İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

SİBER SALDIRILAR VE ÜLKELERİN SİBER GÜVENLİK POLİTİKALARI

Su Dilara ALİOĞLU
113692001

Prof. Dr. Şule Işınsu ÖZMEN

İSTANBUL
2019

Siber Saldırılar ve Ülkelerin Siber Güvenlik Politikaları

Cyber Attacks and Countries Cyber Security Policies

Su Dilara ALİOĞLU
113692001

Tez Danışmanı : Prof. Dr. Şule IŞINSU ÖZMEN (İmza) .....
İstanbul Bilgi Üniversitesi İşletme Fakültesi

Jüri Üyeleri : Prof. Dr. Cem Sefa SÜTCÜ (İmza) .....
Marmara Üniversitesi İletişim Fakültesi

Dr. Öğr. Üyesi Mehmet Bedii KAYA (İmza) .....
İstanbul Bilgi Üniversitesi Hukuk Fakültesi

Tezin Onaylandığı Tarih : 13 Haziran 2019
Toplam Sayfa Sayısı : 241

Anahtar Kelimeler (Türkçe)
1) Siber Güvenlik
2) Siber Saldırı
3) Bilişim Hukuku
4) Güvenlik politikaları
5) Siber Uzay

Anahtar Kelimeler (İngilizce)
1) Cyber Security
2) Cyber Attack
3) İnformation Technology Law
4) Security Policies
5) Cyber Space

İÇİNDEKİLER

KISALTMALAR

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AGİT	Avrupa Güvenlik ve İşbirliği Teşkilatı
ANSSI	The National Cybersecurity Agency of France(Agence nationale de la sécurité des systèmes d'information)
APT	Advanced Persistent Threat
ARPANET	Advanced Research Projects Agency Network
BCS	The Chartered Institute for IT
BGYS	Bilgi Güvenliği Yönetim Sistemleri
BRICS	Brasil, Russia, India, China, South Africa
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojileri Araştırma Merkezi
BİS	Bilgi Ve İletişim Sistemleri
BİT	Bilgi Ve iletişim Teknolojileri
bkz.	bakınız
BM	Birleşmiş Milletler
BOME	Bilgisayar Olaylarına Müdahale Ekibi
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CA	Certificate Authorities
CDI	Critical Data Infrastructure
CERT	Computer Emergency Response Team
CERT/CC	Computer Emergency Response Team Coordination Center
CERT-In	India National Computer Emergency Response Team
CERT-UK	United Kingdom National Computer Emergency Response Team
CIA	Central Intelligence Agency
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CISP	Cybersecurity Information Sharing Partnership
CMK	5271 sayılı Ceza Muhakemesi Kanunu

CMP	Crisis Management Plan
CNCI	Comprehensive National Cybersecurity Initiative
COE	Council Of Europe
CPHC	Council of Professors and Heads of Computing
CPNI	Center for the Protection of National Infrastructure
CSIRT	Computer Security Incident Response Team
CSIRT-UK	United Kingdom Computer Security Incident Response Team-
CYMAT	Cyber Incident Mobile Assistant Team
DDOS	Distributed Denial of Service
DNS	Domain Name System
DOJ	Department of Justice
DOS	Denial of Service
ENISA	European Network and Information Security Agency
EUROPOL	European Police Office
E3A	Einstein 3 Accelerated
FAPSI	Federal Agency for Government Communications and Information-
FBI	Federal Bureau Of Investigation
FSB	Federal Security Service
FTC	Federal Trade Commission
GAÖ	Güven Arttırıcı Önlem
GCHQ	Government Communications Headquarters
GSD	General Staff Department
GSES	Grid Security Expert System
GSOC	The Government Security Operation Coordination Team
HMRC	Her Majesty's Revenue and Customs
HRW	Human Rights Watch
ICS-CSIRT	Industrial Control Systems - Computer Security Incident Response Team
IC-IRC	Intelligence Community-Incident Response Center
IM	Instant Message
IP	Internet Protocol

IPA	Information –Technology Promotion Agency
IPv6	Internet Protocol version 6
ISAC	Information Sharing and Analysis Center
ISC	Internet Systems Consortium
ISS	İnternet Servis Sağlayıcı
ISTF	Inter Departmental Information Security Task Force
MEITY	Ministry of Electronics and Information Technology
NATO	North Atlantic Treaty Organization
NCCC	National Cyber Coordination Center
NCIIPC	National Critical Information Infrastructure Protection Centre
NCSC	National Cyber Security Center
NHPC	National Hydroelectric Power Corporation
NIC	National Informatics Center
NISC	National center of Incident readiness and Strategy for Cybersecurity
NIST	National Institute of Standarts and Technology
NIS	Network and Information Security
NPC	National People's Congress
NSA	National Security Agency,
NSD	National Security Database
NTOC	NSA/CSS Threat Operations Center
NTPC	National Thermal Power Corporation
NTRO	National Technical Research Organisation
OECD	Organisation for Economic Co-operation and Development
OPM	Office of Personel Management
OT	Operasyonel Teknoloji
PGCIL	Power Grid Corporation of India Limited
PLA	People’s Liberation Army
PLC	Programmable Logic Controller
P2P	Peer to Peer communication
SCADA	Supervisory Control And Data Acquisition
SDF	Self- Defence Forces

SGE	Siber Güvenlik Enstitüsü
SLTT	State, Local, Tribal, and Territorial Governments
SOME	Siber Olaylara Müdahale Ekibi
SSCB	Sovyet Sosyalist Cumhuriyeti Birliği
STK	Sivil Toplum Kuruluşu,
SQL	Structured Query Language
TBMM	Türkiye Büyük Millet Meclisi
TCK	5237 sayılı Türk Ceza Kanunu
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TR- BOME	Türkiye Bilgisayar Olaylarına Müdahale Ekibi
TR-CERT	Turkey Computer Emergency Response Team
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UDP	User Datagram Protocol
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
UNIDIR	United Nations Institute for Disarmament Research
US-CERT	United States Computer Emergency Readiness Team
USGT	Ulusal Siber Güvenlik Tatbikatı
USOM	Ulusal Siber Olaylara Müdahale Merkezi
VPN	Virtual Private Network
YÖK	Yüksek Öğretim Kurumu

ABSTRACT

With the problems and responsibilities brought by the development of digital technology, the concepts of cyber crime, cyber security and information security have been an important topic of discussion in our country and in the world in recent years.

The subject of this study is to examine cyber attacks and countries' cyber security strategies.

In the scope of this study, the concept of cyber attack will be examined. In the first part the characteristics of the attacks, the methods of the attacks, the attackers, the protection methods and the damages caused by cyber attacks will be analyzed in detail within technical and legal dimensions.

In the second part the concept of cyber security and information security will be explained and in the scope of these concepts cyber security strategies and the consequences of these attacks in Turkey as well as other countries and International Organizations will be discussed with examples.

Throughout this study, a separate and detailed examination was made on the basis of countries. Cyber security strategy documents of these countries were examined and the documents they have published were evaluated. Within the scope of these strategy documents, cyber security strategy policies were examined in detail and the legal infrastructure, deficiencies and requirements of cyber security were discussed.

ÖZET

Dijital teknolojinin her geçen gün gelişmesiyle birlikte getirdiği sorun ve sorumluluklarla birlikte ülkemizde ve dünyada son yıllarda siber suç, siber güvenlik ve bilgi güvenliği gibi kavramları tartışılmaya başlanmıştır.

Çalışmanın konusu Siber Saldırılar ve ülkeler bazında oluşturulan siber günvelik stratejilerinin incelenmesidir.

Bu çalışma kapsamında birinci bölümde siber saldırı kavramı, çeşitleri detaylı olarak incelenecek olup saldırıların özellikleri, yapılış biçimleri, saldırganlar ve korunma yöntemleri ve siber saldırılar sonucu meydana gelen zararlar teknik ve hukuksal boyutta detaylı analizi yapılacaktır.

İkinci bölümde ise siber güvenlik ve bilgi güvenliği kavramları açıklanacak olup bu güvenliğin sağlanma yöntemleri ile siber güvenlik ve bilgi güvenliği kavramları kapsamında Türkiye'nin, ülkelerin ve Uluslararası Örgütlerin siber güvenlik stratejileri ve siber saldırılara yaklaşımları ile saldırıların sonuçları örneklerle ele alınacaktır.

Çalışma kapsamında ülkeler bazında ayrı ayrı ve detaylı inceleme yapılmış olup incelenen ülkelerin siber güvenlik strateji belgeleri ve yayınladıkları belgeler değerlendirilmiş, bu strateji belgeleri kapsamında siber güvenlik strateji uygulamaları detaylı olarak incelenerek siber güvenliğin hukuki altyapısı, eksiklikler ve gereklilikler tartışılmıştır.

GİRİŞ

1960'lı yıllarda ARPANET ile doğan 1990'lı yıllarda Tim Berners Lee tarafından yaratmış olan World Wide Web (Dünya çapındaki ağ) anlamına gelen internet insanlık tarihin en büyük buluşlarından biridir.

Siber uzayın 27 yılda ulaştığı boyut düşünüldüğünde internet çağında teknolojinin hızlı ilerleyişi, bilgisayarın ve internetin günlük yaşamın her alanına yayılması hayatımızı her anlamda kolaylaştırdığı gibi ihtiyaç duyabileceğimiz her şeyi internet ortamında yapabilmemizi sağlarken , ulusal ve uluslararası düzeyde de birçok problemi, suçu ve sorumluluğu beraberinde getirmiştir. Bu her alana yayılmışlık kolaylıkların yanında zafiyetlerinde artmasına sebep olmuştur.

İnternet gibi her an herkesin ulaşımı altında olan küresel çapta bir bağlantı aracı ile erişimin sağlandığı bir ortamda bilgi ve veri güvenliği her zaman birinci derecede öncelik sağlanması gereken bir sorun olarak ortaya çıkmaktadır. Teknolojinin gelişmesiyle bilgi çoğalmakta ve bilgiye ulaşımın kolaylaşması ile bilgiyi koruma her zamankinden önemli hale gelmektedir. Bilginin erişilmesi, korunması, paylaşılması hatta gerçek bilginin elenmesi bir sorunsal olarak karşımıza çıkmaya başlamıştır.

İnternet her an elimizin altında olduğundan zafiyetleri de beraberinde getirmekte siber alanda her an saldırıya uğrama ihtimalimizi daha da arttırmaktadır. Siber uzayın bu inanılmaz ilerleyişi siber saldırı, siber suç ve siber güvenlik kavramlarını hayatımıza sokmuştur. Siber saldırılar kişi, kurum ve devletlerin güvenliklerini tehdit etmekte ve doğrudan ya da dolaylı bir çok zarara sebebiyet vermektedir.

Bu kapsamda çalışmamızda siber saldırılar kavramı ve saldırıların nasıl yapıldığı bilinebildiği ölçüde açıklanmaya çalışılmıştır. Siber saldırı yöntemleri de siber uzay gibi her geçen dakika gelişmekte, evrim geçirmekte ve alınan her güvenlik önlemine karşı yeni bir saldırı tipi ortaya çıkmaktadır. Bu sebeple çalışma içerisinde siber saldırılar tüketici olarak sayılmamış olup temel saldırı tiplerine değinilmiştir. Tabi ki hayatın her alanında olduğu gibi siber uzayda da en büyük

zaafiyet unsurunun yine kişi faktörü yani insan olduğu görülmüştür. En çok zarar veren saldırı tipi sosyal mühendislik denilen manipülasyon yöntemi ile yapılan saldırılardır. En büyük zararlar alınması gereken önlemlerin alınmaması, en basitinden şifrelerin dahi değiştirilmemesi veya yeterli özenin gösterilmemesi sebebiyle meydana gelmekte, günümüzde her 3 kişiden biri siber saldırıya maruz kalmaktadır. Bu istatistik siber uzayda güvenliğin bu kapsamda siber güvenliğin ne kadar önemli olduğu bir kez daha göstermektedir.

İnternet günlük yaşantının her alanına yayıldığı gibi artık ülkelerin eskiden ulusal sınırları içerisinde kalan ve ülkesel sınırlarla ayrılan ulusal savunma ve güvenlik konuları da bu yayılmadan nasibini almıştır. Her alanda olduğu gibi belki de en büyük risk öğesi olarak ulusal savunma ve güvenlik konularında da bilgi güvenliği en temel sorun haline gelmiştir.

Siber Güvenlik alanında yaşanan zafiyetlerin ve güvenlik ihlallerinin her geçen gün artması, kişileri, kurumları ve devletleri; yazılım, donanım ve çevre faktörlerini de dikkate alarak oluşturulacak yeni güvenlik yaklaşımları geliştirmeye mecbur bırakmaktadır.

Bu durumun doğal bir neticesi olarak bilgi ve bilgi güvenliği kavramları finans, ekonomi, bankacılık, hukuk, ticaret, elektronik imza, eğitim, elektronik devlet uygulamaları ve haberleşme gibi bir çok alanda ortaya çıktığı gibi bu alanlarda yeni düzenlemeler getirilmesini zorunlu kılmıştır (YALMAN Y.)[1].

Ülkeler açısından bakıldığında siber güvenlik kavramı ulusal savunma politikaları içerisinde çok önemli bir konuma gelmiştir. Devletler tarafından ulusal güvenliğin sağlanması için kurulan fiziki orduların yanında artık siber ordular oluşturulmaya başlanmıştır. Savaşlar siber uzaya taşınmış ve bilgi savaşına dönüşmüştür. Siber casusluk ve siber savaşlar ile birlikte ulusal güvenliğe yönelik tehdit algıları farklılaşmış olup bu bağlamda güvenlik algılamaları da değişmiştir. Ülkeler bu kapsamda siber güvenlik politika belgeleri yayınlamakta olup siber

[1] Bkz. Doç. Dr. Yıldıray YALMAN," *Güncel Tehdit ; Siber Saldırılar*", Seçkin Yayınları, 8. Bölüm, Bilgi Güvenliği Riskleri ve Bilgi Güvencesi, s. 207

olaylara müdahale ekipleri kurmuşlar, siber alanda düzeni sağlamak için mevzuatsal düzenlemelere gitmişlerdir. Bu çalışma kapsamında ülkelerin siber güvenlik stratejilerine ilişkin düzenlemeleri ile strateji belgeleri ve neticesinde siber güvenlik alanında yaptıkları ve yapmakta oldukları uygulamalar karşılaştırmalı olarak etraflıca değerlendirilmiştir.

BİRİNCİ KISIM
SİBER SALDIRILARA GENEL BAKIŞ

1. KAVRAMLAR

"Siber uzay, tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortamdır[2]". Bu sebeple siber kavramını sadece internet olarak algılamamak gerekir[3]. Siber uzay öncelikle bir bilgi ortamıdır. Sırf sanal bir ortam olmamakla birlikte yaratılan, saklanan ve paylaşılan dijital verilerden ve bu verileri saklayan bilgisayarlara ilave olarak bunların akışına izin veren sistem ve altyapılardan oluşur. Siber uzay kavramı içerisinde ağ tabanlı bilgisayarların interneti, kapalı intranet sistemler, hücresel teknolojiler, fiber optik kablolar ve uzay tabanlı iletişim bulunmaktadır.

Bilişim teknolojisi, bilgi ve iletişim teknolojileri alanındaki bütün unsurları ifade etmektedir.

Siber kavramı ise; bilgisayar ağlarına ve internete ait olan ve sanal gerçeklik anlamına gelmektedir.

2009 tarihinde ABD Ulusal Araştırma Konseyi Siber Saldırıyı "bilgisayar sistemleri, ağlar veya bilgiyi ve/veya bunlarda yerleşik olan ya da bunları taşıyan programları değiştirmek, bozmak, aldatmak, küçük düşürmek veya yok etmek için yapılan kasıtlı hareketler olarak[4]" tanımlanmıştır. (SİNGER & FRİEDMAN, Mart 2015)

2. SİBER SALDIRILARIN AMAÇ VE UYGULAYICI BAZINDA KATEGORİLENDİRİLMESİ

---

[2] Bkz. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı "2016-2019 Ulusal Siber Güvenlik Stratejisi", s.7, http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf

[3] Bkz. Clarke, Richard A.; Knake, Robert K. , Siber Savaş, (Çeviren:Murat Erduran), İkü YayınEvi, Nisan 2011, s.44

[4] Bkz. Singer,P.W.;Friedman,Allan, Siber Güvenlik Ve Siber Savaş, (Çeviren : Ali Atav), Buzdağı Yayınevi, 1. Baskı, Mart 2015,s.29

Siber Saldırıların saldırının motivasyonu, hedef kitlesi ve saldırılarda kullanılan yöntemler metotlar göz önüne alındığından şu şekilde kategorilendirilebilmesi mümkündür;

- Siber Terörizm kavramı "belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere ve mallara karşı bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla kullanılmasıdır. Terör örgütleri internet ortamında propaganda ve eğitim, haberleşme, bilgi toplama ve sanal saldırı faaliyetleri gerçekleştirmektedir. Terör eylemlerinin internet üzerinden yürütülmesi işlemidir[5]."

- Siber Hacktivizm kavramı İnternet üzerinden örgütlenen kişilerin devletler tarafından saklandığını veya müdahale edildiğini iddia ettiği bilgiye erişme ve bilgiyi topluma açık hale getirmek/yaymak amacıyla yapılan siber alanda yapılan aktivist eylemlerdir[6]. Siber Aktivistler olarak anılan hacktivist kavramı ise "Dünya görüşleri çerçevesinde kötü veya uygunsuz gördükleri toplumsal ya da politik sorunları dile getirmek amacı ile kamu ya da özel sektör siber uzaylarına saldırı düzenleyen şahıs ya da grupları[7]"ifade etmektedir.

- Siber Savaş kavramı bilişim sistemleri vasıtasıyla gerçekleştirilen bir hedefinde şirket, ülke veya grup olan sabotaj ve casusluk yapmak üzere siyasi amaçlı hack eylemi gerçekleştirilmesi anlamına gelmektedir[8]. Bu kavramda amaç belirtilen hedef gruplarına maddi ve manevi zarar vermektir.

- Siber Ordu kavramı ise bir ülke veya bir kurumu siber uzaydan gelebilecek veya mevcut saldırılara karşı koruma ve gerekli olduğunda karşı atak

---

[5]Bkz. Keçeci,Orçun "Siber Suçlar ve Siber Terörizm" oradan dipnot 26 http://mebk12.meb.gov.tr/meb_iys_dosyalar/60/01/201260/dosyalar/2016_03/29105407_siber_suclar_ve_terorizm.pdf (Erişim Tarihi: 29.04.2017)

[6]Bkz.http://www.bilisimhukuk.com/2012/08/hacktivizm-ve-siber-teror/ (Erişim Tarihi: 29.04.2017)

[7]Bkz. Siber Güvenliğe ilişkin Temel Bilgiler,USOM, Temmuz 2014, sy.10 belgenin orjinaline http://some.sdu.edu.tr/assets/uploads/sites/408/files/siber-guvenlige-iliskin-temel-bilgiler-22092017.pdf adresinden erişilmiştir. (Erişim Tarihi:29.04.2017)

[8] Bkz. http://en.wikipedia.org/wiki/Cyberwarfare (Erişim Tarihi: 02.05.2017)

olarak siber saldırı gerçekleştirebilecek bilgi güvenliği uzmanlarından[9] oluşan, uzmanların devlet eliyle yetiştirildiği veya devlet himayesinde kullandıldığı resmi veya gayriresmi birimlerden oluşan ordu anlamına gelmektedir.

- Siber Suç kavramı bilişim sistemi kullanılarak bir bilişim sisteminin güvenliğini, sistemdeki verileri, sistem kullanıcılarını hedef alarak ekonomik bir fayda elde etmek amacıyla işlenen suçlar bütünü olarak tanımlanabilir. Siber Suçlar bilişim sistemleri kullanılarak işlenmesi sebebi ile klasik suçlardan ayrılmaktadır. Bu suç türü bilgisayar ve internete özgü suçlar olarak da adlandırılabilir[10].

- Siber Sabotaj kavramı Bilgi sistemlerinin fonksiyonlarının bozulması veya tahrip edilmesi ve bilgiye hasar veren kasıtlı veya kötü niyetli eylemlerdir.[11] (BAYRAKTAR, 2015)

- Siber Casusluk kavramı ise bilişim sisteminde kullanıcının bilgisi dışında bireysel kullanıcıların, firmaların, kurum ve kuruluşların, devletlerin bilgi sistemlerinden internet veya kapalı devre intranet sistemleri üzerinden çeşitli siber taarruz yöntemleri kullanılmak suretiyle kişisel, kurumsal hassas veya gizli bilgilerin kişisel, askeri ve ekonomik amaçlar için elde edilmesi faaliyetidir[12]. (BAYRAKTAR, 2015)

---

[9]Bkz.https://istihbaratveanaliz.files.wordpress.com/2016/06/siber-tehditler-savunma-yntemleri-ve-hackerlarn-baars.pdf (Erişim Tarihi: 05.05.2017)

[10]Bkz.http://www.istanbul.pol.tr/sibersuclarlamucadele/Sayfalar/Siber_Suclar.aspx (Erişim Tarihi: 06.05.2017)

[11]Bkz.Bayraktar, Gökhan, Siber Savaş ve Ulusal Siber Güvenlik Stratejisi, Yeniyüzyıl yayınevi, 1. Basım, 2015 sy.81

[12]Bkz.Bayraktar, Gökhan, Siber Savaş ve Ulusal Siber Güvenlik Stratejisi, Yeniyüzyıl yayınevi, 1. Basım, 2015 sy.51

Saldırı Türleri	Motivasyon	Hedef Kitle	Metot
Siber Suçlar	Ekonomik fayda	Kişisel Kullanıcılar, Firmalar	Kullanıcı Bilgilerini Çalma, Sahtekarlık, Şantaj, Saldırı, Güvenlik Açığı Kullanımı, Lisanssız Yazılım Kullanımı vb.
Hactivism (Siber Korsanlık)	Politik amaçlar ve değişiklikler, kişisel tatmin	Kurumlar, Devletler	Siber ortamdaki saldırı yöntemlerinin kullanımı
Siber Casusluk	Ekonomik fayda ve kritik bilgi kazanımı	Kişisel Kullanıcılar, Firmalar, Devletler	Siber ortamdaki saldırı yöntemlerinin kullanımı, Güvenlik Açığı Kullanımı,
Siber Terör	Politik değişiklikler	Devletler	Bilgisayar-tabanlı şiddet ve yıkım
Siber Sabotaj	Ekonomik fayda, kişisel tatmin	Kurumlar, Devletler	Güvenlik Açığı Kullanımı, İnsan faktörü,
Siber Savaş	Politik veya askeri fayda	Kritik Bilgi Sistem Altyapıları, askeri bilgi sistemleri	Siber ortamdaki saldırı yöntemlerinin kullanımı, Güvenlik Açığı Kullanımı

13

Siber ortamda yapılan eylemlerin bir çok amacı olabilmektedir. Saldırılar her zaman politik çıkarlar ya da siber savaş amacı ile yapılmamakta olup bu tip saldırılar kişi/kurum güvenliği açısından tehdit oluştursa da ulusal güvenlik açısından tehdit oluşturmamaktadır.

Siber saldırılardan farklı olarak siber suçlar, klasik suçlar gibi belirli bir kişi, kişiler veya suç örgütleri tarafından işlenebilmekte olduğundan ve hukuk düzenine aykırı - hukuka aykırı fiil kapsamında değerlendirildiğinden suç olarak tanımlanmıştır. Bireyler ve kurumlar için tehdit oluşturan siber suçlar ulusal güvenlik tehditi oluşturmamakta ve ekonomik çıkar elde etmek için diğer klasik suçlar gibi işlenebilmektedir. Sadece ekonomik çıkar sağlamak amacı ile işlenen

[13]Bkz.Bilgi Güvenliği Raporu, 3. Kısım Bilgi Güvenliği ve Bilişim Suçları, sy.754 http://www.biakraporu.org/docs/rapor.kisim3.bolum01.pdf (Erişim Tarihi: 09.07.2017)

banka sistemine girilmesi suçu, internet üzerinden çocuk pornografisi yayma gibi eylemler siber suç olarak değerlendirilmekte olup ulusal güvenliği tehdit etmediğinden siber saldırı ya da siber savaş kapsamında sayılamazlar.

Siber saldırı daha geniş bir kavram olmakla birlikte ise, siber alandaki mevcut imkanlar kapsamında bilişim sistemlerine yetkisiz olarak yapılan kötü niyetli faaliyetler bütünüdür.

Bazı siber saldırı türlerinin devletlere bağlı kişi veya kuruluşlar vasıtasıyla işlenmekte olmasına rağmen bu saldıırlar siber savaş veya siber suç kapsamında değerlendirilmemektedir. Örnek olarak, 2011 yılında Çin tarafından Falun Gong isimli ruhani bir grubun internet sitesine Çin devleti tarafından politik ve ulusal güvenlik amaçlı olarak siber saldırı düzenlemiş olup bu saldırılar bir devlet eliyle gerçekleştirilmiş olduğundan siber suç kapsamına girmemekte olup fiilin hedef kişisi başka bir devlet olmadığından siber savaş kapsamında da değerlendirilmemektedir.

Bir başka siber saldırı türü kişi veya gruplar tarafından işlenmesine rağmen suç teşkil etmediğinden siber suç kapsamında değerlendirilmeyen siber saldırılardır.

Bir başka siber saldırı türünde ise devlet dışı kişi ya da grupların suç oluşturan hukuka aykırı faaliyetleri veya bu kişi veya gurpların ulusal güvenliği tehdit edecek politik amaçlı saldırıları hem siber saldırı hem de siber suç kapsamında değerlendirilmesi mümkündür. Bu tip saldırılara devlet dışı kişi ya da grupların politik veya ulusal güvenliği tehdit amacıyla devletin resmi kayıtlarının tutulduğu sistemleri kapatması veya zarar vermesi bu birleşik eyleme örnek gösterilebilir[14]. (Mehmet Yayla, 2014)

Siber saldırılar siber hacktivizm de olduğu gibi politik konular, vatanseverlik, e-demokrasi, siber güvenlik hususlarındaki eksikliklerin ortaya

[14] Bkz. Mehmet Yayla, "Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı", Hacettepe Hukuk Fakültesi Dergisi , Cilt 4, Sayı 2, Yıl 2014, sy.185

çıkarılması, gizli bilgilerin ifşa edilmesi amacıyla yapılabileceği gibi bazen sırf diğerlerinden daha yetenekli olduğunu göstermek için bile yapılması mümkündür.

Siber saldırılar ile ulaşılmak istenen amaç bilgi ve iletişim Sistemlerine(BİS) yetkisiz erişim sağlamak, verileri değiştirmek, yok etmek, ifşa etmek veya üçüncü taraflara vermek olabileceği gibi hizmetin engellenmesi de olabilir.

BİS'e yetkisiz erişim, sisteme erişim yetkisi olmayan kişiler tarafından sistemin mevcut açıklarının tespit edilerek kullanılması veya o sisteme erişim yetkisi olan bir kişinin şifrelerinin sosyal mühendislik, ağ trafiğinin dinlenmesi, kötücül veya zararlı yazılımlar kullanılarak şifrelerin saklandığı dosyalara erişim sağlanması, şifrelenmiş parametrelerin kırılması, çevrebirimleri aracılığıyla casusluk yapılması gibi yöntemlerle ele geçirilerek Bilgi ve iletişim sistemlerine yetkisiz kişilerce erişilmesidir. Yetkisiz erişim, kişisel bilgilerin ve haberleşmenin gizliliğinin ihlal edilmesine sebep olabileceği gibi siber casusluk yapılması amacıyla da kullanılabilir.

Verilerin değiştirilmesi, yok edilmesi, ifşa edilmesi veya üçüncü taraflara verilmesi ise bir bilgi ve iletişim sisteminde saklanan, işlenen, iletilen verinin, sistemlere dışarıdan yetkisiz erişim, verilerin sistem içinden dışarıya sızdırılması veya yetkisiz erişim veya sızdırma olmaksızın klavye izlerinin izlenmesi gibi yöntemlerle ele geçirilmesi, ele geçirilen verilerin, sayısal ortamlar üzerinde bulunduklarından, elektronik, optik ve manyetik donanımlar veya özel yazılımlar kullanılarak kolaylıkla değiştirilebilmesi veya yok edilebilmesidir.

BİS'de ele geçirilen kişisel verilerin bazı yasadışı alanlarda satıldığı bilinmektedir. Bu kişisel veriler içerisinde en çok ele geçirilerek ekonomik amaçlı satılan verileri kişilerin kimlik bilgileri olmakla birlikte bu verilerin büyük ölçüde saklandığı ve işlendiği, eğitim, kamu hizmetleri, sağlık, finans gibi sektörlerde kullanılan bilgi ve iletişim sistemlerin, bu bilgilerin ele geçirilmesi ve ifşasına sebep olabilecek zafiyetler içermektedir. Söz konusu bilgilerin en fazla ifşa edildiği sektörlerin başında ise kamu hizmetleri ve finans sektörleri gelmektedir.

Hizmetin engellenmesi amacında ise bir Bilgi ve İletişim Sistemi -detayı daha sonra açıklanacağı üzere- DoS(Denial of Service), DDoS (Distributed Denial

of Service) veya e-posta bombardımanı gibi saldırı türleri ile iletilemkte olan veri trafiğini taşıyamaz hale gelebilmekte ve bu sebeple saldırı hedefi sisteme erişilememekte ve bu sistemlerden hizmet alınaması mümkün olamamaktadır. Ağ trafiğini farklı hedeflere yönlendirmek amacı ile kullanılan kötücül yazılımlar da hizmet engelleme saldırıları gibi şebekelerin işlerliğini tehdit etmekte, bu tehditler sebebi ile sistem yetkili kullanıcılara hizmet veremez hale gelmekte ve saldırıların hedefleri açısından bütük maddi kayıplara sebep olabildiği gibi itibar kaybına da sebep olabilmektedir[15]. (ÜNVER, CANBAY, & MİRZAOĞLU, 2009)

3. SİBER SALDIRI TÜRLERİ VE YÖNTEMLERİ

Siber uzayda, çok fazla saldırı çeşidi bulunmakta olup gelişen saldırı kapasitesiyle ve alınan güvenlik önlemlerine karşın saldırı çeşitlerine sürekli yenileri eklenmektedir.

Zararlı yazılımlar, Trojenler, Mantık bombaları, virüs ve solucanlar ile hizmeti engelleme saldırıları olan DDOS, sosyal mühendislik atakları, oltalama ve yemleme (phishing) saldırıları, klavye kaydediciler ve daha bir çok yöntem bulunmaktadır. Saldırganlar bu saldırı yöntemlerini kullanarak erişitikleri bilgi iletişim sistemleri üzeirnde sistemi bozucu veya yıkıcı, sistemin hizmetini aksatıcı veya içeriğindeki verileri sızdırıcı bir çok zarar vermeleri mümkündür. Bu zararların kuruluşlar ya da kamu kurumuna maddi zarar vermelerine sebep olabileceği gibi itibarın azalması şeklinde menavi zararlara da sebep olabilmektedir.

Bu bölümde siber saldırılar başlıklar altında türleri ve yapılış şekilleri anlatılmış olup temel saldırı türlerine değinilmeye çalışılmıştır. Günümüzde

---

[15] Bkz.Bilgi Teknolojileri ve iletişim Kurumu, Bilgi Teknolojileri Ve Koordinasyon Dairesi Başkanlığı, ÜNVER, Mustafa; CANBAY,Cafer; MİRZAOĞLU , Ayşe Gül, "*Siber güvenliğin sağlanması: türkiyedeki mevcut durum ve alınması gereken tedbirler*", Mayıs 2009, sy.16-21 https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FSayfalar%2FSiberGuvenlik%2Fsg.pdf (Erişim Tarihi: 20.07.2017)

çoğunlukla uygulanmakta olan bu saldırı türleri dışında sürekli yenilenen ve büyük bir hızla değişiklik gösteren daha bir çok saldırı yöntemi mevcuttur. Bu sebeple siber saldırılar tüketici biçimde sayılmamış temel olarak en çok kullanılan saldırı yöntemleri ve bu saldırıların uygulanış biçimleri kısaca incelenmeye çalışılmıştır.

3.1.Bilgisayar Korsanlığı

Günümüzde güncel ve yaygın kullanımıyla her türlü siber saldırı hack eylemi olarak nitelendirilmekte olup bir bilişim sistemine yasa dışı yollar kullanmak suretiyle giren kişilere hacker veya bilgisayar korsanı denilmektedir. Ancak Hack eylemi olarak bilinen bilgisayar korsanlığının diğer saldırılardan ayırt eden ve en temel özellikleri yapılışında kullanılan sadelik, ustalık ve faaliyetin yasa dışı olmasıdır. Hacker denilen kişi veya hack eylemi gerçekleştiren hackerlardan oluşan gruplar bu bağlamda hack eylemini gerçekleştiren kişiler olmakla birlikteinternet üzerinden erişilebilen, sistem zafiyetlerinin tespit edildiği ve bu zafiyetlerden ve bu faydalanılma yöntemlerinin adım adım anlatılmış olduğu belgeleri uygulamak ve başkaları tarafından bu amaçlarla üretilmiş programlar vasıtasıyla sistemlere girerek yapan saldırganlara lamer, cracker, script kiddie gibi isimler verilmiş olmakla bu faaliyetlere esas itibari ile bilgisayar korsanlığını oluşturmamaktadır.

Özet olarak açıklamak gerekirse bilgisayar korsanlığı kavramı bir bilişim sistemine yetkisiz erişim sağlamak amacı ile sistemin güvenlik tedbirlerini etkisiz hale getirmeye çalışmak olarak ifade edilebilir. Bu saldırı türünün gerçekleştirilmesi için bir çok yöntem kullanılmakta olup genel olarak bu faaliyetler işletim sistemlerinde bulunan zafiyetler, yaygın olarak kullanılan ve çoğunlukla ücretsiz temin edilen uygulama programlarında yada ağ bağlantılarında bulunan zafiyetlerin tespit edilmesi ve bu zafiyetler kullanılmak suretiyle saldırı gerçekleştirilmesi şeklinde olmaktadır.

Güncellenmemiş işletim sistemi veya uygulama programlarının üzerinde çalışan sistemlerin bilgisayar korsanlığına maruz kalması muhtemel riskler içermektedir[16]. (HEKİM & BAŞIBÜYÜK, 2014)

Bilgisayar korsanları tarafından uygulanan yöntemlerden işletim sistemlerinde, yaygın olarak kullanılan uygulama programlarında veya ağ bağlantılarında zafiyetler bularak bu zafiyetlerden faydalanılması yönteminin kullanıldığı saldırıların diğer bir çeşidi Zero-Day-Exploit saldırılarıdır. Türkçeye sıfırıncı gün açığı olarak geçen bu yöntem bilişim sistemi üzerinde keşfedilmiş ancak henüz duyurulmamış olan güvenlik zafiyetlerinin tespit edilmesine dayanmaktadır. Bir açık için Zero Day Exploit oluşturulduğu andan itibaren tecrübeli ya da amatör korsanlar fark etmeksizin ilgili açık herkes tarafından bulunabilir ve zarar verilebilir hale gelmektedir.

Bu saldırı türünde bilgisayar korsanı, üretici firmanın dahi varlığından haberdar olmadığı yeni bir açığı tespit edip kullanmaktadır. Günümüzde bir çok üretici firma bu tip açıkları tespit ederek kullanmak yerine üreticiye bildiren bilgisayar korsanlarına büyük ödüller vermektedir.

Bu yönteme örnek olarak 2014 yılı Nisan ayında tespit edilen bir güvenlik zafiyeti olan Heartbleed güvenlik açığı verilebilir. "Çoğu sunucunun kullandığı açık kaynak kodlu "OpenSSL" kütüphanesinde bulunan güvenlik açığı sayesinde saldırgan; yetkisi olmadığı halde aynı sunucudaki diğer kullanıcıların kredi kartı gibi özel bilgilerine erişebilmektedir. Bu güvenlik zafiyeti keşfedilir keşfedilmez " OpenSSL Zero Day Vulnerability" diye duyurulmuştur. Bu sebeplerle üretici veya geliştirici firma tarafından desteği kesilmiş olan yazılımların kullanılması büyük risk doğurmaktadır[17]."

---

[16] Bkz.Yrd. Doç. Dr. Hakan HEKİM , Doç. Dr. Oğuzhan BAŞIBÜYÜK, "*Siber suçlar ve türkiye'nin siber güvenlik politikaları- cyber crimes and turkey's cyber security policies*", Uluslararası Güvenlik ve Terörizm Dergisi, Cilt 4, Sayı 2, Yıl 2014, sy.142

[17]Bkz.https://www.ercanyuzuk.com/2018/08/zero-day-sfrnc-gun-acklar.html?cv=1 (Erişim Tarihi: 01.01.2019)

Saldırgan tarafından sisteme girildiğinde sistem erişilmez hale getirilebilir, sistemde bulunan bilgiler çalınabilir, değiştirilebilir veya tahrip edilebilir hale gelmektedir. Bazı durumlarda sistemdeki veriler üzerinde değişiklikler yapıldığı fark edilememektedir. Bu halde bilgi gizliliği prensipleri olan verinin gizliliği, bütünlüğü ve erişilebilirliği tümüyle ihlal edilmiş olmasına karşın sistemdeki verinin bütünlüğü hakkında kimsenin bilgisi olmadığından bütünlüğü bozulmuş veriyle kullanılmaya devam edecektir.

3.2.Zararlı Yazılımlar;

Zararlı yazılımlar, bilgisayar sistemlerini kötüye kullanım amacıyla sistem bilgilerine erişim sağlamaya yarayan veya bilgisayar sistemlerine ciddi zararlar verebilen kendileri de birer program olan kötü amaçlı yazılımlardır. Bu kapsamda virüsler, Truva atları, casus yazılımlar ve rootkitler gibi bir çok siber saldırı yöntemi zararlı yazılımlar başlığı altında değerlendirilebilir. Zararlı yazılımlar insanlara, süreçlere ve/veya teknolojilere karşı kullanılabilir. Burada ki temel ve en önemli nokta ise zararlı yazılımların amacının sistemlere yetkisiz erişim hakkını elde etmek veya kritik ve önemli verilerin elde edilmesini sağlanması olduğudur[18]. (USOM, 2014)

3.2.1. BotNet(bot networks)

Botnet, birden fazla botun bir araya gelerek oluşturduğu özel bir ağdır**.**

Günümüzde zararlı yazılımlar saldırganın ileri seviye bir teknik bilgisi olmasa dahi siber saldırı gerçekleştirmesini sağlamaktadır. Bu sebeple zararlı yazılımlar siber saldırılarda kullanılan en temel ve bilindik yöntemlerdendir.

---

[18]Bkz.USOM. (2014). *Siber Güvenliğe ilişkin Temel Bilgiler.* 29 Nisan 2017 tarihinde http://some.sdu.edu.tr/assets/uploads/sites/408/files/siber-guvenlige-iliskin-temel-bilgiler-22092017.pdf adresinden alındı.

Botnet benzeri zararlı yazılımlar sistemler kullanıcıya gönderilen e-posta ekinde bulunan dosyalar veya mesaj içeriğinde yer alan linklere tıklanarak açılan internet sayfaları üzerinden bulaşabileceği gibi truva atı(trojan) olarak adlandırılan bir zararlı yazılım vasıtasıyla da bulaşabilmektedir.

Bu zararlı yazılımlar yoluyla sisteme giren botnetler sistemlerin normal ve kullanıcısı tarafından talep edilen işlevlerinin yanında arka planda bilinmeyen ve program kullanıcısı tarafından istenmeyen işlevler yüklenmiş olan yazılımlar aracılığı ile yüklenebilmekte olup bu yazılımlar sisteme yüklendikten sonra sisteme gizlice giriş yapılabilmesine izin veren arka kapılar açılmasını veya sistemde kayıtlı bulunan bilgilerin saldırgan tarafından belirlenen yerlere gönderilerek aktarılmasını sağlayabilmektedir. Bu tür gizli işlev içeren yazılımlar şirketler veya ülkeler tarafından üretilerek istihbarat amaçlı olarak kullanılmaktadır. Bu türden zararlı yazılımlar APT(Advanced Persistent Threat - Geliştirilmiş Kalıcı Tehditleri) olarak adlandırılmaktadır.[19] (HEKİM & BAŞIBÜYÜK, 2014)

APT kavramı saldırganın sisteme yetkisiz erişim sağlayarak sistem içerisinde uzun süre bulunması/kalması anlamına gelmekle birlikte bu saldırı türünün asıl hedefi kurumsal firmalar ve politik hedefler oluşturmaktadır. Özellikle ülkeler için hayati önem taşıyan ulaşım, doğalgaz, elektrik gibi kritik altyapıların sistemlerine sızmaya çalışan kişiler tarafından kullanılmakta olan bu zararlı yazılım çeşidi kompleks bir yapıya sahip olmakla saldırının amacı en geniş kapsamda etki yaratmaktır. Bu saldırıların temel hedefi kritik altyapıyı felç etmek veya işlerliği durdurmak olmasa da temel hedef devletlerin milli kapsamlı projeleri ve istihbari çalışmalarının saldırılar neticesinde ele geçirilmesidir.

Klasik siber saldırılardan farklı olarak tehdit altındaki hedef bellidir ve yapılacak saldırı uzun süredir planlanmaktadır. Gerekli olması durumunda yıllarca sürebilecek bir uğraş neticesinde hedefe yönelik olarak plan gerçekleştirilmesi amacı ile sistemde saklanması mümkündür. Bu saldırı türünün diğer siber

---

[19] Bkz.Yrd. Doç. Dr. Hakan HEKİM , Doç. Dr. Oğuzhan BAŞIBÜYÜK, "*Siber suçlar ve türkiye'nin siber güvenlik politikaları- cyber crimes and turkey's cyber security policies*", Uluslararası Güvenlik ve Terörizm Dergisi, Cilt 4, Sayı 2, Yıl 2014 , sy.144

saldırılardan temel farkı sisteme hızlıca girerek veya mevcut sistemi etkisiz hale getirmek yerine uzun süreli olarak fark edilmeden sistem içerisinde sızmak ve olabildiğinde kıymetli veri toplamaktır. Siber Casusluk kapsamında bu saldırı türleri kullanılmaktadır. APT saldırılarında APT yazılımı hedefteki sisteme sızmak ve bu sistemden veri/bilgi aktarımı sağlamak üzere programlanmakta olup bu tür saldırılarda kullanılan zararlı yazılımların belki de en bilineni İran nükleer sistemlerini kontrol eden bilgisayarlara sızan Stuxnettir[20].

APT saldırılarının hedefinde kritik altyapılar, kamu kurumları ve önemli nitelikli şirketler olabileceğinden saldırılardan korunmak ve saldırıların önlenmesi için alınması gereken önlemlerin en başında kurumsal bir bilgi güvenliği yönetim sistemi sistematiği belirlenmek sureti ile risk analizi çalışmalarının yapılması, kurumlar bünyesinde tüm ağ sistemlerinin izlenmesi ve dıştan içe- içten dışa olacak şekilde tüm ağ trafiğinin gözden geçirilerek incelenmesi gelmektedir. APT saldırılarını önlemede anti-virüs sistemleri pek etkili olamayacağından sisteme girmiş bir saldırganın dışarı ile iletişime geçmesinin engellenmesi gerekmekte olup sistem dışındaki yabancı IP adresleri ile bağlantıya geçen tüm istekler değerlendirilmelidir. APT saldırılarında sıklıkla kullanılan yöntemler dikkate alınarak sistem güvenlik duvarları, kullanıcı elektronik posta güvenliğinin sağlanması, DLP cihazı kullanımı, etkin antivirüs kullanımı, ağın izlenmesi ve log sisteminden oluşan etkin ve destekli bir savunma sistemi oluşturulması gerekmektedir. Tüm bu alınacak önlemler ve savunma sistemlerinin oluşturulması koordineli olarak çalışacak ve Siber olaylara müdahale (SOME) tecrübesine sahip ekipler tarafından yapılabileceğinden bu ekiplerin kurulması ve donatılması için eksikler tamamlanmalıdır[21].

---

[20]Bkz.http://www.tnetworks.com.tr/cozumler/advanced-persistent-threats-apt (Erişim Tarihi: 30.05.2017)
[21]Bkz.http://www.tnetworks.com.tr/cozumler/advanced-persistent-threats-apt (Erişim Tarihi: 30.05.2017)

3.2.2. Virüsler

Virüsler günümüzde bilgisayar kullanıcılar için en büyük problemi oluşturmakla birlikte özel olarak yazılmış programlardır. Bilgisayar virüsleri çalıştırılması halinde virüsün kendisi sistem dosyalarından veya programlarından biri olarak değiştirdiği bilgisayar kodlarından oluşmaktadır. Virüslerin diğer zararlı yazılımlardan farklı olarak en büyük özellikleri kendilerini diğer programlara bulaştırabilme ve bu sayede çoğalarak yayılmalarıdır[22]. (AKARSLAN, 2015) Virüslerin çalışma sistemlerinde en önemli nokta bir kullanıcı tarafından çalıştırılmaya gerek duymalarıdır. Virüslerin bulaşma ve yayılmaları gelen elektronik postanın açılması veya USB cihazlarının otomatik olarak taranmadan çalıştırılması sonucu virüsün aktif hale gelmesi ve bulaşması ile meydana gelmektedir.

Virüsler internet üzerinden, elektronik posta ile veya cd, usb gibi cihazlar vasıtasıyla bilgisayara bulaşabilmektedir.

Mantık Bombaları , bir tür virüs programı olmakla beraber yerleştiği bilişim sistemlerine yaratıcısı tarafından öncesinde belirlenmiş olan özel durum gerçekleşinceye kadar veya önceden belirli tarihte aktif hale gelmesi için programlanması halinde bu tarih gelinceye kadar zararlı bir işlem yapmayan, yaratıcısı tarafından önceden belirlenmiş şartların gerçekleşmesi veya bir tarihte aktif hale gelmesi için programlanması halinde öncede belirlenen tarih geldiğinde aktif hale gelerek sisteme hasar veren programlar şeklinde zararlı yazılımlardır. Truva atı isimli zararlı yazılım gibi davranan mantık bombaları yaratıcıları tarafından belirlenen şartlar oluşana kadar faydalı bir program izlenimi vermektedir. Mantık bombaları kendilerini gizleme amacı ile çalışan ve sürekli

[22] Bkz.AKARSLAN, Hüseyin, "Bilişim suçları", Seçkin Yayınları, Mayıs 2015, 2. Baskı, İkinci Bölüm, s.91

saklanan truva atlarından farklı olarak yaratıcısı/programlayıcısı tarafından belirlenen şartlar oluştuğunda zarar vermeye başlamaktadır[23]. (BENZER, 2014)

Mantık bombaları yazılımlarının tek hedefi içine yerleştikleri sistemlere zarar vermek olduğundan aktif hale gelip harekete geçtiklerinde sistem için çok yıkıcı sonuçlar doğurmaktadır. Bu bombalar tüm dosyaları ve bilgileri silebileceği gibi sistemin çökmesine de sebep olabilmektedir. En çok bilinen mantık bombası "Çernobil Virüsü"dür.

3.2.3. Solucanlar

Solucanlarda virüsler gibi kendilerini bir bilgisayardan başka bilgisayara kopyalamak amacıyla hazırlanmış zararlı yazılımlar olup virüslerden temel farklılıkları yayılma işlemini ağ üzerinden otomatik olarak kendileri yapmasıdır.

Solucanların otomatik yayılma yapmaları nedeniyle zaman içerisinde bilgisayar ağlarının yavaşlamasına, internette sayfaların donmasına ve geç açılmalarına sebep olmaktadırlar. Solucanlar da virüsler gibi elektronik posta eklerinde gelen dosyalar ile yayılma yapabilecekleri gibi internet üzerinde linkler ve eş düzeyler arasında dosya paylaşımını sağlayan dosya paylaşım ağları aracılığı ile yayılabilmektedir[24]. (USOM, 2014)

"Bununla birlikte bazı solucanlar, ağ paketleri olarak yayılmaktadır. Bunlar bilgisayar belleğine doğrudan girmekte ve ardından solucan kodu etkinleştirilmektedir[25]."

Solucanların virüslerle olan temel farklılıkları yayılmak için bulaşmak zorunda oldukları bir dosyaya ihtiyaç duymamalarıdır. Solucanlar herhangi bir

---

[23]Bkz. BENZER, Dr. Recep, "Güncel Tehdit: Siber Suçlar" Seçkin yayınları, Eylül 2014 , 1. Baskı, 1. Bölüm "Siber Suçlar ve Teorik Yaklaşımlar" s. 28

[24] Bkz.Siber Güvenliğe ilişkin Temel Bilgiler,USOM, Temmuz 2014, sy.12 belgenin orjinaline http://some.sdu.edu.tr/assets/uploads/sites/408/files/siber-guvenlige-iliskin-temel-bilgiler-22092017.pdf adresinden erişilmiştir. (Erişim Tarihi:08.05.2017)

[25]Bkz.https://www.kaspersky.com.tr/resource-center/threats/viruses-worms , (Erişim Tarihi: 10.09.2017)

dosyaya bulaşmadan kopyalanma yoluyla çoğalmakta ve yayılmaktadır. Bu yayılım ağ(network) veya kurumsal bir ağ(LAN/WAN) üzerinden olabileceği gibi internet yada intranet[26] üzerinden de gerçekleşebilmektedir. Bu nedenle solucanlara "ağ solucanları" denilmektedir.[27] (AKARSLAN, 2015)

Bir bilgisayar virüsü sisteme bulaştığında mevcut bir sistem dosyasına yada erişebildiği bir dosyaya daha sonra kullanılmak üzere aktif hale getirilebileceği bir komutu dosyaya ekleyerek dosyayı değiştirmektedir. Bu sebeple virüs ile solucanın arasındaki en önemli fark bilgisayar virüsünün kullanıcı tarafından bir komut veya hareket ile aktif hale getirilinceye kadar bilgisayarda hareketsiz kalmasına rağmen solucanlar içerisine yüklediği bu programların çalıştırılması için bir kullanıcı tarafından işlem yapılmasına veya komut verilmesine gereksinim duymamakta bu sebeple bilgisayara bulaştığı zaman kendiliğinden bulaşabileceği internet alanlarını arayan bir program başlatmaktadır. Bu program sayesinde solucan ağ üzerinden dolaşarak kendisini ekleyebileceği ve yayılabileceği yeni bilgisayarlar arar. Bu sayede ağ üzerinde yayılma işlemi başlamış olur. Solucanın aktif hale gelmesi veya çalışması için herhangi bir kullanıcının hareket veya komutuna gereksinimi olmadığından yayılmak içinde herhangi bir kullanıcı hareket veya komutuna gereksinim duymamaktadır[28]. (AKARSLAN, 2015)

Solucanlara en güncel örnek Mayıs 2017 tarihinde ortaya çıkan ve uzunca bir süre bir çok bilgisayar kullanıcısı ve şirket tarafından büyük zararlara uğranılmasına sebep olan WannaCry isimli fidye yazılımdır. Bilgisayar korsanları tarafından hazırlanmış olan bu fidye yazılımı 150 farklı ülkeden 200 bini aşkın insanı etkilemiştir[29]. Saldırılardan etkilenen ülkeler arasında Türkiye de bulunmaktadır. Zararlı yazılım, sızdığı bilgisayar içindeki verileri Windows'un

---

[26] İntranet, işyerlerinde çalışanlar arası iletişimi sağlamak ve bilgi paylaşmak amacıyla kullanılan özel bir iş ağıdır (network). http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/intranet-(iç-ağ)-ve-extranet-(dış-ağ) , (Erişim Tarihi: 11.11.2017)

[27] Bkz.AKARSLAN, Hüseyin, "Bilişim suçları", Seçkin Yayınları, Mayıs 2015, 2. Baskı, İkinci Bölüm, s.93

[28] Bkz.AKARSLAN, Hüseyin, "Bilişim suçları", Seçkin Yayınları , Mayıs 2015, 2. Baskı, İkinci Bölüm, s.93, dipnot 161.

[29] Bkz. http://www.bbc.com/turkce/haberler-dunya-39915541(Erişim Tarihi 20.06.2017)

kendi dosya şifreleme özelliğini kullanarak şifrelemiş ve belgelerin şifrelerinin mağdura verilmesi karşılığında para talep edilmesi şeklinde işlemekte olup sadece bulaştığı bilgisayardaki dosyaları şifrelemekle kalmayıp aynı zamanda bilgisayarın bağlı olduğu ağa ve bu ağ yolu ile ağa bağlı olan diğer bilgisayarlara da bulaşmaktadır. Bu yazılım bilgisayar üzerindeki dosyaları şifrelemektedir. Bu şifreleme neticesinde kullanıcı yazılımın yaratıcısına Bitcoin isimli para birimi ile ödeme yapılması talep edilmekte, ödeme yapılmaması halinde ise dosyalara erişmek imkansız olmaktadır. Bu zararlı yazılımdan sadece Window işletim sistemine sahip bilgisayarları etkilemiş olup saldırıya maruz kalmamak için işletim sistemlerini güncellemesi, anti-virüs programlarının kullanımı ve programların veri tabanlarının güncel olması gerekmekte olup şüpheli elektronik posta ve linklere dikkat edilmesi gerekmektedir. Ayrıca saldırıya uğrayanların fidye ödememesi gerekmektedir. Saldırı uluslar arası boyutta tarihin en büyük fidye yazılımı saldırısı olarak anılmaktadır.

Yine Haziran 2017 de Petya isimli bir solucan WannaCry solucanı gibi yayılmış ve kendinden önceki diğer zararlı yazılımlardan farklı olarak tek tek dosyaları şifrelememiş bunun yerine tüm dosya sistemini ele geçirmiş ve tüm dosya sistemini şifreleyerek kullanıcılardan fidye ödenmesi talep edilmiştir.

3.2.4. Truva Atı(Trojan)

"Truva atı legal bir program içindeki illegal talimatlar ya da bir işi yapıyormuş gibi görünüp arka planda kullanıcıdan habersiz gizli işlemler yapan zararlı programlardır[30]." (AKARSLAN, 2015)

Truva atları üreticiler tarafından lisanslı ve ücretli olarak üretilen programların internet üzerinde ücretsiz veya yama(crack) içeren versiyonlarına da saldırganlar tarafından ücret ödenmeden kullanılmasını sağlayan ve programın

[30] Bkz.AKARSLAN, Hüseyin, "Bilişim suçları", Seçkin Yayınları, Mayıs 2015, 2. Baskı, İkinci Bölüm, s.93

sistem dosyasının içerisine yerleştirerek lisansı aktif hale gelmesini engelleyen crack dosyalarının bilgisayara indirilmesi marifetiyle bulaşabilmektedir.

Truva atı bilgisayar kullanıcıları tarafından içeriği hakkında çok fazla bilgi sahibi olunmadan yükledikleri zararlı yazılımlardır. Örneğin bir kullanıcı "Flash Player" yüklemesini "Adobe" veya güvenilir bir kaynaktan yüklemek yerine bilmedikleri bir kaynaktan yüklenmesi durumunda program içeriği hakkında bilgi sahibi olmadığından truva atı yüklü bir program gelmesi muhtemeldir[31]. (USOM, 2014)

Genel olarak incelendiğinde Truva atı içeren programlar bir dosyanın sisteme indirilmesi sonrasında sisteme yüklenmesi sonucunda bilgisayar sistemine bulaşmakta olup bu zararlı yazılımın en önemli özelliği kullanıcının bilgisayarının uzaktan erişilebilmesi ve kontrol edilebilmesi veya izlenmesine olanak sağlamasıdır. Truva atı, yüklenmiş olduğu bilgisayarın zombi bilgisayar olarak ta kullanılmasına sebep olmaktadır[32].

Truva atlarının yayılma sistemleri virüs ve solucanlar gibi olmakla birlikte kullanıcıdan habersiz olarak arka planda işlem yapmakta olan bu program sistem internete bağlıyken dışarıya veri aktarımı yaparlar[33]. (BENZER, 2014)

Bir truva atı yazılımı istemci ve sunucu olmak üzere iki ana bölümden oluşmaktadır. Sunucu bölümü hedef kişinin bilgisayarında, istemci bölümü ise uzaktan erişen ve yöneten kişinin bilgisayarında eş zamanlı olarak çalışmaktadır.

Truva atları da virüsler ve diğer bir çok zararlı yazılım gibi kendi başına kullanıcının bir hareket yada komutuna bağlı olarak çalışan programlar olup Truva atı yazılımı kendini kopyalayarak dağıtmış olsa dahi aktif hale gelmesi için

---

[31]Bkz.Siber Güvenliğe ilişkin Temel Bilgiler,USOM, Temmuz 2014, sy.10 belgenin orjinaline http://some.sdu.edu.tr/assets/uploads/sites/408/files/siber-guvenlige-iliskin-temel-bilgiler-22092017.pdf adresinden erişilmiştir. (Erişim Tarihi:08.04.2017)

[32] Bkz.http://www.bilisimterimleri.com/bilgisayar_bilgisi/bilgi/76.html (Erişim Tarihi: 12.11.2017)

[33]Bkz.BENZER, Dr. Recep, "*Güncel Tehdit: Siber Suçlar*" Seçkin yayınları, Eylül 2014, 1. Baskı, 1. Bölüm "Siber Suçlar ve Teorik Yaklaşımlar" s. 28

kurbanın truva atını içeren programı çalıştırması gerekmektedir[34]. (AKARSLAN, 2015)

Truva atları internetten indirilen müzik, dosya ve programların içine yerleştirilmiş veya elektronik posta yolu ile ücretsiz kullanılabilecek basit programlar ile ilgi çekici uygulamalar aracılığıyla bilgisayarlara bulaşabilmektedir.

3.2.5. Spyware (Casus) Yazılımlar ve Adware (Reklam) Yazılımlar

Casus yazılımlar bilgisayarda casusluk yapmak için yaratılmış programlar olup kullanıcıya ait önemli bilgiler ile kullanıcının yaptığı işlemleri kullacının bilgisi haricinde toplayarak toplanan bu bilgilerin kötü niyetli kişilere gönderilmesi amacıyla kullanılmaktadır. Bu yazılımlarda diğer zararlı yazılımlar gibi kullanıcı tarafından sisteme farkında olunmadan bulaştırılmaktadır. Bu yazılımların virüs ve solucanlardan ayıran en temel özellik bulaştıkları sistemde yayılma ihtiyacı duymadan sistemin gizliliğini ihlal etmek ve veri elde etmek amacıyla kullanılmalarıdır. Bu verileri kullanıcının üyelik bilgileri, şifreler, hesap numaraları olabileceği gibi bazı şirketler tarafından davranışsal reklamcılık uygulamaları kapsamında internet kullanıcılarının internet kullanım alışkanlıklarını ve rutinlerini tespit etmek ve belirli istatistikler oluşturmak amacı ile de kullanıcıların verileri casus yazılımlar aracılığı ile toplanabilmektedir[35].

Reklam yazılımları ile bilgisayardaki veriler, gezilen internet siteleri gibi bilgiler belli bir merkeze gönderilerek verilere göre kullanıcıya reklam gösterilebilmekte ve internetten reklam indirilmesi sağlanmaktadır. Bu şekilde davranışsal reklamcılık uygulamaları yapılabilmekte olup toplanan istatistikler şirketlere satılabilmektedir. Ayrıca reklam yazılımları vasıtasıyla yazılımın

---

[34]Bkz. AKARSLAN, Hüseyin, "*Bilişim suçları*", Seçkin Yayınları, Mayıs 2015, 2. Baskı, İkinci Bölüm, s.94

[35]Bkz.Siber Güvenliğe ilişkin Temel Bilgiler,USOM, Temmuz 2014, sy.12 belgenin orjinaline http://some.sdu.edu.tr/assets/uploads/sites/408/files/siber-guvenlige-iliskin-temel-bilgiler-22092017.pdf adresinden erişilmiştir. (Erişim Tarihi:08.05.2017)

bulaştığı program ve tarayıcı sayesinde reklamlara istem dışı tıklanarak reklam gelirlerinden para elde edilebilmektedir.[36]

Casus yazılımlar internet üzerinden veri toplamak amacıyla kullanılabileceği gibi cep telefonları alanında da dinleme yapmak ve kayıt yapmak amacıyla kullanılabilmektedir. Cep telefonları içerisine yüklenmiş olan bir casus yazılım ile telefon görüşmeleri dinlenebileceği gibi kayıt altına da alınabilmektedir. Hatta bazı casus yazılım türleri ile ortam dinlemesi yapmak mümkün olduğu gibi telefon içerisindeki tüm mesaj ve kayıtlara ulaşılabilmektedir. Bu yazılımlar tek başına satıldığı gibi yazılımların yüklü olduğu cep telefonları ile birlikte de satılabilmektedir.[37]

3.2.6. Kök Kullanıcı Takımı (Rootkit)

Rootkitler bir bilişim sisteminde sisteme bulaşması ile mevcut işlemin arkasında saklanabilen, kötü niyetli kişilere sisteme uzaktan tam erişim ve kontrol sağladığı gibi çok zor tespit edilebilen bilgisayar programlarıdır. Rootkitler hedef bilişim sisteminde bulunan dosya ve süreçlerini gizlemek ya da değiştirmek suretiyle yönlendiren programlardır. Bu programların iki temel özelliği bulunmaktadır. Bunlar etkiledikleri sistemde üst düzey erişim yetkilerini gerektiren komutları çalıştırabilmekte olup kendilerini diğer üst düzey erişim yetkilere sahip sistem yöneticilerinden gizleyebilmeleridir.[38] (AKARSLAN, 2015) Rootkitlerin virüslerden farklı olarak amacı sistemi yavaşlatmak ve yayılmak olmamakla birlikte amacı sistemin veya bilgisayar üzerindeki kontrolün ele geçirilmesi ve içine yerleştiği sistemde varlığının tamamen gizlenmesidir.

---

[36] Bkz.AKARSLAN, Hüseyin, "Bilişim suçları", Seçkin Yayınları, Mayıs 2015, 2. Baskı, İkinci Bölüm, s.95

[37] AKARSLAN, Hüseyin, "Bilişim suçları", Seçkin Yayınları, Mayıs 2015, 2. Baskı, İkinci Bölüm, s.95, dipnot 168

[38] AKARSLAN, Hüseyin, "Bilişim suçları", Seçkin Yayınları, Mayıs 2015, 2. Baskı, İkinci Bölüm, s.96

Rootkit programları farklı seviyelerde çalışmakta olan üst düzey yetki (root) ve program(kit) ile birlikte sistemin zaafiyetlerini sömürmekte olan saldırganın sistem yöneticisi kullanıcı tarafından tespit edilme riskini ortadan kaldırmaktadır. Root yetkisi kullanıcıya üstü düzey kök kullanıcı yetkisi tanıyan bir yetki olup rootkit programları ilk olarak Unix tabanlı işletim sistemlerinde ortaya çıkmıştır. Root kit yazılımları bu programlar ile orijinal UNIX tabanlı işletim sistemindeki sistem dosyaları ile yer değiştirip yetkisiz bir kullanıcıya üst düzey erişim yetkisi anlamına gelen root yetkisi verme amacı ile ortaya çıkmıştır. Rootkit yazılımları ile sistemin kontrolü asıl sistem yöneticisinin dahi haberi olmadan saldırgan kişinin eline geçebilmekte olup Unix tabanlı işletim sistemlerinden sonra diğer işletim sistemlerinde de kullanılmaya başlanmıştır[39].

3.2.7. Bukalemun (Chamelon) ve Tavşanlar (Rabbit)

Truva atları ile benzerlik özellik göstermekte olan bukalemunlar normal bir program gibi çalışmasına rağmen bir takım hile ve aldatmalarla sistemlere zarar veren programlardır. Bir bukalemun programı sistemde kullanıcıların şifreleri için giriş iletileri taklit edecek şekilde programlanmakla kullanıcı adı ve şifresini taklit etme özelliği sayesinde gizli dosyalara erişip sisteme giriş yapan tüm kullanıcıların isim ve şifrelerini gizli bir dosyaya kaydeder daha sonra sistemin bir süre bakım için kapatılacağına ilişkin bir mesaj gönderir. Programın programlayıcısı kendi özel şifresi ile sisteme girerek bukalemun tarafından oluşturulmuş tüm kullanıcı isim ve şifrelerini kaydettiği gizli dosyaya ulaşarak kaydedilen kullanıcı adı ve şifrelerine ulaşmasını sağlar.

Tavşanlar ise girdikleri sistem içerisinde sürekli ilerleyen, yerleştiği bellek veya diskteki alanda koloni kurarak sistemi doldurarak sistemin halihazırda sahip olduğu bilgi işlem gücünü azaltan, bilgisayar veya sisteme sürekli olarak gereksiz

---

[39] AKARSLAN, Hüseyin, "Bilişim suçları", Seçkin Yayınları, Mayıs 2015, 2. Baskı, İkinci Bölüm, s.95, dipnot 171

komutlar göndermek suretiyle kendi kendine yetebilen, yaratılış amaçları çok kullanıcılı sistemlerde iletişim ağ ortamlarında ana sistem bilgi işleme gücünü yitirinceye kadar sistemin kaynaklarını kurutmak olan zararlı yazılımlardır. Tavşan isimli bu zararlı yazılımlar virüsler gibi asalak olmamakla iki zararlı yazılım arasındaki en temel fark tavşan isimli bu programların kullanıcı veri kütüklerinin sonuna eklenmemeleri ve kendi kendilerine yetebilmeleridir[40].

3.3.Gizli- Arka Kapılar (Back Doors)

Arka kapı (Backdoor) isimli yazılımlar bir bilgisayar sistemine yönelik normal kimlik doğrulama yöntemini devre dışı bırakarak başka bir yöntemle sisteme giriş yapma ve verilere erişim sağlayan sistemi yapan kişi tarafından veya başkaca programlarla yazılımın içine gizlice yerleştirilebilen bir virüs yazılımıdır.[41] Bilgisayar sistemlerinin normal güvenlik işleyişini atlatarak bilgisayar sistemine erişim için yetkisi bulunmayan kişilerce erişime ve işlem yapmaya açık hale getirmektedir.

Arka kapılar yazılım hatalarından kaynaklanabileceği gibi zararlı yazılımlar tarafından da oluşturulabilir veya üreticiler tarafından da bilinçli olarak bırakılmış olabilir.

Bu program çalıştığı zaman arka kapı isimli yazılımı yerleştiren yaratıcısına uzaktan erişim yönetimi kullanarak ve halihazırda mevcut olan sistem kontrollerine fark edilmeden sisteme sızabilmesine imkan tanır.

Bu programlar yazılımların geliştiricileri tarafından gözden kaçırılan hatalar nedeni ile oluşabilmekte olup bu hatalar ve zafiyetler beyaz şapkalı olarak tabir edilen hackerlar tarafından tespit edildiği zaman yazılım üreticisine bildirilmesi ile bu husus topluma açıklanır ve bu hatanın giderilmesi için bir yazılım güncellemesi

---

[40] AKARSLAN, Hüseyin, "Bilişim suçları", Seçkin Yayınları, Mayıs 2015, 2. Baskı, İkinci Bölüm, s.97 dipnot 177

[41]Bkz. AKARSLAN, Hüseyin, "Bilişim suçları", Seçkin Yayınları, Mayıs 2015, 2. Baskı, İkinci Bölüm, s.98 dipnot 178

yayınlanır. Bu sayede fark edilmeden açılmış olan arka kapılar kapatılır. Yazılımların üretimi sırasında meydana gelen hatalardan kaynaklı arka kapılar sebebi ile meydana gelen zafiyetlerden korunmak için yazılım güncellemeleri büyük önem taşımaktadır. Bu sebeple yasal olmayan korsan olarak tabir edilen yazılımları kullananlar güncellemeleri alamadıkları için risk altında olmaya devam etmektedir.

Aynı arka kapının beyaz şapkalı değil de siyah şapkalı olarak tabir edilen kötü niyetli hacker tarafından önce tespit edilmesi halinde ise bu arka kapı kötü niyetli kişiler tarafından farklı amaçla kullanılabilir.

Bu tür zararlı yazılımlar en çok internet üzerinden ücretli olarak satılan programlar için internet üzerinde bulunan ve programı ücretsiz olarak kullanılmasını sağlayan crack isimli dosyalar ile program seri numarası paylaşan siteler aracılığı ile yayılmaktadır. Bunun yanında yasadışı içerikleri barındıran ve pornografi ve uyuşturucu ile alakalı internet sitelerinde de kendilerine yayılma ortamı bulmaktadır.

Bazı durumlarda program üreticileri kendileri tarafından özellikle bilinçli olarak sistemlere arka kapılar ekleyebilmektedir. Bu şekilde şirketler tarafından programlara veya sistemlere eklenmiş arka kapılar vasıtasıyla kullanıcılara uzaktan erişim yöntemi ile destek verilebilmekte olmasına karşın kötü niyetli kişilerce tespit edilmesi halinde zafiyet olarak kullanılması riski her zaman mevcuttur.

Bunun yanı sıra bazen şirketlerin ürettikleri sistem veya programlar içerisinde devletler tarafından bazı sistemlerde arka kapılar bırakılması istenebilmekte, bu arka kapılarda siber casusluk veya terörizmin önlenmesi maksadı ile kullanılabilmektedir. Bu durum ile ilgili olarak Microsoft ve Apple gibi büyük şirketler tarafından üretilen ürünlerin içerisinde bu türden arka kapıların özellikle konulduğu bilinmekte olup bir kullanıcının bu türde bir arka kapı için yapabileceği çok bir şey olmamasına karşın güvenlik duvarı sisteminde beyaz liste yöntemi kullanılması mümkün olabilir.

Bu türde arka kapılardan korunmak için uygulanan en bilindik yöntem açık kaynak kodlu yazılım kullanmaktır. Açık kaynak kodlu yazılımlar kaynak kodları

yazılımcı olan herkes tarafından internetten okunabildiği için arka kapı kodlarının gizlenme ihtimalini ortadan kaldırmaktadır[42].

3.4.Yemleme (Phishing)

Yemleme saldırıları yasadışı yollar kullanılmak suretiyle kullanıcının sisteme erişim için kullandığı kullanıcı ismi ve şifresi ile kimlik bilgileri, hesap bilgileri gibi verilerin ele geçirilmesi için kullanılan bir saldırı yöntemidir.

Şifre avlamak anlamına gelecek şekilde şifre ve balık sözcüklerinin İngilizce birleşiminden oluşturulmuş phishing saldırılarında saldırgan genelde güvenilen kurum veya işletmelerden gönderilmiş gibi gözüken e-postalar veya mesajlar gibi yöntemlerle kişilere ulaşmakta ve onların kredi kartı veya kullanıcı adı ile şifresi gibi ayrıntılarını istemektedir[43]. (USOM, 2014)

Kullanıcılar güvendikleri bir kurum veya şirketten gönderilmiş gibi gözüken bu gibi elektronik postaları cevapladıkları zaman kullanıcı isim ve şifreleri, banka hesap numaraları ve bir çok kişisel veri çalınabilmektedir. Phishing saldırılarına örnek olarak bir bankadan gönderilmiş gibi gönderilen bir elektronik posta ile kurbanın şifre, kredi kartı numarası gibi bilgilerin verilmesi aksi takdirde hesaplarının tehlikede olduğu belirtilir. Bu yönetimin çok etkili olmasının sebebi korku yaratarak gerçek olmadığının anlaşılmasının önüne geçmek ve kullanıcıyı söylenileni yapmasının sağlamasıdır. Yemleme saldırılarının önüne geçebilmek amacıyla bankalar ve kurumlar tarafından kullanıcılara bankaların veya kurumların kendilerinden hiçbir isim ve gerekçe altında elektronik posta aracılığı ile kişisel verilerini, kullanıcı ismi ve şifrelerini istemeyecekleri, bu gibi mesajlarla karşılaşmaları halinde gelen elektronik postayı kendilerine göndermeleri bildiren uyarı mesajları ve postaları göndermektedirler.

---

[42] Bkz.https://tr.wikipedia.org/wiki/Arka_kapı (Erişim Tarihi : 11.11.2017)
[43] Bkz.Siber Güvenliğe ilişkin Temel Bilgiler, USOM, Temmuz 2014, sy.12 belgenin orjinaline http://some.sdu.edu.tr/assets/uploads/sites/408/files/siber-guvenlige-iliskin-temel-bilgiler-22092017.pdf adresinden erişilmiştir. (Erişim Tarihi:08.07.2017)

Bir diğer örnek ise icloud hesabı üzerinden yüksek meblağlı bir ürün alınmış gibi mail gelir. Bu mailde "yapılan alım sizin değilse tıklayın" şeklinde bir link verilmektedir. Link'e tıklandığından icloud internet sitesi ile birebir görünüşlü ama dikkat edilirse https://www.i-cloud.com olduğu görülecek olan bir siteye yönlendirilerek iade için T.C. kimlik numarası, pasaport numarası, kredi kartı bilgileri, adres ve telefon, anne kızlık soyadı dahil bir çok kişisel veriyi doldurulması gereken bir sayfa çıkmaktadır. Bu şekilde kurbanın tüm kişisel verilerine hatta pasaport numarasına dahi saldırgan tarafından ulaşılması mümkündür.

Phishing son dönemde çok fazla kullanılmakta olan bir dolandırıcılık yöntemi olup esasında sosyal mühendislik saldırılarının bir türüdür.

Sosyal Mühendisliğin en yaygın şekli phishing saldırısıdır. Phishing e-postaları kurbanın bankası, işvereni veya başka bir güvenilir kuruluştan gelen resmi e- postalar gibi görünür. Belki bir hesap hatasını düzeltmek veya sosyal ağ mesajını görmek için hedef kişinin bir eyleminin gerektiğini iddia eden e-posta ile müşterileri gizli bilgilerini girmesi istenen bir web sitesini ziyaret için kandırmak suretiyle gerçekleştirilir. Eğer hedef kişi hesap detay bilgilerini girerse saldırgan o bilgiyle her şeyi yapabilir hale gelecektir. Sahte bilgiler için olan bu web sayfası gerçek olan benzer bir URL'ye sahip olabilir. Eğer yakından bakılmazsa www.garantl.com adresi www.garanti.com adresi gibi görünebilecektir.

3.5. Scanning (Tarama) Yöntemi ve Şifre Kırıcılar

Tarama yönteminde değeri her defasında sıralı bir dizi takip etmek sureti ile değişmekte olan veriler aracılığı ile hızlı olarak peş peşe bilişim sistemine girilerek sistem tarafından olumlu cevap verildiği tespit edilebilen durumların raporlanması amacı ile yapılmakta olan bir işlem olup tarama yöntemi açık portları tespit etmek için yapılan açık port taraması veya internete bağlı IP adres numaralarının taraması şeklinde de yapılabilir. Bu yöntemde sistem bir IP numarasını kendisine başlangıç belirleyen ve bu numaradan başlayarak sürekli her seferinde bir numara arttırmak sureti ile tekrarlanır. İp numarası internete bağlı ise bağlantı sinyali gönderecektir.

Bu şekilde belirlenen aralıktaki internete bağlanan ip numaraları tespit edilebilir. Saldırganlar tarafından en çok kullanılan yöntem port taramasıdır[44]. (BENZER, 2014)

Şifre kırıcılar ise Tarama yönetimde açıklandığı mantıkla çalışmakta olan ve şifrelenmiş olarak korumaya alınmış sistemin şifresini kırmak amacıyla şifre taraması yapılması mantığı ile çalışan ilk ortaya çıktıklarında basit olarak tahmin yürütme ve deneme yanılma yönetimi ile yapılan bu işlem günümüzde bu işlem için özel olarak geliştirilmiş yazılımlar ve "kaba kuvvet" denilen yöntemler kullanılmak suretiyle yapılmaktadır.

