
GAZİ ÜNİVERSİTESİ
Gazi
1926

TÜRKİYE'NİN SİBER GÜVENLİK STRATEJİSİ VE EYLEM PLANININ DEĞERLENDİRİLMESİ

Akın AYTEKİN

YÜKSEK LİSANS TEZİ

BİLİŞİM SİSTEMLERİ ANABİLİM DALI

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

HAZİRAN 2015

Akın AYTEKİN tarafından hazırlanan "TÜRKİYE SİBER GÜVENLİK STRATEJİSİ VE EYLEM PLANININ DEĞERLENDİRİLMESİ" tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Bilişim Sistemleri Anabilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Prof.Dr. Şeref SAĞIROĞLU

Bilgi Güvenliği Mühendisliği Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum .....

Başkan: Prof.Dr. Önder Haluk TEKBAŞ

Savunma Bilimleri Enstitüsü, Kara Harp Okulu

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum .....

Üye: Prof.Dr. Halil İbrahim BÜLBÜL

Bilgi Güvenliği Mühendisliği Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum .....

Tez Savunma Tarihi: 24/06/2015

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

.....

Doç.Dr. Nurettin TOPALOĞLU

Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Akın AYTEKİN

24.06.2015

TÜRKİYE'NİN SİBER GÜVENLİK STRATEJİSİ VE EYLEM PLANININ DEĞERLENDİRİLMESİ

(Yüksek Lisans Tezi)

Akın AYTEKİN

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Haziran 2015

ÖZET

Bu tez çalışmasında, siber güvenlik genel olarak incelenmiş ve ulusal açıdan önemi değerlendirilmiş; muhtemel tehditlere önlem alabilmek için stratejik seviyede yapılması gereken planlama üzerine odaklanılmıştır. Ulusal seviyede sosyal hayatın ve kritik altyapıların idamesini sağlayabilmek maksadıyla koordineli, kapsamlı ve planlı bir stratejinin önemine vurgu yapılmıştır. Stratejik planlama yapılırken nelere dikkat edilmesi gerektiği, siber güvenlik stratejisinin diğer stratejik belgelerden neden farklı olması gerektiği araştırılmış, ülkemizde ve dünyada yapılan siber güvenlik stratejisi geliştirme ile ilgili dokümanlar incelenmiştir. İncelenen dokümanlar doğrultusunda siber güvenlik strateji uygulamalarında dünyada öncü rollere sahip olan İngiltere ve Amerika Birleşik Devletleri ile Türkiye'nin strateji belgeleri karşılaştırılmıştır. Ülkemizin mevcut strateji belgesi ile siber güvenlik politikalarında tespit edilen eksikliklerin giderilmesine ve mevcut durumun iyileştirilmesine ilişkin çözüm önerileri sunulmuştur. Bu tez çalışmasının ülkemiz siber güvenlik stratejisini kritik eden ilk çalışma olması, ülkemiz siber güvenliğine gereken önemin verilmesine katkı sağlaması; özellikle strateji belgesinin oluşturulması ile uygulaması hususunda çalışan kurum ve kuruluşlar için rehber bir kaynak olması ve bu konuda yapılacak yeni çalışmalara ışık tutması beklenmektedir.

Bilim Kodu : 902.1.179
Anahtar Kelimeler : Siber güvenlik, bilgi güvenliği, ulusal siber güvenlik, siber strateji, bilgi güvenliği, kritik altyapılar, eylem planı, karşılaştırma, İngiltere, Amerika Birleşik Devletleri.
Sayfa Adedi : 176
Danışman : Prof. Dr. Şeref SAĞIROĞLU

THE ASSESSMENT OF TURKISH NATIONAL CYBERSECURITY STRATEGY AND ACTION PLAN

(M. Sc. Thesis)

Akın AYTEKİN

GAZİ UNIVERSITY

INSTITUTE OF INFORMATICS

June 2015

ABSTRACT

In this study, cyber security has been investigated, its importance has been assessed, strategic planning that has to be done to reduce impacts of possible cyber threats has been focused. The importance of coordinated, comprehensive and proper-planned strategy in order to maintain social life and critical infrastructure has been stressed. What has to be considered while developing strategic plan, why does cybersecurity strategy differ from other strategic documents has been overviewed, and the studies, which have been made in our country and the rest of the world, about development and execution on cybersecurity strategies has been examined. In the light of these documents, the United Kingdom's, the United States of America's and our national cybersecurity strategies has been compared because of the former countries have been known as a pioneer about cyber issues. Solution suggestions are offered to reduce shortcomings about strategic documents, policies and make existing conditions better to obtain high level cybersecurity. Because of being the first study on the field of national cybersecurity strategy, it aims to conribute necessary importance on national cybersecurity issue, especially being a guide source for insititutions and organizations to raise an awareness of cybersecurity strategy and direct future studies in this field.

Science Code : 902.1.179
Key Words : Cybersecurity, information security, national cybersecurity, cyber strategy, critical infrastructure, action plan, comparison, United Kingdom, United States of America.
Page Number : 176
Supervisor : Prof. Dr. Şeref SAĞIROĞLU

TEŞEKKÜR

Başta Ulu Önder, Başöğretmen Mustafa Kemal ATATÜRK olmak üzere, şahsen üzerimde emeği olan ve olmayan, bilgi birikimlerini ve deneyimlerini öğrencilerine aktarmaya çalışan tüm öğretmenlere şükranlarımı sunarım. Çalışmalarım boyunca değerli katkılarını, yardımlarını esirgemeyen, tecrübesini ve ilmini cömertçe aktarmaya çalışan değerli tez danışmanım Prof.Dr. Şeref SAĞIROĞLU'na; tez sürecinde yoğun mesai programına rağmen her fırsatta beni dinleyen, yolumu aydınlatan ve vatana hizmetin nasıl fedakârlık gerektirdiğini defalarca kez ispatlayan TSK Siber Savunma Komutanı Albay Cengiz ÖZTEKE'ye; hayatım boyunca bana olan inançlarını hiç kaybetmeyen, onurlu ve dürüst insan olmanın yolunu gösteren, aramızda hep uzun mesafeler olsa da aile sıcaklığını daima yanımda hissettiren annem Nezihe Afet AYTEKİN, babam Abdullah AYTEKİN ve kardeşim Aydan AYTEKİN'e teşekkürü bir borç bilirim.

Son olarak; başarılı olmam için desteğini hiçbir zaman esirgemeyen, yaşantıma renk katan, sırdaşım, yoldaşım, hayat arkadaşım ve değerli eşim Ebru AYTEKİN ile hayatıma anlam veren, gözümün nuru, biricik kızım Ela AYTEKİN'e şükranlarımı sunarım.

İÇİNDEKİLER

Sayfa

ÖZET iv
ABSTRACT v
TEŞEKKÜR vi
ÇİZELGELERİN LİSTESİ xi
ŞEKİLLERİN LİSTESİ xii
SİMGELER VE KISALTMALAR xiii
1. GİRİŞ 1
2. MATERYAL VE METOD 13
3. TANIMLAR, TERMİNOLOJİ, KAVRAMLAR VE ÖNEMLİ TEHDİTLER 15
3.1. Bilgi ve Bilgi Güvenliği 15
3.2. Siber, Siber Uzay ve Siber Güvenlik 17
3.3. Siber Güvenlik Olayları 19
3.3.1. Estonya siber saldırıları 20
3.3.2. Stuxnet 21
3.3.3. Duqu 22
3.3.4. Conficker 23
3.3.5. Flame 23
3.3.6. Sony 24
3.3.7. Diğer önemli güvenlik ihlalleri 25
4. STRATEJİ VE STRATEJİ HAZIRLAMA YÖNTEMLERİ 27
4.1. Strateji, Stratejik Planlama ve Stratejik Yönetim 27
4.2. Stratejik Yönetim Süreci 29
4.3. Vizyon, Misyon ve Temel İlkeler 30
4.3.1. Vizyon 30
4.3.2. Misyon 32
4.3.3. Temel ilkeler 32
4.3.4. SWOT (GZFT) analizi 34
4.3.5. Stratejik eksenler/hedefler ve amaçlar 37
4.3.6. Ulusal siber güvenlik stratejisi 45
5. ULUSAL SİBER STRATEJİ HAZIRLAMA YÖNTEMLERİ 47

Sayfa

5.1. Uluslararası Telekomünikasyon Birliği (ITU) Ulusal Siber Güvenlik Strateji Rehberi....47
5.2. Bilgi Teknolojileri ve İletişim Kurumu (BTK) Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler....49
5.2.1. Temel ilkeler....50
5.2.2. Yöntem....51
5.2.3. Siber güvenlik adımları....52
5.3. Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) Ulusal Siber Güvenlik Stratejileri, Geliştirme ve Uygulama Üzerine Pratik Rehber....55
5.3.1. Vizyonu, kapsamı, hedefleri ve öncelikleri belirleme....56
5.3.2. Ulusal risk değerlendirmesi yaklaşımını takip etme....56
5.3.3. Hâlihazırdaki politika, mevzuat ve kapasiteleri dikkate alma....57
5.3.4. Şeffaf bir yönetim yapısı geliştirme....57
5.3.5. Paydaşları belirleme....57
5.3.6. Güvenilir bilgi paylaşım ortamı sağlama....58
5.3.7. Ulusal siber acil durum planları oluşturma....58
5.3.8. Siber güvenlik tatbikatları icra etme....58
5.3.9. Temel güvenlik gereksinimlerini oluşturma....58
5.3.10. Olay raporlama mekanizmalarını oluşturma....58
5.3.11. Kullanıcı farkındalığı....59
5.3.12. Ar-Ge'yi teşvik etme....59
5.3.13. Eğitim programlarını güçlendirme....59
5.3.14. Acil durum müdahale kapasitesini oluşturma....60
5.3.15. Siber suçun tespiti....60
5.3.16. Uluslararası işbirliğini sağlama....60
5.3.17. Kamu-özel sektör işbirliğini sağlama....61
5.3.18. Güvenlik ve mahremiyeti dengeleme....61
5.3.19. Değerlendirme....61
5.3.20. Ulusal siber güvenlik stratejisini güncelleme....62
5.4. NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCD COE) Ulusal Siber Güvenlik Yapı Kılavuzu....62

Sayfa

5.5. Beşinci Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (ISC) Siber Güvenlik Makro Analiz Modeli Önerisi ve Türkiye'nin Analizi 65
5.6. Bilgi Güvenliği Derneği (Ulusal Bilgi Güvenliği Stratejisi) 67
5.7. Değerlendirme 68
6. İNGİLTERE VE ABD'NİN SİBER GÜVENLİK STRATEJİLERİNİN İNCELENMESİ 71
6.1. İngiltere 71
6.1.1. Genel bakış 71
6.1.2. Kritik altyapı tesisleri 73
6.1.3. Kamu-özel sektör işbirliği 73
6.1.4. Sorumlu kurumlar 74
6.1.5. Yasal mevzuat 75
6.1.6. Eğitim, kapasite artırımı ve farkındalık çalışmaları 78
6.1.7. Uluslararası işbirliği 80
6.1.8. Ar-Ge faaliyetleri 81
6.1.9. Acil müdahale ekipleri 82
6.1.10. Diğer hususlar 82
6.2. Amerika Birleşik Devletleri 84
6.2.1. Genel bakış 85
6.2.2. Kritik altyapı tesisleri 88
6.2.3. Kamu-özel sektör işbirliği 89
6.2.4. Sorumlu kurumlar 90
6.2.5. Yasal mevzuat 91
6.2.6. Eğitim, kapasite artırımı ve farkındalık çalışmaları 94
6.2.7. Uluslararası işbirliği 96
6.2.8. Ar-Ge faaliyetleri 97
6.2.9. Acil müdahale ekipleri 98
6.2.10. Diğer hususlar 99
7. TÜRKİYE'NİN SİBER GÜVENLİK STRATEJİSİNİN İNCELENMESİ 101
7.1. Genel Bakış 101
7.2. Kritik Altyapı Tesisleri 104
7.3. Kamu-Özel Sektör İşbirliği 106

Sayfa

7.4. Sorumlu Kurumlar 109
7.5. Yasal Mevzuat 109
7.5.1. Türk Ceza Kanunu'nda bilişim suçları 109
7.5.2. Türk Ceza Kanunu'nda bulunan diğer bilişim suçları 112
7.5.3. Özel kanunlarda bilişim suçları 120
7.5.4. 5070 sayılı Elektronik İmza Kanununda düzenlenen bilişim suçları 122
7.5.5. İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun 123
7.5.6. Sanal ortamda işlenen suçlar sözleşmesi 125
7.6. Eğitim, Kapasite Artırımı ve Farkındalık Çalışmaları 126
7.7. Uluslararası İşbirliği 127
7.8. Ar-Ge Faaliyetleri 127
7.9. Acil Müdahale Ekipleri 127
7.10. Diğer Hususlar 129
7.11. Ağ ve Bilgi Güvenliği Ajansının Belirlediği Kriterler Işığında Stratejilerin Karşılaştırılması 131
8. SONUÇ VE ÖNERİLER 139
8.1. Sonuçlar ve Değerlendirmeler 139
8.2. Öneriler 140
KAYNAKLAR 149
ÖZGEÇMİŞ 161

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge 4.1. TBMM İdari Teşkilatı temel ilkeleri. 33
Çizelge 4.2. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı temel ilkeleri 34
Çizelge 4.3. Örnek SWOT matrisi 36
Çizelge 4.4. TBMM İdari Teşkilatının SWOT matrisi 37
Çizelge 4.5. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı SWOT matrisi 38
Çizelge 6.1. Stratejik hedefler ve sorumluluklar 76
Çizelge 7.1. Kamu-özel sektör işbirliği ile ilgili eylem maddeleri 106
Çizelge 7.2. ENISA kriterlerine göre ülke USGS'lerin karşılaştırılması 138

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil 4.1. Stratejik yönetim süreci.....30
Şekil 5.1. ITU Tarafından önerilen referans modeli 48
Şekil 5.2. Küresel Siber Güvenlik Gündeminin beş önemli çalışma alanı.....50
Şekil 5.3. Siber güvenliğin sağlanması üzerine bir yaklaşım 50
Şekil 6.1. Federal siber güvenlik Ar-Ge programı temel ilkeleri 98

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AFAD	Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı
APT	Gelişmiş Israrcı Tehdit (Advanced Persistent Threat)
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojileri Araştırma Merkezi
BM	Birleşmiş Milletler
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CAE	Ulusal Akademik Mükemmeliyet Merkezi (National Center of Academic Excellence)
CCDCOE	Müşterek Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defence Centre of Excellence)
CERT	Bilgisayar Acil Müdahale Ekibi (Computer Emergency Response Team)
CERT-UK	İngiltere Ulusal Bilgisayar Acil Müdahale Ekibi (UK National Computer Emergency Response Team)
CMA	Bilgisayarların Kötüye Kullanılması Kanunu (Computer Misuse Act)
CPNI	Ulusal Altyapı Koruma Merkezi (Center for the Protection of National Infrastructure)
DDK	Devlet Denetleme Kurulu
DoD	Savunma Bakanlığı (Department of Defense)
DDoS	Dağıtık Servis Dışı Bırakma (Distributed Denial of Service)
DHS	İç Güvenlik Bakanlığı (Department of Homeland Security)
DPA	Verilerin Korunması Kanunu (Data Protection Act)
ENISA	Avrupa Ağ ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency)
FBI	Federal Soruşturma Bürosu (Federal Bureau of Investigation)
FISMA	Federal Bilgi Güvenliği Yönetimi Kanunu (Federal Information Security Management Act)

Kısaltmalar	Açıklamalar
GCHQ	Devlet İletişim Karargâhı (Government Communications Headquarters)
IoT	Nesnelerin İnterneti (Internet of Things)
ISAC	Bilgi Paylaşımı ve Analiz Merkezi (Information Sharing and Analysis Center)
ITU	Uluslararası Telekomünikasyon Birliği (International Telecommunication Union)
KAUBA	Kritik Altyapılar Uyarı Bilgi Ağı
MGK	Millî Güvenlik Kurulu
M2M	Makineler Arası İletişim (Machine to Machine Communication)
NATO	Kuzey Atlantik Antlaşması Örgütü (North Atlantic Treaty Organization)
NCA	Ulusal Suç Ajansı (National Crime Agency)
NCCIC	Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi (National Cybersecurity and Communications Integration Center)
NCSP	Ulusal Siber Güvenlik Programı (National Cyber Security Programme)
NCCU	Ulusal Siber Suç Birimi (National Cyber Crime Unit)
NICE	Ulusal Siber Güvenlik Eğitim Girişimi (National Initiative for Cybersecurity Education)
NIST	Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standarts and Technology)
NSF	Ulusal Bilim Kurumu (National Science Foundation)
OECD	Ekonomik Kalkınma ve İşbirliği Örgütü (Organisation for Economic Co-operation and Development)
PLC	Programlanabilir Mantıksal Denetleyici (Programmable Logic Controller)
RFID	Radyo Frekansı ile Tanımlama (Radio Frequency Identification)
SAA	Sosyal Ağ Analizi
SCADA	Veri Tabanlı Kontrol ve Gözetleme Sistemi (Supervisory Control and Data Acquisition)
SGE	Siber Güvenlik Enstitüsü
SOME	Siber Olaylara Müdahale Ekibi

Kısaltmalar	Açıklamalar
STEM	Bilim, Teknoloji, Mühendislik, Matematik (Science, Technology, Engineering, Math)
SWOT	Güçlülük, Zayıflık, Fırsat, Tehdit (Strength, Weakness, Opportunity, Threat)
TBMM	Türkiye Büyük Millet Meclisi
TCK	Türk Ceza Kanunu
TDK	Türk Dil Kurumu
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UDHB	Ulaştırma, Denizcilik ve Haberleşme Bakanlığı
US-CERT	Birleşik Devletler Ulusal Bilgisayar Acil Müdahale Ekibi (United States National Computer Emergency Response Team)
USGS	Ulusal Siber Güvenlik Stratejisi
USOM	Ulusal Siber Olaylara Müdahale Merkezi
WARP	Uyarı, İhbar ve Raporlama Noktaları (Warning, Advice and Reporting Point)

1. GİRİŞ

Teknoloji, hayatımızın her alanına çok hızlı bir şekilde etki etmektedir. Özellikle bilginin işlenmesi, yönetilmesi, saklanması ve taşınması gibi faaliyetlerde kullanılan bilişim teknolojilerinin ve internet kullanımının yaygınlaşmasıyla insan hayatı daha da kolaylaşmış, zamana ve mekâna bağımlı olmadan günlük hayatta yerine getirilmesi gereken sorumluluklar kolaylıkla üstesinden gelinebilir olmuştur. Günümüzde akıllı telefon, tablet bilgisayarlar vb. mobil cihazların kullanımının artmasıyla fatura ödemekten karmaşık bankacılık işlemlerine, uzaktan eğitimden ev alışverişine kadar her türlü işlem kolaylıkla yapılabilmektedir.

Ocak 2014'de yapılan internet kullanımı araştırmasında, dünya üzerinde bulunan 7,1 milyar kişinin 2,5 milyarlık bölümü (%35) internet kullanırken [1], bu rakam Türkiye'de 76,7 milyonluk nüfusta 36,9 milyondur (%48) [2]. Türkiye'de 2008 yılında 6 milyon genişbant internet abonesi bulunurken, 2014 yılı Eylül ayı itibariyle 40 milyon aboneye yaklaşarak, altı katı aşan bir hızla artış göstermiştir. Yine Eylül 2014 itibariyle, 71 908 742 mobil abone bulunurken, 3G abone sayısı 56 780 787 ve cepten internet hizmeti alan abone sayısı ise 31 104 046 kişi olmuştur [2]. Yapılan araştırmalar sonucu internete bağlı kullanıcı ve hane sayısının gün geçtikçe artacağını tahmin etmek hiç de zor olmayacaktır.

İnsanların teknolojiye kolaylıkla sahip olması, bilgi paylaşımı ve iletişim açısından da büyük değişiklikler meydana getirmiştir. Gazete, televizyon, dizi ve filmler gibi geleneksel medyadan farklılık gösteren; kişilerin bilgilerini yayınlamak ve/veya yayınlanmış bilgilere ulaşabilmek üzere, çift taraflı ve eş zamanlı bilgi paylaşımına imkân veren sosyal medya kavramı bunlardan birisidir.

Kitle iletişim araçlarının gelişimine paralel olarak iletişim kanallarının çeşitliliğinin artması, bir yandan içerik doldurma sorununu beraberinde getirirken, diğer yandan da bu "bilgi" ve "enformasyon" bolluğunda "doğru bilgiye" nasıl erişilebileceği sorunsalını da ortaya çıkarmıştır [3]. Kullanıcılarına paylaşım imkânı sağlayan sosyal medya, aynı zamanda kişisel veya belirli gruplar içerisinde medya içeriği oluşturmasına izin vermektedir. Sosyal medya platformlarının en başında, kişilerin hayat koşuşturmaları esnasında paylaşım, iletişim ve bilgi ihtiyaçlarını karşılamak maksadıyla tasarlanmış sosyal ağlar gelmektedir.

İnternet kullanımı araştırmasına göre, dünya üzerinde 1,85 milyar aktif sosyal ağ kullanıcısı bulunmaktadır. Sosyal ağ kullanıcıları Facebook (1,184 milyar), QQ (816 milyon), QZone (632 milyon), Whatsapp (400 milyon), Google+ (300 milyon) platformlarını daha sıklıkla tercih etmektedir [1]. Aynı araştırmada, Türkiye'de 36 milyon aktif Facebook kullanıcısı olması da ayrıca dikkat çekicidir. Bu tip sosyal platformlarda kişilerle iletişime geçebilmek, video/fotoğraf paylaşımları yapabilmek, bilgi alışverişinde bulunabilmek gibi olumlu faydaların yanında çoğu kişisel bilgileri gönül rızası ile veriyor olmak, kişisel bilgi güvenliğini de riske atmaktadır. Ağa katılan bireylerin üstlendikleri rolleri, davranış kalıplarını ve gizli özelliklerini ayıklamak amacıyla Sosyal Ağ Analizi (SAA) uygulanmaktadır. SAA iletişim, paylaşım, organizasyon, istihbarat, güvenlik gibi birçok alanda etkin olarak bireysel ve toplumsal analiz için kullanılmaktadır [4].

Elektronik iletişim ortamının kullanımının artması, kurum ve kuruluşların hizmetlerinin bu ortamda uygulanması imkânını da sağlamış ve e-ticaret ile e-devlet gibi kavramlar ortaya çıkmıştır. Tüm dünyada olduğu gibi ülkemizde de kamu kurum ve kuruluşları bilgi ve iletişim teknolojilerinden giderek daha fazla yararlanarak; karar destek sistemlerini güçlendirmek, iş süreçlerini hızlandırmak, etkinliği artırmak ve harcamalarında tasarruf sağlayabilmek için proje ve uygulamalar geliştirmişlerdir [5].

Elektronik ortamda gönderilen veya alınan bilgilerin, bunları gönderen kişi veya kuruma ait olduğunun doğrulanması, iletilen veya alınan verilerin tanıdık kişiler tarafından gönderildiğinin belirlenmesi, verileri gönderenlerin gönderdiğini ve alanların da aldığını inkâr edememesi, gönderilen veya alınan bilgilerin içeriğinin değiştirilememesi, başkaları tarafından elde edilse bile içeriğinin başkaları tarafından anlaşılamamasının garanti edilmesi gerekmektedir. Bütün bunlar, elektronik ortamda güvenli haberleşme için gerekli temel özelliklerdir [6].

Günümüzde internetten sadece kişiler ve kurumlar faydalanmamaktadır. Radyo Frekansı ile Tanımlama (Radio Frequency Identification, RFID) gibi teknolojiler ile artık evlerde bulunan beyaz eşyalardan arabalara kadar çeşitli nesneler hem internete erişebilmekte hem de kendi aralarında iletişim kurabilmektedir. Ekonomik Kalkınma ve İşbirliği Örgütü (Organisation for Economic Co-operation and Development, OECD) tarafından hazırlanan rapora göre; 2010 yılında internete bağlı olan cihaz sayısı 80 milyon civarında iken, 2015 yılında 290 milyon civarında olması beklendiği; teknolojik gelişmeler doğrultusunda 2020 yılında 1 milyarı aşkın cihazın internete bağlı olacağı öngörülmektedir [7]. Nesnelerin İnternet'i (Internet of Things, IoT) kavramı ile internete bağlanan cihaz sayısının artması ve bu cihazların insanların hayatına çok fazla dâhil olmasıyla güvenlik ihlallerine maruz kalma riskinin aynı doğrultuda artacağı açıktır.

IoT'ye ek olarak (bazı araştırmalarda IoT'nin bir parçası olarak da gösterilmektedir) makineler arası iletişim de (Machine-to-Machine Communication, M2M) insan hayatını kolaylaştıran teknolojik gelişmelerden birisidir. Trafik sistemleri, ulaşım, lojistik, elektrik, su, doğalgaz sayaçları, akıllı şebekeler, iklimlendirme sistemleri, tıbbi otomasyon, akıllı tarım, görüntüleme ve kontrol sistemleri gibi pek çok alanda cihazların uzaktan izlenmesini ve yönetilmesini sağlayan M2M teknolojisi verimlilik, enerji kaynaklarının planlanması ve çevre sağlığı gibi alanlarda olumlu katkılar sağlamaktadır. Kablosuz iletişim imkânları, gelişen bilgi ve iletişim teknolojileri, düşen yatırım maliyetleri ve kullanıcıların benimsemesi nedeniyle M2M uygulamaları çeşitlenerek artmıştır.

M2M hizmetleriyle insan gücü, makine ve yakıtın verimli kullanılması hedeflenmektedir. Makineden makineye teknolojisiyle özel hayat ile iş yaşantısı kolaylaşmakta ve gelişmektedir. Bu teknoloji, süreçleri kolaylaştırıp, verimliliği artırmakta ve hatta hayat kurtarmaktadır [8]. Fakat söz konusu teknolojiyi kullanan kişilerin, cihazların üzerinde bulunan iletişim altyapısı üzerinde herhangi bir tasarrufunun bulunamayacağı düşünüldüğünde, kişisel verilerin gizliliği açısından güvenliğin ihlal edilebileceği durumlar oluşabilecektir.

İnternet kullanımı ile birlikte insanlar ve makineler tarafından elektronik ortamda bulunan bilgiler muazzam bir şekilde çoğalmaktadır. İnsanoğlu, dünya üzerinde bulunan verinin yüzde doksanına yakın bir bölümünü son iki yılda üretmiştir ve günde yaklaşık 2,5 kentilyon bayt ($2{,}5x10^{18}$ bayt) veri üretmeye devam etmektedir [9]. Bu veri sosyal medya paylaşımları, dijital fotoğraf ve videolar, sensörlerden gelen bilgiler, alışveriş kayıtları, cep telefonu sinyalleri vb. kaynaklardan sağlanmaktadır ve tamamı büyük veri olarak adlandırılmaktadır. Büyük verinin, veri madenciliği gibi tekniklerle işlenmesi ile birlikte otomobil sektöründen sigortacılığa, bankacılıktan enerji sektörüne, telekomünikasyon sektöründen ulaşıma kadar her türlü alanda fayda sağlayacak bilgiler edinilebilmektedir. Hatta ulusal güvenlik açısından değerlendirildiğinde; suç ve tehditlerin tahmini ile önlenmesi, vergi kaçakçılığının engellenmesi gibi hususlarda faydalanabilmektedir. Hızla artan büyük veriden ekonomik ve sosyal fayda sağlamak amacıyla, ülkeler ve şirketler bu alana ilgi göstermekte ve Ar-Ge çalışmaları başta olmak üzere, yüksek miktarda kaynak ayırmaktadırlar. Büyük verinin ulusal güvenliği tehdit edecek unsurlar tarafından işlenmesi ile sağlanacak avantaj yitirilebilecektir.

Ülkeler için stratejik seviyede öneme haiz olan sistemler artık bilgi sistem otomasyonları ile idare edilmektedir. Kritik altyapı tesisleri olarak bilinen bu sistemler, Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında "işlediği bilginin gizliliği, bütünlüğü ve erişilebilirliği bozulduğunda; can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar" şeklinde tanımlanmıştır [10].

Çoğunlukla bankacılık ve finans, enerji, ulaşım, bilgi ve iletişim, elektronik haberleşme, sağlık ve temel kamu hizmetleri gibi sektörler ve bunlara ait altyapılar, ülkeden ülkeye değişmekle birlikte, kritik altyapı olarak ele alınmaktadır [11]. Bu sistemlerin bir ülke için stratejik öneme sahip olduğu düşünüldüğünde, doğal hedefler haline dönüşmeleri olasıdır. Zira bir ülkeye zarar vermek, kaos yaratmak ya da ekonomisine zarar vermek için bu sistemlere bir saldırı yapmak yeterli olacaktır [4].

Teknolojik gelişmelerin ışık hızıyla ilerlediği günümüzde, bu gelişmelere paralel olarak tehdit, zafiyet ve risklerin de aynı hızda artması doğal sonuçtur. İnternet milyarlarca cihaz ile milyonlarca ağın birbirine bağlandığı ağların ağı olarak nitelendirilmektedir ve belirli protokoller çerçevesinde bilgi alışverişi yapılmasına imkân sağlamaktadır. Siber tehditlerin ortaya çıkmasına neden olan üç boyut bulunmaktadır ve bunlar: internet tasarımındaki zafiyetler, donanım ile yazılımlardaki hatalar ve kritik sistemlere çevrim içi erişim imkânıdır. İnternet tasarımında beş önemli zafiyet bulunmaktadır. Bunlar; adresleme sistemi, yönetim eksikliği, internetin çalışmasını sağlayan sistemlerin çoğunun açık ve şifresiz olması, zararlı yazılımları dağıtma kabiliyeti ve internetin merkezî olmayan büyük bir ağ olmasıdır [12].

İnternet, sağladığı imkânlar sayesinde siber güvenlik boyutunda kaygıların artmasına sebebiyet vermektedir. Kişisel siber güvenliğin sağlanmasının sadece insanların kendi güvenliğini sağlaması anlamına gelmeyeceği, aynı zamanda sosyal ağ, elektronik posta gibi hizmetlerin gerektiği gibi kullanılmamasının, bağlantılı olunan diğer kişilerin bilgi ve bilgisayar güvenliğini tehlikeye atacağı aşikârdır [13]. Bilgi ve bilgi güvenliğinin ötesinde 2015 yılında ilk siber cinayetin işlenebileceği ihtimali üzerinde dahi durulmaktadır [14]. Herhangi bir bilgisayar ağında meydana gelen bir güvenlik ihlali bir anda o ağın bağlı olduğu diğer tüm ağları etkileyebilmektedir. Kurumsal ağlar üzerinde haberleşen, sayıları hızla artarak yaygınlaşan ve geniş kitlelerce kullanılan uygulamalar üzerinde tutulan bilgiler düşünüldüğünde kurumsal anlamda bilgi güvenliğinin sağlanmasının önemi daha iyi anlaşılacaktır [15].

Bilgisayar ağları üzerinde gerçekleşen ihlallerin kişisel, kurumsal hatta küresel bakımdan etkileri olmaktadır. İnternet bankacılığı yapmakta olan kişinin hesabında gerçekleşecek bir dolandırıcılık hadisesi, sadece o kişinin parasını kaybetmesine sebep olurken; bir hastanenin veritabanında gerçekleşecek bir güvenlik ihlali, hastaların kişisel bilgilerinin ele geçirilmesine sebebiyet verebilecektir.

İlk örnekte bankanın güvenilirliği ve saygınlığı zedelenirken diğerinde hastanede bulunan hastaların hayatları söz konusu olabilmektedir. Ulusal ve/veya küresel açıdan değerlendirmek gerekirse; gerçekleştirilecek siber saldırılarla ülkelerin milyarlar tutarında maddi kayba uğraması olasılık dâhilindedir. Bir İngiliz sigorta firmasının yaptığı araştırma ile siber saldırıların firmalara yıllık olarak 400 milyar dolarlık bir zarara sebebiyet verdiği sonucuna varılmıştır [15].

Kişilerin bu tür saldırılara maruz kalıp maddi ve manevi kayıplara uğramaması için alması gereken önlemler bulunmaktadır. Belli başlı önlemler; işletim sistemlerinin orijinal olması ve sürekli güncellenmesi, güvenilir bir antivirüs programı ve güncellemeleri, güvenlik duvarı, internette kullanılan şifrelerin kolayca tespit edilemeyecek karmaşıklıkta olması, dosyaların paylaşıma açılmaması, belli aralıklarla yedekleme yapılması, internette gezinti yaparken yapılması ve yapılmaması gereken bazı faaliyetlere dikkat edilmesi vb. şeklinde sıralanabilir. Kurumlar ise, bilgi güvenliği standartlarına uyumluluk kapsamında altyapılarını gözden geçirmeli ve gözden geçirme sonucunda ortaya çıkan ihtiyaçlara bağlı olarak alınması gereken önlemleri ve yatırımları zamanında yapmalıdır [16].

Symantec firmasının 2014 yılında hazırlamış olduğu bir raporda çarpıcı bilgiler bulunmaktadır. 2013 yılında gerçekleştirilen sekiz adet siber güvenlik ihlali, en az 10 milyon adet kimlik hırsızlığı ile sonuçlanmıştır. Aynı yıl içerisinde toplam 552 milyon kimlik bilgisi çalınmıştır. Bu kimlik bilgileri içerisinde; müşterilerin kredi kartı bilgileri, doğum tarihleri, kimlik numaraları, ev adresleri, sağlık kayıtları, finansal bilgileri, elektronik posta adresleri, telefon numaraları, şifreleri ve diğer kişisel bilgileri bulunmaktadır. Saldırganların güvenlik kameraları, yönlendiricileri (router), akıllı televizyonları, arabaları ve hatta bebek izleme monitörlerini hedef almaları da ilgi çekicidir. Bu gibi IoT cihazlarını ele geçirerek daha sonra hedeflenen kişilere ulaşmak için erişim noktası olarak kullanılması hedeflenmektedir [17].

İşte bu noktada kişiler ve kurumlar dışında dijital devrimin kurallarının belirlenmesi ve yönetilmesi hususunda devletlere bir takım görevler düşmektedir. Siber ortamın hayatımızın ayrılmaz bir parçası olmaya başlamasıyla, bu ortama dair kuralların geliştirilmesine ihtiyaç duyulmuştur. Özellikle iş dünyası, araştırma kuruluşları, akademik camia, silahlı kuvvetler ile birçok kuruluş ve sektörün siber ortamı kullanmasıyla, bu ortamın güvenliğine dair kural ve politikaların konulması şart olmuştur. Ülkeler, güvenli bir siber ortam sağlayabilme yolunda, siber ortamın parçası olan bileşenleri siber saldırılara karşı korumak, yapılan saldırılara müdahale etmek, saldıranları cezalandırmak, gerekli yasal mevzuatı oluşturmak ve bütün faaliyetleri yerine getirecek yapıları tesis etmek üzere siber ortama yönelik politika ve stratejiler geliştirmiş ve geliştirmeye devam etmektedir [11].

Türkiye'de siber suçlarla mücadele 2012 yılına kadar Bilim, Sanayi ve Teknoloji Bakanlığının koordinatörlüğünde Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından sivil toplum kuruluşları ve kurumları ile beraber yürütülmüştür [4]. Aralık 2012'de "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" hazırlanarak yürürlüğe girmiştir. 20 Ekim 2012 tarih ve 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" 28447 sayılı Resmi Gazetede yayımlanmıştır.

Kişisel, kurumsal ve ulusal verilerin çalınması, kurumsal ticarî sırların istenmeyen kişiler tarafından ele geçirilmesi, devlet sırlarının açığa çıkarılması gibi pek çok olumsuz sonuçlara sebebiyet verecek tehditlerle mücadele kapsamlı, koordineli ve planlı olması gereken bir faaliyettir. Bu mücadele, ancak stratejik seviyede hazırlanan politikalar ve bu politikaların etkin bir şekilde uygulanması ile gerçekleştirilebilir.

2012 yılında yayımlanan ulusal siber güvenlik stratejimiz incelenmesi sonucunda gelişen siber tehditlere karşı alınması gereken tüm tedbirlere, strateji belgesinde yer verilmediği gözlemlenmiştir. Öncelikle, siber güvenlik konusunda yasal mevzuatın düzenlenmesi, kurumsal yapılanma ve koordinasyon modelinin sağlanması gerekmektedir.

Bilgi teknolojilerinin kullanımının artmasıyla sadece kamu kurumlarının sahip olduğu bilgi sistemleri ve altyapıları değil, özel sektör tarafından işletilen kritik altyapıların bilgi güvenliğinin sağlanması da büyük önem arz etmektedir. Devletin ve özel sektörün sahip olduğu kritik altyapıların neler olduğuna ve bunların siber tehditlere karşı korunmasına dair yapılan herhangi bir girişim bulunmamaktadır. Sosyal ve ekonomik yaşamda büyük rol oynayan bu kritik tesislerin denetim, koordinasyon ve standardizasyon yetki ve sorumlulukları mutlaka belirlenmeli; ulusal siber güvenlik stratejisinde kamu ve özel sektörün üzerine düşen sorumluluklar genel hatlarıyla tespit edilmelidir.

Ülkemizin, ulusal siber güvenlik stratejisinin ilgili eylem maddelerinde tüm kamu kurumları ile kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlara Siber Olaylara Müdahale Ekipleri kurulması ile ilgili görevler verilmiştir. Sektörel ve Kurumsal SOME'lerin kurulması ile kamu-özel sektör arasındaki bilgi akışları hızlanacak, gelişen siber tehditlere karşı etkin mücadele edilmesi söz konusu olacaktır. Bu ekiplerin kurulması ve işletilmesi için çalışma esasları belirlenmeli, eğitim planları hazırlanmalı ve mutlaka Ulusal Siber Olaylara Müdahale Merkezinin koordinasyonunda faaliyetlerinin yürütmelidirler.

Kişisel, kurumsal ve ulusal bilgi güvenliğinin sağlanmasında insan faktörü kuşkusuz en önemli yere sahiptir. Ulusal, kurumsal veya sektörel olarak alınacak güvenlik tedbirleri yeterli olarak eğitim almamış, siber güvenlik konusunda farkındalığa sahip olmayan çalışanların zafiyetleri yüzünden kolaylıkla aşılabilmektedir. Sosyal mühendislik olarak adlandırılan yöntemlerle insan ilişkileri ve/veya insanların dikkatsizlikleri kullanılarak hedef kişi ya da kurum hakkında bilgi toplanabilir; kişinin bilgileri veya kurumsal ağ bağlantıların yapısı hakkında siber saldırıda kullanılacak her türlü bilgi elde edilebilir. Bu tip tehditleri bertaraf etmek ancak yeterli eğitimle sağlanabilir. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında, eğitim ve kullanıcı farkındalığı ile ilgili bölümlerin mutlaka genişletilmesi gerekmektedir.

İnternetin ortaya çıkışı ve iletişim teknolojilerinin yaygın olarak kullanılmanın giderek artmasıyla yeni suç tipleri ortaya çıkmıştır. Bu suçları işleme konusundaki eğilim suçluların kendilerini geliştirme kapasiteleri ve elindeki saldırı araçları güçlendirebileceği varsayımı ile daha da artacaktır. Değişik tekniklerle siber suçlar binlerce kilometre uzaktan rahatlıkla işlenebilmektedir. Bu noktada yeni suç ve suçluların engellenmesi için uluslararası işbirliği olanakları arttırılmalıdır.

Söz konusu işbirliği sadece sempozyum, konferans, toplantı, seminer ve tatbikat seviyesinde kalmamalı; gelişmiş ülkelerde uygulanan Ar-Ge faaliyetleri incelenerek benzer altyapıların kurulması gerekmektedir. Ar-Ge faaliyetleri öncelikle siber güvenlik ürünlerinin (yazılım ve donanım), ilerleyen zamanlarda ise mili işletim sistemi ve SCADA gibi sistemlerinin millî olarak geliştirilmesi planlanmalıdır.

Yukarıdaki paragraflarda bahsedilen hususların tamamının gerçekleştirilmesi için yeterli bir bütçenin tahsis edilmesi gerekmektedir. Dünyada teknoloji konusunda öncü olan ülkeler incelendiğinde; gerek Ar-Ge gerekse eğitim faaliyetleri için bütçeler ayrılmış ve planlı bir şekilde kullanılmıştır. İngiltere sadece siber güvenlik stratejisinin uygulanması için dört yıl için 650 milyon pound, ABD ise yıllık 1 milyar dolara yakın bütçe tahsis etmiştir. Bu devletlerin siber güvenlik politikaları incelendiğinde; gelişen ve değişen koşullar doğrultusunda strateji belgelerinin güncellendiği görülmektedir. Ulusal siber güvenlik stratejisi ve 2013-2014 yılları arasında yapılması gereken eylem planları mutlaka güncellenmeli; güncellenen strateji belgesinde söz konusu eylem planları için bütçenin tahsisi gerçekleştirilmelidir.

Burada kısaca özetlendiği gibi ülkemiz Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı gözden geçirildiğinde, pek çok hususa değinilmesi ve hedefler konulması önemli olsa da, bazı hususların dikkate alınmadığı (bütçe gibi) belirlendiğinden; strateji ve eylem planının detaylı olarak incelenmiş ve bazı gelişmiş ülkelerle karşılaştırılmıştır.

Bu tez kapsamında; literatürde geçen ve geniş tanımlara sahip olan bilgi, bilgi güvenliği, siber, siber güvenlik, siber suç, siber terörizm, siber savaş vb. kavramların açıklanması gerekmektedir. Suçun unsurları Türk hukuk öğretisinde dörtlü ayrıma tabi tutulmaktadır. Bunlar; kanunilik, maddi, manevi ve kusurluluk unsurlarıdır. Kanunilik unsuru gereğince bir eylemin suç olarak kabul edilmesi için ceza kanununda suç olarak tanımlanması ve bunun da ya birebir tanımda gösterilen şekilde gerçekleşmesi yahut eğer serbest hareketli bir suç söz konusu ise bu hareketlerden herhangi birinin gerçekleşmiş olması gerekir. Dolayısıyla çok geniş kapsamı olan bilgi, bilgi güvenliği, siber, siber güvenlik tanımlarının yapılması gerekmektedir. Bölüm 3'te "Tanımlar, Terminoloji, Kavramlar ve Önemli Tehditler" konu başlığı altında gerekli açıklamalar yapılmış ve büyük çaplı ihlallere sebebiyet veren siber güvenlik olayları anlatılmıştır.

Ünlü strateji uzmanı Zhang Yu; "Stratejin derin ve uzağı gören cinsten ise daha savaşmadan sen kazanırsın. Stratejik düşüncen sığ ve kısa erimli ise, daha savaşmadan sen kaybedersin. Zengin strateji yoksul stratejiye üstün gelir, stratejisi olmayanlar yenilmeye mahkûmdurlar. Bu yüzden, muzaffer savaşçıların önce kazanıp sonra savaştığı, mağlup savaşçıların ise önce savaşıp sonra kazanmaya çalıştıkları söylenir." sözleri ile strateji hazırlamanın önemini çok güzel bir şekilde özetlemiştir. Strateji, stratejik yönetim, strateji hazırlama yöntemleri ve Türkiye'de kamu kurum ve kuruluşlarının hazırlamış olduğu örnek stratejilerin incelendiği "Strateji ve Strateji Hazırlama Yöntemleri" Bölüm 4'te kapsamlı olarak anlatılmıştır.

Siber tehditlerin doğası, hızı, sınırlara bağlı olmaması, kaynağının kolayca tespit edilememesi vb. sebeplerden dolayı siber güvenlik stratejisi hazırlamak, diğer strateji belgelerini hazırlamaktan çok farklıdır. Sadece siber güvenlik stratejisi hazırlama üzerine yapılmış onlarca çalışma, yazılmış yüzlerce makale bulunmaktadır. Dünyada konusunda uzman kişi, kurum, kuruluşlar tarafından yazılmış olan siber güvenlik stratejisi hazırlama yöntemleri ile ilgili literatür taraması yapılmış ve Bölüm 5'de ayrıntılı olarak açıklanmıştır.

Altıncı bölümde literatür taraması yapılan belgeler ışığında, siber güvenlik konusunda başarı sağlamış olan İngiltere ve Amerika Birleşik Devletleri'nin siber güvenlik strateji belgeleri Bölüm 5'te incelenmiştir. Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı önceki bölümlerde tespit edilen ana unsurlar ışığında ayrıntılı olarak Bölüm 7'de incelenmiştir. Tez çalışmasının sonunda elde edilen bilgiler, ülkemiz siber güvenlik stratejisine fayda sağlayacağı değerlendirilen kazanımlar ve sunulan öneriler, "Sonuç ve Öneriler" konu başlığı altında Bölüm 8'de sıralanmıştır.

Bu tez çalışması, güncel ve hızla gelişen tehdit olan siber suçlara karşı kişi, kurum ve devlet bazında hazırlanacak olan strateji ve eylem planlarında farkındalık yaratılması amacıyla hazırlanmıştır. Kusursuz siber güvenliğin sağlanmasının imkânsız olduğu dünyamızda, yapılmış olan çalışmalara ek olarak; siber güvenlik stratejimizin günümüz koşullarına uygun hale getirilmesi, olumlu ve olumsuz yanlarının objektif olarak kritik edilmesi, var ise eksikliklerin ortaya konulması ve ülke siber güvenliğini sağlamakla yükümlü kurum ve kuruluşları aydınlatması yönünde katkılar sağlamak amacıyla yapılmıştır.

2. MATERYAL VE METOD

İlk defa ABD'de Savunma Bakanlığı İleri Araştırma Projeleri Ajansı (Advanced Research Projects Agency, ARPA) tarafından başlatılan ARPAnet projesiyle; herhangi bir saldırıya uğraması veya bir bölümünün hizmet dışı kalması ihtimaline karşı faaliyetlerine devam etmek maksadıyla yaratılmış olan internet, protokolleri esnek, güvensiz ve açık olarak tasarlanmıştır. Daha sonra söz konusu ağa daha çok bilgisayar bağlanarak kullanılırlığı ve etkinliği artmıştır. İlk başlarda eğitim ve araştırma ağı olarak tasarlanan internet kamu, özel sektör ve ticari faaliyetler için temel iletişim altyapısı haline gelmiştir. İnternetteki ve diğer iletişim sistemlerini kapsayan siber uzaydaki açıklıklar kişi, kurum, devlet ve organizasyonlar için güvenlik risklerini de beraberinde getirmektedir.

Bilginin tartışmasız büyük bir güç olduğu çağımızda, bilginin güvenliğini sağlamak önemli bir sorun haline gelmiştir ve güvenlik için söz konusu tedbirleri almak devletlerin görevidir. Günümüzde siber tehditlerin tespitinin çok güç olması, saldırganların teknolojiyi etkin bir şekilde kullanması ve iyi organize olmaları münasebetiyle siber suçluların tespiti çok zorlaşmıştır. Kritik altyapı tesislerinin de siber uzaya bağımlılığı ve bu tesislerin siber tehditler vasıtasıyla kullanım dışı kalması ihtimali de devletler tarafından göz önünde bulundurulmalıdır. Ayrıca ulusun siber güvenliğinin tesisi, siber suç ve suçlular ile mücadele, halkın eğitim seviyesi ile farkındalık düzeyinin arttırılması, siber olaylarla mücadele teşkilatlarının etkili şekilde çalışması, siber güvenlik konusunda uzman kurum/kuruluş/devletler ile koordine sağlanması da yine devletlere düşen görevlerdir.

Bu kapsamda; bilgi ve iletişim teknolojilerinin oluşturduğu, kapalı veya internete bağlı iletişim ağlarından oluşan siber uzaydaki ülke etkinliğinin; kritik altyapı tesisleri ile toplumun ekonomik ve sosyal refahının idamesini sağlamak üzere, uygulanabilir stratejik planlama yapılmasına ihtiyaç duyulmaktadır. Bu tez çalışmasında, 2012 yılında yayımlanmış olan USGS incelenmiş ve söz konusu strateji belgesinde tespit edilen hususlar 1. Bölümde kısaca açıklanmıştır.

