABD eski başkanı Bush'un siber güvenlik danışmanı Richard A. Clarke "CyberWar" isimli kitabında yaptığı şu tanımlamadır.

Bir hükümetin, başka bir hükümetin bilgisayar sistemlerine veya ağlarına zarara vermek veya sistemleri kesintiye uğratmak için gerçekleştirdiği sızma faaliyetleridir (Clarkeand Knake, aktaran Ercan, 2015).

2010'da yayımlanan "Clatham House Report" göre siber savaş ve başka savaşlar arasındaki farklar şöyledir.

1. Siyasi ve stratejik hedeflere ulaşmak için silahlı çatışmaya gerek yoktur.

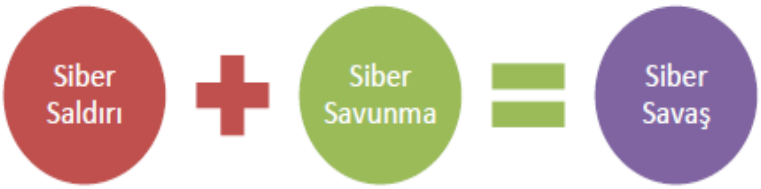
2. Değersiz ve küçük aktörlere sınırsız güç sağlamaktadır.

3. Gerçek olmayan IP'leri ve bilinmeyen sunucular gizli bir şekilde çalışarak belirsizlik gösterebilmektedir.

4. Silahlı savaşlardan fark ise siber ortam olarak bilinen 5. boyutta gerçekleşmektedir.

5. Normal savaş gibi baskı faktörlerden sebep meydana gelse de fiziki baskıları ve çatışmaları yoktur.

Siber savaşla siber saldırı farklı şeylerdir. Siber saldırılar şahısları, şirketleri, kurumlar hedeflerken siber savaş devletleri hedeflemektedir. Siber savaş, siber saldırıyla siber savunmayı kapsayan çok geniş bir kavramdır (Ada & Çakır, 2017).



Şekil 2.3. Siber Savaş Denklemi (Ada & Çakır, 2017).

2.2.7. Siber Terörizm

Siber terörizm, BİT sistemlerine hasar vermek, bu sistemlerin faaliyetlerini sekteye uğratmak gibi amaçlar için en tesirli araç olan internet tabanlı bilişim sistemleri vasıtasıyla bilerek ve kastan gerçekleştirilen teşebbüslerdir.(Stohl, aktaran Ercan, 2015). Siber terörizm, terör örgütlerinin epey ilgi duydukları bir alandır. Teröristleri siber saldırılara teşvik eden sebepler aşağıdaki gibi sıralayabiliriz (Altunok & Çakmak'tan aktaran Ercan, 2015).

- Mali kaynağı ve personel ihtiyacı daha azdır,
- Gerçekleştirilmesi silahlı terörist faaliyetlerinden daha basittir,
- Çok iyi bir eğitime veya ileri derece teknolojiye gerek yoktur,
- Tespit etmek zordur, özellikle kimlik tespiti oldukça güçtür,
- Olası amaçlarının sayısı ve türü çok fazladır,
- Mekân ve zaman gibi herhangi bir engel olmadığından, uzak mesafelerden saldırılar kolaylıkla yapılabilmektedir.

Siber terörizmin açık ve net bir tanımı olmasa da, değişen şartlar ve gelişen teknoloji çerçevesi içinde, konunun uzmanları siber saldırı çeşitlerini sınıflandırabilmek için bazı farklı farklı yaklaşımlarda bulunarak siber saldırıları iki sınıf altında değerlendirmişlerdir. Bunlardan birincisi genellikle kişisel eğlence ve kazanç için ya da yalnızca yapabilme kabiliyetlerini göstermek amaçlı gerçekleştirilen saldırı türleridir. İkincisi ise pek çok bilişim alt yapısını ya da sistemini hedefleyen planlı ve kasıtlı yapılan saldırılardır. Bu tür saldırılar iyice tasarlanmış, düzenlenmiş, organize edilmiş

ve ileri derece bir akılın ürün hususiyetlerini içermektedir (Krause & Tipton'dan aktaran Filiz, 2012).

Desouza ve Hensgen, siber terörizmi saldırılarını "geleneksel" ve "nadir" saldırılar şeklinde vasıflandırmaktadır. Bu şahıslar geleneksel saldırıları açık, nadir saldırıları ise kapalı ya da açık olmayan saldırı şeklinde adlandırmaktadır. Nadir saldırılar teröristlerin birbirleri ile haberleşmeyi sağlamak için elektronik çıkışlar değerlendirilmektedir. Örneğin; sanal dünyadaki birçok kişi için basit mesajlar bazı terörist gruplar için iletişim yöntemi olabilmektedir. Böyle durumlarda bilginin bilgi içinde saklandığı, stenografi gibi yöntemler kullanılmaktadır (Filiz, 2012). Siber suç, siber terör ve siber savaşın ana özellikleri çizelge 2.1'de verilmiştir.

Çizelge 2.1. Siber suç, siber terör ve siber savaşın ana özellikler (Ercan, 2015).

Eylemin	Siber Suç	Siber Terör	Siber Savaş
Niteliği	Doğrudan	Doğrudan, Sembolik	Doğrudan, Sembolik
Şiddeti	Az Yoğun	Yoğun	En Yoğun
Motivasyonu	Kişisel Kazanç	Siyasi	Siyasi, Doğrudan Savaş Kabiliyetini Azaltmak, Casusluk
Failleri	Bireyler, Organize Suç Örgütleri, Anonim	Terörist Örgütler, Hangi Örgüt Olduğu Tahmin Edilebilir.	Fail tam olarak bilinmese de hangi devletlerden kaynaklandığı bilinebilir.
Hedefleri	Kazanç Sağlanacak Hedefler	Kritik Tesisler, Güvenlik Birimleri, Hükümet Temsilcileri	Kritik Tesisler, Ekonomik ve Endüstriyel Altyapılar, Güvenlik Birimleri, Hükümet Temsilcilikleri, Askeri Altyapılar.
Kaynağı	Ülke içinden veya Dışından	Ülke içinden veya Dışından	Ülke Dışından

2.2.8. Siber Casusluk

Siber casusluk ile ilgili evrensel bir tanımlama olmamakla beraber bu konu hakkında öne çıkan bazı tanımlar şöyledir.

Siber casusluk, hasımın veya karşı tarafın önemli bilgilerini ele geçirmek ve düşmana karşı avantajlı olmak amacıyla bilgisayar ya da dijital haberleşme çalışmalarının kastan ve bilerek kullanılmasıdır (Ada, 2018). Diğer bir deyişle

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na göre (2016)

> (…) Ulusal güvenlik veya ticari istihbarat toplamak için e-mail trafiği, metin mesajları ile diğer elektronik haberleşmelerin ve kurumsal verinin gizlice veya sahte kimlikle ele geçirilmesi, Askeri, siyasi veya iş avantajı sağlamak için düşman ya da rakiplerin

sırlarını öğrenmek, hasımın sistem ya da ağlarında bulunan veya transferi yapılan bilginin elde edilmesi amacıyla yapılan her tür girişimdir.

Yukarıdaki tanımlardan yola çıkarak basitçe ifade etmek gerekirse bu girişimler;

- Devletlerarasında yapılmaktadır ancak devlet harici aktörleri de içermektedir.
- Bilgisayar araçlığıyla bilgi elde etmeye dayanmaktadır.
- Ölüm yaralama ya da imha gibi zarara yol açmamaktadır.
- Gizli bir şekilde uzun süreler boyunca yürütülmektedir.

Casusluğu tanımlamak ve casusluk sözcüğünün gerçek anlamıyla kullanmak arasında fark vardır. "Siber casusluk", "siber sömürü" ve "siber keşif" terimleri birbirleriyle karıştırılmaktadır. Oysa bu terimlerin farklı amaçları vardır ve farklı faaliyetlere sahiptir. "Keşif" hedef alınan sistem veya ağların zayıf yönlerini keşfetmektir. Diğer adımlar; "saldırı", yani hasımın ağında bulunan gerçek sızma, "zararlı yazılım" yani zararlı kodların gizlice sisteme eklenmesi ve "temizleme" yani saldırının izlerini, kanıtları silinmesidir. Sonuçta, siber keşif bütünü ile siber saldırının vazgeçilmez bir parçasıdır.

2.3. Siber Güvenlik Olayları

Güvenlik ihlallerini hiçe sayan siber saldırıların pek çok nedeni vardır. Siyasi istekler, verileri izinsiz ele geçirmek ve içeriğini değiştirmek, düşmanın verdiği hizmet kapasitesini sınırlamak ve zarara uğratmak, ekonomi açısından baskı altına almak, propaganda yapmak, hatta yapabildiklerini göstermek ve eğlenmek gibi nedenler bunlardan bazılarıdır. Saldırı eylemlerinin gerçekleşmesinde yararlanılan çok çeşitli yöntemlerin yanı sıra güvenlik açıkları ve çalışan zafiyetleri saldırganların işini kolaylaştırmaktadır (Aytekin, 2015).

Tezin bu bölümünde konunun önemini daha iyi anlamak için, dünya çapında gerçekleştirilen bazı siber güvenlik olayları incelenerek geniş bir şekilde sunulmuştur.

2.3.1. Estonya

Siber güvenlik olaylarından en çok konuşulan ve konunun önemini açık bir şekilde anlaşılmasını sağlayan örneklerden biri olan Estonya saldırısıdır. Estonya

saldırıları siber tehditlerin insan yaşamı üzerinde ne kadar etkili olabileceğini gösteren bir kargaşadan ziyade, gerçek manada bir kıyamet senaryosunu Estonya halkına yaşatmıştır. Dışarıdan bakınca her şey, Estonya hükümetinin Tallinn meydanında bulunan Bronz Asker heykelinin kaldırılmasıyla ortaya çıkmışsa bile saldırıların arka planını anlamak için öncelikle Estonya'nın demografik ve sosyal-kültürel durumunu bilmek gerekmektedir (Yener, 2015).

Avrupa ülkelerinin en kablolu ülkesi" olarak nam salan bu ülke 1991'de bağımsızlık unvanını aldığında vatandaşlarının sadece yarısı temel telefon hatlarına ulaşım sağlaya bilmekteydi. Fakat yeni hükümet bu yetersizliği bir şans olarak gördü telekomünikasyon ve bilgi teknolojileri alanlarında Ar-Ge faaliyetlerini teşvik ederek bu faaliyetler neticesinde ülkenin birçok yeniliğe adım atmasını sağladı. Örneğin; Skype uygulamasında kullanılan yazılım, Estonya kaynaklı bir yazılımdır. Dünyada ilk kez elektronik oy kullanma imkânını 2005'te Estonya halkına sunmuştur, bu dönme artık toplumun yüzde 60 civarında internete ihtiyaç duymaktaydı. Ülke bankacılık işlemlerinin yaklaşık yüzde 96'sını internet araçlığıyla gerçekleştirmekteydi. Ancak tüm bu kayda değer ilerlemelerin geliştiği bu dönemde devlet, internet güvenliği ve siber savunma ile ilgili lazım gelen çalışmaları yapmadığı için bilgi teknolojileri altyapısı zayıf görünmekteydi. Bu görüntü teknolojik altyapı açısından siber saldırı olasılıklarını artırmaktaydı, sonunda Estonya halkını Nazi işgalinden kurtaran Rus askerlerinin hatırası için 1947 yılında dikilen Kızıl Ordu Anıtı'nın kaldırılmasından hemen sonra 26 Nisan 2007 akşamında kaynağı bilinmeyen, oldukça etkili bir siber saldırı gerçekleşmiştir. Bu Saldırı ilk 24 saat fark edilememiştir. Hedefteki ilk kurban iktidarda olan Reform Partisi'nin web sitesi olmuştur. Kısa bir zaman içerisinde diğer siyasi partilerin, devlet sitelerinin ve Estonya Parlamentosu'nun web siteleri de saldırıya uğrayarak saldırılar sonucu sunucularını kapatmaya mecbur kalmışlardır (Yener, 2015).

Bu saldırılar bir hafta sonra genişleyerek ülkenin başta gelen medya şirketleri saldırganlar tarafından hedef alınmıştır. Tam da bu esnada saldırıda kullanılan bilgisayarların IP adreslerinin yurt dışı kaynaklı olduğu ortaya çıkmıştır. Yani bu saldırıların bir nabza da olsa önüne geçebilmek için tek çare yurtdışından gelen internet trafiğini durdurmaktı. Ancak bu durumda da medyalar, ülkelerinin uğradığı saldırıları dünyaya duyurmakta büyük zorluklarla çekeceklerdi (Yener, 2015).

Saldırıların üçüncü haftası, 9 Mayıs'ı 10 Mayıs'a bağlayan gece ülke siber saldırıların en şiddetlisine maruz kalmıştır. Saniyede 4 milyona yakın paket bilgiyi içeren saldırılar ülkenin bankacılık sistemine saldırarak ülkede en büyük banka olan Hansabank'ı hedef alınmıştır bu saldırılara banka sistemleri sunucularını kapatmak zorunda kalmıştır. İlk başta siyasi hedefleri olan saldırganlar daha sonra medya üzerinden vatandaşların bilgi edinme imkânlarını sınırlı duruma getirerek asıl darbeyi ise bankacılık sistemini, yani ekonomiyi hedefleyerek vurmuştur. Saldırıların planlı ve yoğun bir şekilde olmasına rağmen devletin yurtdışı kaynaklı internetin kesmesi kararı oldukça isabetli bir karar olmuş ve saldırıların şiddetinin uygun düzeyde kalmasını sağlamıştır. Bu saldırılardan dolayı hükümet Rusya'yı açık bir şekilde suçlarken Rus hükümeti olayla ilgilerinin olmadığını dile getirmiştir. Rus devleti bu siber saldırıları bir nebze yönlendirmiş olsa da saldırganların genellikle kendi kendilerine hareket ettikleri görülmektedir. Sonuç olarak bu siber saldırıların etkisi sadece Estonya ile sınırlı kalmayıp bu sınırı aşmıştır. Bugün henüz bu ülkenin uğradığı siber saldırılar konuşuluyor ve hemen her siber güvenlik toplantısında Estonya örnek olarak gösteriliyorsa bu bunun bir ispatıdır (Yener, 2015).

Olaylar sonucunda ülkeyi ziyaret eden Kuzey Atlantik Antlaşması Örgütü (North Atlantic Treaty Organization: NATO) uzmanları, Estonya'nın siber saldırılara yönelik geliştirdiği savunma mekanizmaları için oldukça önemli rol almıştır, bunun yanı sıra ülke siber güvenlik alanında önemli bir adım atmıştır. Saldırılara müteakiben 2008'de ülkede mükemmeliyet merkezi kurularak aynı yıllın Ağustos ayında Kooperatif Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defense Center of Excellence: CCD-COE) ismiyle çalışmaya başlamıştır (Yener, 2015). Bunlara ek olarak, Savunma Ligi (Defence League: DL) adıyla ülkenin siber savunma kabiliyetlerini geliştirmek için faaliyete başlamıştır. DL'ye bağlı olarak faaliyet gösteren Siber Güvenlik Birliği (Cyber Security Alliance: SCA) üç başlık altında görev yapmakla sorumludur.

Bu görevler;

Estonya halkının elektronik yaşamlarını korumak, BT uzmanları yetiştirmek ve Siber savunmayla ilgili vatandaşları bilinçlendirmek ve bilgilendirmektir (Yıldız, 2014). Çizelge 2.2. Estonya Siber Saldırısı Zaman Çizelgesini göstermektedir.

Çizelge 2.2. Estonya Siber Saldırısı Zaman Çizelgesi (Ada, 2017)

2.3.2. Stuxnet

İran'ın uranyum zenginleştirme programını durdurmak amacıyla 2006'da Amerika, askeri ve istihbarat kurumu gizli bir siber saldırı planı yapmıştır. Amerika ve İsrail istihbarat yetkililerinin beraber hazırladıkları bu zararlı yazılım 2010 yılında 100 bin civarı santrifüj hedef alınarak donanımları faaliyet gösteremez duruma gelmiştir bu sayı ise İran'da çalışmakta olan santrifüjlerin 1/5'ini oluşturmaktadır. Özellikle Veri Tabanlı Kontrol ve Gözetleme Sistemi (Supervisory Control And Data Acquisition: SCADA) endüstriyel sistemler gibi kritik altyapıları hedefleyen bu zararlı yazılımlar İran'ın nükleer çalışmalarını sekteye uğratmak ve kontrol altında almak için geliştirilmiştir (Yıldız, 2014).

Kasım 2010'da İran'ın üst düzey güvenlikle korunan nükleer silah tesislerine sızarak ülkenin uranyum zenginleştirme programına giriştiği darbe ile gerçek niyetini beli etmiştir. Bu tesislere sızmayı başaran zararlı yazılım ağır ve sağlam adımlarla ilerleyerek hasar vermeye başlamıştır. Stuxnet santrifüjlerin uranyum zenginleştirmede kullanılan programlanabilir Mantıksal Denetleyicisi (Programmable Logic Controller: PLC) kontrol devrelerini hedef seçerek bu devrelerin kontrolünü ele geçirmeyi amaçlamaktadır. Santrifüjler uranyum zenginleştirmede kullanılan ve çok hızlı bir şekilde dönen makinelerdir. Denetici yazılımı arızalanmaya başlayınca hızlı bir şekilde dönen makinelerin dönme hızı kontrol dışı hareket ederek makineler param parça olmaya başlamıştır. Sistem kontrolünü ele geçirip gizlice hasar veren virüsün dehşet veren yanı ise merkez bilgisayarlarına herhangi bir arıza göstermemesidir, böylece içten

içe verilen hasar uzun süre fark edilememiştir. Parçalanan makinelerin yerine yenilerinin getirilmesi ve zarar gören makinelerin virüslerden kurtarılması ve geri yüklenmesi, faaliyetlerin aksamasına epey yol açmıştır. Stuxnet virüsü, İran nükleer faaliyetlerini iki yıl sekteye uğrattığı görülmektedir. Bu virüs dünya üzerinde yaklaşık yüzde 60 İran'ı etkilemiştir, dolaysıyla bu zararlı yazılımın özellikle İran nükleer silahlarını durdurmak ve çökertmek için geliştirildiği ideasını artmıştır (Kara, 2013). Dünya genelinde Stuxnet'en etkilenen bilgisayar oranı çizelge 2.3'te verilmiştir.

Çizelge 2.3. Dünya Genelinde Stuxnet'ten Etkilenen Bilgisayarların Oranı

Ülke	Etkilenen Bilgisayar Oranı
İran	58.85%
Endonezya	18.22%
Hindistan	8.31%
Azerbaycan	2.57%
ABD	1.56%
Pakistan	1.28%
Diğer	9.2%

2.3.3. Duqu

Stuxnet ortaya çıktıktan bir yıl sonra yani Eylül 2011'de Dugu adılı yeni bir zararlı yazılım daha ortaya çıkmıştır. Duqu, ismini oluşturduğu dosyaların adlarına verilen "~DQ" ön ekinden almaktadır.

Duqu'nun, Stuxnet'e benzer bir çalışma şekli vardır, fakat zarara uğratmak yerine endüstriyel kontrol yöntemleri ile ilgili bilgi toplayarak aynısını yapabilmek için keşif çalışmaları yapmayı amaçlamaktadır. Lakin hedefleri bakımından ele alındığında Duqu Stuxnet'e göre oldukça kapsamlı tehditler içermektedir (Aytekin, 2015).

Stuxnet ve Duqu zararlı yazılımlarının benzerlikleri, endüstriyel kontrol sistemlerini hedef seçmeleri, geçerli sertifikalar kullanmaları ve ikisinin de İran'da görülmesidir. Bu 2 virüs arasında bazı benzerlikler olduğu gibi farklılıklarda vardır. Yıkıcı bir etkiye sahip olan Stuxnet, sistemlere zarar vermeyi amaçlamaktadır, Duqu ise, SCADA yöntemleri hakkında önemli bilgileri toplamak amaçlı oluşturulmuştur. Stuxnet saldırıları, sistemlere hasar vermek ve saldırının daha etkin çalışmasını

sağlamak için geliştirilmiştir. Duqu, gelecekle ilgili büyük tehlikelerin gelebileceğine işaret etmektedir (Kara, 2013).

2.3.4. Flame

Birer yıl aralıklı keşfedilen siber olaylara bir yenisi daha eklenmiştir. En büyük ve oldukça karmaşık zararlı yazılımı olarak meydana çıkan, kullanımı siber casusluk amaçlı olan ve hedefe yönelik saldırı yapmak için geliştirilen en karışık saldırı türüdür. Bu zararlı yazılım siber alanda bilgi toplarken senelerce tespit edilememiştir, uzun zaman tespit edilememesinin sebebi ise sürekli kendisini güncellemesidir. 2012'de tespit edilen bu zararlı yazılımın diğer zararlı yazılımlardan ayıran özeliği çok büyük ve modüler olmasıdır (Yıldız, 2014).

Flame Cry SyS Lab (Kriptoloji ve sistem güvenlik laboratuvarı) tarafından tespit edildiğinde en az 5 senedir faaliyet gösterdiği ve en az 5 çeşit şifreleme, 3 çeşit sıkıştırma, en az 5 çeşit dosyalama formatı ve özel kod enjeksiyon yöntemi kullanıldığını belirtmektedir. Bu zararlı yazılım bilgiyi izinsiz elde etmek ve üretmek için oldukça ileri derece işlevlere sahip olmanın yanı sıra, istedikleri bilgileri elde etmek için sızdığı bilgisayarın kapasitelerinin tamamını kapsamaktadır. Stuxnet ile karşılaştırıldığında Stuxnet'ten 20 kat daha karmaşık bir mimarisi olan Flame yapılan çalışmalar göre İran başta olmak üzere bazı Ortadoğu ülkeleri ile beraber 600 üzeri kurum ve kuruluşlar, akademik tesissiler, devlet yöntemleri ve 1000 üzerinde bilgisayar bu zararlı yazılımdan etkilenmiştir (Aytekin, 2015).

Rusya'nın meşhur anti virüs şirketi Kaspersky, Flame zararlı yazılımın bu güne kadar gelmiş geçmiş siber saldırıların tamamından oldukça etkili ve karışık ve aynı zamana üstün bir teknolojiyle geliştirildiğinin altını çizmektedir. Falme virüsü, internet üzerinden sistemler sızarak kullanıcılardan habersiz bir şekilde bilgisayarların ara birimlerini kullanabilmektedir. Uzaktan kontrol edilmesi mümkün olan bu zararlı yazılım, mikrofonu çalıştırarak ses kaydı yapabilmektedir. Elde ettiği bu bilgilerin tamamını tekrar internet araçlığıyla kaynağına iade etmekte ve ne miktarda bilgi elde ettiği bilinmemektedir (DeutscheWelle, 2012).

2.3.5. Conficker

Downup, Downadup ve Kido adı verilen Conficker, 2008 yılının Ekim ayında keşif edilmiş ve Microsoft Windows işletim sistemlerini hedef alan bir yazılım solucanıdır. Bu solucan Windows İşletim Sistemi kullanan kullanıcıların bilgisayarlarına bir arabellek taşması güvenlik zafiyeti üzerinde bulaşmaktadır. Conficker hedef aldığı bilgisayarlarda kod çalıştırma amaçlı özel olarak geliştirilmiş bir Uzaktan Yordam Çağrısı (Remote Procedure Call: RPC) isteği kullanarak şifre kırmakta, güvenlik açıklarından yararlanarak, spam ve zararlı kod yayabilmektedir. Bu virüs bilgisayar kullanılmaya başladığında, Windows Otomatik Güncelleştirmeler, Windows Güvenlik Merkezi, Windows Defender ve Windows Hata Raporlama gibi sistem servisler devre dışı kalmakta ve ilaveten başka bir zararlı yazılım yükleyip özel verilere kötü amaçlı şahısların erişmesi sağlanmaktadır (Vikipedi).

Bu virüsü temizlemek için kurulan uluslararası Conficker Çalışma Grubu, bu solucanın bulaştığı 600 binden fazla IP adresinin varlığını tahmin etmektedir. Sadece şirketler değil aynı zamanda pek çok kişisel kullanıcıyı da hedef alan bu virüs, bir web sunucusu gibi davranmaktadır. Birleşmiş Fotoğraf Uzmanları Grubu (Joint Photographic Experts Group: JPG) uzantılı olarak sistemlere sızan bu zararlı yazılım dünya çapında milyonlarca bilgisayara bulaşarak, bu güne kadar en çok bilgisayara bulaşan solucanlardan biri olarak bilinmektedir. Microsoft, bu virüsle savaşmak için 2009'da Conficker Mücadele ve Teknoloji Sanayi İşbirliği'ni kurarak bu solucanı geliştiren ya da geliştirenlerin bulunması için 250 bin dolar ödül koymuştur (Siberbülten, 2015).

Şekil 2.4. Confickr (Kobitek).

2.3.6. Sony

Dünya çapında ün kazanmış Sony Pictures'in The Interview isimli komedi filmi başrol oyuncularının Kuzey Kore lideri Kim JongUn'a suikast yapmak için görevlendirildiğini konu alan komedi filmi tam bir siber terör vakasına dönüşmüştür. Konusu suikast düzenlemek olan bu komedi filminden dolayı Sony ağır bir siber saldırı ile karşı karşıya kalmıştır, ilk önce Sony personellerinin ekranlarında kurukafalar görülmeye başlamış, sonraki günlerde Sony'nin iç ağları karışık bir saldırı sebebi bozguna uğramıştır. İlerleyen günlerde kendilerini Barışın Koruyucuları olarak adlandıran grup saldırının bu grup tarafından yapıldığını iddia etmiştir. Bu grup, 100 Terabayttan fazla gizli Sony verilerinin ele geçirildiğini ileri sürmüştür (Siberbülten, 2015).

Saldırıların arkasında Kuzey Kore'nin olduğu iddia edilerek suçlansa da Kuzey Kore temsilcisi bu suçlamayı ret etmiş fakat saldırıları destekleyerek saldırganları tebrik etmiştir. Bu saldırı sonucunda Sony Pictures'in bazı filmleri piyasaya çıkmadan internete paylaşılmış ve milyonlarca kez illegal bir şekilde indirilmiş ve izlenmiştir. Böylelikle Sony firması milyon dolarlık zarar görmüştür. 17 yöneticiyle beraber 6 binden fazla personelin maaşları tüm dünyaya yayınlanmıştır. Üst düzey yöneticilerin konuşmaları sızdırılmış, maddi zararların yanı sıra Sony'nin itibarı da zedelenmiştir. Durumun gittikçe kötüleşmesine rağmen filmin başrol oyuncuları Seth

Rogan ve James Franco saldırganlarla dalga geçmeye devam etmiştir (Siberbülten, 2015).

2.3.7. Bangladeş vurgunu

Mart 2016 yılında Bangladeş Merkez Bankasına karşı yapılan siber saldırının kaynağı belirsiz olsa da arkasında yine Kuzey Kore'nin olduğu öne sürülmüştür, saldırganlar söz konusu Banka'nın hesaplarına sızıp bankanın Amerika'da bulunan hesaplarından 81 milyon doları çalarak, Filipin banka hesaplarına aktarılmıştır, olay Amerikalı yetkililer tarafından fark edilerek, hırsızlığın büyümesi engellenmiştir. Tarihte en büyük siber hırsızlıklardan biri olarak yerini alan bu vurgun kim veya kimler tarafından gerçekleştirildiği netlik kazanamamıştır. RDeye isimli siber güvenlik şirketini kuran ve aynı zamanda yöneticiliğini yapan Dor, Sony saldırısında kullanılan yazılım, bu saldırıda da kullandığını ifade etmiştir. Dor, bankaya yapılan saldırının 2 yıllık bir planlamadan sonra yapıldığını da iddia etmiştir. İsrail'i bir yetkili ise bu saldırının ancak ulusal düzeyde verilebilecek bir destekle yapılabileceğini öne sürmüştür (Siberbülten, 2016).

Bankanın Başkanı Atiur Rahman, bu soygundan sonra istifa etmiştir. Siber soygunu bir "deprem" gibi gören Rahman, bankanın ülke içi ve ülke dışı istihbarat servislerini hızlı bir şekilde haberdar ettiğini ve uluslararası uzmanları durumu incelemek üzere ülkeye getirdiklerini belirtmiştir. Olayla alakalı keşif edilen ilk bilgilere göre, saldırganlar bankanın sunucularına sızarak ele geçirdikleri paranın 30 milyon dolarını Filipinlerdeki bir kumarhane sahibinin hesabına gönderilmiştir (Siberbülten, 2015).

2.3.8. Ulusal Güvenlik Ajansı Sızıntısı

Ağustos 2016 yılında Amerikan Ulusal Güvenlik Ajansı (National Security Agency: NSA) bir siber saldırı sızıntısına maruz kalmıştır. Ülkenin siber güvenlik uzmanlarının geliştirdiği ve casusluk eylemlerinde kullanılan siber materyaller internete sızılmıştır. NASA'n hack eylemlerinden sorumlu olan Özel Erişim İşlemleri (Tailored Access Operations: TAO) departmanında görev yapan ajan, bu materyallerin internet üzerinden satışa çıkarılmasıyla beraber büyük kurum kuruluşlar ve devletler için güvenlik açısından çok tehlikeli olduğunu dile getirmiştir (Siberbülten, 2015).

Sızıntıyı kim veya kimlerin gerçekleştirildiği sorusu henüz açıklık kazanmamışken bazı uzmanlar hükümetin desteklediği bilgisayar korsanlarından şüphe ederken, bazıları ise NSA çalışanlarının bilerek veya bilmeden yaptığı bir hata neticesinde bu olayın ortaya çıktığını iddia etmiştir. Bir yandan olay ile ilgili araştırmalar devam ederken diğer yandan Demokratik Ulusal Konvansiyonuna (Democratic National Convention: DNC) siber saldırı yaparak başkan Donald Trump hakkındaki bilgileri dünyaya yayan Rus hackerleri baş şüpheli olarak görülmüştür.

Eski bir TAO personellinin medyaya yaptığı açıklamaya göre, NSA personellerinden biri tarafından yapılan bir hata sonucunda bu bilgilerin internet üzerinden paylaşıldığı kuşkusunu öne sürmüştür. Bu açıklama aslında TAO çalışanlarının görev yaptıkları dijital ortamının yeterince güvenli olmadığının bir belirtisi olarak kabul edilebilmektedir. Sızıntı ile ilgili ortaya çıkan başka bir iddia ise, NSA çalışanlarından herhangi birinin bu bilgileri dışarıya aktardığı iddiasıdır.

Kendilerini Shadow Brokers olarak isimlendiren ve bu sızıntıyı üstlenen grup, ele geçirdikleri dosyaların bazılarını yayınlayarak açık artırmalı bir şekilde satışa koymuşlardır. Bu dosyalar 570 milyon dolara ulaştığı zaman verilerin geri kalan kısmını da dünyaya yayacaklarını söylemişlerdir. Fakat bu teklif siber silah tacirlerinin pek dikkatini çekmemiştir ve sadece 981 dolar teklif edilmiştir (Siberbülten, 2015).

2.3.9. Sabit Sürücülere Yerleştirilen Casus Yazılım

ABD Ulusal Güvenlik Ajansı'nın bazı firmalar tarafından üretilen sabit sürücülere bu cihazlar üzerinden gerçekleşen işlemleri izlenebilmesi için casus yazılım yerleştirildiği öne sürülmüştür. Western Digital, Seagate, Micron, Samsung ve Toshiba gibi şirketlerin sürücülerinde mevcut olan bu casus yazılımı ifşa eden güvenlik firması Kaspersky, 30 ülkede bazı bilgisayarların etkilendiğini, Stuxnet'e benzer bir casus yazılım olduğunu, 'Denklem Grubu' ismi verilen bir grup tarafında yürütüldüğünü ve 20 yıldan beri sürdürülen bir operasyon parçası olduğunu ifade etmiştir. Söz konusu firma aynı zamanda bu casus yazılımın bugüne kadar üretilen casusluk yazılımların içinde en karmaşık tekniklere sahip olduğuna, bilgi elde etmek ve kendini gizlemek açısından oldukça profesyonel olarak geliştirildiğine değinmiştir. Bu casus yazılım, sabit disklerin yazılımı yeniden yazabilme yeteneği olduğundan virüs taraması ve diskin biçimlendirilmesi gibi önlemlerden kurtulabilmektedir. Buna ek

olarak hem gözetleme/izleme yapıyor hem de internete bağlı olduğu sürece veri çalabilmektedir (Siberbülten, 2015).

Bu yazılımdan en çok etkilenen ülkelerin başında İran, Rusya, Pakistan, Afganistan, Çin, Mali, Suriye, Yemen ve Cezayir gelmektedir. Bu casus yazılımın, askeri ve kamu kurum ve kuruluşlarının yanı sıra bankaları, telekomünikasyon şirketlerini, enerjiyi, nükleer çalışmaları, medya şirketleri ve dini gruplara bağlı kurumları hedef aldığı ifade edilmiştir. Yazılımın sürücülere ne şekilde yerleştirildiği ile ilgili herhangi bir bilgi yokken yerleştirilmenin fiziksel olabileceği öne sürülerek, NSA'nın üreten kişilerden kaynak kodlarını talep etmiş olabileceği veya bu yazılım geliştiren firmalara sızmış olma ihtimali de iddia edilmiştir. Western Digital, Seagate ve Toshiba böyle bir olaydan haberdar olmadıklarını söylerken diğer şirketler herhangi bir açıklama yapmamıştır. NSA'nin bu çapta bir casusluk eyleminin arkasında olması ABD'ye olan güveninin zedelenmesine ve bilişim alalında Amerikan kökenli firmaların oldukça zor duruma bırakacağına yönelik güçlü ihtimaller bulunmaktadır (Siberbülten, 2015).

2.3.10. Wannacry

12 Mayıs 2017 yılında etkinliğini gösteren "Wannacry" fidye yazılım siber saldırısı dünya çapında bir problemin yeniden gündeme getirmiştir. Siber saldırıların anı gelişen sarsıntıları, görünmedik boyutlarıyla nasıl global bir soruna dönüştüğünü tüm dünyaya göstermiştir. Çin, Hindistan ve Rusya başta olmakla beraber; ABD'den İngiltere'ye kritik altyapıları da etkileyen geniş çaplı bu saldırı birçok ülkeyi sarsmıştır. Böyle geniş ve güçlü saldırılar uzun bir zamana kadar aktif kalarak etkisini oldukça fazla bir şekilde genişletebilen saldırılar sağlık ve güvenlik sistemlerine içten içe zarar verebilmektedir, bu tür kritik altyapıların bağlı olduğu siber alan her seviyede ülkeler için tehlike sinyallerini benzer saldırılarla gözlemlenmiştir (Güntay, 2017).

Kaynağı neresi veya kim olduğu bilinmeyen bu fidye yazılımı, önce verileri şifreler, sonra bu verilerin şifresini çözmek için 300 ila 600 dolar gibi fidye istemektedir. WannaCry, çoğunlukla spam e-postalarla ek olarak gelen virüslü dosyalardan bulaşmaktadır. Fakat başka fidye yazılımlarından farkı ise, bir Windows güvenlik sisteminin zayıf noktasını bularak ağdaki tüm makinelere yayılabilmesidir. Yukarıda değinildiği gibi bu saldırıdan etkilenen ülkelerden başta gelenlerinden birisi

Rusya'dır. Ülkede bankalar, İçişleri ve Sağlık Bakanlığı ile hükümetin demiryolları gibi kamu kurumları etkilenmiştir. Saldırı sayısına göre Rusya'dan sonra Tayvan ve Ukrayna gelmektedir. Sırasıyla saldırıdan en çok zararı İngiltere görmüştür. Ülkenin Ulusal Sağlık Sistemi (National Health System: NHS) çökmüş bunun yanı sıra bazı otomotiv şirketleri üretimlerine ara vermek zorunda kalmıştır (Siberbülten, 2017).

Türkiye, diğer ülkelere nazaran daha az etkilenerek bu saldırıdan nasibini almıştır. Saldırının yapıldığı ilk 2 saat Türkiye en çok etkilenen 3. ülke olmuştur. 12 Mayısta 8. sıraya gerilen Türkiye, hafta başında ise 14. sırada yerini almıştır. ESET (Enjoy Safer Technology) Türkiye Genel Müdür Yardımcı Alev Akkoyunlu'nun açıklamasına göre, Türkiye'nin en çok hedeflenen ülkeler içerisinde olmasının nedeni, güncellenmemiş yazılımların yaygın olarak kullanılmasıdır.

> ESET (Enjoy Safer Technology) Türkiye Genel Müdür Yardımcı Alev Akkoyunlu'na göre (2017),
>
> (…) Maalesef hem kurumsal hem de bireysel olarak, güncel olmayan işletim sistemi ve güvenlik yazılımı kullanımı çok yaygındır. Aynı zamanda korsan yazılım kullanımı da çok fazladır. Durum böyleyken, Türkiye her çeşit saldırıdan fazlaca etkilenmektedir. Bu tür siber saldırı olaylarında, korunmasız bilgisayarlar, bir botnetin parçası olarak birer saldırı aracına dönüşmektedir. Korunmasız bireysel bilgisayarlardan botnet oluşturularak, küresel düzeyde kurumsal sistemler hedef alınmıştır.

ESET Türkiye Genel Müdür Yardımcısı Alev Akkoyunlu **"**Ne yapmalı sorusuna ise "En son Windows işletim sistemleri güncellenmeli ve yamaları yapılmış olmalıdır" diyerek, aşağıdaki uyarılarda bulunmuştur.

- Kesinlikle yeni ve aktif bir güvenlik yazılımı kullanılmalı.
- Tanımadığımız şahıslardan gelen e-postalardaki ekler açılmamalı.
- İşlerinden dolayı devamlı çeşitli yerlerden e-posta gelen çalışma arkadaşlarınızı uyarınız, mesela muhasebe bölümleri veya insan kaynakları bölümleri.
- Veriler düzenli bir şekilde yedeklenmeli. Bu, risk ihtimali haline; verileri geri yükleyebilmeyi amaçlamaktadır.
- ESET ürünlerinde ESET Live Grid özelliğinin aktif olduğundan emin olunmalıdır.