Yapılan işlem halen bir deneme yanılma yöntemi olmasına karşın programlar tarafından çok hızlı bir şekilde veri tabanlarında bulunan kelimeler ve harf dizileri kullanılarak yapılabilmektedir.

Kullanıcılar tarafından sözcük dizilerinden, rakam veya harflerden seçilerek oluşturulan ve basit şifre denilen şifreler bu sistem ile rahatlıkla çok kısa sürede çözülebilmektedir. Bu programlar mevcut şifreyi tespit edebilmek için veri tabanlarında bulunan sözlük içerisindeki kelimeleri ve harf dizilerini denemekle sistemde yanıt alıncaya kadar bu işlemi sürdürmektedir. Bu programların veri tabanları mantıklı ve anlamlı tüm kelimelerden başlayarak dünya üzerinde en sık kullanılmakta olan şifrelerden oluşan çok geniş kapsamlı sözlükler niteliğindedir[45]. (BENZER, 2014)

3.6.Servis Dışı Bırakma Saldırıları - (Denial-of- Service)

Servis dışı bırakma saldırıları kısa adıyla DoS (Denial of Service) saldırıları bir ilişim sisteminin erişilebilirliğine yönelik olarak düzenlenen ve sistemin hizmetini engelleme amacıyla yapılan saldırılardır.

---

[44]Bkz. BENZER, Dr. Recep, "Güncel Tehdit: Siber Suçlar" Seçkin yayınları, Eylül 2014 , 1. Baskı, 1. Bölüm "Siber Suçlar ve Teorik Yaklaşımlar" s. 31 atıf (Boğa, 2011)

[45] Bkz. BENZER, Dr. Recep, "Güncel Tehdit: Siber Suçlar" Seçkin yayınları, Eylül 2014 , 1. Baskı, 1. Bölüm "Siber Suçlar ve Teorik Yaklaşımlar" s. 31 atıf (Boğa, 2011)

Bu saldırı yönteminin pek çok çeşidi olmasına rağmen tüm yöntemlerin ortak amacı sistemle çok sayıda sahte bağlantı kurulması ile sunucuya aşırı iş yükü bindirmek ve sunucunun gerçekten bağlantı kurmaya çalışan kullanıcılara cevap veremez hale gelmesini sağlamaktır.

Saldırıların asıl amacı hedefteki sistemin imkan ve kapasitesinin çok üzerinde hizmet talebinde bulunarak sunucunun diğer sistem veya bilgisayarlardan gelen hizmet isteklerini normal işleyişe göre yavaş yapması veya bu isteklerin reddedilmesi sebebi ile hizmet veremez hale gelmesini sağlayarak sistemi çökertmektir. Servis reddi saldırıları hedef sistemin sahibini tehdit etmek amacıyla kullanılabilmektedir[46].

DoS saldırıları, bir sistemde siber güvenliğin temel yapıtaşlarından erişilebilirliği engellemeye yönelik olarak yapılan saldırılardır.

Distributed Denial of Service (Dağıtık Servis Reddi) saldırıları ise organize bir şekilde bilgisayar topluluğu tarafından belirli bir hedefe aynı anda DDoS saldırısında bulunulmasıyla yani özel geliştirilmiş yazılımlarla çok sayıda paketin hedef internet sitelerine gönderilmesiyle meydana gelir. Böylece sistem kaynakları tüketilir ve sistem cevap veremez hale gelir. Bu yöntemle saldırı gerçekleşmiş olur ve site bir süre kullanılmaz duruma gelir.

DDoS saldırılarında genel olarak yukarıda açıklanan botnetler kullanılmaktadır. Saldırganlar tarafından binlerce bilgisayara casus yazılım sızdırılarak bu yazılımlarla kontrollerine aldıkları "zombi" bilgisayarları istedikleri zaman kontrol edebilmekte olup binlerce zombi bilgisayar tarafından aynı anda saldırıya geçilmesi ile web sitesi yapılan saldırılar sonucu çökmesine neden olmaktadır. Saldırganlar tarafından binlerce bilgisayara casus yazılım sızdırılarak bu yazılımlarla kontrollerine aldıkları "zombi" bilgisayarları istedikleri zaman kontrol edebilmekte olup binlerce zombi bilgisayar tarafından aynı anda saldırıya geçilmesi ile web sitesi yapılan saldırılar sonucu çökmesine neden olmaktadır.[47]

---

[46]Bkz. https://tr.wikipedia.org/wiki/Denial-of-service(DoS)_Saldırısı (Erişim Tarihi: 10.06.2017)
[47]Bkz.http://www.dijitalteknoloji.net/internet/redhack-nasil-hackliyor.html (Erişim Tarihi: 07.05.2017)

Servis Dışı Bırakma Saldırısı DoS, tek kaynaktan yapılan saldırılar olup altyapı veya yazılımsal açıklıklar kullanılarak yapılabilir.

DDoS, birden fazla kaynaktan yapılan saldırı olup saldırganlar genel olarak saldırıları Sahte ip adresleri üzerinden veya zombi bilgisayarlar aracılığıyla yapmaktadır. DDoS saldırısının gerçekleştirilmesi için Botlara ihtiyaç duyulur.

Trojan, virüs gibi zararlı yazılımlarla botnet genişletilebilir.

DDoS tam anlamıyla bir hackleme faaliyeti olmamakla birlikte bu saldırıda hedef sistemin durdurularak maddi kazanç sağlamak veya prestij kaybetmesine sebep olmak amaçlanmaktadır.

Rusya tarafından Gürcistan'a yapılan saldırılar, Anonymous hacker tarafından Wikileaks'e destek olmak amacıyla yapılan ve bir çok insanın için gönüllü olarak bot olduğu saldırılar da örnek olarak verilebilir.

Türkiye'deki Hacker grubu Redhack'in en çok kullandığı siber saldırı yöntemi DDOS saldırıları olup bu saldırılar bir çok kurum için tehdit haline gelmiş olmakla saldırının hedefi olan ve hizmet veremez hale gelen kurumlar büyük maddi zararlara ve itibar kayıplarına uğramakta olup bu yöntem uluslararası siber savaşlarda etkili olarak kullanılan bir yöntem olarak karşımıza çıkmaktadır[48].

DDoS saldırılarına örnek olarak 2009 yılında yapılan bir DDoS saldırısı neticesinde Sosyal Paylaşım Sitesi Twitter'a saatlerce ulaşılamamıştır.

2011 yılında Suriye rejim yandaşları hükümeti eleştirenlere ve artan şiddetle ilgili yayın yapan haber kuruluşlarına saldırmak için DDoS saldırısını kullanmışlardır.

3.7.Sahte (Fake)- İstemdışı alınan(Spam) Elektronik Postalar

Sahte e-postalarda amaç hedef kişinin e-posta şifresini ele geçirmek olup bu saldırı türünde öncelikle e-posta şifresi ele geçirilmek istenen kişiye sanki e-posta hizmeti aldığı Hotmail, Gmail, Mynet, Yahoo gibi hizmet sağlayıcısından

[48] Bkz.http://shiftdelete.net/ddos-nedir-39493 (Erişim Tarihi: 09.05.2017)

geliyormuş gibi bir e-posta gönderilir. Gönderilen sahte e-postayı cevaplamak için kişi yine sahte hazırlanmış bir internet adresine yönlendirilir ve hedef kişinin kullanıcı adı ve şifresini girdiğinde bilgileri üçüncü kişilerin eline geçer[49]. (AKARSLAN, 2015)

Spam ise hedef kişinin isteği olmadan gönderilen reklam içerikli e-postalar ve internet üzerinde aynı iletinin yüksek oranda kopyasının oluşturulması ve bu kopyaların mesajı alma talebinde bulunmamış kişilere zorlayıcı nitelikte gönderilen elektronik postalardır. Genellikle reklam ve benzeri içerik taşımakla birlikte bazı durumlarda pornografik veya virüs içerikli olabilmektedirler.

3.8.Klavye Kaydediciler(Keylogger)

Klavye kaydediciler klavyede yapılan her vuruşu ve basılan her tuşu kaydeden ve kaydettiği bu veriyi kişisel bilgilere erişmek isteyen kötü niyetli kişilere göndermek üzere programlanmış yazılımlardır. Saldırgan bu program sayesinde istediği zaman kaydedilen bu bilgilere erişerek her tür bilgiyi görebilmektedir. Bu yolla sizin e-mail şifresi, kredi kartı numarası gibi önemli verilere erişilebilir.

Son dönemde bir çok keylogger program bilgisayardan kaydedilen vuruşların yanı sıra anlık olarak ekran görüntüleri de almakta bu sayede o anda yazılan şifre veya bilginin nereye yazıldığını da tespit edebilmektedir. Ayrıca bazı keylogger programları kaydettiği bilgileri e-posta yoluyla da gönderebilmektedir.

Keylogger şirketler tarafından sistem güvenliği amacıyla sistem yöneticisi tarafından yüklenebildiği gibi sistem yöneticisinin bilgisi olmadan da yüklenebilmekte olup sistem yöneticisinin bilgisi dahilinde olmayan bu tip programlar casusluk amacı taşımaktadır[50].

---

[49]Bkz. AKARSLAN, Hüseyin, "Bilişim suçları", Seçkin Yayınları, Mayıs 2015, 2. Baskı, İkinci Bölüm, s.102 dipnot 196

[50]Bkz.http://www.teknolojioku.com/haber/keylogger-nedir-nasil-yapilir-temizlenir-ve-korunulur-101.html, (Erişim Tarihi: 10.11.2017)

3.9.Ip Aldatması (IP Spoofing)

İnternet ortamında spoofing IP numarasındaki değerlerin olduğundan farklı gösterilmesidir. Buna göre bu aldatmadaki amaç iletişimde olunan tarafları kandırmaktır.

İnternet ağı ve bilgisayar ağı üzerinden veril gönderiminde kullanılan temel protokol Internet Protokolü(IP) olarak adlandırılır. IP paketler halinde veri taşınmasına izin veren bir sistem olup bu IP paketlerinin içeriğinden her IP paketinde paketin başlığı, kaynağı ve gideceği adres bulunur. Kaynak adres olarak ise paketin çıktığı adrestir. İp sahteciliği de denilen bu yöntemde sahte kaynak IP adresi ve IP paketleri oluşturularak saldırgan tarafından farklı bir adresi içerecek şekilde paketin başlığı değiştirilmekte ve sanki paket başka bir makine tarafından gönderilmiş gibi görünmesini sağlayarak hedef kişiyi kandırabilmektedir. IP aldatması tüm protokollerde gerçekleşmesi teoride mümkünse de pratik olarak UDP[51] protokolü kullanan uygulamalarda gerçekleştirilebiliyorken, TCP[52] protokolü kullanan uygulamalarda gerçekleştirilememektedir. Bu durumun sebebi ise TCP protokolünde üçlü el sıkışmanın zorunlu olması ve paket başlık bilgisindeki sıra numarasının tahmin edilemez olmasıdır.

IP aldatması en çok servisin reddi olan DoS saldırılarında karşımıza çıkmaktadır. Bu saldırılarda saldırgan saldırı paketlerine yanıt almayı önemsemediğinden ve gönderilen her sahte paket farklı adreslerden geliyormuş gibi göründüğünden saldırının kaynağının ve saldırganın kimliğinin tespit edilmesi imkansız hale gelmektedir[53].

---

[51] UDP (User Datagram Protocol - Kullanıcı Veri bloğu İletişim Kuralları), TCP/IP protokol takımının iki aktarım katmanı protokolünden birisidir. Verileri bağlantı kurmadan yollar. Gelişmiş bilgisayar ağlarında paket anahtarlı bilgisayar iletişiminde bir datagram modu oluşturabilmek için UDP protokolü yazılmıştır.
https://tr.wikipedia.org/wiki/UDP (Erişim Tarihi: 10.11.2017)

[52]TCP (Transmission Control Protocol), TCP/IP protokol takımının aktarım katmanı protokollerinden birisidir. Gelişmiş bilgisayar ağlarında paket anahtarlamalı bilgisayar iletişiminde kayıpsız veri gönderimi sağlayabilmek için TCP protokolü yazılmıştır.
https://tr.wikipedia.org/wiki/TCP (Erişim Tarihi:10.11.2017)

[53]Bkz. https://tr.wikipedia.org/wiki/IP_spoofing (Erişim Tarihi: 10.11.2017)

Bu tip saldırılara verilecek en güzel örneklerden biri ülkemizdeki hacktivist grup Redhack tarafından yapılan Yüksek Öğretim Kurumu(YÖK) saldırısıdır. Yüksek Öğretim Kurumu saldırısında YÖK' ün güvenlik sistemlerindeki zaafiyetlerden faydalanılmıştır. Redhack YÖK'ün internet şebekesinin bir açık ağ haline getirilmiş ve bu sayede ana servera kolayca erişim sağlanmıştır. Bu saldırılar sonucunda Redhack YÖK'ün internet sitesini hackleyerek üniversitelere ait olan çok sayıda evrak ele geçirmiş, bu evrakları da sosyal paylaşım sitesi olan Twitter'daki hesaplarından paylaşmışlardır. Bu ele geçirilen ve paylaşılan evraklar arasında YÖK'e yapılmış olan ihbar ve şikayetler ile Hukuk Müşavirliği'nin çok gizli yazışmaları da bulunmaktaydı. Bu saldırıda IP aldatması yöntemi kullanıldığından saldırılarda kullanılan bilgisayarların IP adreslerinin ya kamu kurumlarına ya da ilgisiz kişiler adına kayıtlı çıkmıştır[54].

3.10. SQL İnjection Yöntemi;

Siber Saldırı yöntemlerinden bir diğer ise SQL İnjection Yöntemidir.

İnternet sitelerinin bir çocuğunda, sayfayı dinamik tutmak için veri tabanından yararlanılmakta olup güncel olan veritabanı yazılımlarının birçoğunda ise Structured Query Language (SQL) isimli orta bir dil kullanılmaktadır.

SQL veri tabanlarında veri alma, veriyi değiştirmeye silme işlemleri için kullanılan basit yapılı bir dil olmakla birlikte günümüzde neredeyse tüm web tabanlı uygulamaların altyapıları veri tabanı destekli olup bu web uygulamaları ise veri tabanı ile SQL dili vasıtasıyla anlaşırlar[55].

SQL Injection yöntemi ise veri tabanına dayalı uygulamalara saldırmak için kullanılan bir saldırı tekniği olmakla birlikte saldırgan tarafından SQL dilinin özelliklerinden yararlanılmak sureti ile standart uygulamanın ekranında ilgili alana

---

[54]Bkz.http://gundem.bugun.com.tr/redhackler-yoke-nasil-sizdi-haberi/218675 (Erişim Tarihi: 08.05.2017)

[55]Bkz. http://www.kodevreni.com/526-sql-injection-nedir-ve-sql-injection-nasıl-önlenir/ (Erişim Tarihi: 09.05.2017)

bir SQL ifadesi eklenir, bu sayede ise saldırgan tarafından veri tabanının içeriklerinin aktarılabilmesi imkanı doğar. Bu saldırıda uygulamaların içerisinde bulunan bir güvenlik zafiyetinden faydalanılır.

SQL Injection yöntemi genel olarak internet üzerinde bulunan web siteleri için kullanılmakta olan bir saldırı türü olarak biliniyor olsa da bu saldırıyı SQL veri tabanına dayalı olan tüm uygulamalar için uygulamak mümkündür.

Bu saldırı yöntemi ile saldırganlar sistemdeki kullanıcının bilgileri ile sisteme giriş yapabilmekte, sistemde bulunan verileri değiştirebilmekte, yok edebilmekte veya ifşa edebilmektedir. Bu saldırı ile saldırgan sistem üzerinde sistem yönetici hakkı kazandığından yöneticisi olarak işlem yapabilmektedir[56].

SQL injection yönetime örnek vermek gerekirse bilinen hacker gruplarından Redhack 2013 tarihinde Diyanet İşleri Başkanlığı'na ait web sitesinin veri tabanına giriş yapmış ve bunun nasıl yapılabileceğini Twitter hesabı üzerinden herkesle paylaşmıştır.

SQL injection saldırılarına engel olabilmek için sistem yöneticisi tarafından alınması gereken en önemli önlem sistem kullanıcı isim ve şifrelerinin birer bilgi yerine parametre hali izin vermemek için sistem yöneticisi tarafından yapılması gereken kullanıcı adını ve parolayı salt birer bilgi olarak oluşturulması yerine parametre haline getirilmesidir[57].

3.11. Sosyal Mühendislik Saldırıları (Social Engineering)

Saldırganlar tarafından siber saldırılarda kullanılan bir başka yöntem ise Sosyal Mühendisliktir.

Sosyal Mühendislik diğer siber saldırılardan farklı olarak bilişim sistemlerinin değil insanların zafiyetlerinden yararlanılarak yapılan bir siber saldırı

[56]Bkz.https://tr.wikipedia.org/wiki/SQL_Injection (erişim Tarihi: 09.05.2017)
[57]Bkz.http://teknolog.radikal.com.tr/redhack-nasil-hackliyor/#sthash.uRZQI5EX.dpuf (Erişim Tarihi: 12.05.2017)

türü olmakla birlikte siber saldırı türleri arasında en çok zarar meydana gelmesine sebep olan saldırı türüdür.

Bu saldırıda hedef bir bilgisayar veya sistem değil bizzat kişidir ve insani zaaflar, güven duygusu gibi insani unsurlardan faydalanmak, kişiler hakkında bilgi toplamak ve bu açıklardan faydalanmak suretiyle yapılır. Saldırılarında hedef insandır ve kişilerin zafiyetlerinden faydalanarak gerekli bilgiyi toplamak üzerine yapılan saldırılardır.

Bu saldırı türünde siber güvenlik alanında tüm önlemler dahi alınmış olsa alınan bu önlemlerin etkisiz hale gelmesini sağlamaktadır. Bu sebeple siber güvenliğin en temel zafiyeti insandır. Saldırı ile amaçlanan insan doğasından istifade ederek farklı aldatma teknikleri ile sistem hakkında bilgi edinerek sistemde mevcut verilerin ele geçirilmesi, değiştirilmesi veya sisteme erişim sağlamaktır[58].

Oltalama ve istenmeyen elektronik postalar gönderilmesi saldırı yöntemleri kullanıcıyı kandırmak suretiyle belirli faaliyetlerin gerçekleştirilmesine çalışıldığından saldırı birer sosyal mühendislik saldırısı olarak değerlendirilebilir..

İnsanlar arasındaki iletişim kişiler arasında, kişiler ile kurumlar arasında ve kurumlar ile kurumlar arasındaki etkileşimler şeklinde olabileceği gibi insan davranışlarındaki zafiyetlerde insanların günlük hayatlarındaki davranışlarındaki bilgisizlikten, dikkatsizlikten ve kişisel zaaflardan faydalanmak suretiyle hedef kişilerin veya kurumların normal yollardan elde edilemeyecek bilgilerine ulaşılarak ve bu bilgiler vasıtasıyla güvenlik süreçlerinin atlatılmasını sağlamaktır.

Sosyal mühendislikte saldırganlar hedef kişiye güvenilir bir kaynak olduklarını hissettirerek veya ortak tanıdıklar üzerinden yakınlık kurarak yaklaşabilecekleri gibi özellikle iletişim araçları vasıtasıyla başkalarını taklit etmek, gizlice zor bir durum oluşturarak hedef kişiye bu zor durumdan çıkmasında

[58]Bkz.http://www.bilgiguvenligi.gov.tr/sosyal-muhendislik/sosyal-muhendislik-saldirilari-3.html (Erişim Tarihi: 12.05.2017)

yardım ediyormuş izlenimi vererek yapılabileceği gibi hedef kişinin çöp kutusunun karıştırılarak kişi hakkında bilgi edinmeye kadar bir çok yöntem izlemektedirler[59].

Sosyal Mühendislik saldırılarında ilk olarak saldırgan hedef kişi veya kurum hakkında bilgi toplamakta, daha sonra topladığı bilgiler ile hedef kişi ile iletişime geçilerek ve bu bilgileri de kullanmak suretiyle hem daha çok bilgiye ulaşır hem de saldırı amacı doğrultusunda kullanabileceği araçları tespit eder. Saldırgan elindeki mevcut bilgileri ve araçları kullanmak suretiyle uygulamaya geçerek nihai amacına ulaşır. Genel olarak bu saldırılarda nihai amaç maddi kazanç elde etmektir.[60] (AKARSLAN, 2015)

Sosyal mühendislik saldırılarına verilebilecek ülkemizde şu anda da çok popüler olan "Telefon Dolandırıcılığı" dır. Telefon dolandırıcılığı yapan saldırganlar sosyal mühendislik kullanarak karşısındaki kişi hakkında bilgi edinmekte ve korkutmak suretiyle hedef kişinin parasını alarak maddi kazanç elde etmektedir.

Bilinen ilk sosyal mühendislik saldırısı ise ilk bilgisayar korsanlarından olan Kevin Mitnick tarafından gerçekleştirilmiş olup kullandığı yöntem ile erişmek istediği sistemde çalışmakta olan çalışana telefon ile ulaşarak kızgın üstleri gibi konuşarak istediği bilgileri elde etmiştir. Bu yöntemi kullanarak Digital Equipment, Sun Microsystems, IBM, Silicon Graphics, Nokia, Motorola ve Fujitsu gibi büyük markaların sistemlerine sızmıştır. Kevin Mitnick 15 Şubat 1995 yılında FBI(Federal Bureau Of İnvestigation) tarafından yakalanmış ve büyük şirketlerin bilgisayar ağlarına izinsiz girmekten suçlu bulunarak 5 yıl hapis cezası ile cezalandırılmıştır[61].

---

[59]Bkz. EREN, Mehmet , "*Avrupa Birliği'nin siber güvenlik politikası*", Beta Yayınları, 1. Baskı, Mart 2017, İstanbul, sy.53

[60]Bkz. AKARSLAN, Hüseyin, Bilişim Suçları, Seçkin Yayınevi, 2. Baskı, Mayıs 2015, Ankara s.104-105

[61] Bkz.https://tr.wikipedia.org/wiki/Kevin_Mitnick (Erişim Tarihi: 09.05.2017)

"Bilgi güvenliğinin en zayıf halkası insandır ve bilgi güvenliğine yönelik yapılan saldırılarda sosyal mühendislik kullanılarak yani insan unsuru kandırılarak gizli bilgilere ulaşılabilir"[62]

2011 yılı içerisinde 6 ülkede yapılan bir araştırma sonucu göstermektedir ki araştırmaya katılan katılımcılardan %43'ü en az bir kere sosyal mühendislik saldırısına maruz kaldığı ve maruz kalan katılımcıların %48'inin de bu saldırıların her birine yaklaşık 25.000 dolar kaybettirdiğini belirtmişlerdir[63]. (HEKİM & BAŞIBÜYÜK, 2014)

Sosyal mühendislik yöntemi insanların güven , korku, yardım isteği gibi duyguları kullanarak hackerların kurbanlara istediğini yaptırmasını sağlayan çok tehlikeli bir silahtır. Saldırganların en güçlü silahı olan sosyal mühendislikte dikkat edilmediği zaman önlenmesi imkansızdır.

3.12. Defacement (Web Sitesinde Tahrifat Oluşturan Ya Da Web Sayfasının Görüntüsünü Değiştiren Saldırılar),

Türkçesi "yüzü bozma" anlamına gelen Defacement saldırıları hedef web sayfasının görüntüsünün değiştirilmesi şeklinde açıklanabilir bu saldırının amacı siyasi bir mesaj vermek olabileceği gibi saldırgan tarafından kişisel reklamını yapmak amacıyla da gerçekleştirilebilir. Bu saldırı yöntemi ile saldırganlar web sayfasının normal görüntüsünü bozarak amaçlarını gerçekleştirirler.

Defacement saldırıları hedef alınan kuruluşun itibarını doğrudan etkilediği için önemli bir saldırı türüdür. Ayrıca bu saldırılar sonucunda saldırıya uğrayan internet sitesi ile aynı sunucuyu paylaşan başka bir sayfadaki zafiyet sonucunda

---

[62] Bkz. AKARSLAN, Hüseyin, "*Bilişim suçları"*, Seçkin Yayınevi, 2. Baskı, Mayıs 2015, Ankara s.104-105 ve orada dn. 204'te anılan Mitnick,Kevin D. Ve William L. Simon, (2005), Aldatma Sanatı, Ankara: Odtü Geliştirme Vakfı Yayıncılık, s.3.

[63] Bkz. Yrd. Doç. Dr. Hakan HEKİM, Doç. Dr. Oğuzhan BAŞIBÜYÜK, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları- Cyber Crimes and Turkey's Cyber Security Policies", Uluslararası Güvenlik ve Terörizm Dergisi, Cilt 4, Sayı 2 , Yıl 2014 , sy.144

şirket de zarar görebileceği gibi Web sayfasının üzerinde bulunduğu sunucudaki veriler çalınabilmesi veya Web sayfasının kullandığı sunucu üzerinde Domain Admin yetkilerine sahip bir hesap tanımlıysa bu hesap bilgileri çalınabilmesi mümkündür[64].

Redhack, 2011 yılında Anonymous olarak bilinen Internet hacktivist örgütü ile ortak gerçekleştirdikleri saldırılar neticesinde 1.000' e yakın Türk sitesini bu yöntem kullanılarak hacklemiş Türk Hükümetine ait 74 adet web sitesine yazı veya resim bırakmışlardır.

3.13. Siber Casusluk Ve İstihbarat Saldırıları

Bu saldırı yönteminde devletler tarafından yapılabileceği gibi şirketler arasında da yapılmakta olup siber casusluk ve istihbarat saldırılarında casuslar tarafından bilgi toplama amacıyla genel olarak sosyal mühendislik saldırı yöntemleri kullanılmaktadır. Bu yöntem sonucunda rakip firma sitesine direkt saldırıda bulunulmakta ve rakip firmanın altyapı bilgileri, finansal durumu, gelecek planları çalınmak amacıyla yapılmaktadır.

Oracle ile Microsoft arasındaki savaş şirketler arasında gerçekleştirilen siber casusluk saldırılarının en güzel örneklerindendir.

Siber casusluk ve istihbarat saldırıları sadece rakip firmalar arasında değil ülkeler arasında da yapılmakta olup bu durum rakip ülkenin ürün ve markalarının kullanımını durdurmaya kadar varabilmektedir. Çin ile Büyük Amerikan şirketleri arasındaki savaş bu durumun en güzel örneğidir. Çin, yaptığı siber casusluk saldırıları ile Microsoft'un gizli işletim şifresini alarak tüm dünyada Cisco ve Microsoft'un yazılımlarını indirimli fiyatlara satmaya başlamış ve fabrika kurarak router denilen yönlendiricilerin korsan üretimine başlamıştır. Çin tarafından ucuza satılan yönlendiricilerin ABD askeri kuruluşları tarafından alındığı ortaya çıkması

[64]Bkz. http://en.wikipedia.org/wiki/Website_defacement (Erişim Tarihi:10.06.2018)

üzerine FBI tarafından yapılan bir soruşturma neticesinde bu cihazların olası bir siber savaş sırasında Amerikan askeri ağlarını çökertmek için kullanılabileceği ortaya çıkmıştır. Daha sonra Çin sahte Cisco üretimini durdurarak Huawei isimli kendi markasını yaratarak yönlendirici pazarına sokmuştur. ABD tarafından 2019 yılı başında Huawei marka ürünlerin satışı tamamen yasaklanmıştır. Ayrıca Microsoft ve Cisco ürünlerindeki zayıf noktaları bilen Çin kendi gizli askeri bilişim sistemlerinde kullanmak için son derece sağlam ve kırılması imkansız olan Kylin isimli kendi işletim sistemini üretmiştir[65]. (CLARKE & KNAKE, 2011)

Günümüzde bireyler birçok uygulama ve akıllı telefonlar vasıtasıyla örnek olarak Foursquare gibi sosyal ağlar üzerinden nerede olduklarını ne yaptıklarını sosyal ağlar vasıtasıyla paylaştıkları bilgilerin kimler tarafından ve nasıl toplandığına bakmadan herkese açık olarak bildirmektedirler. Bu sebeple günümüzde arama motoruna kişinin adının yazılması dahi istihbarat toplamak için yeterli olabilmektedir.

Siber Casusluk ve İstihbarat saldırılarının önlenebilmesi için öncelikle saldırıların en zayıf faktörü olan kişi faktörü olduğu göz önüne alınmak suretiyle devletler yada şirketler bünyesinde çalışan kişilerin düzenli olarak takip edilmesi, çalışanların düzenli aralıklarla rotasyondan geçirilmesi, bir çalışanın bilginin tamamını elde etmesinin engellenmesi, kullanıcıların elektronik ortamdaki faaliyetlerinin denetlenmesi ve sistemlerde erişim yetkilerinin çok dikkatli düzenlenmesi gerekmektedir.

4. SİBER SALDIRILARIN DOĞURDUĞU SONUÇLAR

Günümüzde siber alanda bilişim sistemleri ve bu sistemlere yönelik yapılan saldırıları sebebiyle çok büyük zararlar meydana gelmektedir. İnternetin

[65]Bkz. CLARKE, Richard A.; KNAKE, Robert K. , Siber Savaş, (Çeviren: Murat Erduran), İkü Yayın Evi, Nisan 2011, s.35

hayatımızda bulunduğu her alanda siber tehditler karşımıza çıkması ve bir şekilde bu tehditler neticesinde zarar meydana gelmesi mümkündür. Yapılan saldırılar neticesinde şirketlerin ticari sırları, devletlerin savunma politikaları ve gizli projeleri, kişilerin kişisel verileri, TC kimlik numaraları çalınmakta kredi kartları kopyalanmaktadır.

Hatta ABD de 2016 yılında işlenen bir cinayet soruşturmasında cinayeti araştıran polis Amazon firmasından kadının evinde bulunduğu fark edilen Echo isimli akıllı ev asistanı cihazı olay mahaline yakın olduğundan cinayete ilişkin ses kaydı almış olabileceği varsayımı ile ses kayıt bilgilerini istemiştir.

Saldırıların yaratabileceği zarar zadece bilgisayarlar veya telefonlarla sınırlı kalmamaktadır. Akıllı saatler, akıllı telefonlar, akıllı evler, arabalar hatta sağlık teçhizatları ve kullanılmakta olan birçok elektronik cihaz artık internet sayesinde "akıllı" hale gelmiş olup bu gelişim düzeyi aynı zamanda zafiyetleri de beraberinde getirmiştir. Sağlık için kullanılan kalp pilleri uzaktan erişimle kontrol edilmesi şu an ki durumda muhtemeldir. Bilişim sektörüne bağımlılık saldırganlara ve saldırılara karşı her gün daha da savunmasız hale gelinmesine sebep olmaktadır. Bilişim sistemlerine hayatın her alanında duyduğumuz bağımlılık tehditlerin ne boyutta zarar verebileceğini göstermektedir.

2014 tarihinde Avrupa Polis Teşkilatı Europol ilk online cinayetin yıl sonuna kadar işlenmesini bekledikleri açıklanmış olup Europol tarafından güvenlik şirketi IID'nin raporuna atıf yapılarak yapılan uyarı ile; Raporda hackerların kablosuz internet bağlantısı olan kalp pili üzerinden bir kişiyi öldürebilecekleri online cinayetin kalp pilinin dışında insülin pompaları üzerinden veya hastane odalarındaki akıllı yataklardan da yapılabileceği belirtilmiş olup raporda ayrıca çevremizi saran internet ağları nedeniyle fidye olaylarının da yakın gelecekte artacağı öne sürülmüş ve hackerların akıllı garaj kapısı, asansör veya araba üzerinden istedikleri kişileri rehin alabilecekleri belirtilmiştir[66].

[66]Bkz.https://www.sabah.com.tr/pazar/2014/10/19/ilk-online-cinayet-bir-tik-uzakta (Erişim Tarihi: 21.05.2017)

Bu nedenle öncelikle devletler bazında gerekli siber güvenlik önlemlerinin alınması ve geçerli güncel siber güvenlik politikalarının oluşturulması gerekmekte olup bireylere ve kurum ve kuruluşlara müşterilerinin bilgilerini koruma konusunda gerekli siber güvenlik önlemlerini alma ve bu hususta toplumun bilinçlendirilmesi için önemli bir görev düşmektedir.

Bu görevlerin en kritik olan bilgi güvenliği açısından incelendiğinde ve siber güvenliğinde temel prensipleri içerisinde yer alan olan verinin gizlilik, bütünlük ve erişilebilirliğini koruma görevidir. Bilgiyi saklamakla görevli kurumların, sahip oldukları kurumsal verileri ve müşterileri kişisel verilerinin gerçekliğini, bütünlüğünü ve erişilebilirliğini bunun yanında yetkili kişiler arasında da paylaşılabilirliğini garanti altına alması gerekmekte olup bu amaç doğrultusunda oluşturulmuş ve kullanılmakta olan programların da bilgi güvenliği prensipleri doğrultusunda görevlerini tam ve eksiksiz yerine getirmeleri gerekmektedir[67]. (HEKİM & BAŞIBÜYÜK, 2014)

Türkiye'nin son siber güvenlik strateji belgesi olan Ulusal Siber Güvenlik Stratejisi 2016-2019 Eylem Planı'nda bilgi güvenliği prensipleri şu şekilde tanımlanmıştır;

Gizlilik kavramı bilginin yetkisiz kişiler, varlıklar veya süreçlere kullanılabilir yapılmama ya da açıklanmama özelliğini,

Bütünlük kavramı varlıkların doğruluğunu ve tamlığını koruma özelliğini,

Erişilebilirlik kavramı ise yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliğini, ifade etmektedir[68]. (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016)

Siber saldırılar çok büyük zararlara yol açmakta olup geçmişte bireyler ve şirketler için sadece güvenlik duvarından oluşan güvenlik teknolojileri, günümüzde

---

[67]Bkz. Yrd. Doç. Dr. Hakan HEKİM, Doç. Dr. Oğuzhan BAŞIBÜYÜK, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları- Cyber Crimes and Turkey's Cyber Security Policies", Uluslararası Güvenlik ve Terörizm Dergisi, Cilt 4, Sayı 2 , Yıl 2014 , sy.137

[68] Bkz. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve 2016- 2019 Eylem Planı, Ocak 2016

daha geniş , gelişmiş ve karmaşık bir sistem haline gelmiş durumdadır. Hacker'ların düzenlediği siber saldırılarda güvenlik duvarlarını aşmak için bugün en az bilindiği kadarıyla 800 milyon farklı yöntem denenmektedir. Başlıca TCP/IP protokollerini kandırmak için geliştirilen ve giderek daha komplike ve gelişmiş saldırılara dönüşen bu saldırı çeşitleri Advanced Evasion Techniques (AVT) olarak adlandırılmaktadır[69].

Aşağıda örnekler ve şirketlerin yayınladıkları siber güvenlik raporları kapsamında dünyada meydana gelen siber saldırılar ve meydana getirdikleri zararların büyüklüğü açıklanmaya çalışılacaktır.

- Labris Networks şirketi tarafından 2014 yılı Siber Güvenlik Raporu ve 2015 yılı için Öngörüleri açıklanmış olup bu rapor kapsamında 2014 yılı içerisinde yapılan değerlendirme ve incelemelerde Türkiye'de özellikle spam(istenmeyen elektronik posta) konusunda çok önemli sorunlar yaşandığı, iletilen tüm elektronik postalarda spam oranının %84'e ulaştığı belirtilmiş ve spam içeren elektronik posta oranının önceki seneden %140 arttığı, spamlerde en çok karşılaşılan konuların online ürün satışları olduğu, online ürün satışlarını, zararlı yazılım taşıyan iletiler, kurumsal teklifler, arkadaşlık ağları ve cinsel içerikli elektronik postaların takip ettiği, tehditlerinde önceki yıla nazaran %10 artış gösterdiği, 2014 yılı içerisinde casusluk ve fidye maksadı ile kullanılan zararlı yazılımların en yüksek seviyeye ulaştığı belirlenmiş olup raporda siber dünyanın bir savaş alanı olduğu vurgulanmıştır. Rapora göre 2014 yılı içerisinde Labris SOC'da gözlemlenen kişisel bilgisayar tabanlı zararlı yazılımların %96'sı Windows işletim sistemini hedef aldığı, mobil tabanlı zararlı yazılımların %97'si Android işletim sistemini hedef aldığı belirlenmiştir[70].

[69]Bkz. http://www.memurlar.net/haber/489141/ (Erişim Tarihi: 21.05.2017)
[70]Bkz.http://labrisnetworks.com/tr/tr-labris-networks-2014-siber-guvenlik-raporu-ve-2015-ongoruleri-yayinlandi/(Erişim Tarihi: 22.05.2017)

Cisco tarafından şirketlerin, günümüzde siber güvenlik konusundaki zorlukları daha iyi anlayarak cevap verebilmelerinin sağlanması amacı ile "Güvenlik Manifestosu" nu açıklamıştır.

- Dimensional Research firması tarafından 2011'de sosyal mühendislik saldırılarına yönelik araştırmaya göre; Güvenlik uzmanlarının % 97'si ve tüm Bilişim Teknolojisi uzmanlarının % 86'sı potansiyel güvenlik tehdidinin farkında olup, % 43'ü sosyal mühendislik programlarının hedefi olmuş sadece % 16'sı sosyal mühendislik tarafından hedef alınmadıklarını belirtmiştir. Araştırmaya göre finansal kazançlar, sosyal mühendisliğin ana motivasyonu olup sosyal mühendislik saldırılarının % 51'i mali kazanç motivasyonu ile yapıldığını ortaya konmuştur. Sosyal mühendislik saldırılarının %14'ü ise intikam amacıyla yapılmaktadır. Büyük şirketlerin% 48'i ve her büyüklükteki şirketin% 32'si 25 veya daha fazla sosyal mühendislik deneyimlemiştir. Son iki yılda saldırılar tüm katılımcıların % 48'inde olay başına ortalama maliyet 25.000 doları aşmış olup büyük şirketlerin% 30'u olay başına maliyeti 100.000 dolardan fazla olduğu tespit edilmiştir. Ayrıca araştırma neticesinde yeni çalışanların sosyal mühendislik saldırılarına karşı en hassas grubu oluşturduğu belirlenmiştir[71].

Yukarıda anılan gibi örnekleri binlercesiyle çoğaltmak mümkündür. İnternetin günlük hayatın her anına ulaşmasıyla birlikte günümüzde her üç kişiden biri kimlik hırsızlığının hedefi olmaktadır ve bu oran gün geçtikçe artmaktadır. Bu sebeple siber saldırılara karşı koruyucu önlemler almak ve bilinçlenmek, siber güvenlik politikalarının devletler, bireyler, şirketler ve kurumlar bazında çok sıkı bir şekilde uygulanması ve gerekli her türlü tedbirin alınması gerekmektedir.

[71]Bkz. Dimensional Research (2011). The risk of social engineering on information security: Asurvey of IT professionals belgenin orjinaline https://www.stamx.net/files/The-Risk-of-Social-Engineering-on-Information-Security.pdf adresinden erişilmiştir. (Erişim Tarihi: 01.06.2017)

İKİNCİ KISIM
SİBER GÜVENLİK POLİTİKALARI

1. SİBER GÜVENLİK NEDİR?

Siber Güvenlik, siber alemdeki hayatın güvenliği ve gizliliğinin korunmasıdır.

Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planında siber güvenlik kavramı "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 döndürülmesini " şeklinde tanımlanmıştır[72]. (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016)

Siber güvenlik kavramı bilişim ve iletişim teknolojileri vasıtasıyla savunmasız durumda olan dijital sistem, bilgi ve veriyi güvence altına almakla ilgili olup bunun yanı sıra verilerin saklandığı, depolandığı ve verilerin güvenliğini sağlamak için teknolojinin kullanıldığı bir alan olarak karşımıza çıkar. Siber Güvenlik, siber uzayın saldırılardan korunma ve koruma yeteneği olarak açıklanabilir.[73]

Bu kısımda Siber güvenlikle ilgili bir kavram olarak bilgi güvenliğine de değinmek gerekmektedir.

Buna göre veri işlenmemiş ham bilgi, data olarak tanımlanır.

---

[72] Bkz. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve 2016- 2019 Eylem Planı, Ocak 2016

[73]Bkz. https://www.yazilimbilimi.org/bilgi-guvenligi-ve-siber-guvenlik-arasindaki-farklar-nelerdir/ (Erişim Tarihi:02.01.2019)

Bilgi ise yazılı, basılı, görsel, işitsel ve elektronik ortamlarda var olan, depolanabilen, tanımlanabilen, düzenlenebilen, transfer edilebilen ve erişilebilen ve bilişsel yapıda değişiklik yaratan her türlü veridir. [74]

Bilgi ve veri arasındaki temel farklılık her bilginin bir veri olduğu ancak her verinin bir bilgi olmadığı hususunda ortaya çıkmaktadır. Bir veri bir bağlam kapsamında yorumlandığında ve veriye bir anlam verildiğinde bilgi olarak çağrılabilir. Örnek olarak "101189″ sayı dizisi bir veri iken bu verinin doğum tarihi olduğunu bilmemiz halinde bilgiye dönüşmektedir. Sonuç olarak bilgi anlamlandırılmış veridir.

Bilgi güvenliği kavramı ise bilginin gizlilik, bütünlük ve erişilebilirliğini ifade etmekte olup bu üç kavram bilgi güvenliğinin üç temel prensibini oluşturur. Bu temel prensipler kapsamında bilgiye izinsiz olarak yetkisiz kişilerce erişim sağlanamamasını, kullanılamamasını, bilginin değiştirilememesini, bilginin ifşa edilememesini ve ortadan kaldırılamamasını ifade eder. Bilgi güvenliğinin temel amacı bu yetkisiz müdahaleleri önlemektir.

Bilgi güvenliğinin bu prensipleri temelde siber güvenlik alanında belirlenen prensipler olarak ta karşımıza çıkmaktadır. Her iki alanın siber uzayda iç içe geçmesi sebebi ile ortak prensip kullanmaları sonucu ortaya çıkmıştır. Temel prensipler daha detaylı incelendiğinde ise ;

Gizlilik(confidentiality) kavramı bilginin yetkisiz kişiler tarafından ele geçirilmesine ve yetkisiz erişime karşı korunması anlamına gelmektedir.

Bütünlük (integrity) kavramı bilginin yetkisiz kişiler tarafından değiştirilmemesidir.

Erişilebilirlik(availability) kavramı ise bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanılabilir durumda olmasını ifade etmektedir[75].

---

[74] Bkz. Dr. Türkay Henkoğlu ,"Bilgi Güvenliği ve Kişisel Verilerin Korunması",Yetkin Yayınları, Ankara 2015, s.27-28

[75]Bkz.https://www.sibergah.com/genel/bilgi-guvenligi-nedir-ve-nasil-siniflandirilir/ (Erişim Tarihi: 22.07.2017)

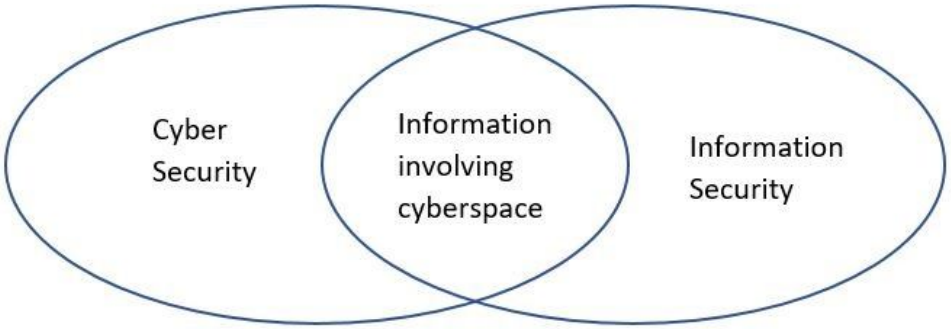
Bu üç temel prensipten birinde veya birden fazlasında herhangi biri zarar veya ihlal meydana gelmesi durumunda ise güvenlik zafiyeti oluşur.

Bilgi güvenliği kavramı fiziksel veya siber ortamda olsun, bilgi ve bilgilerin korunmasıyla ilgilenen daha geniş bir alan olmakla birlikte siber güvenlik ise siber uzay alanının korunması ve onu herhangi bir suç için veya suça karşı kullanmasıyla ilgilenen bir alandır. Bu iki alan günümüzde çoğunlukla bir arada ve iç içe geçmiş şekilde bulunmaktadır. Bu durumun temel sebebi bilginin çoğunlukla siber ortamda varlık göstermesi ve siber uzayın içinde yer almasından kaynaklanmaktadır. Halihazırda siber uzayda yapılmakta olan siber saldırıların bilgiye erişmek, gizli bilgiyi ifşa etmek, bilginin bütünlüğüne ve erişilebilirliğine zarar vermek veya yetkili kullanıcılara erişimi engellemek için gerçekleştirilmesinden kaynaklanmaktadır.

Bilgi güvenliği genel anlamı itibariyle daha geniş kapsamlı bir kavram olup siber uzayda olsun veya olmasın her türlü bilginin güvenliği konusu ile ilgilenmekte olup siber uzay içindeki bilginin tehdit altında olması halinde siber güvenlik kavramı bilgi güvenliğinin alt başlığı olarak karşımıza çıkmaktadır. Siber uzay içerisinde yer almayan bilginin tehdit altında olması halinde ise mevcut tehdit bilgi güvenliği kapsamında değerlendirilecek olup Siber güvenlik kapsamına girmeyecektir.

Kısaca özetlemek gerekirse siber güvenlik kavramı siber uzayda var olan her şeyin güvenliğinin sağlanması ile ilgilenirken bilgi güvenliği siber uzaydan bağımsız olarak bilginin güvenliği ile ilgilenmektedir. Siber güvenliğin sağlanmasında bilgi güvenliği ile aynı temel prensipler geçerli olduğundan ve siber uzayda bilgi hayati önem taşıdığından bilgi güvenliği kavramı siber güvenliğin temel yapıtaşlarından birini oluşturmaktadır.

Her iki alanın birbiri ile olan ilişkisini aşağıdaki şemada görüldüğü üzere kategorilendirmek mümkündür.



[76]

Genel olarak siber güvenliğin siber ortamda bulunan kurum ve kuruluşlar ile kullanıcıların varlıklarının korunması amacı ile kullanılmakta olan araç, politika, güvenlik kavramı, kılavuz, risk yönetim yaklaşımı, faaliyetler, eğitimler, uygulama ve teknolojiler olarak tanımlanması mümkündür.

Çalışma içerisinde bilgi güvenliği kavramı açıklanırken ve bilgi güvenliğinden bahsedilirken siber güvenliğin temel yapıtaşlarından olan ve siber uzay özelindeki bilgi güvenliği konusu açıklanacaktır.

Siber güvenliğin çalışma alanı içerisine kurumlar ve kuruluşlar ile kişiler ver devletler girer. Bu kapsamda siber güvenlik siber ortamda bulunan kurum, kuruluş ve kullanıcıların varlık, bilgi işlem donanımları, personel, altyapı, uygulama, hizmet, telekomünikasyon sistemi ve siber ortamda iletilen ve saklanan her türlü bilgilerin tümünü kapsamakta olup bu varlık ve bilgilerin siber ortamda meydana gelebilecek güvenlik risklerine ve olası saldırılara karşı koyabilecek şekilde oluşturulmasını ve idame ettirilmesini sağlamayı amaçlamaktadır. Siber güvenliğin temel hedefleri de bilgi güvenliği kapsamında belirlenmiş olan 3 temel prensipten oluşmaktadır. Erişilebilirlik, Bütünlük (bütünlük kavramı aslına uygunluk ve inkar edilemezliği de kapsamaktadır) ve Gizlilik.

Siber güvenlikte üç temel prensip aynı zamanda siber güvenliğin 3 temel amacını da belirlemektedir. Bir amaç olarak gizlilik incelendiğinde ise bilginin

[76]Bkz. https://www.yazilimbilimi.org/bilgi-guvenligi-ve-siber-guvenlik-arasindaki-farklar-nelerdir/ (Erişim tarihi: 02.01.2019)

yetkisiz kişiler, varlıklar ya da süreçlere kullanılabilir yapılmama ya da açıklanmama özelliğini ifade etmekte olduğu ortaya çıkmaktadır[77].

Sadece iç sırlar ve hassas kişisel verilerin iyi korunması siber güvenlik açısından yeterli değildir, işleme dair tüm verilerde şirketler ya da bireyler arasındaki ilişkiler hakkında detayları ortaya çıkarabilme yeteneğine sahiptir. Gizlilik kanuni korumaların yanında şifreleme ve erişim kontrolü gibi teknik araçlarla da desteklenmektedir.

Bütünlük ise varlıkların doğruluğunu ve tamlığını koruma özelliğini ifade etmektedir[78]. (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016) Bütünlük sistemin hem kullanılabilir hem de kendisinden beklendiği şekilde davranacağına dair güveni ifade etmektedir. Bütünlük kavramını örnekle açıklamak gerekirse Stuxnet Saldırısında saldırının hedefi olan bilgisayarlar İranlı sahiplerine Stuxnet virüsü[79] onları sabote ederken bile normal olarak işlediklerini söylemekteydiler. Eğer bir sistemin o an ki mevcut işleyişi hakkında söylediklerine güvenirsek, o sistemin normal işleyip işlemediğini bilmek mümkün mü dür[80]?

Erişilebilirlik kavramı ise yetkili bir kullanıcı tarafından talep edilmesi halinde erişilebilir ve kullanılabilir olma özelliğini ifade etmektedir[81]. (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016)

Siber alanı oluşturan bilişim teknolojileri, saldırılarda amaç olabileceği gibi araç olarakta kullanılabilmekte olup bu saldırılar saldırganlar tarafndan kişisel

---

[77]Bkz. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve 2016- 2019 Eylem Planı, Ocak 2016

[78] Bkz.T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve 2016- 2019 Eylem Planı, Ocak 2016

[79] Stuxnet, ABD ve İsrail'in, İran'ın nükleer çalışmalarını sekteye uğratmak için kullandığı solucan yazılımdır. (https://tr.wikipedia.org/wiki/Stuxnet) (Erişim tarihi: 10.06.2017)

[80]Bkz. "SİNGER,P.W.;FRİEDMAN,Allan, "*Siber güvenlik ve siber savaş*", (Çeviren : Ali Atav), Buzdağı Yayınevi, 1. Baskı, Mart 2015, s.56

[81]Bkz. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve 2016- 2019 Eylem Planı, Ocak 2016

çıkar elde etmek veya başka amaçlarla gerçekleştirilebilmektedir. Siber alanda gerçekleştirilen bu saldırılar ile amaç zarar meydana getirmek olup bu saldırı tehditleri ulusal bir güvenlik sorunu haline gelmektedir.

Kısacası özetlemek gerekirse siber güvenlik; siber tehditlere karşı, bilgi ve iletişim sistemleri (BİS) üzerinde saklanan, işlenen ve iletilen bilgi veya verilerin erişilebilirlik, bütünlük, gizlilik prensiplerinin bütün olarak sağlanmasıyla birlikte bu sistemlerde gerçekleştirilen iş ve işlemlerde sağlanması gereken kimlik doğrulama ve inkâr edilemezlik hususlarının korunması anlamına gelmektedir. Bu unsurlardan bir veya bir kaçının korunamaması veya ihlal edilmesi halinde meydana gelecek sorunlar, bireysel ve kurumsal anlamda kayıplara sebep olabileceği gibi ulusal ve küresel çapta ekonomik, siyasi, sosyal bir çok alanda kayıplar yaşanmasına sebep olur[82]

1.1 SİBER GÜVENLİK KAPSAMINDA BİLGİ GÜVENLİĞİNİN ÖNEMİ

Günümüzde kişi , kurum ve kuruluşlar tarafından hemen her türlü işlem elektronik ve internet ortamında gerçekleştirebilmektedir. Bu işlemler bilgisayar yada cep telefonları aracılığıyla ödeme yapılması şeklinde olabileceği gibi para transferlerinin ve bankacılık işlemlerinin online yapılması veya online olarak alışveriş işlemlerinin yapılmasını ve her türlü dokümana ve bilgiye internet ortamında ulaşılabilmesi şeklinde de olabilir.

İnternet gibi her an herkesin ulaşımı altında olan küresel çapta bir bağlantı aracı ile erişimin sağlandığı bir ortamda ise bilgi güvenliği her zaman birinci derecede öncelik sağlanması gereken bir sorun olarak ortaya çıkmaktadır. Teknoloji gelişmesiyle bilgi çoğalmakta ve bilgiye ulaşımın kolaylaşması ile bilgiyi koruma

---

[82]Bkz. ÜNVER, Mustafa ; CANBAY, Cafer ; MİRZAOĞLU, Ayşe Gül, (2009, Mayıs) "Siber Güvenliğin Sağlanması: Türkiyedeki Mevcut Durum Ve Alınması Gereken Tedbirler, Bilgi Teknolojileri ve İletişimi Kurumu, Bilgi Teknolojileri Ve Koordinasyon Dairesi Başkanlığı, sy. 22 https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FSayfalar%2FSiberGuvenlik%2Fsg.pdf (Erişim Tarihi: 12.06.2017)

her zamankinden önemli hale gelmiştir. Bilginin erişilmesi, korunması, paylaşılması hatta gerçek bilginin elenmesi bir sorunsal olarak karşımıza çıkmaya başlamıştır.

İnternet günlük yaşantının her alanına yayıldığı gibi artık ülkelerin eskiden ulusal sınırları içerisinde kalan ve ülkesel sınırlarla ayrılan ulusal savunma ve güvenlik konuları da bu yayılmadan nasibini almıştır. Her alanda olduğu gibi belki de en büyük risk öğesi olarak ulusal savunma ve güvenlik konularında da bilgi güvenliği en temel sorun haline gelmiştir.

Bilgi Güvenliği alanında yaşanan zafiyetlerin ve güvenlik ihlallerinin her geçen gün artması, kişileri, kurumları ve devletleri yazılım, donanım ve çevre faktörlerini de dikkate alarak oluşturulacak yeni güvenlik yaklaşımları geliştirmeyi zorunlu kılmaktadır.

Bu durumun doğal bir neticesi olarak bilgi ve bilgi güvenliği kavramları finans, ekonomi, bankacılık, hukuk, ticaret, elektronik imza, eğitim, elektronik devlet uygulamaları ve haberleşme gibi bir çok alanda ortaya çıktığı gibi bu alanlarda alanda yeni düzenlemeler getirilmesini zorunlu kılmıştır[83].

Dolayısıyla etkin bilgi güvenliğinin sağlanması için öncelikle donanım , yazılım, ağ ve haberleşme sistemlerinin korunması, düzenli tempest (emisyon) uygulamalarının yaptırılarak zafiyetlerin tespit edilmesi, bilgi güvenliğinde en büyük zafiyet unsuru olan kişi unsuru göz önüne alınarak personelin eğitilmesi ve erişim yetkilerinin tesis edilmesi, kriptografinin kullanılması, fiziki mekanlar, doküman güvenliğinin sağlanması gibi bir çok önlem alınmak suretiyle bilgi güvenliği sağlanmaya çalışılmaktadır.

Burada çarpıcı bir örnek vermek gerekirse ABD de 2008 seçimlerinde kullanılan AVC Edge Elektronik Oylama Makinesi Michigan Üniversitesinden iki araştırmacı tarafından müdahaleye duyarlı mühürlerde hiçbir iz bırakmadan Pac-Man oynamak için yeniden programlanmıştır. Bu durum oy verme gibi bir ülkenin

---

[83] Bkz. Doç. Dr. Yıldıray YALMAN, " Güncel Tehdit ; Siber Saldırılar", Seçkin Yayınları, 8. Bölüm, Bilgi Güvenliği Riskleri ve Bilgi Güvencesi, s. 207

kaderini değiştirebilecek bir işlem için kullanılan bu makineler müdahaleye karşı korumalı olmasına rağmen aslında saldırıya karşı ne derece savunmasız olduklarını ortaya koymuştur. Aynı işlem oy verme sürecine etki edecek şekilde makinenin yeniden programlanabileceğini ve bunu müdahaleye duyarlı mühürlerde iz dahi bırakmadan yapılabileceğini bize göstermiştir[84]. (SİNGER & FRİEDMAN, Mart 2015)

Bu durum göstermektedir ki dijital sistemlere olan bağımlılığımız bu dijital sistemlere nasıl güvenebileceğimiz sorusunu daha da önemli hale getirmiştir. Siber güvenliğin sağlanabilmesi için kullanıcılar dijital sistemlere güvenmeli aynı zamanda dijital sistemler de kullanıcılara nasıl güveneceklerini bilmelidir.

1.2.BİLGİ GÜVENLİĞİNİN SAĞLANMASI

Bilgi-Veri güvenliğinin sağlanmasının iki aşaması vardır. Birincisi kullanıcının sistem ve diğer kullanıcılar karşısında güvenli hissetmesi, diğer ise sistemin kullanıcılara nasıl güvenmesi gerektiği aşamalarıdır[85]. (SİNGER & FRİEDMAN, Mart 2015)

Dijital dünyada güven kriptografi[86] temeline dayanmaktadır. Buna göre kriptografi bilginin gizli tutulma aracı olduğu kadar bilginin bütünlüğünü ve ya bilgiye yapılan herhangi bir müdahaleyi tespit etme yeteneğinde eşit derecede önem arz etmektedir.

---

[84] Bkz.SİNGER,P.W.;FRİEDMAN, Allan, Siber Güvenlik Ve Siber Savaş, (Çeviren: Ali Atav), Buzdağı Yayınevi, 1. Baskı, Mart 2015, s.71-72)

[85] Bkz.SİNGER,P.W.;FRİEDMAN, Allan, Siber Güvenlik Ve Siber Savaş, (Çeviren: Ali Atav), Buzdağı Yayınevi, 1. Baskı, Mart 2015, s.29

[86] Kriptografi, gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür.. Bkz. https://tr.wikipedia.org/wiki/Kriptografi (Erişim Tarihi: 23.07.2017)

Kullanıcının sistem ve diğer kullanıcılar karşısında güvenli hissetmesi hususunda kullanılan yöntemler hash fonksiyonu, kriptografik şifrelemeler ve asimetrik- açık uçlu şifreleme sistemidir.

Burada değinmek gereken bir önemli hususta dijital ve çevrimiçi alanda kullanılan kriptografide en önemli unsur olan "Hash" değeridir. MD5 te denilen Hash fonksiyonu, kriptografik bir özet fonksiyonu olmakla kullanımı çok yaygındır. Bu fonksiyon ile girilen verinin boyutundan bağımsız olmak üzere 128-bitlik bir özet değeri üretir.

Hash fonksiyonu, değişken uzunluklu veri kümelerini sabit uzunluklu veri kümelerine haritalayan algoritma veya alt programlara verilen isimdir. Hash fonksiyonu ile örnek olarak bir kişinin adı değişken uzunlukta ise tekil tam sayı olarak hashlenebilmektedir. Hash fonksiyonlarından geri dönen değerler hash değerleri olarak isimlendirilir[87].

Hash değeri almak için md5sum gibi programlar kullanılır.

Kriptografinin yapıtaşı olan hash değerinde; tek taraflı bir fonksiyon olan hash fonksiyonuna input olarak data verilir ve output olarak bir algoritma elde edilir. Bu algoritma asal çarpanlardan oluşur. Elde edilen sonuç sabit uzunlukta olacaktır. Hash değerini geri döndürmek mümkün olmadığı gibi hash değerini değiştirmeden veriyi değiştirmek matematiksel olarak mümkün değildir. Ayrıca aynı hash değerine sahip iki farklı veri bulmakta matematiksel olarak mümkün değildir. Buna göre veride yapılacak en küçük bir değişiklik hash değerinin tamamen değişmesine yol açacaktır. Bu sebeple hash değeri verinin bütünlüğünü ve değiştirilmediğini ispat etmek için kullanılır.

Bir hash fonksiyonunun iki temel özelliği bulunmaktadır. Bunlar fonksiyonun tek yönlü olması bu sebeple de fonksiyona giren orijinal verinin çıktıdan ayırt edilmesinin çok zor olması diğer ise aynı hash değerini oluşturan iki veri girdisinin bulunmasının çok zor olmasıdır.

---

[87]Bkz. https://tr.wikipedia.org/wiki/Hash_fonksiyonu (Erişim Tarihi: 23.07.2017)

Bu sayede hash değeri verinin eşsiz olmasına olanak sağlamaktadır. Verilerin parmak izi olarak nitelendirilmektedir. Eğer veri veya bilginin hash değeri aynı yöntemle sizin ürettiğiniz hash değeri ile uyumlu değil ise veri veya bilginin değiştirildiği anlamına gelmektedir. Sonuç olarak bu hash değeri ile verinin veya bilginin bütünlüğünü doğrulanabilir[88].

Bu hash fonksiyonunu bir belge veya e-postaya "parmak izi" basmak için kullanmamıza olanak sağlar. Artık bu parmak izi bir belgenin bütünlüğünü doğrulayabilir.

Hash fonksiyonu aynı zamanda adli bilişimde delilin bütünlüğünün ve değiştirilmediğinin ispatı içinde kullanılmaktadır.

Kullanıcının sistem ve diğer kullanıcılar karşısında güvenli hissetmesi hususunda kullanılan yöntemlerden bir diğeri Asimetrik-açık uçlu şifreleme yöntemidir.

Kriptografik güvenlik kontrollerini uygulayarak güvenmek ve kimliği tanıtmak için bazı araçlara gerekmektedir. Kriptografik dijital imzalar "asimetrik şifreleme(Açık Anahtarlı şifreleme)" kullanarak bu güveni sağlamaktadırlar[89].

Bir mesajın dijital imzası dijital parmak izi ile anahtar kriptografisinin ortak hareket etmesi neticesinde oluşmaktadır. Dijital imzalar her türlü veri için bütünlük kontrolü yapılabilmesine imkan sağlamaktadır.

Ancak burada başka bir sorunsal meydana gelmektedir. Bir dijital imza sadece umumi anahtarın karşılığı olan özel anahtara erişim anlamına gelmektedir. Ancak umumi anahtarın geçerliliği anlamına gelmemektedir. Umumi araçların geçerliliğini nasıl sorgulanacaktır.

Umumi araçların geçerliliğinin sorgulanmasında bir kuruluş bir umumi anahtara imzalı dijital sertifikalar üreten yetkili kuruluşlar aracılığı ile bağlanır. Sertifika Kuruluşları (CA: Certificate Authorities) bilinen büyük kuruluşlar

---

[88]Bkz. SİNGER,P.W.;FRİEDMAN, Allan, Siber Güvenlik Ve Siber Savaş, (Çeviren : Ali Atav), Buzdağı Yayınevi, 1. Baskı, Mart 2015, s.29

[89]Bkz. https://tr.wikipedia.org/wiki/Açık_anahtarlı_şifreleme , (Erişim tarihi: 11.11.2017)

olmakla sertifikalar bu kuruluşlar imzalanır. Bu kuruluşların umumi anahtarları yaygın olarak bilinmekte olup bu sebeple sahtesi üretilmesi çok zordur. Bu sayede bir sertifika kuruluşuna güvenildiği zaman o kuruluş tarafından imzalanan umumi anahtara da güvenilmektedir.

Umumi anahtarlar, imza ve sertifika kuruluşlarının içinde bulunduğu sistem günümüzde internete hatta sosyal ağlara bağlanan herkesçe farkında olmadan kullanılmaktadır. HTTPS bağlantılı web sitelerini ziyaret edildiğinde güvenli bağlantıyı doğrulamak için adres çubuğunda çıkan küçük kilit simgesi güvenli bir web sitesini ziyaret edildiği anlamına gelmektedir. Bu durumda Sertifika kuruluşuna güvenildiği anlamına gelmekle internette HTTPS bağlantılı web sitesine erişilmek istendiğinden tarayıcı kendi umumi anahtarı ile internet alanına bağlanmakta ve güvenli alanın umumi anahtarı ile Sertifika Kuruluşu(CA) tarafından imzalanmış bir sertifika sormaktadır. O sunucuyu doğrulamanın yanında tarayıcı sertifikanın ait olduğu iddia edilen organizasyonla da konuşarak şifreleme anahtarlarının karşılıklı değişimi sağlanmakta ve güvenli haberleşme mümkün hale gelmektedir.

Bu noktada Sertifika kuruluşları güvenli bağlantı için çok önemli bir rol oynamakta olup bir sertifika kuruluşunun imzalama anahtarının çalınabilmesi halinde güvenli trafiğe müdahale edilebilmesi mümkündür. 2011 yılında Hollandalı bir Sertifika Kuruluşunun imzalama anahtarları çalınmış olup çalan kişi bu anahtarları İranlı kullanıcıların Google'ın gmail hesaplarına erişimlerine müdahale etmek için kullanmıştır.

Yukarıda veri/bilgi güvenliğinin karşılıklı güvenin sağlanabilmesi için güvenin bir tarafı olan kullanıcının sistem ve diğer kullanıcılar karşısında güvenli hissetmesi için kullanılan yöntemleri açıklanmış olup veri güvenliğinin karşılıklı güvenin sağlanabilmesi için güvenin diğer tarafı olan sistemin kullanıcılara nasıl güveneceği hususuna da değinmek gerekmektedir.

Burada bilişim sistemleri kimlik tespiti ve kimlik doğrulamasından sonra kullanıcıyı yetkilendirmektedir. Sistem üzerinde kimin ne yapabileceğini kararlaştırmak için erişim kontrolü yöntemini kullanılmaktadır. Erişim kontrolü bir

işletim sisteminde verinin okunması, yazılması ve kodun yerine getirilmesi yeteneğini sağlamaktadır.

Erişim kontrolü konusunda oluşan zafiyetlerin en bilinen örnekleri 2010 yılında Bradley Manning ve Wikileaks olayı ile 2013 yılında Edward Snowden tarafından NSA'da sistem yöneticisi olarak çalışan düşük seviye bir yüklenicinin basına sızdırdığı birçok tartışmalı ve çok gizli programlara erişimi olduğu gibi son zamanların siber içerikli en büyük erişim kontrolü ihlallerindendir[90].

Bu örneklerden de anlaşılacağı üzere zayıf erişim kontrolleri istedikleri her şeye temel erişim sağlanan düşük yetki seviyesindeki bireyler tarafından erişimin kayıt edilmesine ve kullanılmasına imkan sağlamaktadır.

Zayıf erişim kontrolü gizli verilere erişim yetkisi olmayan kişilerce verilere erişim verinin hatta ticari sırların bile güvenliğinin sağlanması mümkün olamamaktadır.

2. ÜLKELERİN VE ULUSLARARASI TOPLULUKLARIN SİBER GÜVENLİK POLİTİKALARI

Çalışmanın bu bölümünde dünyada siber güvenlik alanında öncü olan yedi devlet, uluslararası topluluk ve Türkiye'nin siber güvenlik alanında oluşturduğu politikalar, uygulamaları ve politik görüşleri detaylı olarak incelenecektir.

Çalışma kapsamında ele alınacak devletler seçilirken siber güvenlik alanında kendi iç ve dış politikaları olan, siber güvenliği devlet politikası olarak benimseyen, dünyaya çalışmaları ile öncü olan devletler seçilmiş olup tüm devletlerin siber güvenlik politikaları örnekleri ile karşılaştırmalı olarak ele alınacaktır.

Dünya üzerine siber alanda, yeni yıkıcı uygulamalar geliştirilmekte olup bunlar; İnternet'in cezaî kullanımı (siber suç) terörist amaçlar, sahte bilgilerin geniş

[90] SİNGER,P.W.;FRİEDMAN, Allan, "*Siber güvenlik ve siber savaş"*, (Çeviren: Ali Atav), Buzdağı Yayınevi, 1. Baskı, Mart 2015, s.76-77)

çapta yayılması, siyasi veya ekonomik amaçlar için casusluk ve sabotaj amacıyla kritik altyapıya (ulaşım, enerji, iletişim vb.) saldırılar şeklinde özetlenebilir.

Devlet veya devlet dışı gruplardan gelen bu siber saldırılar sınırları bilinmeyen, çoğu zaman botnet'lerin veya proxylerin ardında gerçekleştirilen, gerçek suçluları resmen tanımlamanın oldukça zor olduğu ve saldırgan için az maliyetle veya riskle göreli rahatlıkla uygulanabilir olan saldırılar olup vatandaşların, işletmelerin ve idarelerin kullandığı bilgi ve iletişim sistemlerinin (BİS) düzgün işleyişini ve hatta ulusal güvenlik için çok önemli olan alt yapının fiziksel bütünlüğünü tehlikeye atma amacıyla yapılmaktadır.

Siber güvenlik, bu tür saldırılara karşı savunma için alınabilecek tüm güvenlik önlemlerini kapsamakta olup son yıllarda siber saldırıların gelişmişliği ve şiddetinin gözle görülür biçimde artması sonucu gelişmiş ülkelerin esnekliğini sağlamasına ve ulusal siber güvenlik stratejilerini benimsemelerine neden olmuştur[91].

Milli güvenlik ve savunma kavramları Amerika Birleşik Devletlerinde yaşanan 11 Eylül saldırılarından sonra birçok ülkenin gündemine gelmiştir. Bu Yaşanan terör saldırıları uluslararası düzlemde sistemlerin güvenlik tanımları, tehditler ve ülkelerin gündemlerini tamamen değiştirmiş olup uluslararası düzlemde NATO üyelerinden birine karşı gerçekleşmesi mümkün olan "Dijital Felaket" (Dijital 11 Eylül) senaryosunun tartışılmasına sebep olmuştur.

Son yıllarda gerçekleşen siber saldırıların sonuçları gerçekleşmesi muhtemel saldırıların büyüklüğü ve yıkıcılığı konusunda bize fikir vermektedir. Örneğin bir virüs tarafından bireylerin hatta şirketlerin finans kayıtlarının yok edilebilmesi, bir virüsün tüm borsanın durmasına sebep olacak şekilde çalışamayacak hale getirmesi, hatalı bir mesaj veya dışarıdan bir müdahalenin nükleer tesisisin çalışmasını durdurması hatta uçakların, barajların kapaklarını açabilmesi, havaalanı trafik sisteminin karıştırılması sonucu uçak kazalarının

[91]Bkz.https://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/cyber-security/ adresinden erişilmiştir. (Erişim Tarihi: 03.03.2017)

yaşanması gibi hem fiziksel hem de ekonomik zararlara sebebiyet verebileceği hatta daha ileri boyuta ulaşarak can kayıplarına neden olabileceğini bize göstermektedir. Bu örnekleri çoğaltmak mümkündür.

Bugüne kadar yaşanmış olan Estonya[92], Gürcistan[93] ve Stuxnet[94]olayları siber saldırıların ciddiyetini ve ne boyutta zararlar verebileceğine dair iyi örneklerdir.

1999 yılında Sırp bilgisayar korsanları tarafından yapılan saldırılar sonrasında artarak büyüyen siber güvenlik meselesi sonucunda Estonya'ya karşı yapılmış olan siber saldırılar, NATO'nun siber güvenlik konusunda bakış açısının değişmesinde önemli bir rol oynamıştır.

Estonya'ya yapılan siber saldırılar ilk büyük çaplı siber saldırı olarak kabul edilmekte olup bunun sebebi uluslararası boyutta devletlerin savunma politikalarını gözden geçirmelerine sebep olmasıdır[95].

Yukarıda açıklandığı üzere devletler, giderek büyüyen ve gerçekleşmesi muhtemel bir siber saldırının yaratacağı fiziksel hasarın devletler tarafından milli güvenlikle ilişkilendirilmesi neticesinde siber tehdide karşı stratejiler oluşturmanın

---

[92] İkinci Dünya Savaşı sırasında Estonya tarafından dikilen "Bronz Asker Anıtı"'nın yerinden kaldırmasının sebebi ile Rusya kapsamında oluşan tepkinin devamında kaynağı belirsiz geniş çaplı siber saldırılar başlamış olup saldırıların hedefinde Estonya Başkanlığı ve Parlamentosu ile tüm ülkedeki devlet bakanlıkları, siyasi partiler, 3 büyük haber kuruluşu, iletişim firmasının yanı sıra Hansabank ve SEB gibi bankalar bulunmuştur. Saldırının yol açtığı hasar net olarak tespit edilememiştir. Bkz. http://www.tuicakademi.org/ilk-modern-siber-atak-estonya/ adresinden erişilmiştir. (Erişim Tarihi: 01.03.2017)

[93] Rusya tarafından 8 Ağustos 2008'de Gürcistan'a yapılan saldırılar neticesinde Gürcistan'a ait internet sitelerine hizmet engelleme saldırıları düzenlenmiştir. Fiziki saldırılar ile eş zamanlı düzenlenen saldırılar ile Gürcistan'ın resmî internet siteleri Rus bilgisayar korsanları tarafından çökertilmiş olup Gürcü yönetimine ait internet siteleri çökertilerek bu sitelerin içerikleri değiştirilmiş olup Rus saldırganlar resmî sitelerle sınırlı kalmamış olup medya organlarına da saldırılmıştır.Bkz.https://www.timeturk.com/tr/2013/01/17/siber-alemin-kanli-savaslari.html adresinden erişilmiştir. (Erişim Tarihi: 01.03.2017)

[94] Stuxnet isimli solucan cinsi zararlı yazılım Windows tabanlı işletim sistemleri üzerinde yayılan bir endüstriyel virüs olup kötü niyetli yazılımların karşılaşılan en gelişmiş örneğidir. Bkz.http://www.elektrikport.com/teknik-kutuphane/siber-savaslar-stuxnet/4383#ad-image-0 adresinden erişilmiştir. (Erişim Tarihi: 01.03.2017)

[95] Bkz. http://www.tuicakademi.org/ilk-modern-siber-atak-estonya/ (Erişim Tarihi 23.08.2018)

gerekliliğini farkedilmiş ve devletler bazında ulusal siber güvenlik stratejileri oluşturulmuş ve bu stratejiler ulusal güvenlik belgelerine eklenmiştir.

ABD Ulusal Araştırma Konseyi, siber saldırıyı bilgisayar sistemleri veya bu sistemlerden bulunan bilgi ve programların değiştirilmesi, bozulması, aldatılması, azaltılması, yok edilmesi yada bu programlar yada sistemlere erişilmesi olarak tanımlamış olup ABD politikasının yanında ise Şangay İşbirliği Örgütü tarafından siber saldırı araç olarak tanımlanmıştır. Şangay İşbirliği Örgütü tarafından siber saldırıyı bilgi ve iletişim teknolojileri vasıtasıyla barış ve düzenin bozulması olarak tanımlanmış; bilgi ve iletişim teknolojilerinin uluslararası tehdit oluşturduğu, bu tehditlerin sivil ve askeri alandaki mevcut barış ve düzenin bozulmasına sebebiyet vereceği ve bununla mücadele edilmesi gerektiği şeklinde ifade edilmiştir.

Teknolojinin her geçen gün daha da ilerlemesine bağlı olarak siber saldırıların meydana getirdiği zararlar ve oluşturduğu yıkıcı neticeler sebebiyle ülkeler uğramaları muhtemel olan zararlar karşısında siber alanda savunma yeteneklerini arttırmak ve saldırılara karşı önlem alarak ve savunma politikaları geliştirme mecburiyetinde kalmışlardır[96].