Bu tez çalışmasında siber tehditlere karşı planlı, kapsamlı ve koordineli bir USGS'nin hazırlanması maksadıyla aşağıda belirtilen adımlar izlenmiştir:

- Ülkemizde ve dünyada siber güvenlik ve siber güvenlik stratejisi konusunda literatür taraması yapılmıştır. Söz konusu tarama sonucunda, Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının siber tehditlere karşı ulusal temelde mücadele için yetersiz olduğu tespit edilmiştir.
- Siber güvenlik ile ilgili olan kavramlar açıklanmıştır.
- Strateji hazırlama konusu ilk olarak yönetim bilimi açısından incelenmiştir. Kapsam açısından TBMM İdari Teşkilatı ve Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Stratejik Planları incelenmiş ve karşılaştırma yapılmıştır.
- Siber güvenlik stratejisi hazırlama konusunda dünyada ve ülkemizde hazırlanmış kılavuzlar ile çalışmalar incelenmiştir. Bu inceleme sonucunda Avrupa Ağ ve Bilgi Güvenliği Ajansının (ENISA) yapmış olduğu "Ulusal Siber Güvenlik Stratejileri, Geliştirme ve Uygulama Üzerine Pratik Rehber" ile Uluslararası Telekomünikasyon Birliğinin (ITU) hazırladığı "Ulusal Siber Güvenlik Strateji Rehberi" kapsam ve içerik açısından örnek doküman olarak ele alınmıştır.
- Dünyaca siber güvenlik tehditlerine en çok maruz kalan, teknoloji alanında Ar-Ge çalışmalarına öncülük eden, ekonomisinin büyük bir bölümünün internete bağlı ekonominin oluşturduğu, stratejik doküman hazırlama ve uygulama konusunda tecrübe sahibi iki ülke olan İngiltere ve ABD Ulusal Siber Güvenlik Stratejileri, ENISA'nın hazırlamış olduğu doküman doğrultusunda incelenmiştir. Söz konusu doküman ışığında Türkiye'nin USGS müteakiben incelenmiştir. Bu ülkelerin USGS'lerinin, ENISA ve ITU tarafından hazırlanmış strateji hazırlama dokümanlarında izlenmesi gereken yolları takip ettikleri tespit edilmiştir.
- Söz konusu dokümanların incelenmesi sonucunda, Türkiye'nin Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın güncellenmesine olanak sağlayacak şekilde çözüm ve önerilerin sunulması amaçlanmıştır.

3. TANIMLAR, TERMİNOLOJİ, KAVRAMLAR VE ÖNEMLİ TEHDİTLER

Özellikle 20'nci yüzyılın ortalarından itibaren elektronik alanda yaşanan gelişmeler bilginin elde edilmesi, depolanması, işlenmesi ve iletilmesi açısından bir çığır açmış ve bilgi toplumuna dönüşüm sürecini de önemli ölçüde hızlandırmıştır. Son yıllarda ise bilgi ve iletişim teknolojileri ekonomik ve sosyal hayatın tüm alanlarında kullanılan genel amaçlı teknoloji haline gelmiştir. Bu süreçte bilgi ve iletişim teknolojilerinin bizatihi kendisi bilgi içeriği ve katma değeri yüksek bir sektör olarak belirmiş, bu teknolojilerin diğer sektörlerde kullanımı da yeni bilgilerin üretilmesine, yeni ve daha etkin iş yapış yöntemlerinin geliştirilmesine, üretim faktörlerinin üretkenliğinin artmasına, yeni iş ve uzmanlık alanlarının ortaya çıkmasına imkân sağlamıştır. Bu gelişmeler ekonomik, sosyal ve bireysel yaşamı yoğun biçimde etkilemektedir. Ülke ekonomileri arasındaki rekabet de bu gelişmelerden etkilenmekte; bilgi ve iletişim teknolojilerini ve bilgiyi etkin kullanan ülkeler uluslararası rekabet avantajı sağlamaktadır [18].

Tez çalışmasının bu bölümünde konunun öneminin anlaşılabilmesi için bilgi, bilgi güvenliği, siber, siber güvenlik kavramları açıklanmış, büyük çaplı güvenlik ihlaline sebep olan siber güvenlik olayları incelenmiş; tanım ve kavramlar ile karşılaşılabilecek tehditler sunulmuştur.

3.1. Bilgi ve Bilgi Güvenliği

Dijital dönüşüm; bireyler, girişimler, kamu ve sosyal kurumları yeni düzenin ruhuna uygun niteliklere sahip olma baskısıyla karşı karşıya bırakmaktadır. Bu açıdan, bilgi üretme motivasyonu yüksek, günlük hayatında ve karar alma süreçlerinde bilgiyi doğru şekilde yorumlayıp işleyebilen, sistematik düşünme yeteneği gelişmiş, kendisini ve yaşadığı çevreyi sorgulayan ve sürekli/hayat boyu öğrenen bireylerin ve kurumların ağırlıkta olduğu bir toplum yapısı ortaya çıkmaktadır [18].

Çok geniş bir kavrama sahip olan bilginin literatürdeki tanımları şu şekildedir:

Sözlük anlamı olarak bilgi;

- İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat,
- Öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, malumat, vukuf,
- İnsan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf,
- Genel olarak ve ilk sezi durumunda zihnin kavradığı temel düşünceler,
- Bilim,
- Kurallardan yararlanarak kişinin veriye yönelttiği anlam olarak tanımlanmıştır [19].

Claude E. Shannon, bir mesajın içerisindeki belirsizliği olasılık kavramı ile ilişkilendirerek mesajın içerisindeki bilgi miktarını tanımlamıştır. Yani bilgiyi, bir konu hakkında belirsizliği azaltan kaynak olarak tanımlamıştır [20]. Nonaka ve Takeuchi bilgiyi doğruluğu ispatlanmış inançlar olarak tanımlamaktadır [21]. Wiig ise; doğrular ve inanışlardan, öngörüler ve kavramlardan, muhakeme ve beklentilerden, metodolojiler ve teknik bilgilerden oluştuğunu belirtmiştir [22].

Kavramların tam olarak anlaşılması için veri (data), bilgi (information) ve özbilginin (knowledge) de bilinmesi gerekmektedir. Veri (doğru veya doğru olmayan) olaylar, gözlemler veya algılardan oluşur; tek başına ham sayılar ve iddialarla ifade edilir ve anlam ve bağlayıcılık sağlamayabilir [23]. Bilgi sadece birbirleriyle içerik, ilgi ve amaca sahip olan verinin alt kümesidir. Tipik olarak ham verinin içinden anlamlı eğilim ve örüntü elde edilmiş halidir. Özbilgi ise; karar ve eyleme dönüştürülmüş bilgidir [23]. Örnek vermek gerekirse; bir telefon numarası veridir, telefon numaralarının kime ait olduğunu gösteren telefon rehberi bilgidir, fakat bir organizasyondaki/kurumdaki yetkili kişilerin kim olduğuna dair sahip olunan bilgi ise özbilgidir.

Bilgi, içeriğine göre bireysel ve kurumsal olmak üzere ikiye ayrılmaktadır. Bireysel bilgi, kurumsal bilgi tabanının gelişmesi için gerekli olan beceri ve yeteneklerden oluşmaktadır. Kurumsal bilgi, kurum içinde üretilen veya kuruma dışarıdan gelen, o kurumla ilgili kayıtlı ya da kayıtsız her türlü bilgiyi ifade etmektedir. Kurumsal bilgi; bireysel bilgilerin toplamının yanı sıra, diğer kurumlar tarafından kolayca taklit edilemeyecek şekilde insan, teknoloji ve yönetim ilkeleri arasında üretilen bilgi kaynaklarını ifade etmektedir.

Kurumsal bilgilerin diğer kurumlar tarafından taklit edilmesi, söz konusu unsurlar arasında oluşturulan etkileşim, kurumun kendine özgü kültürü ve kurumun tarihçesini de içine aldığından zor ve zaman alıcıdır [16].

Değerli olduğu belirlenmiş bireysel veya kurumsal bilginin gerektiği gibi korunmaması sonucunda maddi, stratejik ve itibar kayıpları yaşanmaktadır. Bu kritik varlığın kendisine sahip olan kişiler, kurumlar ve devletler tarafından korunması gerektiği açıktır. İşte bu hususta bilgi güvenliği kavramı devreye girmektedir.

Bilgi güvenliğinden bahsedebilmek için; gizlilik, bütünlük ve erişilebilirlik gibi güvenlik bileşenlerinin oluşturulmuş olması gerekmektedir. *Gizlilik*; bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilmesi, yetkisi ve izni olmayan kişiler tarafından ele geçirilse bile anlamlı olarak ele geçirilmesinin önlenmesidir. *Bütünlük*; bilginin ve işleme yöntemlerinin doğruluğunu ve değiştirilmediğini temin etme, alıcıdan çıktığı haliyle ulaştırılmasının garanti edilmesidir. *Erişilebilirlik*; yetkili kullanıcıların gerek duyduğunda bilgiye ve ilişkili kaynaklara erişilebileceklerinin garanti edilmesi, gerekli olan tüm önlemlerin alınmasıdır.

Yukarıda bahsedilen bileşenlerin ışığında bilgi güvenliği;

- Bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve şekilde kullanılarak, bilginin her türlü ortamda istenmeyen kişiler tarafından elde edilmesini önleme,
- Kişi ve kurumların bilgisayar teknolojilerini kullanırken daha önceden analizlerin yapılarak gerekli önlemlerin alınma işlemi,
- Kısaca; öneme sahip veya değerli bilgilerin korunmasına yönelik çabaların tümüdür [6].

3.2. Siber, Siber Uzay ve Siber Güvenlik

Siber kelimesinin Türk Dil Kurumu (TDK) sözlüğünde bir karşılığı olmamakla beraber; bilgisayar, bilgi teknolojisi ve sanal gerçeklik ile ilgili kullanılan bir sıfattır [24]. Siber çağ, siber ortam, siber alan, siber uzay, siber savaş, siber terörizm, siber suç sıkça kullanıldığı alanlardır.

İlk olarak William Gibson tarafından Burning Chrome adlı kitabında kullanılan siber uzay (cyberspace) kavramı, tasarladığı karakterler için şifre maksadıyla "çağrışım yapan ve özellikle anlamsız" bir terim olarak tanımlanmıştır [11]. Bu terim daha sonra popüler kültür tarafından bilgi çağının gücü ve yaygınlığı sayesinde evrilerek sıkça kullanılmaya başlanmıştır. Bilgisayarlar ve bilgi teknolojilerinden internete kadar teknolojileri betimlemek için popüler televizyon şovları ve filmlerde kullanılmıştır [25].

Siber uzay (dilimizde siber ortam ve siber alan olarak da kullanılmaktadır) da farklı şekilde tanımlamalara sahiptir [11]:

- Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortamı ifade eder [10].
- Bilgisayar ağlarının oluşturduğu, üzerinde iletişimin gerçekleştiği kavramsal ortamdır [26].
- İnsanların bilgisayarlar ve telekomünikasyon sistemleri aracılığıyla herhangi bir coğrafi sınırlamaya maruz kalmadan tamamen birbirine bağlı olma durumudur [27].
- İnternet, iletişim ağları, bilgisayar sistemleri, gömülü işlemci ve kontrol birimlerini içeren, bilgi teknolojileri altyapılarından meydana gelen, birbirine bağımlı ağların oluşturduğu bilgi ortamındaki küresel bir alandır [28].
- Bilgisayar ve bilgisayar ağlarının ortaya çıkardığı, insanlar ve bilgisayarların bir arada bulunduğu ve çevrim içi faaliyetlerin tüm yönlerini içeren sayısal bir dünyadır [29].

Tanımlar incelendiğinde siber uzayın, birçok iletişim ağından oluştuğu görülmektedir ve iletişim ağlarının birbirine bağlanmasıyla siber uzay her geçen gün büyümektedir. İnternete bağlı olmayan kapalı sistemlerin de siber uzayın bir parçası olduğu göz önünde bulundurulduğunda; internetin siber uzayı oluşturan önemli öğelerden biri olduğu fakat siber uzayın sadece internetle sınırlı kalmayacağı bir gerçektir. İletişim ağları, bilgi sistem teknolojilerini kullanan kapalı ağlar, enerji dağıtım ağları, cep telefonları, yazılım tabanlı telsiz sistemleri, insansız hava araçları, uçaklar gibi birçok sistem; siber uzayın elemanlarındandır [11].

Uluslararası Telekomünikasyon Birliği (International Telecommunication Union, ITU), siber güvenliği, "Siber saldırılara karşı alınacak tedbirlerin bütünüdür. Kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullandığı araçlar, geliştirilen politika ve uygulamalar; yazılı belgeler, elektronik ortam dokümanları, etkinlikler, eğitimler ve bilişim alanında kullanılan güvenlik teknolojilerinin tamamı siber güvenliğin unsurları arasındadır." şeklinde tanımlamaktadır [30]. Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında ise, "Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi" şeklinde ifade edilmiştir [10].

Siber tehditler artık sadece bilgisayar sistemlerine verdikleri zararlar (sistemlere sızma, sistemlerden bilgi çalma ve sistemlere asılsız bilgi koyma) ile sınırlı kalmamaktadır. Bir ülkenin kritik olarak kabul edilebilecek haberleşme sistemlerine, bilgisayar sistemlerine, enerji ve ulaşım ağlarına, askeri komuta ve kontrol sistemlerine zarar verecek ölçüde, asimetrik bir harp çeşidi olarak ortaya çıkmaktadır. Bu nedenle, siber tehditlerin önümüzdeki yıllarda da önemli tehditlerden biri olacağı düşüncesi; tüm dünya tarafından kabul edilmeye başlanmıştır. Bu kapsamda, geçmiş yıllarda yaşanan ulusal çaplı siber güvenlik olaylarının incelenmesi, gelecekte karşılaşılabileceğimiz tehditleri tahayyül edebilmek açısından fayda sağlayacaktır.

3.3. Siber Güvenlik Olayları

Güvenlik ihlallerine sebebiyet veren siber saldırıların birçok sebebi bulunmaktadır. Siyasî talepleri dayatmak, veri çalmak, verilerin içeriğini değiştirmek, hasmın hizmet verme kapasitesine zarar vermek, ekonomik olarak baskı kurmak, propaganda yapmak hatta sadece eğlenmek gibi sebepler bunların başında gelmektedir. Saldırıların düzenlenmesinde kullanılan yöntemler çok çeşitli olmakla beraber güvenlik açıklıkları ve kullanıcı personelin zafiyetleri saldıran tarafa üstünlük sağlamaktadır.

Belli başlı saldırı yöntemleri [31]:

- Bilgi ve veri aldatmacası (Data Diddling),
- Salam tekniği (Salami Techniques),
- Süper darbe (Super Zapping),
- Eşzamansız saldırılar (Asynchronous Attacks),
- Truva atı (Casus Yazılımlar),
- Zararlı yazılımlar (Kötücül Yazılımlar),
- Mantık bombaları (Logic Bombs);
- Oltalama (Phishing),
- Tarama (Scanning),
- Bukalemun (Chamelon),
- İstem dışı alınan elektronik postalar (Spam),
- Çöpe dalma (Scavenging),
- Gizli kapılar (Trap Doors),
- Sırtlama (Piggybacking),
- Yerine geçme (Masquerading),
- Sistem güvenliğinin kırılıp içeri sızılması (Hacking),
- Hukuka aykırı içerik sunulması,
- Web sayfası hırsızlığı ve yönlendirme,
- Sosyal mühendisliktir.

Yakın geçmişte yaşanmış olan önemli siber güvenlik olayları hakkında kısaca bilgiler alt başlıklarda verilmiştir.

3.3.1. Estonya siber saldırıları

Estonya 2007 yılının Nisan ayının sonlarına doğru önceden planlanmış, uyumlu ve haftalar süren siber saldırılara maruz kalmıştır. Bu saldırılarda internet altyapısı, büyük bankalar, devlet kurumları, medya şirketleri ve hatta para çekme makineleri bile hedef alınmıştır. Saldırı, Estonya hükümetinin başkenti Talinn'de bulunan ve Estonyalıları Nazi işgalinden kurtaran Rus askerlerinin hatırası için 1947 yılında dikilen Kızıl Ordu Anıtı'nın kaldırmasından hemen sonra başlamıştır [32].

Heykelin kaldırılması bir takım isyan hareketlerini başlatmış, yüzlerce kişinin yaralanmasına sebebiyet vermiştir. Estonya Savunma Bakanı Aaviksoo, bu saldırıların botnetler[1] vasıtasıyla yapılan ne ilk ne de en büyük saldırı olduğunu, ancak Estonya Cumhuriyeti'nin temel elektronik altyapısının tamamına yakınını hedef alan bir saldırı olduğunu beyan etmiş, ayrıca tüm halkın etkilendiği ve ulusal güvenliğin tehdit edildiği ilk botnet saldırısı olduğunu belirtmiştir [33, 35].

Estonya, e-devleti en etkin kullanan devletlerden biridir. Tüm bankacılık hizmetleri ve devlet internet üzerinden yürütülmekte, hatta parlamento seçimleri internet aracılığıyla yapılmaktadır. Estonyalı yetkililer dağıtık servis dışı bırakma saldırıları[2] (Distributed Denial of Service, DDoS) için Rusya'yı suçlasa da, Rus Hükümeti olayla ilgilerinin olmadığını dile getirmiştir [34, 35].

3.3.2. Stuxnet

Stuxnet adlı bir solucanın[3] Haziran 2010'da, İran'ın nükleer tesislerine sızıp etki yaptığı, nükleer çalışmaları sekteye uğrattığı rapor edilmiştir. Bu solucan, özellikle Siemens üretimi uzaktan kumanda sistemlerini etki etmektedir. Stuxnet solucanı, siber saldırıların etkileri açısından en önemli olaylardan biridir. Veri Tabanlı Kontrol ve Gözetleme Sistemi (Supervisory Control and Data Acquisition, SCADA) olarak adlandırılan endüstriyel sistemleri hedef almıştır [11, 35].

Stuxnet kendi kodunu programlanabilir mantıksal denetleyiciye (Programmable Logic Controller, PLC) aktararak, özellikle SCADA sistemlerinin izlendiği endüstriyel sistemlerden faydalanma mantığı üzerine kurulmuştur. Ayrıca, PLC üzerindeki kodları inceleyen programcının görmesine imkân vermeden kod blokları arasında saklanabilmektedir. Bu kodu PLC'ye entegre ettikten sonra, Stuxnet potansiyel olarak sistemi kontrol etmekte ve çalışma şeklini değiştirebilmektedir [36].

---

[1] Bot: Köken olarak Robottan gelen, saldırganların kendi amaçları doğrultusunda kontrol ettiği sistem. Botnet: Birçok bot'un bir arada hareket edip saldırı yapması.

[2] DDoS: İnternet üzerinden ele geçirilmiş olan sistemler ile saldırı yapılacak sistem veya servislerin aşırı yüklenme sebebiyle kullanıcılara hizmet vermesini engellemek ya da yavaşlatmaktır.

[3] Solucan: Virüsler gibi zararlı yazılımlardır ve virüslerin alt kümesi olarak adlandırılır. Virüs gibi bir programın çalışması sayesinde sisteme bulaşırken hiçbir şekilde müdahaleye gerek duymadan da çalışabilir ve bu solucanı virüsten çok tehlikeli hale getirir. Genellikle sistem açıklıklarını kullanarak bulaşır, hafızayı kullanabilir ve kendini çoğaltabilir.

Uzmanlara göre, Stuxnet diğer zararlı yazılımlara kıyasla çok karmaşık ve çok pahalı bir üretim süreci sonucunda üretilmiştir. Symantec firması programdaki kodlama stillerinin program yazan kişilerde farklılık gösterdiği, bir nevi parmak izi görevi gördüğü düşünüldüğünde, en az otuz farklı kişinin katkıda bulunduğunu iddia etmektedir. Başka bir uzmanın görüşü ise bu solucanın yazılması en az altı aylık süre zarfında gerçekleştirilmiş olduğudur [37].

İran'ın yüksek güvenlikli korunan nükleer tesisinde tespit edilen bu zararlı yazılım; çok sayıda santrifüjün arızalanmasına sebebiyet vermiş, solucanın tespitinden önce 9000 civarında olan sayısının 3700'lere düştüğü iddia edilmiştir. Parçalanan makinelerin yenilenmesi ve kalan makinelerin zararlı yazılımlardan temizlenmesi ve yeniden yüklemelerin yapılması, çalışmaları oldukça aksatmıştır. Stuxnet virüsünün, İran'ın nükleer çalışmalarını iki yıl geriye götürdüğü bilinmektedir. Dünya genelinde virüsün %60'ı aşan bir oranda İran'ı etkilemesi ise bu solucanın özellikle nükleer tesisleri kontrol altına almak ve çökertmek için geliştirildiği düşüncesini arttırmıştır [38].

3.3.3. Duqu

Windows işletim sisteminin açıklıklarını kullanarak bulaşan trojan[1], saldırılan kapıda (portta) arka kapı açarak bilgilerin çalınmasına imkân sağlamaktadır [39]. Çalışma prensibi olarak Stuxnet'e benzemektedir, ancak zarar vermek yerine bilgi toplamak amacıyla yazılmıştır. Verdiği zarar göz önüne alındığında Stuxnet kadar tehlikeli olmayan bu zararlı yazılım, hedefleri açısından değerlendirildiğinde Stuxnet'ten çok daha büyük tehdit içermektedir. Stuxnet ile büyük benzerlikler içeren Duqu'nun hedefi Stuxnet de olduğu gibi sistemlere zarar vermek değil, endüstriyel kontrol sistemleri hakkında bilgi toplamak ve benzerlerinin oluşturulması için keşif çalışması yapmaktır [35, 39].

[1] Trojan (Truva Atı): Mitolojideki Truva atı misali armağan görünümlü olup, çalıştığı sistemde önemli verilere ulaşıp, bunları dışarıya gönderen casus yazılımlardır. Sistemde çalıştırıldıktan sonra arka planda çalışarak bilgi toplamaya başlar.

3.3.4. Conficker

Conficker (Downup, Downadup ve Kido olarak da adlandırılmaktadır) dünya çapında milyonlarca bilgisayara bulaşarak, 2003 yılında Welchia adı verilen bilgisayar solucanından sonra, gelmiş geçmiş en çok bilgisayara bulaşan solucan olarak tarihteki yerini almıştır [11]. Dünya çapında 10 milyon bilgisayardan fazlasına bulaştığı tahmin edilmektedir. Windows işletim sistemindeki güncelleştirmeler, güvenlik merkezi, hata raporlama gibi önemli servislerini ve hatta güvenlik yazılımlarını devre dışı bırakmakta, bilgisayarların güvenlik yazılımları indirebileceği sitelere erişimlerini engellemektedir [40].

Çevrim içi olan Windows işletim sistemine sahip bilgisayarların %30'unu etkileme potansiyeline sahiptir ve bu yaklaşık 300-350 milyon kişisel bilgisayara tekabül etmektedir. Kaynağı Ukrayna olan solucan, dosyaları yok etme gibi bir amaca sahip değildir, fakat uzmanlar gelecekte daha büyük zararlar vermesinden endişelenmektedir [41]. Kendini güncelleme yeteneğine sahip olan Conficker solucanı, etkilediği diğer bilgisayarlarla iletişimini sürdürmekte ve kendine has bir ağ kurmaktadır [42].

3.3.5. Flame

Kriptoloji ve sistem güvenlik laboratuvarı olan CrySyS bu zararlı yazılımı tespit ettiği zaman en az beş yıldır aktif olduğunu, özellikle beş farklı şifreleme, üç farklı sıkıştırma, en az beş farklı dosyalama formatı ve özel kod enjeksiyon teknikleri kullandığını belirtmiştir. Flame bilgi çalmak ve üretmek üzere çok gelişmiş fonksiyonlara sahip olmakla beraber, amaçlarına ulaşmak için bulaştığı bilgisayarın tüm kapasitesini kullanmaktadır. İstihbarat sağlamak için klavye, ekran, mikrofon, depolama cihazları, ağ cihazları gibi tüm olasılıkları değerlendirmektedir. Firma tarafından yapılan analizler çerçevesinde çok önemli ölçüde bütçe ve çaba harcanarak, siber savaş faaliyetlerinde kullanılmak üzere bir devlet veya devlet kurumu tarafından yazılmış olabileceği kanısına varılmıştır [43]. Rusya'nın ünlü antivirüs şirketi Kaspersky, Flame virüsünün şimdiye kadar bilinen tüm sanal tehditlerden çok daha tehlikeli ve karmaşık olduğunu belirtmektedir.

Söz konusu virüs, internet bağlantısını kullanarak bilgisayarların ara birimlerini kullanıcının haberi olmadan çalıştırabilmektedir. Uzaktan kumanda edilebilen virüs, daha sonra mikrofonu açarak sesleri kaydedebilmektedir. Topladığı tüm bu verileri de yine internet ağı üzerinden kaynağına geri göndermekte ve ne kadar bilgi topladığı da daha sonra denetlenememektedir [44].

Stuxnet'e göre 20 kat daha karışık bir mimariye sahip olan ve yapılan incelemeler sonucu başta İran, İsrail, Sudan, Suriye, Lübnan, Suudi Arabistan ve Mısır olmak üzere 600'den fazla kuruluş, akademik kurum ve devlet sistemi Flame ile hedef alınmıştır [45]. Ağ trafiğini kaydetmek, mikrofondan ses kaydı yapmak, ekran görüntüsü kaydetmek belki zararlı yazılımlar için sıradan özelliklerdir. Fakat bunların hepsini aynı anda yapmak, bu özelliklerin yanında ortamdaki Bluetooth aygıtları taramak ve bunlar hakkında bilgi toplamak, bu zararlı yazılımı siber istihbarat için kullanılan bir İsviçre çakısına dönüştürmektedir. Kullanıcı Skype, Siphone gibi bir VoIP uygulaması ile konuşmaya başladığında, bu konuşmayı sıkıştırıp kendi veri tabanı üzerine kaydedebilmektedir. Ayrıca anlık mesajlaşma uygulamaları açıldığı zaman Flame devreye girip ekran görüntüsü alarak görüşmeyi yine SQLite veri tabanına sıkıştırılmış olarak kaydetmekte ve kaydettiği bu verileri belirli aralıklarla göndermektedir [46].

3.3.6. Sony

Dünyaca ünlü Sony Pictures Entertainment yapım stüdyosu, senaryosunda Kuzey Kore lideri Kim Jong Un'a karşı suikast düzenlendiği "Röportaj" isimli komedi filmi sebebiyle siber saldırılara uğramıştır. 2011 yılında Sony'nin bir PS3'ün sistemini kıran hackera dava açması sonucu ardı ardına Anonymous dâhil olmak üzere birçok hactivist grubun hedefi haline gelmiştir. Bu eylemler sonucunda PlayStation ağındaki 11 milyon kayıtlı kullanıcının kişisel bilgileri ele geçirilmiş ve Sony'nin yaptığı açıklamaya göre saldırılar yılsonundaki maliyeti 171 milyon doları bulmuştur [47]. Saldırıların Kuzey Kore kaynaklı olduğu Amerikalı yetkililer tarafından dile getirilmekte ve Sony firmasına yaklaşık 100 milyon dolar civarında zarar verdiği tahmin edilmektedir [48, 49].

Bu saldırının sonucunda firmadan çalınan bilgiler, gösterime girmeden ele geçirilen filmler gibi maddi konulardan ziyade, ifade özgürlüğünün ihlal edilmesi hususu dikkat çekmektedir. Amerika'nın önde gelen bilgisayar güvenlik firması Fusion X LLC'nin yöneticisi Matt Devost; "Bu olay yeni bir çağın başlangıcıdır. Artık sadece para veya entelektüel varlıkların hırsızlığı için değil, aynı zamanda olabildiğince yıkıcı etki sağlayacak ve davranışlarınızı değiştirecek saldırılar için de endişelenmek zorundasınız [50]" sözleriyle olayın önemini vurgulamıştır. Amerika Başkanı Barack Obama ise, "Bazı diktatörlerin ABD'de sansür uygulamaya başladığı bir toplum haline gelemeyiz. Birilerinin hicivli bir filmin yayınlanması noktasında insanları korkutmasına izin verilirse, hoşlanmadıkları bir belgesel veya haber gördüklerinde ne yapmaya başlayacaklarını hayal edin" sözleriyle orantılı yanıt vereceklerini söylemiştir [51].

3.3.7. Diğer önemli güvenlik ihlalleri

Amerika Birleşik Devletlerinde geçmiş senelerde onlarca siber güvenlik olayı meydana gelmiştir. Küresel bazda ses getiren olaylardan bazıları şunlardır [15]:

- Fortune 500 firmalarından biri olan Walmart'ın bilgisayar sistemlerine 2009 yılında sızılmasıyla, yazarkasalardan bilgi hırsızlığı meydana gelmiştir.
- 2013 yılında Target firmasından 110 milyon müşterinin kişisel bilgileri çalınmış ve daha sonra meydana gelen siber saldırılarla beraber 148 milyon dolarlık zarar meydana gelmiştir.
- McAfee firmasının yaptığı araştırmaya göre 2013 yılında siber saldırıların ABD ekonomisine verdiği zarar 154 milyar dolar civarındadır.
- 2014 yılında Home Depot firmasından 60 milyon kredi kartı numarası çalınmıştır.
- 2014 yılında Apple firmasının iCloud hesaplarına sızılarak çoğunluğu dünyaca ünlü film yıldızları olmak üzere kişisel bilgiler ve resimler çalınmış, internette ifşa edilmiştir. Bu olay, firmanın piyasaya süreceği telefon modelinin birkaç hafta gecikmesine sebep olmuştur.
- Cryptolocker virüsü ile etkilenen 234 000 bilgisayar sadece ilk iki ayında 27 milyon dolar zarara uğramıştır.

- 2014 yılında Micheal's şirketinden 2,6 milyon maaş kartı bilgisi, Community Health Systems'den 4,5 milyon hasta bilgisi, ABD Posta Servisinden 905 000 kişisel bilgi, JP Morgan Chase şirketinden 76 milyon hane halkı bilgisi ve 7 milyon özel sektöre ait finansal bilgi, Staples firmasından 1,2 milyon kredi kartı bilgisi çalınmıştır.
- Ponemon Enstitüsünün 2013 yılında temsili olarak alınan 60 firma üzerinde yaptığı araştırma sonucu siber saldırıların firmalara ortalama 11 milyon dolar zarara sebebiyet verdiği, her bir saldırının 1,3 milyon dolar ile 58 milyon dolar arasında maddi kayba yol açtığı ve bir önceki yıl yaptığı araştırmaya nazaran %26 artış gösterdiği saptanmıştır.

İngiltere'de meydana gelen siber güvenlik olayları [15]:

- Kabine Ofisi tarafından 2011 yılında Detica firmasına yaptırılan araştırma sonucuna göre siber saldırıların İngiltere ekonomisine maliyeti yıllık 27 milyar sterlini bulmaktadır.
- Ponemon Enstitüsünün 2013 yılında temsili olarak alınan 36 firma üzerinde yaptığı araştırma sonucunda siber saldırıların firmalara ortalama 3 milyon sterlin zarara sebebiyet verdiği, her bir saldırının 370 000 sterlin ile 17 milyon sterlin arasında maddi kayba yol açtığı ve bir önceki yıl yaptığı araştırmaya nazaran %36 artış gösterdiği saptanmıştır.

4. STRATEJİ VE STRATEJİ HAZIRLAMA YÖNTEMLERİ

Tez çalışmasının bu bölümünde strateji ve stratejik planlamanın yönetim bilimi açısından öneminin anlaşılabilmesi için gerekli kavramlar açıklanmış ve Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planını kritik edebilmek için, iki kamu kurumunun stratejik planları (TBMM İdari Teşkilatı ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı) *kapsam* açısından incelenmiştir.

Bu karşılaştırma için, tüm ulusun TBMM'nin çalışmaları ile ilgili olarak Başbakanlık ve diğer kamu kurum ve kuruluşlarıyla eşgüdümü sağlamakla görevli olduğundan dolayı, TBMM İdari Teşkilatı stratejik planı seçilmiştir. UDHB Stratejik Planının seçilme sebebi ise; siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak, bunların uygulanmasını, koordinasyonunu sağlamak görevinin söz konusu bakanlığa verilmesidir.

4.1. Strateji, Stratejik Planlama ve Stratejik Yönetim

Literatürde stratejinin kelime kökeni bakımından iki kaynağa dayandığı; bunlardan birinin, Latince yol, çizgi veya yatak anlamına gelen 'stratum' kavramıyla, ikincisinin ise, eski Yunanlı General Strategos'un, sanatını ve bilgisini belirtmek için, adıyla ilgili olduğu ifade edilmektedir [52]. Türk Dil Kurumu Sözlüğünde ise "bir ulusun veya uluslar topluluğunun, barış ve savaşta benimsenen politikalara destek vermek amacıyla politik, ekonomik, psikolojik ve askerî güçleri bir arada kullanma bilimi ve sanatı" olarak tanımlanmıştır [53].

Yönetim biliminde strateji, "bir organizasyonun amacına ulaşmak için izleyeceği yollar" anlamında kullanılmaktadır. Özellikle firmaların ya da şirketlerin rakiplerine karşı izleyeceği stratejiler, önce Stratejik Planlama ve daha sonra Stratejik Yönetim adı verilen disiplinin doğmasına neden olmuştur. Günümüzde Stratejik Yönetim, yönetim biliminde çok önemli araştırma alanlarından birini oluşturmaktadır [54].

Strateji bilimsel bir disiplin olarak gelişmesini, askeri alanda taşıdığı öneme borçludur. Savunma ve hücum yönünden askeri amaçları etkin ve verimli olarak gerçekleştirebilme tarih boyunca orduların stratejik gücünün göstergesi olmuştur [52]. Stratejik planlama organizasyonların işini en iyi şekilde yapmasını sağlayan, çalışanlarının işlerini uyum içerisinde yürütmesine imkân veren, yöneticilere uzun vadeli düşünme ve ufku görme fırsatını yaratan bir süreçtir.

Stratejik planlama herhangi bir uygulama ya da yürütme faaliyetine geçilmeden önceki durumu ortaya koymaktır. Uzun dönem planlama yapmanın başarısı, yapılan planların titiz ve her evresinde kontrollü bir biçimde yürürlüğe konmasına bağlıdır.

Stratejik yönetim, bir organizasyonda geleceğe yönelik kararlar alınmasında kullanılan bir yönetim tekniğidir. Stratejik yönetim üç kısımda incelenebilir. 1) Strateji üretme 2) Strateji uygulama 3) Stratejik öğrenme [55]. Bu tez çalışmasında, Türkiye'nin Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın içerik bakımından inceleneceği göz önünde bulundurulduğunda ikinci ve üçüncü kısımlar değerlendirilmeyecektir.

Stratejik yönetimin amacı organizasyonun gelecekteki performansının artırılması, kârlılık ve verimliliğin yükseltilmesidir. Stratejik yönetim geleceğe yönelik vizyon oluşturulmasını amaçlar. Organizasyonda vizyonun belirlenmesinden sonra, bu vizyona ulaşmak için misyon belirlenir. Organizasyonda vizyon ve misyonun tüm çalışanlar tarafından benimsenmesi ve ortak değerler (temel ilkeler) olarak kabul edilmesi büyük önem taşımaktadır. Vizyon ve misyon belirlenmesi organizasyonel başarı için yeterli değildir. Amaca ulaşmak için ayrıca stratejiler ve eylem planları oluşturulmalıdır [54].

Stratejik planlama yapmak 10 Aralık 2013 tarihli ve 25326 sayılı Resmi Gazetede 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu ile yasal yükümlülük haline gelmiştir. Bu kanunla; kalkınma planları ve programlarda yer alan politika ve hedefler doğrultusunda kamu kaynaklarının etkili, ekonomik ve verimli bir şekilde elde edilmesi ve kullanılmasını, hesap verebilirliği ve malî saydamlığı sağlamak üzere, kamu malî yönetiminin yapısını ve işleyişini, kamu bütçelerinin hazırlanmasını, uygulanmasını, tüm malî işlemlerin muhasebeleştirilmesini, raporlanmasını ve malî kontrolü düzenlemek amaçlanmaktadır.

Aynı kanunun 9'uncu maddesinde "Kamu idareleri; kalkınma planları, programlar, ilgili mevzuat ve benimsedikleri temel ilkeler çerçevesinde geleceğe ilişkin misyon ve vizyonlarını oluşturmak, stratejik amaçlar ve ölçülebilir hedefler saptamak, performanslarını önceden belirlenmiş olan göstergeler doğrultusunda ölçmek ve bu sürecin izleme ve değerlendirmesini yapmak amacıyla katılımcı yöntemlerle stratejik plan hazırlarlar" hükmü bulunmaktadır.

4.2. Stratejik Yönetim Süreci

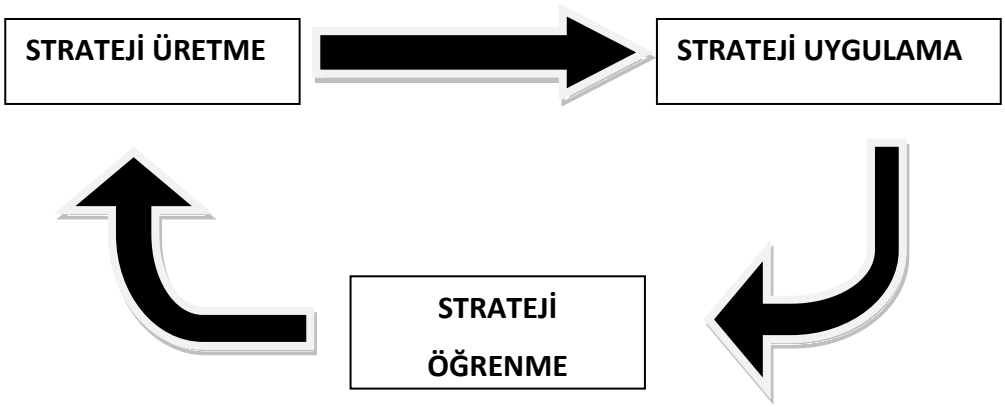
Stratejik yönetim üç kısımda incelenebilir.

1) Örgütün uzun dönemli başarısını belirleyecek karar ve planlarının yapılması, diğer bir ifadeyle stratejik planın oluşturulması: Bu aşamada üst yönetim tarafından organizasyonda iç ve dış yönetime yönelik SWOT analizi yapılır. Organizasyonun vizyon ve misyon bildirileri hazırlanarak organizasyonda amaç, ilke ve değerler ortaya konur. Stratejik planlamada en önemli konu, stratejik kararların alınması ve strateji seçimlerinin yapılmasıdır.

2) Stratejinin yürürlüğe konulması için organizasyon, program, bütçe faaliyet süreçlerinin yapılıp uygulanması: Üst yönetimin sorumluluğunda ve özellikle orta kademe yöneticiler ile işbirliği yapılarak stratejilerin uygulamasına geçilir. Bu aşamada daha önce belirlenen strateji ve eylem planlarının uygulaması yapılır.

3) Başarı için amaçlar ve misyonlarda belirtilen sonuçlara ulaşılıp ulaşılmadığını her evrede sürekli olarak kontrol etme ve düzeltici önlemler alma: Yapılan uygulamaların sonuçları gözden geçirilerek stratejik planlamada gerekirse değişiklikler yapılabilir [52, 54]. Uygulamalar sırasında üretilen bilgilerin ve kazanılan deneyimlerin yeni stratejilerin oluşturulması için kullanılması aşaması olarak değerlendirilen bu adım stratejik öğrenme olarak da değerlendirilebilir.

Bu aşamalar Şekil 4.1'deki gibi her daim bir döngü içerisindedir [55].



Şekil 4.1. Stratejik yönetim süreci

4.3. Vizyon, Misyon ve Temel İlkeler

Vizyon, misyon ve temel ilkeler bir kurumun kurumsal kimliğini oluşturan öğelerdir. Stratejik planlamanın işlevlerinden biri de kurumsal kimlik ile sunulan hizmetler arasında güçlü bir ilişki kurmaktır. Vizyon, misyon ve temel ilkelerin oluşturulması sonucunda, işletmenin varılması istenen noktaya nasıl bir çerçeve içerisinde ulaşacağı, stratejik amaç ve hedeflerin belirlenmesi ile ortaya çıkar. Bu nedenle, vizyon, misyon ve temel ilkelerin doğru şekilde ifade edilmesi stratejik planın başarısı üzerinde belirleyici bir rol oynayacaktır [56].

4.3.1. Vizyon

Vizyon bir kurumun ulaşmayı arzu ettiği geleceğin iddialı ve gerçekçi bir ifadesidir. Kurumun farklı birimleri arasında birleştirici bir unsur olan vizyon, uzun vadede o kurumun neler yapmak istediğinin güçlü bir anlatımıdır.

Vizyon [56];

- Bugünden farklı ve iyi olabilecek bir gelecek tasvir eder.
- Başarılabileceği konusunda insanlara umut verir.
- İlham vericidir ve amaca ulaşmak için kişiyi heveslendirir.
- Organizasyon içerisindeki kişilere birtakım hedefler olarak bildirilmelidir.
- Uygun bir şekilde biçimlendirilmelidir.
- Arıtılmış olmalıdır.
- Erişilebilir olmalıdır.
- Hedeflerin tanımlanmasına yardımcı olmalıdır.
- Stratejinin geliştirilmesine kılavuzluk etmelidir.
- İletişim aracıdır.
- Kısa, tutarlı ve odaklanmış ancak esnek olmalıdır.

Başlıca görevi Genel Kurula, Başkanlık Divanına, komisyonlara, siyasi parti gruplarına ve milletvekillerine her türlü bilgi desteği ile İdari ve teknik destek sağlamak olan TBMM İdari Teşkilatı[1]; 2013-2017 Stratejik Planı'nda TBMM İdari Teşkilatının vizyonunu; "Katılımcı demokrasi ideali doğrultusunda yasama sürecini kusursuz bir işleyişe kavuşturmak amacıyla, iyi yönetişim ilkelerini esas alan, sunduğu hizmetlerle değişime ve dönüşüme öncülük eden ve örnek alınan bir İdari Teşkilat olmak" [57] olarak ifade etmiştir. Ulusal siber güvenliğin sağlanmasına ilişkin politika, strateji ve eylem planları hazırlama görevinin ihdas edildiği [10] Ulaştırma, Denizcilik ve Haberleşme Bakanlığının 2014-2018 Stratejik Planındaki vizyonu; "Güvenle ulaştıran, hızla eriştiren, sevilen, şeffaf, başarı örneği olarak gösterilen bir kurum olmak" şeklinde belirtilmiştir [58].

İki kurumun hazırlamış oldukları stratejik planlardaki vizyonlar incelendiğinde, hedeflerin erişilebilir ve gerçekçi, hedeflerin tanımlanmasına yardımcı olabilecek, ilham verici, esnek ve tutarlı olarak belirlendiği gözlemlenmektedir. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında arzu edilen geleceğe dair vizyon bulunmamaktadır.

[1] 18 Ocak 2011 tarihli ve 28146 sayılı Resmi Gazetede yayımlanan 6253 sayılı Türkiye Büyük Millet Meclisi Başkanlığı İdari Teşkilatı Kanunu md.3.

4.3.2. Misyon

Misyon bir kurumun varlık sebebidir; ne yaptığını, nasıl yaptığını ve kimin için yaptığını açıkça ifade eder. Misyon, stratejik planlamaya temel oluşturur. Misyon [56];

- Vizyonu düzenlemelidir.
- Girişimin analizini desteklemelidir.
- Kurumun faaliyet alanını tanımlamalıdır.
- Amaçların saptanmasına rehberlik etmelidir.
- Stratejik alternatiflere rehberlik etmelidir.
- İletişim aracı olmalıdır.
- Değişim zamanlarında sabit bir referans noktası olmalıdır.
- Zaman boyutu içermez.
- Kısa, açık ve çarpıcı şekilde ifade edilir.

Yine aynı kurumların stratejik planları incelendiğinde, TBMM İdari Teşkilatının misyonu "TBMM'nin yasama sürecinde ihtiyaç duyduğu Bilgi, Yasama Süreci ve Tekniği, Erişim ve Katılım, Tanıtım, Destek hizmetlerini etkin biçimde sunmak" olarak ifade edilmiştir [57]. UDHB'nin ise; "Toplumun yaşam kalitesinin yükseltilmesine ve ülke kalkınmasına katkı sağlamak amacıyla; ulaştırma, denizcilik, haberleşme, uzay ve bilgi teknolojileri alanlarında dengeli, güvenli, ekonomik, erişilebilir, ekolojik yapıyı gözeten, sürdürülebilir, kaliteli hizmet verilmesini sağlamak ve denetlemek" olarak belirlenmiştir [58].

İki kurumun hazırlamış oldukları stratejik planlardaki misyonlar incelendiğinde, vizyonu düzenleyen, amaçların saptanmasına rehberlik eden, zaman boyutu içermeyen, kısa ve açık olduğu görülmektedir. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının varlık sebebine dair misyon bulunmamaktadır.

4.3.3. Temel ilkeler

Temel ilkeler, kurumun temel değerlerinin bir ifadesidir. Kurum değerlerini, yönetim biçimini ve davranış kurallarını ifade eder. Şeffaflık, eşitlik, katılımcılık, ahlaki değerler ve kalite anlayışı temel ilkelere örnek olarak verilebilir.

Bir kurumun temel ilkelerini ortaya koymak stratejik planlama için önemlidir çünkü ilkeler; kurumun vizyonu ve misyonunun gerisinde yatan değer ve inançların temelidir. Bu ilkeler kurumun kararlarına, seçimlerine ve stratejilerin belirlenmesine rehberlik eder. Hayata geçirilen ilkeler, kurum kimliğinin değişiminde ve çalışanların motive edilmesinde güçlü araçlardır. Temel ilkeler;

- Temel değerleri ve inançları açık ve kesin bir dille ortaya koymalıdır.
- Çalışanların işlerini en iyi şekilde yapacaklara şartlara ilişkin temel düşünceyi belirtmelidir.
- Kurumun vizyonunu gerçekleştirmeyi sağlayacak sistem ve süreçleri desteklemelidir [56].

Çizelge 4.1'de TBMM İdari Teşkilatının, Çizelge 4.2'de Ulaştırma, Denizcilik ve Haberleşme Bakanlığının vizyonlarını gerçekleştirmeyi sağlayacak sistem ve süreçleri destekleyen temel ilkeleri gösterilmiştir.

Çizelge 4.1. TBMM İdari Teşkilatı temel ilkeleri.

<table>
<tr><th colspan="3">Çalışma İlkelerimiz ve Değerlerimiz</th></tr>
<tr><th>TBMM</th><th>İdari Teşkilat</th><th>Toplum</th></tr>
<tr><td><u>Tarafsızlık</u>

Paydaşlarımıza hizmet sunumumuzda adaletli ve tarafsız davranma.</td><td><u>Mükemmellik arayışı</u>

Mevcut düzeyimizi yeterli görmeyip öğrenen kurum yaklaşımı ile hizmet kalitemizi sürekli geliştirerek mükemmellik arayışı içerisinde olma.</td><td><u>Güvenilirlik</u>

Sunduğumuz hizmetlerin kalitesinin, etik kurallara uygunluğunun ve kişiye özel bilgilerin gizliliğinin korunmasındaki özenimizin paydaşlarımız gözünde bize kazandırdığı güvenilirliği koruma ve geliştirme.</td></tr>
<tr><td><u>Hizmet sunumunda yasama odaklılık</u>

Yasama sürecinin ihtiyaçlarına cevap verecek yasama odaklı hizmet sunumunu esas alma.</td><td rowspan="2"><u>Kurumsal kalite ve iyi yönetişim ilkeleri</u>

• Hesap verebilirlik
• Şeffaflık
• Etkinlik ve verimlilik
• Katılımcılık
• Politikalar arasında uyum ve bütünlük
• Çözüm odaklılık
• Planlılık
• Kurumlararası işbirliğini önemsemek
• Kurum olarak örnek olmak
• Tarihi ve kültürel değerleri korumak ilkelerini gözetme ve uygulama.</td><td><u>Demokrasinin gelişmesine katkı bilinciyle hareket etme</u>

Demokratik toplum ideali çerçevesinde hizmet sunumumuzda demokrasinin gelişmesine katkı bilinciyle hareket etme.</td></tr>
<tr><td><u>Kurumsal saygınlık</u>

Yaptığımız işlerin TBMM'nin itibarıyla doğrudan ilişkili olduğunun farkında olarak hizmet sunumunda kurumsal saygınlığı gözetme.</td><td><u>Toplumsal sorumluluk</u>

Yasama organının üstlendiği toplumsal sorumluluk çerçevesinde hizmet üretme ve sunumunda gerekli özeni gösterme.</td></tr>
</table>

Çizelge 4.2. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı temel ilkeleri

TEMEL İLKE VE DEĞERLER	
Bilimsellik	Karar alma süreçlerinde bilimsel metotlar kullanır
Çalışan Odaklılık	Çalışanların kurumsal aidiyeti ve memnuniyetini artırmaya çalışır ve yönetime katılımlarını teşvik eder
Dengeli	Ulaştırma türleri ve bölgeler arası dengeyi gözetir
Etik Değerlere Uygunluk	Mesleki değer ve kurallara bağlıdır
Güvenilirlik	Tüm iş ve işlemlerde tutarlı davranır
Katılımcılık	Paydaşların eleştiri, görüş ve önerilerine açıktır, ortak aklı kullanır
Öncü ve Yönlendirici	İhtiyaçları öngörerek yönlendirir
Sonuç Odaklılık	Hizmetlerin planlanmasında, toplumda olumlu değişim sağlaması dikkate alınır
Sosyal Sorumluluk Sahibi	Kamu yönetiminin bir emanet olduğu bilinciyle halkın mutluluğu için genel sorumluluğu taşır
Stratejik Bakış	Geleceğe yönelik gelişmeleri belirleyerek gerekli adımları atan stratejik yönetim anlayışına sahiptir
Süreklilik	Yüksek kalitede kesintisiz hizmet sağlar
Şeffaflık	Tüm tarafların erişimine açık ve hesap verebilirlik anlayışı içinde çalışır
Tarafsızlık	Toplumun tüm bireylerine önyargısız, somu, veri ve bilgiye dayanan adli bir yaklaşım sergiler
Çevreye ve Tarihe Duyarlılık	Tüm ulaşım ve iletişim faaliyetlerinde gelecek nesillerin ihtiyaçlarını dikkate alır ve gözetir
Vatandaş Odaklılık	Vatandaşlar için değer yaratır, vatandaşların isteki, beklenti ve ihtiyaçlarının ne olduğunun bilincindedir ve bu yönde hareket eder
Verimlilik	Kaynakları yerinde, doğru zamanda, etkin olarak kullanır
Yenilikçi ve Gelişimci	Her türlü yeniliğe ve gelişime açıktır, gelişen ve değişen teknolojiyi yakından takip ederek kullanır
Yerli Üretim Odaklı	Yerli üretimi destekler, teşvik eder, kullanımına öncelik verir

Ulusal Siber Güvenlik Stratejisinde göz önünde bulundurulacak ilkeler sıralanmıştır, fakat bu ilkeler kurumun değerlerini, yönetim biçimini ve davranış kurallarını kapsamamaktadır. Yalnızca siber güvenlik sağlanırken dikkat edilecek ilkeler geniş kapsamda listelenmiştir.

