
GAZİ ÜNİVERSİTESİ
Gazi
1926

SİBER GÜVENLİK EKOSİSTEMİNİN GELİŞTİRİLMESİ

Zeynep Ebru IŞIK

YÜKSEK LİSANS TEZİ

ADLİ BİLİŞİM ANABİLİM DALI

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

OCAK 2019

Zeynep Ebru IŞIK tarafından hazırlanan "SİBER GÜVENLİK EKOSİSTEMİNİN GELİŞTİRİLMESİ" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Adli Bilişim Anabilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. Çelebi ULUYOL

Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Gazi Üniversitesi

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

Başkan: Prof. Dr. Şeref SAĞIROĞLU

Bilgisayar Mühendisliği Bölümü, Gazi Üniversitesi

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

Üye: Dr. Öğr. Üyesi Bülent TUĞRUL

Bilgisayar Mühendisliği Bölümü, Ankara Üniversitesi

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

Tez Savunma Tarihi: 23/01/2019

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

.....

Doç. Dr. Aslıhan TÜFEKÇİ

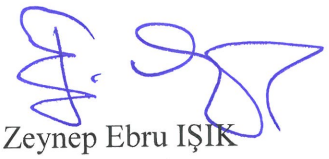
Bilişim Enstitüsü Müdürü

ETİK BEYAN

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

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

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



Zeynep Ebru IŞIK

23/01/2019

SİBER GÜVENLİK EKOSİSTEMİNİN GELİŞTİRİLMESİ

(Yüksek Lisans Tezi)

Zeynep Ebru IŞIK

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Ocak 2019

ÖZET

Ülke bilgi varlıklarının siber risklere karşı korunma düzeyine etki eden en önemli unsur, bu tehditler karşısında paydaşların koordinasyon kabiliyetinin var olmasıdır. Bu açıdan, siber güvenliğin sağlanması, farklı disiplinler arasında sıkı bir iş birliğini ve güçlü bir koordinasyonu gerektirmektedir. Bu çalışmada, siber uzayda siber güvenliğin sağlanmasına katkı sağlayabilecek bir yapı arayışıyla, paydaşların koordinasyonu ve iş birliğine dayanan siber güvenlik ekosisteminin geliştirilmesi konusu araştırılmıştır. Siber güvenlik ekosistemi, farklı disiplinlerin siber güvenliğin sağlanması ve siber risklerin asgari seviyeye indirilebilmesi amacıyla bir araya geldiği, iş birliği ve uyum içerisinde çalışmayı hedefleyen, koordinasyonun tek başlı ve yönetimin devlet üst seviyelerinden sağlandığı organizasyon yapısını ifade eder. Çalışma kapsamında, belirli ülkelerde siber güvenlik uygulamaları araştırılarak bu ülkelerde siber güvenlik ekosistemini oluşturan kurum ve kuruluşlar incelenmiştir. Türkiye özelinde, siber güvenlik ekosisteminin oluşturulmasına zemin hazırlayan çalışmalar incelenerek 2016-2019 Ulusal Siber Güvenlik Stratejisi'nde yer alan kamu kurumlarının siber güvenlik ekosisteminin geliştirilmesine etkileri değerlendirilmiştir. İncelemeler ve değerlendirmeler doğrultusunda siber güvenlik ekosisteminin geliştirilmesine katkı sağlayacak olan temel kıstaslar açıklanarak siber güvenlik ekosistemi model önerisi oluşturulmuştur.

Bilim Kodu : 92401
Anahtar Kelimeler : Siber güvenlik, siber savaş, bilişim hukuku, siber güvenlik organizasyonları, siber güvenlik ekosistemi.
Sayfa Adedi : 181
Danışman : Doç. Dr. Çelebi ULUYOL

DEVELOPING THE CYBER SECURITY ECOSYSTEM

(M.Sc. Thesis)

Zeynep Ebru IŞIK

GAZİ UNIVERSITY

INSTITUTE OF INFORMATICS

January 2019

ABSTRACT

The most important factor affecting the level of protection of country information assets against cyber risks is the existence of coordination of stakeholders in the face of these threats. In this respect, the provision of cyber security requires strong cooperation and strong coordination between different disciplines. In this study, developing the cyber security ecosystem, which is based on the coordination and cooperation of the stakeholders, has been researched in the search for a structure that can contribute to cyber security in cyber space. The cyber security ecosystem refers to the organizational structure provided by co-ordinated, single-headed, and governmental levels that aim to cooperate cooperatively, where different disciplines come together to ensure cyber security and reduce cyber risks to a minimum level. Within the scope of the study, cyber security applications were investigated in specific countries and the institutions of cyber security ecosystems in these countries were examined. Turkey in particular, the studies examining the ground for the creation of a cyber security ecosystem, the effects of public institutions in the 2016-2019 National Cyber Security Strategy on the development of cyber security ecosystem were evaluated. The basic criteria that will contribute to the development of the cyber security ecosystem are explained in the light of reviews and evaluations, and cyber security ecosystem model proposal is established.

Science Code : 92401
Key Words : Cyber security, cyber war, information law, cyber security organizations, cyber security ecosystem.
Page Number : 181
Supervisor : Assoc. Prof. Dr. Çelebi ULUYOL

TEŞEKKÜR

Tez çalışmamı fikirleriyle güçlendiren ve desteklerini esirgemeyen, çalışmanın akademik ve bilimsel değerlere bağlı bir şekilde sonuçlanmasını sağlayan saygıdeğer danışman hocam Doç. Dr. Çelebi ULUYOL'a sonsuz teşekkürlerimi sunarım.

Eşimin özverisi ve kızımın sabrıyla şekillenen, onlar olmaksızın tamamlayamayacağım bu tezin yazımı esnasında, motivasyon kaynaklarım olan güzel ailemin bütün fertlerine ayrıca teşekkür ederim.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

Sayfa

Sayfa

ŞEKİLLER LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklama
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AR-GE	Araştırma Geliştirme
BBK	Federal Sivil Koruma ve Afetler Ofisi
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
BİT	Bilgi ve İletişim Teknolojileri
BMI	Federal İçişleri Bakanlığı (Bundesministerium des Innern, für Bau und Heimat)
BT	Bilgi Teknolojileri
BTK	Bilgi Teknolojileri ve İletişim Kurumu
BTS	Bilgi Toplumu Stratejisi ve Eylem Planı
CNC	İspanya Ulusal Siber Güvenlik Konseyi
CTF	Bayrağı Yakala (Capture The Flag)
DDoS	Dağıtık Servis Dışı Bırakma (Distributed Denial of Service)
DHS	İç Güvenlik Bakanlığı
DIN	Alman Standartlar Enstitüsü
DISA	Savunma Bilgi Sistemleri Ajansı
EPDK	Enerji Piyasası Düzenleme Kurumu

Kısaltmalar	Açıklama
ETSI	Avrupa Telekomünikasyon Standartları Enstitüsü
HAVELSAN	Hava Elektronik Sanayii
HSK	Hakimler ve Savcılar Kurulu
ICS-CERT	ABD Endüstriyel Kontrol Sistemleri Bilgisayar Acil Müdahale Ekibi
ISTAC	İstanbul Tahkim Merkezi
KAMUNET	Kamu Sanal Ağı
KAYSİS	Elektronik Kamu Bilgi Yönetim Sistemi
KHK	Kanun Hükmünde Kararname
KITS	BT Güvenliği Koordinasyon Ofisi
KİK	Kamu İhale Kurumu
KKBT	Komuta, Kontrol ve Bilgi Teknolojileri
LPG	Sıvılaştırılmış Petrol Gazı
MASAK	Mali Suçları Araştırma Kurulu
MİT	Milli İstihbarat Teşkilatı Başkanlığı
MSB	Milli Savunma Bakanlığı
MÜKNET	Mükemmeliyet Ağları
NATO	Kuzey Atlantik Antlaşması Örgütü (North Atlantic Treaty Organization)
NCC	ABD Ulusal İletişim Koordinasyon Merkezi
NCCIC	ABD Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi

Kısaltmalar	Açıklama
OECD	Ekonomik Kalkınma ve İş Birliği Örgütü
RTÜK	Radyo ve Televizyon Üst Kurulu
SOME	Siber Olaylara Müdahale Ekibi
SPK	Sermaye Piyasası Kurulu
TCK	Türk Ceza Kanunu
TİB	Telekomünikasyon İletişim Başkanlığı
TÜBA	Türkiye Bilimler Akademisi Başkanlığı
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TÜBİTAK SGE	TÜBİTAK Siber Güvenlik Enstitüsü
TTGV	Türkiye Teknoloji Geliştirme Vakfı
US-CERT	ABD Ulusal Bilgisayar Acil Müdahale Ekibi
USOM	Ulusal Siber Olaylara Müdahale Merkezi
YÖK	Yükseköğretim Kurulu
YSK	Yüksek Seçim Kurulu

1. GİRİŞ

Bilgi sistemlerini kullanarak çalışan çok sayıda hizmetin varlığı ve bu hizmetlerin yol açacağı iş risklerinin giderek artması siber tehditlerle mücadele konusunda iş birliği ihtiyacını gündeme getirmiştir. Kurum ve kuruluşlar ile toplumu da içine alan geniş bir kitle arasında tehditlere karşı birlik ve koordinasyon sağlanmadıkça siber güvenliğin sağlanamayacağı açık bir gerçektir.

Giderek artan internet kullanımı, çevrimiçi yaşam ile donatılmış insan hayatı, sosyal medya kullanımına olan bağımlıkların ciddi oranda arttığı, nesnelerin interneti, endüstri 4.0 vb. yeni kavramların yoğunlukla gündemde olduğu çağımızda, siber dünya, bireysel kontrolü aşan ve yekûn halinde mücadeleyi gerektiren unsurlar içermektedir. Kötü amaçlı yazılımlar, hesap hırsızlıkları, bilgi sistemlerinin servis dışı bırakılması girişimleri, veri çalma, bilgi sızdırma, siber zorbalık ve siber ortamdaki verilerle şantajlar yapılması vb. sayısını ve yöntemini daha nice arttırabileceğimiz olumsuzlar siber dünyada karşılaşabileceğimiz tehditlere birer örnek teşkil etmektedir.

Bu olumsuzluklarla mücadelenin yalnızca bireyler, yalnızca kurumlar, yalnızca akademik çevre ve diğer yalnız girişimler ile yürütülmesi mümkün değildir. Bu anlamda siber tehditlerle mücadele etmek için birbiriyle uyum içerisinde çalışan bir "Siber Güvenlik Ekosistemi" nin geliştirilmesine ihtiyaç vardır. Kişi ve kurumların siber güvenlik alanında bilgi seviyelerini arttırmasını gerektiren, iş birliğinin önemini vurgulayan siber güvenlik ekosistemi, kendisini oluşturan paydaşların siber tehditlere topluluk halinde karşılık verebilmesini amaçlar.

Bu çalışmada siber güvenlik ekosisteminin geliştirilmesine yönelik olarak belirlenen 14 dünya ülkesinde siber güvenlik organizasyon yapıları literatür taraması yöntemiyle araştırılmıştır. Türkiye'de görev yapan kamu kurum ve kuruluşları 2016-2019 Ulusal Siber Güvenlik Stratejisi'nde yer alan görevleri esas alınarak siber güvenlik bağlamında incelenmiş, mevzuatları da göz önünde bulundurularak değerlendirilmiştir. Ülkemizde Siber güvenlik ekosisteminin geliştirilmesine zemin hazırlayan önemli çalışmaların neler olduğu çalışma kapsamında incelenmiştir. Siber güvenlik ekosistemini oluşturacak paydaşların rolleri, görevleri ve sorumluluklarını konusu irdelenmiş, 2016-2019 Ulusal Siber Güvenlik Stratejisi'nde yer alan ekosistem kavramından hareketle kamu otoritelerine öneri olarak

sunulabilecek bir model elde edilmesi amaçlanmıştır. Çalışmanın bir diğer amacı olarak siber güvenlikte güçlü bir savunma sistemi oluşturabilmenin gereği vurgulanarak, koordinasyonun neden ülke çapında geniş kapsamlı tutulması gerektiği konusu detaylandırılmıştır.

Tezin ikinci bölümünde, çalışmanın amacı, kapsamı, yöntemi ve siber güvenlik ekosisteminin oluşturmanın neden önemli ve gerekli olduğu açıklanmıştır. Bu bölümde ayrıca, siber güvenliğe ilişkin bazı önemli kavramlar çalışmaya baz oluşturması amacıyla kısaca tanımlanmıştır. Siber gücün küresel dünyanın gelecek yıllarda gidişatını nasıl belirleyebileceği konusu tartışılmıştır. Dünyanın hukuki ve politik zeminlerinde siber güvenliği sağlama zorunluluğu vurgulanarak, Tallinn El Kitabı'nın içeriğine değinilmiştir. Ulusal ve uluslararası iş birliğinin siber güvenliği sağlamaya katacağı artı değerler araştırılarak, siber güvenliğin sağlanmasında koordinasyonun önemi açıklanmıştır.

Üçüncü bölümde, Türkiye'de siber güvenlik ekosisteminin geliştirilmesine zemin hazırladığı düşünülen önemli mevzuat çalışmalarına yer verilmiştir. Bu bölüm, ülkemizde siber güvenliğe ilişkin durumu, stratejik belgeler bakımından, tarihsel olarak özet bir şekilde yansıtmaktadır.

Dördüncü bölümde, belirlenen 14 dünya ülkesi, siber güvenlik konusunda görevli olan kurum ve kuruluşlar, siber güvenlik stratejileri, ulusal siber güvenlik olaylarına müdahale merkezleri, siber güvenlik ajansları vb. kıstaslar göz önünde bulundurularak siber güvenlik ekosistemi bağlamında incelenmiştir.

Beşinci bölümde, Türkiye'de 703 nolu KHK yayımlanana değin, siber güvenlikten resmen sorumlu olan Siber Güvenlik Kurulu yapısı incelenerek, kurulu oluşturan kamu kurumlarının mevzuatlarına değinilmiştir. 2016-2019 Ulusal Siber Güvenlik Stratejisi'nde yer alan kurumların görev ve çalışma esasları, yasal mevzuatları incelenerek siber güvenlik ekosistemine ne gibi katkılar sağlayabilecekleri irdelenmiştir.

Altıncı bölümde, siber güvenlik ekosisteminin geliştirilmesi için önemli kabul edilen kıstaslara aşama aşama yer verilmiştir. Paydaşların netleşmesini sağlayabilecek olan bu konu başlıkları, kuruluşların birbirleriyle güçlü iletişim kurmalarının zorunlu olduğu gerçeğini vurgulayan kilit noktaları içermektedir. Siber güvenlik ekosistemi geliştirilirken üzerinde durulması gereken temel konu başlıkları ve bu başlıklarla ilgili öneriler bu bölümde

açıklanmıştır. Bütçelerine göre, kamu kurumları göz önünde bulundurularak, ekosistemde görev alması gereken kurumlara değinilmiştir. Kurumlar kuruluş mevzuatları çerçevesinde kendileri ile ilgili olduğu sonucuna varılan konularla ilişkilendirilmiştir. Özel sektör kuruluşları ve sivil toplum kuruluşları (STK'lar) ile diğer paydaşlar belirtilen hususlar doğrultusunda ekosisteme dahil edilmiştir. Çalışma kapsamında elde edilen bilgiler esas alınarak oluşturulan siber güvenlik ekosistemi model önerisi bu bölümde yer almakta ve açıklanmaktadır. Tezin yedinci ve son bölümünde çalışma genel olarak özetlenerek elde edilen bilgiler doğrultusunda sonuçlara ve önerilere yer verilmiştir.

2. ARAŞTIRMANIN AMACI VE SİBER GÜVENLİK EKOSİSTEMİ OLUŞTURMANIN ÖNEMİ

Teknolojinin küresel anlamda savaş anlayışını baştan aşağı değiştirdiği, uluslararası ilişkilere yön verdiği bilinmektedir. Siber tehditlerin kritik veya kritik olmayan çeşitli hizmet alanlarını hedef alması dolayısıyla, bu tehditlere güçlü bir karşılık verilmesi için güçlü bir iş birliktelik gerekmektedir. Siber güvenlik koordinasyon mekanizmasının tek yönetim organı tarafından işletilmesi; siber tehditlerle mücadelede ülkelerin dayanma gücünü, manevra kabiliyetini arttıracak önemli bir olgudur. Devlet yönetimi, yatırımcılar, akademik çevre ve bireylerin, siber güvenliği sağlamak amacıyla, birlikte çalışması gerekmektedir.

Siber güvenlik disiplinler arasında iş birliğini gerektirir. Ülkemizde siber güvenlik politikalarının uygulanmasında kurumlar arası iş birliğinde ve koordinasyon konusunda eksiklikler olduğu gözlenmiştir. Paydaşlar arasında, rollerin belirsizliği iletişim kopukluklarına neden olmaktadır. Ülkemizde siber güvenlik politikalarını yürüten kurumlar ve organizasyon yapısı, 703 nolu KHK ile değişmiştir. Kritik altyapıların güvenliğinin sağlanmasına ilişkin spesifik politikalar bulunmamaktadır. Farklı kuruluşların siber güvenliğe ilişkin farklı çalışmalar yürüttüğü, farklı mali kaynak tahsis ettikleri gözlenmiştir.

Sayılan bu problemler göz önüne alındığında, 2016-2019 Ulusal Siber Güvenlik Stratejisi'nde eylem maddesi olarak yer alan, "siber güvenlik ekosisteminin oluşturulması" hedefine ulaşmak amacıyla ülkemizin siber güvenliğe ilişkin organizasyon yapısında değişiklikler ve geliştirmeler gerekmektedir. Siber güvenlik ekosisteminin geliştirilmesi ülkemizde siber güvenlik sorunlarının çözümlenmesine katkı sağlayacak bir unsurdur.

Siber güvenlik risklerinin bütüncül olarak ele alınması ve yönetimini de ifade eden siber güvenlik ekosistemi, siber risklerle, ekosistemi oluşturan tüm paydaşların katkısıyla mücadeleyi hedeflemektedir. Siber güvenliğin sağlanmasında ulusal ve uluslararası iş birliği, koordinasyonun gerekliliği ve siber güvenlik ekosistemi oluşturmanın önemi bu bölümde açıklanmaktadır.

Çalışma kapsamında, siber güvenlik ekosisteminin geliştirilmesine katkı sağlayacağı düşünülen;

- Ülkemizde ekosistemin oluşmasına zemin hazırlayan çalışmaların neler olduğu,

- Belirlenen ülkelerde siber güvenlik ekosisteminin unsurlarının neler olduğu ve süreçlerin nasıl işletildiği,
- 2016-2019 Ulusal Siber Güvenlik Stratejisi'ne göre siber güvenlikle ilgili sorumlulukları bulunan kamu kurumlarının incelenmesi,
- Siber güvenlik ekosistemin geliştirilmesinde önemli kıstaslar,

konuları esas alınarak literatür taraması yapılmıştır. Ülkemizdeki mevcut durumu incelemek, örnek ülke uygulamalarını incelemek, ülkemizde sürece ilişkin hangi alanlarda eksiklikler olduğunu araştırmak ve ekosistemin geliştirilmesine yönelik ülkemizde ne gibi çalışmalar yapılabileceğini vurgulamak, çalışmanın amaçları arasındadır.

Temel araştırma yaklaşımı benimsenerek hazırlanan bu tez çalışmasının öncelikli amacı ise; "siber güvenlik ekosistemi" kavramına ilişkin ülkemizdeki bilgi düzeyinin artmasına katkı sağlamaktır. Konuya ilgi duyan diğer araştırmacılar ve uzmanlar tarafından değerlendirilmesi beklenen bu çalışma, siber güvenlik ekosistemi paydaşlarının bilgi dağarcığını genişletmeyi ve dünyada bu alanda ne tür çalışmalar yürütüldüğü konusunda merakını gidermeyi hedeflemektedir [1]. Siber güvenlik ekosistemi kavramına ilişkin ilerleyen zamanlarda geliştirilebilecek uygulamalı araştırmalarda, bilimsel araştırma sahiplerinin kullanacağı araçlara kaynak olmak, çalışmanın amaçları arasındadır [2]. Literatür taraması yöntemine başvurularak elde edilen bilgiler neticesinde oluşturulan siber güvenlik ekosistemi model önerisi, çalışmanın altıncı bölümünde yer almaktadır.

Araştırma, ülkemizde daha önce diğer araştırmacılar tarafından araştırılmamış bir konu olması nedeniyle özgün bir araştırma konusuna sahiptir. Öte yandan gözlem zorluğu, dünya ülkelerinde belgelendirmelerin az olması, belgelendirmelerin ilgili ülkenin ana dilinde yazılmış olması, İngilizce metinlerin az olması, konuya ilişkin bilimsel kaynakların yetersiz kalması gibi etkenler, araştırma çerçevesini ve erişilen bilgileri sınırlamıştır.

2.1. Siber Güvenlik ile İlgili Bazı Önemli Kavramlar

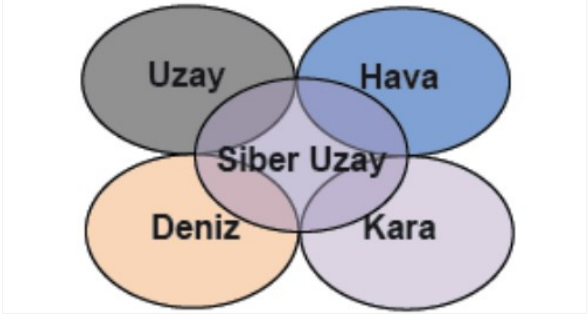
Temel siber güvenlik kavramları olan siber uzay, siber saldırılar, siber suçlar, siber istihbarat, siber savaş, siber güvenlik, siber süreklilik ve kritik altyapılar çalışmaya baz oluşturması amacıyla bu bölümde açıklanmıştır.

2.1.1. Siber uzay

Siber uzay kavramı, bilgisayarların kendi arasındaki iletişimi, bilgi sistemleri altyapısını kullanarak çalışan tüm elektronik cihazlar arası iletişim ile ağda etkileşim halinde olan insanları da içeren soyut ortamı ifade eder [3]. Verilerin aktığı bu elektronik iletişim ortamı temelde sanal bir alanı ifade etmesine rağmen, insanların yoğun etkileşimi sağlamasına olanak tanıması bakımından gerçek dünya ile giderek eş duruma gelmeye başlamıştır.

Amerika Birleşik Devletleri (ABD) Savunma Bakanlığı ve Avrupa Birliği (AB) Komisyonu tarafından siber alanın, küresel elektronik bir ortam olduğu ifade edilmektedir [4]. Siber ortamda yalnızca kişisel bilgisayarlara ait veriler değil, sistem cihazlarının birbirleriyle haberleşmeleri esnasında oluşan veriler de akış halindedir. Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI) raporunda siber uzay; herhangi bir fiziksel formda bulunmayan, teknoloji cihazları ve bunlara bağlı ağlar aracılığıyla internet üzerindeki insanların, yazılımların ve hizmetlerin etkileşimlerinden kaynaklanan karmaşık ortam olarak tanımlanmaktadır [5].

Beşinci harp meydanı olarak kabul edilen siber uzay, insan yapımı ilk çevredir. Siber uzay diğer doğal çevrelerin aksine kolaylıkla kontrol edilemeyecek bir alandır. Siber uzayda yer alan her varlık bir diğeri ile kurduğu iletişim neticesinde hukuki konularda kullanılabilecek dijital deliller ve takip edilebilir nitelikli teknik izler oluşturmasına rağmen, anonimlik ve inkar edilebilirlik gibi riskleri barındırması sebebiyle siber ortamda kimlik tespiti oldukça zordur.



Şekil 2.1. Beşinci harekat alanı olarak “siber uzay” [6]

Siber uzayda güvenliğin tam anlamıyla sağlanması, alanın kontrol edilebilirliği bakımından günümüz şartlarında düşük bir ihtimal olarak görünmektedir. Ancak bir dizi önlem alınarak,

özellikle de organizasyonlar arasında iş birlikleri sağlanarak siber uzayın gerçek dünyaya yansıtacağı güvenlik risklerini minimize etmek mümkündür.

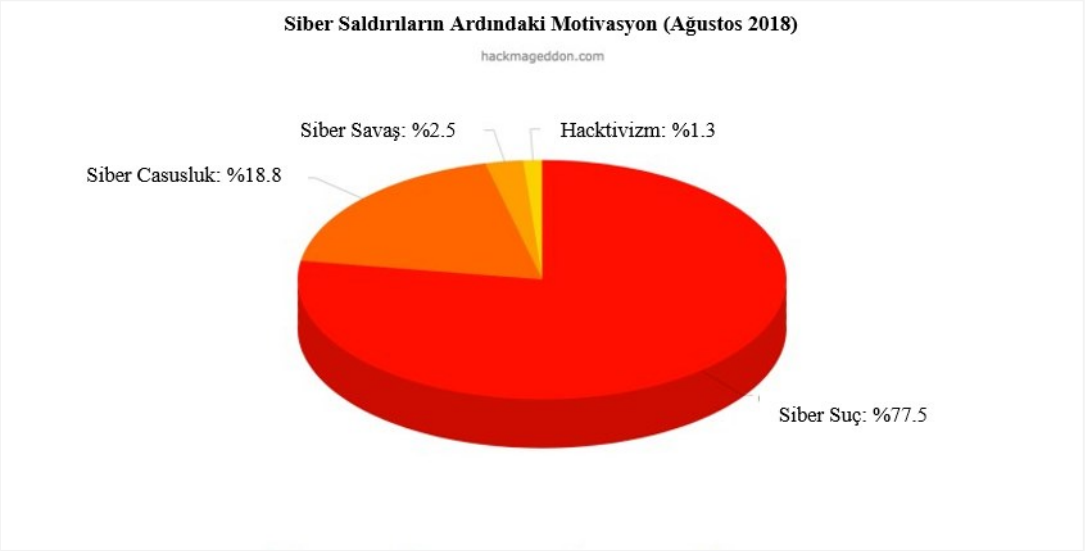
Bilgi sistemleri altyapısında çalışan kritik iş süreçlerinin belirlenmesi ve bu süreçlerin risklerini göz önünde bulundurarak hareket edilmesi diğer birçok savunma ve saldırı alanına etki etmektedir. Bir ülkede siber güvenliğin üst seviyelerde olması, teknolojinin getirdiği avantajları kullanırken olası risklerin yol açacağı büyük tehditlere hazırlıklı olmayı sağlamanın yanında, ülkelerin kara, hava, deniz ve uzay ortamlarındaki başarısının ve gücünün katlanarak artmasına da katkı sağlayacaktır.

Siber uzayın sayısız tehditlerle kuşatılmış olması siber ortamda güvenliği sağlamaya yönelik fikirlerin ortaya çıkmasını tetiklemiştir. Önceleri temel sayısal işlemler için kullanılan iletişim ağları artık her türlü veriye ev sahipliği yapmaktadır. Bu verilerin korunması bireyler, kurumlar ve ülkeler açısından önem teşkil etmektedir. Siber güvenlik kavramının özü, siber uzayda güvenliktir.

2.1.2. Siber saldırı ve siber suç

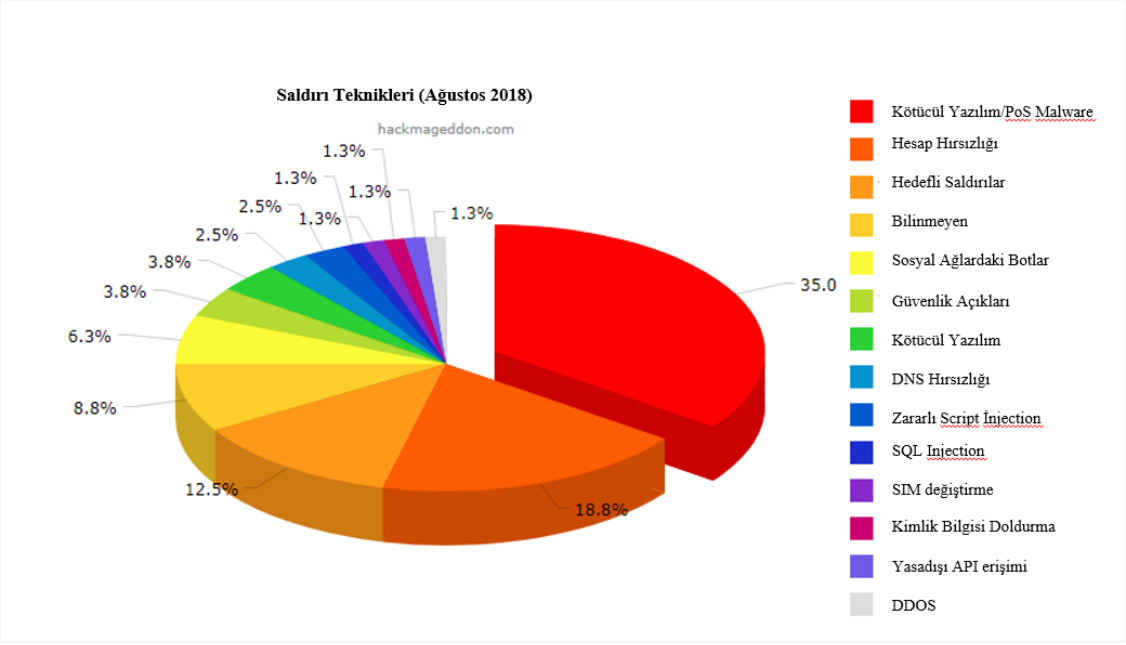
Siber uzaydan, bilgi sistemlerine izinsiz olarak girişi hedefleyen, bu sistemlere uzun ya da kısa vadede zarar vermeyi amaçlayan, veri çalma veya iz sürme vb. niyetlerle ağdan sistemlere sızan her türlü kötü niyetli girişim siber saldırı kavramını oluşturur.

Siber saldırıların birçok olumsuz etkisi olabilir. Bu durumun somut örnekleri, sermaye kaybı, hukuki süreçlerin doğuracağı cezai işlemlere maruz kalınması iken; soyut ve daha ciddi olarak düşünülebilecek etkileri ise güven ve itibar kaybıdır. Fikri mülkiyet hak ihlalleri ile doğan rekabet gücü kayıpları, müşteriler ve iş ortakları nezdinde itimat kaybı, dijital varlıklarda yaşanan tehlikeler ile zora girebilecek şirket yapısı ve hepsi bir araya konduğunda oluşması muhtemel marka ve kurum imajına yönelik güvensizlikler ve itibar kayıpları bir kurumun hisse fiyatını bir anda aşağı doğru çekebilmekte ve bazı uç durumlarda şirketleri iflasa dahi zorlayabilmektedir [7].



Şekil 2.2. Hackmageddon verilerine göre ağustos 2018'de siber saldırılar [8]

Ağustos 2018 istatistiki verilerine göre siber saldırıların temelinde %77,5 oranıyla siber suçlar olduğu görülmektedir. Siber casusluk amaçlı saldırıların Ağustos 2018 itibariyle %18,8 oranında oluğu, hactivisim amaçlı saldırıların ise %1.3 olarak kaydedildiği görülmektedir. Siber savaş amaçlı saldırılar ise bu araştırmaya göre önceki yıllarla kıyaslandığında artış göstermiş olup %2,5 oranındadır.



Şekil 2.3. Hackmaggedon verilerine göre ağustos 2018 saldırı vektörleri [8]

Şekil 2.3'te ifade edildiği gibi ilgili çalışmanın saldırı vektörleri grafiği incelendiğinde, Ağustos 2018 itibariyle %35 oranıyla kötücül yazılımlar ilk sırada yer alan saldırı tipidir. Bu

saldırıları, %18,8 oranı ile hesap hırsızlığı saldırıları takip ederken, üçüncü sırada %12,5 oranıyla hedefli saldırılar yer almıştır.

Siber saldırıların yasal olarak cezai yaptırımlarla karşılık görmesi siber suç kavramının hukuk sisteminde tanımlanmasını gerekli kılmıştır. Siber suçlar kimi zaman bilişim suçları, bilgisayar suçları, teknoloji suçu gibi farklı terimlerle ifade edilmektedir [9]. Yasalarımızda, direkt olarak "siber suç" ifadesi olarak değil "bilişim suçları" olarak yer bulmaktadır.

Siber suç, bilişim sistemlerinin güvenliğini tehlikeye sokmayı kasten veya kasıtsız olarak neden olabilecek eylemleri kapsar. Yetki olmaksızın, bir bilişim sisteminde var olan verilerin izinsiz bir şekilde kaydedilmesi taşınması, kasten bozulması, kopyalanması gibi eylemleri içeren bir dizi farklı durum da siber suç kapsamında düşünülmektedir. Siber suçlar, özel hayatın gizliliğini ihlal, müstehcenlik içeren yayınlar, terörün siber ortamlar vasıtasıyla propagandasının ve finansmanının yapılması gibi birçok farklı boyutta da ele alınabilmektedir. Siber suç işlenmesi için bir bilişim sisteminin kullanılmış olması gerekmektedir [10].

2.1.3. Siber istihbarat

Siber güvenliğe ilişkin gelişmelerin arttığı günümüz teknolojisinde, istihbarat bilgilerinin edinilmesi, siber savaşlarda üstünlük göstergesi olarak kabul edilmektedir. İstihbarat konusunda güçlü olabilmek, güçlü teknolojik altyapıyı ve nitelikli insan kaynağını gerektirir. Olası zafiyetlere karşı korunma mekanizmalarının işletilmesi ve siber tehditlere karşı mücadelenin yürütülmesi için siber istihbarat bilgilerinin güvenilir olması şarttır.

Öte yandan, paylaşıma açılmış her türlü veri doğru analizler yapılarak siber istihbarat bilgisine dönüşebilmektedir. Sosyal paylaşım sitelerinin güçlü ülkeler tarafından bu amaçlar için kullanıldığı yaygınlıkla gündeme gelen bir konudur. Bu nedenle bir ülkenin, salt teknolojik ilerleme kaydetmeye odaklanması, diğer ülkelerde olan teknik gelişmelere gözlerini kapatarak politikalar yürütmesi stratejik bir yanılgı olacaktır. Diğer ülkelerde olan teknik gelişmelerin takip edilmesi, edinilen bilgiler ışığında ülke içi değerlendirmelerin düzenli olarak yapılması, yeni politikaların geliştirilmesi hem siyasi hem teknik üstünlüğün elde edilmesine katkı sağlayacaktır. Tüm bu nedenlerle güvenilir siber istihbarat bilgilerinin edinilmesi ve bu bilgilerin doğru tasnifi ülkeler açısından önem teşkil etmektedir.

Hayatın dijitalleşmesi, ülkelerin istihbarat elde etme biçimine de etki etmiştir. Dijital kaynaklar üzerinden ülkelere veya kişilere dair çeşitli bilgiler elde edilebilmektedir. Çeşitli elektronik hizmetler o hizmetin üreticisine bilgi akışı sağlayabilme gücüne sahip bir istihbarat kaynağına dönüşebilmektedir [11].

Siber uzayın harbin beşinci boyutu kabul edilmesi siber istihbaratı da önemli kılmaktadır. Siber harp alanında elde edilen galibiyetler, diğer savaş alanlarında düşman kabul edilen tarafların çatışma kararlığını kırabilecek güçtedir. Siber savaşın diğer savaş alanlarına olan bu etkisi, güçlü siber istihbarata ve güvenilir siber istihbarat kaynaklarına duyulan gereği göstermektedir [12].

Ulusal istihbarat servisleri ve ulusal hükümetler kendi aralarında tartışma kanalları açmalı ve casusluk faaliyetinin aşırıya kaçırılmaması veya düşmanca niyet göstermek gibi yanlış anlaşılmaması sağlanmalıdır [13]. Türkiye'de istihbarat topluluğu incelendiğinde Şekil 2.4'te yer alan yapı ile karşılaşılmaktadır.

Şekil 2.4. Türk istihbarat topluluğu [26]

Türk istihbarat topluluğu, genel olarak askeri ve sivil istihbarat birimleri olarak gruplandırılabilir. Askeri istihbarat, Genelkurmay Başkanlığı'na, kolluk istihbaratı İçişleri Bakanlığı'na, dış istihbarat ise Başbakan'a bağlı teşkilatlandırılmıştır [14]. 2937 sayılı Kanun'da 2017 yılında yapılan değişiklikler sonucu Milli İstihbarat Teşkilatı Cumhurbaşkanı'na bağlanmıştır. 2018 yılında ise devlet yapılanmasına ilişkin yeni

düzenlemeler neticesinde teşkilatın adı Milli İstihbarat Teşkilatı Başkanlığı olarak değiştirilmiş, Başbakanlık makamı kaldırılmış ve Kamu Düzeni ve Güvenliği Müsteşarlığı görev ve yetkileri İçişleri Bakanlığı'na devredilmiştir.

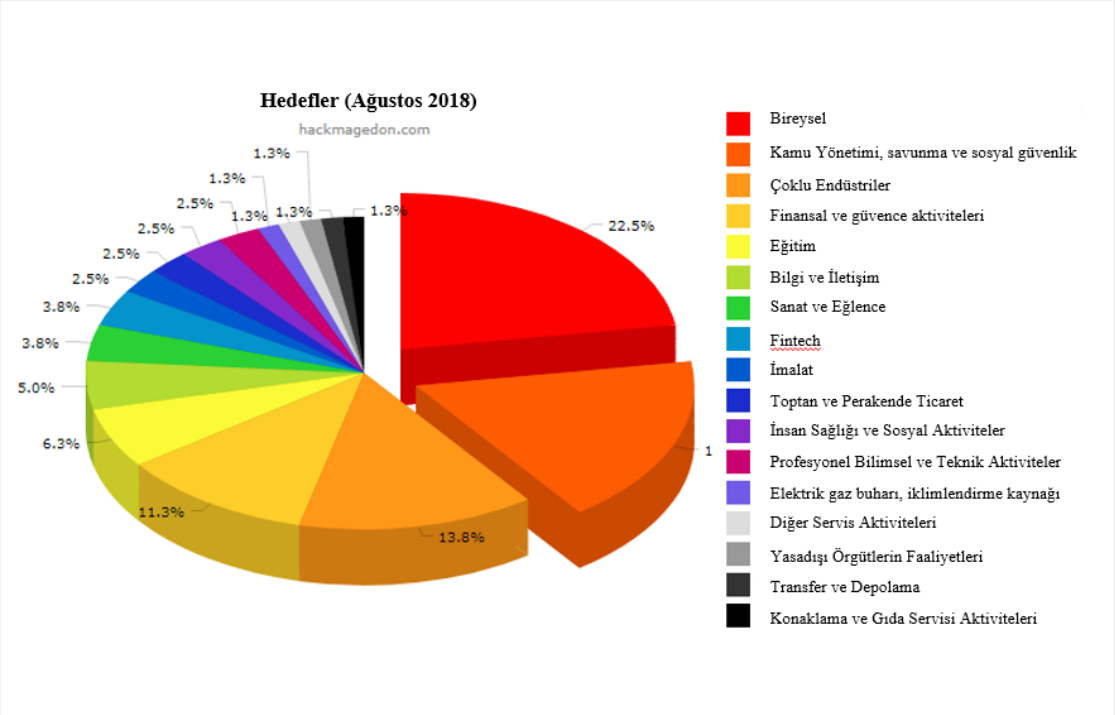
2.1.4. Siber savaş

Bilgisayar ağları kullanılarak devletlerin birbirlerinin sistemlerine yetkisiz ve izinsiz giriş yapması, verilerini değiştirmesi, çalması, kopyalaması, herhangi bir zarar vermesi, veri akışını veya hizmetleri kesintiye uğratması siber savaş olarak tanımlanabilmektedir [13].

Clarke ve Knake, siber savaşların gizli varlığını çatışma amacında olan ülkelerin savaş hazırlıkları yaptığını öne sürerek vurgulamaktadır. Bazı ülkeler, çeşitli tuzaklar ve dijital bombalar kurarak olası savaş tehditlerine ön savunma mekanizması kurmaktadırlar. Gelecekte fiziksel savaşların siber unsurlarla desteklenmesi mümkün görünmekte, hatta tek başına siber harplerin yaşanması ihtimali artmaktadır [13].

Siber savaş küreseldir. Savaş henüz başlamadan çeşitli casus yazılımlar tarafından sistem yönetimi ele geçirilmiş olan yüzlerce köle bilgisayar aynı anda yönetilerek siber silaha dönüşebilmektedir. Bu durumda dünyanın farklı ülkelerine yayılmış her bir uç bilgisayar birer savaş unsuru olarak çalışmaya başlar. Birçok ülke anında devreye girer [13].

Hackmageddon internet sitesinden alınan istatistiki verilere göre, siber saldırıların Ağustos 2018 itibariyle dağılımı Şekil 2.5'te yer almaktadır. Araştırmaya göre siber saldırılarda %22,5 oranıyla bireyler hedef alınmaktadır. Bu saldırıları, %17,5 oranıyla kamu yönetimi, savunma ve sosyal güvenlik ile ilgili sektörleri hedef alan saldırılar takip etmektedir. Siber saldırıların %13,8'i endüstri sektörünü, %11,3'ü finans ve güvence sektörünü hedef almaktadır.



Şekil 2.5. Hackmageddon verilerine göre ağustos 2018 siber saldırı hedefleri [8]

Uluslararası hukuk kurallarının siber savaş konusunda daha belirgin hale gelmesiyle, Şekil 2.5'te ifade edilen %22,5 gibi önemli bir orana sahip devlet yönetimi savunma, sosyal güvenlik alanlarında yapılan siber saldırıların ülkeler arasında siber savaşları tetikleyebileceği tahmin edilmektedir.

2.1.5. Siber güvenlik

Anlam bakımından birbirine yakın tanımlamaları bulunan siber güvenlik kavramı, siber uzayda güvenliğin sağlanmasına odaklanmaktadır. Siber güvenlik; siber saldırılara karşı en basit bireysel korunma yöntemlerinden, küresel tehditlere karşı ülke siyasi perspektifiyle savunma sistemlerinin geliştirilmesine kadar çok geniş bir yelpazeyi içerir.

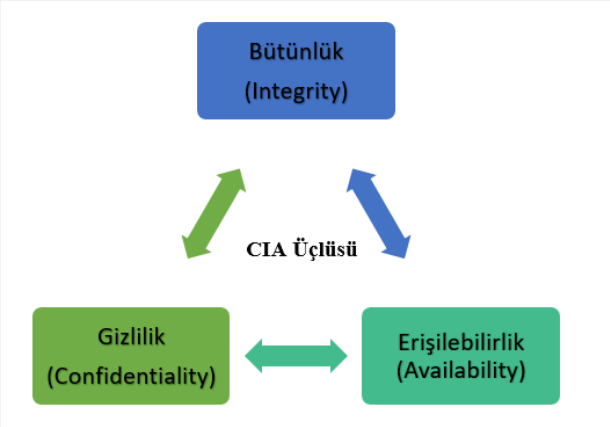
ETSI teknik raporunda yer alan tanımıyla siber güvenlik: "siber çevre ve organizasyon ile kullanıcının varlıklarını korumak için kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, kılavuzlar, risk yönetimi yaklaşımları, eylemler, eğitim, en iyi uygulamalar, güvence ve teknolojiler topluluğudur" [5].

Siber güvenlik, siber ortamda kullanımda, dolaşımda ve depo halinde olan verilerin korunmasını, bu verileri korumayı amaçlayan politika ve prosedürleri, güvenliği sağlayacak olan her türlü teknolojiyi kapsamaktadır. Kuruluşların ve kişilerin siber ortamda barındırdığı

varlıkların hepsini korumayı amaçlayan siber güvenlik, siber ortam tehditlerine karşı güncel teknik gelişmelerin takibi yapılması, politika ve prosedürlerin düzenli olarak gözden geçirilmesi ve uygulanması suretiyle sürekli mücadeleyi gerektirir [15].

Ulaştırma ve Altyapı Bakanlığı'nın (eski adıyla Ulaştırma, Denizcilik ve Haberleşme Bakanlığı) yayımladığı 2016-2019 Ulusal Siber Güvenlik Stratejisi'nde siber güvenliğe ilişkin olarak bilişim sistemlerinin saldırılara karşı korunması, siber uzayda işlenen verilerin bilgi güvenliğinin gereklerine uygun olarak iletilmesi, saklanması, siber güvenlik ihlallerinin tespiti ve siber saldırılara karşı cevapların oluşturulması konuları vurgulanmıştır [16].

Siber güvenliğin ve bilgi güvenliğinin temel prensipleri arasında ilk olarak "Gizlilik (Confidentiality), Bütünlük (Integrity) ve Erişilebilirlik (Availability)" kavramlarını anlamak faydalı olacaktır. Bu temel prensipler kısaca "CIA Üçlüsü" olarak tabir edilmektedir.



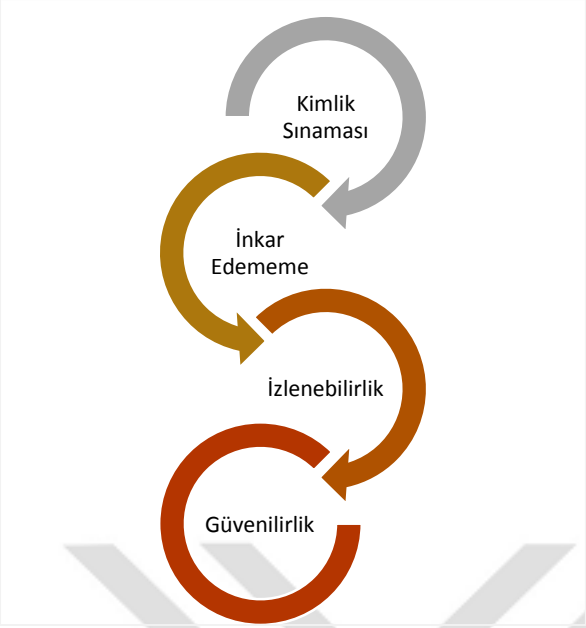
Şekil 2.6. CIA üçlüsü

Gizlilik: Bilginin yalnızca yetkili kişiler tarafından kullanılabilir olmasını ifade eder [17].

Bütünlük: Bilgilerin eksiksiz, tam, tutarlı ve doğru olmasını ifade eder [18].

Erişilebilirlik: Bilginin, yetki sahibi kişiler tarafından istenilen anda erişime açık ve kullanılabilir durumda olmasını ifade eder [16].

Temel üç prensibin yanı sıra, Kimlik Sınaması (Authentication), İnkâr Edememe (Non-Repudiation), İzlenebilirlik (Accountability), Güvenilirlik (Reliability-Consistency) prensipleri de bilgi güvenliğinin önemli prensipleri arasında yer almaktadır.



Şekil 2.7. Bilgi güvenliğinin diğer önemli prensipleri

Kimlik Sınaması: Kimlik doğrulaması olarak da ifade edilen kimlik sınaması, veriyi gönderen kişinin doğrulanmasını ifade etmektedir. Alıcı tarafın, göndericinin iddia ettiği kişi olduğuna ikna olmasına imkan tanır. Sayısal imza ve benzeri teknolojiler çeşitli kriptografik algoritmalar kullanarak kimlik sınaması sağlamaktadır. Öte yandan bir işletim sistemine giriş yapabilmek için kullanıcı adı şifre girilmesi de bilgi güvenliğinin bu prensibini destekleyecek niteliktedir.

İnkar Edememe: Açık anahtarlı şifreleme teknikleri kullanılarak veriyi gönderen ve veriyi alan tarafların ilettiği verileri inkar edememesi sağlanır [17].

İzlenebilirlik: Bilgi sistemleri kullanılarak yapılan her türlü işlemin daha sonra analiz edilmek ve ihtiyaç durumunda incelenebilmek üzere kayıt altına alınmasıdır.

Güvenilirlik: Bir bilgi sisteminin tahmin edilen davranışı ile çalışması sonrası elde edilen çıktılarının kıyaslanması sonrası denk olması gerektiğini ifade eder. Sistemin tasarlandığı şekliyle tutarlı bir şekilde çalışmasını da ifade eder [19].

Dünyadaki tüm depolama birimlerinin toplam boyutu son yıllarda zettabaytlar ile ifade edilmektedir. Sağlık verilerinden kişisel verilere kadar gerçek dünyaya ait hemen her veri siber ortamlarda saklanmaktadır. Çoğu zaman önemsiz görülen farklı nitelikteki veriler artık sosyal medya siteleri yoluyla siber ortamda birçok kişi veya kurum ile paylaşılmaktadır. İnternet tarayıcıları kullanılarak yapılan aramalar işlenerek daha anlamlı veriler haline

getirilmekte, hatta çeşitli yöntemlerle siyasi, ticari vb. toplumsal eğilimleri analiz etme çalışmaları yapılmaktadır.

Siber ortamda teknik kabiliyetleri gelişmiş kişi, kurum ve ülkeler ulusal veya uluslararası yasaların izin verdiği ölçüde, çoğu zaman ise illegal yollarla siber ortamdaki her türlü veriyi, ihtiyacı ve amacı doğrultusunda dilediği şekilde kullanabilme imkanına sahiptir. Dolayısıyla siber ortamda saklanan her veri anlamlı bir bilgiye dönüştüğünde veri sahibi /sahipleri, kurumlar, hatta ülkeler açısından güvenlik riski teşkil etmektedir.

Tüm bu risklerin olabilecek en alt seviyeye indirgenmesi siber güvenliğin konusunu oluşturmaktadır. Gerçek dünyanın aynası olma yolunda ilerleyen siber ortam, siber güvenlik prensipleri temel alınarak atılan adımlarla, teknik envanterlerin iletişim ağlarına uygun konumlandırılmasıyla, kullanılan yazılımlarda güvenlik konusunda alınan önlemlerle ve siber tehditlere karşı organizasyonlar arası iş birliğiyle hem bireyler, hem de ülkeler için daha güvenli bir alan haline dönüşecektir.

2.1.6. Siber süreklilik

Siber süreklilik, siber güvenlik ve iş sürekliliğinin birleşimini ifade etmektedir. Siber güvenlik stratejilerinde süreklilik yalnızca potansiyel siber saldırılara karşı savunmayı değil, aynı zamanda başarılı bir saldırı mekanizmasını işletmeyi de amaçlar. Siber güvenlik ekosisteminin geliştirilmesiyle tüm kamu kurumları ve özel kuruluşlarda siber sürekliliği destekleyen uluslararası standartlar (Örn. ISO270XX) uygulanarak asgari seviyede iş birliktelik ve eş düzeyde farkındalık sağlanmış olacaktır.

Siber sürekliliğin gereği olarak kurumların, siber güvenlik tehditlerinden kaynaklanan potansiyel felaketlere hazırlıklı olması, bu alandaki riskleri tanımlayıp, tespit etmesi, olası felaketleri engelleyici önlemler alması, olası felaketlerde güçlü karşı tepki verebilme kabiliyetinin geliştirmesi beklenmektedir. Yeni teknolojilere paralel olarak kendini yenilemeyi öngören siber süreklilik kavramının ekosistemde yer bulması neticesinde siber güvenlik ekosistemi paydaşlarıyla birlikte canlı gelişim gösteren bir yapı olarak işleyecektir.