Siber güvenlik kavramı içerisinde operasyon güvenliği, bilgi güvenliği ve bilgisayar sistemlerinin güvenliği olan çok geniş bir kavramdır. Bu bağlamda hedef kitleler için farklı anlamlar taşımaktadır.

Kişiler açısından incelendiğinde siber güvenlik kavramı güvende hissetmek, kişisel verilerin ve gizliliğin korunması anlamına gelmektedir.

Kurumlar açısından bakıldığında ise siber güvenlik kavramı işle ilgili olarak kritik önem taşıyan işlevlerin kullanılabiliyor olması, operasyon ve bilgi güvenliği aracılığı ile gizli verilerin ve verilerin gizliliğinin korunmasını sağlamak anlamına gelmektedir.

---

[96]Bkz. Mehmet Yayla, (2014)"*Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı*", Hacettepe Hukuk Fakültesi Dergisi, 4.Cilt, 2.Sayı, sy.185 belgeye http://www.hukukdergi.hacettepe.edu.tr/C4S2tammetin.pdf adresinden erişilmiştir. (Erişim Tarihi: 01.03.2017)

Hükümetler ve devletler açısından ise vatandaşlarının, kurumlarının, kritik altyapılarının ve devlete ait bilgisayar sistemlerinin saldırılara veya verilerinin çalınmasına karşı korunabilmesi anlamını taşımaktadır.

Siber güvenlik kişiler, kurumlar ve hükümetlerin bilgi işlem hedeflerine güvenli, gizli ve güvenilir bir şekilde ulaşmalarına imkan tanıyan ortak etkinlikleri ve kaynakları ifade etmektedir[97].

Toplumların bilgi ve iletişim sistemlerinin gelişmesi ve günlük hayata dahil olmalarıyla birlikte bu sistemlerin ve içerisindeki verilerin güvenliği birçok hükümetin politika önceliği haline gelmiştir. Devletler ve hükümetler bilgi ve iletişim sistemlerinin güvenliklerinin sağlamak, kritik altyapıların korunması üzerine odaklanılması ile siber güvenlik stratejilerinin benimsenmesi üzerine politikalar üretmişlerdir.

Devletlerin suç işleyenleri adalet önüne çıkartarak cezalandırılmalarını sağlamak ve siber suçlara karşı bireyleri ve bireylerin haklarını korumak gibi bir pozitif yükümlülüğe sahiptir.

Güvenli bilgi ve iletişim teknolojilerinin faydalarını fark eden bazı hükümetler, bu gereksinimleri karşılamaya yönelik bir dizi tamamlayıcı plan ve program oluşturmaya başlamıştır.

Uluslararası Kritik Bilgi Altyapısını Koruma Kılavuzu'na göre, yirmiden fazla ülke kritik bilgi altyapısını koruma politikaları geliştirmiş durumdadır.

Birleşmiş Milletler Silahsızlanma Araştırmaları Enstitüsü (UNIDIR), otuz üç eyaletin askeri planlama ve organizasyonu içerisinde siber savaşı içerdiğinin tespit edildiğini savunmayla ilgili siber stratejiler geliştirdiğini bildirmektedir[98]. (LEWİS & TİMLİN, 2011)

---

[97]Bkz. http://sibertehdit.com/siber-guvenlik-nedir/ (erişim Tarihi: 09.05.2017)

[98]Bkz. LEWIS, James A.; TIMLIN, Katrina, (2011), "*Siber Güvenlik ve Siber Savaş, Ulusal Doktrin ve Organizasyon Yapısının Ön Değerlendirmesi, Cybersecurity and Cyberwarfare",* Birleşmiş Milletler Silahsızlanma Araştırmaları Enstitüsü (UNIDIR)", Center For Strategic and International Studies, s.3 Bkz. http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf adresinden erişilmiştir.

"NATO kendi ağına yönelik siber tehditlerin varlığını ilk olarak 2002 Prag Zirvesinde kabul etmiş ve bu çerçevede NATO Bilgisayar Olaylarına Müdahale Kapasitesini(NCIRC) oluşturmuştur. 2008 Bükreş Zirvesinde siber güvenlik alanında savunma politikasının genel çerçevesi oluşturulmuş, 2011 yılında kabul edilen politika belgesi siber güvenlik alanında daha etkili ve merkezi bir yapılanmanın oluşmasını sağlamıştır. Siber Güvenlik alanında bir dizi güven arttırıcı önlem (GAÖ) alınması amacıyla Güvenlik Komitesi adı altında gayri resmi bir çalışma grubu oluşturulmuş ve 2013 yılında Türkiye'nin de katılım sağladığı toplantılar sonucu ilk grup GAÖ'ler listesi tespit edilmiştir. Söz konusu liste sınırı aşan tehditlerle mücadele alanında AGİT'in Çabalarının Güçlendirilmesi başlıklı deklerasyonla 2013 Kiev Bakanlar Konseyi'nde kabul edilmiştir[99]." (EREN, 2017)

İktisadi İşbirliği ve Kalkınma Teşkilatı(OECD) da siber güvenliğini artırmakta olan ülkeleri izlemektedir ve kimlik yönetimine yönelik bir ulusal stratejisi olan veya bu tür bir strateji geliştirmeyi planlayan on sekiz ülkeden derlediği bulguların yer aldığı Uluslararası Kritik Bilgi Altyapı Korunmasına İlişkin (CIIP) Kılavuzu[100] isimli raporunda Devletlerin siber güvenlik stratejilerinin temelinde ;

• Kimlik ve Erişim;
• Yazılım ve Sistem Güvencesi – tedarik zinciri risk yönetimi de dahil;
• Uyumluluk ve İzleme;
• Veri Koruması;
• Dayanıklılık ve Risk Yönetimi;
• Yanıt Verme.

---

[99] Bkz."EREN, Mehmet , "*Avrupa Birliği'nin siber güvenlik politikası*", Beta Yayınları, 1. Baskı, Mart 2017, İstanbul, sy 2 orada dn.1 'den alınan Uluslararası Telekomünikasyon Birliği, 2015; Meral, 2015"

[100] Uluslararası CIIP Kılavuzu 2008/2009, Andreas Wenger, Victor Mauer ve Myriam Dunn Caveltry, Güvenlik Çalışmaları Merkezi, ETH Zurich
Bkz.http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf adresinden erişilmiş olıp çevirisi tarafımdan yapılmıştır.(Erişim Tarihi :04.08.2017)

Öğeleri mevcuttur.[101]

Birçok hükümet yeniliği artıran ve hizmet sağlama maliyetlerini azaltan bulut hizmetleri kullanmanın yollarını da aramakta ve bulut hizmetlerinin ulusal bir siber güvenlik stratejisiyle nasıl birleştirileceğini sormaktadır.

Hükümetlerin buluta ilişkin güvenlik ve özerklik endişeleri taşıması doğaldır. Devlet kurumları bu riskleri tanımlamak ve yönetmek için özel sektör ile birlikte çalışmaktadır; Bulut Güvenliği Birliği gibi çalışmalar, bulut bilgi işlem ortamı içinde güvenlik güvencesi ve diğer tüm bilgi işlem türlerinin güvenliğini sağlamak üzere bulut bilgi işlem ortamının kullanımına yönelik eğitim sağlamanın yolları üzerinde çalışmaktadır.[102]

Ayrıca İktisadi İşbirliği ve Kalkınma Teşkilatı(OECD) tarafından 17 Eylül 2015 – C(2015)115 tarih ve sayılı Dijital Güvenlik Risk Yönetimi OECD Tavsiye Metni ve Yardımcı El Kitabı yayınlamıştır.

Yayınlanan bu tavsiye metni ve yardımcı el kitabı ile devlet yönetimindeki ve kamu ile özel sektör yöneticilerine siber güvenlik risk yönetiminde ekonomik ve sosyal huzurun sağlanması için güven inşa edilmesi ve açık elektronik ortamdan faydalanılmasını amaçlayan bir yaklaşım benimsenmesi konusunda çağrı yapılmış, bu yaklaşım kapsamında sekiz temel ve üst düzey ilke öngörülmüştür.

Tavsiye Metninde belirlenen temel ilkeler şu şekildedir;

Farkındalık, beceri ve güçlendirme ilkesi kapsamında tüm paydaşlar tarafından siber güvenlik riskinin ve riskin nasıl yönetilebileceğini anlaşılması,

---

[101]Bkz.https://www.docdroid.net/6W0tztz/siber-guvenlikcyber-securtiy.doc#page=5 (Erişim Tarihi :04.08.2017)

[102] İktisadi İşbirliği ve Kalkınma Teşkilatı, OECD (2011), "OECD Ülkelerinde Dijital Kimlik Yönetimi İle İlgili Ulusal Stratejiler ve Politikalar", OECD Dijital Ekonomi Makaleleri, No. 177, OECD Yayınları, s. 4.

Sorumluluk ilkesi kapsamında tüm paydaşların siber güvenlik risk yönetiminde sorumluluk üstlenmesi,

İnsan hakları ve temel değerler ilkesi kapsamında tüm paydaşların siber güvenlik risk yönetimi konusunda şeffaf olarak insan hakları ve temel değerler kapsamında tutarlılık içinde bir platformda yürütülmesi,

İşbirliği ilkesi kapsamında tüm paydaşların sınır ötesindekilerde dahil olmak üzere diğer paydaşlar ile işbirliği içerisinde olması ve bu işbirliğinin devlet yönetimi, kamu ve özel sektör kurumlar bünyesinde olmasının yanında kurumlarla kurumlar arasında ve kurumlarla bireyler arasında olacak şekilde geniş kapsamda anlaşılması bölgesel ve sınır ötesi işbirliğinin yaygınlaştırılması,

Risk değerlendirmesi ve müdahale döngüsü ilkesi kapsamında liderlerin ve karar alıcı mekanizmaların siber güvenlik riski konusunda süreklilik arz eden risk değerlendirmeleri kapsamında ele alınmasının sağlanması ve bu risk müdahalelerinin farklı seçenek veya birleşimleri içermesini; bu kapsamda riskin kabul edilerek mevcut riskin azaltılması ve riskten kaçınılması olarak değerlendirilmesi,

Güvenlik önlemleri ilkesi kapsamında ise liderlerin ve karar alıcı mekanizmaların güvenlik önlemlerinde mevcut risk için önlemlerin uyguln ve orantılı olmasını sağlamalı, kurumların mevcut olabilecek olası zafiyetlerin acele olarak ortaya çıkartılarak müdahale edilmesinin sağlanması,

İnovasyon ilkesi kapsamında liderlerin ve karar alıcı mekanizmaların inovasyonun önemi ve önem verilmesini sağlaması gerekliliği,

Hazırlık ve süreklilik ilkesi kapsamında liderlerin ve karar alıcı mekanizmaların hazırlık planları ile devamlılığa ilişkin planların benimsenmesi ve uygulanmasını sağlama gerekliliği ile planların siber güvenlik vakalarının büyüklük ve ağırlıkları yanında siber ortamdaki başkaları üzerindeki etkileri de göz

önüne alan açık yükselme seviyeleri oluşturacak mekanizmalar üretme sağlama gerekliliği belirtilmiştir.

OECD Tavsiye Metninin uygulamaya konulması neticesinde siber uzay alanındaki risklerin değerlendirilmesi ve yönetiminin kapsamlı bir kamu politikası haline gelmesi için teşvik sağlanması ile yerel, bölgesel ve uluslararası düzeyde hem devlet yönetimi içerisinde hem de sivil toplum alanında paydaşlar ile birlikte yeni koordinasyon mekanizmalarının kurulmasının yanında, kamu ile özel sektör kurumlarının işbirliğinin güçlenmesi de beklenmektedir[103].

Dünyada daha çok gelişmiş ülkeler tarafından uygulanan mevcut siber güvenlik stratejileri genel olarak 5 temel alanda şekillenmektedir:

1.)Siber savunma, caydırıcılığı arttırıcı siber operasyon ve askeri istihbarat alt yapılarına sahip olması gereken askeri alan,

2.)Siber suçlarla mücadele alanı,

3.)İstihbarat faaliyetleri gerçekleştirmeyi ve siber casusluk operasyonlarından korunmayı sağlayacak istihbarat alanı,

4.) Siber güvenlik kriz yönetimi ve kritik alt yapıların korunmasını sağlayacak Computer Emergency Response Team (CERT) alanı,

5.) İnternet yönetimi ve siber diplomasi alanıdır.

2.1 Avrupa Birliği

Bilgisayar suçlarının Avrupa'da ilk olarak Avrupa Konseyi tarafından 1976 yılında Strasburg'da düzenlenen Ekonomik Suçların Kriminolojik Yönü Konulu konferans ile ele alınmıştır[104].

---

[103] Bkz. OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en" (Erişim Tarihi :06.08.2017)

[104]Bkz. BAYRAKTAR, Gökhan, "*Siber savaş*", Yeniyüzyıl Yayınevi, 1. Basım, 2015, sy.108-109

Avrupa Birliği tarafından yayınlanan direktifler ile öncelik olarak kişisel veriler ve bilişim suçları alanında temel düzenlemelere yer verilmiştir.

Avrupa Birliği tarafından 2013 yılında yayınlanan ve temel belge niteliği taşıyan strateji belgesi öncesinde yasal düzenlemeler bakımından önemli dönüm noktası taşıyan 23 Kasım 1995 tarihli Veri Korunması Direktifi, 31 Temmuz 2002 tarihli Elektronik Haberleşme Sektöründe Gizliliğin Korunması Direktifi, 24 Şubat 2005 tarihli Bilgi Sistemlerine Saldırılar Hakkında AB Konseyi Çerçeve Kararı ve 15 Mart 2006 tarihli Avrupa Verilerin Saklanması Direktifi yayınlanmıştır.

23 Kasım 1995 tarihli 95/46 sayılı Veri Korunması Direktifi ile kişisel verilerin işlenmesi sırasında kişi hak ve özgürlüklerinin korunması ve mahremiyetin sağlanması amaçlanmıştır[105]. Direktif kapsamında gerçek kişilerin kişisel verilerin işlenmesi ve AB üye ülkeleri arasında serbest dolaşımı için çerçeve kuralları belirlenmiştir. Tüzel kişilerin verileri hakkında ise verilere ilişkin esasların üye devletlerin insiyatifine bırakılması öngörülmüştür[106].

31 Temmuz 2002 tarihli Elektronik Haberleşme Sektöründe Gizliliğin Korunması Direktifi[107]ise 1995 tarihli 95/46 sayılı Veri Koruma Direktifine ek olarak çıkartılmış ve tüzel kişilerin verileri Direktif kapsamında alınarak elektronik haberleşme alanında temel hak ve özgürlüklere saygı gösterilmesi, özel yaşamın

---

[105] Kişisel verilerin işlenmesi ve bu tür verilerin serbest dolaşımına dair bireylerin korunması hakkındaki 95/46/EC sayı ve 24 Ekim 1995 tarihli AVRUPA BİRLİĞİ KONSEYİ VE AVRUPA PARLAMENTOSU DİREKTİFİ 23.11.1995 tarih ve L 281 sayılı Avrupa Birliği Resmi Gazetesi, sayfa.31-50 (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 p. 31-50.)

[106] Bkz. Eren, Mehmet, "Avrupa Birliği'nin Siber Güvenlik Politikası", Beta Yayınları, 1. Baskı, Mart 2017, İstanbul, sy.75 "

[107]Elektronik Haberleşme Sektöründe Gizliliğin Korunması hakkındaki 2002/58/EC sayı ve 12 Temmuz 2002 tarihli Avrupa Birliği Konseyi Ve Avrupa Parlamentosu Direktifi- 31.07.2002 tarih ve L 201 sayılı Avrupa birliği Resmi Gazetesi sayfa. 37-47 (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31/07/2002 p. 37- 47.)

gizliliğinin ve kişisel verilerin korunmasının sağlanması amaçlanmıştır. Bunun yanında ticari elektronik iletiler ve istenmeyen elektronik postalara(spam) yönelik düzenlemelerde direktifte yer almış olup bireylere önceden rıza alınmadan, istenmeyen elektronik posta gönderilmesi yasaklanmış, bu kapsamda doğrudan reklam içeren elektronik posta iletilerinde reklamı gönderenin adının saklanmaması ve göndericinin geçerli adresinin bulunması zorunluluğu getirilmiştir[108].

24 Şubat 2005 tarihli Bilgi Sistemlerine Saldırılar Hakkında AB Konseyi Çerçeve Kararı[109] oluşturulmuş bu karar ile bilgi ve iletişim sistemlerine yönelen siber saldırılar için ceza yargılamasının güçlendirilmesi amacıyla üye devletler arasında işbirliği hedeflenmiş ve 11. Madde uyarınca üye devletler arasında işbirliğinin sağlanabilmesi için 7/24 çalışacak operasyonel iletişim noktaları belirlenmesinin zorunlu olduğu belirtilmiş ve karar kapsamında bilgi sistemlerine yetkisiz kişiler tarafından yapılan erişimler ile sistemin engellenmesinin cezalandırılacak bilişim suçları olarak değerlendirildiği ve üye devletlerin bu bilişim suçları için etkili ve orantılı olarak caydırıcı nitelikte para cezası içeren yasal düzenleme yapmak üzere yükümlü kılınmışlardır[110].

15 Mart 2006 tarihli Avrupa Verilerin Saklanması Direktifi[111] ile de 2002 tarihli direktifte değişiklik yapılmış ve bu kapsamda üye ülkelerin iç hukuk düzenlemelerinde tanımladıkları telefon ve elektronik posta verileri, suçların

---

[108]Bkz. Eren, Mehmet , "Avrupa Birliği'nin Siber Güvenlik Politikası" ,Beta Yayınları, 1. Baskı, Mart 2017, İstanbul, sy.76

[109]Bkz. Bilgi Sistemlerine Saldırılar Hakkındaki 2005/222 sayılı 24 Şubat 2005 tarihli Avrupa Birliği Konseyi Çerçeve Kararı , Avrupa Birliği Resmi Gazetesi , sayfa. 67-71 (COUNCIL FRAMEWORK DECISION 2005/222/JHA of 24 February 2005 on Attacks Against Information Systems OJ L 69, 25/02/2005 p. 67-71.)

[110]Bkz. Eren, Mehmet , "Avrupa Birliği'nin Siber Güvenlik Politikası", Beta Yayınları, 1. Baskı, Mart 2017, İstanbul, sy.76

[111] Verilerin Saklanması hakkındaki 2006/24/EC sayı ve 15 Mart 2006 tarihli AVRUPA BİRLİĞİ KONSEYİ VE AVRUPA PARLAMENTOSU DİREKTİFİ- 13 Nisan 2006 tarih ve L 105 sayılı Avrupa birliği Resmi Gazetesi , sayfa. 54- 63 (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105 13.04.2006 p. 54-63)

soruşturulması ve tespiti ile kovuşturulması amacıyla bu verilerin saklanması ile ilgili konularında üye ülkelerin iç hukuk düzenlemeleri arasında uyum sağlanması amacı ile oluşturulan direktifte gerçek ve tüzel kişilere ait abone ve kayıtlı kullanıcıyı tanımlamak için gerekli yer ve trafik verileri hakkında uygulanmaktadır. Bu kapsamda bu direktif ile üye devlet internet servis sağlayıcılarına iletişim bilgilerinin iletişim tarihinden itibaren 6 aydan az 2 yıldan fazla olmamak üzere saklama yükümlülüğü getirilmiştir.

5 Haziran 2003 tarihinde Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı'nın (European Union Agency for Network and Information Security - ENISA) bir tüzel kişilik olarak kurulması kararı alınmış ve bu kararı takiple 14 Mart 2004 tarihinde ENISA'nın kuruluşu gerçekleştirilmiştir. ENISA- Avrupa Birliği Ağ ve Bilgi Güvenliği Kurumu, AB'nin siber güvenliğinin sağlanması konusunda koordinasyon sağlamak ve Avrupa genelinde üst düzeyde ağ ve bilgi güvenliğinin sağlanmasını amaçlamaktadır[112].

ENISA nın kuruluşundan günümüze kadar gelen süreçte kurum sürekli olarak gelişim göstermektedir. Bu kurum kritik bilgi altyapılarının güvenliği hususunda sertifikasyon hizmeti sunmakta olup üye ülkelerin ağ ve bilgi güvenliğini sağlamaları amacıyla danışma merkezi olarak görev yapmaktadır. AB'nin siber güvenliğini sağlama amacıyla önemli bir rol üstlenmiş olan ENISA üye ülkelerin ulaşım ve enerji gibi kritik altyapıları ile endüstriyel kontrol sistemleri hususunda ulusal siber direnç kapasiteleri geliştirmeleri için yönlendirmek amacı ile 2013 yılında AB için Endüstriyel Kontrol Sistemleri- Bilgisayar Güvenliği Olaylarına Müdahale Ekibi (ICS-CSIRTs)ni oluşturmuştur. Üye Devletleri ve AB Kurumlarını Siber olaylara karşı desteklemeye devam etmek suretiyle siber güvenliğin sağlanması için önemli bir aktör olarak karşımıza çıkmaktadır. Bu bağlamda

[112] Bkz. Eren, Mehmet, "Avrupa Birliği'nin Siber Güvenlik Politikası", Beta Yayınları, 1. Baskı, Mart 2017, İstanbul, sy.73 -77 "

ENISA tarafından kamu özel ortaklığı geliştirilip uzman kişilerce fikir üretilmesi amacıyla toplantılarda düzenlemektedir[113].

Avrupa Birliğinin halihazırda ki siber güvenlik stratejileri kapsamında Avrupa Komisyonu tarafından 2010 yılında Dijital Gündem uygulamaya konulmuştur.

Avrupa Komisyonu Avrupa vatandaşlarını ve işletmelerini giderek artan bu siber tehditlere karşı korumaya yardımcı olmak için Avrupa Siber Suç Merkezi'nin kurulması planlanmıştır.

Bu plan doğrultusunda 27 AB ülkesi siber suçlara karşı aktif bir mücadele ortaya konulması için güçlerini birleştirmiş ve Lahey merkezlik olarak Avrupa Polis Teşkilatı EUROPOL bünyesinde hizmet verecek olan Siber Suçlarla Mücadele Merkezi 11 Ocak 2013 faaliyetine başlamıştır.

Avrupa birliği tarafından ağ ve bilgi güvenliği kurumu ENİSA'nın yetkileri arttırılmış, AB bünyesinde gerçekleştirilen ilerlemelerin yanında ulus devletlerin politikalarını da kapsayacak yasal düzenlemelerin ortaya çıkmasıyla Ulusal otoriterleri de kapsayacak şekilde ortak paydada buluşulmuş 2012 yılında Ağ ve Bilgi Güvenliği (NIS) politikası için merkezi Brüksel de bulunan ve AB'nin kurumlarıyla uyumlu çalışan merkezi AB'nin ilk bilgisayar acil müdahale timi(CERT) kurulmuş, bu timin başlıca görevi AB ve üye ülkelerde ortaya çıkabilecek olan muhtemel kriz anlarında krize acil müdahale edilip gerekli önlemlerin alınarak etkili bir Ağ ve Bilgi Güvenliği (NIS) politikası yürütülmesidir[114].

Avrupa Birliğinin siber güvenlik politikasını oluşturan en temel doküman Avrupa Komisyonunun 7 Şubat 2013 tarihli Avrupa Birliği için Siber Güvenlik Stratejisi isimli belgedir.

---

[113] Bkz.Eren, Mehmet, "Avrupa Birliği'nin Siber Güvenlik Politikası", Beta Yayınları, 1. Baskı, Mart 2017, İstanbul, sy.73 oradan dn.35"

[114] Bkz.Eren, Mehmet, "Avrupa Birliği'nin Siber Güvenlik Politikası", Beta Yayınları, 1. Baskı, Mart 2017, İstanbul, sy.78

Bu strateji belgesi kapsamında günlük yaşamımızın, temel haklarımızın, sosyal etkileşimlerimiz ve ekonomilerin bilgi ve iletişim teknolojilerine olan bağlılığı belirtilmiş, açık ve özgür bir siber alanın dünya çapında politik ve sosyal kaynaşmayı desteklediğini, ülkeler, toplulukla ve vatandaşlar arasındaki sınırları küresel çapta bir etkileşim ve bilgi paylaşımına ve etkileşime izin vererek yıktığını, Özellikle Arap baharı boyunca ifade özgürlüğü ve temel hakların uygulanması ve demokratik ve daha adil bir toplum konusunda insanları cesaretlendiren bir alan sağladığını belirtmiştir.

Strateji Belgesinde; geçmiş yıllarda dijital dünyanın inanılmaz faydalar getirmesinin yanında aynı zamanda ne kadar savunması olduğunu da gösterdiği, siber güvenlik olaylarının kasıtlı veya kazayla da olsa endişe verici bir tempoda arttığını, su, sağlık, elektrik ve mobil servisler gibi kritik altyapı hizmetlerini tedarik edilmesini tehdit ettiğine ve tehditlerin; suç içeren, siyasi amaçlı, terörist veya devlet destekli tehditler olabileceği gibi doğal afetler ve kasıtsız hatalardan da kaynaklı olmak üzere farklı kökenlere sahip olabileceğine ifade edilmiştir[115].

AB tarafından siber uzayın açık ve özgür bir alan olduğu, Siber uzayda korunması gereken temel ilkelerin; temel hakları, demokrasi ve hukukun üstünlüğü ilkeleri olduğu, özgürlüğün ve refah seviyelerinin her gün daha da sağlam ve yeniliğe açık bir internete bağlı hale geldiği, özgürlüğün güvenliği gerektirdiği ve siber uzayın kötü niyetli faaliyetlerden ve yanlış kullanımlara karşı korunması gerektiğinin, bu alanda hükümetlere ve özel sektörlere önemli rol düştüğünün, hükümetlerin erişim ve açıklığı korumak, temel haklara saygıyı, internetin güvenilirliğini ve birlikte işbirliğini korumak için çeşitli görevlerinin olduğunu belirtilmiştir[116].

---

[115] Bkz. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace , Brussels, 7.2.2013, sy.2-3 , Belge aslına https://ec.europa.eu/digital-single-market/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security adresinden erişilmiştir. (Erişim Tarihi : 10.09.2017)

[116] Bkz. Eren, Mehmet, "Avrupa Birliği'nin Siber Güvenlik Politikası", Beta Yayınları, 1. Baskı, Mart 2017, İstanbul, sy.81

AB'nin siber güvenlik stratejisinin temel hedefleri siber dayanıklılığın artırılması ve siber suçları etkili şekilde düşürmek olup strateji belgesi, siber güvenlik politikalarının üç önemli temeli bulunmaktadır. Bunlar güvenlik, dış politika ve ekonomidir.

Siber Güvenlik Strateji Belgesinde AB siber güvenlik politikalarında siber güvenliğin ilkelerini "AB'nin temel Değerleri", "Temel hakların , düşünce özgürlüğünün, kişisel bilgilerin ve gizliliğin korunması", "herkes için erişim", "demokratik ve etkili çok paydaşlı yönetişim" ve "güvenliği sağlamak için paylaşılmış sorumluluk" olarak beş ilke olacak şeklinde belirlenmiştir. Ayrıca bu kapsamda günlük hayatta geçerli yasaların , teamüllerin ve normların siber uzayda da aynı şekilde geçerli olduğu belirtilmiştir[117].

"Siber Güvenlik Stratejisi Belgesinde ile üye devletlere Siber Olaylara Müdahale Ekipleri kurma konusunu zorunlu hale getirilmiş olup aynı zamanda 'bilgi paylaşımı' konusunda özel sektöre önemli yükümlülükler getirilmiştir. Bunların başında özel sektör şirketlerinin karşılaştığı ciddi siber olayları ulusal kurumlara ve Avrupa Ağ ve Bilgi Güvenliği Ajansı'na bildirmeyi zorunluluğu getirilmiştir[118]."

Avrupa Konseyi Siber Suçlar Sözleşmesi (Convention on Cybercrimes) 01 Temmuz 2004 tarihinde imzalanarak toplam 43 ülke ile imzalanarak yürürlüğe girmiştir. Avrupa Konseyi Siber Suçlar Sözleşmesi kapsamında üye devletlerin siber güvelik Stratejilerinin aşağıdaki gibi olması gerektiği ve üye devletlerin iç düzenlemelerin bu yönde olması gerekliliği hüküm altına alınmıştır.

Türkiye yaptığı iç hukuka ilişkin düzenlemeler neticesinde sözleşmeye taraf olmuştur. Dışişleri Bakanlığı tarafından hazırlanan 12/08/2012 tarihli "Sanal

---

[117]Bkz. Eren, Mehmet, "Avrupa Birliği'nin Siber Güvenlik Politikası", Beta Yayınları, 1. Baskı, Mart 2017, İstanbul, sy.84

[118]Bkz.https://siberbulten.com/tag/avrupa-birligi-siber-guvenlik-stratejisi/ (Erişim Tarihi: 09.11.2017)

Ortamdaki İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı" 22 Nisan 2014 tarih ve 6533 sayılı Kanun ile onaylanmış ve 02 Mayıs 2014 tarihinde Resmi Gazete'de yayınlanmak suretiyle yürürlüğe girmiştir.

23 Kasım 2001 tarihli Siber Suçlar Sözleşmesi siber uzaydaki özgürlükler ile insan hakları ve siber uzayın güvenliğinin korunması bu surette mevcut risklerin azaltılmasına ilişkin olarak uluslararası boyutta kabul edilmiş tek rehber niteliği taşıdığından ayrıca önem arz etmektedir. Bu sözleşme devletlerin kendi vatandaşlarını korumasına hizmet eden önemli bir araç niteliği taşımaktadır.

Sözleşme, bilgi güvenliği ve siber güvenliğinin temel ilkeleri olan gizlilik, bütünlük ve erişilebilirliğe yönelik olarak yapılan saldırılar ile bilgi iletim vasıtasıyla işlenen suçları kapsamaktadır.

Bu sözleşme internet ve diğer bilgisayar ağları üzerinden işlenen suçlara bakımından ilk uluslararası anlaşma olma özelliğine sahip olmakla Sözleşme ile siber suçlarla ilgili ulusal düzeydeki yasal düzenlemeler ve bağlantılı hükümlerin uyumlu hale getirilmesi, siber suçların ve ilaveten bilgisayar yardımıyla işlenen diğer suçlar ve elektronik delil içeren klasik suçların soruşturma ve kovuşturulması ile ilgili ulusal usul hukuku yetkilerini sağlamak, Uluslararası işbirliği alanında hızlı ve etkin bir rejim oluşturmak olmak üzere Sözleşmenin üç temel amacı bulunmaktadır.

Ayrıca Avrupa Birliği ve Avrupa Konseyi'nin Katılım Öncesi Mali Altyapısı altında siber suçlarla işbirliğine ilişkin ortak bir bölgesel projesi olan Arnavutluk, Bosna-Hersek, Hırvatistan, Karadağ, Sırbistan, "eski Yugoslav Makedonya Cumhuriyeti", Türkiye ve Kosova'nın yararlanıcı olarak yer aldığı "Cybercrime@IPA Güney Doğu Avrupa'da Siber Suçlara Karşı Bölgesel İşbirliği" başlıklı proje[119] kapsamında "Siber Suçlara Karşı İşbirliğinde Stratejik Öncelikler Deklerasyonu" "CyberCrime@IPA" projesine katılan ülke ve yerlerin İçişleri, Güvenlik, Adalet ve Savcılık Hizmetleri Bakanları ve Üst Düzey Bürokratları

[119]Bkz. http://www.coe.int/en/web/cybercrime/cybercrime-ipa (Erişim Tarihi: 09.05.2017)

Toplantısında 2013 yılında yararlanıcı ülkeler tarafından imzalanmış olup, bu deklerasyonda;

- Siber suç politikaları yada stratejilerinin benimsenmesi konusunda bilgisayarlara karşı ve bilgisayarlar vasıtasıyla işlenebilen suçların yanı sıra elektronik delil içerikli her türlü suça ilişkin olarak etkili bir ceza adalet müdahalesi sağlanması ve siber suç politikaları ile stratejilerinin benimsenmesi,
- Siber suç politikaları ile stratejilerinin temel unsurları olarak önleyici tedbirlerin alınması, mevzuatsal düzenlemelerin yapılması, özel kolluk birimlerinin ve özel savcılık hizmetlerinin sağlanması, kurumlar arasındaki işbirliğinin, kolluk ve adli personelin eğitiminin, kamu ve özel sektörün işbirliğinin sağlanması, etkili uluslararası düzeyde devletlerin işbirliğinin sağlanması, kara para aklama ve dolandırıcılığın önlenmesinin sağlanması amacıyla mali soruşturma yapılması ile cinsel şiddete karşı çocukların korunmasının sağlanması,
- Siber suçlara karşı olarak gerekli önlemler alınırken, insan haklarının ve hukukun üstünlüğü ilkesinin gereksinimlerinin sağlandığından emin olunması,
- Siber suçlar ile ilgili raporlanma yapılması için kamu düzeyinde gerekli online platform ve alanların oluşturulması,
- Siber suç tehditleri ile ilgili ve tehdit eğilimlerinin daha iyi anlaşılmasının sağlanarak ceza adalet faaliyetlerinin kolaylaştırılmasının sağlanması,
- Farkındalık oluşturulması ve her seviyede gereken önleyici tedbirlerin alınabilmesi için teşvik edilmesi,
- Kolluk kuvvetleri ile internet servis sağlayıcıları arasında olacak şekilde kamu ve özel sektör işbirliği hususunda gerekli girişimlerde bulunulması,
- Mümkün olduğu en geniş kapsamda uluslararası düzeyde işbirliği gerçekleştirilmesi için gerekli girişimlerde bulunulması,
- Düzenli aralıklarla siber suçlar açısından bu suçlara karşı olarak yapılan ceza adaletinin etkin olması için gerekli değerlendirmenin yapılarak istatistiki bilginin sağlanması

İlkeleri belirlenmiş olup bu yapılacak istatistiki analizlerin ceza adalet faaliyetlerinin performansını arttırarak iyileştirilmesi amacıyla sahip olunan

kaynakların verimli olacak şekilde belirlenmesi ve tahsisine ilişkin yardımcı bir rol oynayacağı belirtilmiştir[120].

Son olarak Avrupa birliği Siber Güvenlik Yasası[121] hazırlanmış ve 11 Mart 2019 tarihinde AB Parlamentosu'nda onaylanmıştır.

Siber saldırılara karşı önlem almak ve AB'de güçlü bir siber güvenlik oluşturmak için geniş kapsamlı olarak alınacak bir dizi önlem kapsamında önerilmiş olan Yasa içeriği incelendiğinde; ENISA'nın sınırlı olan yetkisi 2020 yılında sonra ereceğinden bu sınırlı yetkinin yerine geçmesi amacı ile kalıcı bir görev verilmesi ve hedeflerine ulaşabilmesi için ENISA'ya daha fazla kaynak tahsis edilmesi amaçlanmaktadır. Ayrıca üye devletlerin siber saldırılarına daha etkin bir şekilde yanıt vermelerine yardımcı olmak amacıyla yeni siber güvenlik sertifikasyonu kapsamında Birlik ile işbirliği ve koordinasyonun sağlanması hedeflenmiştir.

ENISA AB seviyesindeki siber güvenlik imkanlarının arttırılmasına ve kapasite geliştirme ve hazırlığın desteklenmesine yardımcı olacaktır. Ayrıca ENISA, vatandaş ve işletmelerin yüksek düzeyde bilinçlendirilmesi ve AB Kurumlarına ve üye ülkelere politika geliştirme ve uygulama konusunda yardımcı olan bağımsız bir merkez olması planlanmaktadır.

Yasa ayrıca AB genelinde geçerli olacak ürün, işlem ve hizmetlere ilişkin olarak Avrupa Siber Güvenlik Sertifikaları için de bir çerçeve belirlemektedir[122].

Yasa kapsamında ulaşılması hedeflenen amaçlar şu şekilde belirlenmiştir.

-Üye Devletlerin ve işletmelerin yeteneklerinin ve hazırlıklarının arttırılması;

---

[120] Bkz.Avrupa Birliği(AB)/Avrupa Konseyi(AK) Siber Suçlara karşı bölgesel işbirliği ortak projesi "Siber Suçlara Karşı İşbirliğinde Stratejik Öncelikler Deklerasyonu" "CyberCrime@IPA projesine katılan ülke ve yerlerin İçişleri, Güvenlik, Adalet ve Savcılık Hizmetleri Bakanları ve Üst Düzey Bürokratları Toplantısı , Dubrovnik, Hırvatistan, 15 Şubat 2013, https://rm.coe.int/16802f6a42" (Erişim Tarihi :13.05.2017)

[121]Bkz.http://afyonluoglu.org/PublicWebFiles/strategies/Europe/EU%202017%20Cyber%20Security%20Act.PDF

[122]Bkz. https://www2.deloitte.com/tr/tr/pages/risk/topics/cyber-risk/articles/avrupa-birligi-siber-guvenlik-kanunu.html

-Üye Devletler ve AB kurumları, kurumları ve organları arasındaki işbirliğini ve koordinasyonu geliştirmek;
-Üye devletlerin, özellikle de sınır ötesi siber krizler durumunda, eylemlerini tamamlamak için AB düzeyinde kabiliyetlerin arttırılması;
-Vatandaşların ve işletmelerin siber güvenlik konularında farkındalığının arttırılması;
- Dijital tek pazarda ve dijital inovasyonda güveni güçlendirmek için BİT ürün ve hizmetlerinin siber güvenlik güvencesinin genel şeffaflığının arttırılması
- AB'de belgelendirme planlarının ve ilgili güvenlik gereklilikleri ile üye devletler ve sektörler arasındaki değerlendirme kriterlerinin parçalanmasından kaçınılması.

Avrupa Birliği, dayanıklılığı arttırmak ve siber güvenlik hazırlıklarını artırmak için bir dizi eylemde bulunmuştur. 2013 yılında kabul edilen ilk AB Siber Güvenlik Stratejisi, esnekliği sağlamak, siber suçu azaltmak, siber güvenlik politikası ve yetenekleri geliştirmek, endüstriyel ve teknolojik kaynaklar geliştirmek ve AB için tutarlı bir uluslararası siber politika oluşturmak için stratejik hedefler ve somut eylemler belirlemiştir. Bu bağlamda, o zamandan bu yana, özellikle Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA) ve ağ ve bilgi sistemleri güvenliği ile ilgili Direktifin kabul edilmesi ('NIS Direktifi' dahil olmak üzere) önemli gelişmeler yaşanmıştır.

Ayrıca, 2016' da Avrupa Komisyonu, Avrupa'nın Siber Esneklik Sisteminin Güçlendirilmesi ve Rekabetçi ve Yenilikçi Bir Siber Güvenlik Endüstrisinin Geliştirilmesi Konusunda Bir Tebliği kabul etmiştir.

Değerlendirme süreci, Ajansın olası bir reformuna ve Üye Ülkeleri sürdürülebilir bir şekilde destekleme kapasitesinin ve kapasitesinin geliştirilmesine yol açabilir. Bu nedenle, siber güvenlik direncini sağlamada kendisine daha operasyonel ve merkezi bir rol verecek ve Ajans'ın NIS Direktifi kapsamında yeni sorumluluklarını yerine getireceğini kabul edecektir.

NIS Direktifi, temel ekonomik aktörler için güvenlik gereklilikleri, özellikle temel hizmetler sağlayan operatörler (Temel Hizmetler Operatörleri - OES) ve bazı anahtarların tedarikçileri için yasal zorunluluklar olarak getirerek, risk yönetimi kültürünün desteklenmesi amacıyla atılmış ilk adımdır. Dijital

servisler (Dijital Servis Sağlayıcılar - DSP'ler). 2016 İletişimi, toplumun gelişen dijitalleşmesinin faydalarını korumak için gerekli olduğu ve bağlı cihazların (Nesnelerin İnterneti - IoT) hızlı bir şekilde çoğaltılması göz önüne alındığında, gerekli olduğu için, Güvenlik sertifikası için bir çerçeve oluşturma fikrini ileri sürmüştür. Dijital tek pazarda güven ve güvenliği artırmak için BİT ürünleri ve hizmetleri için. BİT siber güvenlik sertifikası, bağlı ve otomatik araçlar, elektronik sağlık veya endüstriyel otomasyon kontrol sistemleri (IACS) gibi yüksek düzeyde siber güvenlik gerektiren teknolojilerin kullanımının artması nedeniyle özellikle önem kazanmaktadır[123].

Yukarıdaki açıklamalar ışığında Avrupa Birliğinin hukuki düzenlemeleri kapsamında Siber Güvenlik Politikası açıklanmaya çalışılmıştır.

2.2.Amerika Birleşik Devletleri

Amerika Birleşik Devletleri internetin ve bilgisayar teknolojilerinin doğum yeri olmakla birlikte devletler bazında incelendiğinde en geniş kapsamında hukuksal düzenlemeler ve stratejinin Amerika Birleşik Devletleri tarafından uygulandığı görülecektir.

ABD'nin "Bilişim" ile ilgili ilk hukuksal düzenlemesine baktığımızda bilişim bağlantılı suçlara ilişkin 1984 tarihli ilk federal kanun "Bilgisayar Sahtekarlığı ve Bilgisayarların Kötüye Kullanılması Kanunu (Counterfeit Access Device and Computer Fraud and Abuse Act)" dur. Bu kanunla 3 temel kategoride suç öngörülmüştür.

Buna Göre;

- Birleşik Devletlere zarar verme maksadıyla bir bilgisayarda gizli bilgilerin olduğunu bilerek veya gizli bilgilerin o bilgisayarda olduğu saikiyle yetkisiz olarak

[123]Bkz.http://afyonluoglu.org/PublicWebFiles/strategies/Europe/EU%202017%20Cyber%20Security%20Act.PDF (Erişim Tarihi: 23.01.2019)

veya halihazırda var olan yetkinin sınırlarını aşmak suretiyle bir bilgisayara bilerek erişim sağlamak,

- Finansal veya kredi kayıtlarını finansal kurumlardan almak maksadıyla yetkisiz olarak veya halihazırda var olan yetkinin sınırlarını aşmak suretiyle bir bilgisayara bilerek erişim sağlamak
- Bilerek ve isteyerek Birleşik Devletler tarafında veya onun adına kullanılan bir bilgisayara hükümetin bu bilgisayara erişimini ihlal edecek şekilde erişim sağlamak Temel suçlar olarak tanımlanmıştır.[124]

1986 yılında "Computer Fraud and Abuse Act" olarak adlandırılan değişiklikle mevcut üç adet suça üç yeni suç daha eklenmiştir.

Bunların dışındaki Kanunlar;

- 1986 tarihli "Elektronik Haberleşme Gizlilik Yasası (Electronic Communications privacy Act)" ,
- 1997 tarihli "İnternette Kumarın önlenmesi Yasası(Internet Gambling Prohibiton Act)",
- 1998 tarihli "Çocukların Çevrimiçi Yayınlardan Korunması Yasası (Child Online Prevention Act)" ,
- 2001 tarihli "Anti Terörizm Yasası(USA- Patriot Anti- terrorism Act)" dir.

ABD Savunma Bakanlığı ve istihbarat organizasyonları arasında 1994 yılı içerisinde "Ortak Güvenlik Komisyonu" kurulmuş olup ağ teknolojilerinin yaygınlaşmasının riskleri değerlendirilmiştir.

Buna göre Ortak Güvenlik Komisyonu tarafından oluşturulan nihai raporda;.

---

[124]Bkz. Greg Pollaro, "Isloyal Computer Use And The Computer Fraud And Abuse Act: Narrowıng The Scope" , Duke Law & Technology Revıew, No:012, (2010), sy.2-3 (https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=https://www.google.com.tr/&httpsredir=1&article=1207&context=dltr, adresinden erişilmiş olup çeviri tarafımdan yapılmıştır. (Erişim Tarihi: 08.09.2017)

- Bilişim sistemlerinin sahip olduğu teknolojinin sistem güvenliğini temel alan bilişim sistemlerinin güvenliği teknolojisinden çok daha hızlı olarak ilerleme gösterdiği,
- Bilgi ve iletişim sistemleri olan bilişim bilişim sistemleri ve ağların güvenliğinin son on yılın en büyük güvenlik sorunsalı olduğu ve bu alanda karşılaşılması muhtemel risklerle ilgili olarak gerekli bilince sahip olunmadığı,
- Pentagon'un yanı sıra özel sektörde gelişen bilişim sistemleri bağımlılığının ülkenin bütünü açısından zayıflığını arttırdığı,

Şeklinde üç ana konsept dikkat çekmektedir. Bu hususlar günümüzde daha da önem kazanmış ve doğrulukları ortaya çıkmıştır.

Bunun üzerine 1995 yılında dönemin Başkanı Bill Clinton tarafından Kritik Altyapı Koruma Başkanlık Komisyonu (Marsh Komisyonu) adında bir çalışma grubu oluşturulmuş olup bu çalışma grubu ABD nin her yerinde yaptığı detaylı çalışmaların sonunda 1997 yılında açıkladığı sonuçlara göre "ABD'ye yönelik en büyük tehdit El Kaide gibi terörist örgütlerin yapacağı saldırılardan çok siber korsanlardan geliyordu." Komisyon " keşfedilen bu riskte bankacılık , elektrik üretimi ve üretim gibi önemli konuların internet kontrolünde olduğu, İnternet ağının ise en ufak bir güvenlik unsuru taşımadığını" belirtmiştir.

Komisyonun tespitleri neticesinde Altyapı Koruma ve Kontra terörizm Ulusal Koordinatörlüğü kurulmuş olup, koordinatörlük tarafından yapılan çalışmalar neticesinde özel sektör ve devlet kuruluşlarında incelemeler yapılmış, 2000 yılında tüm bilgisayarların sıfırlanması sorunu üzerine yapılan incelemeler bilişime ne kadar bağımlı olunduğunu daha net ortaya çıkarmıştır[125].

ABD'de bulunan Ulusal Savunma Üniversitesi tarafından 1995 yılında ilk "siber savaşçı" isimli mezunlar verilmiştir. O tarihlerde siber savaşın, psikolojik

[125]Bkz. Clarke, Richard A.; Knake, Robert K., Siber Savaş, (Çeviren: Murat Erduran), İkü Yayın Evi, Nisan 2011, s.59-59

savaş yani propaganda kullanılarak yapılan savaşın sonucunu etkileme çabası olduğu inanılmaktaydı[126].

1998 yılında Irak Savaşı için ABD silahlı kuvvetlerinin yığınak yaptığı sırada Savunma Bakanlığı bilgisayarlarına hacker'ların sızdığı keşfedilmiştir. FBI yaptığı soruşturma neticesinde siber saldırıyı gerçekleştiren korsanların Iraklı değil İsrailli bir çocuk ve Kaliforniyadan iki çocuğun askeri ağların ne kadar savunmasız olduğunu ispatlamak için oyun oynadıkları ortaya çıkmıştır.

Yine 1999 yılında Hava Kuvvetlerinin bir hava üssünden büyük miktarda veri çalınmıştır. FBI ve NSA in yardıma gelmesine rağmen savunma ağlarından ve Enerji Bakanlığının nükleer laboratuvarlarından yapılan bilgi hırsızlığı durdurulamamıştır.

2000 yılında AOL, Amazon, Yahoo, E-Trade gibi ticari internet siteleri çökmeye başlamıştır. Bu o zamana kadar yapılmış en büyük hackleme eylemi olmakla saldırganın Montreal'den bir komi olduğu ortaya çıkmıştır.

2001 yılında Kod Red isimli solucan virüsü 300,000 bilgisayarı ele geçirmiş ve hepsini zombi bilgisayarlara çevirerek Beyaz Saray'ın web sayfasına saldırtmıştır.

11 Eylül saldırıları sonrasında NIMDA isimli solucan finans sektörüne saldırmıştır. En süt düzey güvenlik imkanlarına sahip olmasına rağmen bankaların ve Wall Street Borsasının önde gelen menkul kıymetler şirketlerinin bilgisayar sistemleri be bilişim ağları çökmüştür.

Tüm bu saldırıların neticesinde güvenlik zafiyetinin ne kadar büyük olduğu ve sonuçlarının ne denli sarsıcı olabileceği bir kez daha ortaya çıkmıştır.

Yukarıda anlatılan gelişmelerin de ışığında 11 Eylül saldırıları sonrasında ABD de gelişen güvenlik ortamın neticesinde aynı hızlı gelişmeler siber güvenlik alanında da kendini göstermiştir. ABD tarafından internet güvenlik politika ve stratejilerinin yeniden programlanması için İç Güvenlik Bakanlığı (DHS-

---

[126] Bkz. Clarke, Richard A.; Knake, Robert K., Siber Savaş, (Çeviren: Murat Erduran), İkü Yayın Evi, Nisan 2011, s.28

Department of Homeland Security) tarafından siber alanda internetin güvenliğinin sağlanabilmesi için tüm sorumluluk üzerine alınmıştır.

2000 yılının başında, Federal Hükümet ağları, kayda değer sayıda siber ihlaller yaşamaya başlaması üzerine Kongre federal örgütler arasında eşgüdüm ve bilgi paylaşımı merkezi bir merkez olarak Genel Hizmetler İdaresi'nde Federal Bilgisayar Olay Yanıt Merkezi (FedCIRC) ortaya çıkmıştır.

2002'de Vatan Güvenliği Departmanı'nın kurulmasıyla bu sorumluluklar yeni Daire'ye devredilmiş olup 2003 yılında FedCIRC "US-CERT" olarak yeniden adlandırılmış ve misyonu, federal sivil yürütme alanı ve siber güvenlik liderliği için sınır koruma sağlanması dahil olmak üzere genişletilmiştir. Bu paylaşılan sorumluluk, zamanla ABD-CERT'yi Federal Hükümet; SLTT(State, Local, Tribal, and Territorial Governments) hükümetleri; özel sanayi; ve uluslararası kuruluşları için siber alanda güvenilir bir ortak ve güvenilir kaynak yapmak için gelişmeye devam etmektedir.[127]

2008 yılında ABD tarafından mevcut siber güvenlik stratejisi yenilenmiş ve "Kapsamlı Ulusal Siber Güvenlik Girişimi" (Comprehensive National Cybersecurity Initiative, CNCI) isimli yeni bir direktif hazırlanmıştır. Bu direktif dönemin başkanı Başkan Bush tarafından imzalanmış olup bu direktif ile ABD'nin siber güvenlik stratejisinde büyük çaplı değişiklikler öngörmüştür.

Bu değişiklikler incelendiğinde öncelikle, Yönetim ve Bütçe Ofisi (Office of Management and Budget) tarafından İç Güvenlik Bakanlığından federal kuruluş ve dış sağlayıcılar arasında mevcut 4000 ağ bağlantısının 4 ay içinde 50 ağ bağlantısına düşürtülmesi talep edilmiş, devamında ise tercihe bağlı bir İç Güvenlik Programı olan ve federal internet siteleri ile normal internet siteleri arasındaki internet trafiğini gözleyen EINSTEIN adlı programın gözlem yetkisinin Ulusal Güvenlik Birimi'ne (National Security Agency) aktarılması ve programın son sürümünde trafikle birlikte içeriğinde yakalanarak takip edilmesi ve federal ağlar yanında özel ağlarında izlenebilmesi özellikleri mevcuttur. Ve son olarak ise bu

[127]Bkz. https://www.us-cert.gov/about-us , (Erişim Tarihi: 08.09.2017)

direktifin içerdiği konular hakkında yatırım ve çalışmaların arttırılması ile siber alanda karşı istihbarat için yapılacak çalışmaların koordine edilerek devlet kurumları arasına bilgi paylaşımı hususunun teşviki ile açıklamaları içerdiği görülmektedir.

Başkan Obama zamanında halihazırda mevcut olan Kapsamlı Ulusal Siber Güvenlik Girişimi planı uygulanmış olup bu planın yanında Beyaz Saray tarafından yapılan çalışmalar neticesinde ABD'nin siber güvenlik stratejisi revize edilmiş ve bu değişiklikler üzerine oluşturulan raporda Beyaz Saray içinde Siber Güvenlik Ofisi kurulması, Bu yapılanmaya lider olarak bir Siber Çar görevlendirilmesi, Çar'ın Ulusal Güvenlik Konseyi'ne üye olması ve Çar'ın Başkan'a hızlıca ve kolayca erişim ayrıcalığı sahibi olması gerektiği, Çar'ın yetkileri arasında bu ofisin kendi başına strateji belirleme yetkisi olmamasına karşın kurumun federal departmanların çalışmalarını yönetmesi ve ortak bir strateji belirlenmesi tavsiyeleri vermesi bu tavsiyeleri ile federal hükümet içindeki tüm siber güvenlikle ilgili faaliyetler hakkında yetki ile rollerin ve sorumlulukların belirlenmesine yardım etmesi bu surette iletişim ve strateji açığı için bir köprü görevi görmesi talep edilmiştir. Bu rapor ile daha önceden yaşanmış olan siber olaylarda taraflar arasında orta olarak verilmiş bir federal tepki olmadığının fark edildiği bu kuruluşlar arasındaki ortak sorumluluğun ortadan kaldırılarak hükümet ağının içinde siber güvenlik ve savunmayla ilgili özellikli rollerin ve kurumların sorumluluklarının belirlenmesi gerektiği vurgulanmıştır[128].

ABD'nin siber güvenlik politikaları öncelikle kamu kurumları genelinde saldırı önleme sistemleri kurulması üzerine kurulmuş olup bu kapsamda kamu kurumları ağlarının ortak bir tek ağ üzerinde güvenli internet bağlantısı ile yönetilme hususu düzenlenmiş, bu düzenleme ile 2003 yılında "Ulusal Siber Uzay Güvenliğini Sağlama Stratejisi"[129] (The National Strategy of Secure Cyberspace,

---

[128] Bkz.İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü, Siber Güvenlik Raporu, Mayıs 2012, İstanbul, Ahmet Ünal, ABD İncelemesi, sy:14

[129]Bkz. The National Strategy of Secure Cyberspace, Şubat 2003,

2003) belgesinde siber güvenlik stratejisi hazırlanmış olup siber savunmanın sağlanması açısından kurumlar arasında ortak harekat planı olarak ortaya konulmuştur.

ABD tarafından kurulan ilk Bilgisayar Acil Müdahale Ekibi Koordinasyon Merkezi olan CERT/CC(Computer Emergency Response Team Coordination Center) ile İç Güvenlik Bakanlığı organizasyonu kapsamında bulunan Ulusal Siber Güvenlik Birimi altında ulusal düzeyde bir acil müdahale timi olan US-CERT (United States Computer Emergency Readiness Team) kurulmuştur.

Bu kapsamda Ulusal Siber Tepki Koordinasyon Grubu ulusal boyutta ektisi olabilecek bir siber saldırının meydana gelmesi durumunda on dokuzdan fazla federal kuruluşun arasındaki koordinasyonu sağlamakla görevlendirilmiştir.

Yayınlanan Ulusal Siber Uzay Güvenliğini Sağlama Stratejisi belgesinde bu kuruluşun (US-CERT) amacının federal sivil ağlar(.gov uzantılı) olarak belirlenmiş olup bazı federal kurumlar tarafından yapılan çalışmaların koordine edilmesi amacı ile İç Güvenlik Bakanlığının acil bir çıkış planı ile uyarı sistemi geliştirmesi istenmiş, ulusal düzeyde bir siber saldırı meydana gelmesi halinde federal kuruluşun çalışmalarını yönetme ve koordinasyonu yetkisi verilmiştir.

Bu belgede özel sektör tarafından gelişmekte olan bir siber tehdit karşısında bu tehdide karşılık verebilmek için daha gelişmiş donanıma ve yapıya sahip olunması gerektiği ve ulusal güvenlik birliği oluşturulmasının önemi ile bu amaçla bir yaklaşım oluşturulması gerektiği belirtilmiştir.[130]

Bu yaklaşım kapsamında federal sivil ağların korunması ve tepki konulması süreci, izleme ve istihbarat toplanması süreci, karşı atak ve ordu ağı savunması sağlanması süreci yer almaktadır.

---

https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf adresinden erişilmiştir. (Erişim tarihi: 08.07.2017)

[130]Bkz. The National Strategy of Secure Cyberspace, Şubat 2003, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf adresinden erişilmiştir. (Erişim tarihi: 08.07.2017)

Bunlara ek olarak yukarıda belirtilen ilk 3 süreç için ortak olarak kullanılan EINSTEIN[131], TIC[132] ve Classified Programs[133] gibi bazı programlar yer almaktadır.[134] (ÜNAL, 2012)

Hukuk boyutunda organizasyonun yeniden yapılandırılması çalışmaları kapsamında FBI ile Ulusal Beyaz Yaka Suç Merkezi (National White Collar Crime Center) işbirliği ile 2001 yılında İnternet Suçu Şikâyet Merkezini (Internet Crime Complaint Center) kurulmuş olup program kurulduğu tarihten beridir kullanılmakta olup büyük bir başarı elde etmiştir. Sadece 2008 yılı içinde sisteme 27.000 den fazla şikayet düşmüş, yapılan bu şikayetlerden %26 sı doğrulanarak hukuki yaptırımın sağlanması amacıyla ilgili hukuki kuruma yönlendirilmiştir. Diğer taraftan ise bu program ülke bazında önemli bir başarı olarak değerlendirilse de FBI tarafından yapılmış bir anket kapsamında internette işlenen suçların önemli bir kısmının önceden tespit edilemediğini, programın sadece ufak bir bölümünü tespit edebildiğini ortaya çıkmıştır. Bu sebeple program başarı oranına rağmen siber suçların önlenmesinde etkili olamamıştır.

FBI tarafından 2003 yılında Bilgisayar Suçları Görev Gücü(Computer Crime Task Forces) isimli bir organizasyon kurulmuş olup bu organizasyonun görevi polis kuruluşuna yerel bilgisayar kaynaklı suçların soruşturulmasında yardım etmektir. ABD'de bu amaçla çalışan 92 kadar görev gücü bulunmaktadır.

Aynı sebepten yola çıkarak, Adalet Departmanı (Department of Justice), Bilgisayar Hackleme ve Fikri Mülkiyet (Computer Hacking & Intellectual Property) isimleri ile bölgesel federal mahkemelerde bulunan ve siber suçların etkili olarak anlaşılmasını ve gereken adli kovuşturmanın yapılabilmesi hususunda avukatlara eğitimler veren birimler kurulmuştur.

---

[131] EINSTEIN, NSA tarafında kullanılan ve özel ağlar dahil olmak üzere internet ağlarının takip edilmesine yardımcı olan gizli bir programdır.

[132] Güvenilir Internet Bağlantıları Programı (Trusted Internet Connections Program, TIC) ise, federal ağ içerisinde bulunan 4000 bağlantının 50'ye düşürülmesinde kullanılan programdır

[133] Gizli Programlar (Classified Programs) adı altındaki programlar da Savunma Departmanı (Department of Defense) tarafından yürütülen ve karşı taarruz ile ilgili teknolojiyi içerdiği varsayılan programlardır.

[134]Bkz. İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü, Siber Güvenlik Raporu, Mayıs 2012, İstanbul, Ahmet Ünal, ABD İncelemesi, sy.14

"Federal Ticaret Komisyonu (Federal Trade Commission- FTC) siber suçların artmasını önlemede aktif bir rol oynamıştır. Her ne kadar bu çalışma spesifik olarak komisyondan istenmemiş olsa da, FTC'nin tüketici haklarını korumasıyla ilgili çalışmalarının yan ürünü olarak ortaya çıkan bu durum FTC'nin şüpheli hosting sağlayan ve yasadışı aktivitelerin yürütülmesine izin veren internet servis sağlayıcıları hakkında resmi şikâyet duyurusunda bulunma ve gerektiği yerde sınırlandırıcı uygulamada bulunmasına da sebep olmuştur. Bu yüzden FTC, STK, CERT ve yerel hükümet kuruluşlarından gelen zaman duyarlı güvenlik uyarılarına hukuki olarak karşı tepki koyma yetkisine sahip olmasından dolayı sektörler arası işbirliğinin oluşmasında da kritik bir rol üstlenmiştir[135]."

2009'da faaliyetine başlayan Ulusal Siber Güvenlik İletişim ve Entegrasyon Merkezi gibi üst kurumlar, kamu ve özel sektör arasında bulunan siber güvenliğe ilişkin iletişimin güçlendirilmesi bakımından önemli bazı misyonlar yüklenmiş olup bu ekiplerin koordinasyonunun sağlandığı ve bilgi paylaşımı görevinin üstlenildiği CERT CC(Computer Emergency Response Team Coordination Center) uzmanlar arasında faydalı olan bir bilgi ağı görevi görmektedir[136].

ABD nin güvenlik politikaları hususunda en büyük eleştiri siber saldırılara ilişkin savunmanın ve politikaların kamu seviyesinde kalması, özel sektör ve bireysel saldırıları konusunda adım atılmamasıdır.

Sonraki dönemlerde ABD'nin Siber güvenlik politikalarının temel unsuru Merkezi düzenlemeler olup ilk aşamada güvenlik stratejisi üç ana sektör üzerinde şekillenmiştir.

İlk sektör internet omurgası olmakla birlikte İnternet omurgasını oluşturan temel ve sınırlı sayıdaki ana İnternet Sağlayıcı şirket (ISS) ABD'de bulunan tüm İnternet Servis Sağlayıcılara bağlanabilmektedir. Binlerce mil uzunlukta fiber optik kabloya sahip olan ana ISS'ler denizaltından uzanan kablolar vasıtasıyla

---

[135]Bkz. İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü, Siber Güvenlik Raporu, Mayıs 2012, İstanbul, Ahmet Ünal, ABD İncelemesi, sy.12

[136]Bkz.https://siberbulten.com/uncategorized/siber-guvenlikte-kamu-ozel-sektor-isbirligi-mumkun-mu/ (Erişim tarihi: 09.12.2018)

dünyanın geri kalanına bağlanmalar mümkün olmaktadır. ABD'nin İnternet trafiğinin yüzde 90'ından fazlası ana omurga üzerinden geçmekte olup omurgayı oluşturan Internet Servis Sağlayıcılardan geçmeden ABD'de dolaşmak mümkün değildir. Bu kapsamda ana internet omurgasının korunmasının sağlanması halinde ABD altyapısının da korunması mümkün olabilecektir.

Savunma Stratejisindeki ikinci sektör elektrik şebekesinin güvence altına alınması olup ABD'yi tamamen felç etmek isteyen bir saldırgan tarafından yapılması gereken en kolay işlem ABD ve Kanada'ya elektrik enerjisi sağlayan Doğu yada Batı şebekelerinden birinin sekteye uğratılmasıdır. Bu sektörün savunulmasında yapılması gereken en önemli şey bir federal düzenleme ile üretim ve ileti şirketlerinin kontrol ağlarının internetten çıkartılmasıdır. İnternet yerine intranet ağlarında bulunacak bu kontrol ağlarında girişlerinde kimlik doğrulaması sistemi ile gerçekleştirilmesi gerekmektedir.

Federal Enerji Düzenleme Kurulu 2010 yılında güvenli siber sistemlere sahip olmayan enerji şirketlerine ceza verileceğini açıklamış, ABD Enerji Bakanlığı da güvenlik uzmanı istihdamı ile bu yönde yaratılan 3,4 milyar dolar tutarındaki Akıllı Şebeke hibe programının yeterli güvenceye alınmış programlara harcanıp harcanmadığını denetlemektedir.

Savunma stratejisinde önem taşıyan son sektör ise savunmanın kendisi olmakla esas itibariyle siber güvenliğin sağlanması için savunmanın ve savunmada olan kurumun ağ güvenliği ile silahlarının uyumluluğu sağlanmalıdır. Savunmada olan kurumun güvenliğinin ise ;

- "Ağın kendisinin korumanın yanında son noktalarında korunması gerekmektedir. Bunun ağdaki bilgisayarların tümünün internete bağlı olup olmadığına bakılmaksızın masaüstü firewall programları, antivirüs ve yetkisiz girişleri önleme yazılımları yüklenerek yapılması mümkündür.
- Tüm ağlardaki kullanıcılar giriş yaparken en az iki kimlik doğrulama işleminden geçirilmelidir.
- Ağlar alt ağlara bölünerek alt ağlara girecek personel sayısı "bilme gereksinimi" kurallarına tabi tutularak kısıtlanmalıdır.

- Şifreleme düzeyinin arttırılması ile fiber kablolar üzerinde hareket halindeki verilerin yanı sıra veri depolama sunucularında durağan haldeki dosyaların da şifrelenmesi gerekmektedir.
- Tüm ağlara yetkisiz girişlere karşı sürekli gözetleme altında tutulmalı, bilinmeyen bilgisayarlar otomatik olarak kapatılmalıdır."[137]

ABD'nin 2010 tarihinde oluşturduğu Ulusal Güvenlik Stratejisinde siber tehditlerin ulusal ve kamu güvenliği ile ekonomik alanda en önemli konular arasında bulunduğu kabul edilmiştir. ABD Savunma Bakanlığı'nın 2011 yılında hazırladığı Siber Uzay Operasyon Stratejisi dokümanında ise siber ortamın fiziksel alanla birlikte bir savaş alanı olduğu kabul edilmiş, akabinde 23 Haziran 2009 tarihinde Stratejik Komutanlığı'na verilmiş olan bir emir gereği siber alanda düzenlenecek operasyonların yönetilmesi amacı ile 21 Mayıs 2010 tarihinde Siber Komutanlık - CYBERCOM kurulmuştur.

ABD tarafından 2011 tarihinde hazırlanan Siber Uzay İçin Uluslararası Strateji isimli strateji belgesinde siber saldırıların karşında uluslararası işbirliği kurulması gerektiği belirtilmiş olup bu belge kapsamında siber uzaya hakim olacak olan kuralların uluslararası hukuk kurallarını yeniden geliştirmeye gerek duymayacağı gibi mevcut hukuk kurallarını da anlamsız kılmayacağı, barış yada savaş ortamında hükümetlerin hareketlerine yön verecek olan kuralların siber uzay alanında da uygulanabileceği belirtilmiş olup bu bağlamda mevcut hukuk kurallarının siber uzayın ve gelişmekte olan teknoloji de göz önüne alınarak yorumlanması gerektiği vurgulamıştır[138].

---

[137]Bkz. Clarke, Richard A.; Knake, Robert K., Siber Savaş, (Çeviren: Murat Erduran), İkü Yayın Evi, Nisan 2011, s.84-90

[138] Bkz. Mehmet Yayla, "Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı", Hacettepe Hukuk Fakültesi Dergisi, Cilt 4, Sayı 2, Yıl 2014, sy.185 belgeye http://www.hukukdergi.hacettepe.edu.tr/C4S2tammetin.pdf adresinden erişilmiştir. (Erişim Tarihi: 01..03.2017)

ABD'nin başlıca siber güvenlik stratejilerini Ar-Ge faaliyetlerinin koordinasyonunun sağlanması ve faaliyetlerin yönetilmesi, mevcut siber operasyon merkezlerinin birbirleri ile bağlantılarının sağlanması veya bağlanması, siber casusluğa karşılık karşı siber casusluk planları geliştirilmesi ile bu planların uygulanması, siber güvenlik alanında eğitim ve bilinçlendirme çalışmaları yürütülmesi ve mevcut çalışmaların genişletilmesi, caydırıcılık sağlayan stratejilerin ve programların tanımlanarak geliştirilmesi ile kritik altyapı alanlarını da kapsayan ve hükümetin sorumlu olduğu alanları tanımlayarak siber güvenlik çalışmalarının geliştirilerek yürütülmesi olarak karşımıza çıkmaktadır.

ABD'de hukuki boyutta yeniden yapılandırma ve siber alanla ilgili mevzuatsal düzenlemeler kapsamında yapılan çalışmalar arasında en önemlilerinden biri FBI, Ulusal Beyaz Yaka Suç Merkezi (National White Collar Crime Center) ile işbirliğinde gerçekleştirilen İnternet Suçu Şikâyet Merkezinin (Internet Crime Complaint Center) kurulmasıdır. 2001 yılında kurulan merkez öncesinde INTERPOL tarafından kurulmuş olan 24/7 ağı ile benzerlikler taşımasının yanında internette işlenen veya internet ile işlenen suçların raporlanması açısından çok önemli bir görev üstlenmesi amacı ile kurulmuş olup sivil toplum kuruluşları, siber olaylara müdahale timleri ve yerel hükümet kuruluşları tarafından yapılan güvenlik uyarılarına hukuki olarak karşı tepki koyma yetkisine sahip olması sebebi ile sektörler arasında işbirliği oluşturulmasında çok önemli bir rol üstlenmiştir.

ABD 2011 yılında ulusal strateji belgesi yayınlamıştır. Bu belgede kamu kurumlarında saldırı önleme sistemlerinin kurulması, ağların güvenli bağlantılar ile yönetilmesi, mevcut siber ortam merkez kuruluşlarının koordine edilerek birlikte yönetilmesi ve karşı siber casusluk planlarının geliştirilerek uygulanması , kritik altyapı alanlarını içine alan genişletilmiş siber güvenlik çalışmalarının yürütülmesi ve Ar-Ge faaliyetlerinin yönetilmesi planlanmıştır[139].

---

[139]Bkz. Doç. Dr. Yıldıray YALMAN, " Güncel Tehdit ; Siber Saldırılar", Seçkin Yayınları, 2. Bölüm, Ulusal Siber Güvenlik stratejisi ve Yürütülen Çalışmalar, s. 58

2009 yılında ABD Birleşik Siber Komutanlık bünyesinde ABD donanması tarafından siber muhabere birimi kurulmuştur.

Yukarıdaki açıklamalar ışığında siber güvenliğin sürekli artan bir ihtiyaç olduğu ve ABD'nin de bu güvenlik ihtiyacına sessiz kalmadığı görülecek olup 1997 yılı ile günümüz arasında, dünyanın her yerinden bilgi ve bilişim sistemleri güvenliği uzmanlarının, hackerların, istihbarat elemanlarının katıldığı her yıl yapılan "Black Hat" toplantılarında eski hackerlar- şimdinin beyaz şapkalı ya da "Etik" Hackerları toplanarak Black Hat konferanslarında eğitimler düzenlenmekte olup sene içinde yapılan araştırmalar, Microsoft Apple gibi teknoloji şirketlerinin, yazılım şirketlerinin hataları, yazılım hataları, ürünlerindeki açıklar ve hatalar tartışılmakta, siber güvenlik üzerine yapılan sunumlar ile güvenlik araçlarının tanıtıldığı tanıtım sunumları yapılmaktadır[140].

2009 yılında Black Hat Konferansı bünyesinde halka kapalı yapılan ve devlet yetkilileri, görevdeki bürokratlar, büyük şirketlerin CISO'ları, akademisyenler ve üst düzey bilgi teknoloji şirketlerinin yöneticilerin oluşturduğu 30 katılımıyla yapılan bir toplantıda hükümetin siber güvenlik ile ilgili yapması gerekenler konuşulmuş ve toplantı neticesinde ;

- Federal devletin siber güvenliğe yönelik Ar-Ge çalışmaları için finansal destek vermesi,
- Siber güvenlik konusunda devlet yaptırımlarının artması gerektiği, örneğin internet omurga taşıyıcıları için federal yönetmelikleri çıkartılması gibi,
- Siber saldırıları kimin yaptığının keşfedilmesi için fazla çaba sarf edilmemesi bunun yerine "sağlamlık" unsurunun geliştirilmesi daha uygun olduğu, (Burada sağlamlıktan kastedilen felaket yaratacak siber saldırılardır)
- Kamu hizmet ağları ve internet arasında bağlantı olmaması gerektiği, "Kritik altyapı" ağlarının mutlaka herkese açık olan internet'ten ayrılması gerektiği,

[140]Bkz.Black Hat Konferansları için bkz. https://www.blackhat.com/us-17/ (Erişim Tarihi: 09.08.2017)

Başkan Obama tarafından teşvik edilen Akıllı Elektrik Şebekesi Projesinin[141] buna aykırı olduğundan iptal edilmesi gerektiği,

- Siber Güvenlik konusunda liderlik eksikliği olduğu,

Hususlarında fikir birliğine varılmıştır[142].

Son olarak ABD'nin günümüzdeki stratejisini değerlendirecek olursak 2017 yılında yeni Başkan olan Donald Trump tarafından verilen ilk bütçe teklifi incelendiğinde federal hükümet ile ABD'nin kritik altyapılarının koruması amacıyla siber güvenlik faaliyetlerine 1.5 milyar USD yatırım yapılacağı açıklanmıştır. Bütçe teklifi kapsamında Anayurt Güvenliği Bakanlığı ve diğer kamu kurumları ile özel sektör arasında daha çok istihbari bilgi paylaşımı yapılması, her bakanlığın kendi içerisinde siber güvenlik kapsamında hesap verebilir hale getirileceği, halihazırda mevcut güvenlik sistemlerinin artırılması ile birimler arasında bilgi teknolojileri idaresinin ele alınacağı ve olası siber saldırılara karşılık verilebilecek duruma gelinmesi hedeflenmekte olduğu belirtilmiştir. Strateji kapsamında Eski Başkan Obama tarafından görevlendirilen ABD Savunma Bilim Kurulu tarafından yayınlanan analiz kapsamında soruşturmanın konusunu oluşturan Kuzey Kore tarafından ABD elektrik santrallerine yapılan siber saldırılarda yeni bütçe planlaması içinde yer bulmuştur. Bu kapsamda kritik altyapıların korunabilmesi için gereken her türlü tedbirin alınacağı belirtilmiştir[143].

İç Güvenlik Bakanlığı tarafından siber tehdit odak noktasında savunma sistemi olarak EINSTEIN 3 Accelerated(E3A)'ın Adalet Bakanlığı, Çalışma ve Enerji Bakanlığı gibi 45 federal kurumun yanında bütün sivil kabine düzeyinde bakanlıkları da kapsayacağı belirtilmiştir, Personel Yönetim Ofisi (OPM)'nin hack skandalı sonrası Kongre tarafından EINSTEIN'ın dağıtımına hız verilmiş ve Bakanlık; E3A(EINSTEIN 3 Accelerated)'nın gün itibariyle ağın içerisinde

---

[141] ABD'de 1890 yılından beri yaygın olarak kullanılmakta olan şebekelerin 21. yüzyıl ağ teknolojisi ile entegre edilmesiyle oluşturulan sistemlere "Akıllı Şebeke" denilmektedir.

[142] Bkz. Clarke, Richard A.; Knake, Robert K., Siber Savaş, (Çeviren: Murat Erduran), İkü Yayın Evi, Nisan 2011, s.66-67

[143]Bkz.https://siberbulten.com/uluslararasi-iliskiler/trumpdan-devrim-gibi-karar-her-bakanlik-kendi-siber-guvenliginden-sorumlu/ (Erişim Tarihi:06.07.2017)

gizlenmiş 1 milyondan fazla muhtemel siber tehdit saptadığı, ve bu tehditleri engellediği, zararlı trafiği tanımlayarak dış aktörlerin içeriye sızmasının engellendiğini açıklamıştır[144].

2015 yılında Amerikan ordusu tarafından Cyber Branch 17 adını verdiği yeni bir siber güvenlik birimi oluşturulması ve sivillerden oluşan bir siber ordu kurulması için planlamalar başlamış olup bu kapsamda işe alımlar yapılmaya başlamıştır[145].