4.3.4. SWOT (GZFT) analizi

Stratejik yönetimin en önemli konularından birisi SWOT analizi yapılmasıdır. SWOT analizi organizasyonun iç ve dış çevresinin değerlendirilmesine imkân sağlayan bir analiz tekniğidir. Aşağıdaki İngilizce kelimelerin baş harflerinden oluşturulmuş bir kısaltmadır.

S: Strength/Güçlü Yönler (Organizasyonun güçlü/üstün olduğu yönler)

W: Weakness/Zayıf Yönler (Organizasyonun güçsüz/zayıf olduğu yönler)

O: Opportunity/Fırsatlar (Organizasyonun sahip olduğu fırsatlar)

T: Threat/Tehditler (Organizasyonun karşı karşıya bulunduğu tehdit/tehlikeler)

SWOT analizi, organizasyonun hem kendi iç durum değerlendirmesine, hem de organizasyon dışındaki pazar yapısının, rakiplerin durumunun analiz edilmesine imkân sağlar. Özetle, iç ve dış analizi içeren bir stratejik yönetim tekniğidir [54].

Organizasyonlarda SWOT analizi yapılmasının iki faydası bulunmaktadır. İlk olarak, organizasyonun mevcut durumu tespit edilir. Bu çerçevede, güçlü ve zayıf yönler ile organizasyonun karşı karşıya bulunduğu fırsatlar ve tehdit unsurları ortaya konmaya çalışılır. Bu anlamda SWOT bir "mevcut durum" analizidir, aynı zamanda organizasyonun gelecekteki durumunun ne olacağını tespit ve tahmin etmeye yarayan bir analiz tekniğidir. İkinci anlamda SWOT "gelecek durum" analizidir [54]. Bu açıklamalar çerçevesinde SWOT analizinde durum değerlendirmesine imkân sağlayacak göstergeleri ya da unsurları Çizelge 4.3'deki örnek bir SWOT matrisi üzerinde gösterebiliriz. Çizelge 4.4'de TBMM İdari Teşkilatının, Çizelge 4.5'de Ulaştırma, Denizcilik ve Haberleşme Bakanlığının mevcut ve gelecek durum analizlerinin yapıldığı SWOT matrisleri gösterilmiştir.

TBMM İdari Teşkilatı Stratejik planlama sürecine başlarken ilk olarak mevcut durum analizi yapılmış, bu çerçevede tarihsel gelişim, önceki plandan bugüne gerçekleşmeler, yasal yükümlülükler, paydaş analizleri, kurum içi analiz ve Güçlü/Zayıf Yönler ile Fırsatlar ve Tehditler (GZFT) analizi yapılmıştır.

Çizelge 4.3. Örnek SWOT matrisi

• Pazar payında üstünlük • Yüksek karlılık ve verimlilik • Organizasyonun pazardaki yerinin sağlamlığı • Pazarlama avantajları • Organizasyonun mali yapısının güçlü olması • Üretim teknolojisinin yeni olması • Kuruluş yeri avantajı • Ar-Ge avantajı • Kalifiye işgücü potansiyeli • Marka ünü ve avantajı • Liderlik üstünlüğü • Bilim ve teknoloji üstünlüğü • Stratejik yönetim avantajı • Toplam kalite yönetiminin uygulanıyor olması v.b.	• Kalifiye olmayan işgücü • İnsan kaynaklarındaki yetersizlik • İletişim eksikliği • Bölümler ve kişiler arası çatışma • Ar-Ge dezavantajı • Etkin olmayan yönetim • Bilim ve teknolojide dezavantaj • Marka dezavantajı • Kötü organizasyon imajı • Personelde sık değişikliklerin yapılması v.b
• Yeni ürünlerin geliştirilebilmesi • Yeri satış ve pazarlama tekniklerine sahip olma • Düşük maliyet avantajı • Yeni Pazar fırsatları • İşgücü verimliliğinin yüksek olması • Organizasyon imajının iyi olması • Pazar büyüme oranının sürekli olarak artması • Rakiplerin azalması • Kaliteli ürünlere sahip olması v.s.	• İç pazarda rekabetin artması • Dış pazarlarda rekabetin artması • Misten isteklerinde hızlı değişim • Ağır vergi yükü • İşgücü maliyetinde artış • Girdi fiyatlarının artması • Pazardaki büyüme oranının azalması • İkame ürünlerin artması • Rakiplerin gücünün artması • Misten tercihlerinin değişmesi • Paranın değer kaybı ve enflasyon v.s.

S W
O T

Yapılan değerlendirmelerde, İdari Teşkilatın sunduğu hizmetler tüm yönleri ile ele alınmış, geleceğe yönelik amaç ve hedef geliştirebilmesi için hangi potansiyele sahip olduğu, hangi yönlerde eksikliği bulunduğu ve hizmet alanlarını etkileyebilecek olumlu ya da olumsuz gelişmelerin neler olduğu değerlendirilmiştir. Tüm bu çalışmalar sonucunda amaç ve hedeflerin gerçekçi bir şekilde belirlenmesine çalışılmıştır [57].

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında mevcut durum ve gelecekteki durumu kapsayan SWOT Analizi bulunmamaktadır.

Çizelge 4.4. TBMM İdari Teşkilatının SWOT matrisi

GZFT Analizi	
Güçlü Yönler • Parlamentoyu destekleme alanındaki deneyimimiz, bilgi donanımımız, kurumsal hafızamız • Politik karar alma süreçlerine yakın olmanın kazandırdığı hızlı karar alabilme yeteneği • Kaynak temininde sorun yaşanmaması • Öğrenek gelişme ve değişmenin kurumsallaştırılması	Zayıf Yönler • İnsan kaynakları uygulamalarının halen geçiş aşamasında olması • Uzmanlaşmanın her düzeyde kurumsallaşmamış olması • Kurumda bilişim okur-yazarlığının yüksek düzeyde olmaması • Milletvekili ile çalışan personelin kuruma intibakının yetersiz olması • Kurumsal kültür ve aidiyet duygusunun güçlü olmaması
Fırsatlar • Artan bilgi ve araştırma talebi • Kamu yönetiminde yeni yaklaşımlar • Yasam sürecine sivil toplum ilgisinin ve katılım talebinin giderek artıyor olması • Hizmetlerde kullanılabilecek teknolojik imkânların artması • Dünya parlamentolarında yasama faaliyetlerinin ağırlığının genel kuruldan komisyonlara doğru bir kayma eğilimi göstermesi	Tehditler • İdari Teşkilatın konumunun siyasal etkiye çok açık olması • Kampüs içinde insan yoğunluğunun fazla olması • Yasam gündeminin belirsizliğinin İdari Teşkilatın sunduğu hizmetlere ilişkin planlamayı güçleştirmesi

4.3.5. Stratejik eksenler/hedefler ve amaçlar

Stratejik planda yer alan ve kurumun ulaşmayı hedeflediği sonuçların kavramsal ifadesidir. Amaçlar bir bütün olarak kurumun stratejik yönünü belirler. Kurumun vizyon ve misyonuna yönelik program ve uygulamaların başarılı olmasına katkıda bulunmalıdır.
Stratejik amaçlar;

- Öncelikli hedefleri ve kurum içi ve dışı değerlendirme sonuçlarını ifade etmeli ve stratejik sorulara yanıt verebilmelidir.
- Amaçlar değişmez gibi dursa da ortaya konuldukları koşullar değiştiğinde, stratejik sorunlar doğduğunda değiştirilebilir.
- En azından üç yıllık bir süreyi kapsarlar. Eğer kurumsal bir amaç üç yıldan öne başarıldıysa o bir hedef olabilir.
- Hizmetlerin mevcut haliyle olması gereken hali arasındaki açıklığı ortaya koyar.
- Kurum için açık bir yön belirler. Ancak spesifik strateji ya da aşamaları ifade etmez; bunu hedefler ve eylemler yapar.

Çizelge 4.5. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı SWOT matrisi

Güçlü Yönler	Zayıf Yönler
1. Ulaşım ve iletişim alanında politika belirleyici konumda olması. 2. Tüm ulaştırma hizmetlerini düzenleme ve denetleme yetkisinin Bakanlığımızda olması. 3. Kurumlar ve vatandaşlar nezdinde kurumsal saygınlığının yüksek olması. 4. Bakanlığımız tarafından üretilen hizmetlerin toplumun her kesimine hitap etmesi. 5. Bakanlık yönetiminde istikrar ve süreklilik olması. 6. Ulusal ve uluslararası alanda işbirliği ve koordinasyona açık olması. 7. Kamu özel sektör işbirliği projelerinde tecrübe sahibi olunması. 8. Kamu yatırımlarının önemli bir bölümünü yönlendiren bakanlık olması. 9. Bütçe dışı mali kaynaklara sahip olunması. 10. İnsan kaynakları açısından çok farklı mesleki profile sahip çalışanların istihdam edilmesi. 11. Elektronik-Haberleşme ile Uzay- Havacılık alanlarında Ar-Ge desteğinin verilmesi.	1. Kurumsallaşmanın tamamlanamamış olması. 2. Bakanlık faaliyetlerinin kamuoyuna etkili duyurulamaması. 3. Bakanlık hizmetlerinin sunumunda yararlanılacak bilişim teknolojilerinin yeterli olmaması. 4. Bakanlıkta yönetişim ve inovasyon konularının yeterince geliştirilememiş olması. 5. Bakanlık çağrı merkezinin ihtiyaca cevap verecek şekilde organize edilememesi. 6. Kurum içi fırsat eşitliğini sağlamaya yönelik liyakat ilkesinin yeterli düzeyde uygulanamıyor olması. 7. 655 sayılı KHK sonucu bazı çalışanların özlük haklarında kayıpların olması. 8. İç kontrol sisteminin bütün unsurlarıyla kurulamamış olması.
Fırsatlar	**Tehditler**
1. Ulaşım, iletişim hizmetlerinin insan yaşamında vazgeçilmez bir ihtiyaç olması. 2. Can ve mal güvenliği, enerji verimliliği, çevresel sorunlara duyarlılık, toplu taşıma, akıllı ulaşım sistemleri, kombine taşımacılık, uzay ve havacılık, erişilebilirlik vb konularda taleplerin her geçen gün artması. 3. Ülkemizin jeopolitik konumunun ulaşım koridorları açısından merkez noktasında olması. 4. Ulaştırma sektöründe serbestleşme eğiliminin artması. 5. Gelişen ekonomik ve sosyal koşullara bağlı olarak kaliteli ulaşım ve iletişim talebinin artması. 6. Dünya ticaretinin büyük oranda denizyoluyla yapılıyor olması. 7. Genç bir nüfusumuzun olması. 8. Ülkemizin ulaştırma, denizcilik ve haberleşme sektörlerinde üretim potansiyeline sahip olması. 9. Teknolojik gelişmelerin ulaştırma faaliyetlerinde denetim ve yönetimi kolaylaştırması. 10. Halkımızın ulaşım ve haberleşmede yeniliklere açık olması ve teknolojik yenilikleri kullanma alışkanlığı olması.	1. İklim değişikliği, deprem, sel gibi doğal felaketlerin mevcut ulaşım ve iletişim altyapılarına zarar verme ihtimali. 2. Ulaştırma ve iletişim alanında hammadde, enerji ve teknoloji açısından dışa bağımlılığımızın devam etmesi. 3. Küresel ve bölgesel siyasi ve ekonomik istikrarın bozulması. 4. Siber saldırıların artması. 5. Taşıma türleri arasındaki dengesizliğinin devam etmesi. 6. Kurumlar arası mevzuattan kaynaklanan görev ve yetki çatışmasının bulunması. 7. Ülkemizde yapılacak uluslararası yatırımların önündeki bürokratik engellerin devam ediyor olması. 8. Uluslararası ulaşım ve haberleşme koridorlarında ülkemiz aleyhine değişikliklerin olması. **9.** Ulaştırma ve haberleşme alanlarında girdi fiyatlarında beklenmeyen artışlar.

Stratejik amaç, kurumun genel bir çerçevede ulaşmayı düşündüğü noktanın ne olduğunu gösterir. Stratejik amaçlar, kurumun işlevini daha ileri bir noktaya götürebilecek nitelikte olmalı ve aynı zamanda gerçekçi, ulaşılabilir bir özellik taşımalıdır [56]. Stratejik planda yer alan stratejik amaçların gerçekleştirilmesine yönelik spesifik ve ölçülebilir alt amaçlarıdır. Hedefler stratejik plan sürecinin "nerede olmayı istiyoruz" kısmını oluşturur.

Stratejik Hedefler [56];

- Belirgin Olmalıdır: Hedefler belirgin strateji ya da eylemleri açık ve anlaşılır biçimde detaylı olarak ifade ederler.
- Ölçülebilir Olmalıdır: Hedefler, ulaşıldığında değerlendirme yapabilmek için ölçülebilir olmalıdırlar. Hesap verilebilirlik mutlaka plan sürecine dâhil edilmelidir.
- Agresif Ulaşılabilir Olmalıdır: Hedefler tartışılabilir, ama olanaksızı istememelidir. Bu anlamda mevcut kaynaklarla uyumlu olmalıdırlar.
- Zamansal İçerikli Olmalıdır: Hedefler için bir yıldan fazla birkaç haftadan az olmayan bir süre kısıtı olmalıdır. Bu arada bütçe süreci ile uyumlu olmalıdır.
- Hedefler, stratejik amaçların tanımlanmış bir zaman dilimi içinde nicelik olarak ifadesidir. Bu nedenle, ulaşılması öngörülen çıktılara dönük, ölçülebilir alt amaçlardır.

TBMM İdari Teşkilatı 2013-2017 Stratejik Planında stratejik amaçlar ve bu amaçların ulaşılmasını sağlayacak hedefler şu şekildedir:

Stratejik Amaç 1. Yasama sürecinde ihtiyaç duyulan bilginin; üretilmesi, derlenmesi ve aktarılması için araştırma kapasitesini geliştirmek ve yetkinleştirmek.

Hedef 1.1. Komisyon odaklı ve yasama gündemine paralel bilgi sunumuna geçmek.

Hedef 1.2. Uluslararası alanda ülkemizin dış politikasına katkı sağlamak üzere parlamenter diplomasi faaliyetlerinin etkin yürütülmesine bilgi desteği vermek.

Hedef 1.3. Yasamaya ilişkin üretilen bilgi, belge ve materyallerin toplandığı kurumsal bir “Yasama Bilgi Havuzu” oluşturmak.

Stratejik Amaç 2. Yasama sürecinin isleyişi ve kanun yapım tekniği konularında sunulan hizmetleri mükemmelleştirmek.

Hedef 2.1. Yasama ve denetim sürecindeki uygulamaları kolaylaştırmaya ve standartlaştırmaya yönelik öneriler geliştirmek.

Hedef 2.2. Yasama süreci ve tekniğine ilişkin mesleki uzmanlaşmayı artırmak.

Hedef 2.3. Yasama ve denetim süreci ile kanun yapım tekniğine ilişkin bilgilendirme faaliyetlerini yaygınlaştırmak.

Hedef 2.4. Yasama ve denetim belgelerinde Türkçenin doğru kullanılmasını sağlamak.

Stratejik Amaç 3. Milletvekillerine zaman, mekân ve imkân sağlayarak uygun ve destekleyici bir çalışma ortamı sunmada yetkinleşmek.

Hedef 3.1. Güvenlik ve ziyaretçi yönetiminde "Teknoloji Yoğun Güvenlik Modeline" geçmek.

Hedef 3.2. Hizmet sunumunda bilişim teknolojisi imkânlarını azami derecede kullanmak.

Hedef 3.3. Destek hizmetlerinde standartlar ve kurallar belirleyerek yüksek kalitede hizmet sunmak.

Hedef 3.4. TBMM'nin çalışmalarında ihtiyaç duyulan fiziki altyapıyı ve çalışma ortamlarını sağlamak ve iyileştirmek.

Hedef 3.5. Faaliyet ve projelerin gerçekleştirilmesinde çevreye duyarlı olmak.

Stratejik Amaç 4. TBMM'yi ve İdari Teşkilatı ulusal ve uluslararası alanda tanıtmak, kurumsal imaj ve itibarını korumak ve geliştirmek.

Hedef 4.1. TBMM'nin yurt dışında tanıtımını yapmak, imaj ve itibarını güçlendirmek.

Hedef 4.2. TBMM'nin yurt içinde tanıtımını yapmak, imaj ve itibarını güçlendirmek.

Hedef 4.3. TBMM'yi ve faaliyetlerini tanıtıcı bilimsel ve sanatsal çalışmaları teşvik etmek amacıyla yarışma vb. etkinlikler düzenlemek.

Hedef 4.4. Kurum Stratejik Planına paralel olarak Milli Saraylar bünyesindeki tarihi ve kültürel varlıklara özel stratejiler geliştirmek.

Stratejik Amaç 5. Sivil toplumun görüş ve önerilerinin yasama sürecine aktarılmasını sağlamak üzere TBMM ile resmi ve sivil çevreler arasında etkileşimin gerçekleşmesine zemin oluşturmak.

Hedef 5.1. Sivil toplumun bilgi, deneyim ve görüşlerinin yasama sürecine aktarılmasını sağlamak.

Hedef 5.2. Kamu kurum ve kuruluşlarının yasama sürecine katkısını artırmak.

Stratejik Amaç 6. İdari Teşkilatın kurumsal kapasitesini geliştirmek, hizmetlerini yüksek kalitede sunmada yetkinlik kazanmak ve sürekli gelişim içinde olmak.

Hedef 6.1. İnsan kaynakları yönetiminin gerektirdiği sistem ve yaklaşımları hayata geçirmek ve geliştirmek.

Hedef 6.2. Kurumsal yönetim kalitesini artıracak yönetsel yaklaşımlar ile sistemleri geliştirmek ve uygulamak.

Hedef 6.3. İdari Teşkilatın stratejisine destek olacak ve kurum içi uzmanlaşma düzeyini artıracak bir eğitim politikası belirlemek [57].

Ulaştırma, Denizcilik ve Haberleşme Bakanlığının 2014-2018 Stratejik Planındaki stratejik amaçlar ve bu amaçların ulaşılmasını sağlayacak hedefler şu şekildedir:

Stratejik Amaç 1. Ulaştırma, denizcilik ve haberleşme altyapı ve hizmetlerini ticari, ekonomik, sosyal ihtiyaçları karşılayacak şekilde gerçekleştirmek ve yaygınlaştırmak üzere, dengeli ve teknolojik yeniliklere uygun politikalar oluşturmak ve planlamak.

Hedef 1.1. Ulaştırma Ana Planı hazırlamak.

Hedef 1.2. Akıllı Ulaşım Sistemleri Strateji Belgesi (2023)' nin eki olarak hazırlanan Eylem Planı (2013- 2015)'nda yer alan eylemleri gerçekleştirmek, gerekli güncellemeler ile tüm eylemlerin izleme ve değerlendirmesini yapmak.

Hedef 1.3. Hareket kısıtlılığı olanların ulaşım ve haberleşme hizmetlerine erişebilirliğini kolaylaştırmak.

Hedef 1.4. Denizcilik, havacılık ve uzay, tehlikeli mal ve kombine taşımacılık alanlarında strateji belgeleri ile ana planları oluşturmak.

Hedef 1.5. Bilgi ve iletişim teknolojilerine yönelik hizmetlerin toplumun tüm kesimlerine ve ülkenin her tarafına yaygınlaştırılmasını sağlamak.

Hedef 1.6. Ulaştırma, denizcilik ve haberleşme alanında uluslararası çok taraflı ve ikili işbirliğini geliştirmek.

Hedef 1.7. Gemi inşa ve yan sanayinin gelişmesine katkı sağlamak.

Stratejik Amaç 2. Can ve mal güvenliğinin en üst seviyede sağlandığı, ekolojik dengeyi gözeten, sürdürülebilir, kesintisiz ulaştırma ve haberleşme sistemlerine kavuşmak için daha etkin düzenleme, uygulama ve denetimleri hayata geçirmek.

Hedef 2.1. Afet ve acil durumlarda ulaştırma ve haberleşme hizmetlerinin aksatılmadan yürütülmesini sağlayacak hazırlık ve planlama faaliyetlerini belirlemek, müdahale yöntemlerini ortaya koymak ve uygulamaları tek merkezden yürütmek.

Hedef 2.2. Denizyolu, karayolu, demiryolu ve havayoluyla tehlikeli madde taşımacılığının emniyetli bir şekilde yapılmasının temini konusunda, gerekli altyapıyı hazırlamak.

Hedef 2.3. Demiryolu ulaşımını geliştirmek ve serbest, adil, sürdürülebilir bir rekabet ortamı sağlamak.

Hedef 2.4. Kamu ve özel işletme ve şirketlerin, standartları belirlenmiş, emniyetli, güvenli ve kaliteli demiryolu hizmeti vermesini sağlamaya katkıda bulunmak.

Hedef 2.5. Denizlerde seyir, can, mal ve çevre emniyetini en üst seviyede sağlamak.

Hedef 2.6. Piyasadan çekilen ekonomik ve teknik ömrünü doldurmuş ticari araç sayısını arttırmak.

Hedef 2.7. Trafikte seyreden emniyetsiz ve ağır kusurlu araç sayısını azaltmak.

Hedef 2.8. Karayolu taşımacılığında mesleki yeterlilik eğitimi alanların sayısını arttırmak.

Stratejik Amaç 3. Ülke kaynaklarını en rasyonel şekilde kullanarak, daha kaliteli, ucuz, hızlı ve güvenli hizmet sunabilmek için ulaştırma, denizcilik ve haberleşme altyapılarını geliştirmek ve yaygınlaştırmak.

Hedef 3.1. Kombine taşımacılığı geliştirmek.

Hedef 3.2. Uluslararası demiryolu bağlantılarını geliştirmek.

Hedef 3.3. Şehirlerarası taşımacılıkta demiryolunun payını arttırmak.

Hedef 3.4. Şehir içi taşımacılıkta raylı sistem payını arttırmak.

Hedef 3.5. Havayolu ulaşımı altyapısını yaygınlaştırmak.

Hedef 3.6. İçsu yolu potansiyelini geliştirmek.

Hedef 3.7. Kıyı yapılarını geliştirmek.

Hedef 3.8. e-devlet uygulamalarının yaygınlaşmasını sağlamak.

Hedef 3.9. Ülkemizin elektronik haberleşme altyapısını teknolojik gelişmelere paralel olarak geliştirmek.

Hedef 3.10. Kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda yer alan sistemlerin güvenliğinin sağlanması ve gizliliğinin korunmasını sağlamak.

Hedef 3.11. Havacılık sanayine ilişkin teknolojik ve hukuki altyapıyı oluşturmak.

Stratejik Amaç 4. Ar-Ge ve yenilikçilik esaslı üretim kültürü oluşturarak, ileri ulaştırma, denizcilik ve haberleşme teknolojilerinin milli kaynaklarla üretimini teşvik etmek ve yaygınlaştırmak.

Hedef 4.1. Elektronik haberleşme ile uzay ve havacılık sektörlerinde Ar-Ge ve teknolojik gelişmeleri ülke genelinde yaygınlaştırmak.

Hedef 4.2. Uydu simülasyonu laboratuvarı kurmak.

Hedef 4.3. Uluslararası ölçekte milli planetaryum ve havacılık uzay müzesini kurmak.

Hedef 4.4. Ülkemizde haberleşme ve gözlem uydularının ve ilgili teknolojilerin geliştirilmesi amacıyla deneysel uydu yapmak.

Hedef 4.5. Ülkemizde Radyo Teleskop altyapısını oluşturmak.

Stratejik Amaç 5. Daha kaliteli hizmet sunmak üzere, kurumsal kapasiteyi geliştirmek.

Hedef 5.1. Bakanlığımızca yürütülen iş ve işlemlerde bilgi ve iletişim teknolojilerinden en üst seviyede yararlanmak.

Hedef 5.2. Bakanlık merkez ve taşra birimlerinin fiziki, teknik ve sosyal ihtiyaçlarına yönelik altyapısını güçlendirmek ve çalışma ortamını modernize etmek [58].

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının amacı;

- Kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin sağlanmasına,
- Kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanmasına,
- Siber güvenlik olaylarının etkilerinin en düşük düzeyde kalmasına, olayların ardından sistemlerin en kısa sürede normal çalışmalarına dönmesine yönelik stratejik siber güvenlik eylemlerinin belirlenmesine ve oluşan suçun adli makam ve kollukça daha etkin araştırılmasının ve soruşturulmasının sağlanmasına yönelik bir altyapı oluşturmaktır [10].

USGS'de kurum içi ve kurum dışı herhangi bir değerlendirme kriteri bulunmamaktadır. Amaçlar; stratejiyi uygulamakla yükümlü olan kurumlara yönelik bir yol belirtmiştir fakat kapsam bakımından yeterli olmadığı değerlendirilmektedir. Siber güvenlik stratejimizin amaçlarını destekleyecek şekilde hedefler belirtilmemiştir.

4.3.6. Ulusal siber güvenlik stratejisi

Kritik altyapılara ait sistemleri ve verileri hedef alan siber saldırıların kimler tarafından organize edildiğinin tespiti neredeyse imkânsızdır. Bu durum siber ortamdaki risk ve tehditlerin asimetrik karakterini ortaya koymaktadır. Bu nedenle; 20 Ekim 2012 tarih ve 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" 28447 sayılı Resmi Gazetede yayımlanmıştır.

Söz konusu karar uyarınca; Ulaştırma, Denizcilik ve Haberleşme Bakanının başkanlığında, Dışişleri, İçişleri, Milli Savunma, UDHB, Ulaştırma bakanlıkları müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşan Siber Güvenlik Kurulu kurulmuştur [10].

Siber güvenlik stratejisi hazırlanırken;

- İlham verici, esnek ve tutarlı vizyon,
- Amaçların saptanmasına rehberlik edecek, kısa ve açık misyon,
- Özellikle insan temel hak ve özgürlükleri ile güvenliğin dengesini sağlayacak şekilde temel ilkeler,
- Stratejiyi uygulamakla yükümlü kurum ve kuruluşlara yönelik stratejik hedef ve amaçlar belirlenmeli ve
- Ulusal siber güvenlik açısından iç ve dış analizi yapmaya imkân verecek SWOT analizi yapılmalıdır.

İletişim ağlarının ve bilgi sistemlerinin işlerliğinin idamesi; vatandaş güvenliği ve kişi-kurum-devlete ait kültürel varlıkların korunmasının sağlanması, kritik altyapılara düzenlenecek siber saldırıların engellenmesi ve bu saldırıların sebebiyet vereceği zararın minimize edilmesi için hazırlanan ulusal siber güvenlik stratejisinin geliştirilmesi en yüksek öncelik arz etmektedir. Ulusal siber güvenlik stratejisi; devlet kurumları üzerine düşecek tüm görev ve sorumlulukları açıkça belirtecek, kamu-özel sektör işbirliğini teşvik edecek ve siber güvenliği destekleyen devlet kaynaklı girişimler oluşturulacak şekilde yapılmalıdır.

Strateji, stratejik planlama ve stratejik yönetim kavramları ile ilgili olarak yönetim bilimi alanında yapılan çalışmaların tamamının belli bir kurum, organizasyon veya şirket genelinde yapıldığı gözlemlenmiştir. Ancak, ulusal siber güvenliğin sağlanması kapsamında strateji hazırlanırken tek bir kurum veya organizasyon yapısı düşünülerek planlama yapılamaz. Ulusal siber güvenliğin sağlanmasından sorumlu olan Siber Güvenlik Kurulunu oluşturan birçok bakanlık, müsteşarlık ve kurum bulunmaktadır. Bu birimler arasındaki eşgüdüm ayrıntılı planlama ile sağlanabilecektir. Siber güvenlik stratejisi hazırlamak, diğer strateji belgelerini hazırlamaktan çok farklıdır. Dünyada konusunda uzman kişi, kurum, kuruluşlar tarafından yazılmış olan siber güvenlik stratejisi hazırlama yöntemleri ile ilgili literatür taraması yapılmış ve Bölüm 5'te ayrıntılı olarak açıklanmıştır.

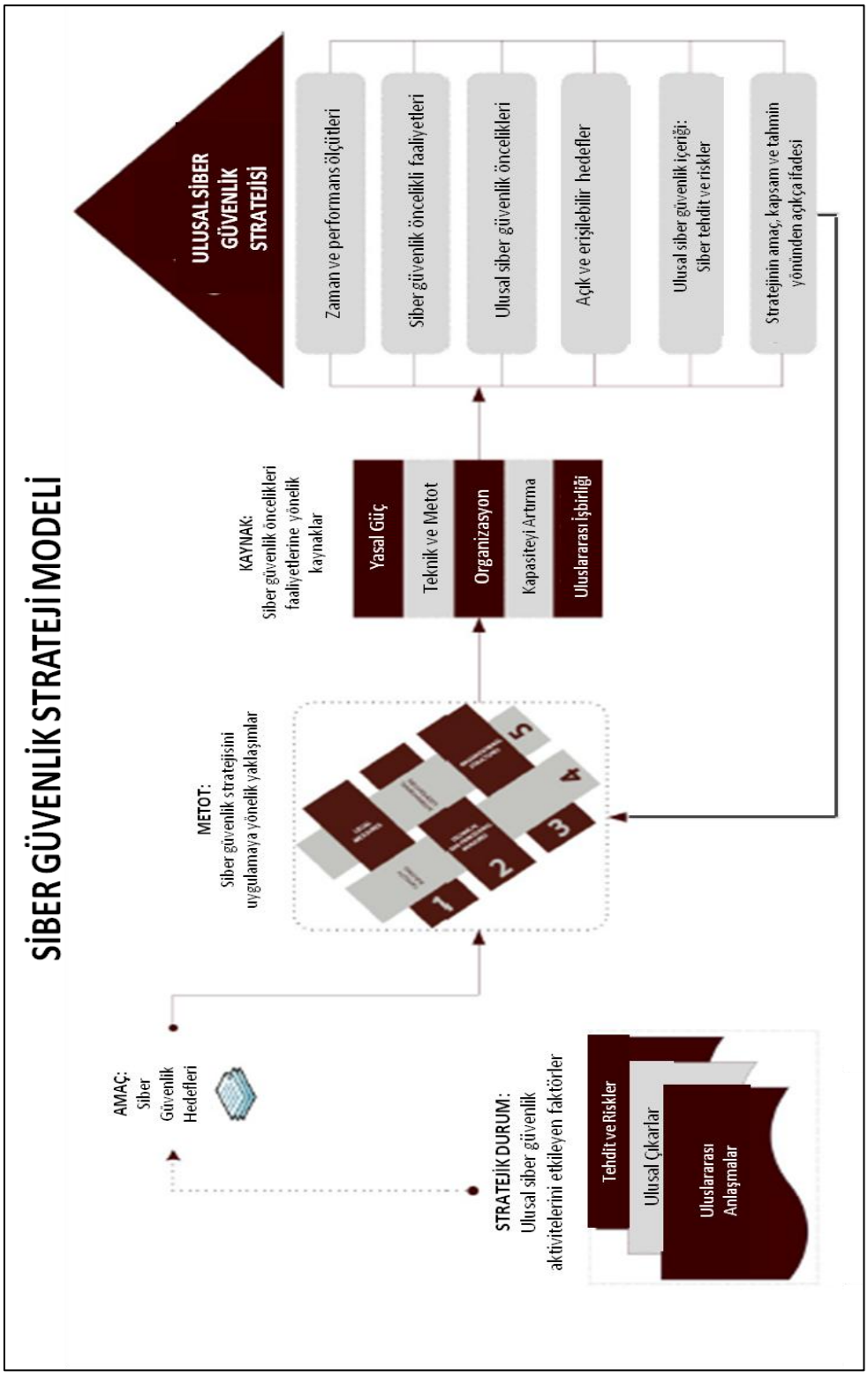
5. ULUSAL SİBER STRATEJİ HAZIRLAMA YÖNTEMLERİ

Önceki bölümlerde ifade edildiği gibi, iletişim ağlarının ve bilgi sistemlerinin işlerliğinin idamesi; vatandaş güvenliği ve kişi-kurum-devlete ait kültürel varlıkların korunmasının sağlanması, kritik altyapılara düzenlenecek siber saldırıların engellenmesi ve bu saldırıların sebebiyet vereceği zararın minimize edilmesi için hazırlanan ulusal siber güvenlik stratejisinin geliştirilmesinin en yüksek öncelik arz etmektedir. Tez çalışmasının bu bölümünde ulusal siber strateji hazırlama yöntemleri ile ilgili yapılan literatür taraması neticesinde konusunda uzman kurum ve kişilerin yaptığı çalışmalar incelenmiştir.

5.1. Uluslararası Telekomünikasyon Birliği (ITU) Ulusal Siber Güvenlik Strateji Rehberi

Bu çalışmada siber güvenliğin sadece bilgisayar güvenliği olmadığı, siber güvenliğin; siber uzayın yasadışı kullanılması vasıtasıyla ekonomi, halk sağlığı, güvenlik ve ulusal güvenlik boyutları bakımından ulusal politikayı ilgilendiren bir husus olduğu vurgulanmaktadır. Devletler temel olarak sosyal düzeni sürdürmek, vatandaşların hayatları ile varlıklarını korumak ve ticaret imkânı sunmak zorundadırlar. Yukarıda bahsedilen hususların temelinde siber güvenlik olduğu için liderlere sorumluluk düşmektedir. Bu rehber devletlere, ulusal güçlerini kullanarak siber riskleri uygun bir şekilde azaltma yönünde öneriler sunmaktadır [60].

Ülkelerin siber güvenlik stratejilerini baştan hazırlamaları veya var olan strateji belgelerini geliştirmeleri için Şekil 5.1'de gösterilen bir referans model önerilmiştir. Amaç-Metot-Kaynak strateji yöntemi kullanılarak hazırlanan bu modelin merkez noktası olarak, ITU'nun bilgi toplumu için gizlilik ve güvenliğin arttırılması için uluslararası işbirliği sistemi olan Küresel Siber Güvenlik Gündeminde (Global Cybersecurity Agenda, GCA) ele alınan beş önemli çalışma alanı temel alınmıştır [61].



Şekil 5.1. ITU Tarafından önerilen referans modeli [60]

Bunlar;

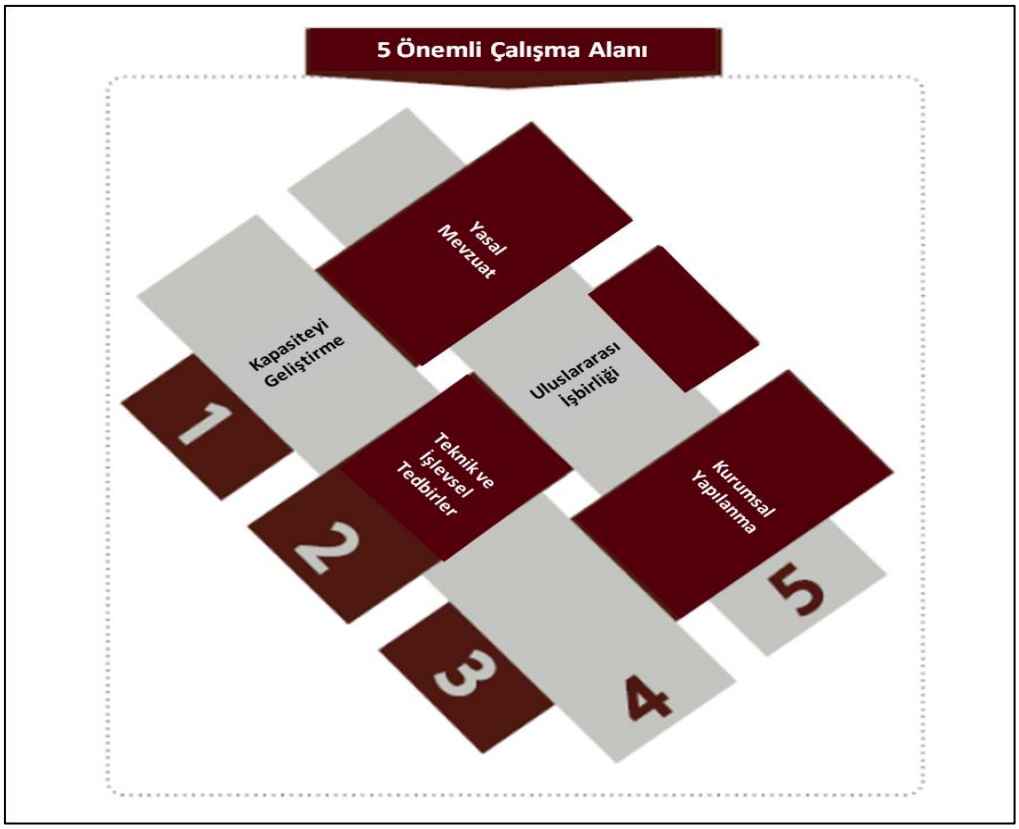
- Ulusal siber güvenlik mevzuatının geliştirilmesi.
- Teknik ve işlevsel tedbirlerin alınması.
- Kurumsal yapılanmanın oluşturulması.
- Ulusal kapasitenin geliştirilmesi ve farkındalığın arttırılması.
- Uluslararası işbirliğinin sağlanması.

Bu çalışma alanlarının birbiriyle nasıl ilişkili olduğu Şekil 5.2'de gösterilmiştir.

5.2. Bilgi Teknolojileri ve İletişim Kurumu (BTK) Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler

Bu çalışmada, siber güvenliğin sağlanması ve kritik bilgi ve altyapıların korunmasının giderek artan önemi göz önüne alınarak, ülkemizde yapılacak çalışmalara katkıda bulunmak üzere bazı tespitlerde bulunulmuştur. Çalışmada, ilk olarak siber güvenlik ile ilgili tanımlar ve açıklamalar yapılmış daha sonra kritik altyapılar ile bilgi teknolojileri arasındaki bağdan söz edilmiştir. Siber tehditler ve amaçları ile ilgili bilgilendirmeyi müteakip ulusal siber güvenliğin sağlanması konusu üzerinde durulmuştur [62].

Söz konusu çalışma Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı hazırlanmadan önce yapılmış ve ülkemizde ulusal siber güvenliğin sağlanması konusunda kritik öneme sahip olduğu değerlendirilen temel ilkeler, yöntemler ve adımlara yer verilmiştir.



Şekil 5.2. Küresel Siber Güvenlik Gündeminin beş önemli çalışma alanı [60]

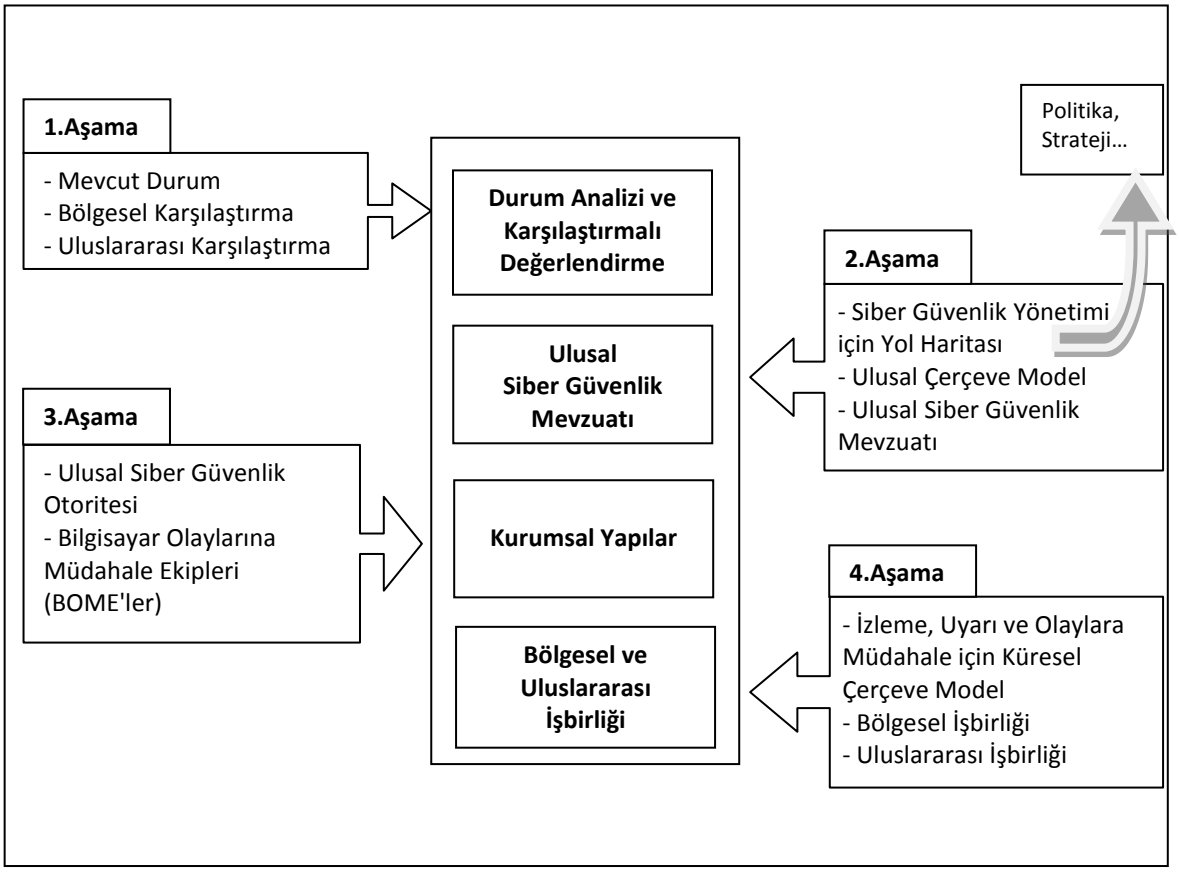
5.2.1. Temel ilkeler

Ulusal siber güvenliğin sağlanmasına yönelik olarak yürütülecek çalışmalarda esas alınması gereken temel ilkeler şunlardır:

- Uluslararası sözleşmelerle teminat altına alınmış temel insan hak ve hürriyetlerinin korunması,
- Demokratik toplum düzeninin gereklerine uyulması,
- Alınacak tedbirlerin Ölçülülük İlkesine göre belirlenmesi,
- Karar alma süreçlerine tüm paydaşların katılımını sağlayacak kapsayıcı bir yaklaşımın benimsenmesi,
- Siber güvenliği hukuki, teknik, idari, ekonomik, politik ve sosyal boyutları ile ele alan bütüncül bir yaklaşımın benimsenmesi,
- Geliştirilecek çözümlerde güvenlik ile kullanılabilirlik arasında denge kurulması,
- Diğer ülke mevzuatlarının göz önünde bulundurulması ve mümkün olabildiğince uyumluluğun sağlanması,
- Uluslararası işbirliğinin sağlanması.

5.2.2. Yöntem

Ulusal siber güvenliğin sağlanmasını hedefleyen çalışmalarda Şekil 5.3'de özetlenen 4 aşamalı yaklaşımın izlenmesi ITU tarafından önerilmektedir.



Şekil 5.3. Siber güvenliğin sağlanması üzerine bir yaklaşım [62].

1. Aşamada; ülkemizin siber güvenlik konusundaki mevcut durumu farklı ülkelerin mevzuatları ile bölgesel ve uluslararası çalışmalar karşılaştırılarak analiz edilmeli ve siber güvenlik konusunda başarılı ulusal planlar, programlar ve mevzuat geliştirmiş olan ülke örneklerinden yararlanılmalıdır.

Bu aşamada önemli olan nokta mevzuatımızdaki eksiklikleri ve bu eksikliklerin nasıl giderilebileceğine ilişkin olabildiğince çok *alternatif yol ve yöntem* tespit edebilmektir.

2. Aşamada; siber güvenlik konusunda ulusal yol haritamız (politika ve strateji) ve ulusal çerçeve model oluşturulmalı ve ulusal siber güvenlik mevzuatımız geliştirilmelidir. Ulusal çerçeve model;

- Ulusal siber güvenlik politikası ve stratejisinin etkin bir şekilde uygulanması,
- Mevcut güvenlik yasalarının siber ortama uyarlanması için gereken çalışmaların yapılması,
- Bilgi iletişim sistemlerini hedef alan saldırıların önlenmesi, tespit edilmesi, bunlara müdahale edilmesi ve en az hasarla geri dönüşün sağlanması için gereken usul ve esasların belirlenmesi,
- Ulusal siber güvenlik kültürünün benimsenmesinin sağlanması,
- Temel paydaşların belirlenmesi,
- Ulusal siber güvenlik programının denetlenmesi, değerlendirilmesi, doğrulanması ve etkinliğinin arttırılması gibi hususları ele almalıdır.

3. Aşamada; ulusal siber güvenlik çalışmalarını yürütecek olan kurumsal yapı oluşturulmalıdır. Bu yapının görev ve sorumlulukları ile diğer paydaşlarla ilişkileri belirlenmelidir.

4. Aşamada; İnternet başta olmak üzere bilgi teknolojilerinin sınır tanımayan küresel yapısı göz önünde bulundurulmalı ve küresel çapta ele alınmaması halinde siber tehditlerin ve saldırıların sonlandırılamayacağı bilinmelidir. Bu itibarla uluslararası bir işbirliği modeli geliştirilmelidir.

5.2.3. Siber güvenlik adımları

Temel ilkeler ışığında ve önerilen yöntem doğrultusunda, ülkemizde mevcut bulunan siber güvenlik çalışmaları ile bölgesel ve uluslar arası örneklerin karşılaştırılması suretiyle tespit edilen eksiklikler ve bu eksikliklerin giderilerek ulusal siber güvenlik çalışmalarının etkinliğinin arttırılması için atılması gereken somut adımlar ITU Küresel Siber Güvenlik Gündeminde ele alınan 5 başlık altında toplanmıştır. Bu adımlar aşağıda kısaca özetlenmiştir [62]:

Ulusal siber güvenlik mevzuatının geliştirilmesi

Bilgi teknolojilerinde yaşanan hızlı gelişmeler siber suçluların çıkar amaçlı kullanabilecekleri yeni fırsatlar yaratırken, siber suçlarla mücadeleyi de oldukça karmaşık hale getirmekte; geçmişte sadece fiziksel varlıklara veya kişilere yönelik suçlarla mücadele alanında görev yapmakta olan kolluk kuvvetlerinin ve adli personelin işlerini güçleştirmektedir.

Siber güvenliğin yasal boyutunda yaşanan güçlüklerin azaltılması, soruşturma ve kovuşturmanın etkinliğinin sağlanabilmesi amacıyla yapılması gereken çalışmalar aşağıda belirtilmektedir.

- Yasal boşluklar giderilmelidir.
- Usule ilişkin yasal eksiklikler ortadan kaldırılmalıdır.
- Siber ortamda koruma ve gözetme yetkileri belirlenmelidir.
- Kolluk kuvvetlerinin ve adli personelin teknik uzmanlığı arttırılmalıdır.
- Siber ortamda yargılama yetkileri belirlenmelidir.
- Ülkemiz ve diğer ülkeler arasında siber saldırganların iadesine ilişkin uzlaşma usulleri belirlenmelidir.