2.1.7. Kritik altyapılar

Kritik altyapıların hangi bilgi sistemleri kaynaklarını ifade ettiğinin kesin ve net olarak tanımının yapılması farklılık arz etmektedir. Ancak temel olarak tasnif edildiğinde;

insanoğlunun temel hayat akışını en derinden etkileyecek ve toplumsal yaşantıyı büyük oranda sekteye uğratabilecek bilgi sistemleri altyapıları kritik altyapılar olarak nitelendirilebilir. Örneğin, su, doğalgaz, elektrik, sağlık ve bankacılık gibi önemli sektörlerde yaşanabilecek bilgi sistemleri kaynaklı problemler, toplumsal hayatı yüksek oranda olumsuz etkileyebilecektir [20].

Ulaştırma ve Altyapı Bakanlığı'nın yayımladığı 2016-2019 Ulusal Siber Güvenlik Stratejisi'nde kritik altyapılar, bilgi güvenliğinin temelini oluşturan unsurlar zedelendiğinde bireyi ve toplumu önemli ölçüde etkileyebilecek zararlar ortaya çıkarabilecek, ülke güvenliğini ulusal düzeyde bozabilecek derecede hassas bir konumda bulunan teknolojik altyapılar olduğuna değinilmiştir. Ayrıca eylem planında; bankacılık-finans, enerji, su, ulaştırma, elektronik-haberleşme sektörleri kritik sektörler olarak tanımlanmıştır [16]. Öte yandan SGK, vergi daireleri, eczaneler gibi bazı kurumların verdiği hizmetler de kritik sistemler olarak tanımlanabilir.

Ağustos 2001'de Amerika Birleşik Devletleri'nin Kaliforniya eyaletinin büyük kısmına elektrik dağıtımında kullanılan bilgisayar sistemine siber saldırganların yetkisiz bir şekilde girdiği medyada yer almıştır. Sızmanın iki hafta boyunca gerçekleştiği tespit edilmiştir. Elektrik dağıtımında kullanılan SCADA sistemine internetten erişilebilmektedir. Sızmaya sebep olan sistem açıklığının bilgisayar korsanları sisteme herhangi bir zarar vermeden kapatıldığı bildirilmiştir. Olay enerji endüstrisinde yaşanan ilk siber saldırılardan birisi olduğu için ciddi bir şok dalgası yaratmıştır [21].

Ohio eyaletindeki Davis-Besse nükleer santralindeki özel bir bilgisayar ağına "Slammer" isimli zararlı yazılım bulaşmış ve bu zararlı yazılım çeşitli sistemleri belirli bir süre devre dışı bırakmıştır. Basında yer alan haberlere göre santral personeli kurum ağı önünde yer alan güvenlik duvarı tarafından korunduklarını düşünürken bu olayın gerçekleşmesi şaşkınlığa yol açmıştır. Bu örnekte de santralin özel bilgisayar ağı internet ile bağlantılı durumdadır. Güvenlik duvarları internetten gelen tehditlere karşı %100 koruma sağlamaz. Güvenlik duvarları servis bazında kısıtlama sağlarlar. İzin verilen servisler üzerinden yapılan sızmaları ve illegal siber aktiviteleri güvenlik duvarları tespit edip engelleyemeyebilir [21].

Stuxnet, bu altyapıları hedef alan ve yaygın olarak bilinen siber saldırı yazılımlarından biridir. Bu zararlı yazılım SCADA sistemlerine bulaştırılarak nükleer sistemler hedef alınmıştır. Çalışma şekli incelendiğinde, öncelikle, sadece nükleer santrallerde kullanılan

belli marka ve model SCADA sistemlerini hedef alan bir yazılımdır. Eğer bulaştığı bilgi sisteminde hedef aldığı SCADA sistemi yoksa kendisini etkisiz hale getirmekte ve sisteme bir zarar vermemektedir. Zararlı yazılımların hazırlanmasında yaygın olarak kullanılmayan bir programlama diliyle hazırlanmıştır. Microsoft Windows işletim sisteminin o zamana kadar bilinmeyen dört adet açıklığını aynı anda kullanmıştır. Ayrıca, işletim sistemi seviyesinde güvenin oluşması ve kolaylıkla yayılması için Güney Kore'deki iki adet firmaya ait sayısal sertifikaların gizli anahtarlarını kullanmıştır. Stuxnet yazılımı tespit edilince yapılan inceleme sonucunda bu anahtarların çalındığı ortaya çıkmıştır. Bu özelliklerinde de görüldüğü üzere Stuxnet kendisinden önceki zararlı yazılımların hiç birisine birçok yönden benzememektedir. Gerek bu özellikleri gerekse hedef aldığı sistemler göz önüne alındığı zaman bireylerden ziyade ülkeler seviyesinde bir çalışma sonucunda oluşturulmuş olması küçük bir ihtimal değildir [21].

Örneklerden yola çıkıldığında; su yönetimi sistemlerine karşı düzenlenecek siber saldırılar sonrası ortaya çıkabilecek salgın hastalıklardan, bankacılık veya enerji sektörlerinde yaşanabilecek kesintilerin neden olabileceği kamu düzeninin bozulmasına kadar geniş bir yelpazede karşımıza çıkabilecek siber güvenlik zafiyetlerine karşı, kritik altyapıların, siber alanda özenle korunması gerekmektedir. Fiziksel olarak alınan önlemler, bilgi sistemleri altyapılarıyla iç içe çalışan kritik altyapılar için artık yetersizdir. Bu nedenle kritik altyapılarda yaşanabilecek olumsuzlukların önüne geçebilmek adına belirli periyotlarla, belirlenmiş bilgi güvenliği testlerinin yapılması gerekmektedir. Çalışan eğitimlerine önem verilmeli, siber saldırganların kritik verilere erişimde, kritik altyapı çalışanlarına ait şifrelere, bilgi istismarı yöntemleriyle daha kolay ulaşılabildiği gerçeği göz önünde bulundurulmalıdır.

Kritik altyapıların sürekli çalışmaları ve devamlı hizmet vermeleri gerekmektedir. Büyük felaketlerin oluşmasına zemin hazırlayacak risklerin önceden tespit edilmesine yönelik bilgi güvenliği testlerinin uygulanması, kesintisiz hizmet anlayışının nedeniyle daha spesifik zaman aralıklarında yapılmak durumundadır. Gün içinde oldukça fazla çevrimiçi işlem gerçekleştiren bankalar, bu gibi güvenlik testlerini gece saatlerinde yaparak bankacılık işlemlerinin aksamadan devam etmesini sağlayabilmektedir. Öte yandan, sürekli açık kalması ve günlük olarak belirli bir miktar enerji üretimi yapması gereken bir elektrik üretim tesisinde, sızma testlerinin yapılması, büyük bir maddi gelir kaybına neden olacaktır [22].

2.2. Siber Tehditlerin Küreselleşmesi

İnsanlar ve makineler birbirleriyle hiç olmadığı kadar yoğun iletişim halindedir. Endüstri ve sanayi üretimleri, montajlar, iş akışları, tedarik süreçleri dünyanın farklı lokasyonlarından yürütülen birçok işlem mesafe sınırı tanımamaktadır. Yalnızca internetin olması, makinelerin ve dolayısıyla insanların protokoller aracılığıyla iletişimde kalmasına, sürekli iletişim halinde kalarak üretim sağlamasına imkanı tanımaktadır. Bu durum çeşitli riskleri de barındırmaktadır. Sistematik riskler, küreselleşen iletişimde karşılıklı bağımlılık nedeniyle dalga dalga yayılabilmektedir. Hızlı yayılım kabiliyetine sahip bu riskler hayatın birçok çeşitli alanına etki edebilmektedir [23].

Siber uzayda caydırıcılık konusu ise saldırganın tespit edilmesinde yaşanan zorluklar ve anonimlik nedeniyle pek mümkün değildir. İhlallerin tespitiyle kıyaslandığında ihlali gerçekleştirenin kimlik tespiti ve iz takibi zordur. Saldırganlar suçu atfedeceği ve suç ile ilgisi bulunmayan kişilerin bilgisayarını kullanmak vasıtasıyla da siber saldırılar gerçekleştirmektedir. Net olmayan bu gibi durumlarla birlikte, siber tehditlerle mücadelede ve siber suçlara karşı caydırıcılığın sağlanmasında küresel bir yapı henüz bulunmamaktadır. [23] Kimi durumlarda siber saldırı amacıyla geliştirilen yazılımlar yazılımı geliştirenlerin aleyhine de çalışabilmektedir.

1982 yılında Sibirya'da yaşanan doğalgaz patlaması, siber ajanlık yapması amacıyla geliştirilen bir yazılımın küresel bir siber tehdide dönüşmesine örnektir. Rusya, 1982'de Kanada'da doğalgaz hatlarını kontrol etmek için kullanılan bir yazılımı siber ajanlık yaparak çalmayı amaçlamıştır. Ancak durumun farkına varılmasıyla, Amerikalılar tarafından bu ajan yazılımın içerisine virüs yerleştirilmiştir. Bir süre sonra virüs tarafından bozulan yazılım boru hatlarındaki akış oranını yükselterek boruların patlamasına sebep olmuştur [24].

1990 yılında Irak Körfez Savaşı'nda ABD, Irak hava savunma, radar ve füze sistemlerini pasifize etmenin yollarını arayarak ve Irak haberleşme sistemlerini dinleyerek teknik yöntemlerle kara ordusu üstünlüğüne sahip olmasına rağmen Irak ordusunu güçsüz bırakabilmiştir.

2007 yılında Estonya Hükümeti'nin Sovyet dönemini hatırlattığı gerekçesiyle Kızıl Ordu heykellerinin yerinin değiştirilmesi konusundaki kararı, Rusya tarafından tepki almıştı. Tepkilerin artmasıyla Estonya'nın iletişim altyapıları, sık kullanılan internet siteleri siber

saldırganların hedefi haline gelerek yoğun Dağıtık servis dışı bırakma (DDoS) ataklarına maruz kalmıştır. Saldırılar neticesinde devlete ait internet sayfalarının, gazetelerin internet sayfalarına ve bankaların internet ortamında sunduğu hizmetlerine erişim mümkün olmamıştır.

2007 sonrasında Gürcistan, Kırgızistan, İsrail ve İran gibi ülkeler de siber saldırıların hedefi olmuştur. Belirli bir döneme kadar yoğunlukla DDoS saldırılarıyla tehdit unsuru olarak görülen siber saldırganlar, sonraki yıllarda daha büyük riskleri barındıran kritik altyapıları hedef almıştır. Özellikle İran siber saldırısında hedef alınan nükleer santraller, siber ortamda yaşanabilecek olası savaşların boyutunu gözler önüne sermektedir.

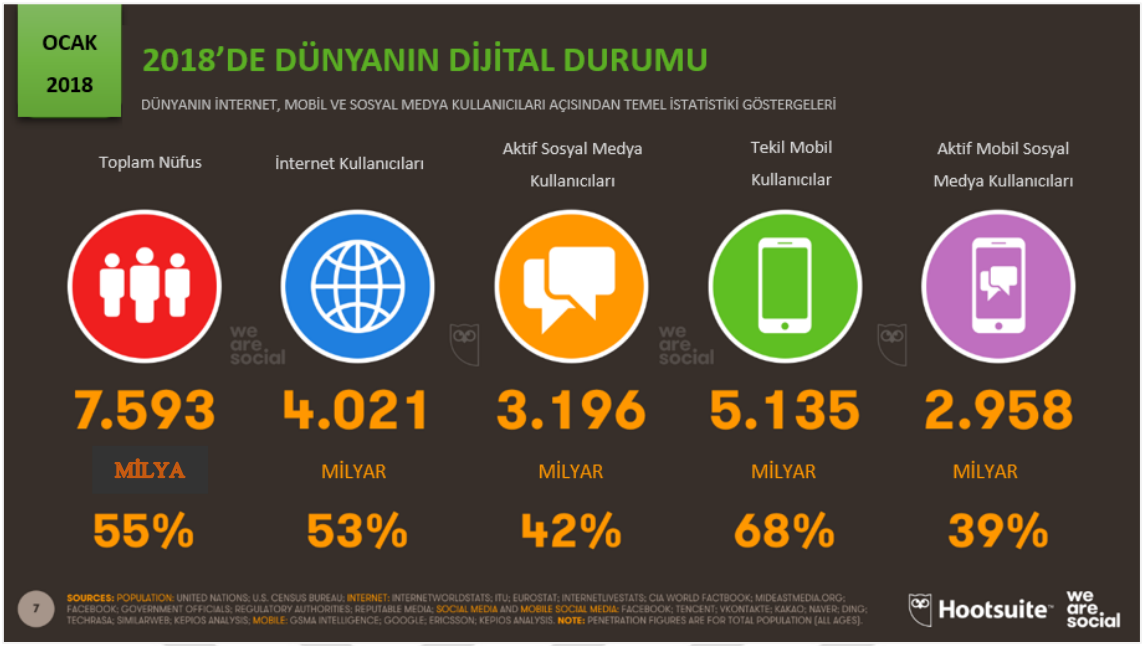
Örneklerde belirtilen siber saldırılar, genellikle zombi bilgisayarlar kullanılarak yapılmaktadır. Dünyanın herhangi bir yerinde bu amaçla kullanılan her bilgisayar, siber savunma noktasında zayıf olan hedefler için birer siber saldırgana dönüşebilmektedir. Siber ortamda yaşanabilecek olumsuzlukların küreselleşen bir tehdit unsuru olarak görülmesinin esas nedeni de aslında bu tip saldırı kaynaklarını tespit etmenin zorluğu ve suç işleyenin ispatı konusunda yaşanan problemlerdir. Bir ülkenin, fiziksel bir bombalama saldırısı sonrası düşmanını net olarak belirleyebilmesi ile kritik bir bilgi sistemleri altyapısına yapılan siber saldırı sonrasında kimi sorumlu tutacağı mukayese edildiğinde önemli ispatlama, delil üretebilme sorunlarıyla karşılaşılmaktadır. Bu nedenle siber savunma kabiliyetlerinin geliştirilmesi, teknik güç kapasitesinin arttırılması, olası ataklara hazırlıklı olunması, toplumun siber güvenlik konusundaki bilgi seviyesinin yükseltilmesi vb. birçok etken, küreselleşen günümüz dünyasında ülkelerin siber tehditlere karşı nasıl bir duruş içerisinde olacağını belirlemektedir.

Öte yandan siber saldırıların hedefinde artık internet sitelerini kullanılamaz hale getirmekten ziyade, hayatı durdurma, yavaşlatma gibi amaçlarla hareket edildiği gözlenmektedir. 2015 yılında ülkemizde yaşanan uzun süreli elektrik kesintileri akabinde siber saldırı iddiaları gündeme gelmiştir. Resmi otoriteler tarafından bu iddialar yalanlanmıştır ancak durum, siber saldırılara karşı her zaman tetikte olmanın gereğini gözler önüne seren ciddi bir örnek teşkil etmiştir. Yaşanan uzun süreli elektrik kesintinin neden olduğu aksaklıkların bilgi teknolojileri altyapılarıyla entegre çalışan diğer tüm sistemlerin çalışmasını olumsuz etkilediği açıkça görülmüştür. Siber güvenlik konusunda kamu tarafından atılacak adımlarda geç kalınmaması gerektiği tekrar gün yüzüne çıkmıştır.

İnsansız hava araçları birkaç yıl öncesine bakıldığında askeri amaçlarla ordular tarafından kullanılmakta iken, günümüzde bu cihazların daha basit yapıda tasarlanmış versiyonları kişisel veya ticari amaçlarla kullanılmaktadır. Bu cihazlar, havadan görüntü alabilme yetenekleri sayesinde basit anlamda fotoğrafçılık, sinema vb. alanlarda iyi niyetli kullanım şekilleriyle karşımıza çıksa dahi, özel hayatın gizliliğini ihlal edebilecek cihazlar olarak kullanılabilmekte, iç savaşların ve siyasi belirsizliklerin yaşandığı Orta Doğu coğrafyasında silahlı terörist gruplar için ucuz teknik envantere dönüşebilmektedir. Bu cihazların kayıt dışı kullanımının yaygınlaşması, izinsiz bölgelerde kullanılması ve daha önemlisi, cihazların kullandığı kablosuz ağ bilgilerinin kötü niyetli kişiler tarafından ele geçirilmesiyle siber güvenlik ihlallerinin ortaya çıkması kaçınılmazdır. Bu örnekten de anlaşılacağı üzere, çok basit amaçlarla üretilen cihazlar dahi teknolojiyi kullanabilme gücü ve kabiliyeti ile birleşince, bu güce sahip şahısların veya otoritelerin niyetlerine göre, küresel siber tehditlere veya birer siber silaha dönüşebilmektedir.

2.3. Yeni Nesil Savaş Sanatı

Clark internetin yaygınlaşmasını "1990'lı yıllarda tüm sektörler internet kullanımını büyük bir hızla benimsedi. Bilişim teknolojisi kullanan sistemler tüm şirketlerin iç işleyişlerinde geniş kullanım buldu. Rafineri ve kimyasal fabrikalarda tüm motorlar, vanalar ve termostatlar dijital cihazlar ile kontrol ediliyor. Tüm şirketler ve devlet kuruluşları her şeyin bilgisayar bazlı sistemlerce çalıştığı bir dünya kurdular. Bilgisayar kontrollerinin yarattığı bağımlılığın en belirgin sakıncası güç dağıtım şebekelerinde ortaya çıkıyor. Elektrik şebekesi üzerindeki cihazların yarısı doğrudan internete bağlı." ifadeleriyle özetlemiştir [2].



Şekil 2.8. Küresel dünyada dijital anlık durum [25]

İnternet kullanıcı sayısı 1990 yılı ile kıyaslandığında dünya nüfusunun yarısını geçmiştir. Dolayısıyla internet ve internet kullanım oranı, radyo ve televizyonun icadı ve yaygınlaşması ile karşılaştırıldığında sarsıcı derecede hızlı bir şekilde artmıştır [26]. Yapılan araştırmalar, Şekil 2.8'de ifade edildiği gibi, toplam popülasyonun %53'ünün internet kullanıcısı olduğunu göstermektedir. Türkiye'de internet kulanım oranları incelendiğinde ise Şekil 2.9'da olduğu gibi %67'lik bir oran göze çarpmaktadır.

Şekil 2.9. Türkiye'de internet kullanım oranları [25]

Sosyal paylaşım sitelerinin yaygın kullanımıyla birlikte basit olabileceği düşünülen herhangi bir konu dünya çapında en çok konuşulan konu haline gelebilmektedir. Paylaşılan verinin doğru olup olmadığının kontrolünün yapılması çoğunlukla göz ardı edilmekte, milyonlarca kişi üzerinde, paylaşılan bilgi doğrultusunda istenilen algı yaratılabilmektedir. Kitlelerin herhangi bir konu üzerine ortak bir amaçla hareket etmesi daha kolay bir eylem halini almıştır. Sosyal paylaşım sitelerinin bu gücü iyi amaçlarla kullanılabileceği gibi, ülke iç savaşlarının çıkmasına kadar varabilecek boyutta, birçok tehlikeye sebep olabilecek kapasitededir.

Güçlü bilgi sistemlerine sahip ülkelerin, güçlü yazılım devlerine ait bilgileri, özellikle de birçok kişisel veriyi barındıran sosyal paylaşım sitelerinde yer alan bilgileri istihbarat aracı olarak kullanabileceği açık bir gerçektir. Dolayısıyla günümüz dünyasında savaş yalnızca belirli alanlarda fiziksel olarak yapılan bir çatışma durumu olmaktan çıkmıştır. Bilgi ve iletişim teknolojilerinin her ortama nüfuzu sayesinde uzaktan kontrol edilebilecek alanların artmasıyla, çeşitli alanlara yönelik illegal faaliyetlerin yürütülmesi neticesinde siber savaşlar yaşanabilmekte, fiziksel olmayan bu alanda sürdürülen gizli savaşlar tahmin edilemeyecek boyutta siyasi etkileşimler yaratabilmektedir.

İnternet, sadece bilginin uçtan uca dağıtımından ibaret olmaktan öte, çeşitli taktikler kullanılarak rakiplerin gerçek ve sanal dünyada mağlubiyetine neden olabilecek gücü bünyesinde barındırmaktadır. Bu durum, sadece elektronik savaşı ifade etmekten ziyade, fiziksel savaş kavramı ile iç içe geçmiş vaziyette olan hibrit savaş kavramını gündeme getirmiştir. İnternetin Rus-Çeçen çatışmasında kullanılması bu duruma önemli bir örnektir [27].

Clark'ın Siber Savaş adlı eserinde ABD Hava Kuvvetleri Siber Uzay Operasyonları Görev Gücü Direktörü, siber uzayda güçlü olunmadığı sürece diğer savaş alanlarında üstün olmanın bir anlamı olmadığını ifade etmektedir. Özellikle gelişmiş ülkelerde siber zafiyetler, saldırıya maruz kalındığında günlük yaşantıyı durduracak derecede ciddi sonuçlara sebebiyet verecektir [13].

Olası hibrit savaşlara hazırlıklı olmak amacıyla Kuzey Atlantik Antlaşması Örgütü (NATO), istihbarat mekanizmalarını güçlendirmektedir. Siber saldırıların erken tespiti ve olayların gelişmesinin engellenmesi saldırının başlangıcı itibariyle hızlı bir şekilde bloke edilmesiyle yakından ilgilidir [28].

Siber tehditlerin her biri, siber ortamda bir siber silaha dönüşebilmektedir. Örneğin, sosyal paylaşım sitelerinde bilginin manipülasyonu, kritik ağları hedef alan DDoS saldırıları, bilgi güvenliği konusunda zayıf bilgilere sahip kullanıcılardan oltalama yöntemleri ile veri sızdırılması, zararlı yazılımlar kullanılarak sızılan ağlardan verilerin kopyalanarak çoğaltılması, dağıtılması ve benzeri birçok tehdit, siber ortamda siber savaş teçhizatına dönüşebilmektedir.

E-devlet uygulamalarıyla erişilen ve kişilere ait vatandaşlık, sağlık, vb. birçok mahrem verinin tutulduğu bilgi sistemleri altyapılarına yönelik düzenlenen saldırılar, ülkeler arasında gerginliklere sebep olabilmektedir. Saldırılar sonrası saldırganların izlerini kolaylıkla silebilmeleri de siber savaşta muhatabınızın kim olduğunu anlama noktasında önemli bir zorluktur. Bu nedenle siber ortamların güvenliğini sağlamak güçlü bir teknik yeterlilik gerektirmektedir. Yeni nesil savaş kültürü, teknolojik gücün önemini, bu alana özgü nitelikli istihdamın, maddi kaynakların, bireysel ve toplumsal eğitimin, iş birlikteliğin çok değerli olduğu gerçeğini ön plana çıkarmıştır. Yeni nesil savaş, siber ittifakı da zorunlu kılmıştır. Ülkeler olası siber tehditlere karşı çıkarları doğrultusunda ittifaklar kurmaktadırlar.

2.4. Tallinn El Kitabı

Tallinn el kitabı resmi bir nitelik taşımamakla birlikte, siber savaş konusunda uygulanabilecek uluslararası hukukun belirlenmesine katkı sağlamayı amaçlamaktadır. 2013 yılında Cambridge Üniversitesi tarafından yayımlanmıştır. Tallinn El Kitabı, herhangi bir savaşa dahil olma, savaşa dahil olunması halinde uyulması gerekenler, savaşa girmenin haklı nedenleri ve ülkelerin savaşa girmelerini yasal zemine oturtabilmelerini sağlamak amacıyla düzenlenen uluslararası hukuki zemin gibi alanları kapsamaktadır. El kitabı siber güvenlik hukuku ve siber silahlı çatışma hukuku olmak üzere iki temel bölümden oluşmaktadır [29].

Tallinn El Kitabı'nda 95 adet konu başlığı belirlenmiştir. Genel olarak, devletlerin kendi sınırları içerisinde ve kendi sınırları dışındaki uygulamalarına ilişkin hukuk kurallarını zedeleyecek girişimlerden uzak durması, kendi sınırlarını içerisinde siber güvenliği sağlamaya yönelik çalışmaları yapması ve sınırları içerisindeki siber güvenlik ihlallerini engellemesi gerektiği vurgulanmıştır. Tallinn El Kitabı, belirlenen 95 kurala ilişkin hukuki açıklamalara yer vermesi bakımından, resmi olarak hukuki boşluğun giderilmesine yönelik yol gösterici olma özelliğindedir.

Tallinn El Kitabı'nın 2017 baskısı barışçıl hukuk rejimlerinden silahlı çatışma yasasına kadar, siber operasyonlara uygulanabilir tam bir uluslararası hukuk yelpazesini kapsamaktadır. Siber alandaki olayları düzenleyen çok çeşitli uluslararası hukuk ilkeleri ve rejimlerinin analizi, egemenlik ve yargı yetkisine ilişkin çeşitli üsler gibi genel uluslararası hukuk ilkelerini içerir. Ayrıca, insan hakları hukuku, hava ve uzay hukuku, deniz hukuku, diplomatik ve konsolosluk hukuku gibi uluslararası hukukun sayısız uzman rejimi siber operasyonlar kapsamında incelenmektedir [30].

2.5. Siber Güvenliğin Sağlanmasında Ulusal ve Uluslararası İş Birliğinin Önemi

İnternete bağlı çalışan cep telefonları, pencere panjurları, klimalar, trafik yoğunluğuna göre devreye giren akıllı trafik ışıkları, ev ve işyerlerinin takip edilebileceği kamera sistemleri ve örneğini daha da arttırabileceğimiz farklı cihaz nesnelerin interneti kavramının doğmasına sebep olmuştur. Nesnelerin internet üzerinden haberleşmesinin sonucu olarak internet tüm çevremizi tam anlamıyla teknoloji ile sarmalamıştır. Çepeçevre siber unsurlarla çevrili bir yaşama sahip olmamız, risklere karşı farklı disiplinler arasında iş birliği yapılarak cevap verilmesini zorunlu kılmaktadır. Gelişmiş ülkelerin gündeme gelmese de harp amaçlı siber altyapı birliktelikleri bilinen bir gerçektir.

2015 yılında Türkiye'nin internet altyapısına yönelik olarak ciddi büyüklükte dağıtık hizmet engelleme saldırıları yapılmıştır. Etkili bir siber saldırı yöntemi olan bu DDoS saldırılarının Rusya tarafından yapıldığı iddia edilmiştir, ancak saldırıyı Anonymous grubu üstlenmiştir. Saldırının ilk günlerinde kamu ve özel kurumlar arasında koordinasyon eksikliğinin olduğu ve Ulusal Siber Olaylara Müdahale Merkezi'nin (USOM) aksiyon almada yaşadığı problemler nedeniyle bazı özel bankalar hizmet verememiştir. Bu durum Türkiye'nin siber saldırılara hazırlıksız olduğunun açık bir göstergesidir. Öte yandan kamunun siber saldırılara karşı cevap verebilme kabiliyetinde yetersizlikler olduğu, kurumlar arası koordinasyonun gerektiği şekilde sağlanamadığı, kriz yönetimi yapılamadığı gözlenmektedir [31].

Bu olayda tecrübe edinildiği üzere siber güvenlik risklerine karşı mücadelede kamu kurumları ve özel sektör arasındaki iş birliği, ülkemizin milli güvenliğinin sağlanması bakımından oldukça önemlidir. Ayrıca koordinasyon mekanizmasının kriz anlarında doğru işletilmesi ve hızlı bir aksiyon alınması, siber saldırıların yayılımını engelleyecek bir unsurdur. Yayılım eğilimi gösterilen alanlarla hızlı iletişim kurulması ve iş birliği sağlanması siber saldırılarla mücadelenin olmazsa olmazlarındandır. Öte yandan siber

dünyada sadece ulusal iş birlikleri ile mücadele etmek ütopik bir yaklaşım olacaktır. Bu anlamda ulusal siber mücadelenin uluslararası iş birlikleri ile desteklenmesi muhakkak gereklidir.

Siber dünya, ülkelerin yalnızca iç işleyişinde etkili olacak politikalar üreterek güvenlik sağlayabilmesini olanaksız kılmıştır. Siber alanın küresel boyutta yayılım gösterebilecek tesirde tehditleri barındırması bu tehditlere daha geniş çerçevede bakılmasını gerektirmektedir. Tehditleri daha etkili bertaraf edebilmenin yolu ülkeler arasında iş birliğinden geçmektedir. Kuruluşlar arasında uluslararası düzeyde faaliyetler yoluyla yürütülen çeşitli çalışmalar, siber tehditlerin azaltılması noktasında daha etkili çalışmaların ortaya çıkmasını sağlayacaktır [32].

Ülkelerin yüzleşmek zorunda kaldığı türlü siber saldırılar, devletleri bu saldırılara karşı güvenlik önlemleri almaya zorlamaktadır. Bu saldırılar tek bir ülkeyi hedef alabileceği gibi zaman zaman birden fazla ülkeyi de hedef alabilmektedir. Bu bağlamda siber terörizm, ülkeler arasında iş birliğini de zorunlu kılmaktadır.

İnternetin tüm nesneler arasında yayılım göstererek iletişim kurmasının bir sonucu olarak dünyanın farklı iki ucu arasında yapılan iletişimlerde her bir ülkenin kendi yasal durumuna göre ilerleteceği hukuki süreçler problem teşkil etmektedir. Örneğin A ülkesi ile Z ülkesinde benzer siber suçlara aynı hukuki yaptırımlar uygulanmamaktadır. Hatta kimi ülkelerde suç kabul edilen ve cezai yaptırımı olan siber ihlaller, diğer kimi ülkelerde yasal zemine oturtulmamış olabilmektedir. Farklı yaptırımları içeren hukuki düzenlemeler nedeniyle uluslararası iş birliği, suça küresel olarak ortak karşılık verilmesi noktasında önemlidir. Uluslararası iş birliğinin sağlanması, temelde basit görünse dahi uzun soluklu bir sürecin işletilmesini gerektirmektedir.

Bütün ülkelerin başvuracağı uluslararası bir merkez kurulursa, saldırı altında kaldığını düşünen ülkeler buraya başvurabilir. Saldırıyı yiyen ülke sabaha karşı bile olsa hemen Talin'deki merkezi arar, saldırının gerçekleştiği ülkeyi arayan merkez de anında botneti çalıştıran internet servis sağlayıcıyı bulmasını ve kapatmasını talep eder. Merkez olaylardan sonra tümüyle ülkelere de gönderilecek özet raporlar hazırlar. Uyumsuz ülkelere bir dizi yaptırım uygulanabilir. Suçlu devletin ülkesine internet akışında kısıtlamalar, ülkeye bilişim ekipmanları ithalatında kısıtlama, bir süre siber uzaya girememe gibi cezalar uygulanabilir [13].

Siber ortamda caydırıcılık istikrarı diğer savaş ortamları kadar rahatlıkla gerçekleştirilebilecek bir olgu değildir. Örneğin siber saldırıya daha ağır bir siber saldırı ile karşılık vermek karşılıklı saldırıların sürüp gitmesine neden olacak ve bu savaşın sonu gelmeyecektir. Yani nükleer saldırılarda caydırıcılık konusunda olduğu gibi misilleme ihtimalinin caydırıcılık özelliği siber ortamda sonuç getirebilecek bir durum değildir. Dolayısıyla, uluslararası iş birlikleri yapılarak sağlanabilecek olan caydırıcılık istikrarı, siber ortamın varlıkları olan dijital bilginin kontrolünde karşılaşılan zorluklar nedeniyle siber tahribatların etkisini ancak minimize edilebilecek düzeyde olacaktır [33].

Siber suçların ispatlanması süreçlerinde hukuka uygun delillerin toplanması bakımından uluslararası iş birlikleri önemlidir. Uygun kanıt elde edilmesi için yetkin niteliklerle donatılmış eğitimli kişilerin istihdamı gereklidir. Bu bağlamda temel gereksinimlerin belirlenmesi ve hukuki gereklerin uluslararası iş birlikleri sağlanarak karşılanması uygun kanıt elde edilmesi için gereklidir [34].

Ülkeler arasında uzlaşmanın ve iş birliğinin sağlanması yoğun emek ve çalışma gerektiren bir konudur. Siber eylemlerin tasnifi konusunda farklı bakış açılarının gündeme gelmesi tahmin etmesi zor olmayan bir durumdur. Adaleti hukuk sistemi sağlamaktadır ancak her ülke kendi sosyo-kültürel yapısı ile uyumlu bir şekilde bu hukuki normları belirlemektedir. Dolayısıyla siber eylemlere karşı barışçıl bir ortamın dizaynı ciddi emek gerektirmektedir [35]. Siber eylemlerin adlandırılması, tasnifinden öte olarak siber alanın askeri olmayan bir alana çevrilmesi konusunda bir iş birliği daha barış dolu bir dünyanın kurulmasına katkı sağlayacaktır.

Siber güvenlik riskleri, bu anlamda yeni uluslararası ilişkilerin ortaya çıkmasını tetikleyecek bir vazifeyi de üstlenmiş durumdadır. Siber silahsızlanmanın sağlanmasına yönelik uluslararası yaklaşımın ortaya konulmaması durumunda, siber güç sahibi ülkeler ile teknik altyapısı daha güçsüz ülkeler birbirleri ile ya tamamen düşman, ya da güçlünün isteklerine boyun eğmek zorunda kalan bir zayıf ülkenin oluşmasına neden olunacaktır. Bu durumda teknolojik sömürge ülkelerin ortaya çıkması kaçınılmaz olacaktır. Siber uzayda sağlanan üstünlükler veya zayıflıklar uluslararası dengeleri değiştirebilme noktasında bu anlamda önemlidir.

Uluslararası iş birliği saldırılara karşı kısa sürelerde önlem almak için gerekli bir şarttır. Ekonomik Kalkınma ve İş Birliği Örgütü (OECD) gibi çok uluslu organizasyonların

çalışmalarını takip etmek ise ortak politika oluşturmak, standardizasyona kavuşmak ve birlikte çalışma kültürü edinmek için önemli fırsatlar sunmaktadır [21].

2.6. Siber Güvenliğin Sağlanmasında Koordinasyonun Önemi

Siber saldırılar esnasında kriz yönetimi, görev dağılımı yapılması ve saldırı hedefleri arasında koordinasyon sağlanması, siber saldırıların bertaraf edilmesi ve siber savunmanın etkili bir şekilde yürütülmesi noktasında kritik öneme sahiptir. Siber uzayda koordinasyon eksikliği nedeniyle günlük hayatı çepeçevre sarmış internet, kendisine bağlı konumdaki tüm nesneleri içine alıp yok edebilecek bir girdap gücündedir. Bu bağlamda hangi paydaşın nerede durması gerektiğini, ne yapması gerektiği belirleyen ve paydaşları yöneten bir koordinasyon makamı hem ulusal hem uluslararası zeminde gereklidir.

Öte yandan farklı kurumların benzer alanlarda ayrı bütçelerle yapacağı çalışmalar iş gücü, zaman ve para kaybının ötesine ulaşamayacaktır. Siber güvenlikte koordinasyon makamının tek olması, onlarca farklı kurumun kendi başına yürüttüğü işlerde karşılaşılabilecek olası iş gücü ve yatırım zayiatlarının önüne geçilmesini sağlayacaktır. Bu anlamda, siber güvenliğe ilişkin politika belirleyici makamın, diğer kurumların siber güvenlik konulu girişimlerine yönelik kapsamlı yetkilere haiz olması gerekmektedir. Bu durum üst bir bakış açısı oluşmasının yanı sıra, eş veya benzer görev yürüten farklı kamu ve özel sektör kurum kuruluşlarının buluşabilmesi, ortak amaçlar için birlikte çalışma, kaynak paylaşımı vb. konularda yardımlaşabilmesine olanak sağlayacaktır.

2.7. Siber Güvenlik Ekosistemi Oluşturmanın Önemi

Siber tehditlere karşı geleneksel yöntemler olan güvenlik duvarı bulundurmak ya da süreçlerde kullanıcıların ve erişimlerin yönetilmesi gibi çözümler artık yetersiz kalmaktadır. Siber uzayın 5. harp alanı olarak görülmesiyle birlikte, siber güvenlik alanındaki ihtiyaçların milli olarak karşılanması zorunluluk halini almıştır. Bilgi güvenliği ve siber güvenlik alanında sorumluluğu olan paydaşların, birbirlerinden bağımsız, habersiz hareket etmelerinin yaratacağı dezavantajlara karşı bu alanda uyum içerisinde hareket etmenin sağlayacağı avantajlar göz önüne alındığında ekosistemin oluşturulması iş birlikteliğini sağlayacak en önemli unsurdur.

Siber güvenlik ekosistemi; etkileşim içindeki insanları ve organizasyonları, birbirinden farklı amaçlarla kullanılan cihazları ve ağları kapsayan entegre bir topluluğu ifade eder [36].

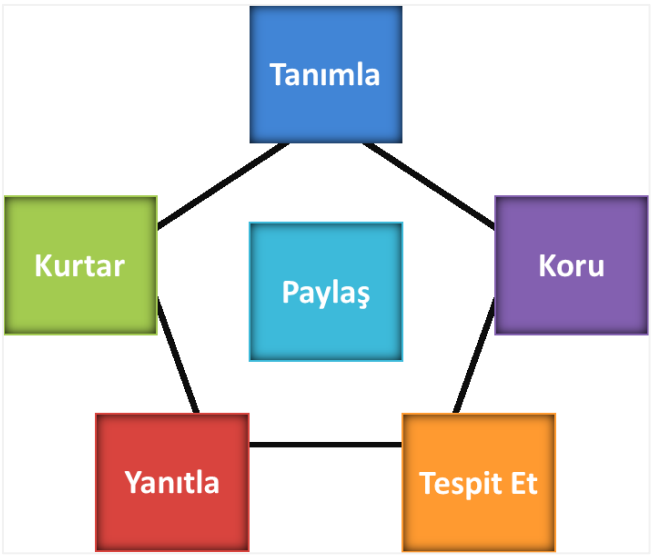
Siber güvenlik ekosistemi oluşturularak; siber olayların tespitinde ve karşı cevapların verilmesinde daha akıllı sistemlerin ve altyapıların kullanılması, kritik bir alana gelecek herhangi bir zararın herkesi etkileyeceği gerçeğine dayanarak, siber saldırılara ortak bir tepki verilmesi amaçlanmaktadır.

Bu anlamda, oluşturulacak siber güvenlik ekosistemi, bedenimizdeki doğal defans sistemine benzer şekilde çalışır, güçlü bir savunma sistemi olarak hareket edilmesini amaçlar. Saldırılara karşı iş birliktelik, paydaşlar arasında görev dağılımı vb. yönleri dikkate alındığında, doğal ekosistem ve insan vücudunun bağışıklık sistemine benzetilebilir [36].

Siber güvenlik, aşağıdakiler için yapılandırılmış eylemlerin devam eden bir döngüsünden oluşur:

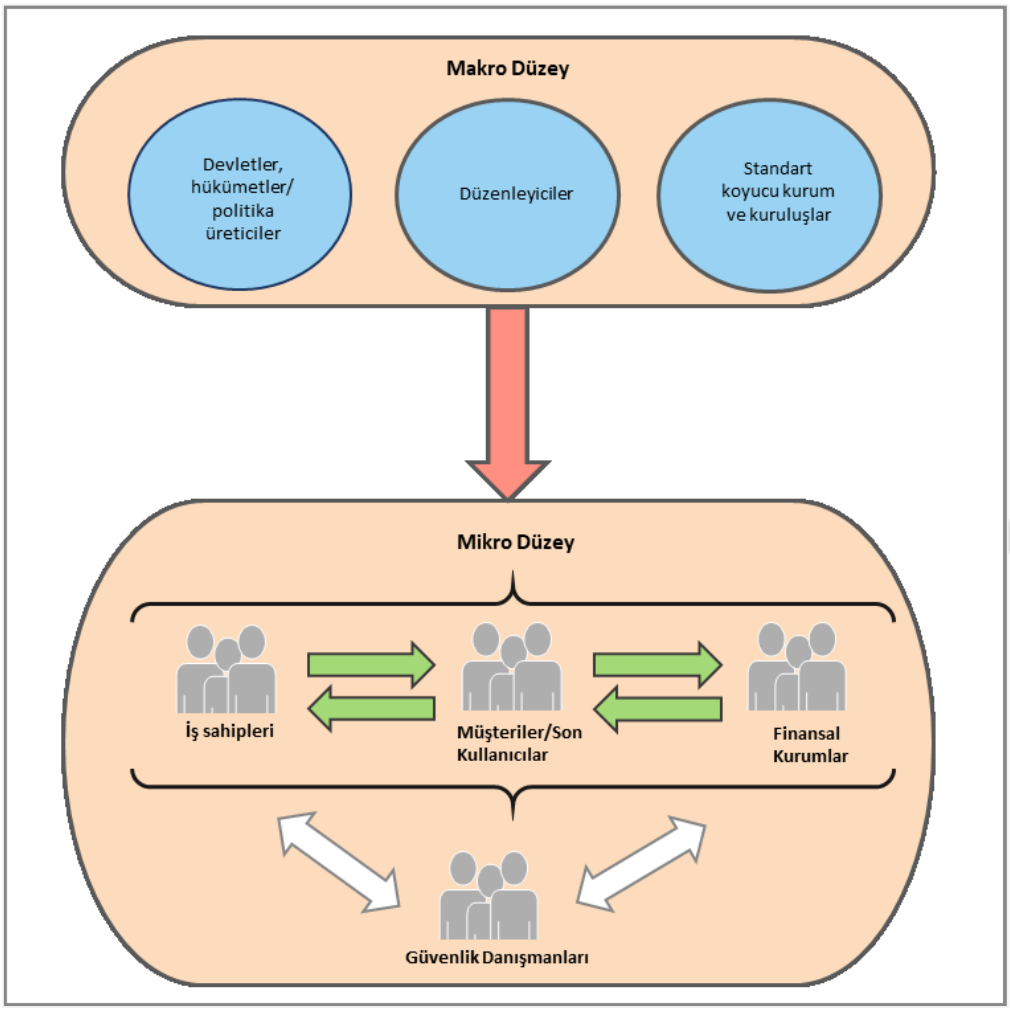
- Tanımla (sistemlere, varlıklara, verilere ve kapasiteye ilişkin durum ve risklerin anlaşılması)
- Koru (Uygun korunma önlemlerin uygulanması)
- Tespit Et (siber güvenlik olayının belirlenmesi)
- Yanıtla (herhangi bir siber güvenlik olayına karşı aksiyon alınması)
- Kurtar (sürekliliğin sağlanması ve yeniden yapılanma kabiliyetinin edinilmesi)

Bütün bu aktiviteler siber güvenlik olayına ilişkili bilginin zamanında ve güvenilir şekilde paylaşımına dayanır [5].



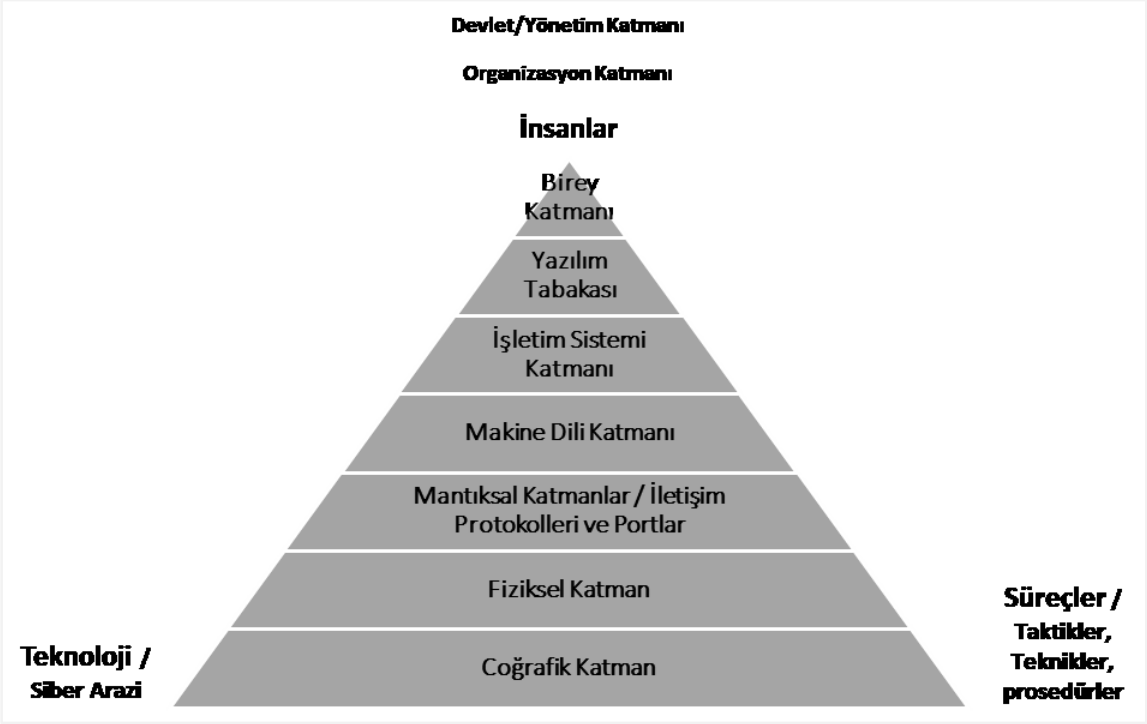
Şekil 2.10. Siber güvenlik ekosisteminin temel bileşenleri [5]

Siber güvenlik ekosistemi temelde iki kategoriye ayrılabilir. Bu kategoriler mikro düzeyde ve makro düzeyde rollerin olduğu paydaşları ifade eder. Mikro seviyede paydaşlar; ilgili topluluğun ekosistemde genel siber güvenlik duruşunu etkileyen son kullanıcılar, şirketler, finansal kurumlar ve güvenlik danışmanlarından oluşur. Makro düzeyde paydaşlar ise; hükümetler, düzenleyiciler, politika belirleyiciler (IETF, NIST vb.) bu ve benzeri görevi olan kurum ve kuruluşlardan oluşur [37].



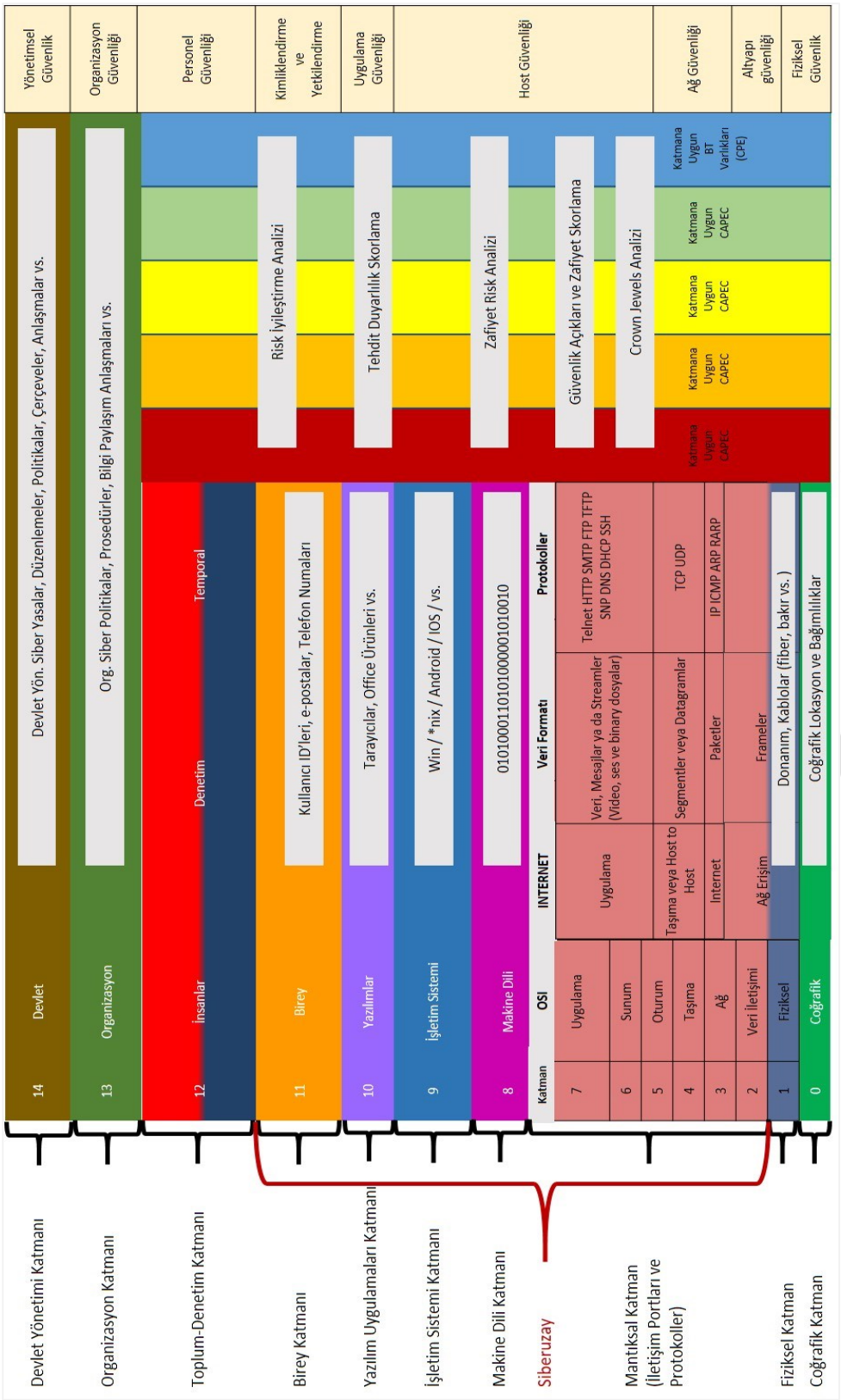
Şekil 2.11. Siber güvenlik ekosistemi [38]

Bütün ekosistemi derinlemesine ele alan yeni bir çalışma siber alan olarak ifade edilmektedir. Bu çalışmaya göre ekosistemde siber güvenliğin temelini "İnsanlar, Organizasyonlar-Süreçler ve Teknoloji" olarak üç başlık oluşturmaktadır. Siber alan katmanlı modeli, siber güvenlik bilgisini yapılandırmaya ve siber alan fiziksel ve mantıksal bölümlerini görselleştirmeye olanak tanıyan 15 katman tanımlar [39]. Siber alan katmanlı modeli Şekil 2.12'de yer aldığı gibidir.



