

NATO ÜYESİ ÜLKELERİN SİBER GÜVENLİK STRATEJİLERİ AÇISINDAN İNCELENMESİ

Mehmet ADA

**YÜKSEK LİSANS TEZİ
ADLİ BİLİŞİM ANABİLİM DALI**

**GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ**

OCAK 2018

Mehmet ADA tarafından hazırlanan NATO ÜYESİ ÜLKELERİN SİBER GÜVENLİK STRATEJİLERİ AÇISINDAN İNCELENMESİ adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ / ~~OY ÇOKLUĞU~~ ile Gazi Üniversitesi Adli Bilişim Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir.

Danışman: Yrd. Doç. Dr. Hüseyin ÇAKIR

Eğitim Fakültesi Bil. ve Öğr. Tek. Eğitimi, Gazi Üniversitesi

Bu tezin kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum



Başkan: Prof.Dr. Refik SAMET

Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, Ankara Üniversitesi

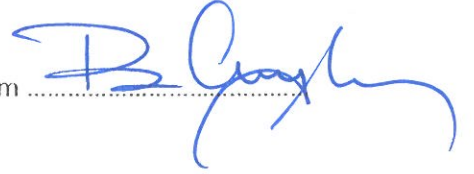
Bu tezin kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum



Üye: Doç.Dr. Bünyamin CİYLAN

Teknoloji Fakültesi Bilgisayar Mühendisliği Bölümü, Gazi Üniversitesi

Bu tezin kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum



Tez Savunma Tarihi: 16/01/2018

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

.....
Doç. Dr. Aslıhan TÜFEKÇİ

Bilişim Enstitüsü Müdürü

ETİK BEYAN

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

- 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 çalışmada 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.

Mehmet ADA

16.01.2018

NATO ÜYESİ ÜLKELERİN SİBER GÜVENLİK STRATEJİLERİ AÇISINDAN İNCELENMESİ
(Yüksek Lisans Tezi)

Mehmet ADA

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

Ocak 2018

ÖZET

Son yıllarda bilgi ve iletişim teknolojilerinde gerçekleşen gelişmeler ile coğrafik sınırların yerini sanal ortamda belirlenen dijital sınırlar almıştır. Siber saldırılara karşı ulusal çıkarların korunması ve siber uzayın sınır güvenliğinin sağlanması hususunda karşılaşılan zorluklar, devletlerin uluslararası anlaşmalar yapmasını kaçınılmaz hale getirmiştir. Bu çalışmada, küreselleşen dünyada ülkeleri aynı çatı altında birleştiren en büyük organizasyonlardan biri olan NATO'nun ve NATO üyesi ülkelerin uyguladığı siber güvenlik stratejisi incelenerek, Türkiye'nin uyguladığı siber güvenlik stratejisine olumlu katkılar yapmak amaçlanmıştır. alt amaçların tespit edilmesi aşamasında siber güvenlik konusunda uzman olan 16 kişiye sunum yapılmış ve görüşleri alınmıştır. Bu kapsamda; NATO CCDCOE, ENISA, BSA, ITU organizasyonlarının yayımladıkları dokümanlar belirlenen alt amaçlar çerçevesinde detaylı bir şekilde incelenmiştir. İncelemeler sonrasında, ülkemizin stratejik planına önemli katkı sağlayacağı değerlendirilen hususlar belirlenmiş ve sonuç bölümünde öneri olarak madde başlıklarıyla sunulmuştur.

Bilim Kodu : 114602

Anahtar Kelimeler : Siber güvenlik, NATO, Ulusal Siber Güvenlik Stratejisi, eylem planı.

Sayfa Adedi : 148

Danışman : Yrd. Doç. Dr. Hüseyin ÇAKIR

INVESTIGATION OF CYBER SECURITY STRATEGY OF NATO MEMBER COUNTRIES
(M. Sc. Thesis)

Mehmet ADA

GAZİ UNIVERSITY
INFORMATICS INSTITUTE

January 2018

ABSTRACT

Because of the fact that developments taking place in recent years in information and communication technology, digital boundaries has taken the place of the geographical boundaries. The challenges of protecting national interests against cyber attacks and ensuring the border security of cyberspace has made it inevitable for governments to make international agreements. In this study, it is aimed to make a positive contribution to the cyber security strategy implemented by Turkey by examining the cyber security strategy applied by NATO, one of the biggest organizations that unite countries under the same roof in the globalizing World, and NATO member countries. During the determination of the sub-objectives, a presentation was made to 16 persons who were experts on the subject of cyber security and opinions were taken. Within this scope; The documents published by NATO CCDCOE, ENISA, BSA and ITU organizations have been examined in detail in the framework of the identified sub-objectives. After the examinations, the issues that are considered to contribute significantly to the strategic plan of our country have been identified and presented as a suggestion in the conclusion section.

Science Code : 114602

Key Words : Cybersecurity, NATO, National Cybersecurity Strategy, action plan.

Page Number : 148

Supervisor : Assist. Prof. Dr. Hüseyin ÇAKIR

TEŞEKKÜR

Çalışmalarım boyunca değerli katkılarını, yardımlarını esirgemeyen, tecrübesini ve ilmini cömertçe aktarmaya çalışan değerli tez danışmanım Yrd. Doç. Dr. Hüseyin ÇAKIR'a; benim bu günlere gelmeme vesile olan, hiçbir zaman benden hem maddi hem de manevi desteklerini esirgemeyen ve kısa bir süre önce kaybettiğim engin düşünceli, civanmert yürekli annem Sevim ADA ve babam Remzi ADA'ya teşekkür ederim.

Son olarak; başarılı olmam için desteğini hiçbir zaman esirgemeyen, çalışmalarımı tamamlamam için büyük fedakarlıklar yapan, yoldaşım, hayat arkadaşım ve değerli eşim Ülkü ADA ile canımdan çok sevdiğim güzel kızım İnci Azra ADA ve biricik oğlum Yakup Efe ADA'ya şükranlarımı sunarım.

İÇİNDEKİLER

	Sayfa
ÖZET.....	iv
ABSTRACT.....	v
TEŞEKKÜR.....	vi
İÇİNDEKİLER.....	vii
ÇİZELGELERİN LİSTESİ.....	x
ŞEKİLLERİN LİSTESİ.....	xi
SİMGELER VE KISALTMALAR.....	xiii
1. GİRİŞ.....	1
1.1. Araştırmanın Problemi.....	1
1.2. Araştırmanın Amacı.....	4
1.3. Araştırmanın Önemi.....	6
1.4. Araştırmanın Kapsam ve Sınırlılıkları.....	7
2. SİBER ORTAM KAVRAMLARI.....	9
2.1. Siber Uzay.....	9
2.2. Siber Güvenlik.....	9
2.3. Siber Saldırı.....	13
2.4. Siber Terörizm.....	17
2.5. Siber Casusluk.....	17
2.6. Siber Suç.....	20
2.7. Siber Savaş.....	22
3. KUZEY ATLANTİK ANTLAŞMA ÖRGÜTÜ (NATO) VE SİBER GÜVENLİK....	25
3.1. NATO'nun Kuruluşu ve Üye Ülkeler.....	25
3.2. NATO Organizasyon Yapısı.....	26
3.3. NATO Siber Güvenlik Stratejisini Etkileyen Siber Savaşlar.....	28
3.3.1. NATO Kosova krizi – 1999.....	29
3.3.2. Estonya siber savaşı – 2007.....	30
3.3.3. Gürcistan siber savaşı – 2008.....	32
3.4. NATO Siber Güvenlik Stratejisi.....	35
4. ULUSAL SİBER GÜVENLİK STRATEJİSİ.....	43

	Sayfa
4.1. Ulusal Siber Güvenlik Strateji Planının Hazırlanması ve Uygulanması.....	44
4.1.1. Uluslararası Telekomünikasyon Birliği (ITU) modeli.....	44
4.1.2. Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA) modeli.....	47
4.2. Türkiye’de Ulusal Siber Güvenlik.....	49
4.2.1. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı.....	52
4.2.2. 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı.....	54
5. YÖNTEM.....	57
5.1. Araştırma Modeli.....	57
5.2. Evren ve Örneklem.....	60
5.3. Verilerin Toplanması.....	60
6. ARAŞTIRMA BULGULARI.....	61
6.1. Ulusal Siber Güvenlik Stratejisi ve Koordinatör Makamı Açısından İncelenmesi.	61
6.2. Bilgisayar Olaylarına Müdahale Ekipleri (CERT) Açısından İncelenmesi.....	63
6.3. Uluslararası İşbirliği Açısından İncelenmesi.....	66
6.4. Ulusal Siber Güvenlik Eylem Maddeleri Açısından İncelenmesi.....	67
6.5. Uluslararası Gelişme Endeksleri Açısından İncelenmesi.....	68
6.6. İnternet Kullanıcı Sayıları Açısından İncelenmesi.....	71
6.7. Kişisel ve Ulusal Bant Genişlikleri Açısından İncelenmesi.....	73
6.8. Hukuki Düzenlemeler ve Yönetmelikler Açısından İncelenmesi.....	76
6.8.1. Kişisel verilerin gizliliği kapsamındaki düzenlemeler açısından incelenmesi.....	76
6.8.2. Kişisel ve kurumsal güvenliğin geliştirilmesini sağlayan düzenlemeler açısından incelenmesi.....	76
6.8.3. Siber suçlar kapsamındaki düzenlemeler açısından incelenmesi.....	77
6.8.4. Fikri mülkiyet haklarının korunması kapsamındaki düzenlemeler açısından incelenmesi.....	77
6.8.5. Fikri mülkiyet hakları kapsamında İSS’lerinin sorumlulukları belirleyen düzenlemeler açısından incelenmesi.....	77
6.8.6. Ulusal ve uluslararası standartları belirleyen düzenlemeler açısından incelenmesi.....	77

6.8.7. E-ticaret kapsamındaki düzenlemeler açısından incelenmesi.....	78
7. SONUÇ VE ÖNERİLER.....	79
KAYNAKLAR.....	85
EKLER.....	94
EK-1. NATO üyesi ülkeler.....	95
EK-2. ITU tarafından önerilen ulusal siber güvenlik strateji süreci.....	96
EK-3. ITU tarafından önerilen ulusal siber güvenlik strateji modeli.....	97
EK-4. Stratejinin tasarlanması ve geliştirilmesi.....	98
EK-5. Stratejinin uygulanması.....	99
EK-6. Stratejinin değerlendirilmesi.....	100
EK-7. Türkiye'nin 2013-2014 siber güvenlik eylem planı.....	101
EK-8. Sorumlu kurumların alt eylem başlıklarına göre dağılımı.....	102
EK-9. Türkiye'nin 2016-2019 siber güvenlik eylem planı.....	103
EK-10. Sorumlu kurumların alt eylem başlıklarına göre dağılımı.....	104
EK-11. Ulusal siber güvenlik strateji planı ve koordinatör makamı açısından incelenmesi.....	105
EK-12. Bilgisayar olaylarına müdahale ekipleri (CERT) açısından incelenmesi.....	107
EK-13. Uluslararası işbirliği açısından incelenmesi.....	108
EK-14. Ulusal siber güvenlik eylem maddeleri açısından incelenmesi.....	109
EK-15. Kişisel verilerin gizliliği kapsamındaki düzenlemeler açısından incelenmesi...	113
EK-16. Kişisel ve kurumsal güvenliğin geliştirilmesini sağlayan düzenlemeler açısından incelenmesi.....	115
EK-17. Siber suçlar kapsamındaki düzenlemeler açısından incelenmesi.....	117
EK-18. Fikri mülkiyet haklarının korunması kapsamındaki düzenlemeler açısından incelenmesi.....	120
EK-19. Fikri mülkiyet hakları kapsamında İSS'lerinin sorumluluklarını belirleyen düzenlemeler açısından incelenmesi.....	125
EK-20. Ulusal ve uluslararası standartları belirleyen düzenlemeler açısından incelenmesi.....	128
EK-21. E-ticaret kapsamındaki düzenlemeler açısından incelenmesi.....	131
ÖZGEÇMİŞ.....	134

ÇİZELGELERİN LİSTESİ

Çizelge		Sayfa
Çizelge 2.1	Zararlı yazılımlar.....	15
Çizelge 5.1	Alt amaçlar.....	59
Çizelge 5.2	Semboller.....	60
Çizelge 6.1	Uluslararası organizasyonlar.....	66
Çizelge 6.2	Uluslararası gelişme endeksleri açısından incelenmesi.....	69
Çizelge 6.3	İnternet kullanıcı sayıları açısından incelenmesi.....	72
Çizelge 6.4	Kişisel ve ulusal bant genişlikleri açısında incelenmesi.....	74



ŞEKİLLERİN LİSTESİ

Şekil		Sayfa
Şekil 1.1	İnternet kullanıcılarının yıllara göre değişimi.....	2
Şekil 2.1	Siber uzay.....	9
Şekil 2.2	Siber güvenlik prensipleri.....	10
Şekil 2.3	Siber güvenlik için 10 adım.....	12
Şekil 2.4	2001-2015 yılları arasında siber suçların uğrattığı maddi hasar.....	21
Şekil 2.5	Siber savaş denklemi.....	24
Şekil 3.1	NATO'nun sivil ve askeri yapısı.....	27
Şekil 3.2	NATO karar verme süreci.....	28
Şekil 3.3	Estonya siber savaşı zaman çizelgesi.....	31
Şekil 3.4	Gürcistan siber savaşı zaman çizelgesi.....	34
Şekil 3.5	NATO CCDCOE yönetim yapısı.....	37
Şekil 3.6	NATO siber savunma yönetim yapılanması.....	38
Şekil 3.7	NCIRC metodolojisi.....	39
Şekil 4.1	Ulusal siber güvenlik stratejisi yaşam döngüsü.....	48
Şekil 4.2	Türkiye'de siber güvenliğin gelişimi.....	50
Şekil 4.3	Türkiye'de siber güvenlik aktörleri.....	52
Şekil 5.1	Katılımcıların yaş durumları.....	58
Şekil 5.2	Katılımcıların eğitim durumları.....	58
Şekil 6.1	Ulusal siber güvenlik yapılanması.....	61
Şekil 6.2	Ulusal siber güvenlik strateji planı.....	63
Şekil 6.3	Ülkelere göre FIRST üyesi CERT sayısı.....	65
Şekil 6.4.(a)	CCDCOE üyelik durumu.....	67
Şekil 6.4.(b)	ENİSA üyelik durumu.....	67
Şekil 6.5	Evlerdeki kişisel bilgisayar oranları.....	69
Şekil 6.6	ITU ICT gelişme endeksi (IDI).....	70
Şekil 6.7	WEF ağ hazırlık endeksi.....	70
Şekil 6.8	Uluslararası bağlanabilirlik endeksi.....	71
Şekil 6.9	İnternet kullanıcılarının nüfusa oranı.....	72
Şekil 6.10	Sabit geniş bant aboneliklerinin internet kullanıcılarına oranı.....	73

Şekil		Sayfa
Şekil 6.11	Kişi başına düşen aktif mobil geniş bant abone sayısı.....	73
Şekil 6.12	Yıllara göre kullanıcı internet bant genişliği değişimi (Bps).....	75
Şekil 6.13	Yıllara göre ulusal internet bant genişliği değişimi (Gbps).....	75



SİMGELER VE KISALTMALAR

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

Kısaltmalar	Açıklamalar
APT	Gelişmiş Sürekli Tehdit (Advanced Persistent Threat)
BM	Birleşmiş Milletler
BOME	Bilgisayar Olaylarına Müdahale Ekibi
BSA	İş Dünyası Yazılımı İttifakı (Business Software Alliance)
BSS	Bulut Servis Sağlayıcısı
CCDCOE	NATO Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defence Centre of Excellence)
CCIRC	Kanada Siber Olaylara Müdahale Merkezi (Canadian Cyber Incident Response Centre)
CDMA	Siber Savunma Yönetim Otoritesi (Cyber Defence Management Authority)
CDMB	Siber Savunma Yönetim Kurulu (Cyber Defence Management Board)
CERT	Bilgisayar Acil Müdahale Ekibi (Computer Emergency Response Team)
CSIRT	Bilgisayar Güvenlik Olaylarına Müdahale Ekibi (Computer Security Incident Response Team)
DDoS	Dağıtık Servis Dışı Bırakma (Distributed Denial of Service)
DHS	İç Güvenlik Departmanı (Department of Homeland Security)
DPPC	Savunma Politikası ve Planlama Komitesi (Defence Policy and Planning Committee)
ENISA	Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (European Union Agency for Network and Information Security)
EU	Avrupa Birliği (European Union)
FIRST	Olay Müdahale ve Güvenlik Ekipleri Forumu (Forum of Incident Response and Security Teams)
IDI	BİT Gelişme Endeksi (ICT Development Index)
IMPACT	Siber Tehditlere Karşı Uluslararası Çok Taraflı Ortaklık (International Multilateral Partnership Against Cyber Threats)

Kısaltmalar	Açıklamalar
ITU	Uluslararası Telekomünikasyon Birliği (International Telecommunications Union)
İSS	İnternet Servis Sağlayıcısı
LOAC	Silahlı Çatışma Yasası (Law of Armed Conflict)
NAC	Kuzey Atlantik Konseyi (North Atlantic Council)
NATO	Kuzey Atlantik Antlaşma Örgütü (North Atlantic Treaty Organization)
NCCIC	Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi (National Cybersecurity and Communications Integration Center)
NCIRC	NATO Bilgisayar Olaylarına Müdahale Yeteneği (NATO Computer Incident Response Capability)
NCSS	Ulusal Siber Güvenlik Stratejisi (National Cyber Security Strategy)
NIS	Ağ ve Bilgi Güvenliği (Network and Information Security)
NRI	Ağ Hazırlık Endeksi (Networked Readiness Index)
OCSIA	Siber Güvenlik ve Bilgi Güvencesi Ofisi (Office of Cyber Security and Information Assurance)
SOME	Siber Olaylara Müdahale Ekibi
TCK	Türk Ceza Kanunu
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UDHB	Ulaştırma, Denizcilik ve Haberleşme Bakanlığı
ULAKBİM	Ulusal Akademik Ağ ve Bilgi
UN	Birleşmiş Milletler
USOM	Ulusal Siber Olaylara Müdahale Merkezi

1.GİRİŞ

“Siber saldırılar, ulusal güvenliğimiz ve ekonomimiz açısından karşılaştığımız en ciddi sorunlardan birisidir. 21’inci yüzyılda ulusumuzun ekonomik refahı, uygulayacağımız siber güvenlik politikalarına bağlıdır.”

Barrack Obama- 16 Eylül 2011 [1].

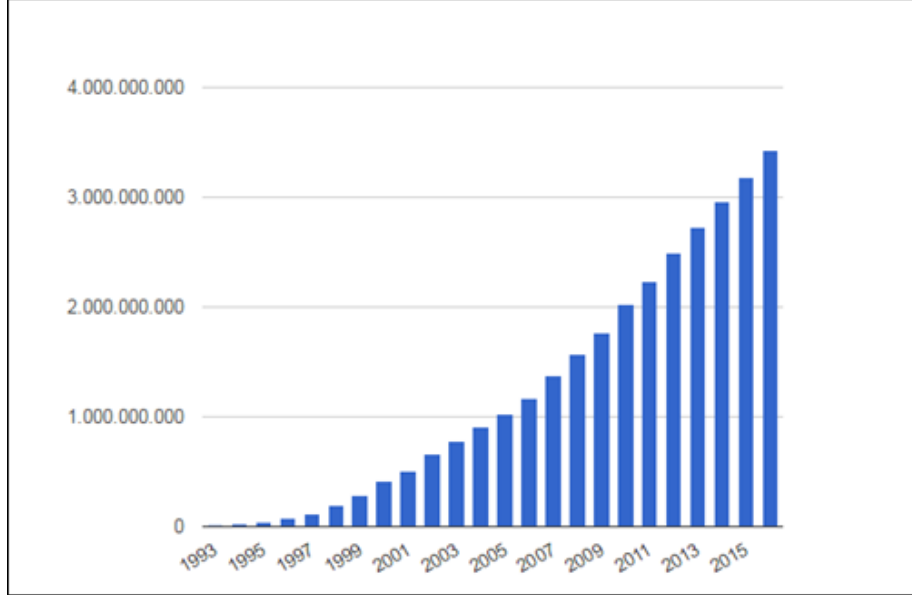
Maslow’un ihtiyaçlar hiyerarşisi teorisine göre güvenlik, insanoğlunun en temel gereksinimlerinden birisidir. Temel unsuru insan olan toplumlar ve devletler kendini korumak ve varlığını sürdürebilmek için geçmişten günümüze farklı güvenlik tedbirleri üretmişlerdir. İlk zamanlardan itibaren uygulanan fiziksel güvenlik tedbirleri günümüzde teknolojinin gelişmesi ile birlikte yetersiz kalmaya başlamıştır. Son 50 yılda bilgi ve iletişim teknolojilerinde meydana gelen gelişmeler, bireysel ve ulusal güvenlik kavramlarının tekrar gözden geçirilmesini sağlamıştır.

1.1. Araştırmanın Problemi

Küresel çapta internetin hızla gelişmesi ve askeri, siyasi, ticari alanda yeni bir araç olarak kullanılması, devletlerin ulusal ve uluslararası güvenlik açısından siber güvenliği birinci önceliğe almasına neden olmuştur. Bilgisayar ağları üzerinde ortaya çıkan tehditler kişisel, kurumsal hatta küresel bakımdan önemli sonuçlar doğurmaktadır. İnternet bankacılığı yapmakta olan kişinin hesabında gerçekleşecek bir dolandırıcılık hadisesi, sadece o kişinin zarar görmesine sebep olurken; bir kurumun veri tabanına karşı yapılan saldırı tüm kurum çalışanlarının ve kurumla irtibatlı olan kişilerin kimlik bilgilerinin ele geçirilmesine, hatta kurumun milli güvenliğe yönelik önemli bilgilerinin yetkisiz insanların eline geçmesine sebep olmaktadır.

İnternetin temel ortaya çıkış amacı iletişimi arttırmak ve bilgi paylaşımını kolaylaştırmak olmasına rağmen internetin tahmin edilenden de hızlı yaygınlaşması yeni bir bağımlılık türü olarak nitelenebilecek internet bağımlılığına yol açmaya başlamıştır. 1969 yılında ağa bağlanan cihaz sayısı dört iken, günümüzde bu sayı on milyarın üstüne çıkmıştır. 2016 yılı

Haziran ayı itibariyle dünyada 3.386.000.000 kişi interneti aktif şekilde kullanmaktadır. Aşağıdaki tablo internet kullanım sayısının yıllara göre değişimini göstermektedir.



Şekil 1.1. İnternet kullanıcılarının yıllara göre değişimi [2]

1988 yılında Harvard Üniversitesi'nde bir yüksek lisans projesi üzerine çalışan Robert Morris'in kendi soyadını taşıyan solucanı üniversitenin sistemine göndermesi sonucu korunmasız sistemlerde oluşan tahribatın ortaya çıkması, siber uzayın tehdit unsuru olarak algılanmasına neden olmuştur. Olaydan hemen sonra hazırlanan rapora göre; Morris solucanı 150 tane bilgisayarın yaklaşık 3 gün boyunca hizmet verememesine sebep olmuş ve ülkesinin en az 72500\$ zarar etmesine sebep olmuştur [3]. Her ne kadar Morris'in yaptığı deney hata sonucu kontrolden çıkan iyi niyetli bir deney olsa da, siber uzayı tehdit unsuru olarak kullanan kişi ve kurumlar için ilham kaynağı olmuştur. Morris deneyi, bilgisayarlar kullanılarak yapılan saldırıların, sadece bireylere değil kurumlara ve ülkelere de büyük zararlar verebildiğini ortaya koymuştur.

Siber saldırılar çok farklı yöntemler kullanılarak gerçekleştirilebilir. 2016 yılının Mart ayında yapılan araştırmaya göre; dünya üzerinde gerçekleşen siber saldırıların %73.9'u siber suç, %12.0'ı hacktivist eylem, %10.9'u siber casusluk, %3.2'si siber savaş olarak gösterilmiştir [4]. Bilgisayar güvenliği ve kriptografi üzerine önemli kitapları bulunan Bruce Schneier teknolojinin gelişmesiyle değişen güvenlik algısını şöyle özetlemiştir.

“Eğer teknolojinin güvenlik sorunlarını çözebileceğini düşünüyorsanız, teknolojiyi de sorunları da anlamamışsınız demektir” [5].

Saldırganlar sadece maddi kazanç sağlamak için saldırmazlar. Bazı saldırılar isim yapma, itibar kazanma, itibarı zedeleme, herhangi bir şeyi protesto etme, ses getirme ve bilgi çalma amacıyla da yapılır. Bu amaçlar doğrultusunda yapılan saldırıların en büyük hedefi genelde devlet kurum ve kuruluşlarıdır. Bir devletin gizli bilgilerinin diğer devletler tarafından bilinmesi ve ya ele geçirilmesi, o devletin zayıf yanlarının ortaya çıkmasına dolayısıyla ülkenin itibar kaybetmesine neden olacaktır. Söz konusu tehditlerin yaygınlaşması, ülkelerin ulusal siber güvenlik tedbirleri almasına ve güvenlik stratejileri uygulamasına zemin hazırlamıştır. 11 Eylül saldırısının ardından ABD Hükümetinin kurduğu İç Güvenlik Bakanlığı (Department of Homeland Security) tarafından 2003 yılında hazırlanan “Siber Uzayın Güvenliği İçin Ulusal Strateji Belgesi (National Strategy to Secure Cyberspace)” dünya devletleri arasında yayınlanan ilk ulusal siber güvenlik yol haritası olma özelliğini taşımaktadır. Diğer ülkelere ilham kaynağı olan ilk ulusal siber güvenlik strateji planı aşağıda belirtilen temel amaçlar doğrultusunda hazırlanmıştır[6]:

1. Ulusal kritik altyapılara karşı gerçekleştirilen siber saldırıları önlemek,
2. Siber saldırılara karşı ulusal güvenlik açığını azaltmak,
3. Siber saldırılar tarafından oluşacak hasarları ve hasarların iyileşme sürecini en aza indirmek.

İlk olarak ABD tarafından 2003 yılında yayımlanan ulusal siber güvenlik planının ardından tüm dünya ülkeleri ulusal güvenliğini artırmak ve bu bağlamda siber güvenlik vizyonunu belirlemek maksadıyla ulusal siber güvenlik strateji dokümanları hazırlamaya başlamışlardır. Ulusal siber güvenlik kavramı, siber güvenlik ve ulusal güvenlik kavramlarının birleşimi olarak tanımlanabilir. Ulusal siber güvenlik aşağıdaki maddelerde sıralandığı gibi idari, ulusal ve uluslararası olmak üzere üç yönlü düşünülmesi gereken bir faaliyettir:

1. İdari: Devleti yönetmekle görevli hükümet yetkilileri, devlet kademelerinde görev yapan ticaret, altyapı, telekomünikasyon gibi görevleri üstlenen devlet daireleri ile

askeri birimler ve kolluk birimleri arasında siber güvenlik sorumluluklarını belirlemelidir.

2. Ulusal: Ulusal siber güvenliğin sağlanması için devlet yetkilileri tarafından güvenlik firmaları ve kritik altyapı firmaları gibi bazı önemli sivil otoriteler ile belirli anlaşmalar yapılması ve firmaların yükümlülüklerinin belirlenmesi önem arz etmektedir. Klimburg, siber güvenlik konularında devlet kurumları ile sivil kurumların belirli politikalar ışığında işbirliği yapmasını “Bütün Ulus (A Whole of Nations)” yaklaşımı olarak tanımlamıştır [7].
3. Uluslararası: Dünyanın küresel köy olarak adlandırıldığı günümüzde hiçbir ulus devlet bireysel siber güvenliğini tek başına sağlayamaz. Devletler siber güvenlik altyapılarını güçlendirmek için uluslararası organizasyonlar aracılığıyla geniş çapta stratejik işbirliğine ihtiyaç duyarlar. Bu kapsamda Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA), NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (NATO CCDCOE), Uluslararası Telekomünikasyon Birliği (ITU) gibi uluslararası organizasyonlar karşılıklı anlaşmalar ile ülkelerin müşterek siber güvenlik gereksinimlerini karşılamaktadır.

1.2. Araştırmanın Amacı

Bu çalışmada, küreselleşen dünyada ülkeleri aynı çatı altında birleştiren en büyük organizasyonlardan biri olan NATO’nun ve NATO üyesi ülkelerin uyguladıkları siber güvenlik stratejilerinin mukayeseli olarak inceleyerek, Türkiye’nin uyguladığı siber güvenlik stratejisine olumlu katkılar yapmak amaçlanmıştır. Belirlenen amaca ulaşmak için incelenecek alt amaçlar şunlardır:

1. Ulusal Siber Güvenlik Stratejisi ve Koordinatör Makamı Açısından İncelenmesi
2. Bilgisayar Olaylarına Müdahale Ekipleri (CERT) Açısından İncelenmesi
3. Uluslararası İşbirliği Açısından İncelenmesi
4. Ulusal Siber Güvenlik Eylem Maddeleri Açısından İncelenmesi
5. Uluslararası Gelişme Endeksleri Açısından İncelenmesi
6. İnternet Kullanıcı Sayıları Açısından İncelenmesi
7. Kişisel ve Ulusal Bant Genişlikleri Açısından İncelenmesi

8. Hukuki Düzenlemeler ve Yönetmelikler Açısından İncelenmesi

8.1. Kişisel Verilerin Gizliliği Kapsamındaki Düzenlemeler Açısından İncelenmesi

8.2. Kişisel ve Kurumsal Güvenliğin Geliştirilmesini Sağlayan Düzenlemeler Açısından İncelenmesi

8.3. Siber Suçlar Kapsamındaki Düzenlemeler Açısından İncelenmesi

8.4. Fikri Mülkiyet Haklarının Korunması Kapsamındaki Düzenlemeler Açısından İncelenmesi

8.5. Fikri Mülkiyet Hakları Kapsamında İSS'lerinin Sorumlulukları Belirleyen Düzenlemeler Açısından İncelenmesi

8.6. Ulusal ve Uluslararası standartları belirleyen Düzenlemeler Açısından İncelenmesi

8.7. E-Ticaret Kapsamındaki Düzenlemeler Açısından İncelenmesi

Yukarıda belirtilen amaç ve alt amaçlar doğrultusunda, ortaya konulacak tezin daha iyi anlaşılabilmesi için;

- İkinci bölümde, literatürde geçen siber uzay, siber güvenlik, siber güç, siber terörizm, siber casusluk, siber tehdit, siber savaş gibi siber ortam kavramları açıklanmıştır.
- Üçüncü bölümde, NATO'nun tarihçesi, organizasyon yapısı, siber güvenlik çalışmaları, içinde bulunduğu siber savaşlar ve birlikte çalıştığı uluslararası organizasyonlar hakkında bilgi verilmiştir.
- Dördüncü bölümde, uluslararası siber güvenlik organizasyonları ve ülkemizin siber stratejisi hakkında bilgi verilmiştir.
- Beşinci bölümde, çalışmanın yöntemi açıklanmıştır.
- Altıncı bölümde ise NATO üyesi ülkelerin siber güvenlik stratejileri, siber güvenlik imkân ve kabiliyetleri belirlenen alt amaçlar doğrultusunda incelenmiş ve bulgular değerlendirilmiştir.

1.3. Araştırmanın Önemi

Son yıllarda bilgi ve iletişim teknolojilerinde gerçekleşen gelişmeler, coğrafi olarak sınırlarla ayrılan toplumların sanal ortamda bir arada olmasını sağlamıştır. Diğer bir deyişle sanal ortamda belirlenen dijital sınırlar ulusal sınırlarla örtüşmemektedir. Siber saldırılara karşı ulusal çıkarların korunması ve siber uzayın sınır güvenliğinin sağlanması hususunda karşılaşılan zorluklar, devletlerin uluslararası anlaşmalar yapmasını kaçınılmaz hale getirmiştir. NATO CCDCOE, ENISA ve ITU gibi uluslararası organizasyonlar aracılığıyla ülkeler siber saldırılara karşı dijital sınırlarını korumakta ve müşterek siber güvenlik stratejileri geliştirmektedir.

2007 yılında Estonya'nın başkenti Talinn'de bulunan bronz kızıl ordu askerini temsil eden heykelin kaldırılması üzerine kamu hizmetlerinin çok büyük bölümünün elektronik ortamda verildiği Estonya'daki bilişim sistemlerine yönelik siber saldırılar başlamış ve temelde kamu hizmetlerini hedef alan bu saldırılar dolayısıyla Estonya'da hayat durma noktasına gelmiştir. Yaşanan bu hadiseler sonrasında Kuzey Atlantik Antlaşma Örgütü (NATO) konu hakkında uzman personelini siber olayların incelenmesi için bölgeye göndermiştir. Yapılan incelemeler sonrasında Talinn'de NATO'nun bir unsuru olarak Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCOE) kurulmuştur. Söz konusu organizasyon, üye ülkelerin müşterek siber savunma stratejileri uygulamasına ve dijital sınırlarını güçlendirmesini sağlamıştır.

Günümüze gelinceye kadar yapılan akademik çalışmalar ile; siber güvenlik stratejisinin tanımlanması ve Aralık 2012 tarihinde hazırlanarak yürürlüğe giren Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın incelenmesi amaçlanmıştır.

Bu çalışma ile; mevcut bulunan akademik çalışmalardan farklı olarak NATO çatısı altında bulunan ulusların uyguladıkları siber güvenlik stratejileri mukayeseli olarak incelenecektir. Bu çalışma, 28 farklı devletin siber güvenlik altyapılarını, siber güvenlik stratejilerini, siber güvenlik faaliyetlerini ortaya koymak suretiyle, ulusal çapta icra edilecek siber güvenlik çalışmalarına yeni bir bakış açısı sunması ve bu konuda farkındalık yaratması açısından önemli bir katkı sağlayacağı düşünülmektedir.

1.4. Araştırmanın Kapsam ve Sınırlılıkları

İlk olarak ABD tarafından 2003 yılında yayımlanan ulusal siber güvenlik planının ardından tüm dünya ülkeleri ulusal güvenliğini artırmak ve bu bağlamda siber güvenlik vizyonunu belirlemek maksadıyla ulusal siber güvenlik strateji dokümanları hazırlamaya başlamışlardır. NATO üyesi 28 ülke bulunmaktadır. 2003 yılından günümüze gelinceye kadar 20 farklı NATO üyesi ülke onaylı Ulusal Siber Güvenlik Strateji belgelerini hazırlamıştır. Bu kapsamda onaylı Ulusal Siber Güvenlik Stratejisi bulunmayan 8 NATO üyesi ülke araştırma kapsamı dışında bırakılacaktır.

Onaylanmış Ulusal Siber Güvenlik Stratejisi bulunan ancak bu kapsamda icra ettikleri faaliyetleri ve planları kısıtlı olan Lüksemburg araştırma dışında bırakılacaktır.

Söz konusu kapsam ve sınırlılıklar göz önüne alındığında, inceleme onaylanmış Ulusal Siber Güvenlik Stratejisi bulunan 19 ülke üzerinde yapılacaktır.

Sayfa 4'te belirtilen ve ülkelerin siber güvenlik stratejileri konusunda genel çerçevesini gözler önüne seren ilk dört alt amaç kapsamında söz konusu 19 ülke incelenmiştir. Detaylı araştırmayı gerektiren sonraki alt amaçlar kapsamında NATO ortaklığında en büyük paya sahip olan 9 ülke (Kanada, Almanya, İspanya, Fransa, İtalya, Polonya, Türkiye, Birleşik Krallık ve A.B.D.) detaylı incelenecektir.



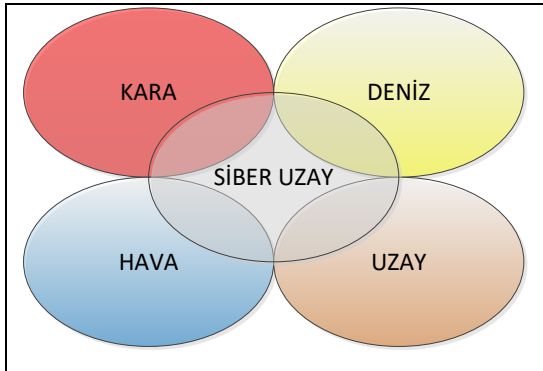
2. SİBER ORTAM KAVRAMLARI

Bu bölümde yaygın olarak kullanılan siber ortam kavramları açıklanacaktır.

2.1. Siber Uzay

İnternetin yaygın olarak kullanılmaya başlanması ile coğrafi kısıtlamalar ortadan kalkmış, insanların her türlü elektronik bilgi hizmetine erişimini mümkün kılan yeni bir dünya oluşmuştur. Bu dünya zamanla siber uzay olarak tanımlanmıştır.

“Siber Uzay” kavramı ilk olarak 1982 yılında bilim kurgu romanlarıyla bilinen William Gibson tarafından “Burning Chrome” adlı romanda kullanılmıştır. Ulusal Siber Güvenlik Stratejisinde “siber uzay” teriminin yerine “siber ortam” teriminin kullanılması tercih edilmiştir. Beşinci boyut olarak ta tanımlanan siber uzay; şekil 2.1’de görüldüğü gibi yeryüzü, hava, deniz hatta uzaydan bağımsız ve iletişim altyapılarını kullanan sanal bir ortamdır[8].



Şekil 2.1. Siber uzay

2.2. Siber Güvenlik

Uluslararası Telekomünikasyon Birliğine (ITU) göre siber güvenlik; kurum, kuruluş ve kullanıcıların bilgi varlıklarını korumak amacıyla kullanılan yöntemler, politikalar, kavramlar, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulama deneyimleri ve kullanılan teknolojilerin bütünü olarak tanımlanıyor [9]. Başka bir ifadeyle siber güvenlik;

bütünlük, gizlilik ve erişilebilirlik prensipleri ışığında bilgi ve erişim güvenliğini sağlamak için kullanılan araç ve yöntemlerin birleşimi olarak tanımlanabilir [10].

Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlamaktadır. Günümüzde oluşan tehditler ve bu tehditlerden bireylerin ve kurumların gördükleri zararlar göz önüne alındığında siber güvenliğin önemi daha iyi anlaşılacaktır. ABD Başkanı Obama 29 Mayıs 2009 yılındaki sunduğu siber güvenlik yasası önerisinde siber güvenliğin önemini şöyle ifade etmiştir:

“Biz enerji dağıtımında, gaz dağıtımında ve su dağıtımında bilgisayar ağı altyapımıza güveniyoruz. Biz toplu taşıma ve hava trafik kontrolü için de ağı altyapımıza güveniyoruz. Ancak, bu altyapıların güvenliğine yatırım yapma konusunda başarısız olduk. Mevcut durum artık kabul edilemez. Tehdit altında birçok yatırımımız mevcut. Biz daha iyisini yapabiliriz ve yapmalıyız”[11].

Siber güvenliğin birçok boyutu olmasına rağmen temel olarak aşağıdaki şekilde gösterilen yedi prensipten oluşmaktadır.

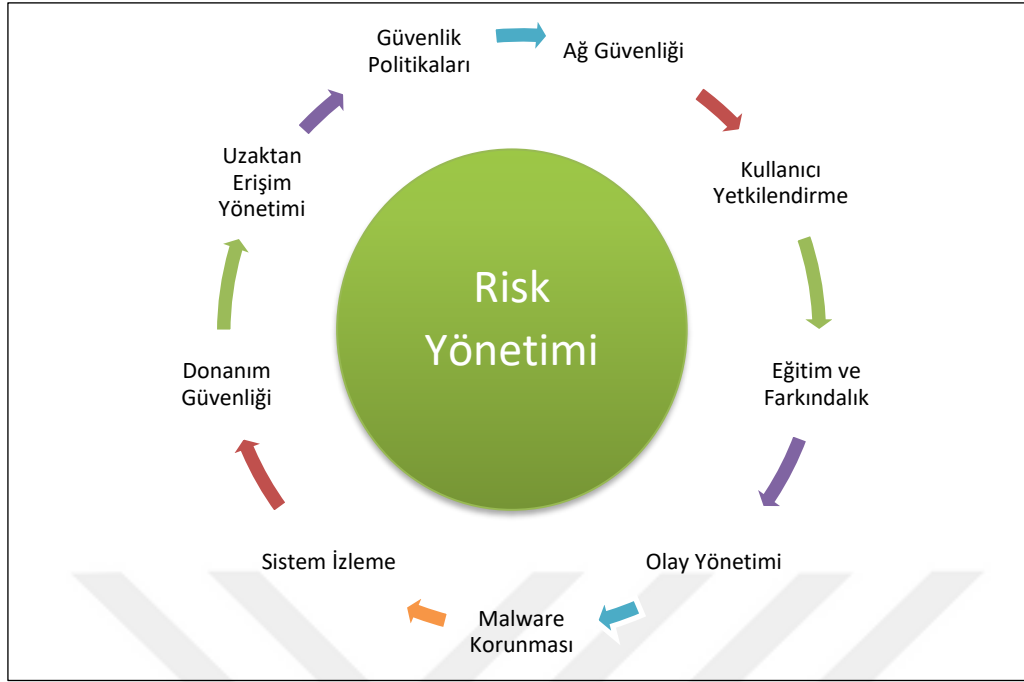


Şekil 2.2. Siber güvenlik prensipleri

Bilgi güvenliğini en üst seviyede sağlamak maksadıyla, uygulanan söz konusu prensipler aşağıdaki gibi tanımlanabilir:

- *Gizlilik:* Veriye sadece yetkili kişi veya sistemlerce erişilebilmesini ifade eder.
- *Bütünlük:* Verinin, göndericiden çıktığı haliyle bozulmadan ve değiştirilmeden alıcısına ulaşmasıdır.
- *Erişilebilirlik:* Yetkili kişilerin ve işlemlerin ihtiyaç duyulan zaman içerisinde ve ihtiyaç duyulan kalitede bilişim sistemlerine erişebilmesi demektir.
- *İzlenebilirlik:* Sistemde gerçekleşen olayların daha sonra analiz edilmez üzere kayıt altına alınmasıdır.
- *Kimlik Doğrulama:* Alıcının, göndericinin iddia ettiği kişi olduğundan emin olmasıdır.
- *Güvenilirlik:* Sistemde beklenen davranışlar ile elde edilen sonuçların birbiri ile tutarlı olmasıdır.
- *İnkâr Edememe:* Göndericinin gönderdiği mesajı, alıcının da aldığı mesajı inkâr edememesidir.

İngiliz Devletini siber saldırılara ve tehditlere karşı korumak amacıyla hükümet tarafından görevlendirilen güvenlik ve istihbarat kurumu olan GCHQ (Government Communications Headquarters), ulusal sanal sınırlarına karşı oluşan tehditleri ve saldırıları önlemek ve tedbirler üretmek için 2012 yılında “Siber Güvenlik için 10 Adım (10 Steps to Cyber Security)” dokümanını yayınlamıştır[12]. İngiliz Hükümeti tarafından ulusal siber güvenlik uygulamalarına rehber olması açısından geliştirilen 10 adımın yaşam döngüsü aşağıdaki şekilde gösterilmiştir.