Teknik ve işlevsel tedbirlerin alınması

Günümüzde teknolojinin gelişimi ile birbirine bağlanan şebekelerin sınırlarının belirsizleşmesi, taşınabilir cihazların kolaylıkla şebekelere dâhil olup ayrılabilmesi, farklı güvenlik seviyelerine sahip şebekelerin birbirlerine bağlanması ve şebekelerin çok çeşitli kullanıcı sınıfları tarafından kullanılması gibi hususlar siber güvenliğin sağlanmasını güçleştirmektedir. Siber saldırılar incelendiğinde, saldırı araçlarının kapsamı ve etkisi arttığı halde, siber saldırganların bu saldırıları düzenlemek için ihtiyaç duydukları bilgi ve uzmanlık düzeyinin giderek azalmakta olduğu görülmektedir.

Siber güvenliğin teknik boyutunda gözlenen eksikliklerin azaltılması, teknik çözümlerin etkinliğinin sağlanabilmesi amacıyla yapılması gereken çalışmalar aşağıda belirtilmektedir:

- Güvenliği kanıtlanmış standartların ve teknik çözümlerin kullanılması,
- Kurum ve kuruluşların bazı teknik ve işlevsel tedbirleri almalarının teşvik edilmesi,
- Farklı güvenlik seviyelerine sahip bilgi ve iletişim şebekeleri arasındaki farkın kapatılması,
- Şebekelerde veya sistemlerde bulunan açıklıkların kamuoyuna açıklanması, incelenmesi ve iyileştirilmesi esnasında belli bir sorumluluk bilinci ve etik anlayışı içinde hareket edilmesi,
- Güvenlik çözümleri üreticilerinin işbirliği içinde çalışması.

Kurumsal yapılanmanın oluşturulması

Çeşitli ülkelerin siber güvenlik yapılanmaları incelendiğinde, siber güvenliği sağlamak amacıyla bazılarının yeni kurumlar oluşturduğu, bazılarının ise mevcut kurumların görev alanını genişlettiği, oluşturulan veya görev alanı genişletilen kurumların daimi komiteler, çalışma grupları, danışma kurulları, disiplinler arası merkezler gibi çok çeşitli yapılara sahip oldukları görülmektedir.

Siber tehditlerle mücadele için etkin kurumsal yapılar oluşturmak ve konuyla ilgili mevcut ve yeni girişimler arasında koordinasyon sağlamayı amaçlayan birimleri tesis etmek son derece önemlidir. Bu bağlamda gerçekleştirilmesi gereken çalışmalar şunlardır:

- Kamu-Özel Sektör-Üniversite-Sivil Toplum işbirliği modelinin oluşturulması,
- Ulusal Siber Güvenlik Otoritesi oluşturulması,
- Ulusal BOME'lerin oluşturulması.

Ulusal kapasitenin geliştirilmesi ve farkındalığın arttırılması

Siber güvenliğin sağlanması konusunda benimsenen genel yaklaşım gerek kamu sektöründe gerekse özel sektörde büyük ölçekli kurum ve kuruluşlarda risk yönetimi uygulamak ve mevcut riski azaltarak bu kurum ve kuruluşların kaynaklarını korumak şeklindedir.

Ayrıca, siber güvenliğin öteden beri sadece teknik boyutta ele alınması ve teknik çözümler geliştirmeye öncelik verilmesi; yasal, idari, ekonomik ve sosyal boyutlarda siber güvenlik kapasitesinin geliştirilmesini engellemektedir.

Siber güvenliği tesis etmek üzere kapasitenin geliştirilmesi ve farkındalığın arttırılması için yapılması gereken çalışmalar şunlardır:

- Ulusal siber güvenlik kültürünün oluşturulması
- Farkındalığın arttırılması
- Ulusal kapasitenin geliştirilmesi

Uluslararası işbirliğinin sağlanması

Siber ortamda koruma, gözetme ve yargılama yetkilerinin belirsizliği ile siber suçların pek çok ülke mevzuatında suç olarak tanımlanmamış oluşu nedeniyle siber saldırganların lehine oluşan güvenli sığınaklar, yurtdışından delil toplama esnasında yaşanan gecikmeler, yurtdışında bulunan suçluların iadesinde yaşanan güçlükler gibi sorunlar, ulusal siber güvenliğin sağlanması hususunda uluslar arası işbirliğinin olmazsa olmaz önemde olduğunu göstermektedir.

Siber güvenlik, bilgi güvenliği ve şebeke güvenliği konusunda yaşanan küresel çaptaki sorunlar ancak temel paydaşları kapsayan uluslararası bir işbirliği stratejisi ve siber güvenlik kültürü ile ele alınabilir. Söz konusu strateji ve kültürün teşkil edilebilmesi amacıyla yürütülmesi gereken çalışmalar şunlardır:

- Bölgesel işbirliğinin sağlanması,
- Uluslararası işbirliğinin sağlanması.

5.3. Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) Ulusal Siber Güvenlik Stratejileri, Geliştirme ve Uygulama Üzerine Pratik Rehber

Avrupa Birliği (AB) ve üye ülkelere ağ ve bilgi güvenliği uzmanlık merkezi olarak danışmanlık yapan ENISA; siber güvenlik stratejisi geliştirmek, uygulamak ve sürdürmek üzere örnek uygulamaları ve önerilerini sunmak için bu dokümanı hazırlamıştır [63].

AB ülkeleri siber tehditlerin sınır ötesi etkilerinden korunmak için esnek ve dinamik stratejilere ihtiyaç duymaktadır. Bu doküman ayrıca; siber güvenlik stratejileri ile ilgili alanları açıklamayı, kamu ve özel sektör paydaşları için faydalı öneriler sunmayı, AB üye ülkelere strateji belgelerini geliştirmek, güncellemek, uygulamak için yardım etmeyi amaçlamaktadır. Yeni bir strateji belgesi oluşturmak, mevcut strateji belgesinin eksikliklerini tamamlamak ve geliştirmek veya mevcut stratejinin eylem planlarının etkinliğini değerlendirmek üzere kullanılabilir. ENISA tarafından hazırlanan kapsamlı rehber doğrultusunda İngiltere, ABD ve Türkiye'nin ulusal siber güvenlik stratejilerinin karşılaştırılması 6. Bölümde yapılmıştır.

5.3.1. Vizyonu, kapsamı, hedefleri ve öncelikleri belirleme

Siber güvenlik stratejisinin amacı global direnci ve bilgi teknolojilerinin güvenliğini arttırmaktır. Açıkça belirtilmiş hedef ve önceliklerin belirlenerek bu amaca erişmede başarı sağlanabilecektir. Bu adımda yapılması gerekenler şu şekildedir:

- Üst düzey hedefleri spesifik zaman belirtilerek (genellikle 5-10 yıl) vizyon ve kapsam tanımlanmalıdır.
- Belirtilen kapsam içerisinde özel sektör ve servislerinin yeri belirtilmelidir.
- Toplum, ekonomi ve vatandaşlara etkisi bakımından hedefler önceliklendirilmelidir.
- Hali hazırdaki politika, strateji, uygulamalar vb. göz önünde bulundurulmalıdır.
- Paydaşlar en başından doğru olarak belirlenmelidir.
- Stratejinin uygulama haritası tanımlanmalıdır.

5.3.2. Ulusal risk değerlendirmesi yaklaşımını takip etme

Siber güvenlik stratejisi hazırlanırken özellikle kritik altyapıların üzerinde durulması gerekmektedir. Risk değerlendirmesi yaklaşımı risk tanımı, risk analizi ve risk değerlendirme adımlarından oluşan bilimsel ve teknolojik bir süreçtir. Bu değerlendirme kaynakların doğru kullanılmasını, beklenmedik olayların stratejinin hedeflerini etkilemesini ve/veya riske atma ihtimalini takip, kontrol ve en aza indirgenmesini kapsamaktadır. Bu adımda yapılması gereken en önemli husus kritik sektör ve altyapıların tanımlanması ve koruma planlarının hazırlanmasıdır.

5.3.3. Hâlihazırdaki politika, mevzuat ve kapasiteleri dikkate alma

- Mevcut politikalar, mevzuat ve uygulamalar değerlendirilip dikkate alındıktan sonra önemli eksiklikler belirlenmelidir.
- Siber güvenliğin ulusal güvenlik politikasının bir parçası olması sağlanmalıdır.
- Siber güvenliği iyileştirecek mevcut örnek uygulamalar belirlenmelidir.
- Kamu sektöründeki rol ve sorumluluklar tanımlanmalıdır.
- Stratejinin gerçekleştirilmesini sağlamak üzere mevcut kanunların yeterliliği değerlendirilmelidir.

5.3.4. Şeffaf bir yönetim yapısı geliştirme

Siber güvenlik stratejisi ancak şeffaf yönetim yapısı oluşturulması ile başarılı olabilecektir. Şeffaf yönetimde roller, sorumluluklar ve ilgili paydaşların görevleri açıkça tanımlanmalıdır. Stratejinin koordinatörü olarak kurumlar arası çalışma grubu veya bir kamu kurumu sorumlu olmalıdır, stratejinin kendisinden ve yaşam döngüsünden bizzat yükümlü olmalıdır.

5.3.5. Paydaşları belirleme

Başarılı bir siber strateji kamu ve özel sektör arasında uygun bir eşgüdüm sağlanmasını gerektirmektedir. Kamu paydaşları politikalar, mevzuat ve operasyonel yetkilere sahipken, özel sektör paydaşları ise çoğunlukla kritik altyapıların sahibi olmaktadır. Bu adımda;

- Kritik altyapıların ve servislerin sahipleri tanımlanmalıdır.
- Stratejinin uygulaması ve geliştirilmesinden sorumlu kamu kurumları tanımlanmalıdır.
- Hem kamu hem de özel sektördeki paydaşların kendi rollerinin özümsenmesi sağlanmalıdır.
- Strateji sürecine katılım sağlanması durumunda verilecek teşvikler (vergi muafiyeti gibi) belirlenmelidir.
- Farkındalık açısından bu sürece sivil toplumun katkısı sağlanmalıdır.
- İlgili bakanlıkların katılımı sağlanmalıdır.

5.3.6. Güvenilir bilgi paylaşım ortamı sağlama

Sürekli değişen ve hızına ayak uydurmakta güçlük çekilen bu çağda, paydaşlar arasında güvenli ve güçlü bilgi paylaşım mekanizmalarının kurulması hayatidir. Özellikle kritik altyapılardan sorumlu olan kurumların karşı karşıya kaldıkları tehditleri, riskleri ve hassasiyetleri diğer kurumlarla paylaşmaları çok önemlidir.

5.3.7. Ulusal siber acil durum planları oluşturma

Özellikle kritik altyapılarla ilgili büyük siber olayların yaşanma ihtimaline karşı acil müdahale ve kurtarma sürecinde geçici tedbirler ve yapılar oluşturulması gerekmektedir. Ulusal acil planlara da uyum sağlamalıdır.

5.3.8. Siber güvenlik tatbikatları icra etme

Toplumun ve kurumların doğal afetlerde, teknolojik arızalarda, siber saldırılarda ve acil durumlarda direncinin ve hazırlık seviyesini arttırmak için siber güvenlik tatbikatları icrası önemlidir. Bu tatbikatlarda; nelerin test edilmesi gerektiği saptanmalı, ulusal tatbikat planlama ekibi kurulmalı ve ulusal siber güvenlik stratejisinin yaşam döngüsüne dâhil edilmelidir.

5.3.9. Temel güvenlik gereksinimlerini oluşturma

Her kamu ve özel sektör kurumu kendi bilgi altyapılarını tehdit ve risklerden korumak maksadıyla gerekli önlemleri almalıdır.

5.3.10. Olay raporlama mekanizmalarını oluşturma

Olay raporlama mekanizmalarının ulusal siber güvenliğin arttırılmasında önemli bir rolü vardır. Bir kişi veya kurumun tehdit ortamı ile ilgili ne kadar çok bilgisi olursa o kadar iyi önlem alması mümkün olmaktadır. Olay raporlama ve analizi alınacak güvenlik tedbirlerinin değiştirmesi ve uygun hale getirilmesinde fayda sağlayacaktır.

5.3.11. Kullanıcı farkındalığı

Farkındalığın artmasıyla kişi ve kurumlar dijital dünyada nasıl hareket edeceklerini ve kendilerini nasıl koruyacaklarını öğrenirler. Güvenlik ile ilgili farkındalık yaratma aktiviteleri organizasyon içinde ve dışında gerçekleştirilebilir. Bu kapsamda;

- Farkındalığı arttırılacak kitleler tespit edilmeli (çocuklar, vatandaşlar, son kullanıcılar vb.),
- Bu kitlelere erişmek için mekanizmalar geliştirilmeli,
- Genel hatalı davranış kalıpları tespit edilip bunların düzeltilmesi ile ilgili önlemler alınmalı,
- Siber güvenlik ayı, haftası veya günü gibi önemli günler organize edilmeli,
- Çok bilinen kamu sitelerine bilgi güvenliği ile ilgili sunum, materyal, dersler konulmalı,
- Bu konu ile ilgili dokümanlar yabancı dillerden dilimize çevrilmelidir.

5.3.12. Ar-Ge'yi teşvik etme

Hayatımız artık yeni bilgi teknolojileri ve servisleri üzerine kurulmaktadır. Bu teknolojiler ticari olarak yaygınlaşmadan önce siber güvenlik yeterliliklerini yerine getirme durumları mutlaka incelenmelidir. Siber güvenlik stratejisi mutlaka araştırma-geliştirme yaşam döngüsünü muhteva etmelidir.

5.3.13. Eğitim programlarını güçlendirme

Maalesef üniversiteler ve Ar-Ge kurumları yeteri kadar siber güvenlik uzmanı yetiştirememektedir. Siber güvenlik bilgisayar biliminin bir parçası olarak değerlendirilmektedir, fakat sürekli değişen ve eğitim gerektiren konulara sahiptir. Bu bağlamda;

- Ulusal bilgi güvenliği eğitim programları başlatılmalı,
- Kritik görevler için yetişmiş personel sertifikalandırılma ve akreditasyon işlemleri desteklenmeli,
- Bilgi güvenliği eğitimi üniversitelerin müfredatına/programlarına dâhil edilmelidir.

5.3.14. Acil durum müdahale kapasitesini oluşturma

Ulusal seviyedeki paydaşlarla acil durum müdahalesinde, Siber Olaylara Müdahale Ekiplerine ve Ulusal Siber Olaylara Müdahale Merkezlerine büyük görev düşmektedir. Aynı zamanda USOM ve SOME'ler diğer ülkelerdeki karşılıkları ile eşgüdüm sağlamakla sorumludurlar.

5.3.15. Siber suçun tespiti

- Gerekli kanun maddeleri yasalaştırılmalı ve konu ile alakalı uluslararası anlaşmalar onaylanmalı,
- Ulusal uzman siber suç birimleri kurulmalı,
- Kolluk kuvvetleri ile yargı mensuplarının sürekli ve özel eğitimlerden geçirilmeleri sağlanmalı,
- Siber suçların uygun şekilde analiz edilmesi için araçlar tahsis edilmeli ve kurallar koyulmalı,
- Kamu ve özel sektör eşgüdümü sağlanarak yeni dijital adli bilişim tekniklerinin uygulanması ve geliştirilmesi sağlanmalıdır.

5.3.16. Uluslararası işbirliğini sağlama

Siber tehditler ve riskler doğası gereği uluslararası mücadeleyi gerektirmektedir. Stratejide uluslararası işbirliği ile ilgili şu bölümlere yer verilmelidir;

- Strateji uluslararası eşgüdümü teşvik etmek için kullanılmalı,
- Hangi ülkelerle ve hangi konularda işbirliği yapılacağına karar verilmeli,
- Ulusal sorumlu kurum veya kuruluşa uluslararası işbirliğini arttırma yönünde görev verilmeli,
- Sadece ülkelerle değil, bilgi güvenliği, bilgi paylaşımı, istihbarat paylaşımı gibi konularda uzman merkezlerle de işbirliği içerisinde olunmalı,
- Uluslararası anlaşmalara katılım sağlanmalıdır.

5.3.17. Kamu-özel sektör işbirliğini sağlama

Kamu-özel sektör işbirliği amaçlara ulaşabilmek için ortak hedeflerin belirlenmesi, tanımlı görev ve çalışma metodolojilerinin kullanılması üzerine kuruludur. Sağlıklı bir işbirliğinin tahsisi için karşılaşılacak güçlükler ve engeller kadar değişik bileşenler dikkate alınmalıdır. Bu bileşenler;

- Siber tehditlerin tahayyülü,
- Diğer organizasyonlarla işbirliği sağlamanın planlanması,
- Yönetici seviyesinde üst düzey işbirliği sağlama,
- Karşılıklı olarak deneyimli personelin işe alınması,
- Bu tip işbirliğinde karşılaşılacak sorunlar için yasal tavsiyeler alınması,
- Bilgi dağıtımı politikaları oluşturulmasıdır.

5.3.18. Güvenlik ve mahremiyeti dengeleme

Siber teröre karşı alınan tedbirler siber suçlara engel olmakla beraber kişisel mahremiyeti bazı durumlarda ihlal etmektedir. Bir siber güvenlik stratejisi kişisel mahremiyetle güvenlik olgusu arasında doğru dengeyi bulmalıdır.

5.3.19. Değerlendirme

Siber güvenlik stratejisi bir kere oluşturulduktan sonra hangi hedeflerin gerçekleştirilebildiği değerlendirilmelidir. Bu sayede tespit edilen hedeflere ulaşabilmek için düzeltici ve önleyici eylemlerde bulunulabilecektir. Değerlendirme safhası için sorumlu kuruluşa, bağımsız bir başka kuruluşa veya üst düzey başka bir kuruma görev verilebilir.

5.3.20. Ulusal siber güvenlik stratejisini güncelleme

Siber güvenlik stratejisi hazırlama bir kereye mahsus yapılması gereken bir süreç değildir. Bu, Planla-Uygula-Kontrol Et-Harekete Geç modeli olan; stratejilerin, politikaların, süreçlerin, ürünlerin oluşturulması safhasında kontrol ve sürekli gelişimi sağlayan bir yapıdır. Siber güvenlik stratejisinde geliştirme, uygulama, değerlendirme ve güncelleme olarak uygulanmaktadır.

5.4. NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCD COE) Ulusal Siber Güvenlik Yapı Kılavuzu

NATO Müşterek Siber Savunma Mükemmeliyet Merkezinde (Cooperative Cyber Defence Centre of Excellence, CCDCOE), ülkeler tarafından oluşturulan siber güvenlik stratejilerinin incelenmesi sonucunda hazırlanan "National Cyber Security Framework Manual" adlı çalışmada Klimburg, strateji belgelerinde ortak hedefleri şu şekilde belirtmiştir [64].

- Güvenli, saldırılara karşı dirençli ve güvenilir siber alanın sağlanması,
- Bilişim sistemleri yordamıyla ekonomik ve sosyal refahın, güvenli iş ortamı ve ekonomik büyümenin teşviki,
- Bilişim ve iletişim teknolojilerinin barındırdığı risklerin kontrol altında tutulması,
- Bilişim altyapılarının dirençli hale getirilmesi.

Söz konusu çalışmada Ulusal Siber Güvenliği tasarlarken göz önünde bulundurulması gereken 3 Boyut, 5 Zorunluluk ve 5 İkilemden bahsetmektedir.

Afganistan ve Irak gibi beklenenden uzun süren operasyonlardan çıkarılan dersler ışığında, farklı aktörlerin eşgüdüm içerisinde çalışmasının önemi ve zorlukları daha belirgin bir şekilde ortaya çıkmıştır. Aynı zorluklar ulusal siber güvenlik stratejisinin belirlenmesinde ve uygulanmasında da karşımıza çıkmaktadır. İşte bu yüzden yetki ve sorumluluk verilirken Devlet Boyutu, Uluslararası Boyut ve Ulusal Boyut göz önüne alınmalıdır.

Devlet Boyutu: Ulusal siber güvenlik stratejisi oluşturulurken yargı, kanun koyucu, ticaret, iç işleri, dış işleri, iletişim, ordu vb. devlet kurumları devreye girmektedir. Bu aktörlerin arasındaki eşgüdümün sağlanması ve iş bölümü yapılması en büyük zorluktur.

Uluslararası Boyut: Hiçbir ulusal siber güvenlik stratejisinin uluslararası boyutu göz ardı etmediği su götürmez bir gerçektir. İnternetin kendisinin de herhangi bir devlete ve kuruma bizzat bağlı olmadığı düşünüldüğünde, USGS hazırlayacak olan ülkelerin sadece diğer ülkeler ve uluslararası anlaşmalar ile değil aynı zamanda ülkeler dışı aktörlerin bizatihi katılımı ile yapılacak anlaşmalara üye olmaları gerekmektedir.

Ulusal Boyut: Bir ülkede bulunan kritik altyapıları işleten şirketler ülke güvenliği için her zaman önemli olmuşlardır. Bu tip aktörlerin artmasıyla USGS'nin kapsamının genişletilmesi doğru orantılı olmak zorundadır.

Ulusal siber güvenlik düşünülürken göz önünde bulundurulması gereken beş zorunluluk kısa şu şekildedir.

1) Askerî Siber Operasyonlar: Ülkenin sahip olduğu bilişim altyapısının korunmasına yönelik siber savunmadır. Siber savunma istihbarat odaklı olup CERT (Computer Emergency Response Team) tarzı, acil durumlara müdahaleye imkân sağlayan bir organizasyonel yapı gerektirmektedir. İkinci askerî beceri düşman unsurların bilişim altyapılarına stratejik nitelikli siber operasyonlar yapabilmektir. Diğer önemli askeri beceri savaş halinde düşmanın sahip olduğu bilişim altyapılarına yönelik siber saldırı gerçekleştirebilmektir. Dördüncü ve son olarak da geleneksel askerî yapıların, bilişim teknolojilerinin sunduğu imkânlardan yararlanılarak modernize edilmesi yoluyla kapasite ve etkinliğinin arttırılmasıdır.

2) Siber Suçlarla Mücadele Edilmesi: Mücadelenin ilk aşaması ulusal ve uluslararası hukuki altyapının oluşturulmasıdır. Bu görev genellikle adalet bakanlıkları aracılığıyla yürütülür. Adalet bakanlıkları ulusal seviyede insan hak ve hürriyetlerini gereğinden fazla kısıtlamayan, caydırıcılığı olan ve polis birimlerine mümkün olduğunca rahat bir çalışma ortamı sağlayan bir hukuki altyapının tesisi için çalışmalıdır. Siber suçların küresel özelliği nedeniyle diğer ülkelerin hukuk sistemlerinin gelişmesine katkı sağlanmalı ve bu alanda işbirliği mekanizmaları geliştirmeye çaba göstermelidir.

3) İstihbarat/Karşı İstihbarat Faaliyetleri: Üçüncü alan olan istihbarat/karşı istihbarat faaliyetleri konusu ilk iki alanla yakından ilişkili olsa da kendine has bir özelliği bulunmaktadır. Günümüzde istihbarat faaliyetleri sadece devlet kurumları arasında değil, ticari sırların çalınması amacıyla özel şirketler arasında da gerçekleşmektedir.

4) Siber Güvenlik Kriz Yönetimi ve Kritik Altyapıların Korunması: Kriz yönetimi becerileri siber saldırılara maruz kaldıktan sonra hasar tespiti, saldırılara karşılık verme, gerekli noktalara acil müdahale ve hasar gören sistemlerin tekrar ayağa kaldırılması gibi kritik fonksiyonlar ihtiva etmektedir. Bu vazifeler genellikle ulusal CERT birimlerince ifa edilmektedirler. CERT birimlerinin gelişen tehditlere yönelik olarak eğitimli olmaları ve güvenlik birimleriyle işbirliği yapmaları önemlidir. Kritik altyapıların korunması öncelikli olarak ulusal çapta bir risk analizinin yapılarak, risk faktörlerinin düzenli olarak güncellenmesini gerektirmektedir. İkinci olarak kritik altyapılara yönelik standartlar geliştirilerek gerekirse kanunlar aracılığıyla özel ve kamuya ait kritik altyapıların bu standartlara kavuşturulması gerekmektedir.

5) Siber Diplomasi ve İnternetin Yönetimi: Önceki bölümlerde belirtildiği gibi uluslararası hukukta siber alana özgü bağlayıcı nitelikte bir metin bulunmamaktadır. Siber alan yeni yeni şekillenmekte olduğundan, özellikle güçlü devletler bu yeni alana ilişkin kuralların kendi ulusal çıkarlarıyla paralel olması için sürekli girişimlerde bulunmaktadırlar. Bu sebeple, ulusal menfaatlere ters bir takım gelişmelerin yaşanmaması için siber diplomasiye önem verilmelidir. Diğer bir konuysa internet ve internete yön veren politika ve standartlardır. İnternet, kuruluşundan bu yana herhangi bir devletin veya özel kuruluşun doğrudan etkisi altına girmemiştir. Merkezi bir yapının olmayışı her türlü fikrin özgürce ifade edildiği bir ortamın oluşmasına katkı sağlamakla birlikte, internetin güvenliğini olumsuz yönde etkilemektedir. İnterneti daha güvenilir bir hâle getirmek içinse şirketler ve bağımsız kuruluşlarca güvenli iletişim protokollerinin ve standart işlemlerin geliştirilmesi yönünde çalışmalar yapılmaktadır. Bu çalışmalar internetin geleceğinin şekillenmesinde etkili olabileceğinden, ulusal güvenlik açısından bu çalışmalara katkı yapmak ve gelişmelerin dışında kalmamak gerekmektedir.

USGS başlı başına bir amaç değil, arzu edilen koşulların sağlanması için hazırlanan/kullanılan bir araçtır. Ülkeler ekonomik potansiyellerini tam kapasiteli kullanmak ve vatandaşlarını iç ve dış risklerden korumak için stratejik hedeflerini tanımlamaktadır. Uluslararası ilişkilerde güvenlik ikilemi (security dilemma) olarak adlandırılan durumun ulusal siber güvenlik stratejisindeki şekli biraz farklılık arz etmektedir. Ulusal Siber Güvenlikteki göz önünde bulundurulacak beş ikilem şunlardır:

- Ekonomiyi canlandırma - Ulusal güvenliği arttırma.
- Altyapı modernizasyonu - Kritik altyapı güvenliği.
- Devlet - Özel sektör.
- Veri güvenliği - Bilgi Paylaşımı.
- İfade özgürlüğü - Politik denge.

5.5. Beşinci Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (ISC) Siber Güvenlik Makro Analiz Modeli Önerisi ve Türkiye'nin Analizi

Değişen güvenlik anlayışı içerisinde, siber savaşa karşı stratejik planlamanın rolünün önemini vurgulamak ve ülkelerin siber güvenlik analizlerinin yapılabilmesi amacıyla; ŞENTÜRK, ÇİL ve SAĞIROĞLU tarafından yedi temel gösterge ve ilgili alt göstergeleri kapsayan bir analiz modeli önerilmiştir [65]. Yedi temel gösterge şu şekildedir:

1) Ulusal Siber Güvenlik Stratejisi,
2) Eylem Planları ve Ulusal Raporlar,
3) Yasal Mevzuat,
4) Sorumlu Kurum/Merkez ve İlgili Organizasyonlar,
5) Siber Güvenlik Programları,
6) Silahlı Kuvvetler Siber Güvenlik Faaliyetleri,
7) Ulusal/Uluslararası İşbirliği.

Bu 7 temel gösterge ve ilgili alt göstergeler aşağıda genel olarak bahsedilmiştir.

Ulusal Siber Güvenlik Stratejisi: Makro düzeyde siber güvenliğin en önemli boyutu stratejik planlamayı da kapsayan stratejik yönetimdir. Siber tehdide karşı konulması için yapılması gereken ilk şey stratejik hedefleri ve hedeflere ulaşılması gereken tedbirleri kapsayan bir Ulusal Siber Güvenlik Stratejisi hazırlamaktır.

Eylem Planları ve Ulusal Raporlar: Belirlenen ulusal strateji doğrultusunda tespit edilen stratejik hedeflere ulaşılması amacıyla stratejik planlamalar yapılmalıdır. Siber güvenlik planlarının da hükümet kurumları ve bakanlıklar tarafından, gerek bağımsız bir doküman olarak hazırlanıp hazırlanmadığı gerekse de mevcut stratejik planlara dâhil edilip edilmediği hususu incelenmelidir.

Yasal Mevzuat: Düzenlenmemesi durumunda ülkelerin, siber güvenliklerinin sağlanmasında en önemli problem sahası olarak ortaya çıkmaktadır. Yapılacak yasal düzenlemelerin uluslararası arenada geçerliliğinin sağlanması gerekmektedir.

Sorumlu Kurum/Merkez ve İlgili Organizasyonlar: Bu ana gösterge ile ülkenin siber güvenliğinin sağlanması amacıyla gerekli teşkilat yapılarının oluşturulup oluşturulmadığı incelenmelidir.

Siber Güvenlik Programları: Belirlenen eylem planlarının gerekli program ve projelere dönüştürülme durumları kamu ve özel sektör bilgi sistemlerinin korunması için gerekli programların uygulanıp uygulanılmadığı, ulusal düzeyde bilinçlendirme, farkındalığı artırma ve eğitim programları yapılıp yapılmadığı ve yürütülen programların değerlendirilmesinin ne ölçüde yapıldığı incelenmelidir.

Silahlı Kuvvetler Siber Güvenlik Faaliyetleri: Bu ana gösterge, siber güvenliğe, 21'inci yüzyılın savaş türü olan siber savaş boyutu açısından yaklaşılarak belirlenmiştir. Siber uzayda alınan tüm elektronik sistemlere karşı askeri tedbir alınması gerektiği, sadece savunma değil saldırı amaçlı yetenek geliştiren ülkeler de olduğu değerlendirildiğinde, ülkelerin bu bağlamdaki faaliyetleri incelenmelidir.

Ulusal/Uluslararası İşbirliği: Ulusal çapta icra edilen faaliyetlerin tek bir merkezden yönetilmesi ve gerekli koordinasyonun sağlanması, yürütülen faaliyetlerin ortak bir amaca hizmet etmesi, etkilerinin toplam faydayı artıracak şekilde sinerji yaratması, ayrıca uluslararası alanda devam eden faaliyetlere katılım sağlanarak, gerekli işbirliği ve koordinasyonun sağlanması, ulusal siber güvenliğin yapı taşlarından birisidir.

5.6. Bilgi Güvenliği Derneği (Ulusal Bilgi Güvenliği Stratejisi)

Bilgi Güvenliği Derneği tarafından Türkiye'nin Ulusal kapsamda siber güvenliğe yönelik ilkelerini, stratejik hedeflerini, bu hedeflere ulaşmak için ele alınması gereken temel uygulamaları ve ilk planda atılması gereken somut adımları özetleyen bir diğer çalışmada; orta ve uzun vadede dikkate alınması gereken bazı konular ve adımlar genel başlıklarıyla şu şekildedir [66].

Uluslararası İşbirliği: İnternetin sayesinde dünyanın her yerinden herhangi bir kuruma ya da ülkeye kolaylıkla saldırı gerçekleştirilebiliyor olması ülkeler arasındaki işbirliğini zorunlu hale getirmiştir. Ülkemizin müttefik ülkelerle dil birliğini azami seviyede tutmak, BM, AB, OECD ve NATO gibi örgütler bünyesinde çalışmalara destek vermek ve katılmak, bölgesel ve küresel anlaşmalara taraf olmak, yapılan konferans, çalıştay, seminer gibi uluslararası aktivitelere katılmak gerekliliği önem arz etmektedir.

Siber Güvenlik Kültürünün Oluşturulması: Özellikle kritik altyapı sistemlerinden başlayarak kamu kurum ve kuruluşlarının yönetici, personeli ve teknik hizmet personeli siber güvenlik tehdit/saldırılar konusunda eğitilmeli ve bilinçlendirilmelidir.

Yasal Düzenlemeler: Uluslararası hukuk kuralları, kamu yararı, kritik altyapı sistemlerinin korunması ve kişisel veri güvenliğinin sağlanması amacıyla siber suçlarla mücadele kapsamında caydırıcı yasal yükümlülükler getirilmeli ve uygulanmalıdır. Yasal düzenlemeler yapılırken kişisel verilerin korunması, herkesin bilgi edinme hakkının korunması ve bilgi güvenliği unsurları kapsamında gerekli tedbirlerin alınmasının önemi gibi kritik konular da göz önünde bulundurulmalıdır.

Kurumsal Yapılanma: Mücadelenin ve savunmanın koordineli bir şekilde yapılması için bir takım kurumsal yapılanların oluşturulmasına önem verilmelidir. Ulusal siber güvenlik merkezi, müdahale merkezi ve strateji belirleme kurumu gibi yapılar oluşturularak hükümet, devlet kurumları ve sivil oluşumlar arasında iş birliği ve koordinasyon sağlanmalıdır.

Eğitim: Siber güvenlikte en önemli ve en zayıf halka olan bireylerin siber güvenlik konusunda eğitilmesi gereklidir. Teknik personelin yetiştirilmesi için gerekli lisans ve lisansüstü eğitim programları açılmalı ve personel bu konuda teşvik edilmelidir.

Kamu, Üniversite ve Özel Sektör İşbirliği: Ar-Ge çalışmalarının yapılması, sektörler arası işbirliğinin arttırılması ve akademik programların yaygınlaştırılmasının yanı sıra kamu-özel sektör, kamu-üniversite ve üniversite-özel sektör arasındaki işbirliğinin teşvik edilmesi ve çalışma ortamlarının sağlanması gereklidir.

Millî Teknoloji Geliştirme: Bilgi teknolojilerinde özellikle siber güvenlik alanında kullanılacak yazılım ve donanımların uluslararası standartlara uygun olarak sermaye ve iş gücüyle üretilmesini teşvik etmek ve millî ürünlerin kullanım tercihi önem arz etmektedir.

Belgelendirme: Bilgi teknolojileri üreten/kullanan kurum ve kuruluşların uluslararası güvenlik sertifikaları ile belgelendirilmiş olmasına özen gösterilmelidir. Kamu kurumlarının belgelendirme konusundaki eksiklikleri giderilmelidir.

5.7. Değerlendirme

Dünya üzerinde en çok siber saldırıya uğrayan ülkelerin başında gelen İngiltere, ABD ve Türkiye'nin [67] siber güvenlik strateji belgeleri ve eylem planlarının inceleneceği beşinci ve altıncı bölümlere esas teşkil etmek üzere, yapılan çalışmalar ışığında incelenecek hususlar aşağıda belirtilmiştir:

- Strateji belgelerinin içerik ve kapsam açısından ele alınması,
- Kritik altyapıların tanımlanması ve korunması,
- Kamu-özel sektör işbirliği,
- Siber güvenlikten sorumlu kurumlar ve kurumsal yapılanma,
- Yasal mevzuat ile ilgili yapılan çalışmalar,
- Eğitim, kapasite attırımı ve farkındalık çalışmaları,
- Uluslararası işbirliği sağlanması,
- Ar-Ge faaliyetleri
- Acil müdahale ekipleri,
- Diğer hususlar.

Dünyada ve ülkemizde yapılan çalışmaların incelenmesi sonucu, stratejinin hazırlanması ve uygulaması ile ilgili olarak farklı yaklaşımlar dikkat çekmekle beraber temel olarak yapılması gereken faaliyetler birbiri ile örtüşmektedir. Önceki bölümlerde de belirttiğimiz gibi siber güvenlik stratejisi geliştirmek, idame ettirmek ve uygulamak birden fazla kurumun, özel sektörün ve vatandaşın ortaklaşa göstereceği gayret ile başarılabilir.

6. İNGİLTERE VE ABD'NİN SİBER GÜVENLİK STRATEJİLERİNİN İNCELENMESİ

6.1. İngiltere

Her gün İngiltere'de milyonlarca insanın siber uzayın sunduğu servislere ve bilgilere muhtaç olduğu, siber uzayın etkili kullanımının hayati öneme sahip olduğu vurgusu yapılarak ve Haziran 2009'da Hükümet tarafından yayımlanan Digital Britain [68] raporunda belirtilen "İngiltere'nin, dünyanın önde gelen dijital bilgi ekonomilerinden biri olma durumunun devamını sağlama" amacına ulaşmanın gereği olarak ilk strateji belgesi [69] 2009 yılında yayımlanmıştır. Bu doküman İngiltere Devletinin siber uzayın güvenliğini, emniyeti ile direncini sağlamak ve siber uzayın sağladığı olanaklardan faydalanmak amacıyla neler yapacağını bildirmektedir [69].

6.1.1. Genel bakış

Haziran 2009'da yayımlanan Ulusal Güvenlik Stratejisinde İngiltere; ulusal güvenliği tehdit edebilecek aktörleri istikrarsız ülkeler, ülkeler arasında çıkabilecek çatışmalar, uluslar-aşırı organize suçlar ve doğal afetler olarak betimlerken; tehdit edilebilecek alanları nükleer ve diğer kitlesel imha silahları, siber uzay, kamuoyu, kültür ve bilgi olarak tanımlamıştır [70]. Ulusal Güvenlik Stratejisi Raporu, açık bir şekilde, farklı ülkelerin İngiltere'ye siber saldırılar düzenlediğini belirtmekte ve siber güvenliğin, raporun düzenlendiği yıl ve onu izleyen beş yıl boyunca en yüksek dereceli ulusal güvenlik risklerinden biri olarak değerlendirilmesi gerektiğinin altını çizmektedir [71]. Siber uzayın sağladığı ekonomik ve sosyal faydaların tamamının güvenliğini sağlamak için siber güvenliğe yaklaşımını değiştirmek zorunda kalındığı 2011 yılı strateji belgesinde açıkça ifade edilmiştir.

İlk yayımlanan stratejiden farklı olarak 2011 yılı strateji belgesindeki vizyonda zaman kısıtı yer almaktadır. Dört yıllık süre için hazırlanan strateji belgesinde *vizyon*: "Temel değerlerimiz olan özgürlük, adalet, şeffaflık, hukukun egemenliği, refahın arttırılması, ulusal güvenlik ve güçlü toplum güdümlü; canlı, sağlam ve güvenli siber uzaydan muazzam ekonomik ve sosyal değer elde etmektir." olarak tanımlanmıştır [72].

İngiltere'nin Siber Güvenlik Stratejisinde dört adet hedef bulunmaktadır. Bunlar:

1) Siber suçu engellemek ve İngiltere'yi siber uzayda ticaret yapılabilecek en güvenli ülkelerden biri yapmak,
2) İngiltere'yi siber saldırılara karşı daha dirençli yapmak ve ülke çıkarlarını siber uzayda korumak,
3) Vatandaşların güvenli olarak kullanabileceği açık, istikrarlı ve sağlam siber uzayın şekillendirilmesine yardım etmek,
4) Tüm siber güvenlik hedeflerine temel teşkil edecek bilgi, kabiliyet ve kapasiteye sahip olmaktır.

Bu hedefleri gerçekleştirmek maksadıyla dört yıllık süre zarfında kullanılmak üzere 650 milyon pound bütçe ayrılmıştır. Strateji raporu sadece siber güvenliğin teknoloji boyutunu değil, özellikle devletin, özel sektörün ve internetten faydalanan halkın davranışını ve yaklaşımını değiştirmeyi amaçlamaktadır [73]. Bu kapsamda ilkeler;

- Hassas ve siber atakların tespit edilmesinin çok güç olduğu, küreselleşen dünyanın tamamını saran sistemlerin tamamının güvenli olamayacağı gerçeğini göz önünde bulundurarak, risk tabanlı,
- Sadece devletin tüm sistemleri korumasının imkânsız olduğu, çoğu altyapının özel sektör tarafından korunmasına ihtiyaç duyulduğu ve devletin kendi limitlerinin farkında olduğu,
- Aynı şekilde sadece ülke sınırları içerisinde alınacak tedbirlerle güvenliğin sağlanamayacağı ve ülkeler arası yardımlaşmanın da ilerlemenin temelini oluşturacağı işbirliği içerisinde,
- Ulusal ve uluslararası kanunlara saygılı, her bireyin temel hak ve özgürlükleri doğrultusunda siber uzayı kullanabilmesi için güvenliğin özgürlük ve mahremiyetle dengeli olması şeklindedir [72].

6.1.2. Kritik altyapı tesisleri

İngitere'de kritik altyapı, "zarar görmesi halinde hayat kaybına yol açabilecek, ulusal ekonomi üzerinde önemli etki doğuracak, toplumun önemli bir kısmını ve hükümetin işleyişini önemli ölçüde etkileyecek, İngiltere'nin ekonomik, politik ve sosyal yaşantısına tesir eden mal varlıkları, hizmetler ve sistemler bütünü" olarak tanımlanmıştır [73]. İngiltere'nin kritik altyapı tesisleri; İletişim, Acil Servisler, Enerji, Finansal Hizmetler, Gıda, Kamu Hizmetleri, Sağlık, Ulaşım ve Su olmak üzere 9 sektörde kategorize edilmiştir [74].

Kritik altyapı tesislerine tehdit olarak siber saldırılar, casusluk ve terörizmin arkasından üçüncü sırada yer almaktadır. 2010 yılında 121 milyar pound değerindeki (İngiltere'nin gayri safi milli hâsılasının yaklaşık %8'i) internete bağlı ekonomiden kaynaklı siber suçun (çoğunlukla özel sektörde gerçekleşen) yıllık maliyeti tahmini olarak 18 ila 27 milyar pound tutarındadır. Siber suçlar vatandaşa 3,1 milyar pound, devlete 2,2 milyar pound ve özel sektöre 21 milyar pound olacak şekilde yıllık maliyete sebep olmaktadır [73, 75-77].

İngiltere'de kritik bilgi altyapısının korunması konusundaki sorumluluk İçişleri Bakanlığına ait olmakla birlikte, uzman desteği sağlamak ve katkıda bulunmakla görevli birçok kurum vardır. Bu katkı ve destekler Ulusal Altyapı Koruma Merkezi (Center for the Protection of National Infrastructure, CPNI) tarafından koordine edilmektedir [78].

6.1.3. Kamu-özel sektör işbirliği

CPNI, kritik bilgi altyapısının sahibi olan ya da kritik bilgi altyapısını işleten ticari işletmelere ve kuruluşlara bilgi, personel ve fiziksel destekten oluşan güvenlik tavsiyelerinde bulunmaktadır. Ayrıca kritik altyapının terör saldırılarına ve diğer tehlikelere karşı korunması, güvenlik açıklıklarının azaltılması suretiyle güvenliğin sağlanması amacıyla kamu kurumlarıyla, üniversitelerle, özel sektörle ve istihbarat sağlayan kurumlarla işbirliği içerisinde hareket etmektedir [78]. Ayrıca bu kuruma karşılıklı fayda sağlayacak şekilde, ulusal altyapılar üzerinden güçlü ortaklıklar kurması gerektiği strateji belgesinde belirtilmiştir [72].

CPNI bünyesinde faaliyet gösteren Uyarı, İhbar ve Raporlama Noktaları (Warning, Advice and Reporting Point, WARP) oluşturulmuştur. Bu noktalar; özel sektörle zafiyetlerin, güncel bilgilerin, tehditler ve bu tehditlere karşı çözümlerin paylaşımının yapılabilmesi maksadıyla, uygun maliyetli, güvenli ortam sağlamaktadır [79].

Bunların yanı sıra, kamu-özel sektör bilgi paylaşımı sağlamaya yönelik olarak çalışan kurum ve kuruluşlar bulunmaktadır. Bunlardan bazıları şöyledir:

- Bilgi Güvencesi Dayanışma Konseyi,
- İngiliz Bilgisayar Topluluğu,
- İnternet Güvenliği Forumu,
- Ulusal Bilgi İşlem Merkezi,
- İnternet İzleme Kurumu,
- İngiltere Sanayi Konfederasyonu,
- Bilgi Güvenliği Uzmanları Enstitüsü,
- Avrupa Bilgi Toplumu Grubu,
- Chatnam Evi,
- Kraliyet Birleşik Hizmetler Enstitüsü.

6.1.4. Sorumlu kurumlar

İngiltere'nin siber güvenlik strateji belgesinde halka, özel sektöre ve devlete düşen sorumluluklar açıkça belirtilmiştir. Verilen görevler kısaca şunlardır:

<u>Halkın Görevi</u>

- Çevrim içi gerçekleşebilecek tehditlerden karşı temel seviyede nasıl korunacağını bilmek,
- İnternete kişisel ve hassas bilgi koyulmaması konusunda dikkatli olmak,
- İşte veya evde tehditleri tanımlama konusunda yardımcı olmak,
- Özel sektör ve devlet ile ilgili işlemleri yaparken şifrelerini korumak, yazılım, işletim sistemleri ve bilgisayarları tehditlerden koruyacak anti-virüs programlarının güncellemelerini yapmanın önemini anlamak gibi üzerine düşen görevleri yerine getirmek ve siber uzaydaki sorumlulukların bilincinde olmaktır.

Özel Sektörün Görevi

- Ticarî olarak hassas bilgi, fikri mülkiyeti ve müşteri bilgilerini koruyacak şekilde siber uzayı kullanmak ve tehditlerin bilincinde olmak,
- Siber uzayda karşılaşılacak tehditleri bertaraf edebilmek için devlet ve kanun uygulayıcılar ile işbirliği içinde çalışmak,
- İngiltere ile dünyanın canlı ve yenilikçi siber güvenlik servislerine olan artan ihtiyacını karşılayacak şekilde sermaye sağlamak,
- Gelecekte ihtiyaç duyulacak siber güvenlik yeteneklerini sağlamak maksadıyla, mükemmeliyet merkezleri yaratmak ve yatırım yapmaktır.

Devletin Görevi

- Yüksek riskli tehditleri tespit ve engellemek için kapasiteyi arttırmak,
- Siber uzayda uluslararası konsensüste 'davranış normlarını' şekillendirmeye yardımcı olmak,
- Kritik altyapı tesislerinde ve devlet sistemlerindeki hassasiyeti azaltmak,
- Siber güvenlik konusunda çalışanların kadrosunu arttırmak,
- Kanunun uygulanmasını sağlamlaştırmak ve siber suçu engellemek,
- Halkın farkındalığını arttırmak,
- Özel sektörün farkındalığını arttırmak,
- İş olanaklarından faydalanmaktır.

Devlet kurumlarına stratejik hedefler ile ilgili olarak verilen görevler ve sorumluluklar Çizelge 6.1'de açıkça belirtilmiştir.

6.1.5. Yasal mevzuat

İngiltere'de bilişim suçları, 29 Haziran 1990 tarihli Bilgisayarların Yanlış Kullanımı Kanunu (Computer Misuse Act, CMA) ile düzenlenmiştir. Üç bölümden ve 18 kısımdan oluşan CMA'da; yetkisiz şekilde bilgisayara girmek, sistem içerisinde değişiklik yapmak veya benzeri müdahalelerde bulunmak suç sayılmıştır [80].

Çizelge 6.1. Stratejik hedefler ve sorumluluklar

HEDEF	ORGANİZASYON	SORUMLULUKLAR
Siber suçu engellemek ve İngiltere'yi siber uzayda ticaret yapılabilecek en güvenli yerlerden biri yapmak	İçişleri Bakanlığı, Organize Suç Birimi, Çocuk İstismarı ve Çevrimiçi Koruma, Polis Merkezi Elektronik Suç Birimi, polis kuvvetleri, Ulusal Dolandırıcılık Birimi Ticaret, Yenilik ve Yetenek Dairesi, Teknoloji Strateji Meclisi, Ticaret ve Yatırım Bakanlığı	Siber suçu engellemek • Online hassasiyeti azaltmak • Online suç faaliyetlerini azaltmak • Etkili ortaklığı teşvik etmek. Ticaret yapılabilecek güvenli hale getirmek • Farkındalığı ve tehditlerin görünürlüğünü arttırmak • Anında müdahaleyi geliştirmek • Bilgi ve servisleri korumak • Risk yönetimi kültürünü geliştirmek • Siber uzay güvenini teşvik etmek
İngiltere'yi siber saldırılara karşı daha dirençli yapmak ve ülke çıkarlarını siber uzayda korumak	Kabine Ofisi, İstihbarat ve Güvenlik Birimleri Savunma Bakanlığı	Kritik altyapıyı koruma • Siber uzay savunmasını kuvvetlendirme • Direnci arttırma ve siber saldırıların etkilerini azaltma • İnternetin terörist amaçlı kullanımını takip etmek Ülke çıkarlarını korumak • Siber uzaydaki tehditleri tespit yeteneklerini arttırma • Saldırıları engelleme ve caydırma kabiliyetini arttırma
Vatandaşların güvenli olarak kullanabileceği açık, stabil ve sağlam siber uzayın şekillendirilmesine yardım etmek	Kültür, Medya ve Spor Dairesi Dışişleri Bakanlığı	Siber uzayın geliştirilmesine yardım etmek • Açık ve birlikte çalışılabilir siber uzayı teşvik etmek • Temel hak ve özgürlükleri sağlamak Yaşam şeklimizi korumak • Değerlerimizden ödün vermeden güvenliği sağlama
Tüm siber güvenlik hedeflerine temel teşkil edecek bilgi, kabiliyet ve kapasiteye sahip olmak	Ticaret, Yenilik ve Yetenek Dairesi Ticaret, Yenilik ve Yetenek Dairesi Kabine Ofisi	Bilgiyi arttırmak • Tutarlı araştırma planı geliştirmek • Tehditleri, zafiyetleri ve riskleri anlamak Yeteneği arttırmak • Riskleri anlama kültürü inşa etmek • Her seviyedeki yeteneği geliştirmek Kapasiteyi arttırmak • Teknik kapasiteyi arttırmak • Olaylara anında tepki kabiliyetini arttırmak

CMA, aşağıdaki bölümler içerisinde yer alan üç temel suç tipini içermektedir.