Şekil 2.12. Siber alan katmanlı modeli [40]

Riley'nin siber alan katmanlı modeli siber güvenliği "İnsanlar, Organizasyonlar-Süreçler ve Teknoloji" temelinde ele almaktadır. Bu üçlü ilişkiyi kurabilmek için hem sanal dünyayı temsil eden hem gerçek dünya katmanlarını içeren ve bu iki dünyayı birleştirebilecek bir model olarak Şekil 2.13'te ifade edilen detaylı yapı geliştirilmiştir [41]. Riley'nin katmanlı modelinde ikinci ve on birinci seviyeler arası siber uzay olarak tanımlanmaktadır.



Şekil 2.13. Siber alan detaylı katmanlı model [40]

Siber ekosistemin geliştirilmesi ile birbiriyle iş birliği içerisinde olan paydaşlar, siber saldırıları engellemek için birbirleriyle kurallar gereği haberleşerek çalışacak, diğer

paydaşlar arasında siber saldırıların yayılması engellenebilecek, siber saldırıların sonuçları minimize edilebilecek, siber saldırılar sonrasında güvenli bir duruma geri dönüş daha kısa zamanda sağlanabilecektir [36].

"Siber Güvenlik Ekosisteminin Oluşturulması" konusu, 2016-2019 Ulusal Siber Güvenlik Stratejisi'nde tanımlanan beş temel amaç arasında yer almaktadır. Diğer dört amaç ise siber savunma ve kritik altyapıların korunması çalışmaları, siber suçlara karşı yapılacak çalışmalar, insan kaynağı ve bilinçlendirme çalışmaları ile milli güvenlik konularında yürütülecek çalışmalar ile ilgilidir.

İlgili stratejik plan kapsamında, Siber Güvenlik Ekosisteminin Geliştirilmesi konusuna; siber uzayı oluşturan tüm paydaşların katılımları ve katkılarıyla hem mevzuat hem de teknolojik gereksinimlerin belirlenmesi ve belirlenen gereksinimlerin giderilmesine yönelik çalışmaları içeren çalışmalar neticesinden baştan uca bir dönüşümün sağlanması olarak değinilmiştir.

Riley'nin sunduğu siber alan detaylı katmanlı modelin [40] "İnsanlar, Organizasyonlar-Süreçler ve Teknoloji" temelinde siber güvenliğe ilişkin olarak kurum, kuruluşlar ve toplumu oluşturan bireylerin rol ve sorumluluklarının belirlenmesine yol gösterici olabileceği düşünülmektedir. Referans alınan bu modeller ile oluşturulan ve altıncı bölümde detayları açıklanan siber güvenlik ekosistemi model önerisinin, ekosistemin işleyişinin ve sürekliliğin sağlanması bakımından planlanma kolaylıkları sağlayacağı düşünülmektedir.

3. TÜRKİYE'DE SİBER GÜVENLİK EKOSİSTEMİNİN GELİŞTİRİLMESİNE ZEMİN HAZIRLAYAN ÖNEMLİ ÇALIŞMALAR

Türkiye'de siber güvenlik ile ilgili çalışmalar 11 Eylül sonrası OECD'nin 2001'de yayımladığı bilgi sistemleri ve ağların güvenliği hakkındaki belgelerin onaylanmasından sonra artmaya başlamıştır. Türk Ceza Kanunu (TCK) ve diğer kanunlar kapsamında bilişim ile ilgili çeşitli alanlarda düzenlemeler yapılmasının yanında özellikle son on yıl içerisinde siber güvenliğe ilişkin strateji belgeleri de yayımlanmıştır. Bu bölümde, ülkemizde siber güvenlik ile ilgili ön plana çıkan ve siber güvenlik ekosisteminin geliştirilmesine katkı sağlayan önemli düzenlemelere yer verilmiştir.

3.1. Bilgi Sistem ve Ağları için Güvenlik Kültürü Konulu Genelge

Türkiye'nin de üyesi olduğu OECD, 11 Eylül 2001 sonrası rehber ilkelerini güncelleyerek yayımlamıştır. 17 Şubat 2003 yılında Başbakanlık tarafından bu konuda bir genelge yayımlanmıştır. Bu belge ile tüm bilgi kullanıcılarına, varlıkların kullanımında rehberde yer alan ilkeleri göz önünde bulundurmaları gerektiği tebliğ edilmiştir.

OECD'nin hazırladığı belgede dokuz önemli ilke bulunmaktadır. Rehberin, dönemin teknolojik şartları itibariyle bilgi sistemlerinin ve bilgi sistemleri kullanıcılarının güvenliği konusunda genel bir çerçeve oluşturduğu görülmektedir. Rehber ilkelerinde; kullanıcı bilinci, kullanıcıların birbirlerinin yasal çıkarlarına saygılı olması, güvenlik tehditlerine tepkinin geciktirilmemesi, gelişen teknolojiye bağlı olarak risk değerlendirmelerinin yeniden gözden geçirilmesi gibi açıklamalara yer verilmiştir.

3.2. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

Mayıs 2007'de yasalaşan 5651 sayılı Kanun ile birlikte içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcı olarak tanımlanan internet hizmeti ve sunucu barındırma hizmeti sağlayan kurum ve kuruluşların yükümlülükleri, riayet etmeleri gereken kurallar belirlenmiştir. Bu yasa ile birlikte belirli log kayıtlarının tutulması zorunlu hale gelerek siber suçların tespitinde hukuki süreçlerin desteklenmesi sağlanmıştır [42].

İçerik, yer, erişim ve toplu kullanım sağlayıcıları ilgili yasada detaylı olarak tanımlıdır. Bu tanımlar doğrultusunda hizmet sağlayan kurum ve kuruluşlar kendi sunucularında barındırdıkları verilerden, elektronik içeriklerden yasal olarak sorumludur. Dolayısıyla olası siber suçların tespitini sağlanması amacıyla veriyi oluşturan kaydeden değiştiren taşıyan kopyalan kişi veya kişilere ya da veri trafiğine ilişkin kayıtların log araçları kullanılarak belirlenen yasal süre boyunca kayıtlı tutulması gerekmektedir. Öte yandan hukuka aykırı içeriklerin varlığı durumunda ilgili içeriklerin kaldırılması veya imhası da tanımlı sağlayıcıların yasal zorunluluğu durumundadır [43].

Kanun'un uygulanmasına yönelik olarak ikincil mevzuatlar yayımlanmıştır. Kanun kapsamında internet ortamında herhangi bir yere erişime ait sistem kayıtlarının (log kaydı) zaman damgalı olarak tutulması gerekmektedir. Ayrıca suç teşkil edebilecek içeriklerin bildirilmesi durumda içerik sağlayıcı tarafından kaldırılması gerekmektedir.

3.3. 6698 Kişisel Verilerin Korunması Kanunu

Mart 2016 tarihinde TBMM Genel Kurulu'nun yasalaştırdığı 6698 Kişisel Verilerin Korunması Kanunu'nun amacı kişisel verilerin izinsiz bir şekilde işlenmesinin önüne geçmektedir. Temel hak ve hürriyetlerin korunmasını amaçlayan bu yasa gerçek ve tüzel kişiler arasında kişisel veri tutanların uyması gereken kuralları belirlemektedir. Özel hayatın gizliliğinin sağlanması da bu yasanın korumayı amaçladığı kişisel haklar arasında yer almaktadır.

Bilgi sistemleri altyapısını kullanarak hizmet üreten birçok kurum ve kuruluş kişilere ait birçok veriyi kendi sistemlerine kayıt etmek suretiyle tutmaktadır. Kimi kurumlar bu kişisel verileri özel amaçlar doğrultusunda haber vermeksizin kullanabilmektedir. İşte bu gibi durumların önüne geçmek amacıyla çıkarılan 6698 sayılı Kanun bireylerin şahsi bilgilerini korumayı amaçlamaktadır. Bu bağlamda Kanun, hem verileri kaydeden ve kullanan gerçek ve tüzel kişileri hem de verileri kurumlar tarafından çeşitli amaçlarla talep edilen gerçek kişileri ilgilendirmektedir.

Bir verinin kişisel veri olarak tanımlanabilmesi için kimliği belirli bir kişiyi ifade edebilecek nitelikte olması gereklidir. Kişisel veriler ile özel nitelikli verilerin Kanun'da belirlenen şartlar dışında açık rıza olmaksızın işlenemeyeceği ifade edilmiştir. Kuruluşların herhangi bir şekilde kendi sistemlerinde tuttukları, farklı yollarla elde ettikleri şahsa ait verileri çıkar

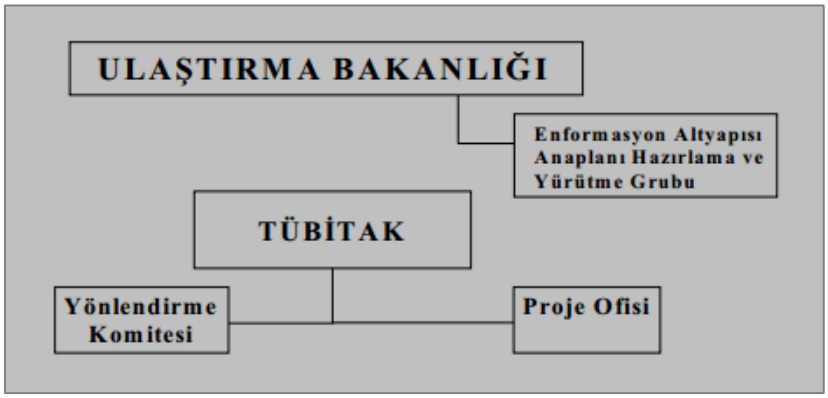
amaçlı kullanması, kullandırması veya başka kuruluşlara satması bu verilerin Kanun'a aykırı olarak işlenmesi anlamına gelmektedir.

Kanun, verilerin işlenmesi sırasında uyulması gereken hususları belirlemesi, kişisel verilerin yok edilmesine veya aktarılmasına ilişkin konulara açıklık getirmesi bakımından önemli konumdadır. Ayrıca veri sorumlusunun yükümlülükleri ile kişisel verileri işlenen gerçek kişilerin hakları ile ilgili konular Kanun'da yer almaktadır.

3.4. Türkiye Ulusal Enformasyon Altyapısı Anaplanı-1999 Ulaştırma Bakanlığı Tuena Raporu

Türkiye Bilimler Akademisi Başkanlığı (TÜBA), Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) ve Türkiye Teknoloji Geliştirme Vakfı'nın (TTGV) oluşturduğu çalışma platformu, 1995 yılında bilişim sektöründeki gelişmelere istinaden planlamaların yapılması gerektiğine karar vererek bu konuda bir çalışma yapılmasını önermiştir. Çalışma platformunun önerisi Başbakanlık tarafından kabul görerek sosyal hayata etki eden unsurlar dahil bilgi kaynaklarına yönelik bir politika geliştirilmesi amaçlı çalışma başlatmıştır. Çalışmanın TÜBİTAK önderliğinde yürütülmesi kararlaştırılmıştır [44].

Ekim 1999'da Tuena Anaplanı Sonuç Raporu yayımlanmıştır. Bu raporda dünya ülkeleri ve Türkiye'de çeşitli sektörlerde enformasyon ve iletişim sektörlerindeki durum incelenmiştir. Geleceğe dair vizyon oluşturulmasına ilişkin araştırma çalışmaları yapılarak hedefler belirlenmiş, Türkiye'deki kurumsal yapılanma incelenerek öneriler sunulmuştur.



Şekil 3.1. Anaplan çalışması örgütsel yapı [45]

Türkiye Ulusal Enformasyon Altyapısı Anaplanı Raporu incelendiğinde ve raporun yayımlanma yılı, çalışmaların yapıldığı dönemde teknolojinin durumu göz önünde

bulundurulduğunda bu planın Ulaştırma ve Altyapı Bakanlığı'nın yayımladığı strateji belgeleri ve Strateji ve Bütçe Başkanlığı'nın (eski adıyla Kalkınma Bakanlığı'nın) yayımladığı Bilgi Toplumu Stratejileri'nin oluşturulmasına temel hazırladığı görülmektedir. Çalışmanın uygulamaya geçirilmesi ile takip çalışmalarına ve izleme çalışmalarına dair verilere ulaşılamaması, kurumlara görev sorumluluk atamalarına dair veri elde edilememesi ve hedeflerin bitirilme yılı bilgilerinin net olarak bilinmemesi durumu, bu alanda şeffaflığa duyulan ihtiyacı da göz önüne sermektedir.

3.5. 2003-2004 Kısa Dönem Eylem Planı (e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı)

Başbakanlık Personel ve Prensipler Genel Müdürlüğü tarafından 3 Aralık 2003 tarihinde yayımlanan genelge ile e-Dönüşüm Türkiye Projesi'nin takibinden Strateji ve Bütçe Başkanlığı sorumlu kılınmıştır. 4 Aralık 2003'te yayımlanan bu konudaki ikinci genelgede, Kısa Dönem Eylem Planı'na ilişkin çeşitli konu başlıkları altında kamu kurumlarına sorumluluklar dağıtılarak kamu kurumlarının Strateji ve Bütçe Başkanlığı ile iş birliği içinde olacağı bir çalışma planı yapılmıştır.

Bilgi Toplumu Stratejisi oluşturulması, teknik altyapı ve bilgi güvenliği alanında ucuz internet hizmeti ve 3G lisans tahsisi konularına ilişkin çalışmaların yapılması, ağ güvenliği ile ilgili pilot çalışmaların yapılması ve diğer konular Eylem Planı'nda yer almıştır. Eğitim ve insan kaynakları konusunda ise; bilgi teknolojileri altyapısına dayanan eğitim sistemlerinin yaygınlaştırılması, bilgi teknolojilerinin eğitim alanında daha aktif ve verimli kullanılması konularına; Hukuki altyapı başlığı altında Elektronik İmza Kanunu, Kişisel Verileri Koruma Kanunu, Ulusal Bilgi Güvenliği Kanunu ve Bilgi Edinme Kanunu'nun çıkarılması, TCK'da bilgi teknolojilerine ilişkin suçlarla ilgili düzenlemelerin yapılması gibi önemli konulara yer verilmiştir. Kısa Dönem Eylem Planı'nda bilgi teknolojilerine ilişkin standartların Türk Standardı olarak yayımlanması ve e-Devlet uygulamalarının geliştirilmesi konularında sorumlu kuruluşlar belirlenmiştir.

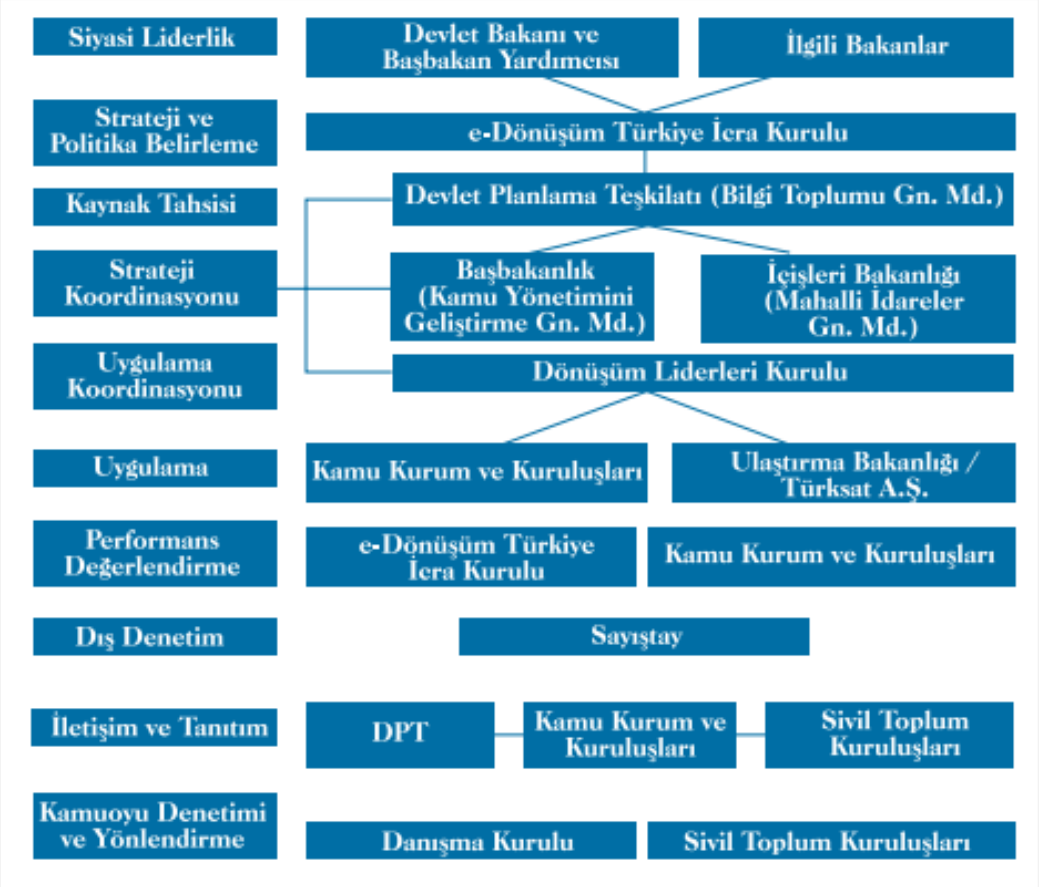
3.6. 2005 Eylem Planı

Mart 2005'te tebliğ edilen e-Dönüşüm Türkiye Projesi 2005 Yılı Eylem Planı'nda 2003'de yayımlanan Kısa Dönem Eylem Planı ile benzer olarak eylemler, sorumlu kuruluşlar ve her bir eylemin amacı liste olarak açıklanmıştır. Süreçlere ilişkin takibin ve koordinasyonun

Strateji ve Bütçe Başkanlığı tarafından yapılacağı belirtilmiştir. Ancak sürecin uygulanmasının takibi, denetimi, yıllık sonuçları ve elde edilen çıktıların ne olduğu konusunda kamuoyu ile paylaşılan herhangi bir rapora ulaşılamamıştır.

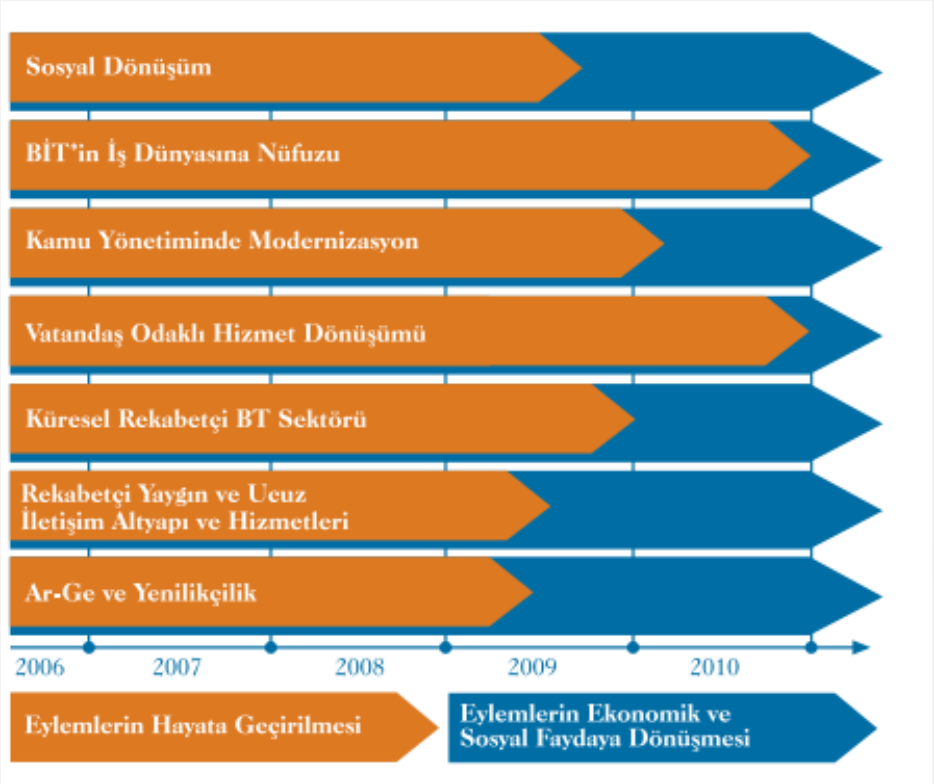
3.7. 2006-2010 Bilgi Toplumu Stratejisi

28 Temmuz 2006 tarihinde Resmi Gazete'de yayımlanmıştır. Belgede Türkiye'nin belirlenen yıl aralığı içerisindeki stratejik önceliğe sahip alanlarına ilişkin stratejik yönler açıklanmıştır. Stratejinin uygulanması için kurumsal yapılanmanın nasıl olacağı Şekil 3.2'de açıklanmıştır.



Şekil 3.2. Bilgi toplumu stratejisi kurumsal yapılanma modeli [46]

Eylem planlaması ve stratejinin uygulama süreci açıklanarak eylem planının uygulanması ve hayata geçirilmesi neticesinde Türkiye'de olması beklenen dönüşüme ilişkin öngörülere yer verilmiştir. Bilgi Toplumu Stratejisi'nin uygulamaya geçirilmesi ile birlikte belirlenen süre sonunda ekonomik ve sosyal faydaların sağlanacağı belirtilmiştir.



Şekil 3.3. Bilgi toplumu stratejisi eksenlerinin uygulama süreci [46]

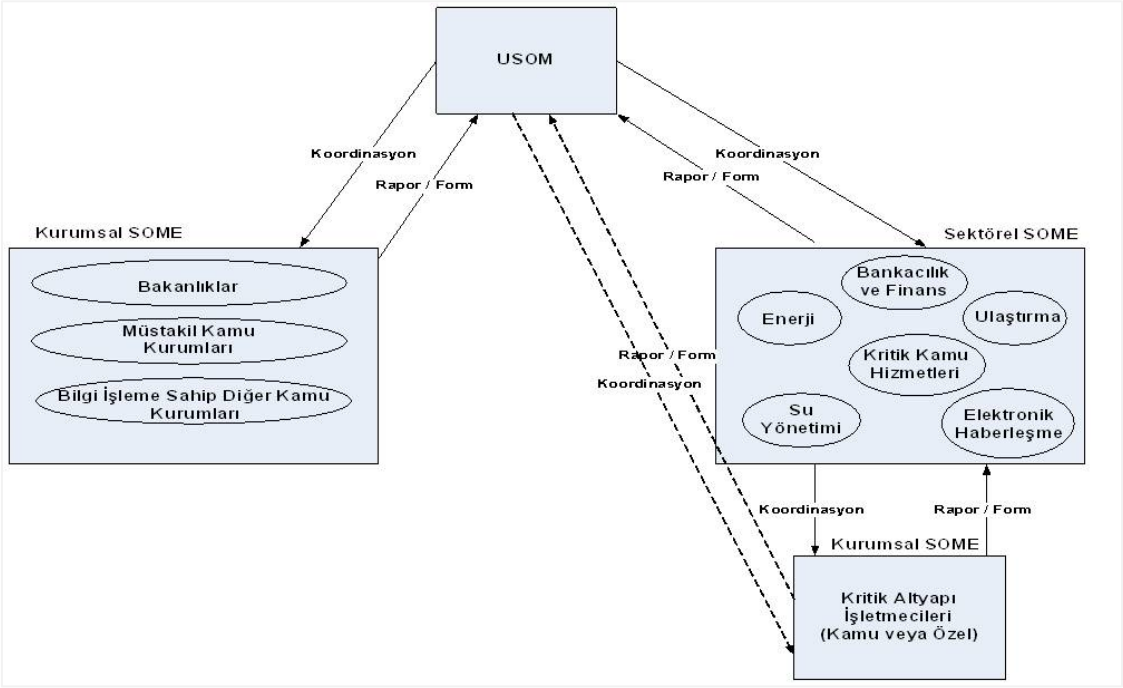
Strateji yedi farklı eksende tanımlanmıştır. Farklı her bir eksen için konuyla ilgili kamu kurumları sorumlu kılınmıştır. Bu eksenlere uygun eylem planları açıklanmıştır. Her bir eksen için zaman planlaması yapılmıştır [47].

3.8. Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ

Kasım 2013 tarihinde yayımlanan tebliğ, ülkemizde siber olaylara müdahaleyi sağlayacak ekiplerin kurulması ile ilgilidir. Bu ekiplerin kuruluş ve çalışma esasları tebliğde açıklanmaktadır. Siber olaylara müdahale kavramı, bilgi sistemlerinde tutulan bilginin üç temel yapıtaşı olan gizliliği, bütünlüğü ve erişilebilirliğini zedeleme ihtimali olan her türlü olayın tespiti ve bu bilgilere gelebilecek olası zararları önlemeyi ifade etmektedir [48].

Kurumsal Siber Olaylara Müdahale Ekipleri (SOME) hizmet gereklerine göre kurularak ihtimal dahilindeki siber olaylara karşı gerekli önlemleri almak, siber olaylara karşı müdahale edebilecek yapıyı kurmak, bilgi güvenliğine yönelik çalışmaları yürütmek ile sorumludur. Suç işlendiğine dair kanaate vardıklarında durumu USOM'a iletme görevleri de mevcuttur.

USOM ise siber olaylar karşısında kurumlar arası koordinasyonu sağlamak ve siber saldırılarla mücadele sorumluluklarına sahiptir [49]. USOM faaliyetlerini Bilgi Teknolojileri ve İletişim Kurumu (BTK) yürütmektedir. Sektörel ve Kurumsal SOME birimleri USOM ile iletişim halinde çalışma yürütmektedirler. Şekil 3.4'te siber olaylara müdahale birimleri arasındaki ilişki şema olarak ifade edilmiştir.



Şekil 3.4. USOM, sektörel some ve kurumsal some ilişkisi [31]

SOME'ler ile iletişimin sürekliğinin sağlanması önemlidir, bu nedenle 7/24 iletişim kanallarının açık olması gerektiği tebliğde belirtilmiştir. Siber olaylara müdahale işleminin sürekli olarak sürdürülmesi gerektiği belirtilmiştir. İlgili Tebliğ'de aynı zamanda Siber Güvenlik Kurulu'nun oluşması kararı da yayımlanmıştır. Siber Güvenlik Kurulu'na siber güvenlik ile ilgili plan ve politikaların hazırlanması ve koordinasyon sağlanması konusunda görevler atfedilmiştir.

SOME ve USOM yapılarının oluşturulması siber olaylarda kurumlar arasında koordinasyon ve bilgi paylaşımı sağlanması, müdahale mekanizmalarının hızlı işletilmesi açısından önemlidir. Siber Güvenlik Kurulu'nun oluşturulması ise siber uzaya dair atılacak adımlarda otorite eksikliğini gidermeye yönelik ihtiyacın karşılanması bakımından önem arz etmektedir.

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

2013 yılında yayımlanan siber güvenliğe ilişkin strateji belgesidir. Bakanlar Kurulu tarafından 25 Mart 2013'te kararlaştırmış ve 20 Haziran 2013 tarihinde Resmi Gazete'de yayımlanmıştır. Bu eylem planının kamuya ait bilgi sistemleri kaynakları ile kamu ve özel sektör tarafından işletilen kritik altyapıları kapsayacağı belirtilmiştir. Siber ortamın risklerine değinilen belgede, siber güvenliğin sağlanmasına yönelik 13 adet ilke belirlenmiştir.

Belirlenen risklere ve ilkelere bağlı olarak stratejik eylemler oluşturulmuştur. Bu eylemlerin oluşturulmasına temel olacak ana başlıklar; "*Yasal Düzenlemelerin Yapılması, Adli Süreçlere Yardımcı Olacak Çalışmaların Yürütülmesi, Ulusal Siber Olaylara Müdahale Organizasyonunun Oluşturulması, Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi, Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi ve Bilinçlendirme Faaliyetleri, Siber Güvenlikte Yerli Teknolojilerin Geliştirilmesi, Ulusal Güvenlik Mekanizmalarının Kapsamının Genişletilmesi*" olarak belirlenmiştir [50].

Belirlenen tarih aralığında üzerinde durulması planlanan 29 eylem ile ilgili çalışmaları yürütmek üzere her bir eylem için birer sorumlu kurum ve çalışmalar esnasında ihtiyaç duyulması halinde başvurulacak ilgili kurum ve kuruluşlar Eylem Planı oluşturulmuştur. Eylem planında her bir alt eyleme ait eylemin bitirilmesi öngörülen hedef ay ve yılı belirlenmiştir. Ulaştırma ve Altyapı Bakanlığı'nın başkanlık yaptığı Siber Güvenlik Kurulu koordinasyonu ile Eylem Planı'nda belirlenen çalışmalara 2015 yılında da devam edilerek toplantılar ve çalıştaylar yoluyla eylem planının uygulanma durumunun takibi ve yenilenmesine yönelik çalışmalar sürdürülmüştür.

Siber güvenlik stratejisi ancak şeffaf yönetim yapısı oluşturulması ile başarılı olabilecektir. Stratejinin koordinatörü olarak kurumlar arası çalışma grubu veya bir kamu kurumu sorumlu olmalıdır, stratejinin kendisinden ve yaşam döngüsünden bizzat yükümlü olmalıdır [51].

3.10. 2015-2018 Bilgi Toplumu Stratejisi

Mart 2015'te resmen yayımlanan 2015-2018 Bilgi Toplumu Stratejisi'nin, Strateji ve Bütçe Başkanlığı koordinasyonunda, belirlenen kurumların çalışmalarıyla hayata geçirilmesi planlanmıştır. Strateji belgesi 8 ana eksen üzerinde durmaktadır. Bu 8 ana eksen; Şekil 3.5'te ifade edildiği gibidir.

Şekil 3.5. Strateji belgesinin eksenleri [47]

Bilgi toplumu stratejisinin odak noktasının büyüme ve istihdam olduğu belirtilen strateji belgesinde iletişim teknolojilerinde yaşanan gelişmelerle aynı doğrultuda, insan kaynağına ihtiyacın hızla arttığı vurgulanmıştır [47].

Küresel yönelimlerin bilgi ve iletişim teknolojilerinin gereksinimlerini karşılama amacıyla şekillendiği, artan veri hacmi, sosyal hayatın dijital ortamlara aktarılmasının yaygınlaşması, akıllı cihaz kullanımı ve mobilizasyonun artışıyla teknolojinin gereklerine göre ülkelerde araştırma geliştirme çalışmalarına ayrılan bütçelerde artış yaşandığı ifade edilmiştir.

Stratejinin "Eylem Planı" bölümünde belirlenen her bir eksen için eylemler tanımlanmıştır. Bilgi Güvenliği ve Kullanıcı Güveni ekseni altında siber güvenlik ile ilgili konu başlıklarına yer verilmiştir. Her eylem başlığı için sorumlu kuruluşlar listelenmiştir. Bilgi Güvenliği ve Kullanıcı Güveni ekseni ile ilgili sorumlu kurumlar Aile ve Adalet Bakanlığı, Telekomünikasyon İletişim Başkanlığı ve Emniyet Genel Müdürlüğü olarak belirlenmiştir.

No	Sorumlu Kuruluş	1. Bilgi Teknolojileri Sektörü	2. Genişbant Altyapısı ve Sektörel Rekabet	3. Nitelikli İnsan Kaynağı ve İstihdam	4. Bilgi ve İletişim Teknolojilerinin Toplumsal Yaşama Nüfuzu	5. Bilgi Güvenliği ve Kullanıcı Güveni	6. Bilgi ve İletişim Teknolojileri Destekli Yenilikçi Çözümler	7. İnternet Girişimciliği ve e-Ticaret	8. Kamu Hizmetlerinde Kullanıcı Odaklılık ve Etkinlik	Yatay Konular	Toplam
1	Başbakanlık								3		3
2	Adalet Bakanlığı					3					3
3	Aile ve Sosyal Politikalar Bakanlığı				3						3
4	Bilim, Sanayi ve Teknoloji Bakanlığı	4					1	2			7
5	Çalışma ve Sosyal Güvenlik Bakanlığı			3							3
6	Çevre ve Şehircilik Bakanlığı		1				1		1		3
7	Ekonomi Bakanlığı	1						1			2
8	Enerji ve Tabii Kaynaklar Bakanlığı						1				1
9	Gümrük ve Ticaret Bakanlığı							3			3
10	İçişleri Bakanlığı								1		1
11	Milli Eğitim Bakanlığı	1		1	2						4
12	Kalkınma Bakanlığı						1			2	3
13	Kültür ve Turizm Bakanlığı						1				1
14	Sağlık Bakanlığı						3				3
15	Ulaştırma, Denizcilik ve Haberleşme Bakanlığı		7		1				7		15
16	Yükseköğretim Kurulu			4							4
17	Bilgi Teknolojileri ve İletişim Kurumu		3								3
18	Telekomünikasyon İletişim Başkanlığı					1					1
19	Sosyal Güvenlik Kurumu						1				1
20	Devlet Personel Başkanlığı								1		1
21	TÜİK				1						1
22	KOSGEB	1						1			2
23	Emniyet Genel Müdürlüğü					1					1
24	İŞKUR			1							1
25	TOBB	1									1
26	ODTÜ Teknokent Yönetim A.Ş.	1									1
TOPLAM		9	11	9	7	5	9	7	13	2	72

Şekil 3.6. Eylemlerin eksenlere ve sorumlu kuruluşlara göre dağılımı [47]

Güvenli İnternet Kullanımında Farkındalığın Artırılması başlıklı eylem maddesi ile ilgili sorumlu kurum olarak TİB; ve diğer iş birliği yapılacak kurumlar belirlenmiştir. Eylemin amacı, bilinçli internet kullanımı ve kullanıcı güvenini arttırmak amacıyla farkındalık çalışmalarının yapılması konularında çalışmaların yürütülmesidir. Eylem tamamlanma yılı olarak 2018 yılı hedeflenmiştir.

Bilişim Suçları İhtisas Mahkemelerinin Kurulması başlıklı eylem maddesi ile ilgili sorumlu kurum olarak Adalet Bakanlığı; iş birliği yapılacak kurum olarak Hakimler ve Savcılar Kurulu (HSK, eski adıyla Hakimler ve Savcılar Yüksek Kurulu) belirlenmiştir. Bu eylem ile bilişim suçlularının yargılanacağı mahkemelerin ayrılması, bu mahkemelerde bilişim alanında yetkin cumhuriyet savcıları ve hakimlerin çalışması amaçlanmaktadır. Eylemin tamamlanma yılı olarak 2015 yılı hedeflenmiştir.

3.11. 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı ve Kamunet Projesi

2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı; Türkiye'nin 2023 vizyonu, Onuncu Kalkınma Planı ve 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı (BTS) çerçevesinde, kurum/kuruluşların stratejik planları, diğer ulusal strateji belgeleri ("Kayıt Dışı Ekonominin Azaltılması Programı Eylem Planı", "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı", "Türkiye Ulaşım ve İletişim Stratejisi Hedef 2023" vb.) ve e-Devlet ekosistemindeki tüm paydaşların ihtiyaçları dikkate alınarak hazırlanmıştır. e-Devlet Stratejisi ve Eylem Planı'yla, Türkiye'nin 2023 ulusal hedefleri doğrultusunda gerekli kabiliyetlerinin oluşturulması ve ülke refahı için kaldıraç etkisinin sağlanması amaçlanmaktadır. Bu doğrultuda, 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı'nın vizyonu "Etkin e-Devlet ile toplumun yaşam kalitesini artırmak" olarak tanımlanmıştır [52].

5809 sayılı Elektronik Haberleşme Kanunu'nun 5. Maddesinin 1 inci fıkrasının h bendi, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı ile Siber Güvenlik Kurulu Kararları uyarınca KamuNet'in oluşturulması çalışmaları Ulaştırma ve Altyapı Bakanlığı'nca yürütülmektedir. KamuNet projesi ile kamu kurum ve kuruluşları arasındaki veri iletişiminin internete kapalı, fiziksel ve siber saldırılara karşı daha güvenli sanal bir ağ üzerinden yapılması; siber güvenlik risklerinin minimize edilmesi, mevcut ve kurulacak olan güvenli kapalı devre çözümlere standart sağlanması, ortak uygulamalar için uygun alt yapının tesis edilmesi amaçlanmaktadır [53].

3.12. 2016-2019 Ulusal Siber Güvenlik Stratejisi

Strateji belgesinin kapsamı, bir önce yayımlanan strateji belgesi ile kıyaslandığında kısmen genişletilmiştir. Önceki planda özel sektörün sadece kritik alanlarıyla ilgili görülen stratejik plan, yeni dönemde ulusal siber uzayın her bir unsurunu kapsayacak şekilde geniş tutulmuştur.

Bir önceki strateji belgesine benzer olarak ilkeler ve siber güvenlik riskleri maddeler halinde belirlenmiştir. Mevcut risklerin asgari düzeye indirilmesini hedefleyen stratejik amaçlar açıklanmıştır. Belirlenen stratejik amaçlar; "*Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması, Siber Suçlarla Mücadele, Farkındalık ve İnsan Kaynağı Geliştirme, Siber Güvenlik Ekosisteminin Oluşturulması, Siber Güvenliğin Milli Güvenliğe Entegrasyonu*" olarak beş eylem başlığında toplanmıştır [16]. Ana eylem başlıkları alt eylem

başlıklarına ayrılarak her bir alt eylemin yürütülmesi ile konusunda sorumlu kuruluş, eylemin yürütülmesi esnasına ihtiyaç duyulması halinde başvurulacak ilgili kuruluşlar belirlenmiştir. Bir önceki eylem planında olduğu gibi, her bir eylemin kurumlar tarafından bitirilme tarihleri için hedefler belirlenerek strateji belgesinde yer alan amaç ve hedeflerin 2016-2019 yılları arasında tamamlanması planlanmıştır.

"Siber Güvenlik Ekosisteminin Oluşturulması" ifadesi ilk olarak bu dönemin strateji belgesinde yer almıştır. Siber Güvenlik Kurulu tarafından kabul edilen bir belgede bu konuya yer verilmesi, siber uzayı oluşturan her bir paydaşa önem verildiğinin açık göstergesidir. Planın sürekliliğinin takibi amacıyla, Ulaştırma ve Altyapı Bakanlığı tarafından çeşitli dönemlerde çalıştaylar düzenlenerek eylem maddelerinin sorumlu ve ilgili kuruluşlar tarafından uygulanıp uygulanmadığı, çalışmalarla ilgili ne aşamada olunduğu izlenmektedir. Bu anlamda 23 Kasım 2016'da ilk çalıştay düzenlenmiş olup ilgili ve sorumlu kuruluşlar, kendilerinin sorumluğundaki eylem maddeleri konusunda yaptıkları çalışmalarda ne aşamada olduklarını, katılımcılar ile paylaşmışlardır.

4. DÜNYA ÖRNEKLERİNİN SİBER GÜVENLİK EKOSİSTEMİ AÇISINDAN İNCELENMESİ

Teknolojinin hayata yoğun olarak nüfuz etmesinin bir sonucu olarak pek çok dünya ülkesi siber güvenlik konusunda strateji belgeleriyle yasal mevzuatlarını güçlendirme yolunda gitmiştir. Yapılan çalışmaların getirisi olarak bu ülkeler, siber güvenlik alanında yatırımlarını ve finansman kaynaklarını arttırmıştır. Dünya ekonomisine yön veren ülkelerin siber güvenliğe olan bakışını anlamak amacıyla, öncelikli olarak G8 ülkelerinin siber güvenliğe ilişkin çalışmaları araştırılmıştır. G8 ülkelerine ek olarak Avustralya, Çin, Güney Kore, Finlandiya, Hindistan ve İspanya'nın siber güvenliğe ilişkin çalışmalarının genel hatları, çalışmanın bu kısmında incelenmiştir.

Siber güvenlik ekosisteminin geliştirilmesine katkı sunması amacıyla belirlenen bu ülkelerde siber güvenlik alanında çalışmalar yürüten kuruluşlara ve her ülkenin kendi siber güvenlik ekosisteminin unsurlarına ilişkin bilgiler araştırılırken, literatürde önemli olarak değerlendirildiği gözlemlenen bazı temel kıstaslar esas alınmıştır. Bu kıstaslar;

- Politika ve stratejik plan üreten otoriteler, koordinasyon makamları,
- Siber olayların yönetimi ve koordinasyonu,
- Siber uzayda siber istihbarat çalışmaları ve siber savunma amaçlı çalışmalar,
- Siber güvenlik ve milli güvenlik ilişkisi,
- Kritik altyapılara ilişkin çalışmalar,
- Siber güvenlik kümelenmeleri,
- Yatırımcılar ile kamu kurumları arasındaki ilişkiler ve yerli üretim mekanizması,
- Sivil toplum kuruluşları ile kamu kurumları arasındaki ilişkiler ve toplumsal bilinçlendirme çalışmaları,
- Uluslararası iş birliğine yönelik çalışmalar,
- Akademik iş birlikleri, eğitim sisteminde siber güvenliğe ilişkin çalışmalar,
- Belgelendirme ve sertifikasyon mekanizmaları,
- Paydaşlarla ilişkiler

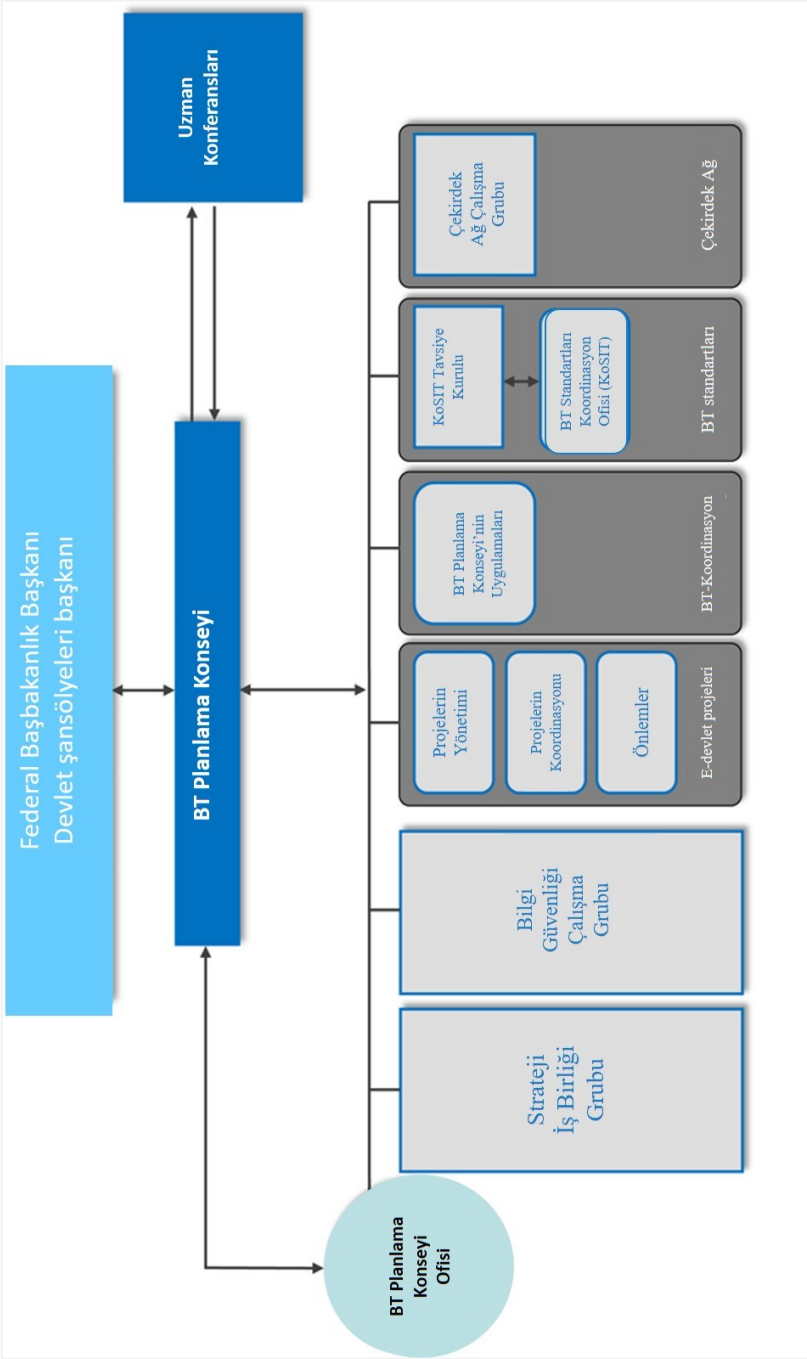
olarak ele alınmıştır.

4.1. Almanya

Siber güvenlik konusunda ülkelerin yaptığı çalışmalar incelendiğinde Almanya'nın bu alanda yaptığı çalışmalar dikkat çekici seviyededir. **Federal Bilgi Teknolojileri Güvenliği Ofisi**'nin (BSI) varlığı ve siber güvenlik konulu stratejik çalışmaları örnek alınabilecek niteliktedir [64]. Ulusal bir siber güvenlik yetkilisi olarak, Federal Bilgi Teknolojileri Güvenliği Ofisi'nin amacı, Almanya'daki bilgi teknolojileri (BT) güvenliğini teşvik etmektir. Federal Bilgi Teknolojileri Güvenliği Ofisi, öncelikle Almanya'daki federal hükümet için merkezi BT güvenlik hizmeti sağlayıcısıdır. Ulusal siber güvenlik otoritesi olarak, devleti, işletmeleri ve toplumu sayısallaştırma yoluyla siber tehditleri önlemek, tespit etmek ve bunlara ilişkin reaksiyon almak suretiyle bilgi güvenliğine ilişkin süreçleri şekillendirmektedir [65].

Federal İçişleri Bakanlığı (BMI, Bundesministerium des Innern, für Bau und Heimat), Almanya'daki iç güvenlikten sorumlu bakanlıktır. BMI, alt ajanslarının (Federal Sivil Koruma ve Afetler Ofisi ve Federal Bilgi Teknolojileri Güvenliği Ofisi dahil) tüm faaliyetlerini koordine eder ve denetler. Ayrıca Almanya'nın e-devlet stratejisini, siber güvenlik stratejisini hazırlayan ve uygulanmasını takip eden bakanlık konumundadır.

BT Planlama Konseyi'nin (IT-Planungsrats) görevleri; "federal ve eyalet hükümetleri arasında bilgi teknolojisi konularında iş birliğini koordine etmek; BT birlikte işlerliği ve BT güvenlik standartlarını benimsetmek; e-devlet projelerini yönetmek; federasyon tarafından kurulacak ve işletilecek olan çekirdek ağın planlanması ve geliştirilmesi" [54] olarak sayılmaktadır. BT Planlama Konseyi organizasyon yapısı Şekil 4.1'de olduğu gibidir.



Şekil 4.1. Almanya BT planlama konseyi organizasyon yapısı [55]

BT Güvenliği Koordinasyon Ofisi (KITS, Koordinierungsstelle IT-Sicherheit), BT Başkanlığı Komitesi'ne tahsis edilen koordinasyon ofisidir [5]. BT güvenliği için farklı yöneticiler arasında arabulucu rolündedir. KITS bilgi alışverişi konusunda görevleri de bulunmaktadır, bu nedenle gerçek anlamda bir standardizasyon kuruluşu değildir. BT güvenliğinde standardizasyon ile ilgili alanlarda çalışmalar da yürütür. BT'ye ilişkin güncel gelişmeler, koordinasyon ofisinde karşılaştırılmaktadır ve bu gelişmeler doğrultusunda standardizasyon önerileri verilmektedir [56].

Alman Standartlar Enstitüsü'nün (DIN, Deutsches Institut für Normung) "Focus.Ict" Başkanlık Komitesi alt kuruluşu olan KITS'in görevleri [57] şunlardır:

- Çeşitli aktörlerin çalışmalarını koordine etmek (standartlar komiteleri, teknik birlikler, BT güvenliği ile ilgili endüstri uzmanları, devlet kurumları),
- BT ile ilgili standartlar üzerinde çalışan güvenlik standartları danışmanlık komiteleriyle çalışmak (örneğin akıllı şebeke, bilişim ve tıp),
- BT güvenliği ile ilgili tüm standart projelerin Alman paydaşlar için bir indeksini tutmak ve BT güvenliğini sağlamak amacıyla Alman Standardizasyon Yol Haritası'nın güncel tutulmasını sağlamak,
- Almanların Avrupa ve uluslararası standartlara uyumu konusunda yapılacak çalışmaları koordine etmek, bu çalışmaları Alman endüstrisinin, kamu otoritelerinin çıkarları doğrultusunda yürütmek.

Almanya'da ordu, siber güvenliği sağlayan makam konumundadır. Ayrıca Almanya devleti, her kurumun kendi bünyesinde siber olaylara müdahale ekiplerini kurmasını önermektedir. Bu yapılanma örneği ülkemizde USOM-SOME ilişkisine benzer mantıkla çalışmaktadır [35].

Ulusal Siber Olaylara Müdahale Merkezi (Nationales Cyber-Abwehrzentrum), Nisan 2011'de siber olayların çözümlenmesine ilişkin çalışmalarına başlamış ve devlet yetkililerinin iş birliğini sağlamayı amaçlamıştır [5].

Anayasayı Koruma Federal Dairesi (BfV, Bundesamt für Verfassungsschutz), Almanya Federal Cumhuriyeti'nin istihbarat servisidir. BfV, BT olaylarına karşı alınan koruyucu önlemlerin ve tepkisel koordinasyonun sağlanması yoluyla Ulusal Siber Olaylara Müdahale Merkezi'ne katkıda bulunan ortaklardan biridir [5].

Siber saldırılar karşısında atılacak adımlar Enformasyon Altyapısının Korunması Ulusal Planı'nda tanımlıdır. Bu plan Federal Bilgi Teknolojileri Güvenliği Ofisi tarafından uygulanmaktadır. İlgili çalışma planında, siber güvenliğe ilişkin çalışmaların sadece yetkili kamu kurumları tarafından değil özel kurumların da katılımı sayesinde ilerletilmesi gerektiği ifade edilmiştir. Bu plan, siber uzayda etkileşimin ve iş birliğinin önemini vurgulayarak siber risklere ilişkin farkındalığın bireyler tarafından iyi anlaşılması gerektiğine değinmekte ve

uluslararası iş birliğinin gerekli olduğuna yer vermektedir. Bu hususlara istinaden Almanya'da uygulanması gereken çalışma hedeflerine planda yer verilmektedir [35].

Almanya siber güvenlik strateji belgesinde on stratejik alan üzerine odaklanıldığı görülmektedir. Bu alanlar şu şekildedir: (1)Kritik önemdeki altyapıların korunması, (2)Ülkedeki güvenli bilgi ve iletişim sistemleri, (3)Kamu yönetiminde bilgi sistemlerinin güvenliğinin güçlendirilmesi, (4)Ulusal siber müdahale merkezi, (5)Ulusal siber güvenlik konseyi, (6)Etkili siber suç kontrolü, (7)Avrupa ve dünya ile etkili bir iş birliğinin sağlanması, (8)Güvenilir bilgi teknolojisi kullanımı, (9)Kamudaki personelin gelişimi ve (10)Siber saldırıları karşılayacak ve cevap verecek araçlar [36]. 2016 yılında Almanya'nın yeni Siber Güvenlik Strateji Belgesi, BMI tarafından yayımlanmıştır.