Şekil 2.3. Siber güvenlik için 10 adım

- **Risk Yönetimi:** Kurumun ve ya organizasyonun yapması gereken en öncelikli faaliyet; sahip olduğu varlıkları korumak için harcayacağı emek ve kaynak ile korumadığı durumda karşılaşılabilecek yasal, finansal ve operasyonel yaptırımlar açısından risk analizi yapmaktır.
- **Güvenlik politikalarının oluşturulması:** Tüm bilgi iletişim teknolojilerinin devam eden süreçlerini güvenli ortamda yönetmek için kurumsal güvenlik konseptinin oluşturulması ve sürekli geliştirilmesi gerekmektedir.
- **Güvenli ağ erişiminin sağlanması:** Organizasyonlar çoğu zaman müşterek çalıştığı diğer organizasyonlar ile iletişime geçerken internet gibi güvensiz bir ağ altyapısı kullanmaktadır. Söz konusu iletişimin iç ve dış tehditlerden koruması için en temel güvenlik prensipleri olan; gizlilik, bütünlük ve erişilebilirlik özellikleri mevcut kullanılan ağ üzerinde uygulanmalıdır.
- **Kullanıcı yetki yönetimi:** Güvenlik denetimlerinin en üst düzeyde yapılması için kullanıcı seviyesinde yetkilendirmeler hassasiyet içinde yapılmalı ve ayrıcalıklı yetkilere sahip kullanıcılar en az seviyede tutulmalıdır.
- **Kullanıcı eğitimi ve farkındalığı:** Tüm yapılan araştırmalar güvenlik zincirinin en zayıf halkasının insan olduğunu göstermiştir. Bu kapsamda, güvenlik farkındalığının oluşturulması ve personelin eğitilmesi en temel güvenlik faaliyetidir.
- **Olay yönetimi:** Etkili olay yönetim politikalarının kurulması; iş sürekliliğini destekleyecek, müşteri ve ortaklarla güven tazeleyecek ve olumsuz finansal sonuçların etkisini azaltacaktır.

- *Kötücül yazılımdan korunma:* Kötü amaçlı yazılımların son kullanıcıya ve sistemlere erişmesi güvenlik duvarları, antivirüs yazılımları gibi yazılımsal tedbirlerle engellenmelidir.
- *Sistemi izleme:* Bilgi ve iletişim teknolojilerinin düzenli şekilde izlenmesi, ağa yapılacak saldırıların ve şüpheli aktivitelerin erken fark edilmesi ve gerekli tedbirlerin zamanında uygulanması için önemlidir.
- *Uç nokta donanım güvenliği:* Kurumsal ağlarda taşınabilir bellekler gibi donanımsal cihazların kullanımının kontrol edilmesi ve takibi veri kayıplarına ve veri kaçaklarına alınacak önemli tedbirlerdendir.
- *Mobil ve uzak bağlantılar için güvenlik politikası:* Mobil cihazların yaygınlaşması ve organizasyonların iş süreçlerinde kullanılması, organizasyonların uzak bağlantılar için yeni güvenlik tedbirleri almasını gerektirmiştir. Son zamanlarda kurumsal olarak kullanımı yaygınlaşan Mobil Cihaz Yönetim (MDM) uygulamaları bu kapsamda değerlendirilebilir.

2.3. Siber Saldırı

Siber tehditler; kişilerin, kurumların ve ülkelerin bilgi varlıkları ve teçhizatlarını hedef alan, onların mahremiyet, güvenlik ve iş görmesini bozan her türlü siber saldırılar ve yetkisiz müdahalelerdir. Siber korsanlar her geçen gün siber ortamda bulunan varlıklara sızmak için yeni yöntemler geliştirmektedirler. Sanal ortamda gerçekleştirilen bu eylemler karşısında olayın kurbanı olan bireyler gerek maddi gerekse manevi olarak mağdur olmaktadır. Siber saldırılardaki amaç; bilginin güvenliğini sağlamaya yönelik üç temel unsur olan gizlilik, bütünlük, erişilebilirlik prensiplerinin olumsuz yönde etkilenmesine neden olmaktır. Siber saldırılar;

- Sisteme yetkisiz erişim,
- Bilgilerin ifşa edilmesi,
- Bilgilerin çalınması,
- Sistemin bozulması,
- Bilgilerin değiştirilmesi,
- Bilgilerin yok edilmesi,
- Hizmetlerin engellenmesini hedeflemektedir.

General James Cartwright siber saldırıyı; bilgisayar, bilgisayar ağı ve ya sistemler kullanılarak düşmanın kritik sistemleri, varlıklarını yok etmeyi ve görevlerini yapamaz hale getirmeyi amaçlayan düşmanca bir davranış olarak tanımlamıştır[13].

Siber uzayda, bireylerin ve siber güvenlik uzmanlarının kendi bilgisayarlarını korumalarını gerektirecek çok fazla saldırı çeşidi bulunmaktadır. Saldırganlar bu saldırı yöntemlerini kullanarak sızmış oldukları bilgisayar ya da bilgisayar ağına değiştirici, yıkıcı, hizmet aksatıcı ya da verileri sızdırma şeklinde çeşitli zararlar verebilmektedir. Bu zararların organizasyon ya da kamu kurumuna maddi zararları olabileceği gibi itibarının azaltılması şeklinde zararları da olmaktadır. Bugüne kadar siber saldırılarla ilgili birçok yöntem geliştirilmiştir. En yaygın kullanılan siber saldırı yöntemleri aşağıda listelenmiştir.

- *Zararlı Yazılımlar:* Zararlı yazılımlar, sistem üzerinde ayrıcalıkları elde etmek, şifreleri öğrenmek, sistem kayıtlarını değiştirmek suretiyle kurban sistemde yetkisiz eylemler gerçekleştirmek için bilgisayar korsanları ve kod kırıcılar tarafından kullanılan virüsler, truva atları, solucanlar ve komutlardır[14]. Zararlı yazılımlar diğer bir adıyla malware, İngilizce “malicious” ve “software” kelimelerinin kısaltılmasından oluşmaktadır. En yaygın olarak saldırı maksadıyla kullanılan zararlı yazılım türleri aşağıdaki tabloda yer almaktadır.

Çizelge 2.1. Zararlı yazılımlar

Zararlı yazılım	Tanım
Virüs	Bilgisayara bulaşmak için dosyalara tutunan ve kendisini çoğaltabilen program parçalarıdır.
Truva atı (Trojan)	Faydalı bir program gibi görünüp arka planda daha farklı işler yapan programlardır.
Solucan (worm)	Kendisini mümkün olduğunca çok bilgisayara dağıtmak için tasarlanan programlardır. Virüslerden farkı; yayılmak için kullanıcıya ihtiyaç duymamasıdır.
Casus yazılım (Spyware)	Kullanıcıya ait bilgileri ele geçirmek maksadıyla yazılan program parçalarıdır
Tuş kaydediciler (Key Logger)	Kullanıcının klavyeden bastığı her tuşu dinleyip, Mouse hareketlerini ve ekran görüntüsünü kaydedebilen ve şartlar oluştuğunda verileri istenilen yere e-posta, ftp yada http protokolü kullanarak gönderebilen programlardır.
Reklam Yazılımı (Adware)	Bilgisayara çoğu zaman kullanıcı farkında olmadan kurulan küçük programlardır.
Fidye Yazılımı (Ransomware)	Bilgisayara bulaştıktan sonra bilgisayar üzerinde bulunan dosyaları şifreleyerek, şifrenin çözümü için belirli bir miktarda fidyenin verilen hesap numarasına yatırılması için uyarıda bulunan programlardır.

- *Oltalama Saldırıları:* Oltalama, istenmeyen e-posta ve ya yasadışı web sitesi aracılığıyla güvenilir bir kurumu taklit ederek; kullanıcı adı, şifre, banka hesap numarası ve ya kredi kartı numarası gibi kurum açısından hassas bilgilerin ele geçirilmesini amaçlayan adli açıdan suç vasfı taşıyan hileli bir süreçtir [15].
Oltalama saldırısı, Türk ceza hukukunda karşılığı olan ciddi bir suçtur. Bu yöntemle bankaların internet sitelerinin benzerlerini yaparak kullanıcıların banka hesap bilgileri ve şifrelerini ele geçiren siber korsan 199 yıl hapis cezası ile cezalandırılmış, verilen bu ceza Yargıtay 8 inci Ceza Dairesi tarafından onanmıştır.

- *İstenmeyen E-Posta:* Çok sayıda alıcıya aynı anda gönderilen gereksiz veya uygunsuz iletilerdir. İstenmeyen epostalar genelde reklam amaçlı olmaktadır. Aynı zamanda bu e-postalar kullanıcıların zararlı sitelere yönlendirilmesini sağlayarak, tıklama sahteciliği, yetkisiz erişim veya bilgi çalma gibi amaçlarla kullanılmaktadır.
- *Trafiğin Dinlenmesi:* Kelime anlamı koklamak olan sniffing, bir ağ üzerindeki bilgisayarlar arasındaki veri trafiğinin dinlenmesi anlamına gelmektedir. Şebeke trafiğinin dinlenmesinde mantık, yönlendiricilere gelen her paketin kabul edilmesi dolayısıyla iki bilgisayar arasındaki tüm verilerin yakalanarak saklanmasıdır[16].
- *Ortakdaki Adam Saldırısı:* Bir ağ üzerinde kurban bilgisayar ile diğer ağ araçları (yönlendirici, modem, ya da sunucu vb.) arasına girerek verileri yakalama ve şifrelenmemiş verileri görebilme ilkesine dayanan bir saldırı çeşididir.
- *Zombi Bilgisayar (Botnet) :* İngilizce Robot kelimesinin ikinci hecesi ile network (ağ) kelimesinin ilk hecesinin birleştirilmesinden oluşturulmuş bir kelimedir. Merkezi bir kontrol noktasına bağlanmış köle bilgisayar topluluğunu ifade etmektedir. Sahibinin haberi olmadan kendisine kötücül bir yazılım bulaşmış, uzaktan erişen yetkisiz kullanıcılara kendisini kullanma ve kontrol etme kabiliyeti veren ve bunlardan dolayı tehlike arz eden bilgisayarlara “zombi bilgisayar” veya “köle bilgisayar” denilmektedir.

Jason Andress ve Steve Winterfeld zombi bilgisayarların oluşturacağı riskleri şöyle açıklamıştır:

“Zombi bilgisayarlar, karmaşık matematiksel problemleri çözmek veya benzeri görevleri gerçekleştirmek için işlem gücünü müşterek kullanan ve hizmet dışı bırakma saldırısı gibi saldırılar icra edebilen büyük bilgisayar gruplarından oluşmaktadır. Bu gruplar savunmasız sistemler üzerinde inşa edilir. Eğer gerekli tedbirler almazsak ve sistemlerimizi korumazsak kurumsal sistemlerimiz, ev bilgisayarlarımız hatta hastane MR sistemi zombi bilgisayar ağına dâhil olacak”[17].

- *Sosyal Mühendislik:* İnsan faktörünü kullanan saldırı tekniklerinden ya da kişiyi etkileme ve ikna yöntemlerinden faydalanarak normal koşullar altında bireylerin paylaşmaktan çekindikleri bilgileri bir şekilde ele geçirme sanatı olarak tanımlanmaktadır[18]. Sosyal Mühendislik, saldırganın kendi isteği doğrultusunda davranmanız için kandırıldığınız bir tür psikolojik saldırıdır.
- *Siber Zorbalık:* Gün geçtikçe yaygınlaşan siber zorbalık; tehdit, taciz, nefret suçları gibi yasaya göre suç olarak sayılan faaliyetlerin bilgi ve iletişim teknolojileri

kullanılarak yapılması olarak tanımlanabilir. E-posta kullanarak yapılan hakaretler, sosyal medya vasıtaları kullanılarak paylaşılan utanç verici resimler, videolar ve web siteleri siber zorbalık faaliyetlerine örnek olarak gösterilebilir[19].

2.4. Siber Terörizm

Siber terörün tehdit potansiyeli gün geçtikçe artış göstermektedir. Günümüzde teknolojinin sunduğu imkânlardan terörist gruplarda faydalanmakta ve propaganda, eğitim, haberleşme, bilgi toplama gibi faaliyetlerde yaygın olarak kullanmaktadır. Siber terörizm söylemi, 1990'ların başlarında, internet teknolojilerinin hızla büyümeye başladığı, “bilgi toplumu” tartışmasının yapıldığı, teknoloji ve bilgisayar ağına fazlaca bağımlı olan ABD'nin karşılaşılabileceği riskleri inceleyen çalışmaların arttığı dönemde başlamıştır.

Terörün bir alt kümesi olarak siber terör, terörist amaçları gerçekleştirmek için bilgisayarların bir silah, bir yöntem ya da bir hedef olarak kullanılmasıdır [20]. Denning'e göre siber terörizm, bilgi sistemleri doğrultusunda elektronik araçların, bilgisayar programlarının veya diğer elektronik iletişim birimlerinin kullanılması aracılığıyla ulusal denge ve çıkarların tahrip edilmesini amaçlayan eylem veya etkinliktir [21].

2.5. Siber Casusluk

Son yıllarda siyasi amaçlı olduğuna inanılan birçok olay yaşandı. Söz konusu olayların büyük çoğunluğunu; kurbanın açık yanlarından faydalanılarak icra edilen istihbarat toplama faaliyetleri, fikri mülkiyet hırsızlığı ve teknolojik bilgi hırsızlığı oluşturmaktadır. Siber casusluk, düşmanın ve ya rakibin hassas bilgilerine erişmek ve rakibine karşı avantaj sağlamak için bilgisayarlar ve ya dijital iletişim faaliyetlerinin kasıtlı olarak kullanılması olarak tanımlanabilir[22].

İngiliz hükümeti, çoğunlukla siber casusluk ve fikri mülkiyet hırsızlığından kaynaklı siber suçların 2011'de ekonomisine maliyetinin yaklaşık 44 milyon dolar olduğunu ya da bir diğer ifadeyle İngiliz yurt içi gayri safi milli hasılanın %2'sine eşit olduğunu tahmin etmektedir[23].

Siber harekâtın karmaşık hukuk problemlerine açıklık getirmek maksadıyla ve NATO Siber Savunma Mükemmeliyet Merkezi (CCDCOE) koordinatörlüğünde ve Uluslararası Bağımsız Uzmanlar Grubu’nun katılımıyla hazırlanan “Siber Savaşta Uygulanacak Hukuk Hakkında Tallinn El Kitabı” 66ncı kuralda siber casuslukla ilgili aşağıdaki iki düzenlemeyi getirmiştir[24]:

1. Silahlı çatışma süresince, siber casusluk veya düşmana yöneltilmiş olan diğer bilgi toplama yöntemleri Silahlı Çatışma Hukukunu ihlal etmez.
2. Düşman kontrolü altındaki topraklarda siber casusluk görevi verilmiş bir silahlı kuvvetler personeli esir olma hakkını kaybeder ve ait olduğu silahlı kuvvetlere katılmadan yakalanırsa casus olarak muamele görür.

Uluslararası siber güvenlik firması McAfee’nin yayınladığı 2016 yılı siber tehdit tahminleri dokümanında, 2014 yılını "sarsılan güven yılı" olarak tanımlamış, 2015 yılını ise siber savaş ve casusluk faaliyetlerinin arttığını yıl olarak belirtmiştir. Aynı raporda, 2016 yılında siber tehditlerin daha karmaşık ve şiddetli olacağı, hassas bilgi çalma ve rakipleri yarış dışı bırakma faaliyetlerinin daha yoğun olacağı belirtilmiştir[25].

Bilgi toplama amacı ile yapılan hedef odaklı saldırıların yaygınlaşması yeni bir kavram olan APT (Advanced Persistent Threat – Gelişmiş Sürekli Tehdit) saldırılarının ortaya çıkmasını sağlamıştır. 2005 yılında sosyal mühendislik yöntemleri kullanılarak geliştirilen e-posta ile gerçekleştirilen ilk APT saldırı uyarıları aynı yıl ABD ve Birleşik Krallık CERT makamları tarafından yayınlanmıştır. 2005 yılında ilk raporlar yayınlanmasına rağmen APT kelimesi ilk olarak 2006 yılında ABD Hava Kuvvetleri’nde görevli Albay Greg RATTRAY tarafından ifade edilmiştir[26]. APT (Gelişmiş Sürekli Tehdit), hedef olarak belirlediği bilgi sistemlerine arasına girmek suretiyle kendini belli etmeden bulunduğu sisteme uyum sağlayan ve hassas bilgilere erişmeyi hedefleyen uzun süreli ve yavaş işleyen bir saldırı türüdür[27].

Günümüzde birçok ülke milli çıkarları doğrultusunda siber casusluk faaliyetleri yürütmektedir. Özellikle bir kısım ülkeler bundan çok büyük avantajlar elde etmektedir.

Ancak hiçbir ülke siber istihbarat sistemini ve bu alanda sahip olduđu imkân ve kabiliyetleri açıklamamaktadır. ABD İstihbarat raporlarına göre, dünya üzerinde gerçekleştirilen siber casusluk faaliyetlerinin büyük kısmı Çin Halk Cumhuriyeti ve Rusya merkezli gerçekleştirilmektedir.

Mandiant firmasının 2013 yılında yayınladıđı raporda, Çin Halk Cumhuriyeti ordusunun içindeki gizli bir birimin, dünyanın en yayılmacı casusluk grubu olduđu öne sürülmüştür. Mandiant şirketine göre, "61398" adlı birlik, dünya genelinde en az 141 kuruluştan "sistemik olarak yüzlerce terabaytlık veri" çalmıştır. 15 farklı ülkede konuşlu bulunan 141 kuruluşun 115 tanesinin ABD bünyesinde yer alması, asıl hedefin ABD'nin bilgi teknolojileri olduđu gerçeğini ortaya çıkarmıştır. Mandiant şirketine göre, 2004 yılından beri yürütöle siber casusluk faaliyetlerinin tamamı Çin Halk Cumhuriyeti Hükümeti tarafından bilinmekte ve desteklenmektedir. Siber casusluk faaliyetlerinin izi süröldüđünde, Şangay'ın Pudong bölgesindeki 12 katlı bir binaya ulaşıldıđını aktaran Mandiant Şirketi, Çin Halk Kurtuluş Ordusu'nun 61398 numaralı birliđinin de aynı yerde olduđuna dikkat çekmektedir[28]. Söz konusu raporun ortaya çıkmasının ardından Çin Halk Cumhuriyeti Savunma Bakanlığı aşğıdaki ifadeyi kullanarak olayı reddetmiştir.

“Çin Halk Cumhuriyeti herhangi bir siber saldırıyı desteklememiştir. Siber saldırılar uluslararası ve anonim özellik taşımaktadır. Herhangi bir kesin kanıt olmadan siber saldırılar konusunda Çin Ordusunun suçlanması profesyonellikten uzak ve iddialar dayanaksızdır”[29].

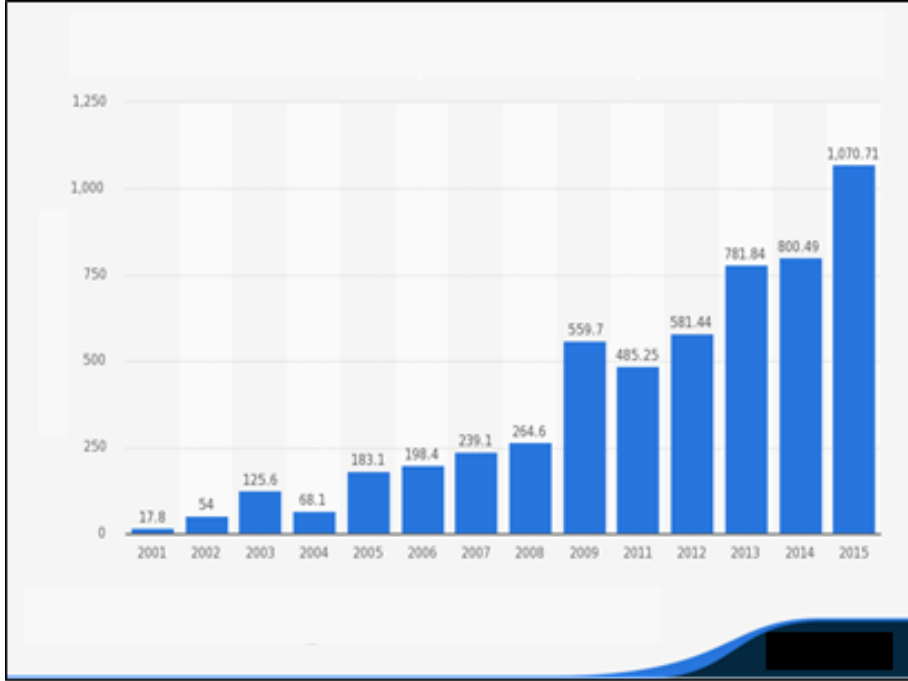
Rusya 2000 yılı sonrasında ulusal çıkarları doğrultusunda bilgi harekâtı stratejilerine ağırlık vermiş ve çevresinde bulunan ülkelere siber saldırılar yapmak suretiyle ülkeler üzerinde varlıđını hissettirmeye çalışmıştır.

“Pawn Storm” isimli Rus siber casusluk grubunun son zamanlarda Dünya’da birçok hükümet kurumunu ve haber kuruluşunu hedef aldıđı bildirildi. Pawn Storm’un son zamanlarda hedef listesine Türkiye’nin de dâhil ettiđi iddia edildi. Pawn Storm’un Türkiye saldırılarında daha önce birçok siber suçlarda kullanılan ve Hollanda’da bir şirket tarafından sağlanan altyapının kullanılabileceđi, bu nedenle çok fazla zarar oluşmadan konuya ilişkin önlemlerin alınması tavsiye edilmektedir[30].

2.6. Siber Suç

Bilişim teknolojilerindeki gelişmelerin topluma getirdiği yenilikler insanlara hayatı kolaylaştırıcı faydalar sağlamıştır. Ancak bütün bu faydalarının yanında bir takım olumsuzluklar da, bu gelişmelerle birlikte hayatımıza girmiştir. Teknolojinin sağladığı imkânlardan faydalanan art niyetli insanlar siber uzayı suç işlemek için yeni bir alan olarak görmüşlerdir.

Bilişim ile ilgili suçlar 1960'lı yılların sonuna kadar bilinmeyen bir olguydu. Bilinen ilk bilişim suçu, 18 Ekim 1966 tarihli Minneapolis Tribune'de yayınlanan "Bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" başlıklı makale ile kamuoyuna yansımıştır[31]. İnternet üzerindeki işlemlerin ekonomik değerinin artması, internetin anonim yapısı, saldırı araçlarının ucuzlaması ve bunlara erişimin kolaylaşması, suçlular arasındaki işbirliğinin kolaylaşması ve artması gibi nedenlerle önümüzdeki dönemde yeni suç türlerinin ortaya çıkması ve siber suçlarda artışın devam etmesi beklenmektedir[32]. Siber saldırılarla ilgili istatistikler tutan "hackmageddon" internet sitesinin Nisan 2016 tarihli araştırmasına göre dünya üzerinde gerçekleşen siber saldırıların %71,1'i siber suç, %14,5'i Haktivizm, %7,2'si siber casusluk faaliyetleri ve %7,2'si ülkeler arası siber savaşlar olarak karşımıza çıkmaktadır[33]. Amerika Birleşik Devletleri'nde FBI bünyesinde kurulan ve 2001 yılında itibaren faaliyet gösteren "İnternet Suç Şikayet Merkezine (Internet Crime Complaint Center)" göre 2001-2015 yılları arasında ilgili merkeze rapor edilen siber suçların maruz bıraktığı maddi hasarın değişimini gösteren grafik aşağıdaki resimde gösterilmiştir.



Şekil 2.4. 2001-2015 yılları arasında siber suçların uğrattığı maddi hasar[34]

Bilişim teknolojilerinin gelişmişliği ve kullanım yaygınlığı dünyanın farklı bölgelerinde ve farklı ülkelerinde değişkenlik göstermektedir. Bu ve benzeri sebeplerden dolayı evrensel bir “bilişim suçu” tanımı dahi yapılamamaktadır. Hatta terim olarak “bilişim suçu” yerine “bilgisayar suçu”, “siber suç”, “ileri teknoloji suçu”, “yüksek teknoloji suçu”, “sanal suç”, “internet suçu”, “bilgisayar bağlantılı suç”, “bilişim sistemi aracılığıyla işlenen suç”, “elektronik suç” gibi terimler kullanılmaktadır[35].

Siber suçlar, bilgisayarlar ve bilgi sistemlerini birincil araç ya da birincil hedef olarak kullanmak suretiyle geniş yelpazede işlenen suç faaliyetlerini ifade eder. Siber suçlar; geleneksel suçları (dolandırıcılık, sahtecilik ve kimlik hırsızlığı), içerikle ilgili suçları (internet üzerinden çocuk pornografisi dağıtımı, ırkçılıklar ilgili nefret suçları) ve bilgi sistemlerine özgü suçları (bilgi sistemlerine karşı yapılan saldırılar, hizmet dışı bırakma saldırısı ve kötücül yazılımlar) içermektedir[36].

Avrupa Konseyi Siber Suç Sözleşmesi’ne göre siber suçlar, bilgisayar veri veya sistemlerinin gizliliği, bütünlüğü ve kullanıma açık bulunmasına yönelik suçlar, bilgisayarlarla ilişkili suçlar,

içerikle ilişkili suçlar ve fikri mülkiyet haklarının ihlali ile ilgili suçlar şeklinde sınıflandırılmıştır[37].

Siber suçların yaygınlaşması ile birlikte siber suçlarla mücadele kapsamında küresel çapta tedbirler alınmaya başlanmıştır. Bu kapsamda, 1996 yılında Avrupa Suç Sorunları Komitesi internet ortamında işlenen suçları gözlemleyebilen uzmanlardan oluşan bir komitenin kurulması konusunda çalışmalar yapmıştır. Oluşturulan bu komite 2001 yılının Haziran ayında Avrupa Konseyi Siber Suç Sözleşmesini (The Council of Europe Convention on Cybercrime) kaleme almıştır. 8 Kasım 2001 tarihinde Avrupa Konseyi Bakanlar Komitesince bu sözleşme onaylanmış 23 Kasım 2001 tarihinde imzaya sunulmuştur. Macaristan'ın başkenti Budapeşte'de imzaya sunulan bu sözleşmeyi 43 Avrupa Konseyi üyesi devlet ve konseye üye olmayan 4 devlet (Kanada, Japonya, Güney Afrika ve ABD) imzalamıştır[38].

Uluslararası alanda yukarıda örnekleri verilen siber suçlarla mücadele kapsamında ülkemizde de çeşitli çalışmalar yapılmaktadır. Örneğin; Türkiye, 10 Kasım 2010 tarihinde Uluslararası Siber Suç Sözleşmesi'ni imzalayarak anlaşmaya taraf olmuş ancak yürürlüğe girmesi 2 Mayıs 2014'te Resmi Gazete'de yayınlanmasıyla gerçekleşmiştir[39]. Siber suçlar diğer bir ifadeyle bilişim suçları, 3756 sayılı Kanun'la TCK 1989 Tasarısı'ndan küçük değişiklikler yapılarak alınmış ve 765 sayılı (mülga) TCK'nın 525a-525d maddelerinde ülkemiz bakımından ilk defa 1991 yılında düzenlenmiştir. Bilişim Suçları Türk Ceza Kanunu'nun ikinci kitabının "Topluma Karşı Suçlar" başlıklı üçüncü kısmında, "Bilişim Alanında Suçlar" başlıklı onuncu bölümünde 243, 244, 245 ve 246. maddelerinde ele alınmıştır.

2.7. Siber Savaş

Siber alandaki faaliyetlerin kolay ve arkada iz bırakmadan yapılabilir oluşu terör örgütlerinin yanı sıra devletlerin de ilgisini çekmeye başlamıştır. Hatta kimi ülkeler siber saldırı ve siber savaş yöntemlerini önemli stratejik savunma ve rakibe zarar verme yöntemi olarak görmektedirler. Ülkelerin kendi çıkarları doğrultusunda bilgi ve iletişim teknolojilerini silah olarak kullanması, klasik konvansiyonel savaşın yerini siber savaşın almasını sağlamıştır.

Eski ABD Başkanı Bush'un Siber güvenlik danışmanı Richard A. Clarke "Cyber War" adlı kitabında siber savaşı şöyle tanımlamıştır:

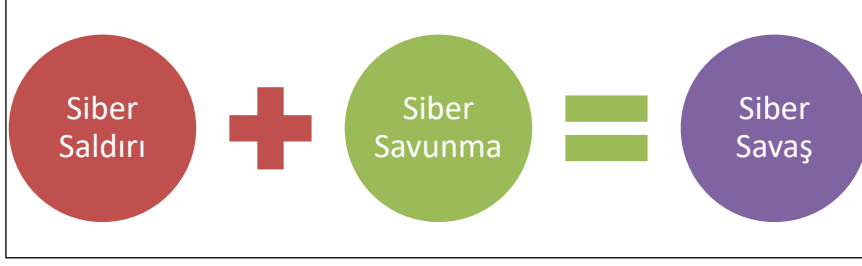
"Siber savaş, bir devletin, diğer bir devletin bilgisayar sistemlerine ve ya ağlarına hasar vermek ya da bozmak amacıyla gerçekleştirdiği faaliyetlerdir."[40]

Siber savaş, kendi içinde birçok yöntem ve teknik barındırmaktadır. Siber savaş meydanında kullanılabilecek çalışma alanları vardır. Casusluk, manipülasyon, propaganda, iletişimin kontrol altına alınması, virüs ve Truva atlarıyla sistemlerin bozulması, siber bombalarla sabotaj, sistem kilitleme, dolandırıcılık, bilgi kirliliği gibi bir çok alan siber savaşın oluşumuna katkı sağlamaktadır[41].

2010 yılında yayınlanan "Clatham House Report" siber savaşı diğer savaşlardan ayıran en temel özellikleri aşağıdaki başlıklar altında sıralamıştır[42].

- Silahlı çatışmaya gerek kalmadan siyasi ve stratejik hedeflere ulaşmayı mümkün kılar.
- Küçük ve nispeten önemsiz aktörlere orantısız güç imkânı verir.
- Sahte IP adresleri ve yabancı sunucuların arkasında faaliyet göstererek kısa süre anonimlik sağlayabilir.
- Konvansiyonel harpten farklı olarak kara, deniz, hava, uzay haricinde siber uzay olarak tanımlanan beşinci boyutta icra edilir.
- Klasik harp çatışma ve baskı rejimi gibi unsurlardan sonra ortaya çıkmasına rağmen siber savaş fiziksel baskı ve çatışma ortamından uzaktır.

Siber savaş ve siber saldırı birbirinden farklı hususlardır. Siber saldırılarda hedef kişi, şirket, kurumlar iken siber savaş ülkeleri hedef almaktadır. Siber savaş, siber saldırı ve siber savunmayı ihtiva eden daha genel bir kavramdır[43].



Şekil 2.5. Siber savaş denklemi



3. KUZEY ATLANTİK ANTLAŞMA ÖRGÜTÜ (NATO) VE SİBER GÜVENLİK

NATO ilk olarak Kosova Krizi esnasında büyük çapta siber saldırıya maruz kaldı. Bu olayda NATO ittifakının e-posta hesabı günlerce ziyaretçilere açık kaldı ve NATO web sitesi sık sık kesintiye uğradı. Bu tarihten itibaren NATO ve NATO üyesi ülkelerin bilgi sistemleri defalarca saldırıya uğradı. Mevcut durum karşısında NATO siber güvenlik çalışmalarına hız vermiştir. NATO'nun Siber Güvenlik yapılanmasının daha iyi anlaşılabilmesi için ittifakın tarihçesi ve gelişim süreci iyi bilinmelidir.

3.1. NATO'nun Kuruluşu ve Üye Ülkeler

İkinci Dünya Savaşının sona ermesi ile birlikte güç dengeleri değişmiş ve savaşın yol açtığı yıkımla zayıflayan Batı Avrupa ülkelerinin aksine; Amerika Birleşik Devletleri ve Rusya iki süper güç olarak tarih sahnesine çıkmıştır. 1945-1949 yılları arasında Amerika Birleşik Devletleri ve Batı Avrupa ülkeleri savaş sonrası yaralarını sarmak için savunma yapılanmalarını küçültme ve savunma kuvvetlerine düşürme yolunu seçerken; Rusya, Doğu Avrupa'da yayılmacı politikayı izlemiş ve savunma yapılanmalarına hız kesmeden devam etmiştir. Rusya'nın yayılmacı politikası karşısında kendilerini tehlikede hisseden Batı Avrupa ülkeleri ve Kuzey Amerika ülkeleri tarafından 4 Nisan 1949 tarihinde imzalanan ve 14 maddeden oluşan Washington Antlaşması ile Kuzey Atlantik Antlaşma Örgütü (NATO) ittifakı kurulmuştur. 12 kurucu ülke tarafından imzalanan Washington Antlaşması'na göre;

- İttifakın temel görevi, Birleşmiş Milletler Yasası ilkeleri doğrultusunda, politik ve askeri yollarla üyelerinin özgürlük ve güvenliğini güvence altına almaktır.
- İttifak'ı destekleyen temel ilke, egemen devletlerarasında üyelerin güvenliğinin bölünmezliği esasına dayanan işbirliği taahhüdüdür.
- İttifak'ın amacı, Kuzey Atlantik sahasında barışçıl ve dostane ilişkiler geliştirmektir.

Ancak, Antlaşma'nın imzalandığı tarihte NATO'nun öncelikli amacı, üyelerini eski Sovyetler Birliği'nin politikası ve giderek büyüyen askeri kapasitesinin oluşturduğu potansiyel tehdide karşı korumaktı[44].

Kurulduğu tarihten itibaren günümüze gelen süreçte ittifaka katılım durumu EK-1’de sunulmuştur[45].

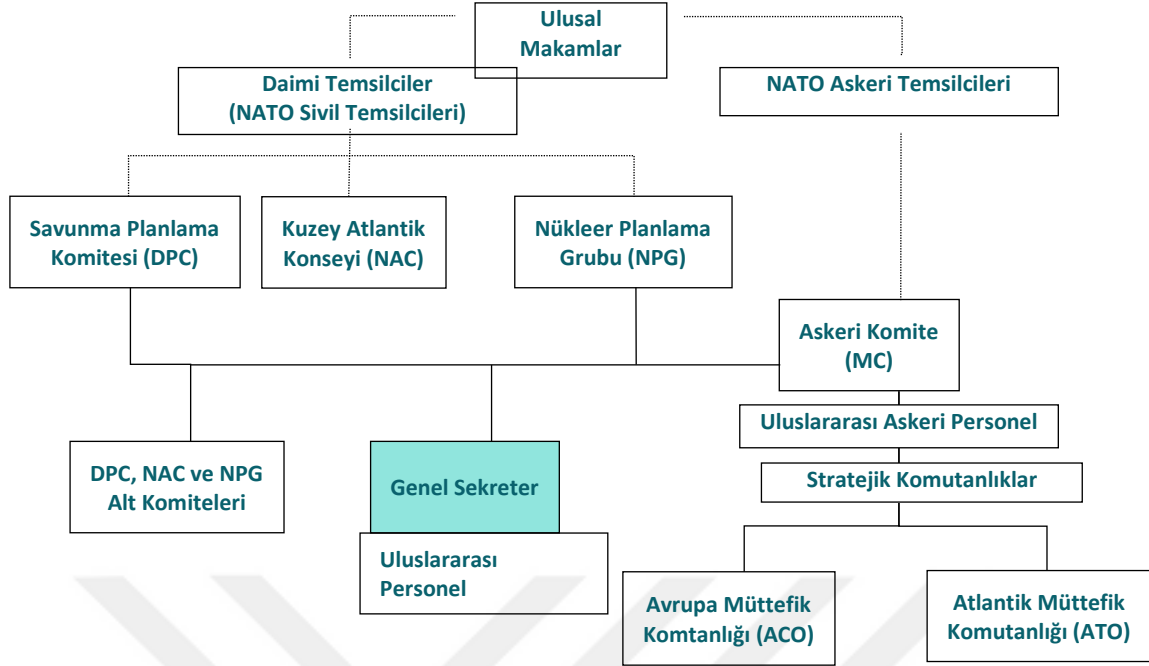
Washington Antlaşması ile Birleşmiş Milletler Yasası’na bağlı ülkeleri bir araya getiren İttifak, temel amacını gerçekleştirmek için “güvenlik”, “dayanışma” ve “caydırıcılık ve savunma” olmak üzere üç temel güvenlik görevini yerine getirir. NATO üyesi ülkeler kendilerine yöneltilen saldırı tehdidine karşı caydırıcılık ve savunma hakkı kapsamında aşağıda belirtilen beşinci maddenin işlemlerini talep edebilirler.

“Taraflar, Kuzey Amerika’da veya Avrupa’da içlerinden bir veya daha çoğuna yöneltilecek silahlı bir saldırının hepsine yöneltilmiş bir saldırı olarak değerlendirileceği ve eğer böyle bir saldırı olursa BM Yasası’nın 51. Maddesinde tanınan bireysel ya da toplu öz savunma hakkını kullanarak, Kuzey Atlantik bölgesinde güvenliği sağlamak ve korumak için bireysel olarak, ve diğerleri ile birlikte, silahlı kuvvet kullanımı da dâhil olmak üzere gerekli görülen eylemlerde bulunarak saldırıya uğrayan Taraf ya da Taraflara yardımcı olacakları konusunda anlaşmaya varmışlardır.

Böylece herhangi bir saldırı ve bunun sonucu olarak alınan bütün önlemler derhal Güvenlik Konseyi’ne bildirilecektir. Güvenlik Konseyi, uluslararası barış ve güvenliği sağlamak ve korumak için gerekli önlemleri aldığı zaman, bu önlemlere son verilecektir”[46].

3.2. NATO Organizasyon Yapısı

NATO içerisinde oluşturulan yapılar, üye ülkelerin politikalarını temel görevleri yerine getirebilecek şekilde koordine etmelerine olanak sağlar. Bu yapılar politik, ekonomik ve askeri olmayan diğer konular üzerinde olduğu kadar, ortak savunma için müşterek planların tasarlanması; askeri kuvvetlerin görev yapabilmesi için gerekli altyapı ve tesislerinin kurulması; müşterek eğitim programları ve tatbikatların düzenlenmesi konularında daimi bir danışma ve işbirliği olanağı sunarlar. Aşağıdaki şekil Kuzey Atlantik Antlaşma Örgütü’nün sivil ve askeri yapılanmasını göstermektedir[47].



Şekil 3.1. NATO'nun sivil ve askeri yapısı

Brüksel'deki NATO Karargâhı İttifak'ın siyasi karargâhı ve Kuzey Atlantik Konseyi'nin daimi mekânıdır. Daimi Temsilcileri ve ulusal delegasyonları, Genel Sekreter ve Uluslararası Yazmanlığı, ulusların Askeri Temsilcilerini, Askeri Komite Başkanını ve Uluslararası Askeri Karargâhı içinde barındırır. Kuzey Atlantik Konseyi'nde her üye devlet bir Büyükelçi veya Daimi Temsilci tarafından temsil edilmektedir. Bu temsilci ülkelerini değişik NATO komitelerinde temsil eden danışman ve görevlilerden oluşan bir ulusal delegasyon tarafından desteklenir.

Genel Sekreter üye hükümetler tarafından, Kuzey Atlantik Konseyi, Savunma Planlama Komitesi ve Nükleer Planlama Grubu'nun Başkanı, diğer üst düzeyli NATO Komitelerinin Fahri Başkanı ve NATO'nun Genel Sekreteri ve en üst düzeydeki yöneticisi olarak tayin edilen üst düzeyli, uluslararası bir devlet adamıdır. Genel Sekreter, İttifak içinde danışma ve karar alma sürecini geliştirmek ve idare etmekten sorumludur.

NATO'nun askeri kanadına üye olmayı seçen tüm ülkeler NATO'ya kuvvet tahsis ederler. Bu kuvvetler İttifak'ın bütünleşmiş askeri yapısını oluştururlar. Entegre askeri yapı demokratik devletlerde politik ve askeri kurumlar arasındaki ilişkileri yönlendiren temel ilkeler

doğrultusunda daima en üst düzeyde siyasi kontrol ve yönlendirme altındadır. Entegre askeri yapının rolü, Kuzey Atlantik Antlaşması'nın 5'inci Maddesi uyarınca üye ülkelerin topraklarını güvenlik ve istikrarlarına yönelik tehditlere karşı koruyacak örgütsel çerçeveyi sağlamaktır.

NATO bir demokrasiler ittifakıdır ve üyesi olan ülkelerin parlamentoları NATO ülkelerinin vatandaşları ile NATO liderleri arasındaki en önemli iletişim kanalıdır. Tüm NATO kararları üye ülkeler arasında tartışma ve istişare sonrasında, oy birliği ile alınır. Aşağıdaki şekil NATO'nun karar verme sürecini özetlemektedir.



Şekil 3.2. NATO karar verme süreci

3.3. NATO Siber Güvenlik Stratejisini Etkileyen Siber Savaşlar

Soğuk savaşın bitmesiyle birlikte siber tehditler ve saldırılar daha yaygın, karmaşık ve zararlı hale gelmiştir. Günümüzde hibrit savaşın bir parçası olarak görülen siber saldırılar, devlet ve devlet dışı aktörler tarafından askeri operasyonlar kapsamında bir tehdit unsuru olarak kullanılmaktadır. 1988 yılında ortaya çıkan ve ciddi zararlara sebep olan Morris solucanının ardından günümüze kadar sayısız siber saldırı gerçekleştirilmiştir. NATO ittifakı uzun bir süredir söz konusu karmaşık tehdit ortamıyla karşı karşıyadır. NATO son yirmi yıl içerisinde siber saldırılara karşı savunmasını güçlendirmek yeni tedbirler üretebilmek için bazı

yöntemler ve stratejiler uygulamaktadır. Bu süreç içerisinde NATO'nun siber güvenlik tedbirleri üretmesine zemin hazırlayan üç önemli siber savaş gerçekleşmiştir.

3.3.1. NATO Kosova Krizi - 1999

Dağılma sürecine giren Yugoslavya Federal Cumhuriyeti ordusunun, bağımsızlık isteyen Kosova Kurtuluş Ordusuna karşı sürdürdüğü operasyonlara NATO müdahale etmiştir. NATO, 30 Ocak 1999 tarihinde yaptığı basın açıklamasında Yugoslavya'daki hedeflere hava saldırı yapma yetkisinin Genel Sekreterde olduğunu belirtmiştir[48].

NATO uçakları Sırbistan'ı bombalamaya başlayınca, "Black Hand" gibi Sırp yanlısı ve Batı karşıtı hacker grupları NATO'nun internet altyapısına saldırmaya başladı. Siber saldırıların, Yugoslavya Federal Cumhuriyeti'nin askeri kuvveti için gerçekleştirilip gerçekleştirilmediği tespit edilemese de, NATO'nun askeri operasyonlarını bozmayı hedeflediği ortadadır. "Black Hand" hacker grubu ismini, 1'inci Dünya Savaşı'nın başlamasına sebep olan Pan-Slav gizli bir topluluktan almıştır. Savaş sırasında "Black Hand" hacker grubunun NATO'ya ait en önemli bilgisayarları ele geçirdiği ve bilgisayarlar üzerindeki tüm verileri sildiği iddia edildi[49].

Kosova Savaşı, NATO'nun karşılaştığı ilk siber savaş deneyimidir. Savaş esnasında siber ortam, aktivistler ve muharip güçler tarafından propaganda yapma ortamı olarak kullanılmıştır. Savaş esnasında kayda değer sayıda web sitesi ele geçirilmiş ve propaganda maksatlı kullanılmıştır. Bazı durumlarda e-postalara eklenen virüsler tahrif etmek amaçlı kullanılmıştır. Çatışma esnasında ABD uçaklarının yanlışlıkla Belgrad'ta bulunan Çin Büyükelçiliğini bombalamasıyla, Çin hackerler siber saldırılara dâhil olmuştur[50].