ABD'nin güncel siber güvenlik strateji politikaları incelendiğinde ise 2018 yılında bir dizi siber güvenlik stratejisi belgesi yayınladığı görülecektir. Bu belgeleri ele almak gerekirse;

-Eylül 2018 yılında yeni bir Ulusal Siber Güvenlik Stratejisi[146] yayınlanmıştır. Strateji belgesi kapsamında stratejinin amacı Amerikan halkını, Amerikan yaşam biçimini ve Amerikan çıkarlarını korumak, Ulusalın ön saflarında yer almak olarak belirlenmiş, Güvenlik Stratejisinin Amerikan bilgi ağlarını korumak için önemi vurgulanmıştır. Strateji belgesine göre hükümet; ağlarını korumaya, kritik altyapıyı korumaya ve siber suçlarla mücadeleye odaklanan bir dizi koordineli eylem gerektirecektir. Birleşik Devletler Hükümeti, özel sektör ve halkın her biri, siber güvenliğini güçlendirmek için acil ve kararlı adımlar atmalıdır; her biri, ağları kontrol altında tutmaya ve birbirlerine uygun şekilde destek vermeye çalışır. Belgenin amacı Federal Ağ ve bilgiyi korumak, kritik altyapıları korumak, Siber Suçlar ile Mücadele ve Olay Raporlamasını iyileştirmek olarak belirlenmiştir.

-15 Mayıs 2018 de ABD İç Güvenlik Bakanlığı tarafından Siber Güvenlik Stratejisi[147] yayınlanmış ve yürürlüğe konulmuştur. 2023 yılına kadar yürürlükte

---

[144]Bkz.https://siberbulten.com/uluslararasi-iliskiler/abdde-kamu-aglarini-einstein-monitor-edecek/ (06.07.2017)
[145]Bkz.https://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/computers-and-technology/cyber-operations-officer.html(06.07.2017)
[146]Bkz. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
[147]Bkz.http://afyonluoglu.org/PublicWebFiles/strategies/America/USA%202018%20DHS%20Cyber%20Security%20Strategy.pdf

kalacak strateji kapsamında yayınlanan stratejinin amacı 2023'e kadar Ulusal Güvenlik Bakanlığının, devlet ağları ve kritik altyapıdaki güvenliği ve dayanıklılığı artırarak ulusal siber güvenlik risk yönetimini geliştirmesi, yasadışı siber aktivitenin azaltılması; siber olaylara tepkilerin iyileştirilmesi; ve birleşik bir departman yaklaşımı, güçlü liderlik ve diğer federal ve federal olmayan kuruluşlarla yakın ortaklık yoluyla daha güvenli ve güvenilir bir siber ekosistemi geliştirmek olduğu açıklanmıştır.

-2018 yılı için ise Savunma Bakanlığı tarafından Siber Güvenlik Stratejisi[148] yayınlanmıştır. Strateji belgesi kapsamında Siber Güvenlik stratejilerinin öncelikle ABD ordusunun siber alan dahil olmak üzere herhangi bir alanda savaşma ve savaş yapma yeteneğini sağlamak olduğunu, İkinci olarak, savunma bakanlığının önemli bir siber olaya neden olabilecek ABD'yi hedefleyen kötü amaçlı siber etkinliği önleme, mağlup etme veya caydırmayı hedeflemekte olduğunu ve savunma misyonundaki temel görevlerinin, hedeflerine ulaşmadan tehditleri durdurmak için odağı dışa doğru kaldırarak ileriye dönük savunma yapmak olduğu üzerinde durulmuş, belge kapsamında bakanlığın ayrıca kamu ve özel sektör ortaklarına diğer Federal bölümler ve kurumlarla koordineli olarak kötü niyetli siber faaliyet göstergelerine ve uyarılarına sahip olduğu vurgulanmıştır. Son olarak Bakanlığın siber kapasiteyi güçlendirmek, birleşik siber operasyonları genişletmek ve karşılıklı çıkarlarını geliştirmek için iki yönlü bilgi paylaşımını artırmak için ABD müttefikleri ve ortaklarıyla birlikte çalışacağı hususu belirtilmiştir.

2.3.Fransa

Fransa'nın siber güvenlik stratejisi genel olarak internet kullanıcılarıyla ilgili güvenlik tedbirlerinin alınmasının yanında siber güvenlik meselesini savunma

[148]Bkz.http://afyonluoglu.org/PublicWebFiles/strategies/America/USA%202018%20DoD%20Cyber%20Security%20Strategy.pdf

ve ulusal güvenlik politikaları ile birleştirilmesi şeklinde iki yönlü bir strateji olarak oluşturulduğunu söylemek mümkündür.

Fransa'nın siber güvenlik stratejilerine ilişkin dört temel belge mevcuttur. Bunlar; "Fransız Savunma ve Ulusal Güvenlik Alanında Beyaz Kitap (The French White Paper on Defence and National Security) (2008), Fransız Bilgi Sistemleri Savunması Ve Güvenlik Stratejisi (Information Systems Defence And Security-France's Strategy, (2011)) , Savunma ve Ulusal Güvenlik Alanında Beyaz Kitap (White Paper on Defence and National Security (2013)) ve Fransız Ulusal Dijital Güvenlik Stratejisi (French National Digital Security Strategy, (2015)) tir.

Fransa'nın ulusal savunma ve güvenlik stratejilerini oluşturan Beyaz Kitap olarak tabir edilen strateji belgelerinden ilki 1972 yılında, ikincisi ise 1994 yılında hazırlanmıştır.

Fransa'nın siber güvenlik anlamında en önemli adım 2008 yılında Cumhurbaşkanı Nicolas Sarkozy'nin talimatı ile hazırlanan "Fransız Savunma ve Ulusal Güvenlik Alanında Beyaz Kitap"(The French White Paper on defence and national security)" isimli kitap oluşturulmuştur.

2008 yılında Cumhurbaşkanı tarafından hazırlatılan bu kitapta, önümüzdeki on beş yıl için stratejik değerlendirmeyi sunulmuş olup sonuçları üzerinden yeni bir savunma ve güvenlik politikası taslağı hazırlamak amacıyla hazırlanmıştır. Rapor Fransız stratejisinin tanımlanmasında büyük bir yenilik getirmekte olup sadece savunma için değil aynı zamanda ulusal güvenlik için bir strateji önermektedir. Amacı, ulusun hayatına zarar verebilecek riskleri ve tehditleri ortadan kaldırmaktır.

Raporda; Tehditlerin Devletlerden veya ulus ötesi Devlet dışı gruplardan gelebileceği gibi risklerin, küresel bir yanıt çağrısında bulunan doğal afetlerden ya da sağlık felaketlerinden kaynaklanabileceği, ülkenin güvenliğinin düşmanca niyetlerin ya da kazalara bağlı arızaların bir sonucu olarak etkilenebileceği, durum ne olursa olsun, ulusal güvenliği tehdit etme ihtimali öngörü, önleme ve hızlı bir tepki gerektirir ve hükümetin elinde olan tüm araçları kullanması gerektiği ve Avrupa ile uluslararası işbirliğini harekete geçirilmesi gerektiği dolayısıyla bu stratejinin hem dış hem de iç güvenlik, askeri araçların yanı sıra sivil olanları, dönemin katı anlamıyla savunma politikasını, iç güvenlik politikasını ve sivil

güvenliğini, dış politika ve ekonomik politika ile birlikte benimsediği, kapsamlı bir güvenlik stratejisinin tanımının yeni bir zorunluluk olduğu, yani küreselleşmeden kaynaklanan karışıklıklara uyum sağlama ihtiyacı için bir cevap olduğu, bunun yalnızca Fransa'da değil aynı zamanda müttefikler ve ortaklarının da görevi olduğu, stratejik güvenlik ortamındaki gelişmelerin gerektirdiği ölçüde Beyaz Kitap'ın güncelleştirilmesi gerektiği belirtilmiştir[149]. (The French White Paper On Defence And National Security, 2008)

Rapor kapsamında toplumda bilişim teknolojilerine her gün artarak çoğalan bir bağımlılık oluştuğu da dikkate alınmak suretiyle siber saldırılar en önemli milli güvenlik sorunlarından biri olarak tanımlanmış ve bu kapsamda siber alanda Fransa'nın egemenlik alanı içerisine dahil olduğu ve bu alanı savunma ve saldırı yeteneklerini arttırmak amaçlı stratejiler oluşturulduğu belirtilmiştir[150]. (TAŞÇI, 2012)

Fransa'nın siber güvenlik alanında temel kurumu olan Ulusal Bilgi Sistemleri Güvenlik Ajansı 2009 yılında kurulmuş olup Ajansın görevleri; siber saldırıların tespit edilmesi ve saldırılara karşı cevap verilmesi, yapılacak AR-Ge faaliyetleri ve araştırmaları aracılığıyla siber saldırılara karşı önlem alınması, saldırıların önlenmesi ile kritik önemi olan kurumlara bilgi sağlamasıdır[151]. (European Network and Information Security Agency, 2010)

Ulusal Bilgi Sistemleri Güvenlik Ajansı organizasyon içerisinde Milli Güvenlik Genel Sekreterliği gözetimi altında doğrudan Başbakana bağlı olarak faaliyetini yürütmektedir.

---

[149]Bkz.The French White Paper On Defence And National Security, 2008, sy: 15-16 Raporun orjinaline http://www.mocr.army.cz/images/Bilakniha/ZSD/French%20White%20Paper%20on%20Defence%20and%20National%20Security%202008.pdf adresinden erişilmiştir. (Erişim Tarihi 15.10.2017)

[150]Bkz. İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü, Siber Güvenlik Raporu, Mayıs 2012, İstanbul, Burak Taşçı, Fransa ve AB İncelemesi, sy.27

[151]Bkz. European Network and Information Security Agency, , France Country Report, Jan, 2010, raporun orjinaline https://joinup.ec.europa.eu/sites/default/files/document/2014-12/France%20Country%20Report.pdf adresinden erişilmiştir. (Erişim Tarihi 15.10.2017)

Siber güvenlik politikasının uygulanmasının yanında Fransa, bünyesindeki kurumları vasıtasıyla kendi siber saldırı kabiliyetini de geliştirmek için çalışmaktadır. Bu husus yukarıda raporu açıklarken değindiğimiz saldırılara cevap verme işlevini yerine getirmek için karşı saldırı planlanabilmesine olanak sağlamaktadır.

Kara Kuvvetleri ve Hava Kuvvetleri bünyelerinde elektronik saldırı birimleri kurulmuş olup bu birimler kapsamında Fransız İstihbarat Teşkilatı tarafından siber saldırı unsurlarını yakından izlenmektedir.

Fransa'nın ilk siber güvenlik stratejisi, ekonomik ve finans bakanlıklarına yapılan casusluk saldırısının ortaya çıkmasından hemen sonra yayınlanmıştır. Saldırı neticesinde siber saldırganların bakanlık ağlarından birini kontrol altına aldıklarını ve aylarca düzenli olarak siyasi ekonomik ve mali bilgileri bu ağdan topladıkları ortaya çıkmıştır. Yapılan saldırılar neticesinde verileri çalınan bir çok boyut, sektör ve kapasitede çok sayıda Fransız işletmesi saldırganlarca hedef alınmış olup işletmeler aynı zamanda takip edilmesi çok zor olan ve karşılığında fidye ödenmesi talep edilen bir çok dolandırıcılığa ve zararlı yazılımlara maruz kalmışlardır[152]. (French National Digital Security Strategy, 2015)

Bu saldırıların ortaya çıkmasından hemen sonra Ulusal Bilgi Sistemleri Güvenlik Ajansı (The National Cybersecurity Agency of France (ANSSI)) tarafından Bilgi Sistemlerinin Savunması Ve Güvenliği ile İlgili Ulusal Strateji Planı 2011 yılında yayınlanmıştır[153]. (Information Systems Defence And Security- France's Strategy , 2011)

Yayınlanan Bilgi Sistemlerinin Savunması Ve Güvenliğiyle İlgili Ulusal Strateji Planı kapsamında Fransa'nın Siber Güvenlik Stratejisi; Siber saldırılara

---

[152]Bkz.French National Digital Security Strategy, 2015, strateji raporunun orjinaline https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf adresinden erişilmiştir.(Erişim Tarihi: 12.10.2017)

[153]Bkz. Information Systems Defence And Security- France's Strategy , 2011, strateji raporunun orjinaline https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf adresinden erişilmiştir. (Erişim Tarihi 16.10.2017)

karşı korumak ve savunmak ve siber alanda Fransız vatandaşları, işletmeler ve ulusun güvenliğini korumak için dört stratejik hedef belirlenmiştir:

1- Siber güvenlik alanında küresel bir siber savunma gücü haline gelerek, özerkliğini korurken bu alandaki büyük ulusların iç çevrelerinde yerini almak,
2- Ulusal Egemenliği ile ilgili bilgileri koruyarak Fransa'nın karar alma özgürlüğünü korumak
3- Ulusal kritik altyapıların siber güvenliklerini güçlendirmek
4- Ve siber uzayda güvenliği korumak.

Olarak belirlemiştir.

Bu dört stratejik hedefi ve bunlardan kaynaklanan ve bu hedefleri gerçekleştirmek için ortaya konması gereken 7 hareket alanın belirlendiği belge, tüm vatandaşların, hükümet eyleminin önceliklerini ve kapsamını anlamasına olanak tanıyacağı belirtilmiştir.

Ayrıca belge ile halen hazırlık aşamasında olan yeni Güvenlik stratejisinin 2015 yılının ikinci yarısında ortaya konulacağı ve Fransa'nın risk önleme ve olay işleme hizmetleri sağlayan bir dizi CERT'ye sahip olduğu ve bu CERT'lerin (Bilgisayar Acil Müdahale Ekipleri), işletmeler ve/veya devlet dairelerine yardımcı olmak için kurulmuş olan siber saldırı uyarısı ve müdahale ekipleri olduğu açıklanmıştır[154].

ENISA tarafından 2012 yılından yayınlanan Ulusların Siber Güvenlik Stratejileri isimli belgede Fransa'nın siber güvenlik stratejisi siber ortamdaki olaylara karşı verilerin kullanılabilirliği, bütünlüğü veya gizliliğinin güvenceye alınması için bilgi iletişim sistemlerinin etkinleştirilmesine odaklanmıştır. Bu kapsamda Fransa Ulusal Siber Güvenlik Stratejileri Siber güvenliğin güçlendirilmesi için ulusal çabaların yolunu belirlemek, bilgi sistemlerinin güvenliği ve siber suçlarla mücadeleyle ilgili teknik araçların ve bir siber

[154] Bkz.https://www.ssi.gouv.fr/en/cybersecurity-in-france/cybersecurity-strategy/

savunmanın kurulmasını vurguladığı belirlenmiştir[155]. (ENISA, National Cyber Security Strategies Setting the course for national efforts to strengthen security in cyberspace, 2012)

Fransa'nın ulusal siber güvenlik stratejilerinde yukarıda açıklanan 4 ana hedefe ulaşılması için izlenmesi gereken yol haritası oluşturulmuş 4 ana hedefe ulaşılabilmesi için 7 ana hareket alanı belirlenmiştir.

Buna göre ;

1. Saldırıları ve İhlalleri Öngörmek ve Analiz etmek ;

Bu madde kapsamında riskler ve tehditlerin siber alanda hızla geliştiği, yeni bir ürünün veya yeni bir yazılım sürümünün piyasaya sürülmesinin, yaygın olarak kullanılan bir yazılım ürününde düzeltilmemiş bir kusurun ifşa edilmesinin, yeni teknolojilerin veya uygulamaların geliştirilmesinin veya hatta politik bir bildiri yayınlanmasının bile bilgi sistemlerinin güvenliğini çok kısa bir zaman aralığında tehdit edebileceği, bu bilgiler ışığında bilgi sistemlerinin güvenliğini ve savunmasını garantiye almak için atılması gereken ilk adımın en son teknoloji gelişmelerini yakından takip ederek izlemenin, analiz etmenin, tamamen anlamanın ve hatta kamu veya özel aktörlerin faaliyetlerini öngörmenin gerekliliği belirtilmiştir.

2. Saldırıları tespit etmek, zarar görmesi muhtemel kişilerin uyarılması ve saldırıya karşılık verilmesi maddesi kapsamında Strateji belgesinde, internetteki şirketlerin, altyapıların ve hizmetlerin artan bağımlılığı göz önüne alındığında ve bazı zayıflıklarla ilgili sistemik risklerden dolayı kusurları ve saldırıları mümkün olan en kısa sürede tespit edebilmek gerektiği bu sayede potansiyel ve bilinen

[155] Bkz. ENISA, National Cyber Security Strategies Setting the course for national efforts to strengthen security in cyberspace, May 2012, raporun orjinaline https://www.enisa.europa.eu/.../cyber-security.../fullReport adresinden erişilmiştir.(Erişim Taihi : 15.11.2017)

mağdurların uyarılması ve zarar görenlere, yapılan analizler ve geliştirmeler neticesinde gerekli yardımın hızlıca sunulması gerektiği belirtilmiştir.

Ayrıca Fransa, Savunma ve Ulusal Güvenlikle ilgili Fransız Beyaz Kitabında planlandığı gibi, bilgi sistemleri saldırıları için bir algılama yeteneği geliştirmekte olduğu, özellikle bakanlık ağlarında yerleştirilen bu sistemlerin, saldırıları karşısında ilgili personelin uyarılması, saldırıların niteliğini değerlendirmesi ve saldırılara uygun gerekli önlemlerin alınmasına yardımcı olacağı öngörülmektedir.

Ulusal ağ durumunun gerçek zamanlı bir resmini elde etmek için ya bu algılama araçları ile toplanan tüm bilgileri, mekanizmaları izlemek ya da ortaklarımız tarafından sağlanan ve bir kriz durumunu yönetmek için yönetmek için ANSSI, zorluklara uyarlanmış bir "operasyon odası" ile donatılmıştır.

Devlet, idari bilgi sistemlerinin veya kritik altyapı operatörlerinin güvenliğini etkileyen ya da tehdit eden büyük krizlere tepki verebilmek için gerekli önlemleri hızlı bir şekilde alabilmesi gerektiği bu amaçla, ANSSI, bilgi sistemleri savunmasından sorumlu ulusal makam olduğu belirtilmiştir.

3. Fransa'nın; Bilimsel, teknik, endüstriyel ve insani becerilerinin arttırılıp kalıcı hale getirilmesi maddesi kapsamında; Bilgi sistemlerinin güvenliği, kendilerine zarar vermek isteyen kuruluşlar ve bireyler tarafından erişilebilen teknoloji ve bilgi birikimine dayandığı, bilgi sistemleri güvenliğinden sorumlu devlet aktörleri yalnızca en yeni teknoloji ile tanışmakla kalmamalı, aynı zamanda araştırma yeteneklerini koruyarak teknolojik gelişmeleri öngörebilmeli hatta ilerisine görebilmeleri gerektiği, ancak bu sayede saldırganın savunmacı üzerindeki taktik avantajı sınırlandırılabileceği belirtilmiştir.

Bunun yanında Fransa'nın, kriptoloji ve resmi yöntemler alanında birinci sınıf araştırma ekiplerine sahip olduğu ve bu sayede bilgi sistemlerinin güvenlik mimarisi gibi diğer alanlarda hızla en gelişmiş uluslara yetişmekte olduğu belirtilmiştir.

4. Devletin ve kritik altyapı hizmetini sunan hizmet sunucularının bilgi sistemlerinin güvenliğinin sağlanması maddesi kapsamında Fransız Ulusal

Savunma ve Güvenlik Beyaz Kitabında belirtildiği gibi, Fransa devlet sırlarını korumak için çok yüksek güvenlikli ürünleri ve devlet kurumları ile hizmetlerinde kullanılabilecek ayrıca iş dünyasında yaygın olarak kullanılabilir hale getirilecek bir dizi garantili güvenilir ürün ve hizmetlerde uzmanlaşması ve geliştirmesi gerektiği, ayrıca "Büyükşehir Fransa'daki karar verme ve komuta zincirinin tamamı için" dirençli güvenli şebekeler kullanılması gerektiği belirtilmiştir.

5. Fransız Hukukunun teknolojide ortaya çıkan yeniliklere uyumlu hale getirilmesi maddesi kapsamında siber gelişim yoluyla uygulanan yeni uygulamaların, yeterince dikkat edilmediği takdirde, bireysel özgürlükleri tehdit ederek, kritik altyapıların işleyişini ve şirketlerin istikrarını tehdit edebileceği bu nedenle mevzuat ve düzenleyici işlemlerin, teknolojideki son gelişmeleri yansıtması gerektiği üzerinde durulmuştur. Yasalar, yeni teknolojiler ve yeni uygulamaların bireylerin güvenliğini güçlendirmek için ortaya çıkarken gözden geçirileceği ve aynı zamanda şirketlerin rekabet edebilirliği üzerindeki etkisini en aza indirme arzusunun ve devletin müdahale edebilme ihtiyacının dengesi sağlanacağı belirtilmiştir.

6. Bilgi sistemlerinin güvenliği, siber suçlarla mücadele ve siber güvenlik hususlarında Fransa'nın uluslararası iş birliklerinin geliştirilmesi maddesi kapsamında Bilgi sistemlerinin güvenliği kısmen çeşitli devletlerin ilgili hizmetleri arasındaki veri alışverişinin niteliğine dayandığı, Fransa'nın gerekli verilerin paylaşımını teşvik etmek için geniş bir yabancı ortak ağı kurmaya çalışacağı (Ör. Ürün ve hizmetlerin zayıflıkları veya kusurları hakkında bilgi) ve siber suçlarla mücadele etmek için ortaklarıyla olan ilişkilerini de güçlendireceği belirtilmiştir.

Benzer şekilde, müttefikler arasındaki güçlü ilişkiler, etkili bir siber savunma politikasının temelini oluşturmaktadır. Fransa, derinlemesine operasyonel değişimlerin düzenleneceği güvenilir ortaklar arasından seçkin bir daire oluşturduğu açıklanmıştır.

Fransa tarafından bu amaçla Almanya ve Amerika Birleşik Devletleri ile özel olarak anlaşma imzalanmış, ayrıca AB ve NATO bünyesinde de uluslararası işbirliği yapılmıştır.

7- Bireylerin bilgi sistemi güvenliğiyle ilgili hususları daha iyi kavrayabilmesi adına bunların düzenli olarak bilgilendirilip, konuyla ilgili ikna olmalarının sağlanması için iletişime geçilmesi maddesi kapsamında bilgi sistemlerinin güvenliğinin, şirketler ve hükümetler tarafından yapılan seçimler ve alınan teknik önlemlere dayandığı kadar organizasyondaki personelin dikkatine de dayanmakta olduğu, ülke ve vatandaşları üzerindeki bilgi sistemlerine yönelik büyük bir saldırının potansiyel sonuçları göz önüne alındığında, bireylerin ve kuruluşların farkındalık ve motivasyonunun sağlanması gerektiği belirtilmiştir[156].

Yukarıda açıklandığı üzere 2008 tarihli Beyaz Kitap'ın 5 yılda bir güncelleştirileceği öngörülmüş olup 2008 tarihli Beyaz Kitap'ın(Fransız Savunma ve Ulusal Güvenlik Alanında Beyaz Kitap (The French White Paper on Defence and National Security) güncelleştirilmesini içeren 2013 tarihli Beyaz Kitap, 29 Nisan 2013 tarihinde Cumhurbaşkanı François Hollande'ın onayıyla yayımlanmıştır.

2013 tarihli beyaz kitap 2008 tarihli Beyaz kitabın güncelleştirilmiş hali olmakla birlikte Fransa'nın güvenliği için gerekli olan ilke ve öncelikler ile eylemler ve araçların çerçevesinin çizilmesi amaçlanmaktadır.

Buna göre 2013 tarihli Fransız Savunma ve Ulusal Güvenlik Beyaz Kitabında özetle siber güvenlik alanında değinilen şu konulara değinilmiştir.

-Siber altyapıların hızlı olarak artması, devlet yada diğer aktörlerin sebebiyet verdiği sibernetik saldırı tehditlerinin de artması sebep olmakta olduğu, bu nedenle ülke için hayati önem taşıyan altyapı bilgi ve silah sistemleri ile askeri stratejilerinin işleyişini etkileyecek saldırıların ulusal güvenlik bakımından ciddi sonuçlar doğuracağı üzerinde durulmuş olup stratejik önceliğin vatandaşların korunması ve devletin işleyişinin devamlılığının sağlanması olduğu, bu kapsamda

---

[156] Bkz.Information systems defence and security- France's strategy , 2011, Strateji belgesinin aslına https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf adresinden erişilmiştir. (Erişim Tarihi 16.10.2017)

ülkeye yönelik olarak yapılan siber saldırıların karşılaşılan risk ve tehditler arasında olduğu belirtilmiştir.

Fransa'nın önceliğinin başkaca ülkeler tarafından Fransa topraklarına yapılacak her türlü saldırının önlenmesinin olduğu belirtilmiştir.

Bu kapsamda 2008 tarihli Beyaz Kitap ta belirtilen öneriler göz önüne alınarak istihbarat servislerinin stratejik olarak yönetimi , iş birliği sağlanarak koordine edilmesi amacı ile "Ulusal İstihbarat Konseyi" ve "Ulusal İstihbarat Koordinatörlüğü" kurulmuş ve ilerleyen dönemde "Ulusal İstihbarat Stratejisi" hazırlanması öngörülmüştür.

- Zorlayıcı müdahalenin gerekli olduğu durumlarda, mevcut üstünlüğün ele geçirilmesi ve korunması amacı ile yapılacak operasyonların kara, hava, deniz, uzay ve siber alan koordinasyonunda olacak şekilde gerçekleştirilmesi gerekliliği ile silahlı kuvvetlerin asimetrik yollarla gerçekleştirilmekte olan hibrit tehditler ile mücadele edebilecek kapasiteye sahip olması gerektiği,

-Bilgi ve iletişim sistemleri güvenliğinin sağlanması amacıyla özellikle kriptoloji ve siber saldırının tespiti için gerekli olacak sistem ve mekanizmanın Fransa tarafından üretilmesine olanak sağlayacak imkanların sağlanmasının ulusal güvenlik için öneminden bahsedilmiştir. Bu alanda Fransa'nın kritik altyapılarına ve elektronik iletişim kanallarına yönelik mevcut siber risklerden etkin koruma sağlanabilmesi için Avrupa politikasının uygulanmasını desteklediği ve halihazırda Avrupa Birliği kapsamında yürütülmekte olan güvenlik ile ilgili terörizm, kriz yönetimi, kitle imha silahları, siber güvenlik alanı ve güvenlik teknolojileri ile ilgili sektörel stratejilerin arasında bulunan uyumun güçlendirilmesi gerektiği belirtilmiştir[157]. (Fransanın Ulusal Savunma Ve Güvenlik Stratejisine İlişkin Beyaz Kitap, 2013)

[157] Bkz.. Fransanın Ulusal Savunma Ve Güvenlik Stratejisine İlişkin Beyaz Kitap, 2013, belgenin aslına https://otan.delegfrance.org/White-Paper-on-Defence-and-National-Security adresinden erişilmiştir. (Erişim Tarihi : 10.10.2017)

-Beyaz Kitap'ın 2008 yılındaki beyaz kitaba nazaran en önemli stratejik değişiklik siber alanın yeni bir çatışma alanı olarak kendine yer bulmuş olmasıdır[158]. (Fransanın Ulusal Savunma Ve GüvenliK Stratejisine ilişkin Beyaz Kitap , 2013)

2011 yılında yayınlanan Siber güvenlik raporundan sonra 2015 yılında Fransa Ulusal Dijital Güvenlik Stratejisi[159] (French National Digital Security Strategy, 2015) yayınlanmıştır. Bu strateji belgesinde Siber Güvenliğe ilişkin 5 stratejik konu öngörülmüştür.

Dijital Güvenlik Stratejisi Göre;

1- Devlet bilgi sistemleri ve kritik altyapıların temel çıkarları, savunması ve güvenliği, büyük siber güvenlik krizi konusu

Fransa, dünya standartlarındaki teknik uzmanlığın desteğiyle özerk stratejik düşünce geliştirerek, siber alanda temel unsurlarının devam eden savunmasını sağlayacağı buna paralel olarak, Fransa, kritik ağlarının güvenliğini ve ulusal ve uluslararası düzeyde özel paydaşlarla işbirliğini genişleterek büyük bir siber saldırı durumunda direncini güçlendirmeye devam edeceği belirlenmiştir.

2- Dijital güven, gizlilik, kişisel veriler, siber kötü niyet konusu

Siber ortamın her ölçekteki şirket ve birey için güvenli kalması amacıyla koruyucu önlemler ve düzeltici önlemler alınacağı belirtilmiştir. Bunun yanında korumanın, kişisel verilerin kullanımı ve kamuoyuna uygun çeşitli dijital güvenlik ürünlerinin geliştirilmesi ile ilgili kamu yetkililerinin artan ihtiyatlılığına

---

[158] Bkz. Fransanın ulusal savunma ve güvenlik stratejisine ilişkin 2013 Tarihli Beyaz Kitap http://mgk.gov.tr/calismalar/calismalar/022_fransa_2013_savunma_beyaz_kitabi.pdf

[159] Bkz. French National Digital Security Strategy, 2015, strateji raporunun orjinaline https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf adresinden erişilmiştir. (Erişim Tarihi: 12.10.2017)

dayanacağını, telafi edici eylemlerin siber kötü niyet mağdurlarına yardım amacıyla teknik ve yasal yardım sağlayacak şekilde yapılandırılacağı belirtilmiştir.

3-Bilinçlendirme, ilk eğitim ve sürekli eğitim konusu:

Bireylerin, toplumun dijitalleştirilmesi ile ilişkili riskler hakkında tam bilgi sahibi olmadıkları, bu nedenle, okul çocukları ve öğrencilerin farkındalığını artırmak için adımlar atılacağı ayrıca, siber güvenlik konusunda kamu ve özel sektörün artan taleplerini karşılamak için bu alana uzmanlar eğitimlerinin arttırılacağını belirtilmiştir.

4- Dijital teknoloji işletmeleri , sanayi politikası, ihracat ve uluslararasılaşma ortamının oluşturulması

Dijital pazarların dünyadaki gelişimi ve bununla bağlantılı güvenlik zorunlulukları, kullanımlarına uyarlanmış bir güvenlik seviyesine sahip olan Fransız dijital ürünlerini ve servislerini tanımlama fırsatı oluşturmaktadır. Devlet, yatırım, yenilikçilik ve ihracatın yanı sıra kamu alımları yoluyla da, güvenli ürün ve hizmetler sunmak için dijital sektördeki Fransız şirketler için uygun bir ortam geliştirecektir

5-Avrupa, dijital stratejik özerklik, siber güvenlik Konusu;

Siber uzayda uluslararası ilişkilerin düzenlenmesi önemli bir konu haline geldiği, Fransa'nın, benzer Üye Devletlerle birlikte, Avrupa'nın dijital stratejik özerklik yol haritasını destekleyeceği ayrıca uluslararası kuruluşlardaki güçlendirmesini sağlayacak ve en az korunan ülkelere rızaları ile kendi siber güvenlik özelliklerini geliştirme ve böylece siber dünyanın genel istikrarına katkıda bulunma konusunda destek sağlayacağı belirtilmiştir.

Dijital güvenlik, dijital Cumhuriyet projesine destek olmak anlamına geldiği bu bağlamda Devletin, bu stratejiyi geliştirmede ve dijital güvenlik uzmanları, kamu ve özel karar alıcılar ve vatandaşlar tarafından sürdürülmesi gereken bir dinamik başlatmada önemli bir rol oynadığı belirtilmiştir[160].

---

[160]French National Digital Security Strategy, 2015, strateji raporunun orjinaline https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf adresinden erişilmiştir. (Erişim Tarihi: 12.10.2017)

2009 yılında kurulan Fransız Ağ ve Bilgi Güvenliği Ajansı (ANSSI), ulusal siber güvenlik konusunda yetkili kurum olup Fransız siber güvenliğinin ön cephesinde, stratejik önem taşıyan kurumları hedef alan bilgisayar olaylarına karşı (standart belirleme dahil) önleme ve müdahale etmekten ve ulusal düzeyde kriz yönetimi tatbikatları düzenlemekle görevlidir. ANSSI 500'den fazla çalışanı mevcuttur.

Savunma Bakanlığı, eylemlerini destekleyen ve dijital mücadeleyi askeri operasyonların kalbinde yerleştiren ağların korunmasını garanti altına almanın ikili işlevlerini yerine getirir. Bakanlığın bu alandaki faaliyetini pekiştirmek için 2017 yılının başında Savunma Görevlisi Şefi'ne rapor veren bir siber savunma komuta birimi (COMSYBER) kurulmuştur.

İçişleri Bakanlığı, ulusal kurum ve çıkarları, ekonomik aktörleri, kamu otoritelerini ve bireyleri hedef alan her türlü siber suçla mücadele etmekle görevlidir. Bu amaçla, Ulusal Polis, Ulusal Jandarma ve İç Güvenlik Genel Müdürlerinin özel merkez ağlarını ve bölgesel ağlarını harekete geçirir. Siber saldırıların faillerini tespit etmek ve adalete teslim etmek için soruşturma yürütmekle görevlidir. Bu hizmetler, diğerlerinin yanı sıra önleme çabalarına katkıda bulunur ve ilgili kişiler arasında farkındalık yaratır.

Fransa Avrupa Birliği'nin dijital stratejik özerkliğini garanti altına almak için üç temel üzerinden vizyon oluşturmuştur.

Bu vizyonun;

Sanayi ve kapasite temeli kapsamında Temmuz 2016'daki Ağ ve Bilgi Güvenliği Yönergesi (NIS yönergesi) kapsamında her Üye Devletin siber güvenliğini güçlendirmek için önemli bir adım atılmıştır. Fransa, Avrupa Komisyonu tarafından, Avrupa'da gerçek bir siber güvenlik ajansı haline gelmesi ve Üye Devletler arasındaki operasyonel işbirliğinin güçlendirilmesi amacıyla Avrupa Ağ ve Bilgi Güvenliği Ajansı'nın (ENISA) güçlendirilmesi yönündeki önerisini de desteklemektedir.

Endüstriyel temeli kapsamında Temmuz 2016'da Avrupa Komisyonu tarafından başlatılan siber güvenlikle ilgili sözleşmeye dayalı kamu özel ortaklığı , Avrupa düzeyinde siber güvenlik alanında araştırma ve geliştirmeyi teşvik

etmelidir. Buna ek olarak, AB'nin stratejik özerkliği, dijital alanda bir sonraki teknolojik devrimin en üst noktasında olma kabiliyetine de bağlı olacaktır. Bu kapsamında Fransa Başbakanı tarafından DARPA'nın Avrupa versiyonu için bir finansman ajansı oluşturulması çağrısının yapılmıştır.

Standart belirlenmesi temeli kapsamında hem siyasi hem de teknik açıdan Fransa, AB'nin kendisini yüksek seviyedeki titizlik ve güvenlikle uyumlu siber standartlarla donatmasını sağlamalıdır. Bu siber güvenlik ürünlerinin sertifikalandırılması ve hassas bilgilerin bulunduğu alanlar için geçerlidir.

Siber alanda stratejik istikrarın ve uluslararası güvenliğin güçlendirilmesi Fransa'nın önceliklerinden biri olmakla birlikte Fransa, güvenli, istikrarlı ve açık bir siber alanı teşvik etmede aktif bir rol oynamaktadır. Fransa'nın Avrupa ve Dışişleri Bakanlığı Fransa'nın siber diplomasi çalışmalarını koordine etmektedir.

Fransa, özellikle siber alanda sorumlu davranış kurallarının tartışıldığı Birleşmiş Milletler bünyesinde faaliyet göstermektedir. Fransa, siber güvenlikle ilgili beş BM hükümet uzmanlarından oluşan gruplara (GGE) katılmış olup bu grupların çalışmaları sayesinde Birleşmiş Milletler Şartına dayalı olarak uluslararası sistemde siber alanı geliştirmek ve devletleri siber alanda önleme, işbirliği ve yaygınlaşmayı önleme amacıyla yönlendirmek mümkündür (2013'te, Birleşmiş Milletler Sözleşmesi de dahil olmak üzere uluslararası hukukun siber alanda uygulanabilirliği kabul edilmiş; 2015 yılında, Devletlerin iyi davranışlarını (sivil alanda "davranış normları") ilişkin bir takım gönüllü taahhütler birleştirilmiştir).

G7 zirvesinde 2016 yılında kurulan ve siber alanla ilgili konular üzerinde çalışmalar yürüten Ise-Shima grubunun çalışmaları neticesinde G7 Dışişleri Bakanları tarafından Siber Sorumlu Devlet Davranışı Üzerine bir Deklarasyon kabul edilmiştir.

Siber alanda güven artırıcı tedbirlerin tanımlanması ve uygulanması için bölgesel bir referans organı haline gelen Avrupa Güvenlik ve İşbirliği Teşkilatı'nda (AGİT) tarafından 2013 ve 2016'da iki yeni güven artırıcı önlem paketi kabul edilmiştir.

2015 yılında Fransız Ulusal Dijital Güvenlik Stratejisi[161] yayımlanmıştır. Strateji belgesi kapsamında 5 stratejik hedef belirlenmiştir.

Bu hedefler;

1*Devlet bilgi sistemleri ve eleştirel altyapı, temel bilgiler sistemlerinin temel ilgileri, savunma ve güvenliğinin sağlanması hedefi kapsamında; Fransa, dünya standartlarında teknik uzmanlık tarafından desteklenen özerk stratejik düşünceyi geliştirerek, temel siberlerin siber uzayda devam etmesini savunmaya devam edecektir. Buna paralel olarak, Fransa, ulusal ve uluslararası düzeylerde özel paydaşlarla işbirliğini genişleterek kritik ağların güvenliğini ve büyük bir siber saldırı durumunda dayanıklılığını güçlendirmeye devam edecektir.

2*Dijital güvenin sağlanması, gizlilik, kişisel bilgiler, siber erişim hedefi kapsamında; her boyuttaki işletme ve birey için siber alanın güvende kalması için koruyucu önlemler ve iyileştirici önlemler alınacaktır. Koruma, kamu yetkililerinin kişisel verilerin kullanımına ve genel halka uyarlanmış bir dizi dijital güvenlik ürününün geliştirilmesine ilişkin olarak yüksek hassasiyete dayanacaktır. Düzeltici faaliyetler, teknik ve yasal yardım sağlayan siber maluliyet mağdurlarına yardım etrafında yapılandırılacaktır.

3*Farkındalığı arttırma, ilk eğitim ve eğitime devam etme hedefi kapsamında Bireyler hala toplumun dijitalleşmesiyle ilişkili riskler konusunda yeterli farkındalığa sahip değiller. Bu nedenle okul çocukları ve öğrenciler bilincini arttırmak için adımlar atılacaktır. Ayrıca, kamu ve özel sektörden siber güvenlik konusundaki artan talepleri karşılamak için, bu alandaki uzmanların eğitimi artırılacaktır.

4* Dijital teknoloji işletmeleri, endüstriyel politika, ihracat ve uluslararası çevre hedefi kapsamında; Dijital pazarların dünya çapında büyümesi, güvenlik gereklilikleri ile birlikte, güvenlik seviyelerine sahip Fransız dijital ürün ve hizmetlerini kullanımlarına uygun hale getirme fırsatı yaratıyor. Devlet, yatırım,

[161]Bkz.http://afyonluoglu.org/PublicWebFiles/strategies/Europe/French%202015%20Digital%20Security%20Strategy-EN.pdf

inovasyon ve ihracatı destekleyerek, aynı zamanda kamu alımlarıyla destekleyerek, dijital sektördeki Fransız şirketleri için güvenli ürünler ve hizmetler sunan uygun bir ortam geliştirecektir.

5* Avrupa, dijital stratejik otonomi ve siber alanın stabilitesinin sağlanması hedefi kapsamında siber dünyadaki uluslararası ilişkilerin düzenlenmesi önemli bir konu haline geldi. Fransa, aynı fikirde olan Üye Devletlerle birlikte, Avrupa dijital stratejik özerkliği için bir yol haritası oluşturacak. Fransa aynı zamanda uluslararası organlardaki etkisini güçlendirecek ve siber alanın genel istikrarına katkıda bulunan siber güvenlik yeteneklerini geliştirme konusundaki rızalarıyla en az korunan ülkelere destek sağlayacaktır[162].

Son olarak, Fransa, özel sektör, sivil toplum ve devlet ortaklarıyla birlikte, sivil alanın istikrarını ve uluslararası güvenliğini güçlendirmede özel aktörlerin rolü ve sorumluluklarını dikkate alınması amacıyla Fransa Avrupa ve Dışişleri Bakanlığı, bu konuyla ilgili bir toplantıya, 18 Eylül 2017'de Birleşmiş Milletler Genel Kurulu (UNGA) 72. oturumunun oturum aralarında başkanlık etmiştir[163].

"Fransa'da konuyla ilgili hukuki düzenlemeler temel olarak şunlardır:

- E-Devlet Kanunu,

- 8 Kasım 2005 tarihli Kamu Kurumları ile Bireyler ve Kamu Kurumları arasındaki Elektronik Etkileşime dair Yönetmelik,

- 6 Ocak 1978 tarihli Bilgi Teknolojileri ve Özgürlükler Kanunu (belirtmek gerekir ki bu kanuna göre veri güvenliğinin temini amacıyla Ulusal Enformatik ve Özgürlükler Komisyonu kurulmuştur)

- e-ticaret mevzuatı,

[162]Bkz.http://afyonluoglu.org/PublicWebFiles/strategies/Europe/French%202015%20Digital%20Security%20Strategy-EN.pdf
[163] https://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/cyber-security/

- e-iletişim mevzuatı,

- siber suçlara karşı mücadeleyi amaçlayan 5 Ocak 1988 tarihli Godfrain Kanunu, bu kanun alanında bir ilk olma özelliği taşımaktadır.

- e-kimlik mevzuatıdır[164].”

2.4. İngiltere;

İngiltere’de bilişim ile ilgili ilk hukuksal düzenleme 1990 tarihli bilişim suçları ile ilgili olarak çıkartılan “Bilgisayarların Kötüye Kullanılması Yasası”(Computer Misuse Act)dır. Anılan kanun bakımından bilişim suçları olarak bilgisayardaki yazılım veya veriye yetkisiz erişim veya yetkisiz giriş, bu kapsamda başkaca suçların işlenmesinin kolaylaştırılması veya başkaca suçların işlenmesine yardım etme amacı ile bilgisayara yetkisiz olarak erişim sağlama ve bilgisayarda bulunan yazılım yada verinin yetkisiz olarak değiştirilmesi gibi faaliyetler sayılmıştır.

İngiliz Hukukunda bilişim suçlarına ilişkin düzenleme içeren anılan kanun haricinde yasa dışı olarak özellikle pornografi ve çocuk pornografisi alanlarında düzenlemeler yapılmıştır[165].

Diğer bir önemli hukuksal düzenleme ise 1998 tarihli “Veri Koruma Yasası(Data Protection Act)[166] dır.

İngiltere 2009 tarihinde kraliçenin emriyle yayınlanan ilk siber güvenlik stratejisi olma özelliğini taşıyan belge olan 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)[167] isimli

---

[164] İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü, Siber Güvenlik Raporu, Mayıs 2012, İstanbul, Burak Taşçı, Fransa ve AB İncelemesi, sy: 28-29

[165] AKARSLAN, Hüseyin, “Bilişim suçları”, Seçkin YayınlarıMayıs 2015, 2. Baskı, Üçüncü Bölüm, s.147

[166] https://www.legislation.gov.uk/ukpga/1998/29/contents

[167] Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space, June 2009, belgenin orjinaline

belge ile suç örgütleri ile düşman ülkelere karşı savunma planlarını içermekte olan ilk siber güvenlik stratejisini ortaya çıkartmıştır.

Strateji belgesi ile şirketler, hükümet ve kişilerin siber saldırılar karşısında risk altında olduğu açıklanış olup bu siber güvenlik stratejisi ile daha kapsamlı olarak hazırlanan Ulusal Siber Güvenlik stratejisi beraber yayımlanmıştır.

Bu siber güvenlik stratejisinde İngiltere'nin siber uzayının güvenliği ile dayanıklılığının sağlanması ve siber uzay tarafından sağlanan imkanlardan faydalanılmak amacı ile nelerin yapılabileceği açıklanmış, sadece devleti değil aynı zamanda vatandaş olan bireylerin de korunması gerektiği bu kapsamda tüm kesimler için dolandırıcılığın her çeşidi ile kimlik hırsızlığı ve teknoloji vasıtasıyla işlenebilen siber suçlara karşı korunmanın nasıl sağlanacağı açıklanmıştır.

Belgede dikkat çeken bir diğer özellik ise devlet ve şirket sırlarının nasıl korunacağı konusuna özel olarak değinilmiş olup bu kapsamda siber suç işleyen kişilerin gelecekte hedef olarak devletin yanında kritik önem arz eden sektör, enerji tesisi, ekonomik pazarlar ve parlamento birimlerini hedef alabileceği, teröristler tarafından sanal ortamın gençlerin radikalleşmesi için kullanıldığı belirli kesimlerin interneti kullanma yeteneklerinin artması ile yapabilecekleri siber saldırıların da çeşitlerinin artarak fazlalaşabileceği konusunda uyarıda bulunulmuştur.

Siber Güvenlik stratejisi siber alanın devlet ve terörist kullanımının yanı sıra suç amaçlı kullanımını siber güvenliğe üç temel tehditten biri olarak saymıştır. Siber Güvenlik stratejisinde, siber güvenliğin sağlanmasına yönelik genel yaklaşımın bir parçasını oluşturmak üzere bir Siber Suç Stratejisi yayınlanacağı belirtilmiştir.

İngiltere'nin 2010 tarihli Ulusal Güvenlik Stratejisi(A Strong Britain in an Age of Uncertainty: The National Security Strategy)[168]"nde ve Stratejik Savunma

---

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf adresinden erişilmiştir. (Erişim Tarihi: 01.11.2017)

[168] A Strong Britain in an Age of Uncertainty: The National Security Strategy, October 2010, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf(Erişim Tarihi: 05.11.2017)

ve Güvenlik Gözden Geçirmesi(The Strategic Defence And Security Review: Securing Britain İn An Age Of Uncertainty)[169] belgesinde 5 yıllık süreçte gelecek güvenlik açısından alınması gereken önlemler kapsamında en öncelik arz eden dört temel konu belirlenmiştir. Buna göre bu dört önemli alandan biri devlet, organize suç örgütleri ve terörist gruplar tarafından gerçekleştirilmesi muhtemel siber saldırılar olarak belirlenmiştir[170].

Bu strateji belgesi kapsamında ulusal güvenlik risk değerlendirmesinin her 2 yılda bir olacak şekilde gözden geçirilmesi öngörülmüş olup Ulusal Güvenlik Kurulunun öncelik sıralamasına göre üç kategoride sıralanmış olan on beş risk faktörü belirlenmiştir.

Bu kapsamda Birinci Kategoride Bulunan Riskler arasında İngiltere'nin bilişim sistemlerine yönelik saldırılar riski belirlenmiş, halihazırda siber suçlar sebebi ile uluslararası boyutta meydana gelen 1 trilyon dolara yakın olduğu ve 2012 yılında Londra da düzenlenecek olan Olimpiyatlar Oyunlarının önemli bir hedef haline geldiği belirtilmekte olup suç örgütleri tarafından halihazırda Olimpiyat Oyunlarıyla ilgili olarak 9500 adetin üzerinde internet adresi oluşturduğu 2008 yılında Pekin'de düzenlenen Olimpiyatlar zamanında günlük ortalama olarak 12 milyon siber saldırı meydana geldiği ifade edilmiştir. Siber saldırılar incelendiğinde kamu kurum ve kuruluşları, askeri ve endüstriyel alan ile iktisadi hedeflere kritik hizmetlerin kesintiye uğramasına sebep olabilecek şekilde zarar verebileceği bunun yanında terörist unsurlarının internet ortamı üzerinden örgütlenmesi ve bu ortamın iletişim ve propaganda eylemleri amacıyla kullanılmakta olduğu belirtilmiştir.

Stratejik Savunma ve Güvenlik Gözden Geçirilmesi ve Ulusal Güvenlik Stratejisi kapsamında Ulusal Siber Güvenlik Programı oluşturulmuş ve 4 yıllık program için 650 milyon sterlin bütçe ayrıldığı belirtilmiştir.

---

[169] The Strategic Defence And Security Review: Securing Britain İn An Age Of Uncertainty, October 2010 belgenin orjinaline https://www.gov.uk/government/publications/the-strategic-defence-and-security-review-securing-britain-in-an-age-of-uncertainty adresinden erişilmiştir.

[170] A Strong Britain in an Age of Uncertainty: The National Security Strategy, October 2010, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf (Erişim Tarihi: 05.11.2017)

Birinci Kategoride bulunan risklerin 5 yıllık sürede gerçekleşme ihtimallerinin ve etki alanlarının yüksekliği dikkate alındığında bu kategori risklerin ulusal güvenlik meselesi olduğu ve öncelik oluşturduğu kabul edilmiştir. Bu kapsamda siber saldırıları en yüksek risk grubunda değerlendirilmiştir.

Ulusal Güvenlik Stratejisi Raporunda başkaca ülkeler tarafından İngiltere'ye siber saldırıların düzenlendiği belirtilmiş ve siber güvenlik meselesinin 5 yıllık süreçte en yüksek derecede ulusal güvenlik meselesi ve ulusal güvenlik risklerinden biri olarak değerlendirilmesinin gerekliliği üzerinden önemle durulmuştur[171]. (KINIKOĞLU, 2012)

Hükümet tarafından Haziran 2009 yılında yayınlanan Güvenlik Stratejisi yayınlanması üzerine Hükümet genelinde stratejik liderlik sağlamak ve Birleşik Krallık Siber Güvenlik Stratejisinin dağıtımını geliştirmek ve koordine etmek için Siber Güvenlik Ofisi Kurulmuştur[172].

2009 tarihli Siber Güvenlik stratejisinde, siber güvenliğin sağlanmasına yönelik genel yaklaşımın bir parçasını oluşturmak üzere bir Siber Suç Stratejisi yayınlanacağı belirtilmiş olup 2010 yılında Siber Suç Stratejisi (Cyber Crime Strategy) yayınlanmıştır.

Bu strateji belgesi ile Hükümet tarafından Haziran 2009 yılında yayınlanan Güvenlik Stratejisi yayınlanması üzerine Hükümet genelinde stratejik liderlik sağlamak ve İngiltere Siber Güvenlik Stratejisinin dağıtımını geliştirmek ve koordine etmek için Siber Güvenlik Ofisi kurulmuş olup İç İşleri Bakanlığı ile siber suçla mücadele politikalarının geliştirilmesi ve İngiltere'nin menfaatleri üzerindeki etkisi ve özellikle vatandaşa yönelik ortak çalışma yürütmeye başlamıştır.

Strateji belgesinin amacı ile Siber güvenlik ofisinin 2009 tarihli Güvenlik Stratejisi politikasını koordine etmek ve yerine getirmek için planını ortaya

---

[171] Bkz.İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü, Siber Güvenlik Raporu, Mayıs 2012, İstanbul, Batu Yakup KINIKOĞLU: Birleşik Krallık İncelemesi , sy: 30

[172]Bkz.Cyber Crime Strategy , March 2010, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf (Erişim Tarihi: 06.11.2017)

konulmuş olup diğer departmanlar ve ajanslarla birlikte çalışılması gerektiğini, özellikle değişen tehditlere ayak uydurmak için Siber Suç Stratejisinin gelişmeye devam etmesini ve ayrıca Siber Güvenlik Ofisi bünyesinde gelişen işle tutarlı kalmasını sağlamaktır. Dolayısıyla İç İşleri Bakanlığının düşüncelerine katkıda bulunmak için Siber Güvenlik ofisi ile yakından çalışacaktır ve bu Siber Suç Stratejisi, Ulusal Güvenlik Stratejisi ve İngiltere Siber Güvenlik Stratejisi üzerinde olgunlaşan çalışmalarla tutarlılık sağlamak için 6 ayda bir gözden geçirileceği belirtilmiştir.

Bu belge, İç İşleri Bakanlığının Siber suçla mücadele konusundaki yaklaşımını ortaya koymakta olup ve doğrudan bir kolluk kararıyla ve tepkisi ile bu tür suçlarla mücadele edileceği ve dolaylı olarak hükümetler arası çalışma, endüstri, hayır kurumlarıyla ilişkilerin geliştirilmesi yoluyla diğer gruplar ve uluslararası alanda nasıl müdahale edileceğini göstermektedir.

Ayrıca Strateji belgesi ile internetin düzenlenmesi ya da internet üzerindeki içerik gibi konularda üstesinden gelmek için halihazırda yapılmakta olan çalışmaları üzerinde çalışmayacağı belirtilmiştir[173].

Kasım 2011'de İngiltere tarafından "Birleşik Krallık Siber Güvenlik Stratejisi: Dijitalleşen Dünya'ya Birleşik Krallığı Taşımak ve Korumak" isimli yeni bir strateji blegesi yayınlamıştır[174]. Bu strateji belgesi ile Ulusal Siber Güvenlik Programı ve ayrıntıları belirlenmiştir.

Ulusal Siber Güvenlik Programı ile İngiltere'nin siber güvenliği alanında köklü değişiklikler yapılmış ve bu kapsamda birçok yeni kurum oluşturulması için çalışmalara başlanmış olup program için ayrılmış olan 650 milyon pound bütçenin

---

[173]Bkz.Cyber Crime Strategy , March 2010, .https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf(Erişim Tarihi: 06.11.2018)

[174] Bkz.The UK Cyber Security Strategy: Protecting and Promoting The UK in a Digital World, November 2011 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (Erişim Tarihi: 07.11.2018)

%59'u İngiltere'nin üç istihbarat ve güvenlik kuruluşu olan MI6, MI5 ve GCHQ para sağlayan fona, kalan %14'lük kısmı da Savunma Bakanlığı'na ayrılmıştır[175].

Bu strateji belgesi ile siber alana olan bağımlılığın artması ile arttırmanın yeni fırsatlar getirmesinin yanı sıra yeni tehditlerde meydana getirdiği, siber alanın açık pazarları ve açık toplumları beslerken, bu açıklığın , kritik veri ve sistemlere zarar vermek veya zarar vermek suretiyle ülkeye zarar vermek isteyen, suçluları, bilgisayar korsanları, yabancı istihbarat servislerine karşı daha savunmasız bırakabileceğini ve bu tehditler açıklanmıştır. Ayrıca Strateji belgesi ile Hükümetin 2015'te İngiltere'deki siber güvenlik vizyonuyla sonuçlanmasını istediği noktalar ortaya konmuştur.

Bu strateji belgesi ile İngiltere'nin 2015 yılı siber güvenlik vizyonunda 4 ana hedefi ortaya konmuş olup bu kapsamda birinci hedef siber suçlarla mücadele edilmesi ve siber alanda iş yapabilmek için dünyadaki en güvenli yerlerden biri haline gelmektir. İkinci hedef ise siber saldırıların karşısında daha dayanıklı olmak ve siber alana olan ilginin daha iyi korunmasıdır. Üçüncü hedef halkın güven içinde kullanabileceği ve açık toplumların desteklendiği istikrar sahibi, canlı ve açık bir siber alan şekillendirilmesine yardımcı olabilmek olan belirlenmiştir. Son olarak ise dördüncü hedef ise alınacak tüm siber güvenlik önlemleri ve hedeflerinin desteklenmesi amacıyla gerek duyulacak olan bilgi ve beceri ile yeteneğe sahip olunması olarak belirlenmiştir.

İngiltere siber güvenlik alanında korunması gereken grupları ve siber güvenlik stratejisini üç temel grup bazında değerlendirmiştir. Bu değerlendirme kapsamında siber saldırıların karşısında devlet ve devlet kurumları ilk korunması gereken gruptur. Diğer korunması gereken grup ise siber alan içerisinde iş veya işlem yapmakta olan özel sektör olup korunması gereken son grup ise halktır.

---

[175] Bkz. İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü, Siber Güvenlik Raporu, Mayıs 2012, İstanbul, Batu Yakup KINIKOĞLU: Birleşik Krallık İncelemesi, sy: 30

Siber Güvenlik Stratejisi raporunda internetin halihazırda gösterdiği gelişim değerlendirdiğimde mevcut tehditlerinde bu gelişim çerçevesinde değiştiği belirlenmiş ve mevcut tehditlerin dört kategori olarak ayrımı yapılmıştır. Buna göre ilk kategoride bilişim sistemlerine yönelik veya bilişim sistemi vasıtasıyla suç işleyen suçlular bulunmaktadır. İkinci kategoride ise diğer devletler bulunur. Bu kapsamda ikinci kategoriyi terörist gruplar oluştururken son ve dördüncü kategoride Kamu ve özel sektöre yönelik saldırı gerçekleştiren ve politik nedenlerle saldıran Hacktivist denen gruplar bulunmaktadır[176].

İngiltere bu belirlediği tehditlere karşı kurduğu siber güvenlik stratejisinde tehditlerin sahip oldukları motivasyonun ve yeteneklerinin azaltılarak siber altyapılara ve hizmetlere yönelik mevcut tehditlerin azaltılmasının sağlanması, tehditleri oluşturan aktörler hakkında bilgi toplanılması bu surette mevcut bilginin ve yetenek ile karar verebilmenin geliştirilmesi, teknik yetenek ve insan yeteneklerinin arttırılması ile kamudaki mevcut bilgi ve farkındalığın arttırılmasının sağlanması, bu hususlarda stratejiler ve doktrinler geliştirilmesi ve bunların uygulanmasının sağlanmasıdır[177]. (KINIKOĞLU, 2012)

Bu strateji belgesi ile yukarıda açıklanan 4 amaca ulaşmak için halka/kişilere, özel sektöre ve devlete düşen görev ve sorumluluklar şu şekilde açıklanmıştır.

Halka ve kişilere düşen görevler; insanların, çevrimiçi tehditler karşısında temel düzeyde korunmayı bilmesi ve karşılaştıkları çevrimiçi tehditlere karşı korunmak için doğru ve güncel bilgilere erişebilmesi, internete ve e-posta eklerine kişisel bilgi ve hassas veri eklenmemesi konusunda dikkatli olunması ve tanımadıkları gönderilerde verilen bağlantılara karşı temkinli davranılması, işte veya evde hileli web siteleri gibi tehditleri tanımlama ve bildirme konusunda

---

[176]Bkz. İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü, Siber Güvenlik Raporu, Mayıs 2012, İstanbul, Batu Yakup KINIKOĞLU: Birleşik Krallık İncelemesi , sy: 30-32

[177] Bkz.İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü, Siber Güvenlik Raporu, Mayıs 2012, İstanbul, Batu Yakup KINIKOĞLU: Birleşik Krallık İncelemesi , sy: 30-32

işbirliği içerisinde bulunulması, özel sektörle ve devletle ilgili yapılan işlemlerde şifrelerin korunması, yazılım ve işletim sistemlerinin, bilgisayarların mevcut tehditlerden korunması amacıyla antivirüs programları kullanılması ve gerekli güncellemelerin yapılmasının gereğinin anlaşılması, dünyanın her yerinde olduğu gibi siber alanda yapılan davranışlardan da sorumlu olunduğunun bilincinde olmak gibi üzerlerine düşen görevlerin bilincinde olarak bu görevlerin yerine getirilmesi ve siber uzayda üzerlerine düşen sorumlulukların bilincinde olarak görevlerini yerine getirmeleridir.

İngiltere'nin siber güvenliğinde önemli bir rol oynamakta olduğu ve siber ortamın büyük bölümü özel şirketler tarafından kullanılmakta olup bu kapsamında Özel Sektöre düşen görev; tehditlerden haberdar olarak siber alanı, ticari açıdan hassas bilgileri, fikri mülkiyet ve müşteri verilerini koruyacak şekilde kullanmak, Siber alanda karşılaşılacak tehditlerin önüne geçilebilmek ve karşılaşılan tehditleri aktif bir şekilde caydırabilmek için devlet ve kolluk kuvvetleri ile ortak çalışılması, siber güvenlik hizmetleri için oluşan talep kapsamında sermaye ve gelişim sağlamak, Özel sektöre gelecekte duyulacak ihtiyaç kapsamında siber güvenlik imkanlarının sağlanması amacı ile gerekli yatırımın yapılmasıdır.

Devletin üstlendiği görev ise üst düzey tehditlerin tespit edilmesi ve engellenmesi için kapasitenin arttırılması, Siber alanda uluslararası bir konsensüs oluşturulması için davranış normlarının şekillendirilmesine yardımcı olunması, Ulusal kritik altyapı tesisleri ve devlet sistemlerinin güvenlik açıklarının ve hassasiyetinin azaltılması, siber güvenlik uzmanları kadrosunun arttırılması ve geliştirilmesi, kanunun uygulanmasının sağlamlaştırılması amacıyla kolluk kuvvetlerinin güçlendirilmesi ve siber suçlarla mücadele edilmesi, Halkın farkındalığının arttırılması ve önlemenin geliştirmek, Özel sektörün farkındalığını arttırmak, İş olanaklarından faydalanmaktır[178].

---

[178]Bkz. The UK Cyber Security Strategy: Protecting and Promoting The UK in a Digital World, November 2011, sy: 22-23, belgenin orjinaline

Savunma Strateji belgesinde savunma Bakanlığı bünyesinde askeri alanda çalışması planlanan iki temel merkez kurulması planlanmıştır. Bunlar silahlı kuvvetler için siber savunma alanında çalışan Küresel Operasyonlar ve Güvenlik Kontrol Merkezi (Global Operations and Security Control Centre) ile 2012 yılında çalışmaya başlayan Siber operasyonlar Savunma Grubu (Defence Cyber Operations Group) dur.

Ayrıca Savunma alanında siber savunmayı geliştirmek için çalışacak Güvenlik Kontrol Merkezine bağlı olarak çalışacak "Joint Cyber Unit" isimli bir kuruluş bulunması ve bu kuruluşun siber alanda kullanılması olası yeni taktik ve teknikler geliştirilmesi amacıyla çalışması öngörülmüştür.

Strateji belgesi ile öncelikler;

• İngiltere'nin kritik ulusal altyapısı ve diğer ulusal çıkar sistemleri üzerinde odaklanarak, gelişmiş siber tehditleri tespit etme ve analizin geliştirilmesi,

• Bunun bir parçası olarak, gerçek bir ulusal yanıt oluşturulması,

• Üst düzey devlet destekli tehditlere karşı savunma ve onları caydırma ve bu teknolojilerin devlet dışı aktörler tarafından kullanılmasını önlenmesi,

• Siber ortamda davranış için uluslararası ilkelerin geliştirilmesi ve uygulanması ve diğer ülkelerle birlikte, tırmanma riskini azaltmak ve yanlış anlaşılmaları önlemek için pratik güven artırıcı önlemler konusunda çalışılması,

• İngiltere, siber suçlarla ilgili Budapeşte Sözleşmesini onaylanmış olduğundan siber suçların sınırlar dışında yargılanabilmesi ve siyasal suçluların güvenli limanlardan yoksun bırakılması için diğer ülkeleri uyumlu yasalar geliştirmeye ikna etmeye çalışılması,

• Siber suçların engellenmesi ve kovuşturulması için etkili bir hukuki çerçeve ve uygulama kabiliyetlerini sürdürülmesi ile siber suçların bildirilmesinin kolaylaştırılarak raporlamadan gelen istihbaratın etkin bir şekilde eyleme

---

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf adresinden erişilmiştir.
(Erişim Tarihi: 08.11.2017)

geçirilmesini ve halka tavsiyede bulunulmasının sağlanması ve uygun durumlarda çevrimiçi zorbalık veya internet dolandırıcılığı gibi siber suçlarla mücadele etmek için gerekli yaptırımların kullanılması,

• Hükümetin kendi sistemlerinde siber güvenlik konusunda en iyi uygulamanın modellenerek hükümete tedarikçilere güçlü standartlar konulması,

• Vasıflı siber güvenlik uzmanlarından oluşan bir kadro geliştirilerek yenilikçi çözümler üretmeye devam etmek için temel araştırma ve geliştirme ile birlikte bu alandaki önemini korunması,

• Anti- malware yazılımlarının düzenli olarak güncellenmesi gibi basit bir yöntemle sistem zayıflıklarından kaynaklanan saldırıların %80 oranında başarılı bir şekilde engellenmesi sağlanabileceğinden, önlemenin kilit önem taşıdığını, farkındalık yaratmak ve çevrimiçi olarak kendilerini korumak için insanlara ve eğitime yetki verecek çalışmaların yapılması,

• İngiliz ticaretini yurtdışında kazanabilir ve büyümeye katkıda bulunabilecek siber güvenlik ürünleri ve hizmetlerinde gelişen bir pazar yaratılacağı ve İngiltere'yi siber alanda iş yapmak için iyi bir yer olarak tanıtılmasını sağlanacağı

şeklinde belirlenmiştir[179].

ENISA tarafından yayınlanan 2012 tarihli Ulusal Siber Güvenlik Stratejileri- Siber ortamda güvenliği artırmak için ulusal çabalar için yol belirlenmesi"(National Cyber Security Strategies Setting The Course For National Efforts To Strengthen Security İn Cyberspace) isimli raporda İngiltere'nin ulusal stratejisi değerlendirilmiş olup; İngiltere'nin yaklaşımının, İngiltere'yi, Bilişim ve internet Teknolojisi alanında yenilik, yatırım ve kalite olarak önemli bir ekonomi haline getirmek ve böylece siber dünyanın potansiyelini ve faydalarını tam olarak kullanabilmek için gelişen siber güvenlik alanıyla bağlantılı olarak ulusal hedeflere

[179]Bkz. The UK Cyber Security Strategy: Protecting and Promoting The UK in a Digital World, November 2011 , sy 26 belgenin orjinaline https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf adresinden erişilmiştir. (Erişim Tarihi: 08.11.2017)

odaklanmakta olduğu, İngiltere'nin stratejisindeki amacın siber alanı vatandaşlar ve işletmeler için güvenli bir alan haline getirebilmek için suçluların, teröristlerin ve devletlerin siber saldırıları gibi siber tehditlerle mücadele etmek olduğu belirtilmiştir[180].

Daha sonra Aralık 2012 tarihinde Ulusal Siber Güvenlik Stratejisinde belirlenen amaçlara ilişkin ilerleme raporu (Progress Against The Objectives Of The National Cyber Security Strategy)[181], 2013 yılı Aralık ayında Ulusal Siber Güvenlik Stratejisi 2013: Gelecekteki Planlar ve Başarılar (National Cyber Security Strategy 2013: Forward Plans And Achievements)[182] isimli ilerleme raporu, 2014 Aralık Ayında Ulusal Siber Güvenlik Stratejisi 2014: İlerleme Ve İleriye Dönük Planlar(National Cyber Security Strategy 2014: Progress And Forward Plans)[183] isimli ilerleme raporu yayınlanmıştır.

Mayıs 2015 güncellenen İngiltere 2010- 2015 Hükümet Politikası: Siber Güvenlik (2010 To 2015 Government Policy: Cyber Security)[184] isimli politika belgesi yayınlamıştır.

Hükümetin 2015 tarihli PwC tarafından gerçekleştirilen bilgi güvenliği ihlalleri anketine göre, büyük İngiliz kuruluşlarındaki siber güvenlik ihlallerinin ortalama maliyetinin 1.4 milyon pound ile 3.14 milyon pound arasında bulunduğu, İngiltere'de bulunan küçük işletmelerin % 74'ünün bilgi güvenliği konusunda

---

[180]Bkz. ENISA, National Cyber Security Strategies Setting the course for national efforts to strengthen security in cyberspace , May 2012, raporun orjinaline https://www.enisa.europa.eu/publications/cyber-security-strategies-paper adresinden erişilmiştir. (Erişim Taihi : 15.11.2018)

[181]Bkz.Progress against the Objectives of the National Cyber Security Strategy – December 2012, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/265401/Cyber_Security_Strategy_one_year_on_achievements.pdf (Erişim Tarihi : 15.11.2017)

[182]Bkz. National Cyber Security Strategy 2013: Forward Plans And Achievements , December 2013 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/265386/The_National_Cyber_Security_Strategy_Our_Forward_Plans_December_2013.pdf (Erişim Taihi : 15.11.2017)

[183]National Cyber Security Strategy 2014: Progress And Forward Plans, December 2014, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf (Erişim Tarihi : 15.11.2018)

[184]Bkz.2010 To 2015 Government Policy: Cyber Security,May 2015, https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security (Erişim Tarihi : 15.11.2018)

sorun yaşamış olduğu ve bu sorunların 75 bin ile 310 bin sterlin arasında zarar meydana getirdiği tespit edilmiştir[185].

Büyük şirketlerin% 81'i ve küçük işletmelerin% 60'ı 2014'te bir siber ihlali bildirdi. En büyük siber güvenlik ihlalinin maliyeti, büyük işletmeler için £ 1.000.000 ila £ 1.15 milyon arasında ve küçük olan işletmeler için £ 65.000 ila £ 115.000 arasında olacağı tahmininde bulundu. hükümet işletmelerin korunması için yeni yollara bakmalı ve İngiltere'yi siber saldırılara ve suçlara karşı daha dayanıklı hale getirmelidir[186].

2015 yılında İngiltere tarafından küçük ve orta boy işletmeler için siber dayanıklılığın güçlendirilmesi amacı ile yaklaşık olarak 1,5 milyon dolar değerinde destek verileceği, internetten gerçekleşmekte olan ticaretin güvenli bir şekilde yapılmasının sağlanmasını siber güvenlik stratejisinin temeline oturtan İngiltere destek kapsamına her alanda faaliyet göstermekte olan ve online varlığı bulunan küçük ve orta boy işletmelere 7,500 dolara kadar destek verileceğini ve desteği alacak firmaların siber güvenlik danışmanlığı da alabilmesini öngörmüştür[187].

Nisan 2016 da Birleşik Krallık Siber Güvenlik Stratejisi 2011-2016: Yıllık Rapor (The UK Cyber Security Strategy 2011-2016: Annual Report)[188] isimli rapor, Kasım 2016'de İngiltere'nin son siber güvenlik stratejisi belgesi olan Ulusal Siber Güvenlik Stratejisi 2016 – 2021 (National Cyber Security Strategy 2016 to 2021)[189] strateji belgesi yayınlanmıştır.

---

[185]Bkz.http://www.computerweekly.com/news/4500247376/Cost-of-UK-cyber-breaches-up-to-314m adresinden erişilmiştir. (Erişim Tarihi : 16.11.2018)

[186]Bkz.2010 To 2015 Government Policy: Cyber Security,May 2015, https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security adresinden erişilmiştir. (Erişim Taihi : 16.11.2018)

[187]Bkz.https://siberbulten.com/strateji-guvenlik/ingiltereden-kobiler-icin-siber-guvenlik-destegi/ (Erişim Tarihi: 17.11.2018)

[188]Bkz. The UK Cyber Security Strategy 2011-2016: annual report , April 2016 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf adresinden erişilmiştir. (Erişim Tarihi : 17.11.2018)

[189]Bkz. National Cyber Security Strategy 2016 to 2021, September 2017 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf adresinden erişilmiştir. (Erişim Tarihi : 17.11.2018)

Aralık 2016 da Siber Güvenlik Düzenlemesi ve Teşvikler İnceleme (Cyber Security Regulations and Incentives Review)[190] isimli inceleme belgesi yayınlanmıştır.

Ulusal Altyapı Koruma Merkezi (Center for the Protection of National Infrastructure, CPNI) tarafından güvenliğe dair mevcut tehditler kapsamında tehditlere cevap olarak verilecek tepkinin belirlenmesi ve durum yönetiminin sağlanması için gerekli tavsiyeleri vermek amacıyla kritik altyapıların sahipleri ve işletmecileri için Müşterek Güvenlik Olayları Müdahale Ekibini (Computer Securtiy Incident Response Team- CSIRT- UK) oluşturmuştur[191].

Mart 2014'te İngiltere Ulusal Bilgisayar Acil Müdahale Ekibi (UK National Computer Emergency Response Team, CERT-UK) kurulmuş olup CERT-UK, İngiltere'nin ulusal siber güvenlik olaylarına karşı hazırlıklı olmasını sağlamak ve hazırlığın koordinasyonunda sorumlu olup görevi devlet kurumları ve endüstriyel ortaklarla tatbikatlar düzenlemek ve özel sektör ve akademik kuruluşlar ile bilgi paylaşımının sağlanmasıdır.

Şubat 2017 de Sivil Nükleer Siber Güvenlik Stratejisi (Civil Nuclear Cyber Security Strategy)[192] yayınlanmıştır.

2016 yılının Kasım ayında İngiltere'nin beş yıllık Ulusal Siber Güvenlik Stratejisi açıklanmış ve siber güvenlik alanında 1.9 milyar sterlin yatırım yapılmıştır. Ekim 2016'da İngiltere'nin Ulusal Siber Güvenlik Merkezi (National Cyber Security Center- NCSC) kurulmuş olup 14 Şubat 2017 yılında Kraliçe tarafından resmi açılışı yapılmıştır. "İngiltere'yi siber saldırılar konusunda en zorlu hedef" haline getirmek amacıyla kurulan merkez İngiltere'nin istihbarat

---

[190]Bkz.Cyber Security Regulations and Incentives December 2016, Review) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/579442/Cyber_Security_Regulation_and_Incentives_Review.pdf adresinden erişilmiştir. (Erişim Tarihi : 17.11.2018)

[191] Bkz.http://www.csirt.org adresinden erişilmiştir. (Erişim Tarihi : 17.11.2018)

[192]Bkz.Civil Nuclear Cyber Security Strategy, February 2017, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/591619/170213_-_Civil_Nuclear_Cyber_Security_Strategy.pdf (Erişim Tarihi : 18.11.2018)

teşkilatlarından siber güvenlikten sorumlu Hükümet İletişim Merkezi'nin (GCHQ) bir parçası olarak halka daha açık ve erişimin kolay bir merkez olarak görev yapması öngörülmüştür.

Merkezin vatandaşlara ve kuruluşlara teknolojik gelişme ve tavsiyeler yoluyla, kritik hizmetlerimizi siber saldırılardan korumak, büyük olayları yönetmek ve İngiltere İnternet'inde yatan güvenliği iyileştirmek için kurulmuş olup amacı İngiltere'yi yaşamak ve çevrimiçi ticaret yapmak için en güvenli yer haline getirmeye yardımcı olmaktır[193].

İngiliz hükümeti tarafından İngiltere'nin ayda 60 ciddi siber saldırı yaşadığı ve 2016 yılının aralık ayından itibaren 2.ve 3. kategorilerde 188 siber saldırı düzenlendiği açıklanmış olup birinci kategori saldırılar en yüksek düzeydeki tehditler oluşturmaktadır. Saldırgan devlet aktörlerinin saldırıları sonucu önemli oranda kişisel verileri ve kritik önemdeki ulusal altyapı bilgilerini kaybedilmiştir. NCSC, hükümet ve iş dünyasına yöneltilen saldırıların yanı sıra ekonomi ve toplumu da korumayı hedefi ile kurulmuştur. Ayrıca Ulusal Siber Güvenlik Merkezi, siyasi partilere ve milletvekilleri gibi önemli makamlarda bulunan kişilere hassas bilgilerini nasıl korumaları gerektiğine yönelik tavsiyelerde de bulunması kararlaştırılmıştır[194].