Birinci bölümde, bir bilgisayara veya bunun içerindeki herhangi bir veri veya programa kasten yetkisiz erişme suç sayılmıştır. İkinci bölümde, birinci bölümdeki kast altında, kendisi veya başkası tarafından gerçekleştirilecek başka bir suçun işlenmesini kolaylaştırmak amacıyla bilişim suçunun işlenmesidir. Üçüncü bölümde, herhangi bir bilgisayardaki içeriğin yetkisiz şekilde değiştirilmesi ya da bilgisayarın çalışmasının bozulması veya bilgisayara ya da içerisindeki programa veya veriye erişimin engellenmesi veya bunlarda değişiklik yapılması suç sayılmıştır [81].

İngiliz hukukunda bilişim suçlarını düzenleyen bu yasa dışında özellikle pornografi ve çocuk pornografisi alanına ilişkin düzenlemeler yapılmıştır. 1964 tarihli "Müstehcen Yayınlar Kanunu" ve 1984 tarihli "Telekomünikasyon Kanununda" yapılan değişikliklerle, "yayınlama" teriminin kapsamına bilişim sisteminde bulunan veriler de dâhil edilmiş, böylelikle sanal alanda yapılan pornografik yayınlar düzenlenmek istenmiştir [82].

İngiltere'de, 1978 tarihli "Çocukların Korunması Kanunu'nda" yer alan "fotoğraf" tanımı, 1994 tarihli "Ceza Adaleti ve Kamu Düzeni Kanunu" ile sanal alanda sayısal formda veri halinde bulunan resimleri de kapsayacak şekilde değiştirilmiş, böylelikle internette veri halinde bulunan çocuk pornografisi resimleri ve bunların montajla yapılmış şekillerini bulundurmak suç haline getirilmiştir [83].

1998 tarihli Verilerin Korunması Kanunu (Data Protection Act, DPA) ile bireylere ait bilgilerin elde edilmesi, paylaşılması veya kullanılması da dâhil olmak üzere kişisel bilgilerin işlenmesi düzenlenmektedir. Söz konusu kanun ile AB'nin 1995 tarihli verilerin korunması direktifine uyum sağlanması amaçlanmıştır. Kanun kapsamında bireylere, küçük bir ücret karşılığı bir kurum tarafından kendisi hakkında tutulan bilgileri görebilme, yanlış olan bilgilerin düzeltilmesinin isteme, bilgilerin zarar verici veya kanuna aykırı amaçlarla kullanılmasını engelleme gibi haklar verilmektedir [78]. Bu kanunda kişisel verilerin korunmasına ilişkin ilkeler yer almaktadır [84].

Bu ilkeler aşağıdaki gibidir:

- Kişisel verilerin adil ve kanunlara uygun olarak işlenebilmesi,
- Kişisel verilerin sadece bir veya daha fazla kanuna uygun ve belirli amaçla elde edilebilmesi,
- Elde edilen kişisel verilerin işlenme amaçlarıyla yeterli, ilgili, orantılı olması, gereğinden fazla bilgi edilememesi,
- Kişisel verilerin doğru ve güncel olması,
- Kişisel verilerin işlenme amacına yetecek süre boyunca muhafaza edilmesi, gerek kalmadığında yok edilmesi,
- Kişisel verilerin güvenli ve gizli tutulması,
- Kişisel verilerin transfer edileceği ülkede o verilerin işlenmesine uygun yeterli düzenleme olmadığı sürece transfer edilememesi.

6.1.6. Eğitim, kapasite artırımı ve farkındalık çalışmaları

Siber güvenlik stratejisinin yayımlanmasını müteakip Kabine Ofisi tarafından takip eden her yılın sonunda ilerleme raporları kamuoyuna açıklanmıştır. Strateji ile ilgili olarak üç senelik süreçte; eğitim, kapasite artırımı ve farkındalık konularında yapılan faaliyetlerden kısaca bahsetmek faydalı olacaktır.

İlk senede;

- İngiliz hükümeti ile silahlı kuvvetlerine bilgi güvenliği ve sinyal istihbaratı sağlamaktan sorumlu olan Devlet İletişim Karargâhı (Government Communications Headquarters, GCHQ) tarafından bilgi güvenliği ve siber güvenlik uzmanlık yeterliliklerini sertifikalandırmak üzere program başlatılmış ve üç yüzden fazla personel sertifikalandırılmış,
- Dünya çapında siber güvenlik araştırmaları yürüten en iyi sekiz üniversite Siber Güvenlik Araştırması Akademik Mükemmeliyet Merkezi (Academic Centre of Excellence in Cyber Securty Research) statüsü verilerek GCHQ tarafından ödüllendirilmiş,
- Siber güvenlik tehditlerinin altında yatan sebepleri incelemek üzere ilk araştırma merkezi kurulmuş,

- Disiplinler arası siber güvenlik konularını kapsayan 48 doktora programı ve Ulusal Siber Güvenlik Programı kapsamında GCHQ sponsorluğunda 30 adet doktora programına fon sağlanmış,
- GCHQ ve diğer istihbarat birimlerinde işe alma fırsatı sağlayacak şekilde üniversite çağındaki öğrencileri siber güvenlik konularında yeteneklerini geliştirmek üzere bir program başlatmış,
- Okullardaki bilgisayar bilimleri öğrenimini güçlendirmek için bilgi ve iletişim teknolojileri müfredatında değişiklik yapılmış,
- Kanun uygulayıcıları, ordu ve sivil hizmetlerde çalışan kişilere siber uzay konusunda eğitim verilmiş,
- 2011 yılı bütçesinden eğitim için 4 milyon pound bütçe ayrılmıştır [85].

İkinci senede;

- İlkokullarda gençlerin teknoloji öğrenmelerini teşvik etmek üzere devlet ve birçok sponsor tarafından desteklenen "Make It Happy" programına 600'den fazla okulun kaydı yapılmış ve 60'dan fazla yarışma başvurusu alınmış [86],
- 10-14 yaş arasında bulunan 135 000 kızı kapsayan Kızlar İçin Bilgisayar Kulübü adı altında, algoritmaların nasıl çalıştığını ve programlama dillerini anlatan yeni bir kod yazma eğitimi başlatılmış,
- Akademik paydaşlarla, Güvenilir Yazılım Girişimi (Trustworhty Software Initiative) kapsamında yazılım tasarım ve geliştirme süreçlerinde güvenlik zafiyetlerini önlemek üzere eğitim materyalleri geliştirilmiş,
- Özel sektör ve akademik paydaşlarla çalışma ortamındaki siber yetenekleri arttırmak üzere Siber Akademi programı desteklenmiş,
- Gençlerin siber kariyer yapmasını teşvik etmek üzere 2010 yılında başlatılan ve 10000'den fazla kişinin yer aldığı Siber Güvenlik Mücadelesi (Cyber Security Challenge) gibi girişimlerde bulunulmuş,
- Farkındalık ve siber yeteneklerin arttırılması amacıyla; Ulusal Arşiv Birimi, Güvenlik ve İstihbarat Birimleri, Kolluk Kuvvetleri, Kraliyet Savcılık Servisi, Savunma Bakanlığı vb. kurumlarda görev yapan yaklaşık 200 000 kişiye eğitim vermiş,
- 2012 bütçesinden 8 milyon pound ayrılmıştır [87].

Üçüncü senede;

- Ulusal Siber Güvenlik Programı (National Cyber Security Programme, NCSP) okullarda 2015 yılında siber güvenlik eğitimi ve eğitim materyalleri alınması için bütçe ayırmış,
- Yüksek Öğretim Akademisi (The Higher Education Academy) Newcastle, Birmingham, Londra ve Liverpool'daki üniversitelerde kullanılmak üzere 135000 pound fon sağlamış,
- GCHQ, siber güvenlik ve şifreleme alanında çalışan gençlere yardım etmek amacıyla, 'Cryptoy' adında uygulama geliştirmiş,
- 200'den fazla başlangıç seviyesinde olan yeni siber güvenlik mesleği yaratılmış,
- 2014 yılı bütçesinden eğitim için 10,7 milyon pound bütçe ayrılmıştır [88].

6.1.7. Uluslararası işbirliği

İnternetin sosyal, politik ve ekonomik açıdan İngiltere için çok önemli olduğu ve topluma karşı tehdit oluşturmasının engellenmesinin gerekliliğini vurgulayan dönemin başbakanı David Cameron, aynı zamanda, siber güvenliğin hükümeti için birincil öneme haiz olduğunu ve bunun sağlanması için polis, güvenlik güçleri, uluslararası paydaşlar ve özel sektörle yakın bir şekilde çalışılması gerekliliğinin üzerinde durmuştur [89,90].

Bu bağlamda, uluslararası paydaşları Avrupa Konseyi bünyesinde hazırlanarak 23 Kasım 2001 tarihinde Budapeşte'de imzaya açılan ve 1 Temmuz 2004 tarihinde Sanal Ortamda İşlenen Suçlar Sözleşmesini daha çok ülkenin imzalaması ve siber suçla mücadele kapsamında uluslararası işbirliğini arttırmaya çaba göstermektedir [85]. Ulusal Suç Ajansının (National Crime Agency, NCA) bir birimi olarak Ulusal Siber Suç Birimi (National Cyber Crime Unit, NCCU) kurulmuştur. NCCU, İngiltere ve dünyada siber güvenlikle ilgili uzman kurum/kuruluşlarla siber suçluları yakalamak için beraber çalışmıştır. Kurulmasını takip eden birkaç hafta içerisinde, ABD Federal Soruşturma Bürosu (Federal Bureau of Investigation, FBI) ile ortak yürüttükleri bir müşterek operasyonda, kişileri ve işletmeleri tahmini olarak 200 milyon dolarlık zarara uğratan 11 kişinin tutuklanmasını sağlamıştır [86].

NCCU hali hazırda ABD, Avustralya ve Avrupa'daki birçok ülke ile müşterek siber soruşturma modelleri geliştirme ve siber suçları kaynağından itibaren engelleme üzerine çalışmalar yürütmektedir. Ayrıca, İngiltere Hükümeti AB üyesi ülkelerle Şubat 2013'te yayımlanan AB Siber Güvenlik Stratejisini geliştirmek üzere işbirliğine devam etmektedir. İnternetin geleceğini ve siber uzayda davranış normlarını belirlemek üzere 2011 yılında Londra Konferansı düzenlemiştir. Oxford Üniversitesinde kurulan Küresel Siber Güvenlik Kapasite Merkezinde diğer ülkeler ve organizasyonlara etkili olarak siber kapasitelerini oluşturma yolunda çalışmalar sürdürülmektedir [86]. 2013 yılı içerisinde Hindistan, Japonya, Kore ve Singapur ile resmi olarak siber diyaloglar kurulmuş, gelecek yıllarda Brezilya, Şili ve Güney Afrika ile görüşmelerin yapılması planlanmaktadır [87].

Hali hazırda NATO Siber Güvenlik Mükemmeliyet Merkezindeki çalışmalara katkı sağlayan İngiltere; uluslararası işbirliği ile ilgili olarak 2011/2012 döneminde 2 milyon pound, 2013/2014 döneminde 2,2 milyon pound harcanmış, 2014/2015 döneminde 2,7 milyon pound harcanması planlanmaktadır [85-87].

6.1.8. Ar-Ge faaliyetleri

Siber güvenlik stratejisinin hedeflerinde dördüncüsü olan "tüm siber güvenlik hedeflerine temel teşkil edecek bilgi, kabiliyet ve kapasiteye sahip olmak" gayesine erişebilmek için İngiltere Hükümeti, sektörler arası tutarlı bir araştırma gündemi takip etmiş ve tehditleri, zafiyetleri, riskleri derinlemesine analiz etme yaklaşımını tercih etmiştir [72]. Bu yaklaşımı izleyebilmek için; siber uzay kullanımını etkileyen teknolojik, yöntemsel ve sosyal davranış kalıplarını analiz kabiliyetlerini arttırmak, her seviyedeki eğitimin nasıl iyileştirilebileceğini tespit etmek, yenilikçi siber güvenlik çözümleri geliştirmenin yollarını tespit etmek, GCHQ'nün üst düzey teknik kapasite ile çalışmasını sağlamak gibi eylem planları takip edilmiştir.

Stratejinin gereği olarak üç yeni araştırma enstitüsü kurulmuştur. Siber Güvenlik Bilimi Araştırma Enstitüsü (The Research Institute in Science of Cyber Security) organizasyonların genel güvenliği üzerine [91], Otomatik Program Analiz ve İnceleme Onaylama Enstitüsü (The Research Institute in Automated Program Analysis and Verification) yenilikçi siber güvenlik araştırmaları ve zafiyetlerin azaltılması üzerine [92], Güvenilir Endüstriyel Kontrol Sistemleri Araştırma Enstitüsü (Research Institute in Trustworthy Industrial Control Systems) ise kritik altyapıların doğru bir şekilde çalışırlığını sağlamak için İngiltere Hükümetinin sağladığı fonlarla kurulmuştur [87, 93]. Söz konusu enstitülere sağlanan fon miktarı sırasıyla 3,8 milyon pound, 4,5 milyon pound ve 2,5 milyon pound tutarındadır [91-93].

İki adet doktora eğitim merkezinde toplam 96 adet doktora programı, 11 adet üniversitede siber güvenlik mükemmeliyet merkezi, ayrıca İsrail ve Singapur ile ortak olarak mali destek sağlanan araştırma işbirliği başlatılmıştır [87,88]

6.1.9. Acil müdahale ekipleri

CPNI, güvenliğe ilişkin tehditler karşısında ne şekilde tepki verileceğinin ve bu durumların nasıl yönetileceğine ilişkin tavsiyelerde bulunmak amacıyla kritik altyapı sahipleri ve işletmecileri için Müşterek Güvenlik Olayları Müdahale Ekibini (CSIRTUK) oluşturmuştur [78]. 2014 yılının Mart ayında İngiltere Ulusal Bilgisayar Acil Müdahale Ekibi (UK National Computer Emergency Response Team, CERT-UK) teşkil edilmiştir [94]. CERT-UK, İngiltere'nin ulusal siber güvenlik olaylarına karşı hazırlık durumunu sağlamak ve idare etmekten sorumludur. Bu görev, devlet kurumları ve endüstriyel paydaşlarla tatbikatlar düzenlemek; özel sektör ve akademik kuruluşlar ile bilgi paylaşımı faaliyetlerini kapsamaktadır.

6.1.10. Diğer hususlar

Stratejik hedefler ile ilgili olarak devlet kurumlarına verilen görevler ve sorumluluklar Çizelge 6.1'de görülmektedir. Tüm aktörleri (Devlet, özel sektör, halk) ilgilendiren minimum çalışma standartları ve prensipleri de belirlenmiştir [95].

Her çapta ve her sektördeki organizasyonun siber tehditlere karşı korunmasını sağlamak maksadıyla temel hedefleri belirleyen Siber Gereksinimler (Cyber Essentials) oluşturulmuştur [96]. Sadece özel sektörü değil, aynı zamanda üniversiteleri, sivil toplum kuruluşları, kamu sektörü organizasyonlarını da kapsayan Siber Gereksinimleri yerine getiren firmaların İngiliz Hükümetinin ortaya koyduğu siber güvenlik yönetmeliğine karşı duyarlı olduğu ve hükümet onaylı standartları yerine getirdiği değerlendirilmektedir. 1 Ekim 2014 tarihi itibariyle kişisel verilere erişecek ve bazı ürün ile servisleri sağlayacak firmaların bu şartları sağlamaları zorunlu hale getirilmiştir [96]. İngiliz Güvenilir Yazılım Girişimi tarafından hazırlanan PAS 754 şartnamesi ile organizasyonların güvenilir yazılımları ayırt edebilme ve kullanabilme süreçleri tanımlanmıştır [95,97].

Bazı hükümet organları ile internet servis sağlayıcıları arasında internetten faydalanan halkın çevrim içi tehditlere karşı korunması, eğitilmesi, bilgilendirilmesi gibi hususları kapsayan prensipler belirlenmiştir [95,98]. Bu prensipler internet servis sağlayıcılarının kullanıcıları siber tehditlere karşı korunmasını sağlayacak faaliyetler, hükümetin tüketiciler ile sektörü korumaya yardımcı olacak aktiviteleri ve hükümet ile internet servis sağlayıcıların kullanıcılar ile sektörü korumaya yönelik beraber yapacakları faaliyetleri kapsayan üç ana başlık altında belirtilmiştir [98]. Ayrıca bakanlar, üst düzey yetkililer ve kanun koyucular siber sistemlerin ve ağların önemini vurgulayan, söz konusu sistemlere yapılacak saldırıların yaratacağı kaos ortamını engellemek maksadıyla, hükümet tarafından yapılması planlanan eylemleri sıralayan bir politika belgesi yayımlamışlardır [99]. Bu belgede firmalara ve pazarlara siber güvenliğin entegre edilmesi için yapılması gerekenler, alınması gereken önlemler açıklanmıştır.

Hükümet tarafından üst düzey İngiliz firmalarının siber risklerle nasıl mücadele edeceğini gösteren [100] ve bilgi güvenliği güvenlik açıklarını detaylı bir şekilde anlatan [101] raporlar yayımlanmıştır. Ayrıca, Ulusal Siber Güvenlik Programı ile otuz adet uluslararası projeye yıllık olarak iki milyon pound tahsis edilmiştir. Oxford Üniversitesindeki merkez (The Global Cyber Security Capacity Centre) dünya üzerindeki diğer ülke ve organizasyonların siber kapasitelerini arttırmasını hedeflemektedir [102].

2011 yılında yayımlanan siber güvenlik strateji raporunu destekleyecek şekilde örnek olarak, bir sene süre içerisinde icra edilen faaliyetler aşağıda sunulmuştur [85].

- Özel sektör ve devlet kurumları arasında bilgi paylaşımını sağlayacak olan "Hub"'ın kurulumu tamamlanmıştır.
- Action Fraud'a (İngiltere'nin sahtecilik ve finansal tabanlı suçlarının rapor edildiği ulusal merkez) yaklaşık olarak 292 milyon pound değerinde 46 000 adet rapor gelmiştir.
- "The Devil's in Your Details" farkındalık kampanyası ile dört milyon kişi bilgilendirilmiştir.
- Çeşitli devlet kuruluşlarında siber suç birimleri açılmıştır.
- 15.000 web sitesi sahtecilik gerekçesi ile kapatılmıştır.
- Gizliliği ifşa edilmiş 2,3 milyon kredi kart bilgilerini ülke içinde ve dışındaki finansal kuruluşlara bildirerek potansiyel olarak 500 milyon pound kaybı önlemiştir.
- Çeşitli görevleri üstlenen kamu kurumları raporlar hazırlayarak bilgilendirme faaliyetlerinde bulunmuşlardır.
- 60 ülkeden 700 den fazla katılımcının iştiraki ile "London Conference on Cyberspace" icra edilmiştir.
- Devlet ve özel sektör paydaşlarının katkılarıyla "Get Safe Online Week" faaliyeti icra edilmiş, söz konusu faaliyet her yılın ekim ayının Küresel Siber Güvenlik Ayı olarak uygulanmasına ön ayak olmuştur.
- Yüksek lisans ve doktora programlarında teşvik uygulanmıştır.

6.2. Amerika Birleşik Devletleri

Amerika siber uzayın oluşturduğu yeni gerçeklere kurumsal tepki veren önder ülkelerden biri olarak görülmektedir. Devlet olarak siber uzayın kurulmasına destek çıkarak ve kullanımını teşvik ederek diğer ülkelere örnek olmuştur. Özellikle Avrupa ve Asya'daki ülkelere siber sorunlar ile başa çıkılması konusunda örnek teşkil ederek bir rol model haline gelmiştir.

6.2.1. Genel bakış

Her ne kadar Amerika siber tehlike ve tehditlere karşı sistem ve altyapısına sahip en güçlü ülkelerden biri olarak görülse de şu anda uygulanmakta olan programlar, sistem ve altyapıların günümüzdeki tehlikelere karşı halen yeterli olmadığı bilinmektedir [71]. Ulusal güvenlik stratejilerinde siber güvenliğe verilen önem [103] ile doğru orantılı olarak ulusal siber güvenliğe yönelik stratejik seviyede dokümanlar hazırlanmıştır. İlk olarak 2001 yılında yaşanan olayları takiben 2003 yılının şubat ayında ABD Başkanı George Bush döneminde "Ulusal Siber Uzay Güvenliğini Sağlama Stratejisi" yayımlanmıştır.

Başkanın önsözünde, siber uzayın korunmasını "federal hükümet, eyalet ve yerel hükümetler ile özel sektör ve halkın koordineli, odaklanmış çabası ile üstesinden gelinebilecek stratejik mücadele" olarak değerlendirmiştir [104]. 2003 yılı stratejisinde temel olarak kapsam belirtilmekte, federal hükümet birimlerine yol gösterilmekte, tüm aktörlere siber güvenliğin geliştirilme yöntemleri ile ilgili bilgi verilmekte ve kamu-özel sektör işbirliğinin öneminden bahsedilmektedir. Üç stratejik amaç (Amerika'nın kritik altyapılarının siber saldırılara karşı korunması, siber saldırılara karşı ulusal hassasiyetin azaltılması ve saldırı sonrası zararın minimum seviyede tutulması) ve beş kritik öncelik (Ulusal Siber Uzay Güvenlik Müdahale Sistemi, Ulusal Siber Uzay Güvenlik Tehdit ve Zafiyet Azaltma Programı, Ulusal Siber Uzay Güvenlik Farkındalık ve Eğitim Programı, Kamu Siber Uzayının Korunması, Ulusal Güvenlik ve Uluslararası Siber Uzay Güvenlik İşbirliği) çerçevesinde İç Güvenlik Bakanlığı (Department of Homeland Security, DHS) sorumlu olarak tayin edilmiştir [104]. Bu stratejinin öncelikli amacı sadece kamuya ait sistemlerin değil özel sektör tarafından işletilen kritik altyapı tesislerinin de siber güvenliğinin arttırılmasıdır [105].

2004 yılında ABD Genelkurmay Başkanlığı tarafından "Ulusal Askerî Stratejisi" yayımlanmıştır [106]. Söz konusu stratejide siber uzayın; kara, deniz, hava ve uzayın yanı sıra bir savaş alanı olarak değerlendirildiği konusuna vurgu yapılmıştır [105]. İki sene sonra yine ABD Genelkurmay Başkanlığı tarafından "Siber Uzay Operasyonları İçin Ulusal Askerî Strateji" yayımlanmıştır [107]. Askerî stratejinin yayımlanma amacı siber alanı, tehdit ve zafiyetleri, ABD Ordusunun siber uzaydaki üstünlüğünün korunması için yapılması gerekenleri tanımlamaktır [105].

2009 yılında Başkan Barack Obama'nın direktifiyle Siber Uzay Politikasının Gözden Geçirilmesi (Cyberspace Policy Review) belgesi yayımlanmıştır [108]. Bu belge sanayi, akademik ve sivil toplum kuruluşları, uluslararası paydaşlar ile kanun koyucu ve uygulayıcı kurumlar tarafından oluşturulmuştur. Siber uzayda gerçekleşen operasyonların strateji, politika ve standartları; tehdit ve zafiyetlerin azaltılması, caydırıcılık, uluslararası işbirliği, acil müdahale, kurtarma politikaları ve eylemleri; ağ operasyonları, bilgi güvenliği, kanuni yaptırımlar, diplomasi; askeri ve istihbarat operasyonlarının küresel bilgi ve iletişim altyapılarının güvenlik ve istikrarı ile ilgilenmektedir. Bu belge, güvenilir ve dirençli dijital altyapının sağlanması için başından sonuna kadar izlenmesi gereken yolu tarif etmektedir.

2008 yılında Başkan George Bush'un talimatıyla hazırlanan Kapsamlı Milli Siber Güvenlik İnisiyatifi (The Comprehensive National Cybersecurity Initiative) gizli tutulmuş ve 2011 yılında Başkan Obama tarafından kamuoyuna ilan edilmiştir [11, 109]. ABD'nin siber uzay güvenliğini sağlamak için bu inisiyatifte; günümüz tehditlerine karşı savunma hattı oluşturulması (farkındalık ve acil müdahale), tüm tehditlere karşı savunma (Karşı istihbarat ve bilgi teknolojilerinin güvenliğinin arttırılması) ve geleceğin siber güvenlik ortamını güçlendirme (Eğitim, Ar-Ge, strateji geliştirme) olmak üzere üç temel hedef konulmuştur [109]. Bu dokümanda on iki adet girişim belirlenmiş ve yapılması gerekenler açıklanmıştır.

ABD Savunma Bakanlığı 2011 yılında siber ortamda faaliyetleri yürütmek ve harekât icra edebilmek için belirlediği beş stratejik girişim ile ilgili bilgi vermek maksadıyla ABD Savunma Bakanlığı Siber Ortamda Harekât Stratejisi (DoD Strategy for Operating in Cyberspace) belgesini yayımlamıştır [11]. Yayımlandığı yıl itibariyle DoD'nin siber uzayı onlarca ülkede yer alan 15.000 adet ağ ve 7 milyon cihaz üzerinde askerî ve istihbarat faaliyetleri ile personel, malzeme hareketlerini ve komuta kontrol sistemleri için kullandığı belirtilmiştir [110].

Söz konusu stratejide belirtilen beş stratejik girişim şunlardır:

- Birinci Girişim: DoD'nin siber uzayın tüm imkanlarından faydalanabilecek şekilde organize edilmesi, eğitimi ve donanımı için tüm siber uzayın harekât alanı olarak değerlendirilmesi.
- İkinci Girişim: DoD ağ ve sistemlerinin korunması için yeni savunma işletim konseptlerinin uygulanması.
- Üçüncü Girişim: Devletin topyekûn siber güvenlik stratejisinin etkinleştirilmesi için, ABD'deki diğer bakanlıklar, kamu kurumları ve özel sektör ile ortak çalışmalar yapılması.
- Dördüncü Girişim: Topyekûn siber güvenliğin güçlendirilmesi için ABD'nin müttefikleri ve uluslararası ortakları ile güçlü ilişkiler kurması.
- Beşinci Girişim: Kalifiye siber işgücü ve hızla elde edilecek teknolojik yenilikler vasıtasıyla milli yeteneklerin geliştirilmesi.

Başkan Barack Obama hükümeti, 2011 yılında daha önce hazırlanmış politika belgelerinden farklı olarak sadece kendi ulusunu değil, dünyadaki uluslararası paydaşlarını da bilgilendirecek şekilde siber uzayın korunması ve karşılaşılacak tehditleri azaltma amacını gerçekleştirmek maksadıyla Siber Uzay İçin Uluslararası Strateji (International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World) belgesi yayımlamıştır [111]. Her geçen gün dijital altyapının; gelişen ekonomiler, güçlü ordular, özgür toplumlar, şeffaf hükümetler, araştırma toplulukları için omurga teşkil ettiği; elektrik-su dağıtımı yapan, hava trafiğini kontrol eden, finansal sistemleri destekleyen kritik altyapıların bilgi sistemlere muhtaç olduğu gerçeği doğrultusunda bu dijital altyapının ülkeler için ulusal varlık olarak değerlendirileceği özellikle belirtilmiştir.

ABD'nin uluslararası stratejideki *amacı*; "uluslararası ticareti destekleyen, uluslararası güvenliği güçlendiren, özgür ifade ve yeniliği teşvik eden, *açık, birlikte çalışan, emniyetli ve güvenilir* bilgi ve iletişim altyapısını desteklemek için çalışmaktır. Bu amaca ulaşmak için, sorumluluk anlayışı doğrultusunda ülkelerin faaliyetlerini destekleyecek, ortaklıkları sürdürecek ve siber uzayda hukukun üstünlüğünü destekleyecek ortamı sağlayacak ve idame ettirecektir" [111]. ABD; karşılaşacakları güçlükler ile mücadele ederken kişisel

özgürlükler, mahremiyet ve bilginin özgür dolaşımı olarak tanımladığı temel prensipleri koruma niyetindedir.

6.2.2. Kritik altyapı tesisleri

ABD Vatanseverlik Kanununun (USA Patriot Act) 1016 numaralı bölümü, Kritik Altyapıların Korunması Kanunu (Critical Infrastructure Protection Act of 2001, 42 USC 5195c.) olarak geçmektedir. Bu bölümde kritik altyapılar; fiziksel veya sanal dahi olsa, ABD için hayati öneme sahip olan, kapasitesi altında çalışma veya imhası halinde güvenlik, ulusal ekonomi güvenliği, ulusal kamu sağlığı veya güvenliği ya da bunların hepsinin birden üzerinde zayıflatıcı etkiye yol açacak olan sistemler ve varlıklar şeklinde tanımlanmıştır [112]. Bu kanunla; Ulusal Altyapı Simülasyon ve Analiz Merkezi kurulması planlanmış, bu merkeze kritik altyapıların tespiti, tehdit ve risk analizi yetkisi verilmiş ve 2002 yılı bütçesinden 20 milyon dolar bütçe ayrılmıştır.

ABD'nin kritik altyapı tesisleri başlangıçta on dört adet olarak tanımlansa da, 21 numaralı ABD Başkanlık Politika Direktifi ile bu sayı on altıya çıkarılmıştır. Bunlar; kimyasal sektör, ekonomik tesis sektörü, iletişim sektörü, kritik imalat sektörü, barajlar, savunma endüstriyel üs sektörü, acil servis sektörü, enerji sektörü, finansal servis sektörü, tarım ve gıda sektörü, kamu sektörü, sağlık ve halk sağlığı sektörü, bilgi teknolojileri sektörü, nükleer reaktör-materyal-atık sektörü, ulaşım sistemleri sektörü ve su olarak belirtilmiştir [113].

Ayrıca, Şubat 2013'te yayımlanan Başkanlık Uygulama Emri ile; kritik altyapıların ulusal güvenlik açısından siber saldırılara maruz kalma ihtimalinin her geçen gün arttığı, ulusun refah ve güvenliğinin bu tesislerin sağlıklı bir şekilde çalışmasına bağlı olduğu, ancak kritik altyapı tesislerine sahip olan ve işletmenlerinin bilgi paylaşımı, ortak çalışması ile güvenlik, özgürlük ve sivil özgürlükleri koruma hedeflerine ulaşılabileceği konusuna vurgu yapılmıştır [114]. Bilgi paylaşımının sağlanması için, yürürlükteki yasalar doğrultusunda İç Güvenlik Bakanlığı, Ulusal İstihbarat birimlerine görevler verilmiştir.

6.2.3. Kamu-özel sektör işbirliği

Ulusal Siber Uzay Güvenliğini Sağlama Stratejisinde bahsedilen kritik önceliklerin birincisi olan Ulusal Siber Uzay Güvenlik Müdahale Sisteminde; olası siber saldırılara çabuk tanı koyulması, bilgi paylaşımı ve iyileştirme ile zararlı siber uzay aktivitesinin sebep olduğu hasarın azaltılmasının sağlanabileceği ve ulusal seviyede bu tür faaliyetlerin etkili olabilmesi için analizlerin yapılması, konu ile ilgili uyarıların yapılması ve müdahale için koordineli olmak üzere kamu ve özel sektörün işbirliği yapmasına ihtiyaç duyulduğu belirtilmiştir. Söz konusu müdahale sistemi DHS tarafından koordine edilen; analiz, uyarı, kritik altyapılarının sürekliliğini sağlama, organizasyonlar arası bilgi paylaşımını destekleyen kamu-özel sektör mimarisidir [104].

Kamu ve özel sektör ağları giderek artan şekilde hedef alındığı için gerçekleşecek olan siber saldırıların tespitini ilk olarak sağlayacak organizasyonlar olmaktadır. İşte burada her kurumun bünyesinde kurulan Bilgi Paylaşımı ve Analiz Merkezleri (Information Sharing and Analysis Center, ISAC) ön plana çıkmıştır. Her bir ISAC kurumsal ve iş süreçlerine karar veren bir yönetim kuruluna sahiptir ve özel sektör tarafından idare edilmektedir. Görevleri; güvenlikle ilgili olaylara ve müdahalelere ilişkin bilgileri toplamak, analiz etmek, paylaşmak ve bu suretle özel sektör ile kamu sektörü arasındaki bilgi alışverişini sağlamaktır [78]. Ulusal Bilgi Paylaşımı ve Analiz Merkezleri Konseyine (National Council of ISACs, NCI) üye olan merkezler kendi sektörlerini temsil etmektedir. Bu ISAC'ler [115]; Havacılık (A-ISAC), Savunma Endüstri Üsleri (DIB-ISAC), Acil Servis (EMR-ISAC), Elektrik Sektörü (ES-ISAC), Finansal Hizmetler (FS-ISAC), Bilgi Teknolojileri (IT-ISAC), Denizcilik (Maritime ISAC), İletişim (NCC), Ulusal Sağlık (NH-ISAC), Nükleer (NEI), Petrol ve Doğalgaz (ONG-ISAC), Araştırma ve Eğitim (REN-ISAC), Su (Water-ISAC) sektörleri ile ilgili bilgi paylaşımı yapmaktadır.

2001 yılında oluşturulan Ulusal Siber Güvenlik İttifakı (National Cyber Security Alliance, NCSA) ile kamu-özel sektör işbirliğine ilişkin farkındalığın artırılması hedeflenmiştir [78]. Söz konusu ittifaka ABD'nin önde gelen bilgi ve iletişim firmaları (Microsoft, ESET, Bank of America, AT&T, Google, Symantec, Intel, Facebook, McAfee vb.) üyedir ve İnternetin ABD genelinde güvenli ve emniyetli bir şekilde kullanılmasını sağlamak üzere eğitim sağlama misyonuna sahiptir [116].

6.2.4. Sorumlu kurumlar

ABD'de siber güvenlikten sorumlu en üst düzeyde dört kurum bulunmaktadır. Bu kurumlar siber güvenliğin tesis edilmesinde birlikte çalışmaktadırlar.

Siber Komutanlık (US Cyber Command, USCYBERCOM)

Ülkenin siber saldırılara karşı savunulmasından, askeri sistem ve ağların siber güvenliğin sağlanmasından sorumludur. Siber Komutanlık ayrıca, siber saldırı ve savunma kabiliyetlerini muharip komutanlıkların harekât planlarına entegre ederek bu komutanlıkları destekler ve kritik altyapıların savunulmasında DHS'ye yardım eder. Resmi olarak 21 Mayıs 2010'da faaliyete başlamış olup, 31 Ekim 2010'da tam harekât kabiliyetine kavuşmuştur. Bu komutanlığın 2010 yılı bütçesi 120 milyon dolar, 2011 bütçesi 150 milyon dolardır [11].

Millî Güvenlik Teşkilatı (National Security Agency, NSA)

NSA, ABD Savunma Bakanlığının kriptografik istihbarat birimi olup, ülke sınırları dışındaki iletişim ve sinyal istihbaratından, ABD devlet iletişim ve bilgi sistemlerinin korunmasından sorumludur. NSA başkanı aynı zamanda USCYBERCOM'un da komutanıdır. NSA'in iletişim dinleme görevi, telsiz yayınları, İnternet, telefon konuşmaları gibi iletişimleri kapsamaktadır [11].

İç Güvenlik Bakanlığı (DHS)

DHS 11 Eylül saldırıları sonrasında, 25 Kasım 2002 tarihinde kurulmuş olup, ABD topraklarını terör saldırılarından, insan yapımı kazalardan ve tabi afetlerden korumakla görevlidir. 2011 yılı bütçesi 98,8 milyar dolardır. DHS, ABD federal devlet birimlerine ait sistem ve ağların siber güvenliğini sağlamaktan sorumludur. Temel rolü, sivil devlet ağlarının korunması, temel kritik altyapı ağlarının siber güvenliğinin güçlendirilmesi ve ulusal çeviklik ve hazırlığın geliştirilmesidir. Gizlilik dereceli olmayan federal sivil devlet ağlarının emniyetli hale getirilmesinde ve özel sektöre de siber güvenlik konularında destek verir. Önemli siber saldırılara karşı koordinasyon yetkisi bu bakanlıktadır [11].

Federal Araştırma Bürosu (FBI)

FBI, ABD Adalet Bakanlığı bünyesinde, federal suçların araştırılması ve ülke içinde istihbarata karşı koyulmasından sorumludur. Yaklaşık 35000 personele sahip olan FBI'ın 2011 yılı bütçesi 7,9 milyar dolardır. FBI, ülke sınırları içerisinde suçla veya istihbarata karşı koyma ile ilgili siber olayların araştırılması ve engellenmesinden sorumludur. Yasa uygulama ve istihbarata karşı koymaya ek olarak, ülke içi siber tehdit istihbaratının en üst düzeydeki yetkili kurumudur. FBI ayrıca siber güvenlik konularında DHS'e bilgi ve destek sağlamaktadır [11].

6.2.5. Yasal mevzuat

Federal bir yapıya sahip olan ve hemen hemen her eyaletinde bilişim suçlarına yönelik düzenlemeleri mevcut olan Amerika Birleşik Devletleri, teknolojik ilerlemelerin en hızlı ilerlediği ve buna bağlı olarak teknolojik yöndeki düzenlemelerin en hızlı biçimde yürürlüğe konduğu ülke konumundadır. Bunun doğal sonucu olarak da, hem öğretideki tartışmalar, hem yasal düzenlemeler ve hem de uygulama örneklerinde ABD mehaz durumundadır [81]. Amerikan Temel Yasasında (U.S.Code) bilişim suçlarına ait düzenlenmeler çoğunlukla 18'inci başlıkta ele alınmıştır.

1984 yılında kabul edilen Erişim Aygıtlarını Taklit Etme ve Bilgisayar Dolandırıcılığı ve Bilgisayarı Kötüye Kullanma Kanunu (The Counterfeit Access Device and Computer Fraud and Abuse Act, CFAA) ve daha sonra yapılan bütün ekleme ve değişiklikleri ABD'de bilişim düzeyde kabul edilen ilk kanun olmuştur. Bilgisayarın suça konu olduğu fiillerde temel adres konumunda olan bu Kanunda, klasik suçlara benzemeyen, özel nitelikteki bilişim suçları yer almaktadır [117].

CFAA'da düzenlenen üç temel konu şöyledir:

- Birincisi, kasten, ABD'nin savunma veya yabancı ülkelerle ilişkileri hakkındaki gizli bilgileri, ABD'nin zararına veya başka bir ülkenin yararına olarak elde etmek için bilgisayarlara yetkisiz veya yetkili olarak erişmek,
- İkincisi, bir suç işlemek amacıyla kasten, finansal yapının mali kayıtlarını veya tüketici raporlarından bir tüketici dosyasını elde etmek için, bilgisayarlara yetkisiz veya yetkili olarak erişmek,
- Üçüncüsü ise kasten, Hükümetin kullanımındaki veya bu kullanımı etkileyecek bir bilgisayarın yetkili olarak kullanımı etkilemek veya bunlardaki bilgileri açığa vurmak veya bilgileri değiştirmek veya zarar vermek için bu bilgisayarlara yetkisiz veya yetkili olarak erişmektir [118].

ABD'de bilişim sahasında; 1986 tarihli Elektronik Fonların Transferi Kanunu (Electronik Fund Transfer Act), 1986 tarihli Elektronik Haberleşme Gizlilik Kanunu (Electronic Communications Privacy Act), 1992 tarihli Bilgi ve Teknoloji Kanunu (Information and Technology Act of 1992), Ulusal Bilgi Altyapısı Kanunu (National Information Infrastructure Act), 1997 tarihli İnternette Kumarın Önlenmesi Kanunu (Internet Gambling Prohibition Act), 1998 tarihli Çocukların Online Yayınlardan Korunması Kanunu (Child Online Prevention Act), 2001 tarihli Anti Terörizm Kanunu (USA-Patriot Anti-Terrorism Act) da belirtilebilir [80].

Çocukların kendileri için zararlı olabilecek içeriğe ulaşmalarının engellenmesi amacıyla, 1996 tarihli İletişim Ahlak Yasası (Communications Decency Act); Amerikan Temel Yasası'nın 18. Bölümünün 2256. maddesinde gerekli değişiklikler yapılarak, çocukların görüntülendiği pornografik yayın ve materyallerin elde bulundurulması, internet üzerinden ticaretinin yapılması veya internetten yayınlanmasını engelleyen Çocuk Pornografisinin Önlenmesi Yasası (Child Pornography Prevention Act) da çocuklarla ilgili yapılan yasal düzenlemelerdir [119].

ABD'de siber suçlarla mücadelede kullanılan bazı kanunlar şunlardır:

U.S. Code 1030 (Bilgisayar Sahtekârlığı ve Bilgisayarların Kötüye Kullanılması Kanunu)

ABD yasasının 18. başlığının 1. kısım, 47. bölüm, 1030. maddesinde düzenlenen bu kanun, bilişim korsanlığı, virüs yayma, dolandırıcılık, şifre kaçakçılığı, zorla para sızdırma gibi birkaç eylemle ilgilidir. Yasa, federal veya korunan bir bilgisayarı hedefleyen davranışları kapsamaktadır. Korunan bir bilgisayar ise, bir bilgisayarın ya yalnızca bir finansal kurum veya federal hükümet tarafından kullanılması veya yalnızca finansal kurum veya federal hükümet tarafından kullanılmayıp suçun etkilerini içererek işleri yürütmesi ya da bir bilgisayarın eyaletler arası veya dış ticarette veya iletişimde kullanılması anlamına gelir. Yasa ayrıca suni varlıklara veya bireylere zarar verici davranışları kapsar [120].

U.S. Code 1029 (Erişim Araçlarıyla İlgili Dolandırıcılık)

ABD yasasının 18. başlığının 1. kısım, 47. bölüm, 1029. maddesi, para, eşya, hizmet veya diğer değerli herhangi bir şey almakta kullanılabilecek herhangi bir kart, kod, hesap numarası, elektronik seri numarası, mobil kimlik belirleme numarası, kişisel kimlik numarası veya diğer haberleşme servisi, donanımı veya diğer hesap giriş araçlarını kapsayan erişim cihazlarını içeren belirli faaliyetlerle meşgul olmayı suç saymaktadır. Yasa ayrıca sahte erişim cihazlarını içeren faaliyetleri de yasaklamaktadır [120].

U.S. Code 2701 (Depolanmış Kablolu ve Elektronik İletişimlere ve Ticari Kayıtlara Yetkisiz Erişim)

Bu düzenlemede, ya elektronik iletişimin sağlandığı bir tesise yetkisiz ve kasten erişim ya da kasten yetki aşılarak böyle bir tesise erişerek elektronik depoda bulunan kablolu veya elektronik iletişime yetkili erişim elde etmek, yetkili erişimi değiştirmek veya önlemek faaliyetleri suç sayılmıştır. Temel ceza; para cezası ve 6 aydan fazla olmamak üzere hapis cezasıdır fakat suçun ticari fayda, kötü niyetli yıkım veya zarar veya şahsi kazanç amacıyla islenmesi durumunda ağırlatıcı sebep öngörülmüştür [120].

Maddenin (c) fıkrasında suça ilişkin bazı istisnalara yer verilmiş ve buna göre hukuka uygunluk halleri belirtilmiştir. Anılan yasanın 2702 ile 2712 maddeleri arasında benzer konularda düzenleme yapılmıştır [121].

U.S. Code 1028 (Kimlik Belirleyici Belgelerde Sahtecilik)

Temel Ceza Yasası'nın 1028. maddesinde düzenlenmiş olup, kimlik belirlemeye yarayan belgelerin sahte olarak üretilmesi, iletilmesi, çalınmış belgelerin sahiplenilmesi, suç işlemek için kullanılması gibi eylemleri konu almaktadır. "Identity Theft and Assumption Deterrence Act of 1998" adını da taşıyan bu yasanın konusunu oluşturan suç, kimlik hırsızlığı veya "phishing" veya "the signature crime of the digital era" olarak da ifade edilmektedir [121].

Federal Bilgi Güvenliği Yönetimi Kanunu (FISMA)

FISMA ile siber güvenliğin ülke için önemi vurgulanmış ve federal hükümetlerin bilgi güvenliğini sağlamaları amacıyla programlar oluşturmaları gerektiği hüküm altına alınmıştır. FISMA'da bilgi güvenliği, bilgilerin ve bilgi ve iletişim sistemlerinin bütünlüğünün, gizliliğinin ve erişilebilirliğinin sağlanması amacıyla yetkisiz erişimden, kullanımdan, engellemeden ya da tahrip edilmeden korunması olarak tanımlanmıştır. FISMA kapsamında NIST bilgi güvenliğine ilişkin standartlar, ilkeler ve metotlar geliştirmekle yükümlü kılınmıştır [78].

6.2.6. Eğitim, kapasite artırımı ve farkındalık çalışmaları

Siber güvenlikle ilgili yaşanan zafiyetler bilgisayar kullanıcılarının, sistem yöneticilerinin, teknoloji geliştirme safhasında yer alan kişilerin, tedarikten sorumlu yetkililerin ve yönetim kademesinde çalışanların siber güvenlik farkındalıklarının eksik olmasından kaynaklanmaktadır. ABD'nin Ulusal Siber Güvenlik Stratejisinin üçüncü önceliği olan "Ulusal Siber Güvenlik Farkındalık ve Eğitim Programı" ile eğitim ve farkındalık için dört önemli eylem ve girişim planlanmıştır.

Bunlar;

- Tüm Amerika halkının kendisi ile ilgili siber uzayı güvenli hale getirecek şekilde kapsamlı bir ulusal farkındalık programı başlatmak,
- Ulusal siber güvenlik ihtiyaçlarını destekleyecek şekilde gerekli eğitim programlarını teşvik etmek,
- Hali hazırdaki siber güvenlik eğitim programlarının etkinliğini artırmak,
- Kamu-özel sektör işbirliğini profesyonel siber güvenlik sertifikasyonları için desteklemektir.

Eğitim ve farkındalığın artırılması konusunda federal ve yerel teşekküllerle, özel sektör organizasyonları ile birlikte koordine kurulmak üzere halkı bilgilendirecek materyallerin temin edilmesi ve StaySafeOnline kampanyasının yaygınlaştırılması görevi DHS'e verilmiştir [104]. Yine ilkokul ve ortaokul seviyesindeki öğrencilerin siber güvenlik eğitimleri için Eğitim Bakanlığı ile koordineli hareket etmek koşuluyla gerekli programları desteklemek ve teşvik etmek görevi de DHS'e verilmiştir.

ABD Eğitim Bakanlığı, yirmiden fazla federal kurum ve ajanslar ile akademik ve sanayi birimlerinin katılımıyla Ulusal Siber Güvenlik Eğitim Girişimi (National Initiative for Cybersecurity Education, NICE) teşkil etmiştir. NICE'ın görevi ABD'nin ulusal siber güvenlik durumunu sağlamlaştırmak için nüfusun her seviyesindeki kişilerin siber güvenlik ile ilgili bilgi ve yeteneklerin geliştirilmesini sağlamak maksadıyla, eğitim kaynaklarının kullanılırlık ve erişilebilirliklerini artırmaktır [122]. Başkan Obama tarafından yayımlanan 2009 yılı Millî Siber Güvenlik İnisiyatifinin desteğinde teşkil edilmiştir.

NICE'ın temel hedeflerinden biri de ABD eğitim sisteminde uygulanan STEM (science, technology, engineering and math) eğitim programına siber güvenlik konularının entegre edilmesini sağlamaktır. NSA ve DHS'nin ortak çabaları ile bilgi güvenliği ve siber savunma için yüksek eğitimin teşviki için kurulan Ulusal Akademik Mükemmeliyet Merkezleri (Naitonal Centers of Academic Excellence, CAE) ile STEM programının yaygılaştırılması sağlanmaktadır. Şu anda 42 eyalette 166 CAE bulunmaktadır [123].