NATO, Kosova Savaşı'nda amacına ulaşmış gibi görünse de siber saldırılara karşısında yetersiz kalmıştır. NATO'ya yapılan saldırıda, web sitelerine bırakılan mesajlar, saldırganların kim olduklarını; olayın evveliyatına bakıldığında ise neden bu saldırıyı yaptıklarını açıkça göstermektedir. NATO, Kosova'da maruz kaldığı siber saldırılar

sonrasında bir dizi önlem almıştır. Bu önlemler NATO'nun siber güvenlik açısından ilk adımları olarak görülmektedir.

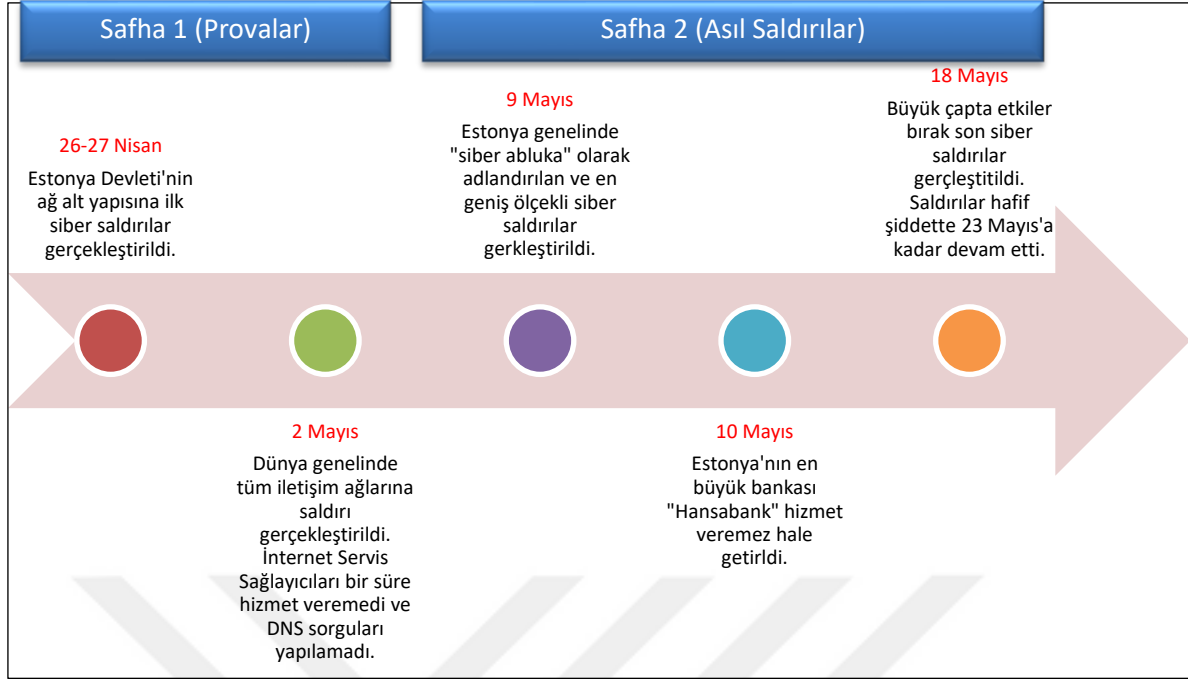
3.3.2. Estonya Siber Savaşı - 2007

2006 yılı Şubat ayında, Amerika Birleşik Devletleri'nde ismi "Cyber Storm" olan devletin bilgi sistemleri ve kritik altyapı elemanları da dâhil olmak üzere geniş bir yelpazede birçok kurumu etkileyen ilk tam ölçekli siber güvenlik tatbikatı düzenlendi[51]. 2007 yılının Nisan ayına gelindiğinde tatbikattaki senaryo Estonya sınırları içerisinde gerçekleşti. Estonya'ya gerçekleştirilen siber saldırılarda üç haftalık zaman dilimi içerisinde Estonya sınırları içerisinde bulunan sunucular ve yönlendiriciler de dâhil olmak üzere 178 farklı ülkeden yaklaşık bir milyon bilgisayar hedef haline geldi[52].

Estonya siber savaşı Sovyetler Birliği'nin Estonya üzerinde baskıcı 50 yılının sonucu olarak ortaya çıkmıştır. Sovyetler Birliğinin 1989 yılında dağılması, Estonya'nın bağımsız bir devlet olarak yerini almasını sağlamıştır. Siber saldırılar, 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[53].

Saldırıların başladığı 27 Nisan tarihinden itibaren Estonya Devlet sitelerinin internet trafiğinin yaklaşık 400 kat artış göstermesi saldırıların daha önceden planlandığını ve iyi koordine edildiğini göstermektedir. Saldırganlar dünya üzerinde dağıtık yapılandırılmış binlerce zombi bilgisayar kullanarak, kısa sürede Estonya Devlet sitelerine hizmet dışı bırakma (DDoS) saldırısı gerçekleştirmiş, Estonya Reform Partisi'nin web sitesini tahrif etmiş ve ülkenin DNS hizmetine müdahale etmek suretiyle ülkede kaos ortamına zemin hazırlamıştır[54].

Aşağıdaki şekil Estonya Siber Savaşı'nda gerçekleşen önemli olayları kronolojik olarak özetlemektedir[55].



Şekil 3.3. Estonya siber savaşı zaman çizelgesi

Üç hafta süren siber saldırılar Estonya'nın ulusal ekonomi ve saygınlığına büyük zararlar vermiştir. Estonya Devleti karşılaştıkları bu siber felaket karşısında aşağıda belirtilen tedbirleri almıştır[56]:

- Siber saldırıların ulusal güvenliğe olan etkilerini azaltmak için Estonya Devleti'nin bilgi teknolojilerinden sorumlu makamları(Estonya Bilgisayar Olaylarına Müdahale Ekipleri, CERT-EE) tarafından müttefik devletlerle koordineli olarak uluslararası bağlantılar engellendi ve sunucular üzerinde trafik azaltıldı.
- Bant genişliği artırılması, birden çok sunucu ile isteklere cevap verilmesi, güvenlik yamalarının uygulanması, güvenlik duvarları ve saldırı tespit sistemlerinin etkin kullanılması gibi teknik önlemler süratle uygulamaya konuldu.
- Estonya Savunma Bakanlığı koordinesinde uluslararası müttefik ülkeler ve kuruluşlar bilgilendirilmiştir. Bu kapsamda, NATO ve Avrupa Birliği gözlemci olarak Estonya'da bulunmuş ve danışmanlık faaliyetlerini yürütmüştür. Ayrıca ABD, Almanya ve Finlandiya ulusal CERT makamları saldırı kaynaklarını bulma ve raporlama konusunda Estonya Devleti'ne yardımcı olmuştur.

- Halkın bilinçlenmesi sağlanmış ve uluslararası otoritelerle müşterek hareket ederek siber suçluları bulma ve onları adalete teslim etme konusunda hukuki düzenlemelere hız verilmiştir.
- Siber saldırılar, Estonya'nın Siber Güvenlik Stratejisini hazırlamışını hızlandırmıştır. Bu kapsamda, Milli Savunma Bakanlığı tarafından koordine edilen ve bünyesinde Eğitim Bakanlığı, Adalet Bakanlığı, Ekonomik İşler ve Haberleşme Bakanlığı, Araştırma Bakanlığı'nın bulunduğu Siber Güvenlik Strateji Komitesi kuruldu ve 2008-2013 dönemlerini kapsayacak siber güvenlik strateji planı hazırlanmasına başlandı.

Estonya'ya karşı yapılan siber saldırılar, NATO'nun siber güvenliğe bakışının şekillenmesinde önemli rol oynadı. NATO'nun 1999 Sırp bilgisayar korsanlarının saldırısı sonrasında artarak büyüyen siber güvenlik ilgisi Estonya'nın uğradığı saldırılar sonrasında gözle görünür hale geldi. NATO, Estonya'nın uğradığı siber saldırılar sonrasında kendi birimindeki en iyi siber-terörizm uzmanlarını araştırma yapmak ve ülkenin elektronik savunma sistemlerini güçlendirici çalışmalar yapmak üzere Tallinn'e sevk etti[57]. NATO'nun Estonya'nın yanında olduğunu göstermesi siber saldırıların önemli bir kısmını üzerine çekmesine neden oldu.

Estonya siber savaşı, NATO'nun siber güvenlik çalışmalarında müttefik devletlerle müşterek hareket etme girişimlerinin başlaması açısından önemlidir. 2008 yılının Nisan ayında Bükreş'te gerçekleştirilen NATO Zirvesinde NATO Siber Savunma Birleşik Politikası kabul edilmiş ve ittifak çapında siber savunma operasyonel yeteneklerini merkezileştirmek için Brüksel merkezli Siber Savunma Yönetim Başkanlığı (CDMA) kuruldu. Aynı yılın Mayıs ayında yoğun siber saldırılara maruz kalan Talinn/Estonya'da NATO Siber Savunma Mükemmeliyet Merkezi (CCDCOE) kuruldu[58].

3.3.3. Gürcistan Siber Savaşı - 2008

Estonya'ya yönelik siber saldırıların üzerinden henüz bir yıl geçmişti ki Ağustos 2008'de Güney Osetya yüzünden Rusya Federasyonu ile Gürcistan arasında çıkan çatışma siber güvenlik konusunu yeniden gündemin üst sıralarına taşıdı. Daha önce Osetler ile Gürcistan

hükümeti arasındaki çatışmalar nedeniyle 1992’de Güney Osetya’da Rusya, Gürcistan ve Güney Osetya birliklerinden oluşan bir barış gücü oluşturulmuştu[59]. Gürcistan ve Rusya arasındaki gerginlik hızla arttı ve 7 Ağustos 2008’te Gürcistan kuvvetlerinin ayrılıkçı grubun provokasyonuna cevap vermesiyle hızla yükselen olaylar sıcak çatışmaya dönüştü. 8 Ağustos’ta Rus güçleri Gürcistan’a askeri operasyonla karşılık verdiler. Bu arada 7 Ağustos 2008 akşam saatlerinde Gürcistan’a karşı siber saldırılar başladı. Gürcistan enformasyon alt yapısının Estonya kadar gelişmiş olmaması saldırının verdiği zararın etkisini azalttı. Ama saldırı sırasında olayların gelişimi ve izlenen yöntemler neredeyse Estonya’dakinin aynısıydı[60].

Gürcistan coğrafi konumu açısından internet bağlantısını Türkiye, Ermenistan, Azerbaycan ve Rusya üzerinden sağlayabilmesine rağmen, internet altyapısının büyük bir kısmı Rusya üzerinden hizmet almaktadır. Ayrıca Azerbaycan üzerinden alınan internet hizmeti ikinci safhada tekrar Rusya üzerinden dünyaya açılmaktadır. Söz konusu koşullarda Gürcistan internet trafiğinin büyük bir Rusya üzerinden geçmesi, Rusya’nın siber saldırılarda elini güçlendirmiştir[61].

Rusya’nın Gürcistan’a karşı yürüttüğü siber operasyonlar 2 safha halinde gerçekleştirilmiştir. Birinci safhada Rus saldırganlar ilk olarak 7 Ağustos akşamı Gürcistan devlet sitelerini ve medya sektörünü hedef almıştır. Dönemin Rus askeri yetkililerinden olan Albay Anatoly Tsyganok, Gürcistan’a karşı yapılan ilk siber saldırıları, Gürcü hackerlar tarafından Güney Osetya’ya yapılan saldırılara misilleme olarak gerçekleştirdiklerini açıklamıştır. Rus hackerlar tarafından birinci safhada gerçekleştirilen siber saldırılar hizmet dışı bırakma saldırısı (DDoS) olarak gerçekleştirilmiştir. Bu safhada gerçekleştirilen siber saldırılar Rus suç örgütleri ile irtibatlı olan zombi bilgisayarlar kullanılarak yapılmıştır. Rusya kaynaklı siber saldırılar ikinci safhada aralarında finans kurumları, işletmeler, eğitim kurumları, batı merkezli medya kuruluşları (CNN, BBC) ve Gürcü siber korsanların internet siteleri gibi kurumları ve toplulukları hedef almıştır[54].

Gürcistan’a yönelik olarak düzenlenen siber saldırılardan çıkartılabilecek en önemli sonuç bunun gerçek bir hibrit savaş niteliği taşımasıdır. Geleneksel savaş yöntemlerini kullanan

Rusya, eş zamanlı olarak siber saldırıları da başlatmıştır. Rusya'nın uyguladığı bu savaş düzenini hibrit savaş olarak tanımlamak mümkündür. Olayın bu şekilde gerçekleşmesi, NATO'nun hibrit savaşa olan inancını kuvvetlendirmiştir[62].

Aşağıdaki şekil Gürcistan Siber Savaşı'nda gerçekleşen önemli olayları kronolojik olarak özetlemektedir[55].



Şekil 3.4. Gürcistan siber savaşı zaman çizelgesi

Yaklaşık üç hafta süren siber saldırılar Gürcistan'ın ulusal ekonomisine ve fiili işleyişine büyük darbe vurmuştur. Gürcistan'ın siber güvenlik altyapısının Estonya kadar gelişmiş olmaması siber saldırıların etkilerini artırmıştır. Gürcistan Devleti karşılaştıkları bu siber felaket karşısında aşağıda belirtilen tedbirleri almıştır[56]:

- Gürcistan'da bulunan akademik camia siber saldırılara tedbirler üretme konusunda faaliyetler yürütmüş ve ulusal CERT rolünü üstlenmiştir.
- Bilgi güvenliği sağlamak ve ulusal internet trafiğini düşürmek için Rus web sitelerine devlet eliyle erişimler engellenmiştir.
- Sunucuları ve ana bilgisayarları yurt dışına taşımak suretiyle hizmet kesintisinin sona erdirilmesi sağlanmıştır.
- Diğer ülkelerin ulusal CERT makamlarından yardım talep edilmiş ve siber saldırılara tedbirler üretmek için diğer devletlerin CERT makamları ile koordineli çalışılmıştır.

Saldırıların ardından Gürcistan ulusal sınırlar içerisinde yukarıda belirtilen tedbirleri alsa da, Rusya merkezli yürütülen siber saldırılar uluslararası sonuçlar doğurmuştur. Gürcistan siber saldırıları kapsamında, 2008 yılının Kasım ayında NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCOE) tarafından “Gürcistan’a Karşı Gerçekleştirilen Siber Saldırıları: Belirlenen Yasal Dersler ” isimli bir bildiri yayınlanmıştır. Bu bildiride, Rus-Gürcistan Savaşı sırasında meydana gelen siber saldırılara karşı Silahlı Çatışma Hukuku’nun (Law of Armed Conflict-LOAC) uygulanabilirliği üzerinde görüşler yer almaktadır[63].

Siber saldırıları gerçekleştirilen siteler incelendiğinde bunların ABD’den çalınan kredi kartlarıyla Rusya ve Türkiye’de açılan siteler olduğu belirlenmiştir. Gürcistan’ın Rusya ile yaşadığı gerginliğin ardında NATO’ya üyelik hedefi yatmaktadır. Fakat Gürcistan’ın ittifaka üyeliği henüz gerçekleşmediği için Gürcistan NATO’nun güvenlik şemsiyesinden faydalanamamıştır. Ancak NATO Rusya saldırısı sonrasında, Gürcistan saldırısını incelemek üzere Siber Savunma Yönetimi Otoritesi’nden (CDMB) uzman bir ekibi bölgeye gönderdi. Tüm bu girişimlere rağmen siber dünyada tehdit düzeyinin artması ve siber araçlarla saldırının çok küçük eğitimlerle gerçekleştirilebildiği gerçeği NATO üyelerini korkutmaktadır. Üye ülkeler, Nisan 2009’da Strazburg/Kehl’de yapılan zirvede yeni siber savunma tavırlarının geliştirilmesini istediler. Siber savunmanın NATO tatbikatlarının parçası haline getirilmesine ve NATO ile üye ülkeler arasındaki bağın siber tehditlere karşı güçlendirilmesine karar verildi.

3.4. NATO Siber Güvenlik Stratejisi

1999 yılında Kosova Savaşı sırasında NATO ve NATO üyesi ülkelere yapılan siber saldırılar sonrasında NATO “siber savunma” konusunu gündem maddelerine almaya başladı. NATO merkezli yapılan ilk siber saldırıların ardından 2002 yılında icra edilen Prag Zirvesi ile NATO Siber Savunma Programı kabul edildi. Bu program kapsamında, aynı yıl siber olayları tespit etmek ve siber saldırıları önlemek amacıyla NATO Bilgisayar Olaylarına Müdahale Birimi (NCIRC) kuruldu[64].

2007 yılında Estonya'nın kamu ve özel kurumlarına yapılan siber saldırılar ve 2008 yılında Rusya-Gürcistan arasında yaşanan çatışmalar konvansiyonel harbin önemli bir bileşeni olarak siber saldırıların ortaya çıkmasını sağladı. Yıkıcı siber araçların geliştirilmesi ve kullanılması, ülkelerin ulusal ve uluslararası güvenliğini tehdit etmesi NATO ve üye ülkelerin daha güçlü ve istikrarlı bilgi iletişim teknoloji altyapısına olan ihtiyacı gün yüzüne çıkardı.

Estonya Siber Savaşı sonrasında 3 Nisan 2008 tarihinde Romanya'nın başkenti Bükreş'te gerçekleştirilen NATO zirvesinde NATO'nun siber savunma faaliyetleri ve kritik altyapıların korunması konusunda gündem maddeleri görüşülmüştür. NATO'nun siber güvenlik uygulamalarına yön veren Bükreş Zirvesi Bildirisi'nin 47'nci maddesi şöyledir:

“NATO, siber saldırılara dayanıklılığını artırmak için ittifak bilgi sistemlerini güçlendirme kararlılığını sürdürecektir. Son zamanlarda NATO siber savunma politikası kabul edildi ve ilgili birimler tarafından geliştirilmeye devam edecektir. Siber savunma politikamız NATO ve müttefik devletlerin siber savunma ihtiyaçlarını karşılamak ve kritik bilgi sistemlerini korumak üzerine yoğunlaşmaktadır. Bu amaç doğrultusunda; faydalı uygulamaların paylaşılması ve siber saldırıya maruz kalan devletin talep etmesi durumunda siber savunma desteği sağlanmalıdır. Biz NATO olarak, siber savunma yeteneklerimizin güçlendirilmesi için müttefik devletler ve ulusal otoriteler ile ilişkilerin geliştirilmesi konusunda istekliyiz.”[65]

Bükreş Zirve'si sonrasında siber güvenlik alanında iki önemli gelişme yaşandı. İlk olarak, Brüksel'de bir NATO Siber Savunma Yönetimi Otoritesi'nin (Cyber Defense Management Authority-CDMA) kurulmasına karar verildi. İkinci olarak, siber savunma kapasitesini bir merkezde toplayarak harekât kabiliyetini arttırmak maksadıyla Tallinn/Estonya merkezli müşterek bir organizasyon kurulmasına karar verildi. Bu kapsamda, 14 Mayıs 2008 yılında Estonya, Almanya, İtalya, Letonya, Litvanya, Slovakya ve İspanya'nın katılımıyla Tallinn/Estonya merkezli NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCOE) kuruldu[66]. NATO ittifakına siber güvenlik konularında destek sağlayan merkezin başlıca görevleri şunlardır[67]:

- Siberle ilgili konularda NATO ittifakı için doktrinler ve kavramlar üretmek.
- NATO'ya üye ülkeler için eğitim kursları, atölye çalışmaları düzenlemek ve tatbikatlar icra etmek.

- Araştırmalar yapmak ve gelişmeler üzerine toplantılar düzenlemek.
- Geçmişteki ve hâlihazırdaki saldırıları inceleyerek dersler çıkarmak.
- Devam eden saldırılarda eğer istenirse tavsiyeler vermek.

Hali hazırda 18 NATO Ülkesinin iştirak ettiği merkeze, Türkiye 3 Kasım 2015 tarihinde Finlandiya ve Yunanistan ile birlikte katılmıştır. NATO CCDCOE belirtilen görevleri yerine getirmek için aşağıdaki şekilde gösterildiği gibi yapılandırılmıştır[66].



Şekil 3.5. NATO CCDCOE yönetim yapısı

Estonya ve Gürcistan siber saldırıları sonrasında NATO ülkeleri tarafından NATO Siber Savunma Politikası onaylandı ve 2010 yılında gerçekleştirilen Lizbon Zirvesi ile siber savunma konusu NATO'nun savunma planlama sürecine dâhil edildi[68].

2010 NATO Strateji Konsepti; siber saldırıları tespit, önleme ve siber saldırılara karşı savunma yeteneğinin geliştirilmesine olan ihtiyacın altını çizdi. NATO siber savunma politikasının temelini oluşturan ve revize edilen NATO Siber Savunma Konsepti 2011 yılının Mart ayında NATO Savunma Bakanlarına sunulmak için hazırlandı. Söz konusu konsept süreç içerisinde genişletilmiş NATO Savunma Bakanları tarafından onaylanmıştır. Onaylanan doküman, NATO'nun kendi yapılanması ve Müttefik kuvvetlerin yapılanması için özel görevleri tanımlayan bir eylem planı da içermektedir[69]. Bu süreç içerisinde NATO'nun siber güvenlik politikasını formüle ederken dört temel zorluk ile karşılaşmıştır[70]:

- Standart tanımlarından farklı olarak; saldırı, savaş ve kuvvet kullanımı ifadelerinin siber uzayda kullanılmasının formüle edilmesi.
- Krizleri zamanında çözmek için oluşturulan stratejik çerçeve ile yönetimlerin desteklenmesi. Bu konu, siber savaş konusunda ulusal ve uluslararası düzeyde sorumlulukların belirlenmesi ve ortaya çıkan yeni çatışma ortamına göre yasaların tekrar düzenlenmesini içermektedir.
- Siber uzay konusunda gerçekleştirilecek düzenlemelerin kolaylaştırılması için davranış normlarının formüle edilmesi. Bu konu, ulusal stratejilerin arasında artan uyumu içeren çok taraflı bir yaklaşım gerektirir.
- Kolektif güvenlik ve bireysel özgürlüklerin korunması arasındaki dengenin sağlanması.

NATO tarafından yürütülen her türlü müşterek siber savunma harekâtı Kuzey Atlantik Konseyi'nin (NAC) kararlarına tabidir. Bu kapsamda NATO siber savunma harekâtı konusunda tepe nokta Kuzey Atlantik Konseyi'dir. NATO Siber Savunma Konseptine göre NATO siber savunma yönetim hiyerarşisi aşağıdaki gibi tanımlanmıştır[71].

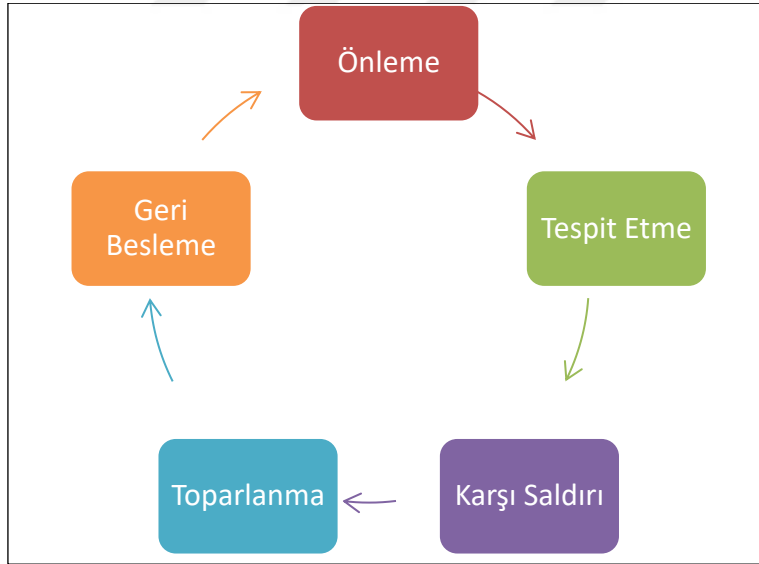


Şekil 3.6. NATO siber savunma yönetim yapılanması

NATO Siber Savunma Konseptine göre NATO Siber Savunma Politikasının odak noktası; NATO ağlarının korunmasının sağlanması ile birlikte toplu savunma ve kriz yönetimi kapsamında ulusal ağların temel görevlerini yürütebilmesi için siber savunma ihtiyaçlarının karşılanmasıdır[71].

NATO, bünyesinde barındırdığı imkânlar ile siber savunma faaliyetlerini aşağıda belirtilen prensipler ışığında gerçekleştirmektedir[72]:

- NATO siber savunma politikasının uygulanması: 2011 yılında kabul edilen NATO Siber Savunma Konsepti ve Eylem Planı süreç içerisinde hızla değişen tehditlere ayak uydurma konusunda yetersiz kalmaya başlamıştır. Daha sağlam bir siber savunma ortamı sağlamak için 2014 yılının Eylül ayında icra edilen Galler Zirvesinde müttefik devletlerin katılımıyla siber savunma konsepti geliştirilmiş ve 2014 Eylem Planı uygulamaya konulmuştur[73].
- NATO siber savunma yeteneğinin geliştirilmesi: Merkezi olarak yapılandırılmış NATO Bilgisayar Olaylarına Müdahale Yeteneği (NCIRC) NATO bünyesinde bulunan ağlara 24 saat esasına göre ve aşağıdaki şekilde görülen metodolojiyi kullanarak destek vermektedir(Şekil 3.7). NCIRC tarafından alınan tedbirlerin hızla gelişen tehdit ortamına ayak uydurması ve gelişimine devam etmesi beklenmektedir.



Şekil 3.7. NCIRC metodolojisi [74]

- NATO siber savunma kapasitesinin artırılması: Siber savunma konusunda teknolojik yeterliliğin yanında insanın yetiştirilmesi ve bilinçlendirilmesi de önem arz

etmektedir. Bu bilgi ışığında NATO, siber savunma şemsiyesini güçlendirmek için eğitim ve tatbikatlar planlar ve icra eder.

- Ortaklar ile işbirliği yapılması: Siber uzayda belirlenen dijital sınırlar ulusal sınırlarla örtüşmemektedir. Müttefik devletlerin dijital sınırlarının korunması ve NATO'nun uluslararası siber güvenliğinin sağlanması, ortak yaklaşımların belirlenmesi, bilgilerin paylaşılması ve müşterek çalışmaya bağlıdır.
- Sanayi ile işbirliği yapılması: Özel sektör siber güvenlik için önemli bir rol üstlenmektedir. NATO ve Müttefik ülkelerin siber savunma yeteneklerinin geliştirilmesi, özel sektörün sahip olduğu teknolojik yeniliklerin ve sivil hayatta kendisini geliştirmiş insan gücünün NATO sistemlerine dâhil edilmesine bağlıdır.

NATO'nun Talinn'de bulunan Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCOE) tarafından 2012 yılında yayınlanan "National Cyber Security Framework Manual" dokümanı NATO bünyesinde bulunan müttefik devletlerin uygulaması gereken siber savunma yöntemlerini 10 adımda tanımlamaktadır[75]:

1. Siber saldırılardan etkilenen devletin kritik altyapılarını korumaya yardımcı olmak için sivil veya askeri yapıyı kullanmak
2. Siber saldırılardan etkilenen devletin kriz yönetim görevlerini yerine getirmesine yardımcı olmak için sivil veya askeri yapıyı kullanmak
3. İncelemelerde yardımcı olmak için adli müfettişlerin görevlendirilmesi
4. Uzman ekipler görevlendirerek siber saldırılara maruz kalan devlet ile NATO ve özel sektör arasında eşgüdümlü çalışmaya yardımcı olmak
5. İnternet Servis Sağlayıcılara (ISP) verilen talimatlar aracılığıyla saldırıya uğrayan devletin saldırı trafiğini engellemek
6. İnternet Servis Sağlayıcılara (ISP) verilen talimatlar aracılığıyla saldırıya uğrayan devletin saldırıları destekleyen ve arkasında olduğundan şüphelenilen devletlerin erişimini engellemek
7. Saldırıların arkasında olduğu tespit edilen komuta-kontrol altyapısını bozmaya yönelik aktif savunma tedbirlerini uygulamak

8. Savunmaya yönelik harekât tarzlarını artırmaya yardımcı olmak için ilave İnternet Değişim Noktaları (IXP) oluşturmak ve yerel internet altyapısını güçlendirmeye yönelik tedbirler üretmek
9. Bilgisayar ve ağ cihazları üreticileri ile yapılacak koordineler sonrasında bölgeye yapacakları sevkiyatlara öncelik verilmesinin temin edilmesi
10. Müttefik ülkeler, saldırıya uğraya devleti rahatlamak ve saldırı yapan unsurları durdurmak maksadıyla bünyesinde bulundurdıkları siber saldırı kuvvetlerini saldırganlar üzerine karşı saldırı yapmak suretiyle kullanabilir. Müttefik devlet bu karşı saldırıyı kendi namına değil bizzat İttifak (NATO) adına gerçekleştirir.

NATO siber savunma politikasının gelişmesi ve gerçekleştirilen siber saldırılara karşı uygulanması ile birlikte uluslararası yasalar ve silahlı çatışma yasalarına ilişkin sorunlar NATO toplantılarının gündeminde yer almaya başladı. NATO CCDCOE koordinatörlüğünde ve Uluslararası Bağımsız Uzmanlar Grubu'nun katılımıyla siber harekâtın karmaşık hukuk problemlerine konularına açıklık getirmek maksadıyla, "Siber Savaşta Uygulanacak Hukuk Hakkında Tallinn El Kitabı" adıyla hazırlanan doküman, 2013 yılının Mart ayında Cambridge Üniversitesi tarafından yayımlanmıştır. Bu doküman iki temel soruya cevap aramaktadır:

1. Savaşa girmenin haklı nedenleri nelerdir?
2. Savaş sırasında uyulması gereken kurallar nelerdir?

Tallinn El Kitabı; "Uluslararası Siber Güvenlik Hukuku" ve "Siber Silahlı Çatışma Hukuku" başlıklı iki ana bölümden ve 95 adet kuraldan oluşmaktadır. Birinci bölümde, "Devletler ve Siber Uzay" (Egemenlik, Yargılama Yetkisi, Kontrol ve Devlet sorumluluğu) alt konuları ele alınırken, ikinci bölümde ise, "Genel Siber Silahlı Çatışma Hukuku", "Düşmanca Davranışlar", "Belirli Kişiler, Nesneler ve Faaliyetler", "İşgal" ve "Tarafsızlık" alt konularına açıklık getirilmiştir[24].



4. ULUSAL SİBER GÜVENLİK STRATEJİSİ

Son yıllarda gerçekleşen teknolojik gelişmeler ile coğrafi kısıtlamalar ortadan kalkmış ve elektronik hizmetler hayatımızın merkezine yerleşmiştir. İş dünyası, toplum yaşantısı, kamu hizmetleri, ulusların milli güvenlik altyapıları bilgi teknolojilerinin ve kritik altyapıların işleyişine bağlıdır. Siber tehditlerin yaygınlaştığı günümüzde, kritik altyapılar üzerinde akan bilgilerin bütünlüğü ve gizliliği ayrıca önem arz etmektedir. Toplumun bilgi teknolojilerine gittikçe daha fazla bağımlı hale gelmesi, bu kritik altyapıların korunmasını ve kullanılabilirliğini ulusal çıkar haline getirmektedir. Böylece siber güvenlik, toplumun her seviyesini etkileyen yatay ve stratejik bir ulusal mesele olarak kabul edilmektedir.

Ulusal Siber Güvenlik Stratejisi gelişen teknoloji, değişen koşullar ve gereksinimler göz önünde bulundurularak, kamu ve özel sektörden gelecek talepler doğrultusunda, ulusal düzeyde sağlanmalı ve eşgüdüm ile güncellenmelidir.

Uluslararası çapta ülkelerin strateji dokümanları incelendiğinde, olası siber güvenlik risklerine ve riskleri ortadan kaldıracak eylemler uygulanırken göz önünde bulundurulacak ilkelere yer verildiği, risklerin ve ilkelerin ülkeden ülkeye çok fazla değişiklik arz etmediği gözlemlenmiştir. Bu kapsamda, ulusal siber güvenliğin sağlanmasına yönelik olarak yürütülecek çalışmalarda esas alınması gereken temel ilkeler şunlardır[76]:

- 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.

4.1. Ulusal Siber Güvenlik Stratejisinin Hazırlanması ve Uygulanması

İlk olarak ABD tarafından 2003 yılında yayımlanan ulusal siber güvenlik planının ardından tüm dünya ülkeleri ulusal güvenliğini artırmak ve bu bağlamda siber güvenlik vizyonunu belirlemek maksadıyla ulusal siber güvenlik strateji dokümanları hazırlamaya başlamışlardır. Ulusal siber güvenlik stratejileri, ulus devletlerin stratejik ilkelerini, yönergelerini, hedeflerini belirleyen ve siber güvenlikle ilgili riskleri azaltmak için özel tedbirler içeren ana belgeleridir.

Siber saldırılara karşı ulusal çıkarların korunması ve siber uzayın sınır güvenliğinin sağlanması hususunda karşılaşılan zorluklar, devletleri siber güvenlik konusunda aynı çatı altında toplanmasına neden olmuştur. Ulusal Siber Güvenlik Stratejisinin belirlenmesi ve uygulanması her devletin kendi sorumluluğundadır. Ancak, bazı uluslararası organizasyonlar Ulusal Siber Güvenlik Stratejisinin hazırlanması ve uygulanması konusunda devletlere rehberlik yapmak ve bu konuda standart oluşturmak maksadıyla belli bir model önermektedir.

4.1.1. Uluslararası Telekomünikasyon Birliği (ITU) Modeli

Uluslararası Telekomünikasyon Birliği (ITU), bilgi ve iletişim teknolojileri alanında Birleşmiş Milletler Örgütü'nün uzman kuruluşudur. 1865 yılında kurulan ve 1947 yılında Birleşmiş Milletler bünyesine katılan kuruluşun temel görevleri şunlardır[77]:

1. Küresel radyo spektrumlarını ve uydu yörüngelerini tahsis etmek,
2. Teknolojiyi kesintisiz bir şekilde birbirine bağlayan ağların teknik standartlarını belirlemek ve geliştirmek,

3. Tüm dünyada yetersiz hizmet alan toplulukların bilgi ve iletişim teknolojilerine erişimini artırmak.

EK-2’de sunulan akış şeması, ITU tarafından önerilen ulusal siber güvenlik strateji sürecini tasvir etmektedir. Ulusların yönetim yapıları, yetenekleri ve ihtiyaçları değiştikçe strateji süreçleri de değişebilmektedir. Bu açıdan, bir ulusun ulusal siber güvenlik çerçevesini nasıl kurabileceğini, uygulayabileceğini, işletebileceğini ve izleyebileceğini gösteren söz konusu akış şeması sadece örnek niteliğindedir. Akış şeması ile belirtilen safların açıklamaları aşağıdaki madde başlıkları ile açıklanmaktadır[78].

Safha 0: Kasten ya da bilmeyerek yapılan büyük veri sızıntıları ve ya ulusal güvenliği ilgilendiren politikalar siber güvenlik strateji faaliyetinin başlamasına yol açabilir. Bu tür durumlarda ulusal kalkınma planları ve ulusal güvenlik stratejileri, siber güvenlik strateji sürecini teşvik etmektedir. Politikalar siber alanı, ulusal ekonomik ve güvenlik hedeflerine ulaşmada hayati önem taşıyan bir alan olarak sınıflandırmaktadır. Bu nedenle, ulusal politikalar, ülkenin siber alanda karşılaştığı tehditlere karşı harekete geçmesini ve vatandaşlarına güven ortamı sunmasını gerektirebilir. Ulusal siber güvenlik stratejisi ile ilgili eylemin nedeni ne olursa olsun, stratejinin geliştiricileri tarafından tüm paydaşlarla koordine edilmiş bir yaklaşımı tercih etmesi önerilir.

Safha 1: İcracı makam, siber güvenlik stratejisinin geliştirilmesine liderlik etmekten sorumludur. Hükümet, birlikte çalışmanın karşılıklı yararlarını vurgulayarak diğer paydaşların desteğini kazanabilir. Her devlet en etkili yaklaşımı seçme hakkına sahip olsa da, Hükümetlerin gündem belirlenmesi ve çalışılması esnasında tüm paydaşlarla birlikte hareket edilmesi önerilir. Anlaşmaya varılan strateji, ulusal ve küresel işbirliği için bir aşamaya gelmektedir.

Safha 2: Bu aşamada Ulusal Siber Güvenlik Stratejisi yayınlanmaktadır. Ulusal siber güvenlik için görevlendirilen organizasyon, ana paydaşların rol ve sorumluluklarını belirlemelidir.

Safha 3: Ulusal Siber Güvenlik Stratejisi uygulayacağı siber güvenlik eylemleri için vizyonunu belirlemektedir. Strateji belgesi, Küresel Siber Güvenlik Gündemi (GCA) konuları üzerine odaklanmaz. Devletler belli kuruluşlara sektörel ve kurumsal siber güvenlik konularında koordinasyon görevi tahsis edebilir.

Safha 4: Bu aşamada, Devlet yetkilileri tarafından koordinasyon makamı olarak görevlendirilen kuruluşlar, sektörel eylem planlarını uygulamaya koymak için diğer paydaşlar ve kritik altyapı operatörleri ile birlikte çalıştığı görülür.

Safha 5: Yetkili siber güvenlik organizasyonu ulusal stratejisinin etkinliğini izlemekle sorumludur. Yetkili organizasyon, siber güvenlik stratejisinin etkinliğini denetlemek için bağımsız değerlendirmeler yapar.

EK-2’de bulunan akış şeması ile tanımlanan süreçlerin tamamı Ulusal Siber Güvenlik Otoritesi tarafından yürütülmeli ve koordine edilmelidir. Ulusal Siber Güvenlik Otoritesi, ulusal siber güvenlik politikasının yönetiminin ve bölgesel ve uluslararası işbirliğinin tek elden koordine edilmesini sağlamalıdır. Ulusal Siber Güvenlik Otoritesi müdahalelerden uzak, bağımsız bir konumda bulunmalıdır. ITU tarafından kurulması önerilen Ulusal Siber Güvenlik Otoritesinin görevleri şunlardır[79]:

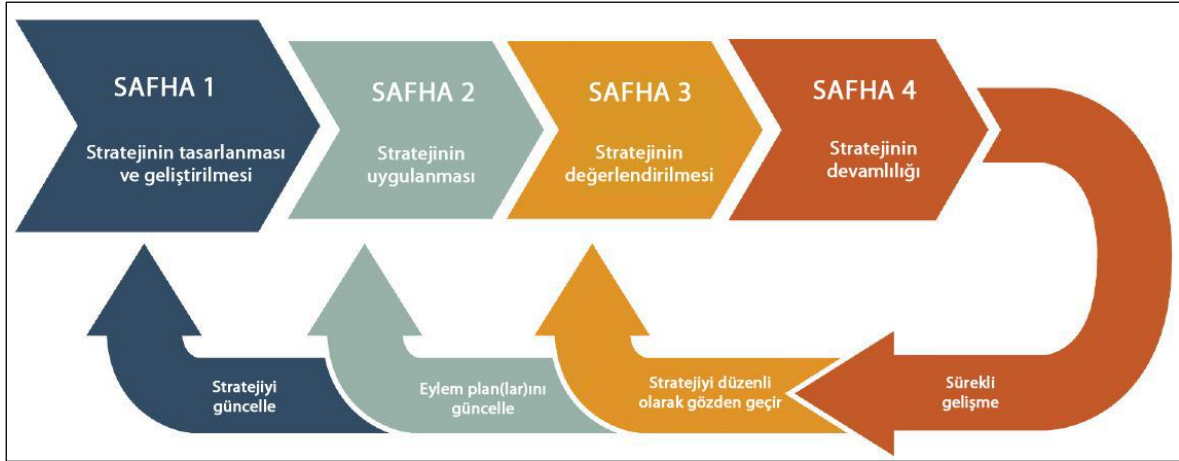
- Ulusal siber güvenlik politikasının tanımlanması,
- Ulusal siber güvenlik girişimleri için önceliklerin belirlenmesi,
- Siber güvenlik faaliyetlerinin ulusal seviyede koordine edilmesi,
- Siber güvenlik sorunlarını ele almak üzere paydaşların ve kamu-özel sektör ilişkilerinin belirlenmesi,
- Bölgesel ve uluslararası taraf, kurum ve kuruluşlarla işbirliği yapılması,
- Siber güvenlik ile ilgili uluslararası standartların uygulanması,
- Bilgi ve iletişim altyapılarının, hizmetlerinin veya işletmecilerinin sertifikasyonu,
- Sayısal kimlik sistemlerinin işletilmesi, geliştirilmesi ve yönetilmesi.

Ulusal Siber Güvenlik Otoritesi tarafından stratejik seviyede yürütülen faaliyetler operatif seviyede Bilgisayar Olaylarına Müdahale Ekipleri (CERT, CSIRT, BOME) tarafından icra edilmelidir. Bilgisayar Olaylarına Müdahale Ekipleri, bilgisayar ve şebeke güvenliğini izleyen ve siber saldırı mağdurlarına olaylara müdahale hizmeti sunan teknik birimlerdir. ITU Dünya Telekomünikasyon Standartları Teşkilatı Meclisi (WTSA) 2008 yılında yayınlanan karar ile ulusal çerçevede BOME teşkilatlarının kurulmasını önermektedir. BOME teşkilatları, açıklıklara ve tehditlere ilişkin uyarılar ve bilgisayar ve şebeke güvenliğini geliştirmeye yönelik bilgiler yayımlar. Ayrıca, farkındalık oluşturma, güvenlik danışmanlığı gibi kalite hizmetleri ve teknolojiyi izleme, güvenlik araçları geliştirme gibi proaktif hizmetlerin yanı sıra, siber saldırılara karşı koyma ve bunların yol açtığı zararın azaltılması gibi reaktif hizmetler de sunarlar. EK-3 ile ITU tarafından önerilen ulusal siber güvenlik strateji modeli sunulmuştur[78].

4.1.2. Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA) Modeli

2005 yılında Yunanistan'da kurulan Avrupa Birliği ve Bilgi Güvenliği Ajansı (ENISA), siber güvenlik konusunda Avrupa Birliğinin uzman kuruluşudur. ENISA'nın temel görevi; vatandaşların, tüketicilerin, işletmelerin ve kamu kurumlarının çıkarlarını gözeterek Avrupa'daki bilgi toplumunu güvence altına almaktır[80].

ENISA, ulusal siber güvenlik stratejilerinin süreçler yoluyla uygulanmasının kontrol edilmesi ve sürekli olarak iyileştirme süreçlerinin takip edilmesi için Ulusal Siber Güvenlik Stratejisi (NCSS) yaşam döngüsünü önermektedir.



Şekil 4.1. Ulusal siber güvenlik stratejisi yaşam döngüsü[81]

Safha 1: Stratejinin Tasarlanması ve Geliştirilmesi

Stratejinin tasarlanması ve geliştirilmesi safhası Ulusal Siber Güvenlik Otoritesi sorumluluğunda yürütülmelidir. Aşağıdaki madde başlıklarında belirtilen her bir alt bölüm Ulusal Siber Güvenlik Strateji taslağı hazırlanırken göz önüne alınması gereken özel adımları ifade etmektedir. Stratejinin tasarlanması ve geliştirilmesi safhasında ENISA tarafından önerilen hususlar değerlendirilerek uygulanacak yol haritasını gösteren tablo EK-4 ile sunulmuştur[81].

Safha 2: Stratejinin Uygulanması

Bu safha, Ulusal Siber Güvenlik Strateji sürecinin yürütülmesine ve uygulanmasına iştirak eden unsurlara rehberlik etmeyi amaçlamaktadır. Stratejinin uygulanmasında başvurulacak temel adımlar EK-5'te gösterilmiştir[81].