Kasım 2016'de İngiltere'nin son siber güvenlik stratejisi belgesi olan Ulusal Siber Güvenlik Stratejisi 2016 – 2021 (National Cyber Security Strategy 2016 to 2021)[195] strateji belgesi yayınlanmış olup bu strateji belgesinde; 2021 yılına kadar İngiltere'nin siber güvenlik vizyonu siber tehditlere karşı güvenilir , olmak, saldırılar karşısında çabuk toparlanmak, sağlam durmak Olarak belirlenmiştir. Bu vizyonun sağlanabilmesi için 3 temel başlıkta hareket edecekleri öngörülmüştür. Bu başlıklar Savunma, Caydırma ve Gelişmedir.

---

[193]Bkz.https://www.ncsc.gov.uk/information/about-ncsc adresinden erişilmiştir. (Erişim Tarihi : 18.11.2018)
[194]Bkz. http://www.bbc.com/turkce/haberler-dunya-38967467(Erişim Tarihi : 19.11.2018)
[195] National Cyber Security Strategy 2016 to 2021, September 2017 belgenin orjinaline https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf adresinden erişilmiştir. (Erişim Tarihi : 19.11.2017)

Özetle bu başlıklarda;

Savunma başlığı altında sivil, çalışan ve kamu sektörünün kendilerini savunmak için gerekli bilinci kazanmaları gerektiği, İngiltere'yi siber tehditlere karşı korumak, olaylara etkili bir şekilde tepki vermek ve İngiltere ağları, veri ve sistemleri korumalı ve esnek olmasını sağlamak için araçlara sahip olduklarını ve Vatandaşlar, işletmeler ve kamu sektörü kendilerini savunma bilgi ve becerisine sahip oldukları belirtilmiş,

Caydırma başlığında İngiltere'nin, siber alanda her türlü saldırganlık için zor bir hedef olacağı, suçluları takip etmek ve kovuşturmak için aleyhlerinde yapılan düşmanca eylemi tespit edecekleri, anlayacakları, araştıracakları ve bozacaklarını, gerek gördüklerinde siber alanda saldırganca hareket etmek için yeterli araçlara sahip olduklarını,

Geliştirme başlığında ise bilimsel araştırma ve geliştirmeler tarafından desteklenmekte olan bir siber güvenlik alanına sahip olduklarını, kamu ve özel sektörlerdeki ulusal ihtiyaçlarını karşılamak için kendi kendini idame ettirecek bir boru hattına sahip olduklarını, üstün analiz ve uzmanlıklarının İngiltere'nin gelecekteki muhtemel tehdit veya tehditleri karşılamasını ve üstesinden gelmesini sağlayacağı belirtilmiştir [196].

Belge kapsamında internet bankacılığı vasıtasıyla yapılan dolandırıcılık oranının %64 oranında artış göstererek 133.5 milyon sterline yükseldiği belirtilmiştir.[197]

Yukarıda özetlenen tüm strateji belgeleri ve raporları neticesinde İngiltere'de Siber güvenlik alanında yaşanan gelişmeler şu şekilde özetlenebilir.

Farkındalık oluşturmak amacıyla "The Devil's in Your Details" isimli bir kampanya başlatılmış olup kampanya kapsamında dört milyon kişi bilgilendirilmiş ve birçok devlet kuruluşu bünyesinde siber suçla mücadele için birimler

[196]Bkz. http://sibertehdit.com/ingiltere-siber-guvenlik-stratejisi/ .(Erişim Tarihi: 18.11.2018)
[197]Bkz. National Cyber Security Strategy 2016 to 2021, September 2017 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

kurulmuştur. Bu birimler tarafından 15.000 i aşkın internet sitesi sahtecilik yapmaktan kapatılmıştır.

60 farklı ülkeden gelen 700 ü aşkın kişinin London Conference on Cyberspace gerçekleştirilmiş olup devlet ve özel sektör ortakları ortak katkıları ile "Get Safe Online Week" faaliyeti uygulanmıştır. Faaliyet kapsamında her yıl ekim ayı Küresel Siber Güvenlik Ayı ilan edilmiştir.

2014 yılı içeresinde The Bank of England isimli bir İngiliz bankası siber güvenliğin arttırılması amacıyla etik hackerların istihdam edilmesine karar vermiştir. Ayrıca hackerlar tarafından son bilinen uygulamalar kapsamında İngiltere Merkez Bankası, İskoçya Merkez Bankası ile birlikte Londra Borsasına güvenlik testi olan pentest uygulanması kararı alınmış olup İngiltere Merkez Bankasının yanı sıra hackerlerın en son yöntemlerle pentest yapılacağı bunlar haricinde 20 bankaya daha hizmet verileceği dışında belirtilmiştir[198].

2011- 2016 yılları arasında İngiltere Hükümeti tarafından 2011 tarihli Siber Güvenlik stratejisinde belirtilen Ulusal Siber Güvenlik Programı kapsamında belirlenen Siber suçlarla mücadele etmek ve İngiltere'yi siber alanda ticaret yapmak için dünyanın en güvenli yerlerinden biri haline getirmek, İngiltere'yi siber saldırılara karşı daha esnek hale getirmek ve siber alanda hakları korumak, açık toplumları destekleyen açık, canlı ve istikrarlı bir siber alanı şekillendirmeye yardımcı olmak ve İngiltere'nin siber güvenlik bilgi, beceri ve yeteneklerini oluşturarak geliştirmek hedeflerine ulaşmak için 860 milyon pound harcanmıştır[199].

Siber Saldırılarla ilgili 10 Bölgesel Bilgi Paylaşım Grubu ve 1750'den fazla kuruluş, Sanayi ve Hükümet için Siber Güvenlik Bilgi Paylaşım Ortaklığı (Cybersecurity Information Sharing Partnership –CISP) kurulmuştur.

---

[198]Bkz.https://siberbulten.com/strateji-guvenlik/ingiltere-merkez-bankasi-hacker-istihdam-edecek/ Erişim Tarihi: 18.11.2018)

[199]Bkz. The UK Cyber Security Strategy 2011-2016: annual report , April 2016 belgenin orjinaline https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf adresinden erişilmiştir. (Erişim Tarihi: 18.11.2018)

2000'den fazla Siber Temel Eğitim ve Gelişmiş eğitim sertifikaları yayınlanmış olup 77.000'den fazla kullanıcı, küçük işletmeler için Siber Temel Eğitim çevrimiçi eğitimini tamamlanmıştır.

"Siber Güvenlik İçin 10 Adım", "Siber saldırılar: Etkiyi Azaltma" ve "Küçük işletmeler: Siber güvenlik hakkında bilmeniz gereken şeyler" isimli siber saldırılardan korunma ve siber güvenlik için rehber yayınlanmıştır.

Siber güvenlik sektörü, 10 milyar sterlininden 17 milyar sterline büyüme kaydetmiş olup Siber Güvenlik alanında mevcut olan 80 şirkette 100 bine yakın kişi istihdam edilmiştir.

İngiltere Gelir ve Gümrük idaresi (HMRC) tarafından, 2014-2015 yılları arasında hükümet sistemlerinden 103 milyon poundluk dolandırıcılık girişimi önlenmiştir.

Ulusal Suçlar Ajansı bünyesinde Ulusal Siber Suçlar Birimi kurulmuş olup ciddi siber suçları engellemek için yerli ve yabancı olmak üzere 170 operasyon yapılmıştır.

Dokuz Bölgesel Organize Suç Birimi'nin her birinde bir Siber Birim kurulmuştur.

Ulusal olaylar ve uluslararası CERT irtibat bürosu ile ortaklaşa çalışacak Bilgisayar Acil Müdahale Ekibi (CERT- UK) oluşturulmuştur.

Merkezi hükümet birimleri ve Kamu Hizmetleri Ağı'ndaki 400'den fazla kamu organı siber saldırıları önlemede görev yapmıştır.

Dijital devlet hizmetleri kullanırken kullanıcıların kimliğini güvenli bir şekilde doğrulamanın yeni bir yolu olarak GOV.UK Doğrulama sistemi oluşturulmuş olup test aşamasında bu sistemle yarım milyon kimlik doğrulaması yapılmıştır.

40'tan fazla devlet dairesi ve ajansı için siber tehdit ve zayıf noktaların değerlendirilmesini sağlayan Siber Değerlendirme Merkezi kurulmuştur.

Hükümet tarafından İnsan Kaynakları, Hukuk, Satın Alma gibi mesleklerde çalışanlar için Siber güvenlik e-eğitimleri hazırlanmıştır.

Bölgesel Organize Suçlarla Mücadele Birimleri (ROCUs), Polis Koleji ve Kral Savcılığın (CPS) siber suçla mücadelede ana akım polis güçlerini eğitilmiş olup 2015'te bir siber koruma ağı kurulmuştur.

Ekim 2016'da İngiltere'nin Ulusal Siber Güvenlik Merkezi (National Cyber Security Center- NCSC) kurulmuştur[200].

2.5. Çin

Çin'in Siber Güvenlik politikasından bahsetmeden önce Çin'le ilgili internet altyapısından bahsetmek gerekmektedir. Altın Kalkan Projesi adıyla bilinen Büyük Çin Güvenlik Duvarı (The Great Firewall) Çin hükümeti tarafından başlatılan dünyanın en büyük internet sansürü ve izleme sistemidir.

1980 li yıllarda Çin siyasetçisi Deng Xiaoping tarafından söylenen "*Temiz hava için pencereyi açıyorsanız, sineklerin içeri girmesini de göze alacaksınız*". Sözünden yola çıkılarak oluşturulan Great Firewall Çin'de internetin kullanılmaya başlanmasından 3 yıl sonra Halk Güvenliği Bakanlığı tarafından Great Firewall'ın ilk kuralı olan "ülke bütünlüğüne zarar veren, ülke sırlarını açıklayan, toplumda kargaşaya neden olacak söylemlerde bulunan, bahis, şiddet ve cinsellik içeren materyaller üreten, çoğaltan herkes suçlu kabul edilmesi" kuralının konulmuş, akabinde 1998′de ise "Çin Demokrasi Partisinin" faaliyetleri bir başka parti olan "Çin Komünist Partisi"nin engelleyemeyeceği boyutlara geldiğinde Komünist Partisinin diğer partinin bütün üyeleri için tutuklama emri çıkartmasıyla birlikte "Altın Kalkan Projesi**"** başlatılmıştır.

Bu proje kapsamında ülkedeki her türlü bilgi paylaşımının komünist partinin kontrol ve denetimi altında olması öngörülmüş olup bu kontrol ve denetimin sağlanması için gerekli proje kapsamında internetin güvenliği, videoların gözetlenmesi, insan yüz tanımlama sistemleri gibi birçok yüksek teknolojiye sahip

[200]Bkz. The UK Cyber Security Strategy 2011-2016: annual report , April 2016, belgenin orjinaline https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf adresinden erişilmiştir. (Erişim Tarihi.20.11.2017)

ürün satın alınarak bu sistem için 30.000 ile 50.000 arası polis görevlendirilmiştir. Bu proje ile birlikte internet üzerinde olan bütün yazılı, sesli ve görüntülü verilere ilişkin trafik sayıları on binleri aşan internet polisleri tarafından sürekli izlenmektedir.

Great Firewall kapsamında;

- İnternet üzerinde bulunan birçok siteye üye olunabilmesi için kimlik numarası girilmesi zorunludur.
- Çin'de yayın yapmakta olan bütün sitelerin İnternet İçerik Üreticisi Lisansı (ICP)almak zorunludur. Site sahibi resmi makamlara başvuru yaptıktan sonra sonuç olumlu ise sitenizin en altına yerleştirilmesi için özel bir kimlik numarası verilmektedir.
- İnternet üzerinde bulunan tüm forum sitelerinde, tüm video ve haber sitelerinde kullanıcı tarafından yapılan yorumların tamamı izlenmekte ve sisteme aykırı içeriklerin girilmesi durumunda içerik derhal internet polisi tarafından silinmektedir.
- Yasaklı kelime havuzu isimli sistemle havuzdaki kelimelerin geçtiği bütün web siteleri (bloglar) anında bloke edilmektedir. Herhangi bir web sitesi veya blokta hükümetin karşı olduğu karşı partinin bir üyesinin isminin yazılması halinde sistem, içeriğin yazıldığı sayfayı anında bloke edilmekte olup sayfaya ulaşılması mümkün değildir. Sayfa ancak "sakıncalı" içeriğin silinmesi ile tekrar ulaşılabilir duruma dönmektedir.
- İnternet kafeler gibi alanlardan internete giriş yaparken sisteme kimlik numarasının kaydedilmesi zorunluluğu olup bu sayede kimin, nerede ve kaç saat internete girdiği de kayıt altına alınmaktadır.
- Anlık mesajlaşmayı sağlayan programlar da sansür kapsamında olup sansür sistemi tarafından sakıncalı olarak önceden belirlenmiş kelimelerin yazılması halinde mesaj karşı tarafa iletilmemektedir.
- "Polis şiddeti", "Tiananmen olayı", "Özgürlük konuşması", "BBC Haberleri", "Amerikanın sesi" gibi kelimelere hiçbir sitede rastlanmamaktadır. Bu kelimelerin internette aratılması halinde dahi hiçbir içerik bulunamamaktadır.

- Çin'de Facebook, Twitter, Youtube gibi internet siteleri yasaklıdır. Bu tür sitelere olan ihtiyacı Çin kendi klonlarını yaratarak çözmüş olup Facebook yerine Renren, Twitter yerine Fanfou, Youtube yerine Youku gibi klon sitelere hükümetin de maddi destek vermekte ve böylece Facebook, Twitter, Youtube gibi sitelere olan ihtiyaç ortadan kaldırılmaya çalışılmaktadır.

Great Firewall'dan proxy ayarı veya DNS ayarı yapmak ile kurtulmak mümkün olmamakla birlikte Proxy siteleri ile programları da %90' oranında internet polisleri tarafından engellenmiştir[201].

1990'lı yılların ortalarında Çin, Körfez savaşından edindiği deneyimler doğrultusunda savaş stratejisinde değişikliğe gitmiş olup yeni stratejisi kapsamında ordusunu küçülterek yeni teknolojilere yatırım yapmaya başlamış olup savaş birlikleri kurulmuştur.

Çin, bilgi teknolojileri ile siber savaş alanında dünya üzerinde lider konumda bulunma hedefini açıkça dile getirmekte olup bu konu hakkında yaklaşık 20 yıldır strateji belgeleri, doktrinler ve raporlar yayınlamaktadır. Bu kapsamda kapsamda çeşitli politikalar geliştirmektedir. 1990 yılından itibaren Çin Ordusu "bilgileştirme" adı verilerek teknoloji çağına ayak uydurmak için bilgi teknolojileri ve siber uzay alanlarında etkin güç haline gelmeyi planlamaktadır.

Bunların yanında Çinde ordu eğitim merkezlerinde siber savaş eğitimleri verilmektedir[202].

2000 yılının başında, Çin'in Merkez Askeri Komisyonu tarafından araştırma yapılması talep edilmiş olup 2004 yılında Çin Ulusal Savunma Beyaz Kitabı

---

[201]Bkz.http://www.cinmacerasi.com/cinin-dev-internet-sansur-sistemi-nasil-calisiyor (Erişim Tarihi: 10.10.2017)

[202]Bkz. İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü, Siber Güvenlik Raporu, Mayıs 2012, İstanbul, Ahmed Furkan GÜL: Çin ve ABD İncelemesi, sy: 19-20

yayınlamıştır. Çin askeri doktrini, çatışmanın ilk evrelerinde siber ve elektronik savaş yeteneklerinin bir birlikte kullanılması gerektiği belirtilmiştir[203].

Bu kapsamda vatandaşlardan hacker gruplar oluşturulmuş, ABD'nin bilişim sistemleri, yazılım ve donanımları üzerinde siber casusluk yapılmış, siber savaşlar için askeri birlikler oluşturulmuş ve ABD altyapısına mantık bombaları yerleştirilmiştir[204].

Çin, hassas verilerin ülke dışına çıkması veya içeri girmesini engelleyen, ülke içerisindeki tüm internet trafiğini kontrol altına alan, aynı zamanda internet özgürlüğünü de engelleyen Altın Kalkan Projesi kapsamında Çin'in Great Firewall ve Yeşil Baraj (Green Dam)[205] projesi olmak üzere iki güvenlik sistemi kurmuştur. Bu iki sistemin en temel özelliği herhangi bir siber savaş tehdidi algılandığı zaman, Çin'i siber uzayını bloke ederek, dünyanın geri kalanından tecrit edebilmesine imkan sağladığından Çin'e büyük avantaj sağlamakta olup her iki projede Çin'in sahip olduğu askeri strateji ve siber güvenliği alanında hazırlanmakta olduğu olası bir siber savaşta Çin'e büyük avantajlar sağlayacaktır.

Altın Kalkan Projesi ve Çin'in Great Firewall'u kapsamında Çin Halk Cumhuriyeti sahip olduğu siyasi organizasyon ve ideolojisi neticesinde ülkenin güvenliği yanında siber güvenliği de büyük oranda ordunun denetimine bırakmış durumdadır[206]. (GÜL, 2012)

---

[203]Bkz. Birleşmiş Milletler Silahsızlanma Araştırmaları Enstitüsü (UNIDIR), James A. Lewis – Katrina Timlin, Siber Güvenlik ve Siber Savaş, Ulusal Doktrin ve Organizasyon Yapısının Ön Değerlendirmesi, Cybersecurity and Cyberwarfare", Center For Strategic and International Studies, 2011, sy. 8 belgenin orjinaline http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf adresinden erişilmiştir.

[204] Bkz.Clarke, Richard A. ; Knake, Robert K. , Siber Savaş, (Çeviren:murat Erduran), İkü Yayın Evi, Nisan 2011, s.33-34

[205] Bkz. Yeşil Baraj (Green Dam) projesi Çin devleti tarafından 2009 yılı itibariyle de başlatılmıştır. Bu proje ile internet trafiği akışı izlenmekte, yasaklı sitelere erişim engellenmekte ve en önemlisi de yabancı ülkeler tarafından bilgisayarlara yüklenmiş zararlı yazılımlar tespit edilebilmektedir .

[206] Bkz. İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü, Siber Güvenlik Raporu, Mayıs 2012, İstanbul, Ahmed Furkan GÜL: Çin ve ABD İncelemesi , sy: 18

Çin'in siber güvenlik ve askeri stratejisi beraber değerlendirildiğinde Çin'in tarafından siber güvenlik stratejisinin askeri stratejisi ile aynı önem derecesine sahiptir. Çin'in siber savaş kapasitesi ise kara, deniz ve hava gücü ile eşit önem derecesinde olduğu ve bu kuvvetler gibi ayrıca bir kuvvet olarak değerlendirilmektedir. Bu anlamda siber kaynaklı tehditlere karşı önlemler alınabilmesi amacıyla gerekli olan yazılım teknolojilerinin geliştirilmesi ve mevcut tehditlere karşılık karşıt saldırı ile cevap verme yeteneğine erişme hedefine sahiptir. Çin tarafından olası bir siber savaş durumunda bu savaşa hazır olabilmek için siber saldırı kapasitesi yüksek birimler kurulmakta ve bilişim altyapısını güçlendirilmesi için çalışmalar yapılmaktadır.

Çin'in siber stratejisi kapsamında genel olarak saldırgan siber savunma taktiği üzerine kurulu olduğu söylenebilir. Çin'e karşı tehdit olabileceği düşünülen ABD ve bir çok ülkenin ticari, askeri ve devlet ağlarına karşı siber saldırılar düzenlemek amacı ile detaylı planlamalar ve hazırlıklar yapmaktadır[207].

Çin'in siber güvenlik altyapısı incelendiğinde Çin Halk Kurtuluş Ordusu'na (People's Liberation Army – PLA) Genelkurmay Başkanlığı bünyesinde oluşturulmuş olan (General Staff Department- GSD)) 3. ve 4. Departmanlar, diğer kuvvetler ile uyumlu olarak ülke dışından gelen sinyali toplayarak ele geçirme ve analiz etmek, Çin sınırları içerisinde bulunan iletişim ağlarını kontrol altına alma, elektronik savaş, bilgi harekatı ve siber saldırılar uygulamak gibi görevleri olmasının yanı sıra ülkenin bilişim altyapısının korunmasından sorumludurlar.

Çin Halk Kurtuluş Ordusu Genelkurmay Başkanlığının 3. Departmanı ayrıca, Çin ordusunun sahip olduğu bilişim altyapısının ve ağların da güvenliğinden sorumlu olmakla sinyal istihbaratından sorumludur ve elektronik bilginin toplanmasına, analiz edilmesine ve kullanılmasından sorumludur. Bunun yanı sıra

---

[207]Bkz. Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalı, Uluslararası ilişkiler Programı, Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme, Yüksel Lisans Tezi, Barış Çeliktaş, Mayıs 2016, Trabzon, sy.67-69

3 adet araştırma kuruluşu da ülkenin siber güvenliğinin geliştirilmesi amacıyla sürekli olarak AR-GE çalışmaları yürütmekte ve Çin'in ileri gelen üniversiteleri de bu çalışmalara destek vermektedir[208]. (GÜL, 2012)

PLA Genel Kurmay Başkanlığının, elektronik karşı tedbirleri ve bilgi savaşı teknolojileri geliştiren araştırma enstitülerini denetleyen 4. Departman askeri birlikten sorumludur. Ayrıca, PLA, yeteneklerini geliştirmek için araştırma üniversiteleri ve kamu sektörü ile ilişkileri sürdürmektedir[209].

PLA bünyesinde bulunan bir başka birim de Birim 61398'dir. Bu birim 2006 yılında faaliyete geçmiş olup birçok batılı üst düzey firma ve devlet kurumuna karşı siber saldırılar yaptığı düşünülmektedir. Bu birim haricinde 2002 yılında kurulan ve yetenekli siber korsanlardan ve akademisyenlerden oluşan devlet adına çalışan hackerlardan oluşan "Gönüllü Bilgi Teknolojileri Milis Birimleri" başka bir ifadeyle İnternet Milis Birlikleridir. Bu gruba Çin'in siber ordusu denilmekte olup diğer devletlere Çin kaynaklı yapılan bir çok saldırının arkasında olduklarından şüphelenilmektedir[210].

PLA'nın yeni nesil savaş stratejileri arasında bulunan "Entegre İletişim Ağı Elektronik Harbi" (Integrated Network Electronic Warfare) stratejisi kapsamında muhtemel bir savaşta düşmanın bilişim sistemini çalışmaz hale getirmek amacıyla kullanılan siber saldırılar ve elektronik ve klasik savaş silahlarının birlikte kullanıldığı bir strateji izlemesi öngörülmüştür. Ayrıca bu strateji kapsamında PLA bünyesinde siber saldırılar karşısında ülkeyi korumakla görevli "Online Mavi Ordu" adı verilen ve düşmanın mevcut Komuta birimleri, Kontrol noktaları,

---

[208]Bkz. İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü, Siber Güvenlik Raporu, Mayıs 2012, İstanbul, Ahmed Furkan GÜL: Çin ve ABD İncelemesi , sy: 18

[209] Bkz.Birleşmiş Milletler Silahsızlanma Araştırmaları Enstitüsü (UNIDIR), James A. Lewis – Katrina Timlin, Siber Güvenlik ve Siber Savaş, Ulusal Doktrin ve Organizasyon Yapısının Ön Değerlendirmesi (
Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization Center for Strategic and International Studies),), 2011 ,sy. 8 belgenin orjinaline http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf adresinden erişilmiştir.

[210] Bkz. Dipnot 206

Haberleşme ağları, Bilgisayar sistemleri, İstihbarat ve Keşif- Gözlem Sistemleri içinde kör noktalar oluşturan, gerek duyulması halinde bu kör noktalar kullanılmak suretiyle bu sistemlere yönelik olarak elektronik savaş, sistemlerin karıştırılması ve uydu aracılığıyla saldırılar düzenlenmesi öngörülen bir saldırı birimi olarak görev yapmaktadır.

Bu kapsamda siber güvenliği ulusal güvenlik aktörlerinden biri olarak gören ve bu kapsamda hareket eden Çin, mevcut siber güvenliğini geliştirmek amacı ile ülkenin en iyi üniversiteleri ile düzenli olarak siber alanda Ar-Ge faaliyetleri yürütmekte, bu anlamda siber savaş, elektronik savaş ve uzay silahları için gerekli olan personelin eğitimi konusunda çok önem vermektedir. Siber güvenlik ve siber savaş alanında dünyanın en etkili gücü haline gelmek amacıyla stratejiler ve projeler üretilmesinin yanı sıra saldırgan savunma stratejisinin uygulanması kapsamında ordunun eğitildiği merkezlerde düşmanın bilgi ve iletişim teknolojilerine ve bilgisayar ağlarına zarar verilmesi ile ilgili konulara dayalı olarak siber savaş üzerine eğitimler vermektedir. Çinde siber ordusuna katkı sağlamak ve muhtemel bir siber savaşta etkinliğini arttırmak amacıyla yetenekli olan genç siber savaşçıların keşfedilmesi ve yetiştirilmesi amacı ile sürekli siber korsanlık üzerine yarışmalar düzenlemektedir[211].

Çin Saldırgan savunma stratejisi kapsamında Microsoft'un gizli işletim şifresini alarak dünya genelinde Cisco ve Microsoft'un yazılımlarını indirimli fiyatlara satmaya başlamış ve fabrika kurarak router denilen yönlendiricilerin korsan üretimine başlamıştır. Çin tarafından ucuza satılan yönlendiricilerin ABD askeri kuruluşları tarafından alındığı ortaya çıkması üzerine FBI tarafından yapılan bir soruşturma neticesinde bu cihazların olası bir siber savaş sırasında Amerikan askeri ağlarını çökertmek için kullanılabileceği ortaya çıkmıştır. Daha sonra Çin sahte Cisco üretimini durdurarak Huawei isimli kendi markasını yaratarak

[211] Bkz. Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü , Uluslararası İlişkiler Anabilim Dalı, Uluslararası ilişkiler Programı, Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme, Yüksel Lisans Tezi, Barış Çeliktaş, Mayıs 2016, Trabzon , sy.67-69

yönlendirici pazarına sokmuştur. Ayrıca Microsoft ve Cisco ürünlerindeki zayıf noktaları bilen Çin kendi gizli askeri bilişim sistemlerinde kullanmak için son derece sağlam ve kırılması imkansıza yakın olan Kylin isimli kendi işletim sistemini üretmiştir[212]. (CLARKE & KNAKE, 2011)

Çin Saldırgan siber savunma stratejisi kapsamında aldığı önlemlerin yanında saldırgan siber savaş silahları da üretmektedir. Buna göre Çin; siber alana bilgi mayınları yerleştirmiş, bilişim keşif unsurları geliştirilmiş, ağ verilerini değiştiren cihazlar üretilmiş, siber uzaya bilişim bombaları yerleştirilmiş, çöp bilgiler ile siber uzay doldurulmuştur. Ayrıca Çin tarafından propaganda dağıtım unsurları kullanılmaya başlanmış, bilişim yanıltma uygulamaları yapılmış, klon bilgiler dağıtılmış, bilişim savunması düzenlemeleri yürütülmüş ve ağ casus istasyonları kurulmuştur.

Castro hükümetinden izin alan Çin Küba'da iki tane ağ casusluğu istasyonu kurmuştur. Bu istasyonların birinden ABD'nin internet trafiğini izlerken diğer istasyondan ABD savunma Bakanlığının iletişim unsurlarını dinlemiştir.[213]

"PLA bünyesinde dünyadaki en hızlı süper bilgisayar sistemlerinden bazıları bulunmaktadır. Jiangnan Bilgisayar Teknolojileri Araştırma Enstitüsü (Jiangnan Computer Technology Research Institute) adıyla da bilinen 56. Araştırma Enstitüsü Çin'deki en eski ve büyük araştırma ve geliştirme organizasyonudur. Çok önemli süper bilgisayar yatırımları yapmakta ve bu süper bilgisayarlarla Çin'deki diğer bilgisayar merkezlerine ve PLA bünyesindeki organizasyonlara destek vermektedir. Burada yer alan süper bilgisayarlar sayesinde diğer ülkelerin kullandıkları karmaşık kodları ve şifreleri kırma çalışmaları hızlanmıştır.

Çin Komünist Partisi'nin resmi gazetesine göre, Çin hükümeti hackleme

---

[212] Bkz. Clarke, Richard A. ; Knake, Robert K. , Siber Savaş, (Çeviren:murat Erduran), İkü Yayın Evi, Nisan 2011, s.35

[213] Bkz. Clarke, Richard A. ; Knake, Robert K. , Siber Savaş, (Çeviren:murat Erduran), İkü Yayın Evi, Nisan 2011, s.35-36

suçlarının mahkemeler tarafından nasıl değerlendirildiği konusunda sıkı yaptırımlar getirmek için çalışmaktadır. Çin ayrıca online bilgi güvenliği ve siber suçların azaltılması gibi konulardaki hukuki yaptırımlarda değişiklikler yapılmasını önermiştir. 2010 yılında Çin, kullanıcıları siber veri hırsızlığı hakkında korumak amaçlı regülasyonlar getirmiş ve Çinli telekom şebekesi operatörü şirketlerin botnet'lere karşı savaşması ve domain alanları kaydı sırasında sahte isim veya kimlik kullanılmasını önlemek amaçlı ek düzenlemeler yürürlüğe koymuştur[214]."

Çin Askeri Bilimler Akademisinin 2013 tarihli Askeri Strateji Belgesinde ağ güvenliği ve ağ savaşlarının belgede önemli yer tutmakta olup[215] bu belge kapsamında Çin Ordusunda 3 çeşit ağ saldırı birimi bulunduğu ifade edilmiştir. Bunlar; Özel Askeri Network Savaş Gücü, Orduya Bağlı Sivil Organizasyonlar ve Sivil Kuvvetlerdir[216].

Çin Devlet Konseyi tarafından 26 Mayıs 2015'te yayımlanan Çin'in Askeri Stratejisi başlıklı belge, 1998'den beri yayımlanmış dokuz ulusal savunma belgesi arasında doğrudan askeri strateji odaklı ilk metindir. Belge; kamu ile paylaşılan ilk strateji belgesi olma özelliği ile birlikte aktif siber savunma ile ilgili tespitler içermektedir.

Belgede ilk kez ordu içerisinde saldırı olarak siber operasyon yapma kabiliyetine sahip siber birim kurma konusu resmi olarak açıklanmış olup hükümetinin ana hedefi bu kapsamından kendi sınırları içerisinde siber alanda tam egemenlik kurmak ve bunu iç ve dış tehditlere karşı savunmadır.

---

[214]Bkz. İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü, Siber Güvenlik Raporu, Mayıs 2012, İstanbul, Ahmed Furkan GÜL: Çin ve ABD İncelemesi, sy.19-20

[215]Bkz. The Chinese Military Updates China's Nuclear Strategy, Full report belgenin orjinaline http://www.ucsusa.org/sites/default/files/attach/2015/03/chinese-nuclear-strategy-full-report.pdf adresinde erişilmiştir. (Erişim Tarihi 11.10.2017)

[216]https://siberbulten.com/uncategorized/cin-yeni-askeri-stratejisini-acikladi-stratejide-savunma-operasyonda-saldiri/ (Erişim Tarihi: 11.10.2017)

Strateji belgesi kapsamında uzayın uluslararası rekabette yeni bir alan haline gelmesi sebebi ile tüm devletler tarafından uzay politikaları geliştirildiği, bu durumun uzayın silahlandırılmasına yönelik taşıdığı, Çin'in uzayın barışçıl bir ortam olmasından yana olduğu ancak bu alanda mevcut çıkarlarının da korunacağı ve uzay güvenliğine yönelen tüm tehditlere karşı mücadele verileceği belirtilmiştir. Bu kapsamda ekonomik ve sosyal ilerlemenin yeni temellerinden olan siber uzay içinde siber uzayın ulusal güvenlik alanı haline geldiği bu kapsamda bir çok ülke tarafından siber kuvvet oluşturulduğu belirtilmiş, Çin'in siber saldırıların başlıca kurbanlarından biri olduğu bu sebeple gerekli siber altyapının korunması amacıyla gerekecek tüm önlemlerin alınacağı bu kapsamda mevcut siber kuvvetlerinin güçlendirilmesi ve siber uzay alanına uyarı sistemleri geliştirilmesi ve yerleştirilmesi ile siber uzay alanının korunabilmesi amacıyla uluslararası boyuttaki alınan önlem ve eylemlere katılınacağı belirtilmiştir[217].

Strateji belgesinde 'stratejik rekabet alanı' olarak kabul edilen siber uzay alanında siber savunma birimi kurulacağı, Siber Savunma kapsamında saldırgan siber faaliyet geliştirilme konusunun destekleneceği Çin'in güvenlik stratejisinde stratejik seviyedeki savunmanın operasyon ve taktik seviyelerinde saldırgan adımlar atmayı gerekli kılabilecek şekilde esnetebileceği belirtilmiştir. Strateji belgesinde siber savunma bilgi güvenliği başlığının altında yer almaktadır[218]. (China's Military Strategy- Çin Askeri Stratejisi , 2015)

Çin tüm dünyada özellikle ABD ye yapılan siber saldırılarla adını duyurmuş olup Çin tarafından gerçekleştirildiği bilinen bazı siber saldırılar şunlardır;

- 2014 yılında Çin yönetimine yönelik olarak düzenlenen eylemlerle haberleşmek için WhatsApp isimli uygulamayı kullanan aktivistler, telefonlarına

[217]Bkz.http://www.bilgesam.org/incele/2111/-cin-in-yeni-askeri-strateji-belgesi/#.Whiuea3BJsM (Erişim Tarihi: 12.10.2017)
[218]Bkz. China's Military Strategy- Çin Askeri Stratejisi , May 2015 belgenin orjinaline http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm adresinden erişilmiştir.

protestoları daha rahat koordine etmeyi sağlayan bir program hakkında tanıtım mesajı ulaşmış olup tanıtım adresine tıklayan göstericilerin indirdiği programın, muhtemelen Çin hükümeti tarafından geliştirilmiş, kullanıcıların telefonlarını hackleyen zararlı bir yazılım olduğu ortaya çıkmıştır. Iphone'lardan bilgi çalabilen nadir rastlanan bir zararlı yazılım olan program Iphone'a yüklendiği andan itibaren telefondaki rehber, mesajlaşma, arama kayıtları ve fotoğraflara ulaşabildiği, telefondaki kayıtları oynatma ve bilgileri başka bir adrese gönderme kabiliyetine sahip olduğu ve İphonedaki uygulamalar, e-mail ve satın alma bilgilerinin bulunduğu anahtar dizinine erişebildiği tespit edilmiştir. Hem iOS işletim sisteminin hem de Android işletim sisteminin zayıf noktaları olmasına karşın İOS işletim sistemi ile çalışan telefonların hacklenmesi kolay olmamakla birlikte bu işlem mümkündür. İOS işletim sistemi eğer telefonlar Apple'ın koyduğu, ne tür uygulamaların çalıştırılacağına ilişkin, engelleri aşması için kırıldıysa, başka bir deyişle ''jailbrake'' sürecinden geçirildiyse hacklenmesi mümkündür. San Francisco'daki Lacoon Mobile Security şirketi tarafından müşterilerinin ağlarında olağan dışı trafik gözlemlenmesi üzerine bu sahte program incelemeye alınmış, şirket araştırmacıları tarafından zararlı yazılımın sinyal yolladığı site incelendiğinde yazılımın "emir komuta" sunucusunun Çince yazıldığını tespit etmiştir. Programla ilgili olarak şirketin CEO'su Michael Shaulov'a göre bu veriler hackerların Çin hükümeti ile çalışıyor olabileceklerini işaret ettiği belirtilmiştir. Dallas merkezli siber istihbarat şirketi iSight Partners'tan John Hultquist'e göre, program Çin istihbarat servisinin Tibetli aktivistleri hedef alan casusluk yöntemlerine benzediği ve 2013 yılında hackerların Çin'deki Uygur topluluğunun bir konferansa katılan üyelerine uygulama gibi görünen zararlı yazılım yolladığı, programı kullananların konferansla ilgili bilgileri gördüler, ancak yazılım arka planda telefon kayıtlarını ve telefonun mikrofonu ile çevrede konuşulanları kaydettiği belirtilmiştir[219].

[219]Bkz.https://siberbulten.com/strateji-guvenlik/cin-hong-kong-protestocularini-mobilden-vurdu/ adresinden erişilmiştir. (Erişim Tarihi :08.10.2017)

- 2015 yılında Çinli siber korsanlar tarafından Çin'de uygulanan internet kısıtlamalarının aşılmasına yardımcı olan bir Amerikan şirketi'ne siber saldırı düzenlenmiştir. Bir tür DDoS saldırısı şeklinde gerçekleştirilen bu saldırılarda Amerikan Federal Soruşturma Bürosu (FBI) tarafından şirketlere gönderilen uyarı amaçlı mesajda Çin'den gelen saldırıların "man-in-the-middle"[220] yöntemi ile gerçekleştirildiği belirtilmiş olup FBI mesajında, "ABD hükümetinin değerlendirmesine göre, Çin dışına giden internet trafiğinin bir yerde kesilerek kullanıcıların, ABD merkezli sitelere istek göndermeleri sağlanıyor. Çin'in internet ağından kaynaklanan bu kasıtlı hareket, ABD merkezli internet sitelerinin hizmetlerinde aksamaya yol açtı" denilmiştir. Bu internet faaliyetlerinin, Çin Unicom ve Çin Telekom siteleri kaynaklı olarak gözüktüğü belirtilmiş olup Çin'in Google'u olarak bilinen Baidu'nun bu saldırılarda kilit bir rol oynamıştır[221].

- Çin ile ABD arasında siber saldırılar konusunda yaşanan gerilimin ardından Amerikalı Mandiant şirketi yayınladığı raporda Şanghay kentindeki Çin ordusuna bağlı 61398 adında gizli bir askeri birimin varlığı belirtilmiş ve bu birimin ABD şirketlerine yönelik yapılan uzun yıllardır devam eden siber saldırılarla bağlantılı olduğunu açıklanmıştır.

- 2013 yılında Microsoft zararlı yazılımların temizlenmesi için kullanılan araçları aracılığı ile topladığı veriler üzerinde yaptığı araştırma neticesinde siber saldırılara en çok kaynaklık eden ülkeler listenin başında %41 ile Çin birinci sırada , %10 ile ABD ikinci sırada yer aldığı görülmüştür[222]. (HEKİM & BAŞIBÜYÜK, 2014)

---

[220] man-in-the-middle saldırısı; Bu tip saldırılarda, sanal korsanlar, kullanıcıların bilgisayarlarına bulaştırdıkları bir küçük program ile hedefteki sitelere pek çok talep gönderilmesini sağlamakla kullanıcıların bu işlemlerden haberi olmamaktadır.

[221] Bkz. https://siberbulten.com/uluslararasi-iliskiler/cin-abdli-sirketlerden-intikamini-aldi/ Erişim Tarihi: 12.10.2017)

[222] Bkz. Yrd. Doç. Dr. Hakan HEKİM, Doç. Dr. Oğuzhan BAŞIBÜYÜK"Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları -Cyber Crimes and Turkey's Cyber Security Policies" , sy.148

Çin 2015 yılında bilgi sistemleri ile internet altyapı sistemlerinin korunması amacıyla geniş kapsamlı bir ulusal güvenlik yasası çıkartmıştır.

Çin'in Siber Güvenlik yasasından önce sistem ve altyapı güvenliğine ilişkin yasa ve yönetmelikler şunlardır;

- Bilgisayar Bilgi Sistemlerinin Güvenliğini Koruma Yönetmeliği,
- Bilgisayar Virüslerinin Önlenmesi ve Tedavisinde İdari Önlemler
- Bilgi Güvenliğini Hiyerarşik Koruma için İdari Önlemler
- Devlet Sırlarını Korunması Hakkında Kanun
- Çin'in Bilişim Güvenliği ile ilgili olarak, Bilgisayarlı Virüsleri Önleme ve Tedavi için İdari Önlemler ve Bilgi Güvenliğini Hiyerarşik Koruma için İdari Önlemler gibi bazı kanunlar, kurallar ve düzenlemeler yapılmıştı.

Kasım 2016 tarihinde Ulusal Halk Kongresi tarafından kabul edilip yayınlanan Siber Güvenlik Kanunu (Cybre Securtiy Law) 1 Haziran 2017'de yürürlüğe girmiş olup kanun kapsamında Çin'in önemli veri tabanlarına yönelik olarak saldırılarda bulunan kişi veya grupların mal varlıklarının dondurulması mümkün hale gelmiştir. Kanun ile Ülkede toplanılan bilgilerin yurt dışına çıkarılmasına denetimi artıran ve kişisel bilgilerin korunmasına ilişkin önlemleri sıkılaştıran düzenlemeler yapılmıştır.

Kanun kapsamında Çin hükümeti tarafından ülke içerisinde ve diğer ülkeler kapsamında siber güvenliğe ilişkin olarak tehditlerin izlenmesi ve bu tehditlere karşı mücadele edilmesi ile ülke içinde ve dışında kilit öneme sahip bilgi ve altyapı yatırımlarının muhtemel siber saldırılardan korunması amaçlamış, Çin'in resmi internet sitelerine saldırı düzenleyen kişi, grup ve ülkelere karşı önleyici cezalar öngörülmüştür. Bu kapsamda Çin'in ulusal güvenlik ve çıkarlarını zedeleyen kişi yada örgütlere karşı yaptırımlar öngörülmüştür. Bu yaptırımlar kapsamında devlet

veri tabanlarına saldıran kişi yada grupların mal varlıklarının dondurulması ve gerekli cezaların uygulanması öngörülmüştür[223].

Kanun kapsamında 79 madde ve 7 alt başlıkta incelenen maddeler değerlendirildiğinde ;

Kişisel Verilerin/Bilgilerin korunması konusunda; kişisel bilgilerin korunması ve kişisel gizlilik konularına daha fazla önem vermektedir. Buna göre; Kişisel bilgilerin toplanması ve kullanılmasını standartlaştırmakta olup işletmeler yalnızca "veri güvenliği" ne değil, aynı zamanda "bireysel gizlilik koruması" na odaklanması gerektiği bunun daha önemli olduğu belirtilmektedir.

Şebeke operatörleri için güvenlik gereksinimleri konusunda; şebeke operatörlerinin ve güvenlik gereksinimlerinin net tanımlarını sunulmuş olup büyük finansal kurumların çoğu "şebeke operatörleri" haline gelebileceği öngörülmüştür.

Bireylerin, şahsi bilgilerdeki hataları düzeltmeleri için şebeke operatörlerine başvurma hakları olduğu ve bu durumda şebeke operatörleri, hataları gidermek veya düzeltmek için önlem almaları gerektiği,

Bireyler veya kuruluşların, kendi ağlarının kullanımından sorumlu oldukları ve hileli amaçlarla veya diğer yasadışı faaliyetler için web siteleri veya iletişim grupları oluşturmalarının yasak olduğu,

Kanun, internet platformlarına ve şebeke operatörlerine, topladıkları kişisel bilgileri de koruması için gerekli önlemleri alma zorunluluğu getirmiştir.

Kritik Bilgi Altyapısı konusunda; kanun, kilit bilgi altyapısının kapsamını belirlemiş olup kilit bilgi altyapısının korunması konusunda yaptırımlar öngörülmüştür. Siber güvenliği koruma ile ilgili olarak devlet, kamuya açık

---

[223]Bkz. Overview of China's Cybersecurity Law , IT Advisory KPMG China ,February 2017 belgenin orjinaline https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf adresinden erişilmiştir. (Erişim Tarihi: 13.10.2017)

iletişim ve bilgi hizmetleri, enerji, finans, ulaştırma, su koruma, kamu hizmetleri ve e-yönetişim ve ayrıca ulusal çapta ciddi zarar verebilecek diğer kritik bilgi altyapısında güvenlik, ulusal ekonomi ve kamusal çıkarlar yoksa, işlevsellik kaybolacağı veya veri sızdırılacağını kritik bilgi altyapısının korunması vurgulamaktadır.

Kişisel bilgilerin ve ticari verilerin yurtdışına aktarmaya ilişkin kısıtlamalar Konusunda ise; Kanun kapsamında kişisel bilgiler kavramı açıklanmış olup buna göre Kişisel bilgiler, gerçek kişinin kimliğini bağımsız olarak veya diğer bilgilerin yanı sıra doğal bir kişinin adını, doğum tarihini, kimlik bilgilerini numara, kişisel biyometrik bilgi, adres ve telefon numarası da dahil diğer kimlik bilgilerini de içerecek şekilde belirleyebilen elektronik veya diğer yollarla kaydedilmiş her türlü bilgiyi ifade etmekte olup bu kapsamda kişisel bilgilerin korunmasını "vatandaşlardan" "gerçek kişilere" genişletmektedir. Yabancı işletmeler ve kuruluşlar normalde Çin dışında bilgi aktarması gerekmesine rağmen hassas verilerin yurtiçinde depolanması gerektiğini öngörmektedir

Cezalar ve yaptırımlar konusunda ise yasayı ihlal edilmesi halinde uygulanacak cezalar açıkça belirtilmiş olup bu ceza ve yaptırımlar ticari faaliyetlerin askıya alınmasını da içermektedir. Bu kapsamında yasadışı ve kanun kapsamında uygun görülmeyen hareketler işletmelerin kapatılmasına veya lisansların iptaline neden olabileceği ayrıca kapsamında kanunu ihlal eden ve siber güvenliği tehlikeye sokan faaliyetlerde bulunanlar 5 ila 15 gün boyunca gözaltına alınabilir ve davanın ciddiyetine bağlı olarak 100.000 RMB - 1.000.000 RMB para cezası verilebileceği öngörülmüştür[224].

Siber Güvenlik Yasası kapsamında, Çinli vatandaşların kişisel bilgi ve verilerinin yurtdışına aktarılması ve depolanmasını düzenleyen kişisel bilgileri

[224]Bkz. Overview of China's Cybersecurity Law , IT Advisory KPMG China ,February 2017 belgenin orjinaline https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf adresinden erişilmiştir. (Erişim Tarihi: 13.10.2017)

Güvenlik Kriterleri ve Ülkeyi Terk Eden Kritik Veriler için Tedbirler (Önlemler) yayınlanmıştır.

Çin'in Siber Güvenlik Yasası'nın (Kanun) bir parçası olan Tedbirler, 1 Haziran 2017 tarihinde yürürlüğe girmesi öngörülmüş olup Siber Güvenlik Yasasının uygulanmasına yardımcı olmak üzere tasarlanmış ve Çin'de yerleşik olan ve Çinli vatandaşların bilgilerini barındırıp, yurtdışında depolayan yabancı şirketler hakkında yeni düzenlemeler getirmiştir.

Buna göre "kişisel bilgilerin" toplanması ve saklanması ile ilgili hükümler, bu şirketlerde çalışan Çinli vatandaşların bilgilerinin İK operasyonlarının merkezileştirilmesi amacıyla şirket tarafından ülke dışında depolaması ve uygulaması açısından yabancı şirketler için zorluk teşkil ettiği ve uygulamada sorun çıkmaması için, Çinli çalışanları bulunan şirketlerin mevcut İnsan Kaynakları ve Bilişim Teknolojileri sistemlerini iyice incelemesi ve yeni gereksinimlere uymak için bunları yeniden yapılandırması ve bazı ihtimalleri kapsayacak yeni planlar geliştirmeleri gerekmekte olup bu kapsamda Çin'deki şirketlerin çalışanları için özel bir İnsan Kaynakları platformu kurması gerektiğini veya uluslararası pratik kullanım için ucu açık, entegre sistemler haline dönüşmesini yani Çin'de bulunan sunuculara yurtdışındaki bir sistemin arka ucunu bağlama anlamına gelen bir uygulamaya dönüşmesini gerektirmektedir.

2016 yılının sonunda Çin Halk Cumhuriyeti Siber Güvenlik Bildirgesi yayınlanmış olup Bildirge kapsamında bilgi teknolojilerinin geniş uygulamasının, siber uzay alanının gelişim ve yükselişi, ekonomik ve sosyal gelişme ve ilerlemeyi önemli ölçüde arttırdığı; aynı zamanda, yeni güvenlik risklerini ve zorluklarını da beraberinde getirdiği belirtilmiştir. Buna göre Siber uzay güvenliği insanlığın ortak çıkarları, küresel barış ve gelişme ve tüm ülkelerin milli güvenliği konularıyla ilgilendiği, Çin'in siber güvenliğinin korunması genel olarak; kısmen refah bir toplum inşa etmenin stratejik düzenlemesinde ilerlemek, kapsamlı bir reform derinleştirmesi, yasalar doğrultusunda ülke yönetimi, partilerin koordine bir şekilde kapsamlı ve kesin yönetimi için önemli bir ölçü ve "Two Centenaries"in objektif

mücadelesini gerçekleştirmek ve Çin halkının büyük yenileştirmesinin "Chinese Dream"i gerçekleştirmek için önemli bir garanti olduğu, Xi Jinping' in küresel internet yönetim sistemi reformunu ilerletmeyi ele alan 4 ilke ve siber uzayda ortak bir kaderin topluluğunu inşa etmek üzerine kurulu "Five Standpoints"i uygulamak; Çin'in siber alanındaki gelişme ve güvenliğini içeren önemli görüşleri üzerinde durmak; Çin'in siber güvenlik işleri ve ülkenin egemenlik, güvenlik ve siber uzaydaki gelişimi ile ilgili çıkarlarını korumak için bu strateji formüle edildiği belirtilmiştir.

Belgenin amacı tüm ulusal güvenlik görüşü rehberliği ile yeniliklere açık, eşgüdümlü, tecrübe edilmemiş, açık ve paylaşımlı gelişme anlayışını uygulamak, risk ve kriz bilincini güçlendirmek, Kapsamlı olarak hem yerli hem de yabancı büyük, geniş olayları ele almak, iki önemli güvenlik meselesini (iç ve dış güvenlik) kapsamlı bir şekilde planlamak, kuvvetli bir şekilde savunmak, etkili bir şekilde karşılık vermek, barışa destek vermek, güvenlik, açıklık, gizlilikten kaçınmak, siber uzayda iş birliği ve düzen, ulusal egemenliğin çıkarlarını korumak, güvenlik, gelişme ve kalkınma, kuvvetli bir siber güç kurma stratejik hedefini gerçekleştirmek olarak belirtilmiştir.

Buna göre belgede ilkeler;

1) Siber Uzayda Egemenliğe Saygı Duymak ve Egemenliği Korumak
2) Siber Uzayın Barışçıl Kullanımı
3) Kanuna göre Siber Uzay Yönetimi
4) Siber Güvenlik ve Gelişimi Kapsamlı Bir Şekilde Yönetmek

olarak belirlenmiş olup, stratejik görevler ise;

- Siber uzaydaki egemenliğin tereddütsüz bir şekilde savunulması görevi kapsamında; ülkenin egemenliği kapsamı içerisinde çevrimiçi faaliyetleri, anayasa, kanunlar ve yönetmeliklere göre yönetilmesi, ülkenin bilgi altyapısının ve bilgi kaynaklarını korunması, ekonomik, idari, bilimsel, teknolojik, yasal, diplomatik ve askeri önlemler de dahil olmak üzere ülkenin siber uzaydaki egemenliğinin istikrarlı bir şekilde sürdürülmesi için tüm önlemlerin alınması

gerektiği belirlenmiştir. Bu kapsamda ülkenin ulusal rejimini yıkmayı veya ağ üzerinden ülkenin egemenliğini yok etmeyi amaçlayan eylemlere kararlı bir şekilde karşı çıkılması gerektiği belirtilmiştir.

- Kritik bilgi altyapısının korunması görevi kapsamında ulusal kritik bilgi altyapısı ulusal ekonomiyi ve halkın geçimini etkileyen bilgi altyapısını ifade ettiği, veri sızdırılmasının bilgi altyapısının işlevselliğini yok edeceği veya kaybolmasına neden olacağı, ulusal güvenlik ve kamu menfaati ciddi zarar görebileceği, bunlarla sınırlı olmamak üzere temel bilgi ağlarını sağlayan kamu telekomünikasyonunu, radyo ve televizyon iletişimini, ve benzeri hizmetlerin yanı sıra bölgelerdeki ve devlet organlarındaki enerji, finans, ulaşım, eğitim, bilimsel araştırma, hidroelektrik, endüstri ve imalat, sağlık ve tıp, sosyal güvenlik, kamu girişimleri, vs., önemli internet uygulama sistemleri, vs. gibi önemli bilgi sistemlerinin zarar görebileceği belirtilmiştir. Kritik bilgi altyapısının ve bunun önemli verilerinin saldırı ve tahribata karşı koruması için gerekli tüm önlemlerin alınması gerektiği belirtilmiştir. Teknoloji ve yönetim üzerine eşit önem verilmesinin sürdürülmesi, aynı anda koruma ve engelleme geliştirilmesi gerekliliği ile kimlik saptaması üzerine odaklanılması gerektiği belirtilmiş, erken uyarı, yanıt, üstesinden gelme ve diğer benzer kollarda da gelişimin sağlanması ve bilgi altyapı koruma sistemleri kurulması ve uygulanması ile önemli bilgi altyapısının güvenlik koruması güçlendirilmesi gerektiği belirtilmiştir.
- Çevrimiçi kültür yapısının güçlendirilmesi görevi ile çevrimiçi ideoloji ve kültür savaş alanlarının inşası, güçlendirilmesi, sosyalist çekirdek değer görünümünün güçlü bir biçimde beslenmesi ve uygulanması, ağ içerikli inşaat projeleri hayata geçirilmesi, olumlu ve artış gösteren bir çevrimiçi kültür geliştirilmesi ve arzu edilen bir çevrimiçi atmosfer oluşturulması gerektiği belirtilmiştir.
- Siber terörizm, saldırı, kanunlara aykırılık ve suç görevinde çevrimiçi terörle mücadele eylemleri, bir düşman tarafından casusluk yapılmasını önlemek veya engellemek için tasarlanan faaliyetler ve hırsızlık önleme kabiliyetlerinin güçlendirilmesi ve siber terörizm ve siber casusluk faaliyetlerine katı bir biçimde karşılık verilmesi gerektiği, kapsamlı yönetimden, kaynak kontrolüne ve yasal

korumaya devam edilmesi, çevrimiçi dolandırıcılık, hırsızlık, silah ve uyuşturucu kaçakçılığı, vatandaşların kişisel bilgilerinin ihlal edilmesi, müstehcen ve cinsel bilgilerin dağıtımı, hack saldırıları, zihinsel mülkiyet haklarının ihlal edilmesi ve diğer yasadışı suç aktivitelerinin önlenmesi için gerekli önlemlerin alınması gerektiği belirtilmiştir.

- Mükemmel ağ yönetim sistemleri oluşturulması görevi kapsamında ağın yasal, açık ve şeffaf bir yolla yönetilme ve idare edilmeye devam edilmesi, yasaların bir dayanak olacağından emin olunması, kanunlara güvenilmesi ve kanunların yürürlüğe konulması konusunda otoriter olunması ile kanun ihlallerinin cezalandırılması gerektiği belirtilmiştir. Siber güvenlik yasası ve yönetmelik sistemlerinin tamamlanması, formüle edilmesi ve yayımlanması, reşit olmayan kişilerin çevrimiçi ortamda korunması için olan yönetmelikler ve diğer bütün kanunların, toplumun her kesiminin görev ve sorumluluklarının netleştirmesi ve siber güvenlik yönetimin gerekliliklerinin açıklığa kavuşturması gerektiği belirtilmiştir.

- Yenilikçi gelişimin sürekliliği, teknolojik yeniliklere faydalı kural çevresinin kuvvetlice yaratılması, kaynak ve güçlerle kapsamlıca uğraşılması, gelişmelerin dayanak noktası olarak görülmesi, endüstri, öğrenme, araştırma ve kullanımın entegre edilmesi, stratejik geçişler üretmek için koordine içinde çalışılması, anahtar teknoloji atılımlarının elde edilmesi için olabildiğince hızlı davranılması gerektiği belirlenmiştir[225]. (Çin Halk Cumhuriyeti Siber Güvenlik bildirgesi)

Son olarak Çin Ulusal Siber Güvenlik Stratejisi[226] yayınlanmıştır. Belgenin amacı genel ulusal güvenlik görüşü olarak, yenilikçi, koordineli, açık ve ortak gelişim konseptini uygulayan, risk bilincinin ve kriz bilincinin güçlendirilmesi, iç

[225]Bkz.Çin Halk Cumhuriyeti Siber Güvenlik bildirgesi, Metin çevirisine https://www.slideshare.net/CezeriSGACezeriSiber/in-halk-cumhuriyeti-siber-gvenlik-bildirgesi adresinden erişilmiştir. (Erişim Tarihi :14.10.2017)
[226]Bkz.http://afyonluoglu.org/PublicWebFiles/strategies/Asia/China%202017%20National%20Cyber%20Strategy-Unofficial%20Translation-EN.pdf

ve dış güvenlik gelişiminin kapsamlı bir şekilde planlanması, kuvvetli bir şekilde savunulması, etkili bir şekilde yanıt verilmesi, siber alanda barışı, güvenliği, açıklığı, işbirliğini ve düzeni teşvik etmek, ulusal egemenlik, güvenlik ve kalkınmanın çıkarlarını korumak ve güçlü bir siber güç inşa etmenin stratejik amacını gerçekleştirmek olarak açıklanmıştır. Temel olarak 5 hedef belirlenmiş olmakla ;

*Barış hedefi kapsamında bilgi teknolojisi kötüye kullanımı etkili bir şekilde engellenmeli, siber alanda silahlanma yarışları ve uluslararası barışa yönelik diğer tehditler etkin bir şekilde kontrol altına alınmalı, siber alanda çatışmalar etkili bir şekilde önlenmelidir.

*Güvenlik hedefi kapsamında siber güvenlik riskleri etkin bir şekilde kontrol edilmeli, ulusal siber güvenlik koruma sistemleri tamamlanmalı ve geliştirilmeli, temel teknolojiler ve ekipman güvenli ve kontrol edilebilir olmalı, ağ ve bilgi sistemleri istikrarlı ve güvenilir bir şekilde çalışmalıdır. Siber güvenlik yetenekleri talepleri karşılamak, tüm toplumun siber güvenlik bilincini, temel koruma yeteneklerini ve ağı kullanma konusundaki güvenlerini büyük ölçüde artırmaktır.

*Açıklık hedefi kapsamında bilgi teknolojisi standartları, politikaları ve pazarları açık ve şeffaf olmalı, ürün dolaşımı ve bilgi yayılımı daha yumuşak hale gelmeli, dijital uçurum her geçen gün kapatılmalıdır. Büyük ve küçük, güçlü ve zayıf, fakir ve zengin arasında ayrım yapmadan, dünyadaki tüm ülkeler ve özellikle gelişmekte olan ülkeler, gelişme fırsatlarını paylaşabilmeli, kalkınma sonuçlarını paylaşabilmeli ve siber yönetişime adil biçimde katılabiliyor olmalıdır.

Açıklık dünya çapındaki tüm ülkeler teknoloji alışverişi, siber terör ve siber suçlara saldırı, vb. alanlarda daha yakın işbirliğini geliştirecek, çok taraflı, demokratik ve şeffaf bir uluslararası İnternet yönetim sistemi tamamlanacak ve mükemmelleştirilecek ve ortak bir topluluk oluşturulacağı belirtilmiştir.

*Düzen hedefi kapsamında halkın bilme, katılma hakkı, fikirlerini ifade etme hakkı, denetleme hakkı ve siber alanda diğer yasal hak ve çıkarlar tamamen korunmalı, siber alanda kişisel gizlilik etkin bir şekilde korunmalı ve insan hakları korunmalı ve tamamen saygı duyulmalıdır. Yerel ve uluslararası yasal yapılar, siber

alan için standartlar ve normlar aşamalı olarak kurulmalı, siber alanda yasaya göre etkili bir yönetişim gerçekleştirilmeli, ağ ortamı dürüst, medeni ve sağlıklı hale gelmeli ve serbest bilgi akışı organik olduğu ve ulusal güvenlik ve halkın çıkarlarının korunması ile birleşik olduğu vurgulanmıştır[227].

2.6.Japonya;

Japonya'nın siber güvenlik stratejilerinin temelinde muhtemel bir siber saldırı karşısında hazırlıklı olunması ve karşı koyulmasına ilişkin planlamanın yapılması ile siber saldırılarda bilgi toplama ve paylaşıma sistemi kurularak sistemin kullanılması, bilgi güvenliğine ilişkin kampanyalar düzenlenmesi ve kişisel verilerin korunması için bilinçlendirme ve teşviklerin yürütülmesi, Uluslararası düzeyde ittifaklar kurularak mevcut ittifakların güçlendirilmesi ile bilgi güvenliğinin sağlanması amacıyla bu alandaki insan kaynağının geliştirilerek yasal mevzuat ve altyapının düzenlenmesi bulunmaktadır.

Japonya'nın Mayıs 2010 yayınlanan Bilgi güvenliği stratejisi(Information Security Strategy for Protecting the Nation)[228] , bir dizi kilit eylem alanı olarak;

- Siber saldırıların olası ihlallerini göz önüne alarak politikaların güçlendirilmesi ve bir karşılık kuruluşu kurulması.
- Bilgi güvenliği ortamındaki değişikliklere uyarlanmış politikaların oluşturulması.
- Pasif olmayan bilgi güvenliği önlemlerinin alınması

Öngörülmüştür.

---

[227]Bkz.http://afyonluoglu.org/PublicWebFiles/strategies/Asia/China%202017%20National%20Cyber%20Strategy-Unofficial%20Translation-EN.pdf

[228]Bkz. Information Security Strategy for Protecting the Nation), May 2010, belgenin orjinaline http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf adresinden erişilmiştir. (Erişim Tarihi :15.10.2017)

Ulusal alanda Siber ortamda güvenliği artırmak için izlenmesi gereken yolu belirleyen stratejinin kapsadığı ana eylem noktaları şunlardır;

- Siber alanda ulusal güvenlik ve kriz yönetimi uzmanlığını güçlendiren bir politika uygulanması
- Sosyo-ekonomik faaliyetlerin temeli olarak BİT politikası ile bütünlük.
- Ulusal güvenlik, kriz yönetimi ve ulus / kullanıcı koruma bakış açılarını kapsayan üçlü bir politika oluşturulması. Ülkenin / kullanıcıların bakış açısına odaklanan bir bilgi güvenliği politikası özellikle önemlidir.
- Ekonomik büyüme stratejisine katkıda bulunan bir bilgi güvenlik politikasının oluşturulması.
- Uluslararası ittifaklar kurulması[229].

Japonya'nın bilgi güvenliği strateji belgesinde atılması gereken önemli adımlar listelenmiş olup ulaşılmak istenen hedefler belirlenmiştir. Bilgi sistemlerinin güvenliği ile ilgili somut önlemler alınmış ve 2020 yılı hedeflenmiştir.

2012 tarihinde Japonya Savunma Bakanlığı tarafından yapılan girişim neticesinde ülkeye yönelik gerçekleştirilen siber saldırılara karşı savunma amaçlı olarak bir bilgisayar virüsünün geliştirilmesi amacıyla çalışmalar yapılmış olup kötü niyetli yazılımlara karşı 'onların yöntemleriyle' savaşılması hedeflenmiştir. Bu kapsamda geliştirilecek 'milli güvenlik virüsünün maliyetinin 2.3 milyon dolar civarında olacağı öngörülmüştür. Fujitsu şirketi tarafından geliştirilmesi planlanan savunma sistemi, üst düzey saldırıları engelleme, virüsleri temizleme, saldırının kaynağını takip edip belirleme ve hatta bulunduğu sunucuları sekteye uğratma gibi kabiliyetlere sahip olması planlanmıştır[230].

---

[229]Bkz. ENISA, National Cyber Security Strategies Setting the course for national efforts to strengthen security in cyberspace , May, 2012 belgenin orjinaline https://www.enisa.europa.eu/publications/cyber-security-strategies-paper adresinden erişilmiştir. (Erişim Tarihi :15.10.2018)

[230]Bkz. https://webrazzi.com/2012/01/06/japonyadan-milli-guvenlik-virusu/(Erişim Tarihi :15.10.2018)

Japonya Savunma Bakanlığı tarafından hazırlanmış olan "Japonya'nın 2013 yılı Savunması" başlıklı Beyaz Kitap, 9 Temmuz 2013 tarihinde yayımlanmış olup bu savunma belgesinde siber güvenlik konusu önemli bir yer teşkil etmektedir.

Bu Beyaz Kitap kapsamında son dönemde küresel orta varlıklar olarak bilinen deniz, uzay ve siber uzay alanlarına yönelik istikrarlı erişime yönelen mevcut riskler kapsamında pek çok ülke tarafından siber saldırılara karşı mücadele edilebilmesi için somut girişimler sergilendiği, uzayın gelişimi ile askeri ve sicil alanlardaki sektörlerin arasında bulunan ilişki kapsamında Çin tarafından uzayın istihbarat bilgi toplanması, haberleşmenin ve deniz trafiğinin askeri amaçlarla dinlenmesi için kullanmasının olası olduğu ve bu durumun tehlikelerinden bahsedilmiş, internet ile ilgili teknolojinin devamlı olarak geliştiği bu sebeple de siber saldırıların her gün daha da kompleks hale geldiği belirtilmiştir. Belge kapsamında siber saldırıların özellikleri şu şekilde açıklanmıştır;

- Çeşitlilik: Saldırganların, yöntemlerin, amaçların ve saldırı şartlarının çeşitliliği.

- Anonimlik: Saldırganların kimliklerini gizlemelerinin kolaylığı.

- Dikkati Çekmeden Gerçekleştirme: Saldırıların varlığının tespitinin, hatta zararın oluştuğunun belirlenmesinin güçlüğü.

- Saldırganların Avantajları: Saldırı araçlarına kolaylıkla erişim ve yazılım zayıflıklarının tamamen giderilmesinin güçlüğü.

- Caydırıcılık: Karşı saldırılar ve savunma tedbirleriyle ancak sınırlı düzeyde caydırıcılığın sağlanabilmesi.

Bu kapsamda değerlendirildiğinde silahlı kuvvetlerin BİS'e bağımlı oluşu da dikkate alındığında siber saldırıların, "asimetrik strateji" kapsamında değerlendirildiği ve tüm dünyada ülkelerin silahlı kuvvetlerinin siber uzay alanındaki savunma kapasitelerini geliştirmek amacıyla düzenlemeler yaptığına dikkat çekilmiştir.

Diğer ülkeler tarafından yapılan bilgi ve iletişim ağlarına erişme amaçlı girişimlerin istihbari bilgi toplamak maksadı ile yapıldığı, aralarında Halkın Kurtuluşu Ordusu (HKO)'nun, istihbarat ve güvenlik kurumlarının da bulunduğu

Çin örgütleri ile özel hackerların siber saldırılara dahil olduğu belirtilmiştir. Çin'in siber uzayla yakından ilgilendiği, HKO tarafından eğitim amacıyla bir siber birim kurulduğu ve HKO ile güvenlik kurumları tarafından bilgi teknolojileri şirketlerinin personellerinin ve bazı özel hackerların kiralandığı, Japon Hükümeti tarafından 2012 ylının Eylül ayında Senkaku Adalarını satın almasına ilişkin kararın alınmasının akabinde Japonya mahkemeleri, idari kurumlar ve üniversite hastanelerine ait internet sitelerinin siber saldırıya maruz kaldıkları belirtilmiştir.

Anılan açıklamalar ışığında Siber uzay alanının kullanımı için bilgi güvenliği alanının ulusal ve küresel güvenliğe etkileri ile muhtemel risklerin insan hayatını her alanda etkileyebileceği bilinci ile bilgi güvenliği için gerekli tedbirlerin alınması amacıyla temel stratejinin belirlenebilmesi için 2005 yılında "Bilgi Güvenliği Siyaseti Konseyi" ve bu konseyin uygulayıcısı olarak "Ulusal Bilgi Güvenliği Merkezi (National center of Incident readiness and Strategy for Cybersecurity - NISC)" kurulmuştur.

2010 yılının mayıs ayında Bilgi Güvenliği Siyaseti Konseyi tarafından 2010-2013 dönemini kapsayacak şekilde "Ulusun Korunması İçin Bilgi Güvenliği Stratejisi" hazırlanmış olup bilgi güvenliğinin etkin bir şekilde sağlanabilmesi için Ulusal Bilgi Güvenliği Merkezi ile yakın ve koordineli olarak çalışması istenen kamu kuruluşları olarak Ulusal Polis Teşkilatı, İçişleri ve İletişim Bakanlığı, Ekonomi, Ticaret ve Sanayi Bakanlığı ve Savunma Bakanlığı olarak belirlenmiştir.

Savunma Bakanlığı bu kapsamda siber saldırılara müdahale konulu eğitim ve personel değişimi programlarına katılmakta olup 2011 yılı içerisinde savunma sanayi şirketlerini hedef alarak yapılan siber saldırılar ile ilgili olarak mevcut birimelere acil destek sağlamak amacı ile Ulusal Bilgi Güvenliği Merkezi tarafından Siber Olaylar Mobil Yardım Timi kurulmuştur.

Savunma Bakanlığı tarafından 2012 yılı eylül ayında "Siber Uzayın İstikrarlı ve Etkin Kullanımına Doğru" başlıklı bir belge yayınlanmış, belge kapsamında Savunma Bakanlığı ve Öz Savunma Güçleri (SDF)'nin siber uzay alanının daha etkin kullanımı ile güvenliğin sağlanabilmesi amacı uygulanacak stratejinin çerçevesi belirlenmiştir.

Siber güvenliğin sağlanması amacı ile Savunma Bakanlığı ve SDF bakımından öncelikle yapılması gereken fırsatların azami olarak kullanılması ancak mevcut risklerin asgariye indirilmesi olarak belirlenmiş bu kapsamda siber uzay alanının istikrarlı kullanımı çerçevesinde siber uzay alanının güvenliğinin sağlanması ile bu alanın kara, deniz, hava ve uzay alanları ile eşit derecede tutularak siber uzay alanında daha etkili olabilmek amacıyla yeteneklerin arttırılması hedeflenmiştir.

SDF içerisinde mevcut C4 (Komuta, Kontrol, İletişim ve Bilgisayar) Biriminin görevi siber saldırılar karışında gerekli müdahalenin yapılabilmesi amacıyla askeri ve güvenliği ilgilendiren alanlardaki iletişim ağlarının sürekli olarak izlenmesidir.

2012 yılı içinde siber saldırılardan kaynaklanacak tehlikeler ile etkin mücadele amacıyla Savunma Bakanlığı ve SDF yapısı içerisinde meydana gelen değişiklik ile "Siber Savunma Grubu" kurulmuş, 2013 yılının şubat ayında ise Savunma Bakan Yardımcısı tarafından başkanlık edilen "Siber Siyaset Komitesi" kurulmuştur[231].

Bilgi Güvenliği Politika Konseyi tarafından 2012 yılında Bilgi güvenliği dokümanı yayınlanmıştır.

Japonya tarafından 17 Aralık 2013 tarihinde yayımlanan ilk Ulusal Güvenlik Stratejisi belgesi kapsamında 10 yıllık planda Japonya devletinin ulusal güvenliğine ilişkin çıkarlarının ve güvenliğe ilişkin sorunlarının küresel ve bölgesel stratejik güvenlik ortamı analizinin temelinde ortaya koyulmakta olduğu belirtilmiş olup belgenin Küresel Güvenlik Ortamı ve Sorunlar başlığı kapsamında 4 Küresel Ortak Varlıklara Yönelik Riskler tanımlamıştır. Bu kapsamda son dönemde deniz, uzay, siber uzay gibi küresel ortak varlıkların kullanımı ve serbest erişimi için engel

[231]Bkz.Japonyanın Savunma Beyaz Kitabı, 2013 http://mgk.gov.tr/calismalar/calismalar/019_japonya_beyaz_kitap_2013.pdf adresinden erişilmiştir. (Erişim Tarihi :16.10.2017)

teşkil etmekte olan risklerin arttığı, son dönemde bilgi toplanması ve gözetlemenin askeri amaç taşıyan haberleşme amacı ile kullanılması karşısında uzayın öneminin önemli ölçüde arttığı, ancak uzayın kullanımının yoğunluğu, uydu savar denemeleri ve uydu çarpışmalarının neden olduğu uzay atıkları, uzayın istikrarlı biçimde kullanımının tehlike altında olduğu ve gizli bilgilerin ele geçirilmesi ile kritik altyapıların işlevselliğinin sekteye uğratılması ve askeri sistemlerin engellenmesi gibi amaçlar ile yapılan siber saldırıların siber uzay alanında kaşılaşılabilen riskler arasında bulunduğu belirtilmiştir.

Strateji belgesi kapsamında Japonya'nın siber güvenliğe olan yaklaşımı incelendiğinde siber güvenliğin arttırılması, siber saldırılara verilecek karşılığın güçlendirilmesi gerektiği, kritik altyapılarının siber saldırılar karşısında korunması gerekliliği, siber uzay alanının özgür ve güvenli kullanımı amacıyla alınan önlemlerin arttırılması gerektiği, Japonya ile ABD arasındaki güvenlik ve savunma alanındaki işbirliğinin arttırılması gerektiği belirtilmiştir. Bu kapsamda Japonya ile ABD arasındaki güvenlik ve savunma alanındaki işbirliği kapsamında ortak tatbikatlar yapılması, ortak istihbaratın paylaşılması, gözetim ve keşif faaliyetleri ile savunma yeteneklerinin Japonya Öz Savuma Kuvvetleri ile ABD tarafından ortak olarak kullanılması ve balistik füze savunması, deniz, uzay, siber uzay alanı ve büyük çaplı afetlere karşılık gibi alanlarda ortak işbirliğinin arttırılması öngörülmüştür[232].

2014 tarihinde yayınlanan Siber Güvenlik Yıllık raporunda Ulusal Bilgi Güvenliği Merkezi (NISC) bünyesindeki Hükümet Güvenliği Operasyon Koordinasyon Ekibi(GSOC- The Government Security Operation Coordination Team) Ihükümet organları tarafından alınan şüpheli e-postalar hakkında bilgi toplamış olup 2013 mali yılı boyunca toplamda 381 uyarı yayınlamıştır.

---

[232]Bkz. Japonya Ulusal Güvenlik Stratejisi
http://mgk.gov.tr/calismalar/calismalar/026_japonya_ulusal_guvenlik_stratejisi.pdf (Erişim Tarihi :16.10.2017)

Raporda 2013 yılında yetkisiz erişim ve kötü amaçlı yazılım kullanımıyla ilgili saldırılarla, hükümet organları, dahil kurumlar ve diğer kuruluşlardan kritik bilgileri çalmak amacıyla çok sayıda bilgi güvenliği vakası olduğunu, genel olarak, hedeflenen e-posta saldırıları, siber saldırıların ilk aşamasında taktik olarak sıklıkla kullanılır. Bunlar, genellikle, ekli bir dosyada kötü amaçlı yazılım veya kötü amaçlı sunuculara bağlantılar içeren hedef e-postalar göndererek başlatılır ve sonuç olarak, e-posta alıcısının terminallerine, bu ek dosyaları açarak veya belirtilen URL'leri tıklatarak e-posta alıcının terminallerine bulaştırıldığı belirtilmiştir.

Hedeflenen e-posta saldırılarındaki eğilimler açısından, 2013 yılında Ulusal Polis Teşkilatı tarafından belirlenen hedeflenen e-posta saldırı sayısı 4928; bir önceki yıla göre 517 azalma (yüzde 51'lik bir yıllık düşüş) olduğu tespit edilmiş olup bu rakamlarla, hedeflenen e-posta saldırılarının tehditleri görünüşte azalmaktadır. Bununla birlikte Ulusal Polis Teşkilatı tarafından yapılan bir analize göre, çok sayıda e-posta ile başlatılan "kimlik avı e-posta kampanyalarında" bir düşüş yaşanırken, "mızrak kimlik avı" sözcüğünde bir artış meydana gelmiştir. Raporda saldırıların büyük çoğunluğunun, sosyal mühendislik biçiminde olduğu ve gelişen taktikler nedeniyle, örneğin, yetkisiz harici bağlantıların tespit edilmesini önlemek için, saldırı yöntemlerinin de geliştiği tespit edilmiştir.