ABD'de siber güvenlik farkındalığı ve eğitimi ile ilgili diğer faaliyetler;

- Öğretmenler için ders programlarına siber güvenlik konularını dâhil edebilmeleri için The Integrated Cybersecurity Education Communities (ICEC) Programı,
- Aileler, eğitmenler ve politika yapıcıların çocuklarına teknoloji ve internetin güvenli ve sağlıklı kullanımını çevrim içi eğitim programları sayesinde öğretmeleri için iKeepSafe Programı ve Cyber Watch Programı,
- Ulusal Bilim Fonu sponsorluğunda üniversite ve daha üzeri eğitim alan öğrenciler için I-Corps programı,
- US-CERT ile birlikte Carnegie Mellon Üniversitesi işbirliği ile artan nitelikli yazılım uzmanı ihtiyacını karşılamak için Yazılım Güvenliği Eğitim Programı hazırlanmıştır [124].
- Öğrencilerin siber güvenlik konularına ilgilerini artırmak için siber yarışmalar düzenlenmektedir.
- Lise çağındaki öğrencilerin siber güvenlik alanına teşvikini sağlamak için yaz kampları düzenlenmekte (Integrated Cybersecurity Education Communities, ICEC) ve söz konusu kamplara okullarda siber güvenlik eğitimi veren öğretmenlerin de katılması sağlanmaktadır.

6.2.7. Uluslararası işbirliği

Barış zamanında ABD devlet kurumları, üniversite araştırma merkezleri ve özel şirketleri, düşmanları tarafından düzenli olarak siber saldırılara maruz bırakılmakta; bu saldırıların bilgi sistemlerinin keşfi, önemli hedeflerin belirlenmesi, kritik sistemlerine arka kapı saldırıları gibi erişim yollarının denenmesi gibi amaçları taşımaktadır. Savaş zamanında ise kritik altyapılar ile önemli ekonomik fonksiyonların hasara uğratılması ile halkta güven kaybı yaşatılması amaçlanmaktadır. Bu tip saldırıların önüne geçmek maksadıyla beşinci kritik öncelik kapsamında, ulusal siber güvenlik stratejisinde uluslararası işbirliğini sağlamak hedefiyle girişim ve eylemler planlanmıştır. Temel olarak; siber konuları içeren karşı istihbarat tedbirlerinin alınması, siber saldırılara karşı tedbirlerin alınması ve cevap verilmesi, uluslararası şirket ve organizasyonlarla çalışılması, ulusal ve uluslararası siber saldırıların tespit edilebileceği sistemler oluşturulması konularını içermektedir [104].

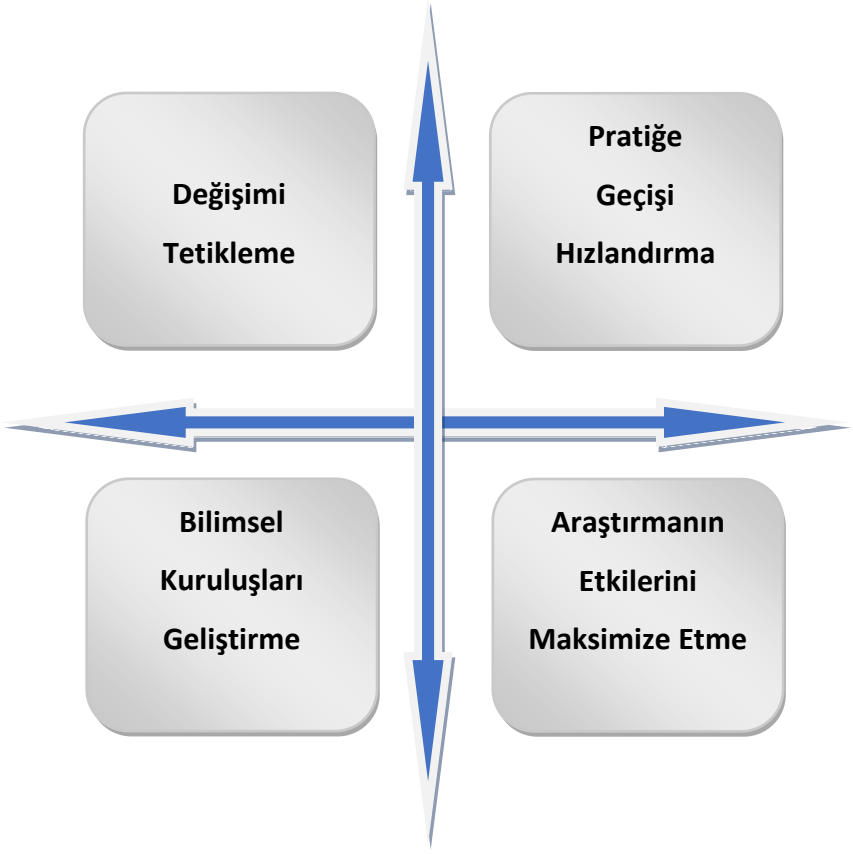
Uluslararası stratejide; ABD dışındaki ülkelerin teknik ve siber güvenlik kapasitelerinin, bilgi ve eğitim düzeylerinin arttırılmasının önemi vurgulanmıştır. Ayrıca, siber güvenlik ile ilgili edinilen başarılı uygulamaların arttırılması ve paylaşımı da akıllı yatırımların yapılmasını ve etkili politikaların geliştirilmesine sebebiyet vereceği değerlendirilmiştir. Özellikle Afrika ve Asya kıtaları başta olmak üzere dünya üzerindeki birçok ülke ve organizasyon ile siber suça karşı mücadele edilmesi konularında işbirliği ve eğitim faaliyetlerine devam edilmesi öngörülmüştür [111].

6.2.8. Ar-Ge faaliyetleri

Amerika Birleşik Devletlerinde 2002 yılında çıkarılan Siber Güvenlik Araştırma ve Geliştirme Kanunu ile;

- Kriptografi, kimlik doğrulama ve diğer güvenli iletişim teknolojileri,
- Adli bilişim ve sızma tespitleri,
- Bilgisayar ve ağ uygulamalarının, işletim sistemlerinin, kontrol sistemlerinin ve iletişim altyapılarının güvenilirliği,
- Güvenlik yetkilendirmesi ve analizi dâhil olmak üzere ağ güvenlik mimarileri,
- Yeni geliştirilen tehditler,
- Hassasiyet analizi ve risk değerlendirmesi,
- Uzaktan erişim ve kablosuz ağ güvenliği ve siber suçların tespiti, soruşturulması ve kovuşturulmasını sağlamak için kanuni uygulamalar için 2003-2007 yılları arasında yaklaşık 900 milyon dolar Ulusal Bilim Kurumuna (National Science Foundation, NSF) tahsis edilmiştir [125].

2011 yılında Beyaz Saray tarafından siber uzayın güvenliğini sağlamak için Ar-Ge planı (Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program) yayımlanmıştır [126]. Bu plan Şekil 6.1'de gösterilen dört temel üzerine kurulmuştur. Bu plan ve Yüksek Performanslı Hesaplama Kanunu (High-Performans of Computing Act of 1991) doğrultusunda teşkil edilen Ağ ve Bilgi Teknolojileri Araştırma Geliştirme Programı (Networking and IT R&D, NITRD) kapsamında, 14 kurum ve kuruluşa, yedi alt program sahasında, yıllık ortalama 4 milyar dolar bütçe tahsis edilmiştir [127].



Şekil 6.1. Federal siber güvenlik Ar-Ge programı temel ilkeleri [127]

6.2.9. Acil müdahale ekipleri

DHS, ABD'nin ulusal kritik altyapılarının fiziksel ve siber tehditlere karşı korunmasından sorumludur. DHS bu yükümlülüğü Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi (National Cybersecurity and Communications Integration Center, NCCIC) vasıtasıyla gerçekleştirmektedir. NCCIC siber güvenlik ve iletişim sektörü paydaşları ile koordine olmakta ve çabaların senkronize edilmesini sağlamaktadır. NCCIC'nin misyonu;

- Federal birimlerin siber uzayda korunmasını sağlamak,
- Kritik altyapı sahipleri ile sıkı ilişkiler içerisinde çalışmak,
- Uluslararası paydaşlarla bilgi paylaşımı yapmak ve siber olaylara müdahalelerde yardımcı olmak,
- ABD'de gerçekleşecek siber olaylara ulusal siber olaylara tepki planı çerçevesinde müdahale etmek, verilerin analizini yapmak ve uygun önerilerde bulunmak,
- Durumsal farkındalık yaratmak, siber tehdit ve zafiyet analiz bilgilerini yayımlamaktır [128].

NCCIC dört birimden oluşmaktadır:

- NCCIC Operasyonları ve Entegrasyonu,
- Birleşik Devletler Ulusal Bilgisayar Acil Müdahale Ekibi (United States National Computer Emergency Response Team, US-CERT),
- Endüstriyel Kontrol Sistemleri Siber Acil Müdahale Ekibi,
- Ulusal İletişim Koordinasyon Merkezi [128].

6.2.10. Diğer hususlar

2004 yılında bilim ve teknoloji için 800 milyon dolar bütçe ayrılırken, bu bütçenin 18 milyon dolarlık kısmı DHS emrine siber güvenlik için kullanılmak üzere tahsis edilmiştir. 2015 yılına gelindiğinde ise 2016 yılı için Kongreye onaylamak üzere gönderilen bütçe ile [129];

- Bütçedeki fonlama, ülkedeki siber güvenliğin artırılması amacıyla çeşitli öneriler sunulmuştur. Bunlar; EINSTEIN isimli siber olay tespit ve engelleme sistemi, federal bilgisayar ağlarının izleme ve teşhisinin yapılması, siber olay müdahale eğitimlerinin yaygınlaştırılması vb. hususlardır.
- Siber güvenlik harcamalarının 1 milyar dolardan 14 milyar dolara çıkarılmasını önerilmektedir.
- Siber güvenlik konusundaki girişimleri ve öncelikleri belirtilmekte ve olay engelleme ile müdahale kabiliyetlerinin geliştirilmesi planlanmaktadır.
- Devletin özel sektörle bilgi paylaşımı kabiliyetlerinin geliştirilmesini ve herhangi bir siber durumda ortaya çıkacak tehditlere karşı kendisini korumasını sağlamak için öneride bulunmaktadır.
- ABD'nin siber tehditlere cevap verme kabiliyetlerinin geliştirilmesi üzerinde durulmaktadır. Bu öneriye göre, sivil bir siber kampüs kurularak daha iyi bilgi paylaşımını ve siber suçlarla mücadele için diğer ülkelerle işbirliğinin sağlanması hedeflemektedir.
- Devlet kurumlarının ve bilgi sistemlerinin korunmasını, öncelik olarak ortaya konulmaktadır.
- Genel olarak Amerikan vatandaşlarının, sistemlerinin ve bilgilerinin, siber tehditlerden korunmasına imkân tanıyacak düzenlemeleri içermektedir.

Siber güvenlikten sorumlu olan DHS siber güvenlik ile ilgili çalışanların sayısını 2012 yılı içerisinde 2010 yılına oranla beş kat arttırmıştır. 2011 yılında US-CERT 106 000 siber güvenlik olayına müdahale etmiş ve 5000'den fazla siber güvenlik uyarısı ve bilgilendirici materyalleri yayımlamıştır [130].

7. TÜRKİYE'NİN SİBER GÜVENLİK STRATEJİSİNİN İNCELENMESİ

Türkiye Cumhuriyeti'ne İngiltere ve ABD'de yaşanan saldırılara benzer şekilde birçok siber olay meydana gelmiştir. Haziran 2011 ve Nisan 2012'de internet özgürlükleri ve ifade hakkının korunmasına yönelik, işbirliği içerisinde çalışan, uluslararası siber korsan topluluğu olan Anonymus; aralarında Adalet, İçişleri ve Dışişleri Bakanlıklarıyla Emniyet Genel Müdürlüğünün de bulunduğu yirmi civarında devlet sitesine, internet erişimini engellemek için saldırmıştır [11]. Kasım 2014'te ise HSBC Türkiye'ye gerçekleştirilen siber saldırılar sonucu 2,7 milyon müşterinin kredi kartı bilgileri alınmış ve banka tarafından müşterilerin korunması amacıyla bir dizi önlem alındığı, ilgili kurumlarla ulusal ve uluslararası işbirliğinin devam ettiği bir basın açıklaması ile bildirilmiştir [131]. 31 Mart 2015 tarihinde tüm Türkiye'de gerçekleşen nedeni hala belirlenememiş olan uzun süreli elektrik kesintisi gerçekleşmiş ve olayın sebepleri arasında siber saldırı ihtimalinin de göz önünde bulundurulduğu açıklanmıştır [132].

7.1. Genel Bakış

Ulusal güvenliğe siber güvenliğin entegre edilmesi kapsamında; İngiltere ve ABD'nin ulusal güvenlik stratejilerinin karşılığı olan Millî Güvenlik Siyaset Belgesi (bu ülkelerin aksine) kamuoyu ile paylaşılmamaktadır. Ancak, Millî Güvenlik Kurulunun (MGK) olağan ve olağandışı yaptığı toplantılar sonucunda alınan kararlar MGK'nın resmi internet sayfasından paylaşılmaktadır. Siber güvenlik konusu ilk defa 27 Ekim 2010 tarihli toplantıda gündeme alınmış ve "Siber tehdidin global düzeyde ulaştığı boyut ve bu tehdidin ulusal güvenliğe etkileri kapsamlı surette ele alınmıştır. Bu bağlamda, siber tehdidin engellenebilmesi açısından millî düzeyde yürütülen çalışmalar değerlendirilmiştir" açıklaması ile verilen önem belirtilmiştir [133].

Türk kamu yönetiminde politika tercihlerini ortaya koyan bir dizi politika metni ve aracı bulunmaktadır. Birincil ve ikincil mevzuat düzenlemeleri, Hükümet Programı, Kalkınma Planı, Orta Vadeli Program, Orta Vadeli Mali Plan, Yıllık program, Bütçe ve Yatırım Programı, kamu kurumlarının stratejik planları, tematik strateji ve eylem planları, bölge ve imar planları, idari teamüller ve nihayet yönetim tercihleri ile yönetim geleneklerini bu metin ve araçlar arasında saymak mümkündür.

Türkiye'nin bilgi toplumu politika alanına yönelik hazırlanan politika belgeleri; Türkiye Ulusal Enformasyon Altyapısı Ana Planı - TUENA (1999), e-Türkiye Girişimi Eylem Planı (2000), e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı (2003-2004), 2005 Eylem Planı ile Bilgi Toplumu Stratejisi ve Eylem Planıdır (2006-2010) [18, 65].

Türkiye'de 2012 yılına kadar Bilim, Sanayi ve Teknoloji Bakanlığının koordinatörlüğünde BTK tarafından sivil toplum kuruluşları ve kurumları ile beraber yürütülen siber suçlarla mücadele, Aralık 2012'de "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının" hazırlanarak yürürlüğe girmesiyle Ulaştırma, Denizcilik ve Haberleşme Bakanlığının sorumluluğuna verilmiştir.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının *amacı*;

- Kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin sağlanmasına,
- Kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanmasına,
- Siber güvenlik olaylarının etkilerinin en düşük düzeyde kalmasına, olayların ardından sistemlerin en kısa sürede normal çalışmalarına dönmesine yönelik stratejik siber güvenlik eylemlerinin belirlenmesine ve oluşan suçun adli makam ve kollukça daha etkin araştırılmasının ve soruşturulmasının sağlanmasına yönelik bir altyapı oluşturmaktır [10].

USGS'nde belirlenen amaca yönelik herhangi özellikli bir hedef belirtilmemekle beraber, ulusal siber güvenliğin sağlanması için hazırlanan yedi ana başlık altındaki 29 adet eylem planı aşağıdaki ilkeler göz önünde bulundurularak hazırlanmıştır:

- Siber güvenlik, risk yönetimini esas alan etkin ve sürekli iyileştirmeye dayalı yöntemler aracılığıyla sağlanır.
- Siber güvenlik için teknik boyutun yanı sıra; hukuki, idari, ekonomik, politik ve sosyal boyutlarda güçlü ve zayıf yönlerin, tehditlerin ve fırsatların belirlenmesini içeren bütüncül bir yaklaşım benimsenir.

- Risk yönetiminde, teknik zaafların giderilmesi, saldırı ve tehdidin önlenmesi ile muhtemel zararın en aza indirgenmesi unsurları esas alınır.
- Siber güvenliğin sağlanmasında birey, kurum, toplum ve devletin tüm hukuki ve sosyal sorumluluklarını yerine getirmesi esas kabul edilir.
- Kritik altyapıların güvenliğinin sağlanması için, özel sektörle, karar mekanizmalarına katılımı da içeren tam işbirliği yapılır.
- Siber ortam güvenliğinin sağlanması ve sürdürülmesinde kamu, özel sektör, üniversiteler ve sivil toplum örgütleri işbirliğinin yanı sıra uluslararası işbirliği ve bilgi paylaşımı esas kabul edilir.
- Uluslararası işbirliği ve bilgi paylaşımı için diplomatik, teknik ve kolluk iletişim kanallarının sürekli ve etkin kullanımı esas alınır.
- İhtiyaç duyulan mevzuat geliştirilirken uluslararası anlaşma ve düzenlemeler göz önünde bulundurulur.
- Hukukun üstünlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması ilkeleri temel esas kabul edilir.
- Siber ortamda şeffaflık, hesap verilebilirlik, etik değerler ve ifade özgürlüğü desteklenir.
- Güvenlik ile kullanılabilirlik arasında denge kurulur.
- Denetleyici ve düzenleyici kurumlar sorumlu oldukları alanlarda siber güvenliğin sağlanmasını gözetirler.
- Siber güvenlik gereksinimlerinin karşılanmasında yerli ürün ve hizmet kullanımı teşvik edilir, bunların geliştirilmesi için araştırma ve geliştirme projeleri desteklenir, inovasyon anlayışı esas kabul edilir [10].

USGS'deki eylem planlarından 31 adet kurum, kuruluş ve organizasyon sorumlu veya ilgili olarak belirlenmiştir.

7.2. Kritik Altyapı Tesisleri

Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı (AFAD) siber tehlikeler ve kritik altyapı çökmeleri konusunu, teknolojik afet (insan kaynaklı afet) konu başlığı altında değerlendirmektedir [134]. Teknolojik afet türleri arasında Büyük Endüstriyel Kazalar, Maden ve Maden Atık Kazaları, Radyolojik ve Nükleer Kazalar, Tehlikeli Madde Taşımacılığı Kazaları, Deniz Kirliliğine Neden Olan Kazalar, Biyolojik Olaylar, Çevresel Tehlikeler (Çölleşme, Kuraklık, Asit Yağmurları, vb), İklim Değişikliği, Kritik Altyapılar ve Siber Güvenlik bulunmaktadır.

Bu bağlamda AFAD tarafından kritik altyapılar; "İşlevini kısmen veya tamamen yerine getiremediğinde çevrenin, toplumsal düzenin ve kamu hizmetlerinin yürütülmesinin olumsuz etkilenmesi neticesinde, vatandaşların sağlık, güvenlik ve ekonomisi üzerinde ciddi etkiler oluşturacak ağ, varlık, sistem ve yapıların bütünü" olarak tanımlanmıştır. AFAD Planlama ve Zarar Azaltma Dairesi Başkanlığı Teknolojik Afetler Risk Azaltma Çalışma Grubu tarafından "2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi" yayımlanmıştır [135]. Söz konusu belge ile;

- Afetin neden olduğu zararların en aza indirgenmesi amacıyla, doğal ve teknolojik afetlerde bütünleşik bir yaklaşımla sivil korunmadan sorumlu olanların hazırlığı ve afet durumunda müdahale konusunda ulusal, bölgesel ve yerel seviyedeki çalışmaları desteklemek,
- Teknolojik afet konusunda sivil korunmayla ilgili AB mevzuatına göre uygulamalar yapabilecek şekilde hukuksal, kurumsal ve teknik çalışmalar yapmayı ve bu mevzuatın özellikle yetkili kurum ve kuruluşlar arasındaki işbirliğiyle ilgili olarak uygulanmasını koordine etmek,
- İnsanların, çevrenin ve malın daha iyi korunmasını sağlamak için, AB sivil korunma mevzuatı, topluluğun sivil korunma müdahaleleri mekanizması ve sivil korunmanın mali araçları ile ilgili çalışmaları başlatarak, müzakereler için gerekli hazırlıkları yapmak,
- Kritik altyapıların korunması için sivil korunma araştırması alanındaki işbirliğinin güçlendirilmesi, risklerin ve zararların azaltılması konusunda araştırma projelerinin hazırlanmasını teşvik etmek,

- Afet izleme ve bilgilendirmesi amacıyla, erken uyarı sistemlerindeki rolleri belirlemek,
- Ülke düzeyinde uygulanacak afet ve acil durum çalışmalarına yönelik risk yönetimi ve zarar azaltma planlarını hazırlatabilmek, risk değerlendirme sonucunda, zararın ortaya çıkma olasılığını azaltma, ortadan kaldırma veya şiddetini azaltmaya yönelik faaliyetlerin ulusal boyutta uygulanmasını yönlendirmek,
- Ülkemizde bulunan ulusal kritik altyapıları belirleyecek kurum ve kuruluşların koordinasyonunu yapmak,
- Ülkemizde ve komşu ülkelerimizde bulunan ve tahrip olması halinde uluslararası ilişkilerimizi etkileyecek sınır ötesi güce sahip kritik altyapıları belirlemek, korunmasına yönelik politikalar üretmek,
- Kritik Altyapılar Uyarı Bilgi Ağı'na (KAUBA) yönelik verileri hazırlamak amaçlanmıştır [135].

Ayrıca aynı raporda; Kritik altyapılar ve bu altyapıların korunması konuları ülkemizde ulusal bilgi güvenliği başlığı altında değerlendirildiği ve ulusal bilgi güvenliği konusunda ülkemizde yürütülen çalışmaların geçmişi ise gelişmiş ülkelerin bu konu üzerinde çalışmalar yaptığı 1990'ların sonlarına kadar gittiği hususlarına vurgu yapılmıştır.

TÜBİTAK'ın Kalkınma Bakanlığı 2012 Yatırım Programı içerisinde yer alan "Kritik Altyapılarda Bilgi Güvenliği Yönetimi Projesi" ve UDHB sponsorluğunda hazırlanan raporlar ülkemizdeki Kritik Altyapıların Bilgi Güvenliği konusunda önemli bir adım olmuştur. Ülkemizdeki net ifadeyle kritik altyapıların çevresel tehdit ve tehlikelerine (deprem, sel vb.) karşı korunmasına yönelik bir yasal düzenleme ise maalesef bulunmamaktadır [135].

AFAD'ın "Ulusal Kritik Altyapı, Varlık ve Tesisleri Belirleme, Risk Değerlendirme ve Önceliklendirme Projesi" ile çevresel tehditler (Deprem, Heyelan, Tsunami vb.) ve siber tehditler göz önüne alınarak ülkemizdeki kritik altyapı envanterin çıkarılması, açıklık ve riskleri dikkate alınarak önceliklendirilmesine ilişkin metodoloji geliştirilmesi, bu açıklık ve risklerin azaltılması amaçlı rehber hazırlanması amaçlanmaktadır. Söz konusu proje TÜBİTAK-BİLGEM (Bilişim ve Bilgi Güvenliği İleri Teknolojileri Araştırma Merkezi), Siber Güvenlik Enstitüsü (SGE) ile ortak yürütülecek olup, projenin süresi 18 aydır [136].

7.3. Kamu-Özel Sektör İşbirliği

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında Çizelge 7.1'de gösterilen iki adet eylem planında kamu-özel sektör işbirliğine vurgu yapılmıştır. Ayrıca 01 Kasım 2011 tarihli, 28102 sayılı Resmi Gazete'de yayımlanan KHK/655 Karar Sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 29.Maddesine dayanılarak oluşturulan İnternet Geliştirme Kurulunun çatısı altında Siber Güvenlik İnisiyatifi oluşturulmuştur.

Çizelge 7.1. Kamu-özel sektör işbirliği ile ilgili eylem maddeleri

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
14	İş sürekliliği ve veri yedekleme sistemleri kurulması	Kamu kurum ve kuruluşlarının ve kritik bilgi sistem altyapılarını işleten özel sektör kuruluşlarının hassas verilerinin yedeklenme usul ve esaslarının belirlenmesi	Ağustos 2013	- UDHB (S) - TÜBİTAK (İ) - Tüm kamu kurum ve kuruluşları (İ) - Kritik sektörleri düzenlemek ve denetlemek ile ilgili sorumlu kurumlar (İ)
		Kamu kurumlarının ve kritik bilgi sistem altyapılarını işleten özel sektör kuruluşlarının elektronik ortamda işlem yapan sistemlerinin ve verilerinin güvenlik risk seviyelerinin belirlenmesi	Eylül 2013	
		Tüm kamu kuruluşları ve kritik bilgi sistem altyapılarını işleten özel sektör kuruluşları tarafından iş sürekliliği planları yapılması	Aralık 2013	
27	Siber güvenlikte yerli ürün ve çözüm çalışmaları	Kamu ve özel sektör, üniversite, sivil toplum kuruluşu ve benzeri tüm bilgi güvenliği paydaşlarının katılacağı düzenli çalışmalar yapılması	Haziran 2013	- UDHB (S) - BTK (İ) - TÜBİTAK (İ) - Üniversiteler (İ) - STK'lar (İ)

Siber Güvenlik İnisiyatifinin görevi; İnternet Geliştirme Kurulu çatısı altında, sektör paydaşlarının katılım sağladığı ve hedefi siber güvenlik alanında çalışmalar yaparak, tüm paydaşların görüşlerini toplayarak, kurumlar arasında fikir alışverişini ve işbirliğini sağlayarak, ortak fikirler ortaya çıkararak, yaptığı çalışmaları Siber Güvenlik Kurulu Başkanlığını yürüten Ulaştırma, Denizcilik ve Haberleşme Bakanına ve Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na sunmaktır. Siber Güvenlik İnisiyatifinin faaliyetlerinden bazıları; vatandaş ve küçük işletmeleri siber güvenlik konusunda bilinçlendirme, farkındalık oluşturma, koruma tedbirlerini oluşturma ve anlatma, pozitif içerik üretimi, veri merkezlerinin internet servis sağlayıcılarının minimum güvenlik kriterlerini belirleme, sektörel risk analizi, siber güvenlik standartlarını belirleme, raporlar ve kılavuzlar yayınlamaktır [137].

Siber Güvenlik İnisiyatifinin bünyesinde bulunan çalışma grupları ve görevleri kısaca şu şekildedir:

- Farkındalık, Eğitim ve Rapor Çalışma Grubu: Siber güvenlik konusunda bireyden, toplumun her kesimine, şirketlere ve kamu kurumlarına uzanan geniş bir yelpazede bilgilendirme, bilinçlendirme, farkındalık ve eğitim çalışmaları yapmak, İnisiyatif'e ait olacak web sayfasında bilgilendirici ve eğitsel görsel ve materyallere yer vermek, bu amaçlar kapsamında ulusal veya uluslararası etkinlikler düzenlenmesini veya düzenlenenlere aktif katılım sağlanmasını önermek üzere çalışmalarını yürütmektedir.
- Siber Olaylarla ilgili Mevzuat ve Koordinasyon Çalışma Grubu: Siber Olaylarla ilgili Mevzuat ve Koordinasyon Çalışma Grubu, siber güvenlikle ilgili olarak yasal düzenleme ihtiyacına cevap vermek üzere yeni düzenleme taslakları hazırlamak veya yürürlükteki mevzuatımıza ilave edilmesi gereken hükümler veya yapılması gereken değişiklikler hakkında tarama çalışmaları yapmak, siber güvenlikle ilgili uluslararası yasal düzenlemelerin seyrini takip etmek, bu amaçla kamu özel sektör ve uluslararası koordinasyonu sağlamak; siber suçların delillerinin toplanması ve suçluya ulaşılması süreci olarak ifade edebileceğimiz adli bilişim konusunda mevzuatımızda yapılması gereken değişiklikler üzerinde çalışmak ve adli bilişimle ilgili farkındalık ve bilinçlendirme için adli makamlar ve kolluk kuvvetleri ile işbirliği yapmak üzere çalışmalarını yürütmektedir.

- Ulusal Siber Olaylara Müdahale Organizasyonu Çalışma Grubu: Özel sektörde ve kamu kurumlarında Siber Olaylara Müdahale Ekipleri (SOME) kurmak, bu ekiplerin Ulusal Siber Olaylara Müdahale Merkezi (USOM) ile koordineli çalışması, kendi yetki alanlarına giren yerlerde önleyici tedbirler geliştirmesi, başarılı çözümlerin duyurulması, kritik altyapılar, risk analizi, acil eylem planları gibi SOME'lerin yapması gereken konularda çalışmak, siber güvenlik tatbikatlarına katılım ve katkı sağlamak ve SOME'ler için rehber dokümanlar hazırlamak üzere çalışmalarını yürütmektedir.
- Teknik Araştırmalar ve Standartlar Çalışma Grubu: Ağ ürünleri, işletim sistemleri, yazılımlar ve bulut bilişim sistemlerinin açıklıklarının, açık kaynaklar ve testler gibi yöntemler ile tespitini yapmak, güvenliğin sağlanmasına yönelik tedbirleri belirlemek ve rehber kılavuzlar oluşturmak, gerekli uyarı ve bilgilendirmeleri yapmak üzere çalışmalarını yürütmektedir.
- Siber Tehditlerle Mücadele Çalışma Grubu: Köle ağlar (Botnet), istenmeyen e-posta (spam), oltalama (phishing), ddos, sosyal mühendislik, kötü amaçlı yazılım (malware) ve benzeri siber tehditlerle mücadele, köle ağların tespiti, siber saldırıların analizi, siber tehditler ile mücadele yöntemlerinin belirlenmesi, güncel tehditlerin belirlenmesi, bilgilendirme ve önleyici faaliyetlerin geliştirilmesi, yaşanan siber olayların olumsuz etkilerinin sınırlandırılması konularında çalışmalarını yürütmektedir [138].

Siber Güvenlik İnisiyatifine Kaspersky Lab, Oracle, Google gibi dünyaca ünlü şirketler ile Bilgi Güvenliği Derneği, Koçsistem, Türk Telekom gibi ülkemizde söz sahibi olan kurum ve kuruluşların bulunduğu 104 adet üyesi bulunmaktadır [137].

7.4. Sorumlu Kurumlar

20 Ekim 2012 tarih ve 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" 28447 sayılı Resmi Gazetede yayımlanmıştır. Söz konusu karar uyarınca; siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla; Ulaştırma, Denizcilik ve Haberleşme Bakanının başkanlığında, Dışişleri, İçişleri, UDHB, Milli Savunma bakanlıkları müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşan Siber Güvenlik Kurulu kurulmuştur.

USGS'nin Yasal Düzenlemeler, Güvenlik Altyapıları, Ulusal Siber Olaylara Müdahale Organizasyonu, Adil Süreçlere Yardımcı Mekanizmalar, Yerli Teknolojilerin Geliştirilmesi, Eğitim ve Bilinçlendirme 7 ana başlığı, 29 eylem maddesi ve 95 alt eylem maddesi doğrultusunda 31 sorumlu/ilgili kurum, kuruluş ve organizasyonu kapsayan görev dağılımı açık bir şekilde yapılmıştır.

7.5. Yasal Mevzuat

7.5.1. Türk Ceza Kanunu’nda bilişim suçları

Bilişim suçları, TCK’da şu numara ve başlıklar altında yer almaktadır:

“Topluma karşı suçlar” kısmının onuncu bölümünde “Bilişim alanında suçlar” başlığı altında md. 243 “hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu”, md. 244/1-2 “bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu”, md 244/4 “bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu”, md. 245 “banka veya kredi kartlarının kötüye kullanılması suçu”.

Bunların yanı sıra TCK'da bilişim sistemleri aracılığıyla işlenebilecek ancak yalnızca bilişim suçu olarak nitelendirilemeyecek suç tipleri de bulunmaktadır. Bunlara örnek olarak aşağıdaki suç tipleri verilebilir.

"Kişilere karşı suçlar" kısmının dokuzuncu bölümünde "özel hayata ve hayatın gizli alanına karşı suçlar" başlığı altında md. 132 "haberleşmenin gizliliğini ihlal suçu", "kişilere karşı suçlar" kısmının yedinci bölümü olan "hürriyete karsı suçlar" bölümünde md. 124 "haberleşmenin engellenmesi suçu"; sekizinci bölüm olan "şerefe karşı suçlar" bölümünde m.125 "hakaret suçu"; malvarlığına karşı suçlar bölümünde md. 142 fkr.2 b. 'e' "nitelikli hırsızlık suçu", md. 158 fkr.1 b. 'f' "nitelikli dolandırıcılık suçu" ile "topluma karşı suçlar" kısmının yedinci bölümü olan "genel ahlaka karşı suçlar" bölümünde md. 226 "müstehcenlik" suçu.

Bilişim sistemine girme (Madde 243)

Bilişim alanında suçlar bölümünde ilk olarak 243. maddede "bilişim sistemine girme suçu" düzenlenmiştir. TCK'da bu maddeye yer vermekle yasa koyucu "bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girme veya orada kalmaya devam etme" eylemini suç tipi haline getirmiştir [119]. Bilişim suçlarının işlenebilmesi için öncelikle bilişim sistemine girmek gerektiğinden yetkisiz girişlerin suç olarak TCK'nın 243'ncü maddesinde düzenlenmesinin son derece yerinde olduğu belirtilmiştir [139].

Bu maddede yer alan suç tipiyle, Avrupa Siber Suç Sözleşmesinin 2. Maddesinde öngörülen "hukuka aykırı erişim" düzenlemesine paralellik ve özellikle veriler ele geçirilmeksizin verilere yetkisiz erişim eylemleri suç tipi haline getirdiği görülmektedir sağlandığı [119, 140, 141]. TCK'nın 243. maddesi ile bilişim sistemine girişlerin cezalandırılması için "verilerin ele geçirilmesi" şartı kaldırılmakta ve bilişim sistemine girme suçu, genel kastla işlenebilen bir suç olarak düzenlenirken aynı maddenin 3. fıkrasında suçun nitelikli hali olarak düzenlenmiş olan ve sisteme girme sonucunda kasıt olmaksızın verilerin yok olması veya değişmesi durumunda ceza ağırlaştırılmıştır [121, 142, 143].

Suçun ikinci fıkrada düzenlenen daha az cezayı gerektiren nitelikli halinin vücut bulması durumunda ise, suçun temel şekli için öngörülen cezanın yarı oranına kadar indirilmesi kabul edilmiştir. Bu yarı oranına kadar indirme seçenek yaptırımları her ikisi bakımından da geçerlidir. Yani faile ister hapis cezası isterse adli para cezası verilmiş olsun, her ikisi de ikinci fıkrada belirtilen halin söz konusu olması durumunda yarı oranına kadar indirilecektir [144].

Sistemi engelleme, bozma, verileri yok etme veya değiştirme (Madde 244)

Bir bilişim sisteminin işleyişini engelleyen ve bozan kişiye bir yıldan beş yıla kadar hapis; bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişiye ise altı aydan üç yıla kadar hapis cezası bu madde ile öngörülmüştür. Bu ihlalin banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sisteminde işlenmesi ise yarı oranında arttırılması şeklinde cezai müeyyide olarak belirlenmiştir (TCK 244 Madde Gerekçesi).

Bu maddede bilişim sistemlerinin engellenişi yıkıcı siber suçları ve özellikle de internet sitelerine genel erişimi engelleyen DDoS saldırılarını ifade etmektedir. 244. Maddenin 2. fıkrasında virüsler, trojanlar, keylogger ve screenlogger kategorisindeki casus yazılımlarla yapılan uygulamalar da kapsam dâhiline alınmıştır [145].

İşlenecek suçların bu madde kapsamında cezalandırılabilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerektiği, örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturması hâlinde, bu fıkra hükmüne istinaden cezaya hükmedileceği madde gerekçesinde açıkça belirtilmiştir. Ayrıca; Kişilere karşı işlenen suçlar ile banka veya kredi kurumlarına ve kamu kurumlarına yönelik işlenen suçların cezaları arasında ayrıma gidilmesi anlamlıdır [146].

Banka veya kredi kartlarının kötüye kullanılması (Madde 245)

Mevduat hesabı veya özel cari hesapların kullanımı dâhil bankacılık hizmetlerinden yararlanmayı sağlayan olarak tanımlanan banka kartı ile nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fizikî varlığı bulunmayan kart numarası olarak tanımlanan kredi kartı ile ilgili işlenecek suçlarda bankaların veya kredi sahiplerinin zarara sokulmasını, bu yolla çıkar sağlanmasını önlemek ve failleri cezalandırmak amacıyla bu madde kaleme alınmıştır.

Temel olarak söz konusu hükümle, banka ve kredi kartlarını hukuka aykırı kullanma, sahte banka veya kredi kartı üretme, satma, devretme veya kabul etme, sahte banka veya kredi kartları oluşturma ve kullanma fiilleri, yaptırım altına alınmıştır [83].

Tüzel kişiler hakkında güvenlik tedbiri uygulanması (Madde 246)

Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunduğu madde metninde belirtilmektedir.

7.5.2. Türk Ceza Kanunu'nda bulunan diğer bilişim suçları

Özel hayata ve hayatın gizli alanına karşı suçlar

Haberleşmenin gizliliğini ihlâl (Madde 132)

Haberleşmenin gizliliğini ihlal, haberleşmenin içeriğinin ifşası, haberleşmenin tarafının haberleşmenin içeriğini diğer tarafın rızası olmadan alenen ifşası ve bu verilerin içeriğinin basın ve yayın yoluyla yayınlanması şeklinde üç fıkra olarak öngören madde ile belirli kişiler arasındaki haberleşmenin içeriğinin öğrenilmesi engellenmek istenmiştir.

Gelişen teknoloji sayesinde, iletişim çoğunlukla bilişim teknolojileri vasıtasıyla yapılmakta ve bunun için internet, elektronik posta, video konferans, anlık mesajlaşma vb. hizmetler yoğun olarak kullanılmaktadır. Özellikle internet olmak üzere, her türlü bilişim sisteminde gerçekleşen, kişiler arasında gerçekleşen iletişimi açıklayan kişiler suç işlemiş olurlar.

Bu hususta kanun koyucu suçun ne şekilde işlendiğinin ve suçu işleyen kişinin haberleşmede taraf olup olmamasının önemli olmadığını vurgulamıştır (TCK 132 Madde Gerekçesi).

Kayıt cihazıyla haberleşmenin kayda alınması suçun bu nitelikli hâli gerçekleştirmekte ise de, kişiler arasındaki haberleşme içeriklerinin belli bir suça ilişkin soruşturma kapsamında Anayasa ve kanunların belirlediği koşullar çerçevesinde öğrenilmesinin veya kayda alınmasının hukuka uygun olduğu savunulmaktadır (TCK 132 Madde Gerekçesi) .

Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması (Madde 133)

Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması da Türk Ceza Kanunu 133. maddede düzenlenmiş bir suçtur. Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki aydan altı aya kadar hapis cezası ile cezalandırılır. Yine katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aya kadar hapis veya adli para cezası ile cezalandırılır. Maddenin son fıkrasına göre, yukarıdaki fıkralarda yazılı fiillerden biri işlenerek elde edildiği bilinen bilgilerden yarar sağlayan veya bunları başkalarına veren veya diğer kişilerin bilgi edinmelerini temin eden kişi, altı aydan iki yıla kadar hapis ve bin güne kadar adli para cezası ile cezalandırılır. Bu konuşmaların basın ve yayın yoluyla yayınlanması halinde de, aynı cezaya hükmolunur.

Kişiler arasındaki aleni olmayan konuşmaların dinlenmesi ve kayda alınması suç olarak tanımlanmaktadır. Bir konuşmanın aleni olmayan konuşma olarak kabul edilmesi için konuşulan yerin önemi yoktur (TCK 132 Madde Gerekçesi). Bir evde veya halka açık bir alanda yapılan konuşma, özel bir gayret gösterilip dinlenebiliyorsa aleni olmayan bir konuşma olarak kabul edilir.

Görüldüğü gibi bu suçun ilk bölümünde izinsiz konuşmaları dinleme ve ses cihazı ile kayda alma suç olarak düzenlenmiştir. Maddenin son fıkrası ise, bu bilgileri kullanma eylemlerini cezalandırmaktadır. İnternette zaman zaman “call center”lardaki konuşmaların kayıtları dolaşmakta ve komiklik olsun diye bunlar herkese e-maille yollanmaktadır. Sadece komiklik olsun diye bunu postalamak “başkasına verme” eylemini oluşturan suçtur.

Yine bunları web sitesine komik videolarla yan yana koyup yayınlamak da “basın ve yayın yoluyla yayınlama” suçunu oluşturmaktadır [82]. Suçun işlenebilmesi için konuşan kişinin rızası olmadan yapılması gerekmektedir ve bu konuşma içeriklerinin basın ve yayın yoluyla yayınlanması, daha ağır ceza ile cezalandırılmayı gerektirmektedir.

Özel hayatın gizliliğini ihlâl (Madde 134)

Kişinin kendine özgü yaşayışı, yaşama tarzı, kendisini ilgilendiren tutum ve davranışı olarak tanımlanan özel hayat’a ait gizliliğin ihlal edilmesi halinde bir yıldan üç yıla kadar hapis cezası, bu ihlalin görüntü ve ses kaydı ile yapılması halinde ise cezanın bir kat oranında arttırılması şeklinde cezai müeyyide belirlenmiştir. Suçun nitelikli unsuru olarak ise ihlalin basın ve yayın yoluyla yapılmış olması şartı aranmaktadır.

Yasa koyucu tarafından, gizli yaşam alanına girerek veya başka suretle başkaları tarafından görülmesi mümkün olmayan bir özel yaşam olayının saptanması ve kaydedilmesinin cezalandırılması (TCK 134 Madde Gerekçesi) amaçlanmıştır. Bu bağlamda özel hayatın gizliliği konut dokunulmazlığı ihlal edilmek sureti ile olabileceği gibi uzaktan fotoğraf çekme, kamera ile kayda alma, çeşitli zararlı yazılımlar veya kişiyi aldatma suretiyle bilgisayar sistemlerine girme ve mahkeme kararı olmaksızın iletişim araçlarının dinlenmesi şeklinde olabilecektir.

Kişinin özel hayatına ilişkin görüntü veya seslerin hukuka aykırı olarak ifşa edilmesi ve yetkisiz kişilerce öğrenilmesi ise ayrı bir suç olarak tanımlanmıştır. Bu bakımdan özel hayata ilişkin kayıtların, savcılık veya mahkemeye verilmesi, duruşmada gösterilmesi ve dinlenmesi halinde, hukuka aykırılık bulunmadığı için söz konusu suç oluşmayacaktır (TCK 134 Madde Gerekçesi).

Özellikle son yıllarda artan ve paparazzi olarak nitelendirilen gazetecilerin yeni teknolojik gelişmeleri kullanarak kişilerin izinsiz fotoğraflarını ya da video görüntülerini çekmek suretiyle kişilik haklarının ihlal edilmesi bu madde ile koruma altına alınmıştır [147].

Kişisel verilerin kaydedilmesi (Madde 135)

Gelişen bilişim teknolojisiyle birlikte ülkemizde ve dünyada çok sık karşılaşılan ve aynı zamanda kişilik haklarına bir saldırı niteliği de taşıyan eylem türü, kişilerin rızaları olmaksızın kişisel verilerinin bilişim sistemlerine yerleştirilmesidir. Özellikle hastanelerin hastalarıyla ilgili, finans kurumlarının ve sigorta şirketlerinin müşterilerinin kredi olanağı ve ödeme gücüyle ilgili, ticari şirketlerin ise reklam ve pazarlama amacıyla bu tür verileri toplayıp kullandığı bilinmektedir. İşte bu tür bilgilerin sanal ortama veri olarak aktarılması ve bu yapılırken bu verilerin ilgilisinin izninin alınmaması inceleme konusu maddeyle suç tipi haline getirilmiştir [119].

Suçun konusunun kişisel verileri (gerçek kişiyle ilgili her türlü bilgi) olduğu, söz konusu suç tanımında kişisel verilerin bilgisayar ortamında veya kâğıt üzerinde kayda alınması arasında bir ayırım gözetilmediği, bu bakımdan, söz konusu suç tanımı ile Avrupa Konseyi bünyesinde hazırlanan Türkiye'nin de 28 Ocak 1981 tarihinde imzalamakla taraf olduğu "Kişisel Nitelikteki Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme"nin ilgili hükümlerine geçerlilik tanındığı madde gerekçesinde belirtilmiştir.

Kişisel verilerin kanuna aykırı bir şekilde kayda alınması suçun oluşması için gereklilik arz ederken, bu kayıtları ifşa eden kişilere uygulanacak cezanın artırımı söz konusudur (TCK 135 Madde Gerekçesi).

Verileri hukuka aykırı olarak verme veya ele geçirme (Madde 136)

Bu madde ile çok sık karşılaşılan ve en fazla işlenen bilişim suçu olan kimlik hırsızlığı eylemlerine karşı yaptırım uygulama imkânı sağlanmıştır.

Verileri yok etmeme (Madde 138)

İşlevi biten verilerin yok edilmesini hem birey hem de devlet ister. Çünkü vatandaşları hakkında sürekli bilgi toplayan ve bunları kaydeden, kısacası vatandaşlarını fişleyen bir devlet asla çoğulcu, özgürlükçü ve demokratik bir devlet olamaz ve vatandaşlarını da bu çağdaş ilkelere bağlı bir toplum haline getiremez. Bu madde ile bunun önüne geçilmek istenmektedir [119].

Hürriyete karşı suçlar

Haberleşmenin engellenmesi (Madde 124)

Kişinin insan olmasından kaynaklanan haberleşme hürriyeti Avrupa İnsan Hakları Sözleşmesinde (10. madde) şu şekilde yer almaktadır: "Herkes düşünceyi açıklama hakkına sahiptir. Bu hak düşünce hürriyetini ve resmi makamların müdahalesi ve memleket sınırları söz konusu olmaksızın, haber veya fikir almak veya vermek özgürlüğünü içerir. Bu madde, devletlerin radyo, sinema veya televizyon işletmelerini bir izin rejimine tabi kılmalarına engel değildir. Bu hürriyetlerin kullanılması, ulusal güvenliği, toprak bütünlüğü, kamu güvenliği, düzenin korunması, suçu önlenmesi, sağlığın ya da ahlakın ve başkalarının şöhret ya da haklarının korunması için, demokratik bir toplumda zorunlu önlemler niteliğinde olarak, gizli haberlerin açıklanmasının engellenmesi ya da yargı erkinin üstünlüğünün ve tarafsızlığının sağlanması bakımından, kanunla belirli işlemlere, koşullara, sınırlamalara ya da yaptırımlara bağlı tutulabilir."

BM Medeni ve Siyasi Haklar Sözleşmesinin 17.maddesine göre; hiç kimsenin haberleşmesine keyfi ya da yasa dışı olarak müdahale edilemez, kişinin bu gibi müdahalelere ve tecavüzlere karşı yasalarca korunma hakkı vardır. Bu sözleşmelere taraf devletler, ülkesinde yaşayan ve yetkisi altında bulunan bütün bireylere haberleşme hak ve özgürlüğünün tanınması ve korunması yükümlülüğü altındadır. Bu bağlamda iç hukukumuzda haberleşme özgürlüğünü korumaya yönelik düzenlemelere yer verilmiştir [148].

Söz konusu özgürlük TCK'da 124. Madde ile koruma altına alınmıştır. Maddenin birinci fıkrasında, kişiler arasındaki haberleşmenin engellenmesi, ikinci fıkrasında ise kamu kurumları arasındaki haberleşmenin hukuka aykırı olarak engellenmesi suç olarak tanımlanmıştır. Haberleşmenin yapıldığı araç önemli değildir. Örneğin, bu haberleşme mektupla veya telefonla yapılabilir. Haberleşmenin engellenmesi, çeşitli suretlerde gerçekleşebilir. Örneğin posta kutusundaki mektupların yırtılması, bir kişiye gönderilen mektupların ilgilisine verilmeyip çöp kutusuna atılması, telefon hatlarının kesilmesi, oluşturulan manyetik alanla telefon görüşmelerinin yapılamaz hâle getirilmesi gibi fiiller, söz konusu suçu oluşturur (TCK Madde 124 Gerekçesi).