Safha 3: Stratejinin Değerlendirilmesi

Bu safha, stratejiyi değerlendirmek ve ayarlamak için gereken açık gereksinimleri kapsamaktadır. Değerlendirme safhası, hedeflere ulaşıp ulaşılmadığının ve planlanan faaliyetlerin yerine getirilip getirilmediğinin belirlenmesi için gereklidir. Mevcut durumuna dair bilgiler edinmenin yanı sıra, değerlendirmenin birincil amacı, bir sonraki stratejinin

hedeflerini belirlemektir. Strateji sürecinin değerlendirilmesi ve raporlanmasında ENISA tarafından önerilen işlem maddeleri Ek-6 ile sunulmuştur[81].

4.2. Türkiye’de Ulusal Siber Güvenlik

2003 yılında Cenevre’de toplanan Dünya Bilgi Toplumu Zirvesi’nin (WSIS) yaptığı çalışmalar Türkiye tarafından yakından takip edilmiştir. Bu çerçevede, elektronik ortamdaki bilgilerin gizlilik ve bütünlüğünün garanti altına alarak kullanılması ve yapılan işlemlerin hukuki geçerliliğinin sağlanması için 2004 yılında “Elektronik İmza Kanunu”, sayıları ve çeşitleri artan bilişim suçlarına yönelik cezaları da içeren “Türk Ceza Kanunu” çıkarılmıştır. Hukuk alanında yapılan bu çalışmalar ile ulusal alanda siber güvenlik konusunda çalışmalara başlanmıştır.

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. Şekil 4.4’de Türkiye’nin 2004-2014 yılları arasını kapsayan ulusal alandaki siber güvenlik gelişim süreci gösterilmektedir.



Şekil 4.2. Türkiye'de siber güvenliğin gelişimi[82]

Siber güvenlik alanında yapılan organizasyonel ve operasyonel çalışmaların hukuken birincil mevzuatla desteklenmesi gerektiği değerlendirmelerinden hareketle 6.02.2014 tarihli ve 6518 sayılı kanunun 106ncı maddesiyle 5809 sayılı kanuna eklenen aşağıdaki madde ile “Siber Güvenlik Kurulu” kurulmuş ve görevleri belirtilmiştir. Aynı kanunun 102.nci maddesiyle 5809 sayılı Kanunun UDHB’nin görevlerini belirleyen 5inci maddesine UDHB’nin görevleri arasına siber güvenlik kurulu sekretaryasını yapmanın yanı sıra ciddi görevler eklenmiştir. İlgili kanun kapsamında Siber Güvenlik Kuruluna yüklenen görevler şöyledir[83]:

- Siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak,
- Kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak,
- Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek,
- Kanunlarla verilen diğer görevleri yapmak.

Ulaştırma, Denizcilik ve Haberleşme Bakanı'nın başkanlığında toplanan Siber Güvenlik Kurulu aşağıda belirtilen kurumlardan ve üst düzey yöneticilerden oluşmaktadır[83]:

- Dışişleri Bakanlığı Müsteşarı,
- İçişleri Bakanlığı Müsteşarı,
- Milli Savunma Bakanlığı Müsteşarı,
- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Müsteşarı,
- 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

Ulusal siber güvenliğin sağlanmasında en önemli unsurlardan biri Siber Olaylara Müdahale Ekipleri (SOME) ve bu ekiplerin ulusal bazda koordineli çalışmasıdır. Bu noktadan hareketle UDHB, "SOME'lerin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğini" 11.11.2013 tarihli Resmi Gazete'de yayınlamıştır. Bu tebliğ ile sektörel ve kurumsal SOME'lerin yapısı ve USOM ile ilişkileri tanımlanmıştır. Tanımlanan görevler ışığında, siber güvenlik aktörlerinin ilişkileri Şekil 4.5'de gösterilmiştir[84].



Şekil 4.3. Türkiye'de siber güvenlik aktörleri[82]

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

Bütün kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler, Siber Güvenlik Kurulu tarafından belirlenen politika, strateji ve eylem planları çerçevesinde kendilerine verilen görevleri yerine getirmek ve belirlenen usul, esas ve standartlara uymakla yükümlüdür.

Bu kapsamda hazırlanan, 2013-2014 döneminde gerçekleştirilmesi planlanan işlere ilave olarak bu yılları aşan periyodik faaliyetler ile eğitim ve bilinçlendirme çalışmaları gibi sürekli yürütülmesi gereken faaliyetlere de yer veren Ulusal Siber Güvenlik Stratejisi ve 2013-2014

Eylem Planı 20/06/2013 tarih, 28683 sayılı Resmi Gazete’de yayınlanarak yürürlüğe girmiştir. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının amacı[85]:

- 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.

Yukarıda belirtilen amaçlar doğrultusunda ve belirlenen ilkeler ışığında, ulusal siber güvenliğin sağlanmasına yönelik stratejik eylemlerin gerçekleştirilmesi planlanmıştır. 2013-2014 döneminde gerçekleştirilmesi planlanan ve 7 ana başlıkta toplanan stratejik eylemler şöyledir[85]:

1. Yasal Düzenlemelerin Yapılması
2. Adli Süreçlere Yardımcı Olacak Çalışmaların Yürütülmesi
3. Ulusal Siber Olaylara Müdahale Organizasyonunun oluşturulması
4. Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi
5. Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi ve Bilinçlendirilme Faaliyetleri
6. Siber Güvenlikte Yerli teknolojilerin Geliştirilmesi
7. Ulusal Güvenlik Mekanizmalarının Kapsamının Genişletilmesi

Her eylem için sorumlu ve ilgili kurum ve kuruluşlar belirtilmiştir. Bu durumda, ilgili tüm kurum ve kuruluşların, sorumlu kurum ve kuruluşların koordinatörlüğünde hareket ederek eylemin gerektirdiği çalışmaları yürütmeleri öngörülmektedir. Eylem planında yer alan

eylemlerin bir kısmı için bitirilme tarihi belirlenmiş, periyodik olarak tekrarlanması ve sürekli olarak yürütülmesi öngörülen eylemler ise ayrıca belirtilmiştir. 2013-2014 döneminde, gerçekleştirilmesi planlanan toplam 29 adet eylem maddesi bulunmaktadır. Eylem planında yer alan 29 adet eylemin, stratejik eylem başlıklarına dağılımı Ek-7’de özetlenmiştir. Ayrıca 29 adet eylem toplamda 86 adet alt eylemden oluşmaktadır[85].

2013-2014 Siber Güvenlik Eylem Planı’nda belirlenen toplamda 86 alt eylemin sorumlu kurumlara göre dağılımını gösteren tablo EK-8 ile sunulmuştur[85].

4.2.2. 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı

Gelişen bilgi ve iletişim teknolojileri, artan güvenlik gereksinimi ve edinilen tecrübeler doğrultusunda, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından ulusal siber güvenlik stratejisinin güncellenmesi ve 2016-2019 dönemini kapsayan eylemlerin belirlenmesi ihtiyacı doğmuştur. Bu kapsamda öncelikle eski eylem planında sorumlu veya ilgili olarak yer alan kurumlarla 10 Mart-7 Nisan 2015 tarihlerinde yedi adet değerlendirme toplantısı yapılmıştır. Toplantılarda eski eylem planında yer alan faaliyetlerin gerçekleşme dereceleri ve karşılaşılan güçlükler ek olarak ileriye dönük değerlendirmeler ve siber güvenlik kapsamında gerçekleştirilmesi gereken faaliyetler de detaylı olarak belirlenmiş ve kaydedilmiştir. Toplantıların ardından kamu kurumları, kritik altyapı işletmecileri, bilişim sektörü, üniversiteler ve sivil toplum kurumlarını temsilen 73 kurum ve kuruluştan toplam 126 uzmanın katılımı ile Ortak Akıl Platformu gerçekleştirilmiştir. İki gün süren platform çalışmaları kapsamında; Türkiye’nin siber güvenlik boyutunda güçlü ve zayıf yönlerinden hareketle stratejik amaçları ve gerçekleştirmesi gereken eylemler belirlenmiştir[86].

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı hazırlanırken paydaşlarla birlikte gerçekleştirilen çalışmalara ilave olarak geri planda kaynak taraması da yapılmıştır. Bu kapsamda, Amerika, Avrupa ve Uzak Doğu’dan çok sayıda ülkenin siber güvenlik stratejileri gözden geçirilmiş, ülkelerin siber güvenlik alanında kapsam, hedefler, öncelikler, organizasyon yapısı, kaynak tahsisi, Ar-Ge (Araştırma ve Geliştirme) koordinasyonu, kamu-özel sektör işbirliği, eğitim gibi başlıklarda üretmeye çalıştığı çözümler değerlendirilmiştir.

Tüm bu çalışmalar kapsamında üretilen bilginin toplanması, incelenmesi ve değerlendirilmesi sonucunda “2016-2019 Ulusal Siber Güvenlik Stratejisi” ve “2016-2019 Ulusal Siber Güvenlik Eylem Planı” hazırlanmıştır.

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planının ana amacı; siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olduğu anlayışının tüm kesimlerde yerleşmesi, ulusal siber uzayda bulunan sistem ve paydaşların tamamının güvenliğini sağlamak üzere idari ve teknolojik önlemlerin alınmasını sağlayacak yetkinliğin eksiksiz bir şekilde kazanılmasıdır. Belirlenen ana amaç doğrultusunda:

- Ulusal siber uzayın tamamını kapsamak şartıyla, bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve bilgi/veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin, gizliliğinin ve mahremiyetinin sağlanmasına,
- Siber güvenlik olaylarının etkilerinin en düşük düzeyde kalmasına, olayların ardından sistemlerin en kısa sürede normal çalışmalarına dönmeye yönelik stratejik siber güvenlik eylemlerinin belirlenmesine ve oluşan suçun adli makam ve kolluk kuvvetlerince daha etkin araştırılmasının ve soruşturulmasının sağlanmasına,
- Siber güvenliğin, gizliliğin ve mahremiyetin sağlanmasında kritik teknolojilerin ve ürünlerin ülkemizde üretilmesine, üretilmiyorsa, dışarıdan alınan teknoloji ve ürünlerin salt bu maksatla ve güvenle kullanılabilmesini sağlayacak önlemlerin alınmasına yönelik bileşenler bu planda yer almaktadır[86].

Yukarıda belirtilen stratejik amaçlara ulaşmak için gerçekleştirilecek eylemler aşağıda belirtilen beş stratejik eylem başlığı altında toplanmaktadır.

1. Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması
2. Siber Suçlarla Mücadele
3. Farkındalık ve İnsan Kaynağı Geliştirme
4. Siber Güvenlik Ekosisteminin Geliştirilmesi
5. Siber Güvenliğin Milli Güvenliğe Entegrasyonu

Her eylem için sorumlu ve ilgili kurum ve kuruluşlar belirtilmiştir. Bu durumda, ilgili tüm kurum ve kuruluşların, sorumlu kurum ve kuruluşların koordinatörlüğünde hareket ederek eylemin gerektirdiği çalışmaları yürütmeleri öngörülmektedir.

Eylem planında yer alan eylemlerin bir kısmı için bitirilme tarihi belirlenmiş, periyodik olarak tekrarlanması ve sürekli olarak yürütülmesi öngörülen eylemler ise ayrıca belirtilmiştir. Bu Eylem Planı döneminde, gerçekleştirilmesi planlanan toplam 41 adet eylem maddesi bulunmakta olup, stratejik eylem başlıklarına dağılımı Ek-9'da özetlenmiştir[87].

2016-2019 Siber Güvenlik Eylem Planı'nda belirlenen toplamda 41 eylemin sorumlu kurumlara göre dağılımını gösteren tablo EK-10 ile sunulmuştur[87].

5. YÖNTEM

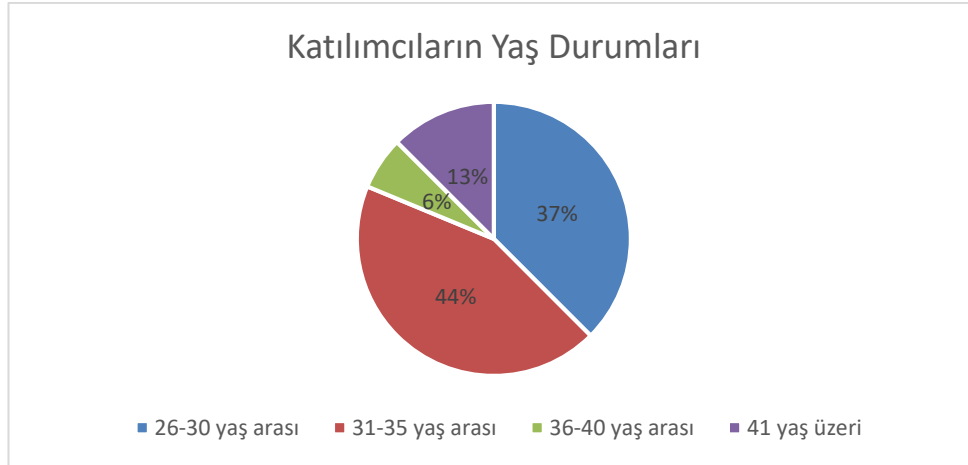
Yöntem bölümünde yapılan çalışmanın modeli, evreni ve araştırmada kullanılan veri toplama araçları hakkında bilgiler yer almaktadır.

5.1. Araştırma Modeli

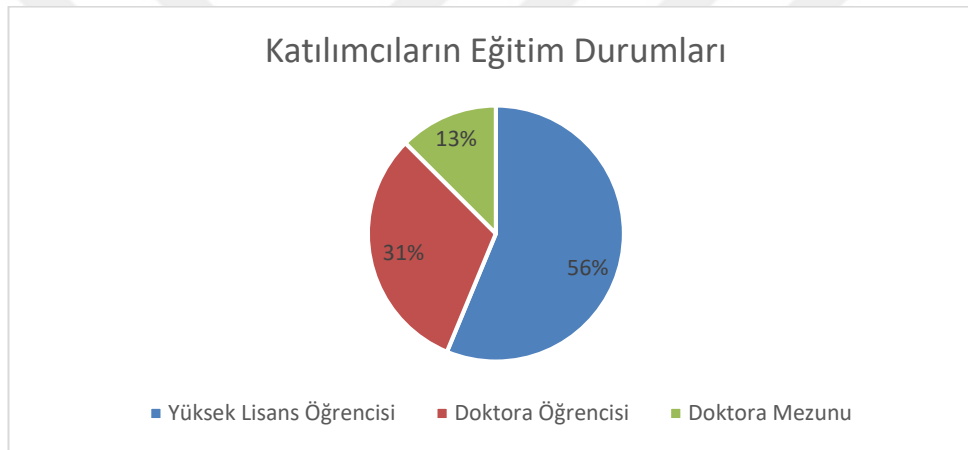
Bu çalışmada teorik düzeyde literatür taraması yapılmış olup, belirlenen sorunun cevabı aranmıştır. Bu kapsamda, araştırma yöntemi olarak doküman incelemesi yöntemi benimsenmiştir. Bu kapsamda özellikle; NATO CCDCOE, ENISA, BSA, ITU organizasyonlarının yayımladıkları dokümanlar detaylı bir şekilde incelenmiştir. Ayrıca, Ulusal-Uluslararası tezler, makaleler, dergiler ve kitaplar taranmış ve tez kapsamında belirtilen alt amaçlar doğrultusunda soruların cevabı aranmıştır.

Tez kapsamında belirlenen alt amaçların tespit edilmesi aşamasında aşağıda belirtilen yöntemler kullanılmıştır:

- ENISA Raporlarında ülke temsilcilerinin tespitleri göz önünde bulundurulmuştur.
- CCDCOE Raporlarında ülke temsilcilerinin tespitleri göz önünde bulundurulmuştur.
- Siber güvenlik konusunda uzman olan 16 kişiden oluşan heyete sunum yapılmış ve görüşleri alınmıştır. Katılımcıların yaşlarının dağılımı Şekil 5.1’de, eğitim durumlarının dağılımı ise Şekil 5.2’de gösterilmiştir.



Şekil 5.1. Katılımcıların yaş durumları



Şekil 5.2. Katılımcıların eğitim durumları

Araştırma, aşağıdaki tabloda gösterilen 3 farklı aşamada gerçekleştirilmiştir. Birinci ve ikinci aşamada belirlenen alt amaçlar ile ülkeler dar kapsamda değerlendirilirken, üçüncü aşamada belirlenen alt amaçlar ile ülkeler geniş kapsamda ve daha detaylı değerlendirilmiştir.

Çizelge 5.1. Alt amaçlar

Aşama 1	1. Ulusal Siber Güvenlik Stratejisi ve Koordinatör Makamı Açısından İncelenmesi
Aşama 2	2. Bilgisayar Olaylarına Müdahale Ekipleri (CERT) Açısından İncelenmesi 3. Uluslararası İşbirliği Açısından İncelenmesi
Aşama 3	4. Ulusal Siber Güvenlik Eylem Maddeleri Açısından İncelenmesi 5. Uluslararası Gelişme Endeksleri Açısından İncelenmesi 6. İnternet Kullanıcı Sayıları Açısından İncelenmesi 7. Kişisel ve Ulusal Bant Genişlikleri Açısında İncelenmesi 8. Hukuki Düzenlemeler ve Yönetmelikler Açısından İncelenmesi 8.1. Kişisel Verilerin Gizliliği Kapsamındaki Düzenlemeler Açısından İncelenmesi 8.2. Kişisel ve Kurumsal Güvenliğin Geliştirilmesini Sağlayan Düzenlemeler Açısından İncelenmesi 8.3. Siber Suçlar Kapsamındaki Düzenlemeler Açısından İncelenmesi 8.4. Fikri Mülkiyet Haklarının Korunması Kapsamındaki Düzenlemeler Açısından İncelenmesi 8.5. Fikri Mülkiyet Hakları Kapsamında İSS'lerinin Sorumlulukları Belirleyen Düzenlemeler Açısından İncelenmesi 8.6. Ulusal ve Uluslararası standartları belirleyen Düzenlemeler Açısından İncelenmesi 8.7. E-Ticaret Kapsamındaki Düzenlemeler Açısından İncelenmesi

Birinci aşamada; belirlenen bir tane alt amaç doğrultusunda 28 NATO üyesi ülkenin tamamı incelenecektir.

İkinci aşamada; günümüz itibariyle onaylı Ulusal Siber Güvenlik Stratejisi bulunmayan 8 NATO üyesi ülke ve onaylanmış Ulusal Siber Güvenlik Stratejisi bulunan ancak bu kapsamda icra ettikleri faaliyetleri, planları kısıtlı olan Lüksemburg araştırma dışında bırakılacaktır. Bu safhada; belirlenen iki adet alt amaç doğrultusunda onaylanmış Ulusal Siber Güvenlik Stratejisi bulunan 19 adet ülke incelenecektir.

Üçüncü aşamada; belirlenen 10 adet alt amaç doğrultusunda NATO ortaklığında en büyük paya sahip olan 9 ülke incelenecektir.

Araştırma Bulguları bölümünde, araştırma verilerinin toplanarak oluşturulan tablolara aktarılması esnasında anlaşılabilirliği artırmak amacıyla aşağıdaki şekiller kullanılmıştır.

Çizelge 5.2. Semboller

✓	Olumlu, Var, Evet
✗	Olumsuz, Yok, Hayır
🌙	Kısmen var, sınırlı
🔒	Erişim yetkisi sınırlı
🔒✗	Erişim yetkisi yok
🔒✓	Erişim yetkisi var
?	Belirsizlik var

Ayrıca, ülke kısaltmalarında uluslararası standartlara uyulması açısından uluslararası plaka kodları kullanılmıştır (BE=Belçika, SK=Slovakya gibi).

5.2. Evren ve Örneklem

Araştırmanın evrenini NATO üyesi olan 28 ülke oluşturmaktadır.

5.3. Verilerin Toplanması

Araştırmada, uluslararası organizasyonlar tarafından yayımlanan aşağıdaki dokümanlar detaylı bir şekilde incelenmiştir.

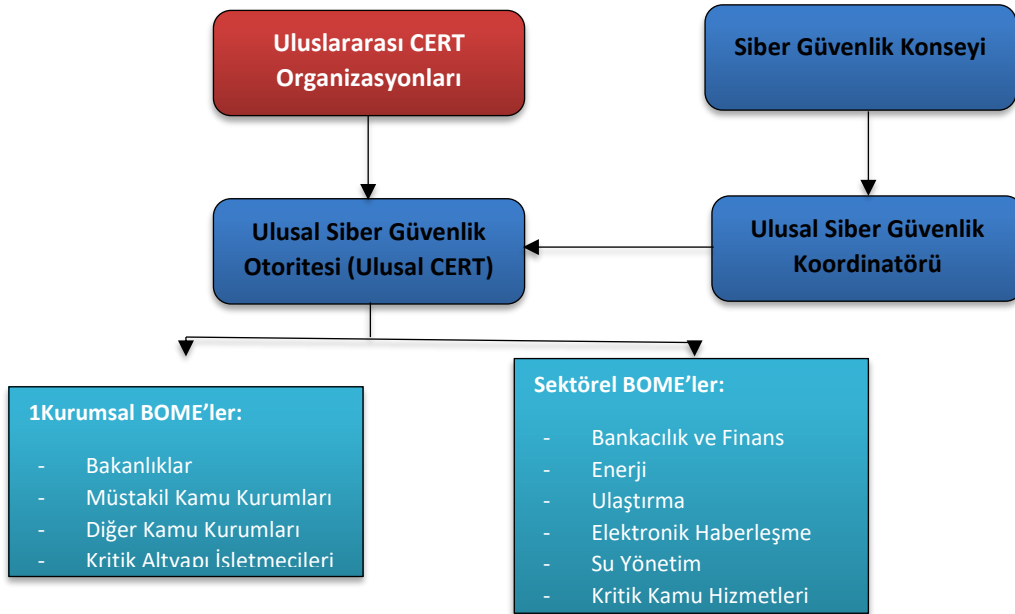
- CCDCOE tarafından 2008 yılından itibaren yayımlanan dokümanlar ve toplantı tutanakları,
- CCDCOE üyesi ülkelerin yayımladıkları Ulusal Siber Güvenlik Organizasyonu (National Cyber Security Organisation) dokümanları,
- ENISA tarafından 2004 yılından itibaren yayımlanan Ulusal Siber Güvenlik Stratejisi kılavuzu ve dokümanları
- ENISA tarafından yayımlanan Ülke Raporları (Country Report),
- BSA tarafından yayımlanan Ülke Raporları (Country Report),

6. ARAŞTIRMA BULGULARI

Bu çalışma ile; mevcut bulunan akademik çalışmalardan farklı olarak NATO çatısı altında bulunan ulusların uyguladıkları siber güvenlik stratejileri mukayeseli olarak incelenecektir. Bu çalışmanın, 28 farklı devletin siber güvenlik altyapılarını, siber güvenlik stratejilerini, siber güvenlik faaliyetlerini ortaya koymak suretiyle, ulusal çapta icra edilecek siber güvenlik çalışmalarına yeni bir bakış açısı sunması ve bu konuda farkındalık yaratması açısından önemli bir katkı sağlayacağı düşünülmektedir.

6.1. Ulusal Siber Güvenlik Stratejisi ve Koordinatör Makamı Açısından İncelenmesi

Çeşitli ülkelerin siber güvenlik yapılanmaları incelendiğinde, siber güvenliği sağlamak amacıyla bazılarının yeni kurumlar oluşturduğu, bazılarının ise mevcut kurumların görev alanını genişlettiği görülmektedir. Oluşturulan veya görev alanı genişletilen kurumlar daimî komiteler, çalışma grupları, danışma kurulları, disiplinler arası merkezler gibi çok çeşitli yapılara sahiptirler. Ülkelerin uyguladıkları yöntemlerde farklılıklar olsa da temel olarak ulusal siber güvenlik faaliyetleri Şekil 6.3'te gösterildiği gibi icra edilmektedir.



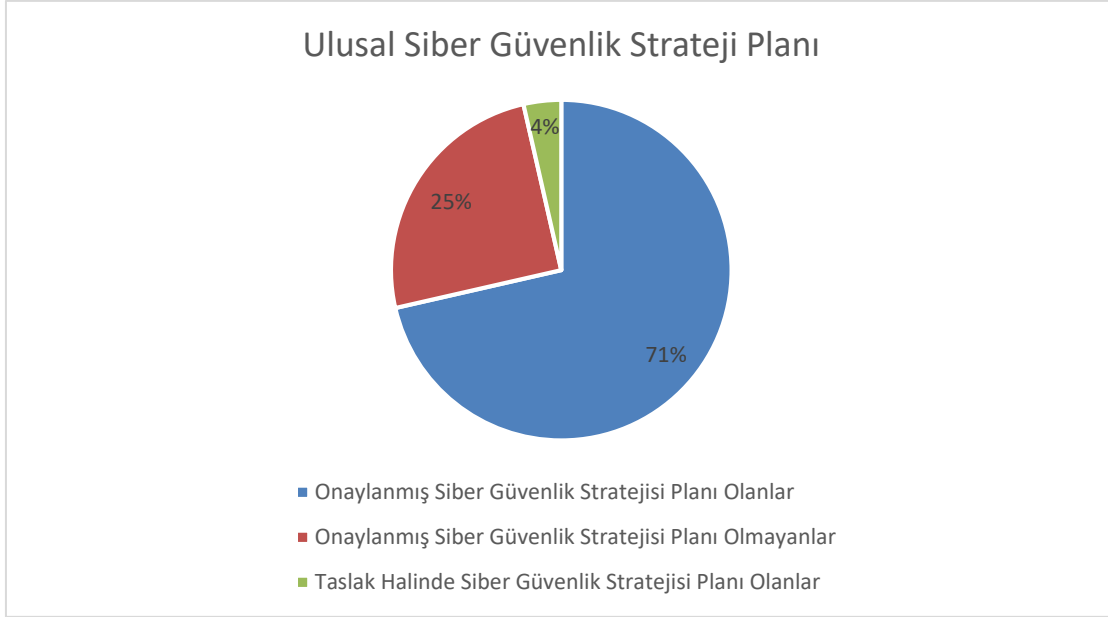
Şekil 6.1. Ulusal siber güvenlik yapılanması

Siber güvenlikle ilgili olarak kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler tarafından alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla ülkelerde “Siber Güvenlik Konseyleri” oluşturulmaktadır. Ülkemizde 1 Başkan ve 11 üyeden oluşan “Siber Güvenlik Kurulu” ulusal çapta bu görevi yürütmektedir.

Ulusal çapta oluşturulan Siber Güvenlik Konseyi, Ulusal Siber Güvenlik Koordinatörü başkanlığında toplanmaktadır. Ulusal Siber Güvenlik Koordinatörü; ulusal siber güvenlik çalışmalarının yürütülmesi, yönetilmesi ve koordinasyonu konularında Hükümetin Başkanı/Başbakanına karşı sorumludur. Ülkemizde bu görev; “Ulaştırma, Denizcilik ve Haberleşme Bakanlığı” tarafından yürütülmektedir. EK-11’de NATO üyesi 28 ülke ulusal siber güvenlik strateji planı ve koordinatör makamı açısından incelenmesi gösterilmektedir.

EK-11’de NATO üyesi olan 28 ülke; ulusal siber güvenlik stratejisinin mevcudiyeti ve bakanlık seviyesindeki koordinatör makamı açısından incelenmiştir. Tablodaki veriler ışığında aşağıdaki bulgulara rastlanmıştır:

- Onaylanmış Ulusal Siber Güvenlik Stratejisi bulunan ülke sayısı :20
- Onaylanmış Ulusal Siber Güvenlik Stratejisi bulunmayan ülke sayısı :7
- Ulusal Siber Güvenlik Strateji Planı taslak halinde olan ülke sayısı :1 (Portekiz)
- Ulusal Siber Güvenlik Strateji Planı ilk olarak Amerika Birleşik Devletleri tarafından 2003 yılında hazırlanmıştır.



Şekil 6.2. Ulusal siber güvenlik strateji planı

Şekil 6.4'te gösterildiği gibi, 28 ülke arasında yapılan incelemede ülkelerin %71'inin onaylanmış Ulusal Siber Güvenlik Strateji Planının olduğu tespit edilmiştir.

Onaylanmış Siber Güvenlik Stratejisi bulunan ancak planları ve faaliyetleri kısıtlı olan Lüksemburg sonraki safhalarda araştırmamızın dışında yer alacaktır.

Araştırmanın sonraki safhasına onaylanmış Ulusal Siber Güvenlik Strateji Belgesi bulunan 19 ülke ile devam edilecektir.

6.2. Bilgisayar Olaylarına Müdahale Ekipleri (CERT) Açısından İncelenmesi

“Siber Güvenlik Koordinatörü”, “Siber Güvenlik Konseyi” tarafından alınan kararları, bünyesinde oluşturulan “Ulusal Siber Güvenlik Otoritesi” aracılığıyla faaliyete geçirir. “Ulusal Siber Güvenlik Otoritesi”, ulusal siber güvenlik politikasının yönetiminin yapılmasını ve bölgesel, uluslararası işbirliğinin tek elden koordine edilmesini sağlamalıdır. Ülkemizdeki karşılığı USOM (Ulusal Siber Olaylara Müdahale Merkezi) olan siber güvenlik otoritesinin görevleri temel olarak şöyledir [76];

- Ulusal siber güvenlik politikasının tanımlanması,
- Ulusal siber güvenlik girişimleri için önceliklerin belirlenmesi,
- Siber güvenlik faaliyetlerinin ulusal seviyede koordine edilmesi,
- Siber güvenlik sorunlarını ele almak üzere paydaşların ve kamu-özel sektör ilişkilerinin belirlenmesi,
- Bölgesel ve uluslararası taraf, kurum ve kuruluşlarla işbirliği yapılması,
- Kamuya ait bilgi sistemin izlenmesi ve risk değerlendirmesi yapılması,
- Siber güvenlik ile ilgili uluslararası standartların uygulanması,
- Bilgi ve iletişim altyapılarının, hizmetlerinin veya işletmecilerinin sertifikasyonu,
- Sayısal kimlik sistemlerinin işletilmesi, geliştirilmesi ve yönetilmesi gibi hususlarda lider rolü üstlenilmesi.

Ulusal siber güvenliğin sağlanmasında en önemli unsurlar Bilgisayar Olaylarına Müdahale Ekipleridir (BOME, SOME). BOME, uluslararası ortamda CERT (Computer Emergency Response Team) veya CSIRT (Computer Security Incident Response Team) olarak ta ifade edilmektedir. Ulusal Siber Güvenlik Otoritesinin en önemli görevlerinden birisi, Bölgesel BOME'ler ile Uluslararası BOME'ler arasında koordinasyonu sağlamaktır. Şekil 6.3'te gösterildiği üzere Ulusal BOME'ler; Kurumsal ve Sektörel BOME'ler olmak üzere ikiye ayrılmaktadırlar.

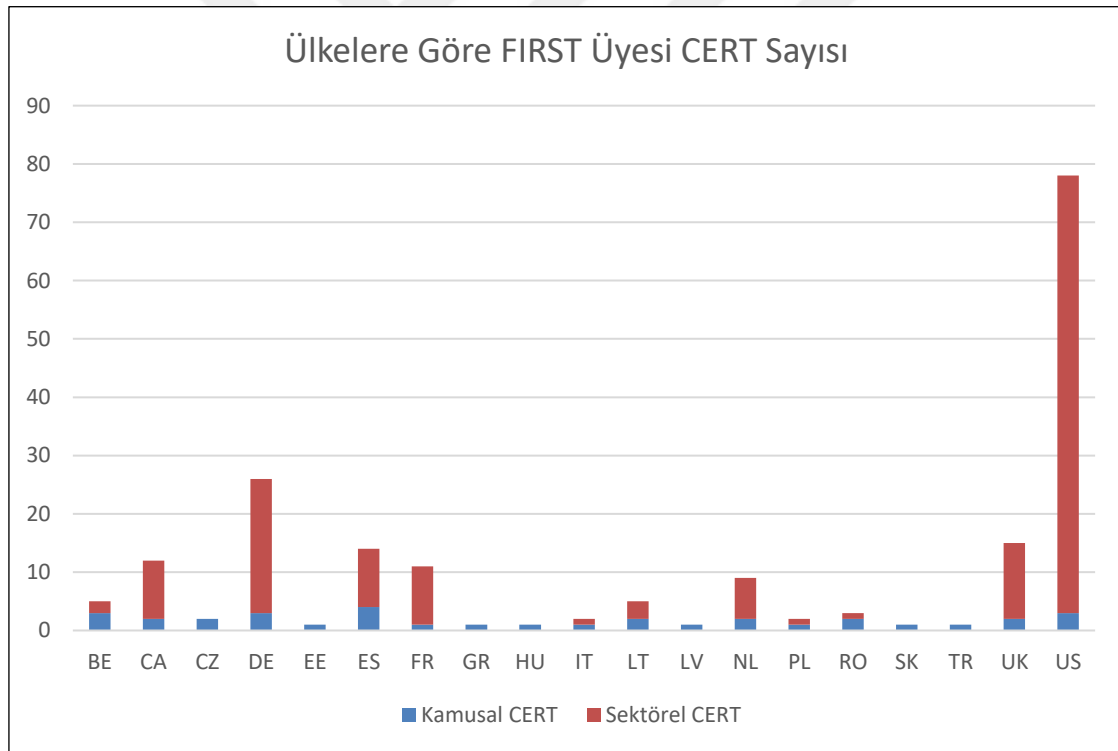
Uluslararası camiada siber saldırılara karşı ortak tepkilerin gerçekleştirilebilmesi maksadıyla bölgesel BOME'ler arasında koordinasyonu sağlayan organizasyonlar mevcuttur. FISRT (Forum of Incident Response and Security Teams), bilgisayar güvenlik olaylarını kooperatif olarak ele alan, olay önleme programlarını teşvik eden ve güvenilir bilgisayar olayları müdahale ekipleri arasında koordinasyonu sağlayan uluslararası bir konfederasyonudur. FIRST temel olarak [107];

- Teknik bilgi, araçlar, yöntemler ve süreçler geliştirir ve paylaşır,
- Kaliteli güvenlik ürünlerinin, politikalarının ve hizmetlerinin geliştirilmesini teşvik eder,
- Bilgisayar güvenlik uygulamaları geliştirir ve ilan eder,

- BOME ekiplerinin oluşturulmasını ve yaygınlaştırılmasını teşvik eder,
- Müşterek bilgi, beceri ve deneyimleri kullanarak güvenli ortamlar oluşturulmasına yardımcı olur.

Ek-12’de onaylanmış ulusal siber güvenlik strateji belgesi bulunan 19 NATO ülkesinin bilgisayar olaylarına müdahale ekipleri FIRST üyelikleri açısından incelenmesi gösterilmektedir.

Ek-12 ile sunulan tabloda yer alan veriler ışığında NATO Üyesi 19 ülkenin FIRST üyesi BOME sayıları Şekil 6.5’te gösterilmektedir (Ülkelerin farklı sayılarda BOME ekipleri mevcut olabilir ancak küresel bir organizasyon olarak FIRST üyelik sayılarını ifade etmektedir).



Şekil 6.3. Ülkelere göre FIRST üyesi CERT sayısı

Yaygın uygulama olarak ülkelerin, Siber Güvenlik Otorite Makamları (Ülkemiz için USOM-TR CERT) Ulusal BOME olarak FIRST üyesidir. FIRST üyesi ulusal BOME’ler uluslararası BOME’ler ile koordinasyon halinde hareket ederek yerel BOME’leri yönlendirir. Ancak A.B.D., Almanya, Birleşik Krallık ve Fransa gibi teknoloji açısından gelişmiş ülkelerde sektörel

BOME'ler etkin rol oynamaktadır. Özellikle Apple, Microsoft, Oracle, Siemens, AT&T gibi küresel çapta faaliyet gösteren kuruluşlar kendi bulundukları ülkelerde de gelişmiş birer sektörel BOME olarak görev yapmaktadır. Teknolojik açıdan gelişmiş ülkelerde FIRST üyesi sektörel BOME'lerin fazla olması bu tür büyük organizasyonların ülkelerinde faaliyet göstermesinden kaynaklanmaktadır.

6.3. Uluslararası İşbirliği Açısından İncelenmesi

Siber saldırılara karşı ulusal çıkarların korunması ve siber uzayın sınır güvenliğinin sağlanması hususunda karşılaşılan zorluklar, devletlerin uluslararası anlaşmalar yapmasını kaçınılmaz hale getirmiştir. NATO CCDCOE, ENISA ve ITU gibi uluslararası organizasyonlar aracılığıyla ülkeler siber saldırılara karşı dijital sınırlarını korumakta ve müşterek siber güvenlik stratejileri geliştirmektedir. Bu uluslararası organizasyonlar hakkında bilgi Çizelge 6.4'te ifade edilmektedir.

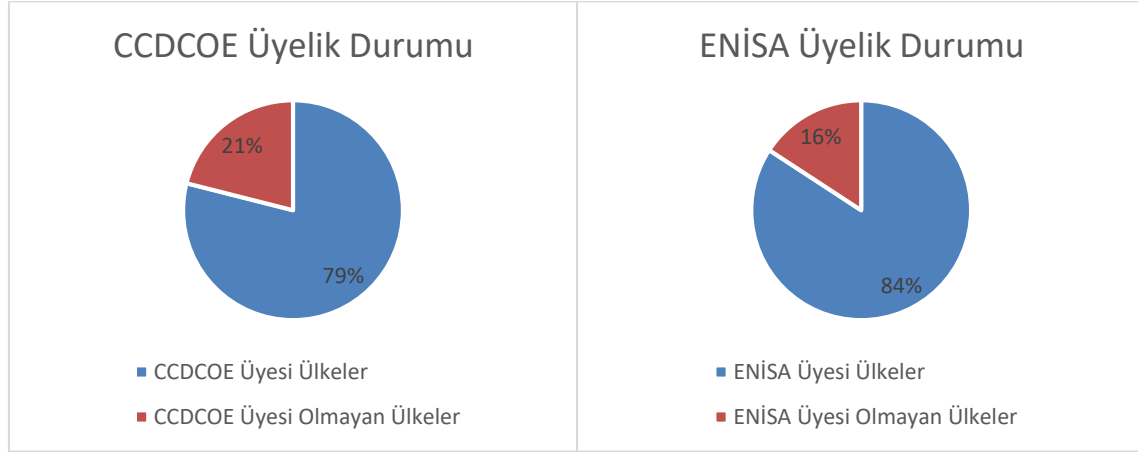
Çizelge 6.1. Uluslararası organizasyonlar

Uluslararası Organizasyonlar	Kuruluş Tarihi	Merkezi
NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCOE)	14 Mayıs 2008	Talinn/Estonya
Avrupa Birliği Ağ Ve Bilgi Güvenliği Ajansı (ENISA)	1 Eylül 2005	Crete/Yunanistan
Birleşmiş Milletler Uluslararası Telekomünikasyon Birliği (ITU)	17 Mayıs 1865	Geneva/İsviçre

Ek-13'te onaylanmış ulusal siber güvenlik strateji belgesi bulunan 19 NATO ülkesinin yukarıda belirtilen uluslararası organizasyonlara üyelikleri açısından incelenmesi gösterilmektedir.

14 Mayıs 2008 tarihinde Estonya, Almanya, İtalya, Litvanya, Letonya, Slovakya ve İspanya'nın bir araya gelmesi ile NATO bünyesinde bulunan Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCOE) kurulmuş ve günümüze gelinceye kadar birçok ülkeyi bünyesine katmıştır.

CCDCOE organizasyonuna üyelikler gönüllülük esasına göre gerçekleştirilirken, ENISA üyelikleri Avrupa Birliği ülkelerinin tamamını kapsamaktadır. NATO üyesi 19 ülkenin CCDCOE ve ENISA üyelikleri Şekil 6.6 ve Şekil 6.7’de oransal olarak gösterilmektedir.



Şekil 6.4.(a). CCDCOE üyelik durumu (b) ENISA üyelik durumu

NATO üyesi 19 ülke arasında yapılan ve Tablo 6.5’te gösterilen veriler ışığında aşağıdaki bulgulara rastlanmıştır:

- Ülkelerin %79’u CCDCOE üyesidir.
- Ülkelerin %84’ü ENISA üyesidir.
- Ülkelerin tamamı ITU üyesidir.
- Ülkelerin %68’i üç organizasyona da üyedir.

Araştırmanın sonraki safhasına NATO ortaklığında en büyük paya sahip olan 9 ülke (Kanada, Almanya, İspanya, Fransa, İtalya, Polonya, Türkiye, Birleşik Krallık ve A.B.D.) ile devam edilecektir. Bu kapsamda, genel konuları içeren ilk üç maddeden farklı olarak söz konusu 9 ülke daha detay gerektiren konularda incelenecektir.

6.4. Ulusal Siber Güvenlik Eylem Maddeleri Açısından İncelenmesi

Ulusal Siber Güvenlik Stratejisinin amacı; ulusal güvenlikle ilgili siber tehditler ve mevcut ulusal yeteneklere ilişkin değerlendirmelere dayanılarak ulusal çerçevede istenen düzeyde

siber güvenliğin oluşmasını olumsuz yönde etkileyen faktörlerin belirlenmesidir. Ülkeler, söz konusu olumsuzlukların üstesinden gelmek ve eksiklikleri gidermek için somut eylemler tanımlamaktadırlar.

Kapsamlı bir eylem planı; ulusal / uluslararası organizasyonlar ve paydaşların sorumlulukları kapsamındaki düzenlemeler de dâhil olmak üzere politik ve hukuki sorumlulukları belirleyen düzenlemeleri de kapsamalıdır.

Ek-14'te NATO üyesi 9 ülkenin güncel Siber Güvenlik Eylem Planına uygun ana eylem maddeleri belirtilmektedir. Her bir ana eylem maddesinin altında daha detaylı hazırlanmış alt eylem maddeleri bulunmaktadır ancak genel çerçeveyi belirlemek adına söz konusu alt eylem maddeleri bu bölümde yer almamıştır.

6.5. Uluslararası Gelişme Endeksleri Açısından İncelenmesi

Uluslararası camiada otorite olarak kabul edilen bazı organizasyonlar ülkelerin bilgi iletişim teknolojileri konularında hazır bulunurluk durumlarını ortaya koymakta ve belirledikleri kriterler çerçevesinde puanlama yapmaktadırlar. Çizelge 6.7'de NATO üyesi 9 ülkenin aşağıda ismi geçen 3 farklı endeks açısından incelenmesi yer almaktadır.

ITU ICT Gelişme Endeksi (IDI), dünya üzerinde 175 ülkenin Bilgi İletişim Teknolojilerinin gelişim düzeyleri konusunda karşılaştırma yaparak gözler önüne seren puanlama sistemidir.

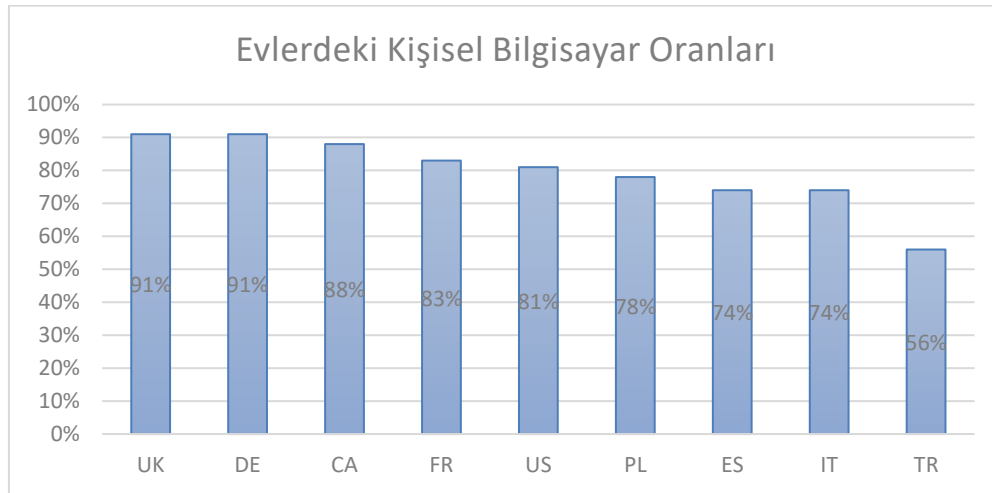
Dünya Ekonomik Forumu Ağ Hazırlık Endeksi (NRI), Dünya Ekonomik Forumu tarafından belirli periyotlarla yayınlanan Küresel Bilgi Teknolojisi Raporu ile ülkelerin ağ gelişim seviyelerini gösteren bir endekstir.