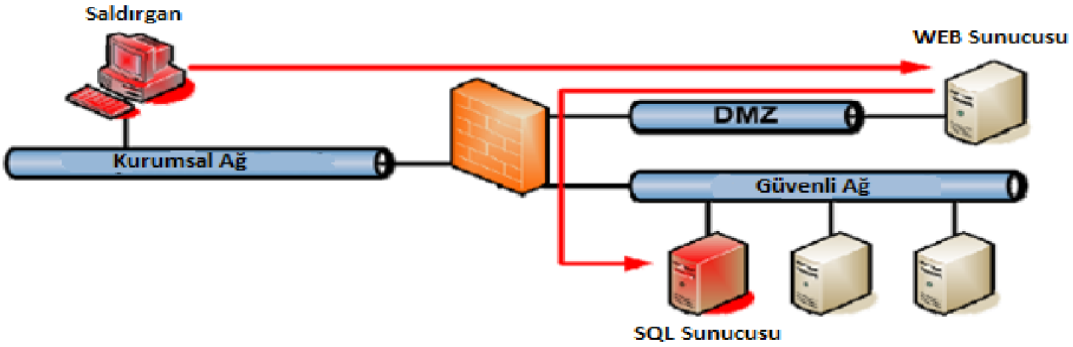
- Kullanılan ESET ürününün ve Virüs İmza Veri tabanı Sürümünün en yeni ve güncel sürümü olduğundan emin olmak gerekmektedir (Siberbulten, 2017).

2.3.11. SQL Enjeksiyonu

Yapılandırılmış Sorgu Dili (Structured Query Language: SQL) sorgulama dil yapısı kullanarak saldırı yapan bu saldırı türü veri tabanından gerçekleştirilen sorgulama işlemini hedef almaktadır (Yıldız, 2014).

"SQL enjeksiyonu ile giriş sayfalarını geçme, veri tabanını kopyalama, hatta Windows işletim sisteminde komut çalıştırma yöntemleri araştırılmaktadır" (Andress ve Linn, Aktaran Bostancı, 2017). Web uygulamalarında, veri tabanı sorgulamalarını yapılabilmesi için belirlenen sorgu komutlarını yöneterek sistem bilgilerine yetkisi olmayan kişiler tarafından erişim sağlanabilmektedir (Bostancı, 2017).

SQL sorgu dilinde yararlanan özel karakterlerin bütünlüğünü garanti altında almayan kişiler girdilerinin yanlış veya yeterli olmayan filtreleme neticesinde ortaya çıkan SQL enjeksiyonu açığı SCADA geçmiş veri tabanını etkileyebilmektedir. Örneğin, bir kötü amaçlı kullanıcı bir veri tabanı sorgulamasında hazır bilgi çıkış karakteri eklemek suretiyle, veri tabanına gelişi güzel bir şekilde okuma/yazma erişimini sağlaması mümkündür. SQL komutu veri tabanı arasındaki iletişimi sağlayarak kimlik sınaması gibi güvenlik denetlemelerinde kullanılmaktadır. SQL enjeksiyonu SQL komutlarını veri tabanına göndererek veri tabanını kötüye kullanabilmektedir. Veri tabanının desteklediği çalışmalar güvenilir ağ kullanarak sunucudan veri elde edebiliyorsa SQL enjeksiyon açısından bir hedeftir. Örneğin, bir istemci uygulaması aşağıdaki şekil 2.5'te görüldüğü üzere arındırılmış bölge anlamını taşıyan ve harici ağlara açık servislerini içeren bu servisleri internet gibi daha kapsamlı ve güvenli olmayan bir ağa maruz kalmasına sebep olan fiziksel veya mantıksal bir alt ağ olan DMZ (Zemilitarized Zone) yalıtılmış Web sunucusunu kullanarak güvenli ağda veri tabanına bağlandığı zaman, SQL enjeksiyonu güvenli ağ üzerinden SQL sunucusuna saldırıları gerçekleştirilebilmektedir. Hatta güvenlik önlemleri sunucuya bağlanan diğer bağlantıların tamamını kese bile kuvvetli bir siber saldırı sonucunda saldırgan güvenilir ağ üzerinden SQL sunucusuna erişip ele geçire bilmektedir (Erkek, 2018).



Şekil 2.5. Web Uygulamaları Üzerinden SQL Enjeksiyonu Saldırısı (Erkek, 2018)

2.4. Siber Saldırılar

Her geçen gün hızlı bir şekilde gelişen teknoloji yararları ile beraber bazı güvenlik problemlerini de getirmektedir. Siber saldırılar sadece bireylere yönelik değil aynı zamanda kurum kuruluş özel sektör ve yahut devletlere yönelik yapılabilmektedir. Ülkeler birbirleri ile siber savaş denilen bir siber rekabet içinde olabilmektedirler. Siber saldırılar için pek çok gereç ucuz ve kolay bulunarak kullanılabilmektedir. Bilgisayarlar, akıllı telefonlar, tabletler ve internette bağlı olan herhangi bir cihazla siber saldırı yapılabilmektedir. Fakat asıl etken internetin ta kendisidir yani internet olmadan siber saldırının gerçekleşmesi mümkün değildir.

2.4.1. Siber Saldırı Nedir?

Siber saldırılar, kişi, firma, kurum veya hükümetin Bilişim Sistemlerinin çalışmasını durdurmak, sistemleri bozguna uğratmak veya iş, ticaret, politik, askeri, yönetim hatta toplumsal hayatı olumsuz etkilemek için kasıtlı ve planlı olarak gerçekleştirilen bir eylemlerdir. Siber saldırılar ulusal veya uluslararası seviyede, yapılabildiği gibi farklı şahıs ve gruplar da çok farklı amaçlarla yapılabilmektedir. Diğer bir deyişle, "Siber saldırı, Ulusal siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın her hangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemlerdir" (T.C. UDHB, 2012).

Gün geçtikçe inanılmaz bir şekilde gelişmekte olan teknolojiden sebep bazı vakalar ortaya çıkmaktadır. Bu vakalardan biri ise siber saldırı diğer bir adıyla sanal ortamda yapılan saldırılardır. Bu saldırılar neticesinde önemli bilgiler (kredi kartı bilgisi, kişisel bilgiler ve ülke güvenliği açısından gerekli bilgiler vs.) saldırgan kişiler

tarafından ele geçirilebilmektedir. Bunun yanı sıra kesinlikle hedef alınan sistem veya toplumun oluşturduğu ortamlarda büyük bir korku ve paniğe sebep olmaktadır (Vasilescu, Aktaran Ercan, 2015).

Bu açıdan siber saldırıları şöyle sınıflandırabiliriz;

- E-posta'lar vasıtasıyla programlara zararlı yazılımlar dâhil ederek hedefteki sistemlere göndermek,
- BİT sistemlerine sızarak illegal bir şekilde bilgi çalmak,
- Kamu ve ticari kuruluşların itibarlarını zedelemek ve psikolojik zarara uğratmak amacıyla web siteleri çökertmek,
- Kamu hizmeti veren kurumların web sitelerine girerek sistem çalışmalarını engellenmek,
- Ülkelerin kritik altyapılarına internet ağları araçlığıyla siber saldırı yapılarak hem maddi hem de itibar kaybı gibi zararlar vermek.

Günümüzde bilgilerin izinsiz ele geçirilebilmesi oldukça yaygınlaşmış durumdadır. Kritik altyapılara karşı gerçekleştirilen saldırılar sistemlerin kumanda ve kontrol mekanizmalarını devre dışı bırakmaktadır (Ercan, 2015).

2.5. **Siber Saldırı Türleri**

Siber uzayda, zararlı yazılımlar, virüsler, solucanlar, mantık bombaları, DOS, DDOS saldırıları ve sosyal mühendislik gibi çok sayıda saldırı türleri vardır. Kötü amaçlı kullanıcılar bu saldırılardan yaralanıp bilgisayarlara ya da sistemlere girerek sistem çalışmalarını durdurmak, bilgileri yok etmek, hizmet aksatmak veya bilgileri sızdırmak gibi çeşitli zararlara uğratmaktadır. Çalışmanın bu kısmında en yaygın bazı siber saldırılar ele alınmıştır.

2.5.1. Hizmet Dışı Bırakma Saldırıları (DOS, DDOS)

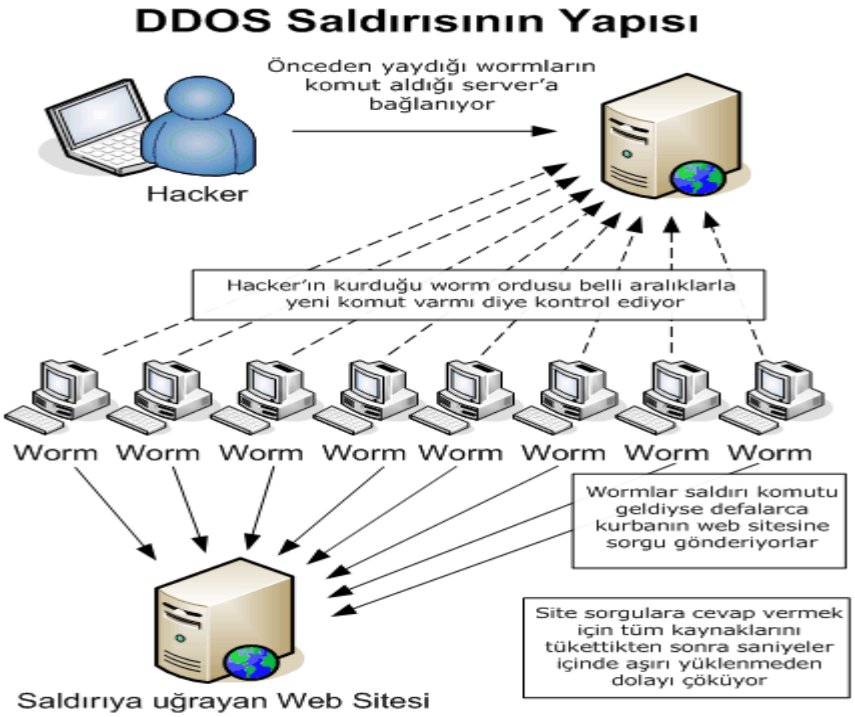
Hizmet Reddi (Denial of Service: DOS), hizmetin aksaması ya da işlevinin tamamıyla engellenmesi anlamına gelir, bilgisayar sistemlerinin kullanılmasına engel olmak ve bu sistemleri çalışamaz duruma sokmak amacıyla yapılan saldırı türleridir. Bu saldırıları daha da etkili hale getirmek için genel olarak, Dağıtılmış Hizmet Reddi (Distributed Denial of Service: DDOS) saldırılarından yararlanılmaktadır (Altundal,

Aktaran Ercan, 2015). Adından da anlaşıldığı gibi DDOS; DOS saldırısının dağıtılmış halidir. Hedef alınan bir hizmetin kullanım dışı bırakmak için yapılan bu saldırıların amacı sistemlere sızmak değil bilişim sistemlerine ulaşımı engellemektir (Çifci, aktaran Ercan, 2015).

DDOS saldırısı sonucunda hizmet veren sunucu bilgisayarlar hizmet veremez duruma gelebilmektedirler. Verilen hizmet bazen tamamen durmaz ama saldırıya uğrayan sistemler iyice yavaşlayarak verilen hizmet kalitesiz hale gelerek nitelik açısından anlamsız kalmaktadır. Bu tür saldırılar sunucu bilgisayarın ağ kaynaklarını tüketmeye çalışarak sunucu bilgisayarın bellek ve işlemcilerine zarar vermektedir, bu nedenle bilgisayarın bellek ve işlemci gücü de önemli rol oynamaktadır.

Bu saldırıları sadece güvenlik duvarı gibi bilgisayar güvenlik programları ya da işletim sistemleri ile %100 bir şekilde engellemek imkânsızdır. DDOS saldırılasılarından başarılı bir şekilde korunmak için sistemin tasarım aşamasından başlayarak ağların tüm aşamalarına kadar lazım gelen tüm güvenlik tedbirlerini almak gerekmektedir (Ercan, 2015).

Saldırı DOS saldırısı ise yani sadece bir IP adresinden yapılmışsa güvenlik duvarıyla engellenmesi mümkündür. Ancak DDOS saldırısı için aynı şey geçerli değildir çünkü bu saldırılar pek çok makine üzerinden gerçekleştirilmekte ve IP adreslerini tespit etmek zorlaşmaktadır. Bu sebeple DDOS saldırısı DOS saldırısına nazaran daha tehlikeli daha etkilidir. Günümüzde sadece bireysel saldırılar değil aynı azmanda grup olarak saldırılar da sık sık yapılabilmektedir. Grup halinde saldırılar farklı yöntemlerle gerçekleştirilebilmektedir (Yıldız, 2014). Şekil 2.6'da DDOS saldırısının yapısı gösterilmektedir.



Şekil 2.6. DDOS Saldırısı (byredwolf, 2012)

2.5.2. Zararlı Yazılımlar

Zararlı yazılımlar, bilgisayar sistemlerini art niyetli kullanmak isteyen etkisiz kişilerin sistem bilgilerini ele geçirmelerini sağlayan veya bu sistemlere ağır hasarlar veren bir zararlı bilgisayar programıdır. Bu yazılımlar geniş bir terim olmakla beraber virüsler, Truva atları, solucanlar casus yazılımlar, tuş kaydediciler, reklam yazılımı ve fidye yazılımı gibi zararlı yazılımları içermektedir. Bu yazılımlar kullanılarak toplum, şirket, kurum ve devletlere karşı siber saldırılar yapılabilmektedir. Burada ki asıl ve en mühim amaç ise sistemlere yetkisiz bir şekilde erişilerek kritik verilerin elde edilmesini sağlamaktır.

Virüs ve Truva atı gibi zararlı yazılımlar çoğunlukla bir e-posta eki olarak kurbanlarına iletilmekte bu eki açan kişilerin bilgisayarlarına bulaşarak kendilerini çoğaltıp bu bilgisayarlarla iletişime geçen sistem ve şebekelere salgın gibi yayılmaktadır. Zararlı yazılımlar genel olarak ücretsiz ya da reklam amaçlı yapılan yazılımlar, uygunsuz web siteleri, oyunlar ve tartışma grupları vasıtasıyla bulaşmaktadır.

Genel olarak tüm zararlı yazılımlar; kendilerini çoğaltma, özelliğine sahiptir. Bu yazılımlar, yaşam döngüsünde farklı yerlerde farklı şeklide davranabilmekte ve kötü

amaçlı kişilerce bizzat elle kurban bilgisayar sistemine yüklenebilmektedir, kendisine karşı kullanılan ve temizlenmesine sebep olan programlar karşısında direnerek, çeşitli taktiklerle bu tür programlardan kurtulabilmektedir (Canbek & Sağıroğlu, 2007).

2.5.3. Kök Kullanıcı Takımı

Kök kullanıcı takımı bilgisayara bulaşıp, çalışmakta olan işlemler arasında gizlenen, kötü amaçlı şahıslara uzaktan sisteme tam yetki veren ve anlaşılması oldukça zor olan bir bilgisayar programıdır. Amacı virüsler gibi sistemin yavaşlamasına neden olmak veya yayılmak değil bilgisayar kontrolünü ele geçirip bulunduğu yerde kendini gizlemektir. Aslında çok kullanıcılı sistemler için kullanıcıların sistem bilgilerine ulaşımını gizlemek için tasarlanmış ve kullanılmış olsa da, kötü amaçlı kullanımı da görülmektedir. Güvenli bir yerden geldiğini düşünerek üst düzey yetkiyle çalıştırılan bir dosya bu zararlı programın sisteme yüklenmesine neden olabilmektedir. Bununla beraber diğer bir yaygın bulaşma yolu ise birden fazla kullanıcısı olan bir sistemde işletim sistemi çekirdeği gibi açıklardan yaralanarak sistemde yetki sahibi olmaktır. Bu kötücül yazılımın aslında hangi belgeleri değiştirdiğini, bulduğu açıklarla hangi parçaları yerleştirdiğini, dosyaların neresinde gizlendiğini, hangi ağ servislerini izleyerek uygun komutla hareket edeceğini belirlemek zordur. Buna rağmen, bazen en uygun komutların ve olası bir rootkit bulaşma noktalarının kendi değerlerinin gizlenerek bunların daha sonra kontrol altında alınması gibi yöntemler kullanılabilmektedir (Vikipedi, 2016).

2.5.4. Yemleme

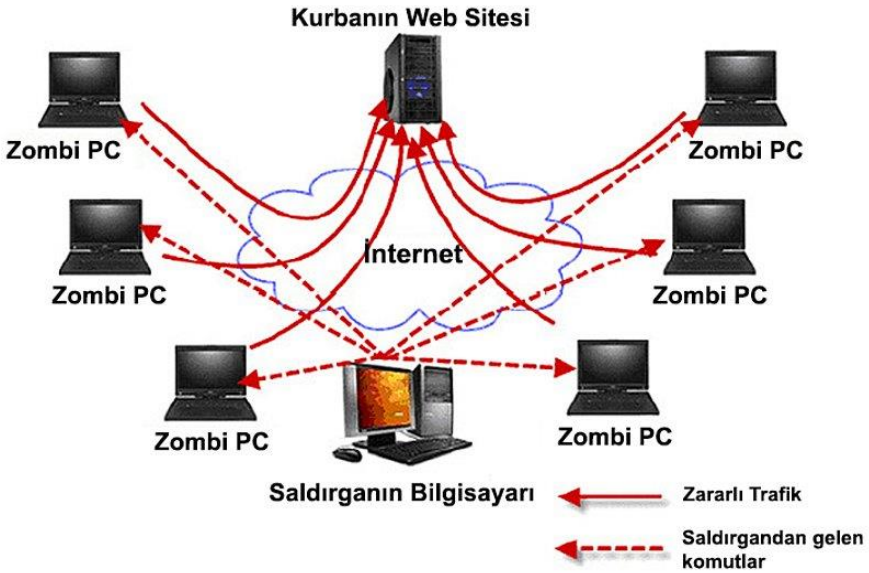
1990'lı yıllarda gelişen en eski siber saldırılardan biri olan ve gittikçe daha karmaşık hal alan bu siber saldırı türü her türlü bireysel ve kurumsal bilgi dolandırıcılığı yapmak için günümüzde de yaygın olarak kullanılmaktadır. Bu saldırı yöntemleri çoğunlukla kullanıcı adı, şifre, kredi kartı bilgileri, ağ kimlik bilgileri gibi önemli ve gizli bilgileri ele geçirmek için yapılmaktadır. Siber saldırganlar, telefon veya e-posta araçlığıyla resmi bir kurum gibi davranıp kullanıcıları kandırarak zararlı bir bağlantıya veya ek olarak gönderdikleri linklere tıklamalarını isteyerek bilgilerini çalmaktadırlar. Amaç; e-postayı alanın, iletide istemiş olduğu veya gerek duyduğu bazı şeylerin olduğunu, müşterisi olduğu bankadan aldığı bir mesaj veya çalıştığı iş yerinden gönderilen e-posta gibi yöntemlerle kandırmaktır. Yemleme sahtekârlığı, e-posta

haricinde, telefon görüşmeleri, kısa mesajlar gibi sosyal medya sistemlerini kullanarak kurbanları kandırabilmektedir.

İngilizce password yani şifre ve fishing yani balık avlama kelimelerinin oluşumundan ortaya çıkan, phishing kelimesi Türkçede "Yemleme" olarak geçmiştir. Şifre avcıları, mağdurlarına genellikle e-posta gibi yollarla ulaşır ve bilgilerini ister. Bu avcılara cevap veren kişilerin hesapları, şifreleri ve özel bilgileri dolandırıcıların eline geçmiş olur. Bu siber saldırının önüne geçmek için bankalar, özel şirketler ve kurumlar müşterilerinden asla e-posta yolu ile özel bilgilerini talep etmeyeceklerini ve bu gibi bir durumda gelen e-postayı veya mesajı kendileriyle paylaşmalarını tavsiye etmektedirler (İsnet, 2019).

2.5.5. Zombi Bilgisayarlar

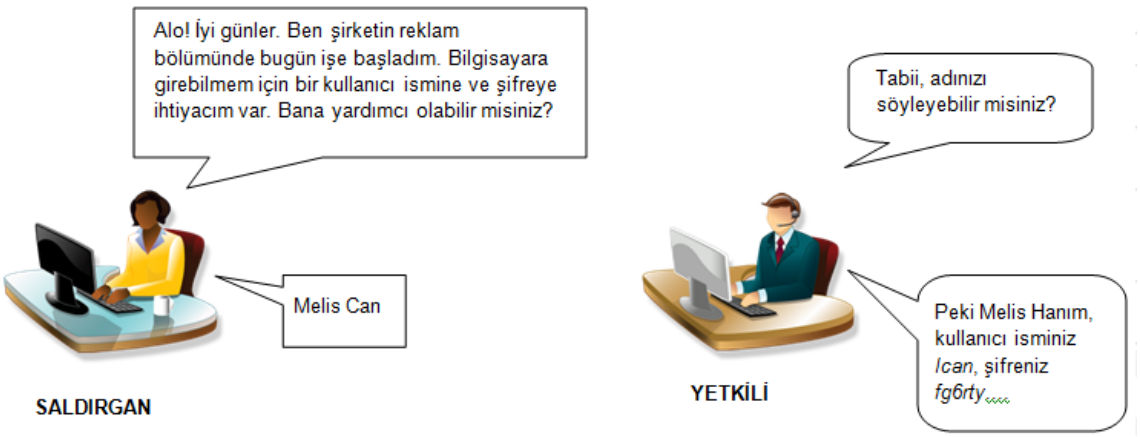
İngilizce Robot sözcüğünün ikinci hecesi ve network yani ağ sözcüğünün birinci hecesinden oluşan Botnet (robot network), saldırganlar tarafından kötücül bir yazılım yerleştirilerek ele geçirilmiş köle bilgisayar topluluğu demektir. Yani zombi hale getirilen bir bilgisayar sahibinin haberi olmadan, yetkisiz kişilerin kendisine uzaktan erişerek robot veya köle gibi istedikleri şekilde kullanma ve kontrol etme etkisi vermektedir, bu da oldukça tehlikeli ve riskli bir durumdur. Zombi bilgisayarlar, karışık matematiksel sorunları çözmek veya buna benzer işleri yapmak için işlem gücünü ortak olarak kullanan, servis dışı bırakma saldırısı tarzı saldıralar yapabilen ve savunmasız sistemler üzerinde kurulan geniş bilgisayar gruplarından oluşmaktadır. Eğer gerekli önlemler alınmazsa ve sistemler koruma altına alınmazsa zombi bilgisayar, kurumsal sistemleri, ev bilgisayarlarını hatta hastane MR (Manyetik Rezonans Görüntüleme) sistemlerini kendi ağlarına dâhil edebilmektedirler (Adress, & Winterfeld, aktaran Ada, 2018). Bu ağ yardımıyla birden fazla komutu aynı anda çalıştırıp saldırı gerçekleştirilebilmektedir. Çoğunlukla, gereksiz e-postalar yani SPAM maili ya da DDOS saldırı olarak yapılmaktadır. Bu tür saldırılara maruz kalan kullanıcılar genelde korunma programları kullanmayan her reklam linklerine tıklayan internet üzerinden sıkça indirme yapan kullanıcılardır. Aşağıdaki şekil 2.7'de bilgisayarların ele geçirilip nasıl Zombi haline getirildiği gösterilmektedir (Selek, 2015).



Şekil 2.7. Zombi Bilgisayarlar (Siber güvenlik haberleri).

2.5.6. Sosyal Mühendislik

Sosyal mühendislik diğer siber saldırı türlerinden farklı olarak kullanıcıların haberleşme, duygu, düşünce, güven kısacası beşeri zayıflıklardan yaralanarak yapılan siber saldırılardır. Bu siber saldırı yöntemi, kullanan saldırganlar hedef seçilen kişilere türlü türlü yalanlar söyleyerek, düzmece senaryolar üreterek, kendilerini güvenli bir kaynak veya yetkili bir kişi olarak tanıtıp ya da basit mükâfatlandırma yöntemleri kullanıp bilgi sızdırmaktadırlar. Buna ek olarak saldırganlar hazırladıkları uydurma e-postalar, telefon konuşmaları, sohbet alanları ve sosyal medya gibi ortamları kullanarak kurbanlarını kandırıp istedikleri bilgilere ulaşabilmektedirler. Bunların yani sıra yazıcıların ortak olarak kullanılması sonucunda iş yerlerinde yapılan çalışmaların çıktılarını alıp gereken düzenlemeleri yaptıktan sonra bu çıktıların yok edilmemesinden dolayı kurum ve kurumun çalışmalarıyla ilgili büyük ölçüde bilginin çalınması ve personellerin çalışma masalarında, kullanıcı adı, şifre veya yaptıkları çalışmalaralar hakkında bıraktıkları notlardan bilgi edinmek gibi yöntemlerde sosyal mühendislik sınırları içindedir. Sosyal mühendislikte kadın sesinin kullanılması erkek sesine göre daha etkili olmakta ve daha başarılı sonuçlar elde edilmektedir. Konunun daha iyi anlaşılması için aşağıdaki şekil 2.8de bununla ilgili kısa bir örnek verilmiştir (Yaşar & Çakır, 2015).



Şekil 2.8. Sosyal mühendislik yöntemi (Yaşar & Çakır, 2015).

BÖLÜM 3

SİBER SAVUNMA

Günümüzde silahlı savaşlardan daha çok siber savaşlar yani bilgisayar başında verilen savaşlar karşımızda çıkmamaktadır, bu sebeple güvenlik son derece önem arz etmektedir. Bundan dolayıdır ki başta devletler olmakla beraber birçok büyük şirketler, bankalar, hosting şirketleri ve kuruluşlar siber savunmaya ciddi önem vermeye başlamışlardır.

Ülkelerin veri/bilgileri ve siber varlıkları, o ülkeler için dijital topraklardır. Normal topraklarımızı nasıl korumak zorunda isek dijital topraklarımızı ve tüm siber varlıklarımızı da aynı şekilde korumak zorundayız. Siber savunma kavramını daha iyi anlamak ve güçlü bir korunma sistemi oluşturmak için tanım ve terimlerin iyi bir şekilde anlamak ve bu kavramın gerçek anlamıyla bilmek gerekmektedir. Siber dünya göz önünde alındığında, gün geçtikçe bir yenisi eklenen birçok terimle karşılaşmaktayız siber savunmayı anlamak için de öncelikle uzmanlar tarafından yapılan bazı tanımlarını bilmemiz gerekmektedir (Sağıroğlu, 2018).

Bu bilgiler doğrultusunda siber savunmayı şöyle tanımlayabiliriz. Siber savunma; siber alanda çalışmakta olan yazılım, donanım ve ağ temellerinden ortaya çıkan bilişim sistemlerine bağlı bir şekilde işlev gören araçlar, donanım, sistemler ve alt yapıları, gerçekleşebilecek siber risklere ve saldırılara karşı korunmak amaçlı alınan tedbirlerdir. Siber saldırıların BİT sistemleri üzerinde olumsuz bir etki oluşturarak bu sistemler yavaşlattığı veya tamamen hizmet dışı bıraktıkları bir gerçektir. Ancak bu saldırılardan korunmak için alınması gereken bir takım önlemler vardır. Bu önlemler doğru ve gerektiği gibi alınırsa sistemlerin faaliyetleri devamlılık sağlayacaktır (Karaarslan vd. aktaran Ercan, 2015).

Bunun sağlanmasında siber savunmanın şu 3 stratejik amacı önemli rol oynamaktadır bu stratejiler, kritik altyapılara gerçekleştirilen siber saldırıları engellemek, bu saldırılara karşı milli açıkları en aza indirmek ve gerçekleştirilen siber saldırılara sonrası sistemin fiziksel veya yazılımsal olarak zarar gören yapılarını en kısa zamanda eski durumuna dönmesini sağlamaktır. Siber tehdit ve saldırıların etkilerini azaltmak için kullanıcılar, genellikle, anti-virüsler, güvenlik duvarları, saldırı tespit sistemleri ve diğer siber savunma yöntemlerine başvurmaktadır. Buna ek olarak büyük anti-virüs firmaları müşterilerini bilerek veya bilmeyerek yapılan siber saldırılar sonucunda meydana gelen olumsuzluklardan korumak için siber tehdit ve saldırıları saptayan, dahası engelleyen bazı araçlar geliştirerek kullanıcılarının hizmetine sunmaktadırlar. Fakat etkili bir savunma kullanıcılara sunulan bu önlemler ve kullanıcıların bu önlemleri en uygun biçimde uygulamasıyla mümkün olmaktadır (Canbek, 2019).

3.1. Siber Savunma Stratejileri

Siber tehditlere yönelik önerilen birtakım savunma stratejileriyle güçlü siber silahlar ile yapılmış olan siber saldırılar tamamen engellenemezse bile, bu saldırıları makul bir ölçüde tutabilmek ve zararların önleyebilmek için savunma yöntemleri bulunmaktadır bunlardan bazı etkili olanları ise aşağıda verilmiştir.

a) Güvenilir Uygulamalar Listesi

Endüstriyel Kontrol Sistemleri Siber Acil Müdahale Ekibi (Industrial Control Systems Cyber Emergency Response Team: ICS/CERT) verilerine göre 2014 - 2015 yıllarında gerçekleşen siber saldırıların %38 gibi bir oranı güvenli uygulama listelerinin kullanılmadığından meydana gelen açıklardan dolayı ortaya çıkmaktadır. Saldırganların hedef sistemlere yerleştirmeye çalıştıkları zararlı yazılımların saptamak ve önüne geçmek için Güvenilir Uygulamalar Listesi önemli bir savunma aracı olarak görülmektedir (Çavuş, 2018).

b) Güncellemeler ve Doğru Yapılandırmalar

Güncel olmayan ve eski versiyonlar kullanan sistemler daha çok siber saldırganların hedefi olmaktadır, bu nedenle, sistemin siber saldırılara maruz kalmaması için güvenilir kaynaklardan devamlı olarak güncellenmesi gerekmektedir. Bunun için

ise kurum ve kuruluşların, bir güncelleme yöntemi uygulaması önerilmektedir. ICS-CERT, güncel olmayan sistem açıklarından dolayı gerçekleşen siber saldırı oranlarını da %29 olarak belirlemiştir (Çavuş, 2018).

c) Saldırıya Uğrayabilecek Alanların Azaltılması

Endüstriyel kontrol sistemlerinin ağlarını tüm güvensiz ağlardan uzak tutulması önemli rol oynamaktadır. Saldırılara uğrayabilecek alanların başında da internet ağı gelmektedir. Burada ise kullanılmayacak olan portların tamamını ve işletim sistemlerini kapatılması ve dış ağlara onaylanmamış işlemler için erişim izni verilmemesi çok önemlidir (Çavuş, 2018).

d) Savunabilir Bir Ortamın Oluşturulması

Kurum ve kuruluşların harici ağlarını koruyan erişim döngüsünün ihlal edilmesi neticesinde ortaya çıkan zararları kısıtlı tutmak ve ağları uygun olarak bölümlere ayırıp hostlar arası (host-to-host) iletişim kanallarını sınırlamak bu noktadaki en etkili taktiklerden birdir. Böylelikle, hem sistemin normal olarak faaliyetine devam etmesini sağlarken hem de bir yolunu bulup içeri sızmayı başaran saldırganların erişimlerini kısıtlayarak ve daha çok bilgiye ulaşmalarının ve zarar vermelerinin önüne geçilebilmektedir (Çavuş, 2018).

e) Yetkilendirme Siteminin Uygulanması

Siber saldırılar genellikle sistemlerde özel yetkisi olan kişilerin hesaplarını ele geçirmek için yapılmaktadır. Bundan dolayı, çok unsurlu deneme yöntemlerinin tatbik edilmesi, yetkili kişilerin yetkileri sınırlanması ve kullanıcılar görevleri açısından hangi yetkilere sahip ise sadece o yetkilerin verilmesi önerilmektedir. Yalnızca şifre gerektiren durumlarda karmaşık ve uzun şifrelerin kullanılmasına özen gösterilmelidir (Çavuş, 2018).

f) Uzaktan Erişim Uygulamalarının Güvenilir Olması

Modemler başta olmakla beraber güvensiz erişim yollarının her durumda yok edilmesi ve açık bırakılan erişimlerin tamamının elden geldiği kadar sınırlanması savunma tedbirleri arasında bulunmaktadır. Tedarikçilerin şirket denetim sistemlerine

kalıcı olarak uzaktan erişilememesi de bu hususta özen gösterilmesi gereken öncelikli konular arasında yer almaktadır (Çavuş, 2018).

g) İzleme ve Müdafaa Uygulamaları

Endüstriyel denetleme sistemlerini gelişmiş siber tehditler ve saldırılardan korunabilmesi için devamlı olarak saldırılara karşı gözlemlenmesi ve gerektiğinde acilen daha önceden kurulmuş olan yöntemler doğrultusunda karşı koyulması gerekmektedir. Buna ek olarak daima bir kurtarma planının olması savunma tedbirleri arasında olduğunun altı çizilmektedir. Bu yönde, kurum ve kuruluşlara sistemlerinin düzgün çalıştığı en son tarihe geri dönmesini kolay bir şekilde sağlayacak "altın" yedek disklerin oluşturulması önerilmektedir (Çavuş, 2018).

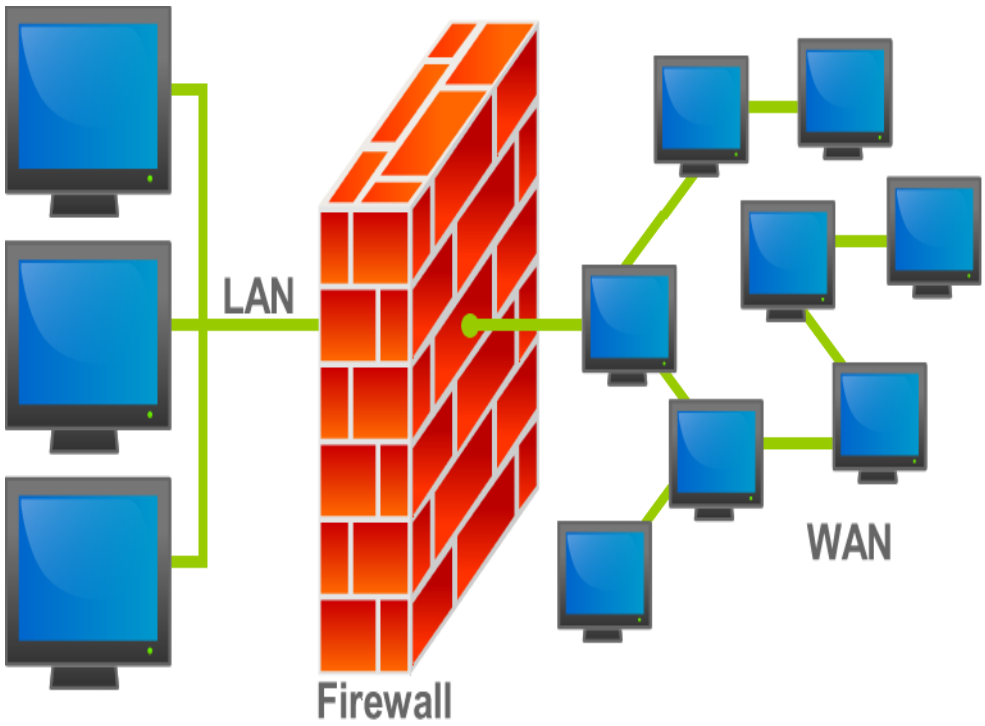
3.2. Siber Savunmanın Unsurları

Hiçbir zaman tam ve yüzde yüz bir savunma yöntemi mevcut değildir, ve hiçbir teknoloji tam olarak tüm siber güvenlik problemlerini tek başına çözebilecek güçte değildir, ancak siber saldırılara karşı başarılı ve iyi bir savunma yapılabilmektedir böyle bir savunma yapabilmek için yerine getirilmesi gereken pek çok savunma unsurları vardır bunlardan bazıları aşağıda verilmiştir, bu unsurlara uyarak daha iyi bir siber savunma yapmamız ve siber varlıklarımızı daha iyi bir şekilde koruyabilmemiz mümkün olacaktır.

3.2.1. Güvenlik Duvarı

İnternet dünyada kapsam açısından daha çok yeni bir teknoloji iken 1980 yılların sonunda ortaya çıkan ve bilgisayar sisteminin bir parçası olan güvenlik duvarı yazılımı, bir kural küme prensibi ile işlev gören, bilgisayar ve internet ağına çıkan giren veri trafiğini denetleyen ve sisteme yetkisi olmayan kişilerin girişlerine engel olan donanım tabanlı ağ güvenlik sistemidir. IP filtreleme, port filtreleme, Web filtreleme, içerik filtreleme gibi çeşitli filtreleme özelliğiyle bilgisayar ve ağın gelen ve giden paketler başta olmakla beraber tüm İnternet yoğunluğunu denetim altında tutmaktadır. Pek çok bireysel bilgisayar işletim sistemleri, siber tehdit ve saldırılardan korunmak amaçlı yazılım esaslı güvenlik duvarları bulundurmaktadır. Ağlar üzerinden bilgi iletişimi yapan birçok yönlendiricide güvenlik duvarı bileşenleri mevcuttur ve temel yönlendirme görevini üstelenmektedir.

Güvenlik duvarları, ilk başlarda kurum kuruluşlar ve özel sektörlerin bilgi sistem ağlarında kullanılmış olsa da gönümüzde kişisel güvenlik için de kullanılmaktadır. Firewall; Geniş Alan Ağına (Wide Area Network: WAN) güvenli ve kontrolü bir şekilde erişimi sağlayan ve WAN üzerinde hizmet sunan servislerin yetkilendirilme işinde ve bu sistemlerin dâhili erişimlerini denetleyen aynı zamanda bu sistemlerin güvenliğinden sorumlu olan, donanım veya yazılım tabanlı programlardır. Donanımsal ve yazılımsal sürümlere sahip olan firewall, kullanılan ağa hangi kullanıcıların ulaşabileceğine, dâhili ağ üzerinden harici ağa kimlerin erişebileceğine, hangi yazılımların aktif olarak çalışmasını onaylayabileceğine kadar ayrıntılı bir şekilde pek çok güvenlik tedbirlerin alınmasında ilk adım güvenlik önlemi şeklinde kullanılacak en temel etkendir. Ağ erişimi ve kullanımı için yetkilendirmenin birinci adımı olarak kabul gören güvenlik duvarları, kişisel manada da siber güvenliğin sağlanması açısından önemli rol oynamaktadırlar (http://en.wikipedia.org, aktaran Karakuzu 2015).



Şekil 3.1. Güvenlik Duvarı (Vikipedi).

3.2.2. İçerik Filtreleme

Son zamanlarda ebeveynlerin çocuklarını sanal âlemin zararlarından biraz da olsa uzak tutabilmek amacıyla başvurdukları yöntemlerden olan içerik filtreleme, haberleşme ağı ya da bilgisayarlara gelen giden yoğunluğun izlenmesi neticesinde hem

zararlı olarak belirlenen hem de istenmeyen veriler ve bilgileri filtre yapan yazılım türleridir. Bu tür yazılımlar vasıtasıyla istenilmeyen web sayfaları, e-postalar, beli kelimeler, fotoğraflar ve uygulamalar filtrelenerek önlenebilmektedir (Stark'tan aktaran Ercan 2015).