Şerefe karşı suçlar

Hakaret (Madde 125. fkr.2)

Onur kırma, onura dokunma, küçültücü söz veya davranış (TDK 2014) olarak tanımlanan hakaret ile ilgili cezai hükümler TCK 125. maddede belirtilmiştir. Bu madde ile hakarete maruz kalan kişinin şeref, haysiyet ve namusu, toplum içindeki itibarı, diğer fertler nezdindeki saygınlığı korunmaktadır. Maddenin ikinci fıkrasında, hakaretin mağduru muhatap alan sesli, yazılı veya görüntülü bir mesajla yapılması hâlinde, birinci fıkra hükmüne istinaden cezaya hükmedileceği kabul edilmiştir. Buna göre, kişiyi muhatap alan mektup, telgraf, telefon vb. araçlarla yapılan hakaret de, huzurda hakaret olarak cezalandırılmalıdır (TCK 125 Madde Gerekçesi).

İnternette bir “özellik”ten söz edilse; mesela, “işkenceci”, “korkak”, “alçak”, “serseri”, “homoseksüel”, “esrarkeş”, “fahişe”, “ayı” dense, bunlar birer kötü huy veya özelliği belirtmeleri sebebiyle, sövme suçunu oluştururlar. Ayrıca, söylenen söz ilgilinin bedeni bir arızasına da ilişkin olabilir. Bir kimse hakkında “şaşı”, “topal”, “kambur”, “sarsak”, “kel” demek veya ruhî ve bedeni bir hastalık yüklemek, yahut gerçek dışı olarak belirli bir din veya ırkın üyesi olarak açıklamak da sövmedir. Bunun gibi, saldırıya uğrayan kişiye bir olay yöneltilmekle beraber, bunu açıklayacak tamamlayıcı unsurlar belirtilmemişse, yine sövme söz konusu olur [82].

Malvarlığına karşı suçlar

Nitelikli hırsızlık (Madde 142.fkr.2 b. "e")

TCK 142. madde ile "Hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi hâlinde, üç yıldan yedi yıla kadar hapis cezasına hükmolunduğu" belirtilmiştir. Bilişim sistemlerinin kullanılması marifetiyle işlenen hırsızlık suçu aynı maddenin birinci fıkrasında belirtilen hırsızlık suçlarına nazaran daha ağır şekilde cezalandırılmayı gerektiren nitelikli unsuru oluşturmaktadır (TCK 142 Madde Gerekçesi).

Nitelikli dolandırıcılık (Madde 158. fkr.1 b. "f")

Dolandırıcılık suçunun bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi hâlinde, iki yıldan yedi yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.

Dolandırıcılık suçunun, bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi de, birinci fıkranın (f) bendinde bu suçun bir nitelikli unsuru olarak kabul edilmiştir. Bilişim sistemlerinin ya da birer güven kurumu olan banka veya kredi kurumlarının araç olarak kullanılması, dolandırıcılık suçunun işlenmesi açısından önemli bir kolaylık sağlamaktadır. Banka ve kredi kurumları açısından dikkat edilmesi gereken husus, bu kurumları temsilen, bu kurumlar adına hareket eden kişilerin başkalarını kolaylıkla aldatabilmeleridir (TCK 158 Madde Gerekçesi).

Genel ahlâka karşı suçlar

Müstehcenlik (Madde 226)

Madde metninde, müstehcenlik ve çocukların bu tür zararlı yayınlara karşı korunmasına ilişkin hükümler düzenlenmiştir (TCK 226 Madde Gerekçesi).

İlgili madde metni şu şekildedir:

(1) a) Bir çocuğa müstehcen görüntü, yazı veya sözleri içeren ürünleri veren ya da bunların içeriğini gösteren, okuyan, okutan veya dinleten,

b) Bunların içeriklerini çocukların girebileceği veya görebileceği yerlerde ya da alenen gösteren, görülebilecek şekilde sergileyen, okuyan, okutan, söyleyen, söyleten,

c) Bu ürünleri, içeriğine vakıf olunabilecek şekilde satışa veya kiraya arz eden,

d) Bu ürünleri, bunların satışına mahsus alışveriş yerleri dışında, satışa arz eden, satan veya kiraya veren,

e) Bu ürünleri, sair mal veya hizmet satışları yanında veya dolayısıyla bedelsiz olarak veren veya dağıtan,

f) Bu ürünlerin reklamını yapan kişi, altı aydan iki yıla kadar hapis ve adlî para cezası ile cezalandırılır.

(2) Müstehcen görüntü, yazı veya sözleri basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden kişi, altı aydan üç yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

(3) Müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları kullanan kişi, beş yıldan on yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır. Bu ürünleri ülkeye sokan, çoğaltan, satışa arz eden, satan, nakleden, depolayan, ihraç eden, bulunduran ya da başkalarının kullanımına sunan kişi, iki yıldan beş yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

(4) Şiddet kullanılarak, hayvanlarla, ölmüş insan bedeni üzerinde veya doğal olmayan yoldan yapılan cinsel davranışlara ilişkin yazı, ses veya görüntüleri içeren ürünleri üreten, ülkeye sokan, satışa arz eden, satan, nakleden, depolayan, başkalarının kullanımına sunan veya bulunduran kişi, bir yıldan dört yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

(5) Üç ve dördüncü fıkralardaki ürünlerin içeriğini basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden ya da çocukların görmesini, dinlemesini veya okumasını sağlayan kişi, altı yıldan on yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

Avrupa Siber Suç Sözleşmesinde tek tek gösterilen çocukların istismarına yönelik her türlü eyleme karşı tedbir alınması gerektiği yaygın bir kanaattir. Günümüzde neredeyse kanayan bir yara haline gelen ve internetin ortaya çıkmasından beri bu çok yararlı ağ sisteminin en zararlı yanı olarak kabul edilen bilişim sistemleri aracılığıyla çocuk pornografisi içerikli verilerin üretimi, dağıtılması ve bulundurulması eylemlerinin bu sözleşme ile ayrıntılı olarak tarif edilmesi ve söz konusu eylemlerin sanal dahî olsa her türlü gerçekleştirilme şeklinin suç olarak düzenlenmesi, bu sözleşmenin dikkati çeken en önemli düzenlemelerinden birisidir. İşte söz konusu sözleşmede de ayrıntılı olarak belirtilen bu eylemlerin suç haline getirilmesinin çok acil şekilde yapılması gerekmesine rağmen TCK'da buna konuyla ilgili düzenleme olan 226. madde bu açıdan son derece yetersizdir [119].

7.5.3. Özel kanunlarda bilişim suçları

TCK dışındaki diğer kanunlarda geçen bilişim suçları ile ilgili maddeler aşağıya çıkarılmıştır.

5846 Sayılı Fikir ve Sanat Eserleri Kanunu

5846 Sayılı Fikir ve Sanat Eserleri Kanunun 2. Maddesinde 07.06.1995 tarih ve 4110 sayılı kanun ile değişiklik yapılmış, eser kavramının tanımı yapılırken bilgisayar programları da koruma kapsamına alınmıştır.

5846 sayılı FSEK' in 6. maddesine 4110 sayılı kanun ile eklenen (10) numaralı bend ile "Bir bilgisayar programının uyarlanması, düzenlenmesi veya her hangi bir değişim yapılması da fikir ve sanat eseri sayılmaktadır."

Manevi, mali veya bağlantılı haklara tecavüz (Madde 71)

Bu Kanunda koruma altına alınan fikir ve sanat eserleriyle ilgili manevi, mali veya bağlantılı hakları ihlal ederek:

1. Bir eseri, icrayı, fonogramı veya yapımı hak sahibi kişilerin yazılı izni olmaksızın işleyen, temsil eden, çoğaltan, değiştiren, dağıtan, her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma ileten, yayımlayan ya da hukuka aykırı olarak işlenen veya çoğaltılan eserleri satışa arz eden, satan, kiralamak veya ödünç vermek suretiyle ya da sair şekilde yayan, ticarî amaçla satın alan, ithal veya ihraç eden, kişisel kullanım amacı dışında elinde bulunduran ya da depolayan kişi hakkında bir yıldan beş yıla kadar hapis veya adlî para cezasına hükmolunur.

2. Başkasına ait esere, kendi eseri olarak ad koyan kişi; altı aydan iki yıla kadar hapis veya adlî para cezasıyla cezalandırılır. Bu fiilin dağıtmak veya yayımlamak suretiyle işlenmesi hâlinde, hapis cezasının üst sınırı beş yıl olup, adlî para cezasına hükmolunamaz.

3. Bir eserden kaynak göstermeksizin iktibasta bulunan kişi; altı aydan iki yıla kadar hapis veya adlî para cezasıyla cezalandırılır.

4. Hak sahibi kişilerin izni olmaksızın, alenileşmemiş bir eserin muhtevası hakkında kamuya açıklamada bulunan kişi, altı aya kadar hapis cezası ile cezalandırılır.

5. Bir eserle ilgili olarak yetersiz, yanlış veya aldatıcı mahiyette kaynak gösteren kişi, altı aya kadar hapis cezası ile cezalandırılır.

6. Bir eseri, icrayı, fonogramı veya yapımı, tanınmış bir başkasının adını kullanarak çoğaltan, dağıtan, yayan veya yayımlayan kişi, üç aydan bir yıla kadar hapis veya adlî para cezasıyla cezalandırılır.

Bu Kanunun ek 4 üncü maddesinin birinci fıkrasında bahsi geçen fiilleri yetkisiz olarak işleyenler ile bu Kanunda tanınmış hakları ihlâl etmeye devam eden bilgi içerik sağlayıcılar hakkında, fiilleri daha ağır cezayı gerektiren bir suç oluşturmadığı takdirde, üç aydan iki yıla kadar hapis cezasına hükmolunur.

Hukuka aykırı olarak üretilmiş, işlenmiş, çoğaltılmış, dağıtılmış veya yayımlanmış bir eseri, icrayı, fonogramı veya yapımı satışa arz eden, satan veya satın alan kişi, kovuşturma evresinden önce bunları kimden temin ettiğini bildirerek yakalanmalarını sağladığı takdirde, hakkında verilecek cezadan indirim yapılabileceği gibi ceza vermekten de vazgeçilebilir.

Koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri (Madde 72)

Bir bilgisayar programının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla oluşturulmuş ilave programları etkisiz kılmaya yönelik program veya teknik donanımları üreten, satışa arz eden, satan veya kişisel kullanım amacı dışında elinde bulunduran kişi; altı aydan iki yıla kadar hapis cezasıyla cezalandırılır.

7.5.4. 5070 sayılı Elektronik İmza Kanununda düzenlenen bilişim suçları

<u>İmza oluşturma verilerinin izinsiz kullanımı (Madde 16)</u>

Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adlî para cezasıyla cezalandırılırlar.

Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

Elektronik sertifikalarda sahtekârlık (Madde 17)

Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile bu elektronik sertifikaları bilerek kullananlar, iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adlî para cezasıyla cezalandırılır.

Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

7.5.5. İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun

Erişimin engellenmesi kararı ve yerine getirilmesi (MADDE 8)

(1) İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir:

a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;

1) İntihara yönlendirme (madde 84),

2) Çocukların cinsel istismarı (madde 103, birinci fıkra),

3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),

4) Sağlık için tehlikeli madde temini (madde 194),

5) Müstehcenlik (madde 226),

6) Fuhuş (madde 227),

7) Kumar oynanması için yer ve imkân sağlama (madde 228),suçları.

b) 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.

(2) Erişimin engellenmesi kararı, soruşturma evresinde hâkim, kovuşturma evresinde ise mahkeme tarafından verilir. Soruşturma evresinde, gecikmesinde sakınca bulunan hallerde Cumhuriyet Savcısı tarafından da erişimin engellenmesine karar verilebilir. Bu durumda Cumhuriyet Savcısı kararını yirmidört saat içinde hâkimin onayına sunar ve hâkim, kararını en geç yirmidört saat içinde verir.

Bu süre içinde kararın onaylanmaması halinde tedbir, Cumhuriyet savcısı tarafından derhal kaldırılır. Koruma tedbiri olarak verilen erişimin engellenmesine ilişkin karara 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz edilebilir.

(3) Hâkim, mahkeme veya Cumhuriyet savcısı tarafından verilen erişimin engellenmesi kararının birer örneği, gereği yapılmak üzere Başkanlığa gönderilir.

(4) 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) numaralı alt bentlerinde yazılı suçları oluşturan yayınlara ilişkin olarak erişimin engellenmesi kararı re'sen Başkanlık tarafından verilir. Bu karar, erişim sağlayıcısına bildirilerek gereğinin yerine getirilmesi istenir.

(5) Erişimin engellenmesi kararının gereği, derhal ve en geç kararın bildirilmesi anından itibaren yirmidört saat içinde yerine getirilir.

(6) Başkanlık tarafından verilen erişimin engellenmesi kararının konusunu oluşturan yayını yapanların kimliklerinin belirlenmesi halinde, Başkanlık tarafından, Cumhuriyet başsavcılığına suç duyurusunda bulunulur.

(7) Soruşturma sonucunda kovuşturmaya yer olmadığı kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda Cumhuriyet savcısı, kovuşturmaya yer olmadığı kararının bir örneğini Başkanlığa gönderir.

(8) Kovuşturma evresinde beraat kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda mahkemece beraat kararının bir örneği Başkanlığa gönderilir.

(9) Konusu birinci fıkrada sayılan suçları oluşturan içeriğin yayından çıkarılması halinde; erişimin engellenmesi kararı, soruşturma evresinde Cumhuriyet Savcısı, kovuşturma evresinde mahkeme tarafından kaldırılır.

(10) Koruma tedbiri olarak verilen erişimin engellenmesi kararının gereğini yerine getirmeyen yer veya erişim sağlayıcılarının sorumluları, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, altı aydan iki yıla kadar hapis cezası ile cezalandırılır.

(11) İdarî tedbir olarak verilen erişimin engellenmesi kararının yerine getirilmemesi halinde, Başkanlık tarafından erişim sağlayıcısına, onbin Yeni Türk Lirasından yüzbin Yeni Türk Lirasına kadar idarî para cezası verilir. İdarî para cezasının verildiği andan itibaren yirmidört saat içinde, kararın yerine getirilmemesi halinde ise Başkanlığın talebi üzerine Kurum tarafından yetkilendirmenin iptaline karar verilebilir.

(12) Bu Kanunda tanımlanan kabahatler dolayısıyla Başkanlık veya Kurum tarafından verilen idarî para cezalarına ilişkin kararlara karşı, 6/1/1982 tarihli ve 2577 sayılı İdarî Yargılama Usulü Kanunu hükümlerine göre kanun yoluna başvurulabilir.

(13) İşlemlerin yürütülmesi için Başkanlığa gönderilen hakim ve mahkeme kararlarına 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre Başkanlıkça itiraz edilebilir.

(14) 14/3/2007 tarihli ve 5602 sayılı Şans Oyunları Hasılatından Alınan Vergi, Fon ve Payların Düzenlenmesi Hakkında Kanunun 3 üncü maddesinin birinci fıkrasının (ç) bendinde tanımlanan kurum ve kuruluşlar, kendi görev alanına giren suçların internet ortamında işlendiğini tespit etmeleri halinde, bu yayınlarla ilgili olarak erişimin engellenmesi kararı alabilirler. Erişimin engellenmesi kararları uygulanmak üzere Telekomünikasyon İletişim Başkanlığına gönderilir.

7.5.6. Sanal ortamda işlenen suçlar sözleşmesi

Avrupa Konseyi bünyesinde hazırlanarak, 23 Kasım 2001 tarihinde Budapeşte'de imzaya açılan ve 1 Temmuz 2004 tarihinde yürürlüğe giren sözleşme, ülkemiz tarafından iç hukuk düzenlemelerinin tamamlanmasının ardından taraf olunmasının uygun olunacağı değerlendirilmiştir. Söz konusu sözleşmeyle ilgili sorumlulukları bulunan bakanlıkların iç hukuk gerekliliklerini yerine getirdiklerini bildirmelerini müteakip sözleşme, 10 Kasım 2010 tarihinde imzalanmıştır.

7.6. Eğitim, Kapasite Artırımı ve Farkındalık Çalışmaları

İlk, orta, lise eğitimi ve yaygın eğitimde siber güvenlik eğitimlerinin yaygınlaştırılması başlığında, USGS'nin 22 numaralı eylem planı doğrultusunda Millî Eğitim Bakanlığının sorumluluğuna;

- Meslek liselerinin bilgisayar programcılığı bölümlerinin müfredatına siber güvenliğin eklenmesi,
- Bilişim teknolojileri alanı altında yer alan kurs programları arasında siber güvenlik konusuna yer verilmesi,
- Fırsatları Arttırma ve Teknolojiyi İyileştirme Hareketi (FATİH) Projesi kapsamına siber güvenlik eğitimlerinin dâhil edilmesi,
- Bilgi teknolojileri eğitimlerinde açık kaynak kodlu ürünlerin de yer alması Alt Eylemleri verilmiştir.

10,6 milyon tablet bilgisayarın temin edilip ortaokul ve lise öğrencilerine dağıtılacağı FATİH Projesi ve Eğitim Bilişim Ağının güvenliğinin sağlanması da öncelikli konular arasında bulunmaktadır. Meslek liselerinin müfredatına siber güvenlik dersleri henüz eklenmemiştir.

İlköğretim ve lise öğrencilerine; Siber Suçlar ve İnternet Güvenliği, Sosyal Ağlar, Siber Zorbalık, Siber Tuzaklar, Siber Hırsızlık, Siber Uzayda Farkındalık vb. eğitimler verilmektedir.

Yüksek Öğretim Kurulu tarafından siber güvenlik konusunda doktora ve yüksek lisans yapacak öğrencilere burs temin edilmesine yönelik karar almış ve komisyon kurmuştur. Ayrıca, TÜBİTAK tarafından siber güvenlik yaz kampı ve üniversiteler arası siber güvenlik yarışması düzenlenmekte ve başarılı olan öğrencilere USOM'da istihdam olanağı sağlamaktadır.

Hali hazırda 7 üniversitede siber güvenlik ve bilgi güvenliği programları adı altında yüksek lisans programı, Gazi Üniversitesi ve İstanbul Teknik Üniversitesinde doktora programı eğitimlerine başlanmıştır.

7.7. Uluslararası İşbirliği

Uluslararası işbirliği ile ilgili olarak USGS'nin 24 numaralı eylem maddesi "Ulusal ve uluslararası siber güvenlik etkinliklerinin düzenlenmesi" UDHB'na vermiştir. Bu kapsamda; uluslararası işbirliğini geliştirmek, siber güvenlik alanındaki kapasiteyi arttırmak, siber saldırılara karşı tepki kabiliyetlerini geliştirmek, kurum içi, kurumlar arası ve uluslararası koordinasyonu geliştirmek ve bu konudaki farkındalık seviyesini arttırmak maksadıyla BTK koordinasyonunda 2012, 2013 ve 2014 yıllarında Siber Kalkan Tatbikatları düzenlenmiştir [149].

7.8. Ar-Ge Faaliyetleri

Ulusal ve uluslararası Ar-Ge çalışmaları yapmak, yüksek lisans ve doktora tez çalışmaları yapmak, ürün/yöntem geliştirmek, patent çalışmaları yapmak, güncel yayınlar yapmak ve çalıştay/konferans düzenlemek maksadıyla Ortadoğu Teknik Üniversitesi bünyesinde 15 Nisan 2014 tarihinde Siber Güvenlik ve Savunma Araştırma Laboratuvarı (CyDeS) teşkil edilmiştir [150]. Etkinlik olarak sadece uluslararası öğrenciler için uygulamalı siber savunma eğitimi ve beş günlük yaz okulu (Cyber Risk Informatics) gerçekleştirilmiştir.

Bilgi ve veri güvenliği kapsamında çalışmalar yapmak üzere BİLGEM bünyesinde 17 adet laboratuvar hizmet vermektedir. Türkiye için kritik ve stratejik önemi olan genetik veri güvenliği, genomik veri analizi (biyoenformatik) ve biyosensör alanlarında çalışmalar yapan İleri Genom ve Biyoenformatik Laoratuvarı, siber tehditlerin etkileri öngörmeye ve muhtemel çözüm önerileri sunmaya çalışan Bilgi Güvenliği Risk Analiz Birimi bu araştırma birimlerine örnek olarak verilebilir.

7.9. Acil Müdahale Ekipleri

Ulusal Siber Güvenlik Stratejisinin 4 numaralı eylem planı, Ulusal Siber Olaylara Müdahale Merkezini ile Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin oluşturulması görevini UDHB sorumluluğunda kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlara ihdas etmiştir.

USGS ve 11 Kasım 2013 tarihli 28818 sayılı Resmi Gazetede yayımlanan Ulaştırma, Denizcilik ve Haberleşme Bakanlığından: Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ ile;

- Bakanlıkların bünyesinde, hizmet gereklerine göre bağlı birimlerini ve ilgili kurumları kapsayacak şekilde kurumsal SOME kurulabileceği,
- Kurumsal SOME'ler kurumlarına doğrudan ya da dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemleri alma veya aldırma, bu tür olaylara karşı müdahale edebilecek mekanizmayı ve olay kayıt sistemlerini kurma veya kurdurma ve kurumlarının bilgi güvenliğini sağlamaya yönelik çalışmaları yapmak veya yaptırmakla yükümlü oldukları,
- Kurumsal SOME'ler 7/24 erişilebilir olan iletişim bilgilerini belirleyerek birlikte çalıştığı sektörel SOME'lere ve USOM'a bildireceği,
- Sektörel SOME'lerin düzenleyici ve denetleyici kurumların bünyesinde kendi sektörlerinde faaliyet gösteren kurum, kuruluş ve işletmeleri kapsayacak şekilde kurulacağı,
- Kritik sektörlerde, sektörel SOME kurulması zorunlu olduğu,
- Düzenleyici ve denetleyici kurumlardaki sektörel SOME'lerin eşgüdümünün Bilgi Teknolojileri ve İletişim Kurumu tarafından yürütüleceği bildirilmiştir.

Bu bağlamda; eylem planında planlanan bitiş tarihi doğrultusunda USOM'un kurulması, çalışma usul ve esasları belirlenmesi Mayıs 2013'te gerçekleşmiştir. Yaklaşık 80 adet kurumsal web sitesi 7 gün 24 saat esası ile siber saldırılara karşı izlenmektedir. USOM'un resmi web sitesinde ise faydalı dokümanlar, tespit edilen zafiyetlere karşı güvenlik bildirimleri güncel olarak yayımlanmaktadır. 31 Ekim 2013 tarihinde düzenlenen Siber Organizasyon Seminerinde, 30 kurumdan 70 temsilcinin katılımıyla USGS'nin bir yıllık hedefleri görüşülmüştür.

Temel görevi USOM ile beraber koordinasyon ve işbirliği olan Sektörel SOME'ler ve kurumların ihtiyacı olan siber güvenlik yönetimini sağlamak olan Kurumsal SOME'lerin sadece BTK, Dışişleri Bakanlığı, PTT, Türksat, THY ve Genelkurmay Başkanlığı tarafından kurulduğu ve Eylül 2014'e kadar diğer kurumlar tarafından kurulması planlandığı Siber Güvenlik Kurulu 3. Toplantısında bildirilmiştir.

Örneğin, Genelkurmay Başkanlığı Kurumsal SOME'si olarak görev yapan TSK Siber Savunma Komutanlığınca; USOM ile eşgüdüm içerisinde çalışıldığı, kendisine bağlı birimlere aylık bilgilendirme raporları hazırlanıp yayımlandığı, kritik görevde bulunan teknik personele şifreli giriş yetkisi verilerek zararlı yazılımların çalışma esasları hakkında bilgilendirme yapıldığı, kendilerine bağlı web sitelerine planlı ve plansız olarak sızma testleri gerçekleştirildiği bilinmektedir.

7.10. Diğer Hususlar

TÜBİTAK Siber Güvenlik Enstitüsü tarafından;

- Daha etkin ve yüksek standartlarda testler gerçekleştirmek için SGE araştırmacıları tarafından yeni açıklık istismar (exploitation) yöntemleri ve araçları araştırılmakta ve geliştirilmektedir. Testlerin kapsamının ve derinliğinin belirlenmesi, test sonuç raporlarının kalitesinin ve tarafsızlığının arttırılmasına yönelik çalıştaylar organize edilmekte, düzenleyici kurumlarla ortak projeler gerçekleştirilmektedir.
- Güvenli yazılım geliştirme eğitimleri, Yazılım geliştirirken yapılan yanlışlıklar sonucunda oluşan açıklıkları tespit etmek için yazılım kaynak kodu analizi, Güvenli yazılım geliştirme süreçlerini daha etkin kılmak için risk analizi ve tehdit modelleme, Yeni güvenli yazılım geliştirme yöntemlerini araştırma ve uygulama, Güvenli yazılım geliştirme çalıştayları ve konferansları gerçekleştirme konularıda kamu kurum/kuruluşlarına ve özel sektöre destek vermektedir.
- APT tespitine yönelik, talep eden kurumlarda bilgisayar ve ağ sistemleri üzerinde analiz çalışmaları yapılmaktadır. Yapılan bu çalışmalar, bilgisayar sistemleri üzerinde davranış temelli analizleri ve ağ adli bilişim analizlerini içermektedir.
- Zararlı Yazılım Analiz Birimi bünyesinde yürütülen çalışmalar ile güncel zararlı yazılım trendini yakından takip etmekte, ülkemizin kritik altyapı ve servislerine yönelik tehdit oluşturabilecek zararlı yazılımların karakteristiklerini analiz etmektedir. Elde edilen sonuçlar ve alınması gereken önlemler bilgi paylaşım ortamları üzerinden ilgili kurumlara sunulmaktadır.

- BT ürün güvenliğine yönelik çalışmalar SGE bünyesinde yer alan BT Ürün Güvenliği Laboratuvarında yapılmaktadır. Laboratuvarda güvenlik fonksiyonu içeren BT ürünlerinin zayıflık ve açıklıklarını tespit ederek bu ürünlerin güvenlik değerlendirmesini gerçekleştirmektedir.
- Ar-Ge, Danışmanlık ve SOME çalışmalarında kazandığı deneyimi verdiği eğitimler aracılığı ile talep eden kurumlara aktarmaktadır. Eğitimler ihtiyaç sahibi kurumların isteği üstüne planlanarak gerçekleştirilmektedir [151].

Uluslararası Siber Savaş ve Güvenlik Konferansında UDHB Siber Güvenlik Daire Başkanı Emine ALTINTAŞ tarafından;

- Türk Standartları Enstitüsü tarafından test laboratuvarında belgelendirmeye yönelik testler yapılmakta ve ayrıca sızma testi yapan personel ile firmalar için idarî ve teknik kriterler hazırlanmış olup belgelendirmelerin yapıldığı,
- Kamu kurumları arasında güvenli bir ağ üzerinden veri aktarımı için Kamunet projesi hazırlandığı ve bu konudaki çalışmaların bitmek üzere olduğu,
- Eylem planı kapsamında Adalet Bakanlığı koordinasyonunda, UDHB ve diğer kamu kurumlarının katkıları ile Siber Güvenlik Kanun Taslağı hazırlandığı,
- UDHB koordinasyonunda kurum/kuruluşlar, özel sektör ve akademisyenlerin katılımı ile gerçekleştirilecek olan “Ulusal Siber Güvenlik Stratejisi Güncellenmesi ve 2015-2016 Eylem Planının” hazırlanması çalışmalarına başlandığı bildirilmiştir [152].

Cumhurbaşkanlığı tarafından, Devlet Denetleme Kuruluna (DDK), Türkiye’de kişisel verilerin korunması konusunun önem kazanması ve bu konuda bilgi sistemlerinin güvenliğinin öneminin ortaya çıkması ile birlikte, gerek mevzuat gerekse uygulama alanında yaşanan eksiklik ve aksaklıkların değerlendirilmesi ve alınması gerekli önlemlerin tespiti amacıyla kamuya ait bilgi sistemlerinin bilgi güvenliği ve kişisel veri mahremiyeti açısından incelenmesi görevi verilmiştir. DDK'nın kamu kesiminin, kişisel verilerin korunması ve bununla bağlantılı olarak bilgi güvenliği açısından genel durumunun ortaya konulması amaçlayan 27 Kasım 2013 tarihli raporu için kişisel verinin en çok kullanıldığı 6 kurum seçilmiştir. Bu kurumlar Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, Tapu ve

Kadastro Genel Müdürlüğü, Gelir İdaresi Başkanlığı, Sosyal Güvenlik Kurumu, Sağlık Bakanlığı ve Adalet Bakanlığıdır.

Söz konusu raporda bilgi sistem merkezlerindeki fiziki güvenlik önlemlerinin yetersiz olması, kaynak kod dâhil bilgi sistemleri üzerindeki işlem kayıtlarının tutulmasında ciddi eksiklikler bulunması, güvenlik önlemi alınmadan bir CD içerisinde 13,8 milyon kişinin adres ve kimlik bilgisinin paylaşıldığı münferit örnekler, felaket kurtarma merkezlerinin bulunmaması, kurumların bazılarında güvenlik, yedekleme, yama, parola politikalarının bulunmaması, bu konudaki uygulamaların çoğu kurumda kişilere bağlı ve bağımlı olarak gerçekleştirilmesi vb. güvenlik zafiyetlerinin bulunması dikkat çekicidir [153].

7.11. Ağ ve Bilgi Güvenliği Ajansının Belirlediği Kriterler Işığında Stratejilerin Karşılaştırılması

Ağ ve Bilgi Güvenliği Ajansının belirlediği kapsamlı kriterler kısaca hatırlatılmış ve üç ülkenin ulusal siber güvenlik stratejilerinin karşılaştırılması yapılarak Çizelge 7.2'de kıyaslanmıştır.

Vizyonu, kapsamı, hedefleri ve öncelikleri belirleme

Siber güvenlik stratejisinin amacı global direnci ve bilgi teknolojilerinin güvenliğini arttırmaktır. Açıkça belirtilmiş hedef ve önceliklerin belirlenerek bu amaca erişmede başarı sağlanabilecektir. Üç ülkenin USGS'leri incelendiğinde İngiltere bu kavramları açıkça belirttiği ve erişilebilir seviyede tuttuğu gözlemlenmektedir. ABD strateji belgesinde ise stratejik amaçlar ve öncelikler tespit edilmiştir. Türkiye'nin strateji belgesindeki hedefler, ilkeler ve amaçlar ülkemize özgü olarak belirlenmemiştir.

Ulusal risk değerlendirmesi yaklaşımını takip etme

Siber güvenlik stratejisi hazırlanırken özellikle kritik altyapıların üzerinde durulması gerekmektedir. Bu adımda yapılması gereken en önemli husus kritik sektör ve altyapıların tanımlanması ve koruma planlarının hazırlanmasıdır. İngiltere'de kritik altyapı sektörleri tam anlamıyla tanımlanmış ve bunlarla ilgili sorumlu kurum teşkil edilmiştir.

ABD'de kritik altyapılara ilişkin özel yasa çıkarılmış, ayrılan bütçe bu yasa ile belirlenmiş ve konunun sorumlu olduğu bakanlık tarafından diğer kuruluşlara görevler verilmiştir. Türkiye'de kritik altyapılarla ilgili bir kurum bulunmamakla beraber bu tesislerin neler olduğu yasal mevzuat kapsamına dahi alınmamıştır.

Hâlihazırdaki politika, mevzuat ve kapasiteleri dikkate alma

Mevcut politikalar, mevzuat ve uygulamalar değerlendirilip dikkate alındıktan sonra önemli eksiklikler belirlenmelidir. Siber güvenliğin ulusal güvenlik politikasının bir parçası olması sağlanmalıdır. Her üç ülke de mevcut politikaların üzerine USGS'lerini inşa etmiştir, fakat Türkiye'de ulusal güvenlik politikasına (Millî Siyaset Belgesine) entegre edilmemiştir.

Şeffaf bir yönetim yapısı geliştirme

Siber güvenlik stratejisi ancak şeffaf yönetim yapısı oluşturulması ile başarılı olabilecektir. Stratejinin koordinatörü olarak kurumlar arası çalışma grubu veya bir kamu kurumu sorumlu olmalıdır, stratejinin kendisinden ve yaşam döngüsünden bizzat yükümlü olmalıdır. 2013-2014 Eylem Planı maddelerinde hangi kurum/bakanlık/kuruluşa hangi görevin verildiği açıkça belirtilmiştir fakat USGS'nin bütçelendirmesi ile ilgili kamuoyuna açıklanan herhangi bir husus yoktur. İngiltere ve ABD'de ise tüm sorumlu kurumlar, her sene bütçeden ne kadar payın hangi konu için ayrılacağı bellidir.

Paydaşları belirleme

Başarılı bir siber strateji kamu ve özel sektör arasında uygun bir eşgüdüm sağlanmasını gerektirmektedir. Kamu paydaşları politikalar, mevzuat ve operasyonel yetkilere sahipken, özel sektör paydaşları ise çoğunlukla kritik altyapıların sahibi olmaktadır. Türkiye'de devlet kurumlarına görevler verilmiş olsa da, özel sektördeki paydaşların belirlenmesi hususunda eksiklikler bulunmaktadır. İngiltere'de ise hangi kuruluşun stratejinin hangi bölümünde görev aldığı açıkça bellidir. ABD'de ise DHS tarafından koordinasyon sağlanmakta, hemen her sektörde bilgi paylaşımını sağlayacak olan Bilgi Paylaşımı ve Analiz Merkezleri teşkil edilmiştir.

Güvenilir bilgi paylaşım ortamı sağlama

Sürekli değişen ve hızına ayak uydurmakta güçlük çekilen bu çağda, paydaşlar arasında güvenli ve güçlü bilgi paylaşım mekanizmalarının kurulması hayatidir. Özellikle kritik altyapılardan sorumlu olan kurumların karşı karşıya kaldıkları tehditleri, riskleri ve hassasiyetleri diğer kurumlarla paylaşmaları çok önemlidir. İngiltere'de kurulu olan "Hub" ile kamu kurumları arasında güvenli bilgi paylaşımı yapılmaktadır. ABD ise güvenilir bilgi paylaşımı İç Güvenlik Bakanlığı bünyesinde teşkil edilen Homeland Security Information Network (HSIN) vasıtasıyla gerçekleştirilmektedir. Türkiye'de ise aynı işleve sahip olacak KamuNet henüz hizmete girmemiştir.

Ulusal siber acil durum planları oluşturma

Özellikle kritik altyapılarla ilgili büyük siber olayların yaşanma ihtimaline karşı acil müdahale ve kurtarma sürecinde geçici tedbirler ve yapılar oluşturulması gerekmektedir. Ulusal acil planlara da uyum sağlamalıdır. Her üç ülkenin acil durum planları mevcuttur, fakat Türkiye'de pek çok kurumun felaket kurtarma merkezleri teşkil edilmemiştir. Ayrıca, AFAD tarafından icra edilen Kritik Altyapılar ve Siber güvenlik grup çalışmasında; ulusal kritik altyapılarını korumak amacıyla Kritik Altyapıları Koruma Planı geliştirmesi ve Ulusal Kritik Altyapılar belirlenirken dikkate alınacak faktörlerin kapsam ve riskin boyutu olduğunun temel gereksinim olduğu belirtilmiştir [154].

Siber güvenlik tatbikatları icra etme

Toplumun ve kurumların doğal afetlerde, teknolojik arızalarda, siber saldırılarda ve acil durumlarda direncinin ve hazırlık seviyesini arttırmak için siber güvenlik tatbikatları icrası önemlidir. Her sene planlı olarak üç ülkede de tatbikatlar icra edilmektedir.

Temel güvenlik gereksinimlerini oluşturma

Her kamu ve özel sektör kurumu kendi bilgi altyapılarını tehdit ve risklerden korumak maksadıyla gerekli önlemleri almalıdır. İngiltere ve ABD'de hemen her kurumun siber güvenliğe dair politikası varken, Türkiye'de kurumsal siber güvenlik planları uygulanamamaktadır.

Olay raporlama mekanizmalarını oluşturma

Bir kişi veya kurumun tehdit ortamı ile ilgili ne kadar çok bilgisi olursa o kadar iyi önlem alması mümkün olmaktadır. Her üç ülkede de söz konusu mekanizmalar işlerken, Türkiye'de hali hazırda SOME teşkilatlanmalarını tamamlamayan kurumlar mevcuttur.

Kullanıcı farkındalığı

Farkındalığın artmasıyla kişi ve kurumlar dijital dünyada nasıl hareket edeceklerini ve kendilerini nasıl koruyacaklarını öğrenirler. Güvenlik ile ilgili farkındalık yaratma aktiviteleri organizasyon içinde ve dışında gerçekleştirilebilir. Örnek olarak, İngiltere ve ABD'de her yılın ekim ayı, siber güvenlik farkındalık ayı olarak kutlanmaktadır, fakat ülkemizde böyle bir uygulama yoktur.

Ar-Ge'yi teşvik etme

Yeni geliştirilen teknolojiler ticari olarak yaygınlaşmadan önce siber güvenlik yeterliliklerini yerine getirme durumları mutlaka incelenmelidir. Siber güvenlik stratejisi mutlaka araştırma-geliştirme yaşam döngüsünü muhteva etmelidir. Ar-Ge konusunda her üç ülke araştırma merkezleri kurmuştur, fakat Türkiye'de bu konuya ayrılan bütçe kısıtlıdır.

Eğitim programlarını güçlendirme

Üniversiteler ve Ar-Ge kurumları yeteri kadar siber güvenlik uzmanı yetiştirememektedir. Siber güvenlik bilgisayar biliminin bir parçası olarak değerlendirilmektedir, fakat sürekli değişen ve eğitim gerektiren konulara sahiptir. Değişik kademelerde görev yapan 200.000'den fazla kamu personeline, her eğitim seviyesindeki öğrencilere yönelik eğitim planları hazırlayan İngiltere Hükümeti eğitime üç yılda 23 milyon pound civarında bütçe ayırmıştır. ABD ise Eğitim Bakanlığı ile koordineli olarak eğitim programları teşkil etmiş; NICE, CAE, ICEC vb. programlar ile eğitim faaliyetlerini desteklemiştir. Türkiye'nin strateji belgesinde eğitim konuları dar kapsamlı olarak ele alınmıştır.

Acil durum müdahale kapasitesini oluşturma

Siber Olaylara Müdahale Ekiplerine (SOME) ve Ulusal Siber Olaylara Müdahale Merkezlerine (USOM) büyük görev düşmektedir. Aynı zamanda USOM ve SOME'ler diğer ülkelerdeki karşılıkları ile eşgüdüm sağlamakla sorumludurlar. Her üç ülkenin de acil durumlara müdahale ekipleri ve planları mevcuttur.

Siber suçun tespiti

Gerekli kanun maddeleri yasalaştırılmalı ve konu ile alakalı uluslararası anlaşmalar onaylanmalıdır. Ulusal uzman siber suç birimleri kurulmalı, kolluk kuvvetleri ile yargı mensuplarının sürekli ve özel eğitimlerden geçirilmeleri sağlanmalıdır. İngiltere'de bu konu ile ilgili İçişleri Bakanlığı, Organize Suç Birimi, Çocuk İstismarı ve Çevrimiçi Koruma, Polis Merkezi Elektronik Suç Birimi, polis kuvvetleri, Ulusal Dolandırıcılık Birimine görevler verilmiştir. Siber suçun tespiti ile ilgili ABD'de; FBI sorumluluğunda, istihbarat birimleri, İç Güvenlik Bakanlığı, kanun uygulayıcılar, akademik kuruluşlar, özel sektörle işbirliği içerisinde söz konusu faaliyet yürütülmektedir. Türkiye'de ise konu ile ilgili olarak çıkarılması gereken kanunlar halen hazırlanma aşamasındadır.

Uluslararası işbirliği sağlama

Strateji uluslararası eşgüdümü teşvik etmek için kullanılmalı, hangi ülkelerle ve hangi konularda işbirliği yapılacağına karar verilmelidir. Ulusal sorumlu kurum veya kuruluşa uluslararası işbirliğini arttırma yönünde görev verilmeli ve uluslararası anlaşmalara katılım sağlanmalıdır. İngiltere, uluslararası işbirliğini yasal mevzuat, eğitim ve siber suçun tespiti konularında dünyanın birçok ülkesi ile ortak yürütülen çalışmalar doğrultusunda sağlamaktadır. ABD, siber güvenlik konusundaki tecrübelerini özellikle Afrika ve Asya kıtası olmak üzere; birçok ülke, organizasyon ve şirketlere aktarmaktadır. Türkiye'de uluslararası işbirliği rutin gerçekleştirilen tatbikatlar seviyesinde gerçekleştirilmektedir.

Kamu-özel sektör işbirliği sağlama

Kamu-özel sektör işbirliği amaçlara ulaşabilmek için ortak hedeflerin belirlenmesi, tanımlı görev ve çalışma metodolojilerinin kullanılması üzerine kuruludur. Sağlıklı bir işbirliğinin tahsisi için karşılaşılacak güçlükler ve engeller kadar değişik bileşenler dikkate alınmalıdır. (Bu madde ile ilgili olarak Paydaşları Belirleme maddesinde gerekli bilgi verilmiştir.)

Güvenlik ve mahremiyeti dengeleme

Siber teröre karşı alınan tedbirler siber suçlara engel olmakla beraber kişisel mahremiyeti bazı durumlarda ihlal etmektedir. Bir siber güvenlik stratejisi kişisel mahremiyetle güvenlik olgusu arasında doğru dengeyi bulmalıdır. Her üç ülke strateji belgelerinde temel insan haklarını koruma konusunda ısrarlı olduklarını bildirmiştir.

Değerlendirme

Siber güvenlik stratejisi bir kere oluşturulduktan sonra hangi hedeflerin gerçekleştirilebildiği değerlendirilmelidir. Bu sayede tespit edilen hedeflere ulaşabilmek için düzeltici ve önleyici eylemlerde bulunulabilecektir.

İngiltere Hükümeti her sene sonunda siber güvenlik stratejilerinin ilerleme durumlarını gösteren raporlar yayımlamaktadır. Aynı şekilde Beyaz Saray tarafından siber güvenlik stratejisi ile ilgili alınan kararlar resmi internet sitesinden duyurulmaktadır. UDHB tarafından strateji belgesi hakkında herhangi bir değerlendirme raporu yayımlanmamıştır.

Ulusal siber güvenlik stratejisini güncelleme

Siber güvenlik stratejisi hazırlama bir kereye mahsus yapılması gereken bir süreç değildir. Bu, Planla-Uygula-Kontrol Et-Harekete Geç modeli olan; stratejilerin, politikaların, süreçlerin, ürünlerin oluşturulması safhasında kontrol ve sürekli gelişimi sağlayan bir yapıdır. Siber güvenlik stratejisinde geliştirme, uygulama, değerlendirme ve güncelleme olarak uygulanmaktadır.

İngiltere 2009 yılındaki stratejisini 2011 yılında güncellemiştir. ABD'de siber strateji belgeleri Beyaz Saray tarafından yayımlanan politika belgeleri ile güncellenmektedir. Türkiye ise 2014 yılında tamamlanması gereken eylem maddelerinin tamamlanma durumları ile ilgili olarak kamuoyunu bilgilendirmemiş, 2015-2016 Eylem Planının hazırlanması faaliyetlerine devam edildiği bilinmektedir.

Çizelge 7.2. ENISA kriterlerine göre ülke USGS'lerin karşılaştırılması

S.NU	GÖREVLER	İNG.	ABD.	TR.
1	Vizyonu, kapsamı, hedefleri ve öncelikleri belirleme	+	+	-
2	Ulusal risk değerlendirmesi yaklaşımını takip etme	+	+	-
3	Hâlihazırdaki politika, mevzuat ve kapasiteleri dikkate alma	+	+	+
4	Şeffaf bir yönetim yapısı geliştirme	+	+	-
5	Paydaşları belirleme	+	+	+
6	Güvenilir bilgi paylaşım ortamı sağlama	+	+	-
7	Ulusal siber acil durum planları oluşturma	+	+	+
8	Siber güvenlik tatbikatları icra etme	+	+	+
9	Temel güvenlik gereksinimlerini oluşturma	+	+	-
10	Olay raporlama mekanizmalarını oluşturma	+	+	+
11	Kullanıcı farkındalığı	+	+	-
12	Ar-Ge'yi teşvik etme	+	+	-
13	Eğitim programlarını güçlendirme	+	+	-
14	Acil durum müdahale kapasitesini oluşturma	+	+	+
15	Siber suçu tespit edebilme	+	+	-
16	Uluslararası işbirliği sağlama	+	+	-
17	Kamu-özel sektör işbirliği sağlama	+	+	-
18	Güvenlik ve mahremiyeti dengeleme	+	+	+
19	Değerlendirme	+	+	-
20	USGS'ni güncelleme	+	+	-

8. SONUÇ VE ÖNERİLER

Gelecek on yıl içerisinde dünyanın en büyük on ekonomisi içerisinde yer alma hedefi olan; bulunduğu jeostratejik ve jeopolitik konum itibariyle kurulduğu ilk günden itibaren birçok düşmanı olan, gelecekte de varlığını istemeyecek düşmanları olacak olan ülkemizde, ulusal bilgilerin güvenliğinin sağlanması hayati öneme haizdir. Ulusal bilgi güvenliğinin (aynı zamanda ulusal siber güvenliğin) sağlanması; bireyler, kurum ve kuruluşlar ile ulusal güvenliği sağlayacak şekilde stratejik seviyede planlama ve söz konusu planın sağlıklı uygulaması ile gerçekleştirilebilecektir.

8.1. Sonuçlar ve Değerlendirmeler

Tez çalışması sonucunda elde edilen en önemli bulgulardan birisi, siber güvenlik konusunun ve siber güvenliğin stratejik seviyede planlanması gerekliliğinin öneminin kamu ve özel sektör tarafından kavranmamasıdır. Dolayısıyla ulusal siber güvenliğin sağlanması için yapılması gereken çalışmalara ihtiyaç duyulmaktadır. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı incelendiğinde;

- Ülkemize özgü amaç, vizyon, misyon, temel ilkeler, stratejik hedef ve amaçların belirlenmediği,
- Stratejik planlama kapsamında vatandaş, özel sektör, kamu kurum ve kuruluşların üzerlerine düşen görevlerin açıklanmadığı,
- Eylem planlarının gerçekleştirilmesi gereken sürelerin aşılmasına rağmen, kamuoyu ile söz konusu eylem planlarının ilerleme durumları ile ilgili herhangi bir bildirim yapılmadığı,
- Siber kelimesinin Türk Dil Kurumu tarafından hazırlanan Büyük Türkçe Sözlükte karşılığının bulunmadığı ve TDK'nın hazırlaması gereken siber güvenlik terminolojisi ile sözlüğünün hazırlanmadığı,
- Siber suçlarla mücadelede mevcut yasaların yetersiz olduğu, Ulusal Bilgi Güvenliği Kanun Taslağı ile Kişisel Verilerin Korunması Kanun Taslağının henüz onaylanmadığı,

- Siber suç ile mücadele kapsamında görev yapan kolluk kuvvetleri ve yargı mensuplarına verilmesi gereken eğitimlere yer verilmediği,
- Kamu ve özel sektör arasında sağlanacak işbirliğine yeteri kadar önem verilmediği,
- Kritik altyapıların belirlenmesi, güvenliği, risk analizi ve alınması gereken tedbirlere yer verilmediği,
- Siber güvenliğin sağlanmasında ulusal istihbarat birimlerine görevler verilmediği,
- Eğitim ve farkındalık ile ilgili konuların yeterli olmadığı,
- Yazılım ve donanım ile ilgili ürün geliştirme standartların belirlenmesi gerektiği,
- Stratejik planlamanın sağlıklı yürütülebilmesi için bütçelendirme yapılmadığı,
- USGS'nin hazırlandığı tarihten günümüze kadar olan süreçte, stratejik doküman ile ilgili olarak ilerleme durumlarını gösteren herhangi bir rapor yayınlanmadığı tespit edilmiştir.

Ulusal siber güvenliğin sağlanması sayesinde kişisel bilgilerin güvenliği, kamu ve özel sektöre ait kritik bilgilerin güvenliği sağlanacaktır. Bu kapsamda ulusal siber güvenlik sadece kişi ve kurumların kendisi için değil ulusal güvenliğimizin sağlanması konusunda da ülkemiz için çok önem taşımaktadır.

8.2. Öneriler

Büyüyen siber tehditlere kişi, kurum veya ülke olarak nasıl karşılık verileceği konusu, kişisel mahremiyetten internetin geleceğine, bölgesel krizden belki de küresel savaşa kadar her şeyi şekillendirebilir. Kişisel veya kurumsal ölçekte ağ ve bilgi güvenliğinin sadece antivirüs yazılımları, güvenlik önlemleri hatta bilgi işlenen ağın internetten bağımsız hale getirilmesi ile bile önlenemeyeceği dünyada gerçekleşen büyük çaplı bilgi, veri, kimlik, para vb. hırsızlıkları ile kanıtlanmıştır. Siber güvenliğin (ulusal, kurumsal veya kişisel) yüzde yüz oranla sağlanması mümkün değildir. Özellikle ulusal çapta siber güvenliğin sağlanması için disiplinlerarası işbirliği içerisinde sıkı bir yapılanma ve çalışmaya ihtiyaç duyulmaktadır. İngiltere ve ABD ulusal siber güvenlik strateji belgeleri ve uyguladıkları politikaların incelendiği bu tez çalışmasında, ülkemizin stratejik planına önemli katkı sağlayacağı değerlendirilen hususlar belirlenmiş ve bu hususlara aşağıda yer verilerek öneriler sunulmuştur.