Federal Sivil Koruma ve Afetler Ofisi (BBK, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe), devlet ve toplum için kritik altyapılara ilişkin oluşturulan KRITIS'in önemine ilişkin işletmelerde ve kamuoyunda farkındalık yaratmak, kritik altyapıların işleyişini ve karşılıklı bağımlılıklarını tanımlamak, yetkililer arasındaki iş birliğini tesis etmek ve yoğunlaştırmak hakkında bilgi vermekle görevlidir. KRITIS için analiz ve koruma kavramlarının geliştirilmesi ve kritik altyapıların korunması için kısa, orta ve uzun vadeli önlemlerin alınması da BBK'nın görevleri arasındadır [5].

BBK, sivil koruma ve afet yardımı görevlerini yerine getirir. Bir felaket durumunda nüfusun korunması için tasarlanmış önleyici tedbirler ve politikalar geliştirir. Ayrıca, kritik altyapıların korunmasına odaklanan çeşitli projelerden de sorumludur [58]. BBK, kritik altyapılara ilişkin Federal Bilgi Teknolojileri Güvenliği Ofisi ile birlikte ortak projeler yürütmektedir. 2017 yılında kritik alt yapıların korunmasına yönelik yedi temel adımın yer aldığı rehber hazırlanmıştır. Aynı belgede kritik altyapı sektörleri Şekil 4.2'de olduğu gibi belirlenmiştir.

Şekil 4.2. Almanya kritik altyapı sektörleri [58]

2004'ten bu yana, Almanya'da federal düzeyde ve eyalet düzeyinde kriz yönetimi sistemi, iki yılda bir yapılan periyodik tatbikatlar, departmanlar arası ve uluslararası kriz yönetimi uygulanması yoluyla, gelişme potansiyeli bakımından değerlendirilmiştir. Bu tatbikatlar Uluslararası Kriz Yönetimi Tatbikatı (LÜKEX, Länderübergreifende Krisenmanagement Exercise) olarak adlandırılmaktadır. Çeşitli bakanlıklar ve federal kurumlar, ülkeler ve yardım kuruluşları ile birlikte sürekli olarak felaket senaryolarını değiştirmektedirler. Katılımcılar, kriz yönetimi için kendi yapılarını ve prosedürlerini bu tatbikat çalışmaları aracılığıyla paylaşarak birbirlerini tanımakta ve bilgi-deneyim alışverişinde bulunmaktadırlar [59].

Almanya, önde gelen sanayi ve teknoloji odaklı uluslardan biridir. Kritik altyapıların korunmasına yönelik ulusal strateji belgesine ek olarak Almanya'nın kritik altyapılarının korunması amacıyla "UP KRITIS" olarak adlandırılan; kamu-özel ortaklığı yapısı oluşturulmuştur [60].

Almanya, siber güvenlik kümelenmeleri açıısndan incelendiğinde Bonn Siber Güvenlik Kümesi ile karşılaşılmaktadır. Bonn Siber Güvenlik Kümesi, Bonn/Rhein-Sieg bölgesindeki bilim, araştırma ve eğitim, işletme, kamu otoriteleri ve kamu kurumları ile siber güvenlik kümesindeki diğer kuruluşların tanıtımını yapmaktadır. Amaç, özellikle Bonn/Rhein-Sieg

bölgesini, ulusal ve uluslararası saygın ve tanınan bir siber güvenlik bölgesi olarak geliştirmeye ve genişletmeye yardımcı olmaktır [61].

Almanya'da, 2009 yılında, Federal Eğitim ve Araştırma Bakanlığı (BMBF) ve Federal İçişleri Bakanlığı arasında BT güvenliğine ilişkin araştırmalar konusunda bir anlaşma imzalamıştır. BT Güvenliği Araştırma Programı (IT Security Research), bilgi güvenliği teknolojilerinde araştırma ve geliştirmeyi kapsamaktadır. BMBF, 2011 yılından beri siber güvenlik alanında lider üniversiteleri ve üniversite dışı kurumları bir araya getiren üç araştırma merkezini desteklemektedir [62].

Alman Standartlar Enstitüsü (DIN, Deutsches Institut für Normung), Avrupa ve uluslararası standart organizasyonlarında Alman menfaatlerini temsil eden bir ulusal standart organıdır. Özellikle, ISO/IEC, JTC1, SC27 sekreterliği olarak hizmet vermektedir [5].

BT Standartları Koordinasyon Ofisi (KoSIT, Koordinierungsstelle für IT-Standards), kamu yönetiminde veri alışverişi için BT standartlarının geliştirilmesi ve işletilmesini koordine etme görevine sahiptir. KoSIT, disiplinlerarasında BT iş birliği yapılması, BT güvenlik standartlarına karar verilmesi, ulusal ve uluslararası e-devlet projelerinin yönetilmesi konularında BT Planlama Konseyi'ni desteklemektedir. KoSIT, sadece federal hükümet ve eyaletlerin değil, belediyelerin ve Federal Bilgi Teknolojileri Güvenliği Ofisi'nin temsil edildiği bir danışma konseyi tarafından yönetilmektedir [63].

4.2. Amerika Birleşik Devletleri

Teknoloji üretiminin merkezi sayılabilecek ve büyük teknoloji firmalarına ev sahipliği yapan bir ülke olarak ABD, bu sektörün riskleriyle de en fazla yüzleşen ülke konumundadır. Bilgi varlıklarının çokluğu, bu varlıkların korunmasına yönelik çalışmaları hızlandırmıştır. Tüm dünyaya yayılım sağlayan birçok teknolojik ürünün üretildiği ve dünyaya pazarlandığı, hem donanım hem yazılım hizmetlerinde sektörde ön sıralarda yer alan ABD, çeşitli zamanlarda siber saldırıların da hedefi olmaktadır. Birçok büyük teknoloji firması farklı dönemlerde siber saldırılar neticesinde bilgi varlıklarının siber saldırganlar tarafından çalınmasıyla yüzleşmiştir, dolayısıyla da bu şirketler itibar kayıpları ile gündeme gelmiştir. ABD'nin bilgi güvenliğini sağlama amaçlı çalışmaları 1990'lı yıllara dayanmaktadır [64]. ABD siber güvenlik sistemi Şekil 4.3'te olduğu gibidir.

İç Güvenlik	İstihbarat	Savunma	Kanuni Yaptırım

• **DHS**- siber güvenlik ve farkındalık çalışmalarının tüm partnerlerle birlikte oluşturulması ve sürdürülmesi için ulusal olarak çalışır.
• **DHS**-Siber olayların yönetimi ve koordinasyonunda ulusal odak noktası olarak hizmet eder.
 	
Koordinasyon Merkezleri
• NCCIC
  ○ US-CERT
  ○ NCC
  ○ ICS-CERT
• NOC
  ○ NICC
  ○ NRCC
 	
İlgili Bakanlık/Otorite
• Kabine Bakanlıkları
• Bağımsız ajanslar ve devlet şirketleri
 	
Dış Paydaşlara Destek
• **Devlet, Yerel, Kabilesel, Bölgesel**-Talep üzerine olay cevaplarını koordine eder ve destek verir.
• **Özel Sektör**-Kaynak tahsisi ve aksiyonların önceliklendirilmesine destek olmak amaçlı bazı gerçek zamanlı verilerin toplanmasını, analizini ve paylaşımını koordine eder.
	• **IC**-Gelecek olayları önlemek ve siber tehditleri ve saldırıları tiplerini karakterize etmek için saldırı algılama ve uyarı mekanizmaları sağlar.
	
	Koordinasyon Merkezleri
	• IC-IRC
	• NTOC
	• NCIJTF
	
	İlgili Bakanlık/Otorite
	• Kabine Bakanlıkları
	• Bağımsız ajanslar ve devlet şirketleri
	
	Dış Paydaşlara Destek
	• **Devlet, Yerel, Kabilesel, Bölgesel-** CIKR kriz yönetimi ve tehdit istihbarat grupları tarafından sektörel etki değerlendirmeleri ve yanıt koordinasyonunda olabilecek en az müdahaleyi sağlayacak şekilde ayıklanmış ve uygun bir şekilde sınıflandırılmış istihbarat bilgisini paylaşır.
		• **DOD**-.mil ağının savunulması ve işletimini yönetir ve durumsal farkındalık paylaşımını oluşturur ve sürdürür.
		• **DOD**-siber tehditlere karşı ortak tavır belirlemek, siber tehditleri azaltma teknikleri belirlemek, ulusal güvenliği büyük ölçüde tehdit eden siber saldırılara karşı savunma ve yok etme amaçlı aksiyonlar almak üzere çalışır.
		• **Ulusal Güvenlik Bürosu**-NG kuvvetlerinin siber olaylara karşılık vermeleri esnasında senkronizasyonunu koordine eder ve iletişimlerini sağlar. (siber uzay, iletişimler ve sinyaller organizasyonunu kapsar ama görevleri bunlarla sınırlı değildir.)
		
		Koordinasyon Merkezleri
		• USCYBERCOM JOC
		• NTOC
		• DC3
		
		İlgili Bakanlık/Otorite
		• Kabine Bakanlıkları
		• Bağımsız ajanslar ve devlet şirketleri
			• **DOJ**-Kanuni yaptırımlara ilişkin durumsal farkındalık oluşturur ve bilgi paylaşır.
			• **AG**-Kriminal soruşturmalara liderlik eder.
			• **DOJ**-Siber suçların kovuşturma ve soruşturma amaçlı ulusal çalışmalara liderlik eder.
			
			Koordinasyon Merkezleri
			• NCIJTF
			• DC3
			
			Dış Paydaşlara Destek
			• **Devlet, Yerel, Kabilesel, Bölgesel-** DOJ/FBI/NCIJTF kanuni yaptırımlarla koordine eder.
			• **Özel Sektör**-FBI InfraGrad çalışmaları ile özel sektörle birlikte siber suça ilişkin soruşturma ve kovuşturma işlerini koordine eder.

Şekil 4.3. ABD'nin siber güvenlik sistemi [38]

İç Güvenlik Bakanlığı (DHS, Department of Homeland Security), doğrudan başkanlık makamına bağlı bir güvenlik kurumu olarak çalışmakta ve siber güvenliğe ilişkin çalışmaları

yürütmektedir. Siber güvenlik politikalarının devlet başkanıyla direkt iletişimde olunarak belirlenmesi, siber güvenliğe verilen önemin bir göstergesidir [65]. DHS'nin çok sayıda yerel güvenlik misyonu vardır ve kritik altyapı ve bilgi sistemlerini güvence altına almak için sanayi ve eyalet, yerel ve bölgesel yönetimlerle çalışır. Analizlerde önemli bir rol oynar, tehditleri azaltır ve uyarılarda bulunur [5].

DHS, ABD sınırları dahilinde siber güvenlikten sorumlu olan başlıca kurumdur. Siber uzayı korumak ve güvenliğini sağlamak için öncelikli alanlar (DHS'nin beş temel görevi) şunlardır: kritik altyapının güvenliğini ve esnekliğini güçlendirmek; federal sivil kurumlara siber güvenlik tedarikleriyle ilgili olarak yardım etmek ve ortak risk temelli politikaların ve en iyi uygulamaların benimsenmesini teşvik etmek; hukuki yaptırımı, olay yanıtını ve raporlama yeteneklerini ilerletmek ve sağlıklı bir siber ekosistem sağlamaktır [66].

Siber politikalara ilişkin sorumluluklar geniş ölçüde dağıtılmış durumda olmasına karşın, temel politika koordinasyon görevleri, Beyaz Saray'daki Ulusal Güvenlik Konseyi'nin Bilgi ve İletişim Altyapısı Kurumlararası Politika Komitesi (ICI-IPC) tarafından yürütülmektedir. ICI-IPC'ye, Ulusal Güvenlik Konseyi Başkanı'nın baş danışmanı olarak görev yapan Siber Güvenlik Koordinatörü (CSC) tarafından başkanlık yapılmaktadır. CSC, ulusal siber güvenlik stratejisi ve politikasının kurumlar arası gelişimini yönetmekte ve ajansların uygulamasını denetlemektedir. CSC, bu çalışmaları yürütürken Ulusal Güvenlik Konseyi'ne rapor verir, Beyaz Saray'daki istişare sürecine öncülük eder ve ABD'nin siber güvenlikle ilgili politika ve faaliyetlerini koordine eder [66].

DHS'ye bağlı çalışan ve siber güvenlik ile ilgili üç önemli bölüm; Siber Güvenlik ve İletişim Ofisi (CS&C, Office of Cybersecurity and Communications), Bilim ve Teknoloji Müdürlüğü (S&T, Science and Technology Directorate) ve Altyapı Koruma Ofisi (IP, Office of Infrastructure Protection)'dir. Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi (NCCIC), ABD Ulusal İletişim Koordinasyon Merkezi (NCC), Endüstriyel Kontrol Sistemleri Bilgisayar Acil Müdahale Ekibi (ICS-CERT) ve ABD Ulusal Bilgisayar Acil Müdahale Ekibi (US-CERT), Siber Güvenlik ve İletişim Ofisi'ne bağlı olarak çalışmaktadır [5].

Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi (NCCIC, The National Cybersecurity&Communications Integration Center), Federal Hükümet, istihbarat topluluğu ve kolluk kuvvetleri için ulusal siber güvenlik ve haberleşme entegrasyonu

sağlayabilen bir yönetim merkezi sunmaktadır. Misyonu, hükümet ve özel sektörün her seviyesi arasındaki iş birliği ve bilgi paylaşımını sağlamaktır. NCCIC, kritik altyapı sahipleri ve operatörleri ile yakın bir şekilde çalışmasına rağmen, özel sektördeki siber güvenlik önlemlerini uygulama yetkisine sahip değildir; faaliyetleri arasında güvenlik açıkları, izinsiz girişler, olayların tespiti, tehditleri azaltma ve veri kurtarma eylemleriyle ilgili durumsal farkındalığın sağlanması yer almaktadır. NCCIC, çalışmalarını, NCCIC Operasyon ve Entegrasyon (NO&I), US-CERT, ICS-CERT ve NCC olmak üzere dört şubeyle sürdürmektedir. Bu şubeler, tüm federal kurumların sistemlerini güvence altına almaları ve FISMA (The Federal Information Security Management Act of 2002) ile belirlenen siber güvenlikle ilgili konulara yardımcı olma konusunda koordinasyon ve destek açısından bir çerçeve sunmaktadır [66].

Devlet Bakanlığı (DoS, Department of State), Başkan'ın siber güvenlik politikasını uluslararası olarak koordine etmek için başlıca kurumdur. DoS ekonomi ve insan hakları konularına internet özgürlüğü ve siber güvenlik açısından yaklaşır. "Siber Konulara İlişkin Koordinasyon Ofisi", bölüm içindeki siber güvenliğe ilişkin konularda koordinasyon sağlar. Ofisin sorumlulukları devlet sekreterlerine siber konularda danışmanlık verme ve Beyaz Saray'ın diğer federal departmanları, ajansları ve özel sektör ile irtibat halinde olmasını kapsamaktadır [66].

Ulusal Güvenlik Sistemleri Komitesi (CNSS, Committee on National Security Systems), ABD Hükümet Departmanları ve Ajansları için ulusal düzeyde bilgi güvenliği politikaları, direktifleri, talimatları, operasyonel prosedürleri ve tavsiyeleri belirler [5].

Savunma Bakanlığı (DoD, Department of Defense), siber güvenlikte operasyonel rollerini ve sorumluluklarını Ortak Operasyon Merkezi (USCYBERCOM), Ulusal Güvenlik Ajansı (NSA), Ulusal Güvenlik Sistemleri Komitesi (CNSS), Savunma Siber Suç Merkezi (DC3) ve Savunma Bilgi Sistemleri Ajansı (DISA) aracılığıyla gerçekleştirilir. Özellikle DISA, askeri ağlara ilişkin bilgi teknolojisi ve iletişim desteği sağlamakla görevlendirilmiştir [66]. DISA, komuta ve kontrol ve bilgi paylaşımı yetenekleri ile dünya çapında erişilebilir kurumsal bilgi altyapısını sağlar, işler ve temin eder. Savunma Bakanlığı'na bağlı olarak görev yapan bir diğer önemli kuruluş ise Siber Güvenlik ve Bilgi Sistemleri Bilgi Analiz Merkezi (CSIAC)'dir. CSIAC, Savunma Teknik Bilgi Merkezi (DTIC) tarafından desteklenen bir Bilgi Analiz Merkezi (DTIC)'dir [5].

Ulusal Güvenlik Ajansı (NSA, National Security Agency), hem istihbarat hem de bilgi güvence misyonunu sürdürmektedir.

ABD 2015 Ulusal Güvenlik Strateji Belgesi'nde, paylaşılan alanlara ilişkin güvence başlığı altında siber güvenliğe yer vermiştir. Bu başlık altında, internetin ortaya çıkışı ile birlikte ABD'nin birbirine bağlı dünyaya liderlik etme konusunda özel bir sorumluluk aldığı ifade edilmiştir. Ekonomi, güvenlik, sağlık gibi birçok alanın birbirine bağlı altyapılar olduğu ve bu yapıların kötü niyetli devletler, suçlular, bireysel aktörler tarafından hedef alındığı belirtilmiştir. 2018 yılında yayımlanan strateji belgesinde ekonominin teknoloji bağımlılığının giderek artmasının bir neticesi olarak inovasyon çalışmalarına daha fazla önem verileceği konusuna yer verildiği gözlenmektedir. Ayrıca hükümetin esnek ve canlı bir siber ekosistemin gelişimi için sürekli gelişim amaçlı çalışmalar yürüteceği ifade edilmiştir [67].

Adalet Bakanlığı (DoJ, Department of Justice), siber güvenliğe ilişkin yasaların uygulanmasından büyük ölçüde sorumludur. Doj, saldırı vakalarını soruşturmak ve yargılamak, ulus devletin desteğini desteklemek için istihbarat toplamak ve diğer birimlere yasal ve politik destek sağlamak suretiyle siber tehdide karşı koyar. DoJ siber suçları yargılamaktadır; kendi yargı yetkisi altındaki siber suçları inceler, özetler ve yabancı istihbarat, terörist veya diğer ulusal güvenlik tehditleri de dahil olmak üzere siber tehditlerle ilgili ulusal güvenlik operasyonlarına öncülük eder; ve siber tehdit bilgilerinin yurt içinde toplanması, analizi ve dağıtılması işlerini yürütür. Ulusal güvenliğe yönelik siber tehditlerle mücadeleye yönelik bir hükümet yaklaşımının sağlanmasında, DoJ'nin Ulusal Güvenlik Bölümü, bölümün diğer bileşenleriyle iş birliği içinde, siber saldırılara daha iyi cevap vermek için ülke çapında Ulusal Siber Güvenlik Uzman Ağı çalışması başlatmıştır. DoJ'nin Bilgisayar Suçları ve Fikri Mülkiyet Hakları Bölümü (CCIPS), diğer devlet kurumları, özel sektör, akademik kurumlar ve yabancı meslektaşlarıyla birlikte çalışarak bilgisayar suçlarını önler, inceler ve kovuşturur [66].

DoJ siber güvenliğe ilişkin çalışmaları yürütürken (CCIPS), Federal Soruşturma Bürosu (FBI), Ulusal Siber Soruşturma Ortak Görev Gücü (NCIJTF) ve Federal İletişim Komisyonu (FCC) ile birlikte çalışmaktadır.

Devlet Hizmetleri İdaresi (DoD, Government Services Administration), DHS ve diğer departmanlar ve ajanslar ile istişare halinde, kritik altyapı sistemleri için devlet çapında

sözleşmeler sağlar ve destekler. Bu tür sözleşmelerin, kritik altyapının güvenliği ve dayanıklılığı için denetim haklarını içermesini sağlar [5].

Federal Acil Durum Yönetim Kurumu (FEMA, Federal Emergency Management Agency), siber güvenliğe ilişkin çeşitli sorumluluklara sahiptir.

Ulusal Siber Güvenlik Mükemmeliyet Merkezi (NCCoE-NIST, National Cybersecurity Center of Excellence), NIST tarafından desteklenen CCoE, ticari işletmelere mevcut teknolojilere dayalı olarak siber güvenlik çözümleri sunmaktadır. Merkez, maliyet etkin, tekrarlanabilir ve ölçeklendirilebilir bir şekilde siber güvenliği sağlamak için endüstri, hükümet ve akademi uzmanlarını bir araya getirmektedir [5].

Ulusal Bilgi Güvencesi Eğitim ve Öğretim Programı (NIETP, National Information Assurance Education and Training Program), NSA ve DHS ve Ulusal Akademik Mükemmeliyet Merkezleri'nin ortaklaşa desteklediği programlardır. Bu programların amacı, siber savunmada yükseköğrenimi ve bilimsel araştırmaları teşvik ederek çeşitli disiplinlerde siber savunma uzmanlığı ile giderek artan sayıda profesyonel ihtiyacını karşılamak suretiyle, ABD ulusal bilgi güvenliği altyapısının gücünü arttırmaktır [5].

SANS Enstitüsü (SysAdmin, Denetim, Ağ ve Güvenlik Enstitüsü), bilgi güvenliği eğitimi ve güvenlik sertifikasyonunu sağlayan ve binden fazla bilgi güvenliği araştırması içeren kaynağa sahip enstitüdür [5].

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST, National Institute of Standards and Technology), siber güvenlik ile ilgili standardizasyon konulu çalışmalar yürütmektedir.

4.3. Avustralya

Avustralya'da siber güvenliğe ilişkin esas çalışmaları, **İletişim Bakanlığı** (Department of Communications and Arts), Maliye Bakanlığı bünyesinde çalışan **Avustralya Hükümeti Bilgi Yönetimi Ofisi** (AGIMO, Australian Government Information Management Office) ve **Avustralya İletişim ve Medya Kurumu** (ACMA, Australian Communications and Media Authority) yürütmektedir.

Siber Güvenlik Politika ve Koordinasyon Komitesi (Cyber Security Policy and Coordination Committee), Avustralya Hükümeti için siber güvenlik politikasının gelişimini koordine eden Avustralya Hükümeti bölümler arası komitedir [5].

Avustralya Siber Güvenlik Merkezi (ASCC, Australian Centre for Cyber Security), Avustralya Hükümeti'nin siber güvenliği iyileştirme çabalarına öncülük etmektedir. Merkez, dünyadaki siber tehditleri günde 24 saat, haftada yedi gün izlemektedir. Avustralya Sinyaller Direktörlüğü'nün (ASD) bir parçası olarak çalışan kurum, iş, hükümet ve akademik ortakları ile Avustralya'daki ve denizaşırı ülkelerdeki uzmanlarıyla siber güvenlik tehditlerine yönelik çözümler araştırmak ve geliştirmek için çalışmakadır. Güncel siber güvenlik konularında 200'e yakın endüstri, hükümet ve akademik ortakla iş birliği yaparak Ortak Siber Güvenlik Merkezleri'nin (Joint Cyber Security Centres) ulusal bir parçası konumundadır [68].

Avustralya Ulusal Bilgisayar Acil Müdahale Ekibi (CERT Avustralya), Avustralya işletmelerini etkileyen siber güvenlik sorunları için tek temas noktasıdır. CERT Avustralya, Canberra ve Brisbane'de ofisleri bulunan Federal Başsavcılık Bakanlığı'nın (AGD, Federal Attorney-General's Department) bir parçasıdır. CERT Avustralya, ayrıca, Avustralya Güvenlik İstihbarat Teşkilatı (ASIO), Avustralya Federal Polisi (AFP), Avustralya Suçları Komisyonu (ACC) ve Avustralya Sinyaller Direktörlüğü (ASD) ile çalışan ve bilgi paylaşımı yapan Avustralya Siber Güvenlik Merkezi'nin (ACSC) bir parçasıdır [69]. CERT Avustralya, Asya Pasifik Bilgisayar Acil Müdahale Ekibi'nin (bölgedeki 20 ekonomideki 28 takımdan oluşan) yönlendirme komitesine başkanlık etmektedir ve dünyanın dört bir yanındaki diğer müdahale ekipleriyle siber tehdit bilgilerini paylaşmaktadır [70].

Federal Polis Teşkilatı (AFP, Australian Federal Police), siber güvenliğe ilişkin sorumlulukları mevcuttur.

Avustralya Sinyaller Direktörlüğü (ASD, Australian Signals Directorate), Savunma Bakanlığı (DoD) bünyesinde çalışmaktadır. ASD, hükümet genelinde bilgi ve iletişim teknolojileri (BİT) güvenliğinin ulusal makamıdır. ASD, Siber Güvenlik Operasyon Merkezi (CSOC) aracılığıyla, tüm bilgi kaynaklarının izlenmesi ve analizi yoluyla, siber güvenlik tehditlerinin kapsamlı bir ulusal resmini sürdürmekten sorumludur. ASD, Ortak Bilgi Düzenlemeleri (JOA) kapsamında Ulusal Bilgi Altyapısını (NII) korumak için Avustralya Güvenlik İstihbarat Teşkilatı (ASIO, Australian Security Intelligence Organisation) ve AFP ile birlikte çalışır. Buna ACSC, CSOC ve Avustralya Hükümet Bilgi ve İletişim Teknolojileri Güvenlik Kılavuzu (ISM) dahildir [5].

Avustralya Güvenlik İstihbarat Teşkilatı (ASIO, Australian Security Intelligence Organisation), ana rolü, Avustralya'nın ulusal güvenliğini tehlikeye atabilecek faaliyetler veya durumlar hakkında hükümeti uyarmasını sağlayacak bilgi toplamak ve istihbarat üretmektir [5].

Avustralya İnternet Güvenliği Girişimi (AISI, The Australian Internet Security Initiative), Avustralya internet sağlayıcılarının müşterilerini siber güvenlik tehditlerinden korumak için CERT Australia ile gönüllü olarak çalışan bir kamu-özel ortaklığı olarak faaliyet göstermektedir [71].

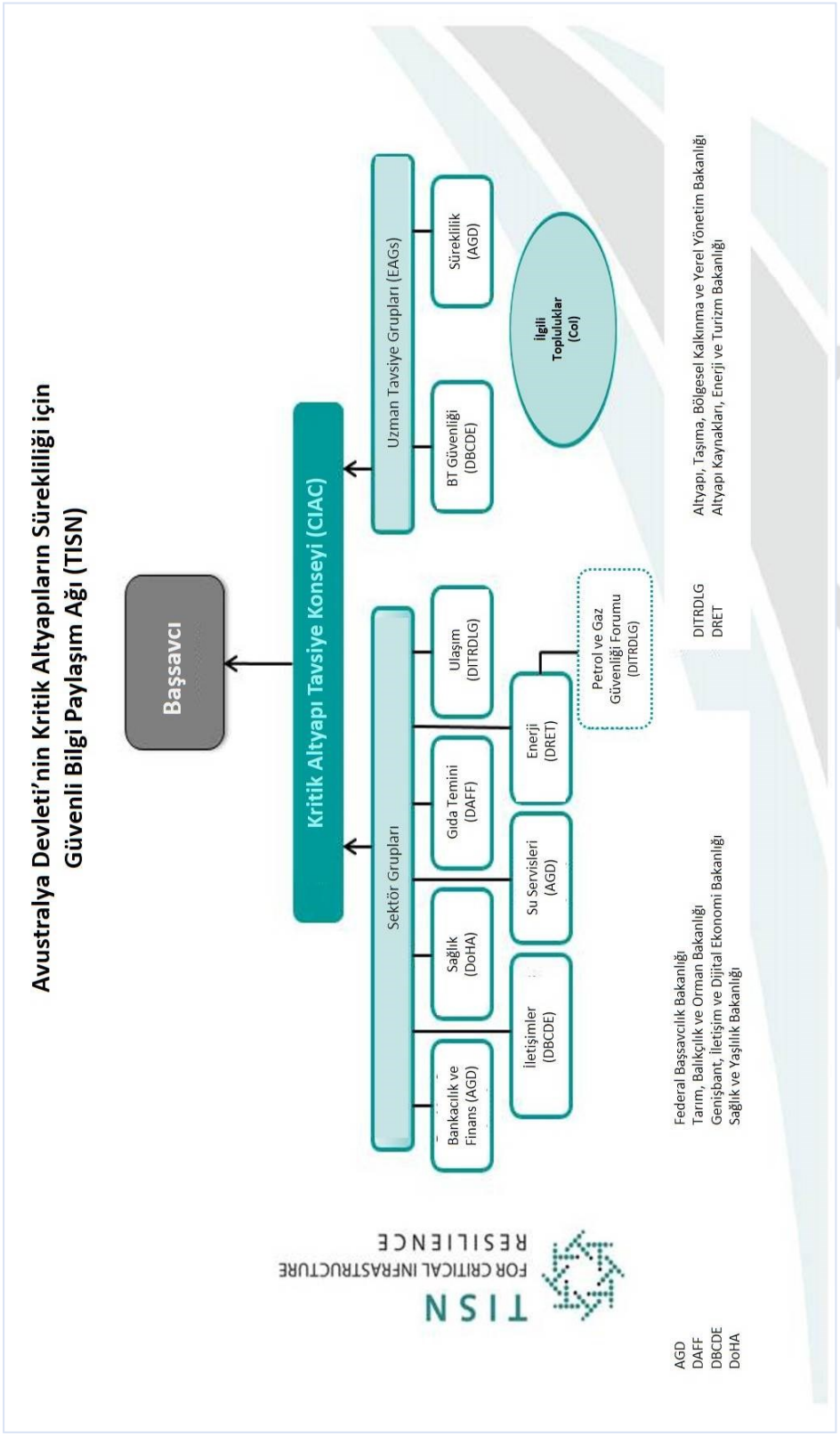
Avustralya'nın siber güvenlik strateji belgesinde üç temel amaç ve bu amaçlara ulaşabilmek adına atılması gereken adımlar 2011 yılı itibariyle detaylı bir biçimde sunulmuştur. Bu üç temel amaç şu şekildedir; (1)Bütün Avustralyalıların siber risklerin farkında olan, bilgisayar, kişisel bilgi ve finansal işlemlerini güvenli bir biçimde yapıp kendilerini koruyabilen vatandaşlar olması, (2)Avustralya işletmelerinin müşterilerinin kimlik bilgilerinin gizliliğini koruyan güvenli bilgi sistemlerine sahip olması ve (3)Avustralya Hükümeti kamunun kullandığı bilgi sistemlerinin güvenliğini ve gizliliğini sağlar [72].

Avustralya Hükümeti'nin son siber güvenlik stratejisi, Avustralya'nın 2020 hedeflerine yönelik siber güvenliğini sağlamak amacıyla beş eylem planından oluşmaktadır. Bunlar; (1)Ulusal bir siber ortaklığı, (2)Güçlü siber savunma, (3)Küresel sorumluluk ve etki, (4)Büyüme ve yenilik, (5)Siber zeki bir millet [70].

Federal Başsavcılık Bakanlığı (AGD, Federeal Attorney-General's Department), Avustralya yasa ve adalet çerçevesini korumak ve geliştirmek, ulusal güvenliğini ve acil durum yönetimini güçlendirmek için programlar ve politikalar geliştirir. CERT Avustralya, AGD bünyesinde yer almaktadır [5].

Kritik Altyapıların Korunması için Güvenilir Bilgi Paylaşım Ağı (TISN, Trusted Information Sharing Network for Critical Infrastructure Protection), 2003 yılında Avustralya Hükümeti tarafından kurulmuştur. Avustralya'nın, kurumsal bilgi paylaşımı altyapısının ve kritik altyapılarının korunması konusunda süreklilik oluşturulması için birincil ulusal mekanizmadır. TISN, sekiz sektör grubundaki kritik altyapı sahipleri ve operatörler için düzenli olarak bilgi paylaşımı yapmak ve güvenlik, iş sürekliliği zorluklarını ele almak için

sektörler arasında iş birliği yapmak üzere güvenli bir ortam sağlamaktadır [73]. Avustralya kritik altyapılarının korunmasını amaçlayan organizasyon yapısı Şekil 4.4'te olduğu gibidir.



Şekil 4.4. Avustralya kritik altyapıların korunması organizasyonu [73]

Kritik Altyapı Koruma Modelleme ve Analiz Programı (CIPMA, Critical Infrastructure Protection Modelling and Analysis Programme), Avustralya Hükümeti'nin Avustralya'nın kritik altyapılarını korumasına yönelik çabalarında önemli bir girişimdir. CIPMA, kritik altyapı sistemlerinin davranış ve bağımlılık ilişkilerini modellemek ve simüle etmek için bir dizi kaynaktan (kritik altyapının sahipleri ve operatörleri dahil) çok çeşitli veri ve bilgileri kullanan bilgisayar tabanlı bir uygulamadır. AGD, CIPMA Programını yönetmektedir ve yeteneklerini geliştirmek için Geoscience Australia (GA) ile yakın çalışmaktadır [74]. TISN, CIPMA programını ve üyelerini desteklemektedir.

2015 yılında yayımlanan Kritik Altyapıların Sürekliliği Strateji Planı'nda (Critical Infrastructure Resilience strategy: PLAN) [75] Fedaral Başsavcılık Bakanlığı'na bağlı olarak görev yapan Kritik Altyapılar Tavsiye Kurulu'nun (CIAC, Critical Infrastructure Advisory Council) yönetiminde kritik altyapıların endüstri ve kamu temsilcilerinin birlikte çalıştığı ifade edilmiştir. Ayrıca ilgili belgede 4 temel amaç vurgulanarak belirlenen kritik altyapı sektörleriyle ilişkilendirilen kamu kuruluşlarının sorumluluklarına yer verilmiştir.

CSIRO Data61, hızla gelişen bir siber güvenlik ekosisteminin ön saflarında yer alan bir gruptur ve siber güvenlik kümelenmelerine bir örnek olarak gösterilebilir. Hem Avustralya'nın en büyük veri odaklı araştırma ve inovasyon organizasyonu hem de dünyanın en önde gelen BT gruplarından biridir [70]. Akademi, hükümet ve sanayiyi bir araya getiren bir ağ olarak çalışarak Avustralya'nın rekabetçi siber güvenlik endüstrisinin genişletilmesi amaçlanmaktadır [76].

Çok sayıda Avustralya şirketi, yüksek katma değerli siber güvenlik ürünleri ve hizmetleri geliştirmeye odaklanmıştır. Bu şirketler yenilikçi girişimlerden çok uluslu organizasyonlara kadar geniş bir yelpazeye sahiptir ve kimlik yönetimi, şifreleme, kablosuz teknolojiler ve güvenilir sistemler konusunda uzmanlığa sahiptirler. Birçoğu hükümet kurumları ve akademik sektör ile iş birliği yapmaktadır [70].

Avustralya İletişim ve Sanat Bakanı, tüm Avustralyalıları siber zorbalığı azaltmak için akıllı, güvenli ve sorumlu olmaya teşvik eden Ulusal eSmart Haftası'nın başladığını duyurarak siber güvenliğe ilişkin toplumsal farkındalık çalışmalarına örnek teşkil eden bir uygulamanın yürütrlüğe girmesini sağlamıştır [77]. Oluşturulan internet sitesi vasıtasıyla toplumsal farkındalığı arttırmak amaçlanmaktadır. Bahsi geçen internet sitesinde, internet ortamında

yaygın olarak kullanılan uygulama ve platformlar için temel güvenlik önlemlerinin nasıl alınabileceğine ilşkin makaleler yer almaktadır [78].

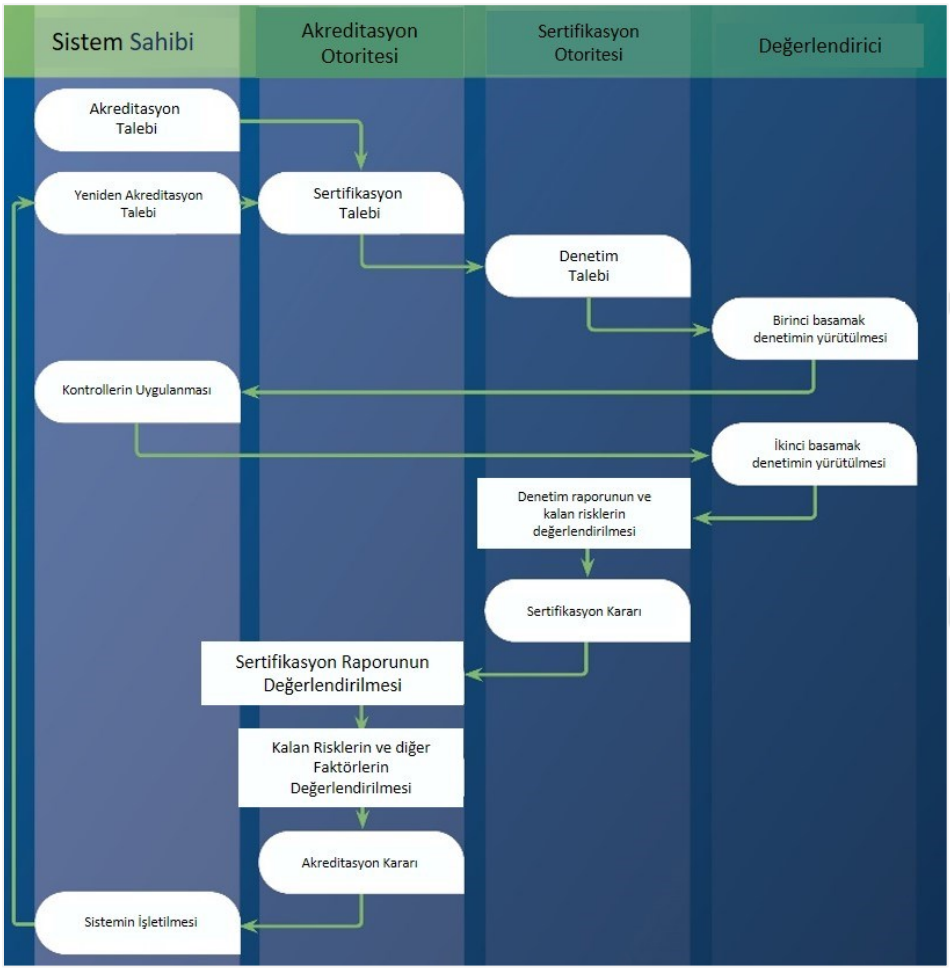
Avustralya Siber Güvenlik Merkezi (ACSC, Australia Cyber Security Center), New South Wales Üniversitesi'nin (The University of New South Wales) Sydney ve Canberra kampüslerinden uzmanları bir araya getiren ve Savunma Bakanlığı tarafından desteklenen disiplinler arası bir siber güvenlik merkezidir [5]. Ek olarak Savunma Bakanlığı, Avustralya Ulusal Üniversitesi (ANU) ile yaptığı bir iş birliği ile yüksek performanslı bilgi işlem, veri analizi ve siber güvenlik gibi alanlarda araştırma yapılmasına olanak sağlayacak yatırım projeleri hayata geçirmektedir [70].

Avustralya New Castle Üniversitesi'nde (The University of New Castle) bulunan Gelişmiş Siber Güvenlik Araştırma Merkezi (ACSRC, Advanced Cyber Security Engineering Research Centre), güvenli ve güvenilir bilgi işlem sistemleri ve hizmetleri sağlayan model ve tekniklerin teorisi, tasarımı ve yönetimi konusunda siber güvenlikte ilerlemeler sağlamayı amaçlamaktadır. ACSRC'nin önemli bir özelliği, dağınık sistemler, kablosuz, geniş bant ve uçtan uca ağlar, mobil cihazlar ve dağıtılmış bilgi hizmetlerini içeren heterojen mobil dağıtılmış ağ ortamında ortaya çıkan güvenlik sorunlarını ele alma konusundaki araştırma yeteneklerine ve uzmanlığa sahip olmasıdır [70].

Avustralya siber güvenlik eğitimi ve eğitimi sağlayıcıları, yükseköğretim sektörünü, mesleki sektörü ve özel sağlayıcıları kapsamaktadır. Birçok Avustralya üniversitesi, küresel yükseköğretim endekslerinin ilk 100'ünde yer almakta ve öğretim ve araştırma mükemmelliği ile tanınmaktadır. Teknik kurslardan siber güvenliğin çevresel yönlerine kadar geniş bir yelpazede kurs ve araştırma dereceleri vardır. Canberra Üniversitesi'nde İnternet Güvenliği Merkezi, siber suçun sosyal, yasal, politik ve ekonomik etkileri ve siber güvenliğe yönelik tehditler hakkında düşünce liderliği ve politika tavsiyesi sağlayarak daha güvenli ve daha güvenilir bir internet oluşturmak için oluşturulmuştur. New South Wales Üniversitesi'nde (The University of New South Wales) bulunan siber güvenlik merkezi ise disiplinler arası bir araştırma ve öğretim merkezi niteliğindedir [70].

Bilgi Güvenliği Kayıtlı Değerlendiriciler Programı (IRAP, Informatıon Securıty Registered Assessors Program), hükümete yüksek kaliteli bilgi ve iletişim teknolojisi ve güvenlik değerlendirme hizmetleri sağlamak için çalışan bir ASD girişimidir. ASD, daha geniş endüstri ve Avustralya Hükümeti sistemlerini güvence altına almak için ilgili güvenlik

hizmetlerine uygun nitelikli BİT profesyonellerini onaylar. IRAP Denetleyicileri, güvenlik uyumluluğunuzu değerlendirerek ve kuruluşunuzun karşılaştığı bilgi güvenliği risklerini vurgulayarak BİT ağlarınızı güvenceye almaya yardımcı olur [79]. IRAP akreditasyon süreci Şekil 4.5'te olduğu gibidir.



Şekil 4.5. IRAP akreditasyon süreci [79]

4.4. Birleşik Krallık

Birleşik Krallık, siber güvenliğe ilişkin ihtiyaçların karşılanması amacıyla temelde üç kurumun çalışmalarıyla yol almaktadır. Bu kuruluşlar, strateji ve politikaların geliştirilmesi, kamu kurumlarında politikaların uygulanması, özel sektörde politikaların uygulanması olarak 3 ayrı konu başlığına göre çalışma yürütmektedirler. Bilgi Güvencesi Merkez Sponsoru (CSIA, Central Sponsor for Information Assurance), siber savunma konusunda politika, strateji ve siyasal geliştirme çalışmalarını yürütmektedir. Ulusal Bilgi Güvencesi Teknik Otoritesi (CESG, National Technical Authority for Information Assurance) kamu kuruluşlarının, Ulusal Altyapının Korunması Merkezi (CPNI, Centre for the Protection of

National Infrastructure) ise özel kuruluşların siber güvenlik gereksinimlerine yönelik çalışmalar yapmaktadır [65]. Öte yandan, siber güvenlik strateji belgelerini Siber ve Hükümet Güvenlik Müdürlüğü (Cyber and Government Security Directorate) yayımlamaktadır.

Siber Güvenlik ve Bilgi Güvencesi Ofisi (OCSIA, Office of Cyber Security & Information Assurance), siber uzayla ilgili öncelikleri belirlemede Kabine Dairesi ve Ulusal Güvenlik Konseyi bakanını desteklemektedir. OCSIA, stratejik yönlendirme sağlar ve hükümet için siber güvenlik programını koordine eder, İngiltere'de siber güvenlik ve bilgi güvencesini artırır. Ulusal Siber Güvenlik Programını (NCSP) koordine eder [5]. Birimin diğer görevleri şunlardır; destekleyici eğitim, farkındalık, eğitim ve öğretim; bilgi alışverişinde ve en iyi uygulamaları teşvik etmede özel sektör ortakları ile çalışmak; İngiltere'nin bilgilerini ve siber güvenlik teknik kapasitesini ve operasyonel mimarisini geliştirmek ve sürdürmek; Hükümet BİT altyapılarının esnekliğini ve güvenliğini sağlamak için Hükümet Baş Bilgi Yetkilisi Ofisi (OGCIO) ile birlikte çalışmak ve siber uzayın güvenliğini ve bilgi güvenliği seviyesini arttırmak için uluslararası ortaklarla ilişki kurmak.

OCSIA, İçişleri Bakanlığı, Savunma Bakanlığı (MOD), Hükümet İletişim Genel Müdürlüğü (GCHQ), CESG, CPNI, Yabanci & Sivil Toplum Bürosu (FCO) ve İş, İnovasyon ve Beceriler Bölümü (BIS) gibi diğer lider devlet daireleri ve kurumlarıyla birlikte çalışmaktadır [80].

Devlet Güvenlik Sekretaryası (Government Security Secretariat), hükümet genelinde stratejik öneme sahip güvenlik ve istihbarat konularında koordinasyon sağlar [5].

Ulusal Siber Güvenlik Merkezi (National Cyber Security Centre), Birleşik Krallık Hükümeti'ne, Akademik Mükemmeliyet Merkezleri (CAE) programı dahil olmak üzere, endüstri ve akademi ile iş birliği içinde iletişim ve elektronik verilerin güvenliği konusunda tavsiye ve rehberlik sağlar. Ayrıca İngiltere Ulusal Bilgisayar Acil Durum Müdahale Ekibi'ne (CERT-UK) ev sahipliği yapmaktadır [5].

Siber Güvenlik Operasyon Merkezi (CSOC, Cyber Security Operation Center), siber olayları izlemek ve koordine etmek, işletmelerle paylaşmak ve Birleşik Krallık ağlarına ve kullanıcılarına yönelik saldırılara dair kamuya açık bilgiler ve tavsiyeler vermek üzere

oluşturulmuştur. Merkez, temsilcilerden oluşan çok ajanslı bir kurumdur. Hükümet, kilit paydaşlar ve bölümler arası bir gözetim kuruluna rapor verir [80].

Güvenlik Servisi (MI5, Security Service), diğer İngiltere istihbarat teşkilatlarıyla birlikte, hükümet departmanları ve endüstri sektörünün bütününü ele alacak şekilde siber tehditlerle mücadele etmek amacıyla çalışır [5].

Savunma Bakanlığı (Ministry of Defence), İngiltere'nin güvenliğini, bağımsızlığını ve çıkarlarını yurtiçinde ve yurtdışında korur [5]. Siber güvenliğe ilişkin sorumlulukları mevcuttur.

İngiltere'nin 2015'te yayımladığı Ulusal Güvenlik Strateji Belgesi, önümüzdeki yıllara ilişkin karşılaşılabilecek dört muhtemel zorluğa işaret etmektedir. İlgili belgede teknolojinin, özellikle siber tehditlerin etkisi ve geniş teknolojik gelişmelerin bu dört zorluktan biri olduğu ifade edilmektedir. Dolayısıyla siber ataklar bu strateji belgesinde üst seviye ulusal güvenlik tehlikesi olarak görülmektedir.

2015 Ulusal Güvenlik Risk Değerlendirme Belgesi'nde ise siber tehditler; terörizm, uluslararası askeri çatışmalar, toplum sağlığı, büyük doğal felaketler gibi birinci seviye risklerle aynı katmanda yer almıştır.

Siber Politika, Yabancı ve Milletler Topluluğu Ofisi Başkanı, Paula Walsh'ın ifade ettiğine göre; Birleşik Krallık Ulusal Siber Güvenlik Strateji Belgesi 2016-202'de (The UK's National Cyber Security Strategy 2016-2021) vizyon olarak "siber tehditlere karşı güvenli ve dirençli, dijital dünyada başarılı ve emin" belirlenmiştir. Strateji belgesine göre kamunun neredeyse her organı stratejinin gerçekleşmesi için en az bir role sahiptir.

Ulusal Altyapının Korunması Merkezi (CPNI, The Centre for the Protection of National Infrastructure), 2007 yılında oluşturulmuştur. Birleşik Krallık'taki kamu-özel ortaklık çabalarını, devletin kritik altyapılarının çoğuna sahip kilit sektörler ve şirketler ağı ile doğrudan çalışan merkezi hükümet organı olarak kolaylaştırmaktadır. CPNI, fiziki güvenlik, personel güvenliği ve siber güvenlik/bilgi güvencesi ile ilgili güvenlik tavsiyeleri sunmaktadır. Siber uzay kaynaklı tehditler dahil olmak üzere terörizm ve casusluk gibi diğer tehditlere karşı ulusal altyapının savunmasızlığını azaltmayı amaçlamaktadır [80].

Siber Güvenlik Araştırmaları Akademik Mükemmeliyet Merkezleri (ACE-CSRs, Academic Centres of Excellence in Cyber Security Research), İş, İnovasyon ve Beceriler Bakanlığı (BIS), CPNI, GCHQ, OCSIA ve İngiltere Araştırma Konseyleri (RCUK) tarafından desteklenmektedir. Mevcut durumda merkeze, on üç üniversite dahil edilmiştir [5].

İngiliz Standartları Enstitüsü (BSI, British Standards Institution) özellikle ISO/IEC'de temsil edilen, İngiltere'nin başlıca standart geliştirme kuruluşlarından biridir [5].

Birlikte Çalışabilirlik Standartları (NICC®-UK, UK Interoperability Stnadards,), Birleşik Krallık iletişim sektörü için Birleşik Krallık'taki kamu iletişim ağları ve hizmetleri için birlikte çalışabilirlik standartlarını geliştiren bir teknik forumdur [5].

4.5. Çin Halk Cumhuriyeti

Sanayi ve Bilgi Teknolojileri Bakanlığı (MIIT, Ministry of Industry and Information Technology), posta servisi, internet, telsiz, yayın, iletişim, elektronik ve bilgi ürünleri üretimi, yazılım endüstrisi ve ulusal bilgi ekonomisinin teşvik edilmesinden sorumludur. MIIT ve çeşitli organları Çin'i siber güvenliğe ilişkin uluslararası faaliyetlerde temsil etmektedir [5]. ABD'de İç Güvenlik Bakanlığı'na benzer yerel sorumluluklar taşır. Bakanlık, ayrıca standartları belirler, tatbikatlar yapar, ağ güvenliğini denetler ve özel bir departman aracılığıyla bilgi ve telekom güvenliğini koordine eder. MIIT ayrıca, ulusal savunma için bilim, teknoloji ve endüstri ile ilgili kurallar, politikalar, yasalar ve yönetmelik taslaklarını hazırlayan Ulusal Savunma Bilim, Teknoloji ve Endüstri için Devlet Yönetimi'ni (SASTIND) de bünyesinde barındırmaktadır [81].

Çin Siber Uzay Yönetimi veya Siber Uzay İşleri Merkez Lider Ofisi (CAC, Cyberspace Administration of China or Office of the Central Leading Group for Cyberspace Affairs), İnternet Güvenlik Acil Komuta Merkezi, Ajans Servis Merkezi ve tehdit bilgi raporlama merkezini barındırır [5].

Politbüro Daimi Komitesi, Danıştay ve Merkez Askeri Komisyonu, Çin'deki en üst düzey karar alıcı konumundadır. Politika oluşturmada, 2006'da 15 Yıllık Plan ve 2012'de Yeni Politika Görüşü gibi siber uzayda olanlar da dahil olmak üzere, genellikle yeni girişimleri benimseyen Devlet Konseyi görevlidir, ancak politikanın yürütülmesiyle görevli birçok farklı devlet kurumu vardır [81].