İçerik filtreleme, elektronik postaların içeriğini filtrelemek veya sınıflandırmak için kullanılmaktadır. Çoklu kullanım ağlarda bulunan ve bu ağların vazgeçilmez bir parçası olan filtreleme istenmeyen veya belirsiz e-postaları sınıflandırmaktadır. Genellikle işlev görmeyen ve önemsiz elektronik postaları çok olan kullanıcılar tarafından kullanılan bu yazılım kişisel olarak da sınıflandırması mümkündür (Vikipedi, 2017).

3.2.3. Elektronik İmza

Gelişen teknolojilerin insan hayatına girmesiyle beraber tüm ortamlarda kullanıldığı gibi kamu, kurum ve kuruluşlarda da güvenlik açısından bazı kolaylık araçları kullanılmaya başlamıştır. Bu kolaylıklardan biriside elektronik veya sayısal imzadır, kişisel ve kurumsal işlerde imza yetkisine sahip olan şahısların imzasını taklit ederek sahtekârlık ve dolandırıcılık gibi durumların engellenmesi için geliştirilmiş bir uygulamadır. Sayısal imza olarak da bilinen bu imza, diğer bir elektronik veriye bulunan ya da elektronik mantıksal veri ile aynı işlevi gören, harf, rakam ve nesnelerden oluşan ve dijital alanda tasarlanarak "akıllı kart" veya "jeton" vasıtasıyla çalışan ve kimlik sınama amacıyla kullanılan bir çeşit elektronik sistemdir. Taklit edilmesi imkânsız olan bu e-imza, tüm işlemlerde geçerli olmakla birlikte herhangi bir değişiklik yapılması veya benzerinin düzenlenmesi gibi durumlar söz konusu değildir (Türkkep, 2013).

Özellikle e-ticaretin hızla gelişmesinden dolayı oldukça önemli hale gelen elektronik imza yardımı ile imzalanmış bilginin, kimin imzalandığı ve güvenli olup olmadığı denetlenmektedir. Bu imza; gönderilen bilginin üçüncü şahısların ulaşmasına gizli bir şekilde, bilginin üzerinde herhangi bir değişiklik olmadan iletilen taraftan çıktığı orijinal hali ile ve her iki tarafın bilgileri doğrulanmak suretiyle gönderildiğini garanti etmektedir (Vikipedi, 2017).

Elektronik imza kavramı çok genel bir tanım olmakla birlikte, el ile atılmış imzaların tarayıcı ile taratılmış şekli olan sayısallaştırılan imzaları, kullanıcıların göz

retinası, parmak izi veya sesi gibi bilimsel özelliklerini kaydedip kullanmakta olduğu biyometrik tedbirleri kapsamaktadır. Bu imza, imzalanmış olan belgeye göre farklılık göstermekte ve içeriklerin matematiksel fonksiyonlardan geçirilip benzersiz olduğuna inanılan bir değer bulunması şartıyla elde edilmektedir. Yani şahısların, elle atıkları imzalarda olduğu gibi sadece bir imzası bulunmamaktadır; bunun yerine imzalamak için kullanılan anahtarları bulunmaktadır.

Elektronik imzanın 3 önemli amacı bulunmaktadır bunlar;

- Veri Bütünlüğü: Veriler üzerinde silme ekleme veya izinsiz erişim gibi durumları önlemek,
- Kimlik Sınama ve Onaylama: İleti ve bu iletiyi gönderen kişinin iletisinin geçerli olma durumunu sağlamak,
- İnkâr Edilemezlik: Kişilerin elektronik ortamda yaptıkları işlemleri inkâr edememelerini sağlamak (eTR Elektronik TicaretRehberi).

3.2.4. Anti virüs

Anti virüs programı ilk başlarda yani 1990 yıllarında, virüsün bulaştığı cihazları belirleyip, bu virüsleri yok eden hatta başka cihazlara yayılmasına engel olan bir yazılım olarak bilinmekteydi. O zamandan beri zararlı yazılım türlerinin artışından dolayı anti virüs programlarının da daha gelişmiş güvenlik önlemlerine odaklanmalarına sebep olmuştur. Günümüzdeki kullanımı ile "antivirüs" kavramı birden fazla koruma katmanı ile virüslerin yanı sıra genel olarak zararlı yazılımları tespit ederek, önleyen ve yok eden, kullanıcıları siber tehditler karşısında koruyan güvenlik yazılımları aynı zamanda temizleme ve kurtarma görevini de yerine getirmektedir (Eset).

Kişisel açıdan, siber tehditlere karşı önlem olarak başvurulabilecek en önemli ve öncelikli tedbir, işletim sistemine sahip elektronik cihazların tamamına güvenli olduğunu ispatlamış bir anti-virüs programı yüklemektir. Son zamanlarda dünyaca ünlü büyük kurum ve kuruluşlar, kendi çalışanlarına bile evindeki bilgisayarlarında kullanabileceği anti-virüs programlarını ücretsiz bir şekilde sunmaktadır. Zira kurum ve kuruluşların güvenliği çalışanlarından başlamaktadır. Bugün kullandığımız güncel bir anti-virüs programının yarının virüsleri için güncel olamayacağının altını çizmek gerekmektedir. Bundan sebep kullanılan hâlihazırdaki anti-virüs programlarını devamlı

güncellemek, yazılımı sağlayan şirketin sağladı güncelleme işlemlerini yapmak gerekmektedir. Son zamanlarda geliştirilen anti-virüs programlarının çoğu siber ortamda bulunan birçok saldırıları engelleyebilmekte ve kullanıcılara mükemmel olmasa da eskilere göre daha iyi bir güvenlik hizmeti vermektedir (Karakuzu, 2015).

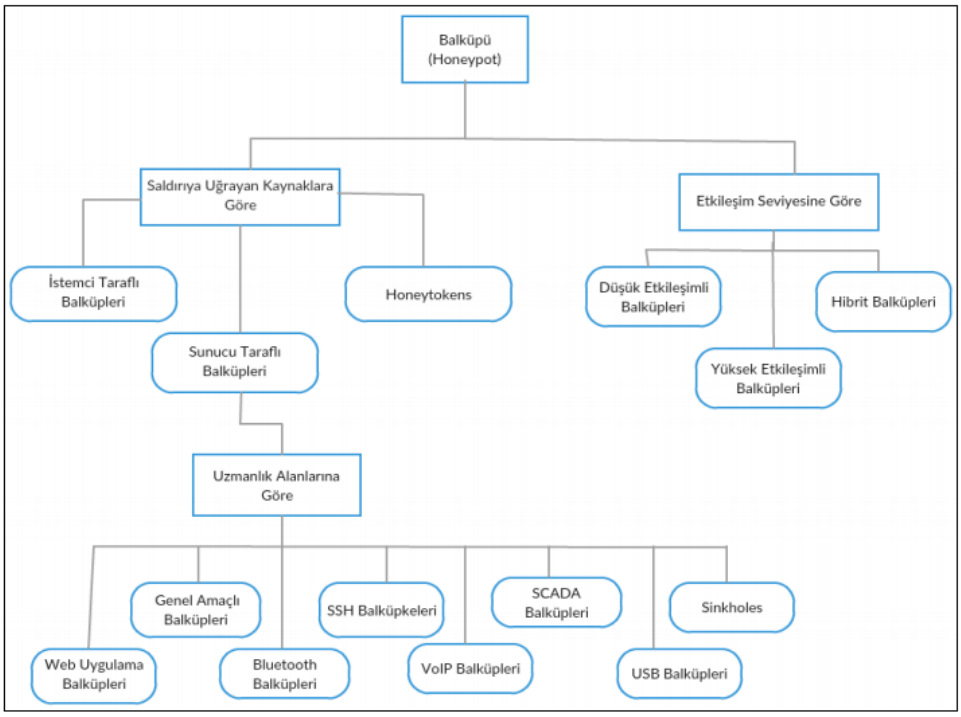
Gelişmiş koruma ürünlerinin çoğu, kullanıcılarının güvenliği açısından pek çok teknoloji kullanmaktadır. Bu da ürünlerin, casus yazılım, kimlik bilgisi hırsızlığı, veriye izinsiz erişim, istenmeyen e-postalar ve dolandırıcılık gibi bazı siber saldırılarla mücadele edebilmeyi güçlendirmektedir. Anti virüs terimi her ne kadar orijinal anlamını kaybetmişse de, çok daha karmaşık ve gelişmiş güvenlik çözümleri için hala yaygın olarak kullanılmaktadır (Eset).

3.2.5. Bal küpü

Bal küpü, bilişim sistemlerine karşı yapılan saldırıları tespit etmek, saldırganları kendine çekerek saldırı ve saldırgan hakkında bilgi toplamak için kullanılan bir güvenlik yazılım türüdür (Gökırmak, Aktaran Ercan, 2015). Diğer bir deyişle bal küpü saldırganları saptamak, yapılan saldırıları çözümlemek veya saldırıların hızını kesmek, saldırganların eline yanlış bilgileri geçmesini sağlamak gibi oluşturulma amacına göre mimarisinde de değişiklik gösteren ağ sistemleridir (Özbay, 2015).

Bilgi sistemlerine yetkisiz erişen kişiler ile ilgili bilgi elde etmeye çalışan bu tuzak sunucular çoğunlukla bir ağın parçası gibi gözüken bilgi veya veriye sahip olan herhangi bir sunucu olabilmektedir. Bal Küplerinin temel çalışma şekilleri şöyledir; Bulundukları ağlarda saldırganların ilgisini çekecek biçimde hareket etikleri için, farkındalık göstermektedirler. Bu işlevi üstlenmiş araçlar herhangi geçerli bir hizmet vermediklerinden, kendilerine gelen her çeşit trafikten kuşku duyarak incelemektedir. Bal küpleri mevcut durumdaki açıklara karşı savunmasız izlenimi vererek, bu açıklardan faydalanmak isteyen saldırganları tespit etmektedir. Bunun yanı sıra, kullanım dışı olan IP'lerin bu cihazlara göndermesi neticesinde meydana gelen yeni saldırıları da tespit etmektedir. Fakat türlü türlü saldırıları kendisine çekeceği için, kullanıldıkları ağ için bir tehdit oluşturabilmektedirler. Bundan sebep bu amaçla kullanılan uygulamanın ayarları iyi yapılmalı ve trafiği denetlenmelidir. Özet olarak; saldırgan bir sisteme saldırmak istediği zaman yapılandırılmış bir sistemle karşılaşır ve bu sisteme güya gerçek bir sistemmiş gibi saldırmaya çalışır, bu esnada bal küpü

devreye girer ve saldırganın davranışlarını, saldırı yöntemini izlemeye başlar ve böylece saldırganın nereden, nasıl ve hangi yollarla saldırmış olduğunu belirleyerek gerçek sistemi bu saldırılardan korumayı amaçlamaktadır. Bal Küpleri kuruluşları, saldırganla etkileşimleri vb. özellikleri açısından aşağıdaki şekil 3.2'de gösterildiği gibi sınıflandırılmaktadırlar (Özbay, 2015).



Şekil 3.2. Bal küplerinin Sınıflandırılması (Grudziecki, Aktaran Özbay, 2015).

Bu çalışma göz önüne bulundurulduğunda sunucu taraflı bal küplerinin sunucularda faaliyet gösteren servisleri (web uygulaması, ssh, voip, telnet) taklit ettiği ve bunlara karşı gerçekleştirilen saldırıları saptamaya yönelik gerçekleştirilen çalışmalarda kullanıldığı görülmektedir. Kullanıcı taraflı bal küpleri ise sunucu taraflıdan farklı olarak kullanıcı davranışlarını taklit etmektedirler. Amacı kullanıcı uygulamalarına gerçekleştirilen saldırıları tespit etmek olan bu bal küpleri sunucularla etkileşim halinde olarak web üzerinden bulaşan zararlı yazılımları tespit etmek için çalışmaktadırlar (Özbay, 2015).

Bal küplerinin, düşük ve yüksek olarak 2 etkileşim seviyesi vardır. Kurulması ve yönetimi kolay olan düşük seviyeli etkileşim sunucu veya kullanıcı taraflı servisi taklit etmekte ve saldırganlar tarafından kolay bir şekilde tespit edilmektedir ve saldırganlarla etkileşimleri gerçek servislere nazaran daha azdır. Yüksek etkileşimli bal küpleri ise gerçek sistem ve kaynaklı araçlardır. Yani bu sistemler taklitten daha çok gerçek

sistemleri barındırmaktadır. Fakat sanal sistemler yardımıyla bir azda olsa taklit edilebilmekte ve çoğu uygulamalar sanal sistemleri kullanmaktadır. Bu şekilde saldırganın sanal sistemler üzerinde etkileşiminin bir sınırı yoktur. Bu sebeple sızma ve enjeksiyon süreçleri tümüyle belirlenebilmektedir. Yüksek etkileşimli bal küplerinin temel avantajları gerçek bir davranış ortaya koymalarıdır (Grudziecki'den ktaran Özbay, 2015).

Etkileşim düzeyinin yükselmesiyle beraber bal küpünün ele geçirilme riski de yükselmektedir bunun yanı sıra saldırganların asıl sistemle etkileşim içinde olmaları sonucunda saldırgan ve saldırı ile ilgili daha çok bilgi elde edilebilmektedir. Bal küpü oluşturulmasında altı çizilmesi gereken diğer bir konuda saldırganların bal küpünü algılayamamasıdır yani saldırgan, saldırdığı sistemi bir bal küpü olarak değil gerçek bir sistem olarak algılamalıdır (Gökırmak'tan aktaran Özbay, 2015).

Bal küpüyle normal internet güvenlik sistemleri yer değiştirmeyecektir bunu unutmamak gerekmektedir. İnternet güvenlik sistemleri ek bir katman veya sistemlerdir. Bal küpünün amacı ise saldırganların sistemlere ulaşmak için nasıl yol izleyerek girişimde bulunduklarını öğrenmek ve izinsiz erişimlerin tespiti veya kovuşturmaya yardım etmek için gerekli adli bilgiler toplamaktır (Even'den aktaran Özbay, 2015).

3.2.6. Siber Tehdit Algılama Sistemi

Siber tehdit algılama sistemi, bağlılaşım kurallarının otomat olarak yükleye bilen tek Güvenlik Bilgileri ve Etkinlik Yönetimi (Security Information and Event Management: SIEM) üreticisi olarak AlienVault, gelen açıklarla ilgili kullanıcıların herhangi bir eyleme girmelerine gerek duymadan tek SIEM çözümlü siber tehdit algılama sistemidir. Bu sistem, sistemde gerçekleşebilecek problemleri belirlemek, gerçekleşen problemlerin gerçeklik payını denetlemek ve ileride gerçekleşebilecek problemlerin algılanmasını sağlamak için pek çok çeşit ürünün bileşkesi şeklinde tasarlanmıştır. Üzerinde bulundurduğu Varlık Yöntem Modülü, Güvenlik Açıkları Modülü**,** Ağ Saldırı İzleme Modülü, Sunucu Saldırı İzleme Modülü, Ağ İzleme Modülü, Dosya Takip Modülü, , Olay Takip Sistemi, Raporlama Sistemi gibi birçok modül sayesinde siber tehditlerin en kısa zamanda tespit edilmesini sağlamakla beraber ağ üzerinde yaşanan tüm olumsuzlukların algılanmasını sağlamaktadır. Bu modüller dışında sistemin en güzel biçimde kullanılmasını sağlamak için kullanıcılara yetki

verme ve oluşan uyarı sonrası verilecek olan karşılıkların planladığı arabirimlerin tamamı bu sistemi oluşturmaktadır. Sahip olduğu bütünsel yaklaşımıyla ağ üzerinden gelebilecek tehditlerin en kısa sürede algılanmasını ve kurumun en az riskle siber dünya ile uyumlu olarak çalışmasını sağlayan tek çözümdür (Akbilge bilişim).

TÜBİTAK Bilgem web sayfasında belirtildiğine göre,

> (…) Birden fazla yerde hizmet sunan kurumsal ağların en büyük sorunlarından bir tanesi siber tehditlerin tek bir yerden anlık olarak izlenebilmesi ve bu saldırılara yanıt verilmesidir. Bu amaçla üretilen Siber Tehditleri Algılama Sistemi sayesinde ağın herhangi bir noktasına gerçekleşen siber saldırılar, anında tespit edilebilmektedir. Ağın kritik noktalarına yerleştirilecek olan bu saldırı tespit sistemleri ile bütün ağı tehdit eden siber saldırılar tek bir noktadan izlenebilmektedir. Yerleştirilen saldırı tespit sistemlerinin kuralları ve çalışma şekilleri merkezi olarak yönetilebilmektedir. Dağıtık ağ yapısı bulunduran kurumlar tarafından kullanılabilecek sistem, ihtiyaçlar duyulduğunda hızlı bir şekilde özelleştirilebilmektedir.

3.2.7. Şifreleme Sistemleri

Şifreleme kelimesi sürekli olarak farklı bağlamlarda ve diğer kelimelerle bağlantılı olarak karşımıza çıkmaktadır. Şifreleme bir iletinin ve bu iletiyi çözmek için bir anahtara sahip olan kullanıcı veya kullanıcılar dışında başkaları tarafından okunmasına engel olan matematiksel bir işlemdir. İnsanlar, tarih boyunca sadece istedikleri kişi veya kişilerin okumasını sağlamak için mesajlarını şifreleme sistemlerini kullanarak iletmişlerdir. Artık gizli haberleşmenin çok ötelerine giden dijital şifreleme teknolojileri mesajları yazan kişileri bile doğrulamak için kullanılmaktadır. Doğru bir şekilde uygulandığında kırılması mümkün olmayan şifreleme sistemi, bilgileri kötü amaçlı, kişilerden, devletlerden ve servis sağlayıcılarından korumak için günümüzde kullanılan en önemli sistemlerden biridir (Surveillance Self-Defense).

Bilgi işlem açısından ise veri güvenliğinin temel yapı taşı olan şifreleme, bilgisayar ortamındaki verilerin kötü niyetli kullanıcıların eline geçmesini ve okunmasını engelleyen en basit ve en önemli güvenlik sistemidir. Kişiler, şirketler kurum kuruluşların yararlandığı bu sistem, tarayıcı ve sunucu arasında iletilen kullanıcı bilgilerinin mahremiyet korumak amacıyla kullanılmaktadır. Gizli bilgilerin ele geçirilmesinin veya tehlikeye atılmasını önlemesi ile beraber bu bilgilerin gerçek olup olmadığını ve doğru kaynaktan gelip gelmediğini de kontrol etmektedir (Kaspersky).

Kullanıcı hesapları açısından ilk güvenlik katmanı olan şifreleme bilgisayar güvenliği için önem arz etmektedir. Zayıf şifreler ağ güvenliğini riske atabilmektedir,

bu nedenle oldukça karmaşık ve güçlü şifreler oluşturmak ve sık sık değiştirmek gerekmektedir. Önerilen şifre değiştirme zamanı en az 6 aydır. Şifre oluşturulurken aşağıda önerilen hususlara dikkat edilmelidir (Yıldız, 2014).

- Sistem yöneticileri her sistem için farklı bir şifre kullanmalıdır.
- Kullanıcılar şifrelerini kâğıtlara veya elektronik ortamlarda yazmamaları ve başkalarıyla paylaşmamaları konusunda eğitilmelidir (Yıldız, 2014).
- Şifrelerin tehimin edilmesi kolay olmamalı ve şifreler en az sekiz ve üzeri karakterden oluşmalıdır.
- Şifreler büyük, küçük harfler, rakam, sıra ve #, %, +, -,?, @, !, *, % gibi özel karakterlerden oluşmalıdır.

BÖLÜM 4

ULUSAL SİBER GÜVENLİK

Tezin bu bölümünde, ilk önce ulusal siber güvenlik konusu ele alınmış akabenden ulusal siber güvenlik stratejisi ve bu stratejilerin hazırlanması, daha sonra Avrupa Ağ ve Bilgi Güvenliği Ajansı (European Network And Information Security Agency: ENISA), Uluslararası Telekomünikasyon Birliği (International Telecommunication Union: ITU) ve son olarak bu konu ile ilgili öncü ülkelerin çalışmaları ve Türkiye'nin Ulusal Siber Güvenlik Stratejileri incelenmiştir.

4.1. Ulusal Siber Güvenlik Tanımı

"Ulusal siber ortamda bilgi ve iletişim teknolojileri aracılığıyla sağlanan her türlü hizmet, işlem, bilgi ve verinin sunumunda yer alan donanım ve yazılım sistemlerinin ulusal ölçekte sağlanan siber güvenliğidir" (T.C. UDHB, 2016).

Ülkelere gerçekleştirilen siber saldırılar ülkedeki insan hayatını durdurabilecek kadar tehlikelidir. Bu nedenle ülkeler, bu siber saldırılardan korunabilmek için strateji belirlemek ve tedbir almak zorundadırlar.

4.2. Ulusal Siber Güvenlik Stratejisi

Günbegün teknolojinin gelişmesi coğrafi mesafeleri ortadan kaldırmış ve elektronik hizmetler insan hayatının önemli bir parçası haline gelmiştir. Günümüzde toplumun bilgi teknolojilerine oldukça bağımlılığından dolay, kritik altyapıların korunması ve kullanılabilirliği ulusal yarar durumuna gelmiştir. Böylelikle siber güvenlik, topluluğun her düzeyini etki eden ulusal bir konu olarak görülmektedir (Ada & Çakır, 2017).

Strateji belgesi, beli devlet organlarının ve bilgi teminatı unsurlarının, özel sektör ve kamu, ilgili uluslararası BİT yöntemlerine ve bu yöntemlerin direk ulusal güvenlik kavramı ile ilgili uygulanmasıdır. Bazen ulusal siber güvenlik konusu, ulusal güvenlik stratejisinin oluşturulmasını öngörmektedir. Stratejilerde hükümet çeşitli risklere karşı tedbir alınması gerektiğinin yanı sıra, hükümet harici aktörlerle beraber çalışılarak da sorunların çözülebileceğine inanmaktadır. Devletler, ulusal seviyede stratejik eylem planlarını ve siber güvenlik açısından kurumlarını da dâhil ederek ulusal düzeyde belge ve girişimler geliştirmeye çalışmaktadırlar (Klimburg, aktaran Ünver, 2017).

Bir stratejinin geliştirilmesi, politikacılar açısından bir araç olmakla beraber, iyi hazırlanmış bir strateji, politikacılara ana hedefleri, gerekli kaynakları ve bunları en iyi biçimde nasıl kullanabileceklerini göstermelidir. Her strateji, siber yarar ve siber zarar arasındaki dengesizliği vurgularken, siber dünyanın önemi dijital bir topluluğun elde etmelerini doğrulama ile başlamaktadır. Stratejiler genellikle hassas kavramları de tanımlamaktadır, lakın bazen siber güvenlik stratejilerinin tamamı aynı tanımları kullanmamaktadırlar. Örneğin, bir kısmı "siber ortamı" yalnızca internet için, diğer bir kısmı ise daha genel bir tanımlama kullanmaktadırlar. Devletlerin uluslararası sorunlarda nasıl tepki vereceğini anlatan ve diğer stratejiler ile bağlantılı olan bir strateji belgesi oluşturması gerekmektedir (Klimburg, aktaran Ünver, 2017).

"Uluslararası çapta ülkelerin strateji dokümanları incelendiğinde, olası siber güvenlik risklerine ve riskleri ortadan kaldıracak eylemler uygulanırken göz önünde bulundurulacak ilkelere yer verildiği, risklerin ve ilkelerin ülkeden ülkeye çok fazla değişiklik göstermediği görülmektedir" (Ünver & Mirzaoğlu, 2011).

Ulusal siber güvenliğin sağlanabilmesi için yürütülecek faaliyetlerde temel alınacak ilkeler aşağıdaki gibidir.

- Uluslararası sözleşmeler ile güvence altına alınan temel insan haklarını ve hürriyetini korumak,
- Demokratik topluluğun nizamının gerektirdiği ortama uymak,
- Alınacak önlemlerin ölçülü prensibine uygun olarak belirlemek,
- Karar almada paydaşların tamamının katılmasını sağlamak için geniş bir yaklaşımı benimsemek,

- Siber güvenliği teknik, hukuki, ekonomik, idari, politik ve sosyal boyutlarıyla beraber araştırmaya alan bütüncül bir yaklaşımı benimsemek,
- Geliştirilecek olan çözümler için güvenlikle kullanılabilirlik arasındaki dengeyi kurmak,
- Başka devlet yöntemlerine bakarak mümkün olduğu kadar benzerliği sağlamak ve uluslararası iş birliği yapmak (Ada & Çakır, 2017).

4.3. Ulusal Siber Güvenlik Stratejilerinin Hazırlanması

Ulusal siber güvenlik stratejilerinin hazırlanması karmaşık bir iştir. Siber tehditlere karşı tedbirler politik, teknolojik, yasal, ekonomik, yönetsel veya askeri gibi alanlardan gelmekte ve beli risklere uygun diğer disiplinleri içermektedir. Güçlü bir güvenlik ile tehditlere karşı durabilmek için tüm bu etkinliklerin birlik olması gerekmektedir. Ulusal bir stratejinin farklı amaçları olabilmektedir. Bunlardan bazıları, tüm devlet kurum ve kuruluşlarının bakış açılarının aynı olmasını sağlamak, özel planlama ile kamu planlamasını tutarlı olarak oluşturmak, eş güdümlemek ve tüm hissedarlar arasındaki öngörülen rolleri, sorumlulukları ve ilişkileri ilerletmek ve bir şahısın milli amacını başka milletlere ve paydaşlara iletmektir (Klimburg, aktaran Ünver, 2017).

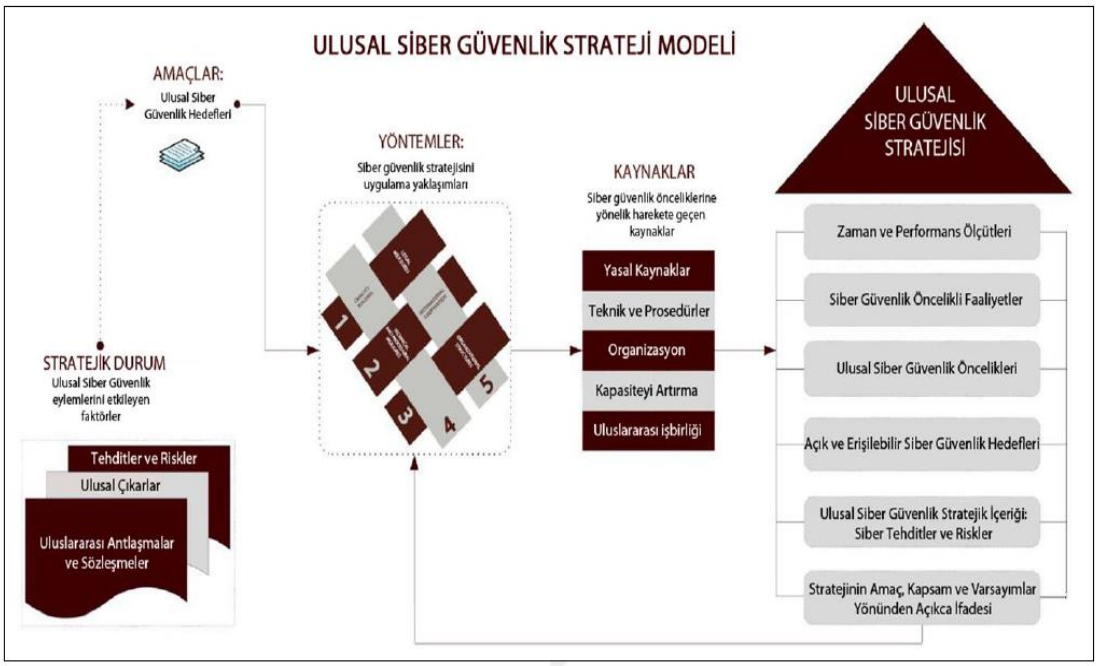
Ulusal siber güvenlik planını ilk defa 2003'te ABD yayımlamıştır, daha sonra tüm ülkeler ulusal güvenliklerini yükseltmek ve bu konuda siber güvenlik vizyonunu tanımlamak için ulusal siber güvenlik strateji belgelerini hazırlamaya başlamıştır. Bu belgeler ulus hükümetlerinin temel düşüncelerini, prensiplerini, yönergelerini, amaçlarını belirleyen ve siber güvenlik açısından riskleri azaltma konusunda önemli ve özel önlemler bulunduran esas belgelerdir. Her ülke kendi Ulusal Siber Güvenlik Stratejisini belirlemek ve uygulamakla sorumludur. Fakat bazı uluslararası düzenlemeler Ulusal Siber Güvenlik Stratejisinin hazırlanması ve uygulanması için ülkelere kılavuz olmak ve bu konuda standart teşkil etmek amacıyla modeller tavsiye etmektedirler (Ada, 2018).

Ülkeler kendi ulusal siber güvenlik stratejik belgelerini hazırlamış ve siber güvenlik kavramını değişik şekillerde tanımlayarak yaptıkları tanımları doğru olarak kabul etmiştir, bu nedenle göz ardı edilen en önemli konu ise "Ne için, Kim için ve

Nasıl bir siber güvenlik" sorusudur. Fakat bu belgelerde söz konusu soruların cevaplarını bulabilmek çok zordur (Akyeşilmen'den aktaran Ünver, 2017).

Ulusal strateji dokümanlarında tanımlanan siber güvenlik kavramı veri, bilişim sistemleri ve ağ sistemlerinin güvenliğidir. Hâlbuki siber ortamın en önemli unsuru kullanıcıdır. Fakat strateji belgelerinde yapılan tanımlarda kullanıcı çoğunlukla dikkatte alınmamaktadır. Bu sebeple kimin için veya ne için güvenlik sorusu oldukça önemlidir. Siber uzayın paydaşları kişiler, şirketler ve devletlerdir, siber güvenlik ancak bu paydaşların istek ve taleplerinin dikkate alınması ile sağlanabilmektedir. Ulusal siber güvenlik strateji dokümanının legal boyutunda meydana gelen zorlukların azaltmak, soruşturma ve kovuşturmanın etkili bir rol alabilmesi için yapılacak olan faaliyetlerde önlemlerin alınması gerekmektedir. Bu nedenle; Yasal açıklıklar giderilerek yasal yetersizlikler ortadan kaldırılmalı ve siber alanda koruma ve gözetleme yetkileri tespit edilmelidir (Ünver, Canbay & Mirzaoğlu, 2009).

Devletlerin siber güvenlik stratejilerini yeniden hazırlanması ya da mevcut stratejilerini güncellemeleri için Şekel 4.1'de gösterildiği gibi bir referans modeli önerilmiştir. Amaç-Metot-Kaynak strateji yöntemi ile hazırlanan bu model için beş önemli çalışma alanı temel alınmıştır (Wamala, aktaran Aytekin, 2015).



Şekil 4.1. ITU'nun Önerdiği Referans Modeli (Wamala, aktaran Aytekin, 2015).

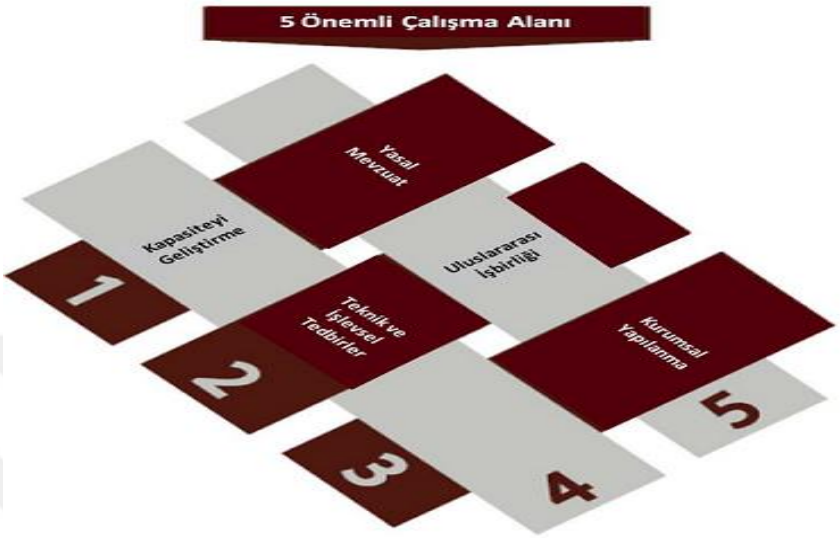
1) Ulusal siber güvenlik konularının gelişmesini sağlamak,
2) Teknik ve fonksiyonel önlemleri almak,

3) Kurumsal yapılandırmayı oluşturmak,

4) Ulusal kapasitenin geliştirilmesi ve farkındalığın arttırılması,

5) Uluslararası işbirliği yapmak

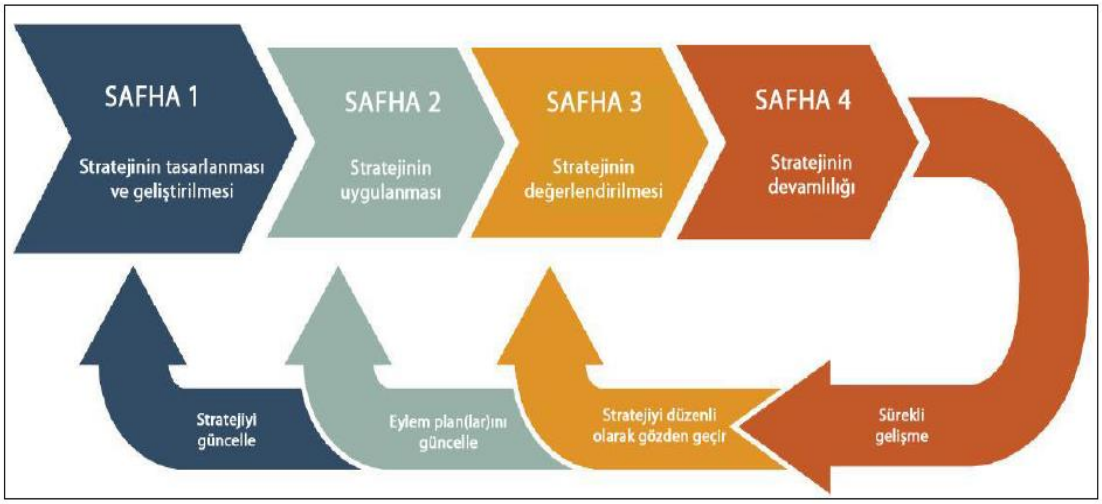
Bu çalışma alanları arasındaki ilişki aşağıdaki şekil 4.2'de gösterilmiştir.



Şekil 4.2. Siber Güvenliğin 5 Önemli Çalışma Ortamı (Wamala, aktaran Aytekin 2015)

4.3.1. Avrupa Ağ ve Bilgi Güvenliği Ajansı

Avrupa Birliği ve Bilgi Güvenliği Ajansı (European Network And Information Security Agency: ENISA), 2005'te Yunanistan'da kurulmuş olan ve siber güvenlik hususunda Avrupa Birliğinin uzman kuruluşudur. Asıl görevi ise halkın, tüketenlerin, şirketlerin ve kurum kuruluşların menfaatlerini göz önüne alarak Avrupa'da bulunan bilgi toplumunu korumaktır. ENISA, ulusal siber güvenlik stratejilerinin süreçleriyle uygulanması kontrol altında alınması ve iyileştirme süreç takibinin devamlılığı için şekil 4.3'te gösterilen ulusal siber güvenlik stratejisi yaşam döngüsünü önermektedir (Ada, 2018).



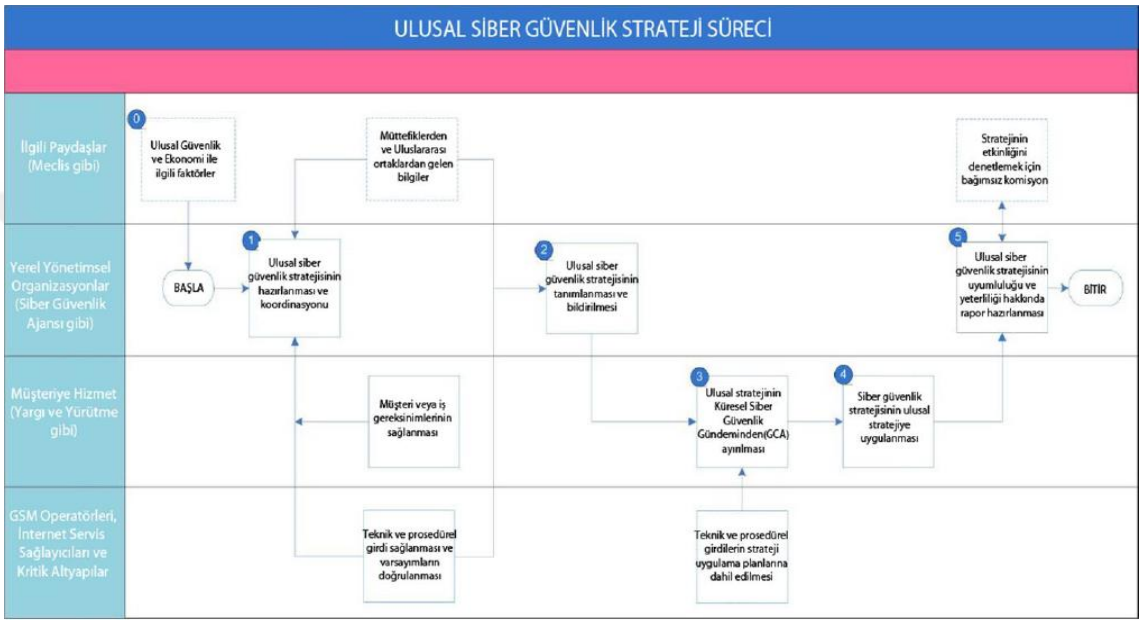
Şekil 4.3. Ulusal Siber Güvenlik Strateji Yaşam Döngüsü(ENISA, Aktaran, Ada, 2018)

- Stratejiyi tasarlamak ve geliştirmek safha1: Ulusal siber güvenlik yetkilisi sorumluluğu altında yürütülmelidir. Bu safhada ENISA'nın tavsiye edilen maddeler değerlendirilip uygulanacaktır.
- Stratejinin Uygulanması safha2 amaç: Ulusal siber güvenlik stratejik süreçlerinin yürütülmesinde ve uygulanmasında katılan ülkelere önderlik yapmaktır.
- Stratejinin Değerlendirilmesi safha3: Stratejiyi değerlendirmek ve ayarlamak için gereken açık gereksinimler ise bu merhale kapsamındadır. Bu safha, amaçlara erişip erişilmediğini ve planlanmış faaliyetler konusunda gerekenin yapılıp yapılmadığını belirlemek için gerekmektedir. Var olan durum hakkında bilgiler elde etmekle beraber, değerlendirmenin ilk amacı, bir sonraki stratejinin amaçlarını belirlemektir (Ada, 2018).