(1) Ülkemizde siber güvenliğin sağlanmasına dair Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı adlı politika belgesi bulunmaktadır. Yedi başlık altındaki 29 eylem planı haricinde kalan strateji bölümü ülkemize has olarak hazırlanmalıdır. Son yıllarda hazırlanan ve 4.Bölümde ayrıntılı olarak bahsedilen strateji belgelerinde olduğu gibi USGS'ne özgü amaç, vizyon ve temel ilkeler belirlenmelidir. Temel ilkeler belirlenirken; siber güvenlik sağlanırken kişisel hak ve özgürlükler mutlaka düşünülmeli ve güvenlik-özgürlük dengesi hiçbir zaman kullanıcıyı mağdur edecek şekilde planlanmamalıdır.

(2) Ülkemiz siber stratejisi belirlenirken; bilgi güvenliğinin idamesi ve siber uzayın faydalarının azaltılmaması göz önünde bulundurulmalıdır. Devletin siber güvenlikteki rolü kesin olarak belirlenmeli, vatandaşlara karşı sorumluluk asla göz ardı edilmemelidir. Stratejik eksenler belirlenmeli, stratejik amaçları destekleyecek belirgin, ulaşılabilir ve zaman eksenli alt hedefler tespit edilmelidir. USGS'nin eylem planlarının tamamlanma durumları ile ilgili olarak çalışmalar sürmektedir. Stratejinin güncellenmesinden önce mevcut eylem planlarının tamamlanma ve ilerleme durumları kamuya açıklanmalıdır.

(3) Ülkemizdeki iç ve dış çevrenin değerlendirilmesine yönelik SWOT Analizi yapılmalıdır. Belirlenecek iç ve dış tehditlerle ilgili olarak siber suçun tespiti kapsamında öncelikle siber güvenlik ile ilgili olan tanımlamalar yapılmalıdır. USGS'nin mevzuat çalışmaları ile ilgili 2 numaralı eylem maddesindeki alt eylem olan ve TDK'na sorumluluğu verilen "Siber güvenlik terminolojisinin ve sözlüğünün oluşturulması" konusundaki çalışmaların sonlandırılması ve kamuoyuna açıklanması gerekmektedir.

(4) Adalet Bakanlığı tarafından sürdürülen Ulusal Bilgi Güvenliği Kanun Taslağı, Anayasanın 20'nci maddesi ile temel hak olarak koruma altına alınan kişisel verilerin korunması ile ilgili olarak Kişisel Verilerin Korunması Kanun Taslağı derhal yasalaşmalıdır. Ayrıca 2014-2018 Bilgi Toplumu Stratejisi ve Eylem Planında (Taslak) da belirtilen bilişim alanında ortaya çıkan yeni suç türleri ile etkin mücadelenin sağlanması amacıyla siber suçla mücadele kurumlar arası koordinasyonu güçlendirmeyi amaçlayan Ulusal Siber Suç Stratejisi hazırlanmalı ve USGS'ne entegre edilmelidir.

(5) Siber suçla mücadelenin sağlam bir şekilde yapılması maksadıyla soruşturma ve kovuşturmanın adil bir şekilde gerçekleştirilmesi için adli bilişim ve delil tespiti süreçlerine önem verilmesi, bu safhalarda görev alan personelin teknik seviyede eğitim verilmesi gibi konular hazırlanması gereken Ulusal Siber Suç Stratejisinde yer almalıdır.

(6) Ulusal siber güvenlik stratejisinin güncellenmesi ve 2015-2016 Eylem Planının hazırlanması devlet kurumları üzerine düşecek tüm görev ve sorumlulukları açıkça belirtecek, mevcut yapıdaki yetki çatışması veya görev ve yetki açısından belirsizlikleri giderecek, kamu-özel sektör işbirliğini teşvik edecek ve siber güvenliği destekleyen devlet kaynaklı girişimler oluşturulacak şekilde ivedi olarak yapılmalıdır.

(7) Günümüz toplum yaşantısında, bilişim suçlarına sıradan suçlara uygulanan yaklaşım tarzı ile müdahale etmek veya önleyici önlemler almamak uygun bir hareket tarzı olmayacaktır. Hayatın her alanına giren teknolojik gelişmeler (özellikle cihazlar) kişiler tarafından hızla içselleştirilmekte, yaygın olarak kullanılmakta iken; bu yenilikler ile ilgili hukuki düzenlemelerin yapılmasında aynı çabukluk gösterilememektedir. Salt hukuk ve bilgisayar bilim insanlarının değil; aynı zamanda sosyoloji, psikoloji bilimine hizmet eden bilim insanlarının aktif katkıda bulunmaları gerekmektedir. Zira teknolojide gerçekleşen bir yeniliğin baş döndürücü hızına ayak uydurmak maksadıyla akademik ve yasal çalışmalar yapılması gerekmektedir. Ayrıca; ülkeler arası işbirliği ve yardımlaşmanın arttırılması öncelikli olacak şekilde, uluslararası sözleşmelerin imzalanması gerekmekte ve kanunu uygulayan personelin bu konuda eğitilmesi sağlanmalıdır. TCK'da "topluma karşı işlenen suçlar" bölümünde bulunan "bilişim alanında suçlar" bölümü yetersiz kaldığı aşikârdır. ABD ve Avrupa ülkelerinin kanunları incelenerek gerekirse ceza kanunu dışında, hâlihazırda işlenen tüm suçlara atıf yapılacak şekilde gerekli tanımlamalar yapılarak bilişim kanunu hazırlanmalı; özellikle mal varlığına ve çocukların istismar edilmesine karşı verilecek suç miktarları en üst düzeyde tutulmalıdır.

(8) Hayatımızın merkezinde bulunan temel ihtiyaçlarımızın bağlı olduğu fiziksel, ekonomik, sağlık, güvenlik konularını da kapsayan kritik altyapıların güvenliği ön plana çıkmaktadır. Sadece USGS için değil ulusal güvenliğimizi sağlayan Millî Güvenlik Siyaset Belgesine de dâhil edilecek şekilde kritik altyapılarımızın belirlenmesi yönünde çalışma yapılması önem arz etmektedir.

(9) Ülke bazında sorumlu bir kurum teşkil edilmeli, her kurum ve kuruluşun sahip olduğu varlıkların risk değerlendirmeleri yapılmalı ve kritiklik dereceleri belirlenmelidir. Bu bağlamda İngiltere'de teşkil edilen CPNI örnek teşkil edebilir. Ayrıca kritik altyapılarla ilgili ulusal bir plan hazırlanmalı ve bu planın Kritik Bilgi Altyapılarını ilgilendiren bölümleri USGS içerisinde yer almalıdır. UDHB Siber Güvenlik Daire Başkanlığı tarafından kritik altyapılar (Ulaşım, Finans, Kritik kamu servisleri, Telekomünikasyon, Kritik üretim tesisleri, Enerji ve Su) yeniden değerlendirilmeli ve kapsamı genişletilmelidir.

(10) Siber güvenliğin sağlanması için özel sektör, kamu sektörü, sivil toplum ve uluslararası kurum kuruluşlar uyum içerisinde çalışması gerekmektedir. Telekomünikasyon, enerji, finans gibi sektörlerin çoğu özel sektör tarafından işletilmektedir. Kamu-özel sektör işbirliğinin sağlanması ancak sağlıklı bilgi paylaşımı ile sağlanabilir. Yeni siber tehditlerin tespiti, etkin mücadelenin sağlanması, yazılımsal ve donanımsal önlemlerin alınması ile ilgili konularla ilgili bilgi alışverişi hızlı bir şekilde gerçekleştirilmelidir. Sektörel ve Kurumsal SOME teşkilatlanması ivedi olarak tamamlanmalı, söz konusu bilgi paylaşımı USOM vasıtasıyla yapılmalı ve bilgi paylaşım isteksizliğinde bulunulmaması sağlanacak tedbirlere USGS'nde yer verilmelidir. Unutulmamalıdır ki; edinilen bilgi paylaşıldıkça, tüm aktörlerin bilgi seviyeleri, durumsal farkındalıkları ve siber güvenlik hazırlık seviyeleri aynı oranda genişler. Ayrıca başta internet servis sağlayıcıları olmak üzere özel sektöre de stratejik seviyede görev bölümü yapılmalıdır. Bu işbölümü için İngiltere'nin yaptığı uygulamalar baz alınabilir.

(11) Siber Güvenlik Kurulu teşkilat yapısı incelendiğinde; sivil toplum kuruluşları, özel sektör temsilcileri ve hatta akademisyenlerin yer almadığı görülmektedir. Siber uzayı çoğunlukla halk kullanmakta, güvenliğini tahsis etme devletin sorumluluğunda olsa da; özel sektör tarafından siber güvenliğin sağlanması yönünde tedbirler alınmakta veya uygun çözümler sağlanmaktadır. Dolayısıyla siber güvenlikle ilgili alınacak kararlara özel sektör, akademik toplum ve sivil toplum kuruluşları tarafından katılım sağlanmalıdır.

(12) İngiltere ve ABD stratejileri ve teşkilatlanmaları incelendiğinde, ulusal istihbarat birimlerinin etkin şekilde görevlendirildiği göze çarpmaktadır. Siber güvenliği sadece savunma boyutu ile değil, aynı zamanda veri madenciliği, sosyal medya mühendisliği, büyük veri gibi olguları kullanarak önleyici tedbirlerin bu birimler tarafından alındığı bilinmektedir. Bir siber silah olarak geliştirilen ve İran'ın nükleer programını sekteye uğratan Stuxnet gibi siber silahların varlığı artık inkâr edilemez. Bu tip siber silahların yapılabileceğinin kanıtlanmasıyla, belki de bir silahlanma yarışına doğru bir sayfa açılmıştır [9]. Strateji sadece siber tehditlere karşı sürekli savunmada kalmayı tercih edecek tarzda olmamalıdır. Ülke istihbarat birimleri, karşılıklı bilgi akışını sağlayacak şekilde proaktif olmalıdır.

(13) Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında eğitim konusunda büyük eksiklikler bulunmaktadır. Sadece kurumların bilgi sistemlerinden ve siber güvenliğinden sorumlu üst düzey personeli, teknik personel, iç denetim birimleri; siber güvenlik konusunda yüksek lisans ve doktora programlarının açılması, Türkçe makale ve yayınların çoğaltılması; meslek liselerinin bilgisayar programcılığı bölümlerinin müfredatına siber güvenlik konularının eklenmesi gibi önlemlerle siber güvenlik konusunda bilinçlenme ve farkındalık yaratılması sağlanamaz. Özellikle bilgisayar, akıllı telefon, tablet vb. cihazlarının kullanımın çağının okul öncesine kadar düştüğü, sosyal ağlar sayesinde siber zorbalık gibi kavramların hayatımıza dâhil olduğu göz önüne alınarak ilkokul çağından itibaren gerekli eğitimlerin verilmesi sağlanmalıdır. Bu konuda planlanan eğitimler sadece teknik seviyede kalmamalı; psikologlar, sosyologlar, çocuk gelişim uzmanları vb. uzman personelin nezaretinde gerçekleştirilmelidir. FATİH Projesi ile 10 milyondan fazla öğrencinin alacağı cihazların ve söz konusu ekipmanın bağlı olacağı Eğitim Bilişim Ağının (EBA) güvenliği de göz önünde bulundurulmalıdır.

(14) Ülkemizin en büyük avantajlarından biri olan genç nüfusun, siber güvenlik konularında eğitilmesi ile yetişmiş personel istihdamı konusundaki sıkıntıların giderileceği değerlendirilmektedir. Nitelikli personelin sağlanması ancak uluslararası düzeyde geliştirilen ve geçerliliği olan programlar sayesinde gerçekleştirilebilecektir.USGS'nin eylem maddelerindeki yüksek lisans ve doktora programlarının tüm üniversitelerde açılmasının sağlanması gerekmektedir. Ayrıca bilgi ve siber güvenliğin önemini belirtecek şekilde kullanıcı, teknik personel, yönetici seviyesindeki kişiler için farkındalık eğitimleri, konferanslar, çalıştaylar düzenlenmeli; İngiltere ve ABD'deki örneklerine benzer şekilde siber güvenlik farkındalık ayı uygulaması başlatılmalı, mevcut yapı genişletilmelidir.

(15) Türkiye önümüzdeki dönemlerde kendi millî uçağını, millî tankını, millî helikopterini üretebilen, tamamen yerli üretim akıllı telefon sektörü içerisinde hak ettiği yeri edinebilecek, kısacası teknoloji üretiminde söz sahibi olacak ülke konumuna gelecektir. Bu alanda kullanılan yazılım ve donanımın mutlaka iç kaynaklardan üretilmesi, yerli işletim sisteminin daha aktif olarak kullanılması ile sağlanmalıdır. Bununla ilgili olarak TSE'de hazırlanan ürün geliştirme standartları, kullanılacak tüm yazılım ve donanım için geçerli olacak şekilde genişletilmelidir.

Bir yazılımın veya donanımın üretim ve tedarik safhasında kimlerle temas ettiği/edebileceğinin tespitine imkân yoktur. İngiltere'de teknik şartnamenin gerekliliklerini yerine getiremeyen firma, yazılım ve donanımların hiçbir şekilde devlet kademesinde yapılan ihalelere kabul edilememesi örneğinin birebir uygulanması doğru bir hareket tarzı olacaktır. Bu faaliyetlerin gerçekleştirilmesi özellik arz eden Ar-Ge yatırımları ile mümkün olabilecektir.

(16) Teknoloji sektöründe yer alan firmalara vergi düzenlemeleri gibi teşvik edecek yöntemlerle Ar-Ge yatırımlarının arttırılması konusunda mutlaka planlama yapılmalı ve USGS'nde yer almalıdır. Ar-Ge faaliyetlerinde kullanılabilecek ulusal test veri tabanları oluşturulmalı ve araştırmacıların kullanımına sunulmalıdır. Teknik seviyede, kontrollü çevreler siber savunma (aynı zamanda siber saldırı) için bilimsel ortam sağlarlar. Birçok kez saldırılacak ve savunulacak şekilde hazırlanan simülasyonlarla; hazırlanan yazılım ve donanımların testleri gerçekleştirilebilir.

(17) İngiltere ve ABD ulusal siber güvenlik stratejileri incelendiğinde en çok dikkat çeken husus mali şeffaflıktır. Özellikle İngiltere 4 sene için ayırdığı 650 milyon pound tutarındaki meblağı, bu süre zarfında nasıl kullandığını ve hangi konulara tahsis ettiğini her sene sonunda yayımladığı ilerleme raporlarında belirtmektedir. Bu raporlarda; stratejilerinden elde ettikleri başarılar, siber suçların engellenmesi ile ne kadarlık bir zararın engellendiği, ne kadar suçlunun ele geçirildiği vb. istatistiklere açıklıkla yer verilmektedir. Bu minvalde, Türkiye'nin USGS ile ilgili mali konularla ilgili olarak kamuoyuna herhangi bir bilgi verilmemiştir. Stratejinin uygulanmaya başladığı 2013 yılından itibaren ulusumuza yarattığı marjinal fayda ve devlet hazinesinden harcanan meblağ açıklanmamıştır. Hali hazırda güncellenmekte olan USGS ve 2015-2016 Eylem Planında bu konuların yer almasının uygun olacağı değerlendirilmektedir.

(18) Siber güvenlik stratejisi ve eylem planı uygulanmaya başladıktan sonra belirli periyotlarla (altı aylık veya yıllık) ilerleme durumlarını gösterir raporlar yayımlanmalıdır. Bu raporlarda, söz konusu stratejinin sağladığı katkılara mutlaka yer verilmelidir. Bu sağlıklı geri bildirim için de gerekli bir husustur. Sivil toplum kuruluşları ve bağımsız denetleyici kuruluşların verecekleri katkılarla siber güvenlik açıklıkları ve korunma yöntemlerinin değerlendirilebileceği ulusal raporlar yayımlanmalıdır.

Ayrıca, yeni yayımlanacak eylem planlarının ilerleme durumlarını, izleme komitesi gibi bir birimin teşkil edilmesiyle takip edilebilir.

(19) Disiplinlerarası (belki de disiplinler üstü) olan stratejide devlet, özel sektör ve vatandaş mutlaka eşgüdüm içerisinde olmalıdır. Kurumlararası işbirliğinin, gelişen teknolojinin hızına ayak uyduracak şekilde hızlı olması kritiktir. Bunun sağlanması amacıyla Ulusal Siber Güvenlik Stratejisinin hazırlanması, uygulanması ve koordinatörlük görevi Ulaştırma, Denizcilik ve Haberleşme Bakanlığına bağlı Haberleşme Genel Müdürlüğünün sorumluluğundan alınıp yeni kurulacak bir başka birime/bakanlığa/genel müdürlüğe verilmesi daha uygun olacaktır. Kurumsal eşgüdümü sağlamakla görevli olacak birim, Siber Güvenlik Kurulunda bulunan tüm bakanlık, müsteşarlıklarla hizmetlerinin düzenli, süratli, etkili, verimli ve ekonomik bir şekilde yürütülebilmesi maksadıyla T.C. Başbakanlık'a bağlı olarak teşkil edilebilir.

(20) Önceki paragraflarda bahsedilen tespitleri kapsayacak şekilde ulusal siber strateji belgesi ve eylem planları yeniden kurgulanabilir.

Tez çalışmasında;

- İncelenen konu ile ilgili daha önce yapılan bir çalışmaya rastlanmaması,
- Kaynaklara ve karşılaştırma yapılan ülkeler ile ilgili dokümanlara çoğunlukla internet vasıtasıyla erişim sağlanma zorunluluğunun olması,
- Konu ile ilgili yazılmış kaynakların çoğunluluğunun İngilizce olması,
- Tez konusunun stratejik planlama seviyesinde olması, siber güvenliğin birçok disiplini içerecek şekilde ele alınması gerekliliği,
- Çalışma içerisinde ele alınan konuların neredeyse tamamının tez konusu olabilecek özellikte öneminin olması,
- Ülkemiz strateji belgeleri ve ilerleme durumlarını gösterir dokümanlara erişme konusunda sıkıntılar yaşanması gibi güçlüklerle karşılaşılmıştır.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının gelecek yıllarda yapılan güncellemelerinde; belirtilen hususlara dikkat edimesi, strateji dokümanı ile eylem planının daha etkin olması ve kurumlara daha çok katkılar sağlanması beklenmektedir.

KAYNAKLAR

1. İnternet: We Are Social. (2014). Social, Digital & Mobile Worldwide in 2014. URL: http://etonpreneurs.com/uploads/Global%20Social,%20Digital%20Digital%20Mobile%20Statistics,%20Jan%202014.pdf. Son Erişim Tarihi: 29.01.2015.

2. Bilgi Teknolojileri ve İletişim Kurumu. (2014). Türkiye Elektronik Haberleşme Sektörü Üç Aylık Pazar Verileri Raporu; 2014 Yılı 3. Çeyrek Temmuz-Ağustos-Eylül, *Ankara*: Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı, 37-68.

3. T.C. Millî Eğitim Bakanlığı Talim ve Terbiye Kurulu ve TC. Radyo ve Televizyon Üst Kurulu. (2006*). İlköğretim Medya Okuryazarlığı Dersi Öğretim Programı ve Kılavuzu*; Ankara: T.C. Millî Eğitim Bakanlığı Talim ve Terbiye Kurulu ve TC. Radyo ve Televizyon Üst Kurulu, 5-6.

4. Yılmaz, S., Sağıroğlu, Ş. (2013). *Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi*. 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 323-331, Ankara.

5. Altunbaş, S. (2012). *E-Devlet Uygulamalarında Web Servisler ve Bilinmeyen Numaralar Servis Uygulaması*. Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

6. Sağıroğlu, Ş., Alkan, M. (2005). *Her Yönüyle Elektronik İmza* (Birinci Baskı). Ankara: Grafiker Yayınları, 51-72.

7. OECD (2012). *Machine-to-Machine Communications: Connecting Billions of Devices*; OECD Digital Economy Papers, No. 192, OECD Publishing, 1-45.

8. Bilgi Teknolojileri ve İletişim Kurumu. (2003). *Makineler Arası İletişim (M2M);* BTK, 3-6.

9. Singer, P.W. ve Friedman, A. (2015). *Siber Güvenlik ve Siber Savaş* (Birinci Baskı). Ankara: Buzdağı Yayınevi, 31-35.

10. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2012). *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*; Ankara: UDHB*,* 9-47.

11. Çifci, H. (2013). *Her Yönüyle Siber Savaş* (Birinci Baskı). Ankara: TUBİTAK Popüler Bilim Kitapları, 3-184.

12. Clarke, R.A., Knake, R.K. (2010). *Cyber War-The Next Threat to National Security and What to Do About It*. New York: HarperCollins Publishers, 74-85.

13. İnternet: Forbes. (2014). Why Cyber Security Matters Everyone? URL: http://www.forbes.com/sites/larrymagid/2014/10/01/why-cyber-security-matters-to-everyone. Son Erişim Tarihi: 03.11.2014.

14. İnternet: The Independent. (2014). Cyber crime: First online murder will happen by end of the year, warn US firm. URL: http://www.independent.co.uk/life-style/gadgets-and-tech/news/first-online-murder-will-happen-by-end-of-year-warns-us-firm-9774 955.html. Son Erişim Tarihi: 03.11.2014.

15. İnternet: Fortune. (2015). Lloyd's CEO: Cyber attacks cost companies $400 billion every year. URL: http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds. Son Erişim Tarihi: 03.02.2015.

16. Vural, Y. (2007). *Kurumsal Bilgi Güvenliği ve Sızma Testleri.* Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

17. Symantec. (2013*). Internet Security Threat Report 2014*; Symantec Corporation, 7-8.

18. T.C. Kalkınma Bakanlığı (2014). *2014-2018 Bilgi Toplumu Stratejisi ve Eylem Planı (Taslak)*; Ankara: Kalkınma Bakanlığı, 9-51.

19. İnternet: Türk Dil Kurumu. (2015). Büyük Türkçe Sözlük, Bilgi. URL: http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.54d1e74f08f1b0.85580471. Son Erişim Tarihi: 04.02.2015.

20. Shannon, C.E. (1948). A Mathematical Theory of Communication. *Bell System Technical Journal*, 27, 379-423.

21. Nonaka, I., Takeuchi, H. (1995). *The Knowledge Creating Company: How Japanese Create the Dynamics of Innovation*. New York: Oxford University Press, 26-29.

22. Wiig, K. (1999). *Knowledge Management Hand Book - Introducing Knowledge Management into Enterprise*. CRC Press, Boca Raton, FL, 3-1-41.

23. Becerra-Fernandez, I., Gonzalez, A., Sabherwal, R. (2004). *Knowledge Management, Challenges, Solutions and Technologies*. New Jersey: Pearson Prentice Hall, 10-22.

24. İnternet: Oxford Dictionaries. (2015). British & World English, Cyber. URL: http://www.oxforddictionaries.com/definition/english/cyber. Son Erişim Tarihi: 05.02.2015.

25. İnternet: Wired. (2009). March 17, 1948: William Gibson, father of Cyberspace. URL: http://archive.wired.com/science/discoveries/news/2009/03/dayintech_0317. Son Erişim Tarihi: 05.02.2015.

26. İnternet: Oxford Dictionaries. (2015). British & World English, Cyberspace. URL: http://www.oxforddictionaries.com/us/definition/american_english/cyberspace. Son Erişim Tarihi: 05.02.2015.

27. Hildreth, S. A. (2001). *Cyberwarfare Congressional Research Service Report for Congress;* Congressional Research Service & The Library, 1-9.

28. United States Department of Defence. (2010). *Department of Defence Dictionary of Military and Associated Terms*; DoD*,* 13-71.

29. North Atlantic Treaty Organization. (2011). *NATO Cyber Defense Concept*; NATO, 3-45.

30. International Telecommunication Union. (2008). *Series X: Data Networks, Open System Communications and Security, Overview of Cybersecurity*; ITU-T Recommendation, 8-12.

31. Benzer, R. (2014). *Siber Suçlar ve Teorik Yaklaşımlar*. H. Çakır, M.S. Kılıç (Editörler). *Güncel Tehdit: Siber Suçlar.* Birinci Baskı. Ankara. Seçkin Yayıncılık, 21-41.

32. İnternet: Washington Post. (2009). Estonia Incident Demonstrated Power of Russia Based Cyber Networks. URL: http://archive.wired.com/science/discoveries/news /2009/03/dayintech_0317. Son Erişim Tarihi: 09.02.2015.

33. İnternet: Wired. (2009). Hackers Take Down the Most Wired Country in Europe. URL: http://archive.wired.com/politics/security/magazine/15-09/ff_estonia. Son Erişim Tarihi: 09.02.2015.

34. İnternet: BBC News. (2007). Estonia hit by 'Moscow cyber war'. URL: http://news.bbc.co.uk/2/hi/europe/6665145.stm. Son Erişim Tarihi: 09.02.2015.

35. Burlu, K. (2012). *Bilişimin Karanlık Yüzü* (Üçüncü Baskı). Ankara: Nirvana Yayınları, 113-146.

36. İnternet: Symantec. (2010). W32.Stuxnet. URL: http://www.symantec.com /security_response/writeup.jsp?docid=2010-071400-3123-99&tabid=2. Son Erişim Tarihi: 09.02.2015.

37. İnternet: Vanity Fair. (2011). A Declaration of Cyber-War. URL: http://www. vanityfair.com/news/2011/04/stuxnet-201104. Son Erişim Tarihi: 09.02.2015.

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

39. İnternet: Ulusal Bilgi Güvenliği Kapısı. (2011). DUQU: Yeni Nesil Keşif Uçağı. URL: http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/duqu-yeni-nesil-kesif-ucagi.html. Son Erişim Tarihi: 09.02.2015.

40. İnternet: Silikon Vadisi. (2015). Tüm Zamanların En Etkili 11 Hack Saldırısı. URL: http://www.silikonvadisi.tv/genel/tum-zamanlarin-en-kotu-11-hack-saldirisi-60791. html. Son Erişim Tarihi: 09.02.2015.

41. İnternet: Network World. (2009). Downadup/Conflicker worm: When will the next shoe fall? URL: http://www.networkworld.com/article/2273085/lan-wan/ downadup-conflicker-worm--when-will-the-next-shoe-fall-.html. Son Erişim Tarihi: 09.02.2015.

42. İnternet: Symantec. (2008). W32.Downadup. URL: http://www.symantec. com/security_response/writeup.jsp?docid=2008-112203-2408-99. Son Erişim Tarihi: 09.02.2015.

43. Laboratory of cryptography and System Security. (2012). *sKyWIper (a.k.a Flame a.k.a. Flamer): A Complex Malware for Targeted Attacks*; CrySyS Lab, 2-12.

44. İnternet: Deutsche Welle. (2012). En tehlikeli virüs: Flame. URL: http://www.dw.de/en-tehlikeli-vir%C3%BCs-flame/a-15988868. Son Erişim Tarihi: 09.02.2015.

45. İnternet: msHOWTO. (2012). Flame Virüsünün Detayları, Tespiti ve Temizlenmesi. URL: http://www.mshowto.org/flame-virusunun-detaylari-tespiti-ve-temizlenmesi.html. Son Erişim Tarihi: 09.02.2015.

46. İnternet: Ulusal Bilgi Güvenliği Kapısı. (2012). #Flame: En büyük, En Karmaşık Siber Casusluk Yazılımı. URL: http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/flame-en-buyuk-en-karmasik-siber-casusluk-yazilimi.html. Son Erişim Tarihi: 09.02.2015.

47. Keleş, A.R. ve Sal, Y. (2013). Hack Kültürü ve Hacktivism: Yeni Bir Siyaset Biçimi. *Alternatif Bilişim Derneği Yayını*, 33-34.

48. İnternet: NBC News. (2014). North Korea Behind Sony Hack: U.S. Officials. URL: http://www.nbcnews.com/storyline/sony-hack/north-korea-behind-sony-hack-u-s-officials-n270451. Son Erişim Tarihi: 09.02.2015.

49. İnternet: Reuters. (2014). Cyber attack could cost Sony studio as much as $100 million. URL: http://www.reuters.com/article/2014/12/09/us-sony-cybersecurity-costs-idUSKB N0JN2L020141209. Son Erişim Tarihi: 09.02.2015.

50. İnternet: Slate. (2014). The New Age of Cyberwarfare. http://www.slate.com/articles/news_and_politics/war_stories/2014/12/sony_pictures_attack_is_a_new_era_in_cyber_warfare_is_it_an_attack_on_the.html. Son Erişim Tarihi: 09.02.2015.

51. İnternet: NTVMSNBC. (2014). Sony'yi Kuzey Kore hack'ledi. URL: http://www.ntv.com.tr/arsiv/id/25557022/. Son Erişim Tarihi: 09.02.2015.

52. Eren, E. (2005). *İşletmelerde Stratejik Yönetim ve İşletme Politikası* (Yedinci Basım). İstanbul: Beta Basım, 5-70.

53. İnternet: Türk Dil Kurumu. (2015). Büyük Türkçe Sözlük, Strateji. URL: http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.54e10650d9cd35.23553542. Son Erişim Tarihi: 15.02.2015.

54. Aktan, C.A. (2008). Stratejik Yönetim ve Stratejik Planlama. *Çimento İşveren Dergisi,* Temmuz 2008 Sayı:4 Cilt:22, 4-21.

55. Pamuk, G., Erkut, H., Ülengin, F., Ülengin, B, Akgüç, Ö., Alpay,Y., Koşma,H. (1997). *Stratejik Yönetim ve Senaryo Tekniği*. İstanbul: İrfan Yayıncılık, 2-73.

56. Bütüner, H. (2014). *Sistematik Stratejik Planlama*. İstanbul: Scala Yayıncılık, 12-55.

57. Türkiye Büyük Millet Meclisi. (2013). *TBMM İdari Teşkilatı 2013-2017 Stratejik Pl*anı; Ankara: TBMM, 13-85.

58. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2014). *Stratejik Plan 2014-2018*; Ankara: UDHB, 66-91.

59. European Network and Information Agency (2012). *National Cyber Security Strategies, Practical Guide on Development and Execution (Setting the course for national efforts to strengthen security in cyberspace)*; ENISA, 2-15.

60. Wamala, F. (2011). *ITU National Cybersecurity Strategy Guide*; ITU, 18-91.

61. İnternet: International Telecommunication Union. (2007). Global Security Agenda. URL: http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx. Son Erişim Tarihi: 23.02.2015.

62. Ünver, M., Canbay, C:, Mirzaoğlu, A.G. (2009). *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler*; Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı, 22-52.

63. European Network and Information Security Agency (2012). *National Cyber Security Strategies, Practical Guide on Development and Execution*; ENISA, 8-34.

64. Klimburg, A. (2012). *National Cyber Security Framework Manual*; NATO CCD COE Publication, 44-108.

65. Şentürk H., Çil C.Z., Sağıroğlu Ş. (2012). *Siber Güvenlik Makro Analiz Modeli Önerisi ve Türkiye'nin Analizi*. 5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 38-49, Ankara.

66. Alkan M., Sağıroğlu Ş., Türekçi T., Atalay A.H., Bilirgen C., Canbek G., İnceefe M.A., Özbilen A., Ünver M., Yazıcı A. (2012). Ulusal Bilgi Güvenliği Stratejisi. *Bilgi Güvenliği Derneği;* 14-31.

67. İnternet: CNBC. (2014). These Countries Are the Biggest Cyberattack Targets. URL: http://www.cnbc.com/id/102093393. Son Erişim Tarihi: 06.03.2015.

68. Department of Business, Innovation and Skills (2009). *Digital Britain: Final Report*; BIS, Cm 7650, 40-41.

69. Kabine Ofisi (2009). *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space*; Cm 7642, 7-32.

70. Kabine Ofisi (2009). *The National Security Strategy of the United Kingdom: Update 2009, Security for the Next Generation*; Cm 7590, 49-87.

71. İstanbul Bilgi Üniversitesi. (2012). *Siber Güvenlik Raporu*; Bilişim ve Teknoloji Hukuku Enstitüsü, 30-31.

72. Kabine Ofisi (2011). *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*; 5-43.

73. National Audit Office (2013). *The UK cyber security strategy: Landscape review*; TSO*,* 5-36.

74. İnternet: CPNI. (2015). Center for the Protection of National Infrastructure. http://www.cpni.gov.uk/about/cni. Son Erişim Tarihi: 29.09.2014.

75. Detica and the Cabinet Office (2011). *The Cost of Cyber Crime*; Detica Limited, 18-25.

76. Anderson, R., Barton, C., Böhme, R., Clayton, R., Eeten, M., Levi, M., Moore, T., Savage, S. (2012). *Measuring the Cost of Cyber Crime*; WEIS 2012, 1-31.

77. Pricewaterhouse Coopers (2011). Global Economic Crime Survey 2011–UK Report; PWC, 1-25.

78. Turhan, M. (2010). *Siber Güvenliğin Sağlanması, Dünya Uygulamaları ve Ülkemiz İçin Çözüm Önerileri*. Yayımlanmamış Uzmanlık Tezi, Bilgi Teknolojileri ve İletişim Kurumu, Ankara.

79. İnternet: WARP. (2015). About Us. URL: https://www.warp.gov.uk/about-us/. Son Erişim Tarihi: 10.03.2015.

80. Kurt, L. (2005). *Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması*. Yayımlanmamış Yüksek Lisans Tezi, TODAİE Kamu Yönetimi Bölümü, Ankara.

81. Karagülmez, A. (2011). *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*. Ankara: Seçkin Yayıncılık, 7-60.

82. Aytekin, A. (2014). Karşılaştırmalı hukuk açısından siber suçlar. H. Çakır, M.S. Kılıç (Editörler). *Güncel Tehdit: Siber Suçlar.* Birinci Baskı. Ankara. Seçkin Yayıncılık, s.181-203.

83. Mahmutoğlu, F.S. (2001). Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu, *İÜHFM*, İstanbul, C:LIX S:1-2, s.39-49.

84. İnternet: İngiltere Hükümeti Resmi Web Sitesi. (2014). Data Protection. URL: https://www.gov.uk/data-protection/the-data-protection-act. Son Erişim Tarihi: 11.03.2015.

85. Kabine Ofisi (2012). *Progress Against the Objectives of the National Cyber Security Strategy*; 2-19.

86. Kabine Ofisi (2013). *National Cyber Security Strategy Our Forward Plans*; 1-14.

87. Kabine Ofisi (2013). *Progress Against the Objectives of the National Cyber Security Strategy*; 3-18.

88. Kabine Ofisi (2014). *The UK Cyber Security Strategy, Report on Progress and Forward Plans*; 3-24.

89. İnternet: İngiltere Hükümeti Resmi Web Sitesi. (2011). Government Publishes Cyber Security Strategy. URL: https://www.gov.uk/government/news/government-publishes-cyber-security-strategy. Son Erişim Tarihi: 11.03.2015.

90. İnternet: İngiltere Hükümeti Resmi Web Sitesi. (2011). The Cyber Security Strategy Sets Out How the UK Will Build a More Trusted and Resilient Digital Environment. URL: https://www.gov.uk/government/news/protecting-and-promoting-the-uk-in-a-digi tal-world--3. Son Erişim Tarihi: 14.03.2015.

91. İnternet: RISCS. (2015). The Research Institute in Science of Cyber Security. URL: http://www.riscs.org.uk/. Son Erişim Tarihi: 15.03.2015.

92. İnternet: The Research Institute in Automated Program Analysis and Verification. (2015). Home. URL: http://verificationinstitute.org/. Son Erişim Tarihi: 15.03.2015.

93. İnternet: CPNI. (2015). Research Institute in Trustworthy Industrial Control Systems. URL: https://www.cpni.gov.uk/advice/cyber/Cyber-research-programmes/tci/Rese arch-institute-in-trustworthy-industrial-control-systems-/. Son Erişim Tarihi: 15.03.2015.

94. İnternet: CERT-UK. (2015). About Us. URL: https://www.cert.gov.uk/what-we-do/. Son Erişim Tarihi: 15.03.2015.

95. İnternet: İngiltere Hükümeti Resmi Web Sitesi. (2011). Policy: Keeping the UK safe in cyber space; Supporting detail: Working with industry on minimum standards and principles. URL: https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace/supporting-pages/working-with-industry-on-minimum-standards-and-principles. Son Erişim Tarihi: 24.11.2014.

96. Department for Business, Innovation and Skills (2014). *Cyber Essentials Scheme: Requirements for Basic Technical Protection from Cyber Attacks*; BIS, 14/696, 5-13.

97. Publicly Available Specification. (2014). *Software Trustworthiness. Governance and Management*; BSI*,* 10-76.

98. Department for Business, Innovation and Skills (2013). *Guiding Principles on Cyber Security: Guidance for Internet Service Providers and Government*; BIS*,* 3-8.

99. Department for Business, Innovation and Skills (2014). *Policy Paper, Communique: Strengthening The Cyber Security of Our Essential Services*; HM Government*,* 1-2.

100. Department for Business, Innovation and Skills (2013). *FTSE 350 Cyber Governance Health Check Tracker Report*; BIS, 6-46.

101. Department for Business, Innovation and Skills (2014). *2014 Information Security Breaches Survey: Technical Report*; BIS*,* 3-21.

102. İnternet: İngiltere Hükümeti Resmi Web Sitesi. (2011). Policy: Keeping the UK safe in cyber space; Supporting detail: Building cyber security capacity internationally. URL: https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace/ supporting-pages/setting-up-a-global-centre-for-cyber-security-capacity. Son Erişim Tarihi: 24.11.2014.

103. The White House. (2015). *The National Security Strategy*; 1-13.

104. The White House. (2003). *The National Strategy to Secure Cyberspace*; 19-53.

105. US Army War College Strategic Studies Institute (2013). *An Assessment of the Department of Defense Strategy for Operating in Cyberspace*. The Letort Papers. 1-29.

106. Joint Chiefs of Staff. (2004). *The National Military Strategy of the USA. A Strategy for Today; A Vision for Tomorrow*; Joint Chiefs of Staff, 5-42.

107. Joint Chiefs of Staff. (2006). *The National Military Strategy for Cyberspace Operations*; Joint Chiefs of Staff, 3-19.

108. The White House. (2009). *Cyberspace Policy Review, A Trusted and Resilient Information and Communications Infrastructure*; 1-37.

109. The White House. (2008). *The Comprehensive National Cybersecurity Initiative;* 1-5.

110. Department of Defense. (2011). *DoD Strategy for Operating in Cyberspace;* DoD*,* 5-13.

111. The White House. (2011). *International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World*; 3-25.

112. The White House. (2001). *Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (Usa Patriot Act) Act Of 2001.* US. Government Printing Office*,* 6-16.

113. İnternet: ABD İç Güvenlik Bakanlığı Resmi Sitesi. (2015). Critical Infrastructure Sectors. URL: http://www.dhs.gov/critical-infrastructure-sectors. Son Erişim Tarihi: 01.04.2015.

114. The White House. (2013). *Presidential Executive Order 13636. Improving Critical Infrastructure Cybersecurity*; Presidential Documents, 3-8.

115. İnternet: National Council of ISACs. (2015). Members. URL: http://www.isaccouncil.org/memberisacs.html. Son Erişim Tarihi: 05.04.2015.

116. İnternet: NCSA. (2015). About. https://www.staysafeonline.org/about-us/overview/. Son Erişim Tarihi: 05.04.2015.

117. Ditzion R., Geddes E., Rhodes M. (2003). Computer Crimes. *American Criminal Law Review*, 4 No2, 82-91.

118. Andreano, F.P. (1999). The Evolution of Federal Computer Crime Policy: The Ad Hoc Approach to an Ever-Changing Problem. *AM.J.CRIM.L*., Vol.27:81, 85-90.

119. Dülger, M.V. (2004). *Bilişim Suçları*. Ankara: Seçkin Yayıncılık, 212-272.

120. İnternet: Goodman,M.D., Brenner,S.W., (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. URL: http://www.lawtechjournal.com/ articles/2002/03_020625_goodmanbrenner.php. Son Erişim Tarihi: 31.12.2013.

121. Pallı, H. (2008). *Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları*. Yayımlanmamış Yüksek Lisans Tezi, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Kayseri.

122. İnternet: National Initiative for Cybersecurity Careers and Studies. (2015). About the National Initiative for Cybersecurity Education. URL: http://niccs.us-cert.gov/footer/about-national-initiative-cybersecurity-education. Son Erişim Tarihi: 06.04.2015.

123. İnternet: CAE. (2015). National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD). URL: https://www.nsa.gov/ia/academic_ outreach/nat_cae/index.shtml. Son Erişim Tarihi: 06.04.2015.

124. İnternet: NICCS. (2015). Curriculum Resources. URL: http://niccs.us-cert.gov/education /curriculum-resources. Son Erişim Tarihi: 06.04.2015.

125. The White House. (2002). *Cyber Security Research and Development Act*. *US.* Government Printing Office*,* 1-14.

126. The White House (2011). *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*; 1-17.

127. İnternet: NITRD. (2015). The Networking and Information Technology Research and Development Program. URL: https://www.nitrd.gov/about/about_nitrd.aspx. Son Erişim Tarihi: 08.04.2015.

128. İnternet: NCCIC. (2015). National Cybersecurity and Communications Integration Center. URL: https://www.us-cert.gov/nccic. Son Erişim Tarihi: 07.04.2015.

129. İnternet: Siber Bülten. (2015). ABD Siber Bütçesini 14 Kat Arttırdı. URL: http://siberbulten.com/strateji-guvenlik/abdnin-siber-butcesini-14-kat-arttirdi. Son Erişim Tarihi: 07.04.2015.

130. İnternet: Department of Homeland Security. (2015). Cybersecurity Results. URL: https://www.dhs.gov/cybersecurity-results. Son Erişim Tarihi: 10.04.2015.

131. İnternet: Milliyet Gazetesi. (2015). HSBC Türkiye'ye Siber Saldırı Şoku. URL: http://www.milliyet.com.tr/hsbc-turkiye-ye-siber-saldiri-bilisim-1969049. Son Erişim Tarihi: 14.04.2015.

132. İnternet: Star Ana Sayfa. (2015). Bakan Yıldız Açıkladı; Elektrik Kesintisinin Nedeni Siber Saldırı Mı? URL: http://haber.star.com.tr/guncel/bakan-yildiz-acikladi-3b-elektrik-kesintisinin-nedeni-siber-saldiri-mi/haber-1015959. Son Erişim Tarihi: 01.04.2015.

133. İnternet: Milli Güvenlik Kurulu Sekreterliği. (2010). 27 Ekim 2010 Tarihli Toplantı. URL: http://www.mgk.gov.tr/index.php/27-ekim-2010-tarihli-toplanti. Son Erişim Tarihi: 14.04. 2015.

134. İnternet: T.C. Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı. (2015). Teknolojik Afetler Risk Azaltma Çalışma Grubu. URL: https://www.afad.gov.tr/tr/HaberListele.aspx?ID=203. Son Erişim Tarihi: 30.03.2015.

135. T.C. Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı. (2014). *2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi*; AFAD*,* Ankara, 14-50.

136. İnternet: T.C. Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı, Teknolojik Afetler Risk Azaltma Çalışma Grubu. (2015). Projeler. URL: https://www.afad.gov.tr/tr/IcerikListele.aspx?ID=210. Son Erişim Tarihi: 30.03.2015.

137. İnternet: İnternet Geliştirme Kurulu. (2010). Siber Güvenlik İnisiyatifi. URL: http://www.internetkurulu.org/tr/SGInsiyatifi.aspx. Son Erişim Tarihi: 16.04.2015.

138. İnternet: Haberleşme Genel Müdürlüğü. (2013). Sektörel Faaliyetler, Ulaşan ve Erişen Türkiye 2013. URL: http://www.ubak.gov.tr/BLSM_WIYS/ UBAK/tr/dokuman_ust_menu/projeler_faaliyetler/20130319_101648_204_1_64.pdf. Son Erişim Tarihi: 24.11.2014.

139. Erdoğan, Y. (2010). Bilişim Sistemine Girme ve Kalma Suçu. *Dokuz Eylül Hukuk Fakültesi Dergisi*, Cilt:12, Sayı: Özel S., sf. 1363-1433.

140. Değirmenci, O. (2005). 2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi. *TBB Dergisi*, Sayı:58, sf. 195-208.

141. Yazıcıoğlu, Y. (2004). Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi. *Hukuk ve Adalet: Eleştirel Hukuk Dergisi*, İstanbul, Y:1, S:1, Ocak-Mart, 78.

142. Akbulut, B., (1999). *Türk Ceza Hukukunda Bilişim Suçları*. Yayınlanmamış Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya.

143. Değirmenci,O. (2002). *Bilişim Suçları*. Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

144. Karakehya, H. (2009). Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu. *TBB Dergisi*, Sayı:81, sf. 1-24.

145. İlbaş, Ç. (2009). *Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Analizi*. Yayımlanmamış Yüksek Lisans Tezi, Başkent Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

146. Yılmaz, S. (2011). 5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar. *TBB Dergisi*, Sayı:92, sf. 62-100.

147. Eker Kazancı, B. (2007). Kişilerin İzinsiz Görüntüsünün Alınmasının TCK M.134 Çerçevesinde Korunması. *Dokuz Eylül Hukuk Fakültesi Dergisi*, Cilt:9, Sayı:1, s. 131-164.

148. Yokuş Sevük, H. Haberleşme Hakkının Kullanımının Türk Ceza Kanunu Hükümleriyle Korunması. Dicle *Üniversitesi Hukuk Fakültesi Dergisi*, Cilt:12-13, Sayı:16-17-18-19, 159-195.

149. İnternet: Bilgi Teknolojileri ve İletişim Kurumu. (2014). Uluslararası Etkinlikler. URL: http://www.tk.gov.tr/sayfa.php?ID=328. Son Erişim Tarihi: 23.04.2015.

150. İnternet: CyDeS. (2015). Hakkımızda. URL: http://cydes.ii.metu.edu.tr/tr/node/2. Son Erişim Tarihi: 23.04.2015.

151. İnternet: Bilgi Teknolojileri ve İletişim Kurumu. (2015). Teknoloji ve Çözümler. URL: http://sge.bilgem.tubitak.gov.tr/tr/cozumler/cozumler-0. Son Erişim Tarihi: 23.04.2015.

152. İnternet: International Cyber Warfare and Security Conference. (2014). URL: http://www.icwcturkey.com/presentations. Son Erişim Tarihi: 23.04.2015.

153. T.C. Cumhurbaşkanlığı Devlet Denetleme Kurulu (2013). *Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları*; Ankara: DDK, 784-806.

154. T.C. Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı. (2014). *2014-2023 Teknolojik Afetler Yol Haritası Belgesi*; AFAD, Ankara, 69-70.



ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı	:	AYTEKİN, Akın
Uyruğu	:	T.C.
Doğum tarihi ve yeri	:	25/02/1982 İzmir
Medeni hali	:	Evli
Telefon	:	0 (312) 418 33 20
e-posta	:	akin.aytekin@yahoo.com

Eğitim Derecesi	**Okul/Program**	**Mezuniyet Yılı**
Yüksek lisans	Gazi Üniversitesi/Bilişim Enstitüsü Bilişim Sistemleri Anabilim Dalı	Devam Ediyor
Lisans	Kara Harp Okulu/İnşaat Müh.	2003
Lise	Maltepe Askeri Lisesi	1999

İş Deneyimi, Yıl	**Çalıştığı Yer**	**Görev**
2003-Devam Ediyor	Türk Silahlı Kuvvetleri	Subay

Yabancı Dili

İngilizce

Yayınlar

1. Aytekin, A. (2014). Karşılaştırmalı hukuk açısından siber suçlar., H. Çakır, M.S. Kılıç (Editörler). *Güncel Tehdit: Siber Suçlar.* Birinci Baskı. Ankara. Seçkin Yayıncılık, s.181-203.

2. Aytekin, A., Sağıroğlu,Ş. (2015). Türkiye ve İngiltere Ulusal Siber Güvenlik Stratejilerinin Karşılaştırılması. (Kara Harp Okulu Savunma Bilimleri Dergisinde yayımlanmak üzere gönderildi.)

Hobiler

Basketbol, Masa Tenisi, Bilardo, Voleybol, Dağ Maratonu.



GAZİ GELECEKTİR..