Ulusal Bilgisayar Ağı Acil Durum Müdahale Teknik Ekibi/Koordinasyon Merkezi (CNCERT/CC, National Computer Network Emergency Response Technical Team/Coordination Center), Çin'in siber güvenlik acil durum müdahale topluluğu için koordinasyon ekibidir. CNCERT, Çin'in siber güvenlik duruşunu iyileştirmek ve kritik altyapı siber güvenliğini korumak için çabalamaktadır. CNCERT siber güvenlik tehditlerini ve olayları önlemek, tespit etmek, uyarmak ve koordine etmek için çaba göstermektedir [5]. MIIT Siber saldırılara yanıt vermenin birincil görevi Ulusal Bilgisayar Ağı Acil Durum Müdahale Teknik Ekibi/Koordinasyon Merkezi'ne aittir [81].

Çin Ordusu, siber güvenliğe ilişkin konuların takibi ve denetiminde söz sahibi konumdadır. Ordunun çalışmalarını siber güvenlik alanında çalışmalar yapan ve ülke üniversitelerinden destek alan enstitüler desteklemektedir [65].

Kamu Güvenliği Bakanlığı (MPS, The Ministry of Public Security), siber suçları araştırmaktadır ve geniş bir araştırma ağı kullanarak geliştirme çalışmaları ile birlikte kritik altyapı korumasını birlikte ele almaktadır. Ayrıca hükümet tarafından kullanılan ticari ürünlerin denetlenmesinden ve tüm ticari bilgi güvenliği şirketlerinin kontrolünden de sorumludur. Önemli olarak, Çin Büyük Güvenlik Duvarı'nı işletir ve ayrıca iç istihbaratın yürütülmesi konusuyla ilgilenir [81].

Devlet Güvenlik Bakanlığı (MSS, The Ministry of State Security) istihbarat, karşı istihbarat, yabancı istihbarat sağlama işlerini yürüten bir organ olarak çalışmaktadır. Amaçları arasında Komünist Partinin üç varoluşsal mücadelesi olarak tanımlanan ayrılıkçılık, terörizm ve dinsel aşırılığa karşı durmaya konularına odaklanmak vardır. Kamuoyunun dikkatini çekmemiş olmasına rağmen, MSS, yabancı hükümetler, sivil toplum örgütleri ve yerel muhalifler hakkında siber yeteneklerin tespitine ilişkin, politik ve ekonomik veri toplama amaçlı çalışmalarını önemli ölçüde arttırmıştır [81].

Şubat 2006'dan bu yana, tüm bilgi güvenliği gelişmeleri ve ilgili politikalar "Orta ve Uzun Vadeli 2006-2020, Bilim ve Teknoloji Ulusal Programı " ına dayanmaktadır. Strateji, sadece Çin teknolojik hedeflerinden ve siber uzaydan bahsetmekle kalmayıp yaşam kalitesi ve gelir düzeyini yükseltme hedefiyle, teknolojinin daha geniş bir bağlamda analiz edilmesi gerektiğini vurgulamaktadır [81].

Çin İnternet Topluluğu (ISC), yasal şirketler, araştırma enstitüleri, akademik dernekler, üniversiteler ve internet ile ilgili çeşitli faaliyetlerde bulunan diğer kuruluşlardan oluşan 400'den fazla üyeye sahiptir. ISC'nin ana görevi, Çin'de internetin gelişimini teşvik etmek ve gelişmiş bir bilgi toplumu inşa etmek için çaba sarfetmektir [5].

Çin Mühendislik Akademisi ve Çin Bilimler Akademisi (Chinese Academy of Engineering, and the Chinese Academy of Sciences) altında doğrudan faaliyet gösteren Çin Çağdaş Enternasyonal İlişkiler Enstitüsü (Chinese Institute of Contemporary International Relations) gibi bir dizi hükümet bağlantılı araştırma kurumu önemli konumdadır. Çin'in en önemli iki akademik kurumu olan Tsinghua Üniversitesi ve Pekin Üniversitesi, hükümetin bilgi teknolojisi ile ilgili araştırma çalışmaları ile yakından ilgilidir. Daha derin stratejik kalkınma, Askeri Bilimler Akademisi ve PLA Bilgi Mühendisliği Üniversitesi gibi kurumlar aracılığıyla PLA tarafından yürütülmektedir [81].

Çin Bilgi ve İletişim Teknolojileri Akademisi (CAICT), daha önce Çin Telekomünikasyon Araştırmaları Akademisi (CATR) olarak bilinen, çok çeşitli güvenlik standartlarından ve tekniklerin geliştirilmesinden sorumludur [5].

Belgelendirme, sertifikasyon ve standardizasyon çalışmalarında Çin'de çeşitli kurum ve kuruluşlar görev yapmaktadır. Bunlar arasında; Çin İletişim Standartları Derneği (CCSA, China Communications Standards Association), bulut güvenliği için güvenlik yönergelerini içeren güvenlik standartları geliştirmesinden sorumlu Ulusal Bilgi Güvenliği Standardizasyon Teknik Komitesi (TC260, National Information Security Standardization Technical Committee), ISO ve IEC standardizasyon çalışmasının yönetimi ve koordinasyonu ile ilgili sorumlulukları olan Çin Standardizasyon İdaresi (SAC, Standardization Administration of China) yer almaktadır [5].

Çin Elektronik Standardizasyon Enstitüsü (CESI, China Electronics Standardization Institute), MIIT bünyesinde elektronik ve bilişim sektöründe standartlaşma amacıyla görev yapan profesyonel bir enstitüdür. CESI'nin temel işi, elektronik ve bilgi teknolojisi alanında standartlaşma çalışmalarını yürütmektir. Test, ölçüm, sertifikasyon, bilgi servisi ve standartlar için bilimsel araştırmalar geliştirerek hükümetin stratejik çalışmalarında, endüstri yönetiminde ve stratejik kararlar verebilmesinde profesyonel destek sağlar. Ek olarak standardizasyon alanında topluma teknik servis sağlar [5].

4.6. Finlandiya

Fin İletişim Düzenleme Kurumu (FICORA, Finnish Communications Regulatory Authority), Ulusal Siber Güvenlik Merkezi Finlandiya (NCSC-FI) bünyesinde çalışmaktadır [5].

Güvenlik Komitesi (The Securıty Committee), Savunma Bakanlığı bünyesinde çalışmaktadır ve ayda bir kez toplanmaktadır. Çeşitli örgütler, iş çevreleri ve diğer iş birliği ortakları ile seminerler ve kamu tartışmaları düzenleyerek, toplumdaki güvenliğin geliştirilmesi için ihtiyaç duyulan bilgileri tartışmayı ve toplamayı amaçlamaktadır. Güvenlik Komitesi, çoğunlukla sorumlu bakanlık veya başka bir üyenin talebi üzerine kapsamlı güvenlikle ilgili konularda öneriler hazırlar. Fin Siber Güvenlik Stratejisi, Komitenin rehberliğinde tamamlanan çalışmanın iyi bir örneğidir. Program, 2014 yılında Komite tarafından yayımlanmıştır [82].

Finlandiya'nın siber güvenlik strateji belgesinde tamamen vizyonu ortaya koyan bileşenler listelenmiştir. 2016 yılı itibariyle ülkenin siber güvenlik konusunda saldırılara karşı koyabilecek ve saldırıları yönetebilecek yapısı vurgulanmıştır. Ülkenin savunma kapasitesi, uluslararası etkinlikler, kamusal işlerin yönetimi ve denetimi, kriz ve saldırı yönetiminin psikolojik boyutları, altyapı çalışmaları ve iç güvenlik ana başlıklarında Finlandiya'nın siber güvenlik stratejisi vizyonu detaylandırılmıştır [72].

Maliye Bakanlığı, devletin bilgi güvenliğinin yönlendirilmesinden ve geliştirilmesinden sorumludur. Hükümet, merkezi hükümetin bilgi güvenliğini artırma konusundaki kararında, yönetim, yetkinlik, risk yönetimi ve idari gelişimin önemli bir parçası olarak bilgi güvenliğini geliştirmeye yöneliktir. Merkezi hükümette, bilgi güvenliği için ortak başlangıç noktaları, kendi operasyonlarının bilgi güvenliği için her bir kuruluşun sorumluluğunu, yönetmeliklerin öngördüğü bilgi güvenliği yükümlülüklerini, Hükümet'in merkezi bilgi güvenliğini artırma konusundaki kararını, Finlandiya'nın Siber Güvenlik Stratejisini; Maliye Bakanlığı tarafından yayımlanan VAHTI bilgi güvenliği talimatları ve diğer politika tanımları belirlemektedir [83]. VAHTI, Devlet Bilgi Güvenliği Yönetim Kurulu (Government Information Security Management Board), tarafından belirlenen bilgi güvenlik talimatları, dünyadaki en kapsamlı bilgi güvenliği talimatlarından biridir. Kamu yönetimine ek olarak, VAHTI uluslararası bilgi güvenliği talimatları işletmeler, topluluklar ile eğitim ve sivil faaliyetler arasında yaygın olarak kullanılmaktadır [84].

Ulusal Siber Güvenlik Merkezi (NCSC-FI), uyarılar, bilgi güvenliği makaleleri ve güvenlik açığı raporları yayımlamaktadır [5].

Finlandiya, Danimarka, İzlanda, Norveç ve İsveç; Nordik Ulusal CERT İş Birliği ile birlikte çalışmalar yürütmektedir. Bu çalışmalar, siber güvenliği güçlendirmek, olay müdahale süreçlerini araştırmak ve bölgedeki bilgi paylaşımını geliştirmek için teknik iş birliği ve siber güvenlik uygulamalarını içerir [62].

Finlandiya Toplum için Güvenlik Stratejisi, 2017 yılında yayımlanmıştır. Bu strateji, ulusal hazırlık ilkelerini uyumlu hale getiren ve hazırlıkları çeşitli idari dallarda yönlendiren bir hükümet kararıdır [85]. Ek olarak Finlandiya Güvenlik Komitesi, siber güvenlik stratejisinin 2017-2020 yılları arasında uygulanmasına yönelik olarak kuruluşların görev dağılımının yer aldığı bir strateji belgesi de yayımlamıştır [86].

Jyväskylä Güvenlik Teknolojisi (JYVSECTEC), Finlandiya'da lider bağımsız siber güvenlik araştırma, geliştirme ve eğitim merkezidir. JAMK Uygulamalı Bilimler Üniversitesi Bilgi Teknolojileri Enstitüsü'nün bir parçası olarak hizmet vermektedir [87]**.**

4.7. Fransa

Ulusal Bilgi Sistemleri Güvenliği Ajansı (ANSSI, Agence Nationale de la Sécurité des Systèmes d'Information), devlet bilgi sistemlerinin korunmasına yönelik kurallar önermek ve kabul edilen önlemlerin uygulanmasını doğrulamaktan sorumludur. Savunma, bilişim sistemleri alanında, devlet ağları dahil olmak üzere siber saldırıları izlemek, tespit etmek, önelm almak ve karşılık vermek için çalışmalar yürütür [5].

Fransa CERT, bilgisayar saldırılarına karşı izleme, uyarı ve yanıt verme konularında başlıca hükümet merkezidir. ANSSI ve Savunma ve Ulusal Güvenlik Genel Sekreterliği (SGDSN) tarafından işletilmektedir.

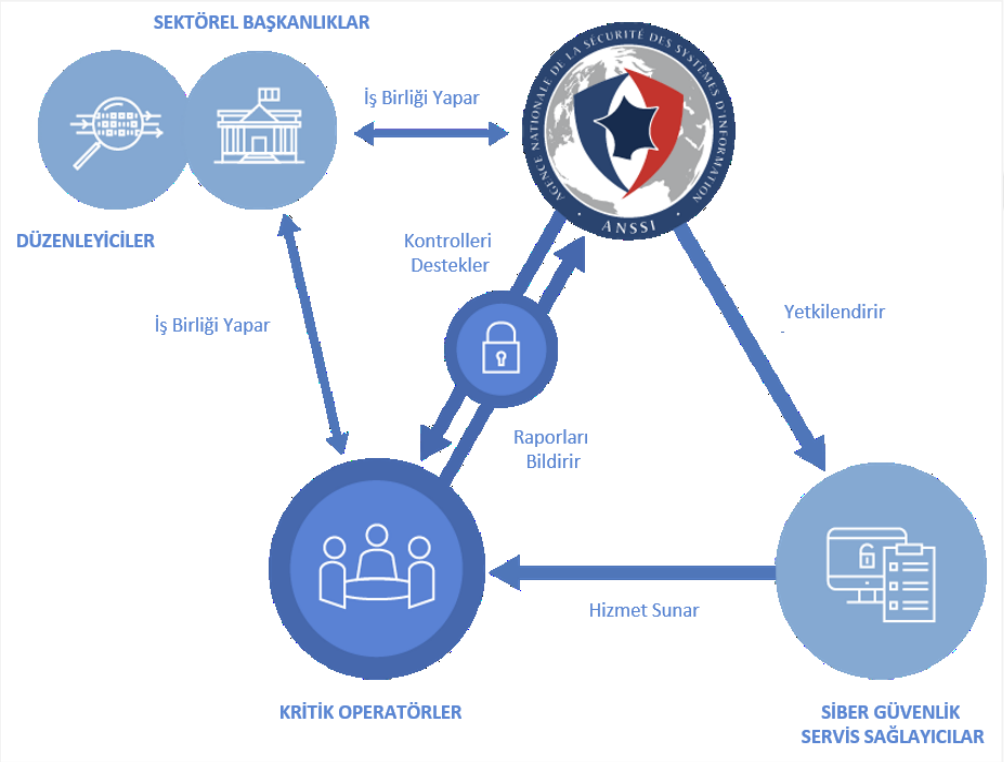
Savunma ve Ulusal Güvenlik Genel Sekreterliği (SGDSN, Secrétariat Général de la Défense et de la Sécurité Nationale) tehditlere karşı siber savunmayı sağlamaktadır [5].

Fransa'nın siber güvenlik stratejisinde dört ana amaç ve yedi eylem maddesi dikkat çekmektedir. Bu dört ana amaç şu şekildedir: (1)Siber savunmada bir dünya gücü haline gelme, (2)Fransa'nın kendi egemenliğine ilişkin bilgilerin korunması hususunda alacağı

kararlar, (3)Kritik altyapı bilgi sistemlerinin güçlendirilmesi ve (4)Siber güvenliğin sağlanması [72].

Fransa'nın 2012'de yayımladığı Stratejik Ufuklar raporunda siber uzayın potansiyel bir çatışma alanı yaratacağı, bilgi ve iletişim teknolojilerine bağımlılığın siber saldırılara alan açacağı ve siber saldırıların oranlarında artış yaşanacağına vurgu yapılmıştır. Siber teknolojilerin küçük ülkelerin büyük ülkelere bağımlılığını arttıracağı belirtilmiştir.

Fransız menfaatlerine karşı siber saldırıların artan sayısını ve karmaşıklığını kabul eden Fransa, 2008 yılında kritik altyapıların veya "Kritik Altyapılar Bilgi Koruması" nın (CIIP) siber güvenliğini pekiştirme ihtiyacını stratejik bir öncelik olarak kabul etmiştir. 2013 yılında, özel bir CIIP yasası çıkarılmıştır [88]. Şekil 4.6'da Fransa'nın kritik altyapı bilgi kaynaklarının korunmasında kurulan irtibatlar kısaca anlatılmaktadır.



Şekil 4.6. Fransa'da kritik altyapılara ait bilginin korunması süreci [88]

Fransız Standardizasyon Birliği (AFNOR, Association Française de Normalisation), Fransa'nın ana standart geliştirme kuruluşlarından biridir, özellikle ISO/IEC konusunda çalışmalar yürütmektedir [5].

4.8. Güney Kore

Güney Kore siber güvenlik yapılanmasında; cumhurbaşkanı ve kendisine direkt bağlı olarak çalışan, başkanlığını Güney Kore Ulusal İstihbarat Servisi başkanının yaptığı güvenlik strateji konseyi yer almaktadır. Cumhurbaşkanının liderliğinde geliştirilen siber güvenlik politikalarının konsey tarafından takip edilerek kuruluşların bu politikaları uygulaması sağlanmaktadır. Siber güvenlik politikalarının devletin en üst yönetim birimleri tarafından belirlenmesi ve takibi, bu konuya verilen önemin açık bir göstergesidir [65].

Kamu Yönetimi ve Güvenliği Bakanlığı (MOPAS, Ministry of Public Administration and Security), bilgisayar korsanlığı ve diğer siber saldırılara karşı etkin bir şekilde yanıt veren güvenilir kişisel bilgi güvenliği sistemi ile siber uzayda güvenliği sağlamayı amaçlamaktadır. Kaliteli bilgi toplumunun oluşturulması için, MOPAS, bilgi etiği ve bilgi kültürü üzerine çeşitli eğitim programları ve kampanyalar yürütmektedir [89].

Ulusal Bilgi İşlem ve Bilgi Ajansı (NCIA, National Computing and Information Agency) Kamu bilgi kaynaklarını arttırılmış güvenlik ve azalan hata süresi ile entegre etmek ve paylaşmak için kurulmuştur [89].

Hali hazırdaki BİT ile ilgili hükümet yapısına (hükümet yeniden yapılanması; 26 Temmuz 2017) bakıldığında, Bilim ve Bilişim Bakanlığı (Ministry of Science and ICT) BİT, radyo ve yayıncılıktan sorumlu iken Kore İletişim Komisyonu (KCC) yayın ve iletişimi düzenlemek ve kullanıcıları korumaktan sorumludur. İçişleri ve Güvenlik Bakanlığı (MOIS), e-Devlet ve kişisel bilgilerin korunmasından sorumludur. Kültür, Spor ve Turizm Bakanlığı (MCST) oyunlardan, video içeriklerinden vb. sorumludur. Ticaret, Sanayi ve Enerji Bakanlığı (MOTIE), yarı iletkenler ve ekran panelleri de dahil olmak üzere gömülü SW, e-öğrenme ve ICT bileşenli endüstrilerden sorumludur [90].

Ulusal Siber Güvenlik Merkezi (NCSC), siber olaylara ilişkin koordinasyon ve yönetim işlemlerini yürütür. Kore Bilgisayar Acil Müdahale Ekibi (KN-CERT), NCSC'nin bir bölümü olarak görev yapmaktadır [91].

Ulusal İstiharat Servisi (NIS), ulusal düzeyde kapsamlı ve sistematik siber güvenlik için, politikaların yürütülmesini formüle ederek, koordine ederek ve gerekli şemaları ile kılavuzları hazırlayarak siber güvenliğe ilişkin politikayı denetler [92].

Kore Ticaret-Yatırım Teşvik Ajansı (KOTRA, South Korea Trade Centre), uluslararası ticareti ve yatırımı teşvik etmek amacıyla kurulan, Kore Cumhuriyeti'nin kar amacı gütmeyen hükümet kuruluşudur. KOTRA, Kore şirketleri ile ABD dahil denizaşırı ülkelerdeki potansiyel ortaklar arasında karşılıklı olarak fayda sağlayacak iş ortaklarını eşleştirerek şirketler arasında bir köprü görevi görmektedir. Kuruluş bilişim ve siber güvenlik alanında çalışmalar yapmaktadır [93].

4.9. Hindistan

Elektronik ve Bilgi Teknolojileri Bakanlığı (MeitY, Ministry of Electronics & Information Technology), "Vatandaşları güçlendirmek, Elektronik, Bilişim ve Bilgi Teknolojileri endüstrilerinin kapsayıcı ve sürdürülebilir büyümesini teşvik etmek, Hindistan'ın internet yönetişimindeki rolünü arttırmak, insan kaynağını geliştirmek, AR-GE ve inovasyonu teşvik etmek, verimliliği artırmak için çok yönlü bir yaklaşım benimsemek ve e-Yönetişimi teşvik etmek, dijital hizmetler ve güvenli bir siber alanın sağlanması" MeitY'in misyonu olarak belirlenmiştir. Çalışma alanları arasında e-devlet, e-endüstri, e-inovasyon/R&D, e-öğrenme, e-güvenlik, internet yönetişimi konuları yer almaktadır [94]. MeitY'e bağlı olarak çalışan Ulusal Bilişim Merkezi'nin (NIC, National Informatics Centre) siber güvenlik ile ilgili çalışmaları mevcuttur.

Ulusal Siber Koordinasyon Merkezi (NCCC), ülkedeki siber uzayda durumsal farkındalık oluşturmak için siber güvenlik tehditlerine karşı taradığı, çok paydaşlı bir organ olduğu ve ilgili çalışmaların Elektronik ve Bilgi Teknolojileri Bakanlığı'ndaki Hint Bilgisayar Acil Müdahale Ekibi (CERT-In) tarafından yürütüldüğü [95] ifade edilmektedir. NCCC, her türlü siber istihbarat ve siber güvenlikten sorumludur [5].

Kritik Bilgi Altyapısını Koruma Merkezi (NCIIPC, National Critical Information Infrastructure Protection Centre) 16 Ocak 2014'te yayımlanan bildiri ile oluşturulan Hindistan Hükümeti'nin bir kuruluşudur. Kritik Bilgi Altyapısının Korunması Konusunda Ulusal Nodal Ajans olarak belirlenmiştir. NCIIPC'nin vizyonu, ülkenin kritik sektörleri için güvenli, emniyetli ve esnek bir bilgi altyapısı sağlamaktır. NCIIPC, siber güvenlik, bilgi teknolojisi, operasyonel teknoloji, politika, kritik bilgi altyapısının genel güvenliğini hedef alan tehditlerle sürekli olarak mücadele etmektedir [96].

Ulusal Bilgisayar Acil Müdahale Ekibi (CERT-In, National Computer Emergency Response Team), siber olayları kurumlarda yer alan CISO'lar ile iletişim halinde kalarak takip etmek ve bu siber olaylara karşı mücadele etmek ile görevlidir [97]. Ayrıca NCCC'nin de siber olayların yönetiminde sorumlu olduğu görülmektedir [95].

2017 yılında "Bilgi ve İletişim Teknolojileri Operasyonlarını Yöneten Bakanlıklar/Daireler ve Kuruluşlarda Baş Bilgi Güvenliği Görevlilerinin (CISO'lar) Kilit Rolleri ve Sorumlulukları" MeitY tarafından yayımlanmıştır. CISO'lar kuruluşlarda bilgi güvenliğine ilişkin çalışmaları yürüten ve uygulamaları takip eden en üst düzey bilgi güvenliği sorumlusudur [98]. CISO'lar CERT-In ile kurumların birlikte çalışabilmesi için iletişim noktası konumundadırlar [97].

Hindistan'ın 2013 yılında yayımladığı ulusal siber güvenlik strateji belgesinde 14 amaç ve bu amaçlara ulaşabilmek adına yapılması ve uygulanması gereken stratejiler açıklanmıştır. Bu stratejiler epey fazladır. Bu nedenle bazıları şu şekilde sıralanabilir: Güvenli bir siber ekosistem oluşturulması, altyapının oluşturulması, standartların belirlenmesi, altyapının güçlendirilmesi, siber suç ve saldırılara karşı mekanizmaların belirlenmesi, e-devlet servislerinin güvenliği, kritik öneme sahip bilgi sistemlerinin güvenliği, siber güvenlikle ilgili AR-GE çalışmaları gibi [72].

İlgili belgede güvenli bir ekosistem oluşturulması başlığı alt maddeleri incelendiğinde, siber güvenlik ile ilgili tüm hususları açıkça tanımlanmış rol ve sorumluluklarla koordine edecek bir ulusal nodal ajansın belirlenmesi listenin ilk sırasında yer almaktadır. Diğer maddeler incelendiğinde, oluşturulması hedeflenen bu ajansın, siber güvenliğe ilişkin sorumlulukları olan diğer kurumları koordinasyon kabiliyetine sahip olması gerektiği ifade edilmiştir [99].

Hindistan Yazılım Teknolojisi Parkları (Software Technology Parks of India) ülke genelindeki bilgi teknolojisinin büyümesini ilerletmeyi amaçlayan mükemmel altyapı ve yasal destek ile eş anlamlıdır. Hindistan Yazılım Teknolojisi Parkları, Hindistan'dan yazılım ihracatını teşvik etmek ve artırmak amacıyla, 1991 yılında MeitY tarafından kurulan özerk bir topluluktur. Hindistan Yazılım Teknolojisi Parkları, danışmanlık, eğitim ve uygulama hizmetleri sağlamak için mühendislik kaynaklarını korur. Hizmetler; ağ tasarımı, sistem entegrasyonu, montaj, farklı alanlardaki uygulama ağları ve tesislerinin işletimi ve bakımı gibi başlıklardan oluşmaktadır. Süreç geliştirme, Kalite Yönetim Sistemine dayanmaktadır [100].

Hükümet, yayımladığı tebliğ ile gelir ve istihdamı artırmak amacıyla Hindistan'da mal ve hizmetlerin üretimini teşvik etmeyi amaçlamıştır. MeitY, siber güvenliğin stratejik bir sektör olduğunu bildirerek tüm tedarikçilerin sivil güvenlik ürünleri için belirtilen Kamu Alımları (Hindistan'da Yapma Tercihi) emri uyarınca, yerel olarak üretilen siber güvenlik ürünlerinin satın alınmasının kuruluşlar tarafından tercih edilmesi gerektiğini bildirmektedir [101].

Standardizasyon, Test ve Kalite Belgelendirme Ofisi (STQC, Standardisation Testing and Quality Certification), MeitY'ye bağlı bir ofis olup ülke genelinde laboratuvar ve merkez ağı aracılığıyla elektronik ve bilişim teknolojileri alanında kalite güvence hizmetleri sunmaktadır. Bu hizmetler arasında kamu ve özel kuruluşlara test, kalibrasyon, bt & e-yönetişim, eğitim ve sertifikalandırma işlemleri yer almaktadır [102].

4.10. İtalya

İletişim Güvence Kurumu (AGCOM, Autorità per le Garanzie nelle Comnicazioni), 1997 tarihinde kurulan bağımsız bir otoritedir. Telekomünikasyon, görsel-işitsel yayıncılık ve daha yakın bir zamanda posta sektörlerinde düzenleyici ve denetleyici işlevler yürütmektedir. Sesin, videonun ve verilerin (internet erişimi dahil) iletilmesini sağlayan sinyalin dijitalleştirilmesinde meydana gelen değişikliklerin incelenmesi süreçleri kurum tarafından takip edilir. AGCOM kurum organizsyonunda yer alan konsey, kurum başkanı ve komisyonlardan oluşur. Hükümete, teknolojik yenilikler ve iletişim sektörünün ulusal ve uluslararası olarak evrimi ile ilgili olarak yasal düzenlemeler de dahil olmak üzere; özel düzenlemelerin hazırlanması yoluyla iletişim araçlarına ve altyapılarına erişim ile ilgili yasal kuralların uygulanması bakımından öneriler sunar [103].

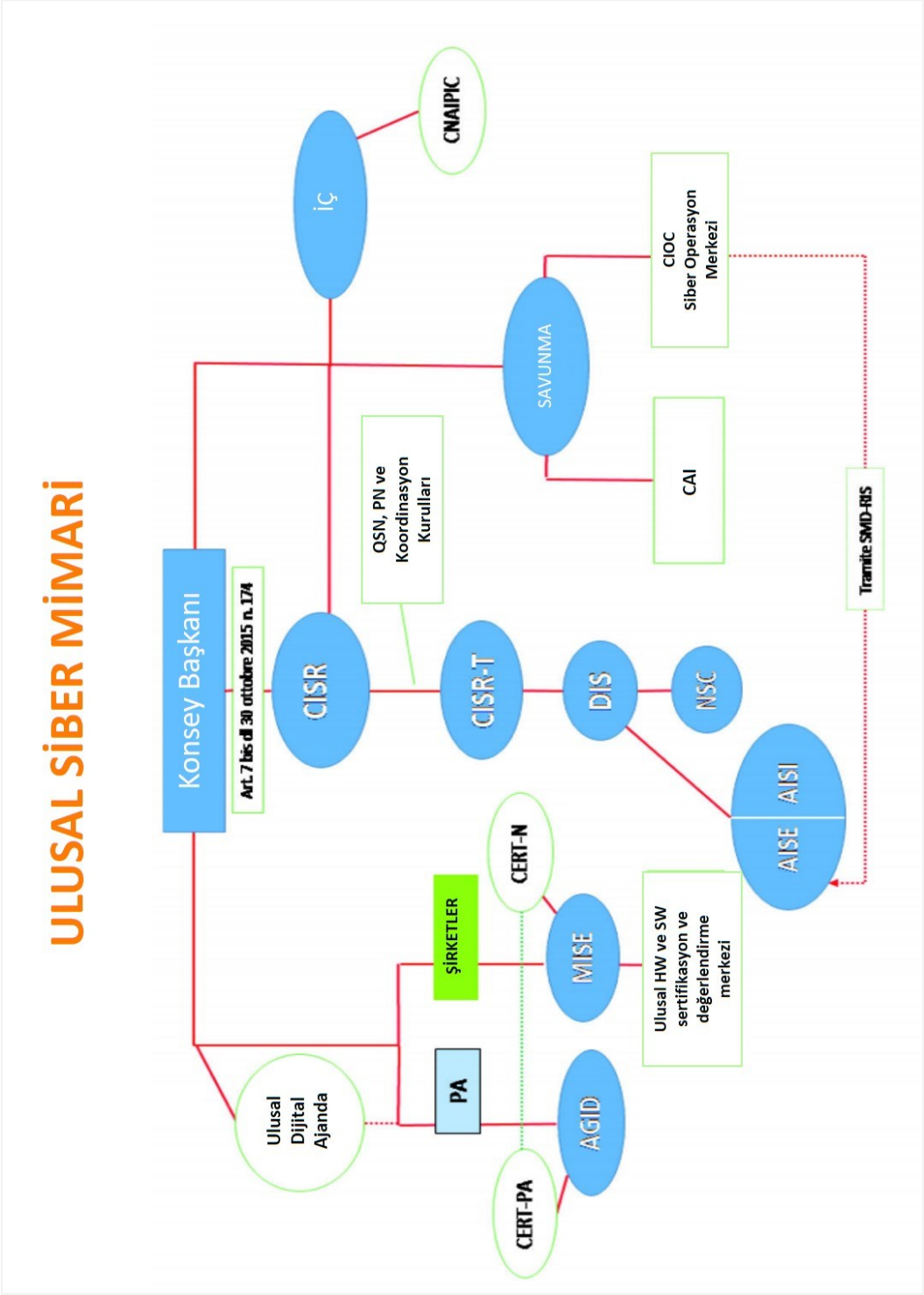
Cumhurbaşkanlığı Cumhuriyet Güvenliği Komitesi (CISR, Comitato interministeriale per la sicurezza della Repubblica) bir danışma organıdır, güvenlik için bilgi politikasının ilkeleri ve genel hedefleri hakkında öneriler ve kararlar sunan bir komitedir [104]. Ulusal siber güvenlik konusundaki genel sorumluluk, CISR tarafından desteklenen Başbakan'a aittir. Aynı zamanda siber güvenliğin iyileştirilmesine yönelik tedbirlerin onaylanmasında karar verici bir rolü vardır. Ulusal siber planın uygulanmasına paralel olarak, CISR, Avrupa Birliği veya NATO gibi uluslararası iş birliğine katılmak gibi girişimleri yürütmektedir.

Güvenlik İstihbarat Dairesi Başkanlığı (DIS, Sistema di informazione per la sicurezza della Repubblica), siber tehditlerin analiz ve değerlendirmelerini yaparak siyasi seviyeyi desteklemektedir. DIS, siber güvenlik bilincini desteklemede önemli bir role sahiptir ve siber

tehditlerle ilgili uyarılar ve bilgi sağlayan Siber Güvenlik Birimi ile bir bağlantısı vardır. Bölüm, Bilgi ve Güvenlik Ajansı (AISI, Agenzia Informazioni e Sicurezza Interna) ve Bilgi Teknolojileri Güvenliği için Dış Bilgi ve Güvenlik Ajansı (AISE, Agenzia Informazioni eSicurezza Esterna) ile birlikte BİT güvenliği için kamu yetkilileri, akademi ve kamu elektronik iletişim ağları ve servis sağlayıcılar ile çalışmaktadır. Siber Güvenlik Birimi (Nucleo la la Sicurezza Cibernetica), siber güvenlikten sorumlu kurumların faaliyetlerini koordine eder, siber olayları ele alır ve ağ işlevselliğini geri kazandırır ve diğer uluslararası kuruluşlarla etkileşime girer. Birim, Başbakanlık Askeri Müşavirliği Ofisi bünyesinde kurulmuştur. Siber Güvenlik Birimi, Ekonomi ve Maliye, Sağlık, Dışişleri, İçişleri, Savunma, Adalet Bakanlıkları ile AISE, AISI, DIS ve Sivil Koruma Bölümü temsilcilerinden oluşmaktadır [105].

Dijital İtalya Ajansı (AgID), Bakanlar Konseyi Başkanlığı'nın teknik ajansıdır. Amacı, İtalyan dijital gündeminin geliştirilmesi hedefine ulaşmak ve inovasyonu ve ekonomik büyümeyi teşvik etmek amacıyla bilgi ve iletişim teknolojilerinin yagınlaşmasını teşvik etmektir. AgID, Kamu İdarelerinde Bilgi Teknolojisi için Üç Yıllık Plan'ın uygulanmasında kamu idarelerini koordine etme görevine sahiptir. AgID, dijital inovasyonu destekler ve aynı zamanda uluslararası ve ulusal kurum ve kuruluşlarla iş birliği içinde dijital becerilerin yaygınlaştırılmasını destekler [106].

2017 yılında yayımlanan siber güvenlik strateji belgesinde İtalya siber güvenlik organizasyon yapısı Şekil 4.7'de olduğu gibidir.



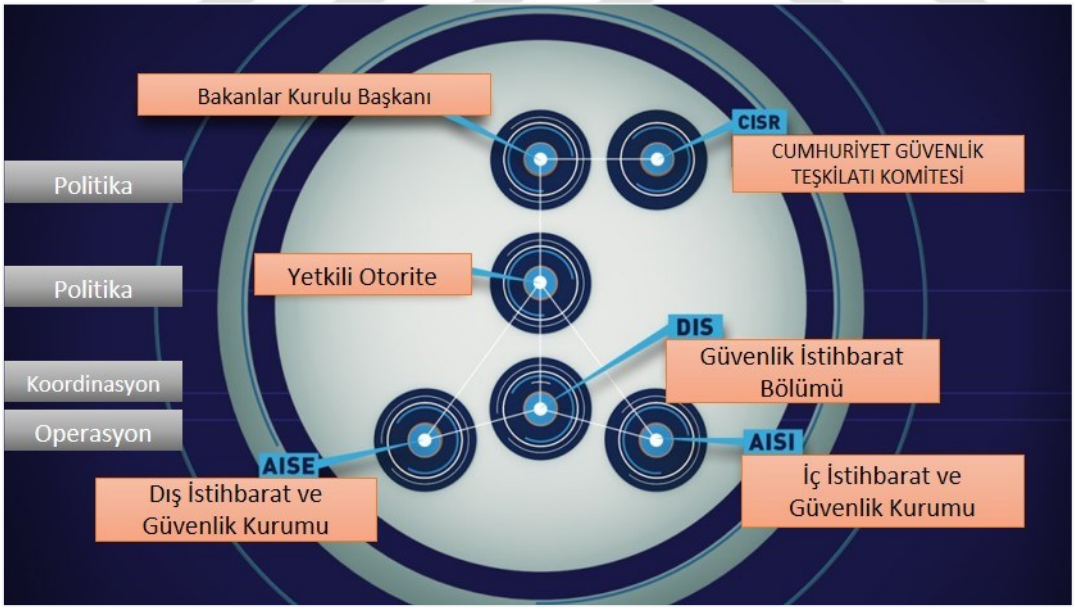
Şekil 4.7. İtalya siber güvenlik organizasyonu [107]

Ekonomik Kalkınma Bakanlığı, elektronik iletişim sistemlerinde güvenlik ve bütünlük konularında merkezi düzenleyici organdır. Bakanlık, siber olayları önlemek ve bu tür olaylara ulusal müdahaleyi koordine etmekle görevli Ulusal Bilgisayar Acil Müdahale Ekibi'ne (CERT-N) ev sahipliği yapmaktadır. CERT-N'nin ana rolü, devletin kriz yönetimi kabiliyetini ve gerektiğinde özel sektörle etkileşimini sağlamaktır [105]. Ulusal CERT ile

ilgili faaliyetler 2013 yılı itibariyle Başbakanlık kararıyla Yüksek İletişim ve Bilgi Teknolojileri Enstitüsü'ne (ISCOM, dell'ıstituto Superiore delle Comunicazioni e delle Tecnologie dell'ınformazione) verilmiştir [108].

Ulusal CERT'e ek olarak, İtalya'nın özel rollere veya faaliyet alanlarına adanmış birkaç sektörel CERT'i vardır. Kamu yönetiminin CERT'i, CERT-PA, Kamu İdaresi'ndeki siber olayların önlenmesi, yanıtlanması ve kurtarılması ile görevlendirilmiştir. CERT-PA, kamu yönetimi içerisinde devam eden ve sonlandırılan güvenlik olaylarının önlenmesi, izlenmesi, bilgi paylaşımı ve değerlendirilmesinden sorumlu olan CERT Kamu Bağlanabilirlik Sistemi (CERT SPC) tarafından tamamlanmaktadır. İtalyan Silahlı Kuvvetleri, kendi CERT kapasitesine sahiptir [105].

Kamu Yönetiminde Bilgisayar Acil Müdahale Ekibi (CERT-PA, Computer Emergency Response Team of the Public Administration), AgID bünyesinde çalışır. Her türlü bilgisayar güvenliği olayını ele almaktan sorumludur. CERT-PA birimi, 2014 tarihinden bu yana, olay müdahalesinden sorumlu olarak faaliyet göstermektedir [106].



Şekil 4.8. İtalya siber istihbarat sistemi [104]

Ülke Güvenliğine Yönelik İtalya'nın İstihbarat Sistemi; istihbarat politikaları, istihbarat koordinasyonu ve istihbarat operasyonlarından sorumlu yetkililere ve kuruluşlara verilen ortak addır. Güvenlik İstihbarat Sistemi Şekil 4.8'de ifade edildiği üzere şunları içermektedir; Bakanlar Kurulu Başkanı, Yetkili Otorite, Cumhuriyet Güvenlik Teşkilatı

Komitesi (CISR), Güvenlik İstihbarat Bölümü (DIS), Dış İstihbarat ve Güvenlik Kurumu (AISE), İç İstihbarat ve Güvenlik Kurumu (AISI) [104].

Savunma Bakanlığı, İtalya'nın siber alandaki askeri yeteneklerini koordine etmektedir. Ulusal Güvenlik Çerçevesi, İtalyan Silahlı Kuvvetleri'nin siber alandaki tehditlere karşı savunma amaçlı Bilgisayar Ağı İşlemleri (CNO) yapabileceğini belirtmektedir. İtalyan Silahlı Kuvvetleri yönetiminde olan CERT Savunma (CERT Difesa) bu anlamda teknik destek sağlamaktadır ve siber uzayda bilgisayar sistemlerini ve ağları hedef alan kötü niyetli faaliyetlere karşı ülkeyi savunmaktadır. CERT Savunma Koordinasyon Merkezi, ulusal CERT'lerin yanı sıra özel sektör ve akademi ile de kritik alt yapıya yönelik tehditler hakkında bilgi paylaşmaktadır. CERT Savunma'nın ulusal stratejik çerçevedeki faaliyet hedefi, askeri ve operasyonel planlamalara tamamen entegre olmaktır [105].

İtalya'nın 2013 yılında yayımladığı siber güvenlik strateji belgesinde 6 temel stratejik kural belirlendiği gözlenmektedir. Bu stratejik kurallar: (1)Bütün paydaşların teknik, operasyonel ve analitik yetkinliklerinin geliştirilmesi, (2)Kritik altyapıların, stratejik varlıkların ve tüm paydaşların korunmasına yönelik kapasitenin geliştirilmesi, (3)Özel sektör kamu iş birliklerini geliştirmek, (4)Siber güvenlik kültürünü yaygınlaştırma, (5)Online suç aktiviteleri ve yasadışı içeriklere yönelik ülke kapasitesini yeniden yapılandırma ve (6)Uluslararası iş birliklerini geliştirme başlıklarıyla belirlenmiştir [109].

2017 yılında revize edilen, Bakanlar Kurulu Başkanlığı tarafından yayımlanan ulusal siber güvenlik strateji belgesinde esas hedefler; (1)Ulusal kritik altyapıların savunma yeteneklerinin ve ülke sistemi için stratejik öneme sahip aktörlerin güçlendirilmesi, (2)Bütünleşik bir yaklaşıma göre, katılan kurumsal aktörlerin teknolojik, operasyonel ve analitik becerilerinin geliştirilmesi, (3)Ulusal kurumlar ve şirketler arasındaki iş birliğinin teşvik edilmesi, (4)Siber güvenlik kültürünün tanıtılması ve yaygınlaştırılması, (5)Siber güvenlik konusunda uluslararası iş birliğinin güçlendirilmesi, (6)Çevrimiçi yasadışı faaliyetlerle ve yasadışı içerikle mücadele yeteneğinin güçlendirilmesi olarak belirlenmiştir [107].

Kritik Altyapıların Korunması ve Suçla Mücadele Ulusal Bilgi Merkezi (CNAIPIC, Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastructure Critiche), ulusal öneme sahip bilgi işlem altyapılarına karşı işlenebilecek ortak, örgütlü veya terörist nitelikteki siber suçların önlenmesi ve bastırılmasından sorumludur [110].

4.11. İspanya

İspanya Veri Koruma Ajansı (AEPD, Spanish Data Protection Agency), erişim, düzeltme, sınırlama, muhalefet, silme (unutulma hakkı), taşınabilirlik vb. hakları koruyan devlet kurumudur [111].

Ulusal Siber Güvenlik Enstitüsü (INCIBE, Spanish National Cybersecurity Institute), özellikle kritik altyapıları hedef alan siber olaylara karşı çalışan bir kurumu olan Enstitü, siber güçlendirme misyonuyla, Sanayi, Enerji ve Turizm Bakanlığı'na bağlıdır. Aynı zamanda Telekomünikasyon ve Bilgi Bakanlığı'nın bir üyesidir. Bilgi toplumu hizmetlerinin güvenlirliğinin yanı sıra siber güvenlik ve gizlilik ile ilgili misyonları vardır. INCIBE, siber güvenlikten sorumlu ulusal ve uluslararası kuruluşlarla yapılacak çalışmaları koordine eder. Ciddi bir tehdit durumunda, INCIBE bunu ilgili devlet sekreteryasına havale etmektedir [112]. INCIBE'nin faaliyetleri üç temel dayanak üzerine kuruludur: hizmet sunumu, araştırma ve koordinasyon [113].

İspanya Siber Güvenlik Araştırmaları Mükemmeliyet Ağı (RENIC), İspanya'daki araştırma merkezlerini ve siber güvenlik ekosisteminin diğer temsilcilerini içeren, üyeliğe dayalı bir sektörel dernektir. RENIC, İspanya'da siber güvenlik alanında bilimsel araştırma, teknolojik gelişme, yenilikçilik, bilgi ve teknoloji transferini ve AR-GE gelişimini desteklemeyi amaçlamaktadır. RENIC'in ana mantığı, siber güvenlik araştırmalarında rekabetçiliğin arttırılmasına katkıda bulunmak, riskleri azaltan ve ortaya çıkan tehditleri azaltan, pazarın ihtiyaçlarına cevap veren çözümler geliştirmeye katkıda bulunmaktır [114]. Kurucu üyelerinin genellikle üniversitelerden oluştuğu gözlenmiştir.

İspanya Bilgisayar Güvenliği ve Olay Müdahale Ekibi/Bilgisayar Acil Durum Müdahale Ekipleri, CSIRT.es forumu vasıtasıyla bilgi paylaşmaktadır. İlgili forumda siber olaylara müdahale amacıyla görev yapan üyeler yer almaktadır. Bu forumun ana hedefleri, İspanya siber uzayını korumak, siber güvenlik hakkında bilgi alışverişinde bulunmak ve İspanya'daki farklı kurumları aynı anda etkileyebilecek herhangi bir olay durumunda hızlı ve koordineli bir şekilde hareket etmektir. Bu forum, faaliyet alanı veya faaliyet gösterdiği kullanıcı topluluğu İspanya topraklarında bulunan CSIRT/CERT müdahale ekiplerinden oluşan bağımsız, kar amacı gütmeyen, güvenilir bir platform olarak çalışmaktadır [115]. CERT-SI, INCIBE-CERT, CCN-CERT, ESPCERTDEF önemli siber olaylara müdahale ekipleridir.

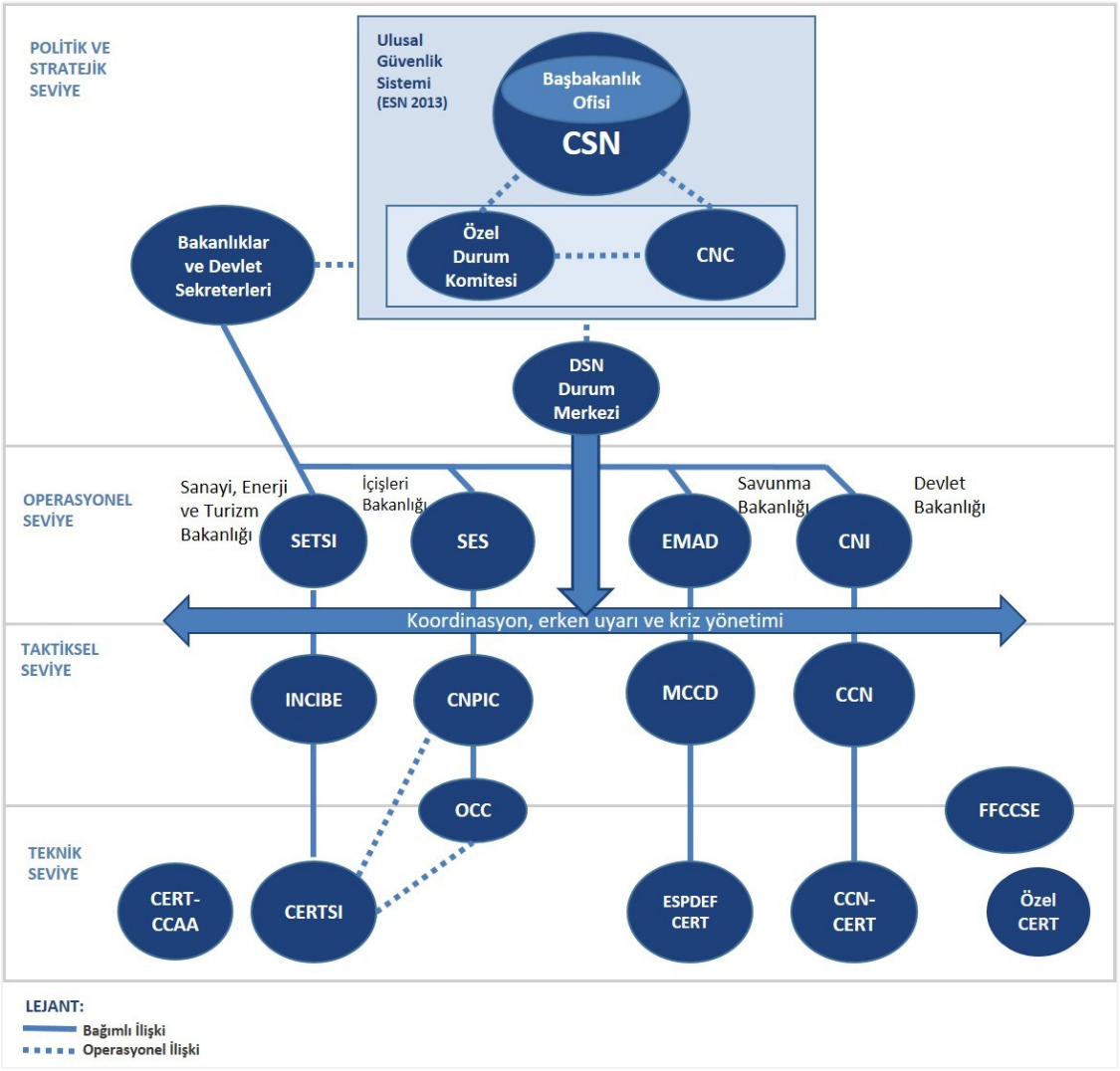
CCN-CERT, Kamu Sektörünün Yasal Rejimi Kanun'u uyarınca, herhangi bir kamu kuruluşunu veya şirketi etkileyen siber olayların yönetiminden sorumludur. Kamu sektöründe kritik siber olayların yönetimi, CNPIC ile koordineli olarak CCN-CERT tarafından gerçekleştirilmektedir [116].

INCIBE-CERT, Ekonomi ve Ticaret Bakanlığı (MINECO) altında Dijital İlerleme Devlet Sekreteri (SEAD) tarafından işletilen INCIBE-CERT, İspanya'daki vatandaşlar ve özel hukuk kuruluşları için birincil siber güvenlik müdahale merkezidir. Kritik özel sektör operatörlerini etkileyen olay yönetimi durumunda, INCIBE-CERT, İçişleri Bakanlığı Altyapı Koruma ve Siber Güvenlik Ulusal Merkezi ve CNPIC tarafından ortaklaşa işletilmektedir. INCIBE-CERT, ağ ve bilgi sistemlerini içeren suçlara karşı mücadelede verimliliği artırarak kamu güvenliği üzerindeki etkilerini azaltan ulusal ve uluslararası ekiplerin geri kalanıyla koordine halinde çalışan olay müdahale ekiplerinden biridir [117].

Ulusal İstihbarat Merkezi (CNI, National Intelligence Centre), Cumhurbaşkanlığı'nın bir parçası olan istihbarat birimidir [5].