4.3.2. Uluslararası Telekomünikasyon Birliği

Uluslararası Telekomünikasyon Birliği (International Telecommunication Union: ITU), bilgi ve iletişim teknolojileri alanında Birleşmiş Milletler Örgütü'nün uzman kuruluşudur. 1865'te kurulmuş ve 1947'de Birleşmiş Milletler bünyesine yerini almıştır. ITU'nin asıl görevleri ise global radyo spektrumlarını ve uydu yörüngelerini oluşturmak, teknolojiyi hiç kesilmeksizin aralarında bağlantı oluşturan ağların teknik standartlarını belirleyerek gelişmesini sağlamak ve yer yüzündeki yetersiz hizmet verilen tüm toplumun bilgi ve iletişim teknolojilerine erişimini artırılmasını sağlamak (Ada, 2018).

Aşağıdaki şekil ITU'nun önerdiği ulusal siber güvenlik strateji sürecini göstermektedir. Milletlerin idare biçimleri, kabiliyetleri ve gereksinimleri değişiklik gösterdikçe strateji süreçleri de değişiklik göstermektedir. Bu nedenle, bir milletin ulusal siber güvenlik stratejisini nasıl geliştirebileceği, uygulayabileceği ve izleyebileceğini gösteren bu akış şeması sadece örnek olarak verilmiştir. Akış şemasında bulunan safhaların açıklamaları da anlatılmaya çalışılmıştır (Wamala'dan, aktaran Ada, 2018).



Şekil 4.4. Ulusal Siber Güvenlik Strateji Süreci(Wamala, aktaran Ada & Çakır, 2017).

Safha 0: Bilerek veya bilmeden gerçekleştirilen büyük bilgi sızıntıları ya da ulusal güvenlikle ilgili politikalar siber güvenlik strateji çalışmasının ortaya çıkmasına sebep olabilir. Böyle durumlarda ulusal iyileşme planı ve ulusal güvenlik stratejisi, siber güvenlik strateji sürecini teşvik etmektedir. Politikalar siber ortamı, ulusal ekonomik ve güvenlik amaçlarına ulaşması için önemli rol oynayan bir ortam şeklinde sınıflandırmaktadır. Bundan dolayı, ulusal politikalar, devletlerin siber ortamındaki tehditlere karşılık vermesini ve halkın güven içinde olmasını gerektirebilmektedir. Ulusal siber güvenlik stratejisi konusunda eylemlerin sebebine bakmaksızın, strateji geliştiricilerinin tüm paydaşlar ile eşgüdümlü bir yaklaşımın tercih edilmesi önerilmektedir.

Safha1: İcra makamı, siber güvenlik stratejilerinin geliştirilmesinde önderlik yapmakla sorumlu olan makamdır. Devlet, beraber faaliyet göstermenin karşılıklı faydalarının üzerine durarak diğer paydaşların desteklerini alabilmektedir. Devletler en

etkin yaklaşımı seçmekte özgür olsa bile, devletlerin gündem belirlenmesi ve faaliyetleri sırasında paydaşların tamamı ile beraber hareket edilmesi önerilmektedir.

Safha2: Bu safha da Ulusal Siber Güvenlik Stratejileri yayımlanmaktadır. Ulusal siber güvenlik için görev alan kurum, temel paydaşların görev ve mesuliyetlerini belirli kılmaktadır.

Safha3: Ulusal Siber Güvenlik Stratejisi, uygulanacak olan siber güvenlik faaliyetleri için gelecek görüşlerini belirlemektedir. Strateji dokümanın odak noktası, Küresel Siber Güvenlik Ajansı (Global Cyber Security Agency: GCSA) değildir. Hükümetler belirli kurum ve kuruluşlara şirket ve kurum ile ilgili siber güvenlik açısından eşgüdüm görevi verebilmektedir.

Safha4: Bu adımda, hükümetin koordinasyon makamı olarak tayin ettiği kuruluşlar, sektör ile ilgili eylem planlarını yerine getirmek için kritik altyapı operatörleri ve diğer paydaşlarla işbirliği içinde olduğu görülür.

Safha5: Ulusal stratejinin etkinliğini izlemek, siber güvenlik stratejisinin etkinliğini kontrol etmek için bağımsız değerlendirmeler yapan yetkili siber güvenlik organizasyonunun sorumluluğundadır (Ada, 2018).

4.4. Öncü Ülkelerin Çalışmaları

Siber saldırılardan nasibini alan dünyanın hemen, hemen tüm ülkeleri bu siber tehdit ve saldırılardan gördükleri zararları en aza indirmek ve bu saldırıları bir nabza da olsa engelleyebilmek için bazı çalışmalar yapmıştır. Tezin bu kısmında ABD, Rusya, Çin, Kuzey Kore, Almanya ve İsrail gibi üncü ülkelerin çalışmalarına yer verilmiş ve aynı başlık altında Türkiye'nin ulusal siber güvenlik stratejisinden de kısaca bahsedilmiştir.

a) ABD

Kendisine yapılan siber saldırıları bir savaş sebebi olarak değerlendireceklerini açıklayan ABD dünyaya sunduğu siber ortamı ve icat ettiği 5.boyut silah karşısında kendisini bile korumaya çalışmakta ve bu sebeple yeni güvenlik stratejileri geliştirmektedir (Kara, 2013).

ABD'nin siber güvenlikle ilgili ilk geniş ve kapsamlı belgesi 2003'te Beyaz Saray'ın yayınladığı Güvenli Siber Uzay (Secure Cyberspace) belgesidir. Bu belgede "siber güvenlik" terimi sadece 3 defa kullanılmakta ve siber güvenlik yerine çoğunlukla güvenli siber uzay veya siber alan kelimelerine yer verilmektedir (WH, aktaran Göçoğlu, 2018). Bu belgede, ulusal güvenliğin sağlanması için aşağıdaki önceliklere yer verilmiştir.

- Ulusal bir siber ortam güvenliğini sağlamak için karşılık sistemleri,
- Ulusal bir siber ortam güvenliği için tehdit ve güvenlik zafiyet savunma sistemi,
- Ulusal bir siber uzay güvenliği için geliştirme ve farkındalık,
- Devletin siber uzayı sistemini güvence altına almak,
- Ulusal güvenlik ve uluslararası siber ortam güvenliği için işbirliği yapmak.

ABD 2003 yılında yayınladığı belge dışında siber güvenlik politikası üzerine, ulaşılabilir diğer bazı belgeler de yayınlamıştır (WH, aktaran Göçoğlu, 2018). 2008 yılının Ocak ayında eski Başkan George W. Bush'un imzaladığı Kapsamlı Ulusal Siber Güvenlik Girişimi (Comprehensive National Cybersecurity Initiative: CNCI) adlı ve bazı büyük çaplı politika değişikliklerini içeren bir belge ile siber politikasını yenilemiştir (Kara, 2013). Bunlara ek olarak 2011'de yeni bir siber güvenlik strateji belgesi yayınlamıştır, bu belgede 5 stratejik öncelik bulunmaktadır.

1. Savunma Departmanının (Department Of Defense: DOD) siber uzayın tüm potansiyeline hâkim olabilmesi için onu organize etmek, geliştirmek ve donatmak üzere operasyonel bir bağlam olarak ele alması.

2. DOD sistem ve ağlarını korumak için yeni operasyonel savunma içerikleri temin etmek.

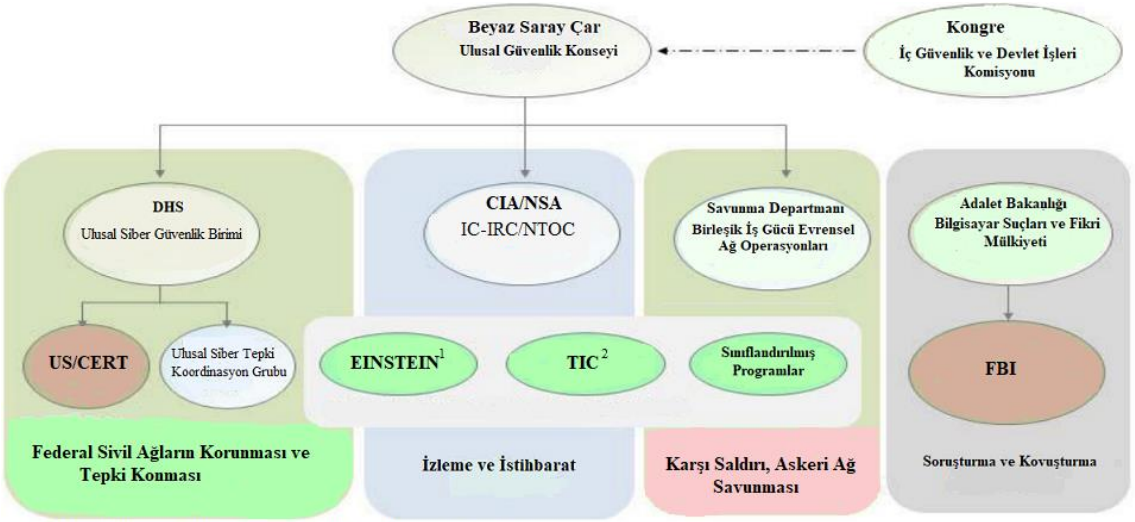
3. Bütünsel bir siber güvenlik stratejisi oluşturmak üzere diğer devlet ve özel sektör kurumlarıyla işbirliği içinde olmak.

4. Kolektif siber güvenliği sağlamak için ABD müttefikleri ve uluslararası ortaklarla güçlü ilişkiler kurmak.

5. Daha iyi bir siber güç ve teknolojik inovasyon kabiliyeti için ulusun yaratıcılığını artırmak (Göçoğlu, 2018).

DOD 2013'te, "Savunma Bölümünün Ağları, Sistem ve Bilgiyi Savunma Stratejisi" adında bir belge yayınlamıştır. Bu belgede stratejinin temel amaçları yer almaktadır bunlar; Esnek bir siber savunma yapısı oluşturmak, Siber savunma operasyonlarını dönüştürmek, Siber olay farkındalığını geliştirmek ve çok geniş ve kapsamlı siber saldırılara karşı koyabilecek sistemler geliştirmektir (Göçoğlu, 2018).

2003 yılında yayınlanan belgede yer alan ve siber güvenliğin sağlanmasından sorumlu olan İç Güvenlik Bakanlığı (Department of Homeland: DHS) siber savunmanın sağlanması için 2 taraflı bir yaklaşım ortaya koymuştur. Bilgisayar Acil Durum Hazır Ekibi Koordinasyon Merkezi (Computer Emergency Readiness Team Coordination Center: CERT/CC) ile DHS işbirliği yaparak federal sivil ağları kurumak için ABD Siber Acil Müdahale Ekibi (United States Computer Emergency Readiness Team: US/CERT) kurmuştur. Bu birimin organizasyon şeması aşağıdaki şekil 4.5'te gösterildiği gibidir. Bu şemaya göre Beyaz Saray'da görev yapan aynı zamanda Ulusal Güvenlik Konseyi üyesi ve kongreye bağlı bir şekilde faaliyet gösteren bir Çar liderliğinde dört temel iş kavramı ile ilgili federal kuruluşların arasındaki bağlantıları gösterilmeye çalışılmıştır. Federal Sivil Ağların Korunması ve Tepki Konmasında DHS çatısı altında bulunan Ulusal Siber Güvenlik Birimi (National Cyber Security Division: NCSD) önderliğinde US-CERT ve Ulusal Siber Tepki Koordinasyon Grubu (National Cyber Response Coordination Group: NCRCG) gibi kuruluşların faaliyet göstermesi öngörülmüştür. NCRCG dünya çapında etkili olabilecek bir siber saldırı halinde 19 üzerinde federal kurumlarda koordinasyon sağlama görevini üstelenmektedir. US/CERT ise önceden mevcut olan CERT/CC'nin görevini üstelenmiştir. İzleme ve İstihbarat sürecinde ise Merkezi İstihbarat Ajansı (Cetral Intelligence Agency: CIA) ve Ulusal Güvenlik Ajansı (NSA) işbirliği ile İstihbarat Topluluğu Olay Tepki Merkezi (Intelligence Community Incident Response Center: IC/IRC) ve Ulusal Güvenlik Kuruluşu Tehdit Operasyonları Merkezi (National Security Agency/Threat Operations Center: NSA/NTOC) gibi kurumlar görev yapmaktadır. Karşı saldırı ve Ordu Ağı Savunması sürecinde ise Savunma Departmanı'na bağlı (DOD) Birleşik İş Gücü Evrensel Ağ Operasyonları (Joint Task Force Global Network: JTFGN) önderliğinde faaliyetler gösterilmektedir (Yıldız, 2014).



Şekil 4.5. ABD Ulusal Siber Güvenlik Birimi (Yıldız, 2014).

DOD tarafından 2015 yılında yayınlanan belgeye ise Siber Strateji adı verilmiştir. Bu belge daha önceki "siber uzay güvenliği" ya da "siber güvenlik" adı verilen belgelere göre daha geniş bir stratejiyi ifade etmektedir. Bu belge ele alındığında, güncel bir siber stratejinin ön görüldüğü ve strateji ile ilgili atılan somut adımların olduğu göze çarpmaktadır (Göçoğlu, 2018).

b) İsrail

Siber güvenlik konusu ile yakından ilgilenen ülkelerden biride İsrail'dir, ulusal güvenliğin ana yatırımlarına ek olarak, 82 milyar dolarlık bir siber güvenlik endüstri hacmi bulunmaktadır. Ülkede 2017'den bu yana siber güvenlik alanında çalışmakta olan 150 aktif firma mevcuttur (BVP, aktaran Göçoğlu, 2018). İsrail'in siber güvenlik alanında en büyük imtihanı, 2014 yılında Gazze'ye gerçekleştirdiği saldırıdan sonra Filistin'in yanında olduklarını göstermek için Türkiye dâhil bazı ülkelerden başlatılan çeşitli siber saldırılarla karşı karşıya kaldığı zaman olmuştur. Bu saldırılar İsrail'in devlet kurumları, iletişim altyapıları, Adalet Bakanlığı, Devletin Arşiv Portalı ve Ulusal Reklam Ajansı gibi birçok bakanlık ve kurum web sitelerini hedef almıştır (Aljareeza'dan, aktaran Göçoğlu, 2018).

Çok sayıda siber saldırıya maruz kalmasına rağmen, İsrail siber güvenlik ve savunma stratejisi iyi olan ülkelerden biridir. Ülke siber güvenlikten sorumlu 4 temel kuruluşa sahiptir. Bunlar;

- İsrail Savunma Kuvvetlerine bağlı olarak, 1952'de kurulan Birim 8200, askeri personel ve subaylardan oluşmakta ve odak alanları ise İstihbarat toplamak, savunma yapmak ve saldırı gerçekleştirmektir.

- Shin Bet: Bu birim ülkedeki bilgisayar sistemlerinin güvenliğini sağlamak, ulusal altyapı ve devlet yöntemlerinin savunmasını sağlamak ile görevli olan iç istihbarat birimidir.

- Komuta, Kontrol, Haberleşme, Bilgisayar ve İstihbarat (Command, Control, Commonications, Computers, Intelligence: C4I): Bu birim tüm sistemlerden, kolordu haberleşme ve siber savunma çalışmalarından sorumludur,

- 2012'de kurulan ve görevi bilgisayar sistemlerindeki siber saldırılara karşı savunma yapmak olan İsrail Ulusal Siber Bürosu (Israel National Cyber Bureau: INCB), bu birim aynı zamanda güvenlik sistemlerini, iş ve akademi dünyası ile işbirliği yaparak savunma sistemlerini organize etmeyi hedeflemektedir (Kara, 2013).

İsrail, siber güvenliğini devlet içinde gerçekleştirdiği organizasyonlar ve uyguladığı politikalarla beraber uluslararası anlaşmalar ve işbirlikleri ile de sağlamaya gayret göstermektedir. Bu hususta en büyük müttefiki Amerika olmasına rağmen başka devletlerle de işbirliği yapmaktadır. Ülke, siber güvenlik ile ilgili yaptığı faaliyetlerden ötürü siber tehditlere karşı en hazırlıklı devletlerden biri olmanın yanı sıra ülkede siber güvenlik konusu devlet ve halkın ortak bir çalışma alanı ve sorumluluğu olarak kabul edilmektedir. Bu ülke, kritik işlemlerini internet ağından farklı bir Ethernet ağ üzerinde tutmakta ve böylece sistemlerini harici tehditlere karşı korumaktadır (Yılmaz & Sağıroğlun'dan, aktaran, Göçoğlu, 2018).

c) Çin

Çin siber güvenlik ve iletişim teknolojilerine 20. Yüzyılın sonlarından, yani bu teknolojilerin ortaya çıktığından beri önem vermektedir. İlk önce 1986'da ekonomik bilgilerin yönetimi ile ilişkin küçük bir ekip kurulmuş ve 2001 yılına kadar etkin olarak görev yapmıştır. 2003'te ise siber güvenlikle ilgili Belge 27 isminde ilk sivil belge yayınlanmıştır. BİT'lerin artmasından dolayı ülkede, siber suç ve siber saldırılar çoğalmış ve siber güvenlik konusu bu ülkenin de öncelik verdiği bir konu olmuştur. Çin'in Siber güvenlik konusunda bakış açısı da başka ülkelerle hemen, hemen aynıdır.

Fakat tehditlere karşı ülkenin uyguladığı siber güvenlik yöntemi daha ulusal ve uluslararası platforma nispeten kapalı olduğundan dolayı batı ülkelerine göre farklılık göstermektedir. Bu ülkenin, başka ülkelerden farkı ise kendi ulusal siber ağlarını kullanarak ve dünyada yoğun olarak kullanılan birçok ağın kullanmasına yasak getirerek ya da kullanımını kısıtlayarak en etkili savunma sistemlerini geliştirmiş olmasıdır. Bu şekilde izlenen bir yöntem ülkeyi, siber güvenlik açısından batı ülkelerine göre daha güvenli kılmaktadır (Göçoğlu, 2018).

Çin bir yandan Ulusal Kalkınma Stratejisi her alanda bilişim teknolojilerinin geliştirilmesini ve kullanılmasını önerirken, diğer yandan da temel bilgi ağlarının ve kritik alt yapılarının, güvenlik sistemlerini güçlendirilmesini göz önünde bulundurmuştur. Ülkenin siber güvenlik ve siber savunmasının sorumluluğu Halk Kurtuluş Ordusu (Peoples Liberation Army: PLA) tarafından sağlanmaktadır. Buna ek olarak, binlerce uzman personelden oluşan ve devlet tarafından desteklendiği düşünülen Çin 61398 nolu birliği 2006'dan beri faaliyet göstermektedir (Kara, 2013).

Ülkede 2014 öncesi yapılan çalışmalarda siber güvenlik ve sistemsel altyapılara önem verilmiş, devletin oluşturduğu konsey bilgisayar bilgi güvenliği yöntemleri kurulmuş, Kamu Güvenliği Bakanlığı (Ministry of Public Security: MPS) tarafından zararlı yazılımlara karşı savunma ve internet için bazı standartlar geliştirilmiştir. 2014 yılında ise siber güvenlik grubu, Çin devlet başkanı Xi Jinping önderliğinde kurulmuş ve yapılan çalışmalara aynı yılın hükümet raporunda yer verilmiştir. 2015'te Ulusal Halk Kongresi Daimi Komitesi (Standing Committee of the National People's Congress: SCNPC) kamu oy birliği ve vatandaşların fikirleri dikkate alınarak Siber Güvenlik Kanunu tasarlanmıştır. Kongre bu kanunu, 2016 yılının Haziran ayında 2.defa tartışmaya açarken, Temmuz ayında ise Siber Güvenlik Kanunun son halini resmi internet sayfasında yayınlayarak kamuoyunun ilgisine sunmuştur (Göçoğlu, 2018).

d) Rusya

Siber güç alanında en önemli ülkelerden biri olan Rusya, 2000 yılının başlarından bu yana, siber uzay alanında etkisini göstermek niyetiyle plan ve strateji geliştirmektedir. 1979 ve 1989 yıllarında gerçekleşen Afganistan savaşı sırasında, Sovyet Ordusu psikolojik savaş tekniklerini kullanamamış ve Moskova Riyaseti Afganistan'daki bağlantıları ile etkili bir haberleşme sağlayamamıştır. Bunun yanı sıra

1994 ve 1996 yıllarında Çeçen Savaşında da, internet üzerinden yapılan iletişimin başarısızlığından dolayı savaş sırasındaki gelişmeler Rusya açısından oldukça olumsuz olmuştur. Bu iki olayın olumsuz sonuçlanmasıyla, Rus devleti siber güvenlik ve askeri ağ teknolojilerini hızla geliştirmeye başlamıştır (Darıcılı, 2017).

24 Ocak 2000 yılında Rusya Federasyonu Ulusal Güvenlik Konsepti (National Security Concept of the Russian Federation: NSCRF) belgesi yürürlüğe girmiştir. Bu belgede genel olarak, bilişim güvenliğinin önemi ve bu konuda ülke menfaatlerine yönelik harici ve dâhili tehditlere karşı alınacak önlemler ele alınmaktadır. Ayını yılın Eylül ayında belirlenen ve ülkenin siber güç olma yönündeki ilk ana belgesi olan Rusya Federasyonu Bilgi Güvenliği Doktrini (Information Security Doctrine of the Russian Federation: ISDRF) belirtilmiştir. Söz konusu belge, ülkenin bilgi güvenliği ile ilgili çalışmalarını, prensiplerini, hedeflerini ve konu ile ilgili resmi görüşlerini genel hatlarıyla kapsamaktadır. Belgede, biri ülkenin siyasi ve kültürel yapısına etki yaratabilecek psikolojik savaş diğer ise siber savaş olarak iki tehdit kaynağına odaklanılmıştır (Darıcılı, 2017).

Rusya'nın 2015 yılında yayınladığı ulusal güvenlik stratejisinde güvenlikle ilgili kişisel, kamusal, çevresel, ekonomik, ulaştırma ve enerji güvenliği konuları özel olarak ele alınırken, belgede "siber güvenlik" terimi hiç kullanılmamakla beraber ulusal güvenlik tehdidi, ulusal menfaatlere direk veya endirekt olarak hasar verebilecek tüm durumlar ve faktörler olarak tanımlanmıştır (Göçoğlu, 2018, s.116).

2020'ye doğru Rus Ulusal Güvenlik Stratejisi (Russia's National Security Strategy to 2020) belgesine bakıldığında bütünüyle güvenlik konusuna odaklanmış bir belge olduğu görülmektedir. Bu belgede, öncelik ekonomi olmakla beraber, sağlık ve güvenlik stratejisi ile ilgili fikir ve düşünceler yer alırken, bilgi güvenliğinden dolaylı bir şekilde bahsedilerek belgenin hedefinin güven artırıcı ve işbirliği olduğu anlaşılmaktadır (Darıcılı, 2017). Bu belge aynı zamanda, federal devletleriyle Rusya'nın uluslararası bilgi güvenliğini sağlamak için, devletlerarası amaçlarını, konu hakkında hukuki ve örgütsel fonksiyonlarını da içerecek şekilde, daha gelişmiş bir uluslararası bilgi güvenliği sistemi olarak hazırlanmıştır. Belge, bilgi güvenliği yönünden 2000 yılının belgesine göre daha geniş tanımları içermektedir (Göçoğlu, 2018, s.120).

Ülkede; Federal Güvenlik Servisi (Federal Security Service: FSB), Dış İstihbarat Servisi (Foreign Intelligence Service: SVR) ve askeri Ana İstihbarat Direktörlüğü (Main Intelligence Directorate: GRU) siber güvenlik alanında görev yapan ve ülkenin siber savunma ve saldırı gücünü belirleyen kurumladır. Bunlardan GRU, Savunma Bakanlığı'na bağlı olarak Rus Silahlı Kuvvetlerinin (RSK) emrinde çalışırken FSB ve SVR, doğrudan Rusya Devlet Başkanı'na bağlı çalışmaktadır. FSB'nin görevi siber saldırılarla mücadele etmek ve ülke siber güvenliğini sağlamaktır (Darıcılı, 2017). Diğer taraftan çalışmanın kayda değer bir konusu da Rusya'nın siber güvenliğe bakış açısı saldırıdan daha çok savunmaya yönelik olmasıdır. Fakat gelişim sürecinde saldırıya saldırı anlayışıyla güvenlik düşüncesini değiştirerek farklılaştırdığı görülmektedir (Göçoğlu, 2018).

e) İngiltere

Bu ülke 2009 yılında kraliçenin buyruğu ile Siber Güvenlik Stratejisi Birleşik Krallık Güvenlik/Güvenlik ve Siber Alanda Dayanıklılık (Cyber Security Strategy Of The United Kingdom Safety/Security And Resilience İn Cyber Space: CSSUKS/SRCS) adlı ilk siber güvenlik strateji belgesini yayımlanmıştır. Bu belgede bir yandan şirketler, devlet ve vatandaşların siber tehditlerle karşı karşıya olduğu açıklanırken diğer yandan daha geniş bir şekilde hazırlanan Ulusal Siber Güvenlik strateji belgesi yayınlanmıştır. Bu belgede devleti, şirket ve halkın korunması gerektiği vurgulanırken, siber alandan gerçekleşebilen tüm siber suçlara karşı nasıl korunması gerektiğine dair açıklamalara yer verilmiştir. Aynı yılın Haziran ayında, stratejik liderliği sağlamak ve Birleşik Krallık Siber Güvenlik Stratejisini geliştirmek ve koordine etmek için Siber Güvenlik Ofisi Kurulmuştur. İngiltere 2010'da Siber Suç Stratejisi (Cyber Crime Strategy) belgesini yayımlanmıştır. Bu belgenin amacı, 2009'da ki Siber Güvenlik Strateji politikasını koordine etmek ve uygulamak, siber güvenlik ofisinin diğer bölümler ve ajanslarla birlikte hareket etmesini sağlamak, özellikle gelişen tehditlere karşı hazırlıklı olmak için Siber Suç Stratejisinin geliştirilmesini ve Siber Güvenlik Ofisi çatısı altında gelişen işlemlere uyumlu olmasını sağlamaktır (Alioğlu, 2019).

2011 yılının Kasım ayında ülke; Dijitalleşen Dünya'ya Birleşik Krallığı Taşımak ve Korumak" adlı başka bir strateji dokümanı yayımlayarak Ulusal Siber Güvenlik planını detaylı olarak ele almış ve ülkenin siber güvenliği ile ilgili önemli değişikliklere

gidilmiş ve bu çerçevede pek çok yeni kurum oluşturulması için faaliyetlere başlanmıştır. Bu strateji belgesine göre ülkenin 2015 yılının siber güvenlik vizyonunun dört temel amacı olacaktır. Bunlar;

- Siber suçlara karşı koyabilmek ve siber ortamda boy gösterebilmek için dünyada en güvenli yerlerden birisi olmak,
- Siber saldırılara yönelik daha güçlü olarak siber ortamı daha iyi korumak,
- Vatandaşların güvenli bir şekilde yararlanabileceği ve açık toplulukların desteklendiği istikrara sahip, aktif ve açık bir siber ortam geliştirilmesine yardımcı olabilmek,
- Alınacak siber güvenlik tedbirlerin tümüne ve amaçlarına arka çıkmak, gerekli olan bilgi ve beceri ile yetenek sahibi olmak (Alioğlu, 2019).

Mart 2014'te kurulan ve ülkenin ulusal siber güvenlik vakalarına karşı tedbirli olmasından ve düzenlenmesinden sorumlu olan İngiltere Ulusal Bilgisayar Acil Müdahale Ekibi (United Kingdom National Computer Emergency Response Team: UK/CERT), aynı zamanda hükümet kuruluşları ve endüstriyel ortaklarla tatbikatları yapmak, akademik kurumlar ve özel sektörle bilgi paylaşmakla görevlidir. Mayıs 2015'te ise güncellenen 2010 - 2015 İngiltere Devlet Siber Güvenlik Politikası (2010 To 2015 Government Policy Cyber Security) adlı politika belgesini yayımlamıştır (Alioğlu, 2019).

2016 yılının Kasım ayında ülkenin son Ulusal Siber Güvenlik Stratejisi (National Cyber Security Strategy 2016 to 2021) yayınlanarak 5 senelik ulusal siber güvenlik strateji raporu açıklanmış ve siber güvenlikle ilgili alanlarda 1.9 milyar sterlin yatırım yapılmıştır. Aynı yılın Aralık ayında Siber Güvenlik Düzenlemesi ve Teşvikler İnceleme (Cyber Security Regulations and Incentives Review: CSRIR) adlı bir inceleme belgesi daha yayınlanmıştır. Yine aynı yılın Ekim ayında ülkenin Ulusal Siber Güvenlik Merkezi (National Cyber Security Center: NCSC) kurulmuş ve resmi açılışını 14 Şubat 2017'de Kraliçe yapmıştır. Kasım 2016'de yayınlanan belgede 2021 yılına kadar ülkenin siber güvenlik vizyonu siber tehditlere karşı güvenilir olmak, saldırılara karşı dayanıklı olmak ve güçlü durmak şeklinde ifade edilerek vizyonun sağlanması için

Savunma, Caydırma ve Gelişme olarak 3 ana başlığı dikkatte almışlardır (Alioğlu, 2019).

Yukarıda kısaca incelenen tüm strateji dokümanları ve raporları sonucunda ülkenin siber güvenlikle ilgili çalışmaları aşağıdaki gibi özetlenebilir.

Siber Saldırılara dair 10 Bölgesel Bilgi Paylaşım Grubu ve 1750 üzerinde kurum, Sanayi ve Devlet için Siber Güvenlik Bilgi Paylaşım Ortaklığı (Cybersecurity Information Sharing Partnership: CISP) kurulmuştur. Siber güvenlik şirketleri, 10 milyardan 17 milyar sterline yükseltilmiş, Siber Güvenlik ortamında bulunan 80 şirkette yaklaşık 100 bin personel alınmıştır. Devlet dijital servisleri kullanarak vatandaşların kimlik bilgilerinin güvenli bir bicimde doğrulamasının yeni bir yöntem olarak GOV.UK sınama sistemi oluşturulmuş bu sistem sayesinde yarım milyon kimlik sınaması test edilmiştir (Alioğlu, 2019).

f) Almanya

Bu ülkede bilgi güvenliği için başlatılan faaliyetler siber güvenlik terimi meydana gelmeden çok daha eskilere dayanmaktadır. İkinci Dünya Savaşı esnasında Nazi Almanya'nın kullandığı Enigma isimli aygıt, Alman askerleri arasında gizli bilgiler için şifre kullanılması ve bu şifreleri tekrar çözülmesi için yararlanılan ve aynı zamanda başka devletlerin iletişim bilgilerini de deşifre edebilen bu aygıt tarih sayfalarında kendine yer bulmuştur. Ülkenin siber güvenlik stratejisini çoğunlukla Alman ordusu belirlemektedir. Fakat siber güvenliğin oldukça kapsamlı olması ve siber saldırıların nasıl, nerden gelebileceğinin ve hangi büyüklükte olduğunun bilinmediğinden dolayı birçok uluslararası kuruluşla da işbirliği yapmaktadır (Göçoğlu, 2018).

Ülkenin siber güvenlikle ilgili düzenlediği belgelere bakıldığında ilk defa 1989'da Ulusal Politika belgesi yayınlanmıştır. Daha sonra 2005'te Bilgi Güvenliği ve Kritik Altyapıların Korunması ile ilgili Ulusal Strateji Belgesi yürürlüğe konulmuştur. Bu belgeden sonra 2011'de yayımlanan Alman Ulusal Siber Güvenlik Stratejisi, özellikle siber ortamdan gelebilecek risk ve tehditlere karşı koyabilmek için odaklanmıştır. Ülkenin siber güvenliğinin sağlanması için temel yapı olarak önemli katkılarda bulunan Alman Federal Bilgi Güvenliği Örgütünün birimlerine ise siber güvenlik ile ilgili uzmanlaşan bir politika takip etmektedirler. Bu örgüt, Siber Güvenlik

Dairesi, Kriptoloji Dairesi, Güvenli Elektronik İşlemler Sertifikasyon ve Standardizasyon Dairesi, Profesyonel Ağ Savunma Birimi gibi birimleri içermektedir (Tuluk & Seferoğlun'dan, aktaran Göçoğlu, 2018).

Almanya'da gün geçtikçe karmaşıklaşan bilgi altyapılarına ve güvenlik zafiyetlerine bakıldığında, siber güvenlik durumu ilerleyen zamanlarda da kritik bir şekilde devam edecektir. Alınması gereken bazı stratejik amaçlar ve tedbirler vardır.

German'dan, aktaran Ünver'e göre (2017),

> (…) Kritik bilgi ve altyapıların korunması, ülkede güvenli bilgi ve iletişim teknolojileri sistemlerinin oluşturulması, kamu yönetiminde bilgi ve iletişim teknolojileri sistemlerinin güçlendirilmesi, ulusal siber güvenlik konseyi ve yanıt merkezinin kurulması, siber alanda da etkili suç kontrolünün yapılması, Avrupa'da ve dünyada siber güvenliği sağlamak için etkin ve uyumlu bir eylem koordine edilmesi, güvenli ve güvenilir bilgi teknolojisinin kullanılması ve siber saldırılara tepki veren araçların yapılması gerekmektedir (s.114).

4.5. Türkiye'nin Siber Güvenlik Stratejisi ve Eylem Planlarının İncelenmesi

Türkiye 2012 tarihine kadar siber güvenlikle yakından ilgilenmemiştir. Türkiye'nin siber güvenlikle ilgili attığı ilk önemli adım 12 Aralık 2012 yılında Ulusal Siber Güvenlik Strateji Belgesini yayımlaması olmuştur. Bu belge gereği Ulusal Siber Güvenlik Koordinasyon Kurulu oluşturulmuş ve Ulaştırma Denizcilik ve Haberleşme Bakanlığı (UDHB) Koordinasyon Makamı olarak belirlenmiştir. Daha sonra 2013-2014 Siber Güvenlik Eylem Planının hazırlanması ve yürürlüğe konulması ülkede hükümetin ve kuruluşların siber güvenlik anlayışının kurumsal olması oldukça önem arz etmiştir. 2015'te, ise 2013-2014 Eylem Planının artıları ve eksilerine bakılarak, 2015-2017 Eylem Planı geniş bir katılım çalışmalarıyla hazırlanmıştır(Yazıcı & Akkaya, 2015).

Siber Olaylara Müdahale Ekiplerinin (SOME) kurulması ve UDHB'nin Koordinasyon Makamı olarak belirlenmesi Türkiye'de hükümetin ve kurum kuruluşların siber güvenliğe bakış açısını ve yaklaşımını tümüyle değiştirmiştir. 2015'te UDHB, 2015-2017 Siber Güvenlik Eylem Planını kapsamlı katılımlı çalıştaylarla daha aktif ve zengin bir sürece götürmüştür ancak resmi olarak yayınlanmamıştır (Yazıcı, Akkaya, 2015).

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

Çalışmanın bu bölümünde, ulusal siber güvenlik stratejisi dâhilinde 2013-2014 dönemi, ulusal siber güvenlik için belirtilen maddeler çerçevesinde sağlanması açısından eylemler bulunmaktadır.

4.6. Stratejik Siber Güvenlik Eylemleri

Gün geçtikçe artan tehditleri ortadan kaldırmak ve ulusal siber ortamdaki zafiyetleri en aza indirmek ve bilgi teknolojilerini kullanmaya geçiş sürecinin en verimli ve emin bir şekilde ilerlemesi Türkiye'nin hedefleri için büyük rol oynamaktadır. Bu süreçte, BİT'lerin aktif, kaliteli ve uygun fiyatla kullanılması ile beraber, bu teknolojilere yönelik bilişim sistemlerinin kullanımında siber güvenliğin sağlanması da oldukça önem arz etmektedir. Bundan dolayı, siber güvenlik; bilgi topluluğuna geçmeyi amaçlayan topluluğun refah ve huzuru, ülkenin istikrar ve ekonomik kalkınması ve ulusal güvenliğin sağlanması gibi birçok alana etki eden çok paydaşlar olan stratejik bir meseledir. Bu sınırlar içinde, 2013-2014 dönemi için, bazı stratejik eylemlerin gerçekleştirilmesi planlanmıştır. Bu eylemler, aşağıdaki gibi gruplandırılmaktadır (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2013).

4.6.1. Yasal Düzenlemeler

2013-2014 dönemi için, ulusal siber güvenliğin sağlanması açısından var olan alanların eksiklerinin giderilmesinin yanı sıra kurumların görevleri, yetkileri ve sorumluluklarının tanımlamasını, hedefleyen mevzuat oluşturulma faaliyetlerine başlanacaktır. Bu faaliyetler, medeni hukuk, ceza hukuku, idari yargı ve bunlarla ilgili usul devletlerinin tümünü düzenlenmesi için arka çıkacak bir nitelik sunulacaktır (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2013).

4.6.2. Adli Süreçlere Yarda Bulunacak Faaliyetlerin Yürütülmek

Uluslararası hukuk kanunları içerisinde, siber saldırılara uğrayan kurum ve kuruluşların haklarının korunabilmesi için, saldırının nerden ve kimin tarafından yapıldığını tespit ederek saldırıya uğrayan sistemlere ve bu sistemlerin hizmet verdiği kullanıcıların ne boyutta etkilendiğini belirlenmesi gerekmektedir. Bu bilgilerin üretilebilmesi için ulusal siber ortamın güncel teknolojilere uyumlu olması ve güvenilir

kayıt mekanizmalarıyla donatılması gerekmektedir (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2013).

4.6.3. Ulusal Siber Olaylarla Mücadele (USOM) Organizasyonunun Oluşturulmak

Yakın bir zamanda; siber alanda meydana gelen saldırıların hızlı bir şekilde tespit edilmesi, gerçekleşebilecek siber olayların etkilerini en aza indirmeye veya tamamen yok etmeye yönelik tedbirlerin alınması ve uygulanması için ulusal seviyede etkili bir biçimde faaliyet gösterecek Siber Olaylara Müdahale Organizasyonu kurulacak, böylelikle kurumlar ve kuruluşlar siber güvenlik olaylarına karşı koyabilecek yeteneğe sahip olacaktır. Ülkemize etki edebilecek tehditler karşısında, 7/24 müdahale temeline yönelik faaliyet gösterecek USOM kurularak, bu kuruluşun eşgüdümünde çalışacak sektörel SOME kurulacaktır. Bu SOME'ler siber vakalara müdahale etmekle beraber kendilerine bağlı SOME'lere ve ilgilendiği sektörlere özel bildirim ve bilgilendirme çalışmaları yürütecektir. Ayrıca kurumlarda da sektörel SOME'lerin eşgüdümünde faaliyet gösterecek SOME'ler oluşturulacaktır. USOM ve SOME'ler siber olaylara müdahalede bulunurken suç soruşturmalarına destek verebilecek bilgilerin elde edilmesi için adli makam ve kolluklarla koordineli olarak çalışacaktır. USOM ulusal iletişim noktası olarak başka ülkelerin eş değer makamları ve uluslararası kuruluşlar ile yakından işbirliği içinde olacaktır (T.C. UDHB, 2013).