Uluslararası Bağlanabilirlik Endeksi (Connectivity Scorecard), küresel çapta 52 ülkeyi kapsayan ve ülkelerin bilgi iletişim teknolojisi altyapılarının seviyesini gösteren bir endekstir.

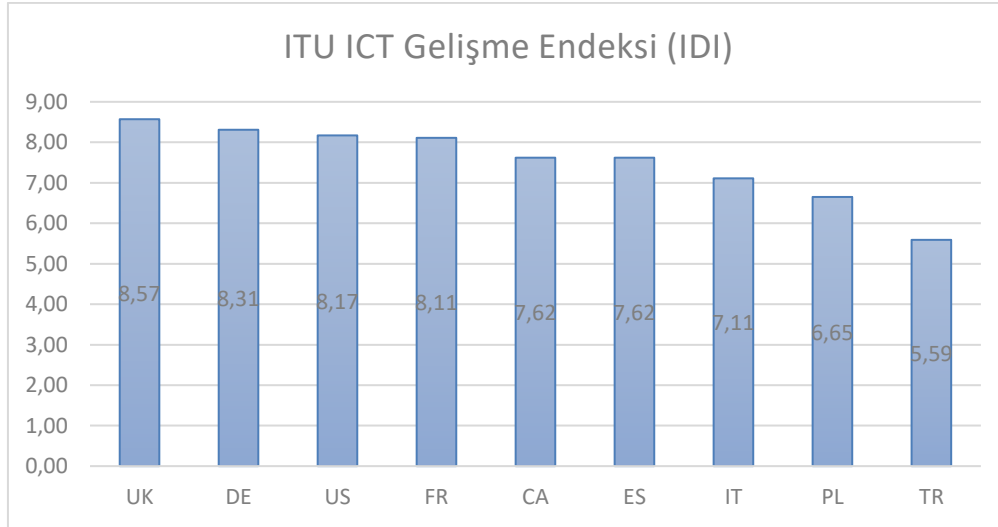
Çizelge 6.2. Uluslararası gelişme endeksleri açısından incelenmesi

ÜLKELER		Evlerdeki Kişisel Bilgisayar Oranı (2014) (183 ülke) [120]		ITU ICT Gelişme Endeksi (IDI) (2015) (175 ülke) (Puanlama 10 üzerinden) [121]		Dünya Ekonomik Forumu Ağ Hazırlık Endeksi (2016) (143 ülke) (Puanlama 7 üzerinden) [122]		Uluslararası Bağlanabilirlik Endeksi (2014) (52 ülke) (Puanlama 10 üzerinden) [123]	
		Oran	Sıra	Puan	Sıra	Puan	Sıra	Puan	Sıra
	CA	%88	Sıra: 17	7,62	Sıra: 25	5,6	Sıra: 14	5,27	Sıra: 19
	DE	%91	Sıra: 13	8,31	Sıra: 12	5,6	Sıra: 15	5,42	Sıra: 14
	ES	%74	Sıra: 44	7,62	Sıra: 26	4,8	Sıra: 35	4,33	Sıra: 28
	FR	%83	Sıra: 26	8,11	Sıra: 16	5,3	Sıra: 24	5,04	Sıra: 21
	IT	%74	Sıra: 45	7,11	Sıra: 37	4,4	Sıra: 45	3,76	Sıra: 34
	PL	%78	Sıra: 41	6,65	Sıra: 50	4,5	Sıra: 42	3,28	Sıra: 41
	TR	%56	Sıra: 73	5,59	Sıra: 70	4,4	Sıra: 48	4,13	Sıra: 31
	UK	%91	Sıra: 12	8,57	Sıra: 5	5,7	Sıra: 8	5,90	Sıra: 7
	US	%81	Sıra: 31	8,17	Sıra: 15	5,8	Sıra: 5	6,46	Sıra: 3

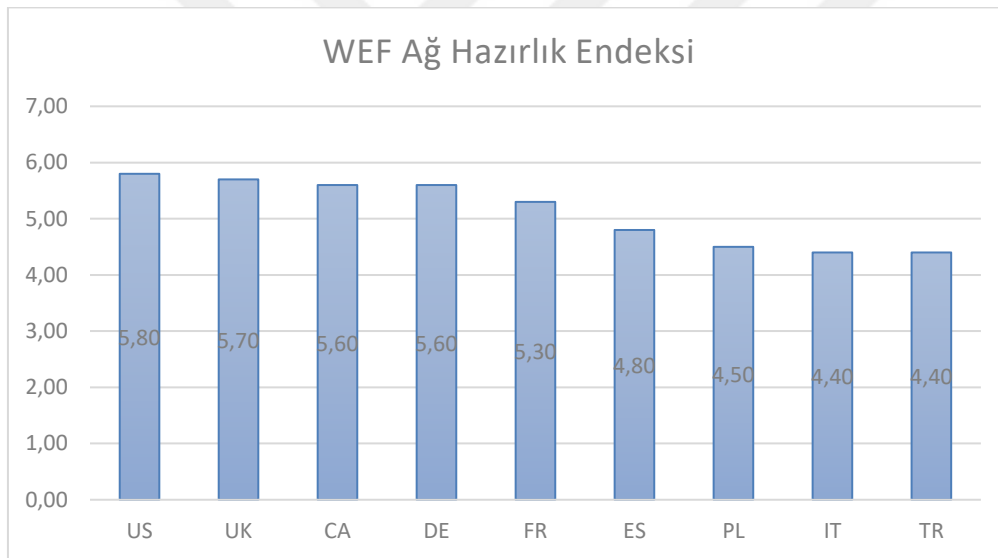
Yukarıdaki tabloda dört başlık altında toplanan verilerin grafiksel gösterimi Şekil 6.8, Şekil 6.9, Şekil 6.10 ve Şekil 6.11’de mevcuttur.



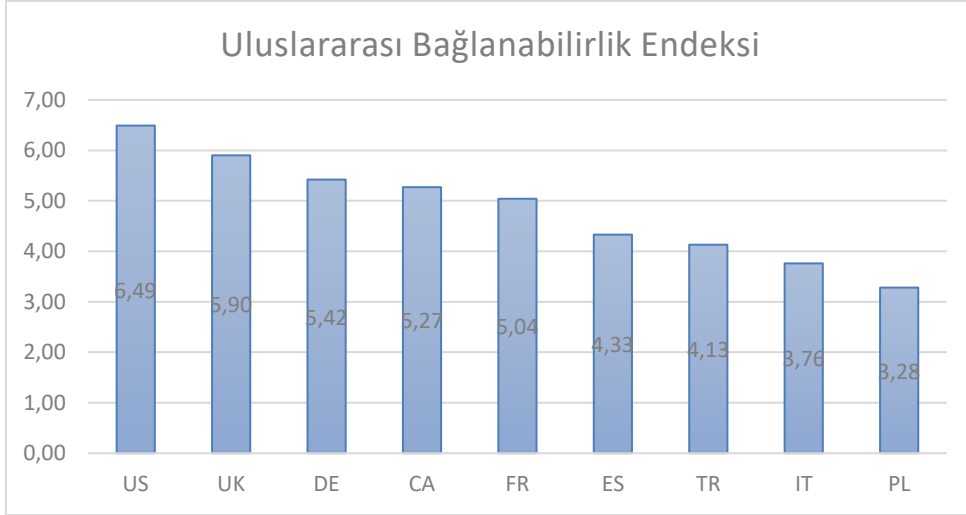
Şekil 6.5. Evlerdeki kişisel bilgisayar oranları



Şekil 6.6. ITU ICT gelişme Endeksi (IDI)



Şekil 6.7. WEF ağ hazırlık endeksi



Şekil 6.8. Uluslararası bağlanabilirlik endeksi

6.6. İnternet Kullanıcı Sayıları Açısından İncelenmesi

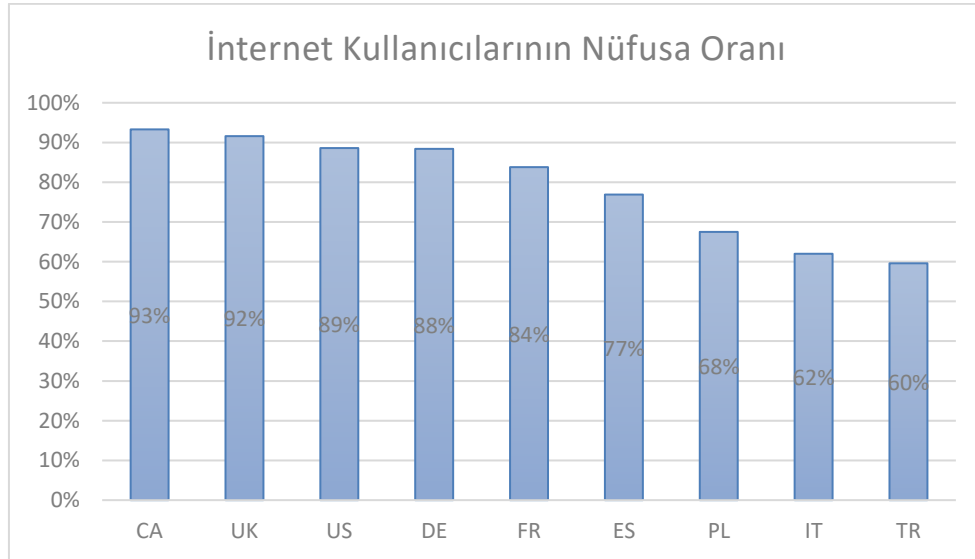
Uluslararası Telekomünikasyon Birliği'ne (ITU) göre, günümüzde dünya nüfusunun yaklaşık %49'unun internet erişimi bulunmaktadır. Diğer bir ifadeyle, dünya üzerinde bulunan 7,5 milyar insandan yaklaşık 3,7 milyarı çevrimiçi hizmetlerden faydalanmaktadır. Gelişmiş bazı ülkelerde bu oran %90'ların üzerine çıkmaktadır.

İnternet kullanıcılarının artmasıyla sabit geniş bant abonelikleri ve mobil geniş bant abonelikleri de sürekli artış göstermektedir. Çizelge 6.8'de 9 NATO ülkesinin internet kullanıcı sayıları, sabit geniş bant abonelikleri ve mobil geniş bant abonelikleri açısından incelenmesi yer almaktadır.

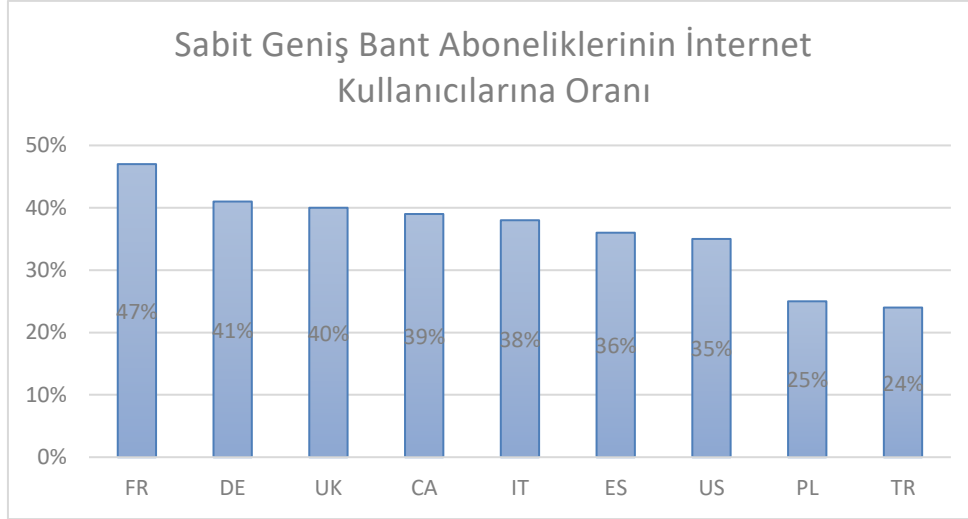
Çizelge 6.3. İnternet kullanıcı sayıları açısından incelenmesi

ÜLKELER	İnternet Kullanıcılarının Nüfusa Oranı (2016) [124]	Sabit Geniş Bant Aboneliklerinin İnternet Kullanıcılarına Oranı (2014) [120]	Kişi Başına Düşen Aktif Mobil Geniş Bant Abone Sayısı (2014) [121]
 CA	%93,3	39%	0,54
 DE	%88,4	41%	0,64
 ES	%76,9	36%	0,77
 FR	%83,8	47%	0,66
 IT	%62,0	38%	0,71
 PL	%67,5	25%	0,56
 TR	%59,6	24%	0,43
 UK	%91,6	40%	0,89
 US	%88,6	35%	1,03

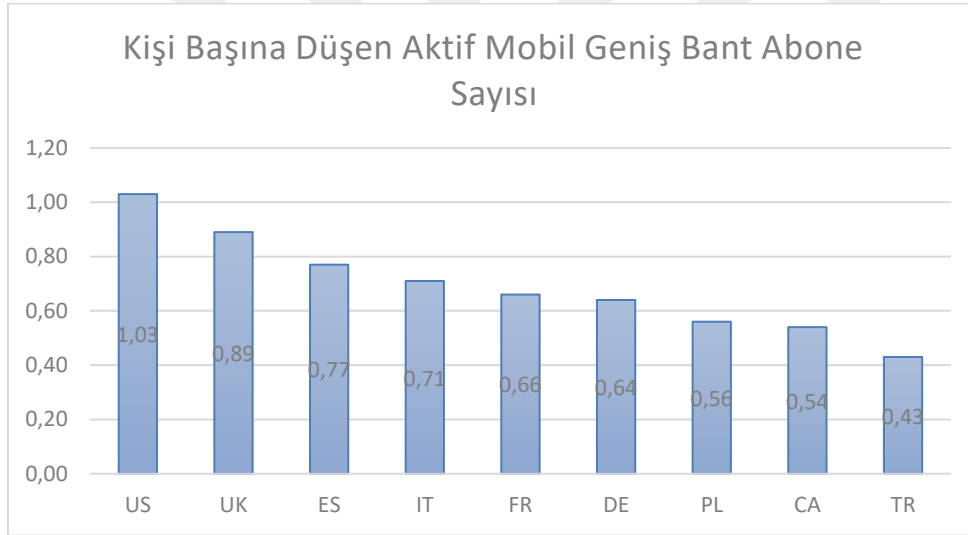
Yukarıdaki tabloda yer alan verilerin grafiksel gösterimi Şekil 6.12, Şekil 6.13 ve Şekil 6.14’de gösterilmektedir.



Şekil 6.9. İnternet kullanıcılarının nüfusa oranı



Şekil 6.10 Sabit geniş bant aboneliklerinin internet kullanıcılarına oranı



Şekil 6.11. Kişi başına düşen aktif mobil geniş bant abone sayısı

6.7. Kişisel ve Ulusal Bant Genişlikleri Açısında İncelenmesi

Uluslararası Telekomünikasyon Birliği (ITU), üye ülkelerin talepleri doğrultusunda 2009 yılından itibaren belirli periyotlarla bilgi iletişim teknolojileri konusunda gelişmişlik endeksi yayınlamaktadır. Söz konusu endeks ile;

- BİT alanında zaman içerisinde yaşanan gelişim ve düzeyin ölçülmesi ve diğer ülkeler ile kıyaslanması,

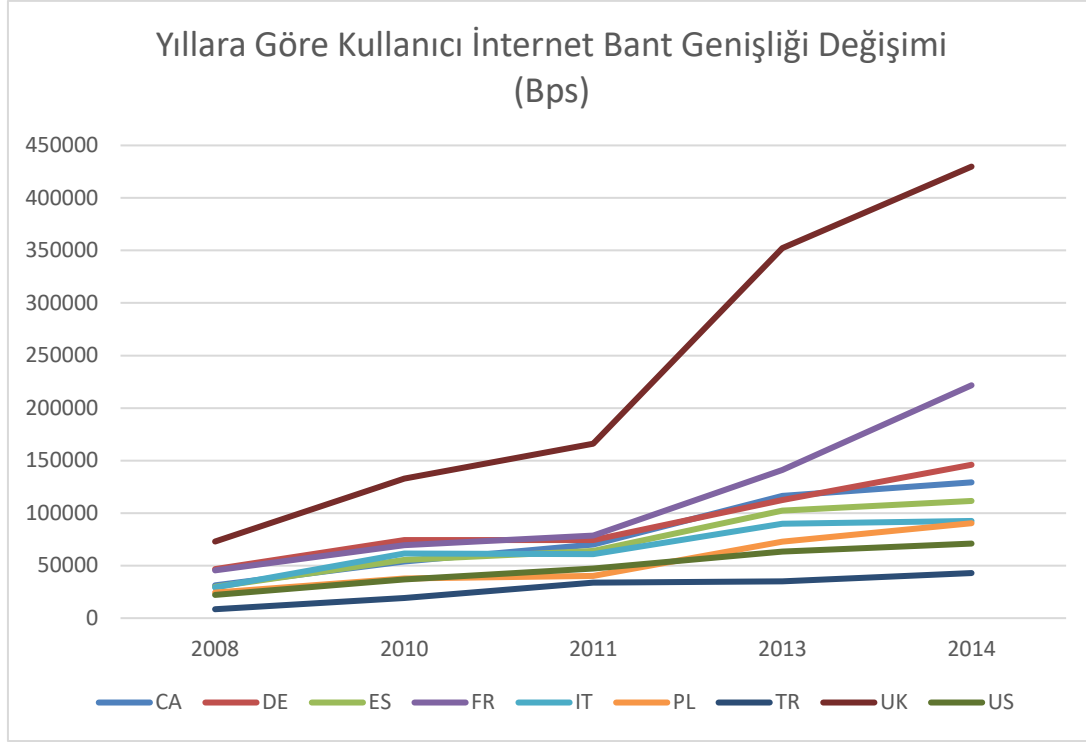
- Gelişmiş ve gelişmekte olan ülkelerde BİT alanındaki gelişimin ölçümü,
- Dijital farklılığın (ülkelerin BİT alanındaki düzey farklılıklarının) ortaya konulması amaçlanmaktadır.

ITU tarafından yayınlanan ve BİT konusunda gelişmişlik endekslerini gösteren dokümanlar ışığında Çizelge 6.9’da 9 NATO ülkesinin sahip oldukları ulusal internet bant genişliği ve kişi başına düşen bant genişliği açısından incelenmesi yer almaktadır.

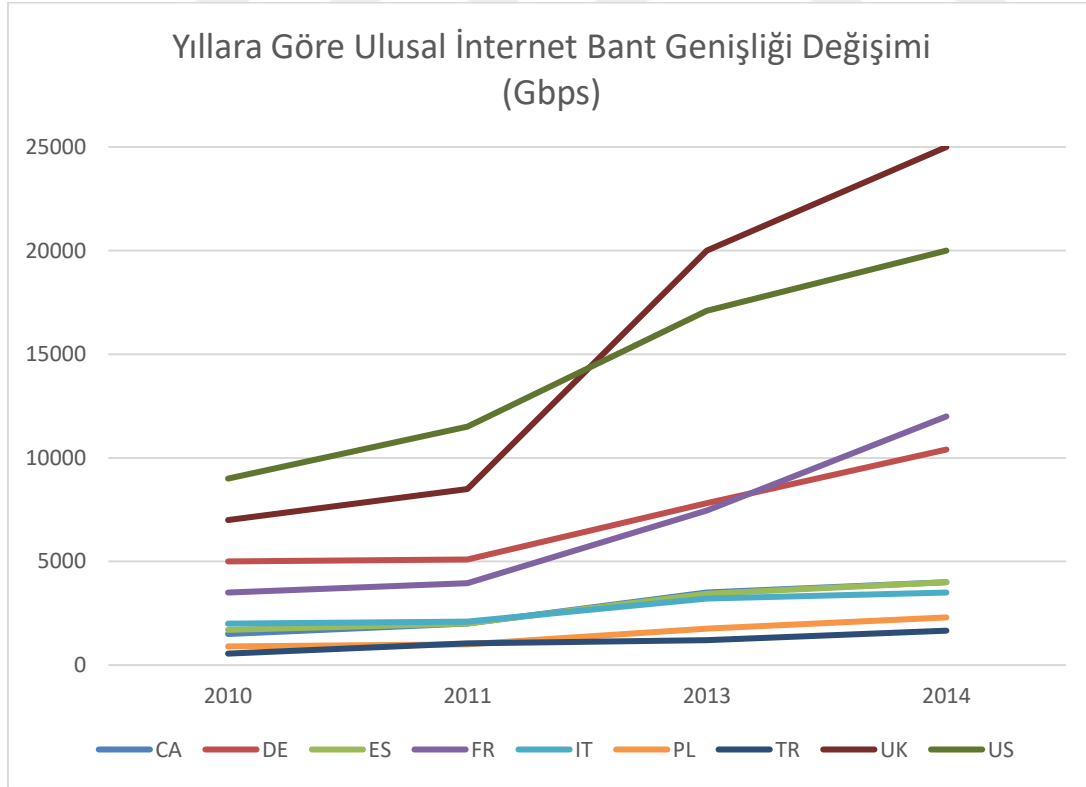
Çizelge 6.4. Kişisel ve ulusal bant genişlikleri açısından incelenmesi

ÜLKELER	Kullanıcı İnternet Bant Genişliği (2014) [126]			Ulusal İnternet Bant Genişliği (2014) [126]		
	İnternet Kullanıcısı Başına Saniyedeki Bit Sayısı (Bps)	2013-2014 Yılları Arası Büyüme Oranı	2009-2014 yılları arası büyüme oranı (CAGR)	Ülkeye Göre Toplam Saniyedeki Gigabit Sayısı (Gbps)	2013-2014 Yılları Arası Büyüme Oranı	2008-2013 Yılları Arası Büyüme Oranı (CAGR)
 CA	129,244	%11	%21,9	4,000	%14	%25,2
 DE	145,990	%30	%19,1	10,400	%33	%21,1
 ES	111,545	%9	%26,1	4,000	%16	%32
 FR	221,660	%57	%27,2	12,000	%61	%32
 IT	92,497	%3	%22,2	3,500	%9	%28,5
 PL	90,356	%24	%32,4	2,300	%31	%35,7
 TR	42,911	%23	%35,9	1,661	%38	%47,2
 UK	429,830	%22	%34,7	25,000	%25	%38
 US	70,970	%12	%17,4	20,000	%17	%23,4

Yukarıdaki tablodan da anlaşılacağı gibi Birleşik Krallık, gerek kişisel gerekse ulusal bazda en yüksek bant genişliğine sahip ülkedir. Şekil 6.15 internet kullanıcısı başına düşen saniyedeki bit sayısının (Bps), Şekil 6.16 ise ülkeye göre saniyedeki Gigabit sayısının (Gbps) son yıllardaki değişimini göstermektedir.



Şekil 6.12. Yıllara göre kullanıcı internet bant genişliği değişimi (Bps)



Şekil 6.13. Yıllara göre ulusal internet bant genişliği değişimi (Gbps)

6.8. Hukuki Düzenlemeler Ve Yönetmelikler Açısından İncelenmesi

Ülkelerin ulusal siber güvenlik stratejilerini belirlerken öncelik verdiği konuların başında, siber ortamda işlenen suçlar hakkında hukuki düzenlemeler yapılması ve siber suçların azaltılmasına yönelik tedbirlerin oluşturulması yer almaktadır. Ülkemizden örnek verecek olursak, UDHB tarafından yayımlanan 2013-2014 Eylem Planında ve 2016 -2019 Ulusal Siber Güvenlik Eylem Planında Hukuki düzenlemelere yer verilmiştir.

Bu bölümde, 9 NATO ülkesinde siber alanla ilgili yapılan hukuki düzenlemeler aşağıda belirlenen 7 alt başlık altında incelenecektir;

6.8.1. Kişisel Verilerin Gizliliği Kapsamındaki Düzenlemeler Açısından İncelenmesi

İnternet kullanıcıları, dünyanın herhangi bir bölgesinde saklanan şahsi verilerinin İnternet Servis Sağlayıcıları (İSS) ve Bulut Servis Sağlayıcılar (BSS) tarafından kullanılmayacağına ve açığa vurulmayacağına güvenmelidir. Ülkeler, vatandaşlarının kişisel verilerini güvence altına almak için ulusal çerçevede İSS'ları ve bulut sağlayıcıları da kapsayan gizlilik yasaları belirler. Ancak, gereksiz yere yapılan kısıtlamalar kullanıcıların internetten ve bulut ortamından ihtiyaç duyduğu ölçüde faydalanamamasına da sebep olabilir. Bu sebepten dolayı, yapılan düzenlemelerin hassas bir dengeyle yapılması önem arz etmektedir. EK-15'te kişisel verilerin gizliliği kapsamındaki düzenlemeler detaylı olarak incelenmektedir.

6.8.2. Kişisel ve Kurumsal Güvenliğin Geliştirilmesini Sağlayan Düzenlemeler Açısından İncelenmesi

Bulut bilişim kullanıcıları, verilerinin bulut ortamında güvenli bir şekilde saklanması ve çalıştırılmasının sağlanması konusunda BSS'lar tarafından gerekli güvenlik tedbirlerinin alınmasına ihtiyaç duymaktadır. Genel olarak, birçok ülke, yeni siber güvenlik çerçeveleri, yasaları ve politikaları geliştirerek ve bunları uygulayarak ortaya çıkan siber güvenlik tehditlerine karşı gerekli tedbirler almıştır. EK-16'da ülkelerin güvenlik ölçütlerini nasıl düzenledikleri, hangi dayanakları kullandıkları hususu yer almaktadır.

6.8.3. Siber Suçlar Kapsamındaki Düzenlemeler Açısından İncelenmesi

İnternet ve bulut ortamlarında tutulan verilerin birçoğu organize suç örgütleri tarafından hedef halinde bulunmaktadır. Ülkeler, sürekli gelişen siber tehditlere karşı hukuki düzenlemeler yapar ve uygularlar. EK-17’de ülkelerin hazırladıkları siber suç yasalarının dayanakları ve içerikleri konusunda bilgileri yer almaktadır.

6.8.4. Fikri Mülkiyet Haklarının Korunması Kapsamındaki Düzenlemeler Açısından İncelenmesi

Telif hakları da dediğimiz fikri mülkiyet hakları, eser üzerindeki haklar ve komşu haklardan oluşmaktadır. Dijital iletişim çağının en önemli sorunlarından biri de fikri hakların internet ortamında korunmasıdır. EK-18’de her ülkede yürürlükte olan fikri mülkiyet haklarının internet ortamında korunması kapsamındaki düzenlemeler yer almaktadır.

6.8.5. Fikri Mülkiyet Hakları Kapsamında İSS’lerinin Sorumlulukları Belirleyen Düzenlemeler Açısından İncelenmesi

İnternet kullanıcıları patentler, telif hakları, ticari sırlar ve diğer fikri mülkiyet hakları konusunda İSS’leri ve BSS’lerine güvenmelidir. EK-19’da fikri mülkiyet haklarının internet ortamında korunması kapsamında İSS’lerin sorumluluklarını belirleyen düzenlemeler incelenmiştir.

6.8.6. Ulusal ve Uluslararası Standartları Belirleyen Düzenlemeler Açısından İncelenmesi

İnternet kullanıcıları, dijital ekonomiden tam anlamıyla faydalanabilmek için veri taşınabilirliğine (mobility) ve kesintisiz çevrimiçi birlikte çalışabilirliğe ihtiyaç duymaktadır. BT (Bilgi Teknolojileri) endüstri kuruluşları söz konusu ihtiyaçları karşılayabilmek için uluslararası standartlar geliştirmektedir. Ayrıca, e-ticaret kuralları konusunda ülkelerin uluslararası uyumlulukları gerçekleştirmesi tavsiye edilmektedir. EK-20’de ülkelerin BT

endüstri kuruluşları liderliğinde gerçekleştirilen süreçler ve uluslararası e-ticaret yasalarına uyumlulukları açısından incelenmesi yer almaktadır.

6.8.7. E-Ticaret Kapsamındaki Düzenlemeler Açısından İncelenmesi

E-ticaret yasaları genel olarak, elektronik ticaret sürecinde yer alan kişilerin sorumluluklarını, aralarındaki sözleşmeleri ve bilgi verme yükümlülüklerini düzenlemektedir. İSS'ları ve BSS'ları tarafından sağlanan hizmetlerin başarımı bölgesel ve küresel pazarlara erişmesine bağlıdır. EK-21'de ilgili ülkelerdeki e-ticaret düzenlemeleri ve uygulamaları yer almaktadır.



7. SONUÇ VE ÖNERİLER

Günümüze gelinceye kadar yapılan akademik çalışmalar ile; siber güvenlik stratejisinin tanımlanması ve Aralık 2012 tarihinde hazırlanarak yürürlüğe giren Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın incelenmesi amaçlanmıştır.

Bu çalışma ile; mevcut bulunan akademik çalışmalardan farklı olarak NATO çatısı altında bulunan ulusların uyguladıkları siber güvenlik stratejileri mukayeseli olarak incelenmiştir. Bu çalışma ile, 28 farklı devletin siber güvenlik altyapılarını, siber güvenlik stratejilerini, siber güvenlik faaliyetlerini ortaya koymak suretiyle, ulusal çapta icra edilecek siber güvenlik çalışmalarına yeni bir bakış açısı sunması ve bu konuda farkındalık yaratması açısından önemli bir katkı sağlayacağı düşünülmektedir.

Çalışma başlıklarının belirlenmesi esnasında, önceki bölümde ifade edildiği üzere siber güvenlik konusunda tecrübe sahibi 16 kişi ile mülakat yapılmış ve görüşlerinden istifade edilmiştir. NATO üyesi ülkelerin strateji belgeleri ve uyguladıkları politikaların incelendiği bu tez çalışmasında, ülkemizin stratejik planına önemli katkı sağlayacağı değerlendirilen hususlar belirlenmiş ve bu hususlar aşağıdaki madde başlıklarında sunulmuştur.

1. Yapılan incelenmelerde özellikle Amerika Birleşik Devletleri olmak üzere gelişmiş ülkelerde siber güvenlik otorite makamları (Ulusal CERT) nitelikli ve yeter kadar personelden oluşmaktadır. Bu kapsamda; ülkemizde siber güvenlik otoritesi olarak görevlendirilen USOM (Ulusal Siber Olaylara Müdahale Merkezi), gerek yetişmiş personel açısından gerekse yetki açısından desteklenmelidir.
2. Almanya, İspanya, Fransa, İtalya, Polonya, Birleşik Krallık ve Amerika Birleşik Devletleri gibi NATO bünyesinde söz sahibi olan ülkelerin siber güvenlik konusunda uluslararası ortaklıklar yaptığı gözlemlenmektedir. Ayrıca söz konusu ülkeler uluslararası ortaklıklar yapılması konusuna ulusal siber güvenlik eylem planında yer vermektedir. Bu kapsamda;

- Gönüllü ülkelerle birlikte stratejik ortaklıklar desteklenmeli, istikrarlı ve güvenilir siber alanlar oluşturulmalı,
 - Uluslararası siber güvenlik organizasyonlarına personelin katılımının üst düzeyde tutulması sağlanmalı,
 - Siber güvenlik konusunda dünya ülkeleri ile uyumlu hale gelinmeli ve USOM aracılığıyla uluslararası koordinasyon geliştirilmelidir.
3. Fransa, İtalya ve Amerika Birleşik Devletleri; Eğitim-Öğretim 'de siber güvenlik kültürünün oluşturulması ve farkındalığın artırılması konusunu ulusal siber güvenlik eylem maddelerine dâhil etmişler ve ilköğretimden itibaren çocukları küçük yaşlarda projelere dâhil etmişlerdir. Bu kapsamda;
- Siber Güvenlik farkındalık eğitimleri ilköğretim seviyesine kadar indirilmeli,
 - Ulusal eğitimde, araştırma-geliştirmeye verilecek destek genişletilmeli,
 - Siber güvenlik zincirinin en zayıf halkası olan insanın eğitim seviyesi yükseltilmeli,
 - Siber güvenlik uzmanlığı konusunda işgücü genişletilmeli ve çalışanların eğitim seviyesinin artırılması için stratejiler geliştirilmelidir.
4. Risk analizi; tehlikelerin belirlenmesi, bu tehlikelerin riske dönüşmesine yol açan faktörler ile tehlikelerden kaynaklanan risklerin analiz edilerek derecelendirilmesi ve kontrol tedbirlerinin kararlaştırılması amacıyla yapılması gerekli çalışmaların yapılması olarak tanımlanabilir. Özellikle İtalya ve Amerika Birleşik Devletleri risk analizi konusunda çalışmalar yapmış ve yapılan çalışmaları ulusal siber güvenlik eylem planına dâhil etmişlerdir. Bu kapsamda, sanal ortamda paylaşılan bilgilerin önem derecelerine göre değerlendirilmesi, risk yönetim mekanizmasının kurulması, ekonomik faktörlerin değerlendirilmesi ve öncelikler belirlenmesi sonrasında siber güvenlik tedbirleri konusunda ulusal çapta bütçe planlamalarının yapılması önem arz etmektedir.
5. Kişisel Verilerin Korunması kapsamındaki hukuki düzenlemeler, incelenen ülkelerin büyük çoğunluğunda 1990'lı yılların sonlarında uygulanmaya başlamışken

lkemizde 24.03.2016 tarihinde yrrlge girmiřtir. Bundan dolayı sanal ortamdaki hayatların korunması konusunda ge kalındığı ve henz istenen seviyeye gelmediğı sylenebilir. Bu kapsamda; dijital ortamda gizlilik, kiřisel verilerin mahremiyeti ve siber sorumluluklar konusunda siber alan kullanımı geliřtirilmeli ve sayısal ortamdaki hayatlar mevzuatlarla garanti altına alınmalıdır.

6. Son yıllarda kresel apta uygulanan politikalarla verilerin bulut biliřim teknolojisi kullanılarak merkezileřtirilmesi sz konusudur. Bu kapsamda; Almanya, İřpanya, Fransa, İtalya, Polonya, Birleřik Krallık ve Amerika Birleřik Devletleri İSS'ları ile BSS'ları da kapsayan hukuki dzenlemeler yapmıřken lkemiz henz BSS'ları kapsayan hukuki dzenlemeler yapmamıřtır. Bu kapsamda, vatandaşların kiřisel verilerini gvence altına almak iin ulusal erevede İSS'ları ve bulut saėlayıcıları da kapsayan gizlilik yasaları belirlenmelidir. Ancak, gereksiz yere yapılan kısıtlamalar kullanıcıların internetten ve bulut ortamından ihtiya duyduėu lde faydalanamamasına da sebep olabilir. Bu sebepten dolayı, yapılan dzenlemelerin hassas bir dengeyle yapılması nem arz etmektedir.
7. Amerika Birleřik Devletleri; doėal afet, kriz veya atıřma gibi durumlarda kullanılmak zere siber gvenlik acil durum yeteneklerini geliřtirmeye ynelik tedbirler retmekte ve uygulamaktadır. Bu kapsamda; iř srekliliėinin devam etmesi ve kriz ortamının abuk atlatılabilmesi iin siber gvenlik acil durum planları yapılmalı ve felaketten kurtarma senaryoları geliřtirilmelidir.
8. İncelenen lkeler arasında İřpanya, Fransa ve Amerika Birleřik Devletleri siber gvenlik konusundaki bařarımda kamu ve zel sektr arasındaki uyuma dikkat ekmiř ve bu konuyu ulusal siber gvenlik eylem planına dahil etmiřtir. Bu kapsamda; dnyadaki olumlu rnekler gz nnde bulundurularak, siber olayları nleme, tespit etme ve bunlara tepki vermeye yardımcı olmak iin hkmet ve zel sektr arasında sre geliřtirilmelidir.

9. 31 Mart 2015 tarihinde Türkiye genelinde elektrik kesintisi yaşanmıştır. 6 saat süren ve Türkiye ekonomisine yaklaşık \$100.000.000 maliyeti olan kesintinin nedeni yetkililer tarafından “400kw iletim hattının aşırı yüklenerek servis dışı kalması” olarak ifade edilmiştir. Bununla birlikte, 6 saat süren bir elektrik kesintisinin devleti uğrattığı zarar ve yaşattığı kaos ortamı ortadadır. Ayrıca, devasa ölçekli sanayi işletmelerinden, çok karmaşık yapıya sahip tren yollarına, enerji tesislerinden küçük kapasiteli üretim tesislerine kadar birçok alanda SCADA sistemleri kullanılmakta ve yaygınlaşmaya devam etmektedir. Bu sistemler zaman, işgücü ve işlevsellik açısından avantajlar sağlamakla birlikte olası siber saldırı durumunda çok büyük zararlarla karşılaşılabilme ihtimali yüksektir. Kritik altyapılara ve SCADA sistemlerine yapılan benzeri saldırıların oluşturduğu tehdit ortamını gören Amerika Birleşik Devletleri ulusal CERT otoritesinin yanında ISC CERT (The Industrial Control Systems Cyber Emergency Response Team - Endüstriyel Kontrol Sistemleri Siber Acil Müdahale Ekibi) otoritesini kurmuş ve kritik altyapılara yapılacak muhtemel saldırılara karşı daha etkili tepkiler vermeyi amaçlamıştır. Bu kapsamda, kritik altyapıları destekleyen Bilişim ve Telekomünikasyon sistemlerinin güvenliğinin sağlanması için Amerika Birleşik Devletleri’nde uygulanan söz konusu yöntemin ulusal çapta uygulanabileceği değerlendirilmektedir.
10. Ulusal güvenliğin tehdit edilmesi durumunda, öncelikle ulusal güvenlik güçlerinin (asker, polis) ve istihbarat birimlerinin haberleşmesi ve irtibat kanalları muhtemel hedef olarak alınacaktır. Bu bağlamda güvenlik güçleri ve istihbarat birimlerinin siber savunma yeteneklerinin güçlendirilmesi önem arz etmektedir.
11. Ülkemizde günümüze gelinceye kadar, 2013-2014 ve 2016-2019 yıllarını kapsayan 2 adet onaylı Ulusal Siber Güvenlik Strateji ve Eylem Planı hazırlanmıştır. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı 7 ana başlık ve 29 eylem maddesinden, 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ise 5 ana başlık 39 eylem maddesinden oluşmaktadır. Bu kapsamda önümüzdeki süreçte hazırlanacak Ulusal Siber Güvenlik Stratejisinin kapsamı genişletilmeli ve görevlendirilen kurum/kuruluşlar üzerindeki takip ve koordinasyon artırılmalıdır.

Eylül 2016’da açıklanan ve yürürlüğe giren “2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı” ile yapılan güncellemelerde “Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının” kapsamı genişletilmiş ve detaylandırılmıştır. Önümüzdeki yıllarda yapılacak güncellemelerde; yukarıda belirtilen hususlara dikkat etmek suretiyle, strateji dokümanı ile eylem planının daha etkin olması ve kurumlar ile sektöre daha çok katkılar sağlanması beklenmektedir.





KAYNAKLAR

1. Creasey, J., Glover, I. (2013). *Cyber Security Incident Response Guide-Version 1*. CREST. USA.
2. İnternet: İnternet Users in the World. URL: <http://www.internetlivestats.com/internet-users/>, Son Erişim Tarihi: 08.06.2016.
3. Fisher, D. Finger, H. Kramer, W. Stanle, J. (1988). *Report Of Computer Virus Incident At Ames*.
4. İnternet: March 2016 Cyber Attacks Statistics. URL: <http://www.hackmageddon.com/category/security/cyber-attacks-statistics/>, Son Erişim Tarihi: 16.05.2016.
5. Schneier, B. (2000). *Secrets and Lies, Digital Security In A Networked World*, Wiley Publishing.
6. The White House. *The National Strategy to Secure Cyberspace*. (2003). Washington: The White House.
7. Klimburg, A. (2011). The Whole of Nation in Cyberpower, *Georgetown Journal of International Affairs*, 171-179.
8. Libicki, M.C. (2009). *Cyberdeterrence and Cyberwar*. United States of America: RAND Corporation, 12-13.
9. International Telecommunication Union. (2008). *ITU-T X.1205. Overview of cybersecurity*.
10. Hill, R. (2015). Dealing With Cyber Security Threats: International Cooperation, ITU and WCIT. *7th International Conference on Cyber Conflict*, 119-134.
11. İnternet: FACT SHEET: Cybersecurity Legislative Proposal. URL: <https://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal> Son Erişim Tarihi: 29.04.2016.
12. The Information Security Arm Of GCHQ. (2012). 10 Steps to Cyber Security. Office Of Cyber Security & Information Assurance. Cabinet Office.
13. General James Cartwright, J,E. (2011). Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations 5

14. Rittinghouse, J.W., and Hancock, W.M. (2003). *Cybersecurity Operations Handbook*. Elsevier Digital Press, 334.
15. Schreier, F. (2015). *On Cyberwarfare*. DCAF Horizon 2015 Working Paper No.7, 61.
16. Ögün, M.N., and KAYA, A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. *Güvenlik Stratejileri Dergisi*, 9(18), 145-181.
17. Adress, J., and Winterfeld, S. (2011). *Cyber Warfare Techniques, Tactics and Tools for Security Practitioners*. USA:Elsevier.
18. Thion, R. (2008). *Network-Based Passive Information Gathering*. France: Idea Group Publishing. University of Lyon, France.
19. Zeisloft, C.S. (2013). *Hacking and U.S. Financial Institutions*. Master Thesis of Science in Cybersecurity, A Capstone Project Submitted to the Faculty of Utica College.
20. Collin, B.C. (2004). *The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge*, 11th Annual International Symposium, Institute for Security and Intelligence.
21. Denning, E.D. (2000). Cyberterrorism, *Global Dialogue [abstract]*.
22. O'Hara, G. (2010). *Cyber-Espionage: A Growing Threat to the American Economy*, 19 COMLAW CONSPECTUS, 241.
23. Özbay, R. (2015). *Aktif Siber Savunma Teknikleri ve Performans Analizi*. Yayınlanmış Yüksek Lisans Tezi, İnternet ve Bilişim teknolojileri Yönetimi Anabilim Dalı, Fen Bilimleri Enstitüsü, Afyon Kocatepe Üniversitesi, Ankara.
24. SCHMITT, M. N. International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence. (2013). *Talinn Manual On The International Law Applicable to Cyber Warfare*. UK:Cambridge University Press.
25. Intel Security. (2016). McAfee Labs 2016 Threats Predictions Report.
26. Hutchins, E.M. Cloppert, M.J., and Amin, R.M. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Lockheed Martin Corporation*.
27. Friedberg, I. Skopik, F. Settani, G., and Fiedler R. (2015). Combating advanced persistent threats: From network event correlation to incident detection. *Computers & Security* 48, 35-57.
28. Mandiant. (2013). Exposing One of China's Cyber Espionage Units. *Mandiant APT1 Raporu*.