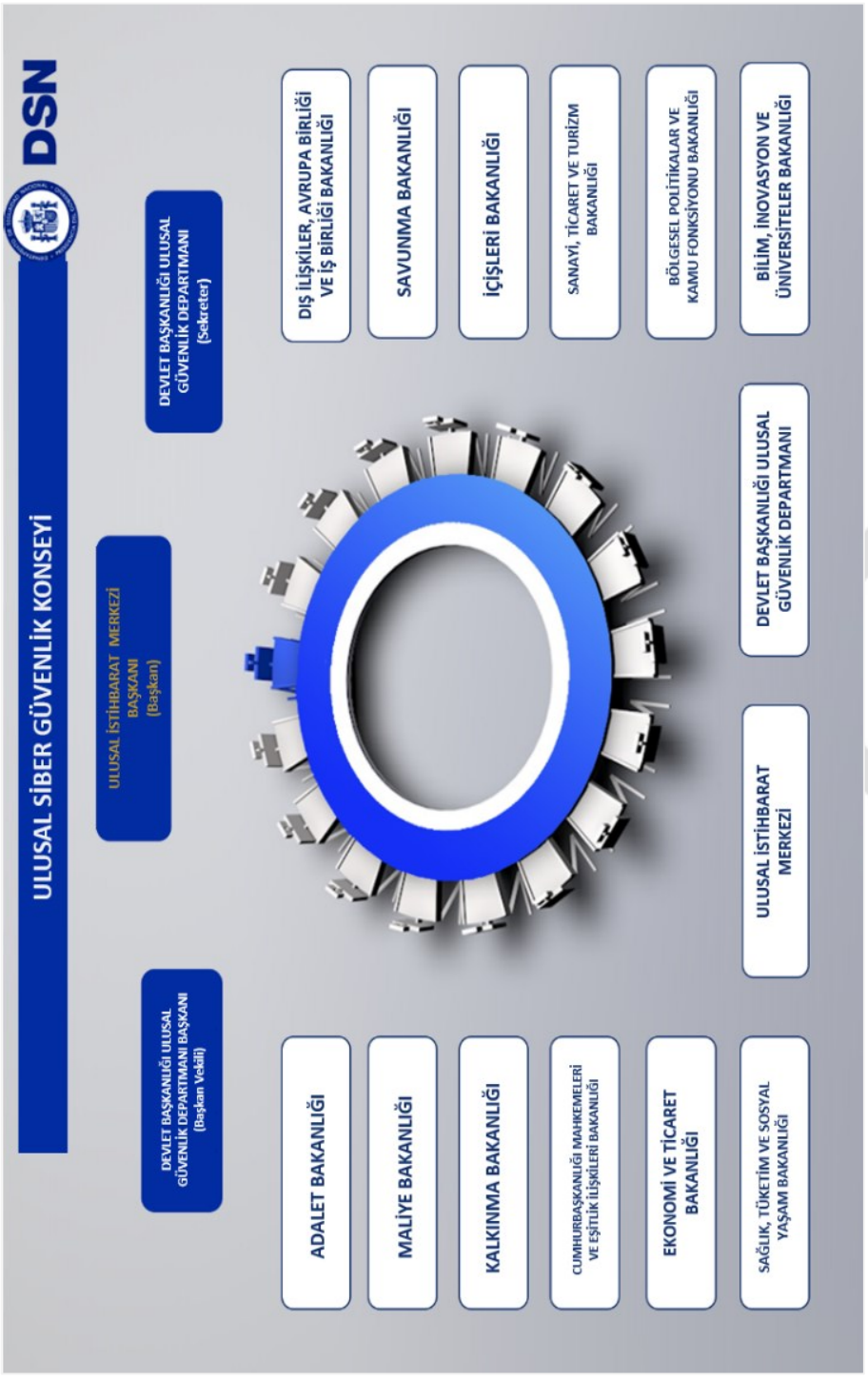
Ortak Siber Komutanlık (MCCD, Mando Conjunto de Ciberdefensa), Savunma Bakanlığı içindeki siber savunma işlerinden sorumlu İspanyol siber komuta organıdır. İspanya savunma personeli ortak şeflerinin bir parçası olarak, bu kurum, bilgi güvenliği uygulama politikalarının geliştirilmesi, yönetimi ve kontrolü de dahil olmak üzere, siber uzayda ordu kuvvetlerinin faaliyetlerini yönetir ve koordine eder. Görevi, silahlı kuvvetlerin telekomünikasyon ağlarında ve bilgi sistemlerinde veya kendisine verilebilecek diğer ağlarda askeri siber savunma eylemlerini planlamak ve yürütmektir. MCCD, taktiksel düzeyde, siber alanda ulusal savunmayı etkileyebilecek risklere veya tehditlere en iyi şekilde yanıt verilmesine katkıda bulunur. Bu anlamda, bilgi güvenliği olaylarına cevap olarak INCIBE ve CNI gibi ulusal merkezlerle iş birliği yapmakta ve siber savunma alanındaki farkındalık ve özel eğitim faaliyetlerinin tanımlanması, yönetimi ve koordinasyonu için sorumluluk almaktadır [112].

İspanya Ulusal Siber Güvenlik Stratejisi'nde (2013), siber uzay ve siber güvenlik, İspanya'da siber güvenliğin sağlanması için amaçlar ve prensipler, ulusal siber güvenliği sağlamada alınacak aksiyonlar ve Ulusal Güvenlik Sistemi içerisinde siber güvenliğin yeri konuları açıklanmıştır. İspanya siber güvenlik organizasyonu ise Şekil 4.9'da olduğu gibidir.



Şekil 4.9. İspanya siber güvenlik organizasyonu [112]

Ulusal Güvenlik Bakanlığı (DSN, El Departamento de Seguridad Nacional), organizasyon yapısı ve işlevsel olarak Hükümet Başkanlığı Kabinesi'ne bağlıdır. DSN'de yer alan iki konsey siber güvenlik ile ilgili çalışmalar yürütmektedir. Ulusal Güvenlik Konseyi (CSN, National Security Council), Ulusal Güvenlik Politikası ve Ulusal Güvenlik Sistemi doğrultusunda hükümet başkanına yardım etmekten ve aynı zamanda Ulusal Güvenlik Yasası'nda kendisine atfedilen ve yönetmeliklerle atanan işlevleri yerine getirir. Konseyde yer alan Ulusal Siber Güvenlik Konseyi (CNC, Consejo Nacional de Ciberseguridad) Ulusal Güvenlik Konseyi'ne destek veren bir hakem kuruluştur. Özel sektörün ilgili diğer aktörleri ve katkısı gerekli görülen uzmanlar konseye katılabilmektedir [118]. Konseyin yapısı Şekil 4.10'da olduğu gibidir.



Şekil 4.10. İspanya ulusal siber güvenlik konseyi [118]

Ulusal Altyapıların ve Siber Güvenliği Koruma Merkezi (CNPIC, Spanish Government National Cryptologic Center), İçişleri Bakanlığı'ndaki İspanyol kritik altyapılarının ve siber güvenliğin korunmasına ilişkin tüm politika ve faaliyetlerin tanıtımından, koordinasyonundan ve denetlenmesinden sorumlu organdır. CNPIC, nihayetinde Kritik Altyapıların Korunması Ulusal Sistemi'nden ve Bakanlık'ın siber güvenlik politikalarından

sorumlu olan Devlet Güvenlik Sekreteri'ne bağlıdır [119]. Ajans taktik seviyesinde faaliyet göstermektedir [112].

İspanya, siber güvenlik kümelenmesi konusunda örnek alınabilecek çalışmalar yürütmektedir. Savunma Sanayii Müsteşarlığı'nın Ankara'da düzenlediği 3. Siber Savaş ve Güvenlik Konferansı'nda İspanya'nın Yenilikçi Siber Güvenlik Kümelenmesi Modeli sunulmuştur. Bu modele göre; yapı ve çalışma grupları oluşturularak, standardizasyon ve sertifikasyon süreçleri, teknolojik pazarda ürünlerin dağıtımı, sektörel talepler, kobilerin ihtiyaçları, eğitim süreçleri, stratejik amaçlar için bilim ve teknolojik komitelerin yürütmesi gerekenler gibi altı farklı alanda çalışmalar yürütülmüştür [120]. Bu çalışmalar neticesinde kümelenme gerçekleşmiştir. Gerçekleştirilen bu proje Avrupa Birliği tarafından maddi olarak desteklenmektedir.

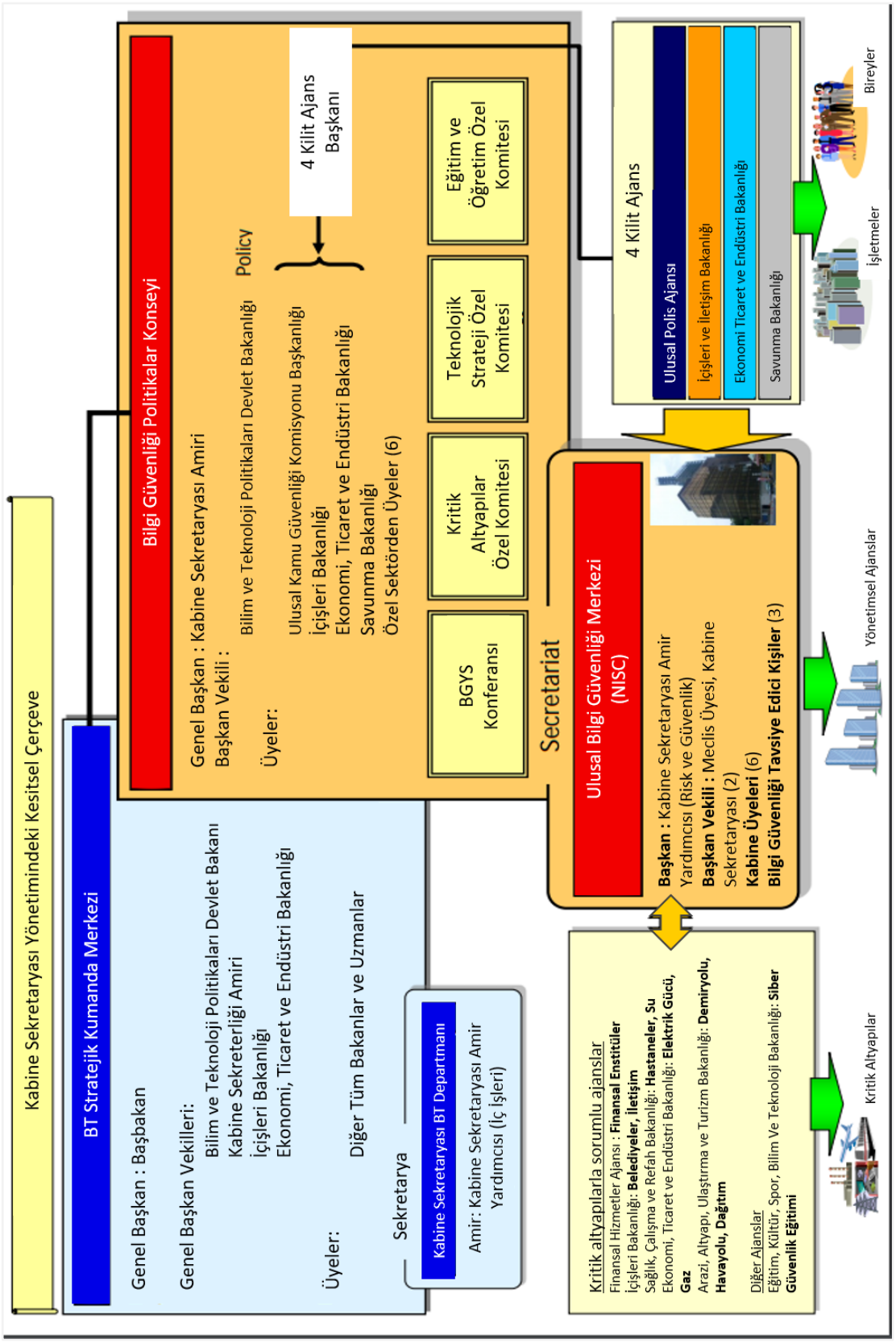
Özel sektör kuruluşları ile kamu kurumlarının koordinasyonu, ulusal ve uluslararası siber güvenliğin sağlanması konularında Başbakan'a destekleyici bilgiler sağlayan Ulusal Siber Güvenlik Konseyi (CNC) görevlidir.

Bilgi Toplumu ve Dijital Gündem Politikaları İspanya'da, teknolojinin geleceğe yön verecek unsurlardan biri olduğunu kabul ettiğini gösteren örneklerdendir [114]. İspanya Maliye Bakanlığı ile Ekonomi ve Ticaret Bakanlığı'nın ortak çalışmalarıyla İspanya Dijital Gündemi belirlenmektedir. İspanya Dijital Gündemi, 2015 ve 2020'de Avrupa için Dijital Gündem'in amaçlarının yerine getirilmesi için BİT ve elektronik idaresi açısından yol haritasını çizer ve İspanya'da ekonominin ve dijital toplumun gelişimini amaçlar. İspanya, dijital ekonominin ve dijital içeriğin stratejik olarak önemli olduğunu kabul ederek teknolojiyi büyüme, istihdam ve gelecekteki fırsatların itici gücü olarak kabul etmiştir. Gündem, hem kamu yönetiminin hem de özel sektörün katıldığı dijital içerik endüstrisi için kapsamlı bir planın geliştirilmesini sağlamıştır. Dijital ekonomiyi ve dijital içeriği artırmaya yönelik mevcut plan, bu sektörde girişimciliği teşvik eden, şirketlerin büyümesini kolaylaştıran, dışa açılmalarını teşvik eden tedbirlerle dijital ekonominin gelişimine katkı sağlamaktadır [121].

4.12. Japonya

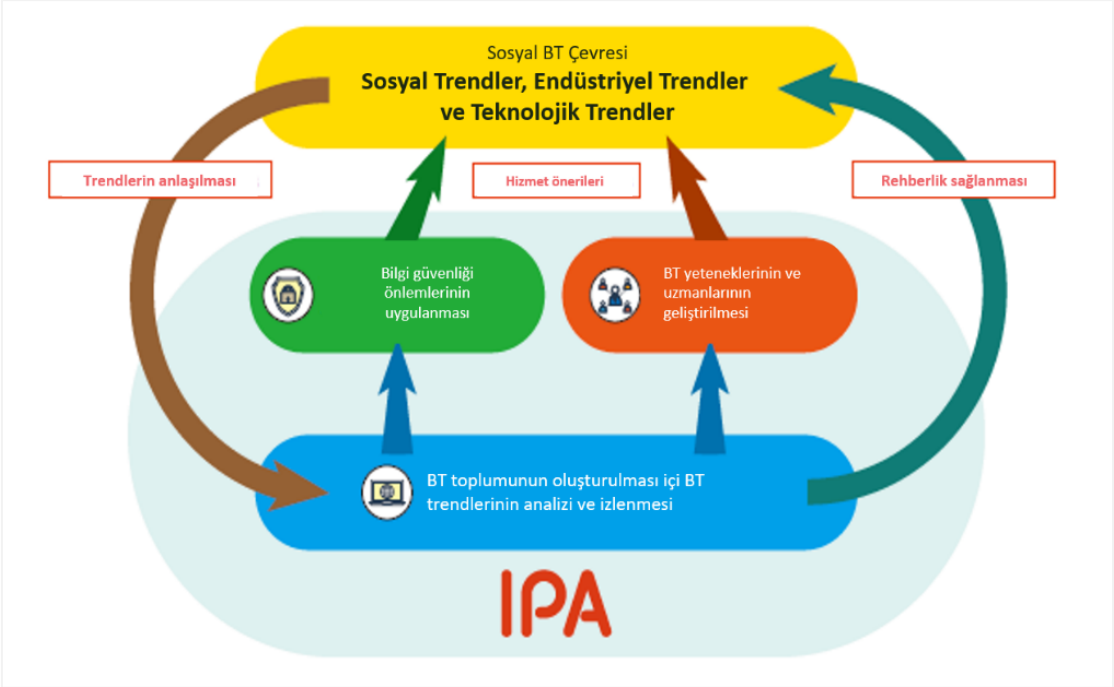
Ulusal Bilgi Güvenliği Merkezi (NISC, National Information Security Center), Japonya'da bilgi güvenliği politikasının düzgün ve etkin bir şekilde uygulanmasını sağlamak için

Bakanlar Kurulu Sekreteryası'nda kurulan bilgi güvenliği ile ilgili temel organizasyonudur [122]. Japonya Bilgi Güvenliği Merkezi yapılanması Şekil 4.11'de olduğu gibidir.



Şekil 4.11. Japonya bilgi güvenliği merkezi yapılanması [123]

Bilgi Teknolojileri Tanıtım Ajansı (IPA), politika üretici bir diğer kuruluştur. IPA'nın amaçları; Bilgi güvenliği önlemlerini uygulamak, BT yeteneklerini ve profesyonellerini beslemek, BT topluluğu için bir temel oluşturmak üzere BT eğilimlerini izlemek ve analiz etmektir. IPA'ya bünyesinde güvenlik önlemleri konusunda çalışan bir merkez olarak; IPA/ISEC katkı sağlamaktadır. Bilgi Teknolojileri Güvenlik Merkezi (ISEC), Japonya'da bilgi güvenliğini desteklemek için bir kamu bilgi paylaşım merkezidir. 1 Ocak 1997 tarihinde IPA'nın bir bölümü olarak kurulmuştur. IPA, Ekonomi, Ticaret ve Sanayi Bakanlığı'na (METI) bağlı bir kuruluştur [124]. IPA'nın rolü Şekil 4.12'de olduğu gibidir.



Şekil 4.12. IPA'nın rolü [124]

Ulusal İleri Endüstriyel Bilim ve Teknoloji Enstitüsü (AIST), Japonya'daki en büyük kamu araştırma kuruluşlarından biridir. Japon endüstrisi ve toplumu için faydalı teknolojilerin yaratılması ve pratik olarak gerçekleştirilmesine ve yenilikçi teknolojik tohumlar arasındaki boşluğu "köprülemeye" odaklanmaktadır. AIST, sürdürülebilir bir toplum inşa etmek ümidiyle "Yeşil Teknoloji", "Yaşam Teknolojisi" ile sağlıklı ve güvenli bir yaşam sürerek, "Bilgi Teknolojileri" ile süper akıllı bir toplum aracılığıyla zengin ve çevre dostu bir toplum elde etmeyi amaçlamaktadır. AIST Bilgi Teknolojisi Ve İnsan Faktörü Bölümü'nün araştırma birimleri arasında Siber Fiziksel Güvenlik Araştırma Merkezi de yer almaktadır [125].

Ulusal Bilgi ve İletişim Teknolojileri Enstitüsü (NICT, National Institute of Information and Communications Technology), Japonya'nın bilgi ve iletişim teknolojisi alanında uzmanlaşmış ulusal araştırma ve geliştirme ajansı olarak çalışmaktadır. BİT sektörünün yanı sıra ekonomik büyümeyi sağlamak ve BİT alanında zengin ve güvenli bir toplum oluşturmak, araştırma ve gelişmeyi teşvik etmekle görevlidir [126]. NICT bünyesinde bulunan Siber Güvenlik Araştırma Enstitüsü, gelişmiş siber güvenlik araştırma laboratuvarlarına sahiptir.

JPCERT/CC, Japonya Bilgisayar Acil Durum Müdahale Ekibi/Koordinasyon Merkezi, internette meydana gelen izinsiz girişler ve hizmet reddi gibi bilgisayar güvenliği ile ilgili insan kaynaklı olaylara cevap veren bir organizasyondur. JPCERT/CC, Japonya'daki internet siteleriyle ilgili raporları kabul etmekte, izinsiz giriş, hizmet reddi, kaynakların yasa dışı kullanımı, verilerin imha edilmesi, istenmeyen bilgilerin açıklanması vb. bilgisayar güvenliği olaylarını takip etmekte ve bunlara karşılık vermektedir. JPCERT/CC, siber olaylara ilişkin durumu kavrama, imza analizi, tekrar oluşmayı önleme, tedbirleri ve tavsiyeleri inceleme gibi teknik açıdan yürüten kar amacı gütmeyen organizasyondur [127].

Asya Pasifik Bilgisayar Acil Durum Müdahale Ekibi (APCERT, Asia Pacific Computer Emergency Response Team), Asya Pasifik bölgesindeki Bilgisayar Güvenliği ve Olay Müdahale Ekibi (CSIRT) ve Bilgisayar Acil Durum Müdahale Ekibi (CERT) organizasyonları arasındaki iş birliğini teşvik etmekte ve desteklemektedir [128].

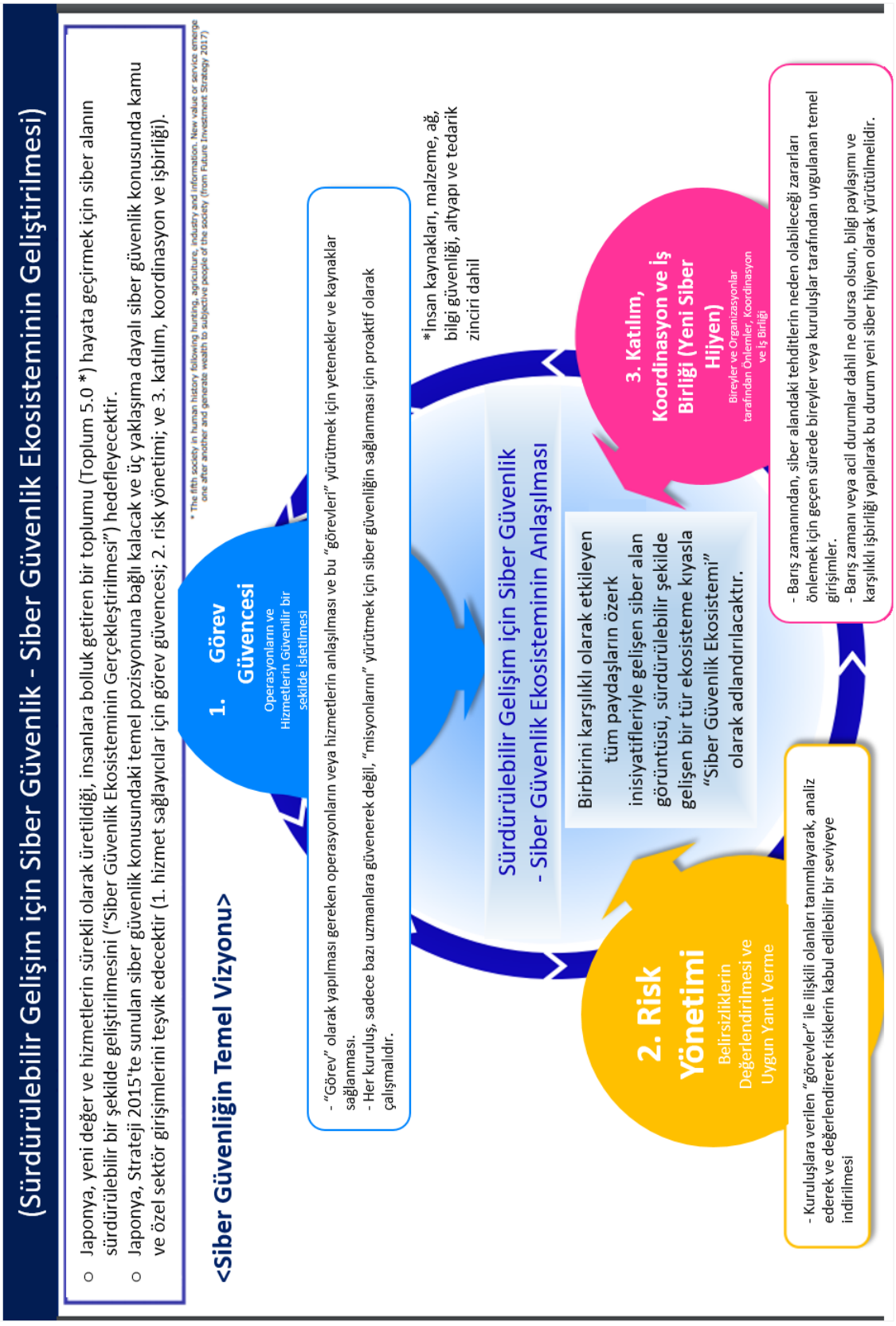
Japonya ASEAN Güvenlik Ortaklığı (JASPER, Japan-ASEAN Security PartnERship), Japonya ve ASEAN arasında siber güvenlik konusundaki iş birliği anlaşmalarını ifade eder. İş birliği sonucunda, Japonya, bu platformda, 2018-2020 dönemi için Malezya ve Singapur'la birlikte BT'lerin Güvenliği Eş Başkanı olarak görev yapmaktadır [129].

Uluslararası İş Birliği Yoluyla Siber Saldırılara Karşı Proaktif Yanıt Sistemi (PRACTICE, Proactive Response Against Cyber-attacks), 2011'de kurulmuştıur. Hedefleri arasında dünya çapında siber tehditleri izleme sistemleri kurmak, siber saldırı semptomlarını tespit etmek ve bunlara cevap vermek gibi konular yer almaktadır [130].

Japonya Ulusal Güvenlik Strateji Belgesi'nde küresel ortak varlıklara yönelik riskler arasında siber saldırılara yer verilmiştir. Siber saldırıların gizli bilgilerin ele geçirilmesi, kritik altyapıların işleyişinin sekteye uğratılması, askeri sistemlerin engellenmesi gibi siber

uzay risklerini barındırdığı vurgulanmıştır. İlgili belgede Japonya'nın kabiliyetlerini güçlendirmek ve genişletmek için siber güvenliğin arttırılması konusuna yer verilmiştir [131].

2018 yılında güncellenerek yayımlanan Japonya Siber Güvenlik Strateji Belgesi'nde [132] "Özgür, Adil ve Güvenli Bir Siber Alanda Fikirlerini Paylaşmak" başlığı altında, özerk ve sürdürülebilir şekilde gelişen bir siber ekosistemi korumak için, devletler tarafından bilgi akışını kontrol etmek gibi kontrol ve düzenleme yoluyla Japonya siber güvenliğini sağlama çabaları yerine, paydaşlar arasındaki koordinasyon ve iş birliği yoluyla siber ortamdaki güvenliği sağlamayı amaçlayan bir yol izleneceği vurgulanmıştır. Strateji belgesinde yer aldığı haliyle, siber güvenlik ekosisteminin temel vizyonu [133] Şekil 4.13'te ifade edildiği gibidir.



Şekil 4.13. Japonya siber güvenlik ekosisteminin temel vizyonu [133]

Doğal afetlerin yoğun yaşandığı bir konumda bulunan Japonya, bilgi güvenliğini sadece siber saldırıların sebep olabileceği aksaklıklar açısından değil, doğal afetlerin neden olabileceği kritik altyapılarda karşılaşılabilecek önemli problemleri de göz önüne alarak değerlendirmektedir [64].

2018 yılında güncellenmiş olarak yayımlanan Japonya Kritik Altyapıların Korunması için Siber Güvenlik Politikası [134] (1)Kritik altyapı politikasının amacı, (2)Temel ilkeler, (3)Kritik altyapı operatörleri, devlet kuruluşları ve siber güvenlikle ilgili kurumlar gibi paydaşların sorumluluğu ve (4)Üst yönetimin sorumlulukları başlıklarıyla tasnif edilmiştir. Kritik altyapılara ilişkin hedefler, belirtilen bu kilit hususlar baz alınarak belirlenmiştir.

Japonya'da NISC bünyesinde, CEPTOAR olarak adlandırılan, kritik altyapılara ilişkin politika üreten ve politikaların uygulanmasını takip eden bir konsey bulunmaktadır.

4.13. Kanada

Kamu Güvenliği Bakanlığı (Public Safety Canada)**,** 2003 yılında kurulmuştur. Kanada halkının, doğal felaketler, suç ve terörizm gibi konulara karşı güvende kalmalarını sağlamak Bakanlık'ın görevleri arasındadır. Bakanlık, siber güvenlik ile ilgili çalışmaları da yürütmektedir. Kanada Kamu Güvenliği Bakanlığı, Ulusal Acil Müdahale Sistemi'nin (NERS) merkezi olarak Devlet Operasyon Merkezi'ne ev sahipliği yapmaktadır. Kanada Siber Olay Müdahale Merkezi (CCIRC), Devlet Operasyon Merkezi için ulusal öneme sahip siber olayları takip etmekte ve bu olaylara yanıt sistemlerini koordine etmektedir [5].

Kanada Siber Olay Müdahale Merkezi (CCIRC, Canadian Cyber Incident Response Centre), siber olayların önlenmesi ve azaltılması, siber olaylara hazırlıklı olma, müdahale etme ve siber tehditleri bertaraf etmek amacıyla çalışan bir merkezdir [5].

Akıllı Siber Güvenlik Ağı (SERENE-RISC, Smart Cybersecurity Network), siber güvenlik bilgilerinin değişimini kolaylaştırmak için Kanada merkezli bir mekanizmadır [5].

Kanada İletişim Güvenliği Oluşumu (CSEC, Communications Security Establishment Canada), Kanada'nın yabancı kaynaklı siber istihbaratları toplamasından sorumlu kriptoloji ajansıdır. CSEC, Kanada'nın uluslararası kriptoloji topluluklarıyla iletişim kuran topluluğudur. Siber güvenlik için araştırma ve geliştirme çalışmaları yürütmektedir. CSEC, hükümete karşı yürütülen karmaşık siber tehditleri tespit ederek ve bunlara cevap vererek

Kanada Hükümeti ağlarını izler ve savunur. CSEC, siber olayları azaltma ve siber tehditlerden korunma önerileri vererek hükümet departmanlarına rehberlik sağlar [5].

Kanada Güvenlik İstihbarat Servisi (CSIS, Canadian Security Intelligence Service), ulusal güvenlik araştırmaları yapmak, Kanada Güvenlik İstihbarat Servisi Yasası'nda tanımlandığı şekilde Kanada güvenliğine tehdit oluşturan faaliyetleri Kanada Hükümeti'ne raporlamak ve danışmanlık yapmakla görevlidir. Kanada Hükümeti'ne, siber tehditleri ve Kanada'da ve yurtdışında faaliyet gösteren siber aktörlerin Kanada güvenliğini tehdit eden niyetlerini ve yeteneklerini anlamalarında yardımcı olmak için analizler sunar [5].

Savunma AR-GE Kanada (DRDC, Defence Research and Development Canada), askeri siber güvenlik bilimi ve teknolojisinin gelişmesine öncülük eder. DRDC Güvenlik Bilimi Merkezi (DRDC CSS), Kamu Güvenliği Kanada ile ortak bir şekilde çeşitli çalışmaları da yürütür. Bu çalışmalar, Kanada Güvenlik Programı (CSSP) kapsamındadır [5].

Kanada Kraliyet Atlı Polisi (RCMP, Royal Canadian Mounted Police), izinsiz bilgisayar ve veri kullanımı, şüpheli işlemler, yanlışlıklar gibi siber olaylara karşı cezai soruşturma yapar. Şüpheli siber güvenlik olaylarına karşı ulusal soruşturma işlemlerini yürütür. Siber suç tehditlerine ilişkin tavsiyelerle yerel ve uluslararası ortaklara rehberlik sağlar [5].

Kamu Güvenliği Bakanlığı, 2009 yılında Kritik Altyapılar için Aksiyon Planı Belgesi'ni hazırlamıştır. Aynı yıl Kritik Altyapılar için Ulusal Strateji Belgesi yayımlanmıştır. İlgili belgelerde enerji, finans, beslenme, ulaşım, bilgi ve iletişim teknolojileri, sağlık, su, güvenlik, ticaret gibi başlıklar kritik altyapılara olarak belirlenmiştir. Federal hükümetin, bölgesel hükümetlerin ve kritik altyapı sahibi operatörlerin sorumlulukları tanımlanmıştır. 2010 yılında yayımlanan Siber Güvenlik Strateji Belgesi; devlet sistemlerinin güvenliği, dış devletlerle güvenli siber sistemlerin devamı için ortaklık ve Kanadalılar'ın çevrimiçi güvenliğini sağlamaya yardım etmek olmak üzere 3 ana başlığa odaklanmıştır.

Stratejinin hukukun üstünlüğü, hesap verebilirlik ve gizlilik gibi Kanada değerlerini yansıtmakta olduğu ifade edilmiştir. Ayrıca stratejinin; ortaya çıkacak tehditlere karşı kendisini sürekli geliştiren; Kanadalılar ile bölgeler, iş ve akademi dünyası arasında iş birlikteliğini vurgulayan; müttefiklerle yakın çalışma ilişkileri kurulmasını sağlayan yönleri olduğu ifade edilmiştir. 2016 yılında yayımlanan Kanada'nın Kritik Altyapı Toplulukları

için Siber Güvenliğin Temelleri adlı belgede siber güvenliğe ilişkin riskleri azaltmaya ve farkındalık oluşturmaya yönelik bazı temel önlemler yer almaktadır.

Kanada Endüstrisi (IC, Industry Canada), sağlam ve güvenilir bir telekomünikasyon sisteminin geliştirilmesinden sorumludur. IC, güvenli bir çevrimiçi pazar ortamı sağlamak için politikalar geliştirmekte ve acil durumlarda telekomünikasyon sistemlerinin sürekliliğini sağlamaya yardımcı olmaktadır [5].

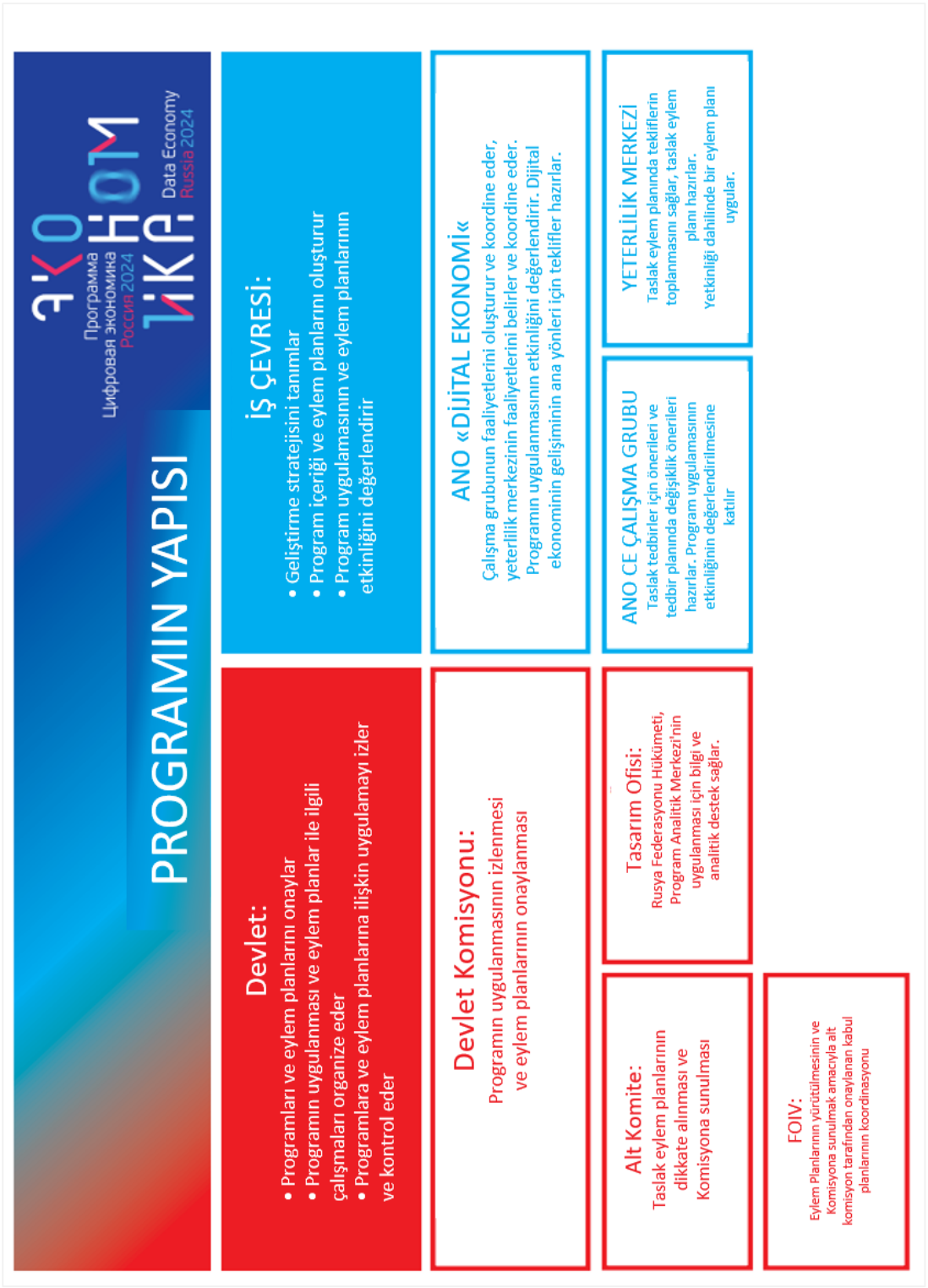
Kanada, yatırımcıların ve ülkenin sermaye piyasalarındaki ticari faaliyetlerini denetleyen ulusal öz-düzenleme kuruluşu olan Yatırım Sektörü Düzenleme Örgütünü (IIROC) oluşturmuştur. IIROC, üyeleri için iyi siber güvenlik uygulamaları rehberini yayımlamıştır [62].

Kanada Kamu Güvenliği Bakanlığı, son kullanıcıların çevrimiçi güvenliğini sağlamaya yönelik internet siteleri vasıtasıyla bilgilendirmeler de yapmaktadır. Bakanlık, ayrıca, siber güvenliğin önemi hakkında halkı bilgilendirmek için, her yıl Ekim ayında, uluslararası bilinirliği olan Siber Güvenlik Farkındalık Ayı etkinliklerini düzenlemektedir.

4.14. Rusya

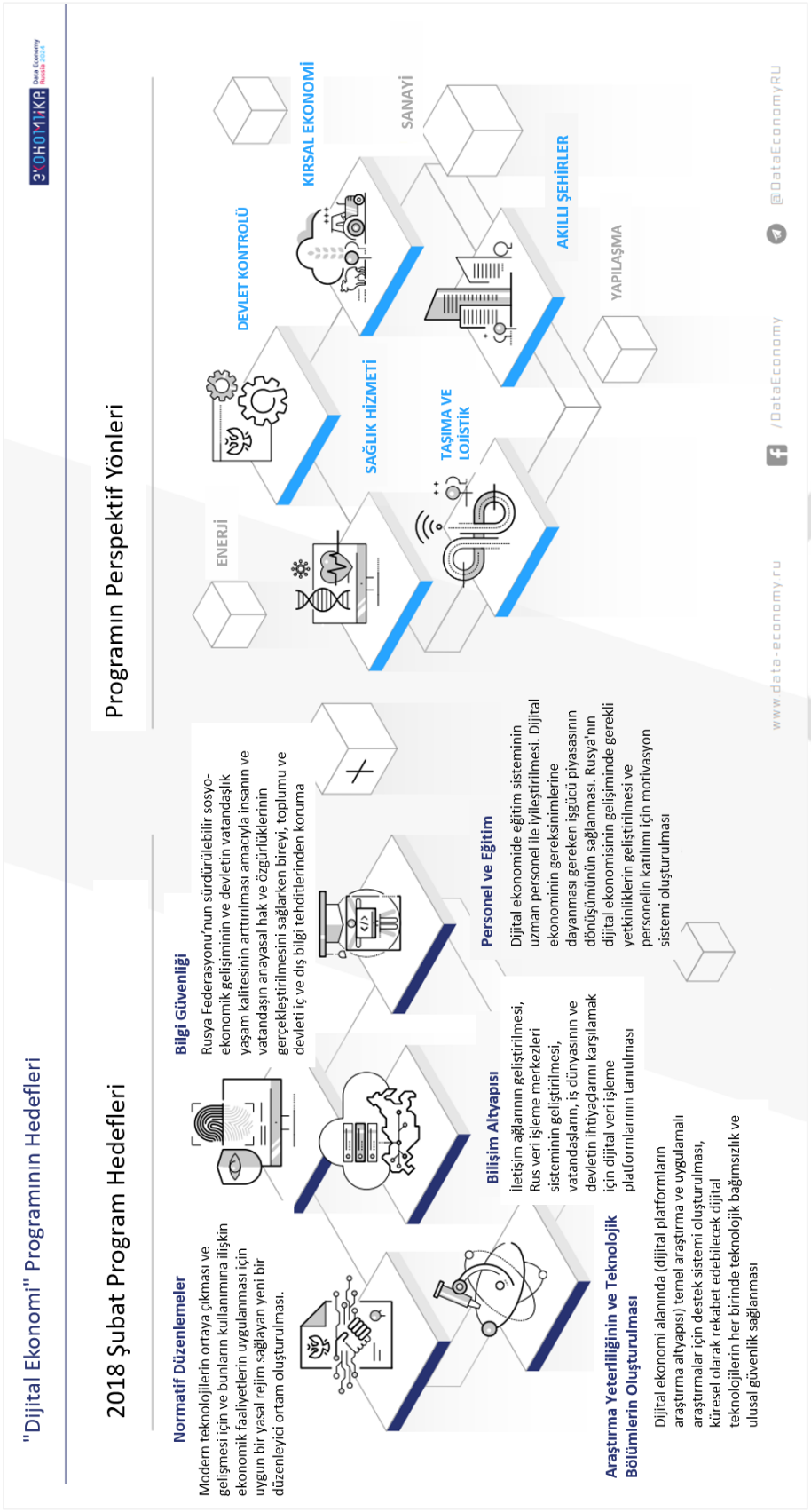
İletişim Merkezi Araştırma Enstitüsü (ZNIIS, Central Research Institute of Communications), siber güvenliğe ilişkin sorumlulukları olan kuruluşlar arasında yer almaktadır [5].

2017'de, Rusya Federasyonu Hükümeti, ülkenin dijital bir ekonomiye geçişi için şartlar yaratacak bir program geliştirmiş ve bu programı onaylamıştır. Programın etkin bir şekilde uygulanması, geliştirilmesi ve değerlendirilmesinde uzman ve iş dünyası toplulukları yer almaktadır. Bu topluluğun koordinasyonunu ise, Rus ileri teknoloji şirketleri tarafından oluşturulan ANO "Dijital Ekonomi" platformu sağlamaktadır. "Dijital Ekonomi" örgütü, Rusya Federasyonu'ndaki dijital ekonominin geliştirilmesine yönelik hizmetler sunmak ve bu alandaki sosyal açıdan önemli projeleri ve girişimleri desteklemenin yanı sıra dijital ekonomiyi oluşturan iş dünyası ile bilimsel ve eğitim kuruluşları, diğer topluluklar ve resmi makamlar arasındaki etkileşimi koordine etmek amacıyla kurulmuştur [135]. Dijital Ekonomi Program Yapısı [136] Şekil 4.14'te olduğu gibidir.



Şekil 4.14. Dijital ekonomi program yapısı [136]

Dijital Ekonomi programının hedefleri ise Şekil 4.15'de [137] olduğu gibidir.



Şekil 4.15. Rusya dijital ekonomi programı hedefleri [137]

FinTsERT, Bilgisayar saldırıları ile mücadele konusunda Rusya Federasyonu Merkez Bankası ile Kredi ve Finans Alanındaki Bilgisayar Saldırılarını İzleme ve Cevaplama Merkezi arasındaki iş birliği ilişkin anlaşmasına dayanan Bilgi Güvenliği Bölümü'nün yapısal bir birimidir [138].

Rus Federasyonu Bilgi Güvenliği Doktrini adıyla 2000 yılında yayımlanan belgede dört temel bileşeni detaylı olarak açıklanmıştır. Bu bileşenler: (1)Bireysel özgürlük ve güvenin önemi, (2)Kamudaki bilgi sistemlerinin güvenliği, (3)Modern bilgi sistemlerinin kullanımı ve (4)Bilgi ve iletişim sistemlerinin saldırılara karşı korunmasıdır [72].

2013 yılında Rusya Federasyonu, Dış Politika Konsepti'ni resmen kabul etmiştir. Rusya Federasyonu bu stratejilerde belirtilen alanlar doğrultusunda kendi ağ ve sistemlerinin yıllık denetimini gerçekleştirir [62].

2017'de "Rusya Federasyonu'nun Dijital Ekonomisi" programının uygulanmasına yönelik bir eylem planı, bilgi teknolojilerinin kullanımı ve yaşam kalitesini arttırmaya yönelik bir toplantıda kabul edilmiştir. Medeni Kanun ve Vergi Kanunları'nın yanı sıra kişisel veriler, iletişim sektörü ve diğer düzenleyici mevzuat hakkındaki yasaları kapsayan 50'den fazla yasal önlem paketinin hazırlanmasını gerektiren bu eylemlerin 2018-2019 yılları arasında yapılması planlanmaktadır [139].

4.15. Belirlenen Ülkelere Genel Bakış

Ülke incelemeleri sonucunda erişilen kaynaklar dahilinde oluşturulan genel tablo aşağıda yer almaktadır.

PARAMETRELER / ÜLKELER	Almanya	ABD	Avustralya	Birleşik Krallık	Çin Halk Cumhuriyeti
Politika Üreten Otoriteler, Koordinasyon Makamları	BMI, BBK, BT Planlama Konseyi, KITS	DHS- CS&C, NCCIC, ICI- IPC, CSC, DoS	Attorney- General's Department, AGIMO, ACMA, İletişim Bakanlığı	OCSIA, CESG, CPNI	Sanayi ve Bilgi Teknolojileri Bakanlığı, SASTIND, Çin Siber Uzay Yönetimi veya Siber Uzay İşleri Merkez Lider Ofisi
Siber Olayların Yönetimi ve Koordinasyonu	BSI, Enformasyon Altyapı Savunması İçin Ulusal Plan, Nationales Cyber- Abwehrzentrum	US- CERT, NCC, ICS- CERT, NCC, NICC, NRCC, Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi	CSOC, Siber Güvenlik Politikası ve Koordinasyon Komitesi, ACCS, ASD, CERT Avustralya	ACE- CSRs, Ulusal Siber Güvenlik Merkezi, Siber ve Hükümet Güvenlik Müdürlüğü, NCSP, CERT- UK	İnternet Güvenlik Acil Komuta Merkezi, Ajans Servis Merkezi, Tehdit Bilgi Raporlama Merkezi, CNCERT/CC
Siber Uzayda Siber İstihbarat ve Siber Savunma Amaçlı Çalışmalar	BfV	IC- IRC, NTOC, NIJTF, NSA, FBI, FCC	DCD, DSD	MCD, FCO, Government Security SecretariaT	Politbüro Daimi Komitesi, Danıştay ve Merkez Askeri Komisyonu, Kamu Güvenliği Bakanlığı, Devlet Güvenlik Bakanlığı
Siber güvenlik ve milli güvenlik ilişkisi	Almanya Ordusu	DOD, USCYBERCOM JOC, DISA, NTOC, DC3	ASIO, AFP, ACC	MI5, MoD	Kamu Güvenliği Bakanlığı, Devlet Güvenlik Bakanlığı
Kritik Altyapılara İlişkin Kurumlar	BBK, Federal Sivil Koruma ve Afetler Bürosu, KRITIS	FEMA, FISMA	TISN, CIPMA, CIAC		Kamu Güvenliği Bakanlığı
Siber Güvenlik Kümelenmeleri	Bonn Siber Güvenlik Kümesi		CSIRO Data61		
Yatırımcılar ile İlişkiler, Yerli Üretim		NCCoE– NIST	Joint Cyber Security Centres	CSOC	Çin İnternet Topluluğu
Sivil Toplum Kuruluşları ile İlişkiler ve Toplumsal Bilinçlendirme Çalışmaları	UP KRITIS	NCCoE– NIST	AISI, Ulusal eSmart Haftası		Çin İnternet Topluluğu
Uluslararası İş Birliği			Asya Pasifik Bilgisayarı Acil Müdahale Ekibi		
Akademik İş Birlikleri, Eğitim Sisteminde Siber Güvenliğe İlişkin Çalışmalar	BMBF, IT Security Research Programı	NCCoE– NIST, NIETP	Joint Cyber Security Centres, ACSC, ACSRC, İnternet Güvenliği Merkezi	CSOC, BIS	Çin Mühendislik Akademisi ve Çin Bilimler Akademisi, Çin İnternet Topluluğu, Askeri Bilimler Akademisi, PLA Bilgi Mühendisliği Üniversitesi
Belgelendirme ve Sertifikasyon	Alman Standartlar Enstitüsü (DIN), KoSIT	SANS Enstitüsü, NIST	IRAP	BSI, Birlikte Çalışabilirlik Standartları	CAICT, Çin İletişim Standartları Derneği, Ulusal Bilgi Güvenliği Standardizasyon Teknik Komitesi, Çin Standardizasyon İdaresi, Çin Elektronik Standardizasyon Enstitüsü

Şekil 4.16. Ülkelere ilişkin bilgiler-1

PARAMETRELER / ÜLKELER	Finlandiya	Fransa	Güney Kore	Hindistan	İtalya
Politika Üreten Otoriteler, Koordinasyon Makamları	Maliye Bakanlığı, Fin İletişim Düzenleme Kurumu, Güvenlik Komitesi	ANSSI	Güney Kore Ulusal İstihbarat Servisi, Kamu Yönetimi ve Güvenliği Bakanlığı, Kore İletişim Komisyonu	Elektronik ve Bilgi Teknolojileri Bakanlığı	Cumhurbaşkanlığı Cumhuriyet Güvenliği Komitesi , İletişim Güvence Kurumu , Başbakanlık Askeri Müşavirliği Ofisi - Siber Güvenlik Birimi , Dijital İtalya Ajansı
Siber Olayların Yönetimi ve Koordinasyonu	NCSC-FI, JYVSECTEC	Fransa CERT	Ulusal Siber Olaylara Müdahale Merkezi, Ulusal Bilgi İşlem ve Bilgi Ajansı, KN-CERT	NCCC, Ulusal Bilişim Merkezi, CERT-In, Ulusal Siber Olaylara Müdahale Ekibi	CERT-N, CERT-PA, CERT SPC, CERT Difesa
Siber Uzayda Siber İstihbarat ve Siber Savunma Amaçlı Çalışmalar	Savunma Bakanlığı	Savunma ve Ulusal Güvenlik Genel Sekreterliği	Ulusal İstiharat Servisi		Savunma Bakanlığı, Güvenlik İstihbarat Dairesi Başkanlığı , İtalyan Silahlı Kuvvetleri, DIS, AISI, AISE
Siber güvenlik ve milli güvenlik ilişkisi	Devlet Bilgi Güvenliği Yönetim Kurulu, VAHTI		İçişleri ve Güvenlik Bakanlığı , Kültür, Spor ve Turizm Bakanlığı, Ticaret, Sanayi ve Enerji Bakanlığı		Savunma Bakanlığı, Ekonomik Kalkınma Bakanlığı
Kritik Altyapılara İlişkin Kurumlar		ANSSI, Kritik Altyapılar Bilgi Koruması		Kritik Bilgi Altyapısını Koruma Merkezi, NCIPC	Kritik Altyapıların Korunması Ulusal Suçla Mücadele Bilgi Merkezi
Siber Güvenlik Kümelenmeleri			Kore Ticaret-Yatırım Teşviki		
Yatırımcılar ile İlişkiler, Yerli Üretim			Kore Ticaret-Yatırım Teşviki	Hindistan'ın Yazılım Teknolojisi Parkları, Kamu Alımları (Hindistan'da Yapma Tercihi)	
Sivil Toplum Kuruluşları ile İlişkiler ve Toplumsal Bilinçlendirme Çalışmaları					
Uluslararası İş Birliği	Nordik Ulusal CERT		Kore Ticaret-Yatırım Teşviki		
Akademik İş Birlikleri, Eğitim Sisteminde Siber Güvenliğe İlişkin Çalışmalar	JYVSECTEC				
Belgelendirme ve Sertifikasyon		Fransız Standardizasyon Birliği		Standardizasyon, Test ve Kalite Belgelendirme Müdürlüğü	

Şekil 4.17. Ülkelere ilişkin bilgiler-2

PARAMETRELER / ÜLKELER	İspanya	Japonya	Kanada	Rusya
Politika Üreten Otoriteler, Koordinasyon Makamları	Ulusal Güvenlik Bakanlığı, Ulusal Güvenlik Konseyi , Ulusal Siber Güvenlik Konseyi, Ulusal Siber Güvenlik Enstitüsü (INCIBE)	Ulusal Bilgi Güvenliği Merkezi, IPA/ISEC Bilgi Teknolojileri Tanıtım Ajansı	Kanada Kamu Güvenliği (Public Safety Canada),	İletişim Merkezi Araştırma Enstitüs0, ü, Dijital Ekonomi" örgütü
Siber Olayların Yönetimi ve Koordinasyonu	CSIRT.es , CERT-SI, INCIBE-Cert, CCN-CERT, ESPCERTDEF	Ulusal İleri Endüstriyel Bilim ve Teknoloji Enstitüsü, Ulusal Bilgi ve İletişim Teknolojileri Enstitüsü, JPCERT/CC	Kanada Siber Olay Müdahale Merkezi, Akıllı Siber Güvenlik Ağı	FinTsERT
Siber Uzayda Siber İstihbarat ve Siber Savunma Amaçlı Çalışmalar	Ulusal İstihbarat Merkezi		CSEC, Kanada Güvenlik İstihbarat Servisi	Bilgi Güvenlik Doktrini
Siber güvenlik ve milli güvenlik ilişkisi	Ortak Siber Komutanlık, İspanya Veri Koruma Ajansı		Savunma AR-GE Kanada, Kanada Kraliyet Atlı Polisi	Rusya Federasyonu Dış Politika Konsepti
Kritik Altyapılara İlişkin Kurumlar	Ulusal Altyapıların ve Siber Güvenliği Koruma Merkezi , Ulusal Siber Güvenlik Enstitüsü (INCIBE)	NISC-CEPTOAR		
Siber Güvenlik Kümelenmeleri			Kanada Endüstrisi	
Yatırımcılar ile İlişkiler, Yerli Üretim	Ulusal Siber Güvenlik Konseyi			
Sivil Toplum Kuruluşları ile İlişkiler ve Toplumsal Bilinçlendirme Çalışmaları	Ulusal Siber Güvenlik Konseyi		Siber Güvenlik Farkındalık Ayı	
Uluslararası İş Birliği		Asya Pasifik Bilgisayar Acil Durum Müdahale Ekibi, Japan –ASEAN Güvenlik Ortaklığı , Uluslararası İş birliği Yoluyla Siber Saldırılara Karşı Proaktif Yanıt Sistemi		
Akademik İş Birlikleri, Eğitim Sisteminde Siber Güvenliğe İlişkin Çalışmalar	İspanya Siber Güvenlik Araştırmaları Mükemmeliyet Merkezi			
Belgelendirme ve Sertifikasyon			Yatırım Sektörü Düzenleme Örgütü	

Şekil 4.18. Ülkelere ilişkin bilgiler-3

5. 2016-2019 ULUSAL SİBER GÜVENLİK STRATEJİSİ'NDE YER ALAN KURUMLARIN SİBER GÜVENLİK EKOSİSTEMİNİN GELİŞTİRİLMESİ AÇISINDAN DEĞERLENDİRİLMESİ

Ülkemizde siber güvenlik ve ilgili konularda sorumlu olmak üzere Siber Güvenlik Kurulu kurulmuştur. Siber Güvenlik Kurulu'nun, Kanun'la belirlenen ve aşağıda detayları açıklanan çeşitli kamu kurumları ile birlikte görevlerini yürütmesi planlanmıştır. 703 nolu KHK ile kurulun görevleri iptal edilmiştir. Bu bölümde, 703 nolu KHK'nın yayımlanmasına değin ülkemizde siber güvenlikten sorumlu makam olarak görev ifa eden Siber Güvenlik Kurulu'nun yapısı incelenmiştir. Kurul'da yer alan kurumların mevzuatları göz önünde bulundurularak bu kurumların siber güvenlik konusu ile bağlantıları irdelenmiştir.