Siber ortamda riskin her geçen gün arttığı, bir mali yılda, yani 2013 yılına kadar, büyük İnternet servis sağlayıcılarına yetkisiz erişime bağlı olarak kullanıcıların bilgilerini ifşa eden 1 milyondan fazla vaka olduğu, buna ek olarak, bazı yöntemlerle Internet bankacılığı ve SNS gibi çevrimiçi hizmetler için oturum açma kimlikleri ve parolalarını çalmak için üçüncü şahıslar tarafından yetkisiz erişim (yasadışı oturum açma) içeren olaylar yaşandığı, genel Bilişim Teknolojileri kullanıcılarının tehdit altında olduğu, 2013 yılında yetkisiz erişim denemelerinin sayısı (tespit edilen vakaların sayısı) 2012'ye göre yaklaşık 2.4 kat fazla olduğu, bu kötü amaçlı faaliyetlerin amaçları açısından, 2012'de çoğunluk vakalarda çevrimiçi oyunları manipüle etmek iken 2013'te internet bankacılığı ve / veya alışveriş amaçlı para kazanma amacına kaydığı tespit edilmiştir.

2009 mali yılından bu yana Şubat ayında uygulanmaya başlanan "Bilgi Güvenliği Farkındalık Ayı" ile ilgili olarak, bu ayın ilk iş günü, 2013 mali yılının

beşinci kutlamasında "Siber Güvenlik Günü" olarak belirlenmiştir. Bu ayın ana fikri halkın bilinçlendirilmesini sağlamak olup aynı zamanda, yeni oluşturulan "Bilgi Güvenliği ve Bilinçlendirme" logomark ve animasyon videoları gibi PR araçlarını kullanarak halkın bilinçlendirilmesi sağlanmaya çalışılmıştır.

Siber alanın giderek genişlediği ve tüm kuşaklara, her yerde ve her faaliyette yaygınlaştığı son duruma bakıldığında, 2011 Temmuz ayında kurulan "Bilgi Güvenliği Uzlaşması ve Farkındalık Programı" ulusal farkındalığını artırmak amacıyla gözden geçirilmiştir. ve bilgi güvenliği için müdahale olanakları ve Temmuz 2014'te "Yeni Bilgi Güvenliği Uzmanlığı Bilinçlendirme Programı" kurulmuştur.

Ayrıca, hükümet organları, siber saldırılar durumunda, GSOC, CYMAT[233] ve CSIRT[234] arasındaki koordinasyonun geliştirilmesi ve Siber eğitimi uygulamak suretiyle risk yönetim sistemlerinin genişletilmesi ve güçlendirilmesi konusunda ilerleme kaydedilmiştir.

CII operatörleri ile ilgili bilgi güvenliği tedbirleri açısından, "Kritik Bilgi Altyapısının Korunması Temel Politikası" nın ikinci baskısına dayanarak bazı sonuçlar elde edilmiştir. Bununla birlikte, toplumsal ve teknolojik açıdan çeşitli çevresel değişiklikler olduğu için, ikinci baskının kabul edildiği zamana kıyasla, Siber Güvenlik Stratejisi doğrultusunda yeni bir politika üzerinde görüşmeler yapılmıştır.

---

[233]Bkz. Siber Olaylar Mobil Yardım Timi, Cyber Incident Mobile Assistant Team, Hükümet, Nisan 2005'te Kabine Ofisi bünyesinde Ulusal Bilgi Güvenliği Merkezi (NISC) ve temel bilgi güvenliği politikası ve stratejisi hakkında karar vermek için Bilgi Güvenliği Politikası Konferansında kurulmuş olup CYMAT, NISC bünyesinde 2012 yılında kurulmuştur. http://www.shield.ne.jp/ssrc/topics/SSRC-ER-12-022-en.html

[234]Bkz. Bilgisayar Güvenliği Müdahale Ekibi (Computer Security Incident Response Team) JPCERT / CC, Japonya'da kurulan ilk CSIRT (Bilgisayar Güvenliği Olayı Müdahale Ekibi) dir. Kuruluş, şebeke servis sağlayıcıları, güvenlik sağlayıcıları, devlet kurumları ve endüstri dernekleri ile koordine eder. Bu nedenle, Japon topluluğunda "CSIRTs CSIRT" olarak hareket eder. Asya Pasifik bölgesinde, JPCERT / CC, APCERT (Asya Pasifikli Bilgisayar Acil Müdahale Ekibi) oluşturulmasına yardımcı olmuş ve APCERT için bir sekreterya görevi yapmıştır. Uluslararası Olay Yanıtlama ve Güvenlik Takımları (FIRST) Forumu üyesi olarak, JPCERT / CC dünya genelindeki güvenilir CSIRT'lerle işbirliği yapmaktadır. https://www.jpcert.or.jp/english/about/

Araştırma ve geliştirme ile ilgili olarak, Temmuz 2011'de kurulan "Bilgi Güvenliği Araştırma ve Geliştirme Stratejisi", siber ortamdaki mevcut çevresel değişikliklerin analizlerine ve Teknolojik Strateji Özel Komitesinin görüşlerine dayanarak Temmuz 2014'te revize edilmiştir. Gözden geçirilmiş strateji, Ar-Ge öncelikleriyle ilgili incelemeyi değil, aynı zamanda siber saldırılara karşı algılama ve önleme yeteneklerini geliştirmeye yönelik yaklaşımları, sosyal sistemlerin korunması için güvenlik teknolojilerinin geliştirilmesini içermektedir[235].

Eylül 2015 te yayınlanan Siber Güvenlik stratejisinin amacı Serbest, adil ve güvenli bir siber ortam sağlayarak sosyo-ekonomik canlılık ve sürdürülebilir kalkınmanın geliştirilmesine, insanların güvenli yaşayabileceği bir ortamın oluşturulmasına ve uluslararası toplumun barış ve istikrarının sağlanmasına ve ulusal güvenliğin sağlanmasına katkıda bulunmaktadır.

Japonya, Siber Güvenlik Stratejisinin amacına ulaşmak için politika planlamasında ve uygulanmasında aşağıdaki 5 temel ilke öngörmüştür.

Buna Göre;

1- Bilginin Serbest Akışının Güvencesi İlkesi; Siber alanın yenilikler ve ilham merkezi olarak gelişmesi, siber alanda özgürce bilgi akışının güvencesi üzerine kurulu olduğu, iletilen bilgilerin herhangi bir yasal gerekçeyle sansürlenemeyeceği veya değiştirilemeyeceği ve amaçlanan alıcılara teslim edileceği bir siber ortamı yaratmak ve sağlamak zorunluluğu bulunduğunu ifade eder.

Siber ortamdaki düzenlemeleri incelerken, bilginin serbest dolaşımı tamamen dikkate alınmalı ve bireysel gizliliğin korunması için de dikkatli olunmalıdır; bu anlamda, gerekli yönetmeliklerle mahremiyetin korunması arasındaki dengeyi sağlamak için dikkat edilmesi gereken hususlar dikkate alınmalıdır. Siber uzayda bilginin özgürce dolaşımının temel şartı olarak, ahlak ve

---

[235]Bkz. Cybersecurtiy Annual Report, July 2014, belgenin orjinaline http://www.nisc.go.jp/eng/pdf/CYBERSECURITY_ANNUAL%20REPORT_2013_eng.pdf adresinden erişilmiştir. (Erişim Tarihi 17.10.2017)

sağduyudan başkalarının hak ve menfaatlerini rahatsız etmemesi gerekliliği belirlenmiştir.

2-Hukuk Kuralı İlkesi; Birbirine bağlı ve yakınsamış bilgi toplumunda, hukukun üstünlüğü, siber alana, fiziksel alanda uygulandığı gibi iyice uygulanması gerektiği, hukukun üstünlüğü, siber alanın herkes için eşit erişime sahip güvenli ve güvenilir bir alan olarak geliştirilmesi için gereklidir. Japonya'da siber alanlar yasalara ve diğer kurallara ve normlara tabidir. Benzer şekilde, Japonya açısından, uluslararası hukuk ve diğer uluslararası kurallar ve normlar siber alan için de geçerlidir ve bu nedenle siber alan uluslararası bir bağlamda de hukukun üstünlüğü tarafından yönetilmelidir. Dahası, siber alan genişlemeye devam etmiş ve tüm dünyadaki farklı aktörler tarafından kullanılmaya başlandığından, uluslararası toplumun barış ve istikrarı için özgürlük ve demokrasi gibi evrensel değerlere uygun uluslararası kurallar ve normlar oluşturmak gerekmektedir. Japonya tarafından bu ilke kapsamında uluslararası kuralların ve normların geliştirilmesi ve uygulanmasına aktif olarak katılmaya ve yurt içindeki durumlara dayalı olarak her ülkede bu kuralların ve normların istikrarlı bir şekilde devreye girmesine devam edileceği belirtilmiştir.

3-Açıklık İlkesi; Japonya, siber alanın sadece belli bir grup aktörün egemenliğinde olmaması bunu kullanmak isteyen tüm insanlara açık olması gerektiği ve siber alanın fikirleri ve bilgiyi birbirine bağladığı ve açıklığıyla ve emin bir şekilde birlikte çalışabilirliğini sürdürerek dünyaya yeni değerler getireceği aynı zamanda insanların siber alana erişiminin belirli bir küçük grubun siyasi kazanımları nedeniyle reddedilmemesi gerektiği ifade edilmiştir.

4-Özerklik İlkesi; Son on yılda İnternetin çeşitli katılımcı aktörlerin özerk yönetimi tarafından geliştirilmiş bir ilerleme kaydettiği, siber tehditler, ulusun tüm çabalarını gerektiren ulusal zorluklara dönüşmüş olsa dahi, bir hükümetin siber alanda düzen sağlamak için tüm suçlamaları üstlenmesinin pratik ve uygun olmayacağı, siber ortamda düzen ve yaratıcılığın bir arada bulunması için Japonya'nın, İnternetin geliştirdiği öz-yönetim yeteneklerine saygı duyduğu ve İnternet yönetimine ilişkin her paydaşın kendine güvenen faaliyetlerini siber yönetişimin temeli olarak görerek gelişmeyi teşvik edeceği ve siber alana bağlı

çeşitli sosyal sistemlerin görev ve görevlerinin yerine getirilmesi için özerk bir mekanizmanın işletilmesi ve kötü niyetli siber faaliyetlerin caydırılması gerektiği belirtilmiştir.

5-Çoklu Paydaşlar Arasında İşbirliği İlkesi; Siber uzayın çeşitli paydaşların çeşitli katmanlardan oluşan çok boyutlu bir alan olduğu ve bu açıdan bakıldığında, Hükümet ve Kritik Bilgi Altyapısı (CII) operatörleri, işletmeleri ve bireyleri de içeren tüm siber alanla ilgili menfaat sahipleri, siber güvenlik konusunda ortak bir vizyon paylaşmak ve örgütsel sorumluluklarını ve görevlerini yerine getirmek ya da bireylerin çabalarını gerçekleştirmek için gerekli olduğu, hükümetin bu paydaşlar arasında doğru bir şekilde koordine edilmiş ilişkilerin geliştirilmesi sorumluluğunu taşıdığı, bu tür eşgüdümlü ilişkiler kurarken hızla gelişen sofistike siber saldırılar gibi mevcut durumsal faktörleri dikkate alarak etkileşimli ve gerçek zamanlı bilgi paylaşımı ve diğer eylemleri getirerek dinamik önlemler almaya kararlı olunduğu ifade edilmiştir.

Stratejinin bu ilkeleri üzerine, barışı tehdit eden herhangi bir terör eylemi ve diğer davranışlar ile terörizme ya da böyle yıkıcı davranışları desteklemek için herhangi bir harekete insanların özgürlüğü açısından göz yumulmayacağı belirtilmiş olup; bunun yerine bu ilkeler insan güvenliği ve güvenliğinin yanı sıra ulusal güvenlik perspektifleriyle uyumlu olarak siber güvenlik politikalarına da yansımalıdır. Bu beş ilkeye uygun olarak ve insanların güvenliğini, güvenliğini ve haklarını korumak için Japonya, uygulanabilir ve etkili önlemleri, yani politik, ekonomik, teknolojik, hukuki, diplomatik ve diğer uygulanabilir tüm önlemleri saklı tuttuğu belirtilmiştir.

İlkeler Neticesinde hedefe ulaşmak için kullanılması gereken politika yaklaşımları şu şekilde belirlenmiştir.

1-Sosyo-Ekonomik Yaşamın ve Sürdürülebilir Kalkınmanın Geliştirilmesi politikası kapsamında yapılacaklar; Güvenli IoT Sistemlerinin(Internet Of Things (Nesnelerin İnterneti))oluşturulması, bir güvenlik zihniyetine sahip işletme yönetiminin geliştirilmesi ve siber güvenliği iş ortamının iyileştirilmesidir.

2-İnsanlar için Güvenli ve Güvenli Bir Toplum Oluşturma politikası kapsamında yapılacaklar; halkın ve toplumun korunmasına yönelik tedbirler

alınması, kritik bilgi altyapısının korunması için önlemler alınması ve hükümet organlarının korunmasına yönelik tedbirler alınmasıdır.

3-Ulusal Güvenliğin ve Uluslararası Topluluğun Barış ve İstikrarını Sağlanması politikası kapsamında yapılacaklar ; ulusal güvenliği sağlanması, uluslararası topluluğun barış ve istikrarını sağlanması, dünyadaki ülkelerle işbirliği yapılmasıdır.

4-Siber Güvenlikle Kesişen Yaklaşımlar Geliştirme politikası kapsamında yapılacakları; Ar-Ge çalışmalarının yürütülmesi, siber güvenlik gücünün geliştirilmesi ve güvenceye alınmasıdır[236]. (Cybersecurity Strategy , 2015)

Yukarıda açıklanan siber güvenlik politikası kapsamında 2016 yılı Ağustos ayında Nesnelerin İnterneti Sistemleri için Genel Çerçeve yayınlanmıştır[237].

Japon hükümeti, 2020 Tokyo Yaz Olimpiyat Oyunları'na kadar üç yıl kala, ulusal siber güvenlik özelliklerini ve politikalarını düzenli olarak gözden geçirmektedir. Hükümet tarafından 2017 yılında üç ulusal siber güvenlik stratejisi yayınlanmıştır. Nisan ayı ortasında ilan edilen Kritik Altyapı için 4.Uygulama Güvenlik Eylem Planı (4th Information Security Action Plan for Critical Infrastructure)[238] ve Siber Güvenlik İnsan Kaynaklarının Geliştirilmesi Programı (Program for Cybersecurity Human Resources Development) ve 2018 için planlanan Siber Güvenlik Araştırma ve Geliştirme Stratejisi (Cybersecurity Reserach and Development Strategy) yayınlanmıştır.

Kritik Altyapı İçin Bilgi Güvenliği Eylem Planı ve Bilgi Güvenliği İnsan Kaynakları Geliştirme Programı ile karşılaştırıldığında,

İlk olarak; Mayıs 2014'te yeni stratejilerinde iki önemli değişiklik yapılmıştır. Birincisi, her iki strateji de işletme yöneticilerinin siber güvenlik alanında proaktif olarak yer almaları gerektiğini ve stratejilerini stratejilerinin

---

[236]Bkz. Cybersecurity Strategy , September 2015, http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf adresinden erişilmiştir. (Erişim Tarihi :19.10.2017)

[237]Bkz. General Framework for Secure IoT Systems belgenin orjinaline http://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf adresinden erişilmiştir. (Erişim Tarihi :19.10.2017)

[238]Bkz.http://afyonluoglu.org/PublicWebFiles/strategies/Asia/Japan%202017%20Cyber%20Security%20Policy%20for%20Crtical%20Infrastructure-EN.pdf

ayrılmaz bir parçası olarak ele alarak risklerini yönetmesi gerektiğini kabul edilmiş olup bu Japon hükümetinin Aralık 2015'teki İş Liderliği için Siber Güvenlik Yönergeleri (Aralık 2016'da revize edilmiş) tarafından sunulan felsefe ile uyumludur. Kritik Altyapı için 4. Uygulama Güvence Eylem Planı, bu dikeydeki örgütlerin liderliğinin, iş stratejilerinde risk değerlendirmesi ve yönetimi dahil ederek bilgi güvenliğine daha fazla karışması gerektiğini ortaya koymaktadır.

Bu aynı zamanda, siber güvenliğin daha fazla iş değeri ve uluslararası rekabet gücü ürettiğine işaret eden Siber Güvenlik İnsan Kaynaklarını Geliştirme Programı için de geçerlidir. Belge, iş dünyası liderliği için siber güvenlik yönergelerini yansıtmakta ve siber güvenlik biriminin bir maliyet merkezi olarak değerlendirilmek yerine fırsatlar getirdiğini ileri sürmektedir. Kılavuzlar, iş adamlarının katılımını teşvik etmek ve siber güvenlik önlemlerini hızlandırmak için Japon siber güvenlik politikalarının ve stratejilerinin geleceğinde önemli bir rol oynamaktadır.

Siber Güvence İnsan Kaynaklarının Geliştirilmesi Programı, Japon iş adamlarının Amerikan ve Avrupa meslektaşlarıyla karşılaştırıldığında hala siber güvenlik konusunda farkındalık yarattığını gösteren bazı endişe verici istatistikler sunulmuştur. Bilgi Teknolojileri Tanıtım Ajansı'nın (IPA) tarafından hazırlanan 2017 raporuna göre, bir çok Japon şirketi çalışanlarının liderlerinin risklere karşı hassas olmadığını ve siber güvenlik altındaki bütçelerinin yetersiz olduğunu düşündüğünü ortaya koymuştur.

Siber Güvenlik Zekası Geliştirme Programı(Program for Cybersecurity Human Resources Development), siber güvenliğin yenilikçiliğin bir unsuru olduğunu savunmasına karşın, kurumsal liderlerin siber güvenlik alanındaki çıkarlarının eksikliği, bu kuruluşların bu tür fırsatlardan yararlanmasını güçleştirmektedir. Japonya'daki siber güvenlik bilincini artırmak, siber tehdit manzarasını ve en iyi uygulamalarını açıklamak ve iş stratejisi ve risk yönetimi perspektiflerinden kaynaklanabilecek olası riskleri basit ve kolay anlaşılır terimlerle açıklamak çok önemlidir.

İkinci olarak, her iki strateji de sektörler arası işbirliği ve bilgi paylaşımının gereğini vurgulanmıştır. Kritik Altyapı için 4.Ulusal Bilgi Güvenliği Eylem Planı,

bu sektördeki şirketleri, çalışanlarına bilgi teknolojisi ve operasyonel teknoloji arasındaki farkı köprülemek ve eğitmek için kendi organizasyonlarına bir göz atmaya teşvik etmektedir. Siber güvenlik ekiplerini de içeren Bilişim Teknoloji departmanları, bilgi güvenliği ilkesi "gizlilik, bütünlük ve erişilebilirlik" öncelikli olma eğilimindeyken, tesisler ve fabrikalarda çalışan Operasyonel Teknoloji Ekipleri, operasyonların ve hizmetlerin çalışmasını sağlamak için kullanılabilirlik ve güvenliği önceliklendirmektedir. Böylece, Eylem faaliyetleri yavaşlarsa, Operasyonel Teknoloji Ekipleri güvenlik ekibinin aciliyetini anlayamamasına sebep olabileceği gibi bu durum kritik altyapı şirketlerinin kontrol sistemlerinin internete bağlı olması ve siber saldırıların elektrik kesintilerine neden olarak hassas bilgileri çalmak ve operasyonlarını aksatılmasına sebep olunabileceği belirtilmiştir.

Bilişim Teknoloji(BT) ve Operasyonel Teknoloji(OT) ekipleri arasındaki başarıyla gerçekleştirilen işbirliğinin siber saldırıların kritik altyapıya yönelik yapılan siber saldırıları önlemek için çok önemli olduğundan Bütçe, kültür ve yapı için işbirliğini teşvik etmek için IT ve OT'yi köprü kurmak için ekip oluşturma gerekliliği vurgulanmıştır.

Nisan 2017'de Japonya Ekonomi, Ticaret ve Endüstri Bakanlığı, 100 Orta Kariyer ve İş İdarecisi yetiştirmek üzere IPA kapsamında Mükemmellik Sınai Siber Güvenlik Merkezi'ni oluşturulmuştur.

Kritik Altyapı için 4. Uygulama Güvence Eylem Planında belirtildiği gibi, siber tehdit istihbarat paylaşımı, başarılı siber saldırıların kritik altyapıya karşı önlenmesi için şarttır. Belge ayrıca, kritik altyapı şirketlerini BT ve OT işlevleri arasında siber tehdit istihbaratını paylaşmada ilk adımı atmanın önemini vurgulamıştır. Güven inşa etme, yüz yüze diyaloglar yoluyla zaman aldığından, COE girişimleri, kritik altyapı şirketlerinin BT ve OT insanlarını diğer kuruluşlardan tanımaları için büyük bir fırsat olacağı belirtilmiştir.

Siber Güvenlilik İnsan Kaynakları Geliştirme Programı, C düzeyinde ve teknik insanlar arasındaki uçurumu kapatan siber güvenlik profesyonellerinin paylaşımına odaklanmaktadır. Onları siber tehdit istihbaratı yerine akademik, endüstri ve hükümet arasında eğitmek ve değerlendirme gerekliliği belirlenmiştir.Stratejide ilk kez üç sektör arasındaki işbirliğinden bahsedilmiştir.

Program, Haziran 2015'te kurulan ve enerji, finans, IT, üreticiler, medya ve demiryolu sektörlerinden 48 büyük Japon şirketi kapsayan ve Sivil Toplumla Mücadele için İnsan Kaynaklarının Geliştirilmesi konusundaki endüstrinin katılımının önemini vurgulayan Sektör Güvenliği İnsan Kaynakları Geliştirme Sektörü Çapraz Sektör Komitesine atıfta bulunmaktadır. Sektörler arası Komite, siber güvenlik uzmanlarını okullar, üniversiteler ve hükümetle işbirliği içinde eğitmek, işe almak, işe almak, eğitmek ve korumak için bir ekosistem kurmayı amaçlamaktadır. Komite Eylül 2016'da çeşitli siber güvenlik işleri ve Japon şirketlerin sahip olması gereken yetenek haritaları ile siber güvenlik eylemlerinin dış kaynak kullanımı hakkında bilgi vermek üzere bir rapor yayınlamıştır.

Komite, Ağustos 2016, Aralık 2016 ve Şubat 2017'de NISC'nin Farkındalık Arttırma ve İnsan Kaynaklarını Geliştirme Siber Güvenlik Komitesine katılarak çalışmalarını paylaşmıştır.

Kuruluşlara verilen kılavuzlara ek olarak, Japonya dışındaki hükümetler ve ticaret dernekleri, Japonya'nın dikkate alması gereken ilgili yönergeleri, mevzuatı ve politikaları haritalandırması gerekmekte olup Japonya'daki ortakları dijital çağda siyasal saldırıları önlemek için yeni nesil siber güvenlik uzmanlarını yetiştirerek ile kritik altyapıyı korumak ve en iyi uygulamaları paylaşmak için gelecekteki stratejileri konusunda birlikte çalışmanın gerekliliği belirtilmiştir[239].

Son olarak Temmuz 2018 yılında Siber Güvenlik Stratejisi[240] yayınlanmıştır.

Strateji belgesi ile hedef olarak sosyo-ekonomik değişim ve sürdürülebilir kalkınma yapmak, insanlar için güvenli bir toplum kurulması , uluslararası topluluk ve Japonya'nın ulusal güvenliğinin barış ve kararlılığına katkısı, siber güvenliğin sürdürülebilmesi için çapraz kesme yaklaşımları belirlenmiş olup Siber güvenlik yaklaşımları açıklanmıştır.

---

[239]Bkz.https://researchcenter.paloaltonetworks.com/2017/11/cso-japans-new-cybersecurity-strategies-right-priorities-mind/ adresinden erişilmiştir. (Erişim Tarihi :19.10.2017)

[240]Bkz.http://afyonluoglu.org/PublicWebFiles/strategies/Asia/Japan%202018%20National%20Cyber%20Security%20Strategy-EN.pdf

Strateji belgesinde 2015 Yılı strateji belgesinde 2018 yılına kadar ki gelişmelere özellikle değinilmiştir. Buna göre 2015 strateji belgesi ile bu belge arasında 2015 Stratejisinin oluşturulmasının ardından, Kamu ve Özel Sektör Verilerinin Kullanımına İlişkin Temel Yasa ve Kişisel Bilgilerin Korunmasına İlişkin Değişiklik Yasası dahil olmak üzere, verilerin kullanımına ilişkin yasal bir temel hazırlanmıştır. Siber-alanın gerçek alanla yüksek düzeyde bütünleştirilmesi yoluyla hem ekonomik gelişme hem de sosyal sorunların çözülmesini sağlayan, insan merkezli bir toplumu gerçekleştirme politikasını benimsemiştir. Bu koşullar altında, sensörler ve cihazlar tarafından gerçek uzayda üretilen büyük miktarlarda veri şu anda siber alanda toplanmakta ve analiz edilmekte olduğu ayrıca gerçek verilerde veri kullanımıyla değer katan yeni ürün ve hizmetlerin sunumu, birçok alanda döngüsel olarak ortaya çıkmakta ve gelişmekte olduğu belirtilmiştir. Artık siber ve gerçek alan bağımsız varlıklar olarak değil ayrı sayılmayacakları şekilde karşılıklı etkileşimde bulunan varlıklar olarak var olduğu belirtilmiştir. Bu nedenle, iki boşluk sürekli gelişen tek bir organik varlık olarak görülmesi gerekliliği vurgulanmıştır.

Siber alan ile gerçek mekanın birleşmesi üzerinde durulmuş, bu birleşmenin topluma bolluğu sağlama potansiyelini önemli ölçüde artırdığı aynı zamanda, kötü niyetli aktörlerin siber kötüye kullanımına yönelik fırsatları da arttırdığı belirtilmiştir. Bu birleşme kapsamında ekonomik ve sosyal kayıp ya da gerçek alandaki hasar riskinin katlanarak artması ve hızlanması beklendiği belirtilmiştir.

Bu şartlar altında, ekonomik toplumun temeli olarak hizmet veren siber alanın güvenliği sağlanması gerektiği ve aynı zamanda topluma sürdürülebilir ilerleme ve refah elde etmek için özerk bir şekilde devam eden evrim ve gelişme gelişmesi sağlanması gerektiği vurgulanmaktadır. Belgede bazı ülkelerin devlet tarafından hakim durumdaki yönetim ve kontrolü vurgulayarak siber tehditlere cevap verme eğilimi olduğu bununla birlikte devlet tarafından yönetim ve siber alanın kontrolünün güçlendirilmesi, özerk ve sürdürülebilir kalkınma olasılığını engelleme etkisine sahip olduğu, bu nedenle günümüzde tüm paydaşların özerk girişimleriyle geliştirilen siber alanlara saygı gösterilmesi ve siber güvenlik bu

paydaşlarla işbirliğine dayalı ve işbirliğine dayalı girişimlerle güvence altına alınması gerektiği üzerinde durulmuştur.

Bu strateji, Japonya'nın ileriye doğru götürdüğü siber güvenliğe ilişkin temel pozisyonu ve yaklaşımı netleştirirken, ortak iç anlayış ve eylem için temel teşkil etmek amacıyla önümüzdeki üç yıl için hem iç hem de uluslararası olarak çeşitli önlemlerin amaçlarını ve uygulama politikalarını açıkça göstermektedir.

2.7.Hindistan

Hindistan, dünyada politik ve stratejik anlamda en önemli ülkelerden birisi olması sebebiyle Bilişim ve Teknoloji alanında önemli yatırımlar yapmakta olup siber alanda güvenliği sağlamak için çeşitli düzenlemeler yapmaktadır.

Hindistan, belirli stratejik eksiklikler, tehdidin yeteri kadar takdir edilmemesi, politikaların oldukça gergin ve kararsız uygulanması nedeniyle siber müdahalelere karşı çok savunmasızdır. Hindistan, siber müdahalelerle başa çıkmak için yasal bir politika belgesi olarak 2000 yılında Bilgi Teknolojisi Yasası'nı ilan etmeye çalışan uluslardan biri olup benzer bir şekilde, Elektronikle İlgili Ulusal Politika 2012'de ve 2013'de Ulusal Siber Güvenlik Politikası yayınlanmıştır.

Hindistan'ın siber güvenlik sorumlusu Gulshan Rai tarafından Temmuz 2017'de parlamentonun finans kurulunda yapılan açıklamada, siber tehditlerin 2000'lerin başındaki virüslerden ve "sıkıntılı" saldırılarından hızlı bir şekilde evrim geçirmiş zararlı yazılımlara ve gelişmiş hizmet reddine dönüştüğünü ve ağır tahribatlı saldırılara maruz kalabileceği, şu anda bir haftada 200 milyon malware ile ilgili siber tehditlerle karşı karşıya kalındığı belirtilmiş olup, Hükümet - Merkez ve devletler - hırsızlık, casusluk ve veri çıkarımı ile taklitçilik arasında değişen nedenlerle yönlendirilen siber saldırıların ana hedefi olduğu ve 2015 ve 2016'da devlet sektörüne yapılan saldırıların tüm siber saldırıların% 27'sini ve% 29'unu oluşturduğu belirtilmiştir. Siber suçluların öncelikli listesinde yüksek olan diğer sektörler, bankacılık, enerji, telekomünikasyon ve savunma sektörünün hükümetle birlikte tüm siber saldırıların dörtte üçünü oluşturduğu belirtilmiştir.

2000 yılındaki Bilgi Teknolojisi Kanunu (Information Technology Act) çıkartılmıştır. Kanun kapsamında genel olarak hacker saldırıları, bilişim sistemi altyapılarındaki güvenlik ihlalleri gibi durumlarla mücadelenin yasal altyapısını oluşturulmuştur. Bu kanun kapsamında kritik bilgi altyapısını doğrudan ya da dolaylı olarak etkileyen bütün bilgisayar ekipman veya kaynakların korunması gereken sistemdir. CERT-In siber savunmayla ilgili gerekli müdahaleleri yapmak ile görevlendirilmiştir[241]. (DURNA, 2012)

Hindistan Bilişim sistemlerine ve bilgi güvenliğine karşı mevcut tehditler karşısında muhtemel tehditlerin tespit edilerek önlem alınması için Hindistan Devleti Bölümlerarası Bilgi Güvenliği Görev Gücü (Inter Departmental Information Security Task Force -ISTF) kurulmuş olup bu kuruluş ve Hindistan'ın Ulusal Güvenlik Konseyi (National Security Council) ile birlikte en üst düzeyde yetkilendirmiştir.

Bu kapsamda Hindistan Devleti Bölümlerarası Bilgi Güvenliği Görev Gücü (Inter Departmental Information Security Task Force –ISTF)nin önerileri ile Ulusal Siber Güvenlik Politikası oluşturulmuştur.

Bu öneriler kapsamında devlet düzeyinde Ulusal bilgi güvenliğine yönelik tehditlerin saptanarak kritik altyapıların tehditlere karşı korunmasının sağlanması ile bilgi güvenliği kapsamında gerekli yasal mevzuatın hazırlanarak siber güvenlik alanında farkındalığın yaratılması, bu kapsamda personelin eğitiminin düzenlenmesi, siber güvenlik alanında gerekli Ar-Ge faaliyetlerinin yürütülmesi amacıyla gereken desteğin verilmesi ve bu çalışmalar için özel sektör ve üniversitelerle ortak çalışmaların yürütülmesi uygulamaya konulmuştur.

Hindistan'ın ilk siber güvenlik strateji belgesi değerlendirildiğinde siber uzay alanının güvenliğinin sağlanması amacıyla Hindistan'ın ana hedef olduğu

---

[241]Bkz. İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü, Siber Güvenlik Raporu, Mayıs 2012, İstanbul, İlke Deniz DURNA: Çalışma Grubu Genel Koordinasyonu + Çin ve Hindistan İncelemesi , sy.6

ülkenin kritik bilişim sistem ve altyapılarına yönelen saldırılar karşısında önlemlerin alınması, saldırıların önlenmesi ve saldırıların karşısında oluşan zafiyetin azaltılması gerektiği belirlenmiştir. Bu hedefler kapsamında siber uzay alanının güvenliğinin sağlanması amacıyla uygulanması planlanan eylem planı hazırlanmış olup bu eylem planı kapsamında bilişim ve bilgi teknoloji sistemlerinin geliştirilerek 7 gün 24 saat saldırı analizlerinin yapılması, ulusal açıdan kritik önem taşıyan altyapıların, ağların ve bilişim sistemlerinin korunması, erken uyarı ve tespit sistemlerinin geliştirilmesi, organize siber saldırılar Hindistan ekonomisine zarar vereceğinden organize siber saldırılara karşı koruma sağlanması, kritik sektörlerde görev yapan şirketlerin bilişim sistemlerinin güvenliğini en üst düzeyde sağlayabilmeleri için onlara araştırma ve geliştirme desteğinin verilmesi öngörülmüştür[242]

Bunların yanı sıra, Hindistan'a ait ağları ve kritik altyapıların korunmasının sağlanması amacıyla Bilgi Güvenliği Çerçeve Politikası hazırlanmış,ulusal düzeyde yürütülen bir Bilgi Güvenliği Farkındalığı ve Eğitimi Kampanyası düzenlenmiştir ve bu kampanya devam etmektedir[243]. (LEWİS & TİMLİN, 2011)

1990'ların sonunda, Hindistan ordusu, elektronik savaş ve bilgi işlemlerini doktrinine dahil etmek için politikasını değiştirmiş olup bu değişiklikle bilgi teknolojileri, elektronik savaş, kritik altyapı koruması ve ordu hareketliliği olmak üzere dört askeri unsurun modernize edilmiştir. Aralık 2009'da, kıdemli Hint Ordusu subayları, Hindistan'ın asimetrik tehditlere, özellikle de siber tehditlere

---

[242]Bkz. İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü, Siber Güvenlik Raporu, Mayıs 2012, İstanbul, İlke Deniz DURNA: Çalışma Grubu Genel Koordinasyonu + Çin ve Hindistan İncelemesi , sy.6

[243]Bkz. Birleşmiş Milletler Silahsızlanma Araştırmaları Enstitüsü (UNIDIR), James A. Lewis – Katrina Timlin, Siber Güvenlik ve Siber Savaş, Ulusal Doktrin ve Organizasyon Yapısının Ön Değerlendirmesi (Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization Center for Strategic and International Studies), s.13-14 (2011) http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf adresinden erişilmiştir.

karşı yeteneği geliştirme gereğini yinelemiştir.

Hindistan, Savunma Bakanlığı bünyesinde siber güvenlikten sorumlu birden fazla birim bulunmaktadır. Bu birimler Savunma Bilişim Savaş Ajansı(The Defence Information Warfare Agency), Savunma istihbarat ajansı(The Defence Intelligence Agency), Ulusal Teknik İstihbarat İletişim Merkezi(National Technical Intelligence Communication Centre)dir.

Savunma Bilişim Savaş Ajansı; bilgi savaşı yanıtlarını koordine etmektedir. Savunma İstihbaratı Ajansı ve Ulusal Teknik İstihbarat İletişim Merkezi; hükümeti potansiyel siber açıklara karşı uyarmak için yasal olarak kesilecek ortak bir "siber tim" oluşturmaktadır. Hindistan Savunma Araştırma ve Geliştirme Organizasyonu (Defence Research and Development Organization) , elektronik savaş sistemlerini test etmek için iki birim geliştirmiştir.

2005 yılında Hint Ordusu, bölünme düzeyinde şebekeleri güvence altına almak ve güvenlik denetimlerini gerçekleştirmek için Siber Güvenlik Kuruluşu(Cyber Security Establishment)'nu kurmuştur.

Ordu, Nisan 2010'da Telekomünikasyon Mühendisliği Askeri Koleji'nde Siber Güvenlik Laboratuvarını da kurmuştur.

Başbakanlığın Araştırma ve Analiz Kanadı elektronik istihbaratın ana kaynağı olup bu kanatta Ulusal Teknik İstihbarat İletişim Merkezi, farklı kurumlara teknik ve elektronik istihbarat sağlamakta ve düşmanlardan gelen haberleşmeyi kesmekle görevlidir.

Hindistan Ulusal Güvenlik Danışma Kurulu((National Security Council Advisory Board) tarafından, ABD'nin Siber Komutanlığı üzerinde modellenen merkezi siber güvenlik talimatının oluşturulmasını ve bu kapsamda Siber Komutanlığın kurulması önerilmiş olup bu kapsamda Ulusal Teknik Araştırma Organizasyonu, Savunma İstihbarat Ajansı ile birlikte, saldırgan siber yeteneklerin geliştirilmesinden sorumludur. Hindistan, siber tehditleri engellemek için teknik ve

operasyonel işbirliğine olanak tanıyan Birleşik Devletlerle bağlayıcı olmayan bir mutabakat muhtırası imzalamıştır[244].

Hindistan Devleti Bölümlerarası Bilgi Güvenliği Görev Gücü'nün önerileri doğrultusunda, Ocak 2004'te Hindistan Acil Bilgisayar Müdahale Ekibi (Indian Computer Emergency Response Team – CERT-In) Bilgi Teknolojileri Departmanı (Department of Information Technology) bünyesinde kurulmuş olup bu ekibin amadı bilgisayar güvenliğine ilişkin olaylara zamanında hızlı ve kapsamlı olarak müdahale etmektir.

Hindistan Acil Bilgisayar Müdahale Ekibi (CERT-In)'in görevleri arasında siber uzay alanının gözetiminin sağlanması ile bu kapsamda siver güvenliğin sağlanması, devletin düzeyleri ve ktirik sektörler için güvenlik standartlarının arttırılması sureti ile uyum sağlama sürecinin yönetilerek güvence altına alınması, erken uyarı ve müdahale sistemleri geliştirilmesi ile bu sistemlerin faaliyete geçirilmesi, bu alanda bilgi paylaşımının sağlanması ve işbirliği kurulması olup kurum bünyesinde adli bilişim laboratuvarları oluşturularak en yeni zararlı kodların analizi düzenli olarak yapılmaktadır.

Ekip (CERT-In) tarafından zafiyetlerin ve açıkların tespit edilmesi amacıyla devlet kurumlarına ve özel sektördeki şirketlere belirli aralıklarla penetrasyon testleri uygulanmakta olup tespit edilen zafiyetlerin giderilmesi için destek verilmektedir.

Hindistan Acil Bilgisayar Müdahale Ekibi (CERT-In) tarafından 2010 yılında Siber Saldırılar ve Siber Terörizme Karşı Kriz Yönetimi Planı

---

[244]Bkz. Birleşmiş Milletler Silahsızlanma Araştırmaları Enstitüsü (UNIDIR), James A. Lewis – Katrina Timlin, Siber Güvenlik ve Siber Savaş, Ulusal Doktrin ve Organizasyon Yapısının Ön Değerlendirmesi (Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization Center for Strategic and International Studies), s.13-14 (2011) http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf Adresinden erişilmiş olup çeviri tarafımdam yapılmıştır.

oluşturmuştur.

Kritik sektörlerde ve devlet kurumlarında siber saldırılara karşı savunmanın arttırılması ve güvenliğin güçlendirilmesi için, kritik sektörlerde iş yapan şirketlere Devlet tarafından, ISO 27001 Bilgi Güvenliği Yönetimi Standardı kapsamında gerekli bilgilendirmeler yapılarak şirket organizasyonlarının dönüşümün yapılması sağlanmaktadır.

"CERT-In Hindistan Bilgi Teknolojileri Departmanına ulusal siber güvenlik stratejisi ve ulusal bilgi güvenliği yönetimi politikası oluşturulması konularında danışmanlık yapmaktadır. CERT-In gelecek için yol haritasını çizerken, sadece olaylara karşı müdahale mekanizmasının siber güvenliği sağlamada tam olarak yeterli olmayacağını, aynı zamanda proaktif bir siber güvenlik politikası oluşturularak gerçek zamanlı bilgi paylaşımına dayalı bir sistemin oluşturulması gerekliliğini saptamıştır. Böylece siber güvenlikle ilgili olay gerçekleşmeden belirli risk parametrelerine ulaşılacak ve gerçek zamanlı bilgi paylaşımına dayalı olarak olay engellenebilecektir.

Hindistan Hükümeti Basın Bilgi Bürosu, yaptığı yazılı bir açıklamada, Hindistan Siber Güvenlik Politikası kapsamında, hassas düzeyde ve devletin güvenliğini ilgilendiren gizli bilgilerin, internete bağlı olan bilgisayarlarda kesinlikle tutulmadığını açıklamıştır. Özellikle Hindistan Dışişleri Bakanlığı'nın, yurtdışındaki misyonlarıyla yaptığı iletişim ve yazışmalar için özel güvenlik standartları geliştirilmiş, bu çerçevede görev yapan bütün personel özel bilgi güvenliği eğitimlerinden geçirilmiş ve bu eğitimler düzenli olarak belirli zaman aralıklarıyla devam ettirilmektedir.

National Informatics Center (NIC) isimli Hindistan Devletine bağlı kuruluş, Hindistan çapında ağ omurgasını sunmakta ve denetlemekte, ayrıca Hindistan Federal Devleti ve bünyesindeki federe devletlere, daha küçük idari birimlere ve belediyelere e-devlet hizmetleri sunulması konusunda destek vermektedir. Bu yüzden NIC altyapısının güvenliği Hindistan Devleti için kritik önemdedir.

Bütün bu sayılanların dışında Ulusal Güvenlik Veri Tabanı (National Security Database-NSD) isimli bir oluşum kurulmuş ve bünyesinde siber güvenlik ile ilgili ve ulusal kritik altyapıların ve bilişim sistemlerinin korunmasıyla ilgili çalışan güvenilir ve donanımlı uzmanların listesi oluşturulmuştur. Bu veri tabanı sayesinde ülkedeki kritik sektörlerde görev yapmak isteyen kişilerin de belli testlerden ve güvenlik soruşturmalarından geçmeleri sağlanmakta ve böylece özel sektörde de bilgi güvenliği açısından insan kaynaklı hataların en aza indirilmesi hedeflenmektedir. Daha yüksek pozisyonlarda ve önemli noktalarda çalışmak isteyen uzmanların, Ulusal Güvenlik Veri tabanı bünyesindeki konumu ve eylemlerine bakılmakta ve ona göre karar verilmektedir.

NSD, Hindistan tarafından da desteklenen kar amacı gütmeyen Information Sharing and Analysis Center (ISAC) isimli bir sivil toplum kuruluşunun projesi olarak geliştirilmiştir. ISAC siber güvenlik alanında kamu-özel sektör işbirliğinin Hindistan'daki başarılı bir örneğidir. NSD'nin amacı, ülkenin neresinde olursa olsun, devletin çok hızlı bir biçimde müdahale etme olanağı olmayan siber güvenlik olaylarında, sivil uzmanların da olaylara müdahale etme kapasitesinin kullanılmasıdır. Bir diğer amaç ise, bilgi güvenliği ve siber güvenlik alanında çalışan nitelikli kişilerin envanterinin çıkarılması ve kritik alanlarda NSD'deki güvenilirlik seviyelerine göre işlerde çalışmalarının sağlanmasıdır[245]."

Hindistan ilk ve tek ulusal siber güvenlik politikasını 2013 yılında yayınlamış olup Ulusal Siber güvenlik Politikası (National Cyber Security Policy)[246] isimli strateji belgesi siber güvenlik ve devlet stratejisi alanlarını kesiştiren ilk

[245]Bkz. İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü, Siber Güvenlik Raporu, Mayıs 2012, İstanbul, İlke Deniz DURNA: Çalışma Grubu Genel Koordinasyonu + Çin ve Hindistan İncelemesi , sy.6

[246]Bkz.http://afyonluoglu.org/PublicWebFiles/strategies/Asia/India%202013%20National%20Cyber%20Security%20Strategy-EN.pdf

belgedir[247].

Hindistan Hükümeti kalkınma politikasının merkezi bir parçası, bağlantıyı artırarak, erişimi genişleterek ve hükümet hizmetlerinin elektronik sunumunu geliştirerek sayısız Hint vatandaşlığını güçlendirmeyi amaçlayan "Dijital Hindistan" kampanyasıdır.

Strateji belgesinde siber güvenlik politikası için kapsamlı bir çerçeve ortaya konulmamış olup temel ilkeler belirlenmiştir.

Stratejiye göre siber saldırılar, suçluların algılamayı artan bir hassasiyetle kaçmasına yardım eden teknikler ve araçlar kullanıyor ve bu hükümetin siber güvenliği "stratejik alan" olarak tanımasına ve uluslararası düzeyde işbirliğini derinleştirmeye yönelik stratejiler geliştirmesi gerekmekte olup siber güvenlik görevleri olan bir dizi sivil ve savunma ajansı kurulduğu belirtilmiştir.

Stratejinin amacı ülkede güvenli bir siber eko sistem oluşturulmasını sağlamaktır.

Strateji belgesi kapsamında Siber Güvenlik Mimarisi Oluşturulması öngörülmüş olup Hindistan, tehdit değerlendirmesi ve paydaşlar arasında bilgi paylaşımı için Ulusal Siber Koordinasyon Merkezi'ni (NCCC) oluşturacak kendi "siber güvenlik mimarisi" ni kuracağı ve NTRO bünyesindeki Siber Operasyon Merkezi ve NTRO bünyesindeki Ulusal Kritik Bilgi Altyapı Koruma Merkezi (NCIIPC) ile silahlı kuvvetler tarafından kritik sektörlerin zaafiyetlerini azaltma ve "kritik bilgi altyapısı" nın savunmasının güçlendirilmesi için iren tehdit yönetimi için ortaklaşa çalışılacağı belirtilmiş olup Aynı zamanda hükümet, siber güvenlikle başa çıkmak için yasal bir çerçeve önermektedir; bu tehdide karşı daha fazla farkındalık yaratmak ve gerekli becerilere sahip insan kaynakları yaratacağı belirtilmiştir.

---

[247]Bkz.National Cyber Security Policy- 2013 belgenin orjinaline http://164.100.94.102/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf adresinden erişilmiştir. (Erişim Tarihi :16.11.2017)

Yukarıda strateji amaçları çerçevesinde Hindistan siber güvenliğin sağlanması ve stratejinin uygulanması için bir takım uygulamaları yürürlüğe koymuştur. Strateji belgesi kapsamında siber güvenliğin sağlanması için yapılan uygulamalar şöyledir.

- Ulusal Siber Koordinasyon Merkezi (NCCC) Siber Güvenlik stratejisinde belirlendiği üzere 2015 yılında Birlik Elektronik Ve Bilgi Teknolojisi Bakanlığı(MEITY), bünyesindeki Hindistan Bilgisayar Olaylarına Acil Müdahale Timi (Indian Computer Emergency Response Team (CERT-In)) e bağlı olarak kurulmuş olup amacı siber güvenlik tehditlerini tespit etmek için ülkenin web trafiğini taramaktır. NCCC'nin ilk aşaması şimdi faal durumdadır ve durumsal farkındalık kazanmak ve bu tehditleri zamanında savuşturmak için meta veri ve çeşitli permütasyonlar kullanarak siber güvenlik açısından büyük yarar sağlaması öngörülmektedir[248].

NCCC, Hindistan'ın hacker ve casus yazılımlara karşı siber güvenliğinin yanı sıra hattaki terörist faaliyetleri izleyen önemli bir bileşeni olmakla bir grup siber güvenlik uzmanı tarafından merkezin işleyişine ve yasadışı ve terör faaliyetlerinin izleneceği, ABD, İngiltere, Fransa ve Almanya'da olduğu gibi benzer çizgilerle ilerlenmesini sağlamak üzere siber istihbarat paylaşımından sorumlu olması öngörülmüştür.

- Botnet Temizleme ve Kötü Amaçlı Yazılım Analiz Merkezi (Cyber Swachhta Kendra Projesi) botnet'lerden kaynaklanan tehditleri engellemek ve sınırlamak amacıyla kurulmuştur. Hindistan'daki botnet saldırılarının tespit edilerek güvenli bir siber alan yaratmak için Ülkede güvenli bir siber eko sistem oluşturulmasını öngören "Ulusal Siber Güvenlik Politikası" kapsamında Elektronik ve Bilgi Teknolojisi Bakanlığı (MeitY) bünyesinde kurulmuş olup Hindistan Hükümetinin Dijital Hindistan girişiminin bir parçasıdır. Proje, güvenli bir siber yaratmayı hedeflemekte olup çeşitli siber suçları için kullanılan botnetlerin sistem

[248]Bkz.https://www.medianama.com/2017/08/223-national-cyber-coordination-centre-launch/ (Erişim Tarihi: 18.11.2017)

tarafından otomatik olarak algılanması ve cihaz sahibinin yardımlarıyla cihazından çıkarması için kullanılacaktır. Bu merkez, İnternet Servis Sağlayıcıları ve Ürün / Antivirüs şirketleri ile yakın koordinasyon ve işbirliği içinde çalışmakta olup web sitesinde, kullanıcıların sistemlerini / cihazlarını güvence altına alacak bilgileri ve araçları sağlamaktadır. Bu merkez, 2000 yılı Bilişim Teknolojisi Yasası uyarınca Hindistan Bilgisayar Acil Müdahale Ekibi (CERT-In) tarafından işletilmektedir[249].

- Strateji belgesi kapsamında Merkezi İzleme Sistemi (Central Monitoring System -CMS) kurulmuştur.

Hükümetin iddialı elektronik istihbarat izleme sistemi olan Merkezi İzleme Sistemi, 2017 yılı sonuna kadar tamamen çalışmaya başlayacak olup İçişleri Bakanlığı yetkililerine göre, telefon görüşmelerine, yazılı mesajlara ve kolluk kuvvetlerine gerçek zamanlı olarak yapılan sosyal medya sohbetlerine engelsiz erişim sağlayacak olan yüksek teknoloji birimi, Delhi ve Bangalore'deki açılış evresinde iki birim olacak şekilde öngörülmüştür.

- Kritik bilgi altyapısına bakacak ve onları bir siber saldırıdan korumak için uygulamaları, politikaları ve prosedürleri geliştirecek özel bir merkez kurulmasına ihtiyaç duyulması sebebiyle bilgi teknoloji yasası kapsamında Ulusal Kritik Bilgi Altyapı Koruma Merkezi (NCIIPC) kurulmuş olup bu kritik sektörleri yöneten diğer güvenlik kurumları ve özel şirketlerle işbirliği içinde karşı önlemler almak üzere, Teknik İstihbarat Ajansı, Ulusal Teknik Araştırma Kurumu (National Technical Research Organization) bünyesinde oluşturulmuştur.

- Strateji belgesi kapsamında Güç Sektörünün Korunması hedeflenmiş olup Aralık 2010'da, Enerji Bakanlığı tarafından enerji sektörü için CERT'ler (Bilgisayar Acil Müdahale Ekipleri) oluşturulmuştur. Bunlar; CERT-Termal (Ulusal Termik Güç Şirketi (National Thermal Power Corporation -NTPC)), CERT-Hydro (Ulusal Hidroelektrik Santrali Kurumu (National Hydroelectric Power Corporation - NHPC)) ve CERT-İletim (Elektrik Şebekesi Limited Şirketi(Power Grid

[249]Bkz. http://www.cyberswachhtakendra.gov.in adresinden erişilmiş olup çeviri tarafımdan yapılmıştır. (Erişim Tarihi: 18.11.2017)

Corporation of India Limited -PGCIL)) dır. Bu CERT lerin amacı kendi alanlarındaki siber saldırıları önlemek için gerekli önlemleri almaktır. Devlet Güç Yardımcı Programlarından, kendi sektörel Kriz Yönetim Planı'nı (Crisis Management Plan -CMP) hazırlamaları ve gerekli eylemler için Kilit Ajanslarla, (NTPC, NHPC ve PGCIL ve CERT) ortak çalışmaları öngörülmüştür.

- Strateji belgesi kapsamında Şebeke Güvenliği Uzman Sistemi (Grid Security Expert System - GSES) kurulmuştur.

Şebeke Güvenliği Uzman Sistemi (Grid Security Expert System-GSES), POWERGRID tarafından geliştirilen ve 132 kV'a kadar olan istasyonlara kadar Gözetim ve Veri Toplama (SCADA) sistemi, sayısal röleler ve Uzak Terminal üniteleri ile güvenilir Optik Fiber Topraklama kablosu bilgi tabanlı ilrtişim sistemidir. GSES'in amacı güvenilir ve güvenli şebeke operasyonunu kolaylaştırmak için Otomatik Savunma mekanizmasının uygulanmasıdır.

- Hindistan, hükümet, kamu ve özel sektör kaynaklarının ve hizmetlerinin kritik bilgi sistemlerinin işleyişinde büyük çaplı aksamanın önlenmesi için strateji belgesi kapsamında siber saldırılara ve siber teröre karşı çıkan bir Kriz Yönetim Planı (Crisis Management Plan -CMP) hazırlamıştır. Siber saldırılara ve siber teröre karşı mücadele için hazırlanan Kriz Yönetim Planı (CMP) ile kritik ulusal süreçleri etkileyen siber olayları hafifletmek ve iyileştirmek için hızlı tanımlama, hızlı yanıt ve telafi edici eylemler için siber olaylarla mücadele için bir çerçeve ortaya konulmuştur.

- Ağ Trafiği Analizi Sistemi (Network Traffic Analysis System- NeTRA) kurulmuş olup bir izleme ve elektronik gözetim projesidir. Hint hükümetinin bireysel hedeflerden çok toplu gözetim girişimi üzerinde gelişmektedir. Bu sistemin Twitter gibi sosyal ağ siteleri üzerindeki faaliyetleri ve postaları tarayacak ve internet trafiğindeki sesleri ve hatta sohbet dökümlerini izleyebileceği öngörülmüştür[250].

[250]Bkz. Yazının orjinaline http://indiafoundation.in/services-view/indias-cyber-security/ adresinden erişilmiştir.(Erişim Tarihi :19.11.2017)

2.8.Rusya:

Rusya'nın internet ve siber güvenlik alanında hukuksal düzenlemelerine bakıldığında, 2003 tarihli İletişim Kanunu[251], 2006 tarihli Kişisel bilgilerin güvenliği konusunda Federal Kişisel Veriler Kanunu (Federal Law on Personal Data)[252] ve 2006 tarihli Bilgi, bilgi teknolojileri ve bilgilerin korunması Bilgi Kanunu[253] un ilk hukuksal düzenlemeler olduğu görülecektir.

Daha sonra 2005 yılında Rusya, 1981 Avrupa Konseyi Kişisel Verilerin Otomatik İşlenmesi (1981 Sözleşmesi) ile İlgili Bireylerin Korunması Sözleşmesini onaylamıştır. Bu kapsamda Rusya, 2006 yılında verinin korunması alanındaki birincil mevzuat kaynağı olan ve bir çok bakımdan AB veri gizliliği mevzuatıyla aynı olan Federal Kişisel Veriler Yasasını kabul etmiştir.[254].

2012 tarihinde "Çocukların Sağlık Ve Gelişimleri İçin Zararlı Bilgilerden Korunmasına İlişkin Federal Kanun Ve Diğer Kanunlarda Değişiklik Yapılmasına İlişkin Federal Kanun" ("On Amending The Federal Law 'On Defending Children From İnformation Harmful To Their Health And Development' And Other Laws Of The Russian Federation (Limiting Access To İllegal İnformation On The Internet)[255] çıkartılmış olup bu kanun "Kara liste Kanunu" olarak da adlandırılmaktadır. Bu kanun kapsamında çocukların zararlı içeriklerden korunması için özellikle uyuşturucu kullanımını öven, intiharı savunan veya intihar yöntemlerini savunan veya çocuk pornografisini içeren içerik ve "aşırılıktan şüphelenilen", "yasadışı toplantı çağrısı içeren", "nefret uyandıran" ve "kurulan

---

[251] Federal Law no 126 "The Law on communications", (2013)
[252] Federal Law no 152 "On personal data protection" (2006)
[253] Federal Law no 149 "On İnformation, information technolojies and protection of information The Law on information"
[254]Bkz.http://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-3/1140166/russia

[255] Federal Law No139"("On amending the Federal Law 'On defending children from information harmful to their health and development' and other laws of the Russian Federation (limiting access to illegal information on the Internet) (2012)

düzeni ihlal eden" diğer tüm eylemlerin, Savcılık tarafından mahkeme kararı olmaksızın engellenebileceği hüküm altına alınmıştır.

2013 tarihinde Bilgi-Telekomünikasyon Ağlarındaki Fikri Mülkiyete Yönelik Rusya Federasyonu Kanunlarında Değişiklik Yapılması Hakkında Kanun "On Amending Laws Of The Russian Federation Which Address Questions Of Protecting İntellectual Property İn İnformation- Telecommunication Networks"[256]çıkartılmış olup bu kanun kapsamında internet korsanlığıyla mücadele etmek için fikri mülkiyet sahipleri ve temsilcileri yapılan görüşmeler neticesinde hazırlanmış olup bu alanda düzenlemeler öngörülmüştür.

2013 tarihinde 'Bilgi, bilgi teknolojisi ve korunması hakkında Federal Kanunun Yasalara aykırı olarak dağıtılan bilgilere erişimi sınırlama prosedürlerini belirleyen bölümün değiştirilmesi hakkında Kanun "On amending the Federal Law 'On information, information technology and protecting information' (the portion that establishes the procedures for limiting access to information which is distributed illegally)"[257]çıkartılmıştır.[258]

2014 tarihinde "Rusya Federasyonu'nun" Bilgi, Bilgi Teknolojisi Ve Bilginin Korunması Hakkındaki Kanunun Ve Diğer Kanunların Bilişim Telekomünikasyon Şebekelerini Kullanarak Bilgi Alışverişi Yapmak İçin Değişiklik Yapılması Hakkında Kanun" "On Amending the Federal Law 'On information, information technology and protection of information' and other laws of the Russian Federation, with regard to codifying information exchanges using

---

[256] Federal law No 187 "On amending laws of the Russian Federation which address questions of protecting intellectual property in information-telecommunication networks(2013)

[257] Federal Law No 398"On amending the Federal Law 'On information, information technology and protecting information' (the portion that establishes the procedures for limiting access to information which is distributed illegally)"(2013)

[258]Bkz. The Berkman Center for Internet & Society at Harvard University , Andrey Tselikov, Research Publication No. 2014-15 November 20, 2014 "The Tightening Web of Russian Internet Regulation", sy.2-4-6 belgenin orjinaline https://cyber.harvard.edu/publications/2014/runet_regulation adresinden erişilmiştir. (Erişim Tarihi: 22.11.2017)

information- telecommunication networks)[259] çıkartılmış olup bu Kanun The Blogger Yasası olarak bilinmektedir. Kanun ile mevcut terörle mücadele yasasında veri yerelleştirme ve veri saklama koşullarını içeren bir değişikliğe gidilmiş olup bu kanun kapsamında Blog yazarlarının isimsiz kalamamalarını sağlamak için gerekli tedbirleri alınması öngörülmüştür. Popüler sosyal medya platformlarının çoğuna yönelik sunucularında sosyal ağların kullanıcıları için altı aylık bir veri bulundurması zorunluluğu getirilmiştir. Rusya'da blogları medya kuruluşu olarak kaydeden ve blog sahiplerinin medya kuruluşları için belirlenen tüm standartlara uymasını zorunlu kılan kanun ile günlük tekil ziyaretçi sayısı 3 bin üzerinde olan tüm blogların yetkili mercilere kayıt olması zorunluluğu getirilmiştir. Ayrıca Rusça içerik sunan ve hedef kitlesi Rusya vatandaşları olan blog yazarları, Rusya dışında yaşasalar bile kanun kapsamında değerlendiirlecek olup yasaya uymayan bloglara Rusya içinden erişim engellenebilecektir[260].

2014 tarihinde "Rusya Federasyonu'nun Bilgi Telekomünikasyon Şebekelerinde Kişisel Bilgilerin İşlenmesi İçin Gerekli Prosedürleri Belirleyen Bazı Kanunlarda Değişiklik Yapılmasına İlişkin Federal Kanun" ("On amending certain laws of the Russian Federation to specify the procedures of processing personal information in information-telecommunication networks")[261] çıkartılmış olup The Localization Law olarakta bilinen bu kanun, Rus kullanıcılarını kişisel bilgilerin Internet üzerinde "işlenmesi" üzerinde daha fazla kontrol sahibi olmalarını sağlamak amacıyla hazırlanmıştır. ("Kişisel bilgilerin işlenmesi", 152 sayılı Federal Kanun'da tanımlanan, toplama, kayıt, sistematizasyon, biriktirme,

---

[259] Federal Law No 97 "On amending the Federal Law 'On information, information technology and protection of information' and other laws of the Russian Federation, with regard to codifying information exchanges using information- telecommunication networks(2014)

[260]Bkz. The Berkman Center for Internet & Society at Harvard University , Andrey Tselikov, Research Publication No. 2014-15 November 20, 2014 "The Tightening Web of Russian Internet Regulation", sy 7 , belgenin orjinaline https://cyber.harvard.edu/publications/2014/runet_regulation adresinden erişilmiştir.(Erişim Tarihi: 22.11.2017)

[261] Federal Law No 242 On amending certain laws of the Russian Federation to specify the procedures of processing personal information in information-telecommunication networks) (2014)

depolama, güncelleme, çıkartma, kullanma, aktarma ve dağıtma gibi bir takım faaliyetlerden herhangi biri olarak tanımlanmıştır.)[262].

2017 yılında "Bilgi, Bilişim Teknolojileri ve Bilgiyi Koruma" konulu Federal kanunda Değişiklik yapılması hakkında Kanun (On Amending Federal Law "On Information, Information Technologies and Information Protection) yayınlamış olup kanun kapsamında kara listeyi uygulamayan anonimleştiriciler ve VPN hizmetleri de dahil olmak üzere Rusya'daki internet filtrelemesini önleme ile ilgili tüm yazılımları ve web sitelerini yasaklanmıştır.

2017 de yayınlanan Rusya Federasyonu Kritik Veri Altyapısının Güvenliği Hakkında Kanun (On the Security of the Russian Federation's Critical Data Infrastructure", Which İntroduces Requirements For İnfrastructure Security (the "CDI Law)[263] kapsamında Rusya'nın kritik verilerin altyapılarının siber saldırılar karşısında güvenli ve istikrarlı olması için düzenlemeler öngörmüş olup CDI Yasası 1 Ocak 2018'de yürürlüğe girecek olup uygulama yönetmelikleri henüz Rus yürütme organları tarafından kabul edilmemiştir[264].

2017 yılında yayınlanan Veri, Bilgi Teknolojileri ve Veri Güvenliği Üzerine olan ve kısıtlı web sitelerine erişmek için kullanılabilecek teknolojileri düzenleyen Federal Kanun[265]da değişikli yapılmasına ilişkin kanun kapsamında (VPN Kanunu) veri ve telekomünikasyon ağları sahipleri ile sınırlı web sitelerine ("VPN teknolojisi") erişmek için kullanılamayan veri kaynakları kullanıcılara VPN

---

[262] Bkz. TSELİKOV, Andrey. (2014, Nov. 20) "*Research Publication No. 2014-15"* The Tightening Web of Russian Internet Regulation. The Berkman Center for Internet & Society at Harvard University, sy 2, belgenin orjinaline https://cyber.harvard.edu/publications/2014/runet_regulation adresinden erişilmiştir.(Erişim Tarihi: 22.11.2017)

[263] Federal Law No. 187 "On the Security of the Russian Federation's Critical Data Infrastructure", which introduces requirements for infrastructure security (the "CDI Law)

[264]Bkz.https://www.cliffordchance.com/briefings/2017/10/new_legislation_regulatingcybersecurityandth.html

[265] Federal Law No. 276 "On Amendments to the Federal Law "On Data, Information Technologies and Data Security", which regulates the technologies that can be used to access restricted websites in Russia (the "VPN Law")

teknolojisi sunmaktan yasaklanmış olup Rusya'daki müşteriler için reklam yayınlayan internet arama motorlarının operatörlerine de belirli yükümlülükler getirilmiştir[266].

2017 yılında yayınlanan Anlık mesajlaşma servis sağlayıcıları için özel yönetmelikleri (" IM Kanunu") tanıtan" Veri, Bilgi Teknolojileri ve Veri Güvenliği Hakkında "Federal Yasanın 10.1 ve 15.4 Maddelerinde Değişiklik Yapılması Hakkında Kanun (On Amendments to Articles 10.1 and 15.4 of the Federal Law "On Data, Information Technologies and Data Security) [267] kapsamında 1 Ocak 2018 tarihinden itibaren anında mesajlaşmanın ("IM") anonim kullanımı yasaklanacak olup IM(Instant Message) servis sağlayıcılarının ("IM Sağlayıcıları") IM Yasası kapsamında bazı yükümlülükleri olması öngörülmüştür. Sohbet sağlayıcılarının getirilen asıl zorunluluk, sohbet kullanıcılarını kendi cep telefon numaralarıyla belirlenmesi zorunluğu olup bu amaçla, IM Sağlayıcıları mobil operatörler ile bir anlaşma yapılması gerekmektedir..Rus IM Sağlayıcılarına mobil operatörler tarafından herhangi bir yardım almadan IM kullanıcılarını tanıma izni verilmiş olup Sohbet sağlayıcıları, sohbet kullanıcılarının tanımlanmasıyla ilgili verileri saklama zorunluluğu öngörülmüştür[268].

Rus bilgi güvenliği politikasının gelişimi jeopolitik ve küresel askeri çatışmaların siber boyutu için önemli etkilere sahiptir. Rusya'nın Ukrayna ve Suriye ile olan ilişkileri konusunda çözülmemiş kriz, Kremlin liderliğini ülkenin bilgi güvenliği politikası için önemli sonuçlar doğurabilecek ilginç bir konuma getirmiştir.

---

[266]Bkz. New legislation regulating cyber security and the internet in Russia (English)https://www.cliffordchance.com/briefings/2017/10/new_legislation_regulatingcybersecurityandth.html (Erişim tarihi: 04.04.2019)

[267] Federal Law No. 241-FZ "On Amendments to Articles 10.1 and 15.4 of the Federal Law "On Data, Information Technologies and Data Security", which introduces specific regulations for instant messaging service providers (the "IM Law")

[268]Bkz. New legislation regulating cyber security and the internet in Russia (English)https://www.cliffordchance.com/briefings/2017/10/new_legislation_regulatingcybersecurityandth.html (Erişim tarihi: 04.04.2019)

Rusyanın askeri alanda siber güvenliğe verdiği öneme değinecek olursak Rusya için savaşın yeni alanı olarak siber uzayın görülmeye başlamasıyla askeri AR-GE çalışmalarına ağırlık verilmiştir. Bu kapsamda 2010 yılında yayınlanan Askeri Doktrinle askeri alanda siber güvenlik faaliyetleri ve korunması değerlendirilmiş olup bu doktrin belgesinde askeri ve askeri olmayan güç ve kabiliyetlerinin modern askeri çatışmalar içerisinde kullanılması ile bilgi savaşının bu çatışmalar içerisindeki rolünü belirtilmiştir. Doktrin belgesi ile olası bir savaş durumunda siber uzaydan gelebilecek tehditler karşısında ordunun hazırlık seviyesini arttırmak ve davranış biçiminin belirlemek amacıyla Rusya Silahlı Kuvvetleri içerisinde her birimde siber birliklerin kurulmasına karar verilmiştir. Ayrıca Rusyanın ulusal çıkar ve amaçları doğrultusunda bu çıkarları gerçekleştirmek ve korumak için ileri ve karmaşık siber saldırı teknikleri kullanılabileceği belirtilmiştir.

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

2000'li yılların başları itibariyle ABD askeri ve istihbarat servislerinin yüksek bilgi ve iletişim teknolojilerine sahip olması Rusya'nın iki devlet arasında olabilecek bir siber savaşı kaybedebileceği korkusunu doğurmuş, bu sebeple de siber güvenlik ve savunma konularında çalışmalarını hızlandırmak durumunda kalmıştır[269]." (ÇELİKTAŞ, 2016)

---

[269] Bkz. ÇELİKTAŞ, Barış. (2016, Mayıs) "*Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme"* Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü , Uluslararası İlişkiler Anabilim Dalı, Uluslararası ilişkiler Programı, Yüksek Lisans Tezi, Trabzon ,

Rusya Federasyonu'nun iç güvenliğinden sorumlu teşkilatı olan Federal Güvenlik Servisi (FSB), internet ve haberleşme dâhil olmak üzere kritik altyapı sektörlerinin korunmasından sorumludur.

Devlet İletişim ve Bilişim Federal Teşkilatı (FAPSI), ülkeye karşı içten ve dıştan gerçekleşebilecek siber saldırıları önceden tespit etmek ve bu saldırılar karşısında gerekli önlemleri alabilmek için gerekli istihbarat çalışmalarını yapmakla sorumludur.

"FAPSI ve FSB'nin casusluk üzerine muhtemel girişimlerde bulunduğuna dair kuvvetli şüpheler uyandıran bilgi toplama programını yürüttüğü düşünülmektedir.

Rusya'nın askeri strateji belgesinde ve ulusal siber savaş doktrini içerisinde siber silahlar büyük öneme arz etmektedir. Bu kapsamda düşman keşif ve elektronik sistemleri üzerinde üstünlük sağlamak maksadıyla çatışma başlamadan önce veya esnasında güç çarpanı olarak kullanılacak olan bu siber silahların, FAPSI ve FSB tarafından uzun dönemli planlama ve istihbarat çalışmaları neticesinde siber savaşta kullanmak amacıyla hazırlanmış, siber hedefler listesi bulunmaktadır[270]."

Ulusal Sınırları içerisindeki kritik internet altyapısının kontrolünü elinde tutan Rusya aynı zamanda çıkardığı mevzuatla yukarıda detaylı açıklandığı üzere internet servis sağlayıcıların yabancı bir ülkenin yetkili birimlerine ağ trafiği ile ilgili bilgi vermesini de yasaklamış ve bilgilerin ulusal sınırları içerisinde kalmasını sağlamaya çalışmıştır. Rusya bilgi güvenliğinin teknik yanlarından çok bilginin içeriğine değer vermekte olup stratejilerini de bilginin içeriğinin erişilememesi ve

---

sy.65-67

[270] Bkz. ÇELİKTAŞ, Barış. (2016, Mayıs) "*Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme"* Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü , Uluslararası İlişkiler Anabilim Dalı, Uluslararası ilişkiler Programı, Yüksek Lisans Tezi, Trabzon , sy.65-67

gizliliğinin sağlanması üzerine kurmuştur.

"Son yıllarda Rusya hükümetinin yakın işbirliği içerisine girdiği yer altı suç örgütleri marifetiyle, onlara araç, malzeme ve zımni destek sağlayarak siber casusluk ve diğer siber saldırı faaliyetlerini gerçekleştirdiği düşünülmektedir. Siber saldırıları özellikle civarındaki ülkelerin kendi çıkarları doğrultusunda hareket etmeleri için bir baskı aracı olarak kullandığı ileri sürülmektedir. Bunun en somut örnekleri arasında yakın geçmişte yaşanmış olan 2007'de Estonya, 2008'de Gürcistan, 2009'da Kırgızistan, 2014-15'te Ukrayna ve 2015'te ise Türkiye siber saldırıları bulunmaktadır[271]."

Rusya tarafından 2013 yılında 2020'ye Kadar Sürecek Uluslararası Bilgi Güvenliği Alanında Rusya Federasyonu Devlet Politikasının İlkeleri(Basic Principles for State Policy of the Russian Federation in the Field of International Information Security (2013)) [272]isimli bir stratejik planlama belgesi yayınlanmıştır.

Rusya Federasyonu'nun stratejik planlama belgesi olan belge kapsamında Uluslararası bilgi güvenliği alanındaki ana tehditler, uluslararası bilgi güvenliği alanında Rusya Federasyonu'nun devlet politikasının amacı, görevleri ve öncelikli yönergeleri (daha fazla - Rusya Federasyonu'nun devlet politikası) ve bunların uygulanma mekanizmaları ile temel ilkeleri tanımlanmaktadır.

Bu belge ile 2020 yılına kadar Rusya Federasyonu'nun ulusal güvenlik Stratejisi belirlenmiş olup uluslararası bilgi güvenliğinin sistemini kurma, hukuki, örgütsel ve diğer sağlayıcı türlerini geliştirme dahil olmak üzere Rus girişimlerinin uluslararası sahnede tanıtımını yapmak; Rusya Federasyonu'nun uygulandığı uluslararası bilgi güvenliği alanında ve eyalet ve federal hedef programlarının katıldığı eyaletler arası hedef programların oluşturulması, uluslararası bilgi

[271]Bkz. Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü , Uluslararası İlişkiler Anabilim Dalı, Uluslararası ilişkiler Programı, Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme, Yüksel Lisans Tezi , Barış Çeliktaş, Mayıs, 2016, Trabzon , sy.65-67

[272]Bkz. Basic Principles for State Policy of the Russian Federation in the Field of International Information Security (2013) belgenin orjinaline https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf adresinden erişilmiş olup çeviri tarafımdan yapılmıştır. (Erişim Tarihi:01.11.2017)

güvenliği alanında Rusya Federasyonu'nun devlet politikasının uygulanmasında bölgeler arası etkileşimin organize edilmesi, ekonominin reel sektöründe bilgi ve iletişim teknolojilerinin daha yaygın kullanımı nedeniyle önde gelen dünya güçleri ile teknoloji paritesinin başarılması ve sürdürülmesi amaçlanmıştır.

Uluslararası bilgi güvenliği alanında ana tehdit, bilgi ve iletişim teknolojilerinin kullanılması olduğu belirtilen ilke belgesinde tehdit unsurları olarak ;

a) Devletlerin toprak bütünlüğünün ihlal edilmesi ve uluslararası barış, emniyet ve güvenlik için tehdit oluşturan, düşman eylem ve saldırganlık eylemlerinin uygulanması için, uluslararası hukuka aykırı olarak askeri-siyasi amaçlardaki bilgi silahı olarak, egemenliğin itibarının bozulması; stratejik istikrar;

b) kritik bilgi altyapısı unsurları üzerinde yıkıcı etki yaratmak ve terörün teşvik edilmesi ve yeni destekçilerin terörist faaliyetlerine cazibe edilmesi dahil olmak üzere terörist amaçlar;

c) egemen devletlerin iç işlerine müdahale etmek, düzensiz davranış, uluslararası, ırklararası ve uluslar arası düşmanlığı teşvik etmek, ırkçı ve yabancı düşmanlığı önermek veya nefret ve ayrımcılık yapan teorileri teşvik etmek, şiddete teşvik etmek;

d) yasadışı olarak bilgisayar bilgilerine erişimini içeren suçların işlenmesi için zararlı bilgisayar programlarının oluşturulması, kullanılması ve dağıtımı belirlenmiştir. Bu tehditler karşısında Rusya'nın devlet politikasının amacı, uluslararası bilgi güvenliği sisteminin oluşturulması için koşulların oluşturulmasına yönelik uluslararası hukuk rejiminin kurulmasına yardım etmektir.