29. İnternet: Chinese hackers suspected in attack on The Post's computers. URL: https://www.washingtonpost.com/business/%20technology/chinese-hackers-suspected-in-attack-on-the-posts-computers/2013/02/01/d5a44fde-6cb1-11e2-bd36-c0fe61a205f6_story.html, Son Erişim Tarihi: 13.06.2016.
30. İnternet: Pawn Storm Group Targets Turkey. URL: <http://www.securityweek.com/pawn-storm-group-targets-turkey> Son Erişim Tarihi: 14.06.2016.
31. Aydın, E. (1992). *Bilişim Suçları ve Hukukuna Giriş* (1'inci Baskı). Ankara: Doruk Yayınları.
32. T.C. Kalkınma Bakanlığı. (2014). *2014-2018 Bilgi Toplumu Stratejisi ve Eylem Planı*. Ankara: T.C. Kalkınma Bakanlığı.
33. İnternet: Motivations Behind Attacks. URL: <http://www.hackmageddon.com/2016/06/01/april-2016-cyber-attacks-statistics>, Son Erişim Tarihi: 15.06.2016.
34. İnternet: Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2015 (in million U.S. dollars). URL: <http://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/>, Son Erişim Tarihi: 15.06.2016.
35. Akarslan, H. (2011). *Bilişim Suçları, Bilişim Yoluyla İşlenen Suçlar ve Adli Bilişim Ayrımı*. Yüksek Lisans Tezi, Polis Akademisi, Adli Bilimler Anabilim Dalı, Güvenlik Bilimleri Enstitüsü, Ankara.
36. European Commission. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Brussels: European Commission.
37. Council of Europe. (2001). *Convention on Cybercrime*. Budapest: Council of Europe.
38. Mahmutoglu, F.S. (2002, 02 Mayıs). *Karşılaştırmalı Hukuk Bakımından İnternet Sürelerinin Ceza Sorumluluğu*. İ.Ü. Hukuk Fakültesi, Ceza Hukuku ve Kriminoloji Araştırma ve Uygulama Merkezi'nde yapılan, "İnternet Ortamında Ceza Sorumluluğu" konulu panelde sunuldu. İstanbul.
39. Özçoban, C. (2014). *21. Yüzyılda Ulusal Güvenliğin Sağlanmasında Siber İstihbaratın Rolü*. Yüksek Lisans Tezi, Harp Akademileri, Stratejik Araştırma Enstitüsü, İstanbul.
40. Clarke, R.A., and Knake, R.K. (2010). *Cyber War*. HarperCollins e-books. 11.

41. Kara, M. (2013). *Siber Saldırıları – Siber Savaşlar ve Etkileri*. Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, İstanbul, 40-41.
42. Cornish, P. Livingstone, D. Clemente, D. Yorke C. (2010). On Cyber Warfare. *A Clatham House Report*. 1.
43. Stallard, C. (2011). *At The Crossroads of Cyber Warfare: Signposts For The Royal Australian Air Force*. Yüksek Lisans Tezi, School of Advanced Air and Space Studies, Maxwell Air Force Base, Alabama, 47.
44. İnternet: What is NATO. URL: <http://www.nato.int/nato-welcome/index.html> Son Erişim Tarihi: 20.06.2016.
45. İnternet: NATO Member Countries. URL: http://www.nato.int/cps/en/natohq/nato_countries.htm Son Erişim Tarihi: 20.06.2016.
46. Kuzey Atlantik Antlaşması. (1949). Washington DC.
47. İnternet: NATO Organisation. URL: <http://www.nato.int/cps/en/natohq/structure.htm> Son Erişim Tarihi: 25.06.2016.
48. İnternet: Statement by the North Atlantic Council on Kosovo. URL: <http://www.nato.int/docu/pr/1999/p99-012e.htm> Son Erişim Tarihi: 25.06.2016.
49. Arquilla, J., and Ronfeldt, D. (2001). *Networks and Netwars The Future of Terror, Crime, and Militancy*. USA: RAND Corporation. 240-248.
50. Denning, D. (2001). *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. USA: RAND Corporation. 239-288.
51. Department of Homeland Security. (2006). Cyber Storm Exercise Report. DHS. USA.
52. Joshua, D. (21 Ağustos 2007). Hackers Take Down the Most Wired Country in Europe. *Wired Magazine, Issue 15.09*.
53. Kaiser, R. (2015). The birth of cyberwar. *Political Geography* 46. 11-20.
54. Shakarian, P. Shakarian, J., and Ruef, A. (2013). *Introduction To Cyber-Warfare: A Multidisciplinary Approach*, Elsevier, 16-20.
55. Wrenn, C.F. (2012). *Strategic Cyber Deterrence*, Doktora Tezi, The Faculty of The Fletcher School of Law and Diplomacy, USA, 178.

56. Kadri, K. Eneken, T., and Lijs, V. (2010). *International Cyber Incidents: Legal Considerations*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn:CCDCOE.
57. İnternet: That cyberwarfare by Russia on Estonia? It was one kid in Estonia. URL: <https://www.theguardian.com/technology/blog/2008/ian/25/thatcyberwarfarebyussiaon> Son Erişim Tarihi: 29.06.2016.
58. Herzog, S.(2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses, *Journal of Strategic Security*, Number 2, Volume 4, 54-55.
59. İnternet: GEORGIA AND NATO. URL: <http://www.nato-pa.int/Default.asp?SHORTCUT=1776> Son Erişim Tarihi: 29.06.2016.
60. Bıçakçı, S. (2014). NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik, *Uluslararası İlişkiler*, Cilt 10, Sayı 40, 101-130.
61. Eneken, T. Kadri, K. Runnimeri, K. Kert, M. Tali harm, A. Lijs, V. (2008). Cyber Attacks Against Georgia: Legal Lessons Identified, *NATO Cooperative Cyber Defence Centre of Excellence*, Tallinn.
62. Bıçakçı, S. (2012). Yeni Savaş Ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu, *Uluslararası İlişkiler*, Cilt 9, Sayı 34, 205-226.
63. Carr, J. (2010). *Inside Cyber Warfare*, O'Reilly Media, USA, 31.
64. Check, T. (2015). Book Review: Analyzing the Effectiveness of the Tallinn Manual's Jus Ad Bellum Doctrine on Cyberconflict: A NATO-Centric Approach, Cleveland State University, 495-512.
65. NATO CCDCOE. (3 Nisan 2008). *NATO Bucharest Summit Declaration*.
66. İnternet: History of CCDCOE. URL: <https://ccdcoe.org/history.html> Son Erişim Tarihi: 10.07.2016.
67. İnternet: 173 DSCFC 09 E BIS – NATO and Cyber Defence. URL: <http://www.nato-pa.int/default.Asp?SHORTCUT=1782> Son Erişim Tarihi: 10.07.2016.
68. NATO CCDCOE. (20 Kasım 2010). Lisbon Summit Declaration.
69. İnternet: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. URL: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf Son Erişim Tarihi: 08.07.2016.

70. Rapporteur Noshiravani, R. (20 Mayıs 2011). NATO and Cyber Security: Building on the Strategic Concept, Chatham House.
71. NATO. (19 Ağustos 2011). *Defending the Networks: The NATO Policy on Cyber Defence* (Brussels: North Atlantic Treaty Organization).
72. İnternet: Cyber defence. URL: http://www.nato.int/cps/en/natohq/topics_78170.htm Son Erişim Tarihi: 08.07.2016.
73. NATO. (4-5 Eylül 2014). NATO Wales Summit Guide.
74. Fidler, D, P. Pregent, R. Vandurme, A. (2013), *NATO, Cyber Defence and International Law, Digital Repository of Maurer School of Law: Indiana University*.
75. Klimburg, A. (2012). *National Cyber Security Framework Manual*, NATO CCDCOE Publication, Talinn, 180-188.
76. Ünver, M. Canbay, C. Mirzaoglu, A.G. (2009). *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler*, Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı, 22-52.
77. İnternet: About ITU. URL: <https://www.itu.int/en/about/Pages/default.aspx> Son Erişim Tarihi: 24.11.2016.
78. Wamala, F. (2011), *ITU National Cybersecurity Strategy Guide*, 25-65.
79. ITU. (2008). ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG) Global Strategic Report. 92-101.
80. EU ENISA. (21 Mayıs 2013). ENISA Regulation (EU) No 526/2013 of The European Parliament and of The Council of 21 may 2013.
81. ENISA. (Kasım 2016). ENISA NCSS Good Practice Guide – Designing and Implementing National Cyber Security Strategies.
82. Ünver, M. *Türkiye’de Siber Güvenlik*. Bilgi Güvenliği Derneği.
83. İnternet: Resmi Gazete. URL: <http://www.resmigazete.gov.tr/eskiler/2014/02/20140219-1.htm> Son Erişim Tarihi: 12.12.2016.
84. İnternet: Resmi Gazete. URL: <http://www.resmigazete.gov.tr/eskiler/2013/11/20131111-6.htm> Son Erişim Tarihi: 12.12.2016.
85. T.C.Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2013). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı.

86. T.C.Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi.
87. T.C.Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2016). 2016-2019 Ulusal Siber Güvenlik Eylem Planı.
88. ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı). Belgium Country Report. Greece.
89. Canada Public Safety (Kanada Kamu Güvenliği). (2010). Canada's Cyber Security Strategy 2010. Canada.
90. ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı). Czech Republic Country Report. Greece.
91. ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı). Germany Country Report. Greece.
92. ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı). Estonia Country Report. Greece.
93. ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı). Spain Country Report, Greece.
94. ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı). France Country Report. Greece.
95. ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı). Greece Country Report. Greece.
96. ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı). Hungary Country Report. Greece.
97. ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı). Italy Country Report. Greece.
98. ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı). Lithuania Country Report. Greece.
99. ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı). Luxembourg Country Report. Greece.
100. ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı). Latvia Country Report. Greece.
101. ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı). Netherlands Country Report. Greece.
102. ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı). Poland Country Report. Greece.
103. ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı). Romania Country Report. Greece.
104. ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı). Slovakia Country Report. Greece.
105. ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı). United Kingdom Country Report. Greece.
106. Pernik, P. Wojtkowiak, J. Verschoor-Kirss, A. (2016), *National Cyber Security Organisation: United States*, CCDCOE publication.
107. İnternet: FIRST Vision and Mission Statement. URL: <https://www.first.org/about/mission> Son Erişim Tarihi: 10.02.2017.
108. İnternet: FIRST Members around the World. URL: <https://www.first.org/members/map> Son Erişim Tarihi: 11.02.2017.
109. İnternet: URL: <https://www.enisa.europa.eu/> Son Erişim Tarihi: 18.02.2017.

110. İnternet: Member States. URL: <https://www.itu.int/en/membership/Pages/member-states.aspx> Son Erişim Tarihi: 18.02.2017.
111. Canada Public Safety (Kanada Kamu Güvenliği). (2010). Action Plan 2010-2015 for Canada's Cyber Security Strategy. Kanada.
112. The BSI (Bilgi Güvenliği Federal Ofisi). Cyber Security Strategy for Germany. Almanya.
113. Espana Departamento De Seguridad Nacional (İspanya Ulusal Güvenlik Birimi). (2013). National Cyber Security Strategy. İspanya.
114. Republique Française Premier Ministre (Fransa Cumhuriyeti Başbakanlığı). French National Digital Security Strategy. Fransa.
115. Italy Presidency Of The Council Of Ministers (İtalya Bakanlar Kurulu Başkanlığı). (2013). The National Plan For Cyberspace Protection and ICT Security. İtalya.
116. Republic Of Poland Ministry of Administration and Digitisation, İnernal Security Agency (Polonya Cumhuriyeti İdare ve Sayısallaştırma Bakanlığı, İç Güvenlik Ajansı). (2013). Cyberspace Protection Policy Of The Republic Of Poland. Polonya.
117. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2016). 2016-2019 Ulusal Siber Güvenlik Eylem Planı. Türkiye.
118. UK Cabinet Office (Birleşik Krallık Bakanlar Kurulu). (2011). The UK Cyber Security Strategy. Birleşik Krallık.
119. White House (Beyaz Saray). Cyberspace Policy Review. ABD.
120. Galexia Consulting. (2016). 2016 BSA Global Cloud Copmuting Scorecard – Confronting New Challenges. BSA Report.
121. Sanau B. (2016). Measuring the Information Society Report. ITU.
122. Baller, S., Dutta, S., Lanvin, B. (2016). The Global Information Technology Report 2016 – Innovating in the Digital Economy. Insight Report. World Economic Forum.
123. İnternet: International Connectivity Scorecard (2013). URL:<http://www.connectivityscorecard.org> Son Erişim Tarihi: 11.02.2017.
124. İnternet: URL: <http://www.internetworldstats.com/stats4.htm> Son Erişim Tarihi: 18.02.2017.
125. İnternet: 2016 BSA Canada Country Report. URL: http://cloudscorecard.bsa.org/2012/assets/PDFs/country_reports/Country_Report_Canada.pdf, Son Erişim Tarihi: 05.01.2018.

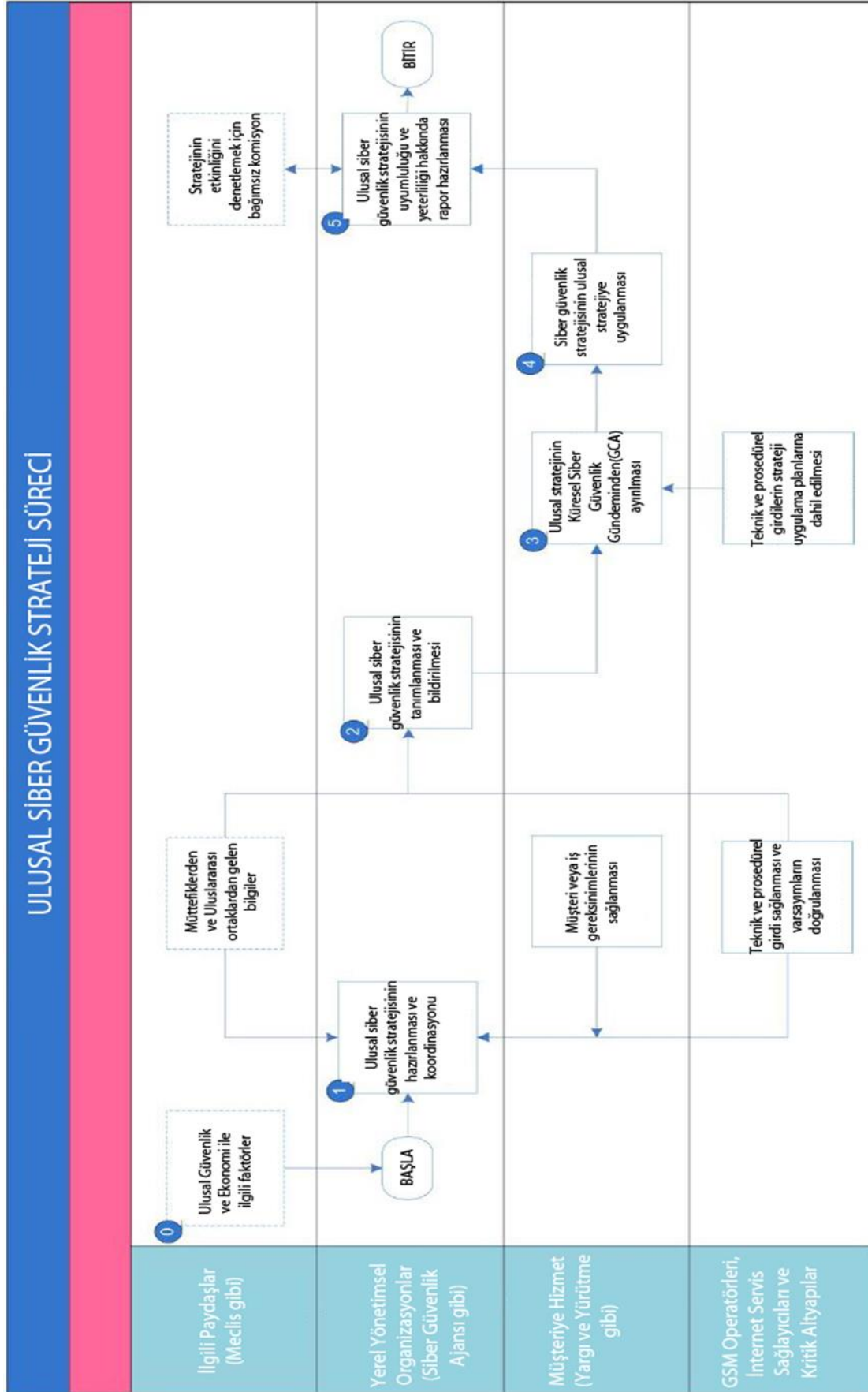
126. İnternet: 2016 BSA Germany Country Report. URL: http://cloudscorecard.bsa.org/2016/pdf/country_reports/2016_Country_Report_Germany.pdf , Son Erişim Tarihi: 05.01.2018.
127. İnternet: 2016 BSA Spain Country Report. URL: http://cloudscorecard.bsa.org/2016/pdf/country_reports/2016_Country_Report_Spain.pdf , Son Erişim Tarihi: 05.01.2018.
128. İnternet: 2016 BSA France Country Report. URL: http://cloudscorecard.bsa.org/2016/pdf/country_reports/2016_Country_Report_France.pdf , Son Erişim Tarihi: 05.01.2018.
129. İnternet: 2016 BSA Italy Country Report. URL: http://cloudscorecard.bsa.org/2016/pdf/country_reports/2016_Country_Report_Italy.pdf, Son Erişim Tarihi: 05.01.2018.
130. İnternet: 2016 BSA Poland Country Report. URL: http://cloudscorecard.bsa.org/2016/pdf/country_reports/2016_Country_Report_Poland.pdf , Son Erişim Tarihi: 05.01.2018.
131. İnternet: 2016 BSA Turkey Country Report. URL: http://cloudscorecard.bsa.org/2016/pdf/country_reports/2016_Country_Report_Turkey.pdf , Son Erişim Tarihi: 05.01.2018.
132. İnternet: 2016 BSA United Kingdom Country Report. URL: http://cloudscorecard.bsa.org/2016/pdf/country_reports/2016_Country_Report_UnitedKingdom.pdf , Son Erişim Tarihi: 05.01.2018.
133. İnternet: 2016 BSA United States Country Report. URL: http://cloudscorecard.bsa.org/2016/pdf/country_reports/2016_Country_Report_UnitedStates.pdf , Son Erişim Tarihi: 05.01.2018.



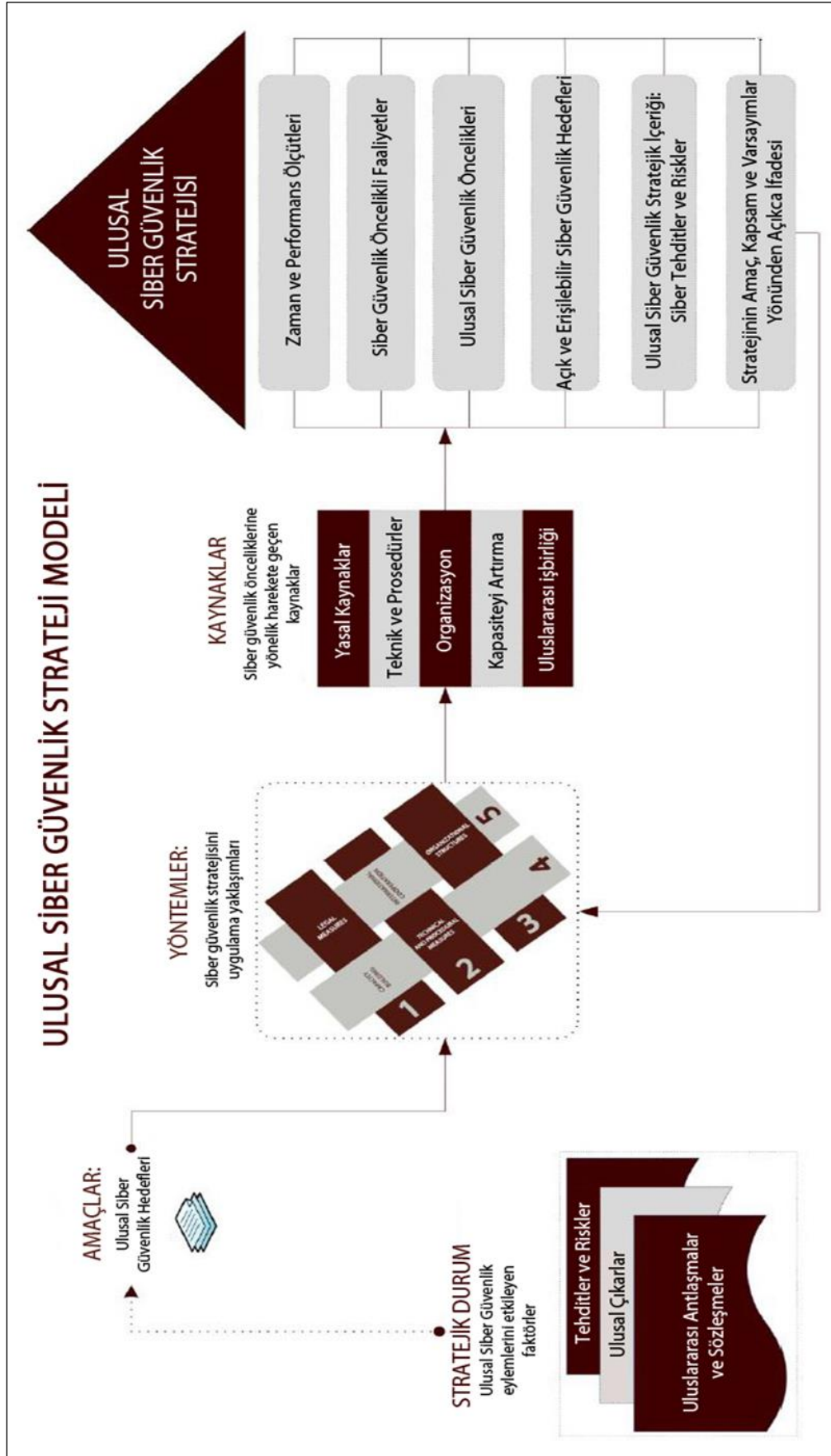
EK-1. NATO üyesi ülkeler

KATILIM TARİHİ	ÜLKELER	GENİŞLEME
4 Nisan 1949	 Belçika	Kurucu Üyeler
	 Kanada	
	 Danimarka	
	 Fransa	
	 İzlanda	
	 İtalya	
	 Lüksemburg	
	 Hollanda	
	 Norveç	
	 Portekiz	
	 Birleşik Krallık	
	 Amerika Birleşik Devletleri	
18 Şubat 1952	 Yunanistan	İlk Genişleme
	 Türkiye	
9 Mayıs 1955	 Almanya	İkinci Genişleme
30 Mayıs 1982	 İspanya	Üçüncü Genişleme
12 Mart 1999	 Çek Cumhuriyeti	Dördüncü Genişleme
	 Macaristan	
	 Polonya	
29 Mart 2004	 Bulgaristan	Beşinci Genişleme
	 Estonya	
	 Letonya	
	 Litvanya	
	 Romanya	
	 Slovakya	
	 Slovenya	
1 Nisan 2009	 Arnavutluk	Altıncı Genişleme
	 Hırvatistan	

EK-2. ITU tarafından önerilen ulusal siber güvenlik strateji süreci



EK-3. ITU tarafından önerilen ulusal siber güvenlik strateji modeli



EK-4. Stratejinin tasarlanması ve geliştirilmesi

1. Vizyon, kapsam, hedefler ve önceliklerin belirlenmesi

- Üst düzey hedefleri belirli bir zaman periyodunda (genellikle 5-10 yıl) gerçekleştirebilmek için vizyonu ve kapsamı tanımlayın,
- Bu strateji kapsamında yer alan özel sektörleri ve hizmetleri tanımlayın,
- Hedeflerin topluma, ekonomiye ve vatandaşlara etkisi açısından önceliklendirin,
- Stratejinin uygulanması için bir yol haritası belirleyin.

2. Risk analizi yaklaşımı belirlenmesi ve uygulanması

- Kullanılacak bir risk değerlendirme metodolojisi üzerinde anlaşmaya varın,
- Ulusal bir otoriteyi ve ya sektörel yetkili mercileri risk değerlendirmesi yapmakla görevlendirin,
- Risk tanımlama ve değerlendirme yaklaşımı tasarlayın ve takip edin,
- Kritik bilgi altyapılarını tanımlamak bir yöntem geliştirin.

3. Varolan politikaların, düzenlemelerin ve yeteneklerin toplanması

- Siber güvenlik alanında yıllar içerisinde geliştirilen politikaları toplayın.
- Siber güvenlikle ilgili AB politikaları, direktifleri ve şartları bir araya getirin.
- Siber güvenlik stratejinizi, kritik altyapıların korunması ve kriz yönetimi gibi alanlarla zenginleştirin.
- Siber güvenliğin etkinleştirilmesinde farklı sektörler tarafından uygulanan tüm düzenleyici önlemleri ve etkilerini tanımlayın.
- Mevcut düzenleyici mekanizmaları tanımlayın ve bunların hedeflerine ne ölçüde ulaştıklarını değerlendirin.
- Siber güvenlik politikaları, yönetmelikleri ve işletilmesi ile uğraşmakta olan kamu kurumlarının rollerini ve sorumluluklarını analiz edin. Çakışmaları ve boşlukları belirleyin.
- Stratejik gelişim için süreci şeffaf hale getirin.

4. Açık bir yönetim yapısı kurulması

- Stratejinin yönetimi ve değerlendirmesinden sorumlu kimliği tanımlayın.
- Yönetim yapısını tanımlayın.
- Yetkileri tanımlayın.
- Siber güvenlik politikası ve yönetmeliğinin başlatılması ve geliştirilmesinden sorumlu kurumların görevlerini tanımlayın veya doğrulayın.
- Tehdit ve zafiyetleri toplamak, siber saldırılara tepki vermek, kriz yönetimini güçlendirmek sorumluluğu bulunan kurumların görevlerini tanımlayın.
- Kamu ve özel sektörde belirlenen Bilgisayar Olaylarına Müdahale Ekiplerinin (BOME) rolünü tanımlayın.

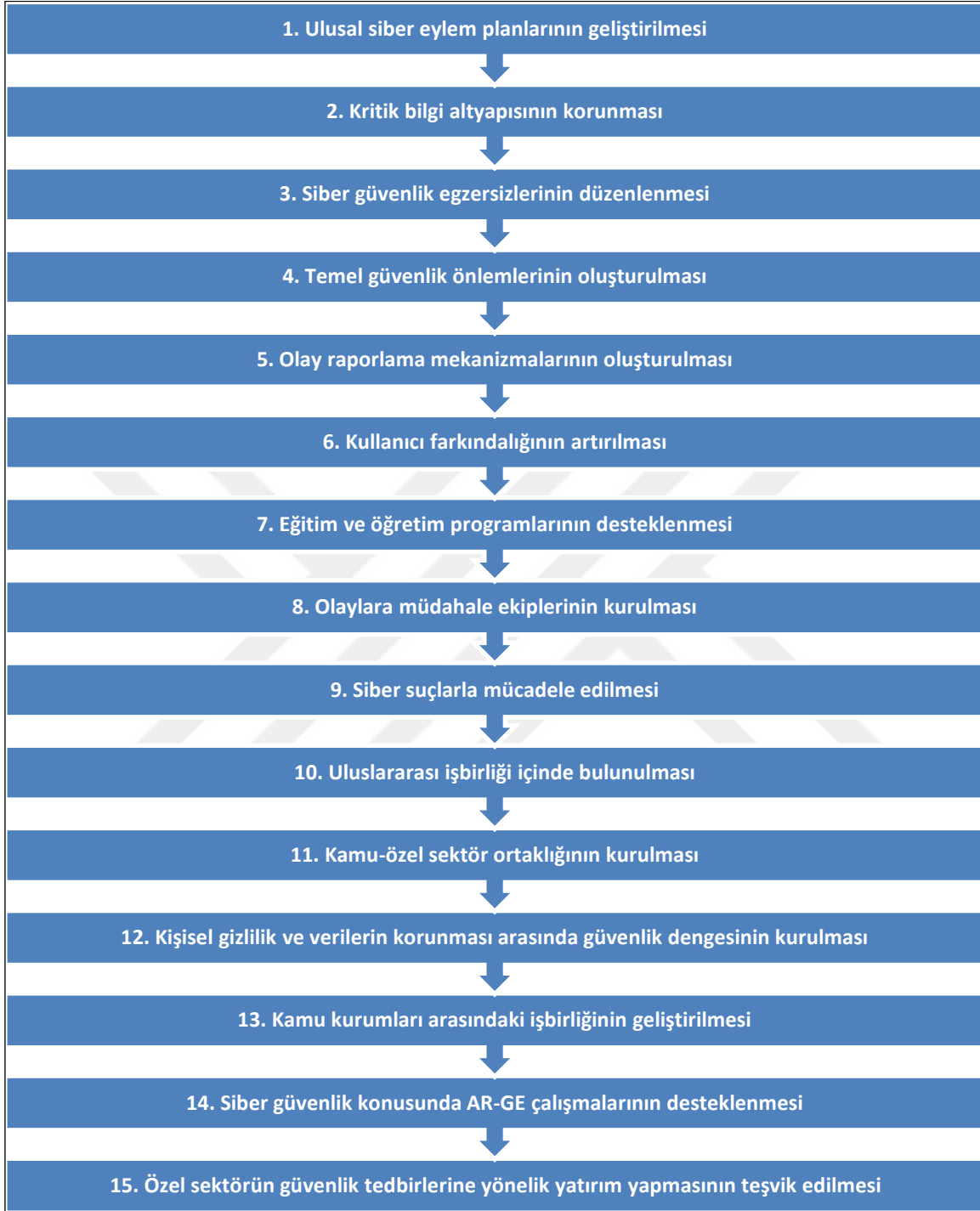
5. Paydaşların belirlenmesi ve anlaşmaların yapılması

- Kamu paydaşlarını belirleyin.
- Rollerini ve sorumluluklarını açıkça tanımlayarak hem kamusal hem de özel paydaşları sürece dâhil edin.
- Stratejinin geliştirilmesi sürecinde doğru paydaşları doğru zamanda dâhil edin.
- Belirlenen paydaşların stratejinin amaçlarına, eylem planlarına nasıl katkı sağlandığını açıklayın.
- Bilgi paylaşımı, (uluslararası) işbirliği ve risk yönetimi konularında hükümet yetkililerine süreci kolaylaştırıcı roller tanımlayın.
- Aidiyetlerini artırmak için üst düzey temsilcileri sürece dâhil edin.
- Özel ve kamusal paydaşların sürece katılmalarını sağlayan uygun teşvikleri tanımlayın.

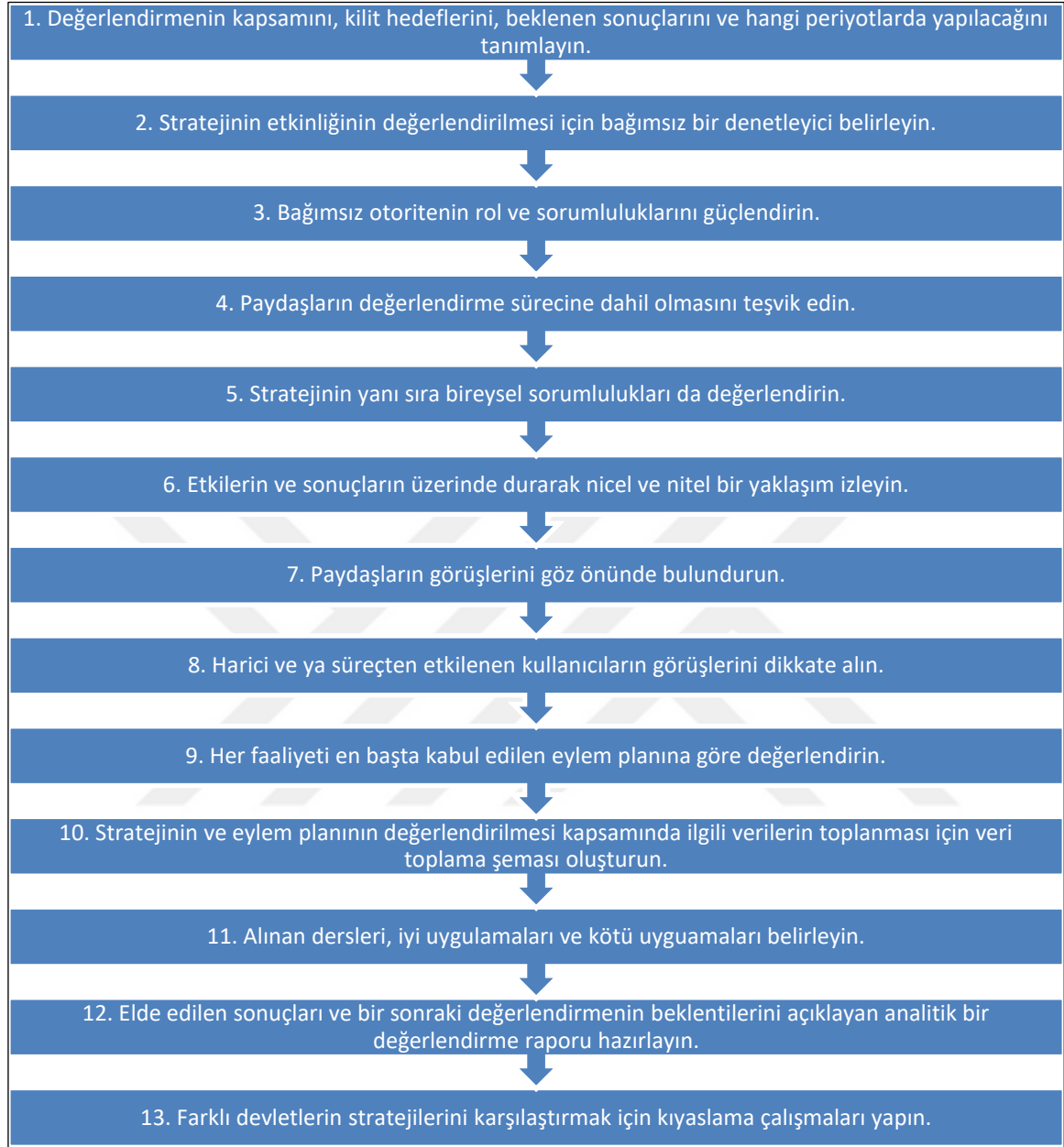
6. Güvenilir bilgi paylaşım mekanizmalarının kurulması

- Bilgi paylaşım mekanizmasını ve mekanizmayı yöneten temel ilke ve kuralları tanımlayın.
- Bilgi paylaşımı içi bir sektör yaklaşımını benimseyin (İSS'lerin bilgi paylaşım platformu gibi).
- Sektörler arası iletişimi teşvik edin ve koordinasyonu sağlayın.
- Stratejik konulara, kritik tehditlere ve zayıf noktalara odaklanın.
- Paydaşları "bilmesi gereken" prensibine göre hassas bilgilere erişebilmesi ve paylaşabilmesi için teşvik edin.
- Uygun profile sahip uzman personelin projeye katılmasını sağlayın.
- Güvenilir bilgi paylaşım mekanizmasına kolluk, istihbarat, kanun düzenleyici kurumlar ve ulusal BOME'ler gibi kurumların hangilerinin dahil olacağını belirleyin.
- Uzmanlar arasında güven mekanizmasının gelişmesi için bilgi paylaşım ağını daraltın.
- Hassas bilgileri paylaşmak için düzenli (yüz yüze) toplantılar düzenleyin.
- Uluslararası güvenilir bilgi paylaşım ağını belirleyin ve karşılıklı anlaşmalar yapın.
- Ulusal risk kayıt defterini güncelleyin ve toplanan bilgileri erken uyarı sistemleri vasıtasıyla uygun hedef kullanıcılara dağıtın.

EK-5. Stratejinin uygulanması



EK-6. Stratejinin değerlendirilmesi



EK-7. Türkiye'nin 2013-2014 siber güvenlik eylem planı

1. Yasal Düzenlemelerin Yapılması

- Siber Güvenlik Kurulunun Faaliyetlerine Başlaması
- Siber Güvenlik Konusunda Mevzuat Çalışmalarının Yapılması

2. Adli Süreçlere Yardımcı Olacak Çalışmaların Yürütülmesi

- Siber Olayların Delillendirilmesi

3. Ulusal Siber Olaylara Müdahale Organizasyonunun oluşturulması

- Ulusal Siber Olaylara Müdahale Merkezinin (USOM) Kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) Oluşturulması

4. Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi

- Kritik Altyapılarda Bilgi Güvenliği Yönetimi Programı
- Kamu Bilgi Güvenliği Programı
- Siber Güvenlik Eğitim Altyapısının Güçlendirilmesi
- Siber Güvenlik Tatbikatlarının Düzenlenmesi
- Kamu Güvenli İletişim Kurallarının Belirlenmesi
- Yazılım Güvenliği Programının Yürütülmesi
- Siber Tehditleri Önleme Projesinin Yürütülmesi
- Siber Güvenlik Konusunda Ürünlerin ve Hizmet Sağlayıcıların Belgelendirilmesi
- Adli Bilişim Konusunda Hizmet Sağlayıcılara Güvenlik Belgesi Verilmesine Yönelik Kuralların Belirlenmesi
- İş Sürekliliği ve Veri Yedekleme Sistemleri Kurulması
- Kamu Kurum ve Kuruluşlarının İnternet Sayfalarının Yerli Veri Merkezlerine Taşınması
- Veri Sızmasını Tespite Yönelik Test Altyapısı Geliştirilmesi ve Uygulamaya Alınması
- Kamu Kurumlarında Verilere Erişim Düzeylerinin Belirlenmesi
- Açık Kaynak Kodlu Ürünlerin Kullanımının Teşvik Edilmesi

5. Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi ve Bilinçlendirilme Faaliyetleri

- Siber Güvenlik Konusunda Akademisyen Yetiştirilmesi
- Üniversitelerde Siber Güvenlik Eğitiminin Yaygınlaştırılması
- Siber Güvenlik Uzmanlığına Yönlendirme Programının Yürütülmesi
- İlk, Orta, Lise Öğretimi ve Yaygın Eğitimde Siber Güvenlik Eğitimlerinin Yaygınlaştırılması
- Bilgisayar Kullanıcılarının Siber Güvenlik Konusunda Bilinçlendirilmesi
- Ulusal ve Uluslararası Siber Güvenlik Etkinlikleri Düzenlenmesi

6. Siber Güvenlikte Yerli teknolojilerin Geliştirilmesi

- Ar-Ge Faaliyetlerinin Teşvik Edilmesi
- Siber Güvenlik Konusunda AR-GE Laboratuvarlarının Kurulması
- Siber Güvenlikte Yerli Ürün ve Çözüm Çalışmaları
- Yerli Ürünlerin Teşvik Edilmesi

7. Ulusal Güvenlik Mekanizmalarının Kapsamının Genişletilmesi

- Ulusal Siber Güvenliğin Milli Güvenliğe Entegrasyonu

EK-8. Sorumlu kurumların alt eylem başlıklarına göre dağılımı

S.Nu.	Sorumlu Kuruluş	1.Yasal Düzenlemelerin Yapılması	2.Adli Süreçlere Yardımcı Olacak Çalışmaların Yürütülmesi	3.Ulusal Siber Olaylara Müdahale Organizasyonunun oluşturulması	4.Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi	5.Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi ve Bilinçlendirilme Faaliyetleri	6.Siber Güvenlikte Yerli teknolojilerin Geliştirilmesi	7.Ulusal Güvenlik Mekanizmalarının Kapsamının Genişletilmesi	TOPLAM
1	Adalet Bakanlığı	2			1				3
2	Bilim Sanayi ve Teknoloji Bakanlığı						1		1
3	Bilim ve Teknoloji Yüksek Kurulu						3		3
4	Bilgi Teknolojileri İletişim Kurumu					2			2
5	Kritik sektörleri denetlemekten sorumlu k.		1		5				6
6	İçişleri Bakanlığı		1			1			2
7	Milli Eğitim Bakanlığı					1			1
8	Siber Güvenlik Kurulu				2			3	5
9	Tüm Kamu Kurum ve Kuruluşları				1				1
10	TSE				1				1
11	Türk Dil Kurumu	1							1
12	TÜBİTAK				16	2	1		19
13	Ulaştırma Denizcilik ve Haberleşme Bakanlığı	2	1	3	16	2	1		25
14	USOM			4					4
15	YÖK					10	2		12
TOPLAM		5	3	7	42	18	8	3	86

EK-9. Türkiye'nin 2016-2019 siber güvenlik eylem planı

1. Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması

- Siber Güvenlik konusunda birincil mevzuat çalışmasının tamamlanması.
- Kurumsal SOME kurması gereken kamu kurumlarında siber güvenlik bütçesinin oluşturulması.
- SOME'lerde çalışan siber güvenlik personelinin iş tanımlarının belirlenmesi.
- ISO 27001 Bilgi Güvenliği Yönetim Sistemi standardının kamu kurumları ve kritik altyapı sektörlerindeki özel işletmeciler için zorunlu hale getirilmesi.
- Siber güvenlik konusunda güvenlik testi yapan (sızma testi, APT vb.), gerçek ve tüzel kişilerin belgelendirilmesi.
- Güvenlik testi (sızma testi, APT analizi vb.) hizmetlerinin belge sahibi gerçek ve tüzel kişilerden alınacağını belirtmesi konusunda kurumların mevzuatlarını güncellemesi.
- Kurumlarda sızma testlerinin zorunlu hale getirilmesi.
- Ulusal Siber Güvenlik Yönetim Süreci.
- Kamu ve kritik altyapı sistem odalarının sahip olması gereken asgari kriterler.
- Kurumlar arası bilgi/veri paylaşımı esnasındaki iletişim güvenliğinin sağlanmasına yönelik güvenlik esaslarının oluşturulması.

2. Siber Suçlarla Mücadele

- Detaylı ve gerçekçi durum analizinin yapılması.
- Siber suçlar ile ilgili ceza ve muhakeme mevzuatının düzenlenmesi.
- Güvenli IPv6 kullanımının yaygınlaştırılması.
- İDN'ye ilişkin mevzuat ve kurulum çalışmalarının tamamlanması.
- Milli adli analiz kapasitesinin geliştirilmesi.
- Adli analiz uzman havuzu oluşturulması ve kriterlerinin belirlenmesi.
- Siber suçları tespit için büyük veri analizi altyapısının kurulması.

3. Farkındalık ve İnsan Kaynağı Geliştirme

- Siber güvenlik terimleri sözlüğünün oluşturulması.
- İlk, orta, lise öğretimi ve yaygın eğitimde siber güvenlik eğitimlerinin yaygınlaştırılması.
- Siber güvenlik yaz kampları ve yarışmalarının düzenlenmesi.
- Siber güvenlik tatbikatlarının düzenlenmesi.
- Ulusal ve uluslararası siber güvenlik tatbikatlarının düzenlenmesi.
- Siber güvenlik alanında uluslararası işbirliğinin güçlendirilmesi.
- Kurumlarda siber güvenlik ve SOME'lerin faaliyet alanlarının önemi konusunda üst düzey yöneticilerin farkındalığının artırılması.
- Bilişim hukukçusu yetiştirilmesi.
- Hâkim ve savcılara siber güvenlik, siber suçlar ve bilişim hukuku konularında eğitimlerin verilmesi.
- Siber güvenlik farkındalığı kamu spotlarının oluşturulması.
- Siber güvenlik uzmanı eğitim içeriklerinin oluşturulması.
- Siber güvenlik alanında ileri teknolojilerin kazanımı için yüksek lisans ve doktora düzeyinde siber güvenlik ders içeriklerinin oluşturulması.