4.6.4. Ulusal Siber Güvenlik Altyapısının Güçlendirilmek

Orta ve kısa vadede; kurumların tümü, bilişim sistemlerinin siber güvenliğine destek çıkacak büyük kapsamlı altyapı projeleri yapılacaktır. Başta kritik altyapılarının bilişim sistemleri olmakla beraber kurumsal siber güvenliği sağlamak için faaliyetler gösterilecektir. Kritik altyapıların bilişim sistemleri, kritiklik düzeyleri, aralarındaki ilişkiler ve sorumlukları tanımlanacaktır. Kritik altyapıların bilişim sistemlerine ait siber güvenlik teknoloji tedbirleriyle birlikte idari önlem ve süreçler de sağlanacaktır. Bu açıdan kurum ve kuruluşlarda idari ve teknolojiği içeren eğitim vasıtasıyla öncelikli ileri düzey idareciler olmakla beraber tüm personellerin siber güvenlikle ilgili yetkilerinin artırılması sağlanacaktır. Kurumsal siber güvenliği sağlamak için gereken yetkinliği sağlayamayan kurumlar için destek verilecektir (T.C. UDHB, 2013).

4.6.5. Siber Güvenlik Konusunda İnsan Kaynağı Yetiştirmek ve Bilinçlendirmek

Uzun ve orta vadede; siber güvenlik konusunda yeteri kadar ve yetkin insan kaynağı oluşturulması ile ilgili faaliyetler gerçekleştirilecektir. Orta ve yükseköğretimde siber güvenlik konusuna yer verilmesi için düzenlemeler gerçekleşecektir. Bilişim sistemlerini denetleyenlerin, teknoloji geliştirenlerin, sistemi yönetenlerin ve ilgililerin tümünü siber güvenlik bilinç ve farkındalığın artırılması ve aldıkları sorumluluklar hakkında bilgi vermeleri için etkinlikler yapılacaktır. Kurumsal dâhili kontrol proseslerin de siber güvenlikle ilgili kontrol aşamalarının yeterli bir şekilde incelenmesi için faaliyetler gösterilecektir. İlaveten, siber güvenlik farkındalığının oluşturulması ve geliştirilmesi için tüm topluluğa yönelik bir eğitim sistemi oluşturularak bu eyleme hizmet veren girişimlere destek verilecektir (T.C. T.C. UDHB, 2013).

4.6.6. Siber Güvenlikte Yerli Teknolojilerin Geliştirilmesi

Orta ve uzun vadede; siber güvenlik alanında ülkeye ait teknik birikim, imkân ve yetenekler artırılacaktır. Kamu ve özel şirketlerin Ar-Ge ihtiyaçlarının giderilmesi yönündeki eylemlerin tümünde çalışmalar işbirliği yapılarak gerçekleşecektir. Kurumlar bilişim sistemleri için yerli ürünlerin kullanmaları, bu ürünler bulunmadığında ise güvenlik testleri yerli olarak yapılmış sertifikalı ürünleri kullanmaları tavsiye edilecektir (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2013).

4.7. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2016-2019)

Gün geçtikçe gelişmekte olan BİT sistemleri, değişen güvenlik ihtiyaçları ve elde edilen deneyimler sonucunda, Ulaştırma, Denizcilik ve Haberleşme Bakanlığınca Ulusal Siber Güvenlik Stratejisinin güncellenmesi ve 2016 - 2019 dönemi için eylem planlarının belirlenmesine ihtiyaç duyulmuştur. Bu Strateji ve Eylem Planının hazırlanmasında paydaşlar ile beraber yapılan faaliyetlere ilaveten geri planlamada kaynaklar taranmış, Amerika, Uzak Doğu ve Avrupa'dan birçok ülke siber güvenlik stratejileri incelenmiş, bu ülkelerin siber güvenlik ortamında, kapsamlar, amaçlar, öncelikler, organizasyonlar, kaynak tahsisleri, Ar-Ge koordinasyonları, kamu ve özel sektör ortaklığı ve eğitimler gibi başlıklar altında çözümler üretilmeye çalışılarak tüm bu çalışmalar sonucunda 2016 - 2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı hazırlanmıştır (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016).

4.7.1. Misyon

Ulusal Siber Güvenliğin sağlanabilmesi için, etkili ve devamlı politikaları belirlemek, eşgüdümü sağlayarak uygulamasını yapmak.

4.7.2. Vizyon

Vatandaşların refahı ve güven içinde yaşaması, ülke ekonomisinin gelişmesi ve verimliliğine katkı sağlamasında BİT'lerden en etkili biçimde yaralanabilmek için, siber güvenlik açısından tüm paydaşlar işbirliği yaparak siber ortamdaki risk ve tehditleri yetkin bir şekilde yönetilen siber güvenlik ortamında enternasyonal bir yarış gücü olan bir eko-sistem oluşturmaktır.

4.7.3. Amaç

Bu Ulusal Siber Güvenlik Stratejisi ve Eylem Planının temel hedefi; siber güvenlikle ulusal güvenliğin tek bir parça olduğunun bilincinin tüm sektörlerde yer alması, ulusal siber ortamda var olan sistemlerle paydaşların güvenliğinin sağlanması için yönetimsel ve teknoloji açısından tedbirlerini almak için yetkinliklerin tam olarak kazanılma durumudur. Bu temel hedefi yapabilmek için, amaçların ve alt eylem planlarının belirlenip gerçekleştirilmesi ve kontrol edilmesi de bu belgenin amaçları içerisindedir.

4.7.4. Kapsam

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na göre (2016),

> (…) 2016 - 2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, kamu bilişim sistemlerine ve kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerine ek olarak küçük ve orta ölçekli sanayi, tüm özel ve tüzel kişiler de dâhil olmak üzere ulusal siber uzayın ülkemiz ölçeğindeki bütün bileşenlerini kapsar (s.9).

4.7.5. Güncelleme

Gelişen teknolojiler değişen koşul ve ihtiyaçlar dikkate alınarak özel sektör ve kamudan gelecek isteklere yönelik, ulusal seviyede sağlanacak koordinasyonla güncel tutularak 2019 yılında bitmeyen eylemler bir sonraki eylem planına aktarılacaktır (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016)

BÖLÜM 5

AFGANİSTAN ULUSAL SİBER GÜVENLİK STRATEJİSİ

Günümüzde, siber saldırılar gün geçtikçe artmakta ve bilişim sistemlerine önemli zararlar vererek siber ortamın geleceği için oldukça sorunlar ve zorluklar yaratmaktadır. Diğer taraftan, Afganistan devletinin, siber saldırılara yönelik iyi belirlenmiş bir strateji planı yokken, Afganistan'ın siber ortamında felâketle sonuçlanan olaylara sebep olan diğer ülkelerden aktarılan büyük miktarda zararlı veriler mevcuttur. Bu sorunlar göz önüne alınarak, çalışmanın bu bölümünde Afganistan'da siber saldırı ve siber istismarlar, bilgi güvenliği açısından yaşanan güçlülükler, siber saldırıların Afganistan mevcut ağ altyapıları üzerindeki etkileri ve mevcut siber tehditler incelenmiştir. Bununla beraber, siber güvenlikle ilgili Afganistan'ın şuan ki siber ortamına, gelecekteki siber güvenlik durumuna ve bu alanda yaşanabilecek güvenlik zorluklarına ilişkin sorunlara da bu bölümde yer verilmiştir (NCSA, 2014).

2001 yılında Taliban rejiminin çöküşünden sonra, Afganistan hükümeti siber güvenlik konusunda önem vermekte, güvenli sanal bağlantı sistemleri ve güvenilir internet bağlantısı için yıllık büyük miktarda bütçe ayırmaktadır, ancak buna rağmen, ülkede siber güvenlik ve siber zorluklarla ilgili ciddi bir eksiklik ve endişe bulunmaktadır. Temel olarak, Afganistan Ulusal Güvenlik Konseyi (Afghanistan National Security Council: ANSC) ve Afganistan hükümeti tarafından finanse edilen telekomünikasyon bakanlığı Siber Araştırma Merkezi ve dünya bankası tarafından desteklenen Bilgi Teknolojileri Araştırma Merkezi (Information Technology Research Center: ITRC), mevcut siber güvenlik, siber tehdit ve veri gizliliğini korumak için tüm sosyal ve devlet sistemlerinde verimliliği ve şeffaflığı sağlamak için güvenilir güçlü e-devlet sistemleri oluşturmaktadır (NCSA, 2014).

2001 yılının sonlarına doğru, geçici hükümetin kurulmasından sonra, Afganistan teknolojik, siyasi, ekonomik, endüstriyel, ticari ve sosyal iyileştirme ve yeniden yapılanma ufuklarına adım atmıştır, daha sonraki geçiş sürecinde seçilen Afgan hükümet başkanı, kurum kuruluşlar ve özel şirketlere ülkede siber güvenlik konusunda yatırım yapmalarını desteklemiş ve Afganistan halkına telekomünikasyon ve BİT hizmetleri de dâhil olmak üzere çeşitli hizmetler sağlayan yeni yasalar getirmiştir. İletişim ve Bilgi Teknolojileri Bakanlığı (Ministry of Communications and Information Technology: MCIT), Afganistan'daki özel sektörler ve devlet kurumları arasında yeni stratejiler ve politikalar tasarlayan ve özel sektörlerin telekomünikasyon ve bilişim sektörlerine büyük yatırım yapmalarını sağlayan ilk şirket olmuştur (NCSA, 2014).

2009 yılında, MCIT Afganistan'ın ilk Siber Acil Müdahale Ekibini (Cyber Emergency Response Team: CERT) resmi olarak kurmuş ve ilk Afgan Acil Müdahale Ekibi(Afganistan Cyber Emergency Response Team: AFCERT) olarak adlandırmıştır. AFCERT'in görevi siber tehditlere, siber saldırılara ve siber suçlara karşı mücadele etmek, devlete ve özel sektörlere siber güvenlik konusunda farkındalık yaratmak ve yaşanan sorunlara karşı çözümler öğretmektir. AFCERT, faaliyetinin ilk iki yılında, MCIT üst yönetimine, ülkedeki siber ve elektronik suçlarda yaşanan artış konusunda resmi bir rapor sunmuştur. Söz konusu suçlarla mücadele etmek için, tüm devlet BİT altyapılarının risk değerlendirmesini yapmak ve bu riskleri azaltmak için bir çözüm bulmak hayati önem taşımaktadır. AFCERT'in ülke için bir Siber Güvenlik Stratejisi taslağı hazırlama önerisi MCIT ve BİT konseyi tarafından kabul edilmiş ve bu amaçla MCIT ve BİT konseyi bir komite oluşturmuştur (NCSA, 2014).

2012'de Afganistan Ulusal Siber Güvenlik Stratejisi (National Cybersecurity Strategy of Afghanistan: NCSA)'nın hazırlanmasına ilişkin ilk bilinçlendirme çalıştayı, ABD Ticaret Bakanlığı tarafından desteklenen ve finanse edilen Bilgi ve İletişim Teknolojileri Enstitüsü (Information And Communications Technology Institute: ICTI)'de yapılmıştır. 4 gün süren bu çalıştaya tüm hükümet Sanayi Kuruluşları Organizasyonları (Congress of Industrial Organizations: CIO), BİT başkanları, özel sektör yöneticileri ve bilim adamları katılmış ve üzerinde çalışılmış daha sonra farklı ülkelerden çeşitli stratejiler incelenmiştir. NCSA komitesine MCIT Bilgi Sistemleri Güvenlik Müdürlüğü başkanlık etmiş ve bir yıl boyunca düzenli toplantılarını ve değerlendirmelerini yapmıştır. Bu değerlendirme ve öneriden sonra, NCSA komitesi,

eylem planını gözden geçirmek ve uyarlamak için 2014 – 2015 stratejinin ilk taslağını MCIT ve BİT Konseyine sunmuştur (NCSA, 2014).

5.1. Afganistan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2014 - 2015)

Bu kısım, Afganistan ulusal siber güvenlik stratejisi ve 2014 – 2015 dönemi için belirlenen ilkeler ışığında ulusal siber güvenliğin sağlanması için eylemleri incelenmektedir. Bu gibi durumlarda, ilgili tüm kuruluşların ve ajansların, öncü kuruluş ve ajansın koordinasyonunda gerektiği şekilde hareket etmesi gerekmektedir (NCSA, 2014).

Bilgi ve iletişim teknolojilerinin kullanımı tüm dünya da olduğu gibi Afganistan'da da hızla gelişmekte ve bu sistemler insan hayatının her alanında önemli roller oynamaktadır. Kamu kurum ve özel şirketlerin yanı sıra, ekonomi, enerji, sağlık gibi kritik altyapı sektörlerinde de hizmet sunan kuruluşlar, havacılık, iletişim ve finansal hizmetler de yoğun olarak bilgi ve iletişim sistemlerini kullanmaktadır. Bu sistemler hizmet sunumunun kalitesini ve hızını arttırmakta, böylece kuruluşların daha verimli çalışmasına ve yaşam standartlarının iyileştirilmesine yardımcı olmaktadır (NCSA, 2014).

Kamu ve özel sektör organizasyonlarımız, bilgi ve iletişim teknolojilerini daha güzel ve daha verimli hizmet verebilmek için kullandıklarından dolayı, bu teknolojilerin güvenliğini sağlamak için ulusal güvenliğimizin ve rekabet gücümüzün önemli bir yönü olmuştur. Bilgi ve iletişim teknolojilerinde ortaya çıkan güvenlik açıkları hizmetin reddedilmesine veya hizmetlerin kötüye kullanılmasına neden olabilmektedir; bu da yüksek oranda ekonomik kayıplara, kamu düzeninin bozulmasına ve/veya ulusal güvenlik tehditlerine yol açabilmektedir (NCSA, 2014).

Siber alan, bilgi sistemlerine ve verilere gerçekleştirilen siber saldırılar açısından anonim olma durumu ve inkâr etme olanaklarına zemin hazırlamaktadır. Saldırılar için gereken malzeme ve bilgilerin genellikle ucuz ve basit bir şekilde bulunabilmesi ve dünyadaki herhangi bir kişinin veya kişilerin coğrafi sınır tanımadan, bilerek ya da bilmeden siber saldırılara katılabileceği mümkündür, bu kalıcı ve gelişmiş siber saldırıları kimin finanse ve organize ettiğini belirlemek neredeyse imkânsızdır. Bu gerçekler ve koşullar, siber alandaki risklerin ve tehditlerin asimetrik doğasını ortaya

koymakta, dolaysıyla oluşan risklerin ve tehditlerin üstesinden gelmeyi daha da zorlaştırmaktadır (NCSA, 2014).

Mesuliyet ve sorumluluklar ortaya konduktan sonra bu konuda daha fazla netlik olacaktır. Afganistan ulusal siber güvenlik stratejileri için 2014-2015 döneminde gerçekleşmesi planlanan bazı eylem maddeleri vardır. Bu eylemler için son tarih belirlenir ve periyodik olarak tekrarlanması öngörülen ve/veya kronik olay olan eylemler özellikle vurgulanacaktır (NCSA, 2014).

5.1.1.Vizyon

Afganistan hükümeti, işletmeleri, ticaret alanları ve vatandaşları için güvenli, emin ve esnek bir siber alan oluşturmak ve elde etmek (NCSA, 2014).

5.1.2. Misyon

Afganistan'ın siber alanındaki veri, bilgi ve bilgi teknolojilerinin altyapısının güvenliğini sağlamak ve güvence altına almak, siber tehditleri önlemek ve bunlara müdahale etme kapasitelerini arttırmak, Afgan çocuklarını ve gençlerini siber alanda korumak, güvenlik açığı risklerini, çeşitli yolardan kaynaklanan siber tehditlerden ve siber olaylardan gelebilecek her türlü zararları azaltmak (NCSA, 2014).

5.1.3. Hedef

1) Devlet BİT altyapısını korumak, vatandaşlar için güvenli bir siber ortam sağlamak, siber güvenlik profesyonel becerilerini geliştirmek ve korumak, kamu ve özel sektör ortaklıklarını teşvik etmek, uluslararası işbirliğini artırmak ve sürdürmek.

2) Bilgi güvenliği güvencesi, bilgi güvenliği politikaları, uluslararası standartların adaptasyonu ve en iyi uygulamalar için bir sistem ve alt yapı oluşturmak.

3) Esnek bir siber alan ve ekosistemini sağlamak için düzenleyici bir yapı oluşturmak.

4) AFCERT'in siber tehditlere ve siber suçlara karşı mücadele yeteneklerini arttırmak, devlet için afet kurtarma planları hazırlamak ve geliştirmek ve ülkedeki kritik bilgi ve bilişim altyapılarını geliştirmek.

5) Ulusal güvenlik gereksinimlerine göre uygun teknolojiler, süreçler geliştirmek ve uygulamak.

6) Ülkede uygulama ve yazılım geliştirmeyi standartlaştırmak ve geliştirmek için test ve onaylama kuruluşları oluşturmak.

7) Ülke genelinde bilgi ve siber güvenlik uzmanları için eğitimleri desteklemek ve kolaylaştırmak.

8) Önemli veriler için koruma mekanizmalarını sağlayarak devlet, işletmeler ve vatandaşların veri gizliliğini güvence altına almak.

9) Ülkedeki siber güvenliğin esnekliğini artırmak için kamu ve özel sektörlerle ortak işbirliği yapmak ve katkılarda bulunmak.

10) Siber ve elektronik suçların, etkin bir şekilde önlenmesi, soruşturulması ve araştırılmasının sağlanması ve güçlendirilmesi, etkin bir siber kanun ve mevzuatla kolluk kuvvetlerinin uygulanması.

11) Siber suçlarla mücadele için uluslararası işbirliğini geliştirmek ve güçlendirmek (NCSA, 2014).

5.2. Ulusal Siber Güvenlik Stratejilerimiz

5.2.1. Afganistan'da Esnek Bir Siber Ekosistemin Oluşturulması

a) Ülkedeki siber güvenlik ve bilgi güvenliği ile ilgili tüm sorunları koordine etmek için İletişim ve Bilgi Teknolojileri Bakanlığı (MCIT) ve Kuruluşundan bu yana AFCERT'i yönetmekte olan Bilgi Sistemleri Güvenlik Müdürlüğü (Information Systems Security Directorate: ISSD), devlet yapısında bağımsız bir varlık haline gelmelidir. Bu, ISSD'nin tam bütünlüğünü sağlayan diğer hükümet ve sivil toplum kuruluşlarının siber güvenlik görevleri ve kararları üzerindeki her türlü istenmeyen ve yersiz etkilerinden kaçınılacaktır.

b) Hem kamu hem de özel sektörlere, üst düzey bir yöneticiye Güvenlik Görevlisi Şefi (Chief Security Officer: CSO) atayarak, onlara siber güvenlik mesuliyetini ve ülkedeki girişimlerin sorumluluğunu vererek, kamuya ve özel sektörün ortaklıklarını sağlama konusunda teşvik ve tavsiye etmek.

c) Kamu ve özel sektörleri, uluslararası standartlara ve en iyi uygulamalara uygun olarak, iş profillerini ve hizmetlerini uygun bilgi güvenliği politikalara göre hazırlamak ve geliştirmek. Bu politikalar geniş kapsamlı olmalı, olağanüstü durum kurtarma planı ve iş sürekliliği dâhil olmak üzere çeşitli veri güvenliği metodolojileri ile güncel olmalıdır.

d) Kamu ve özel sektör, siber güvenlik ve bilgi güvenliği faaliyetleri ve girişimleri için bütçelerini adamalı, bu bütçe, BİT altyapı koruma mekanizmaları, lisanslı yazılımlar ve BİT personeli için kapasite geliştirme dâhil olmak üzere genel siber güvenlik girişimleri için olmalıdır.

e) AFCERT, profesyonel kadro ve iyi bir itibara sahip olarak hem siber hem de bilgisayar olaylarına ilk müdahaleci olarak kamu ve özel sektöre hizmet verecek ve tüm varlıkların, AFCERT tarafından belirlenmiş prosedürlere ve uygulamalara uyup uymadıklarından emin olunacak.

f) Güvenlik açısından MCIT, hükümetin Bilgi Teknolojisi (Information Technology: IT) ile ilgili tedariklerin onaylanması, web barındırma şirketleri, yazılım geliştiriciler ve IT hizmetleri sağlayıcısı için yeni ilkeler ve politikalar ortaya koyacaktır (NCSA, 2014).

5.2.2. Bilgi Güvenliği Güvencesi ve Politikaları İçin Bir Altyapının Oluşturulması

a) MCIT'nin ISSD'si, devlet sistemlerinde bilginin gizlilik, erişilebilirlik ve bütünlüğünü sağlamak amacıyla uluslararası standartların, bilgi güvenliği için en iyi uygulamalarının ve uygunluğun uyarlanmasını sağlamalıdır.

b) ISSD sayesinde Bilgi Güvenliği Yönetim Sistemi (Information Security Management System: ISMS) için uluslararası standartların bilgi güvencesi, bilgi sistemleri ve IT altyapısı denetimlerinin, güvenlik açıklarının değerlendirmesi, Kritik Bilgi Altyapılarının (Critical Information Infrastructures: CII), risk yönetimi, ticaret konularında süreklilik, Yazılım Geliştirme Yaşam Döngüsü (Software Development Life Cycle: SDLC) ve en iyi uygulamalar ve IT altyapılarının test edilmesi ve uygulama güvenliğinin sağlanması.

c) Veri gizliliğini ve verimliliğini sağlamak için erişim denetimlerini (Fiziksel, Teknik ve İdari) uygulamak ve tüm kamu kurumlarının veri sınıflandırmasını sağlamak.

d) CII'nin periyodik olarak risk değerlendirmesi ve güvenlik standardı uygunluğunu yapılması (NCSA, 2014).

5.2.3. Düzenleyici Bir Alt Yapı ve İskeletin Oluşturulması

a) MCIT, yasal bir alt yapı oluşturmak, geliştirmek ve siber güvenlik konularını ele almak için Adalet Bakanlığı (Ministry of Justice: MoJ) ile iş birliği içinde olacaktır.

b) Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu (United Nations Commission On International Trade Law: UNCITRAL) ve Siber Tehditlere Karşı Uluslararası Çok Taraflı Ortaklığı (International Multilateral Partnership Against Cyber Threats: IMPACT) desteği ve işbirliği ile Afganistan siber güvenlik yasasını ve Afgan genç ve çocuklarını çevrimiçi koruma politikasının geliştirilmesi sağlanacaktır.

c) Özel Sertifika Yetkilisi (Certification Authority: CA) için yasal alt yapı, ticari ve finans kurumları için güvenli elektronik işlem sistemi geliştirmek.

d) Güvenli mobil bilgi işlemi, mobil yönetim ve internet yönetimini sağlamak için yasal sistemler ve politikalar geliştirmek.

e) Hükümet sistemlerindeki siber güvenlik açıklarını kapatılması ve hükümete IT hizmetleri sunan Çözüm Sağlayıcıları (Solution Provider: SP) için IT altyapılarını denetlemek ve onaylamak için düzenleyici bir sistem geliştirmek.

f) Tüm düzenleyici sistemler için farkındalık kampanyası düzenlemek ve gelişen teknolojik ilerlemelerle periyodik olarak güncellemek (NCSA, 2014).

5.2.4. AFCERT Kabiliyet ve Yeteneklerini Geliştirmek

a) Hükümet ve özel sektörde ortaya çıkan herhangi bir siber olay veya bilgisayar suçlarına karşı ilk olarak AFCERT müdahile edecektir.

b) Ağ Operasyon Merkezi (Network Operation Center: NOC), atölye çalışmaları, seminerler, e-postalar, dergiler ve haber bültenleri aracılığıyla tüm hükümet ve sivil toplum kuruluşlarına siber güvenlik ile ilgili farkındalığın sağlanması.

c) Çalışma saatlerini iki yıl içinde 7/24 hizmet verilebilir duruma getirilmesi.

d) Siber suçlara karşı savaşmak için bölgesel Siber Acil Müdahale Ekibi (CERT) ile güçlü ilişkiler ve koordinasyonun sağlanması.

e) Siber güvenlik uygulamalarını koordine etmek ve bölgesel CERT'lerle siber tatbikatlar yapmak.

f) AFCERT'in kapasite ve performansını artırmak için periyodik olarak gelişmiş eğitimler ve kapasite geliştirme programlarının düzenlenmesi (NCSA, 2014).

5.2.5. Güvenli ve Sürdürülebilir E-Devletin Kurulması

a) MCIT, güvenli ve güvenilir bir e-Devlet hizmetleri sağlamak için kapsamlı bir bilgi güvenliği sistemi uygulamalıdır.

b) Afganistan Temel Sertifika Yetkilisi (Afghanistan Root Certification Authority: ARCA), politikaları uygulamak ve hükümet içindeki tüm e-Gov ve m-Gov hizmetleri için dijital imza kullanımını zorunlu kılmak (NCSA, 2014).

5.2.6. Test Etme Ve Onaylama Ekibinin Oluşturulması

MCIT, test süreçleri tüm uluslararası standartlara uygun olacak şekilde yazılım ve uygulamaları test etmek ve onaylamak için, profesyonel programcılardan oluşan bir ekip oluşturacak ve bu yazılım ve uygulamaların güvenliği ve bütünlüğü kurulmuş olan bu ekip tarafından sağlanacaktır (NCSA, 2014).

5.2.7. Bilgi ve Siber Güvenlik Uzmanları için Eğitimleri Kolaylaştırmak

a) MCIT, tarafından devlet ve özel sektörlerdeki personeller için bilgi güvenliği eğitimleri, seminerleri ve atölye çalışmaları sağlamak amacıyla eğitim ve kapasite geliştirme programları sağlanarak yürütülecek ve koordine edilecektir.

b) Yüksek Öğretim Bakanlığı (Ministry of Higher Education: MoHE) ve kamu hizmetleri komisyonu ile birlikte çalışılarak bilgi güvenliği alanındaki yüksek lisans programlarına burs imkânları sağlanacaktır (NCSA, 2014).

5.2.8. Toplumun Veri Gizliliğini ve Güvenliğini Korumak

a) ISSD, Kritik bilgi altyapısının korunması için bir plan ve bilgi güvenliği sistemi geliştirecektir. Bu plan, olağanüstü durum kurtarma ihtiyacını karşılayan bilgi akışı için güvenli mekanizmalar içermelidir.

b) Risk yönetimi, kriz yönetimi ve siber/elektronik suç soruşturma ve araştırması için ilkeler ve uluslararası standartlar oluşturulacaktır (NCSA, 2014).

5.2.9. Kamu ve Özel Sektör İşbirliğinin Desteklenmesi ve Güçlendirilmesi

a) Hükümeti destekleyebilecek özel veri ve bilgi merkezlerinin kurulması, ücretsiz hizmetlerin sunulması ve desteklenmesi için özel sektörlerin kamu kurumları ile yakın ilişiklerde ve iş birliğinde bulunması teşvik edilecektir. Bu iş birliği sadece sağlıklı bir rekabet piyasasını teşvik etmekle kalmaz, aynı zamanda hükümette BİT ekonomisini de güçlendirir ve her iki sektör arasında güven oluşturur.

b) Siber güvenlik ve kritik bilgi altyapısının korunması, özellikle siber güvenlik eylem planının uygulanması, uluslararası güvenlik standartlarının uygulanması ve en iyi uygulamalar konularında paydaşlar arasında (hükümet ve özel sektör) işbirliği ve bu işbirliğinin kolaylaştırılması (NCSA, 2014).

5.2.10. Uluslararası İşbirliği

a) MCIT, ACERT'ler, bilgi güvenliği kuruluşları, kolluk kuvvetleri, tüzel kişiler ve adli kuruluşlar aracılığıyla bölge ve diğer ülkelerle siber alanlarda çok taraflı bir ilişki kurulması (NCSA, 2014).

b) MCIT, siber suçlarla mücadele için Siber Tehditlere Karşı Uluslararası Çok Taraflı Ortaklık (IMPACT), Uluslararası Telekomünikasyon Birliği (ITU) ve diğer yerel ve uluslararası kuruluşlarla yakın ilişki ve işbirliği içinde olup bu iş birliğini sürdürmelidir (NCSA, 2014).

5.3. Afganistan'daki Siber Saldırılara Kısa Bir Bakış

Tezin bu kısmında, Afganistan devletinin resmi web sitelerinde gerçekleştirilen bazı önemli siber saldırı olaylarından bahsedilecektir. Bu saldırılar, askeri altyapılar, hükümetin iletişim sistemleri ve finansal piyasalar gibi önemli organları hedef almaktadır. Bilindiği gibi tüm dünyada uluslararası siber güvenlik tehditleri ve saldırıları gün geçtikçe artarak ülkeler arasında gelecekteki siber savaşlarda belirleyici bir silah haline gelmektedir. Kuşkusuz ki, Afganistan da bu tür siber silahların ve siber saldırıların bir istisnası değildir (Habib, 2018).

Afganistan'da genellikle siber saldırılara neden olan iki ana sebep vardır, birincisi coğrafi konumuna göre, bu ülke Çin, Pakistan ve Rusya'nın yanı sıra batıdan da güneydoğu ve kuzey yönleriyle İran ile sınırdır. Ayrıca, bu ülkenin orta doğu ülkelerine

stratejik konumu bulunmaktadır, bu nedenle ağırlıklı olarak Afganistan'ın coğrafi konumu ve orta doğu ülkeleri ile sınır olması ister istemez Afganistan'ı siber savaş alanına sürüklemektedir. İkincisi ise iç zorluklar ve çatışmalardır, Afganistan'ın iç savaşlarından dolayı Afgan hükümeti henüz siber saldırılara karşı yeterli bir siber savunmaya sahip olmamakla berber siber güvenlik alalında diğer gelişmiş ülkelere göre oldukça zayıf ve savunmasızdır. 16 Aralık 2014 yılında Çinli hacker grubu tarafından Afganistan'ın İletişim ve Bilgi Teknolojilerine (MCIT) siber saldırı gerçekleştirilmiştir bu saldırıdan MCIT oldukça yetkilenmiş ve büyük miktarda zarar görmüştür. Öte yandan, El Kaide ve Taliban gibi köktendinci radikal gruplar, tüm dünyaya ve özelikle Afganistan'da yayılmış durumdadır. El Kaide Afganistan'ın geçmişinden şu anki durumuna kadar büyük rol oynamıştır; 5 Mart 2012'de, bir hacker grubu El Kaide'nin desteğini arkasına alarak Afganistan'ın ulusal güvenlik konseyinin web sitesine saldırmıştır. Hackerler daha sonra ele geçirdikleri bu siteye El Kaide rehberi Usama bin Ladin resmini yayınlamıştır. Bunlara ek olarak, 2016'nın başlarında yine bir grup korsanlar Afganistanlı yöneticileri Irak ve Şam İslam Devletlerinin (IŞİD) maddi yardımları ile suçlayarak Afganistan'ın ulusal güvenlik konseyine saldırı düzenlemiştir, özellikle Afganistan resmi web sitelerine yapılan bu kasıtlı siber saldırılar, web sitelere ve alt yapılara ciddi zararlar vermiştir, aslında, bu hackerların amacı sadece devletin finansal varlıklarını hedeflememiş, aynı zamanda, uluslararası birlikler veya Kuzey Atlantik Antlaşması Örgütü (North Atlantic Treaty Organization: NATO) katılımcıları kendi çıkarları için 2001'deki Amerikan işgalinden sonra Afganistan'da çalışmaya başlamıştır, bu siber saldırılar bu birliktelikleri de hedef almaktadır. Örneğin 23 Eylül 2016'da Afganistan'da kaybolan Alman askerlerinin yerini tespit etmek için bir grup Alman korsanları Afganistan'daki Mobil İletişim Küresel Sistemi (Global Systemfor Mobile Communications: GSM) şebekelerini hacklemeye çalışmıştır. Afganistan'ın GMS şebekelerine yapılan bu saldır devlet sistemlerinin yanı sıra özel sektörleri de hedef almıştır (Habib, 2018).

5.3.1. GOV.AF Web Sitelerine Yapılan Siber Saldırılar

Afganistan Ulusal Veri Merkezi'nin (Afghanistan National Data Center: ANDC) Web Sitesi ve E-posta Sistemleri rutin olarak izlenirken bu sistemler 19 Aralık 2014'te kaynağı tam olarak beli olmayan bir siber saldırıya uğramıştır. Yetkililer verilerin

bazılarını değiştirildiğini fark etmiş, ancak hemen ne olduğunu anlayamamışlardır. Konu daha ayrıntılı olarak incelendiğinde, 20 Aralık 2014'te Merkezi Veri Ağı (Centralize Data Network: CDN) güvenliğinin ihlal edildiği fark edilmiş ve bunu fırsat bilen saldırganlar, bir şekilde sızmayı başarmıştır. Ancak, 20 Aralık 2014'te web sitelerinin verileri üzerinde hiçbir etkisi olmadan 24 saat içinde tehdit aşılmıştır. Afgan hükümet yetkilileri bu saldırının amacının, .GOV.AF web sitelerini harici saldırılar için proxy olarak kullanmak olduğunu belirterek Bilgisayar korsanının ANDC tarafından barındırılan web sitelerine nasıl sızdığını araştırıyoruz şeklinde bir açıklama yaparak şunları dile getirmiştir. Son 4-5 yıl içinde, ANDC çeşitli başarısız siber saldırılara uğramıştır ve sistemlere zarar vermeden bunların üstesinden gelinmiştir. Çin kaynaklı olduğu düşünülen, .GOV.AF web sitelerine yapılan bu siber saldırıların bağlantısının siyasi bir nedeni olabileceğine inanılmaktadır. Dünya genelinde her gün çeşitli siber saldırı girişimleri gerçekleştirilmektedir. Bu nedenle, bu küresel bir konudur ve yapabileceğimiz en iyi şey uygun önlemleri almak ve tehditleri en aza indirmektir. Hiç kimse bu saldırıların riskini tamamen ortadan kaldıramaz, yapabileceğimiz tek şey kendimizi korumak ve bu tür saldırıların etkilerini azaltmak için güvenliğimizi güçlendirmektir (MCIT, 2014).

5.4. Mevcut Siber Stratejiler

Siber güce sahip olmayan ve siber alanlarda zayıf olan Afganistan gibi ülkeler için, siber savaşlar, iç olaylar ve yeterli siber güce sahip ülkeler, mevcut siber alanın en büyük risk ve zorlukları olmakla beraber gelecekteki en büyük siber tehditlerdir. Afganistan hükümeti siber güvenlik üzerinde çalışmakta ve gelecekteki siber alanın güvenliği ve emniyeti için bir siber savunma ekibi kurmaktadır. Afgan Telekomünikasyon Düzenleme Kurumu (Afghan Telecommunications Regulatory Authority: ATRA), Afganistan MCIT ile birlikte çalışmakta ve mevcut teknolojik projelerin yaygınlaşma ve dijitalleşme alanındaki iyileştirme kriterleri konusunda stratejiler geliştirmiş ve uygulanması için yoğunlaşmaktadırlar (Habib, 2018).

2014 yılında yayınlanan “Afganistan Ulusal Siber Güvenlik Stratejisi”, MCIT, ISSD ve ulusal parlamento gibi birçok devlet kurumunun işbirliği ve anlaşmasıyla açıklanmış, özellikle siber suçlarla bağlantılı yasa ve politikaları ve eylemleri belirlenerek yürütüle konulmuştur. Bilgi güvencesi, bilgi sistemleri ve IT altyapı

denetimleri, güvenlik açığı değerlendirmesi, CII risk yönetimi, iş sürekliliği, SDLC ile Uygulama güvenliğinin sağlanması ve en iyi uygulamalar ve IT altyapılarının testi " 2014 yılında yayınlanan "Afganistan Ulusal Siber Güvenlik Stratejisine göre doğrudan yürütülmüştür (Habib, 2018).

Devlet kurumları arasında siber alanla ilgili düzenlenen konferanslar, burada belirtilen, yasa taslağı, e-İşlem taslağı ve e-İmza yasal prosedürleri taslağı, Ulusal Siber/Bilgi güvenliği Politikası taslağı, Afgan hükümetinin siber alandaki önemli önceliklerden biridir. Bilişim güvenliği, Güvenlik Duvarı Politikaları, Bilgisayar suç olayı müdahale prosedürünün taslağı, IT güvenlik eğitimi müfredatının/programının ve Çocuk Çevrimiçi Koruma Politikasının taslağı Adalet Bakanlığı ve diğer devlet kurumlarıyla işbirliği yaparak iyimser sonuçlar getirmiştir (Habib, 2018).

5.5. Güncel Siber Prosedürler ve Politikalarımız

Siber tehdit ve savunmasızlıkların değerlendirilmesi bir ülkedeki güvenlik otoritelerinin temel kaygılarından biri olduğu açık ve nettir, değerlendirmelerin teknik olarak uygulanması ya da stratejik olarak yapılması gerekmektedir. Risk değerlendirme konusu son derece önemli bir konudur, çünkü çoğu durumda riskleri önemli ölçüde azaltmaya ya da düşük orandaki risklerin ve güvenlik açıklarını kapatmaya önemli katkılarda bulunabilmektedir. Ulusal ağ altyapısı ile ilgili tehditlerin, risklerin ve zayıf noktaların gösterimi, kritik ve kritik olmayan altyapı ve ulusal güvenlik sistemlerine kazara veya kasten yapılan siber saldırıları ortaya çıkaran riskleri analiz etmek, yönetmek ve çözmek için bir yöntemdir (Habib, 2018).

Buradaki temel hedeflerimiz, devlet kurumları tarafından tanımlanan Afganistan'ın mevcut siber güvenlik seviyesini belirli bir çerçevede değerlendirmek, mevcut altyapımıza karşı yapılan siber saldırılarla ilgili siber güvenliği değerlendirmek ve gelecekte kritik ve kritik olmayan ağ temellerimizi açıkça ifade etmektir. Bazı verilere, güvenlik planları ile ilişkin bilgilere ve kuruluşların siber stratejileri ile ilgili önemli bilgilere ulaşmanın nerdeyse imkânsız olduğu açıktır. Çünkü hem devlet hem de özel kuruluşlar kamuya bu tür bilgileri asla sunmaz ve kimsenin ulaşmasını asla istemezler, ancak burada, mevcut ağ altyapısı, bilgi güvenliği zorlukları ve gelecekteki siber tehditler ile ilgili kamuya açık belgeler ve bilgiler halka açık veri ve bilgi analizi ve değerlendirmeleri olabilmektedir (Habib, 2018).