Rusya Federasyonu'nun devlet politikasının amacına ulaşılması için bir eylem planı öngörülmüş olup bu eylem planı kapsamında ;

a) ikili, çok taraflı, bölgesel ve küresel seviyelerde uluslararası bilgi güvenliğinin sisteminin oluşturulması;

b) Hükümetten vazgeçme, devletlerin toprak bütünlüğünü ihlal etme ve uluslararası barışa tehdit oluşturan düşmanca eylemlerin uygulanması için saldırı ve saldırı eylemleri için bilgi ve iletişim teknolojilerinin kullanımında riski azaltacak koşulların oluşturulması, güvenlik ve stratejik istikrar;

c) terörist amaçlarla bilgi ve iletişim teknolojilerinin kullanım tehditlerine karşı mücadelede uluslararası işbirliğinin mekanizmalarının oluşturulması;
d) egemen devletlerin iç işlerine müdahale etmek de dahil aşırılık yanlısı amaçlarla bilgi ve iletişim teknolojilerinin kullanım tehditlerine karşı mücadele için şartların oluşturulması;
e) bilgi ve iletişim teknolojileri kullanımı alanında suç işlemesine karşı uluslararası işbirliğinin etkinliğinin artırılması;
e) Bilgi ve iletişim teknolojileri alanında devlet egemenliğini sağlamak ve gelişmiş ve gelişmekte olan ülkeler arasındaki bilgi eşitsizliğinin aşılmasına yönelik koşulların oluşturulması belirlenmiştir.

Rusya Federasyonu devlet politikasının ana hatları ile şöyledir;

1- İki taraflı, çok taraflı, bölgesel ve küresel seviyelerde uluslararası bilgi güvenliği sisteminin oluşturulması göreviyle bağlantılı olan Rusya Federasyonu devlet politikasının ana hatları;
a) Birleşmiş Milletler Sözleşmesinin üye ülkeler tarafından uluslararası bilgi güvenliğinin sağlanması konusunda gelişme ve kabul edilmesi gereken Rusya girişimi uluslararası alanda tanıtım koşullarının oluşturulması,
b) Birleşmiş Milletler hükümet uzmanlarından oluşan grubun bilgi toplama ve telekomünikasyon alanında elde ettiği başarılarla ilgili olarak yayınlanan sonuç belgelerinde, uluslararası bilgi güvenliği sisteminin oluşturulması alanına giren Rus girişimlerinin kurulmasına yardım edilmesi, uluslararası güvenliğin içeriği ve aynı zamanda Birleşmiş Milletlerin himayesinde, Rusya Federasyonu'nun ulusal çıkarlarına uygun uluslararası bilgi güvenliğinin sağlanmasına ilişkin kuralların geliştirilmesine yardım edilmesi,
c) ikili ve çok taraflı uzman istişarelerini düzenli olarak yapılması, Şangay işbirliği örgütün üye devletlerinin pozisyon ve eylem planlarını onaylanması,
d) bilgi ve telekomünikasyon "Internet" in uluslararasılaştırılmasında Rusya girişimi uluslararası sahnede teşvik edilmesi ve Uluslararası Telekomünikasyon Birliği'nin rolü bağlamında arttırılması;
e) Rusya Federasyonu devlet politikasının uygulanmasına katılan federal icra makamlarının yapısal bölümlerinin örgütsel ve düzenli olarak güçlendirilmesi ve

aynı zamanda bu alanda federal icra makamlarının etkinliğinin koordinasyonunun geliştirilmesi,

e) Uluslararası bilgi güvenliği sisteminin oluşturulması alanındaki Rus girişimlerinin tanıtımının yapılmasını sağlayan analitik ve bilimsel ve metodik geliştirmede Rus uzman topluluğunun katılım mekanizmasının oluşturulması,

g) Uluslararası bilgi güvenliğinin sağlanması için Rusya Federasyonu ile uluslararası devlet anlaşmalarının yabancı devletleri arasında sonuç alınması için şartların oluşturulması,

h) Şanghay üye devlet hükümetleri arasında imzalanan Anlaşmanın katılımcılarının yapısının genişletilmesine yönelik uluslararası bilgi güvenliğinin sağlanmasında işbirliğine ilişkin işbirliğinin işbirliğinin güçlendirilmesi,

i) Birleşmiş Milletler'in bilimsel, araştırma ve uzman kapasitesinin, uluslararası bilgi güvenliği sisteminin oluşturulması alanındaki Rus girişimlerinin tanıtımı için diğer uluslararası organizasyonların kullanılması,

2- Egemenlik, devletin toprak bütünlüğünün ihlal edilmesi ve uluslararası barış, güvenlik ve stratejik istikrar için tehdit oluşturması sebebiyle bilgi ve iletişim teknolojilerinin saldırı eylemlerinin uygulanması riskini azaltma koşullarını yaratma görevinin çözümü ve saldırganlık eylemlerinin uygulanması için uygulanacak Rusya Federasyonu devlet politikasının ana hatları;

a) Askeri-siyasi amaçlar doğrultusunda bilgi ve iletişim teknolojilerinin geniş çapta kullanımı ile bağlantılı olarak ortaya çıkan zorluklara ve tehditlere karşı mücadelede ulusal yaklaşımlar konusunda ilgili devletlerle diyalog geliştirilmesi,

b) düşmanca eylemler ve saldırganlık fiillerinin uygulanması için bilgi ve iletişim teknolojilerinin kullanım tehditlerine karşı mücadele alanında ikili ve çok taraflı düzeyde güven artırıcı önlemlerin geliştirilmesine katılım sağlanması,

c) Bölgesel sistemlerin geliştirilmesine ve uluslararası hukukun geleneksel ilke ve düzenlemelerine (devlet egemenliğine saygı, diğer devletlerin iç meselelerine müdahale etmeme, gayri meşru müdafaa, uluslararası ilişkilerde güç ve tehdit tehdidi kullanımı, bireysel ve toplu kendini savunma hakkı, kişinin haklarına ve temel özgürlüklerine) saygı;

d) Birleşmiş Milletler üye devletlerinin, bilgi ve iletişim teknolojileri kullanımı alanındaki uluslararası insancıl hukuk ilkelerinin ve düzenlemelerinin uygulanmasını düzenleyen uluslararası hukuki düzenlemeler hazırlanması ve kabul etmesi için yardım edilmesi,

e) bilgi silahının yayılmaması için uluslararası yasal rejimin oluşturulması için koşulların oluşturulması.

3- Terörist amaçlarla bilgi ve iletişim teknolojilerinin kullanım tehditlerine karşı uluslararası işbirliğinin mekanizmalarının oluşturulması göreviyle bağlantılı olarak Rusya Federasyonu devlet politikasının ana hatları;

a) Şanghay İşbirliği Örgütü üyesi devletlerle, Bağımsız Devletler Topluluğu Taraf Devletleri, Kollektif Güvenlik Anlaşması Teşkilatı üye ülkeleri, BRICS Taraftarları ile önleme, tanımlama, bastırma, açıklama ve soruşturmayı teşvik eden işbirliği geliştirme ulusal kritik bilgi altyapısı unsurları üzerindeki yıkıcı etkilerin eylemleri, bu tür fiillerin uygulanmasının etkilerinin en aza indirilmesi ve aynı zamanda bilgi ve telekomünikasyon "İnternet" ve diğer bilgi ve telekomünikasyon şebekelerinin terörizmi ve cazibe teşvik amacıyla kullanılmasını engellenmesi,

b) Birleşmiş Milletlerin üye devletlerinin, kritik bilgi altyapısının unsurlarının işleyişinin güvenliği konusunda ileri düzeydeki pratikçiler hakkında bilgi alışverişinde bulunma sırasını belirleyen düzenlemeye hazırlanması ve kabul edilmesi.

4-Egemen devletlerin iç işlerine müdahale etmek de dahil aşırılık yanlısı amaçlarla bilgi ve iletişim teknolojilerinin kullanım tehditlerine karşı mücadele koşullarının oluşturulması göreviyle bağlantılı olarak Rusya Federasyonu devlet politikasının ana hatları;

a) belirtilen tehditlere karşı mücadele için önlemlerin devletlerarası sisteminin geliştirilmesi ve satılması;

b) egemen devletlerin iç işlerine müdahale etmek de dahil aşırılık yanlısı amaçlarla bilgi ve iletişim teknolojilerinin kullanılmasının önündeki sürekli kontrolün uluslararası mekanizmasının oluşturulmasına yardım edilmesi.

5- Bilgi ve iletişim teknolojilerinin kullanımı alanındaki suçla mücadelede uluslararası işbirliğinin verimliliğini artırma göreviyle bağlantılı olarak Rusya Federasyonu devlet politikasının ana hatları;

a) Rus girişimi uluslararası sahnede teşvik edilmesi ve bilgi suçunun karşı tarafı ile mücadele alanında Birleşmiş Milletler'in ve ayrıca Şangay örgütünün üye ülkeleri ile işbirliğinin etkinleştirilmesi, Bağımsız Devletler Topluluğu Taraf Devletleri, Toplu Güvenlik Anlaşması Teşkilatı üye ülkeleri, bu girişimin desteklenmesine ilişkin BRICS Taraf Devletleri ile işbirliğinin zorunlu olduğu

b) bilgi suçu ile mücadele alanında Şanghay'daki işbirliği örgütlenmesinin üye ülkeleri, Bağımsız Devletler Topluluğu Taraf Devletleri, Kolektif Güvenlik Anlaşması Teşkilatının üye ülkeleri, BRICS'in Taraf Devletleri ile üye ülkeler Asya-Pasifik ekonomik işbirliği, üye ülkeler "sekiz Grubun", "Yirmi grup", diğer devletler ve uluslararası yapılar arasında işbirliğinin geliştirilmesi;

c) bilgi ve iletişim teknolojileri kullanımı suçlarında soruşturma süresince eyaletlerin kolluk kuvvetleri arasındaki bilgi alışverişinin etkinliğinin artırılması;

d) Soruşturma teknikleri hakkında bilgi değişimi mekanizmasının geliştirilmesi ve mahkeme tarafından, bilgi ve iletişim teknolojileri kullanımı alanında suçlarla ilgili olarak duruşmanın yapılması.

6-Bilgi ve iletişim teknolojileri alanında devlet egemenliğini sağlamak ve gelişmiş ve gelişmekte olan ülkeler arasındaki bilgi eşitsizliğinin aşılmasına yönelik koşulların yaratılması görevinin çözümü ile ilgili görevi bağlantılı olarak Rusya Federasyonu devlet politikasının ana hatları;

a) gelişmiş ve gelişmekte olan ülkeler arasındaki bilgi eşitsizliğinin aşılmasını teşvik eden uluslararası programların geliştirilmesi ve uygulanmasına yardım edilmesi;

b) ulusal bilgi altyapılarının geliştirilmesine yardım etmek ve dünya topluluğunun devletlerinin küresel bilgi ağlarının ve sistemlerinin oluşturulması ve kullanılması süreçlerine katılımının sağlanmasıdır[273].

Belge kapsamında bakıldığında Rusya'nın uluslararası örgütler ile bilgi güvenliği ve siber güvenlik alanında işbirliğine çok önem verdiği ve ulusal stratejisini de uluslararası örgütlerin belirlediği çerçevede çizdiği görülecek olup ilke belgesi kapsamında Rusya bir çok düzenleme ve uygulamayı hayata geçirmiştir.

11 Eylül 2001'de ABD'de meydana gelen terörist saldırıların ardından teröristlerin kullandığı yöntemler çarpıcı bir şekilde değişmiş olması Rusya'yı da saldırılarla mücadele için yeni güvenlik önlemleri almaya zorlamış olup bu durum Rusya'nın Başkanlık İdaresi'nin resmi bir temsilcisi tarafından "Sosyal ağların ve mikro blogların gittikçe artan popülaritesi, terör ideolojisinin internet üzerinden büyük çapta yayılmasına katkıda bulunmuştur. Modern bilgisayar teknolojileri, teröristlerin intihar bombacısı bulma fırsatı sağlamış olup aynı zamanda siber suçluların sayısı da artmıştır ve özellikle de kişisel bilgilerin çevrimiçi çalındığı ve elektronik ödeme sistemlerine girenlerin sayısı artmıştır. Yeni strateji, ülkedeki bilgi ve BT güvenliğini artırmamıza ve siber suçlularla daha aktif bir şekilde mücadele etmeye başlamamıza yardımcı olmalı. " denilmiş olup anılan gelişmeler ışığından 2014 yılında Rusya yeni bir siber güvenlik strateji belgesi yayınlamıştır.

Rusya tarafından 2014 yılında yayınlanan Rusya'nın Siber Strateji Konsepti(Concept of Russia's Cyber Security Strategy)[274] isimli strateji belgesine

[273] Bkz. Basic Principles for State Policy of the Russian Federation in the Field of International Information Security (2013) belgenin orjinaline https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf adresinden erişilmiştir.(Erişim Tarihi:01.11.2017)

[274]Bkz.Concept of Russia's Cyber Security Strategy, (2014, Jan) https://ccdcoe.org/cyber-security-strategy-documents.html belgenin orjinaline adresinden erişilmiştir. (Erişim Tarihi:01.11.2017)

göre Rusya siber faaliyetleri iç ve dış politikasını etkileyen veya destekleyen casusluk, organize suç siber korsanları tehdit unsuru olarak görmektedir.

2014 strateji belgesi , Rusya Cumhurbaşkanı Vladimir Putin'in 2013 yılında imzaladığı "2020'ye kadar sürecek uluslararası bilgi güvenliği alanında Rusya Federasyonu Devlet Politikasının İlkeleri" politika belgesinde sayılan ilkelerin ve eylem planının bir parçası olarak çıkartılmış olup Rus Güvenlik Konseyi, Dışişleri Bakanlığı, Savunma Bakanlığı, İletişim Bakanlığı ve Adalet Bakanlığı tarafından ortaklaşa hazırlanmıştır.

Ancak Rusya için, siber uzaydaki tehditler hükümet, bireysel özgürlük üzerinde farklı bir perspektif de dahil olmak üzere kimin ve neyin bir tehdit oluşturduğuna dair çok farklı bir görüş birliği içeriyor olsa da Batı devletleri ile tamamen aynı doğrultudadır.

Strateji belgesi ile Rus hükümeti yeni bir siber strateji ile bilgi güvenliğinin sağlanmasının yanı sıra siber suç ve kimlik hırsızlığıyla mücadele için harekete geçmiştir.

Strateji belgesinin amacı, Rus web kaynaklarını ve İnternet faaliyetlerini bilgisayar korsanları, siber teröristler ve yabancı siber casuslar tarafından saldırıya karşı korumak olarak belirtilmiş olup odak noktası, kamu ağlarının ve devlet internet kaynaklarının korunmasıdır. Stratejinin bir parçası olarak hükümet, web sitelerindeki ve kaynaklarındaki siber saldırıları iktidarı ele geçirme girişimleri olarak görmekte olduğu ve bu nedenle katı bir cezai sorumluluk öngörüldüğü belirtilmiştir.

Bu strateji belgesinde Rusya'nın karşı karşıya kaldığı dört temel bilgi ve siber güvenlik tehdidini özetlemektedir.

Birincisi, ulusal hedefleri gerçekleştirmek için kullanılan bilgi silahları olarak, düşman ve agresif fiiller gerçekleştirmek amacıyla bilgi ve iletişim teknolojilerinin kullanılmasıdır.

İkincisi, terörist amaçlar için bilgi teknolojilerinin kullanılmasıdır.

Üçüncü tehdit, bilgisayar bilgilerine yasa dışı olarak erişmenin yanı sıra kötü amaçlı programların oluşturulması ve dağıtılması da dahil olmak üzere giderek artan sayıda siber suçların ortaya çıkmasıdır.

Dördüncü tehdit ise belirgin bir şekilde Rus ve dahili devlet işlerine müdahale etmek, kamu düzenini bozmak, ulusal nefreti (Rusya'da çok büyük bir sorun olarak görülen, pek çok bölgesel gruplaşmalar göz önüne alındığında) harekete geçirmek ve devlet yıkıcı propaganda yapmak için internet teknolojilerinin kullanılmasını içermektedir.

Rusya göre dördüncü tehdidin varlığının temel nedeni, son zamanlarda yaşanan siyasi olayların ve "Arap Baharı[275]" nı takiben Ortadoğu'nun bazı kesimlerinde yaşanan Hükümet karşıtı eylemleri organize etmek ve koordine etmek için kullanılacak internet (özellikle sosyal ağlar) kitlesel karışıklıkların bir sonucu olarak Stratejinin uygulanmasının hem iç hem de uluslararası düzeyde gerçekleşmesi amaçlanmıştır. İkinci olarak ise hükümet, stratejiyi 2013 tarihli ilke belgesinde eylem planı olarak belirttiği üzere müttefikleri ve özellikle Şanghay İşbirliği Örgütü, Kollektif Güvenlik Anlaşması Örgütü ve BRICS üyesi ülkelerle işbirliği içinde uygulamayı planlamaktadır.

Ayrıca strateji belgesi ile Rusya önemli uluslararası bilgi güvenliği girişimlerinin Birleşmiş Milletler tarafından kabul görmesini ve bu kapsamda uluslararası bilgi güvenliğinin sağlanması, siber uzayda uluslararası alanda kabul görmüş bir davranış kurallarının geliştirilmesi, internet yönetim sisteminin uluslararasılaştırılması ve bilgi silahlarının yayılmaması için uluslararası yasal bir rejimin kurulmasını amaçlamaktadır[276].

2000 yılında Rusya ilk Bilgi Güvenliği Doktrinini (Information Security

---

[275] Arap halklarının demokrasi, özgürlük ve insan hakları taleplerinden ortaya çıkmış; bölgesel, toplumsal bir siyasi-silahlı harekettir. Protestolar, mitingler, gösteriler ve iç çatışmalar yaşanmıştır. Bkz. https://tr.wikipedia.org/wiki/Arap_Baharı (Erişim Tarihi: 02.11.2017)

[276]Bkz.https://www.scmagazineuk.com/russia-revamps-its-infosec-strategy/article/541537/ (Erişim Tarihi: 01.11.2017)

Doctrine of the Russian Federation)[277] yayınlanmış olup bu doktrin 2016 yılında Doctrine of Information Security of the Russian Federation[278] ismiyle yenilenmiştir.

Rusya 5 Aralık 2016 tarihinde yayınlanan yeni Siber Güvenlik Doktrini(Doctrine of Information Security of the Russian Federation) belgesi ile son zamanlarda ortaya çıkan ülkenin ulusal güvenliğine yönelik yeni zorlukları ele alınmış olup Ekonomik bir varlık olarak, diğer endüstriyel veya tarımsal kaynakların aksine, bilgilerin ticari olarak değerli bir kaynak sayıldığı strateji belgesi bu açıdan bir ilk olma özelliği göstermiştir. Strateji belgesinde bilgi güvenliği, bilginin bütünlüğünü, güvenilirliğini, erişilebilirliğini, gizliliğini ve zamanlamasını korunması olarak belirtilmiştir.

Rusya'da, bilgi güvenliği sorunları farklı bir şekilde algılanmaktadır.

Birincisi, İnternet teknolojileri, Rusya toplumuna Batı'da olduğu kadar nüfuz etmemiştir. Rus toplumu henüz internete bağımlı değildir. Bununla birlikte, Rusya'nın dünya ekonomisine entegrasyonu ve küreselleşme sürecine katılımı, İnternet'in daha da gelişmesini gerektirmektedir. Bilgi güvenliği ile ilgili zorluklar, diğer siyasi sorular arasında halihazırda öncelik taşımaktadır.

Rusya da kabul edilen ilk bilgi güvenliği 2000 yılında kabul edilmiş olup bu doktrinde internetin o dönem henüz çok yeni oluşu gibi sebeplerle internetten bahsedilmemiştir. Rusya'nın ikinci stratejisi ise (arada yapılan bir çok düzenleme ve strateji belgesi yukarıda açıklandığı üzere mevcut olmasına rağmen Doktrin olarak hazırlanan 2. Belge) tam 16 yıl sonra ortaya çıkmıştır. Bu sebeple günümüz koşullarına daha uygun ve güncel olan bu belge ile önceki stratejik belgesinde belirlenen hükümlerin çoğu geliştirilerek güncellenmiş olmasına rağmen ilk Doktrin belgesi ile benzer bir yaklaşım öngörülmüştür.

---

[277] Information Security Doctrine of the Russian Federation (2000)

[278] Bkz. Doctrine of Information Security of the Russian Federation , December 2016 belgenin orjinaline http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163 adresinden erişilmiştir.(Erişim Tarihi: 01.11.2017)

Bu belge kapsamında karşılaştırıldığında Batılı Devletlerin politikaları esas olarak bilgi güvenliğini teknik güvenlik olarak sağlamaya odaklanmışken, Rusya bilgi içeriğini daha hayati olarak değerlendirmektedir.

Doktrin belgesinin ana hatları şunlardır;

Yeni Doktrin belgesi, bilgi güvenliği konularını bireysel, toplumsal ve hükümet olmak üzere üç aşamalı olarak ele almıştır, 2000 tarihli ilk Doktrinde bireysel menfaatleri önceliklendirilmişse de yeni doktrin ile öncelik olarak bilgi alanındaki ulusal çıkarlara odaklanmıştır. Bilgi alanında Rus ulusal çıkarlarının korunması için mevcut yaklaşımlar güncellenmiştir.

Son yıllarda Rusya hükümeti, bilgi güvenliği için devlet sorumluluğu düzeyini önemli ölçüde artıran bir dizi yasayı onaylamış olup detayı yukarıda açıklanmakla yakın tarihli mevzuatla, tüm İnternet servis sağlayıcılarının (ISS'ler), verileri Rusya'nın topraklarında fiziksel olarak bulunan sürücüler üzerinde depolamaları zorunluluğu getirilmiştir. Bir başka mevzuat ise İnternet Servis Sağlayıcılarının(ISS), kişisel verilerin büyük bir bölümünü toplamasını, altı ay boyunca tutmasını ve özel bir yargılama prosedürü olmaksızın istihbarat ajanslarıyla paylaşmasını gerektirmektedir. Yeni doktrin belgesi bu düzenlemeleri de dikkate alarak hazırlanmış olup yeni stratejinin bir diğer önemli kısmı da dış ilişkilerdir. Belgeye göre, ulusal güvenlik için en ciddi tehditlerden biri olan uygun içeriğin önemi teknolojik güvenlikten daha önemli görülmektedir.

Strateji belgesi kapsamında, askeri siber yeteneklerin kullanılarak geleneksel tehditlerin caydırabileceği belirtilmiş olup bu alanlarda ve siber güvenliğin sağlanmasında uluslararası işbirliğinin önemi vurgulanmaktadır.

Belgede ulusal bir İnternet yönetimi sisteminin geliştirilmesi ve bilgi güvenliğini sağlamak için örgütsel temelli hiyerarşik bir düzen oluşturulması gerektiği, hükümetin bu sistemin çekirdeğini oluşturacağı belirtilmiş olmasına rağmen internet kullanıcıları katılımcılarından bahsedilmemektedir. Bunun yerine, yönetimin güçlendirilerek bilginin merkezileştirilmesi üzerinde durulmuştur. Bu kapsamda strateji belgesi ile Rusya'nın kendisini düşmanca bir ortamda uzun vadeli

bir çatışma ortamına hazırlamak için savunma amaçlı ve saldırgan bir siber yetenek geliştirdiği belirtilmiştir[279].

Strateji belgesi siber güvenliği, gizlilik ve bilgi güvenliğini Rusya'nın ulusal çıkarları için hayati olarak tanımlamış ve bunların korunması için kamu politikası ile halkla ilişkilerin yanı sıra bilgi güvenliğini arttırıcı sistemlerin oluşturulması gerektiği belirtilmiştir.

Belgeye göre Ulusal çıkarlar;

- Vatandaşların anayasal hak ve özgürlüklerinin teşvik edilmesi ve korunması
- Demokratik kurumları, sivil toplumun etkileşim mekanizmasını ve devletini desteklemek
- Rus çok uluslu insanların kültürel, tarihsel, manevi ve ahlaki değerlerinin korunması
- Ve saldırganlık yabancı eylemlerine karşılık olarak barış ve savaş zamanında kritik ulusal bilgi altyapısının sürdürülebilir ve kesintisiz işlemesini sağlama
- Bilgi teknolojileri alanında Rusya Federasyonu'nun gelişimi
- Siber güvenlik ve savunma alanlarında ulusal ve uluslar arası politikalar geliştirmek
- uluslararası siber güvenlik teşvik etmek olarak belirlenmiştir.

Rus hükümeti için kritik önem taşıyan doktrinde yabancı ülkelerden gelen tehditlerde değerlendirilmiş olup, gizlilik kadar, vatandaşların hak ve özgürlüklerinin korunması ilkelerini de önemi belirtilmiştir. Rus enformasyon altyapısının sürdürülebilir ve kesintisiz çalışması için barış zamanında yanı sıra doğrudan tehdit ve saldırganlık zamanlarında birleşik telekomünikasyon ağı olarak özellikle önemli objeler üretilmesine ihtiyaç duyulduğu belirtilmiştir.

---

[279] http://www.russia-direct.org/opinion/what-behind-new-russias-information-security-doctrine (Erişim Tarihi: 05.04.2019)

3. TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKALARI

Dünyada pek çok uluslararası kuruluş ve devlet siber güvenlik stratejileri geliştirmektedir.

Türkiye açısında istatistikler incelendiğinde ülkemizde Emniyet Genel Müdürlüğüne bağlı olarak çalışan ve 2011/2025 sayılı Bakanlar Kurulu Kararıyla[280] kurulan Siber Suçlar Dairesi Başkanlığı'nın kurulmasından önce bilişim suçları ile mücadele görevini Kaçakçılık ve Organize Suçlarla Mücadele Dairesi Başkanlığı yürütmekte olup bu daire tarafından bilişim suçları kapsamında hazırlanan 2011 tarihli istatistikler incelendiğinde; banka ve kredi kartı kullanılarak yapılan dolandırıcılığın bilişim sistemlerine yönelik işlenmiş suçlar arasında en çok rastlanmakta olan suç kategorisi olduğu, 2007-2011 döneminde bilişim suçları alanında kayıtlara giren olay ve şüphelilerin sayısının yükselerek arttığı, genel olarak değerlendirildiğinde işlenmekte olan siber suçları; banka ve kredi kartı dolandırıcılığı, interaktif bankacılık kullanılarak dolandırıcılık, bilgi ve iletişim sistemlerine yönelik suçlar ile internet kullanılarak yapılan dolandırıcılıklar olduğu görülmüştür[281].

2010 yılında bilişim alanında güvenlik problemi yaşamış olan işletme bazında Türkiye'nin 27 ülke arasında 12. Sırada olduğu, tüm dünyada zararlı yazılımların bulaşma oranı kapsamında değerlendirme yapıldığında Türkiye'de zararlı yazılımların bulaşma oranının dünya ortalamasının 3,8 katından fazla olduğu, Türkiye'de %90 oranında Microsoft tabanlı işletim sistemlerinin kullanıldığı, virüs bulaşan internet kullanıcı sayısı bazında bakıldığında 2010 yılı içinde 26 ülkede Türkiye'nin 7. Sırada olduğu, 2005 yılı ile karşılaştırıldığında bu

---

[280] 15 Temmuz 2011 Tarihli ve 27995 Sayılı Resmî Gazetede yayınlanan 2011/2025 sayılı Emniyet Genel Müdürlüğünün Merkez Teşkilatında 1 Adet Daire Başkanlığı ve 9 Adet Şube Müdürlüğü Kurulması Hakkında Bakanlar Kurulu Kararı

[281] Bkz.Kaçakçılık ve Organize Suçlarla Mücadele Dairesi Başkanlığı, Kaçakçılık ve Organize Suçlarla Mücadele 2011 Raporu, KOM Yayınları, Mart 2012, Ankara, sy 63 http://www.kom.pol.tr/Sayfalar/Raporlar.aspx

oran araştırma kapsamındaki ülkelerin büyük çoğunluğunda azalmasına karşın Türkiye'de artışın meydana geldiği tespit edilmiştir[282].

Bunun yanında siber güvenlik alanında çalışmalar yapmakta olan Host Exploit isimli internet sitesi yayınladığı Mart 2014 raporunda Türkiye'nin en kötü 10 ülke listesinde 4. Sırada yer aldığı belirtilmiş, Türkiye; Zeus botnet'leri ve Botnet C&C(Saldırganların yaymış oldukları zararlı yazılımları kontrol eden sunucular) zararlı yazılım barındırma kategorilerinde ilk sıralarda yer almıştır[283].

Aralık 2015'te Türkiye'nin isim çözümleme altyapısı (nic.tr)'ye yönelik siber saldırılar gerçekleştirilmiş, bu saldırılar sonucunda .tr uzantılı internet sitelerine yurtdışı üzerinden erişimlerde ciddi problemler yaşanmış olup bu saldırıları Anonymous adlı uluslararası hacker grubu tarafından üstlenilmiştir. Anonymous tarafından yayınlanan mesaj ile mevcut saldırılarının devam ettirileceği ve sonraki hedeflerin Türkiye'nin finans ve ulaşım gibi kritik altyapıları olduğunu belirtilmiştir. Anonymous grubu tarafından Türkiye'deki birçok bankaya siber saldırılar gerçekleştirilmiş ve bu bankaların bazılarında uzun süreli hizmette kesintiler meydana gelmiştir. Bu saldırıları neticesinde bankacılık sistemleri, ATM cihazları, POS makinaları çalışmadığından siber saldırıların ne kadar etkili olabileceğini ve hayatı durma noktasına getirebileceğini göstermiştir.

2016 yılının Mart ayında İstanbul toplu taşıma araçlarının bilgilendirme yarayan ekranlarında bir hacker "Ekber was here(Ekber buradaydı)" mesajı bırakmıştır. Vatandaşların bilgilendirilmesi maksadı ile kullanılmakta olan bir

---

[282] Bkz.Yrd. Doç. Dr. Hakan HEKİM ; Doç. Dr. Oğuzhan BAŞIBÜYÜK , "Siber Suçlar Ve Türkiye'nin Siber Güvenlik Politikaları -Cyber Crimes and Turkey's Cyber Security Policies", Uluslararası Güvenlik ve Terörizm Dergisi, Cilt 4, Sayı 2 Yıl 2013 sy.146-147

[283]Bkz.HostExploit's World Hosts Report , March 2014 , sy 8 http://hostexploit.com/downloads/world_hosts_report_201403.pdf adresinden erişilmiş olup çeviri tarafımdan yapılmıştır.(Erişim Tarihi: 20.11.2017)

sisteme sızan kişi bu sistemin kullanıldığı tüm araçlarda gösterilen mesajı yazarak ve sistemden çıkmıştır[284].

Yukarıda belirtilen ve çoğaltılabilen istatistikler ve örnekler ışığında siber güvenlik stratejilerinin üretilmesi ve uygulanması öncelikle teknoloji alanında bilgi ve insan kaynağı sağlanmasını gerektirmekte olup bu kaynakların sağlanması için ise ekonomik yeterliliğe ve uluslararası rekabet edebilme potansiyeline ulaşılması gerekmektedir.

Türkiye'nin etkin bir siber güvenlik stratejisi üretme bakımından hukuki ve teknik bir altyapıda eksiklikleri bulunmasına rağmen son dönemde özellikle yapılan düzenlemeler ile siber güvenlik stratejisi kapsamında önemli adımlar atılmıştır.

Türkiye siber güvenlik konusunda en önemli gelişmeler TÜBİTAK bünyesinde Bilgisayar Olaylarına Müdahale Ekibi (TR-BOME) oluşturulmuş olup 2007 tarihli 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'[285]nun Ve 2016 tarihli 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun[286] çıkartılmıştır.

Türkiye'de Siber Güvenliğe ilişkin Hukuki Altyapı incelendiğinde öncelikle hukuki mevzuat değerlendirilmelidir.1926 tarihinden beri 79 yılı aşkın süredir yürürlükte olan ve 06 Haziran 1991 tarihinde ilk olarak bilişim suçları kavramının metne girdiği 765 sayılı (eski TCK) Türk Ceza Kanunu[287]'nu yürürlükten kaldıran

---

[284]Bkz.Bilişim İnovasyon Derneği Siber Güvenlik Raporu , sy 17-18 http://www.bilisiminovasyon.org.tr/webfiles/userfiles/files/siber_guvenlik_raporu.pdf (Erişim Tarihi: 17.05.2017)

[285] 23 Mayıs 2007 tarihli 26530 Sayılı Resmi Gazete de yayınlanan 2007 tarihli 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'

[286] 7 Nisan 2016 Tarihli ve 29677 Sayılı Resmî Gazete de yayınlanan 2016 tarihli 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun

[287] Kabul Tarihi: 01/03/1926 kabul tarihli 13.03.1926 tarihli ve 320 sayılı Resmi Gazetede yayınlanan 765 sayılı Türk Ceza Kanunu 13/11/2005 tarih ve 25642 S.R.G. de yayımlanan 04/11/2004 tarih ve 5252 sayılı kanunun 12. maddesi ile, 1 Haziran 2005 tarihi itibariyle tüm ek değişiklikleriyle birlikte yürürlükten kaldırılmıştır.

Avrupa Birliği'ne uyum yasaları kapsamında hazırlanmış olan ve suçlar ile cezalara yeni düzenleme getiren 5237 sayılı Türk Ceza Kanunu (TCK)[288] 1 Haziran 2005 tarihi itibari ile yürürlüğe girmiş olup kanunun metnini özümsediği eski 765 sayılı TCK ya ek olarak bilişim alanında işlenen suçlara oldukça geniş yer verilmiştir.

Yeni TCK ile birlikte; Bilişim Suçları, onuncu bölüm altında "Bilişim Alanında Suçlar" başlığı altına ayrıca düzenlenmiş ve eski TCK düzenlemelerine ek olarak Banka ve Kredi Kartlarına karşı işlenen suçlar ve Tüzel Kişilerin bilişim suçları işlemesine dair düzenlemeler konulmuştur. Kanun kapsamında bilişim alanında suçlar ayrıca düzenlendiği gibi klasik suçların bilişim veya elektronik ağlar vasıtasıyla işlenmesi suçun nitelikli hali olarak değerlendirilmiştir. Örnek olarak bilişim vasıtaları kullanılarak işlenen dolandırıcılık suçu "nitelikli dolandırıcılık" olarak Dolandırıcılık klasik suçunun nitelikli hali sayılarak değerlendirilmiş ağırlaştırıcı sebep olarak kabul edilmiştir.

TCK'da Onuncu Bölüm olarak Bilişim Alanında Suçlar değerlendirilmiş olup TCK md.243, 244,245 ve 246 da Bilişim alanında suçlar tanımlanmıştır.

TCK'nın anılan maddeleri incelendiğinde elektronik ağlar aracılığı ile işlenen suçların büyük çoğunluğuna yer verildiği görülmekte olup siber güvenlik konusunda ise Türk Ceza Kanunu'nda belirlenen bilişim alanında suçların çok genel tasnif edilmesi ve suç ve ceza belirlenirken failin failin motivasyonunun göz önüne alınmaması kanunun en büyük eksiğidir. Bu kapsamda kanunda bu suçlara ilişkin düzenlenen cezaların fail tarafından hedef alınan sistemin hassasiyeti ile failin amacı birlikte değerlendirilerek dengenin sağlanması gerekmekte olup mevcut durumda en yaygın siber ihlallerden olan casusluk yapılması ya da terörist aktivite amacıyla siber alanın kullanılması ve siber saldırılar düzenlenmesi durumunda saldırıyı düzenleyen kişi ile, kendini ispatlamak veya sırf eğlence olsun diye siber saldırı düzenleyen kişi arasında bir fark gözetilmemiş fail ayrımı yapılmamıştır. Terörizm veya casusluk faaliyetleri kapsamında bilişim suçu işleyen fail ile böyle bir amacı olmaksızın

[288] 12.10.2004 Resmi Gazete Tarihi ve 25611 sayılı Resmi Gazete de yayınlanan 2004 tarihli 5237 sayılı Türk Ceza Kanunu (TCK)

hackerlık yapan bir kişi arasında ayrım gözetilmemiş olup ceza hukuku bakımından hackerlık, hacktivizm ve siber terör kavramları birbirinden ayrılabilmiş ve netleştirilmiş değildir. Ayrıca bir çok ülkenin aksine siber terörizm konusunda Terörle Mücadele Kanunu'nda da özel bir düzenleme yapılmamıştır.

Bilişim suçları alanında bir diğer bir kanun 5271 sayılı Ceza Muhakemesi Kanunu[289]dur (CMK). Kanun kapsamında "*bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma*" başlıklı 134. maddesinde dijital delillerin toplanma ve muhafaza edilme usulüne ilişkin hükümler düzenlenmiştir.

Siber güvenlik alanında Türkiye için iç hukuk mevzuatlarının yanında Avrupa Konseyi Siber Suçlar Sözleşmesi[290]nin de iç hukukta yürürlüğe konması çok önemli bir gelişmedir. Türkiye, 2001 yılında kabul edilen Avrupa Konseyi Siber Suçlar Sözleşmesi'ni 10/11/2010 tarihinde çekinceler belirtilerek imzalamış, Onay kanunu 02.05.2014 tarihinde Resmi Gazetede yayınlanmıştır[291].

Ülkemizin sözleşmeye taraf olması siber güvenlik açısında önemi bir gelişme olup, Sözleşmenin onaylanması ve uygun iç hukuk düzenlemelerinin yapılması ile siber güvenlik politikası bakımından önemli bir ilerleme kaydedilmiştir. Avrupa Konseyi Siber Suçlar Sözleşmesi 26/12/2012 tarihi itibari ile ABD dahil olmak üzere 38 ülke tarafından kabul edilmiştir.

5237 sayılı TCK ile karşılaştırdığında sözleşmenin daha detaylı olarak hazırlanmış olduğu ve çocuk pornografisine ilişkin tanımın yapılarak bu alanda başkaca ek tanım ve hükümleri de içerdiği görülmektedir.

---

[289]Bkz.17.12.2004 tarihli ve 25673 sayılı Resmi Gaztede yayınlanan 2004 tarihli 5271 Sayılı Ceza Muhakemesi Kanunu (CMK)

[290]Bkz.ETS No:185 Convention On Cybercrime, Budapest, 23/11/2001 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (Erişim Tarihi: 20.11.2017)

[291] Bkz.02.05.2014 tarihli ve 28988 sayılı Resmi Gazetede yayınlanan 22.04.2014 kabul tarihli 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunmasına Dair Kanun

Sözleşmeye ek olarak Avrupa konseyi tarafından AB üyesi ülkelerin hukuki ve kurumsal alanda uyumlarının sağlanması amacı ile çerçeve niteliğinde kararlar alınarak yürürlüğe konulmuş, bu çerçeve kararları da iç hukukumuzda yapılması gereken mevzuat değişikliklerinde dikkate alınması gereken uluslararası metinlerdir.

Türkiye'de Siber Güvenliğe ilişkin Hukuki Altyapı incelendiğinde değinilmesi gereken bir diğer kanun 2007 tarihli 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'[292]dur.

5651 sayılı Kanun kapsamında yasadışı içerikler ve siber ortamda bulunanların sorumlulukları düzenlenmiş olup Kanunun yürürlüğe girmesinden sonra uygulamanın düzenlenmesi amacıyla bir takım yönetmelikler de çıkarılmıştır. Buna göre; yasa dışı içerikleri ile içerik, yer ve erişim sağlayıcılarının sorumlulukları ve yükümlülükleri belirlenmiş olup yasadışı içerikler hakkında hangi hallerde ve hangi makamlar tarafından erişimin engellenmesi yapılabileceği düzenlenmiştir. Kanunun 8 inci maddesi kapsamı dışındaki erişimin engellenmesi kararlarının uygulanabilmesinin sağlanması amacıyla Erişim Sağlayıcılar Birliği kurulmuş olup Birliğe üye olmayan internet servis sağlayıcılarının faaliyette bulunamayacağı hükme bağlanmıştır. Bu sayede erişim engelemeleri kararlarının tek noktadan idaresi mümkün hale getirilmiştir.

Erişim engellenmesi yöntemi ve 8. Maddenin 4. Fıkrasında "İçeriği birinci fıkrada belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulunsa bile, içeriği birinci fıkranın (a) bendinin (2) ve (5) ve (6) numaralı alt bentlerinde yazılı suçları oluşturan yayınlara ilişkin olarak erişimin engellenmesi kararı re'sen

[292] Bkz.23 Mayıs 2007 tarihli 26530 Sayılı Resmi Gazete de yayınlanan 2007 tarihli 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

Başkan tarafından verilir. Bu karar, erişim sağlayıcısına bildirilerek gereğinin yerine getirilmesi istenir." Hükmü çok tartılışmakta olup Cumhuriyet Savcısına dahi hakim onayına sunulmak üzere verilen erişim engelleme tedbirinin uygulanması yetkisinin Bilişim Ve Teknoloji kurumu Başkanına münhasıran verilmesi kanunun en çok tartışılan hükmü olmuştur. Bu madde kapsamında belirtilen suçlar 2) Çocukların cinsel istismarı 5) Müstehcenlik (madde 226) ve 6) Fuhuş (madde 227), maddeleridir.

Mevzuat Konusundaki düzenlemeler Türkiye açısından bakıldığında son yıllarda gelişme kaydedilmiş olmasına rağmen hem ceza kanunlarında hem de diğer kanunlardaki eksiklikler sebebiyle yaptırımsal yönden eksik kalmaktadır. Bu nedenle TCK ve CMK kapsamında siber suçlara karşı etkili bir mücadele verilmesine olanak tanıyacak düzenlemelerin yapılması gerekmektedir.

Bu konuda önemli bir diğer eksiklikte siber terör alanında mevzutta herhangi bir tanım yapılmamasıdır. Siber terör ile hukuk kuralları kapsamında mücadele edilebilmesi için öncelikle tanımın yapılması gerekmekte olup akabinde bu kapsamdaki fillere uygulanacak yaptırımlar belirlenmeli ve bu alanda düzenlemeler yapılmalıdır.

Türkiye'nin siber güvenlikle ilgili olarak kurulmuş ilk kurumu Bilgi Teknolojileri ve İletişim Kurumu(BTK)dur. 2000 yılında kurulmuş olan BTK olup elektronik haberleşme alanında düzenleyici bir kurum olarak görevlendirilmiş olup kurum olarak görevlendirilmiştir. Bağımsız olması öngörülen kurumun görevi siber güvenliği sağlanmasıdır.

09.11.2016 tarih ve 6757 sayılı Yasa ile 5809 sayılı Elektronik Haberleşme Kanunu'na eklenen maddeler ile BTK'ya kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunma bu saldırılara karşı caydırıcılık sağlamak için gerekli her türlü önlemin alınması yada aldırılması görevi verilmiştir. Bu görevin yanında kamu kurum ve kuruluşları da dahil olacak şekilde ilgililere yaptırım uygulanması yetkisi de BTK'ya verilmiştir. Ayrıca BTK'ya söz konusu görevi kapsamında ilgili yerlerden bilgi, belge, veri, kayıt alma ve değerlendirme;

arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanma, bunlarla irtibat kurma ile kamu kurum ve kuruluşları da dâhil olmak üzere ilgili taraflara yaptırım uygulama yetkisi de verilmiştir.

Bilgi Teknolojileri ve İletişim Kurumu(BTK) tarafından 2010-2012 Stratejik Planı, 2013-2015 Stratejik Planı ve son olarak 2016-2018 Stratejik Planı olmak üzere üç adet stratejik plan yayınlamıştır.

BTK tarafından yayınlanan 2016 Faaliyet Raporu kapsamında, 2017 yılın içerisinde aşağıdaki çalışmaların gerçekleştirilmesi planlanmıştır.

Buna göre dört temel program belirlenmiştir.

1-Kapasite İnşası Programı (İK ve Eğitim)

2-Hızlı tespit – Erken müdahale programı (Teknolojik önlemler)

3-Siber tehdit istihbarat edinimi ve paylaşımı programı (iş birliği ve iletişim)

4-Kritik altyapıların ve verilerin korunması programı olarak belirlenmiştir[293]. (Bilgi Teknolojileri ve İletişim Kurumu Faaliyet Raporu, 2016)

BTK Elektronik Haberleşme Kanunu[294]'nun 6. Maddesi ile BTK "Siber güvenlik ve internet alan adları konularında Bakanlar Kurulu, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri yerine getirmek" hususunda görevlendirilmiş, 2016 faaliyet raporu kapsamında İşletmecilerin Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği[295]'nde belirtilmiş

[293]Bilgi Teknolojileri ve İletişim Kurumu Faaliyet Raporu (2016) https://www.btk.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fSayfalar%2fFaaliyet_Raporlari%2f2016_Faaliyetraporu_TR.pdf (Erişim Tarihi: 21.11.2017)
[294]Bkz. 10.11.2008 tarihli 27050 sayılı mükerrer resmi Gazetede yayınlanan 5809 sayılı 05.11.2008 tarihli Eketronik Haberleşme Kanunu
[295]Bkz.13.07.2014 tarihli ve 29059 sayılı Resmi Gazete'de yayımlanan Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği.

olan yükümlülüklerin yerine getirilmesinin kontrolünün yapılması amacı ile planlı denetimlerin yürütülmesi öngörülmüş, bunun yanında siber saldırıların, hizmet kesintilerinin ve diğer güvenlik ihlallerinin önlenmesi amacıyla alınması gereken tedbirler ve yapılması gereken faaliyetlerin incelenerek plansız denetimler gerçekleştirilmiş ve buna bağlı olarak 2016 yılı içinde toplamda 19 işletmecinin denetlendiği belirtilmiştir[296].

2011 yılında Devlet Planlama Teşkilatı tarafından "e-Türkiye İnsiyatifi Eylem Planı 2002", e-Dönüşüm Türkiye Projesi ve Kısa Dönem Eylem Planı (2003- 2004)" ve "e-Dönüşüm Türkiye Projesi 2005 Eylem Planı" isimli belgeler yayınlanmıştır.[297]

Siber Güvenlik alanında düzenlenen diğer kanunlar ise 2004'te kabul edilmiş olan 5070 sayılı Elektronik İmza Kanunu[298], 2008'te kabul edilmiş olan haberleşme sektöründe düzenlemeler yapan Elektronik Haberleşme Güvenliği Yönetmeliği[299], 2006 yılında 28242 sayılı Resmi Gazete'de yayınlanan 2006/38 sayılı Yüksek Planlama Kurulu Kararı[300]yayınlanmış olup kararın ekinde Bilgi Toplumu Stratejisi ve Bilgi Toplumu Stratejisi Eylem Planı sunulmuştur.

---

[296]Bkz.Bilgi Teknolojileri ve İletişim Kurumu Faaliyet Raporu , 2016 https://www.btk.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fSayfalar%2fFaaliyet_Raporlari%2f2016_Faaliyetraporu_TR.pdf

[297] Bkz.BIÇAKÇI, Doç. Dr. Salih; ERGUN, E. Doruk, ÇELİKPALA, Prof. Dr. Mithat (2016, Mart) "*Türkiye'de Siber Güvenlik ve Nükleer Enerji"*, Türkiye'de Siber Güvenlik, EDAM, 1. Baskı, İstanbul, sy.31 http://edam.org.tr/document/CyberNuclear/SiberKitapTR/edam_siber_guvenlik_raporu.pdf (Erişim Tarihi:21.11.2017)

[298]Bkz.23.01.2004 tarihli 25355 sayılı Resmi Gazetede yayımlanan 15.01.2004 tarihli 5070 sayılı Elektronik İmza Kanunu

[299]Bkz.20.07.2008 tarihli 26942 sayılı Resmi Gazetede yayınlanan Elektronik Haberleşme Güvenliği Yönetmeliği

[300]Bkz.28.07.2006 tarihli 26242 sayılı Resmi Gazetede yayınlanan 11.07.2006 traihli yüksek Planlama Kurul Kararı ve eki Bilgi Toplumu Stratejisi ve Bilgi Toplumu Stratejisi Eylem Planı http://www.bilgitoplumu.gov.tr/Documents/1/BT_Strateji/Diger/060500_BilgiToplumuStratejisi.pdf

Bilgi Toplumu Stratejisi Eylem Planı kapsamında Stratejinin Öncelikleri ve Eylemlerle İlişkisi belirlenmiş olup 2006-2010 dönemini kapsayan Bilgi Toplumu Stratejisi ve eylem planında ana hedef olarak güvenlik ve kişisel verilerin korunması yer almakta olup plan kapsamında siber güvenlik alanındaki tehditlerin düzenli olarak takibinin yapılması, alınması gereken tedbirler hakkında uyarıların yapılarak uyarı yayınlanması, alınması gereken tedbirler hakkında gerekli bilgilendirme ve koordinasyonun sağlanması amacı ile Bilgisayar Olaylarına Acil Müdahale Merkezi (TR-BOME) kurulması öngörülmüş, bu kapsamda Türkiye Bilimsel ve Teknik Araştırma Kurumu (TÜBİTAK) bünyesindeki Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) sorumlu kurum olarak tespit edilmiştir[301]. (BIÇAKÇI, ERGUN, & ÇELİKPALA, 2016)

Belge kapsamında stratejik öncelikler ve hedefler ;

a)Sosyal Dönüşüm hedefi ile vatandaşlar tarafından bilgi ve iletişim teknolojilerinin gündelik ve iş hayatından etkili kullanılmasının sağlanması ile ekonomik ve sosyal alanda faydanın arttırılması hedeflenmiştir.

b)Bilgi ve iletişim teknolojilerinin iş dünyasına etkisi hedefi ile küçük orta ve büyük işletmelerin bilgisayar sahibi olması ve internete erişimlerinin arttırılması suretiyle elektronik ticaretin teşvikinin sağlanması ve stratejik öneme sahip sektörlerin ve bölgelerin bilgi ve iletişim teknolojilerine olan ihtiyaçlarının belirlenerek bu ihtiyaçların karşılanması amacıyla sektörlere özel olarak verimliğe dair programların uygulamaya geçirilmesi hedeflenmiştir.

Belirlenen hedeflerin ana teması olarak ise devlet ile yapılacak işlerde kolaylık sağlanması, bilgi edinme ortamı sağlanması, işletmelerin ve çalışanlarının bilgi iletişim teknolojilerinde yetkinliklerinin geliştirilmesi ile e-ticaretin geliştirilmesi öngörülmüştür.

---

[301] Bkz.BIÇAKÇI, Doç. Dr. Salih; ERGUN, E. Doruk, ÇELİKPALA, Prof. Dr. Mithat (2016, Mart) "*Türkiye'de Siber Güvenlik ve Nükleer Enerji"*, Türkiye'de Siber Güvenlik, EDAM, 1. Baskı, İstanbul, sy.31 http://edam.org.tr/document/CyberNuclear/SiberKitapTR/edam_siber_guvenlik_raporu.pdf

c)Vatandaş Odaklı Hizmet Dönüşümü hedefi ile kamu hizmeti, bilgi ve iletişim teknolojilerinin de yardımı ile, kullanımı yoğun ve getirisi yüksek hizmetlerden başlamak üzere elektronik ortama taşınması ve iş süreçlerinin kullanıcının ihtiyacına yönelik olarak yeniden yapılandırılmak suretiyle hizmetin sunulmasında etkinlik sağlanması hedeflenmiştir.

d)Kamu Yönetiminde Modernizasyon hedefi kapsamında verimliliğin ve vatandaşın memnuniyetinin öncelikle gözetilerek ilkenin koşulları ile uyumlu örgütsel ve süreç yapılandırmalarına sahip etkili bir elektronik devlet (e-devlet) oluşumunun sağlanmasının bilgi ve iletişim teknolojileri desteği ile hayata geçirilmesi hedeflenmiştir.

Hedefin ana teması olarak ise bilgi toplumu kurumsal yapılanması ve yönetişimi, ortak teknolojik hizmet ve altyapının sağlanması, etkin tedarik yönetiminin sağlanması, veri ve bilgi yönetimi, elektronik iletişim sağlanması, insan kaynağı ve yetkinlik gelişimi ile güvenlik ve kişisel bilgilerin mahremiyetinin sağlanması belirlenmiştir. Güvenlik ve Kişisel Bilgilerin Mahremiyeti teması altında ise bilgi güvenliği alanında gerekli mevzuat düzenlemelerinin yapılması eve bilgisayar olaylarına acil müdahale merkezlerinin kurularak kamu kurumlarının bilişim güvenliğinin sağlanması eylemleri sayılmıştır.

e)Küresel Rekabetçi Bilgi Teknolojileri Sektörü hedefi ile bilgi teknolojileri hizmet alanı kapsamında proje bazlı hizmetlerin ve kamu ile özel sektörün işbirliği ile sektörel yetkinliğin geliştirilmesi suretiyle dış pazara açılım yapılması ile paket yazılım alanında rekabet avantajı sağlatan sektör bazlı çözümlenerek odaklanılması hedeflenmiştir.

f)Rekabetçi, Yaygın ve Ucuz İletişim Altyapı ve Hizmetleri hedefi kapsamında iletişimin altyapısı ve hizmetlerinin geliştirilmesi ve yaygın olarak kullanılmasının sağlanması amacıyla telekomünikasyon sektörünün hizmet ve altyapılarında etkili bir rekabet ortamının tesis edilmesi ve bu sayede hızlı, güvenli, sürekli ve kaliteli iletişim hizmetinin daha uygun bedellerle sunulması ile yeni teknolojiye dayanan telekomünikasyon altyapıları kurulması için uygun zemin yaratılması hedeflenmiştir.

Bu hedefin ama temaları kapsamında; telekomünikasyon sektöründe rekabetçi ortam oluşturulması, iletişim hizmetlerine ilişkin vergi düzenlemesi ile iletişim altyapısının yaygınlaştırılarak geliştirilmesi belirlenmiştir.

g)Ar-Ge ve Yenilikçiliğin Geliştirilmesi hedefi kapsamında küresel pazarda giderek artan talepler kapsamında yenilikçi ve yüksek katma değere sahip bir alan olan bilgi ve iletişim teknolojileri sektörü için araştırma ve geliştirme faaliyetlerine öncelik verilmesi ile bu alan için yeni teknolojiler geliştirilerek üretime dönüştürülmesinin desteklenmesi hedeflenmiştir. Diğer yandan araştırma-geliştirme ve yenilikçi faaliyetlerin geliştirilerek etkinleştirilmesi amacıyla bilgi ve iletişim teknolojilerinden maksimum fayda sağlanması hedeflenmiştir[302].

Hukuksal mevzuatımız açısından en önemli düzenlemelerden biri de 2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun[303]dur.

Avrupa Konseyi tarafından hazırlanarak 28 Ocak 1981 tarihinde Strazburg'ta imzaya açılmış olan ve 1 Ekim 1985 tarihinde yürürlüğe giren 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, Türkiye tarafından 28 Ocak 1981 yılında imzalanmış olmasına rağmen uzun süre onaylanmamış ve gerekli iç hukuk düzenlemeleri yapılmamıştır. Yaklaşık 21 yıllık bir bekleyişin ardından 30 Ocak 2016 tarihinde kabul edilen 6669 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun ile onaylanmak suretiyle 18 Şubat 2016 Tarih ve 29628 Sayılı Resmî Gazetede yayımlanarak aynı tarihte yürürlüğe girmiştir.

Uygun bulma kanunu kapsamında ülkemizde kişisel verilerin korunması amacıyla özel bir kanun hazırlanmak üzere ilk komisyon 1989 yılında kurulmuş

---

[302]Bkz. http://www.resmigazete.gov.tr/eskiler/2006/07/20060728-7.htm adresinden erişilmiştir. (Erişim Tarihi:23.11.2017)

[303] Bkz.7 Nisan 2016 Tarihli ve 29677 Sayılı Resmî Gazete de yayınlanan 2016 tarihli 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun

olmasına karşın kanun uzun bekleyişin ardından 6698 sayılı Kişisel Verilerin Korunması Kanunu 24 Mart 2016 tarihinde nihayet TBMM'nde kabul edilerek kanunlaşmıştır. Kanunun amacı kişisel verilerin işlenmesinde özel hayatın gizliliği, kişilerin temel hak ve özgürlüklerini korunması ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasların düzenlenmesi olup kanunun kapsamı ise kişisel verileri işlenen gerçek kişiler ve bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanmasıdır.

Bu kanun kapsamında kişisel verilerin işlenmesi hakkında ilkeler belirlenmiştir. Bu ilkeler; işlemenin hukuk ve dürüstlük kurallarına uygun olması, doğru ve gerektiğinde güncel olması, kişisel verilerin belirli, açık ve meşru amaçlar için işlenmesi, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ile ilgili mevzuatta öngörülmüş olan veya işlendikleri amaç için gerekli olduğu süre kadar muhafaza edilmesidir. Kural olarak kişisel verilerin ilgili kişinin açık rızası bulunduğu durumlar veya maddede sayılmış olan istisnalar haricinde işlenmesi yasaktır. Kanun kapsamında kişinin açık rızası olmasa dahi kişisel verilerin işlenebileceği özel haller ayrıca düzenlenmiş olup kanunun getirdiği bir diğer yenilik ise kişinin Sendika üyeliği kişisel veri olarak sayılmıştır[304].

Yukarıda detaylıca açıklanan hukuksal düzenlemeler neticesinde Türkiye'de siber güvenlik alanında Bilgisayar Olaylarına Müdahale Ekibi (TR-BOME), TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) bünyesinde kurularak faaliyete başlamıştır.

---

[304]Bkz. KORKMAZ,İbrahim (2016) "*Kişisel verilerin korunması kanunu hakkında bir değerlendirme (an assessment of the law on protectıon of personal data)*".TBB Dergisi. Sayı 124, sy.83 http://tbbdergisi.barobirlik.org.tr/m2016-124-1571 (Erişim Tarihi: 23.11.2017)

Türkiye'nin Bakanlar Kurulunca alınan Haziran 2012 tarih ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar[305] ile Ulaştırma Denizcilik ve Haberleşme Bakanlığı başkanlığında ulusal siber güvenliğin sağlanmasına yönelik politikaları belirlemek, strateji ve eylem planlarını hazırlamakla görevli Siber Güvenlik Kurulu oluşturulmuştur.

Bunun yanı sıra anılan Bakanlar Kurulu Kararında; kamu kurum ve kuruluşlarına ait bilgi ve verilerin güvenliği ile gizliliğinin güvence altına alınmasının sağlanmasına dair usul ve esasların hazırlanması, ulusal bilgi teknolojileri ve iletişim altyapısı ve sistemleri ile veri tabanlarının güvenliğinin sağlanması, kritik altyapıların belirlenerek bu altyapılara yönelen siber tehdit ve saldırıların izlenmesi, müdahale ve önlem sistemlerinin oluşturulması amacıyla ilgili merkezlerin kurulması ve kurdurulması, bu sistemlerin denetimlerinin yapılması ile işletiminin ve sürekli olarak güçlendirilmesine dair çalışmaların yapılması Ulaştırma, Denizcilik ve Haberleşme Bakanlığının görevleri arasında sayılmıştır[306].

Ulusal siber güvenlik alanında kamu kurum ve kuruluşları tarafından yapılması gereken çalışmalar için gerekli olan maddi kaynağın planlanma ve kaynağın tahsisinin öncelikle yapılması öngörülmüştür.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın bu konu hakkındaki görevleri belirlenmiş, buna göre bakanlık ulusal siber güvenlik alanında güvenliğin sağlanması amacıyla politikaların belirlenmesi, strateji ve eylem planlarının hazırlanması, kamu kurum ve kuruluşlarına ait olan bilgi ve verilerin güvenliğinin

---

[305]Bkz. 20.10.2012 tarihli 28447 sayılı Resmi gazetede yayınlanan 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Kararın yürürlüğe konması hakkında Bakanlar Kurulu Kararı

[306]Bkz.20.10.2012 tarihli 28447 sayılı Resmi gazetede yayınlanan 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Kararın yürürlüğe konması hakkında Bakanlar Kurulu Kararı
http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf

ve gizliliğinin sağlanması amacıyla usul ve esasların belirlenmesi ile bu konuda gerekli altyapının oluşturulmasının takip edilmesi ile görevlendirilmiştir.

Bu karar kapsamında Telekomünikasyon İletişim Başkanlığı bünyesinde siber güvenliğe dair meydana gelen olaylarda ulusal koordinasyon ve uluslararası işbirliği birimi olarak faaliyet göstermesi için 27 Mayıs 2013'te Ulusal Siber Olaylara Müdahale Merkezi (USOM- TR CERT) kurulmuştur. Telekomünikasyon İletişim Başkanlığı'nın mülga olmasının akabinde faaliyetlerine 2000 tarihinde kurulan Bilgi Teknolojileri ve İletişim Kurumu(BTK) kapsamında devam etmektedir. USOM, 6757 sayılı Kanun[307]ile doğrudan BTK'ya bağlanmış olup USOM tarafından 31.10.2016 tarihinde USOM - SOME 1. İstişare Toplantısı düzenlenmiştir. Bu toplantıya elektronik haberleşme alanında faaliyet gösteren işletmecilerin SOME ekipleri katılmış olup, toplantı konuları olarak USOM tarafından yürütülmekte olan projeler ve en ulusal siber güvenliğin sağlanması amacıyla koordineli çalışılması ve bilgi paylaşımının yapılması görüşülmüştür[308]. (Bilgi Teknolojileri ve İletişim Kurumu Faaliyet Raporu , 2016)

BTK'ya bağlı Ulusal Siber Olaylara Müdahale Merkezi (USOM – TRCERT) tarafından Temmuz 2014 te Siber Güvenliğe İlişkin Temel Bilgiler isimli bir rehber hazırlanmış ve yayınlamış olup rehberde Temel Siber Güvenlik Kavramları, Siber Saldırıların Kaynakları, Siber Saldırı Türlerine ilişkin bilgiler verilmiştir[309]. (Bilgi Teknolojileri Ve İletişim Kurumu, 2014)

---

[307] Bkz. 24.11.2016 tarihli ve 29898 sayılı Resmi Gazete'de yayımlanan 6757 sayılı Olağanüstü Hal Kapsamında Bazı Kurum ve Kuruluşlara İlişkin Düzenleme Yapılması Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabul Edilmesine Dair Kanun.

[308]Bkz.Bilgi Teknolojileri ve İletişim Kurumu Faaliyet Raporu, 2016 https://www.btk.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fSayfalar%2fFaaliyet_Raporlari%2f2016_Faaliyetraporu_TR.pdf (Erişim Tarihi: 23.11.2017)

[309]Bkz.Bilgi Teknolojileri Ve İletişim Kurumu,Telekomünikasyon İletişim Başkanlığı, (2014, Temmuz) Ulusal Siber Olaylara Müdahale Merkezi (USOM -TRCERT). *Siber Güvenliğe İlişkin Temel Bilgiler,*

Ayrıca Merkez tarafından 17.12.2014 tarihinde DDOS El Kitabı, 17.12.2014 tarihinde Akıllı Telefonlar ve Güvenlik, 17.12.2014 tarihinde Çevrimiçi Oyunlar, 17.12.2014 tarihinde Taşınabilir Cihaz Kullanımına İlişkin Riskler, 05.01.2015 tarihinde Sızma Testi Teknik Kriterleri Programı, 06.01.2015 tarihinde Siber Olaylara Müdahale Ekipleri Kurulum Adımları, 13.01.2015 tarihinde Sızma Testi Hizmeti Veren Personeli Ve Firmalar İçin Yetkilendirme Programları, 2015-02-02 tarihinde Kurumsal SOME Etkinliği Sunumları, 2016-08-04 tarihinde Kurumsal SOME Rehberi ve 2016-08-04 tarihinde Sektörel SOME Rehberi yayınlanmıştır[310].

2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar kapsamında kurulan siber güvenlik Kurulu tarafından yapılan çalışmalar sonucunda Ulusal Siber Güvenlik Stratejisi 2013-2014 Eylem Planı belirlenmiş olup Türkiye'nin ilk Ulusal Siber Güvenlik Stratejisi olan Ulusal Siber Güvenlik Stratejisi 2013- 2014 Eylem Planı[311] yayınlanmıştır. Bu eylem planı kapsamında büyük kitlelere sunulan kritik hizmet ve servislerin çoğunun altyapısının internete dayalı olması sebebi ile siber güvenlik imkanlarının araştırılarak ihlallerin soruşturulmasına dair ulusal ve uluslararası hukuksal düzenlemelerin yetersiz kalması, kurumların siber güvenlik konusunda bilişim sistemleri altyapısı; çalışanlar bilgi, bilinç ve tecrübelerinin yetersizliği ile donanım/yazılım alanında yerli üretimin yeterli seviyede olmaması Türkiye'nin siber güvenlik politikasında dikkate alınması gereken etkenlerdendir.

Yayınlanan bu eylem planına göre yeni yasal düzenlemeler yapılması ve müdahale ekipleri kurulması planlanmıştır.

Eylem Planında belirlenen hedeflere göre; ulusal alanda siber güvenliğin sağlanabilmesi konusunda öncelikle mevcut eksikliğin giderilmesi amacıyla mevzuatsal düzenlemeler yapılması gerekliliği, siber saldırıların kaynağının tespit

---

[310] Bkz.https://www.usom.gov.tr/dokuman.html (Erişim Tairih:24.11.2017)

[311] Bkz.20.06.2013 tarihli 28683 sayılı Resmi Gazete de yayınlanan 2013/4890 sayılı Bakanlar Kurulu Kararı ve ekinde Ulusal Siber Güvenlik Stratejisi 2013- 2014 Eylem Planı http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf.

dilmesi ile saldırıların etkilerinin belirlenebilmesi amacıyla güvenilir kayıt mekanizmaları ile USOM'la koordineli çalışacak sektörel ve kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) oluşturulması gerekliliği, tüm kurumların bilişim sistemlerinin siber güvenlik altyapılarının güçlendirilerek gerekli teknolojilerin sağlanması, siber güvenlik konusunda insan kaynağının yetiştirilerek gerekli bilinçlendirme faaliyetleri yapılması, siber güvenlik alanında yerli teknoloji geliştirilmesi ile ulusal güvenlikten sorumlu kurumların siber güvenlik alanında çalışmaları ile savunmalarının kapsamlarının genişletilmesi planlanmaktadır.

Ulusal Siber Güvenlik Stratejisi kapsamında siber güvenlik alanında belirlenmiş olan stratejik hedeflere yönelik atılacak somut adımlar öncelikle ulusal Siber Güvenlik Kurulu kurulması, siber güvenlik alanında farkındalığının artırılması, ülkemizde siber güvenlik kültürü yaygınlaştırılması için çalışmalar yapılması, kişisel ve kurumsal bilginin korunması amacıyla gereken tedbirlerin alınması, uluslararası alanda işbirliğinin güçlendirilerek ulusal siber güvenliğe dair araştırma ve geliştirme politikalarının oluşturulması ve yerli teknolojilerin geliştirilmesinin sağlanması, üniversitelerde bu alanda bilimsel çalışmaların arttırılması amacıyla çalışmalar yapılması, insan kaynaklarının yetiştirilmesi ve mevcut kaynakların geliştirilmesi amacıyla çalışmalar yapılması, kurumsal siber güvenlik yeteneklerin arttırılması amacıyla çalışmalar yapılması ve kurumların siber güvenliklerinin test edilebilmesi amacıyla sızma testleri (pentest)uygulamaları yapan bağımsız merkezlerin oluşturulması ve gereken mevzuatsal düzenlemelerin düzenlenmesi olarak belirlenmiştir[312].

Siber suçlarla mücadele için öncelikle ulusal ve uluslararası hukuki alt yapının etkililiği sağlayacak bir şekilde düzenlemesi gerekmektedir. Siber alanın ülkeler ve sınırlarla bağlı olmaması nedeniyle uluslararası işbirliğinin sağlanması ve uluslararası sözleşmelerin imzalanması en az iç hukuk mevzuatının düzenlenmesi kadar önem taşımaktadır.

---

[312]Bkz.http://www.karabulut.co/ulusal-siber-guvenlik-stratejisi/ (Erişim Tarihi:24.11.2017)

Eylem planı, diğer strateji belgeleri ile e-Dönüşüm Türkiye Projesi kapsamında, TÜBİTAK'a Bilgisayar Olaylarına Müdahale Merkezi kurma görevi verilmiştir.

TÜBİTAK BİLGEM (Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) ve Bilgi Teknolojileri ve İletişim Kurumu ortaklığında 2011 yılı Ocak ayında siber tatbikat gerçekleştirilmiştir. Yine Ocak 2013'te 2. Siber Güvenlik Tatbikatı gerçekleştirilmiş olup Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın ortaklığında BTK ve TÜBİTAK tarafından birlikte yürütülen ve siber saldırılara hazırlık amaçlı yapılan Ulusal Siber Güvenlik Tatbikatı 2013'e 61 kamu ve özel sektör kuruluşu katılmıştır. Tatbikat 24 Aralık 2012 - 11 Ocak 2013 tarihleri arasında gerçekleşmiştir.

Tatbikata katılan katılımcıların büyük çoğunluğunu kamu kurumları oluşturmasına karşın özel sektör ve sivil toplum kuruluşları da katılmıştır.

Tatbikat katılımcıları arasında elektronik haberleşme, enerji, savunma, finans, sağlık vb. kritik altyapıların yönetilmesi ve işletilmesinden sorumlu kurum ve kuruluşlar ile adli ve kolluk birimleri katılmış olup katılımcıların teknik, hukuk ve iletişimden sorumlu birim personelleri tatbikat kapsamında görevlendirilmiştir. Yapılan tatbikatla katılımcılar arasında kurumlar içi ve kurumlar arası işbirliğinin sağlanması, koordine hareket edilmesi, siber saldırılara karşı yeteneklerinin geliştirilmesi ile siber güvenlik alanında farkındalığın arttırılması ile ulusal siber güvenliğe katkı sağlanması amaçlanmıştır.

2013 yılındaki Ulusal Siber Güvenlik Tatbikatına katılan katılımcıları sayısı 2011 yılındakilerin % 50 fazlasını oluşturmuş olması siber güvenlik alanında ulusal ulusal farkındalığın arttığını göstermektedir[313].

[313] Bkz.https://www.btk.gov.tr/tr-TR/Sayfalar/SG-Ulusal-Siber-Guvenlik-Tatbikati-2013 (Erişim Tarihi: 23.11.2018)

2011 tarihli Ulusal Siber Güvenlik Tatbikatı(USGT) 41 kurum ve kuruluş katılım sağlanmış, tatbikat kapsamında 500 den fazla yazılı enjeksiyon uygulanmış, bunun yanında port taraması, dağıtık servis dışı bırakma saldırısı (DDoS), web uygulamaları denetim ve kayıt dosyalarının analizi içerikli gerçek saldırılar yapılmıştır. Türkiye tarafından düzenlenen bu tatbikatlar diğer ülkelerden farklı olarak gerçek saldırı ve savunma teknikleri kullanıldığında siber güvenliğin pratik uygulamalarının gösterilmesi yönünden büyük önem taşımakta mevcut duruma çok yakın uygulamaların yapılmasını sağlamaktadır.

USGT 2011'in sonuçlarını gösterir sonuç raporunda bazı dikkat çekici tespitlere yer verilmiştir. Buna göre;

Bazı katılımcıların yaşanmakta olan güvenlik olayları karşısında sadece teknik çözüm aradıkları ancak güvenlik zincirinde en tepede bulunan insan faktörünün göz ardı edildiği, birtakım katılımcı kurum ve kuruluşların çalışanlarını sosyal mühendislik saldırıları için farkındalık sağlanması için gerekli eğitimlere tabi tutmadıkları, bir kısım katılımcıların bu tip saldırıların engellenmesi amacı ile kullanıcılarına periyodik olarak uyarı amaçlı elektronik postalar göndermek ve kurum içinde belli yerlerde bilgi güvenliğine ilişkin uyarıcı asmak vb hatırlatıcı yöntemleri etkili olarak kullanmadıkları, bir kısım katılımcıların çalışanlarının bu tip saldırılar karşısında bağışıklığının arttırılması amacıyla düzenlik olarak sosyal mühendislik testleri yaptırmadığı, bir kısım katılımcıların merkezi antivirüs sunucuları imza dosyalarını periyodik olarak güncellemediği, bir kısım katılımcıların erişim amacıyla iş ve güvenlik gereksinimleri kapsamnda bir erişim kontrol politikası bulunmadığı, bu sebeple çalışanların kendileri ile alakası bulunmayan bilgi ve hizmetlere erişim sağlayabildiği, bir kısım katılımcıların internete bağlı olan bilgi sistemlerinde gerçekleştirilen "Port Tarama" saldırısının varlığını algılayamadıkları, bir kısım katılımcıların internete bağlı olan bilgi sistemlerine yönelik gerçekleştirilen DDoS saldırıları sonucu kurumların çoğunda hizmetlerin kesintiye uğradığı, hizmetlerinde kesinti yaşamayan katılımcıların İSS'lerinden bu tip saldırılara karşı koruma sağlanması amacı ile hizmet satın aldığı, belirlenmiştir. Bu tespitler bilgi güvenliğinin sağlanabilmesi için kurumların

arasındaki iletişim ve işbirliğinin önemi ile koordineli çalışmanın gereklerini ortaya koymuştur.

Rapor kapsamında bir kısım katılımcıların siber güvenlik konusunda ulusal mevzuat ile ilgili yeterli bilgi sahibi olmadıkları, bu sebeple tatbikat kapsamında gerçekleştirilen yazılı senaryolarda bulunan ve yasal düzenlemelerde bilişim suçu kapsamında tanımlanmış bazı faaliyetleri adli merciye bildirmediği belirlenmiştir.

Tatbikat neticesinde katılımcı kurum ve kuruluşların bilgi güvenliği kapsamında büyük miktarda açığının bulunduğu ortaya çıkmıştır.

Tespit edilen açıkların giderilmesi amacıyla bilgi teknolojileri kapsamında yapılacak donanımsal ve yazılımsal satın alımları ile diğer yatırımların yeterli olamayacağı, öncelikle bu kurum ve kuruluşları yöneticileri başta olmak üzere personelin tamamının da bilgi güvenliği alanında yeterli eğitimi alması ve bu alanda kurumsal iş süreçlerini hayata geçirmeleri gerekmektedir.

Tatbikat sonucu ve yapılan tespitler birlikte değerlendirildiğinde kurumsal alanda siber güvenlik önlemlerinin alınması ve siber güvenliğin hayata geçirilmesi amacıyla çalışmalar yapılırken alınacak önlemlerin personelin bilgi ve yeteneğine olan bağımlılığı azaltılması, gerekli denetim ve iyileştirme anlayışının kuruma yerleştirilmesi amacı ile Bilgi Güvenliği Yönetim Sistemleri (BGYS)'nin gerekliliği görülmüş bu kapsamda tatbikat senaryoları gerçekleştirilirken bilgi güvenliği olayına gerekli müdahalenin yapılması aşamasında BGYS'ye sahip olan kurumların daha sistematik olarak sorunları çözmeye çalıştıkları görülmüştür.

Hizmet kesintilerinin önlenmesi ve mevcut bir kesinti durumunda sistemin en kısa sürede tekrar çalışır hale getirilmesinin sağlanması kapsamında ise iş sürekliliği çalışmalarının önemi ortaya çıkmıştır. Yapılacak analizler ile kurumların öncelikli olarak iş sürekliliği planları oluşturmaları gerekmekte olup öncesinde iş sürekliliği kapsamında belirli çalışmaları yapmış olan kurum ve kuruluşların tatbikatta gerçekleştirilen senaryolarda meydana getirilen hizmet kesintileri ile daha etkili olarak mücadele ettikleri ve sistemleri çok daha kısa sürelerde çalışır hale

getirdikleri tespit edilmiştir.