4. Siber Güvenlik Ekosisteminin Geliştirilmesi

- Siber güvenlik ekosistemi ulusal iş modelinin oluşturulması.
- Siber güvenlik teknoloji yol haritasının ve araştırma gruplarının oluşturulması.
- Siber güvenlikle ilgili yerli teknoloji ve ürünlerin desteklenmesi.
- "Güvenli yazılım geliştirme ve güvenli yazılım kullanımı" kültürünün yaygınlaştırılması.
- Pardus'un yaygınlaştırılması.
- Laboratuvar/test yatağı altyapısının kurulması.
- Kritik siber güvenlik teknolojilerinin kazanımı.
- Siber güvenlik alanında hizmet veren firma envanterinin çıkarılması.
- Kritik ürünleri denetleyecek ve sertifikalandıracak mekanizmaların çalıştırılması.
- Ulusal Siber Güvenlik Portalının oluşturulması.

5. Siber Güvenliğin Milli Güvenliğe Entegrasyonu (2 adet alt eylem maddesi içermektedir.)

EK-10. Sorumlu kurumların alt eylem başlıklarına göre dağılımı

S.Nu.	Sorumlu Kuruluş	1. Siber Savunmanın Güçlendirilmesi ve Kritik Altyapılarının Korunması	2.Siber Suçlarla Mücadele	3.Farkındalık ve İnsan Kaynağı Geliştirme	4.Farkındalık ve İnsan Kaynağı Geliştirme	5.Siber Güvenliğin Millî Güvenliğe Entegrasyonu	TOPLAM
1	Adalet Bakanlığı	1	2	1			4
2	Bilim Sanayi ve Teknoloji Bakanlığı				3		3
3	BTK		1				1
4	EGM		1				1
5	Maliye Bakanlığı	1					1
6	Millî Eğitim Bakanlığı			1			1
7	Sektörel SOME'ler		1	1			2
8	TSE	2					2
9	TÜBİTAK		1	2	4		7
10	Tüm Bakanlıklar, Düzenleyici ve Denetleyici Kurumlar	3			1		4
11	Ulaştırma Denizcilik ve Haberleşme Bakanlığı	3	1	5	2	2	13
12	YÖK			2			2
TOPLAM		10	7	12	10	2	41

EK-11. Ulusal siber güvenlik strateji planı ve koordinatör makamı açısından incelenmesi

Ülkeler	Ulusal Siber Güvenlik Stratejisi Mevcut Mu?	Koordinatör Makam (Bakanlık Seviyesinde)	Tarih Aralığı	Kaynak
 AL	✗	✗	✗	✗
 BE	✓	İçişleri Bakanlığı	2012-...	[88]
 BG	✗	✗	✗	✗
 CA	✓	Kamu Güvenliği Bakanlığı	2010-...	[89]
 CZ	✓	İçişleri Bakanlığı	2011-...	[90]
 DE	✓	İçişleri Bakanlığı	2011-...	[91]
 DK	✗	✗	✗	✗
 EE	✓	Savunma Bakanlığı Ekonomik İşler ve Haberleşme Bakanlığı	2009-2011 2011-...	[92]
 ES	✓	İçişleri Bakanlığı	2011-...	[93]
 FR	✓	Dışişleri ve Uluslararası Kalkınma Bakanlığı	2011- ...	[94]
 GR	✓	Altyapı, Ulaştırma ve Ağlar Bakanlığı	2015-...	[95]
 HR	✗	✗	✗	✗
 HU	✓	İçişleri Bakanlığı	2013-...	[96]
 IS	✗	✗	✗	✗
 IT	✓	Başbakanlık Askeri Müşavirliğinde Kurulan Siber Güvenlik Birimi	2013-...	[97]
 LT	✓	Savunma Bakanlığı	2011-...	[98]
 LU	✓	Ekonomi ve Dış Ticaret Bakanlığı	2013	[99]
 LV	✓	Savunma Bakanlığı	2014-...	[100]
 NL	✓	Güvenlik ve Adalet Bakanlığı	2011-...	[101]
 NO	✗	✗	✗	✗
 PL	✓	İdare ve Dijitalleştirme Bakanlığı	2013-...	[102]
 PT	ⓘ	ⓘ	✗	✗
 RO	✓	İletişim ve Bilgi Toplumu Bakanlığı	2013-...	[103]
 SK	✓	Maliye Bakanlığı	2009-...	[104]
 SL	✗	✗	✗	✗

EK-11.(devam) Ulusal siber güvenlik strateji planı ve koordinatör makamı açısından incelenmesi

	TR		Ulaştırma, Denizcilik ve Haberleşme Bakanlığı	2013-...	[85]
	UK		Başbakanlığa bağlı Milli Güvenlik Sekreterliği	2011	[105]
	US		İç Güvenlik Bakanlığı	2003-...	[106]

EK-12. Bilgisayar olaylarına müdahale ekipleri (CERT) açısından incelenmesi

ÜLKELER		FIRST Üyesi Kurumsal CERT Durumu [108]				FIRST Üyesi	FIRST Üyesi
		Sayı	İsim	Açıklama	Kuruluş Tarihi	Sektörel CERT Sayısı	Toplam CERT Sayısı
	BE	3	BELNET CERT CERT-EU NCIRC-CC	Ulusal BOME (Belçika Araştırma ve Eğitim Ağı) AB BOME NATO BOME	2004 2011 2004	2	5
	CA	2	CCIRC CANCERT	Kanada Siber Olay Tepki Merkezi Kanada Ulusal BOME	2003 1998	10	12
	CZ	2	CSIRT.CZ GovCERT.CZ	Çek Cumhuriyeti Ulusal BOME Çek Cumhuriyeti Hükümeti BOME	2008 2012	0	2
	DE	3	CERT-Bund KIT-CERT RUS-CERT	Bilgi Güvenliği Federal Dairesi BOME Karlsruhe Teknoloji Enstitüsü BOME Stuttgart Üniversitesi BOME	2012 2008 1998	23	26
	EE	1	CERT-EE	Ulusal BOME (Estonya Bilişim Merkezi)	2006	0	1
	ES	4	CCN-CERT CERTSI CESISAT-CERT esCERT-UPC	Hükümet Ulusal Kripto Merkezi BOME Ulusal Güvenlik ve Sanayi BOME Katalonya Bilgi Güvenliği Merkezi CERT Katalonya Politeknik Üniversitesi BOME	2006 2007 2010 1994	10	14
	FR	1	CERT-FR	Ulusal BOME	2004	10	11
	GR	1	FORTHcert	Araştırma ve Teknoloji Vakfı BOME	2007	0	1
	HU	1	CERT-Hungary	Ulusal BOME	2013	0	1
	IT	1	PI-CERT	İtalyan Posta İdaresi BOME	2013	1	2
	LT	2	CERT-LT LTU MOD CIRT	Ulusal BOME (İletişim Düzenleme Kurumu) Savunma Bakanlığı BOME	2006 2009	3	5
	LV	1	CERT.LV	Ulusal BOME (Mat. Ve Bilg. Bil. Enst.)	2006	0	1
	NL	2	DefCERT NCSC-NL	Savunma Bakanlığı BOME Ulusal Siber Güvenlik Merkezi BOME	2010 2002	7	9
	PL	1	CERT POLSKA	Ulusal BOME (Akademik Bilgi Ağı)	1996	1	2
	RO	2	CERT-RO RoCSIRT	Ulusal BOME Ulusal Eğitim Ajansı BOME	2011 2008	1	3
	SK	1	CSIRT.SK	Ulusal BOME (Maliye Bakanlığı)	2009	0	1
	TR	1	TR-CERT	Ulusal BOME (Bilgi Teknolojileri Kurumu)	2013	0	1
	UK	2	CERT.UK WAR-CSIIRT	Ulusal Siber Güvenlik Merkezi BOME Warwick Üniversitesi BOME	2007 2009	13	15
	US	3	CERT/CC JC3-CIRC US_CERT	BOME Koordinasyon Merkezi Enerji Dep. Siber Guv. Koor.Merkezi Ulusal BOME	1984 2008 2003	75	78

EK-13. Uluslararası işbirliği açısından incelenmesi

ÜLKELER		CCDCOE [66]		ENISA [109]		ITU [110]	
		Katılım Durumu	Katılım Tarihi	Katılım Durumu	Katılım Tarihi	Katılım Durumu	Katılım Tarihi
	BE	✗	✗	✓	01.09.2005	✓	01.01.1866
	CA	✗	✗	✗	✗	✓	01.07.1908
	CZ	✓	03.06.2014	✓	01.09.2005	✓	01.01.1993
	DE	✓	14.05.2008	✓	01.09.2005	✓	01.01.1866
	EE	✓	14.05.2008	✓	01.09.2005	✓	22.04.1992
	ES	✓	14.05.2008	✓	01.09.2005	✓	01.01.1866
	FR	✓	03.06.2014	✓	01.09.2005	✓	01.01.1866
	GR	✓	03.11.2015	✓	01.09.2005	✓	01.01.1866
	HU	✓	23.06.2010	✓	01.09.2005	✓	01.01.1866
	IT	✓	14.05.2008	✓	01.09.2005	✓	01.01.1866
	LT	✓	14.05.2008	✓	01.09.2005	✓	12.10.1991
	LV	✓	14.05.2008	✓	01.09.2005	✓	11.11.1991
	NL	✗	✗	✓	01.09.2005	✓	01.01.1866
	PL	✓	16.11.2011	✓	01.09.2005	✓	01.01.1921
	RO	✗	✗	✓	01.01.2007	✓	09.02.1866
	SK	✓	14.05.2008	✓	01.09.2005	✓	23.02.1993
	TR	✓	03.11.2015	✗	✗	✓	01.01.1866
	UK	✓	03.06.2014	✓	01.09.2005	✓	24.02.1871
	US	✓	16.11.2011	✗	✗	✓	01.07.1908

EK-14. Ulusal Siber güvenlik eylem maddeleri açısından incelenmesi

ÜLKELER		REFERANS DOKÜMAN	TOPLAM EYLEM MADDESİ	STRATEJİK EYLEM MADDELERİ
	CA	Action Plan 2010-2015 for Canada's Cyber Security Strategy (Kanada'nın Siber Güvenlik Stratejisi için 2010-2015 Eylem Planı) Yıl: 2013 [111]	3	1. Devlet sistemleri güvenliğinin sağlanması 2. Hayati siber sistemlerin güvenliğinin sağlanması için Federal Hükümet dışında ortaklıklar kurulması 3. Kanada vatandaşlarının çevrimiçi ortamda güvenliğinin sağlanması
	DE	Cyber Security Strategy for Germany (Almanya için Siber Güvenlik Stratejisi) Yıl: 2011 [112]	10	1. Kritik bilgi altyapılarının korunması 2. Almanya'daki BT sistemlerinin güvenli hale getirilmesi 3. Kamu yönetiminde BT güvenliğinin güçlendirilmesi 4. Ulusal Siber Müdahale Merkezi'nin geliştirilmesi 5. Ulusal Siber Güvenlik Konseyi'nin tanımlanması 6. Siber alanda gerçekleşen suçların kontrol altına alınması 7. Siber güvenliğin sağlanması konusunda Avrupa ve Dünya ile uyumlu hale gelinmesi 8. Güvenilir ve emniyetli bilgi teknolojisinin kullanılması 9. Federal makamlarda kişisel gelişimin sağlanması 10. Siber saldırılara tepki veren araçların geliştirilmesi ve kullanılması
	ES	National Cyber Security Strategy (Ulusal Siber Güvenlik Stratejisi) Yıl: 2013 [113]	8	1. Siber tehditleri önleme, teşhis etme, bunlara cevap verme becerisinin artırılması 2. Kamu makamlarını destekleyen Bilgi ve Telekomünikasyon sistemlerinin güvenliği konusunda düzenlemeler yapılması 3. Kritik altyapıları destekleyen Bilişim ve Telekomünikasyon sistemlerinin güvenliği konusunda düzenlemeler yapılması 4. Siber terörizm ve siber suçları soruşturma ve kovuşturma yeteneğinin geliştirilmesi 5. Özel sektördeki BİT'nin güvenliği ve direncinin artırılması 6. Bilgi, beceri ve AR-GE faaliyetlerinin güçlendirilmesi 7. Toplumda siber güvenlik kültürü oluşturulması 8. Uluslararası siber güvenlik faaliyetlerinin teşvik edilmesi

EK-14.(devam) Ulusal Siber güvenlik eylem maddeleri açısından incelenmesi

	FR	French National Digital Security Strategy (Fransız Ulusal Dijital Güvenlik Stratejisi) Yıl: 2015 [114]	5	1. Siber alanda temel çıkarlar doğrultusunda güvenliğin sağlanması ve kritik altyapılarının sayısal güvenliğini güçlendirilmesi 2. Dijital ortamda gizlilik, kişisel verilerin mahremiyeti ve siber sorumluluklar konusunda siber alan kullanımının geliştirilmesi ve sayısal hayatların korunması 3. İlköğretim ve devamındaki eğitimde çocukların siber güvenlik farkındalığının artırılması 4. Dijital teknoloji işletmeleri, endüstriyel politika, ihracat ve uluslararası ticaret konularında güvenlik ve rekabet faktörleri göz önüne alınarak araştırma ve inovasyona elverişli ortamlar oluşturulması 5. Gönüllü Üye Ülkelerle birlikte Avrupa stratejik ortaklığın desteklenmesi, istikrarlı ve güvenilir siber alanın oluşturulması
	IT	The National Plan For Cyberspace Protection and ICT Security (Siber Koruma ve Bilgi Paylaşımı Güvenliği İçin Ulusal Plan) Yıl: 2013 [115]	11	1. İstihbarat, polis, askeri savunma yeteneklerinin güçlendirilmesi 2. Ulusal çapta özel ve kamusal paydaşlar arasındaki örgütlenme ve koordinasyonun artırılması 3. Eğitim-Öğretim 'de siber güvenlik kültürünün oluşturulması ve yaygınlaştırılması. 4. Uluslararası işbirliği ve çalışmaların artırılması 5. Ulusal CERT makamlarının tam operasyonel kabiliyete ulaştırılması 6. Geçici yasal düzenlemelerin teşvik edilmesi ve uluslararası yükümlülükler uyulması. 7. Güvenlik standartlarına ve protokollere uyulması 8. Endüstriyel ve teknolojik gelişmenin desteklenmesi 9. Etkili bir iletişimin kurulması için bilgi içeriğine ve uyarılara karşı farkındalığın geliştirilmesi 10. Siber güvenlik tedbirleri konusunda önceliklerin belirlenmesi ve ekonomik faktörlerin değerlendirilmesi 11. Ulusal çapta paylaşılan bilgilerin önem derecelerine göre değerlendirilmesi ve risk yönetim mekanizmasının kurulması.

EK-14.(devam) Ulusal Siber güvenlik eylem maddeleri açısından incelenmesi

	PL	Cyberspace Protection Policy Of The Republic Of Poland (Polonya Cumhuriyeti Siberuzay Koruma Politikası) Yıl: 2013 [116]	7	1. Devlet bilgi ve iletişim teknolojileri altyapısının güvenliğinin artırılması 2. Siber uzaydan gelen tehditleri önleme ve mücadele etme kapasitesinin geliştirilmesi 3. BİT güvenliğini tehdit eden olayların etkisinin azaltılması 4. Siber güvenlikten sorumlu kurumların yetkinliklerinin belirlenmesi 5. Devlet yönetim birimleri için siber güvenlik yönetiminin tutarlı bir sisteminin oluşturulması, uygulanması ve bu alanda devlet dışı aktörler için yönergeler oluşturulması 6. Siber güvenlikten sorumlu kurumlar ile kullanıcılar arasında koordinasyon ve bilgi paylaşımı için sürdürülebilir bir sistem oluşturulması 7. Siber ortamdaki yöntem ve güvenlik önlemleri konusunda kullanıcılarda farkındalık oluşturulması
	TR	2016-2019 Ulusal Siber Güvenlik Eylem Planı Yıl: 2016 [117]	5	1. Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması 2. Siber Suçlarla Mücadele 3. Farkındalık ve İnsan Kaynağı Geliştirme 4. Siber Güvenlik Ekosisteminin Geliştirilmesi 5. Siber Güvenliğin Milli Güvenliğe Entegrasyonu
	UK	The UK Cyber Security Strategy (Birleşik Krallık Siber Güvenlik Stratejisi) Yıl: 2011 [118]	4	1. Siber suçlarla mücadele etme ve siber alanda iş yapma konusunda İngiltere'nin dünyanın en güvenli yerlerinden biri yapılması 2. Siber saldırılara karşı daha dayanıklılığın artırılması ve siber alandaki çıkarların korunması yönünde çalışmalar yapılması 3. Halkın güvenle kullanabileceği, açık toplumları destekleyen, istikrarlı ve canlı bir siber alanın oluşturulması 4. Siber güvenlik hedeflerinin desteklenmesi için ihtiyaç olunan bilgi, beceri ve kabiliyete erişilmesi
	US	Cyberspace Policy Review (Siber Alan Politika İncelemesi) Yıl:2009 [119]	14	1. Kanunların yorumlanması ve siber güvenlik operasyonlarının uygulanması arasındaki anlaşmazlıkların giderilmesi 2. Siber güvenlik hedeflerini gerçekleştirirken bütçe planlaması kapsamında OMB (Office of Management and Budget) program değerlendirme çerçevesi kullanılmasının teşvik edilmesi

				3. Ulusal eğitimde, temel eğitim programlarına ve araştırma ve geliştirmeye verilecek desteğin genişletilmesi 4. Federal hükümette siber güvenlik uzmanlığı konusunda işgücünün genişletilmesi ve çalışanların eğitim seviyesinin artırılması için stratejilerin geliştirilmesi 5. Durumsal farkındalığı korumak, stratejik uyarılar almak ve olaylarla mücadele yeteneklerini bildirmek maksadıyla etkili mekanizmaların belirlenmesi 6. Risk yönetimi kararları, iyileştirme planlaması ve Ar-Ge'nin önceliklendirilmesi için kullanılabilecek bir dizi tehdit senaryosunun geliştirilmesi 7. Siber olayları önleme, tespit etme ve bunlara tepki vermeye yardımcı olmak için hükümet ve özel sektör arasında süreç geliştirilmesi 8. Gizlilik ve mülkiyet bilgileri ile ilgili endişeleri gidermek ve karşılıklı yarar sağlayan bilgi paylaşımını sağlamak için siber güvenlikle ilgili bilgi paylaşım mekanizmalarının geliştirilmesi 9. Doğal afet, kriz veya çatışma gibi durumlarda ağ tarafsızlığı sağlayan acil durum iletişimi yeteneklerinin geliştirilmesi 10. Ağ olayları ve güvenlik açıklarıyla ilgili bilgilerin önemli müttefiklerle paylaşımının artırılması ve sivil özgürlükleri ve gizlilik haklarını koruyacak ikili ve çok taraflı düzenlemelerin yapılması 11. Araştırma ve teknoloji geliştirme yeniliklerinin hızla benimsenmesi için akademik ve endüstriyel laboratuvarlar arasındaki işbirliğinin geliştirilmesi 12. Ulusal ve uluslararası standartlar kapsamında hedefler belirlemek için Ar-Ge faaliyetlerinin geliştirilmesi 13. Çevrimiçi işlemlerde güven oluşturmak ve gizliliği artırmak için kimlik yönetim sistemlerinin etkin kullanılması 14. Devlet satın alma stratejilerinin hassaslaştırılması ve güvenli, esnek donanım ve yazılım ürünlerinin temin edilmesi
--	--	--	--	---

EK-15. Kişisel verilerin gizliliği kapsamındaki düzenlemeler açısından incelenmesi

ÜLKELER	1. Kişisel bilgilerin toplanması, kullanılması veya işlenmesi ile ilgili yasalar veya yönetmelikler mevcut mudur?		2. Gizlilik yasalarının yürütülmesi ile ilgili olarak görevlendirilen bir kurum var mıdır?		3. Kişisel verilerle işlem yapanlar kayıt tutma zorunluluğundan muaf mıdır?		4. Sınır ötesi bilgi aktarımları kayıt tutma zorunluluğundan muaf mıdır?		5. İhlal bildirimi ile ilgili bir yasa var mıdır?	
		Açıklama		Açıklama		Açıklama		Açıklama		Açıklama
 CA [125]	✓	Kişisel Bilgilerin Korunması ve Elektronik Belgeler Yasası (PIPEDA - 2000). 2015 yılında Dijital Gizlilik Yasası ile güncellendi.	✓	Kanada Gizlilik Komiseri Ofisi (OPCC) ulusal düzenleyici görevi görür.	✓	Kanada gizlilik yasasında kayıt tutma zorunluluğu bulunmamaktadır.	✓	Kayıt tutma zorunluluğu yoktur. Ancak, verilerin sınır ötesine aktarımı için PIPEDA'da belirli kurallar vardır.	✓	Dijital Gizlilik Yasası (2015) ile ihlal bildirim şartı getirildi.
 DE [126]	✓	Federal Kişisel Verilerin Korunması Yasası (2001)	✓	16 adet gizlilik otoritesi sektörel seviyede düzenleyici görevi görür.	ⓘ	Çoğu veri işleme faaliyetinde kayıt tutma zorunluluğu bulunmaktadır. Ancak kayıtlı veri koruma görevlisi bulunan yerde muafiyet uygulanmaktadır.	✓	Kuruluşlar, yalnızca yeterli bir koruma seviyesi sağlıyorsa AB dışı ülkelere veri aktarabilirler.	ⓘ	Mesleki sırlara giren veriler, ceza veya idari suçlarla ilgili veriler ve banka/kredi kartı hesapları gibi verilerde ihlal oluşursa bildirimde bulunmalıdır.
 ES [127]	✓	Kişisel Verilerin Korunması Kanunu (1999). 2009 ve 2010 yıllarında güncellendi.	✓	İspanya Veri Koruma Ajansı ulusal düzenleyici olarak görev yapar.	✗	Muafiyet bulunmamaktadır. İspanya Veri Koruma Ajansı kişisel veriler için veritabanı bulundurmaktadır.	✗	AB ülkeleri haricinde muafiyet bulunmamaktadır. Veri Koruma Direktörü koordinatörlüğünde prosedürün işleyişi yasanın 33'üncü maddesinde açıklanmıştır.	ⓘ	Sınırlı düzenleme mevcuttur. AB'nin 611/2013 numaralı yönetmeliğine göre, servis sağlayıcıların veri ihlallerini çevrimiçi bildirim formu ile 24 saat içinde bildirmeleri gerek.
 FR [128]	✓	Veri İşleme Yasası (1978). 2004 yılında Özel Bilginin İşlenmesi kapsamında Kişilerin Korunmasına ilişkin kanunla revize edildi.	✓	Ulusal Bilgisayar Bilimleri ve Özgürlükleri Komisyonu kişisel verilerin korunmasından sorumlu bağımsız bir kurumdur.	✗	Muafiyet bulunmamaktadır. Veri İşleme Yasasının 4'üncü bölümü veri işleme ile ilgili formaliteleri belirler.	✗	Veri İşleme Yasasının 23'üncü maddesi sınır ötesi işlemler ile ilgili düzenlemeleri belirler.	ⓘ	Sınırlı düzenleme mevcuttur. 2011-1012 sayılı yönergesi ve AB'nin 611/2013 numaralı yönetmeliği ile ihlal bildirimi düzenlenmiştir.
 IT [129]	✓	Veri Koruma Kanunu (2003)	✓	İtalyan Veri Koruma Kurumu ulusal düzenleyicidir.	✗	Muafiyet bulunmamaktadır. Sağlık verileri, kredi uygunluğu, yer verileri, genetik bilgi, pazar araştırması verileri gibi verilerin aktarımı için İtalyan Veri Koruma birimine bildirim yapılması gerekir	✓	AB Ülkeleri ve Veri Koruma Kurumu tarafından listelenen ülkelere veri aktarılabilir.	ⓘ	Sınırlı. Veri Koruma Kanunu ve AB'nin 611/2013 numaralı yönetmeliği ile ihlal bildirimi düzenlenmiştir.

EK-15.(devam) Kişisel verilerin gizliliği kapsamındaki düzenlemeler açısından incelenmesi

	PL [130]	✓	Kişisel Veri Koruma Yasası (1997). 2003 ve 2004 yıllarında güncellendi.	✓	Kişisel Veri Koruması Genel Müfettişi ulusal düzenleyicidir.	🕒	Yasa gereği veri denetleyicisi, müfettişliğe kayıt için bildirim yapmakla mükelleftir.	✓	Kişisel Veri Koruma Yasasına göre listelenen şartları yerine ülkelere sınır ötesi veri aktarımı yapılabilir.	🕒	Sınırlı. AB'nin 611/2013 numaralı yönetmeliği ile ihlal bildirimi düzenlenmiştir.
	TR [131]	✓	Kanun tasarısı 2014 yılında Meclise gönderildi ve 24.03.2016 tarihinde yasalaştı.	✓	Kanun taslağında Kişisel Verileri Koruma Kurumu oluşturulması teklifi bulunmaktadır.	✓	Kayıt tutma zorunluluğu yoktur.	✓	Sınır ötesi veri aktarımı ile ilgili bir kısıtlama yoktur.	✗	Türkiye'de veri ihlali bildirimi konusunda bir yasa bulunmamaktadır.
	UK [132]	✓	Veri Koruma Kanunu (1998). Bir çok kez güncellendi.	✓	Bilgi Komisyon Bürosu (ICO) ulusal düzenleyicidir	✗	Veri denetçileri tarafından ICO'nun bilgilendirilmesi gerekmektedir. Muafiyet için az sayıda istisna mevcuttur.	✓	Veri Koruma Kanunu ile belirlenen şartlar ile sınır ötesi veri aktarımı yapılabilir.	🕒	Bir düzenleme bulunmamaktadır. Ancak ICO, organizasyonları ciddi ihlalleri bildirmesi konusunda uyarmıştır.
	US [133]	🕒	Gizlilik yasası bulunmamaktadır. Ancak, Sağlık ve finans sektörü gibi bazı sektörler için gizlilik yükümlülüklerini yerine getirmek için sektörel yasalar mevcuttur.	✓	Federal Ticaret Komisyonu (FTC), Federal İletişim Komisyonu (FCC) gibi organizasyonlar federal ve sektörel olarak gizlilik gözetim rolüne sahiptir.	✓	Kayıt tutma zorunluluğu yoktur.	🕒	Verilerin sınır ötesine aktarımı ile ilgili sınırlama yoktur. Ancak, sınır ötesi aktarmaların kontrol edilmesini teşvik eden kuruluşlar tarafından uygulanan prosedürler mevcuttur.	✓	Çok sayıda ve tutarlı olmayan veri ihlali bildirim yasası mevcuttur. Yasalarla düzenlenen düzenleyici birimler veri ihlali olması durumunda bildirimde bulunur.

EK-16. Kişisel ve kurumsal güvenliğin geliştirilmesini sağlayan düzenlemeler açısından incelenmesi

ÜLKELER	1. Elektronik imzaya net bir yasal geçerlilik kazandıran bir yasa veya düzenleme var mıdır?		2. İnternet Hizmet Sağlayıcılar (ISP) ve içerik hizmet sağlayıcılar filtreleme veya sansür zorunluluğundan muaf mıdır?		3. Dijital veri barındırma ve bulut hizmeti sağlayıcılar konularında genel güvenlik şartlarını içeren kanunlar veya hükümler mevcut mudur?		4. Dijital veri barındırma ve bulut hizmeti sağlayıcılar konularında özel güvenlik denetimi şartlarını içeren kanunlar veya hükümler mevcut mudur?		5. Teknolojik ürünler için belirli sertifikasyonları zorunlu tutan güvenlik yasaları ve düzenlemeleri var mıdır?	
		Açıklama		Açıklama		Açıklama		Açıklama		Açıklama
 CA [127]	✓	Kanada Düzensiz Elektronik Ticaret Yasası (UECA -1999). 2005 yılında yayımlanan Güvenli Elektronik İmza Tüzüğü dijital imzalar için ek kurallar içermektedir.	✓	İnternet içeriğine sansür uygulanmaz. ISS'ları isteğe bağlı çocuk pornografisi içeriklerine filtre uygular. Zorunluluk yoktur.	✗	Kanada, bulut bilişim güvenliği konusunda herhangi bir resmi yönerge, standart veya yönetmelik çıkarmamıştır.	●	Devlet kurumları için bilgi güvenliği ile ilgili çeşitli düzenlemeler mevcuttur. Ancak, bulut bilişim ve dijital veri barındırma denetimleri kapsamında kurallar içermemektedir.	✓	Ortak Kriterler Tanıma Sözleşmesi (CCRA) nezdinde sertifika otoritesidir.
 DE [128]	✓	Dijital İmza Yasası (2001)	●	Soykırım ve Katliam gibi spesifik içeriklerle ilgili ciddi sansür yasaları mevcuttur.	●	Veri koruma yasası, kuruluşların, bilgilerin güvenliğini sağlamak için teknik ve organizasyonel önlemler almaları gerektiğini belirtmektedir.	✗	Parlamento tarafından defalarca önerilmesine rağmen, herhangi bir güvenlik denetim şartı bulunmamaktadır.	✓	Almanya, Ortak Kriterler Tanıma Sözleşmesi (CCRA) nezdinde sertifika yetkilendirme üyesidir (en üst düzey üyelik).
 ES [129]	✓	Elektronik İmzalar Yasası (2003)	✓	İnternet içeriğine sansür uygulanmaz. Ancak yasalar ayrımcılık, nefret ve şiddeti teşvik eden materyallerin internet aracılığıyla yayılmasını yasaklamaktadır.	●	Verilerin mahremiyet konusunda sınırlı güvenlik tedbirleri mevcuttur.	✗	İspanya'da uygulanan herhangi bir güvenlik denetimi şartı yoktur.	✓	Almanya, Ortak Kriterler Tanıma Sözleşmesi (CCRA) nezdinde sertifika yetkilendirme üyesidir (en üst düzey üyelik).
 FR [130]	✓	Elektronik İmzalar Kanunu (2000)	●	Dijital Ekonomi Güvenliği Yasası (LCEN) gereği ISS'ları tarafından Çocuk pornografisi ve hükümet kara listesinde bulunan web sitelerine sansür uygulanmaktadır.	●	Veri İşleme Yasası'nın 34. Maddesi, verilerin güvenliğini korumak ve üçüncü şahıslar tarafından erişilmesini önlemek amacıyla, kuruluşların verilerin niteliğine göre gereken tüm güvenlik önlemlerini almalarını gerektirir.	●	2011-1012 Sayılı Yönerge gereği İSS'ları güvenlik denetimlerinden hükümete karşı sorumludur. Denetim maliyeti İSS'ları tarafından karşılanmaktadır.	✓	Fransa, Ortak Kriterler Tanıma Sözleşmesi (CCRA) nezdinde sertifika yetkilendirme üyesidir (en üst düzey üyelik).

EK-16.(devam) Kişisel ve kurumsal güvenliğin geliştirilmesini sağlayan düzenlemeler açısından incelenmesi

	IT [131]	✓	30 Ocak 2002 tarihli Elektronik İmzalar Hakkında Kanun Hükmünde Kararname	🔄	29 Ocak 2007 tarihli İnternet üzerindeki Çocuk Pornografisi ile Mücadele Kararnamesi İSS'ların çocuk pornografisi web sitelerine erişimi engellemesini şart koşturmuştur.	✓	İtalyan Veri Koruma Kanunu (2003), kullanıcı kimlik doğrulaması ve güvenlik duvarları için gereksinimler gibi konularda detaylı güvenlik önlemlerini kapsamaktadır.	🔄	Veri Koruma Kanunu (2003), denetim gereksinimlerini içermez. Ancak, denetim çerçevesini içerecek güvenlik risk yönetimini ve uyumluluklarını belirler.	✓	Türkiye, 2010 yılında Ortak Kriterler Tanıma Sözleşmesi (CCRA) nezdinde sertifika yetkilendirme üyesi olarak kabul edildi (en üst düzey üyelik).
	PL [132]	✓	Elektronik İmzalar Kanunu (2001)	✓	İnternet sansür yasası 2011 yılında önerildi ancak protestolar sonrasında öneri kabul edilmedi.	✓	Girişimciliği teşvik etmek için yayımlanan Ekonomik Faaliyeti Kolaylaştırma Yasası (2015) şirketlere veri koruma denetimleri zorunlu kılar.	🔄	Ekonomik Faaliyeti Kolaylaştırma Yasası gereğince şirketler güvenlik denetimlerini vermeye mecburdur. Kişisel Veri Koruma Müfettişi bu denetimlerin kurallarını belirler. Denetimler en az yılda bir kez yapılır.	🔄	Ortak Kriterler Tanıma Sözleşmesi (CCRA) üyesi değildir. Ancak, Polonya İç Güvenlik Ajansı (ABW), yüksek standartlara uygun BT ürünleri için güvenlik sertifikaları verir.
	TR [133]	✓	5070 sayılı Elektronik İmza Kanunu (2004).	✗	Sitelere erişim, 5651/2007 sayılı İnternet Yasasına çeşitli nedenlerden dolayı engellenebilmektedir. 2014 yılında güncellendi.	✗	Türkiye'de dijital veri barındırma ile ilgili uygulanan herhangi bir zorunlu güvenlik şartı yoktur.	✗	Türkiye'de uygulanan herhangi bir güvenlik denetimi şartı yoktur.	✓	Türkiye, 2010 yılında Ortak Kriterler Tanıma Sözleşmesi (CCRA) nezdinde sertifika üretici ülke olarak kabul edildi (en üst düzey üyelik). Türkiye'de teknolojik ürünlerde sertifikasyon kullanımı düşüktür, ancak artmaktadır.
	UK [134]	✓	Elektronik Haberleşme Yasası (2000). 2002 yılında Elektronik İmza Düzenlemeleri ile 1999/93/EC sayılı Avrupa Yönergesi yürürlüğe konulmuştur.	✓	İngiltere'de içeriğin filtrelenmesi zorunlu değildir. Ancak İSS'lerinin çoğunluğu pornografi, uyuşturucu kullanımı, intihar, şiddet ve hack faaliyetleri gibi bir dizi konuyla ilgili içeriği gönüllü olarak filtrelemektedir.	🔄	Veri Koruma Yasası, kuruluşların kişisel verileri hırsızlığa, yetkisiz erişime veya kazara kaybına karşı korunmasını temin etmeyi zorunlu kılar.	🔄	İngiltere'de sadece finans sektöründe güvenlik denetim zorunluluğu vardır. Bununla birlikte, Bilgi Komisyon Bürosu (ICO), güvenlik denetimlerinin yapılmasını şiddetle tavsiye eder.	✓	Birleşik Krallık, Ortak Kriterler Tanıma Sözleşmesi (CCRA) nezdinde sertifika yetkilendirme üyesidir (en üst düzey üyelik).

EK-16.(devam) Kişisel ve kurumsal güvenliğin geliştirilmesini sağlayan düzenlemeler açısından incelenmesi

	US [135]		Elektronik İşlemler Yasası (1999). 2000 tarihli Küresel ve Ulusal Ticaret Yasasındaki Elektronik İmzalar (ESIGN) Yasası, elektronik imzaların tanınması için daha ayrıntılı bir yasal çerçeve sunmaktadır.		ABD yasalarında İnternet içerik filtreleme zorunluğu yoktur.		ABD yasalarında genel bir güvenlik şartı bulunmamaktadır. Bununla birlikte, sadece California Eyaleti kişisel bilgileri içeren veritabanları için şifreleme gibi güvenlik gereksinimlerini uygulamaktadır.		ABD'nde güvenlik denetim zorunluluğu yoktur. Gizlilik yasalarının eksikliğinde, güvenlik gereksinimlerinin çoğu tüketici yasalarından karşılanmaktadır.		Birleşik Devletler, teknoloji ürünleri için güvenlik sertifikalarının dünyada en aktif kullanıcısıdır ve yerli BT tedarik kurallarının çoğunda uluslararası Common Criteria programını uygular. ABD, Ortak Kriterler Tanıma Sözleşmesi (CCRA) Sertifika Yetkilendirme Üyesidir(en üst düzey).
---	---------------------------	---	--	---	--	---	--	---	---	---	---

EK-17. Siber suçlar kapsamındaki düzenlemeler açısından incelenmesi

ÜLKELER	1. Siber suçlarla ilgili mevcut yasalar var mıdır?		2. Siber suçlar ile ilgili yasalar, Siber Suçlarla ilgili Budapeşte Sözleşmesi ile uyumlu mudur?		3. Yasal makamlar, veri barındırma hizmeti sağlayıcılar, mobil operatörler veya diğer hizmet sağlayıcılarda bulunan veya bu kurumlar tarafından aktarılan şifrelenmiş verilere erişmek için ne gibi olanaklara sahiptir?		4. Yasalar sınır ötesi suçlar konusunda çözüm getirir mi? Getirirse nasıl bir çözüm olur?	
		Açıklama		Açıklama		Açıklama		Açıklama
 CA [127]	✓	Kanada siber suçlarla mücadele konusunda kapsamlı bilgisayar yasaları sahiptir. Bununla birlikte, Kanada'nın çevrimiçi soruşturma ve uygulama araçlarının eksikliğiyle ilgili kanunlarında tanınmış sınırlamalar bulunmaktadır.	✓	Kanada'da, Avrupa Konseyi Siber Suçlar Sözleşmesi 2001 yılında imzalanmış, 2015 yılında onaylanmıştır.	Sınırlı Erişim 	Kolluk kuvvetleri, Kanada'daki şifreli verilere emirle erişebilir. Böyle bir emir verilmesi için kesin koşullar belirsizliğini korumaktadır. Şubat 2013'te yürürlüğe giren "Bill C-55" yasası ile belirli sınırlı koşullar altında polis memurunun kişisel iletişimi engelleme yetkisi bulunmaktadır.		Kanada bilgisayar suç hükümleri yerel ceza kanununda bulunmaktadır. Kanunun 447.1 E bölümü mahkemenin yetkisini belirler. Kanun sınır dışında çok sınırlı durumlarda uygulanabilir.
 DE [128]	✓	Alman Ceza Kanunu, bilgisayar suçları ve siber suçlarla ilgili kapsamlı hükümler içermektedir.	✓	2009 yılında Avrupa Konseyi Siber Suçlarla Mücadele Sözleşmesi onayladı.	Sınırlı Erişim 	Belli devlet kuruluşları, Telekomünikasyon Kanunu'nun 113'üncü Bölümü uyarınca şifre ve şifreleme anahtarları talep etme yetkisine sahiptir.		Alman kanunları, siber suçlar için yerel yasalar konusundaki geniş kapsamı içeriyor. Söz konusu yasalar, fiziksel olarak farklı bölgelerde bulunan vatandaşların yargılanabilmesine de zemin hazırlıyor.
 ES [129]	✓	İspanyol Ceza Kanunu siber suçların kapsamını içeriyor. Ayrıca, 3/2010 sayılı Kraliyet Kararnamesi mevcut yasaları kuvvetlendirmiştir.	✓	İspanya, Siber Suç Sözleşmesini Haziran 2010'da onayladı. Ayrıca, İspanyol Ceza Kanunu, Siber Suç Sözleşmesine uyum sağlamak amacıyla 3/2010 Kraliyet Kararnamesi ile değiştirildi ve güçlendirildi.	?	Şifreli verilerin üçüncü kişiler tarafından erişimi konusu henüz İspanyol mevzuatında bulunmamaktadır. Bununla birlikte, bu hukuk alanında reform yapmak için birkaç öneri mevcuttur.	✗	İspanya Yasaları genel olarak bölgesel hukuk ilkesi ve kişisel hukuk ilkesi ile sınırlıdır.
 FR [130]	✓	Fransa'nın Ceza Kanunu (21 Haziran 2004 tarihli ve 2004-575 sayılı Kanunla değiştirilen) siber suçlar konusunda kapsamlı bir çerçeve oluşturur.	✓	Fransa 2006 yılında Siber Suç Sözleşmesini onayladı.	Sınırlı Erişim 	15 Kasım 2001 tarihli ve 2001-1062 sayılı Topluluk Güvenliği Hakkında Kanun, bir soruşturma esnasında karşılaşılan şifrelenmiş bilgiye erişilebilmesi için üçüncü kişinin görevlendirilmesine müsaade eder.		Yahoo müzayede sitelerinde Nazi hatıra ürünlerinin Fransız vatandaşlarına tanıtımını içeren yüksek profilli bir dava, Fransa'nın ceza yasasının sınır dışında uygulanmasına yol açmıştır.

EK-17.(devam) Siber suçlar kapsamındaki düzenlemeler açısından incelenmesi

	IT [131]	✓	İtalya Ceza Kanunu (2011) kapsamlı siber suç hükümlerini içermektedir.	✓	İtalya, 2008 yılında Siber Suç Sözleşmesini onayladı ve Ceza Kanununu sözleşme hükümlerini içerecek şekilde değiştirdi.	Sınırlı Erişim 	Şifreli verilere erişim, sınırlı koşullar altında ve bir yargı iznine tabidir. Yasadışı faaliyetleri saklamak için şifreleme yöntemini suç saymak için önerilen yasa 2004 yılında reddedilmiştir.	✗	İtalyan Ceza Kanunu, İtalyan topraklarında işlendiği suçlara sınırlama getirmektedir.
	PL [132]	✓	Polonya Ceza Kanununda 2004, 2008 ve 2009 yıllarında siber suçlar konusunda kapsamlı değişikliklere gidilmiştir.	✓	Polonya Siber Suç Sözleşmesini 2001 yılında imzaladı ve Sözleşmeyi 2015 yılında onayladı. Ceza Kanunu sözleşme hükümlerine göre geliştirildi.	Erişim yetkisi yok 	Polonya'da, şifrelenmiş verilere kolluk kuvvetlerinin erişimi konusunda kararlar henüz alınmadı. Her ne kadar bir emir ile erişim mümkün olsa da, vatandaşlar verilerin gizliliği konusunda güçlü anayasal haklara sahiptir.	🌐	Polonya Ceza Kanunu'nun 113. maddesi, işlenen suçun bulunduğu yerde uygulanan kanunlara bakılmaksızın, Polonya vatandaşlarının yargılanabileceğini belirtmektedir. Uygulamada, bu genellikle savaş suçları ve insan kaçakçılığı gibi ciddi suçlarla sınırlandırılmıştır.
	TR [133]	✓	Türk Ceza Kanunu (2005 yılında değiştirilen şekliyle) bilgisayar ile ilgili çok sayıda suç içermektedir. Tartışmalara konu olan 2007 tarihli İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda da çeşitli siber suçlar kapsam içine alınmıştır.	✓	Türkiye'de, Avrupa Konseyi Siber Suçlar Sözleşmesi 2010 yılında imzalanmış, 2014 yılında onaylanmış ve 2015 yılında yürürlüğe girmiştir.	Sınırsız Erişim 	Türkiye'de şifrelenmiş verilere erişimle ilgili belirli bir yasa veya yönetmelik bulunmamakla birlikte, hükümet yetkilileri şifreleme kullanımını tasvip etmemektedir.	🌐	Türk vatandaşları sınır dışında nerede olursa olsun Türk Ceza Kanunu'nun kapsamı içindedir. Türkiye aynı zamanda Siber Suçlar Sözleşmesi'nin bir üyesidir ve siber suçların soruşturulmasında diğer yargı bölgelerindeki yasal makamlar ile işbirliği yapmaktadır.
	UK [134]	✓	Birleşik Krallık'ta, 1990 tarihli Bilgisayarlı Kötüye Kullanma Yasası ve 2006 tarihli Sahtecilik Yasası siber suçların temel kapsamını oluşturmaktadır.	🌐	Birleşik Krallık 2011 yılında Siber Suç Sözleşmesini onaylamış ancak sözleşmede cihazların kötüye kullanımı açıklayan 6'ncı maddesini uygulamadığını ifade etmiştir. Bunun dışında, mevcut yasalar sözleşme hükümleriyle büyük ölçüde uyumludur.	Sınırsız Erişim 	2000 tarihli Müfettişlik Yetkileri Yasası Yönetmeliğine göre polis, şifreleme anahtarını ifşa etmemek koşulu ile yargı talimatı olmaksızın belirli erişimler yapabilir. 2015 yılında kolluk kuvvetlerinin şifreleme anahtarlarına daha geniş erişimi ulusal çerçevede tartışmalara sebep oldu.	🌐	Birleşik Krallık, Siber Suç Sözleşmesi hükümlerine uygun olarak diğer ülke kolluk kuvvetleri ile işbirliği yapmaktadır.