Dijital güvenlik veya yazılım dünyasından bahsederken, gelecekteki kamu, özel sektörler, ulusal endüstriler ve askeri güçlerin hareketine kadar her yönden finansal varlıkların veri güvenliği siber alanlarda önemli olaylardan biridir. Kötü niyetli internet kullanıcıları kendi siyasi ve ekonomi hedefleri ve çıkarları için veri ve bilgileri basit yöntemler ve araçlar kullanarak çalabilmektedirler, bu zararlı siber saldırıların ve veri kaybının siyasi, ekonomi, ticari hatta halkın üzerinde ciddi olumsuzluklar ve etkiler oluşturduğu aşikârdır. Bu olaylar gösteriyor ki tüm dünyada olduğu gibi Afganistan'da komşu ülkeleriyle, Rusya, Çin ve hatta uluslararası birlikler de dâhil olmak üzere siber savaş alanına girdiği açıkça görülmektedir. Özellikle TUTAP[1], TAPI[2] ve CASA-1000[3]gibi ekonomik projelerin uygulanmasından sonra bu ülke sık, sık kısa ve uzun vadeli siber saldırılara maruz kalmaya başlamıştır. Bu projelerin uygulanmasının Afganistan'ın ekonomik ve endüstriyel tesislerinin geleceğinde hayati bir rol oynadığı gibi Afganistan'ın tüm komşu ülkeleri için Çin ve Rusya gibi ülkelere de önemli bir finansal fayda sağlamaktadır (Habib, 2018).

Bu projelerin tamamlanması ve uygulanması, Afganistan'ın içindeki temel altyapıları iyileştirmekte ve bu ülkeyi kendi ayakları üzerinde durabilmesi için bazı önemli adımlar atmasına imkânlar sağlamaktadır. Bu nedenle, Afganistan'da yıllardır çeşitli rekabet içinde yer alan ülkeler, elbette ki bu durumdan memnun değiller ve Afganistan'ın gelişmesini ve bağımsız bir ülke olmasını istememektedirler. Böyle bir durumda, bu projelerin siber güvenliği gelecekteki siber saldırılara karşı korunamaz ve bu projelerde rekabet eden ülkeler hiçbir siber saldırıdan kaçınamayacaklardır. Bir taraftan, bu tür ekonomik projelerin güvenliği doğrudan kamuya açık internetin emniyetine ve güvenliğine bağlanmaktadır. Siber güvenlik teorileri ile ilgili olarak, bu kritik ağ bağlantılı sistemlerin altyapıya kamuya açık internetten erişilmesi genellikle basit ve kolaydır. Bununla birlikte, Afgan hükümetinin elindeki sahip olduğu büyük ticari ve ekonomik projelerin ticarileştirilmesi ve metalaştırılması için, hizmetlerin erişilebilirliğini ve kalitesini artırmak amacıyla en azından kamuya açık güvenli bir

[1] Türkmenistan-Uzbekistan-Tajikistan-Afganistan-Pakistan hattında oluşan elektrik boru hattıdır.

[2]Türkmenistan-Afganistan-Pakistan-Hindistan hattında oluşan bir doğal gaz boru hattıdır.

[3]Orta Asya-Güney Asya enerji projesi, bu tez yazıldığında yapım aşamasında olan 1.16 milyar dolarlık bir projedir ve Kırgızistan ve Tacikistan'dan Afganistan ve Pakistan'a fazla hidroelektrik ihracatı sağlayacaktır.

altyapıya sahip olmalıdır, ama bu siber tehditlerin ve saldırıların birçok nedenden dolayı kaçınılmaz olduğu ve siber savaşların ve saldırıların her geçen gün artmakta olduğu ve ülkeyi tehdit altına aldığı unutulmamalıdır. Bu tür sistemlere siber saldırıların yapılması ve tehditlerin ve zayıf noktaların bulunması sistemleri hizmet vermekten aciz kalmasına ya da tamamen hizmet dışı bırakılmasına, sebebiyet vermektedir. Bu nedenle, öncelikle bu tarz sistemlerin siber alanlardaki güvenliği ve siber savunma sistemleri yetkili ve şeffaf bir şekilde sağlanmalı ve uygulanmalıdır. Eğer sağlanamazsa bu tür sistemlere siber saldırılar, altyapı bileşenlerini anormal koşullara sokarak ciddi zararlara yol açabilmektedir. Afganistan'daki ekonomik projelerdeki mevcut rekabet nedeniyle, siber saldırılar, Afganistan'ın bölgesel ve uluslararası ilişkilerinin geleceğinde ciddi bir sorun yaratacak ve bu ülkenin gelişmesine ve güçlenmesine engel olacaktır. Diğer taraftan mevcut siyasi ve ekonomik duruma NATO, Çin, Rusya ve komşu ülkelerin katılımı da gelecekteki siber sorunların ana nedenlerinden bazılarıdır (Habib, 2018).

Sonuç olarak, hükümet kuruluşları, siber suçlar ve siber saldırıları önleme yasaları ve ilkeleri sorumlu olan adalet bakanlığıyla işbirliği yaparak, siber saldırı önleme ve siber savunma konusunda siber prosedür ve politikaları uygulayarak iletişim ve bilgi teknolojisi bakanlığını desteklemektedir. Aslında, saldırgan siber saldırılarda MCIT'nin bazı kilit performanslarını daha önce belirttiğimiz gibi, ağ üzerinden, bu devlet kuruluşu siber saldırıların önlenmesinde de önemli bir rol oynamaktadır. MCIT ve adalet bakanlığının yayınladığı aylık ve yıllık dergilere göre, siber saldırı prosedürü ve politikası aşağıdaki gibidir (Habib, 2018).

5.5.1. Önleme Prosedürleri Ve Politikaları

Bu başlık altında genel olarak, siber saldırı önlemleri, siber saldırı önleme tanımları ve siber saldırı önleme etkinlikleri ile ilgili konulara değinilecektir, özellikle Afganistan MCIT'nin, siber saldırıların önlenmesini doğrudan engellemek için MCIT güvenlik müdürlüğünün ana sorumluluklarından bahsedilecektir, bu sorumlukları, genel olarak aşağıdaki gibi sıralayabiliriz (Habib, 2018).

1. Kamu ve özel sektörlere yönelik yapılan, siber saldırılara karşı siber savunma, ağ altyapısı uygulama prosedürleri, tüm ağlar üzerinde siber güvenlik politikalarının uygulanması ve siber saldırıların neden olduğunun risk değerlendirmeleri durumunda ağ güvenliği ve belirli kural ve politikaların gerçekleştirilmesi.

2. Farkındalık açısından, devlet kurumu çalışanlarına siber güvenlik eğitimi vermek, siber güvenlik uzmanları yetiştirmek, gerekli teknolojileri sağlamak ve uygulamak.

3. Devlet kurumlarının yanı sıra, ticari alanları, kişisel bilgi hırsızlığını, güvenlik stratejilerini koordine etmek, siber saldırılar konusunda kamuoyunu bilinçlendirmek ve herhangi bir saldırıya karşı gerekli politikaları uygulamak.

4. Bilgi sistemlerinin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin sağlanması için ülkedeki kritik bilgi altyapılarının ölçülendirmek.

Aslında, siber alanların güvenliğine göre, önleme, ağ altyapıları üzerinde her türlü siber saldırılara karşı standart bir yöntemdir, ne olursa olsun, bu tür ağlar Yerel Ağ Bağlantısı (Local Area Network: LAN), Geniş Alan Ağı (Wide Area Network: WAN) ve internet üzerinden yapılandırılır veya aynı şekilde hava ara yüzü ağı altında kurulur, GSM haberleşmesi kablosuz geniş bant şebekesi ve uydu yayın servisleri tarafından sunulmaktadır (Habib, 2018).

Siber saldırılar yalnızca fiziksel ağ altyapısı üzerinde etki etmez, aynı zamanda kötü amaçlı komut, dosyaların ve kodların tüm ağlarda çalıştırarak birden fazla seçeneğe ve olumsuz etkilere sahiptir. Veri Kaybı Önleme Politikalarına (Data Loss Preventions Policies: DLP) göre, bir kuruluş siber saldırılara karşı iyi bir önleme politikası yönetiyor ve düzenliyorsa, siber saldırıları başarıyla önleyebilir ve sistemlerini koruyabilir, bu siber saldırıların önlenmesi, kuruluşların kayda değer ve önemli performanslarından biri sayılabilir, nadiren de olsa, bu tür kuruluşlar, önceden tanımlanmış veri sızıntısına göre filtrelenen kötü amaçlı komut dosyalar ve kodlar nedeniyle ağ üzerindeki kötü amaçlı saldırılardan etkilenmekte ve önleme politikaları zarar görebilmektedir (Habib, 2018).

5.5.2. Kovuşturma Prosedürleri ve Politikaları

Bu bölümde, özellikle resmi dergilere ve Afganistan cumhurbaşkanı ve bakanlık yasama organı tarafından yeni onaylanan Afganistan adalet bakanlığının resmi gazetesine dayanan siber saldırıların bazı önemli kovuşturma kuralları ve politikaları yer almaktadır. Adalet Bakanlığı ve özellikle MCIT ile işbirliği yaparak genel yasama idaresi, siber saldırıların yasama yasalarından ve kovuşturma politikalarından

sorumludur. Ayrıca, yasama otoritelerinin kendi siber suç ve siber saldırı tanımları da vardır. Bu, kovuşturma politikası belgesi 15 Mayıs 2017 tarihinde onaylanmış ve yeni yayınlanmış olduğuna dikkat edilmelidir. Genel olarak, bu kurallar ve politikalar, iç ağ altyapısını, bilgi ve iletişim sistemlerini tahrip etmeye çalışan siber suçluların iç kovuşturması için yeterlidir. Ancak, harici siber tehditler ve siber savaş durumunda, yetkili kişiler ve kuruluşlar sürekli olarak profesyonel siber saldırıları önleme ekiplerine ve yeterli olanaklara ihtiyaç duyulmaktadır (Habib, 2018).

5.6. Mevcut Siber Tehditler ve Güvenlik Açıkları

Siber tehditler ve saldırılar son yıllarda yeni bir fenomen olarak ortaya çıkmaktadır, bilgi teknolojileri ve ağ iletişim dünyasının evrimi ile tehdit ve risk dünya çapında geniş bir internet ağı üzerinden meydana gelmektedir. Genel olarak, bilgisayar korsanlarının ve saldırganların, sistemleri ve ağ alt yapılarını hedef almak için kullandıkları birçok tehdit ve farklı yöntemler vardır, ciddi bir şekilde gerçekleşen ve güvenlik önlemlerine engel olan popüler güvenlik açıkları ve tehditler bulunmaktadır (Habib, 2018).

Afganistan'ın siber alanının mevcut durumuna bakıldığında yapılan araştırma ve soruşturmalara göre, bu ülke güçlü milletler ve komşu ülkeler tarafından yönetilen siber saldırılardan önemli ölçüde etkilenmektedir. Komşu ülkelerin müdahalesi, uluslararası birlikteliklerin ve bölgesel ulusların ekonomik, siyasi ve endüstriyel rekabeti, Afganistan'ı olumsuz bir rekabet pazarına dönüştürmüş ve bu olumsuz rekabetin sanal alanın siber alanı ve güvenliği üzerinde doğrudan etkileri olmuştur. Bununla birlikte, siyaset ve büyük ekonomi projelerindeki rekabet, Afganistan'daki siber alanlara yönelik saldırıların son zamanlarda artığını göstermektedir, Afganistan'da bulunan birçok uluslararası ülke, Afganistan'ın komşu ülkeleri ve iç çatışmaları arasındaki bu rekabet mevcut siber tehditlerden bazılarıdır. Bunlara ek olarak Afganistan'ı endişelendiren iç ve dış tehditler olmak üzere iki tür temel siber tehdit bulunmaktadır (Habib, 2018).

5.6.1. Dış Tehditler

Siber saldırılar, ülke dışından, hackerler ve bilgisayar korsanları tarafından, yönetilmekte ve hasımın sistemlerine zarar vermektedir. Böyle bir yöntemde, resmi bir organizatör saldırgan tarafından ülke dışında örgütlenen önemli siber saldırganlar, bu

organizatörlerin yetkili araçları vardır ve diğer ülkelerin ağ altyapısı ve bilgi sistemlerine kasıtlı siber saldırılar gerçekleştirebilecek yetenektedirler. Bu tarz saldırılar kamu çevrimiçi hizmetlerini veya özel sektörleri ve sanayi şirketlerini hedefler. Sosyal veya politik olarak motive edilen bu tür siber saldırılarda, öncelikle internet üzerinden gerçekleştirilen siber saldırılar, saldırgan grupları belirli bir hedefi çökertmek ve kritik alt yapılara yönelik siber saldırılar için zaman ve yeterli bütçe ayırmakta ve daha sonra siber saldırı gerçekleştirmektedirler. Dış saldırganların hedeflerindeki kilit faktörler aşağıda listelendiği gibidir (Habib, 2018).

1. Güncel yazılımların hata noktasını hedefleyen saldırganlar; bu tür saldırganlar kurbanların sunucularında veya sistemlerinde var olan güvenlik boşluklarını ve kritik yazılım hatalarını bularak sistemlere zarar vermeyi amaçlar.

2. Enerji şebekesi sistemleri; güç şebekesi sistemlerini veya enerji istasyonlarını hedefleyen saldırılardır, bu saldırılar dış saldırganlar tarafından hedeflenen kritik siber saldırılardan biri olarak kabul edilir, örneğin, petrol istasyonlarına yapılan saldırılar.

3. Ağ altyapıları ve iletişim sistemlerine yapılan siber saldırılar; aslında ağ altyapısı, siber saldırılardan etkilenen popüler sistemlerden biridir, bu yöntemde bilgisayar korsanları, sistem alt yapılarını yıkmak ve hizmet dışı bırakmak için ağın temelini hedeflemeye çalışmaktadır.

4. Ekonomik ve çevrimiçi hizmet; saldırgan çalışmayı durdurmak ve ya tamamen ortadan kaldırmak için çevrimiçi hizmetleri hedeflemeye çalışır, saldırılarını etkin bir şekilde koordine eder ve veri sızıntısı, çalınan veriler ve finansal faydalara yönelik kötü amaçlı yazılımlar geliştirir ve uygular.

5. Veri tabanlarını hedef alan saldırılar; bilgi hırsızlığı, ekonomik zarar ve hassas belge ve kimlik hırsızlığını içermektedir (Habib, 2018).

5.6.2. İç Tehditler

Dâhili siber tehditler, genel olarak tehdit, sistemlerin ve kaynakların arızalanmalarına yönelik bir yaklaşımdır, özellikle iç siber güvenlik hatalarının ve içeriden ilişkili güvenlik risklerini tanımlanmaması ve ele alınmaması bu tarz tehditlere sebep olmaktadır. Dâhili problemler ve savunmasızlıklar harici problemler ve savunmasızlıklardan daha tehlikeli ve daha risklidir, çünkü iç altyapı üzerindeki

verilerin yok edilmesi, ekonomik, eğitim kurumu, kamu ve özel sektörlerin günlük faaliyetlerini büyük ölçüde etkilemekte ve büyük sorunlar ortaya çıkarmaktadır. Afganistan'da siber saldırılara neden olan temel iç tehditler aşağıda belirtilmiştir (Habib, 2018).

1. Yasadışı Abone Kimlik Modülü Kartlarının (Subscriber Identity Module: SIM) Satışı: Afganistan'da telekomünikasyon hizmetleri, internet ve text mesajlaşma hizmetleri sunan uluslararası ve ulusal şirketler, hükümet izni olmadan SIM kartlarını üretip satmaktadırlar, bu hatlar ucuz ve kolayca elde edildiği için neredeyse tüm Afgan halkı bu SIM kartları kullanarak internete bağlanmaktadır. Çoğu zaman, devletin veya telekomünikasyon şirketlerinin bu hatları kayda geçirmediği için çok rahat tehdit ve risk üretebilmektedir. Bu süreç genel olarak siber ortamda risk ve tehditlere neden olabilmekte ve ciddi sonuçlar doğurabilmektedir. Örneğin, 25 Kasım 2016'da Afganistan Ulusal Güvenlik Müdürlüğü'nün web sitesine karşı yapılan siber saldırı bir grup hacker tarafından içeriden gerçekleştirilmiştir. Bu durumda, eğer hükümet tüm internet kullanıcılarını kayıt altında alıp kontrol ederse bu tür siber saldırılar def edilebilir (Habib, 2018).

2. Güncel olmayan yazılımların satışı: Eski ve güncel olmayan yazılım satışları, dünyanın her yerinde kontrolü hiç kolay olmadığı gibi Afganistan'da da bunun önüne geçebilmiş değiliz bu da büyük sorunlar yaratmaktadır. Ancak diğer ülkelerde yazılım ürünleri ve lisansları devletin veya resmi yetkili bir kurumun kontrolü altındadır, Afganistan'da ise devlet henüz yasa dışı ve güncel olmayan yazılımların satışını kontrol altında alabilmiş değildir. Aslında, ticari ve ticari olmayan yazılımların yasadışı kullanımı tamamen yasaktır, ancak ne yazık ki, Afganistan'da, hükümet kaçak ve güncel olmayan yazılımların satışını engelleyememektedir ve hatta bazı resmi devlet kurumları bu tür yazılımların satışına destek olmakta ve bu yazılımları kullanmaktadır. Afganistan'ın komşu ülkeleri, özellikle de İran ve Pakistan, Microsoft yazılım ürünlerini kırarak, kötü amaçlı kodları yazılım kaynak kodlarına dâhil edip Afganistan'a ihraç etmektedirler (Habib, 2018).

3. Yasadışı internet kafelerinin sağladıkları internet hizmetleri: Ülkenin dört bir yanındaki internet kafelerinde milyarlarca bilgisayar ve elektronik cihaz internete bağlanmakta ve özellikle Afganistan'ın başkenti Kabil'de bu sayı her geçen gün

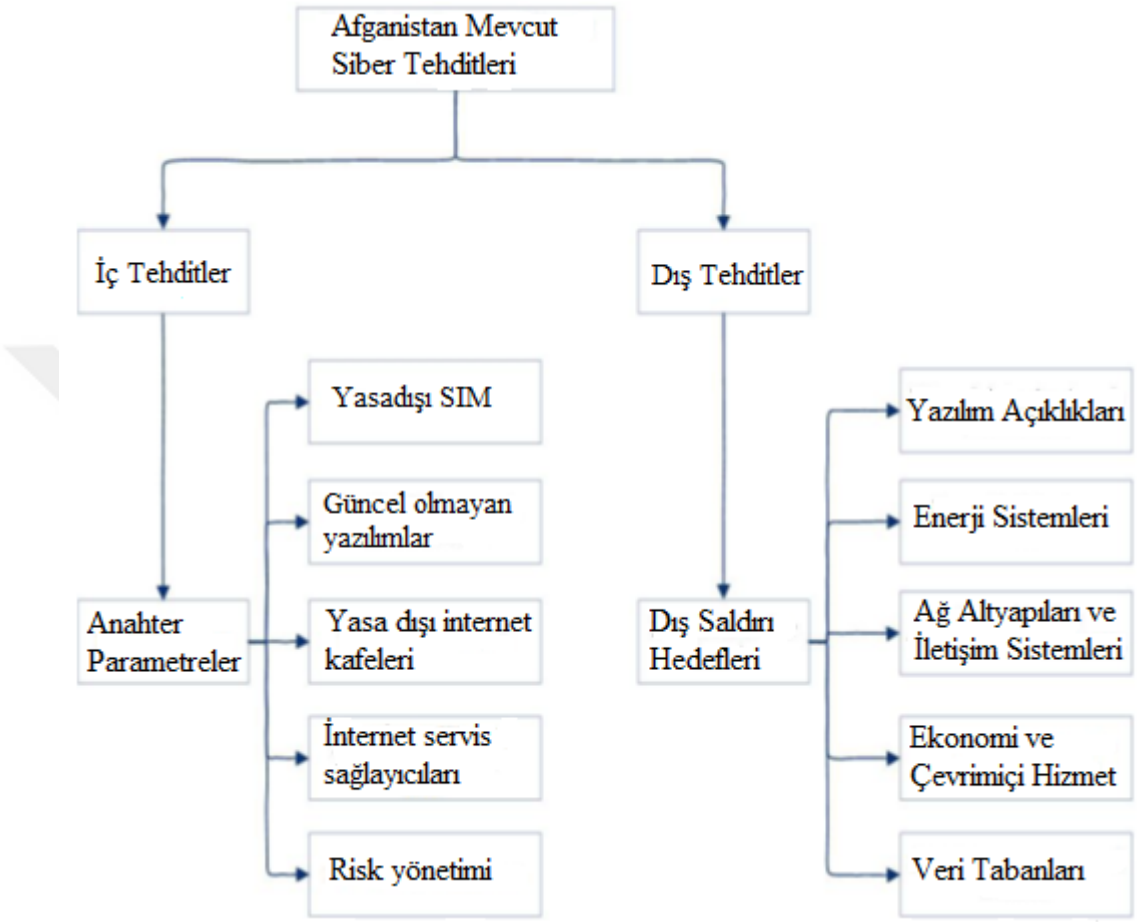
artmaktadır. Basit güvenlik sistemleriyle korunan bu internet kafeleri, büyük güvenlik sorunları yaşatmaktadır ve ayrıca güvenliği önceden tanımlanmış bir koruma politikası kapsamında değillerdir. Kimliği bilinmeyen saldırganlar bu internet kafelerini kullanarak içeriden saldırdıkları için devlet ve güvenlik ekibi, bunları kolayca izleyememekte ve tespit edememektedir, kafe net internet hizmetlerini kullanan bir saldırganı tespit etmek nerdeyse imkânsızdır. Bunun önüne geçmek için, internet kafelerinin güvenliği hükümet tarafından sağlanmalı veya resmi bir yetkili tarafından güvenlik ekibi fiziksel koruma, erişim kontrolleri, şifreleme, yedeklemeler ve virüs koruması için gereksinimleri içermelidir. Ayrıca, kafe ağları paylaşılan veya mobil cihazları kurumsal ağlara bağlama ve halka açık yerlerde kullanımları konusunda yasalar ve kurallar getirilmelidir (Habib, 2018).

4. Telekomünikasyon şirketleri ve internet servis sağlayıcılarının güvenli olmayan anlaşmaları: 20 milyondan fazla Afganistan nüfusu GSM hizmetlerini (Sesli iletim, Kısa Mesaj Servisi ve İnternet 3G ve 4G) kullanmaktadır. Hükümet, karaborsalardaki telekomünikasyon ürünlerini kontrol edemez ve hükümetin yetersizliği nedeniyle, genellikle telekomünikasyon şirketleri resmi bir devlet kurumuna kayıt olmadan SIMcard, 3G-4G Dongles ve ortamları sağlamaktadır (Habib, 2018).

5. Risk yönetiminin sorumluluğu: Devlet kurumları için ortaya çıkan en önemli sorunlardan biridir, ancak bu sorumluluğu alan kurumların birçoğu siber tehdit ve siber saldırı riskleri ile hiç ilgilenmemektedir. Yetersiz risk değerlendirmeleri özellikle yanlış bir güvenlik düşüncesi verdiğinden tehlikeli olabilir bu tarz düşünceler yıkıcı tahrip edici sonuçlara yol açabilmektedir (Habib, 2018).

Sonuç olarak, mevcut ve gelecekteki siber alan üzerinde kritik zorluklar olabilecek kritik konular hakkında endişe duyulmakla birlikte, bu sorunların çözümleri ele alınmamaktadır, çünkü mevcut siber durumun ve gelecekteki stratejinin ayrıntılarıyla analizi ve değerlendirilmesi için yeterli zaman ve incelemeye ihtiyacı vardır. Örneğin, hükümet ve GSM sistemleri tarafından dağıtılan frekans spektrumlarının güvenliğinin değerlendirilmesi, temel olarak ses ve verinin GSM şebekeleri üzerinden iletilmesi, veri ve sesin standart şifreleme yöntemlerinden biri ile şifrelenmesine rağmen, yine de bu şifreleme yöntemi güvenli değildir ve GSM iletimi yeni ve modern teknoloji ile kolayca tehlikeye girebilmektedir. Siber güvenlik

stratejileri açısından, her iki durumda da, (harici siber saldırılar veya dâhili siber saldırılar durumunda), mağdurlarının, ulusal güvenlik kurumları siber saldırıları savunmaktan, tanımaktan ve caydırmaktan sorumludur (Habib, 2018). Siber tehditlere ve veri sızıntısına neden olan genel sorunlar aşağıdaki şekil 5.1'de gösterilmiştir.



Şekil 5.1. Siber saldırılara ve veri sızıntısına neden olan tehditler (Habib, 2018).

5.7. Ulusal Siber Güvenliğimizle İlgili Önerilen Stratejiler

Bu stratejiler, ulusal güvenliğimizi kapsamlı bir şekilde düzenlemek, planlamak, hazırlamak ve yönetmek için, tüm varlıklarımızla (finansal, kültürel, tarımsal, hayati ve nihayet tüm değerlendirmelerle) bağlantılı olarak siber güvenliğimizi ilgilendirmektedir, ayrıca, toplumumuzu, çevremizi, ekonomimizi tüm yatırımlarımızı hatta ülkemizi iyi tanımlanmış bir ulusal güvenlik stratejisi ile kurtarabiliriz. Bu sadece siber güvenlik için geçerli değildir, iyi tanımlanmış bir strateji halkın tüm yaşamını olumlu yönlerde etkilemekte ve güven vermektedir, bu stratejiler genel olarak farklı ekosistem ortamlarının geniş bir alanına ve özel olarak siber alanın güvenliğine şeffaf ve dikkat çekici bir şekilde dâhil edilebilmelidir. Günümüzde siber zorluklar, tehditler ve

saldırıların artmasının nedenlerinden biri de iyi tanımlanmış siber planların ve stratejilerin bulunmamasıdır (Habib, 2018).

Ulusal siber güvenlik prosedürleri tarzında, bir strateji sadece sanal iletişim ile sınırlı olmayıp, benzer şekilde hükümetin ve birçok özel sektörlerin çalışması, devlet güvenliği ve siber ekiplerin iç tutarlılığı, siber alan ve siber suçlar, siber casusluk ve siber farkındalık gibi birçok alan bu stratejiye dâhil edilebilir. Bir stratejinin iki tarafı vardır, biri genellikle üst yönetim yetkilileri tarafından belirtilen bir toplumun veya bir ülkenin gelişimi ile ilgili planları ve diğer ise teknik olarak yoğunlaşmaktır (Habib, 2018).

Ulusal siber güvenlik açısından ve uluslararası kuruluşun siber alan gizliliği göz önüne alındığında, ülkeler geçmişte yasadışı eylemlerden kaçınmak ve siber alanlarını güvence altına almak için açıklayıcı politikalar uygulamışlardır, ancak bizim hükümet yönetimimiz 2001 yılından bu yana iç ve dış yasadışı faaliyetleri ve siber alanları kontrol edememiştir. Dünya Bankası ve diğer tedarikçilerin yıllık raporları göz önüne alınarak MCIT'in siber alanda kalkınma projelerine büyük yatırım yaptığı ortaya çıkmaktadır, ancak siber güvenlik ve güvenlik sorunlarının Afganistan'da yeni etkileşime girdiği ve tehditlerin gelecekte de devam edeceği gözükmektedir. Bazı ülkelerin siber alanlarını ve dâhili siber araçlar zorluklarını kontrol etmek için başvurduklarını belirten bazı önemli performanslar vardır. Bu bölümde, teknik veya teknik olmayan bir stratejiye değinilecektir, ancak her iki durumda da, hükümet ulusal güvenliği tehdit eden herhangi bir konuyu doğrudan dâhil etme sorumluluğuna sahiptir. Mevcut sanal iletişim ve bilgi sistemlerinin durumu açısından, Afganistan'ın mevcut ağ mimarisine, akademik dergilerine ve hükümetin üzerinde çalıştığı uluslararası projeleri destekleyerek teknolojik materyalleri önerisine göre bazı çözümler ve stratejiler bulunmaktadır (Habib, 2018).

5.7.1. Teknik Stratejiler

Akademik araştırmalar, teknik araç geliştirmeleri ve özellikle teknik araçların bütçeleri ve kaynakları göz önünde bulundurularak teknik olarak yapılandırılması gereken önerilebilecek ve çözülebilecek stratejilerdir. Ülkelerin farkında olmaması ve teknik kaynakların eksikliği nedeniyle çalınan, bozulan ve yok olan çok sayıda veri ve kişisel kimlik bilgileri vardır. Aslında, bilgi sistemlerinin teknik özellikleri, bilgisayar

korsanları ve dâhili saldırganlar tarafından hedef alınabilecek faktörlerden biridir. Bilgisayar korsanları, herhangi bir donanım veya yazılım ürününün veya elektrikli aletlerin talimatlarını okuyarak bu özelliklere kolayca erişebilir. Bu nedenle, iç teknisyenlerin iyi tanımlanmış bir politik stratejiler altında ulusal halkla etkileşimde bulunmaları ve hükümet sanal riskleri ve tehditleri azaltabilmeleri, mevcut stratejimizdeki siber tehditleri, gelecekteki siber alanlarımızı güvence altına almak ve güvenlik açıklarını kısıtlamak için temel teknik stratejileri anlamaya yardımcı olabilecek bu tarz stratejileri tanımlamak ve uygulamak gerekmektedir (Habib, 2018).

5.7.1.1. Elektronik Cihaz Üretimi

Dizüstü ve masaüstü bilgisayarlar, akıllı telefonlar, televizyonlar, akıllı kartlar ve elektrikli cipler gibi milli elektronik cihazların üretimi bir ülkenin güvende tutmak için en iyi çözümlerden bazılarıdır, ama maalesef, bizim ülkemiz Afganistan'ın mevcut durumuna göre bu nerdeyse imkânsızdır. Çünkü mali bütçeler ve insan kaynakları içeren mevcut kaynaklarımızın (Koordinatörler, yöneticiler, teknisyenler, uzmanlar vs.) yeterli değildir. Belki gelecekte bu sorunları çözerek diğer ülkeler gibi kendi elektrik cihazlarımız üretip ülkemizi daha güzel yerlere getirerek saldırılardan kuruya biliriz. Gelecek nesillerimizi siber saldırı ve siber tehditlerden kurumak için yeterli kaynak tahsis ederek yasal ve uygulanabilir bir strateji hazırlamamız gerekmektedir (Habib, 2018).

Eğer kendi elektrik cihazlarımızı üretemiyorsak, hükümetin sorumluluğu altında mevcut teknoloji pazarında ki, bu elektronik cihazlarını kontrol etmek, güvenli bir şekilde kullanımları için belirli ve güvenli türlerini ithal etmek gerekmektedir. Çünkü paylaşılan bu cihazlar, kişisel bilgisayarlar ve gömülü sistemlerde kurulan çipler gibi, basit bir kötü amaçlı yazılım veya kodlar yerleştirilerek güvenlik kolayca ihlal edilebilmektedir. Bu elektrikli çipler tüm gizli bilgilerin kopyalama yeteneğine sahiptir elektrik cihazlarına yerleştirilen bu çipler bilgileri kopyalayıp daha sonra onları organizatörlerine gönderir ve ulusal varlıkları ne kadar riske sokacağını kimse hayal bile edemez (Habib, 2018).

5.7.1.2. Hava Bantları ve Frekans Spektrumu

Öncelikle milletlerin güvenliği hükümetlerinin elindedir, bir milleti yöneticiler aralarına girmeden kurtarmak imkânsızdır ve hükümetin güvenliği doğrudan halkın güvenliğine bağlıdır. Afganistan'ın mevcut siber uzay durumu ile ilgili olarak, hükümetin yapabileceği şey, frekans spektrumu, anten bantları, radyo frekansları ve diğer hava iletişim sistemleri de dâhil olmak üzere tüm hava alanlarını kontrol etmektir. Benzer hava iletişim bantlarının yanlış kullanımı açısından birçok olası risk büyüyebilmektedir. Radyo, televizyon kanallarının güvenliği, uydu iletişim bantları, telekomünikasyon hizmetiyle ilgili kanal bantları ve daha da önemlisi, ulusal ordunun gizli stratejilerini kapsayan askeri gizli iletişim sistemlerinin hava spektrumuna bağımlı olmasıdır (Habib, 2018).

2002'den bu yana, hava frekansı spektrumları tarafından yasal veya yasadışı olarak kolaylaştırılan birçok ulusal ve uluslararası kuruluş bulunmaktadır. Afganistan'daki iç terörist gruplar için yaygın olarak bir iletişim sistemi olmakla birlikte, frekans spektrumunun kısıtlı aralığı ve kontrolü, hem sanal hem de gerçek dünyada ulusal güvenliğimizin korunması için son derece önem taşımaktadır, ancak Afganistan'ın mevcut teknoloji ve yönetim kuruluna göre bunlar kontrol etmek ve sürdürebilmek imkânsız görünmektedir (Habib, 2018).

5.7.1.3. Elektronik Cihazların Kullanım Politikası

Afganistan'a ithal edilen şüpheli elektronik cihazlar, yasadışı siber faaliyetlerin, tehditlerin ve siber saldırıların sonucu açısından etkili olabilmektedir. Her elektronik aygıtın benzersiz bir kimlik numarası vardır. Örneğin: Akıllı telefonlarda Uluslararası Mobil Cihaz Kimliği (International Mobile Equipment Identity: IMEI) veya seri numaraları ve kişisel bilgisayar için Medya Erişim Denetimi (Media Access Control: MAC) adresleri gibi. Bu açıdan, her şeyden önce, tüm elektronik cihazları yönetme ve düzenleme stratejisinin yasal hükümet yetkilileri tarafından onaylanması gerekmektedir (Habib, 2018).

Afganistan'da farklı alanlarda, özellikle sanayi şirketlerinde, ekonomik projelerinde, teknolojik projelerde ve diğer kalkınma işletmelerinde faaliyet göstermekte olan pek çok yabancı şirket vardır, bu yabancı şirketler, elektrikli cihazları için vergi veya herhangi bir ödeme yapmadan ücretsiz iletişim hizmetlerinden

yararlanmaktadır. Bu durum genel olarak, ulusal siber güvenliğimizi tehdit etmez belki ama şimdiye kadar terörist gruplar ve radikaller de hükümet ile ilişkisi olmadan bu tür hizmetlerden yararlanmaktadırlar. Bu nedenle, elektronik cihazların kullanım politikası siber alanımızdaki belirgin siber tehditleri ele alır ve azaltır. Afganistan'daki iç yasadışı siber faaliyetleri kontrol etmek ve azaltmak için bir başka olasılık, şu anda endüstriyel teknoloji pazarlarının çoğunun Internet Protokolü (Internet Protocol: IP) adresinin dördüncü sürümünü(Internet Protocol version4: IPv4) kullanması nedeniyle, mantıksal adresin IP standart dağılımıdır (Habib, 2018).

Uluslararası Standartlar Örgütü (International Organization for Standardization: ISO) tarafından sunulan iletişim modeli, özellikle Açık Sistemler Bağlantıları (Open Systems Interconnection: OSI), Afganistan'daki mevcut ağ iletişim sistemlerinde kullanılmaktadır. Hem temel hem de gelişmiş ağ güvenliğinde, İletim Denetimi Protokolü/Internet Protokolü (Transmission Control Protocol/Internet Protocol: TCP/IP) güvenliği, hizmet sunumu için iletimlerin önemli endişelerinden biridir, bu katmanları kesmek ve durdurmak için tasarlanmış Hizmet Reddi DOS saldırısı ve Adres Çözümleme Protokolü olan IP sahtekârlığı, Etki Alanı Adı Sistemleri de dâhil olmak üzere kimlik sahtekârlığı gibi birçok yöntem ve saldırı türü vardır (Habib, 2018).

Ancak, yeni cihazlar kaynak merkezi tarafından tanınıp yetkilendirildikten sonra bunların kamu hizmeti almalarına kullanılmasına izin verilir. İyi tanımlanmış bir teknik strateji, şimdiki ve gelecekteki varlıklarımızda kesinlikle faydalı olacaktır. Buna ek olarak, yakın gelecekte, özel sektör ve hükümet kurumları, özellikle de hükümetin iç büro uyumlulukları, bir kamuoyu savunması ve caydırıcılığı iyi tanımlanmış stratejiler hazırlamak için birbirleriyle işbirliği yapmazsa, büyük siber tehditler ve siber saldırılarla karşı karşıya kalacaklardır (Habib, 2018).

5.7.1.4. Standart Veri Şifreleme Politikasının Uygulanması

Şifreleme, emniyet açısından bir güvenlik seviyesidir, teknik şifreleme TCP / IP uygulama katmanında veya OSI modelinin uygulama, sunum ve oturum katmanına eşittir. Bu katmanlar bilgisayar korsanları ve saldırganlar tarafından kolayca ele geçirilebilir, çünkü bu katmanlardan okunabilir veriler iletilir ve işlem bu katmanlardaki bilgisayar korsanları tarafından kolayca elde edilebilir (Habib, 2018).

Pratik olarak, işlevsel verileri şifreleyerek, mevcut teknolojide yaygın olarak kullanılan iki tip klasik ve modern şifreleme algoritmaları ve prosedürlerini mümkün olduğunca güvence altına almak gerekmektedir. Klasik şifreleme, güvensizlik nedeniyle artık modern teknolojide pek kullanılmamaktadır ve şifrelenmiş verilerin kırılması veya şifrelerinin çözülmesi için de birçok yöntem bulunmaktadır. Modern şifreleme yöntemlerinde ise karmaşık algoritmalar söz konusu olduğundan, bu algoritmalarının şifresinin çözülmesi, bu tür karmaşık modern şifreleme sistemlerinin mevcut ve gelecekteki veri iletim sistemlerinde uygulanabildiği karmaşıklık nedeniyle oldukça zordur. Afganistan koordinasyon ve düzenleme, özel ve kamu şirketlerini, özellikle çevrimiçi bankacılık sistemlerinde ve çoğunlukla ağ üzerinden gizli veri aktarımı olan yüksek gizli iletişimde, sanal iletişim hizmetlerinde standart güvenli bir modern şifreleme sistemleri kullanmaya motive etmekten memnuniyet duyacaktır (Habib, 2018).