Siber güvenlik alanında siber güvenliğin sağlanmasının ilk adımı insanı eğitmektir. Bu kapsamda öncelikli olarak çalışanlara gerekli eğitimlerin verilmesi, yeterli sayıda çalışan istihdamının sağlanması, sistem yöneticilerinin işlettikleri sistemlere yönelik hakimiyetlerinin arttırılması amacıyla eğitimler planlanması ve bilgi güvenliğinde uzman personelden oluşan ayrı bir birim kurularak gerekli uzmanlık eğitimlerinin planlanması gerekmektedir.

Meydana gelen bilgi güvenliğine dair olaylara kurum ve kuruluşların tek başlarına mücadelesi mümkün değildir. Bu anlamda kurum ve kuruluşlar arasındaki koordinasyonun sağlanması ve kurum içi tüm birimlerin veya kurum dışı işbirliklerinin güçlendirilmesi büyük önem taşımaktadır[314].

Bunların yanında Türkiye'de yaşanan siber güvenlik gelişmeleri şu şekilde özetlemek mümkündür;

2011'de Ulusal Siber Güvenlik Strateji Belgesi Çalıştayı düzenlenmiştir.

Siber terörizm Milli Güvenlik Siyaset Belgesi'ne dahil etmiştir.

2013-2014 Eylem Planı kapsamında USOM'un koordinasyonunda çalışması planlanan sektörel ve kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) oluşturulmuştur.

Eylem planı kapsamında kamu kurum ve kuruluşlarının bünyesinde faaliyet gösterecek SOME'ler (Kurumsal SOME, Sektörel SOME) oluşturulması öngörülmüştür.

Ulaştırma Bakanlığı'nın başkanlığında kurulacak Siber Olaylara Müdahale Ekipleri (SOME) ler Suçları ve saldırıları önlemeye yönelik görev yapacak olup bünyesinde İçişleri Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu, Telekomünikasyon İletişim Başkanlığı, Emniyet Genel müdürlüğü, Jandarma Genel

[314] Bkz. 2011 tarihli Ulusal Siber Güvenlik Tatbikatı Sonuç Raporu, sy 24-44

Müdürlüğü, TÜBİTAK gibi kurumlar bulunması planlanmış olup Siber suçlarla mücadele ekipleri(SOME), kolluk kuvvetleri ile koordineli çalışması ve olaylara derhal müdahale yetkisine sahip olması öngörülmüştür.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın dördüncü Eylem Maddesi "Ulusal Siber Olaylara Müdahale Merkezinin (USOM) kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) oluşturulması" kapsamında Kasım 2013 Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ[315]" Resmi Gazete'de yayımlanmıştır.

Kurumsal SOME kurma yükümlülüğü taşıyan kurumların faydalanabilmesi için "Kurumsal SOME Kurulum ve Yönetim Rehberi" ve "Sektörel SOME Kurulum ve Yönetim Rehberi" isimli rehberler hazırlanmıştır.

Genelkurmay Başkanlığı bünyesinde siber saldırı tehdidine karşı Muhabere ve Siber Savunma Komutanlığı, Türk Silahlı Kuvvetleri'nin bilgi güvenliğini korumak amacıyla oluşturulmuştur.

2006 yılında 2006-2010 dönemini kapsayan Bilgi Toplumu Stratejisi[316] yayınlanmış olup strateji belgesi kapsamında Ulusal Bilgi Sistemleri Güvenlik Programı'nın en önemli unsurlarından birisi olarak Ulusal Bilgi Güvenliği Kapısı Projesi öngörülmüştür. Türkiye'de bilgi güvenliği alanında internet üzerinde bilgi paylaşım yapılmasına yarayan bir bilgi paylaşım alanı oluşturulması amacıyla kurulan web sitesi www.bilgiguvenligi.gov.tr adresi üzerinden (adres linki https://egitim.sge.gov.tr olarak değişmiştir.) 2008 tarihinden itibaren yayın yapmaktadır. Site içerisinde bilgi güvenliği alanında okuyucunun bilgilendirilmesi amacıyla teknik içerikli yazılar, bilgi güvenliğine dair kılavuzlar ve ülkemizde

---

[315] Bkz. 11 Kasım 2013 Tarihli ve 28818 Sayılı Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ

[316] Bkz. 28.07.2006 tarihli 26242 sayılı Resmi Gazetede yayınlanan 11.07.2006 traihli yüksek Planlama Kurul Kararı ve eki Bilgi Toplumu Stratejisi ve Bilgi Toplumu Stratejisi Eylem Planı http://www.bilgitoplumu.gov.tr/Documents/1/BT_Strateji/Diger/060500_BilgiToplumuStratejisi.pdf

yapılması planlanan etkinlikler, toplantı ve sempozyum gibi organizasyonlar duyurulmakta ve önemli zafiyetlerle ilgili olarak güvenlik bildirisi sayfası bulunmaktadır.

Ulusal Bilgi Güvenliği Kapısı'nın, ülkemizde bilgi güvenliği alanında yetkinliğe sahip tüm kurum veya kişiler tarafından yapılmasına olanak sağlanmakta olup kişiler siteye kayıt olduktan sonra, bilgi güvenliği alanında oluşturduğu rehber, doküman veya makale, oluşturulacak değerlendirme komitesinin gözden geçirmesinin ardından internet sitesinde yayınlanmaktadır. Ulusal Bilgi Güvenliği Kapısının kurularak işletilmesi 2006 - 2012 yılları arasında Ulusal Bilgi Güvenliği Programı ve 2012 yılı sonrasında ise Kamu Bilgi Sistemleri Güvenliği Programı kapsamında TÜBİTAK BİLGEM tarafından gerçekleştirilmiş olup kapının amacı, bilgi güvenliği ile alakalı güncel uyarıların, bilgilendirici rehberlerin ve teknik yazıların yayınlanması olup yayınlamaktır. Kapıya içerik olarak katkıyı, bilgi güvenliği ile ilgilenmekte olan her kişi ve kurumun yapabilmesi hedeflenmiştir.

Bu sayede kapı ülkemizde bilgi güvenliği alanında ihtiyaç duyulan bilgi birikiminin oluşturulması işlevini yerine getirmesi amaçlanmış ve bilgi güvenliği ile alakalı kamu kurumları çalışanları arasında doğrudan bilgi alışverişinin yapılabilmesi amacıyla elektronik posta listelerinin oluşturulması gibi interaktif bir ortamın sağlanması amacına hizmet etmesi öngörülmüştür. Kapının önemli bir kısmının tüm ülkeye hizmet etmesi öngörülmüş bilgi güvenliği alanında bilgilendirme amaçlı tüm unsurların bu hizmet kapsamında verilmesi hedeflenmiştir[317].

Ulusal Bilgi Güvenliği Kapısı şu anda TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü bünyesinde Siber Güvenlik Eğitim Portalı adı altında hizmet vermekte olup Siber Güvenlik Eğitim Portalı ile toplumda siber güvenlikle alakalı konulardan farkındalığın arttırılması, yükseköğretim öğrencileri tarafından siber

[317] Bkz.http://sge.bilgem.tubitak.gov.tr/tr/bilgi-guvenligi-kapisi (Erişim Tarihi: 20.05.2018)

güvenlik teknolojileri alanında teknik bilginin edinilmesinin sağlanması, siber güvenlik konusunda çalışmakta olan uzmanların yetkinliklerinin arttırılması için gerek duyulan eğitimlerin çevrimiçi olarak verilmesi planlanmış olup portal Türkiye'nin 2016-2019 Siber Güvenlik Stratejisi kapsamında belirlenmiş olan hedeflerin gerçekleştirilmesine hizmet ettiği belirtilmiştir[318].

2011 yılında bir sivil toplum kuruluşu olan Siber Güvenlik Derneği kurulmuştur[319].

Siber güvenlik alanında İnternet Geliştirme Kurulu bünyesinde sektör katılımcılarının katıldığı ve siber güvenlik konusunda çalışmalar yapılması amacıyla tüm katılanların görüşlerinin toplanarak kurumlar arasındaki bilgi ve fikir alışverişi ile işbirliğinin sağlandığı, ortak fikirler üzerinde buluşularak yapılan çalışmaların Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na sunulması amacıyla Siber Güvenlik İnisiyatifi kurulmuştur.

Siber Güvenlik İnisiyatifi'nin faaliyetleri ise birey ve küçük işletmelerin siber güvenlik alanında bilinçlendirilmesi, farkındalık oluşturulması, gerekli koruma tedbirlerinin oluşturulması ile anlatılması, pozitif içeriğin üretilmesi, veri merkezleri oluşturulması ile internet servis sağlayıcıları hakkında en az güvenlik kriterlerinin belirlenmesi, sektör bazında risk analizi yapılması, siber güvenliğe dair standartların belirlenmesi, rapor ve kılavuzların yayınlanması şeklinde özetlenebilir[320].

Bilgi Güvenliği Derneği tarafından 2012 yılı Haziran ayında Ulusal Siber Güvenlik Stratejisini yayınlamış olup bu kapsamda ulaşılması gereken hedefler olarak ;

- Bireylerin siber güvenlik alanında bilgilendirilip bilinçlendirilmesi ve siber güvenlik kültürünün oluşturulması ile yaygınlaştırılmasının sağlanması,

---

[318]Bkz. https://egitim.sge.gov.tr/mod/page/view.php?id=10 (Erişim tarihi: 19.02.2019)
[319]Bkz. http://www.siberguvenlik.org.tr/hakkimizda/dernek-hakkinda/ (Erişim Tarihi: 24.11.2017)
[320]Bkz.https://www.btk.gov.tr/tr-TR/Sayfalar/SG-Siber-Guvenlik-Inisiyatifi (Erişim Tarihi: 25.11.2018)

- Ülkenin kritik altyapılarının tanımlanması ile dökümünün oluşturulması,
- Siber güvenlik alanında ulusal teknolojilerin geliştirilmesi için teşvik edilmesi ile ulusal teknolojilerin kullanılmasının özendirilmesi,
- Siber güvenlik ve savunma alanında yasal mevzuatın geliştirilmesi,
- Siber güvenlik uzmanlarının yetiştirilmesi,
- Siber güvenlik stratejisinin oluşturulması ile geliştirilmesinin sağlanması bu amaçla Siber güvenlik danışma kurulu oluşturulması,
- Belgelendirme kuruluşları tarafından onaylanmış güvenlik hizmetlerinin ve sistemlerinin kullanılmasının teşvik edilmesi veya zorunlu kılınması
- Uluslararası kurumlarla işbirliği ve koordinasyonun sağlanması ile geliştirilmesi

belirlenmiştir[321].

Türkiye açısından önemli bir siber güvenlik strateji belgesi olan 2013- 2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planından sonra Ulusal Siber Güvenlik Stratejisi ve 2016- 2019 Eylem Planı Ocak 2016 da T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı tarafından yayınlanmış olup[322] yeni strateji belgesi kapsamında gelişmekte olan bilgi ve iletişim teknolojileri ile artan güvenlik ihtiyacı ve edinilmiş olan tecrübeler kapsamında Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından ulusal siber güvenlik stratejisinin güncellenerek 2016-2019 döneminini kapsayacak faaliyetlerin belirlenmesi ihtiyacı doğrultusunda siber güvenlik alanında gerçekleştirilmesi hedeflenen faaliyetler belirlenmiştir.

Strateji belgesi incelendiğinde 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nın temel amacının siber güvenlik kavramının ulusal güvenliğin bütünsel bir parçası olduğunun tüm kesimler tarafından anlaşılması, ulusal siber

---

[321]Bkz.Bilgi Güvenliği Derneği, Ulusal Siber Güvenlik Stratejisi, Haziran 2012 http://www.bilgiguvenligi.org.tr/wp-content/uploads/2016/03/Ulusal_Siber_Guvenlik_Stratejisi.pdf (Erişim Tarihi: 25.11.2018)

[322] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı, Ocak 2016

uzay alanındaki sistemlerin ve paydaşların güvenliğinin sağlanması amacıyla gerekli idari ve teknolojik önlemler alınarak bu önlemler için yetkinliğin kazanılması olarak belirlenmiş olup bu temel amacın gerçekleştirilmesi kapsamında hedefler ve alt eylem maddeleri belirlenmiştir.

Bu kapsamda;

• Ulusal siber uzay alanını da kapsayacak şekilde bilgi ve iletişim teknolojileri kapsamında sağlanmakta olan her türlü hizmetin, işlemin ve verinin ve bu kapsamda bunların sunulması amacıyla kullanılan sistemlerin güvenlik, gizlilik ve mahremiyetinin sağlanması,

• Siber güvenliğe dair olayların etkilerinin minimum seviyede kalması ve meydana gelen olaylar sonrasında sistemlerin en kısa zamanda normal işleyişlerine dönebilmeleri amacıyla stratejik olarak siber güvenlik eylemleri belirlenmesi ve meydana gelen suçların adli makam ve kolluk kuvvetleri tarafından daha etkili olarak araştırması ve soruşturmasının sağlanması,

• Siber güvenlik, gizlilik ve mahremiyet sağlanmasına ilişkin olarak kritik önem taşıyan teknolojiler ile ürünlerin ülkemizde üretiminin sağlanması, mümkün olmaması halinde ise dışardan alınmış olan teknolojileri ile ürünlerin sırf bu amaçla ve güvenli olarak kullanımının sağlanması için gerekli önlemlerin alınması,

amacıyla gerekli planlamalar yapılmıştır.

Bu kapsamda diğer ülkelerin stratejileri ve planlarının incelendiğinin belirtildiği dokümanda diğer devlet politikalarında en önemli ilkeler olarak ;

a. Siber güvenlik alanında bireylerin, kurumların, toplum ve devletim tüm hukuksal ve sosyal sorumluluklarının yerine getirilmesi,

b. Kamu ve özel sektörün, üniversitelerin ve sivil toplum kuruluşlarının koordinasyonunun sağlanması ile ortak katılımın ve işbirliği ile bilgi paylaşımının sağlanması,

c. Uluslararası Siber Güvenlik Operasyon Merkezleri arasında gelişmiş siber olay yönetimi işbirliği sağlanması,

belirlenmiş olup tespit edilen riskler ise; toplumda sosyal ağlara olan bağımlılık, kritik kurumlar ile kuruluşların siber uzayda mevcut konumları, farklı siber casusluk alanındaki çalışmalar ile siber casusluk hedefi ile düzenlenen saldırılar, çalışanlar ve yetkinlik düzeyindeki yetersizlikler, kurumlar arasındaki koordinasyonun eksikliği, siber uzay alanında faaliyet göstermekte olan farklı boyutlardaki sektörlere yönelik olarak ekonomik kaygıların olduğu tespit edilmiştir.

Bu ilkeler ve riskler kapsamında hazırlanmış olan eylem planı ile siber güvenlik alanında amaç ve eylemler şu şekilde belirlenmiştir;

*Öncelikle ulusal kritik altyapıların envanterlerinin oluşturularak kritik altyapıların güvenliğine dair gerekli ihtiyacın karşılanması ve bu altyapıların bağlı bulundukları kurumlarca denetiminin yapılması.

*Siber güvenliğin sağlanabilmesi için denetim gerektiren yaklaşımları da içermekte olan uluslararası standartlar kapsamında gerekli ve uygun mevzuatsal çalışmalar yapılarak mevzuatların oluşturulması.

*Sektörel düzenleyici kurumlar ve Bakanlıklar gibi kuruluşların siber güvenlik alanında gerekli düzenlemelerin ve denetlemelerin yapılması amacıyla denetleme farkındalıkların ve yetkinliklerinin geliştirilmesi.

*Kurumlar bazında kullanılan bilişim sistemlerinin sadece olası saldırılardan değil, kullanıcılar tarafından yapılan hatalar ve afetlerden de korunabilmesi amacıyla gerekli düzenlemenin yapılması.

*Tüm kurumların kendi bünyesinde bilgi güvenliği yönetim sürecini çalıştırabilecek yetkinliğe erişmesi.

*Siber güvenlik alanında kurum yöneticilerinin farkındalıklarının arttırılması.

*Siber güvenlik kapsamında yetkin personelin yetiştirilmesi ile bu alanda uzmanlaşmak isteyen personel, araştırmacı ve öğrencilerin teşvik edilmesi.

*Toplumun her alanında siber güvenlik konusunda gerekli bilincin oluşturulması, eğitim kurumlarının çalışmalara ek olarak yazılı ve görsel medyada farkındalığın sağlanması amacıyla çalışmalar yapılması.

*Kamu kurumları bünyesinde siber güvenlik alanında uzmanlaşmış personel istihdamının sağlanması amacıyla gerekli mevzuatsal desteğin sağlanması ve personellerin özlük haklarının iyileştirilmesi.

*Kurumsal ve Sektörel SOME'lerin etkinliğini arttırmak amacıyla gerekli mevzuatsal desteğin sağlanması, mali düzenlemeler yapılarak yetkin personelin ihtiyaçlarının karşılanması, gerekli bilişim altyapısı sağlanması ve ulusal siber olaylara müdahale organizasyonu bünyesinde bilgi paylaşımının geliştirilmesi.

*Siber güvenlik alanı kapsamında gereken koordinasyonun sağlanarak bu amaçla güçlü bir merkezi kamu otoritesi oluşturulması.

*Kamu kurumları, özel sektörler, STK'lar (Sivil Toplum Kuruluşu), denetleyici kurum ve üniversiteler, geliştirici firmalar ve tüm diğer paydaşların katılım ve koordinasyonu hedefi ile ulusal siber güvenlik eko-sisteminin oluşturulması.

*Ulusal Siber güvenlik eko-sistemi içerisinde güzel örneklerin yaygınlaştırılarak, danışmanlık hizmetleri verilmesi, açıklık, tehdit ve faydalı uygulamaların paylaşılmasının sağlanması.

*Bilişim sistemlerinde kullanılan, ulusal ya da yabancı donanım ile yazılım ürünlerinde mevcut açıkların kötüye kullanımının engellenmesi amacıyla zafiyet analizleri ile sertifikasyon çalışmaları yapılması.

*Güvenli yazılım geliştirilme ve tedarik yönetiminin bir kültür olarak oluşturulması.

*Siber güvenlik alanında dışa olan bağımlılığın azaltılması amacıyla araştırma ve geliştirme faaliyetlerine önem verilmek suretiyle yerli ürün geliştirilmesi.

*Tehdit faktörlerinin saldırılar meydana gelmeden engellenmesi amacıyla ulusal proaktif siber savunma yeteneklerinin geliştirilmesi.

* Tehdit faktörlerinin siber uzay alanındaki en büyük avantajı olan anonimliğin ortadan kaldırması amacıyla etkili yönetimi ve IPv6 (Internet Protokolü sürüm 6) teknolojilerinin yaygınlaştırılması[323].

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı tarafından 2016 yılının mart ayında 2016-2019 Ulusal e- devlet stratejisi ve eylem planı[324] yayınlamış olup bu belge kapsamında Türkiye'de e-devlet (Elektronik devlet) politikası şekillendirilerek uygulamaya konulması amacıyla bütünsel ve sürdürülebilir bir "e-devlet Ekosistemi" oluşturulması ve sürdürülmesi amacıyla stratejik bir vizyon benimsenmiş ve bu alanda e-devlet politikaları belirlenerek, hizmetler geliştirilmesi, hizmetlerin sunumu, kullanımı amacıyla yürütülmekte olan çalışmaların tüm paydaşlar arasında düzenli ve koordineli bir şekilde işbirliği içinde sağlanacağı belirtilmiştir.

BTK, ulusal siber olayların önlenebilmesi ve siber güvenliğin sağlanması yönelik olarak Siber Güvenlik Uzmanı alımının yarışma ile gerçekleştirileceği bu amaçla üst düzeyde çalışabilecek olanların tespit edilmesi ve teknolojiye olan yatkınlığı üst seviyede olan gençlerin potansiyelinin açığa çıkartılması suretiyle

---

[323] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı, Ocak 2016

[324]Bkz. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı "2016-2019 Ulusal e- devlet stratejisi ve eylem planı".Mart 2016, http://www.edevlet.gov.tr/2016-2019-ulusal-edevletstratejisiveeylemplanitaslagi.pdf

uzman ihtiyacının karşılanması hedeflenmiş olup mezuniyet şartı aranmadan Türkiye'nin siber savunmasında destek verebilecek gençlere bu alanda çalışabilmeleri için "SİBER YILDIZ" olarak adlandırılan bir yarışma yapılacağı açıklamıştır. BTK Başkanı tarafından USOM İstişare Toplantısında yarışmanın 20 Ocak 2017'de yapılacağını ve yarışma sonunda 25 bin başvuru arasından yarışma sonucunda belirlenecek yetkin kişilerden siber ordu oluşturacaklarını açıklamıştır[325].

Uluslararası siber güvenlik kuruluşu Arbor Networks'ün yönetimindeki ATLAS tarafından yapılan bir araştırmada dünya genelinde 400 ü aşkın internet servis sağlayıcısının anonim trafik bilgileri ve tehditleri inceleyerek elde ettiği sonuçlara göre; , Türkiye'de 2017 yılının Eylül ayında dakikada 3, günde 466 adet saldırı gerçekleştiğini rapor etmiştir. Meydana gelen saldırıların yüzde 30'unun Amerika kaynaklı olduğu, yüzde 29'unun Türkiye içinden gerçekleştiği, 2017 yılı Eylül ayı boyunca süresince 130 binden fazla siber saldırı gerçekleştiği, Türkiye'nin özellikle online erişimin engellenmesine yönelik yapılan saldırılar alanında dünya genelinde en fazla saldırıya hedef olan ilk 8 ülke arasına girdiği belirtilmiştir[326].

20-21 Ekim 2017 tarihlerinde 10. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı gerçekleştirilmiş olup konferansın teması **"**Siber Güvenlik ve Yapay Zeka**"** olarak belirlenmiştir. Konferansta Yapay Zeka alanında meydana gelen gelişmeler, Türkiye'nin yapay zeka alanındaki stratejisi, yerli ve milli olarak geliştirilen yapay zeka uygulamaları ele alınmıştır. Bilgi Güvenliği ve Kriptoloji Konferansları bilgi alışverişinin sağlandığı en önemli etkinlikler olarak kabul görmekte olup ISCTurkey 2017 Konferansı, Avrupa Ağ ve Bilgi güvenliği Ajansı (ENISA) tarafından da desteklenmekte ve Avrupa Siber Güvenlik Ayı etkinlikleri arasında yer almaktadır[327].

---

[325]Bkz.https://www.btk.gov.tr/tr-TR/Kurumdan-Haberler/SIBER-YILDIZ-OLMAK-ICIN-BAYRAGI-YAKALA (Erişim Tarihi: 25.11.2018)

[326]Bkz. https://siberbulten.com/strateji-guvenlik/turkiyeye-dakikada-3-siber-saldiri/ (Erişim Tarihi: 26.11.2018)

[327]Bkz. http://www.iscturkey.org (Erişim Tarihi: 26.11.2018)

ÜÇÜNCÜ KISIM
SONUÇ VE DEĞERLENDİRME

"Yakın gelecekte çıkabilecek büyük bir savaşta ilk mermi internette atılacaktır." Nato Güvenlik Danışmanı Rex Hughes tarafından söylenen bu söz internetin gelişimini ve bu gelişimin meydana getirmesi muhtemel sonuçları hakkında bize fikir vermektedir.

Günümüzde teknolojinin büyük bir hızla gelişmesi ve internetin hayatın her alanında yaygınlaşmasıyla birlikte siber güvenlik ülkelerin en temel politika sorunlarının başında yer almaya başlamıştır. Bilgi ve iletişim sistemleri ile internet kullanıcıların hayatını büyük ölçüde kolaylaştırdığı gibi diğer taraftan güvenlik zafiyetleri sebebi ile sistemlerin kötüye kullanıma açık hale gelmesine ve suçun işlenebileceği yeni bir alan doğmasına sebebiyet vermiştir. Siber alanda yapılan her türlü saldırı hedefine büyük zararlar verebilmekte olup siber suçlardan, siber casusluk ve siber savaşa, siber hacktivizme kadar bir çok farklı motivasyon ile saldırılar gerçekleştirilmektedir.

Bilgi ve iletişim teknolojilerinin bu önlenemez ve kontrol edilemez gelişimi beraberinde her gün artmakta olan savunma ihtiyacı, bilginin önemi ile siber güvenliğe duyulan ihtiyacın da artmasına sebep olmaktadır. Hiçbir sorun siber güvenlik sorunu kadar hızlı ilerlememektedir.

İnternet artık sadece sosyal medya hesaplarının kullanıldığı, oyun oynanan veya siteler arası gezinmeyi sağlayan bir araç olmaktan çıkmış, bilgi savaşlarının yapıldığı, gerçek orduların kurulduğu, devletlerin savunma stratejileri geliştirdiği, içerisinde en kıymetli olan bilginin bulunduğu korunması elzem olan bir siber uzay haline gelmiştir.

Evler akıllı hale gelmiş, yapay zekalar ve robotlar geliştirilmeye başlanmış, yüz ve damar izi tanıma sistemleri gibi sistemlerde kişilerin en gizli ve ayırt edici verileri depolanmaya başlanmış, nesneler her geçen gün büyük bir hızla internete erişebilir hale gelmiş bunun sonucu olarak ta güvenlik ihlallerini beraberinde getirmiştir.

Günümüzde tüm devlet işleri elektronik alanda yapılmaya başlanmıştır. Nükleer enerji santralleri, elektrik, ulaşım, haberleşme, doğalgaz gibi kritik altyapıların tüm sistemleri bir bilgi iletişim sistemi üzerinden yönetilmekte, atom bombalarının kodları bir sistem aracılığıyla aktive edilebilmekte kısacası insanoğlu her şeyi bilgi ve iletişim sistemleri vasıtasıyla yerine getirmektedir. Bu durum kişisel verilerin korunması, bilgi güvenliği ilkelerinin önemi ve siber güvenliğin sağlanması ile siber savunma alanlarının her zamankinden önemli bir sorun haline gelmesine sebep olmuştur.

Milli güvenlik ve savunma alanlarında terör saldırıları, uluslararası boyutta sistemlerin güvenlik tanımlarını, tehditleri ve ülkelerin gündemlerini tamamen değiştirmiş olup uluslararası düzlemde NATO üyelerinden birine karşı gerçekleşmesi mümkün olan "Dijital Felaket" (Dijital 11 Eylül) senaryoları tartışılmaya başlanmıştır. Halihazırda mevcut olan tehditlerin devamlı olarak artmakta olduğu göz önüne alındığında siber güvenlik ülkelerin en büyük sorunu haline gelmiştir.

Siber alandan kaynaklanan tehditler çok farklı boyutlarda ve düzenli şekilde artmakta olup siber saldırıları gerçekleştirenler tarafından banka hesapları boşaltılabilmekte, elektrik dağıtımını sağlayan şebekelerin devre dışı kalması sağlanabilmekte, mevcut su kaynakları kontrol edilebilmektedir.

İnsanların ve kurumların siber alana olan bağımlılığı çok büyük zafiyetler ortaya çıkmasına sebep olduğundan bu alanın çok dikkatli bir şekilde ve özellikle korunmasına gereksinim duyulmaktadır.

Suçu işleyenin tespitinin teknik olarak çok zor olması, mevcut hukuki düzenleme ve yaptırımların yeterli olmaması, siber uzayın ulusal sınırları aşan kapsamı ile uluslararası alanda işbirliğinde yaşanan sorunlarda siber alandaki tehditlerin hareket kabiliyetini arttırarak siber tehditleri birer ulusal güvenlik sorunu haline getirmektedir.

Saldırıların kişiler, kurumlar ve devletler olmak üzere temel mağdurları saldırılar neticesinde büyük zayiatlar vermektedir. Bireyler ekonomik kayba uğrayabilmekte veya verileri çalınabilmekte, yetkisiz kişilerce verilere erişilebilmekte ve veriler değiştirilebilmektedir. Devletlerin savunma sırları,

teknolojileri çalınabilmekte, siber alanda seçim sonuçları değiştirilebilmekte ya da kritik altyapılara yapılacak en küçük bir saldırı devletleri büyük zararlara uğratabildiği gibi terör saldırılarına maruz kalmalarına sebep olabilmektedir. Kurumların ise ticari sırları, fikri mülkiyetlerindeki ürünleri çalınabilmekte, operasyonel sistemleri işlevsiz hale getirilebilmektedir. Hatta evlerin bile akıllı hale geldiği şu günlerde siber saldırılar neticesinde kişilerin öldürülmesi dahi mümkün hale gelmiştir.

Bu sebeple siber güvenlik kavramı, bilgi güvenliğinden operasyon güvenliğine ve bilgisayar sistemlerinin güvenliğine kadar birçok farklı kavramı içinde barındırmakla bireyler açısından kendini siber alanda güvende hissetmek ve kişisel verilerinin korunması, gizliliğin koruması anlamına gelmektedir.

Bireyler açısından bakıldığında siber saldırılar maddi zararlara sebebiyet verebildiği gibi tüm özel hayatın kamuya deşifre edilmesi, verilerinin siber ortamda paylaşılması hatta siber alanda işlenebilecek bir çok suça hedef haline gelinebilmesine sebep olmaktadır.

Kurumlar açısından değerlendirildiğinde ise kurumun işle ilgili kritik öneme sahip işlevlerinin kullanılabilir olmasını, operasyon ve bilgi güvenliği sayesinde gizli verilerinin ve ticari sırların korunmasının sağlanması anlamına gelir. Kurumsal düzeyde incelendiğinde DDOS saldırıları gibi siber saldırılar hizmet verilmesini engellediği gibi kurumların ticari itibarlarının zedelenmesine dahi sebep olabilmektedir.

Devletler açısından bakıldığında ise vatandaşlarının, kurumlarının, kritik altyapılarının ve bilgisayar sistemlerinin saldırılara ya da verilerin çalınmasına karşı korunması, siber casusluk ve siber savaş faaliyetleri kapsamında gereken önlemlerin alınarak yüksek gizlilik seviyesindeki savaş planları, altyapı planları dahil bir çok devlet sırrının ifşasının önlenmesi ve kritik altyapıların işleyişlerinin bozulmasının önlenmesi anlamına gelir.

Siber saldırılar, ekonomik, fiziksel yıkımlara sebep olmasının yanında, yaralanmalara, ölümlere ve büyük yıkımlara sebep verebilecek boyutlara ulaşmıştır. Yapılacak siber saldırı sonucu hedefteki ülkenin gizli bilgilerine ve

istihbaratlarına ulaşılabilmesi, kurum ve kurumlarının işlerin aksatılarak sistemin çökmesi ile büyük zararlara uğratılabilmek mümkündür.

Siber alanda mevcut tehditler sadece bilgisayarlara verilen zararları ile sınırlı kalmamış gelişerek ülkelerin haberleşme sistemleri, enerji, ulaşım altyapıları, askeri alanda komuta ve kontrol sistemleri olmak üzere farklı alanlarda da zarar verebilecek boyuta ulaşmıştır.

Siber güvenlik kavramı günümüzde devletlerin fiziki ordularının yanında en çok ihtiyaç duyacakları savunma alanı olarak karşımıza çıkar. Artık sadece 3 temel savunma alanı yoktur. Kara, hava ve deniz alanlarının yanında savunulması ve dış tehditlere karşı korunması gereken bir de siber uzay alanı kavramı ortaya çıkmıştır.

Tüm dünyada teknolojinin gelişmesiyle birlikte yeni bir savaş türü ve bu savaş türüne yönelik yeni stratejilere ihtiyaç doğmuştur. Siber savaşlar ve siber saldırılar günümüzde konvansiyonel silahların yanında önemli bir silah haline gelmiştir.

Çalışma kapsamında öncelikle siber saldırıların özellikleri anlatılmıştır. Bu kapsamda siber saldırıların meydana gelmesinde en büyük zafiyet unsurunun insan olduğu tespit edilmiştir.

Bir sistemin korunması için gerekli her türlü önlem alınsa dahi insan faktörü siber alanda bilinçlendirilmediği zaman tüm savunma önlemlerinin zedelendiği görülmüştür. Aynı şekilde siber saldırıların yapılışları, sistemlerin hangi zafiyetlerden faydalandıkları, sistemlerin açıkları detaylıca anlatılmaya çalışılmıştır.

Devletlerin siber güvenlik alanında karşılaşılması muhtemel riskler çerçevesinde hem ulusal yapıları ile sistemleri hem de vatandaşlarının korunması amacıyla ortaya çıkan ihtiyaç kapsamında siber güvenlik politikaları oluşturmaları zorunluluğu doğmuştur.

Çalışma kapsamında devletlerin siber uzay alanına bakış açıları, siber güvenlik kavramından ne anladıkları ve bu alanın korunması amacıyla oluşturdukları siber güvenlik strateji belgeleri, hukuksal mevzuatları, bilişim

suçlarına ilişkin oluşturdukları merkez ve kurumlar ile siber güvenlik politikaları devletler bazında ayrı ayrı değerlendirilmek suretiyle detaylıca incelenmiştir.

Değerlendirilen ülkelerin politikalarına genel olarak bakıldığında; siber saldırılar konusunda ülkelerin bilinçlenmiş oldukları ve saldırılar ile oluşması muhtemel zararlara ilişkin tehlikenin farkında oldukları, siber uzay alanını ulusal savunma alanı olarak görmeye başladıkları ve bu durumu strateji belgelerinde ifade ettikleri, siber güvenlik alanında duyarlı oldukları, birçok ülkede siber güvenlik alanında yasal düzenlemeler yapıldığı, ancak bazı ülkelerde yasal düzenlemelerin internet ve kişi özgürlüklerinin kısıtlanması ile siber güvenliğin sağlanması arasındaki çizginin net çizilemediği, bazı ülkelerin yasal düzenleme yoluna gitmesine rağmen yasal zorunluluk sağlamadığı veya yeterli yaptırım öngörmediği, ulusal anlamda siber savunma sorumluluğu ve görevinin bazı ülkelerde bağımsız kurulan birimlere verilmesine rağmen bazılarında devlet kurumları arasında bölündüğü, bazılarında kurulan merkezler arasında koordinasyon eksikliği mevcut olduğu ve çok fazla birim mevcut olduğu, tüm ülkelerin siber tehdidin farkında olmasına rağmen ortak bir siber güvenlik ilkeleri ve genel çerçeve kurallar belirlenemediği ve mevcut bir saldırı hususunda atılması gereken adımların net bir şekilde ortaya konulmadığı, bazı ülkelerin savunma bazlı strateji oluştururken bazılarının saldırgan tutumlu proaktif siber savunmadan yana olduğu, siber güvenlik alanında ortak bir yaklaşım olmadığı ve bu sebeple her ülkenin kendi yaklaşımını uyguladığı ortak siber güvenlik ilkeleri tespit ederek bu alanda her ülkenin mevzuatlarındaki ve kurumlarındaki eksikliklerin giderilmesi için çalışmalarının eksik olduğu görülmüştür.

Devletlerin öncelikle milletlerarası kurumlar kapsamında ortak siber güvenlik politikaları ve siber güvenliğe dair ilkelerini belirlenmesi gerekmektedir.

Bu alanda Avrupa Birliği, BM ve NATO da bir takım çalışmalar yapılmakta ve ortak ilkeler belirlenmekte ise de devletlerin iç hukuk düzenlemelerine yansıması gerekmektedir. Bu anlamda kat edilecek daha çok yol vardır.

Tüm dünyada bilgi ve iletişim altyapılarına ve internete olan bağımlılığın artması ile buna bağlı olarak siber alanda taşınan riskler de her geçen gün

büyümektedir. Siber tehdidi doğru algılayarak ölçebilmek ve tehditler karşısında etkili stratejiler geliştirebilmesi için öncelikle farkındalık sağlanması, gözlem yapılması, takip edilerek analiz yapılması ve hızlı müdahale imkanı sağlayan yetkin birimlerin varlığına ihtiyaç vardır.

Siber güvenliğin sadece internet güvenliğini değil tüm iletişim altyapılarını kapsayan geniş bir kavram olması nedeniyle sonraki adım olarak çok sektörlü bir yaklaşımla ulusal siber güvenlik politikasının belirlenmesi ve devamında uluslararası siber güvenlik ilke ve kuralarının oluşturulması gerekmektedir.

Ciddi bir siber saldırıya maruz kalınması yıkıcı sonuçlar meydana getirebilecek olduğundan pasif savunma stratejilerinin yanında aktif saldırıları da kapsayan stratejilerin de tesis edilerek gerekli tedbirlerin alınması gerekmektedir.

Ancak siber güvenlik alanında tedbirler alınırken güvenlik-demokrasi ve özgürlük dengesinin iyi kurulması, kişi hak ve özgürlükleri konusunda uluslararası düzenlemelerin göz önüne alınması ve rehber kabul edilmesi büyük önem taşımaktadır.

Hukuksal olarak devletlerin siber alanın güvenliğini sağlayabilmesi için öncelikle bireyin eğitilmesi gerekmektedir.

Bireylerde siber farkındalığın oluşturulması siber güvenliğin temelini oluşturur. Devamında ise siber suç kavramını doğru olarak teşhis etmeli ve bu kavramların devletlerin iç hukuk düzenlemelerinde yerini almasını sağlamalı, siber alanın siber saldırılara karşı korunabilmesi amacıyla mevcut saldırılara müdahale edilmesi ile saldırganların tespitini sağlayan birimler ile teknik altyapıların oluşturulması, saldırıları gerçekleştirenlere yaptırımlar uygulanarak ceza adalet sürecinin işletilmesi, bu kapsamda gerekli hukuksal mevzuatın oluşturulması ve bu faaliyetlerin yerine getirilmesi ile görevli birimlerin kurulması sağlanmalı, siber suçlarla mücadeleye yönelik hukuki altyapılar güçlendirilmeli, mevzuatsal eksiklikler giderilmeli, bilişim suçları kapsamına giren eylemler belirlenirken her gün artarak gelişen bilişim suçları ve siber saldırı türlerinin hızına erişilebilmesi için düzenli olarak güncellenmeli ve siber suçlarla daha etkin mücadeleye imkân verecek düzenlemelerin yapılması gerekmektedir.

Bu alanda sadece kurumlar ile devletlerin koordinasyonu değil siber suçların birey mağduru olan vatandaşlar ile kanun koyucunun da işbirliği içinde ortak hareket etmesi, toplumsal farkındalığın arttırılması için çalışmalar yapılması ve ortak bilgi platformlarının oluşturulması büyük önem arz etmektedir.

Siber saldırılar bir savaş türü olarak karşımıza çıkmaktadır. Bu nedenlerle öncelikle etkili siber savunma sistemleri inşa edilerek acil durum eylem planları hazırlanması büyük önem taşımaktadır. Saldırıların gerçekleşmeye başladığı anda tespitine yarayan sanal yada fiziksel bariyerlerin inşa edilerek, ulusal boyutta siber güvenlik stratejileri geliştirilmeli ve bu alanda farkındalık yaratılmalıdır.

Siber güvenliğin muhatapları devlet yönetimleri, kanun koyucular, kişiler, kurum ve kuruluşlardır. Siber güvenlik kavramı çalışmada detaylıca anlatıldığı üzere siber alanda gelebilecek muhtemel tehditler karşısında bilgi ve iletişim sistemleri üzerinde saklanan, işlenen veya iletilen verinin erişilebilirlik, bütünlük ve gizliliğinin korunması ile bu sistemlerde gerçekleştirilen işlemlerde gerekli olan kimlik doğrulaması ile inkâr edilemezlik unsurlarının korunması anlamına gelmekle bu unsurlardan bir veya bir kaçında zafiyet meydana gelmesi durumunda oluşacak sorunlar bireysel veya kurumsal boyutta kalmayacak olup bu riskler ulusal, hatta uluslararası boyutta ekonomik, siyasal, sosyal pek çok alanda kayıplar verilmesine neden olacaktır.

İnsan faktörü güvenlikle alakalı pek çok alanda olduğu gibi siber güvenlikte de en önemli etkendir. Bir sistem içerisinde her türlü güvenlik önlemi alınsa dahi insandan meydana gelen bir zafiyet sistemi her zaman savunmasız hale getirecektir. Sosyal mühendislik gibi yöntemi insan olan saldırılar karşısında kişilerin ve kurum çalışanlarının siber güvenliğe ilişkin konularda eğitilmeleri ve bilinçlendirilmeleri gerekmektedir.

Kurumlar bazında sistemlerin güvenliğinin kurulum aşamasında sağlanması gerekmekte olup erişim kontrollerinin dikkatli tesis edilmesi, personele siber güvenlik eğitimlerinin verilmesi ve personel için çalışma politikalarında standardizasyon yapılması gerekmektedir. Ayrıca sistemlerin düzenli olarak penetrasyon testlerinden geçirilerek güvenlik zafiyetlerinin tespit edilerek önlem alınması gerekmektedir.

Siber güvenlik alanında yapılan tatbikatlar, sistemlerin zafiyetlerinin tespiti ve gerekli önlemlerin alınması açısından büyük önem taşımaktadır.Teknolojinin sürekli gelişmesi karşısında siber güvenlik alanındaki gelişimler o kadar hızlı ilerlemektedir ki bu alanda alınmış olan önlemler ve düzenlemeler bu sebeple yetersiz kalabilmekte ve muhtemel tehditler karşısında alınmış olan kararlar ileriye yönelik güvenliğin sağlanabilmesinde beklenen etkiyi gösterememektedir.

Her an yeni bir siber saldırı türü ortaya çıkmakta olup bilgi ve iletişim sistemlerine yönelik alınan önlemler ile güvenlik stratejileri uzmanlar tarafından gerçekleştirildiğinden genellikle kullanıcılar bu tedbirlerden haberdar olamamaktadır.

Bu sebeple siber uzay alanında mevcut tüm tehditler karşısında devletlerin, kurumların ve bireylerin koordineli çalışmasının sağlanması ile uluslararası boyutta işbirliği sağlanarak ortak bir siber güvenlik bilinci oluşturulması gerekmektedir. Siber alandaki tehditlerin oluşturabileceği sonuçlar itibariyle ortaya çıkacak maliyetlerin savunma alanında yapılacak yatırımlardan çok daha fazla olacağı öngörülerek siber güvenlik alanında gerekli yatırımların yapılması, altyapı sistemlerinin güçlendirilmesi gerekmektedir.

Sonuç olarak; her devletin siber güvenlik stratejileri farklı olmasına rağmen her devlet kendi stratejileri doğrultusunda somut adımlar atmış, strateji belgeleri yayınlayarak bu belgeler kapsamında uluslararası işbirliğinin önemine ve siber uzay alanının ulusal alan olmasına değinmiş, her ne kadar siber tehditlerin gelişimi karşısında yetersiz kalsa da ulusal sınırları içerinde siber uzayı ve ulusal güvenliklerini korumak için birimler kurmuştur. Devletler siber güvenliğin önemini yavaş yavaş kavrayarak daha sıkı ve yaptırımsal önlemler almaya yönelmişlerdir.

Ancak mevcut gelişmeler ve siber alandaki tehditlerin gelişim hızı karşısında devletlerin, bireylerin, kurum ve kuruluşlar ile kanun koyucunun seri ve ciddi olarak harekete geçmesi ile gerekli önlemlerin alınarak tehditlerin vereceği zararın minimuma indirilmesi veya tamamen önlenebilmesi için koordineli çalışma yapılması ve siber güvenlik alanında farkındalığın arttırılarak toplumun bilinçlendirilmesi gerekmektedir.

KAYNAKÇA

https://istihbaratveanaliz.files.wordpress.com/2016/06/siber-tehditler-savunma-yntemleri-ve-hackerlarn-baars.pdf adresinden 05.05.2017 tarihinde alındı

https://www.ercanyuzuk.com/2018/08/zero-day-sfrnc-gun-acklar.html?cv=1 adresinden 01.01.2019 tarihinde alındı

http://www.bilisimhukuk.com/2012/08/hacktivizm-ve-siber-teror/ adresinden 29.04.2017 tarihinde alındı

http://en.wikipedia.org/wiki/Cyberwarfare adresinden 02.05.2017 tarihinde alındı

http://www.istanbul.pol.tr/sibersuclarlamucadele/Sayfalar/Siber_Suclar.ax adresinden 06.05.2017 tarihinde alındı

Bilgi Güvenliği Raporu, *Bilgi Güvenliği ve Bilişim Suçları* , 3. Kısım. sy.754 http://www.biakraporu.org/docs/rapor.kisim3.bolum01.pdf adresinden 09.07.2017 tarihinde alındı

https://www.sibergah.com/genel/bilgi-guvenligi-nedir-ve-nasil-siniflandirilir/ adresinden 22.07.2017 tarihinde alındı

https://www.docdroid.net/6W0tztz/siber-guvenlikcyber-securtiy.doc#page=5 adresinden 04.08.2017 tarihinde alındı

http://www.coe.int/en/web/cybercrime/cybercrime-ipa adresinden 09.05.2017 tarihinde alındı

https://www.us-cert.gov/about-us , adresinden 08.09.2017 tarihinde alındı

https://www.medianama.com/2017/08/223-national-cyber-coordination-centre-launch/ adresinden 18.11.2017 tarihinde alındı

http://www.cyberswachhtakendra.gov.in adresinden 18.11.2017 tarihinde alındı

http://indiafoundation.in/services-view/indias-cyber-security/ adresinden 19.11.2017 tarihinde alındı

http://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-3/1140166/russia adresinden 19.11.2017 tarihinde alındı

https://www.cliffordchance.com/briefings/2017/10/new_legislation_regulatingcybersecurityandth.html adresinden 04.04.2019 tarihinde alındı

https://tr.wikipedia.org/wiki/Arap_Baharı adresinden 02.11.2017 tarihinde alındı

https://www.scmagazineuk.com/russia-revamps-its-infosec-strategy/article/541537/ adresinden 01.11.2017 tarihinde alındı

http://www.russia-direct.org/opinion/what-behind-new-russias-information-security-doctrine adresinden 05.04.2019 tarihinde alındı

http://www.resmigazete.gov.tr/eskiler/2006/07/20060728-7.htm adresinden 23.11.2017 tarihinde alındı

http://www.tnetworks.com.tr/cozumler/advanced-persistent-threats-apt adresinden 30.05.2017 tarihinde alındı

https://www.kaspersky.com.tr/resource-center/threats/viruses-worms adresinden 10.09.2017 tarihinde alındı

http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/intranet-(iç-ağ)-ve-extranet-(dış-ağ) adresinden 11.11.2017 tarihinde alındı

http://www.bbc.com/turkce/haberler-dunya-39915541 adresinden 20.06.2017 tarihinde alındı

http://www.bilisimterimleri.com/bilgisayar_bilgisi/bilgi/76.html adresinden 12.11.2017 tarihinde alındı

http://en.wikipedia.org/wiki/Rootkit adresinden 09.05.2017 tarihinde alındı

https://tr.wikipedia.org/wiki/Arka_kapı , adresinden 11.11.2017 tarihinde alındı

https://tr.wikipedia.org/wiki/Denial-of-service(DoS)_Saldırısı adresinden 10.06.2017 tarihinde alındı

http://www.dijitalteknoloji.net/internet/redhack-nasil-hackliyor.html adresinden 07.05.2017 tarihinde alındı

http://shiftdelete.net/ddos-nedir-39493 adresinden 09.05.2017 tarihinde alındı

http://www.teknolojioku.com/haber/keylogger-nedir-nasil-yapilir-temizlenir-ve-korunulur-101.html, adresinden 10.11.2017 tarihinde alındı

https://tr.wikipedia.org/wiki/TCP adresinden 10.11.2017 tarihinde alındı

https://tr.wikipedia.org/wiki/UDP adresinden 10.11.2017 tarihinde alındı

https://tr.wikipedia.org/wiki/IP_spoofing , adresinden 10.11.2017 tarihinde alındı

http://gundem.bugun.com.tr/redhackler-yoke-nasil-sizdi-haberi/218675 adresinden 08.05.2017 tarihinde alındı

http://www.kodevreni.com/526-sql-injection-nedir-ve-sql-injection-nasıl-önlenir/ adresinden 09.05.2017 tarihinde alındı

https://tr.wikipedia.org/wiki/SQL_Injection adresinden 09.05.2017 tarihinde alındı

http://teknolog.radikal.com.tr/redhack-nasil-hackliyor/#sthash.uRZQI5EX.dpuf adresinden 12.05.2017 tarihinde alındı

http://www.bilgiguvenligi.gov.tr/sosyal-muhendislik/sosyal-muhendislik-saldirilari-3.html adresinden12.05.2017 tarihinde alındı

https://tr.wikipedia.org/wiki/Kevin_Mitnick adresinden 09.05.2017 tarihinde alındı

http://en.wikipedia.org/wiki/Website_defacement adresinden 10.06.2018 tarihinde alındı

https://www.sabah.com.tr/pazar/2014/10/19/ilk-online-cinayet-bir-tik-uzakta adresinden 21.05.2017 tarihinde alındı

http://www.memurlar.net/haber/489141/ adresinden21.05.2017 tarihinde alındı

https://www.techinside.com/sirketler-siber-saldirilara-hazir-degil/ adresinden 22.05.2017 tarihinde alındı

http://labrisnetworks.com/tr/tr-labris-networks-2014-siber-guvenlik-raporu-ve-2015-ongoruleri-yayinlandi/ adresinden 22.05.2017 tarihinde alındı

https://tr.wikipedia.org/wiki/Stuxnet adresinden 10.06.2017 tarihinde alındı

https://tr.wikipedia.org/wiki/Kriptografi adresinden 23.07.2017 tarihinde alındı

https://tr.wikipedia.org/wiki/Hash_fonksiyonu adresinden 23.07.2017 tarihinde alındı

https://tr.wikipedia.org/wiki/Açık_anahtarlı_şifreleme adresinden 11.11.2017 tarihinde alındı

https://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/cyber-security/ adresinden 03.03.2017 tarihinde alındı

http://www.tuicakademi.org/ilk-modern-siber-atak-estonya/ adresinden 01.03.2017 tarihinde alındı

https://www.timeturk.com/tr/2013/01/17/siber-alemin-kanli-savaslari.html adresinden 01.03.2017 tarihinde alındı

http://www.elektrikport.com/teknik-kutuphane/siber-savaslar-stuxnet/4383#ad-image-0 adresinden 01.03.2017 tarihinde alındı

http://sibertehdit.com/siber-guvenlik-nedir/ adresinden 09.05.2017 tarihinde alındı

http://www.radikal.com.tr/turkiye/hackerlardan-en-cok-turkiye-zarar-gordu-1160474/ adresinden 22.05.2017 tarihinde alındı

https://www2.deloitte.com/tr/tr/pages/risk/topics/cyber-risk/articles/avrupa-birligi-siber-guvenlik-kanunu.html adresinden 25.05.2017 tarihinde alındı

http://afyonluoglu.org/PublicWebFiles/strategies/Europe/EU%202017%20Cyber%20Security%20Act.PDF adresinden 23.01.2019 tarihinde alındı
https://siberbulten.com/uncategorized/siber-guvenlikte-kamu-ozel-sektor-isbirligi-mumkun-mu/ adresinden 06.07.2017 tarihinde alındı

https://siberbulten.com/uluslararasi-iliskiler/trumpdan-devrim-gibi-karar-her-bakanlik-kendi-siber-guvenliginden-sorumlu/ 06.07.2017 tarihinde adresinden alındı

https://siberbulten.com/uluslararasi-iliskiler/abdde-kamu-aglarini-einstein-monitor-edecek/ adresinden 06.07.2017 tarihinde alındı

https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf adresinden 01.01.2019 tarihinde alındı

http://afyonluoglu.org/PublicWebFiles/strategies/America/USA%202018%20DHS%20Cyber%20Security%20Strategy.pdf adresinden 02.01.2019 tarihinde alındı

https://www.ssi.gouv.fr/en/cybersecurity-in-france/cybersecurity-strategy/ adresinden 03.01.2019 tarihinde alındı

http://afyonluoglu.org/PublicWebFiles/strategies/Europe/French%202015%20Digital%20Security%20Strategy-EN.pdf adresinden 03.01.2019 tarihinde alındı

https://www.legislation.gov.uk/ukpga/1998/29/contents adresinden 03.01.2019 tarihinde alındı

https://siberbulten.com/strateji-guvenlik/ingiltereden-kobiler-icin-siber-guvenlik-destegi/ adresinden 17.11.2018 tarihinde alındı

http://www.bbc.com/turkce/haberler-dunya-38967467 adresinden 19.11.2018 tarihinde alındı

https://www.ncsc.gov.uk/information/about-ncsc adresinden 18.11.2018 tarihinde alındı

://siberbulten.com/strateji-guvenlik/ingiltere-merkez-bankasi-hacker-istihdam-edecek/ adresinden 18.11.2018 tarihinde alındı

http://www.cinmacerasi.com/cinin-dev-internet-sansur-sistemi-nasil-calisiyor adresinden 10.10.2017 tarihinde alındı

http://www.bilgesam.org/incele/2111/-cin-in-yeni-askeri-strateji-belgesi/#.Whiuea3BJsM adresinden 12.102.17 tarihinde alındı

https://siberbulten.com/strateji-guvenlik/cin-hong-kong-protestocularini-mobilden-vurdu/ adresinden 08.10.2017 tarihinde erişilmiştir.

https://siberbulten.com/uluslararasi-iliskiler/cin-abdli-sirketlerden-intikamini-aldi/ adresinden 12.10.2017 tarihinde alındı

http://afyonluoglu.org/PublicWebFiles/strategies/Asia/China%202017%20National%20Cyber%20Strategy-Unofficial%20Translation-EN.pdf adresinden 01.04.2019 tarihinde alındı

https://webrazzi.com/2012/01/06/japonyadan-milli-guvenlik-virusu/ adresinden 15.10.2018 tarihinde alındı

https://www.jpcert.or.jp/english/about/ adresinden 02.04.2019 tarihinde alındı

http://www.shield.ne.jp/ssrc/topics/SSRC-ER-12-022-en.html adresinden 02.04.2019 tarihinde alındı

http://afyonluoglu.org/PublicWebFiles/strategies/Asia/Japan%202017%20Cyber%20Security%20Policy%20for%20Crtical%20Infrastructure-EN.pdf adresinden 04.04.2019 tarihinde alındı

https://researchcenter.paloaltonetworks.com/2017/11/cso-japans-new-cybersecurity-strategies-right-priorities-mind/ adresinden 19.10.2017 tarihinde alındı

https://www.usom.gov.tr/dokuman.html adresinden 24.11.2017 tarihinde alındı

http://www.karabulut.co/ulusal-siber-guvenlik-stratejisi/ adresinden 24.11.2017 tarihinde alındı

http://www.siberguvenlik.org.tr/hakkimizda/dernek-hakkinda/ adresinden 24.11.2017 tarihinde alındı

http://sge.bilgem.tubitak.gov.tr/tr/bilgi-guvenligi-kapisi adresinden 20.05.2018 tarihinde alındı

https://egitim.sge.gov.tr/mod/page/view.php?id=10 adresinden 19.02.2019 tarihinde alındı

https://www.btk.gov.tr/tr-TR/Sayfalar/SG-Siber-Guvenlik-Inisiyatifi adresinden 25.11.2018 tarihinde alındı

https://www.btk.gov.tr/tr-TR/Kurumdan-Haberler/SIBER-YILDIZ-OLMAK-ICIN-BAYRAGI-YAKALA adresinden 25.11.2018 tarihinde alındı

https://siberbulten.com/strateji-guvenlik/turkiyeye-dakikada-3-siber-saldiri/ adresinden 26.11.2018 tarihinde alındı

http://www.iscturkey.org adresinden 26.11.2018 tarihinde alındı

Avrupa Birliği Konseyi Çerçeve Kararı. (2005, Şubat 24). *Bilgi Sistemlerine Saldırılar Hakkındaki 2005/222 sayılı 24 Şubat 2005 tarihli Avrupa Birliği*

Konseyi Çerçeve Kararı , Avrupa Birliği Resmi Gazetesi, sayfa. 67-71 (COUNCIL FRAMEWORK DECISION 2005/222/JHA of 24 February 2005 on Attacks Against Information Systems OJ L 69, 25/02/2005 p. 67-71.).

ÇELİKTAŞ, B. (2016, Mayıs). "*Siber güvenlik kavramının gelişimi ve türkiye özelinde bir değerlendirme*. Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü , Uluslararası İlişkiler Anabilim Dalı, Uluslararası ilişkiler Programı. sy.67-69.

Çin Halk Cumhuriyeti Siber Güvenlik bildirgesi
https://www.slideshare.net/CezeriSGACezeriSiber/in-halk-cumhuriyeti-siber-gvenlik-bildirgesi adresinden 14.10.2017 tarihinde alındı

20.10.2012 tarihli 28447 sayılı Resmi gazetede yayınlanan 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Kararın yürürlüğe konması hakkında Bakanlar Kurulu Kararı
http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf adresinden 14.10.2017 tarihinde alındı

28.07.2006 tarihli 26242 sayılı Resmi Gazetede yayınlanan 11.07.2006 traihli Yüksek Planlama Kurul Kararı ve eki Bilgi Toplumu Stratejisi ve Bilgi Toplumu Stratejisi Eylem Planı
http://www.bilgitoplumu.gov.tr/Documents/1/BT_Strateji/Diger/060500_BilgiToplumuStratejisi.pdf adresinden 14.10.2017 tarihinde alındı

2010 To 2015 Government Policy: Cyber Security, (2015, May)
https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security . adresinden 15.11.2018 tarihinde alındı

2011 tarihli Ulusal Siber Güvenlik Tatbikatı Sonuç Raporu.

https://siberbulten.com/tag/avrupa-birligi-siber-guvenlik-stratejisi/ adresinden 09.11.2017 tarihinde alındı

https://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/computers-and-technology/cyber-operations-officer.html adresinden 06.07.2017 tarihinde alındı

http://www.csirt.org adresinden 17.11.2018 tarihinde alındı

https://www.yazilimbilimi.org/bilgi-guvenligi-ve-siber-guvenlik-arasindaki-farklar-nelerdir/ adresinden 02.01.2019 tarihinde alındı

A Strong Britain in an Age of Uncertainty: The National Security Strategy. (2010, Ocak).https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf adresinden 11.05.2017 tarihinde alındı

AKARSLAN, H. (2015, Mayıs). "*Bilişim suçları"* (2. Baskı).2. Bölüm. Seçkin Yayınları.

AVRUPA BİRLİĞİ KONSEYİ VE AVRUPA PARLAMENTOSU. (2002, 07 12). 2002/58/EC sayı ve 12 Temmuz 2002 tarihli Avrupa Birliğli Konseyi Ve Avrupa Parlamentosu Direktifi.

AVRUPA BİRLİĞİ KONSEYİ VE AVRUPA PARLAMENTOSU. (1995, 11 23). Kişisel verilerin işlenmesi ve bu tür verilerin serbest dolaşımına dair bireylerin korunması hakkındaki 95/46/EC sayı ve 24 Ekim 1995 tarihli Avrupa BirliğİKonseyi Ve Avrupa Parlamentosu Direktifi.

AVRUPA BİRLİĞİ/AVRUPA KONSEYİ. (2013, Şubat 15). Siber Suçlara karşı bölgesel işbirliği ortak projesi *"Siber Suçlara Karşı İşbirliğinde Stratejik Öncelikler Deklerasyonu" "CyberCrime@IPA projesine katılan ülke ve yerlerin İçişleri, Güvenlik, Adalet ve Savcılık Hizmetleri Bakanları ve Üst Düzey Bürokratları Toplantısı".*Dubrovnik, Hırvatistan*, https://rm.coe.int/16802f6a42 adresinden 13.05.2017 tarihinde alındı*

TURİZM VE ULAŞTIRMA BAKANLIĞI. "*2016-2019 Ulusal Siber Güvenlik Stratejisi". (* s.7) . http://www.udhb.gov.tr/doc/siberg/2016-2019 guvenlik.pdf adresinden 14.05.2017 Tarihinde alındı

Basic Principles for State Policy of the Russian Federation in the Field of International Information Security (2013) belgenin orjinaline https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf adresinden 01.11.2017 tarihinde alındı

BAYRAKTAR, G. (2015). *Siber Savaş ve Ulusal Siber Güvenlik Stratejisi* (Cilt 1. Basım). Yeniyüzyıl Yayınevi.

BENZER, D. R. (2014, Eylül). *Güncel Tehdit: Siber Suçlar* (Cilt 1. Baskı). Seçkin yayınları.

BIÇAKÇI, D. D., ERGUN, E. D., & ÇELİKPALA, P. D. (2016, Mart).*Türkiye'de Siber Güvenlik ve Nükleer Enerji*. (1. Baskı). s. 31.

Bilgi Güvenliği Derneği. (2012, Haziran). *Ulusal Siber Güvenlik Stratejisi* http://www.bilgiguvenligi.org.tr/wp-

content/uploads/2016/03/Ulusal_Siber_Guvenlik_Stratejisi.pdf adresinden 25.11.2018 tarihinde alındı

Bilgi Teknolojileri ve İletişim Kurumu Faaliyet Raporu . (2016). https://www.btk.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fSayfalar%2fFaaliyet_Raporlari%2f2016_Faaliyetraporu_TR.pdf adresinden 23.11.2017 tarihinde alındı

Bilgi Teknolojileri Ve İletişim Kurumu, T. I.-T. (2014, Temmuz). *Siber Güvenliğe İlişkin Temel Bilgiler.*

Bilişim İnovasyon Derneği Siber Güvenlik Raporu. http://www.bilisiminovasyon.org.tr/webfiles/userfiles/files/siber_guvenlik_raporu.pdf adresinden 17.05.2017 tarihinde alındı

Black Hat Konferansları için bkz. https://www.blackhat.com/us-17/ adresinden 09.08.2017 tarihinde alındı.

China's Military Strategy- Çin Askeri Stratejisi . (2015, Mayıs). http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm adresinden 17.11.2018 tarihinde alındı

Civil Nuclear Cyber Security Strategy,. (2017, Şubat). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/591619/170213_-_Civil_Nuclear_Cyber_Security_Strategy.pdf adresinden 18.11.2018 tarihinde alındı

CLARKE, R. A.& KNAKE, R. K. (2011). *Siber Savaş, .* (M. Erduran, Çev.) İkü Yayın Evi

.

Concept of Russia's Cyber Security Strategy, (2014, Jan) https://ccdcoe.org/cyber-security-strategy-documents.html adresinden 01.11.2017 tarihinde alındı

Convention On Cybercrime,(23/11/2001) ETS No:185 ,Budapest, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 adresinden 01.11.2017 tarihinde alındı

Cyber Crime Strategy. (2010, Mart). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf adresinden 11.06.2018 tarihinde alındı

Cyber Security Regulations and Incentives . (2016, Aralık). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/579442/Cyber_Security_Regulation_and_Incentives_Review.pdf adresinden 17.11.2018 tarihinde alındı

Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space. (2009, Haziran). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf adresinden 01.11.2017 tarihinde alındı

Cybersecurity Strategy . (2015, Eylül). http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf adresinden 19.10.2017 tarihinde alındı

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace . (2013, Şubar 07). https://ec.europa.eu/digital-single-market/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security adresinden 09.10.2017 tarihinde alındı

Cybersecurtiy Annual Report. (2014, Temmuz). http://www.nisc.go.jp/eng/pdf/CYBERSECURITY_ANNUAL%20REPORT_2013_eng.pdf adresinden 17.10.2017 tarihinde alındı

AVRUPA BİRLİĞİ KONSEYİ VE AVRUPA PARLAMENTOSU DİREKTİFİ (1995) *Kişisel verilerin işlenmesi ve bu tür verilerin serbest dolaşımına dair bireylerin korunması hakkındaki 95/46/EC sayı ve 24 Ekim 23.11.1995 tarih ve L 281 sayılı* Avrupa Birliği Resmi Gazetesi, sayfa.31-50 (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 p. 31-50.)

AVRUPA BİRLİĞİ KONSEYİ VE AVRUPA PARLAMENTOSU DİREKTİFİ (2002) *Elektronik Haberleşme Sektöründe Gizliliğin Korunması hakkındaki 2002/58/EC sayı ve 12 Temmuz 2002 tarihli* Avrupa Birliği Konseyi Ve Avrupa Parlamentosu Direktifi- 31.07.2002 tarih ve L 201 sayılı Avrupa birliği Resmi Gazetesi sayfa. 37-47 (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31/07/2002 p. 37- 47.

AVRUPA BİRLİĞİ KONSEYİ VE AVRUPA PARLAMENTOSU, (2006) *Verilerin Saklanması hakkındaki 2006/24/EC sayı ve 15 Mart 2006 tarihli AVRUPA BİRLİĞİ KONSEYİ VE AVRUPA PARLAMENTOSU DİREKTİFİ*- 13 Nisan 2006 tarih ve L 105 sayılı Avrupa birliği Resmi Gazetesi , sayfa. 54- 63 (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic

communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105 13.04.2006 p. 54-63 .

Doctrine of Information Security of the Russian Federation , (2016,December) http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163 adresinden 01.11.2017 tarihinde alındı

DURNA, I. D. (2012, Mayıs). *Çalışma Grubu Genel Koordinasyonu + Çin ve Hindistan İncelemesi*. Siber Güvenlik Raporu. (sy.6)

ENISA. (2012, Mayıs). *National Cyber Security Strategies Setting the course for national efforts to strengthen security in cyberspace*. https://www.enisa.europa.eu/publications/cyber-security-strategies-paper adresinden 15.11.2017 tarihinde alındı

EREN, M. (2017, Mayıs). *"Avrupa Birliği'nin Siber Güvenlik Politikası"* (1. Baskı). İstanbul: Beta Yayınları.

European Network and Information Security Agency. (2010, 01). *France Country Report.* https://joinup.ec.europa.eu/sites/default/files/document/2014-12/France%20Country%20Report.pdf adresinden 15.10.2017 tarihinde alındı

Fransanın Ulusal Savunma Ve Güvenlik Stratejisine ilişkin Beyaz Kitap. (2013). http://mgk.gov.tr/calismalar/calismalar/022_fransa_2013_savunma_beyaz_kitabi.pdf adresinden 17.11.2017 tarihinde alındı

Fransanın Ulusal Savunma Ve Güvenlik Stratejisine İlişkin Beyaz Kitap. (2013). 10 10, 2017 tarihinde https://otan.delegfrance.org/White-Paper-on-Defence-and-National-Security adresinden alındı

French National Digital Security Strategy. (2015). 12.10.2017 tarihinde https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf adresinden alındı

General Framework for Secure IoT Systems . http://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf adresinden 19.10.2017 tarihinde alındı

GÜL, A. F. (2012, Mayıs). Siber Güvenlik Raporu, *Çin ve ABD İncelemesi* .

HEKİM, Y. D., & BAŞIBÜYÜK, D. D. (2014). *Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları- Cyber Crimes and Turkey's Cyber Security Policies"*. Uluslararası Güvenlik ve Terörizm Dergisi, 4(3), 142,143,144.

HENKOĞLU,T. (2015) “Bilgi Güvenliği ve Kişisel Verilerin Korunması” ,Yetkin Yayınları, Ankara , s.27-28

HostExploit’s World Hosts Report . (2014, March). http://hostexploit.com/downloads/world_hosts_report_201403.pdf adresinden 20.11.2017 tarihinde alındı

http://www.computerweekly.com/news/4500247376/Cost-of-UK-cyber-breaches-up-to-314m adresinden 16.11. 2018 tarihinde alındı

https://siberbulten.com/uncategorized/cin-yeni-askeri-stratejisini-acikladi-stratejide-savunma-operasyonda-saldiri/ adresinden 11.10.2017 tarihnde alındı.

KORKMAZ,İbrahim (2016) “*Kişisel verilerin korunması kanunu hakkında bir değerlendirme (an assessment of the law on protectıon of personal data*)”.TBB Dergisi. Sayı 124, sy.83 http://tbbdergisi.barobirlik.org.tr/m2016-124-1571 adresinden 23.11.2017 tarihİnde alındı.

ÜNAL, A. (2012, Mayıs). ABD İncelemesi. *Siber Güvenlik Raporu.* İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü *(*sy.14)

Information Security Strategy for Protecting the Nation. (2010, Mayıs). http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf adresinden 15.10.2017 tarihinde alındı

Information Systems Defence And Security- France’s Strategy . (2011). https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf adresinden 16.10.2017 tarihinde alındı

İngilterenin 2016-2021 Ulusal Siber Güvenlik politikası(National Cyber Security Strategy 2016 to 2021). (2017, Eylül). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf adresinden 12.11.2018 tarihinde alındı

ÜNVER, M., CANBAY, C., & MİRZAOĞLU, A. G. (2009, Mayıs). *“Siber Güvenliğin Sağlanması: Türkiyedeki Mevcut Durum Ve Alınması Gereken Tedbirler,* https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FSayfalar%2FSiberGuvenlik%2Fsg.pdf adresinden 20.07.2017 tarihinde alındı

Japonya Ulusal Güvenlik Stratejisi .
http://mgk.gov.tr/calismalar/calismalar/026_japonya_ulusal_guvenlik_stratejisi.pdf adresinden 16.10.2017 tarihinde alındı

Japonyanın Savunma Beyaz Kitabı. (2013).
http://mgk.gov.tr/calismalar/calismalar/019_japonya_beyaz_kitap_2013.pdf adresinden 16.10.2017 tarihinde alındı

KAÇAKÇILIK VE ORGANİZE SUÇLARLA MÜCADELE DAİRESİ BAŞKANLIĞI . (2012, Mart). *Kaçakçılık ve Organize Suçlarla Mücadele 2011 Raporu*. s. 63. KOM Yayınları. Ankara. (sy.63)
http://www.kom.pol.tr/Sayfalar/Raporlar.aspx adresinden 14.12.2017 tarihinde alındı

KINIKOĞLU, B. Y. (2012, Mayıs). *Birleşik* Krallık İncelemesi . İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü (s.30).

LEWİS, J. A., & TİMLİN, K. (2011). *Siber Güvenlik ve Siber Savaş, Ulusal Doktrin ve Organizasyon Yapısının Ön Değerlendirmesi, Cybersecurity and Cyberwarfare", Center For Strategic and International Studies,*.
http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf adresinden 23.05.2017 tarihinde alındı

YAYLA,M. (2014). "*Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı*". Hacettepe Hukuk Fakültesi Dergisi , 4(2), sy.(185).

National Cyber Security Policy. (2013)
http://164.100.94.102/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf adresinden 16.11.2017 tarihinde alındı

ENİSA,*National Cyber Security Strategies Setting the course for national efforts to strengthen security in cyberspace* . (2012, 05).
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper adresinden 15.10.2018 tarihinde alındı

National Cyber Security Strategy 2014: Progress And Forward Plans. (2014, Aralık).
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf adresinden 15.11.2018 tarihinde alındı

National Cyber Security Strategy 2016 to 2021. (2017, Eylül).
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf adresinden 17.11.2018 tarihinde alındı

National Cyber Security Strategy 2013: Forward Plans And Achievements ,(2013, Aralık) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/265386/The_National_Cyber_Security_Strategy_Our_Forward_Plans_December_2013.pdf adresinden 15.11.2017 tarihinde alındı

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en" adresinden 06.08.2017 tarihinde alındı

KEÇECİ, O. *"Siber Suçlar ve Siber Terörizm"*. http://mebk12.meb.gov.tr/meb_iys_dosyalar/60/01/201260/dosyalar/2016_03/29105407_siber_suclar_ve_terorizm.pdf adresinden 03.04.2017 tarihinde alındı

Overview of China's Cybersecurity Law , IT Advisory KPMG China. (2017, Şubat). https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf adresinden 13.10.2017 tarihinde alındı

POLLARO,G. (2010)"*Isloyal Computer Use And The Computer Fraud And Abuse Act: Narrowıng The Scope*" , Duke Law & Technology Revıew , No:012, sy.2-3 (https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=https://www.google.com.tr/&httpsredir=1&article=1207&context=dltr, adresinden 08.09.2017 tarihinde alındı

RESEARCH, D. (2011). *The risk of social engineering on information security: Asurvey of IT professionals.* https://www.stamx.net/files/The-Risk-of-Social-Engineering-on-Information-Security.pdf adresinden 15.10.2017 tarihinde alındı

Progress against the Objectives of the National Cyber Security Strategy (2012, December) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/265401/Cyber_Security_Strategy_one_year_on_achievements.pdf adresinden 15.11.2017 tarihinde alındı.

SİNGER, P., & FRİEDMAN, A. (Mart 2015). *Siber Güvenlik Ve Siber Savaş,* (1. Baskı b.). (A. Atav, Çev.) Buzdağı Yayınevi.

T.C. ULAŞTIRMA DENİZCİLİK VE HABERLEŞME BAKANLIĞI. (2016, Ocak). *Ulusal Siber Güvenlik Stratejisi ve 2016- 2019 Eylem Planı,*

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2016). *"2016-2019 Ulusal Siber Güvenlik Stratejisi"*. (s.7). http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf adresinden 17.12.2018 tarihinde alındı

T.C. Ulaştırma ve Denizcilik Bakanlığı. (2014, Ağustos). *Siber Güvenliğe ilişkin Temel Bilgiler,USOM.* http://some.sdu.edu.tr/assets/uploads/sites/408/files/siber-guvenlige-iliskin-temel-bilgiler-22092017.pdf adresinden 29.04.2017 tarihinde alındı

TAŞÇI, B. (2012, Mayıs). Fransa ve AB İncelemesi. *Siber Güvenlik Raporu*, (sy.27)

The Chinese Military Updates China's Nuclear Strategy, Full . http://www.ucsusa.org/sites/default/files/attach/2015/03/chinese-nuclear-strategy-full-report.pdf adresinden 11.10.2017 tarihinde alındı

The French White Paper On Defence And National Security. (2008). http://www.mocr.army.cz/images/Bilakniha/ZSD/French%20White%20Paper%20on%20Defence%20and%20National%20Security%202008.pdf adresinden 15.10.2017 tarihinde alındı

The National Strategy of Secure Cyberspace. (2003, Şubat). https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf adresinden 08.07.2017 tarihinde alındı

The Strategic Defence And Security Review: Securing Britain İn An Age Of Uncertainty, . (2010, Ocak). https://www.gov.uk/government/publications/the-strategic-defence-and-security-review-securing-britain-in-an-age-of-uncertainty adresinden 09.07.2017 tarihinde alındı

The UK Cyber Security Strategy 2011-2016: annual report , April 2016 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf adresinden 17.11.2018 tarihinde alındı

The UK Cyber Security Strategy: Protecting and Promoting The UK in a Digital World. (2011, November). Sy.22-23 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf adresinden 08.11.2018 tarihinde alındı

TSELİKOV, Andrey , (2014, November 20) Research Publication No. 2014-15, "The Tightening Web of Russian Internet Regulation", The Berkman Center for Internet & Society at Harvard University, sy.2-4-6 belgenin

orjinaline https://cyber.harvard.edu/publications/2014/runet_regulation adresinden 22.11.2017 tarihinde alındı

WENGER, A. W., MAUER, V. & CAVELTRY, M. D. *Uluslararası CIIP Kılavuzu 2008/2009.* Güvenlik Çalışmaları Merkezi, ETH Zurich.

YALMAN, D. D. *Güncel Tehdit ; Siber Saldırılar, Bilgi Güvenliği Riskleri ve Bilgi Güvencesi* (Cilt 8. Bölüm). Seçkin Yayınları.