5.1. Siber Güvenlik Kurulu

Siber Güvenlik Kurulu 2012 yılında kurulmuştur. Kurul'un Ulaştırma ve Altyapı Bakanlığı başkanlığında toplanmasına karar verilmiştir. Siber güvenlik konusunda çalışmaların yürütülmesi, plan ve politikaların geliştirilmesi kurulun görevleri olarak belirlenmiştir. Karara göre, kurul çalışma grupları ve kendi içinde alt kurullar oluşturabilme yetkisine haiz olarak tanımlanmıştır [50].

Siber güvenliğim sağlanması ve siber güvenlik politikalarının geliştirilmesi anlamında öncü rol oynayan resmi bir oluşumun kurulması, konunun askeri boyutu, siyasi politikalara yön verebilme özelliği, milli istihbarata katkısı vb. durumlar göz önüne alındığında yeterli olmamasına rağmen, ülkemiz açısından önemli bir adımdır.

Ancak uygulamada yetersizliklerin olduğu geçen yıllar içerisinde gözlenmiştir. Çalışmanın ilerleyen bölümlerinde açıklanacağı üzere, siber güvenlik konusunda koordinasyon makamının yapacağı çalışmalar oldukça önemlidir ve yaptırım kabiliyetinin yüksekliği politika geliştirme düzeyini ve politikaların uygulanma derecesini belirleyen bir unsurdur.

703 sayılı KHK ile Siber Güvenlik Kurulu sekretarya işlemlerinin artık Ulaştırma ve Altyapı Bakanlığı tarafından yürütülmeyeceği ve icra kurulunun iptal edildiği kesinleşmiştir. Bu bağlamda şu an ülkemizde siber güvenliğin yönetimi konusunda önemli büyüklükte bir eksiklik bulunmaktadır.

5.1.1. Ulaştırma ve altyapı bakanlığı

Ulaştırma ve Altyapı Bakanlık'ının kurulması; 6/4/2011 tarihli ve 6223 sayılı Kanun'un verdiği yetkiye dayanılarak, Bakanlar Kurulu'nca 26/9/2011 tarihinde kararlaştırılmıştır. İlgili 655 sayılı KHK 1 Kasım 2011'de resmi gazetede yayımlanmıştır. Bakanlık bünyesinde; 20 hizmet biriminden oluşan Merkez Teşkilatı, 13 bölge müdürlüğünden oluşan Taşra Teşkilatı, 3 Denizdibi Tarama Başmühendislik birimi ve 70 Liman Başkanlığı bulunmaktadır.

Bakanlık bünyesinde Haberleşme Genel Müdürlüğü siber güvenliğe ilişkin konularda iş süreçlerinin yürütülmesinden sorumlu tutulmuştur. Bakanlar Kurulu tarafından 2012'de kurulan Siber Güvenlik Kurulun'na başkanlık, Ulaştırma ve Altyapı Bakanlığı tarafından yapılmıştır. Siber güvenlik konusundaki sorumluklar, Ulaştırma ve Altyapı Bakanlığı'nın Haberleşme Genel Müdürlüğü'ne bağlı Siber Güvenlik Daire Başkanlığı tarafından yerine getirildiği gözlenmiştir.

Haberleşme ile ilgili süreçlerin yürütülmesi ve yönetilmesine ilişkin görevleri bulunan Haberleşme Genel Müdürlüğü, siber güvenlik konusundaki sorumlulukları Bakanlar Kurulu kararıyla yerine getirmiştir. Ulaştırma ve Altyapı Bakanlığı'nın resmi internet sitesinde Siber Güvenlik Kurulu ve Haberleşme Genel Müdürlüğü'nün siber güvenlik konusundaki organizasyonu Şekil 5.1'de olduğu gibidir.

Şekil 5.1. Ulusal siber güvenlik organizasyonu [140]

Ulaştırma ve Altyapı Bakanlığı, siber güvenlik eylem planları doğrultusunda kurulan SOME'ler ile ilgili "Kurumsal SOME Kurulum ve Yönetim Rehberi" bilgilendirme dokümanlarını 2014'te yayımlamıştır. Bu rehber kamu kuruluşlarının ve özel sektörün, almış oldukları siber güvenlik önlemlerini ölçebilmelerine katkı sağlamak amacıyla oluşturulmuştur. Çeşitli dönemlerde yaygınlaşan CryptoLocker vb. virüsler ile ilgili bilgi notları da Bakanlık resmi internet sitesinde yayımlanmıştır. Ulaştırma ve Altyapı Bakanlığı'nın yayımladığı siber güvenlik eylem planlarında belirtilen sorumluluklar doğrultusunda TÜBİTAK SGE tarafından bilgi güvenliğine ilişkin temel bazı kriterler belirlenerek, kamu kurumlarına tebliğ edilmiştir. Bu tebliğ ile kurumların uyması gereken temel siber güvenlik ilkeleri vurgulanmıştır. Benzer amaçlarla, TÜBİTAK SGE tarafından hazırlanan temel yazılım güvenliği konularına ilişkin kurallar belgesi kamu kurumlarına tebliğ edilmiştir. Bu sayede yazılım projelerinde faydalanılabilecek temel güvenlik kuralları oluşturulmuştur.

Ulaştırma ve Altyapı Bakanlığı, ülkemizde mevcut mevzuata göre siber güvenlik konusunda ilk görev sahibi kamu kuruluşudur. Diğer kamu kurumları ile iletişimi ve koordinasyonu Siber Güvenlik Kurulu eliyle yürütmüştür. Ancak, siber istihbaratın ve askeri boyutta siber savunmanın hayati önem taşıdığı, dünya siyasi politikalarının şekillenmesinde siber

güvenlik konusunun ciddi bir rolü olduğu göz önünde bulundurulduğunda, Bakanlık tarafından yapılan çalışmaların yetersiz kalabileceği gözlenmektedir.

5.1.2. Dışişleri bakanlığı

6004 sayılı Kanun ile Dışişleri Bakanlığı'nın kuruluş, görev ve yetkilerine ilişkin esaslar belirlenmiştir. Bakanlık'ın, Merkez Teşkilatı, Yurtdışı Temsilcilikleri'nden oluşmaktadır. İlgili Kanun'da Bakanlık'ın görevleri arasında yer alan maddeler incelendiğinde; teknik konularda uluslararası iş birliği noktasında Bakanlık'ın sorumlulukları bulunmaktadır. Strateji ve Bütçe Başkanlığı'nın yayımladığı 2015-2018 Bilgi Toplumu Stratejisi Eylem Planı'nda uluslararası boyutta bağlantıların ihtiyaç duyulan konularda Dışişleri Bakanlığı iş birliği yapılacak kurumlar arasında yer almaktadır.

Teknolojik küreselleşmenin neden olacağı olumsuzluklara karşı uluslararası iş birliğinin, ülke politikalarında önemli yere sahip olduğu gerçeği, siber güvenlik konusunda Dışişleri Bakanlığı'nın izleyeceği politikalarda güncel teknolojiye bağımlı hareket etmesini zorunlu kılmaktadır. Dünya ülkelerinin güncel siber politikalarının takibi ve ilgili kamu kurumları ile yeni bilgilerin paylaşımı siber istikrar noktasında önem arz etmektedir. Yeni gelişmelere ayak uydurabilmek için öncelikle bu gelişmelerden haberdar olmak gereklidir. Bu amaçla, teknoloji iş birlikteliklerinin sağlanmasında Dışişleri Bakanlığı'nın izleyeceği siyasi politikalar, siber tehditlere karşı savunmada güç dengelerini belirleyecektir.

Bakanlık'ın Temel Dış Politika Konuları arasında yer alan "Silahların Kontrolü ve Silahsızlanma" başlığı incelendiğinde siber silahsızlanma kavramına yer verilmediği görülmektedir. Dışişleri Bakanlığı'nın siber uzaya bakışında teknolojik gelişmelere dair eksiklik göze çarpmaktadır. Bakanlık tarafından, asimetrik tehditlere karşı müttefik ülkelerle gerekli sözleşmelerin imzalanmasına yönelik gerekli çalışmaların yürütülmesi, halihazırda üyesi olduğumuz uluslararası oluşumların belirlediği hukuki sınırlar göz önüne alınarak değerlendirilmelidir. Bakanlık resmi internet sitesinde konuyla ilgili olarak "*Ülkemiz halihazırda, askeri eğitim, teknik ve bilimsel konularda ve savunma endüstrisi iş birliği alanlarında Müttefik ve dost ülkelerle pek çok ikili anlaşmalar imzalamıştır. Bu tarz iş birliği mekanizmaları, NATO üyeleriyle ve Balkanlar, Ortadoğu, Güney Akdeniz, Kuzey Afrika, Orta ve Uzak Doğu Asya ve Güney Amerika'da yer alan önemli sayıdaki ülkelerle geliştirilmiştir. Askeri Eğitim Anlaşmaları üçüncü taraflara karşı olmayıp, birlikte çalışabilirliğin geliştirilmesini teminen güvenlik alanında iş birliği yapılmasını*

amaçlamaktadır." ifadesine yer verilmiştir. Bu ifadeden anlaşılan, özellikle vurgulanmasa dahi teknik konularda siber tehditlere karşı müttefik ülkelerle bir iş birliktelik halinde olunduğudur, ancak siber tehditler ve siber savunma özelinde herhangi bir anlaşmanın vurgulanmadığı gözlenmektedir.

Buna karşın, Dışişleri Bakanlığı tarafından hazırlanan ve Dışişleri Komisyonu'nun esas, Adalet Komisyonu ve Bayındırlık, İmar, Ulaştırma ve Turizm Komisyonu'nun tali komisyon olarak yaptığı çalışmalar neticesinde oluşturulan rapor gerekçe gösterilerek 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun'un kabul edilmiştir. Avrupa Konseyi tarafından 23 Kasım 2001'de kabul edilen Siber Suçlar Sözleşmesi, ülkemiz tarafından 10 Kasım 2010 tarihinde Strazburg'da imzalanmış, 20 Aralık 2012'de tamamlanan Dışişleri Bakanlığı koordinasyonundaki komisyon raporları gerekçesiyle 22 Nisan 2014 tarihinde TBMM Genel Kurulu tarafından, 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun kabul edilmiştir.

Tarihsel süreç irdelendiğinde, 2004 yılında evrensel bir sözleşme niteliğinde yürürlüğe giren bu sözleşme, ülkemizde maalesef 2012 yılında incelenip raporlanarak, 2014 yılında onaylanmıştır. Siber terörizm ile mücadelede uluslararası ilişkiler, yasadışı eylemlerde bulunan kişi ya da kişilerin tespitinde kilit rol oynamaktadır. Dış ilişkilerin geliştirilmesinde, siber güvenlik alanında diğer ülkelerle ilişkilerin geliştirilmesi zorunlu hale gelmiştir.

5.1.3. İçişleri bakanlığı

İçişleri Bakanlığı'nın görevleri 3152 sayılı Kanun'da belirtilmiştir. Kolluk kuvvetlerinin İçişleri Bakanlığı'na bağlı olması ve istihbarat kurumu olarak değerlendirilebilecek kurumların Bakanlık organizasyonunda yer alması, siber suçlarla mücadelenin sağlanmasında Bakanlık görevleri olduğunun bir göstergesidir. Devletin taşradaki temsilcisi olan Valilikler de İçişleri Bakanlığı'na bağlıdır. Öte yandan İçişleri Bakanlığı, Belediyeler, İl Özel İdareleri, Birlikler ve Köyler'den oluşan mahalli idareler üzerinde vesayet yetkisine sahiptir, mahalli idarelerin iş ve işleyişine yönelik Bakanlık'ın görev ve sorumlulukları mevcuttur. Bu bağlantılar İçişleri Bakanlığı'na, Valilikler ve mahalli idareler eliyle siber güvenlik konusunda halkın bilinçlendirilmesi faaliyetlerinin yürütülmesi fırsatını sunmaktadır. İçişleri Bakanlığı teşkilat şemasının devlet yapılanmasında ana omurga olan

kurumları barındırması siber güvenlik yönünden görev ve sorumluluklarını arttırmakta, bu alanda Bakanlık tarafından yapılabilecek ülke içi işlerin alanını genişletmektedir.

Bakanlık bünyesinde yardımcı birimler arasında yer alan Afet ve Acil Durum Yönetim Merkezi resmi internet sitesinde terör olaylarının çalışma alanı olarak belirtildiği, ancak siber terörizm konusuna değinilmediği gözlenmektedir.

Bakanlık, yurdun iç güvenliği ve asayişini, kamu düzenini ve genel ahlakını, Anayasada yazılı hak ve hürriyetlerini kendisine bağlı Emniyet Genel Müdürlüğü eliyle korumaktadır. İnternet, faydalarının yanında suçluların kolaylıkla yasadışı faaliyetler yürütebileceği bir alan konumundadır. Özellikle sosyal medya aracılığıyla art niyetli kullanıcılar yurdun iç güvenliği ve asayişini tehdit eden riskleri arttırmakta, kamu düzenini ve genel ahlakı zedeleyici içeriklerde paylaşımlar internet sitelerinde kolaylıkla kitlelere ulaştırılabilmektedir. Anayasada ve diğer yasalarda belirtilen birçok kişisel hak ve hürriyet ihlal edilebilmektedir. Bu gibi suçların takibinin yapılması, hukuki makamlara yönlendirilmesi, Emniyet Genel Müdürlüğü eliyle yürütülen çalışmalar neticesinde İçişleri Bakanlığı'nın çalışma kapsamını oluşturmaktadır.

Siber suçların soruşturulması ve dijital kanıtların elde edilmesi, değerlendirilmesi amacıyla Emniyet Genel Müdürlüğü bünyesinde Bilişim Suçlarıyla Mücadele Daire Başkanlığı kurulmuştur. Daire başkanlığı merkez ve taşra arasında koordinasyon olmadan yürütülen çalışmaları azaltmayı da hedeflemiştir. Bu sayede maddi kayıpların ve iş gücü kayıplarının azaltılması amaçlanmıştır. Daire adı, daha sonra Siber Suçlarla Mücadele Daire Başkanlığı olarak değiştirilmiştir. Ülkemizde özellikle sosyal medya hesaplarının çalınması gibi bireysel siber saldırılar karşısında ilgili daire vatandaşların sıklıkla muhatabı konumundadır [141].

2015-2018 Bilgi Toplumu Stratejisi Eylem Planı'nda "Kamu Hizmetlerinde Kullanıcı Odaklılık ve Etkinlik" ekseninde "Kent Yönetimi Bilgi Sistemi Geliştirilmesi" başlıklı eylem planı İçişleri Bakanlığı sorumluğuna verilmiştir. Bu sorumluluk dışında diğer eylemler arasında ilgili kuruluş olarak yer aldığı eylemler de mevcuttur.

Özetle, İçişleri Bakanlığı ve Bakanlık'a bağlı diğer kamu kurumlarının siber istihbarat, siber terörizm, dış ilişkiler, valilikler ve belediyeler vb. eliyle, siber suçların tespiti, önlenmesi,

kamu düzeninin sağlanması ve toplumsal bilinci arttırmaya yönelik faaliyetlerin gerçekleştirilmesi gibi konularda geniş yetki alanı bulunmaktadır.

5.1.4. Milli savunma bakanlığı

1325 sayılı Kanun ile Milli Savunma Bakanlığı'nın görevleri ve teşkilat yapısı açıklanmıştır. Kanun'da "*Kara, Deniz ve Hava Kuvvetleri Komutanlıkları Milli Savunma Bakanına bağlıdır. Bu Kanuna aykırı olmayan ve diğer kanunlarla Genelkurmay Başkanlığı'na verilen görev ve yetkilere ilişkin hükümler saklıdır.*" ifadesi yer almaktadır. Mili Savunma Bakanlığı Genel Kurmay Başkanlığı'na verilen diğer özel yetkiler haricinde kara deniz ve hava kuvvetlerinin yönetimini sağlamaktadır. Bakanlık, siber uzayda yaşanan saldırılara, karşı cevapların üretilmesi noktasında kritik konumdadır.

Teşkilat yapısında askeri ve sivil müsteşar yardımcıları, genel müdürlükler, daire başkanlıkları barındırması bakımından askeri ve sivil otoritelerin yakın irtibat kurabilmeleri mümkündür. Bu iletişim yapısının siber güvenlik konularında proje üretmeye olanak tanıyacak bir ortam olabileceği görülmektedir.

Savunma sistemlerinin standardizasyon faaliyetleri uluslararası iş birlikleri kapsamında Bakanlık tarafından yürütülmektedir. Bakanlık, savunma sanayi güvenliği konusunda ülkeler arasında askeri tasnifli bilgi paylaşımları yapmaktadır. Savunma Sanayi Müsteşarlığı adıyla, Milli Savunma Bakanlığı'na bağlı ve tüzel kişiliği haiz kuruluş olarak görev yapmakta iken, siber güvenliğe ilişkin önemli çalışmalar öncülük eden Savunma Sanayii Müsteşarlığı'nın ismi, 2018 yılı devletin yeniden yapılanması sürecinde çıkarılan kanunlarla Savunma Sanayi Başkanlığı olarak değiştirilmiş olup Cumhurbaşkanlığı makamına bağlanmıştır. Başkanlık'ın siber güvenlik kümelenmelerine yönelik çalışmalarına hız verdiği görülmektedir.

Siber güvenliğe ilişkin çalışmalar yürüten Başkanlık birimleri arasında Siber Güvenlik ve Elektronik Harp Sistemleri Daire Başkanlığı bulunmaktadır. Savunma Sanayi Başkanlığı Teknoloji Yönetim Stratejisi 2011-2016 belgesinde teknolojik üstünlüğün diğer alanlarda rekabeti sağlayıcı esas unsurlar arasında olduğu vurgulanmaktadır. Savunma Sanayi Başkanlığı'nın bu belgesinde askeri alanda güç göstergesi odaklarının teknoloji ağırlıklı olarak yön değiştirdiği ifade edilmiştir. Kurum bünyesinde çalışmaların, evrim geçiren askeri yapılanmalara uygun olarak değişim ve dönüşüm sağlamanın mutlak gerekliliği göz

önünde bulundurularak yapıldığı vurgulanmaktadır. İlgili belgede teknoloji ve siber güvenlik konusunda yatırımlar yapılmasına önem verildiği gözlenmektedir.

TSK'da teknik altyapının iyileştirilmesi, stratejik hedefler arasında yer almaktadır. S Savunma Sanayi Başkanlığı'nın 2016 yılına kadar geçerli olan strateji belgesinde, Mükemmeliyet Ağları Projesiyle, oluşturulan MÜKNET Çalışma Grubu'nun, teknik gelişmelerin sağlanması konusunda çalışmalar yapacağı belirtilmiştir. MÜKNET Alanları arasında "Elektronik Harp" alanının olması dikkat çekicidir. Bu alanda, siber güvenliğe ilişkin çalışmaları da içerebilecek, RF teknolojileri ve elektronik altyapılar ve haberleşme sistemleri kullanılarak gerçekleştirilen yanıltma, maskeleme çözümleri ile ilgili girişimlerin sorumluluk kapsamında olduğu ifade edilmiştir. Komuta, Kontrol ve Bilgi Teknolojileri (KKBT) kapsamında ise öncelikli yürütülmesi gereken çalışmalar arasında "Siber Savunma, Strateji ve Taktik Geliştirme" başlığı dikkat çekmektedir.

Savunma Sanayi Başkanlığı resmi internet sitesinde "Siber Güvenlik ve Koruma" başlığı altında "Petrol ve Doğalgaz Boru Hatlarının Güvenliği Projesi" ve "TSK Siber Savunma Merkezi Projesi" projelerinin yürütüldüğü görülmektedir. 2017 yılı Şubat ayı itibariyle Ulaştırma ve Altyapı Bakanlığı ve MSB arasında Siber Güvenlik İş Birliği Protokolü imzalanmıştır. Siber güvenlik konusunda sorumlu merci olan Ulaştırma ve Altyapı Bakanlığı, bu protokol ile MSB'nin ve ilgili, ilişkili kuruluşlarının yetkinlikleri ve tecrübelerinden, imkanlarından faydalanmayı amaçlamaktadır. Bu protokolün siber uzayda milli bütünlüğün korunması ve tehditlere karşı siber savunmanın yapılmasına katkı sağlaması ön görülmektedir. Bu protokole ek olarak aynı tarihte Ulaştırma ve Altyapı Bakanlığı Haberleşme Genel Müdürlüğü ile Türk Silahlı Kuvvetlerini Güçlendirme Vakfı'nın bir kuruluşu konumundaki HAVELSAN arasında siber güvenliğe ilişkin, birlikte yürütülecek çalışmalara yönelik alt protokol imzalanmıştır.

5.1.5. Kamu düzeni ve güvenliği müsteşarlığı

Kurum İçişleri Bakanlığı'na bağlıdır. Terörle mücadele konusunda koordinasyon sağlamak, politika geliştirmek amacıyla kurulan bu kurum çalışma esasları bakımından incelendiğinde mahalli istihbarat örgütü olarak tanımlanmaktadır. Kuruluş operasyonel görevlere sahip değildir [142].

Müsteşarlık, bilgi edinme yoluyla siber terörizm konusunda talep edilen bilgi talebine muhatap olarak Ulaştırma ve Altyapı Bakanlığı'yi göstermiştir. Bu anlamda müsteşarlığın siber terörizm ile mücadele konusunda kurumlar arası koordinasyon dışında herhangi bir çalışma yürütmediği düşünülmektedir.

2018 yılı devlet yapılanmasında yapılan değişiklikler neticesinde 703 nolu KHK ile kurum kapatılarak bütün yetkileri İçişleri Bakanlığı'na devredilmiştir.

5.1.6. Milli istihbarat teşkilatı başkanlığı

MİT, 644 sayılı Milli İstihbarat Teşkilatı Kanunu'yla "Başbakanlığa" bağlı olarak kurulmuş olup devletin birincil istihbarat kaynağıdır [143]. Kurum adı 2018 yılı itibariyle Milli İstihbarat Teşkilatı Başkanlığı olarak değiştirilerek Cumhurbaşkanlığı makamına bağlanmıştır.

MİT yapılanmasında "Elektronik Teknik İstihbarat Başkanlığı" siber tehditlere karşı çalışmalar yürütmektedir. Başkanlık, haberleşme sistemleri kullanılarak gerçekleştirilebilecek terörist faaliyetlerin önüne geçebilmek adına iletişimin tespiti, dinlenmesi, kaydedilmesi, ses ve görüntü analizlerinin yapılması gibi görevleri yerine getirmektedir. MİT yapılanmasında yer alan "İstihbarata Karşı Koyma Daire Başkanlığı" yabancı devletlerin casusluk faaliyetlerinin tespiti ve engellenmesiyle görevlidir. MİT yapılanmasında yer alan diğer başkanlıklar ile birlikte bu başkanlıklar siber güvenliğin sağlanmasında siber istihbarat bilgilerini edinme ve karşı önlemler alabilecek siyasi politikaların geliştirilmesinde önemli role sahiptir.

Ülke siyasetini belirleyiciliği bakımından güçlü konumda olan MİT, siber güvenlik alanında özellikle istihbarat noktasında yön verici olabilmektedir. Milli teknoloji yatırımlarının yapılması amacıyla ülke içinde atılacak önemli adımlar, yabancı ülkelerin ve yabancı ülke istihbarat kaynaklarının takip ettiği konular arasında yer almaktadır. Yenilik ve geliştirme çalışmalarının önünü kesmeyi hedefleyen girişimleri engelleyebilmek noktasında MİT'in çalışmaları değerlidir. Ayrıca siber uzayda milli bütünlüğü bozmaya yönelik içten veya dıştan gelebilecek tehditlerin önceden tespiti ve ilgili kurumların bu konu ile ilgili zamanında bilgilendirilmesini kapsayan siber istihbaratın edinilmesi noktasında MİT Başkanlığı kilit kurum konumundadır.

5.1.7. Genelkurmay başkanlığı

Genelkurmay Başkanlığı, ülke güvenliğinin sağlanması, sınırların güvenli bir şekilde korunmasının temini gibi temel görevlerin yanında siber uzayda güvenliğin sağlanması noktasında sorumluluklara da sahiptir. Askeri teçhizatların bilgi teknolojileri kaynakları ile donatılmış durumda olması, diğer çalışma alanlarında olduğu gibi, askeri alanda da bilgi ve tecrübe sahibi personel ile siber alanı kapsayacak politikaları içeren çalışmaların yürütülmesini zorunlu kılmaktadır. TSK; Kara Kuvvetleri Komutanlığı, Deniz Kuvvetleri Komutanlığı, Hava Kuvvetleri Komutanlığı, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı'ndan oluşmaktadır. Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı sefer dönemleri haricinde İçişleri Bakanlığı'na bağlı olarak görev yapmaktadır [144].

TSK bünyesinde, siber olaylarda savunma mekanizması olarak çalışması amacıyla "Siber Savunma Komutanlığı" kurulmuştur. Siber tehditlere karşı savunmanın, askeri disiplin çerçevesinde yürütülmesi önemli bir avantajdır. Ancak başarılı bir savunma mekanizmasının yürütülmesi için diğer kamu kurumlarıyla iş birliği ve koordinasyon şarttır.

5.1.8. Bilgi teknolojileri ve iletişim kurumu

Kurum ana hizmet birimleri ve taşra teşkilatından oluşmaktadır. Kurumun elektronik ve haberleşme, bilgi teknolojileri ve posta sektöründe görevleri vardır. Telekomünikasyon sektöründe uluslararası kuruluşların faaliyetlerine de katılmaktadır. 2813 sayılı Kanun ile kurulan BTK, Ulaştırma ve Altyapı Bakanlığı ile ilişkili düzenleyici ve denetleyici bir kurumdur. Elektronik ve haberleşme sektöründe kilit kurum konumundadır.

Siber saldırıların tespiti ve bu saldırıların bertaraf edilmesi görevlerini yerine getirmesi amacıyla BTK bünyesinde çalışan USOM (TR-CERT) kurulmuştur [145]. BTK, USOM-SOME yapılanmaları ile ilgili, siber güvenlik ihbarları, kurumsal bilinçlendirmelerin arttırılması ve gelecekten beklentiler konusunda fikir paylaşımları yapılmasına olanak tanıyan ikinci istişare toplantısını Ocak 2017'de düzenlemiştir. İlgili olduğu sektörü denetlemeye ve düzenlemeye yetkili kurum olması siber tehditlere karşı kurum ve kuruluşların uygulayabileceği siber güvenlik politikalarını belirlemeden öncü olabilecek konumdadır. Kurum elektronik haberleşme sektöründe yetkilendirmeler yapmaktadır.

TİB görev ve yetkilerinin 671 sayılı KHK ile BTK'ya devri neticesinde, daha önceden TİB'in yerine getirdiği çeşitli alanlarda ihbarları değerlendirmektedir. İnternet üzerinden, 5651 sayılı yasa kapsamında, "*İntihara Yönlendirme, Çocukların Cinsel İstismarı, Uyuşturucu veya Uyarıcı Madde Kullanılmasını Kolaylaştırma, Sağlık için Tehlikeli Madde Temini, Müstehcenlik, Fuhuş, Kumar Oynanması için Yer ve İmkân Sağlama, Atatürk Aleyhine İşlenen Suçlar*" başlıklarıyla ilgili ihbarlar BTK tarafından değerlendirilmektedir. Bu anlamda kurum, siber güvenlik ve siber suçlar konusunda ihbar yolunun açık olduğu kolluk kuvvetlerine ek mekanizmayı barındırmaktadır.

5.1.9. Türkiye bilimsel ve teknolojik araştırma kurumu

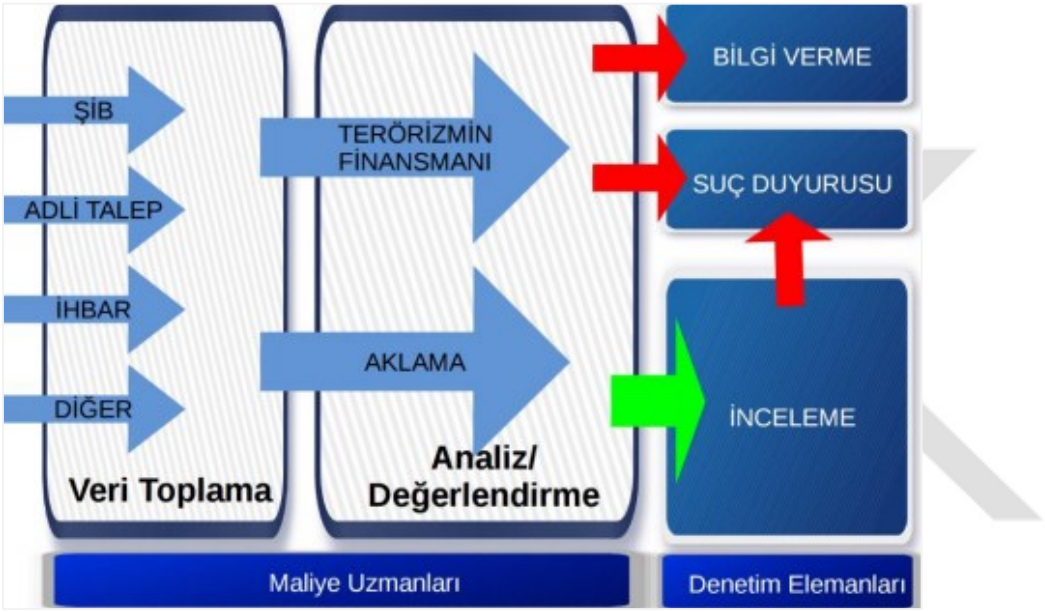
278 sayılı Kanun ile kurulan TÜBİTAK, en temelde bilimsel ve teknik gelişmeler göz önünde bulundurularak toplumsal bilinci arttırmak dahil, bilimsel ve teknolojik politikalar geliştirmek, bu politikaların uygulanması için kurum kuruluşlar ile iş birliği yapmak, araştırma geliştirme faaliyetleri yapmak suretiyle bilim ve teknolojide rekabet etme kabiliyetinin artmasını sağlamak gibi çeşitli görevlere sahiptir [146]. Sanayi ve Teknoloji Bakanlığı'na (eski adıyla Bilim, Sanayi ve Teknoloji Bakanlığı'na) bağlı olarak kurulmuştur.

Geniş kapsamlı bir görev skalasına sahiptir. Bilimsel ve teknolojik araştırmalara ilişkin çalışmaların yürütülmesi ve koordinasyonunu TÜBİTAK sağlamaktadır. Hem kamu kurumlarının hem özel sektörün teknik gelişimlerini daha iyi seviyelere ulaştırmak amacıyla teşvik ve destek sistemleri geliştirmek kurumun görevleri arasındadır. Uluslararası iş birlikleri ile bilimsel ve teknolojik araştırmalarda rol sahibidir, görev alanındaki konularda ulusal ve uluslararası bilimsel toplantılar düzenlemek, gerçekleştirilen toplantılara katılmak ile sorumludur. Bilim adamlarının, araştırmacıların yetiştirilmesi konusunda da kurumun görevleri bulunmaktadır. Bütününe bakıldığında teknik her türlü gelişmenin takibi ve uygulanmasına yönelik sorumluluk, TÜBİTAK'ın çalışmaları kapsamındadır.

TÜBİTAK, bünyesinde bulunan araştırma merkezleri yoluyla siber güvenlik alanında etkin rol oynayabilecek bir kurumdur. Bu anlamda; Ulaştırma ve Altyapı Bakanlığı'nın yayımladığı siber güvenlik eylem planlarında belirtilen sorumluluklar doğrultusunda birçok çalışmanın TÜBİTAK önderliğinde yürütüldüğü görülmektedir.

5.1.10. Mali suçlar araştırma kurulu

Doğrudan Hazine ve Maliye Bakanlığı'na bağlı olarak çalışır. Suç gelirlerinin aklanmasını önlemek, terörün finansmanının önlenmesine yönelik çalışmalar yapmak MASAK'ın temel görevleridir. Bu görevler kapsamında ilgili olayların değerlendirilmesi, koordinasyonu, denetim ve inceleme faaliyetleri kurum tarafından icra edilir. Masak kendisine ulaştırılan bildirimleri Şekil 5.2'de ifade edildiği gibi değerlendirmektedir.



Şekil 5.2. Masak'a yapılan bildirimlerin değerlendirilmesi [147]

5.1.11. Telekomünikasyon iletişim başkanlığı

TİB, Türkiye'de iletişim ağlarında akan verinin içeriğini kontrol görevine sahip devlet kurumu olarak çalışmakta iken 2016 yılında kapatılarak görevleri BTK'ya aktarılmıştır [148].

5.2. 2016-2019 Ulusal Siber Güvenlik Stratejisi'nde Düzenleyici ve Denetleyici Kurumlar

2016-2019 Ulusal Siber Güvenlik Stratejisi'nde 15 kamu kurumu, düzenleyici ve denetleyici kurum olarak belirtilmiştir. Bu kurumlar; Bankacılık Düzenleme ve Denetleme Kurumu (BDDK), Bilgi Teknolojileri ve İletişim Kurumu (BTK), Enerji Piyasası Düzenleme Kurumu (EPDK), Hakimler ve Savcılar Kurulu (HSK), İstanbul Tahkim Merkezi Başkanlığı (ISTAC), Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumu (KGK), Kamu İhale Kurumu (KİK), Radyo ve Televizyon Üst Kurulu (RTÜK), Rekabet Kurumu, Şeker

Kurumu, Sermaye Piyasası Kurulu (SPK), Türkiye Cumhuriyet Merkez Bankası (TCMB), Tütün ve Alkol Piyasası Düzenleme Kurumu (TAPDK), Yüksek Seçim Kurulu (YSK), Yükseköğretim Kurulu (YÖK) olarak listelenmiştir. Belirlenen bu kurumlar, mevzuatları ve kuruluşları bakımından incelendiğinde, tümünün bütçelerine göre düzenleyici ve denetleyici kurumlar kategorisinde bulunmadığı gözlenmektedir.

HSK, İstanbul Tahkim Merkezi Başkanlığı, Şeker Kurumu Başkanlığı, TCMB, YSK ve YÖK bütçe ve idari yapı olarak incelendiğinde, bu kurumların düzenleyici ve denetleyici kurum özelliklerine haiz olmadıkları görülmektedir.

Ayrıca strateji belgesinin yayımlanma tarihi dolayısıyla, bütçe ve idari yapılanma bakımından düzenleyici ve denetleyici kurumlar kategorisinde yer alan Kişisel Verileri Koruma Kurumu bu listede yer almamaktadır. Bu anlamda listenin revize edilmesi gereklidir.

5.2.1. Bankacılık düzenleme ve denetleme kurumu

BDDK, 5411 sayılı Bankacılık Kanunu'nda finansal piyasalarda düzenleme ve denetleme yetkisine sahip üst kuruldur. Kredi sisteminin doğru bir şekilde işlemesi, mali piyasanın gelişimi, mal sahiplerinin haklarının korunması gibi çeşitli görevleri ilgili kanunda tanımlanmıştır. Ayrıca şirketlerin birleşmesi ayrılması, tasfiyeleri gibi süreçlerde de görevleri mevcuttur. Üst kurul bu alanları düzenleyici politikaları oluşturmak, bu politikaların uygulanmasını sağlamak ve politikalara uygun olmayan davranışların tespiti için denetim yapmak amaçlı çalışmalar yürütmektedir [149]. Kurum yayımladığı genelgeler ve tebliğler ile denetimine tabi konumdaki bankaların uyması gereken asgari bilgi güvenliği kurallarını belirlemiştir.

Bankaların işleyişinde uymaları gereken bilgi sistemleri kriterlerini belirlemiş olan BDDK, bilgi sistemleri denetiminin uygulanması konusunda ülke genelinde öncü kurum konumundadır. Yayımlamış olduğu "İlkeler Tebliği" siber tehditlere karşı bankaların korunmasına katkı sağlamaktadır. Bankalar, kurumun yayımladığı tebliğler ve yönetmelikler uyarınca, asgari temelde bilgi sistemlerinde belirlenen güvenlik şartlarını yerine getirmek durumundadır. Belirli dönemlerde kurum tarafından denetim çalışmaları yapılarak, BDDK'nın düzenleme, denetleme yetkisine sahip olduğu sektör, mevzuata uygunluk konusunda takip edilmektedir.

Bankacılık sektörü, siber saldırganların popüler hedefleri arasındadır. Anlık kesintilerin büyük maddi kayıplara yol açması, siber risklere karşı sektörde daha güçlü korunmayı zorunlu kılmaktadır.

5.2.2. Bilgi teknolojileri ve iletişim kurumu

Kurum ana hizmet birimleri ve taşra teşkilatından oluşmaktadır. Kurumun elektronik ve haberleşme, bilgi teknolojileri ve posta sektöründe görevleri vardır. Telekomünikasyon sektöründe uluslararası kuruluşların faaliyetlerine de katılmaktadır. 2813 sayılı Kanun ile kurulan Ulaştırma ve Altyapı Bakanlığı ile ilişkili düzenleyici ve denetleyici bir kurumdur. Elektronik haberleşme sektöründe kilit kurum konumundadır.

BTK, kendi denetleme ve düzenleme yetkisine sahip olduğu iş alanıyla ilgili olarak oldukça geniş yelpazede iş ağına sahiptir. Dolayısıyla USOM'u bünyesinde barındırması bakımından siber güvenlik konusunda söz sahibi konumda görünmesine karşın, siber güvenliğe ilişkin çalışmaların askeri, toplumsal, sağlık, bankacılık, enerji vb. gibi farklı boyutları göz önüne alındığında, konuyu bir bütün olarak tek başına yönetmesi mümkün değildir. Bu bağlamda değerlendirildiğinde, siber güvenliğe ilişkin politikaların belirlenmesi ve uygulanması süreçlerinde daha üst bir bakış açısına ihtiyaç duyulmaktadır.

5.2.3. Enerji piyasası düzenleme kurumu

EPDK, enerji piyasasında kaliteli elektrik üretimi sağlanması, uygun maliyetle kullanımının sağlanması ve piyasada sürekliliğin sağlanması gibi çeşitli amaçlarla kurulmuştur. Bu amaçlarla kurulan kurum elektrik piyasasını düzenlenmekte ve elektrik üretimi ya da iletimi yapan kurum ve kuruluşların uygun şartlarda çalıştığına dair denetim görevlerini yerine getirmektedir [150]. Enerji ve Tabii Kaynaklar Bakanlığı ile ilişkili düzenleyici, denetleyici kurumdur. Elektrik, petrol, doğalgaz ve sıvılaştırılmış petrol gazı (LPG) piyasalarını düzenlemek ve denetlemektedir.

Ülkemizin nükleer santral kurma konusundaki girişimleri devam etmektedir. Stuxnet örneği de göz önünde bulundurulduğunda, enerji sektöründe yaşanabilecek aksaklıklar, toplumsal hayatın durmasına kadar uzanabilecek ölçüde problemlerin yaşanmasına neden olabilmektedir. Enerji sektörünün, toplumsal hayatın aksamasına neden olabilecek tehditlere ve siber saldırganlara karşı güçlü bir şekilde korunması gerekmektedir.

5.2.4. Hakimler ve savcılar kurulu

Genel bütçe kapsamında çalışan kamu kurumudur. HSK, bir mahkeme konumunda değildir. Görevleri incelendiğinde, mahkemelerin tarafsız ve bağımsız bir şekilde karar verebilmeleri ve hakim savcıların özlük işlemlerine yönelik düzenlemeleri yapmak ile sorumlu olduğu görülmektedir. Herhangi bir mahkemede hakim veya savcıya ilişkin problemlerin giderilmesi veya mahkemenin yargılama çerçevesinin değiştirilmesi benzeri konulardaki öneriler HSK tarafından değerlendirilerek bağımsızlığın ve tarafsızlığın zedelendiği durumlarda veya mahkemelerde uygun olmayan yargılama çerçeveleri ile karşılaşıldığında gerekli değişiklikler kararlaştırılmaktadır. TC Anayasasında yüksek mahkemeler arasında sayılmasa da yargı bölümünde yer verilen ve yargılama yetkisi bulunmayan Kurulun mahkemelerin bağımsızlığı ve hâkimlik teminatı esasları çerçevesinde idari görevleri bulunmaktadır [150].

16 Nisan 2017 tarihinde yapılan Anayasa değişikliğine göre; Hâkimler ve Savcılar Kurulu on üç üyeden oluşur; iki daire halinde çalışır. Kurulun Başkanı Adalet Bakanıdır [151]. Çalışma alanı incelendiğinde siber güvenliğe ilişkin düzenlemeler noktasında HSK'ya danışma organı olarak başvurulabileceği düşünülmektedir. Bilgi Toplumu Stratejisi'nde yer alan bilişime yönelik ihtisas mahkemelerinin kurulması, bilişim alanında bilgi düzeyi yüksek hakim ve savcıların yetiştirilmesi konularında çalışmaların HSK tarafından yürütülmesi, siber güvenlikle ilişkili kabul edilebilecek beklentiler arasındadır.

5.2.5. İstanbul tahkim merkezi

İstanbul Tahkim Merkezi (ISTAC), Türkiye'deki ve yurtdışındaki ticari kuruluşlar arasında arabuluculuk hizmeti sağlayan bağımsız kurumdur. Uyuşmazlıkların çözümünde üye olma zorunluluğu aramamaktadır. Merkez, çoğunluğu yabancı ve ünlü hukukçulardan oluşan Milletlerarası Tahkim Divanı vasıtasıyla tahkim süreçlerinin devamlılığını sağlamaktadır [152].

6570 sayılı Kanun ile kurulan kurum, uyuşmazlıkların çözümü ile ilgilenmektedir. Merkezin görevleri uyuşmazlıklara yönelik kuralları belirlemek bu gibi hizmetlerin yürütülmesini sağlamaktır. Uyuşmazlıkların çözümüne yönelik bilimsel çalışmaları desteklemek ve ilgili kişi kurumlarla iletişim kurarak iş birliği yapmak da kurumun görevleri arasındadır [153].

Siber güvenlik konusunda uluslararası hukuk kurallarının takibinin yapılması ve ülkemize hukuki düzlemde yansımasının sağlanmasında, ISTAC hukukçularının danışma organı olarak fayda sağlayabileceği düşünülmektedir.

5.2.6. Kamu gözetimi, muhasebe ve denetim standartları kurumu

KGK, yönetim kurulu tarafından belirlenmiş kriterlere uyum sağlayan kurum ve kuruluşların finansal tablolarını gerçeğe uygun olarak yansıtmasını sağlamak amacıyla piyasayı düzenleme ve denetleme yetkisine sahip kamu kurumudur. Kurum, finansal tabloların doğruluğunu yayımladığı uluslararası standartlarla uyumlu Türkiye Denetim Standartları ve Türkiye Muhasebe Standartlarını referans alarak, bağımsız denetçiler eliyle yapılan denetim çalışmaları yoluyla sağlamaktadır. Kurum bağımsız denetim şirketlerinin yaptığı denetimleri inceleyerek finansal tabloların doğru sunumunda kamu çıkarlarının gözetmektedir. Kurum aynı zamanda bağımsız denetçileri ve bağımsız denetim kuruluşların eğitim ve yetkilendirme süreçlerinin devamlılığını sağlamaktadır [150].

660 sayılı KHK ile kurulan kurum Hazine ve Maliye Bakanlığı ile ilişkilidir. Denetimine tabi olan kuruluşlarda, finansal tabloların kurum tarafından yayımlanan muhasebe ve denetim standartlarına uygun olarak düzenlenip düzenlenmediğinin denetlenmesi, bu amaca yönelik gözetim faaliyetlerinin yerine getirilmesi, bağımsız denetimde kalitenin sağlanması kurum görevleri arasındadır.

5.2.7. Kamu ihale kurumu

İhalenin başlangıcından sözleşmenin imzalanmasına kadar olan süre içerisinde idarece yapılan işlemleri incelemek ve buna ilişkin hukuki düzenlemeleri hazırlamak, uygulamayı yönlendirmek üzerek kurulmuştur [150]. Kurum, 4734 sayılı Kamu İhale Kanunu ile 4735 sayılı Kamu İhale Sözleşmeleri Kanunu'nun uygulanmasına ilişkin standart ihale dokümanı, tip sözleşme, yönetmelik ve tebliğler çıkarmaya yetkilidir.

Kurul ve Kurum, yetkilerini düzenleyici işlemler tesis ederek ve özel nitelikli kararlar alarak kullanır [154]. Kamu İhale Kurumu ihale süreçlerinin nasıl yürütüleceğine ilişkin politika ve prosedürlerin belirlenmesi hususunda görevlidir. Hani miktar için hangi tip ihale yapılması gerektiği, yapılmış ihalelerin uygun ve doğru olarak yürütüldüğünün temini kurum görevleri arasındadır. Yerli yatırımcıların girişimlerini destekleyecek ihale

sözleşmelerinin oluşturulmasında zemin hazırlayacak mevzuata ilişkin çalışmalar, KİK çalışma alanına girmektedir.

5.2.8. Radyo ve televizyon üst kurulu

RTÜK, yayın hizmetleri sektöründe düzenleme ve denetleme yetkisine sahip kamu kurumudur. Yoğun olarak radyo ve televizyon yayınlarının belirlenen kriterlere uygun olarak yapıldığının teminini sağlamak kurum görevleri arasındadır. İsteğe bağlı yayın hizmetlerini düzenleme yetkisi de RTÜK kontrolündedir [150].

Kurulun belirlediği sorumluluklara riayet etmeyen ve kriterlere uymayan kurum ve kuruluşlara karşı cezai yaptırımlar bulunmaktadır. RTÜK, yayın kuruluşları tarafından riayet edilmesi beklenen kurallara uyulmadığına kanaat getirilmesi halinde, kuralları uygulamayan kuruluşları uyarır ya da uygun olmayan yayın için aynı kuşakta açık bir şekilde özür dilenmesini talep eder, kimi durumlarda cezai yaptırımlar yoluna gider. Cezai yaptırımlar para cezası olabileceği gibi, ilgili yayın saatlerinde kurul tarafından belirlenen kamu bilgilendirmesi kapsamında değerlendirilebilecek çeşitli yayınların yapılmasını da içerebilmektedir [155].

Siber uzayda güvenliğin sağlanması bağlamında düşünüldüğünde, siber ortamın kötü kullanımında radyo ve televizyon gibi kaynakların kullanılması, internet yayınlarında sakıncalı içeriklerin yaygınlık göstermesi gibi konularda kurul ile çalışmalar yürütülebileceği öngörülmektedir.