EK-17.(devam) Siber suçlar kapsamındaki düzenlemeler açısından incelenmesi

	US [135]		ABD’de siber suçların temel hükümleri; 1986 yılında yürürlüğe giren Bilgisayar Dolandırıcılığı ve Kötüye Kullanım Yasası (CFAA) ve 2001 yılında yürürlüğe giren PATRIOT Yasası ile belirlenmiştir.		ABD 2006’da Siber Suç Sözleşmesini onaylamıştır. Ayrıca, ABD yasaları Siber Suç Sözleşmesi ile uyumludur.	Sınırlı Erişim 	Şifreli verilere erişim yargı talimatı olduğu sürece mümkün olabilmektedir. Ancak hukuki durum eyaletlere göre farklılık göstermektedir. 2015 yılında, kolluk kuvvetlerinin şifrelenmiş verilere daha fazla erişim gereksinimini artıran öneriler yapıldı. Bu konu ABD’de halen tartışılmaktadır.		CFAA bölgelerarası arası hükümlere sahip değildir. Ancak 2001 yılında yürürlüğe giren PATRIOT Yasası, ABD dışında gerçekleştirilen iletişimi etkileyen faaliyetler ve çevrimiçi dolandırıcılık faaliyetlerinde bilgisayarlarla ilgili hükümleri içermektedir.
---	---------------------------	---	--	---	---	---	--	---	---

EK-18. Fikri mülkiyet haklarının korunması kapsamındaki düzenlemeler açısından incelenmesi

ÜLKELER		1. Ülke, Ticaretle Bağlantılı Fikri Mülkiyet Hakları Anlaşması (TRIPS) üyesi midir?	2. TRIPS'in uygulanması için Fikri Mülkiyet yasaları yapılmış mıdır?	3. Ülke Dünya Fikri Mülkiyet Örgütü (WIPO) Telif Hakları Anlaşması'na taraf mıdır?	4. WIPO Telif Hakları Anlaşması'nı hayata geçiren yasalar yapılmış mıdır?	5. Telif hakkı sahiplerinin eserlerinin izinsiz olarak internet üzerinde yayınlanmasına karşı özel hukuk yaptırımları mevcut mudur?	6. Telif hakkı sahiplerinin eserlerinin izinsiz olarak internet üzerinde yayınlanmasına karşı cezai yaptırımlar mevcut mudur?
		Açıklama	Açıklama	Açıklama	Açıklama	Açıklama	Açıklama
	CA [127]	✓ 1995'te TRIPS Anlaşmasına üye oldu.	✓ 1996'da yerel yasalar ile TRIPS Anlaşması hükümlerini yürürlüğe koydu.	✓ 1997'de WIPO Telif Hakkı Antlaşması imzalandı, Mayıs 2014'te onaylandı, Ağustos 2014'te yürürlüğe girdi.	✓ 2014'te WIPO Antlaşması onaylandı, ancak hükümlerin birçoğu, 2012'de Telif Hakkı Modernizasyonu Yasası'nın (CMA) yürürlüğe girmesi ile zaten uygulanmıştı.	✓ CMA 2012'de kabul edildi ancak mevzuatın önemli kısımları Ocak 2015'ten sonra yürürlüğe girdi.	ⓘ Telif Hakkı Yasasında ki 42 ve 43'üncü bölümde yer alan cezai yaptırımlar ancak sınırlı koşullar altında geçerlidir.
	DE [128]	✓ 1995'te TRIPS Anlaşmasına üye oldu.	✓ TRIPS Anlaşması yerel yasalarla uygulanmıştır.	✓ 1996'de WIPO Telif Hakkı Antlaşması imzalandı, 2009'da onaylandı, Mart 2010'da yürürlüğe girdi.	✓ Urhebergesetz (Telif Hakkı Yasası), WIPO Telif Hakkı Antlaşması hükümlerini birleştirmek için birkaç kez güncellendi.	✓ Eser sahibinin bir dosya paylaşım ağı içinde çalışmalarının izinsiz yayınlanmasına düzenleme getiren Telif Hakkı Yasası'nın 19(A) bölümü 2003 yılında tanıtıldı.	ⓘ Sınırlı koşullarda, telif hakkıyla korunan eserlerin kopyalanması konusunda cezai yaptırımlar uygulanabilir. Ancak, cezai yaptırımlar, başkalarının mülkiyet haklarına müdahale etmek gibi ciddi vakalarla sınırlıdır.

EK-18.(devam) Fikri mülkiyet haklarının korunması kapsamındaki düzenlemeler açısından incelenmesi

	ES [129]	✓	1995'te TRIPS Anlaşmasına üye oldu.	✓	TRIPS Anlaşması yerel yasalarla uygulanmıştır.	✓	1996'de WIPO Telif Hakkı Antlaşması imzalandı, 2009'da onaylandı, Mart 2010'da yürürlüğe girdi.	✓	İspanya antlaşma hükümlerini yasayla uygulamaya koydu.		2011 tarihli Sürekli Ekonomi Yasası (Ley Sindee) yalnızca telif hakkını ihlal edebilecek hizmet sağlayıcılarına odaklanmaktadır. Telif hakkıyla korunan materyalleri yasadışı olarak üreten kullanıcılar kapsama dahil değildir. İspanyol telif hakkı yasası, 1 Ocak 2015'te güncellendi		İspanyol Ceza Kanunu'nun 270. maddesi telif hakkıyla korunan bir eserin çoğaltılması, intihal edilmesi, dağıtılması veya kamuya açıklanmasının suç olduğunu, belirtmektedir. Suçlular altı aydan iki yıla hapis ve para cezası ile cezalandırılabilirler. Ancak, İspanya Savcılığı Ofisi'nden 1/2006 sayılı Genelgesi ile Ceza Kanunu'nun 274. Maddesi uyarınca cezai suç olarak görülen bu tür fiiller "ticari kâr amaçlı" olmadıkça şu teşkil etmez.
	FR [130]	✓	1995'te TRIPS Anlaşmasına üye oldu.	✓	TRIPS Anlaşması hükümleri yerel kanunlarda uygulanmaktadır.	✓	1997'de WIPO Telif Hakkı Antlaşması imzalandı, 2009'da onaylandı, Mart 2010'da yürürlüğe girdi.	✓	Yerel yasalarla WIPO Telif Hakkı Antlaşması'ndaki hükümler uygulanmıştır.	✓	Fransa, 2009'da "Yaratıcı Eserlerin İnternette Dağıtımını ve Korunmasını Teşvik Eden Kanunu (HADOPI)" tanıttı. Temmuz 2013'te hükümet İnternet erişiminin askıya alınmasının yaptırım olarak kullanılmayacağını açıkladı.	✓	Fransız Fikri Mülkiyet Yasası'nın L'112-1 maddesi, herhangi bir orijinal eserin telif hakkıyla korunabileceğini belirtir. Ayrıca, L335-2, L335-3 ve L122-6 maddeleri de telif hakkı ihlali konularını düzenlemektedir.

EK-18.(devam) Fikri mülkiyet haklarının korunması kapsamındaki düzenlemeler açısından incelenmesi

	IT [131]	✓	1995'te TRIPS Anlaşmasına üye oldu.	✓	TRIPS Anlaşması hükümleri yerel kanunlarda uygulanmaktadır.	✓	1996'da WIPO Telif Hakkı Antlaşması imzalandı, 2009'da onaylandı, Mart 2010'da yürürlüğe girdi.	✓	Telif Hakkı ve Komşu Hakları Korunması Kanunu (22 Nisan 1941 tarih ve 633 sayılı Kanun). 2000/31 sayılı AB E Ticaret Direktifi esaslarına uygun olarak 70/2003 Yasama Kararnamesi ile güncellendi.	✓	Telif Hakkı ve Komşu Hakları Korunması Kanununun 171-174. maddelerinde, 2.500 ila 15.000 avro para cezası da dahil olmak üzere, telif hakkı ihlaline ilişkin iç hukuk cezaları mevcuttur.	✓	128/2004 sayılı kanun, 43/2005 sayılı kanunun telif hakkı yasasında değişiklik yapmayı öngören ve genel adı Urbani Kararnamesi olan düzenlemede elektronik iletişim ağları kullanılarak işlenen telif hakkı ihlalleri için cezai müeyyideler bulunmaktadır.
	PL [132]	✓	1995'te TRIPS Anlaşmasına üye oldu.	✓	4 Şubat 1994 tarihli Polonya Telif Hakları Kanunu, TRIPS Anlaşması hükümlerine göre güncellendi.	✓	WIPO Telif Hakkı Antlaşması 2004 yılında Polonya'da yürürlüğe girmiştir.	✓	Değiştirilen 4 Şubat 1994 tarihli Polonya Telif Hakları Yasası Telif Hakkı Antlaşması'nı uygular.	✓	Uyarı mektubu teslim edildikten sonra sivil yaptırımlar uygulanır.	✓	Yasalarla belirlenen cezai yaptırımlar mevcuttur.
	TR [133]	✓	Türkiye 1995 yılında TRIPS Anlaşması'nın bir üyesi olmuştur.	✓	5 Aralık 1951 tarih ve 5846 sayılı Fikir ve Sanat Eserleri kanunu (Telif hakkı yasası) uluslararası anlaşmalara ve AB yönergelerine uyumlu olacak şekilde düzenli olarak güncellenmektedir.	✓	WIPO Telif Hakları Antlaşması Türkiye'de 2008 yılında yürürlüğe girmiştir.	✓	Türkiye'deki Telif Hakları Yasası WIPO Telif Hakları Antlaşması ile çok büyük ölçüde uyumludur.	✓	Telif hakkı bulunan herhangi bir çalışmanın izinsiz bir şekilde kamuya iletilmesi durumunda uygulanacak yaptırımlar vardır.	?	Bu tür malzemelerin yalnızca yayınlanmasında cezai yaptırımlar uygulanıp uygulanmadığı belli değildir.

EK-18.(devam) Fikri mülkiyet haklarının korunması kapsamındaki düzenlemeler açısından incelenmesi

	UK [134]	✓	1995'te TRIPS Anlaşmasına üye oldu.	✓	TRIPS Anlaşması hükümleri yerel kanunlarda uygulanmaktadır.	✓	1997'de WIPO Telif Hakkı Antlaşması imzalandı, 2009'da onaylandı, Mart 2010'da yürürlüğe girdi.	✓	1988 tarihli Telif Hakkı, Tasarımlar ve Patent Yasası ve 2010 tarihli Dijital Ekonomi Yasasının birleşimi, WIPO Telif Hakkı Antlaşması hükümlerini uygulamaktadır.	✓	Telif Hakkı, Tasarımlar ve Patent Yasası'nın 20. maddesi, lisans olmaksızın telif hakkı bulunan çalışmayı bulundurmaya yasaklamaktadır.	✓	Hem sivil yaptırımlar hem de cezai yaptırımlar uygulanmaktadır.
	US [135]	✓	1995'te TRIPS Anlaşmasına üye oldu.	✓	TRIPS Anlaşması hükümleri yerel kanunlarda uygulanmaktadır.	✓	1997'de WIPO Telif Hakkı Antlaşması imzalandı, 1999'da onaylandı, Mart 2002'de yürürlüğe girdi.	✓	Dijital Milenyum Telif Hakkı Yasası, WIPO Telif Hakkı Antlaşması hükümlerini uygular.	ⓘ	Telif Hakkı Yasası'nın 106 (3). maddesi, uluslararası telif hakkı sözleşmelerine uyumlu olacağını ifade eder. Ancak bazı mahkeme kararlarında tutarsızlıklara rastlanmaktadır.	ⓘ	Telif hakkı ihlali için cezai yaptırımlar mevcuttur. Ancak, tutarsızlıklardan dolayı hukuk davalarında henüz cezai yaptırımlar uygulanmamıştır.

EK-19. Fikri mülkiyet hakları kapsamında İSS'lerinin sorumluluklarını belirleyen düzenlemeler açısından incelenmesi

ÜLKELER	1. Telif hakkını ihlal eden içerikle ilgili İSS'ların sorumluluğunu düzenleyen yasalar var mıdır?		2. İSS'larının sitelerinde veya sistemlerinde bulunan ve telif haklarını ihlal eden içerikten dolayı sorumlu tutulabilecekleri bir yasal zemin var mı?		3. Telif hakkı sahibi bildirimde bulunduğu İSS'ların telif hakkını ihlal eden içeriği kaldırma zorunluluğu var mıdır?		4. İSS'ların bildirim aldıklarında abonelerine dönerek abonenin, İSS'nın sunduğu hizmeti telif hakkını ihlal eden bir içeriği yaymak için kullanmakta olduğunu bildirmesi zorunlu mudur?		5. Bulut bilişim hizmetlerinin kötüye kullanımına karşı zorlamalar dâhil olmak üzere açık bir yasal koruma var mıdır?	
		Açıklama		Açıklama		Açıklama		Açıklama		Açıklama
 CA [127]	✓	İSS'ların yükümlülükleri, Telif Hakkı Modernizasyonu Yasası (2012) ile netleştirildi ve güçlendi. Hükümler, 2015 yılının başında yürürlüğe girdi.	✓	Telif Hakkı Yasası'nın CMA ile değiştirilen şartlarına göre, hak ihlali yapılan içerikten dolayı İSS'lar sorumlu tutulabilir.	✗	CMA, içerik kaldırma şartları içermez; yalnızca bildirim konularını içerir.	✓	CMA, sadece abonelere bildirimlerin iletilmesini gerektiren bir hükümler içerir.	✓	Kanada yasaları, bulut bilişim konusunda açık bir koruma sağlamak üzere düzenlendi.
 DE [128]	✓	İSS'ların yükümlülükleri, AB E-Ticaret Direktifi (2000/31/EC) ve 2007 tarihli Almanya Telemedia Yasası ile belirlenmiştir.	✓	Telemedia Yasası'nın 8. Maddesi; erişim sağlayıcıların, kullanıcılar ile işbirliği yapmadıkça, müşterilerinin içeriğinden yasal olarak sorumlu olmadığını belirtmektedir.	✓	Telemedia Yasası'nın 10. Maddesi uyarınca: Servis sağlayıcılar, müşterisi için sakladığı üçüncü şahısların bilgilerinden sorumlu değildir (10.madede belirtilen 2 istisna durum hariç).	✗	İSS'lar üzerinde herhangi bir yükümlülük bulunmamaktadır.	✓	Almanya kapsamlı gizlilik yasası ve siber suç yasasına sahiptir. Bu yasaların bileşimi, Almanya'daki bulut bilişim servisleri için açık bir koruma sağlamaktadır.
 ES [129]	✓	34/2002 Sayılı Bilgi Toplumu Hizmetleri ve Elektronik Ticaret Kanunu (LSSI), AB Elektronik Ticareti Yönergesi (2000/31/EC) ve Fikri Mülkiyet Kanunu (21/2014) İSS'lerinin yükümlülüklerini ortaya koymaktadır.	✓	Bilgi Toplumu Hizmetleri ve Elektronik Ticaret Kanunu'nun 16. Maddesi, İSS ihlalin bilgisine sahipse ve hak ihlalinde bulunan içeriğe erişimi kaldırmak veya engellemek gibi tedbirler uygulamamışsa sorumlu olduğunu ifade etmektedir.	✓	Sürekli Ekonomi Yasası uyarınca, hak ihlalinde bulunduğu içeriği içeren web sitesinin kapatılabilmesi için aynı yasada beşirtilen 6 başlık altında toplanan önlemlerin alınması gerekir. Ayrıca LSSI 11'inci maddesi gereği, İSS'ları içeriğin kaldırılması ve durdurulması durumlarında yetkili birimle işbirliği yapma yükümlülüğünde.	✗	İSS'larının bildirimde bulunma yükümlülüğü bulunmamaktadır.	✓	İspanya'nın telif hakkı korumasında bazı küçük boşluklar bulunmaktadır. Bulut bilişim servisleri için genel koruma seviyesi, uygulamada tutarsızlıklar içermektedir.

EK-19.(devam) Fikri mülkiyet hakları kapsamında İSS'lerinin sorumluluklarını belirleyen düzenlemeler açısından incelenmesi

	FR [130]	✓	İSS'ların yükümlülüklerini LCEN (Dijital Ekonomide Güvenin Artırılması) Kanunları düzenlemektedir.	✓	Fikri Mülkiyet Yasası, LCEN Yasası ve HADOPI Yasası'nın birleşimi bu kapsamda değerlendirilir. İSS'ları sitenin editörü olmadıkça ve ya içeriğin yetkilendirilmesi yapılmadıkça sorumlu olmayacaktır. Bununla birlikte; HADOPI Yasası, telif hakkı ihlali durumunda İSS'nin gerçekleştirmesi gereken şartları içermektedir.	✓	Fransız mahkemeleri, içeriğin ihlal edildiği konusunda bilgilendirildikten sonra, tekrar yayınlanmasının önüne geçmek için servs sağlayıcıları üzerinde ilave yükümlülükler getirmiştir.	✓	2013 yılında güncellenen HADOPI Yasası ile, telif hakkı ihlallerinde üç aşamalı süreç işletilmektedir (1.Tebliğ, 2.Uyarı, 3.Cezalandırma). Düzenleme kullanıcılara ve internette indirenlere yöneliktir.	✓	Fransa'da, kapsamlı siber suç yasaları ve güncel telif hakkı yasası bulut bilişim hizmetleri için güçlü koruma sağlamaktadır. Söz konusu yasaların eksiksiz uygulanmasına rağmen telif hakkının çalınması hadisesine sıklıkla rastlanmaktadır.
	IT [131]	✓	2000/31 sayılı AB Elektronik Ticaret Direktifini uygulayan 70/2003 sayılı Yasama Kararnamesi İSS'larına yükümlülükler getirmektedir. İSS'ları hak sahiplerinden bildirim aldıktan sonra telif hakkı ihlallerini önleme yönünde tedbirler alması gerekiyor.	✓	Aralık 2013'te İtalya'nın Yasal İletişim Kurumu (AGCOM), İSS'ların telif hakkı ihlallerine karşı sorumluluğunu düzenleyen düzenlemeler yayınladı. Mart 2014'te yürürlüğe giren düzenleme, hakları ihlal eden içeriğin çevrimiçi olarak kaldırılabilceğini ifade etmektedir.	ⓘ	2014 AGCOM Yönetmelikleri, hak ihlali bulunan içeriğin kaldırılması gerektiği hususunda düzenlemeler getirir de, İSS'ları üzerinde sıkı yasal zorunluluklar bulunmamaktadır.	✗	İtalya'daki geçerli yasa veya yönetmeliklerde aboneleri haberdar etme zorunluluğu yoktur.	✓	İtalya, güçlü siber suç yasalarına ve kapsamlı gizlilik kanunlarına sahiptir. Ayrıca telif hakkı yasası bulut bilişim hizmetleri için yeterli koruma sağlamaktadır.
	PL [132]	✓	2002 tarihli Elektronik Araçlarla Hizmetler Sağlama Yasası (2008'de değiştirildi), İSS'lar için yükümlülükler getirmektedir. Bu yasa bildirim ve yayından kaldırma durumunda telif hakları yasası ile etkişime geçmektedir.	✓	İSS'lar yalnızca uyarı mektubunu aldıktan sonra sorumlu tutulabilirler.	✓	Polonya kanunları İSS'ların uyarı mektubu aldıktan sonra harekete geçmesini gerektirir. Uygulamada Polonya mahkemesi, İSS'ları ile hak sahipleri arasında işbirliği yapılmasını önermektedir.	✗	Bildirimde bulunma zorunluluğu yoktur. Veri koruma düzenleyicisi, İSS'ların bazı durumlarda telif hakkı sahipleri ile abone bilgilerini paylaşabileceğine karar vermiştir, ancak bu durumun yasal bir geçerliliği yoktur.	✓	Polonya, siber suç yasaları, telif hakkı mevzuatı ve veri koruma mevzuatının yararlı bir birleşimine sahiptir. Bunların hepsi bulut bilişim hizmetleri için kapsamlı koruma sağlar.

EK-19.(devam) Fikri mülkiyet hakları kapsamında İSS'lerinin sorumluluklarını belirleyen düzenlemeler açısından incelenmesi

	TR [133]	✓	Telif hakkı yasasına 2004 yılında yapılan değişikliklerle eklenen 4. maddede İSS sorumluluğu ve işbirliği basit bir şekilde düzenlenmiştir.	✓	Telif hakkı ihlali bulunduğunu öne süren sahipleri içerik sağlayıcıya ihlalin durdurulması talebinde bulunabilirler.	✓	İçerik sağlayıcılar üç iş günü içinde telif hakkı ihlalini durdurmazsa, telif hakkı sahibinin cumhuriyet savcısından ilgili İSS'na içerik sağlayıcıya verdiği hizmeti durdurmasını isteme hakkı vardır. Uygulamada telif hakkı ihlalleri yaygın durumdadır; kapatma bildirimleri ve askıya almalar seyrekler.	✗	İSS'larının her ne kadar savcılar tarafından verilecek emirlere göre yayın durdurma uyarıları yapmaları gerekiyorsa da, öne sürülen telif hakkı ihlallerini abonelerine bildirme konusunda doğrudan bir rolleri yoktur.	🕒	Türkiye'de bulut hizmetleri ile ilgili olarak siber suçlar ve telif hakkı yasalarının sağladığı sınırlı düzeyde bir koruma mevcuttur. Bununla birlikte, her iki yasada da küçük boşluklar vardır ve Türkiye'de henüz veri koruma yasaları yoktur.
	UK [134]	✓	2010 tarihli Dijital Ekonomi Yasası, İSS'lar telif hakkı konusunda sınırlı bir sorumluluk kapsamı oluşturmuştur. Dijital Ekonomi Yasasının uygulamada yetersiz kalması durumunda, İSS'lar halen 1988 tarihli Telif Hakkı, Tasarımlar ve Patent Yasası'nın 20. Bölümünün ilgili hükümlerine tabidir.	✓	Genellikle, İSS'lar yalnızca doğrudan bilgiye sahip oldukları içerikler için sorumludur.	🕒	Takdir hakkı mahkemelere ve İSS'larına bırakılmıştır. 2010 tarihli Dijital Ekonomi Yasası'nın (Bölüm 17 ve 18) bildirim ve yayından kaldırma hükümleri hiçbir zaman tamamen uygulanmadı ve 2014 yılının ortalarında Birleşik Krallık hükümeti tarafından terk edildi.	🕒	Bildirim gereksinimleri 2010 Dijital Ekonomi Yasasına dahil edildi, ancak bu hükümler hiç uygulanmadı. Creative Content UK uyarı programı olarak bilinen gönüllü bir eğitim ve uyarı sistemi geliştirdi. Bu program bazı temel uyarı hükümlerini içermekle birlikte, henüz uygulanmamıştır.	✓	İSS'ların yükümlülüklerini belirleme konusunda eksiklikler olmasına rağmen; Birleşik Krallık siber suç kanunları, telif hakkı koruması ve bulut bilişim hizmetleri için gizlilik koruması konularında güçlü temellere dayanmaktadır.
	US [135]	✓	Çevrimiçi Telif Hakkı İhlali Sorumluluk Yasası (OCILLA), ihlalden haberdar olmadıkça ve telafi isteklerine derhal yanıt verdikleri sürece, İSS'larını sorumlu tutmamaktadır.	✓	İSS'lar, Dijital Milenyum Telif Hakkı Yasası'nın (DMCA) güvenli liman koşullarına uymazlarsa, farkında olan içeriği ihlal ettiği için sorumlu tutulabilirler.	✓	Bazı istisnalar hariç olmak üzere DMCA yasasının yayından kaldırma bildirimlerinin kullanımı ABD'nde yaygındır.	🕒	İSS'ları gönüllü olarak telif hakkı ihlali bildirimlerini abonelere bildirir. Ancak, bu durum yasa ile zorunlu hale getirilmemiştir.	🕒	Telif hakkı yasalarının çevrimiçi ortama uygulanması konusunda ve gizlilik yasasında bazı boşluklar olmasına rağmen, bulut bilişim hizmetleri için mevcut koruma seviyesi yeterlidir.

EK-20. Ulusal ve uluslararası standartları belirleyen düzenlemeler açısından incelenmesi

ÜLKELER		Verilerin taşınabilmesini ve karşılıklı çalışabilmesini sağlayacak standartları oluşturacak çerçeveyi hazırlayacak yasa, düzenleme veya politikalar var mıdır?		Ülkede standartların geliştirilmesinden sorumlu bir düzenleyici kurum var mıdır?		E-ticaret ile ilgili mevcut yasalar var mıdır?		Uygulamaların veya dijital verilerin yabancı bulut hizmet sağlayıcılardan indirilmesi tarifelerden veya diğer ticari engellerden muaf mıdır?		Uluslararası standartlar ulusal standartların üzerinde midir?		Devlet uluslararası standart belirleme sürecine katılıyor mu?	
		Açıklama		Açıklama		Açıklama		Açıklama		Açıklama		Açıklama	
	CA [127]	✓	Standartların belirlenmesi konusunda güçlü ve köklü bir çerçeveye sahiptir.	✓	Standartların ayar ve yönetiminden Kanada Standartları Derneği (CSA Group) sorumludur.	✓	1999 tarihli Kanada Elektronik Ticaret Yasası (UECA).	✓	Dijital veri veya buluta bağlı hizmetler konusunda herhangi bir tarife veya ticaretle ilgili engel bulunmamaktadır.	✓	Dijital ekonomi sektöründe yerli ve yabancı standartların bir karışımı kullanılmaktadır.	✓	Uluslararası standartlar belirleme süreçlerinde aktif katılımcıdır.
	DE [128]	✓	Almanya'da standartların belirlenmesi mevzuattan çok devlet sektör politikasına tabidir.	✓	Alman Standardizasyon Enstitüsü(DIN), standartlar geliştirme, belgelendirme, akreditasyonu yönetme konularında Alman hükümeti ile sözleşmelidir.	✓	Elektronik Ticaret Çerçeve Koşulları Yasası 2001 yılında kabul edildi.	✓	Almanya'da bu kapsamda engelleme yoktur.	✓	Bilgi teknolojisi sektöründe AB standartlarını ve uluslararası standartları desteklemekte ve uygulamaktadır.	✓	DIN, Almanya'yı Uluslararası Standartlar Örgütü'nde temsil etmektedir ve Almanya, uluslararası standartlar sürecinde etkin rolü vardır.
	ES [129]	✓	1986 yılında kanun hükmünde kararname ile İspanya Standardizasyon ve Sertifika Birliği (AENOR) kurulmuştur.	✓	AENOR, özel, kâr amacı gütmeyen bir organizasyondur ve sorumlu kuruluştur.	✓	34/2002 sayılı Bilgi Toplumu Hizmetleri ve Elektronik Ticaret (LSSI) yasası bulunmaktadır.	✓	İspanya'da herhangi bir tarife veya ticaretle ilgili engel bulunmamaktadır.	✓	İspanya, AB ve uluslararası standartları desteklemektedir.	✓	İspanya, AB ve Uluslararası Standartlar Organizasyonu (ISO) için aktif bir katılımcıdır.

EK-20.(devam) Ulusal ve uluslararası standartları belirleyen düzenlemeler açısından incelenmesi

	FR [130]	✓	Fransa'da, Ürün Güvenliği Yönergesi gibi AB standartlarını ve düzenlemelerini, ulusal yasalara uygulayan düzenlemeler mevcuttur.	✓	Fransız Standardizasyon Derneği (AFNOR) Fransa'daki standartların merkezidir.	✓	Fransa, 2004'te Dijital Ekonomi Yasasını (LEN) meclisten geçirdi.	✓	Fransa, e-ticaretle ilgili faaliyetlerde hiçbir tarife veya engel oluşturmaz.	✓	Fransa, çoğu sektörde AB standartlarını ulusal standartların üstünde tutuyor.	✓	AFNOR, Fransa'yı uluslararası standartlar belirleme süreçlerinde temsil etmektedir. Fransa, ISO'nun kurucu üyesi ve aktif katılımcısıdır.
	IT [131]	✓	İtalya AB standartlarını, direktiflerini politikalarını ulusal politikalarına uygulamaktadır.	✓	İtalya Standardizasyon Teşkilatı (UNI) genel standartlar konusunda sorunludur. UNI'nin birleşik bir organı olan UNINFO, İtalya'nın ulusal standart organıdır.	✓	9 Nisan 2003 tarihli 70 sayılı İtalyan Yasama Kararı, e-ticaret yasasının ana kaynağıdır.	✓	İtalya'da dijital veriler üzerinde etkili olacak belirli bir tarife veya engel bulunmamaktadır.	✓	İtalya birçok sektörde AB standartlarına ve uluslararası standartlara öncelik veriyor. Özellikle bilişim sektöründe uluslararası standartlar tercih edilmektedir.	✓	İtalya UNI aracılığıyla, uluslararası standart geliştirme süreçlerinde etkin bir katılımcıdır.
	PL [132]	✓	2002 tarihli Standartlaştırma Yasası ile Polonya Standardizasyon Komitesi (PKN) kuruldu.	✓	PKN, hükümetin finanse ettiği ve ulusal standartlar organı bilinmektedir.	✓	2002 tarihli Elektronik Ödeme Araçları Yasası ve 2001 tarihli Elektronik Araçlarla Hizmet Sunma Yasası, e-ticaretin kapsamlı bir şekilde ele alınması amacıyla bir araya getirilmiştir.	✓	Polonya'da dijital veriler üzerinde etkili olacak belirli bir tarife veya engel bulunmamaktadır.	✓	Polonya başlangıçta ulusal standartları tercih etti. Ancak, Polonya 2002'den sonra AB ve uluslararası standartların bir karışımını tercih etti. Özellikle bilişim sektöründe uluslararası standartlar mevcuttur.	✓	Polonya ISO'nun standart geliştirme süreçlerinde aktif katılımcıdır.
	TR [133]	✓	Türkiye'de standartlar 132 sayılı ve 1960 tarihli Türk Standartları Enstitüsü Kuruluş Kanununa göre düzenlenir.	✓	Türk Standartları Enstitüsü (TSE).		15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Yasası sınırlı bazı e-ticaret hükümleri içermektedir.	✓	Türkiye mevcut durumda tarife oluşturma konusunda AB politikasını izlemektedir ve Bilgi ve İletişim Teknolojileri (ICT) sektörü ile ilgili tarife veya başka engeller yoktur.	✓	Türkiye'de AB ve Uluslararası standartların bir karışımı ulusal standartların üzerinde tutulmaktadır.	✓	Türkiye ISO komitelerinin ve çalışma gruplarının aktif bir katılımcısıdır.

EK-20.(devam) Ulusal ve uluslararası standartları belirleyen düzenlemeler açısından incelenmesi

	UK [134]	✓	2002 yılında Birleşik Krallık Hükümeti tarafından standartların yönetilmesi görevi İngiliz Standartları Enstitüsüne (BSI) verildi.	✓	19001 yılında kurulan BSI 2002 yılında gerçekleşen anlaşma ile standartlardan sorumlu kurum olarak görev yapmaktadır.	✓	E-ticaret yasaları çok sayıda mevzuatta dağılmıştır ve sözleşme ile tüm yasalar Elektronik Ticaret Yönergesine (EC Directive) dahil edilmiştir.	✓	İngiltere'deki bilgi teknolojisi sektörü tarife ve ticaret engelleri içermemektedir.	✓	İngiltere, uluslararası standartları ulusal standartlardan daha fazla desteklemektedir.	✓	BSI, uluslararası standart geliştirme süreçlerinde ülkeyi temsil eder ve bir çok BT standartları komitesinde etkin bir katılımcıdır.
	US [135]	✓	Standartlar, düzenli olarak güncellenen bir ABD Standartları Stratejisi olan bir politika belgesi ile yönlendirilmektedir. Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) bilgi teknolojileri standartlarını belirlemektedir.	✓	Amerikan Ulusal Standartlar Enstitüsü (ANSI), ABD'yi uluslararası standart geliştirme süreçlerinde temsil eden kâr amacı gütmeyen bir kuruluştur. Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), bilgi teknolojileri standartlarını belirlemektedir.	✓	Birleştirilmiş Elektronik İşlemler Yasası (UETA), e-ticaret düzenlemelerini içermektedir.	✓	ABD'de herhangi bir tarife veya ticaretle ilgili engel bulunmamaktadır.	✓	ABD standartları uluslararası standartlarla uyumlu bulunmaktadır.	✓	Hem ANSI hem de NIST, uluslararası standartlar belirleme süreçlerine dahildirler.

EK-21. E-ticaret kapsamındaki düzenlemeler açısından incelenmesi

ÜLKELER	Ülke yönetiminde teknolojiye yansızlığı yerleştiren kanun veya politikalar mevcut mudur?		Bulut bilişim hizmetleri, çeşitli ürünlerin, hizmetlerin, standart ve teknolojilerin kullanılmasını zorunlu kılan kanun veya politikalarından muaf mıdır?		Bulut bilişim hizmetleri çeşitli ürünlerin, hizmetlerin, standart ve teknolojilerin kullanılması yolunda imtiyazlar tesis eden kanun veya politikalarından muaf mıdır?		Bulut bilişim hizmetleri, satıcının, geliştiricinin veya hizmet sağlayıcının uyuşuna göre ayrımcılık uygulayan yasalardan mıdır?	
		Açıklama		Açıklama		Açıklama		Açıklama
 CA [127]	✓	Kanada 2006 yılında; rekabetin sağlanması, hükümetler ve işletmeler için faydaların en üst düzeye çıkarılması için teknolojilerin seçiminde esnekliğe izin veren düzenlemelerinin teşvik edilmesini amacıyla APEC Teknoloji Seçimi İlkelerini kabul etmiş ve imzalamıştır.	✓	Kamu alımları için açık, şeffaf ve ayırım gözetmeksiz bir yaklaşım mevcuttur ve bulut bilişimiyle ilgili zorunlu teknolojilerin kullanımı için herhangi bir kısıtlama veya gereklilik bulunmamaktadır.	✓	Bulut bilişim ile ilgili herhangi bir ürün veya hizmette imtiyaz yoktur.	✓	Savunma ve ulusal güvenlikle ilgili yalnızca birkaç küçük istisna dışında tedarik için ayırım gözetmeksiz bir politikaya sahiptir. Kanada, güncellenmiş WTO çok taraflı Devlet İhale Anlaşması'na Nisan 2014'te katıldı.
 DE [128]	✓	2009 yılında güncellenen Kamu Sözleşmelerinin Ödüllendirilmesine İlişkin Yönetmeli, bazı istisnai istisnalar dışında, teknoloji ihaleleri açısından tarafsız bir yaklaşımı desteklemektedir.	✓	Almanya'da bu konu ile ilgili zorlayıcı koşullar yoktur.	ⓘ	Alman hükümeti, açık kaynak kodlu yazılımı BT politika öncelikleri arasında göstermektedir. Bu kapsamda, Almanya'daki tescilli teknoloji platformlarına, Alman vatandaşlarını yurt dışı kaynaklı casusluk faaliyetlerine karşı koruması önerilmektedir.	✓	Tedarik konusunda ayrımcılık uygulayan yasalar yoktur. Almanya, güncellenmiş WTO Çok Taraflı Hükümet Satın Alma Sözleşmesini (tüm AB üyeleri ile birlikte) Nisan 2014'te imzalamıştır.
 ES [129]	✓	2007 tarihli Kamu Hizmetlerine Yurttaşların Elektronik Erişimine Dair Yasası (E-Devlet Yasası) teknoloji tarafsızlığı ilkesini kapsar.	✓	İspanya'da bu konu ile ilgili zorunluluk yoktur.	✓	Bununla birlikte, İspanya Parlamentosu, 2007'de açık kaynak yazılımını tanıtan bağlayıcı olmayan bir kararı onayladı. Bazı yerel hükümet bölgelerinde açık kaynak politikaları uygulamaktadır.	✓	İhale konuları, 30/2007 sayılı Kamu Sektör Sözleşmeleri Hakkında Kanuna tabidir. Yerli ürün olması zorunluluğu mevcut değildir. İspanya, güncellenmiş WTO Çok Taraflı Hükümet Satın Alma Sözleşmesini (tüm AB üyeleri ile birlikte) Nisan 2014'te imzalamıştır.

EK-21.(devam) E-ticaret kapsamındaki düzenlemeler açısından incelenmesi

	FR [130]		Savunma Bakanlığı açık kaynak çözümleri tercih etse de, Fransa'nın çoğu teknoloji açısından tarafsız bir yaklaşım benimsemiştir.		Fransa'da bu konu ile ilgili zorunluluk yoktur.		Fransa Savunma Bakanlığı ve Eğitim Bakanlığı'nda resmi olarak açık kaynak çözümleri tercih edilir. Söz konusu sınırlı istisnalar dışında imtiyazlar bulunmamaktadır		Fransa'da satıcı uyruğuna dayalı herhangi bir ayrımcılık yapılmamaktadır. Fransa, güncellenmiş WTO Çok Taraflı Hükümet Satın Alma Sözleşmesini (tüm AB üyeleri ile birlikte) Nisan 2014'te imzalamıştır.
	IT [131]		Teknoloji tarafsızlığını destekleyen ulusal kanunlar veya politikalar bulunmamaktadır. Ancak, belirli bölgelerde tarafsızlık teşvik edilmektedir.		Ulusal düzeyde herhangi bir zorunlu kullanım gerekliliği bulunmamakla birlikte, ulusal politika gereği açık kaynaklı yazılımlar tavsiye edilmektedir.		2014 yılında, İtalyan Dijital Ajansı, tüm kamu kurumlarının lisans almadan önce açık kaynaklı yazılımlar kullanmayı düşünmesini gerektiren yeni ulusal kurallar yayınladı.		İtalya'da satıcı uyruğuna dayalı herhangi bir ayrımcılık yapılmamaktadır. İtalya, güncellenmiş WTO Çok Taraflı Hükümet Satın Alma Sözleşmesini (tüm AB üyeleri ile birlikte) Nisan 2014'te imzalamıştır.
	PL [132]		2007-2010 dönemi Ulusal Bilgisayarlaştırma Planı teknoloji tarafsızlığını zorunlu kılmıştır.		Polonya'da bu konu ile ilgili zorunluluk yoktur.		Polonya'da herhangi bir ürün veya hizmette imtiyaz yoktur.		29 Ocak 2004 Kamu İhale Kurumu bu kapsamda bazı düzenlemeler içermektedir. Ancak, mevcut düzenlemeler IT sözleşmeleri kapsamında engel oluşturmamaktadır. Polonya, güncellenmiş WTO Çok Taraflı Hükümet Satın Alma Sözleşmesini (tüm AB üyeleri ile birlikte) Nisan 2014'te imzalamıştır.
	TR [133]		Teknoloji tarafsızlığını destekleyen ulusal kanunlar veya politikalar bulunmamaktadır.		Türkiye'de bu konu ile ilgili zorlayıcı koşullar yoktur.		Türkiye'de bu konu ile ilgili imtiyaz yoktur; ancak pek çok devlet kuruluşu (savunma dâhil) önemli açık kaynak projeleri yürütmektedir.		Türkiye Dünya Ticaret Örgütü (WTO) Çok Taraflı Kamu Alımları Anlaşması'na bir üye olarak değil, gözlemci olarak katılmıştır. Türkiye'de kamu ihale yasası yurt içi tekliflere hala yüzde 15'i bulan bir fiyat tercihi sağlamaktadır.

EK-21.(devam) E-ticaret kapsamındaki düzenlemeler açısından incelenmesi

	UK [134]		Birleşik Krallık Kamu İhale Kanunu, bu kapsamda AB direktiflerini kendi yasalarında uygulamaktadır.		Mart 2015 tarihli Satın Alma Politikası Not:07/15'te yazılımların birlikte çalışabilirliği ve gereksinimleri belirlenirken iki şart yerine getirilmesi yazılmıştır: 1. Açık standart ilkelerinde tanımlanan tanıma uyan açık standartların denklik ilkesine bağlı olarak benimsenmesi, 2. Kabul edilen zorunlu açık standart profillerinin kullanılması.		Satın Alma Politikası Not 07/15: Hükümet genelinde kullanım için onaylanan bazı belirli standartların tercih edilmesi gerektiğini ifade etmektedir.		Birleşik Krallık'ta satıcı uyuşuna dayalı herhangi bir ayrımcılık yapılmamaktadır. Birleşik Krallık, güncellenmiş WTO Çok Taraflı Hükümet Satın Alma Sözleşmesini (tüm AB üyeleri ile birlikte) Nisan 2014'te imzalamıştır.
	US [135]		Ocak 2011 tarihli Beyaz Eşya, Teknoloji Tarafsızlığına İlişkin Mutabakat Zaptı bu kapsamda ABD Hükümetinin resmi politikasıdır.		Amerika Birleşik Devletleri'nde bu konu ile ilgili zorunluluk yoktur.		Amerika Birleşik Devletleri'nde herhangi bir ürün veya hizmette imtiyaz yoktur.		Düzenli olarak güncellenen 1993 tarihli Amerikan Satın Alma Yasası (BAA) bazı konularda yerli tercihler uygulamaktadır. Bununla birlikte, BAA hükümleri IT sektörü için nadiren geçerlidir. BAA; Dünya Ticaret Örgütü (WTO), Hükümet Satın Alma Sözleşmesi (GPA) ve serbest ticaret anlaşmaları (FTA'lar) hükümlerini de içermektedir.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı : ADA, Mehmet
 Uyruğu : T.C.
 Doğum tarihi ve yeri : 30/01/1984 Ankara
 Medeni hali : Evli
 E-posta adresi : mehmetada@gmail.com

Eğitim Derecesi	Okul/Program	Mezuniyet Yılı
Doktora	Gazi Üniversitesi/Bilişim Enstitüsü Yönetim Bilişim Sistemler Anabilim Dalı	Devam Ediyor
Yüksek lisans	Gazi Üniversitesi/Bilişim Enstitüsü Adli Bilişim Anabilim Dalı	2018
Yüksek lisans	Gazi Üniversitesi/Bilişim Enstitüsü Bilişim Sistemleri Anabilim Dalı	2014
Lisans	Orta Doğu Üniversitesi Bilg. ve Öğr. Tek. Eğt. (BÖTE)	2007
Lise	Keçiören Anadolu Meslek Lisesi	2002

İş Deneyimi, Yıl Çalıştığı Yer

2008-Devam Ediyor Türk Silahlı Kuvvetleri Subay

Yabancı Dili

İngilizce

Yayınlar

1. ADA, M. (2014). Personel Performans Değerlendirmesinde Kullanılan Karar Destek Sisteminde AHP ve TOPSIS Çok Kriterli Karar Verme Yöntemlerinin Uygulanması, Yüksek Lisans Bitirme Projesi. Bilişim Sistemleri Anabilim Dalı, Bilişim Enstitüsü, Gazi Üniversitesi.
2. ADA, M. ÇAKIR, H. (2017). Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi, Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 5(2), 635-656.

Hobiler

Basketbol, Bilişim teknolojileri, Kitap okuma, Kır yürüyüşü.