5.7.1.5. Yazılım Üretimi

Yazılımın güvenilirliği, uygulama ve yazılımla sistem esnekliği nedeniyle siber güvenliğin ilk ve önemli koşullarından biri yazılım üretimidir. Yazılımdaki riskler, hatalar, modern teknolojide, siber saldırılar açısından tartışılmaz sorunlar yarattığı bir gerçektir, tehditler ve saldırılar çevrimiçi ve çevrimdışı uygulamalardaki hatalar nedeniyle artar, teknik olarak içeriden ve dışarıdan gelen saldırılar ve yazılım veya uygulamalarda bulunan eksiklikler iyi bir yazılım üretimi ile çözülebilir (Habib, 2018).

Burada, yazılım ve uygulamanın işletim sistemleri, web tabanlı sistemler, Windows tabanlı bilgi sistemleri ve uygulamaları gibi siber alanda hizmet veren her türlü enstrümanı içerdiğini varsayarak, eğer bir ülke bu tür uygulamalar ve yazılımlar üretebiliyorsa, iç ve dış siber tehditleri ve siber saldırıları azaltması mümkün olabilmektedir. Ancak elektrik çiplerin üretimi gibi, mevcut durumda, özellikle eldeki imkânlarımız ve uzman eksikliğimizle işletim sisteminin ve yerli yazılımlarımızı üretmemiz oldukça zor ve nerdeyse imkânsızdır. Yapabileceğimiz ilk olarak, Linux ve Unix gibi açık kaynaklı işletim sistemlerinin özelleştirilmesi ve daha sonra sosyal ihtiyaçlarımıza yönelik bilgi sistemlerimizin dâhili üretimine derin bir önem verilmesidir (Habib, 2018).

Sonuç olarak, yazılım üretimi hem özel sektörde hem de kamu sektöründe birçok verimliliğe sahiptir. Hükümetimizin izleyebileceği ve sürdürebileceği geçerli ve kabul edilebilir strateji, mevcut sistemlerimizi doğru bir şekilde sürdürmek ve daha sonra yakın zamanda kısa bir süre içinde iç bilgi sistemleri ürünleri oluşturmak ve yürürlüğe koymak bu yazılımların bir parçasıdır. Ayrıca, kamu kuruluşlarının ve özel şirketlerin birlikte çalışabilirliği, sosyal hizmet amacıyla iş uygulamaları ve küçük yazılımlar geliştirerek bu alanda çalıştıkları ve iş birliği yapmaları, özellikle kritik bilgi sistemleri ile bağlantılı olarak çalışmalar çok önemlidir (Habib, 2018).

5.7.2. Politik ve Yasal Stratejiler

Teknik sistemin sorunları ve enstrümanları ile ilgili olarak, hükümet teknik sorunlarla ciddi bir endişe duysa bile, modern teknoloji ve bu alanlardaki yatırımlarda bu sorunlar kolayca çözülebilmektedir, bu stratejiler büyük bütçeler ayrılarak ve özel sektörlerle iş birliği yapılarak sağlanabilir. İnsani yetenekler ve uzman kişiler açısından özel sektörler, Afganistan'da hükümetten çok daha fazla yatırım yapmaktadırlar. Ancak, kritik sistemlere ve kritik altyapılara yönelik siber saldırılara karşı etkili bir uygulanabilir strateji tanımlamak ve yönetmek için siyasi düzenleme ve hükümet yönetimi dâhil edilmelidir. Her halükarda, yasal yönetim stratejisinin ve özel sektörlerle işbirliğinin iyi tanımlanmasıyla yetkili hükümet yönetim kurulunun yönetimi gelecekteki muhtemel siber tehditleri ve siber saldırıları hafifletebilecek ve azaltabilecek hatta engelleyebilecektir (Habib, 2018).

5.7.3. Karaborsa Kontrolü

Aslında, karaborsaların zorlukları sadece Afganistan'da değil, aynı zamanda tüm siber alanlarda ve fiziksel olarak etkili yasadışı faaliyetlerde bütün dünyada önemli zorluklara neden olmaktadır. Ancak, düzenli olarak diğer ülkeler: Çin, ABD, Avrupa Birliği, Rusya ve hatta komşu ülkelerimiz, özellikle ulusal güvenlikleri açısından en azından siber araçların ihracatını kontrol etmek ve önlemek için kaynak imkânlara sahiptirler, ama maalesef bizim ülkemiz bu imkânlara sahip değildir. Afganistan'a ithal edilen ve kontrol edilmeyen birçok siber araç türü vardır veya bunları karaborsalarda kontrol etmek imkânsızdır. Mevcut siber güvenlik durumlarıyla ilgili olarak, hükümetimiz siber tehdit ve siber saldırıları kısmen önleyebilmektedir, ancak kayıt dışı SIM kartlar, elektrikli cihazlar, güvenli olmayan halka açık internet ve kafe ağları,

günlük hayatımızı tehdit etmektedir. Profesyonel bir siber saldırı içeriden veya hackerler tarafından yahut bir ön saldırı planına sahip olmayan kişiler tarafından yapılamaz, karaborsadan satın alınan bir bilgisayar veya bir SIM kart, hackerler tarafından, kamu hizmetlerini veya internet web sayfalarını hedef seçerek zarar vermek için bir tehdit olabilmektedir. Bu tür tehditlerin önüne geçebilmek için kamu hizmetleri ve kurumları ve hatta sosyal veri merkezleri tarafından elektronik pasaport, elektronik kimlik numarası, elektronik sürücü belgesi, sağlık sigortası ve çevrimiçi bankacılık sunucuları gibi devlet hizmetlerini kaydetmek için bir veri merkezinin geliştirilmesi ve uygulanması gerekmektedir (Habib, 2018).

5.8. Siber Güvenlikle İlgili Gelecek Plan ve Çalışmalarımız

Bir ülkenin siber tehdit ve siber saldırılara maruz kalmaması için yaptığı çalışmalar gelecekteki plan ve programları bir yüksek lisans tezi çalışmasına sığabilecek kadar kısıtlı ve sınırlı değildir, karmaşık tartışmalı yönlere sahip ve karmaşık sanal dünyaya yayılmış durumdadır. Çünkü bu tür karmaşık şeylerin kesin bir incelemesi ve doğru bir değerlendirmesi, öncelikle tek bir kişinin yeteneği dışında olduğu bilinmelidir, şüphesiz hiç kimsenin böyle yetenekleri yoktur. Bu nedenle, Afganistan'ın ciddi siber tehdit sorunlarını, bu ülkede özellikle siber savaşlar ve siber teröristler olmak üzere tamamen yeni bir fenomen olarak değerlendirmek ve analiz etmek kesinlikle gereklidir. Bundan dolayı, bu hedeflere ulaşmak ve kabul edilebilir iddialarla başarılı bir sonuç araştırması elde etmek için daha fazla zamana ve imkâna ihtiyaç vardır, gelecekteki gerekli çalışmalar tam olarak ağ güvenliği ile ilgili araştırmalardır çünkü ağ altyapılarının riskleri kritik ve kritik olmayan ağ temellerini içermektedir. Uygulanabilir bir algoritma ve algoritmanın uygulanması ve önerilen teknik stratejilerin çoğunu yerine getirmek ve bilgi sistemlerinin geliştirilmesi için geniş bir araştırma ve analiz gerekmektedir. Siber güvenlik alanında Afganistan devleti gelecek için birçok çalışma yapmaktadır bunlardan bazıları aşağıdaki başlıklar altında verilmiştir. Bu çalışmalar sonucunda MCIT'in Teknoloji Projeleri dâhil olmakla beraber siber alanda pek çok önemli adımlar atılmıştır (Habib, 2018).

5.8.1. E-Devlet Hizmeti

Bu hizmet büyük ve önemli dijital projelerin bir parçası olarak elektrik hükümeti adına önemli dijitalleştirilmiş projelerin geliştirilmesini hedeflemektedir. MCIT, bu

projelerin uygulanmasıyla Katma Değer Hizmetleri (Value Added Services: VAS) sağlamaya çalışmaktadır. Aşağıda ortak olan bileşenler bu projenin uygulanması kapsamındadır.

a) Afgan elektronik ulusal kartının veya kimlik kartının dağıtımı,
b) E-devlet hizmetlerinin ülkenin her yerinde merkezlenmesi,
c) Hizmet sunumu ve birlikte çalışabilirlik web sitelerinin geliştirilmesi,
d) Kimlik kartları, Pasaportlar gibi belgelerin elektronikleştirilmesi,
e) Bir BİT merkezinin kurulması,
f) Ülke genelinde e-devlet uygulamasının geliştirilmesi,
g) BİT eğitiminin ve dijital okuryazarlığın geliştirilmesi.

Sürücü ehliyeti ve Ulusal Kimlik, Araç Tescili, Dijital İmza ve Biyometrik sistemleri, bu dijitalleşme ve geliştirme projeleri kapsamında yer alan ortak bileşenlerdir. Diğer ulusal ve uluslararası işbirliği ile Afganistan İletişim ve Bilgi Teknolojileri Bakanlığı kuruluşlar bu projenin uygulanmasına büyük yatırımlar yapmaktadır (Habib, 2018).

5.8.2. M-Devlet Hizmeti

Bu hizmet, verimlilik ve etkinliklerini artırmak için mobil telefon kullanarak devlet hizmetleri sağlamayı amaçlayan bir bileşendir. Bu dijitalleşme projesi, sonuç olarak dijital hizmetleri amaçlayan bileşenleri kapsamaktadır bu bileşenler şunlardır.

a) Mobil Hükümetin Etkinleştirilmesi,
b) Yenilikler İcat Etme Programı.

5.8.3. Posta Sektörü Modernizasyonu

Bu bileşen, erişim ve hizmet sunumunu iyileştirmek için posta sektörünü modernleştirmeyi amaçlamaktadır. Aşağıdaki unsurlar doğrudan iletilecektir.

a) Ülkenin dört bir yanındaki devlet kurumlarının posta hizmetlerinden sorumlu olan Afgan Post Organizasyonlarının (Afghan Post Organizations: APO) yenilenmesi, iyileştirilmesi, modernizasyonu ve montajı,
b) Posta usul yasalarının yeniden düzenlenmesi,
c) MCIT tarafından gizlenmiş bağımsız bir kurumun planında posta temel düzenleyicisinin uygulanması (Habib, 2018).

5.8.4. İletişim ve Bilgi Teknolojileri Bakanlığının Güçlendirilmesi

Bu unsur, mevcut ve gelecekteki modern toplumda sorunları yetkin ve etkileyici bir şekilde yakalayabilmesi için MCIT'yi güçlendirmeyi hedeflemektedir. Bu geliştirme unsuru aşağıdaki önemli alt bileşenler aracılığıyla gerçekleştirilecektir.

a) Bakanlığın yeniden düzenlenmesi,

b) Siber zorluklar ve sorunlarla mücadele etmek amacıyla siber güvenlik merkez ofisini yeniden inşa edilmesi,

c) MCIT bakanlığının yetkilerinin ve kapasitesini arttırmak, aynı zamanda Afganistan İslam Cumhuriyeti (Islamic Republic Of Afghanistan: IROA)'nın diğer bakanlıklarının kapasite artışını sağlamak,

d) Tüm devlet daireleri ve kurumlarına Bilişim Kurulu Başkan (Chief Information Officer: CIO) çerçeve kurallarının belirlenmesi,

e) Ülke çapındaki hükümet, iletişim eğitim merkezleri ve BİT kurumları için BİT iyileştirmeleri ve geliştirmeleri hedefi ile güçlü bir kurumun yeniden oluşturulması (Habib, 2018).

5.8.5. Ağ Altyapısının Genişletilmesi

Yeterli kaynakları ve temel çerçeveyi belirleyerek BİT ağ sektörünün fiziksel omurgasını yerine getirecek telekomünikasyon ağı dâhil ağların fiziksel altyapısının genişletilmesi. Telefon Ağı, İnternet ve Geniş Bant Bağlantısı gibi ağlar (Habib, 2018).

5.9. Siber Güvenlik Bilinç ve Farkındalığı

Sistemlerin güvenliği, onları kullanan insanlara bağlıdır. Bilgi güvenliğine yönelik en büyük tehditlerden birinin aslında şirket veya kurum içinden gelebileceği için içeriden gelen saldırıların en tehlikeli saldırılar olduğu unutulmamalıdır, çünkü bu saldırıya ortak olan insanlar altyapıya zaten aşinadır. Tehdit altında olan kişiler her zaman siber casusular değil genellikle, kötü niyetli olmayan bilgisiz kullanıcılardır. Siber güvenlik bilinç odak noktası, kötü amaçlı yazılım bulaşmış web sitelerini ziyaret ederek, kimlik avı e-postalarına yanıt vererek, giriş bilgilerini güvenli olmayan bir yerde saklayarak veya hatta maruz kaldığında telefon üzerinden hassas bilgiler vererek ağlara zarar verebilecek bilgisiz kullanıcılar üzerinde olmalıdır. Güvenlik bilinç ve farkındalık eğitimlerinde ele alınması gereken önemli konulardan bazıları, kuruluşların güvenlik

politikası, veri sınıflandırması ve kullanımı, çalışma alanı ve masaüstü/dizüstü bilgisayarın güvenliği, kablosuz ağlar, şifre güvenliği, kimlik avı, aldatmacalar, kötü amaçlı yazılımlar, dosya paylaşımı ve sosyal mühendisliktir. Bu eğitim her kuruluş için önemli bir gerekliliktir. Eğer kullanıcı neye dikkat edeceğini, önleme ve iyileştirme prosedürleri hakkında uygun şekilde bilgilendirilirse, bu altyapıyı ve şirketi bir bütün olarak etkileyebilecek birçok potansiyel sorunu önleyebilir. Önleme ve korumanın anahtarı genellikle farkındalıktır. Güvenlik bilinci eğitimi, tek başına veya birbirleriyle birlikte kullanılabilecek çeşitli şekillerde gerçekleştirilebilir. Bu ortamlar, daha kapsamlı bir sınıf stili eğitimi, bir güvenlik bilinci web sitesi oluşturulması gibi yararlı ipuçlarını bilgisayarlara göndermek ve/veya yardımcı ipuçlarını haftalık veya aylık olarak e-postayla göndermek ve posterler gibi görsel yardımcıları kullanmaktan oluşabilmektedir (MCIT, 2015).

5.9.1. Güvenlik Farkındalığı Web Sitesi

Güvenlik bilinci programının uygulanmasının başka bir yolu, bir güvenlik bilinci web sitesi oluşturmaktır. ISSD, kapsanması gereken farklı alanlara sahip farklı bölümlerden oluşabilecek web siteleri geliştirmektir, güvenlik bilinci web sitesinin başka bir uygulaması, kullanıcıların giriş yapabileceği ve bu site sayesinde kendi kendilerine bir eğitici olabilir, girişleri kullanmak, eğitimi kimin aldığını (ve daha önemlisi kimin almadığını) takip etmenin bir yolu olabilir (MCIT, 2015).

5.9.2. Sosyal Medya

Siber güvenlikle ilgili konular ve faaliyetler hakkında farkındalık yaratmak için Facebook Youtube ve Twitter vb. gibi sosyal medyanın kullanılması siber güvenlik açısından farkındalık yaratan konulardan bazılarıdır (MCIT, 2015).

a) Youtube Kanalı

Siber güvenlik BİT uzmanları tarafından Afganistan'daki siber güvenlik tehditleriyle ilgili teknik incelemelere sahip resmi Youtube kanalı oluşturmak. Farkındalık kampanyaları veya teknoloji ile ilgili bilgilendirici belgeseller yayınlamak ve videoları en iyi teknoloji kullanımı uygulamaları hakkında yerel dillerde yapılacak şekilde özelleştirmek örneğin; akıllı kartlar, ATM kullanımı, çevrimiçi bankacılık vb. (MCIT, 2015).

b) Profesyonel Makaleler İçin Resmi Site/Blog

Siber güvenlik ile ilgili konularda açık tartışmalar için resmi blog siteleri yayınlanacaktır. Bu siteler yeni fikirler üretmek, ilgili alandaki profesyonellerden en iyi fikirleri almak için Afganistan'daki siber güvenlik faaliyetlerini iyileştirecek şekilde düzenlenecektir. Farkındalık ekibinin, forumu güncel tutmak için düzenli olarak bu foruma daha fazla BİT uzmanlarının bir araya getirmesi gerekmektedir (MCIT, 2015).

c) Radyo Kanalları

Siber güvenlik bilinci ve bunun topluluk üzerindeki etkisi hakkında kısa belgeseller/senaryolar ve günlük teknoloji suç bilinci hakkında kısa reklamların yapılması (MCIT, 2015).

d) Gazeteler

Afganistan'da meydana gelen büyük siber güvenlik olaylarının yerel gazetelerde ayrıntılı raporlarına yer verilmesi (MCIT, 2015).

e) Kamu Bilinci

Kamu ve özel kuruluşlara Siber Bilinçlendirme Seminerleri. Bu seminerler üniversiteleri, kurumsal sektörü, okulları/kolejleri, önde gelen İnternet Servis Sağlayıcılarını (Internet Service Provider: ISP), özel sektörü ve hükümet organizasyonlarını amaçlamaktadır.

Çoğu internet kullanıcısı çevrimiçi tehditlere karşı kendisini savunmasız hissetmesine rağmen birçok kullanıcı, bilinmeyen bir kaynaktan gelen e-postaları açmak veya bir bilgisayarda saklanan kişisel bilgileri koruyamamak gibi çevrimiçi risk almaktadır. Siber Güvenlik Bilinci teknik desteği sırasında çevrimiçi güvenlik uygulamalarımızı gözden geçirmeye fayda vardır. Siber güvenlik her gün herkes için önemlidir (MCIT, 2015).

Aşağıdaki basit adımları uygulayarak siber alanı daha güvenli hale getirmek için üzerimize düşeni yapmamız gerekmektedir.

1. Kimlik korunması: Farklı hesaplar için farklı kullanıcı adları ve farklı şifreler kullanılmalıdır. Harfleri ve sayıları birleştirerek tahmin etmeyi zorlaştıran şifreler kullanılmalı ve sık sık değiştirilmelidir.

2. Güvenlik duvarlarının aktif olması: Güvenlik duvarları ilk savunma hattıdır, bilinmeyen veya sahte sitelere olan bağlantıları engeller, virüslerin ve bilgisayar korsanlarının bilgisayarınıza erişmesini önler.

3. Anti-virüs yazılımı kullanılmalı: Virüslerin bilgisayarlarımıza bulaşmasını önlemek için anti virüs programları yüklenmeli ve düzenli olarak güncellenmelidir.

4. Casus yazılım saldırıların engellenmesi: Casus yazılımları bilgisayarımıza yüklenmesini önlemek için casus yazılım önleme programları yüklenmeli ve düzenli olarak güncellenmelidir.

5. İşletim sistemlerimizin güncel olması: Uygulamalarınızın ve işletim sisteminizin siber alandan gelebilecek tehditlere karşı hep güncel olması gerekmektedir.

6. Dosyaların yedeklenmesi: Dosyaları harici bir sürücüye veya çıkarılabilir bir ortama düzenli olarak yedekleyerek önemli dosyaları virüslerden ve sel, yangın gibi fiziksel hasarlardan korumak için güvenli bir yerde saklanmalıdır.

7. Kablosuz ağını korunması: Kablosuz (Wireless Fidelity: Wi-Fi) ağlar, yüklendikten sonra korunmazlarsa davetsiz misafirlere karşı savunmasızdır. Bu nedenle kablosuz ağlar korunmalıdır.

8. Bilinmeyen e-postaları silinmesi: Bilinmeyen kişilerden gelen e-postalar veya ekler asla açılmamalı ve bu e-postalarda yer alan web sitelerinin bağlantıları asla ziyaret edilmemelidir, bu tür e-postaları hemen silinmelidir.

9. İnternet siteleri güvenli bir şekilde ziyaret edilmeli: İnternet üzerinden yapılan işlemlerde (ör. Alışveriş, fatura ödeme vb.), ad-soyadı, adres, telefon numarası ve kart bilgileri gibi kişisel bilgileri paylaşırken dikkatli olunmalı ve web sitelerinin güvenli olduğundan ve gizlilik ayarlarının açık olduğundan emin olunmalıdır.

10. Uzman yardımı alınmalı: Çevrimiçi şüpheli içerik (çocuk istismarı gibi) görüldüğünde veya bilgisayar suçu, kimlik hırsızlığı ve aldatmacadan şüphelenildiğinde yerel polise ihbar edilmelidir. Bilgisayar yazılım bakımı veya kurulumu konusunda yardıma ihtiyaç duyulduğunda, bir bilgisayar uzmanını veya yerel tedarikçiyle iletişime geçilmelidir (MCIT, 2015).

5.10. Siber Tehditler İçin Alınması Gereken Güvenlik Önlemleri

Artık güvenlik farkındalık ve bilincinin uygulanmasında olası yöntemler ele alınmalı ve uygulanmalıdır. Bu konular, çalışanların güvenlik bilincinin neden önemli olduğunu anlamalarına ve olayların nasıl önleneceğini ve meydana gelmesi durumunda ne yapılacağını bilmelerine yardımcı olacak ve rehberlik edecektir (MCIT, 2015).

5.10.1. Bilgisayar Güvenliği

Bilgisayar güvenlik bölümü, parola korumalı bir ekran koruyucuya sahip olmanın veya daha da iyisi, kullanıcılar uzaklaştıklarında bilgisayarları kilitleme alışkanlığı önemlidir. Bir ekran koruyucu zaman aşımı kullanılmalıdır, böylece bir kullanıcı bilgisayarından uzaklaştığında, parola korumalı ekran koruyucu ortaya çıkacaktır. Potansiyel bir saldırganın kullanabileceği taktikler ele alınmalıdır (MCIT, 2015).

5.10.2. Kablosuz Ağların Güvenliği

Kablosuz ağların güvenli olmayan doğasının yanı sıra, "koklama" tehlikelerine karşı bilgisayarları dikkatli kullanmak ve sağlamlaştırmak için ipuçları ve püf noktaları ele almalıdır. Kablosuz bir ağa erişecek bilgisayarlarda herhangi bir hassas bilginin saklanmasına da önem verilmelidir. Bilinmesi gereken bir diğer konu da güvenlik duvarlarının önemidir. Windows güvenlik duvarları tek başına yeterli değildir, şirket tarafından sağlanan bilgisayarlarda çoğu zaman şirketler, satın alınmış bir güvenlik duvarı kullanırlar, ancak şirketin kablosuz ağını kullanabilecek kişisel bilgisayarların üzerinde bir güvenlik duvarı olması gerekmektedir (MCIT, 2015).

5.10.3. Şifre Güvenliği

Parola güvenliği bölümü, tahmin edilmesi ve kırılması daha zor olan parolalara vurgu yapan güçlü ve güvenli bir parola oluşturulmalıdır. Bu bölüm ayrıca kuruluşun minimum parola gereksinimlerini de belirtmelidir. Şifrelerin paylaşılması ve kullanıcı dışında başka bir kullanıcının erişebileceği yerlerde kullanılması kesinlikle önerilmez (MCIT, 2015).

5.10.4. Aldatmacalar

Sahtekârlıklar plan ve programlarda ele alınmalıdır çünkü sahte e-postaları okumak ve iletmek çok fazla zaman ve olanak gerektirebilir. Bilinen aldatmacaları kullanmak en iyi seçenektir, çünkü kavraması daha kolay olacaktır. Ayrıca, aldatmacaları virüslerle karşılaştırmak da yararlı olabilir çünkü sürekli yayıldıkları için virüsleri de yönlendirebilmektedirler. Aldatmacaların tehlikeleri de ele alınmalıdır çünkü bazı aldatmacalar bir virüsü uyarır ve kullanıcılara geçerli ve bazen önemli sistem dosyalarını silmelerine sebep olabilir (MCIT, 2015).

5.11. Afganistan Siber Olay Müdahale Ekibi

Bir olayın müdahale sürecinde, Siber Acil Müdahale Ekibinin veri ve bilgi kaybını en aza indirmek için olayı mümkün olan en kısa sürede azaltması çok önemlidir. Süreç, iyi tanımlanmış bir olay müdahale çerçevesine göre geliştirilen aşağıdaki şekilde gösterildiği gibi uygun bir kılavuzu takip etmelidir. Hazırlık, tanımlama kapsama, yok etme, kurtarma ve takip gibi 6 aşamadan oluşan bu çerçeve, bu tür olayların ele alınmasında tutarlı ve sistematik bir yaklaşım sağlar. Bu sistematik yaklaşım, AFCERT ekibinin siber güvenlikle ilgili her türlü olayı uygun ve standart bir şekilde ele almasını sağlayacaktır (MCIT, 2015).

5.11.1. Amaç

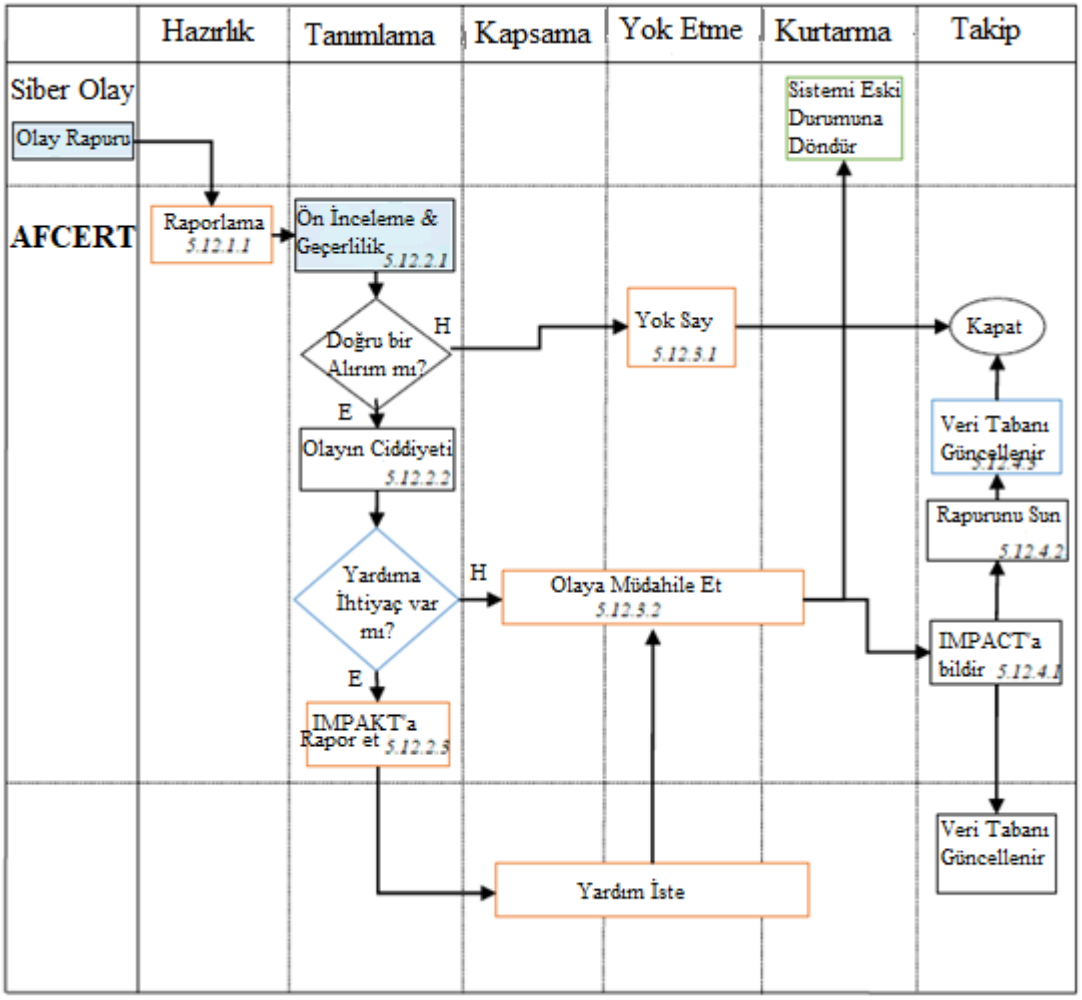
Bu belge, AFCERT için güvenlik ile ilgili olayların ele alınmasında sistematik bir yaklaşım ortaya koymaktadır (MCIT, 2015).

5.11.2. Kapsam

Bu belgenin birincil kitlesi, tüm AFCERT ve hazırlık, tanımlama, sınırlama, eradikasyon, kurtarma ve takip çabalarına katılabilecek diğer kişileri içerir (MCIT, 2015).

5.12. Prosedür

Aşağıdaki şekil 5.2'de, olay müdahale süreci akış şeması ayrıntılı olarak gösterilmektedir. Buna ek olarak AfCERT işleme aşamaları aşağıdaki başlıklar altında anlatılamaya çalışılmıştır.



Şekil 5.2. AfCERT olay yanıtı akış şeması (MCIT, 2015).

5.12.1. Hazırlık

5.12.1.1. Raporlama

Bu aşama olayın işleme sürecinin başlangıç aşamasıdır ve bu sırada olayın AFCERT'e bildirilmesi gerekmektedir. Olay çeşitli yollarla raporlanabilmelidir; AFCERT'in portali, e-posta, telefon, faks veya diğer gerekli araçlar (MCIT, 2015).

Alınan rapor, mümkün olduğu kadar aşağıdaki bilgileri içerecek şekilde olay tanımını yapabilmelidir; ancak ek bilgi elde etmek için sonraki eylemlere başvurulmalıdır.

- Raporlama ajansı adı.
- İsim, telefon ve e-posta adresi dâhil iletişim bilgileri.
- Saat dilimi dâhil olay tarihi ve saati

- IP kaynağı, bağlantı noktası ve protokol
- Hedef IP, bağlantı noktası ve protokol
- Sürüm, yamalar vb. Dâhil İşletim Sistemi
- Sistem İşlevi ör. Alan adı sunucusu (Domain Name Server: DNS) /web sunucusu vb.

Yüklenmiş virüsten koruma yazılımı, sürüm ve en son güncellemeler dâhil olayla ilgili sistem(ler)'in yer ve konumu. Olayı tanımlamak için kullanılan yöntem ör. Güvenlik duvarı, denetim analizi, sistem yöneticisi vb.

Her vakaya benzersiz bir olay numarası atanmalıdır. Olayın kritikliğine bağlı olarak, raporlama ajansı için raporlamadan önce tüm bilgileri toplamak her zaman mümkün olmayabilir. Bu durumda, ekip daha fazla bilgi toplarken olay müdahale sürecinin bir sonraki adımına devam edilecektir (MCIT, 2015).

5.12.2. Tanımlama

5.12.2.1. Ön İnceleme ve Geçerlilik

Bir olay raporlanırken, olayın geçerliliğini belirlemek için ön inceleme yapılır. Bu süreçte, ekip bunun gerçek bir olay mı yoksa sadece yanlış bir alarm mı olduğunu tespit etmelidir. Yanlış alarm, sistemin yanlış yapılandırması, internet servis sağlayıcısı (ISP) hizmet kesintisi, ağ bileşeni arızası vb. gibi birçok olaydan dolayı tetiklenebilir. Geçerli bir olay bildirimi ise, olayın ciddiyetini belirlemek için adım 5.12.2.2 takip edilir. Yanlış bir alarm ise, alarmı kapatmak için adım 5.12.3.1 takip edilir ve kapatılır (MCIT, 2015).

5.12.2.2. Olayın Ciddiyetini Belirleme

Olayın geçerli olduğu teyit edildikten sonra, olayın ciddiyet seviyesi belirlenecektir. Olayın şiddetinin tanımlaması, olayı düzeltmek için yapılması gereken eylemlerin belirlenmesine yardımcı olacaktır. Ekip, sistemin etkilenen kullanıcılarını ve ayrıca olay nedeniyle risk altındaki bilgilerin sınıflandırılmasını dikkate alarak olayın önem derecesini sınıflandırabilir. Şiddetin belirlenmesinde ekibe yardımcı olması istenebilecek soruların bazıları AFCERT olay raporlama formunda listelenmiştir (MCIT, 2015).

5.12.2.3. Olayı IMPACT'a Bildirme

Ekibin olayın çözümünde yardıma ihtiyacı olduğunda, yardım istemek için IMPACT'ın Küresel Yanıt Merkezi'ne (Global Response Centre: GRC) bildirilebilir. Ekip, olayı bildirmek için GRC portalini kullanabilir veya e-posta, faks ve telefon gibi gerekli diğer yollarla bildiri yapabilir (MCIT, 2015).

5.12.3. İyileştirme

5.12.3.1. Olayı Kaydedip Yok Saymak

Bildirilen olayın yanlış alarm olduğu durumlarda, ekip olayı günlüğe kaydedecek ve olayı göz ardı edecektir. Ekip bildirilen olayın kapatılması hakkında bilgilendirilecektir (MCIT, 2015).

5.12.3.2. Düzeltici Olay

Olayı düzeltmek için ekip genellikle olay bölgesinde aşağıdakilere yardımcı olmaktan ve/veya tavsiyelerde bulunmaktan sorumludur.

- Sistemi izole etmek
- Olayı izlemek
- Olaydan etkilenen ilgili sistemleri haber vermek ve onlara acil durum talimatları sağlamak
- Gerekirse ilgili kolluk kuvvetlerine rapor etmek
- IMPACT veya diğer ilgili kurumlardan ek kaynaklar istemek

Ekip, olayı kendi başına çözebilecek ya da IMPACT'tan yardım isteyecek kapasiteye ve yeteneğe sahip olup olmadığına karar verecektir. Ekibin yardıma ihtiyacı varsa, GRC portali, telefon, e-posta veya faks gibi mevcut iletişim kanalları tarafından IMPACT'a bir rapor verecektir (MCIT, 2015).

Ekip, olayı düzeltmek için önerileri ve tavsiyeleri olay bölgesine iletir ve normal faaliyetine devam edebilmesini sağlar. Denenen ancak sistemlere başarısız olan müdahaleler gibi nispeten basit olaylar, yalnızca olayın sistem yazılımını veya sistemde depolanan verileri hiçbir şekilde etkilemediğini garanti eder. Çalışanlar tarafından yerleştirilen kötü amaçlı kod gibi karmaşık olaylar, yedeklemelerden sonra tam bir geri yükleme işlemi veya işletim sisteminin ve yazılım uygulamalarının tamamen yeniden

yüklenmesini gerektirebilir. Bir geri yükleme işleminin başarılı olduğunu ve sistemin normal duruma döndüğünü doğrulamak önemlidir (MCIT, 2015).

5.12.4. Takip

5.12.4.1. Gerektiği Durumlarda Olayı IMPACT'a Bildirme

Ekip, bilginin dünyadaki diğer topluluklara fayda sağlayacağına inanıyorsa, olay müdahale sürecinin herhangi bir bölümü hakkındaki bilgileri IMPACT'a bildirebilir. Bilgiler yalnızca kuruluşa özgü ve ülkeye özgü bilgiler kaldırıldıktan sonra paylaşılacaktır (MCIT, 2015).

5.12.4.2. Olay Bölgesine Raporun Sunulması

Bir olay raporu oluşturulacak ve olay müdahale tatbikatının sonunda olay bölgesine dağıtılacaktır. Rapora dâhil edilebileceği düşünülen unsurlardan bazıları şöyledir.

- Olay sırasının tam olarak açıklanması
- Olayların türü ve şiddeti
- Düzeltme önleminin uygulamaya konulması
- Atılan iyileştirme adımlarının yeterli olup olmadığını belirlemek için değerlendirilmesi
- İyileştirme için önerilerin dikkate alınması gerekmektedir.

Rapor, etkilenen olay bölgesinde serbest bırakılmadan önce yönetim tarafından gözden geçirilecektir. Bunun amacı, belgenin uygun şekilde hazırlanmasını ve olay bölgesi tarafından ihtiyaç duyulan yeterli bilgiyi içermesidir (MCIT, 2015).

5.12.4.3. Veri Tabanını Güncellenmesi

Raporlama bölgesi normal faaliyetine devam ettiğinde, ekip veri tabanını günceller. Güncellenecek diğer konuların yanı sıra, olayla ilgili ayrıntılar, bunun nasıl düzeltildiği ve ayrıca alınan notlar, belirlenen alanlarda iyileştirilmesi ve gelecekteki olaylar için referans olarak kullanılabilir (MCIT, 2015).

5.13. Tehdit Danışmanlığı

AfCERT'in önemli rollerinden biri, tehdit danışmanlığı sağlamaktır. Ekip, tehdit önerilerini yaymak için aşağıdaki şekil 5.3'te gösterilen iş akışını izleyecektir.

Şekil 5.3. AfCERT danışmanlık dağıtım iş akışı (MCIT, 2015)

5.13.1. GRC'den Tehdit Bilgisi Edinmek

Olayla ilgili tavsiyelerde bulunmak için, AfCERT, IMPACT, GRC portalından tehdit bilgilerini rutin olarak gözden geçirecektir (MCIT, 2015).

5.13.2. Danışma Raporu Oluşturmak

Öneriler alındıktan sonra ekip, GRC portalından elde edilen bilgileri, olaylar için bir danışma raporu oluşturmak için kullanacaktır (MCIT, 2015).

5.13.3. Olayla İlgili Danışmanlıklar Yaymak

Danışma raporu tamamlandığında, AFCERT raporu e-posta iletişimi yoluyla olay bölgelerine dağıtılacaktır (MCIT, 2015).

5.13.4. AFCERT Portalında Tehdit Bilgilerini Doldurmak

Tehdit bilgisi, AFCERT portalına bilgi yüklenerek olay bölgesi ve halk için de sağlanabilir (MCIT, 2015).

5.13.5. Belgeleme

Olay müdahale süreciyle ilgili tüm detaylar, geri izlemek ve kolay erişebilmek için belgelenecek ve dosyalanacaktır. Bu, olayların gidişatını değiştirmek için önemli bilgiler sağlayacaktır. Belgeleme için aşağıdaki maddelerin takip edilmesi önerilir (MCIT, 2015).

- Sistem olayları (günlük kayıtlar)
- Olayın özeti (olayın nasıl gerçekleştiği, olayın kategorisi, ciddiyeti vb.)
- Alınan olay müdahale eylemi (bir eylemin gerçekleştirildiği zaman dâhil)
- Tüm dış taraflarla iletişim (iletişimin tarihi ve saati ve içeriği dâhil).

5.14. Şifreleme

Şifreleme, bir anahtarı kullanarak korunmasız verileri veya düz metni şifrelenmiş verilere veya şifreli metine dönüştürmektir. Şifreleme anahtarı hakkında bilgi sahibi olmadan, şifreli metin tekrar düz metine dönüştürülemez. Şifreleme anahtarlarının güvenliğini korumak için uygulama, hiç kimsenin şifreleme anahtarını belirlemek için gereken tüm bilgilere erişemeyeceği şekilde olmalıdır. Son kullanıcı cihazlarında depolanan verileri şifrelemek için tam disk şifrelemesi, birim ve sanal disk şifrelemesi ve dosya/klasör şifrelemesi gibi birçok şifreleme teknikleri mevcuttur aşağıda farklı şifreleme türlerinin kısa bir özeti bulunmaktadır (MCIT, 2015).

5.14.1. Tam Disk Şifrelemesi

Tam Disk Şifrelemesi (Full Disk Encryption: FDE), bilgisayarın işletim sistemi de dâhil olmak üzere bir bilgisayarı ön yüklemek için kullanılan, yalnızca başarılı kimlik doğrulamasından sonra verilere erişime izin veren ve verilerin güvenliğini sağlayan sabit sürücüdeki tüm verileri şifreleyen şifreleme türüdür (MCIT, 2015).

5.14.2. Sanal Disk Şifrelemesi ve Birim Şifrelemesi

Birçok dosya ve klasörü tutabilen ve yalnızca doğru kimlik doğrulaması sağlandıktan sonra kap içindeki verilere erişime izin veren sanal disk şifrelemesi bir sanal diske bağlanmaktadır. Bu şifreleme her türlü son kullanıcı cihaz depolama alanında kullanılmaktadır. Kapsayıcı, mantıksal bir birim içinde bulunan tek bir dosyadır. Birimlere örnek olarak kişisel bilgisayardaki ön yükleme, sistem ve veri birimleri ve tek bir dosya sistemiyle biçimlendirilmiş bir Evrensel Seri Veri yolu (Universal Serial Bus: USB) flaş sürücü verilebilir. Birim şifreleme ise, tüm mantıksal birimin şifrelenmesi ve yalnızca uygun kimlik doğrulaması sağlandıktan sonra birimdeki verilere erişime izin verilmesidir. Birim şifreleme çoğunlukla sabit sürücü veri birimlerinde ve USB flaş sürücüler ve harici sabit sürücüler gibi birim tabanlı çıkarılabilir ortamlarda gerçekleştirilmektedir (MCIT, 2015).

5.14.3. Dosya/Klasör Şifrelemesi

Dosya şifreleme, bir depolama ortamındaki dosyaları tek tek şifreleme ve şifrelenmiş verilere ancak uygun kimlik doğrulaması sağlandıktan sonra erişime izin

verme işlemidir. Klasör şifreleme, dosya şifrelemeye çok benzer, yalnızca dosyalar yerine tek tek klasörlere yöneliktir. Bu yöntem şeffaftır, yani dosya sistemine erişimi olan herkes İşletim Sistemi (Operating System: OS) erişim kontrolü özellikleri ile korunmuyorsa şifrelenmiş klasörlerdeki dosyalar ve klasörler dâhil şifrelenmiş dosya ve klasörlerin adlarını ve muhtemelen diğer verilerini görüntüleyebilir. Tüm depolama türlerinde kullanılmasının yanı sıra, sürücüler, hizmetler ve uygulamalar da dâhil olmak üzere birçok şekilde uygulanabilir. Bir kullanıcı şifrelenmiş bir dosyayı açmaya çalıştığında yazılımın önce başarılı bir şekilde kimlik doğrulaması yapması gerekir. Bu yapıldıktan sonra, yazılım seçilen dosyanın şifresini otomatik olarak çözecektir. Her seferinde tek bir dosyanın şifresini çözdüğü için, dosya/klasör şifrelemesinin performans etkisi minimum olmalıdır. Dosya/klasör şifrelemesi, en çok sözcük işlemci belgeleri ve elektronik tablolar gibi kullanıcı veri dosyalarında kullanılmaktadır (MCIT, 2015).

BÖLÜM 6

SONUÇLAR VE TARTIŞMA

İnternet tarafından sağlanan hürriyet ve özgürlük kişilere, özel sektörlere kurum kuruluşlara ve hatta ülkelere siber olayların kontrol edilemeyeceği bir siber ortamın bulunduğunu his ettirmektedir. Bu ortam tarafından gelebilecek tehditler, kritik altyapıları ve toplumun yaralandığı sistemleri riske atabilmektedir, bundan dolayı insanoğlunun standart yaşamı zorlaşmakta ve hata durabilmektedir. Tam bu sebeptendir ki siber güvenlik toplumun vazgeçilmez bir parçası olmuştur. Özel hayatımızda nasıl güvenlik önlemleri alıyor kapıları kilitliyor, güvenlik kamere sistemleri ve alarm sistemleri gibi farklı güvenlik sitemlerine başvuruyorsak siber ortamda da aynı hassasiyeti göstermemiz gerekmektedir. Siber alanda risk ve tehditler artarak devam etmektedir. Bu tehdit ve risklerin zamanında fark edip daha büyük felaketlere yol açması engellenmelidir.

Siber güvenliğin temel bileşenleri insan, eğitim ve teknoloji birlikteliği iken, temel omurgası ise gizlilik, bütünlük ve erişilebilirliktir. Siber güvenlik alanında üst düzeyi farkındalığın sağlanması, siber ortamı, alanında uzman yöneticilerin yönetmesi, ağ bilgi sistemlerini güvenlik açısından ciddiye alınması, neyin nasıl korunması veya korunmaması gerektiğini bilinmesi, gözetleme ve kontrol sistemlerinin kurulması, gibi atılan adımlar güvenliği artırmak için atılan önemli adımlar olacaktır.

Siber ortam yeryüzünün düzenini alt üst edebilecek bir konudur. Bizde filli karıncaya ezdirmek diye bir söz vardır, bunun Türkçe karşılığı sanırım, aslanı kediye boğdurmaktır. Tabiri caizse bu söz tam siber ortam için söylenmiş bir sözdür. Çünkü düşük bilgiye sahip insanlar yüksek düzeyi teknolojiler sayesinde oldukça etkili siber saldırılar gerçekleştirebilmektedirler. Bunun yanı sıra herkes her yerden siber saldırılara katılarak siber ortamın bir parçası olabileceği gibi çok küçük maliyetlerle çok büyük

zararlar verilebilmektedir. Siber güvenlik sadece bir kişi, şirket, kurum kuruluş veya bir ülkeyi ilgilendiren bir konu değildir, dünya çapında işbirliğinin sağlanmasını gerektiren, ortak siber güvenlik politikasına ve hukukuna gereksinimi olan bir konudur. Ancak bu konu ile ilgili herhangi bir girişim olmadığından herkes kendi imkân ve olanaklarıyla başının çaresine bakmak zorundadır.

Tüm bunlara ek olarak kurumsal siber güvenlik tehditlerinin ağ sistemlerinden web uygulamalarına yönlenmesi, karmaşık ve hızlı bir şekilde ilerlemesi kullanıcıları verimli ve etkin bir siber güvenlik önlemleri almak zorunda bırakmıştır. Bu durumda güvenlikle kullanılabilirlik arasındaki uyum göz önünde alınarak kurumsal siber güvenlik yaşayan bir süreç olarak ele alınması gereken bir meseledir. Teknolojik gelişmelerin ışık hızında ilerlemesi siber güvenlik konusunda yapılan çalışmalar, alınan önlem ve tedbirler siber suçlarlar ve saldırılara karşı koymak için yeterli olmamaktadır. Global olan bu tehditlerle mücadele edebilmek için ulusal organizasyonlar ve milli çözümler şarttır.

Hayatı derece de önemli olan diğer bir mesele ise kritik altyapılarına yönelik yapılan risk değerlendirmeleridir. Özellikle ülkenin güvenliğini sağlamak için her ülke altyapılarına yönelik siber saldırılar için risk değerlendirme yöntemlerinden faydalanmalıdır. Bu altyapıların hasar görmesi, siber saldırılara maruz kalması durumunda faaliyet gösteremeyecek, hizmet veremeyecek ve çok ciddi olumsuzlara yol açabilecek risklere karşı karşıya kalabilecektir, bu durum toplumun düzenini bozacak ve hatta ulusal güvenliği tehlikeye atabilecektir. Siber saldırılar maddi ve manevi zararların yanı sıra saldırıya uğrayan şirket kurum ve kuruluşlar için müşteri kaybı itibar zedelenmesi gibi önemli zararlar verebilmektedir. Bu zararları tümüyle ortadan kaldırılması imkânsız olsa da, zamanında ve yerinde alınan güvenlik tedbirleri sayesinde zararı minimum tutabilmek mümkündür. İşte burada hedef alınan bilgi sistem üzerindeki yazılım ve donanımsal eksiklerin, açıklıkların ve zafiyetlerin giderilmesi oldukça önem arz etmektedir.

Bu eksikler ve açıklıkların tamamlanması için ilk önce, bu alanda görev yapan tüm personelin siber güvenlikle ilgili yeterince bilgi ve eğitime sahip olmaları, sahip değilse yeterli eğitimi almaları gerekmektedir. Eski ve güncel olmayan eğitim sistemlerinin teknolojik gelişmeler için yetersiz kaldığı göz önüne bulundurularak bu

gelişmelere paralel olarak kurumlar tarafından yeni ve güncel eğitimlerin planlanması gerekmektedir. Bilinmesi gereken diğer bir husus, topluluğun siber güvenlik ve siber güvenliğin öneminin farkında olunması ve bilgilendirilmesidir. Bu çerçevede, ilköğretimden başlayarak siber güvenlik konusunun öğretim programlarına eklenmesi gerekmektedir.

Üzerinde durulması gereken başka bir mesele ise yetki vermektir. Çalışanların yetkilerini kısıtlayarak her veri ve bilgiye ulaşabilmeler sınırlanmalıdır, çalışanlar kullanıcı adı ve şifre gibi bilgilere istedikleri zaman erişememelidir. Bununla beraber kurum ve kuruluşlarda, yetkisi olmayan, şahısların dosyaları değiştirmesi, kopyalaması veya yok etmesi gibi konuların önüne geçilmelidir. Özellikle kritik yazılımlar konusunda görev yapan çalışanlarda görev ayrımı yapılmalıdır. Yazılımları geliştiren kişiler ve bu yazılımları test eden kişiler farklı kişiler olmalıdır. Böylece yazılımlardaki eksiklikler, hatalar, zafiyetleri ve açıklıklar tespit edilebilecektir unutmayalım ki, bir sistem için en tehlikeli bileşen insandır.

Siber güvenlik alanında yapılması gereken diğer konu da kritik elemanların yedekli bir şekilde çalıştırılmasıdır. Böylelikle, sözü geçen elemanların denetimi yapılmakla beraber, elemanlar herhangi bir nedenle işten çıktıkları zaman sistem durdurulmadan çalışmasına devam edebilecektir. Siber bağımlılığın oldukça artarak devam ettiği günümüzde göze çarpan önemli bir eksiklikte yerli teknolojik ürünlerin üretilememesidir. Siber ortamda gerçekleşen olaylara bakıldığında yerli teknolojik ürünler çok önemli rol oynamaktadır. Bu nedenle yerli ürünler geliştirilmeli ve uygulanmalıdır. Bu konuyu hızlandırmak için üniversite sanayi işbirliğinin yapılabilmesi gerekmektedir. Güvenlik eksikliklerini ve tehditleri tespit etmek için saldırı tehdit algılama mekanizmaları kurulmalı, geliştirilmeli, güçlendirilmeli ve uygulanmalıdır.

Bu tez çalışmasında ele alınan önemli bir konu da siber savunma konusudur. Ulusal savunma tedbir ve önlemleri siber saldırı ve tehlikeler tarafından gelebilecek zararları azaltacaktır. İlk olarak ülkelerin kritik alt yapılarının internette bağlı olmayan İntranet gibi bir ağ araçlığıyla faaliyet göstermesi sağlanmalıdır. Bu sayede internet üzerinden gerçekleşebilecek saldırılar az da olsa engellenebilmektedir. Ulusal güvenlik politikaları belirlenerek milli yazılımlar olabildiği kadar çok kullanılmalıdır. Diğer

ülkelerin ürettiği yazılımlar güvenli değildir. Siber ortamda saldırının kaynağını tespit etmek zordur ama imkânsız değildir. Bundan dolayı uluslararası işbirliği yapmak ve örgütlenmek gerekmektedir. Bu örgütlenme kapsamında oluşturulacak laboratuvar ve Ar-Ge merkezleri tarafından uluslararası tahkikatlar ve cezalandırmalar yapılmalıdır.

Siber alanda savunma yapabilmek için ülkeler hızlı bir şekilde karşılık verebilen düzenlemelere ihtiyaç duymaktadır. Siber güvenlik konusunda donanım ve yazılım sistemlerinin ne kadar önemli olduğuna dikkat ederken bu sistemleri kullanan insanların zincirin en zayıf halkası olduğu unutulmaması gerekmektedir.

Ülkelerin üç ana savunma alanı olan, kara, hava ve deniz alanlarının yanı sıra son zamanlarda savunmak ve tehditler karşısında korumak zorunda oldukları dördüncü bir alan olarak siber alan meydana çıkmıştır. Siber alanın korunmasını gerektiren tüm tedbirler alınsa bile bu alanı kullanan kişiler bilinçlendirilmediği müddetçe savunma önlem ve tedbirlerinde açıklıklar ve eksiklikler hep olacaktır. Siber saldırılarla artık kaçınılmaz bir savaş tarzı olarak karşı karşıya kalmaktayız. Bu sebepledir ki ilk önce etkili ve güçlü bir siber savunmaya sahip olmamız hayatı önem arz etmektedir.

Bu tez çalışmasında yapılan literatür taramaları neticesinde siber savunmanın diğer savunma sistemlerinin yanı sıra bir güvenlik sistemi olarak kullanılması kanıtına varılmıştır. Güvenlik duvarı, anti virüsler, balköpü, şifreleme vb. savunma unsurları, siber savunma önlemlerinden bazılarıdır. Bu önlemler, bir yandan güvenliği artırırken diğer yandan da saldırıları yavaşlatarak etkisini azaltmaktadır. Karşı atak yöntemleri için inandırıcı ve saldırganların dikkatini çekecek şekilde bir balküpü kurularak saldırganların bu balköpü ziyaret ettikleri halinde saldırganlar ve saldırı ile ilgili daha fazla bilgi edinebilmekte ve hatta saldırgan makineler ele geçirilebilmektedir. Bundan dolayı bu güvenlik yöntemlerinin kullanılması şiddetle önerilmektedir.

Bu Tez Çalışmasında Ele Alınan Bazı Ülkelerin Siber Güvenlik Çalışmalarının Karşılaştırma Sonucu

ABD: Kendisine yapılan siber saldırıları bir savaş sebebi olarak değerlendiren ABD daha 2000'li yıllarda siber güvenliğin farkında varmıştır. Ülkenin 2015'te yayınladığı strateji belgesi incelendiğinde, bu süre içerisinde yayınlanan diğer belgelere göre somut adımların atıldığı ve bu farkındalığın henüz gelişmekte olduğu görülmektedir.

İsrail: Bu ülke siber güvenlik ile ilgili yaptığı faaliyetlerden ötürü siber tehdit ve risklere karşı en hazırlıklı ülkeler arasındadır. İsrail devleti ve halkı siber güvenlik konusunu ortak bir çalışma alan ve sorumluluk olarak görmektedir.

Çin: Bu ülkenin siber güvenlik anlayışı saldırıya yöneliktir, en güçlü savunma yönü kendi yerli ağlarını kullanması ve diğer ağların yasaklanması veya kısıtlanmasıdır. Bu şekilde izlenen bir yöntem ülkeyi batı ülkelerine göre daha güvenli kılmaktadır.

Rusya: Siber güç alanında en önemli ülkelerden biri olan Rusya'nın siber güvenlik anlayışı saldırıdan daha çok savunmaya yöneliktir. Ancak siber alanda gelişen olay ve hareketler sonucunda güvenlik anlayışını değiştirerek saldırıya saldırı anlayışıyla diğer ülkelerden farklılaştığı görülmektedir.

İngiltere: İngiltere'nin siber güvenlik anlayışı, siber tehdit ve risklere karşısında güvenilir olmak, saldırılara karşı dayanıklı olmak ve güçlü durmak şeklindedir. Siber güvenliği sağlamak için Savunma, Caydırma ve Gelişme olarak 3 ana başlığı dikkate almaktadır kısacası karşı koymaya odaklıdır.

Almanya: Ülkenin siber güvenlik alanında daha çok kurumsal yapılar ve düzenlemelere odaklanmaktadır. Ülkede oluşturulan kurumsal altyapıyla siber güvenlik ve kritik altyapıları korumak için belirlenmiş olan strateji ve amaçların çok geniş ve sistemli bir biçimde oluşturulduğu görülmektedir.

Türkiye: Siber güvenlikle ilgili ilk ciddi adımını Aralık 2012 yılında Ulusal Siber Güvenlik Strateji Belgesini yayınlayarak atmıştır. Ardından 2013 - 2014 diğeri ise 2016 - 2019 Ulusal Siber Güvenlik Stratejisi olmak üzere iki önemli strateji belgesi yayınlamıştır. Bu belgeler incelendiğinde siber savunmayı güçlendirmek ve kritik altyapıları korumak daha çok öne çıkmaktadır. Yani daha çok savunma önlemlerine yöneliktir. Bu tez çalışma araştırmalarına göre, ülkede son birkaç yıldır siber güvenlikle ilgili yüksek lisans ve doktora tezlerinin yazıldığı görülmektedir. İlerleyen zamanlarda, başta yazılım ve bilgisayar mühendisliği olmak üzere diğer bölümlerde de yazılacak olan bu tarz tezler siber güvenlik konusunda katkıda bulunacaktır.

Afganistan'ın Siber Güvenlik Çalışmalarıyla İlgili Sonuçlar

Afganistan da siber güvenlik terimi hala tamamıyla idrak edilememiş, bu konuyla ilişkin önlemler ve tedbirler alınamamış ve yetkinleşmemiş bir terimdir. Ülkede

var olan güvenlik güçlerinin yetenek ve imkânları çerçevesinde yetişen kişi sayısı yok denebilecek kadar azdır, bu tez çalışmasının Afganistan ulusal siber güvenliğini konu alan ilk tez çalışması olması bunun bir ispatıdır. Bilindiği gibi Afganistan'da yıllardır iç savaşlar ve çatışmalar devam etmektedir, ülke yöneticileri henüz vatandaşlarının normal güvenliğini sağlayabilmiş değildir. Bu nedenle ülke teknoloji alanında diğer ülkelerden epey geridedir. Buna rağmen Afganistan siber güvenlik alanında, Afgan Acil Müdahale Ekibi (AFCERT) kurulması ve Afganistan ulusal siber güvenlik stratejisi (2014-2015) yayınlanması gibi bazı önemli adımlar atmıştır.

Afganistan'da siber güvenlik konusunda özel sektörler daha hassasiyet göstermektedir. Devlet kurumları ise özel sektörün gerisinde kalmaktadır. Bilgi ve iletişim teknolojilerinin kullanımı tüm dünya da olduğu gibi Afganistan'da da hızla artmaktadır. Ancak bu artışın güvenli bir şekilde ilerlemesi ve sunulan hizmetlerin sekteye uğramaması önemlidir. Aksi halde ülkemiz geri dönüşü olamayan felaketlerle karşı karşıya kalabilecektir. Afganistan diğer ülkelere göre daha çok siber tehdit ve risk altındadır, bu ülke, bilgi eksikliği, yeterli eğitimin olmaması, yanlış yönetim ve siber ölçümlerin düzensizliği nedeniyle genel olarak bu tehditlerden daha fazla etkilenmektedir.

Sonuç olarak, ülkenin sanal iletişim sistemleri üzerindeki siber güç potansiyelini artırmak ve dijital savaşların yakınsaması gelecek nesillerimizi tehdit eden ortak zorluklardır. Ancak, günümüzde gerekli önlemlerin alınması, tehdit önleme stratejileri, gelecekte güvenli bir siber alana sahip olmayı sağlayacaktır. Gelecekteki siber tehditlerin ve riskleri azaltmak, kontrol etmek, izlemek ve denetlemek için bu araştırmanın çözüm niteliğindeki önemli kısımlarına atıfta bulunarak, bu amaç için önerilerde bulunmuş ve akış şemaları göstererek teoriler ve stratejiler sunulmuştur.

Bu tez çalışmasının genel bir değerlendirmesini yapacak olursak ülkelerin siber güvenlik stratejileri farklılık göstermektedir her ülke kendi stratejileri kapsamında önemli çalışmalar yapmış, önemli birimler kurmuştur. Ancak tüm ülkelerin üzerinde durduğu bazı önemli noktalar vardır. Bu önemli noktalar, uluslararası işbirliği, siber güvenlik alanında koordineli çalışmaların yapılması, bu alanda farkındalığın arttırılarak toplumun bilinçlendirilmesi, özel sektör ve devlet kurumları arasında koordinasyonun sağlanması, eğitim ile milli çözümler ve yerli ürünlerin üretilmesidir.

Siber güvenliğin sağlanması için devletlere, özel sektörlere kurum ve kuruluşlara hatta kişilere büyük sorumluklalar düşmektedir. Kısacası, Siber Güvenlik, konusu sadece bir kişinin, bir şirketin ve kurumun ya da sadece bir ülkenin düşünüp çözmesi gereken bir konu değildir, bugün için alınan önlemlerin yarının tehditleri için yeterli olmadığı düşünce ve kaygısı ile hep akılda olması ve paydaşların tamamını içerecek biçimde gereken tedbirlerin acil bir şekilde alınması gereken küresel bir konudur.

Gün geçtikçe büyüyerek daha da karmaşıklaşan siber tehditler ve siber saldırılar karşısında ağ ve bilgi güvenliği sadece anti virüsler, güvenlik duvarları ve diğer güvenlik önlemleri ile engellenemeyeceği, Estonya, Sony, Stuxnet, Flame gibi dünya çapında meydana gelen siber güvenlik olaylarıyla ispatlanmıştır. Özellikle ulusal siber güvenliği sağlamak için uluslararası işbirliği kapsamında güçlü ve etkili bir oluşum ve faaliyet gerekmektedir.

Şirket ve kurum kuruluşların zafiyet ve açıklıklarının olup olmadığını belirlemek için sızma testleri bağımsız kurumlarca beli zaman aralıklarında kesinlikle gerçekleştirilmelidir. Bu sayede açıklıkların olup olmadığı tespit edilecek ve açıklıklar varsa kapatılacaktır. Bir ülkenin güvenliği için, daha önce sözü geçen alanlar (kara, deniz ve hava) alanlarının gücü ne kadar önemli ise siber güvenlik alanındaki güçte o kadar önem arz etmektedir. Gelecekteki siber saldırılar ve siber olaylarla mücadele edebilmek için bu alanla ilgili faaliyetlere ve çalışmalara olabildiği kadar hız verilmeli ve geliştirilmelidir. Kullanılan araçlarda güvenlik önlem ve tedbirlerinin tam ve eksiksiz bir şekilde alınması gerekmektedir. Siber güvenlik alanında en zayıf varlığın kullanıcıların olduğunu bir kez daha vurgulayarak, çalışanların bu konuyla ilgili eğitilmesi ve bilinçlendirilmesi gerekmektedir.

KAYNAKLAR

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

Ada M., & Çakır, H. (2017). Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, *5*(2017), 632-656.

Alioğlu, S.D. (2019). *Siber Saldırılar ve Ülkelerin Siber Güvenlik Politikaları*, (Yüksek Lisans Tezi). İstanbul Bilgi Üniversitesi/Lisans Üstü Programalar Enstitüsü, İstanbul.

Altun, M. (2017). Siber Güvenliğin Önemi ve Temel Kavramlar. 5 Mart 2019 tarihinde http://www.altunmustafa.com/siber-guvenligin-onemi-ve-temel-kavramlar/ adresinden erişildi.

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

Ayvaz, T. Mediaclick, Siber Saldırı Nedir. 29 Mart 2019 tarihinde https://www.mediaclick.com.tr/blog/siber-saldiri-nedir adresinden erişildi.

Akbilge Bilişim, AlienVault - Siber Tehdit Algılama Sistem. 29 Mart 2020 tarihinde https://www.akbilgebilisim.com/siber-tehdit-algilama adresinden erişildi.

Arşivden.com. 5 Mart 2019 tarihinde https://www.arsivden.com/siber-guvenlik/ adresinden erişildi.

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

Bostancı, Ü. (2017). *Türkiye'de ve Dünya'da En Çok Kullanılan İşletim Sistemlerinin Barındırdıkları Açıklıklar Dikkate Alınarak Analiz Edilmesi*, (Yüksek Lisans Tezi). Gazi Üniversitesi/Bilişim Enstitüsü, Ankara.

Bilim Çağı, Bal Küpü (Honeypot) Nedir (2017). 27 Mart 2020 tarihinde https://www.bilimcag.com/nedir/bal-kupu-nedir/ adresinden erişildi

Canbek, G. (2019). *BGD* Siber Güvenlik ve Savunma Kitap Serisi2, 306-307: Cilt 2. *Siber Güvenlik ve Savunma*. Problemler ve Çözümler.

Canbek, G., & Sağıroğlu, Ş. (2007). Kötücül ve Casus Yazılımlar. *Gazi Üniversitesi, Mühendislik-Mimarlık Fakültesi Dergisi*, *22*(1), 121-136.

Conficker. (2009). Vikipedia. 26 Şubat 2020 tarihinde https://tr.wikipedia.org/wiki/Conficker adresinden erişildi.

Çavuş, M. (2018). btGünlüğü, Siber Saldırılara Karşı 7 Etkin Savunma. 22 Mart 2020 tarihinde https://www.btgunlugu.com/siber-saldirilar-a-karsi-7-etkin-savunma/ adresinden erişildi.

Darıcılı, A.B. (2017). Demokrat Parti Hack Skandalı Bağlamında ABD ve RF'nin Siber Güvenlik Stratejilerinin Analizi, *Uluslararası Çalışmalar Dergisi. 1*(1), 1-24.

Deutsche Welle. (2012). En tehlikeli virüs: Flame. 25 Şubat 2020 tarihinde https://www.dw.com/tr/en-tehlikeli-vir%C3%BCs-flame/a-15988868 adresinden erişildi.

Devlette, Siber Saldırı Nedir Siber Saldırı Nasıl Yapılır. 29 Mart 2019 tarihinde https://www.devlette.com/siber-saldiri-nedir-siber-saldiri-nasil-yapilir/ adresinde erişildi.
Docplayer, Siber Savaş, Siber Savunma, USOM 21 Mart 2020 tarihinde https://docplayer.biz.tr/1207453-Sunum-icerigi-1-siber-savas-siber-teror-2-siber-savunma-3-usom.html adresinden erişildi.
Ercan, M. (2015). *Kritik Altyapıların Korunmasına İlişkin Belirlenen Siber Güvenlik stratejileri*, (Yüksek Lisans Tezi). Gebze Teknik Üniversitesi/Sosyal Bilimler Enstitüsü, Gebze.
Erkek, İ. (2018). *Modbus Temelli Scada Sistemlerinin Siber Güvenliği İçin Yeni Bir Yaklaşım*, (Yüksek Lisans Tezi). Gazi Üniversitesi/Fen Bilimleri Enstitüsü, Ankara.
Elektronik İmza. (2017, 13 Ocak). Vikipedi, Elektronik İmza. 25 Mart 2020 tarihinde https://tr.wikipedia.org/wiki/Elektronik_imza#cite_note-1 adresinden erişildi.
ESET, Antivirus nedir? 26 Mart 2020 tarihinde https://www.eset.com/tr/antivirus-software/ adresinden erişildi.
eTR Elektronik Ticaret rehberi. 25 Mart 2020 tarihinde http://www.elektronikticaretrehberi.com/eimza_nedir.php#Elektronik%20imzan%C4%B1n%20%C3%B6zellikleri%20nelerdir adresinden erişildi
Filiz, S. (2012). *Siber Güvenlikte Biyometrik Sistemler ve Yüz Tanıma*, *(*Yüksek Lisans Tezi). Bilgisayar Bilimleri Gazi Üniversitesi/Bilişim Enstitüsü, Ankara.
Göçoğlu, V. (2018). *Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi,* (Doktora Tezi). Hacettepe Üniversitesi/Sosyal Bilimler Enstitüsü, Ankara.
Güntay, V. (2017). Siberbulten, Beklentilerin Üstünde Bir Siber Saldırı Wannacry. 3 Mart 2020 tarihinde https://siberbulten.com/makale-analiz/beklentilerin-ustunde-bir-siber-saldiri-wannacry/ adresinden erişildi.
Habıb, S.Z. (2018). *Investıgatıon Of Afghanıstan Network Infrastructure For Cyber Securıty* (Çev.). Yüksek Lisans Tezi, T.C. Sakarya Üniversitesi/Fen Bilimleri Enstitüsü, Sakarya.
İçerik Filtreleme. (2017, 2 Mart). Vikipedia, İçerik Filtreleme Programı. 25 Mart 2020 tarihinde https://tr.wikipedia.org/wiki/%C4%B0%C3%A7erik_filtreleme_program%C4%B1 adresinden erişildi.
Information System Security Directorate (Çev.). IslamicRepublic of Afghanistan. 15 Mart 2020 tarihinde http://nic.af/en/page/what-we-do/cyber-crime/cyber-awareness adresinden erişildi.
Information Systems Security Directorate İslamc Republic OF Afghanistan (Çev.). National Cybersecurity Strategy of Afghanistan. (2014). 12 Mart 2020 tarihinde http://nic.af/en/page/knowledge-base/national-cyber-security-strategy adresinden erişildi.
İsnet, Oltalama-Yemleme Saldırısı nedir. (2019). 20 Nisan 2019 tarihinde https://www.isnet.net.tr/BlogIcerik/Phishing-Oltalama-Yemleme-Sald%C4%B1r%C4%B1s%C4%B1-Nedir-isnet-blog adresinden erişildi.
Jstor. (2017). Vikipedi, Güvenlik Duvarı. 24 Mart 2020 tarihinde https://tr.wikipedia.org/wiki/G%C3%BCvenlik_duvar%C4%B1 adresinden erişildi.
Kamis, E. (2017). Siber Güvenlik nedir. 3 Mart 2019 tarihinde https://www.eneskamis.com/siber-guvenlik-nedir/ adresinden erişildi.

Karakuzu, Ö. (2015). *Bilgi Toplumu Dönüşüm Sürecinde E-Devlet Kavramının Siber Ülke Güvenliği Açısından Değerlendirilmesi*, (Yüksek Lisans Tezi). T.C. İnönü Üniversitesi/Sosyal Bilimleri Enstitüsü, Malatya.
Kara, M. (2013). *Siber Saldırılar, Siber Savaşlar ve Etkileri*, (Yüksek Lisans Tezi). İstanbul Bilgi Üniversitesi/Sosyal Bilimler Enstitüsü, İstanbul.
Kariyer Geliştirme Uygulama ve Araştırma Merkezi, Bilişim'de Kariyer, İstanbul Üniversitesi. 2 Nisan 2019 tarihinde http://cdn.istanbul.edu.tr/FileHandler2.ashx?f=bilisimdekariyer2.pdf adresinden erişildi.
Kaspersky, Veri Şifreleme Nedir? 30 Mart 2020 tarihinde https://www.kaspersky.com.tr/resource-center/definitions/encryption adresinden erişildi.
Kök Kullanıcı Takımı. (2006). Vikipedia, 11 Nisan 2029 tarihinde http://www.0wikizero.com/index.php?q=aHR0cHM6Ly90ci53aWtpcGVkaWEub3JnL3dpa2kvS8O2a19rdWxsYW7EsWPEsV90YWvEsW3EsQ adresinden erişildi.
Ministry of Communications and Information Technology (Çev.). Information Regarding The Potential Cyber-Attack On The .GOV.AF Websites. 14 Mart 2020 tarihinde https://mcit.gov.af/information-regarding-potential-cyber-attack-govaf-websites-3 adresinden erişildi.
Ministry of Communications and Information Technology (Çev.). Draft Cybersecurıty Plan. (2015). 19 Nisan 2020 tarihinde https://mcit.gov.af/sites/default/files/2018-12/DRAFT%20CYBER%20SECURITY%20PLAN%20%20Dec%205%202015.pdf adresinden erişildi.
Özbay, R. (2015). *Aktif Siber Savunma Teknikleri Ve Performans Analizi*, (Yüksek Lisans Tezi). Afyon Kocatepe Üniversitesi/Fen Bilimleri Enstitüsü, Afyonkarahisar.
Sağıroğlu, Ş. (2018). BGD Siber Güvenlik ve Savunma Kitap Serisi1, 1-21: Cilt 1. *Siber Güvenlik ve Savunma.* Farkındalık ve Caydırıcılık.
Selek, A. (2015). Elektrik port, Zombi Bilgisayar Nedir? 2 Mayıs 2020 tarihinde https://www.elektrikport.com/teknik-kutuphane/zombi-bilgisayar-nedir-1-bolum/14933#ad-image-0 adresinden erişildi.
Sertçelik, A. (2015). Siber Olaylar Ekseninde Siber Güvenliği Anlamak, *Medeniyet Araştırmaları Dergisi*, 2(3) https://dergipark.org.tr/en/pub/mad/issue/35779/443816
Siber Tehdit. (2016). Siber güvenlik nedir. 5 Mart 2019 tarihinde http://sibertehdit.com/siber-guvenlik-nedir/ adresinden erişildi.
Siberbulten, Conficker yedi yaşında ama ilk günkü kadar zararlı (2015). 26 Şubat 2020 tarihinde https://siberbulten.com/siber-guvenlik/conficker-yedi-yasinda-ama-ilk-gunku-kadar-zararli/ adresinden erişildi.
Siberbulten, Sony'nin hacklenme hikâyesi. (2015). 28 Şubat 2020 tarihinde https://siberbulten.com/uluslararasi-iliskiler/sonynin-hacklenme-hikayesi-sacma-bir-komedi-siber-teroru-nasil-tetikledi/ adresinden erişildi.
Siberbulten, Bangladeş vurgunun arkasında Kuzey Kore mi var. (2016). 29 Şubat 2020 tarihinde https://siberbulten.com/siber-guvenlik/banglades-vurgunun-arkasinda-kuzey-kore-mi-var/ adresinden erişildi.
Siberbulten, Bangladeş Merkez Bankasına siber soygun vurgunu. (2016). 29 Şubat 2020 tarihinde https://siberbulten.com/siber-guvenlik/banglades-merkez-bankasina-siber-soygun-vurgunu/ adresinden erişildi.
Siberbulten, NSA Sızıntısı. (2016). 2 Mart 2020 tarihinde https://siberbulten.com/uluslararasi-iliskiler/nsa-sizintisi-milyon-dolarlik-siber-silahlar-cocuklarin-eline-mi-gecti/ adresinden erişildi.

Siberbulten, Dünya şokta, 30 ülkedeki sabit sürücülere casus yazılım. (2015). 2 Mart 2020 tarihinde https://siberbulten.com/uluslararasi-iliskiler/dunya-sokta-30-ulkedenki-sabit-suruculere-casus-yazilim-yerlestirilmis/ adresinden erişildi.
Siberbulten, WannaCry'in Türkiye'ye etkisi sınırlı kaldı. (2017). 3 Mart 2020 tarihinde https://siberbulten.com/sektorel/glbl/wannacryin-turkiyeye-etkisi-sinirli-kaldi/ adresinden erişildi.
Surveillance Self-Defense, Şifreleme Hakkında Bilinmesi Gerekenler. (2018). 30 Mart 2020 tarihinde https://ssd.eff.org/tr/module/%C5%9Fifreleme-nedir adresinden erişildi.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2012). *Bilgi Güvenliği Derneği.* 23 Mart 2019 tarihinde https://www.bilgiguvenligi.org.tr/wpcontent/uploads/2016/03/Ulusal_Siber_Guvenlik_Stratejisi.pdf adresinden erişildi.
Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2013). 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı. 3 Mart 2019 tarihinde https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf adresinden erişildi.
T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı. 15 Mayıs 2020 tarihinde https://www.uab.gov.tr/siber-guvenlik adresinden erişildi.
Terramedusa. (2013). Sürekli Veri Elde Etme Siber Casusluk. 7 Mayıs 2019 tarihinde https://terramedusa.com/surekli-veri-elde-etme-siber-casusluk/ adresinden erişildi.
TurkHack Team, Syber Security Platform. 20 Mart 2019 tarihinde https://www.turkhackteam.org/web-server-guvenligi/961285-guvenlik-prensipleri.html adresinden erişildi.
Tübitak, Bilgem, Siber Güvenlik Enstitüsü. 29 Mart 2020 tarihinde https://sge.bilgem.tubitak.gov.tr/tr/cozumler/stams-siber-tehditleri-algilama-merkezi-sistemi adresinden erişildi.
Türk Dil Kurumu, Bilişim. 22 Mart 2019 tarihinde https://sozluk.gov.tr/?kelime=B%C4%B0L%C4%B0%C5%9E%C4%B0M adresinden erişildi.
Türkkep, e-İmza (Elektronik imza) nedir? 25 Mart 2020 tarihinde https://www.turkkep.com.tr/e-imza adresinden erişildi.
Ünver, G.N. (2017). Güvenlik Strateji Belgelerinde İnsan Hakları**,** *Cyber Politik Journal, Siber Plitikalar Dergisi, 2*(3), 101-126.
Ünver, M., Canbay, C. & Mirzaoğlu, A.G. (2011). Siber güvenliğin sağlanması, Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler. 25 Nisan 2019 tarihinde https://www.academia.edu/24841538/Ulusal_Siber_G%C3%BCvenli%C4%9Fin_Sa%C4%9Flanmas%C4%B1 adresinden erişildi.
Yaşar, H., & Çakır, H. (2015). Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri, *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*. 3(2), 488 - 507
Yazıcı, A., & Akkaya, M.U. (2015). Siber Güvenlik ve Kritik Altyapı Güvenliği Çalışma Grubu, *Türkiye Bilişim Derneği*, Kamu Bilişim Merkezleri Yöneticileri Birliği. 18 Nisan 2020 tarihinde http://www.kamu-bib.org.tr/kamubib-17/wp-content/uploads/2015/10/Kamu-BIB-CG1-Siber-Guvenlik-ve-Kritik-Altyapilar.pdf adresinden erişildi.

Yener, Y. (2015). Siberbulten, 8.Yılda Estonya Saldırılarına Çok Boyutlu Bir Bakış. 14 Şubat 2020 tarihinde https://siberbulten.com/siber-saldirilar-2/8-yilinda-estonya-saldirilarina-cok-boyutlu-bir-bakis/ adresinden erişildi.
Yıldız, M. (2014). *Siber Suçlar ve Kurum Güvenliği*. (Denizcilik Uzmanlık Tezi). T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

ÖZGEÇMİŞ

1990 yılında Afganistan'ın Badakshan (Bahdahşen) şehrinde dünyaya geldim ilkokul, ortaokul ve lise eğitimimi aynı şehirde Sayed Abdul Karim Husaini lisesinde tamamladıktan sonra dost ve kardeş ülke Türkiye'ye tam burslu olarak gelip Trakya Üniversitesi Bilgisayar Mühendisliği Bölümünde 2017 yıllında Lisan ve 2020 yılında ise Yüksek Lisans eğitimimi tamamladım.