Devlet yapılanmasında yapılan yeniliklere ilişkin KHK'lar ile RTÜK'e, internet ortamında yapılan yayımların kontrolüne ilişkin bazı görevler verilmiştir.

5.2.9. Rekabet kurumu

Düzenleyici ve denetleyici kurumdur. Mal ve hizmet piyasalarında hakimiyeti olan kuruluşların rekabet ortamını zedeleyecek girişimlerde bulunmasını engellemek, sahip oldukları piyasa hakimiyetini kötü amaçlarla kullanmasına engel olmak amacıyla çalışmaktadır. Bu amaçlar doğrultusunda politika ve prosedürler üretmek düzenleyici çalışmalar yapmak ve kuruluşların çalışmalarını denetlemek kurumun görevleri arasındadır.

Kurumun kuruluş amaçları 4054 sayılı Kanun ile ifade edilerek piyasada sağlıklı ve serbest bir rekabet ortamı sağlamak, kanunun uygulanmasını gözetmek Rekabet Kurumu'nun görevleri arasında sayılmıştır [156].

5.2.10. Şeker kurumu

Şeker Kurumu, 4634 sayılı Şeker Kanunu ile kurulmuştur. Kamu tüzel kişiliğine sahiptir. Şeker Kanunu ile kendisine verilen yetkiler doğrultusunda şeker piyasasında düzenlemeler yapmaya yetkilidir. Yurtiçinde ve Yurtdışında Türkiye'nin uygulayacağı şeker üretim politikalarının belirlenmesine yönelik çalışmaları Şeker Kurumu yapmaktadır. Fiyatlandırma ve Pazar yönetimine ilişkin çeşitli konularda karar verici konumda olan kurumun en önemli görevi ülke içinde şekere olan arz ve talep ilişkisinde dengeyi sağlamaktır [157].

Ulaştırma ve Altyapı Bakanlığı'nın yayımladığı siber güvenlik strateji belgesinde Şeker Kurumu'nun siber güvenliğe ilişkin sorumluklar açısından ne yönden değerlendirildiği konusunda belirsizlik olduğu düşünülmektedir. Kendi düzenleme yetkisi olan piyasada bilgi güvenliği kriterlerini yerine getirmesi siber uzayda yer alan diğer tüm paydaşlarla benzer olarak kurumun en temel siber güvenlik sorumluluğu olarak ifade edilebilir.

Şeker Kurumu, 696 sayılı KHK ile kapatılarak şeker ticaretine ilişkin tüm görevleri Tarım ve Orman Bakanlığı'na devredilmiştir.

5.2.11. Sermaye piyasası kurulu

SPK, sermaye piyasasının adil ve şeffaf olarak işletilmesini sağlamak amaçlı çalışmalar yürütmektedir. Bu amaçlarla kurulan SPK, düzenlemekle sorumlu olduğu sermaye piyasasında dünya genelinde yaşanan gelişmeler doğrultusunda politika ve prosedürler üretmek ve bu politika prosedürlerin uygulanmasını sağlamak üzere denetimler yapmakla görevlidir [150].

SPK düzenleyici ve denetleyici kurum olarak görev yapmaktadır. Düzenleme, İzahname ve İhraç Belgesi Onayı, İzin Verme, Gözetim, Denetim, Tedbir ve Yaptırım Uygulama, Finansal Raporlama Ve Bağımsız Denetim Standartları, Uyuşmazlık Çözme ve Lisanslama Faaliyetleri SPK'nın temel fonksiyonlarıdır. Ancak 2011 yılında KGK'nın kurulması

sonrasında Bağımsız Denetim Standartlarının oluşturulması ve uygulanmasına ilişkin SPK'nın sorumlulukları KGK'ya devredilmiştir.

SPK, 2018 yılı itibariyle kendi denetimine tabi kuruluşların bilgi sistemleri denetimi yapmasını esas alan Bilgi Sistemleri Bağımsız Denetim Tebliği'ni yayımlamıştır.

5.2.12. Türkiye cumhuriyet merkez bankası

Özel Bütçeli Kuruluşlar arasında yer almaktadır. Merkez Bankası, 1211 sayılı Kanun'a göre anonim şirket konumundadır. Bütçe kanunları kapsamına alınmaması bakımından değerlendirildiğinde diğer kamu kurumlarından farklı bir hukuki statüde bağımsız yapıda olduğu görülmektedir [158].

Fiyat istikrarının sağlanması Türkiye Cumhuriyet Merkez Bankası'nın gerçekleştirmek istediği temel amaçlarındandır. TCMB, fiyat istikrarını sağlamak amacıyla çeşitli politikalar üretir ve bu para politikalarının belirlenmesinde tamamen bağımsızdır. Bunun yanı sıra, temel amaç olan fiyat istikrarını sağlama amacıyla uyuşmazlık göstermediği sürece Hükümet politikaları, TCMB tarafından desteklenmektedir. Bankanın bağımsız bir şekilde para politikalarını belirlemesi ve uygulaması yatırımcıların piyasaya olan güvenini arttırıcı etkiye sahiptir [150].

Siber güvenlik açısından değerlendirildiğinde, para politikalarını belirleyen kritik konumdaki Merkez Bankası'nın güçlü teknolojik cihazlar kullanması açık bir zorunluluktur. Bankalar arası hesaplaşmaların Merkez Bankası üzerinden sağlandığı gerçeği, bu kurumun kritik bir veri akış noktası konumunda olduğunun göstergesidir.

5.2.13. Tütün ve alkol piyasası düzenleme kurumu

Tütün, tütün mamulleri, alkol ve alkollü içki piyasalarının, önemli sosyal değerlerin korunması suretiyle düzenlenmesi ve denetlenmesi (regülasyonu) amacıyla kurulmuştur [150]. 4733 sayılı Kanun ile teşkilat yapısı ve görevleri belirlenen, Tarım ve Orman Bakanlığı (eski adıyla, Gıda, Tarım ve Hayvancılık Bakanlığı) ile ilişkili olarak çalışmakta olan TAPDK, düzenleyici ve denetleyici kurumlar arasında yer almaktaydı. 696 sayılı KHK ile kurum kapatılarak görev ve yetkileri Sağlık Bakanlığı ile Tarım ve Orman Bakanlığı'na devredilmiştir.

5.2.14. Yüksek seçim kurulu

Seçimlerde ve Anayasa değişikliklerine ilişkin kanunların halkoyuna sunulmasına ilişkin iş ve işlemleri yerine getirmek üzerek kurulmuştur. TC Anayasasında "Yasama" bölümünde yer verilmiş olmakla birlikte seçimlerin genel yönetim ve denetiminin düzenlendiği Anayasanın 79' uncu maddesinde yargı organı olarak nitelendirilmiştir [150].

Genel bütçe kapsamında değerlendirilen YSK, yargısal nitelikli kuruluşlar statüsünde görev yapmaktadır. YSK siber güvenlik açısından değerlendirildiğinde, halkın yönetime katılımını sağlayan seçim süreçlerinde şeffaflığın sağlanması bakımından kritik kamu kurumları arasında görülmektedir. Bilgi teknolojilerinin diğer alanlarda olduğu gibi seçim süreçlerine de sirayet etmesinin bir sonucu olarak verilerin hızlı ve doğru bir şekilde aktarımının sağlanması seçim süreçlerinde hassas bir kurum konumundadır. Bu anlamda hem siber saldırıların hedefi olabilme noktasında hem de diğer siber risklerle karşılaşabilme konusunda incelendiğinde YSK'ya siber güvenlik konusunda görevler düşmektedir.

5.2.15. Yükseköğretim kurulu

Milli Eğitim Bakanlığı'na bağlı özel bütçeli kamu kurumudur. Yükseköğretim kurumlarının müfredatlarını belirlemek, düzenlemek ve denetlemek üzere kurulmuştur. Kurumlara ayrılan kaynakların tahsisi ve öğretim elemanlarının yetiştirilmesine yönelik çalışmaları yapmak, YÖK görevleri kapsamındadır [150]. YÖK'ün siber güvenlik konularında ders içerikleri belirlemesi ve bu alanda öğretim elemanları yetişmesine olanak tanımlayacak bölümlerin kurulmasını, bu konuda yapılan çalışmaları desteklemesi birincil beklentiler arasındadır.

5.3. 2016-2019 Ulusal Siber Güvenlik Stratejisi'nde Sektörel SOME'ler

Kamunun vatandaşlara sağladığı bazı kritik hizmetlerin devamlılığını sağlamak amacıyla, strateji belgesinde belirlenen kurumlar su, sağlık, SGK hizmetleri, vergi, nüfus, güvenlik ve benzer alanlarda hizmet göstermektedir. Bu alanlarda hizmet gösteren kamu kurumları da Sektörel SOME'ler arasında sayılmıştır.

Ulaştırma sektöründe belirlenen kurumların hepsi Ulaştırma ve Altyapı Bakanlığı'na bağlı genel müdürlükler statüsündedir. Bu anlamda ulaştırma ile ilgili kritik alanlarda siber tehditlerle karşılaşılması halinde esas irtibat kurulacak bakanlık, Ulaştırma ve Altyapı Bakanlığı'dır.

Elektronik haberleşme, enerji ve finans sektörlerinde belirlenen kurumların, bütçe ve idari yapılanmaları incelendiğinde, görev yaptıkları sektörü düzenleme ve denetleme yetkisine sahip olmaları nedeniyle, kendi denetim ağları ile kuvvetli bağlara sahip olmaları durumunda USOM ile daha güçlü bir koordinasyon sağlanacaktır.

Sektörel SOME'lerin, denetlemeye ve düzenlemeye yetkili oldukları çalışma alanlarında ikincil düzenleme ihtiyaçlarını belirlemeleri ve USOM ile koordineli olarak çalışmaları beklenmektedir. Kurumsal SOME'ler ise yine siber saldırılara karşısında USOM ile karşılıklı çalışacak şekilde planlanmıştır. Strateji Belgesinde, SOME yapılanmasının sektörel ve kurumsal olarak ayrılmasındaki amaç; kritik hizmetlerin aksamasını engellemek, piyasanın siber risklere karşı düzenleme gereken alanlarını belirlemek ve politika üretmek, siber saldırılara karşı koordinasyonu ve birlikte hareket edebilirliği arttırmaktır.

6. SİBER GÜVENLİK EKOSİSTEMİNİN GELİŞTİRİLMESİ

Sağlıklı ve sürdürülebilir bir siber güvenlik ekosistemine sahip olmak için dünyadaki teknolojik gelişmelerin takibi, doğru analizi ve bu gelişmelerle eş zamanlı olarak ülke menfaatleri göz önünde bulundurularak milli teknolojik gelişimin sağlanması gerekmektedir. Bu bölümde siber güvenlik ekosisteminin gelişim basamakları açıklanmaktadır. Bu anlamda, üzerinde en fazla durulması gereken konu; siber uzayda güçlü bir konumda yer alabilmenin bir şartı olarak ileriye dönük sağlam adımları atabilecek, paydaşlar arasında koordinasyonu sağlayabilecek bir kamu otoritesine ihtiyaç olduğudur.

6.1. Siber Güvenlik Ekosisteminin Geliştirilmesinde Önemli Kıstaslar

6.1.1. Güçlü otoritenin belirlenmesi ve devlet hiyerarşisinde konumlandırılması

Ülkemizde siber güvenlik politikalarına 703 nolu KHK yayımlanana değin, Siber Güvenlik Kurulu'nun önderlik ettiği bilinmektedir. Siber güvenlik ile ilişkili süreçlerin ilerletilmesi, yasal düzenlemeler ile kamu kurumları arasında dağıtılmıştır. Ülkemizde, siber güvenlik denince birçok çalışmayı yürütmesi bakımından akla gelen ilk kuruluşlar, Ulaştırma ve Altyapı Bakanlığı, BTK ve Sanayi ve Teknoloji Bakanlığı'na bağlı olarak kurulmuş olan TÜBİTAK'tır.

Öte yandan çeşitli yıllarda Bilgi Toplumu Strateji Belgeleri'ni oluşturması ve yayımlaması bakımından incelendiğinde Strateji ve Bütçe Başkanlığı, siber güvenlik konusunda ciddi çalışmalar yürütmüş bir kamu otoritesi durumdadır.

Ekim 1983 tarihindeki kurulan Bilim ve Teknoloji Yüksek Kurulu, siber teknolojiler ile ilgili aktif çalışmalar yapan kurumlar arasında yer almayan bir kurul konumundadır. Oysa Yüksek Kurul'un görevleri arasında teknoloji plan ve programlarının hazırlanmasında devlet yönetimine destek olmak yer almaktadır [159]. Çok hızlı gelişen teknolojileri barındıran bir alan olan siber güvenlik alanında, Yüksek Kurul'un hükümete vereceği destek oldukça önemsenmesi gereken bir konudur. BTYK son toplanma tarihinin 17 Şubat 2016 olduğu görülmektedir.

Bu alanda değerli çalışmalar yürütmesi bakımından dikkate alınması gereken bir diğer kurum Savunma Sanayi Başkanlığı (eski adıyla Savunma Sanayi Müsteşarlığı)'dır.

Başkanlığın siber güvenlik konusunda insiyatif alarak çalışmalar yürüttüğü, siber güvenlik kümelenmeleri bağlamında önemli adımlar attığı bilinmektedir.

Siber Güvenlik Kurulu'nu oluşturan kurumlar ve kurula başkanlık eden Ulaştırma ve Altyapı Bakanlığı, siber alana ilişkin gerekli yasal düzenlemelerin, politika ve mevzuatların oluşturulmasında ilk rol sahibi kurumdur. Siber tehditlere karşı mücadelede dünya standartlarıyla uyumluluğun gözetimini sağlamak üzere oluşturulan Siber Güvenlik Kurulu'nda Türk Standardları Enstitüsü'nün bulunmadığı görülmektedir. Öte yandan siber güvenlik alanında kurumsal ve toplumsal olarak bütün halinde mesafe kat edebilmek için, siber güvenlik konulu eğitimlerin planlanması, alanında kalifiye elemanların yetiştirilmesinin sağlanması amacıyla üniversitelerin bu sürece direkt olarak dahil edilmediği görülmektedir. Dolayısıyla tüm üniversiteleri temsilen Yüksek Öğretim Kurulu Başkanlığı'nın da kurulda temsili gereklidir. Birçok kamu hizmetinin bilgi sistemleri altyapısını kullandığı göz önüne alındığında geniş bir yelpazede etkiye sahip siber risklerle mücadeleyi gerçekleştirebilmek amacıyla özellikle kritik altyapılara yönelik olası siber tehditlerin önüne geçilmesi önceliklendirilmelidir. Enerji, sağlık, haberleşme gibi sektörlerin kritik altyapılara yönelik siber saldırılarda birincil hedef olacağı açık bir gerçektir. Bu kritik altyapıların korunmasına ve olası tehditlere karşı kriz yönetiminde yol gösterici olarak Afet ve Acil Durum Yönetim Başkanlığı'nın (AFAD), Siber Güvenlik Kurulu'nda yer almadığı görülmektedir.

Siber güvenlik ekosisteminin oluşturulması ve geliştirilmesi için konudan sorumlu otoritenin güçlendirilmesi gereklidir. Mevcut durumda siber güvenlik konusundan sorumlu Siber Güvenlik Kurulu 703 nolu KHK ile Ulaştırma ve Altyapı Bakanlığı bünyesinde görevine devam etmemektedir. Deneyimlendiği üzere böylesine geniş kapsamlı bir konu bağlamında yalnızca Siber Güvenlik Kuruluna dahil olan kurumlar ile birlikte kararlar alınması gelişen teknolojiyle giderek önemini arttıran bir kavramın dar bir alana sıkıştırılmasına neden olmaktadır. Öte yandan, siber güvenliğe ilişkin konuların kurula başkanlık eden Bakanlık düzeyinde takip edilmesi, etkin işlemeyen süreçlerin ortaya çıkmasına neden olmuştur. Siber dünyadaki tehlikelere karşı teknik altyapısı ve nitelikli insan kaynağı ile sürekli teyakkuzda olan ve alandaki gelişmeleri takip eden bir otoritenin kurulması son savaş alanı olarak tabir edilen siber dünyada daha güçlü bir konuma ulaşılmasına katkı sağlayacaktır. Siber güvenliğin sağlanmasında üzerine düşen vazifeleri yerine getirmeyen paydaşlara karşı yaptırımların ve cezai süreçlerin işletilmesi bu alanda daha fazla yetki ile donanmış sürekli

olarak bu işle ilgilenen bir otoriteyi gerektirmektedir. ETSI raporu dünyada, siber güvenliğin arttırılması için teknik standartlar veya operasyonel pratikler üzerinde uzlaşmaya varmak amacıyla kurulmuş sürekli bir kurumun [5] var olması gerektiğine işaret etmektedir.

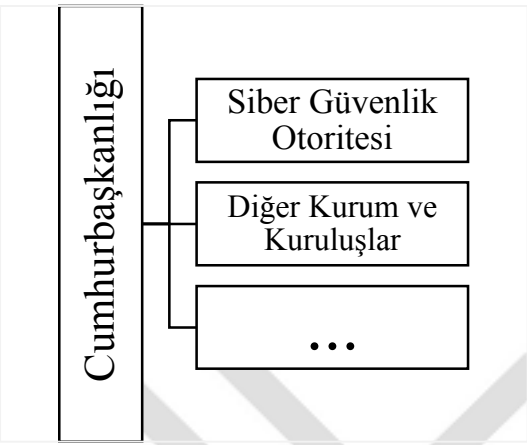
Strateji geliştirme süreci tek ve yetkili bir makam tarafından koordine edilmelidir. Yürütme organları, stratejinin geliştirilmesine öncülük etmesi için bir bakanlık, ajans veya bir departman gibi önceden var olan veya yeni oluşturulan bir kamu kuruluşu tayin etmelidir [160]. Siber olaylar akabinde kulak verilecek tek mercie sahip olunması ülke içi hızlı koordinasyonun sağlanmasında büyük öneme sahiptir. Koordinasyon eksikliklerinden kaynaklanan riskler, tehditlerin hızla büyüyerek yayılabildiği siber dünyada ülkemiz için yakın gelecekte siber saldırılara karşı daha savunmasız hala gelinmesine sebep olacaktır.

Tüm bu nedenler detaylı bir şekilde irdelendiğinde siber güvenliğin, alanında denetim ve düzenleme gücü olan, yaptırımlar uygulayabilen, siber güvenlik koordinasyonunda birincil yetki sahibi bir otorite tarafından başlı başına ele alınması gereken ciddi önem düzeyinde bir konu olduğu görülmektedir. Bu nedenle konuyla ilgili daha geniş etki alanında sahip olması gereken otorite eksikliğinin bir an önce giderilmesi gerektiği düşünülmektedir.

Siber güvenlik alanında önemli çıktılar elde etmek amaçlandığında, sayılan birçok farklı kurumun kendi başına, biri diğerinin çalışmalarından kopuk bir şekilde bu alanda yol almaya çalışması, irtibatsızlıkların neden olacağı iş gücü, zaman ve kaynak kaybı gibi problemlere bir an önce set çekilmesi gerçeği gün yüzüne çıkmaktadır. Bu bakımdan siber güvenlik ekosisteminin geliştirilmesi güçlü bir koordinasyon mekanizmasının işletilmesi noktasında oldukça önemlidir.

Tezin içeriğinde ele alındığı üzere; öncelikle siber güvenliğe ilişkin girişimlerin tek kanal üzerinden yürütülmesi amacıyla daha güçlü bir güvenlik otoritesinin kurulması gerekmektedir. Farklı kurumların yalnızca kendi bakış açılarıyla yetinerek yürüttüğü siber güvenliği sağlama girişimleri hem maddi zararlara yol açmakta hem de insan kaynağının sonuçlandırılamayan iş süreçleri ile baş başa kalmasına neden olmaktadır. Bu nedenle siber güvenlik alanında kurumlar arasında koordinasyon sağlamayıcı bir otoritenin oluşturulması, siber güvenliğe ilişkin politikaların geliştirilmesini hızlandırmanın yanı sıra yapılan çalışmaların uygulamaya geçirilmesi noktasında da büyük fayda sağlayacaktır. Bu sayede yatırımlar karşılık bulabilecek, iş gücü daha nitelikli yönetilebilecek konuma gelecektir. Öte yandan otoritenin devlet hiyerarşisinde yer aldığı konum da önemlidir. Bakanlıklar

düzeyinde veya bakanlıklara bağlı bir kurum olmaktan ziyade, devlet yönetiminin en üst mercii ile ilişkili bir kuruluş olması kurumun diğer kurumlar tarafından kabul edilebilirliğini arttıracak bir durumdur.



Şekil 6.1. Siber güvenlik otoritesinin devlet yönetiminde konumu

6.1.2. Siber olayların yönetimi ve koordinasyonu

Devlet hiyerarşik yapısında siber güvenliğin yeri, kurulacak yeni otorite ile daha güçlü hale getirilmelidir. BTK, Ulaştırma ve Altyapı Bakanlığı ve diğer kamu kuruluşlarının yürüttüğü siber güvenliğe ilişkin spesifik sorumlulukları yeni kurulacak otoritenin koordine etmesi ve yürütmesi daha uygun olacağı öngörülmektedir.

Siber olayların yönetimi ve koordinasyonu sağlanırken dünyada yaygın olarak çalışmalar yürüten FIRST, CERT-EU, OIC-CERT gibi çeşitli organizasyonlarla iş birliğine gidilmesi fayda sağlayacağı düşünülmektedir

6.1.3. Siber uzayda siber istihbaratın önemine yönelik çalışmaların arttırılması ve milli savunmanın sağlanması

Siber istihbarata gerekli ve yeterli önemin verilmesi, siber uzayda milli savunmanın sağlanmasının ilk aşaması olacaktır. Siber istihbarat savaş ortamına girmeden önce elde edilebilecek avantajlardan bir tanesi olan savunma hattının güçlü kalabilmesine olanak tanır. Rakiplerinin ne durumda olduğunu bilmek, yeni gelişmelere ve değişimlere kulak açmak yeni siber risklere karşılık verme amaçlı çalışmaları kolaylaştırır.

Clark, siber uzayda savunma ve istihbarat amaçlı çalışmaların yürütüldüğünü belirtmektedir. Çin kullandığı iki güvenlik sistemi ile olası siber saldırılara karşı kendi iç ağını dış dünyaya

kapatabilmektedir. Bu durum Çin'in savunmaya ne kadar önem verdiğinin göstergesidir. Clark, "Siber Savaş" adlı eserinde, "Çin, aynı zamanda siber ataklar yapmak amacıyla çeşitli siber savaş silahlarını da üretiyor: Bilgi mayınları yerleştiriliyor. Bilişim keşif unsurları geliştiriliyor. Ağ verilerini değiştiren cihazlar üretiliyor. Bilişim bombaları siber uzaya salınıyor. 'Çöp bilgiler' ile siber uzay dolduruluyor. Propaganda dağıtım unsurları kullanılıyor. Bilişim yanıltma uygulamaları yapılıyor. Klon bilgiler dağıtılıyor. Bilişim savunması düzenlemeleri yürütülüyor. Ağ casus istasyonları kuruluyor." ifadeleriyle, Çin'de yürütülen siber istihbarat çalışmalarını vurgulamaktadır [13].

Siber uzayda daha güçlü hala gelebilmek amacıyla gelişmiş ülkelerin girişimleri ile siber dünyadaki gelişmeler, kurulacak güçlü otoritenin istihdam edeceği siber güvenlik uzmanları tarafından yakından takip edilmelidir. Yayılım gösteren zararlı yazılımların ülke içine sızmadan tespit edilebilmesi, yerli olarak üretilmiş güçlü cihazların kullanılarak ağ trafiğinin izlenmesi ile olacaktır. Dünyadaki siyasi değişimlere ve gelişmelere paralel olarak meydana gelecek siber atakların tahmin edilebilmesi için güvenli kanallar üzerinden Milli İstihbarat Teşkilatı Başkanlığı ile bilgi alışverişi yapılmalıdır. Kamu düzenini bozabilecek olası siber ataklarda hızlı savunma mekanizmasının geliştirilmesi ve siber suçluların tespiti konusunda; Milli İstihbarat Teşkilatı Başkanlığı, Milli Savunma Bakanlığı ve MSB'ye bağlı Genelkurmay Başkanlığı ile İçişleri Bakanlığı'na bağlı kolluk kuvvetleriyle irtibat halinde olunmalıdır.

Siber yollara başvurularak yasadışı gelir elde edenlerin, yasadışı faaliyetlerle elde edilen finansmanları aklayıcıların, terörün finansmanında siber ortamdan faydalanan suçluların tespitinde Hazine ve Maliye Bakanlığı'na bağlı MASAK ile iletişim içinde olunmalıdır.

Şekil 6.2. Siber güvenlik otoritesinin diğer siber istihbarat birimleri ile bağlantısı

Siber savunma mekanizmalarının hızlı işletilmesi ve hızlı aksiyon alınmasını sağlamak amacıyla kurumlar arasında güvenilir veri altyapısı kurulmalıdır. Siber tehditlere karşı tüm durumlarda aksiyon alıcı ve diğer kurumları yönlendirici kurum, kurulacak yeni otorite olmalıdır.

Milli savunma ve siber savunmanın birbiri ile çok sıkı iletişim içinde olduğu gerçeği her zaman gözünde bulundurulmalıdır. Bu nedenle siber güvenlik otoritesinin, ülke politik gündemi ve siber dünyadaki gelişmelerin birbirinin yansıması olduğunun bilinciyle daima alarm durumunda olması gereklidir. İstihbarat yoluyla elde edilen en ufak verilerin bile ülkenin milli güvenliği açısından kıymetli bilgi olabileceği konusuna yüksek özen gösterilmelidir.

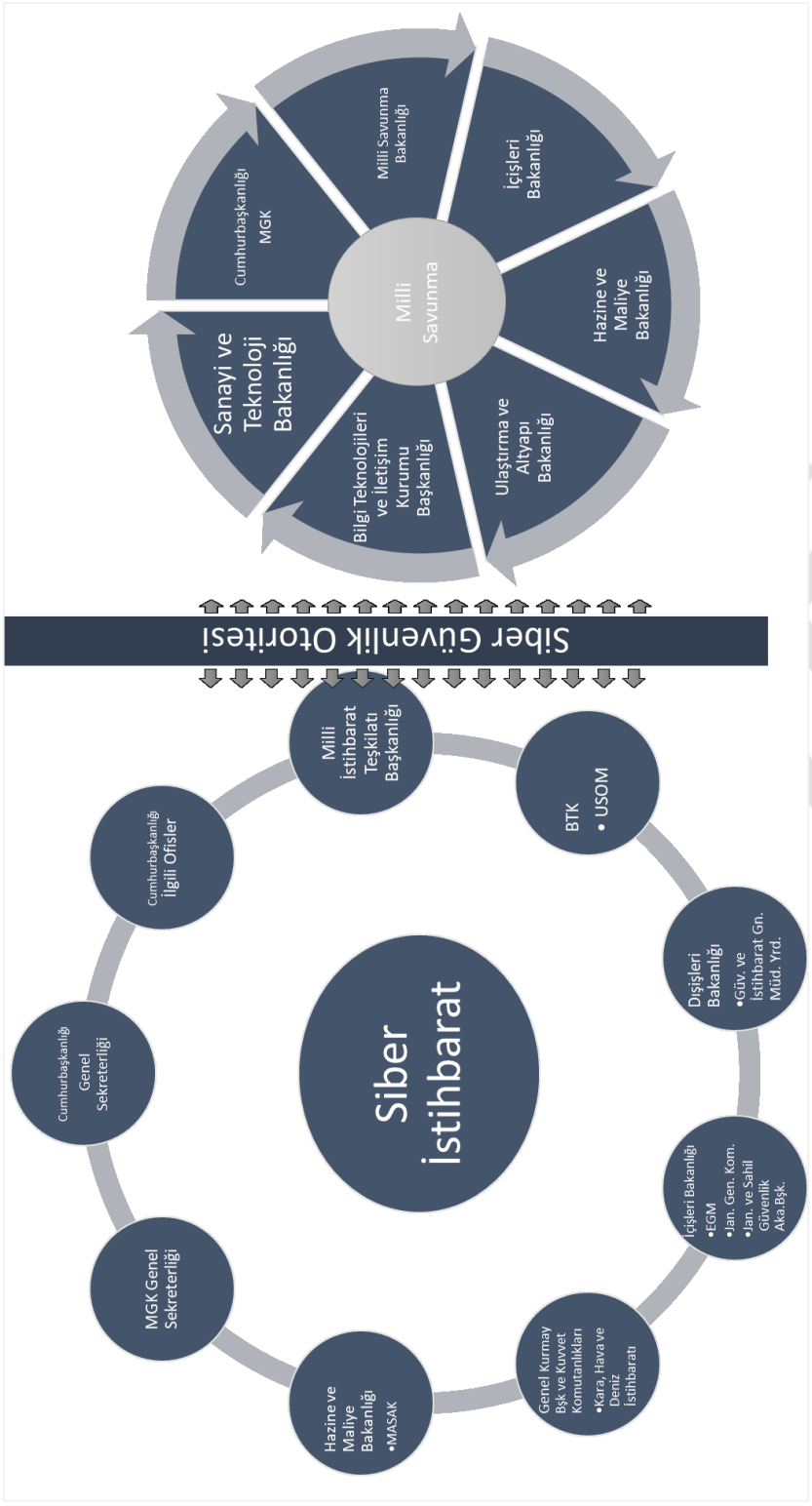
Teknolojiye ve internete artan bağımlılığın arka planına karşı ittifak, NATO ağlarını günlük olarak hedef alan geniş siber tehditlerle yüzleşme çabalarını ilerletmektedir. NATO beş siber güvenlik eylemi ile ilerlemiştir: Siber savunma konusunda NATO politikası geliştirmek, Müttefiklere yardım etmek, NATO siber savunma kapasitesini artırmak, ortaklarla iş birliği yapmak ve endüstri ile iş birliği yapmak. Müttefikler ayrıca siber saldırıların önlenmesi, azaltılması ve kurtarılmasında bilgi paylaşımını ve karşılıklı yardımı arttırmayı taahhüt etmişlerdir. NATO bünyesinde yer alan Siber Savunma Mükemmeliyet Merkezi, üye ülkeleri ve siber savunmadaki ortakları arasında eğitim, araştırma ve geliştirme, öğrenilen

dersler ve danışma yoluyla yetenek, iş birliği ve bilgi paylaşımını arttırma misyonuyla, Estonya'da bulunan NATO içindeki bir merkezdir [5]. Oluşturulacak otoritenin bu merkez ile iletişimi aktif tutması önemlidir.

Siber güvenlik otoritesi ülke genelinde düzenli aralıklarla siber tatbikatlar gerçekleştirmelidir. Dönemsellik içeren test senaryolarıyla kamu ve özel kuruluşları güvenlik açıklarına odaklanması konusunda teşvik etmelidir. Bu sayede siber sürekliliğin sağlanmasında önemli aşamalar kaydedilecektir.

Kamu düzenini bozabilecek nitelikte büyük ölçekli zarar verici riske sahip her türlü siber güvenlik açığının ortadan kaldırılabilmesi amacıyla diğer kurumlarla iş birliği yapılmalıdır. Zamanında ve doğru kurumla iletişim sağlayarak siber tehditlerin neden olabileceği riskler asgari düzeye çekilmelidir.

Siber istihbarat verilerinin elde edilmesi ve kullanılması konusunda mevcut istihbarat kaynaklarından beslenilmesi, bu kaynakların yeni kurulacak siber güvenlik otoritesinin iç istihbarat birimlerinin çalışmalarıyla birleştirilmesi gerekecektir. Siber istihbaratın sağlanması ve milli savunma politikalarının geliştirilmesi kamu kurum ve kuruluşları arasında yoğun istişareler gerektirmektedir. Siber güvenlik otoritesinin organize edeceği, gündem belirleyeceği ve toplantılar sonucu öneriler sunabileceği bir ortamın oluşması, siber risklerin asgari düzeye çekilmesine katkı sağlayacaktır. Ayrıca farklı istihbarat kaynaklarından gelen verilerin filtre edilmesi, siber tehditlerin öncelik ve risk durumuna göre sınıflandırılması politika oluşturma süreçlerini kolaylaştıracaktır.



Şekil 6.3. Siber istihbarat ve milli savunma stratejisi oluşturmada kamu kurumları

Dünya genelinde siber saldırıların azaltılmasına yönelik olarak Gelişmiş Siber Savunma Merkezi (ACDC, Advanced Cyber Defence Centre) [5] gibi kuruluşların çalışma

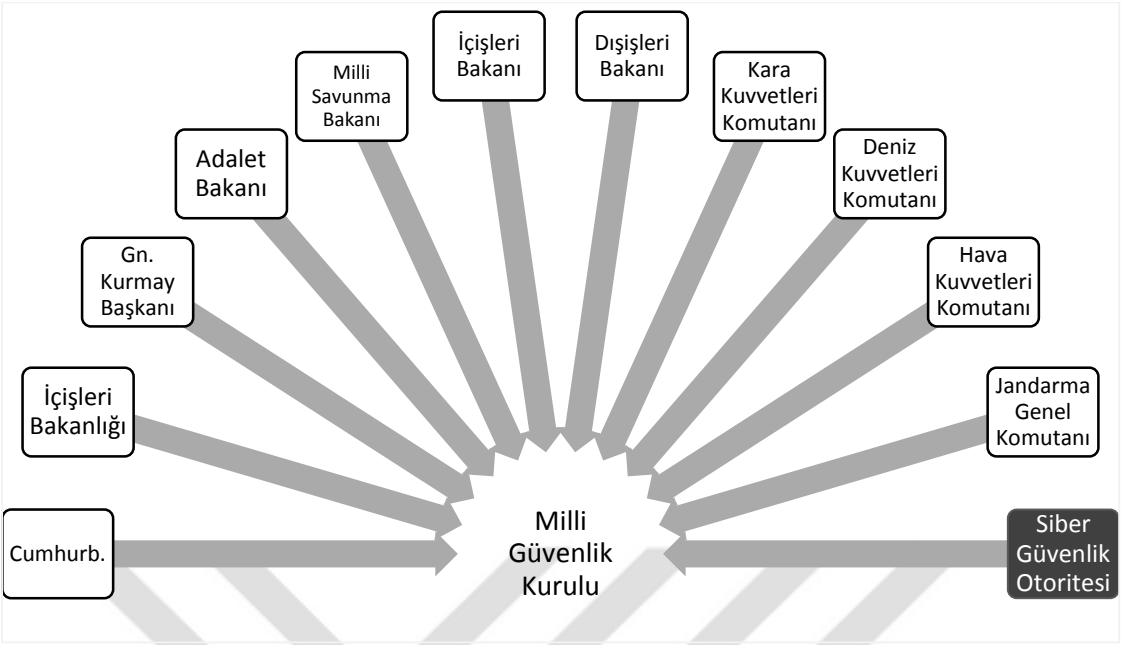
ortamlarının incelenmesi, bu kuruluşlar ile USOM arasında iş birliklerine gidilmesinin siber uzayda milli savunma faaliyetlerine katkı sağlayabileceği düşünülmektedir.

6.1.4. Siber güvenlik otoritesinin milli güvenlik kurulu'nda temsili ve siber güvenlik politikalarının uygulanması

Milli Güvenlik Kurulu, devlet yönetiminin en üst seviyeli koordinasyon makamlarından biridir. Ülkenin askeri ve sivil en üst temsilcileri milli güvenlik riskleri ve bu risklere karşı çözümlerini, plan program ve politikalarını bu kurul toplantıları vasıtasıyla görüşüp karara bağlamaktadır [161].

Bir kurumda bilgi güvenliği politikalarının, kurumsal yönetim düzeyinde ele alınmadıkça yürütülebilir olmamasına benzer şekilde, siber güvenliğe ilişkin politikalar da devletin en üst makamlarının gündeminde olmadıkça maalesef bu alanda önemsenebilir bir ilerleme kaydedilemeyecektir. Milli güvenlik ve milli savunma ile iç içe bir kavram olan siber güvenliğin, ülkenin milli savunma gündemini belirleyen Milli Güvenlik Kurulu toplantılarında temsili, kurulacak yeni otoritenin dünyadaki siber tehditleri devletin üst mercilerine aktarabilmesi, gelişmeler ile ilgili bilgi akışını sağlayabilmesi açısından çok uygun bir platformdur.

Siber güvenlik otoritesinin geliştirdiği politikaların ve çalışmaların uygulamada daha hızlı yer edinebilmesi amacıyla Milli Güvenlik Kurulu'nda temsili sağlanmalıdır. Siber güvenliğin gelişen teknolojiyle birlikte nasıl savaş tehdidine dönüşebileceği bağlamında konuya verilen önemin bir göstergesi olarak siber güvenlik otoritesinin MGK'da temsili milli menfaatler açısından kritik değere sahiptir. Bu sayede, güvenlik politikaları belirlenirken siber dünyada yaşanan gelişmelerden bağımsız hareket edilmesinin önüne geçilmesi sağlanacaktır. Teknik konularda milli yatırımların yapılması ve ihtiyaçların giderilmesine yönelik öngörü çalışmalarına yer verilmesi siber ortamda milli vizyonun belirginleşmesine destek olacak bir konudur.



Şekil 6.4. Siber güvenliğin MGK'da temsili

Kurulacak yeni otoritenin Milli Güvenlik Kurulu'nda temsili yoluyla siber güvenliğe ilişkin konular daha düzenli olarak takip edilerek milli güvenlik ve milli savunma açısından gerekli adımların atılması sağlanarak tehditlere karşı tedbirlerin alınması rutine dönüşecektir. Yayımlanan genel kurul sonuç bildirgelerinde ve basın açıklamalarında yer alacak siber güvenlik ile ilgili maddeler her birey için yol gösterici olacaktır. Dünyada değişen güvenlik anlayışına ülkemizin adaptasyonunu sağlayacağı düşünülen bu adım, her yanımızı kuşatan teknolojinin risklerine ve siber tehditlere karşı mücadelede devletin üst makamlarında söz ve politika birliğini geliştirecektir.

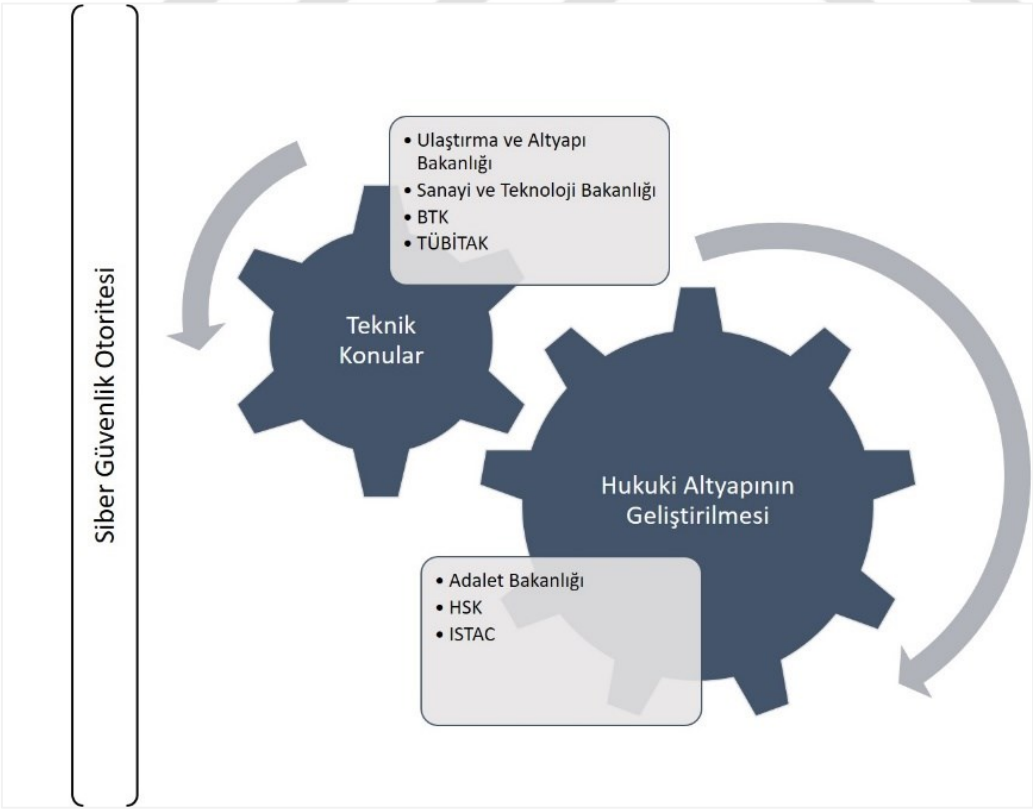
Siber güvenlik stratejisi ancak şeffaf yönetim yapısı oluşturulması ile başarılı olabilecektir. Stratejinin koordinatörü olarak kurumlar arası çalışma grubu veya bir kamu kurumu sorumlu olmalıdır, stratejinin kendisinden ve yaşam döngüsünden bizzat yükümlü olmalıdır [51] Ulusal Siber Güvenlik Otoritesi, ulusal siber güvenlik politikasının yönetiminin ve bölgesel ve uluslararası iş birliğinin tek elden koordine edilmesini sağlamalıdır [162].

6.1.5. Hukuki altyapının güncellenmesine destek verilmesi

İnternet, suçlulara düşük riskli ve yüksek kârlı suç ortamı yarattı. Üstelik ileri teknoloji bilgilerine sahip suçlular, internet alanında kendilerine sığınma yeri bulabiliyor [163]. Kurulacak otorite, dünya uygulamalarını ve teknik gelişmeleri göz önüne alarak ülkemizin hukuk sisteminde gerekli olduğu düşünülen güncelleştirmeler konusunda önerilerde

bulunmalıdır. Bilişim dünyasının hızlı bir şekilde gelişmesi, hukuki altyapının da güncel teknolojiyle uyumlu bir düzeyde değişmesini gerektirmektedir.

Siber güvenlik otoritesinin kendi içinde diğer paydaşların ihtiyaçları ve uluslararası normlara cevap verecek ölçütlerde hukuki gereksinimleri karşılamayı hedefleyen iç hukuk birimine ihtiyacı olacaktır. Hukuki gereksinimlerin giderilmesi ve siber ortamda yaşanan ihlallerin hukuki altyapıyı güncellemek suretiyle ortadan kaldırılması veya azaltılması otoritenin yapacağı durum tespit çalışmalarıyla şekillenecek olan süreçlerdir. Bu anlamda Adalet Bakanlığı ve Barolar Birliği vb. kurumlardan alınan siber ortam ile ilişkilendirilebilecek hukuki örnekler; istihbarat kaynaklarından alınacak siber suçların nitelikleri; dünyada siber suçlar konusunda ne gibi çalışmaların yapıldığı şeklinde kısaca örneklendirilebilecek başlıklarda çeşitli analiz çalışmaları yürütülebilir. Bu çalışmaların sonuçları ve gereksinimler uygun mercilere sunularak gerekli görülmesi halinde yasal mevzuata kazandırılması çalışmaları otorite tarafından takip edilebilir. Çalışmaların koordinasyonunu siber güvenlik otoritesi sağlamalı ve çalışma planlarının uygulamaya yönelik yansımaları siber güvenlik otoritesi tarafından periyodik olarak izlenmelidir.



Şekil 6.5. Hukuki altyapıya ilişkin koordinasyon ve ilgili kurumlar

Siber suçla mücadelenin sağlam bir şekilde yapılması maksadıyla soruşturma ve kovuşturmanın adil bir şekilde gerçekleştirilmesi için adli bilişim ve delil tespiti süreçlerine önem verilmesi, bu safhalarda görev alan personelin teknik seviyede eğitim verilmesi [51] gerektiği siber güvenliğe ilişkin yapılan çalışmalarda göze çarpan bir konudur.

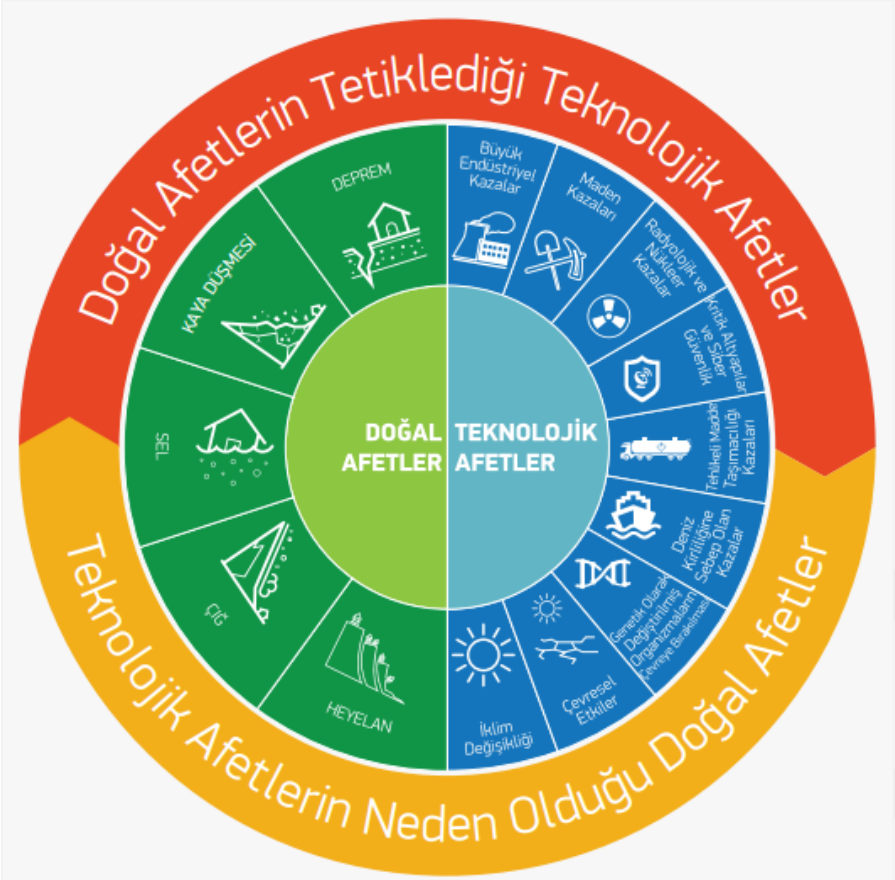
Adalet Bakanlığı ve Milli Savunma Bakanlığı'nın siber kabiliyetlerin silah olarak kullanımını kapsayan suçları tanımlayan, bu gibi suçlar veya saldırılar ile karşılaşılması halinde yasal olarak ne gibi adımlar atılabileceğine ilişkin çalışmalar gibi yeni ve güncel mevzuat çalışmaları yürütebileceği düşünülmektedir. Bu gibi çalışmalar yapılırken siber güvenlik otoritesi ile iş birliktelik sağlanabilir. Son dönemde özellikle ABD yasa tasarılarında bu ve benzeri güncel hukuki altyapı çalışmalarının ele alındığına rastlanılmaktadır [164].

6.1.6. Kritik altyapıların korunması

Siber uzay, kritik altyapılara karşı yapılan organize saldırıların uzaktan gerçekleştirilebilmesi için imkanlar sağlamaktadır. Bu saldırılar yalnızca saldırganların ihtiyaç duydukları teknolojik ürünleri gerektirir ve onlara kimlikleri ile mevkilerini gizleme imkanı verir [165]. Siber güvenlik ile iş sürekliliği arasında çok sıkı bir ilişki bulunmaktadır [166].

Kritik altyapılara yönelik siber saldırılar geleneksel terör saldırılarından daha büyük yayılım ve etki gösterebilecek niteliktedir. Örneğin bir bankanın siber saldırılar neticesinde birkaç saat hizmet verememiş olması, bilgi sistemlerine bulaşan bir yazılım nedeniyle yanlış miktarlarda nakit akışlarına sebep olması vb. durumlar ulusal para piyasasına etki edebilecek bir unsur olmanın yanı sıra toplumsal hayata etki edecek özelliktedir [165].

AFAD, ülkemizde çeşitli afet ve acil durumlar karşısında politika üretimi ve aksiyon alınması noktasında sorumlu kuruluştur [167]. Şekil 6.7'de AFAD'ın yayımladığı raporda [167] yer alan şekliyle doğal afetler ile teknolojik afetler arasındaki ilişki aşağıda olduğu gibi şematize edilmiştir. İncelenen ülkeler göz önünde bulundurulduğunda, kritik bilgi sistemleri altyapısının korunmasına ilişkin spesifik kurumlar oluşturulmasının ve bu alana özel stratejik politika belgeleri oluşturulmasının fayda sağlayacağı düşünülmektedir.



Şekil 6.6. Afetlerin sınıflandırılması ve aralarındaki ilişki [167]

2016-2019 Ulusal Siber Güvenlik Stratejisi'nde belirtilen çeşitli sektörleri hedef alacak siber saldırılar, bir ülkeyi toplumsal kaosa sürükleyebilecek niteliktedir. Bu nedenle belirlenen sektörlerin daha güçlü donanım ve yazılımlarla korunması gerekmektedir. Yerli ve milli yazılımlar üretilmedikçe tam anlamıyla güvenlik sağlanması mümkün değildir. Bu nedenle belirlenen sektörlerin ihtiyacına paralel olarak güçlü yazılımların ve donanımların milli ve yerli olarak üretilmesi girişimlerine hız verilmesi gerekmektedir. Düzenleyici ve denetleyici kurumların AR-GE faaliyetlerini kendi sektörlerinin ihtiyaçlarına göre güçlendirmesi, eş zamanlı olarak siber güvenlik otoritesi ile iş birliği içerisinde olması kritik altyapıların korunması bağlamında bir zorunluluk olarak karşımıza çıkmaktadır.

ABD'de kritik altyapılara ilişkin özel yasa çıkarılmış, ayrılan bütçe bu yasa ile belirlenmiş ve konunun sorumlu olduğu bakanlık tarafından diğer kuruluşlara görevler verilmiştir. Türkiye'de kritik altyapılarla ilgili bir kurum bulunmamakla beraber bu tesislerin neler olduğu yasal mevzuat kapsamına dahi alınmamıştır [51]. Düzenleyici ve denetleyici kurumların ve diğer tüm kamu kurumlarının kendi alanlarında gerçekleşebilecek olası siber riskleri belirlemesi, bu riskleri düzenli aralıklarla yeni kurulacak siber güvenlik otoritesi ile

paylaşarak geri bildirimde bulunması sağlanmalıdır. Bu sayede değişen iş süreçlerinde karşılaşılabilecek risklere karşı otorite tarafından yeni politikaların üretilmesi sağlanarak siber saldırılara karşı iş birliği yapılabilecek ve güçlü bir savunma döngüsü işletilecektir.

Otorite, kritik altyapıların korunmasına yönelik yerli yazılımların ve yerli teknolojilerin üretilmesini sağlamak amacıyla çeşitli mekanizmalar işletebilmelidir. Kritik altyapıları etkileyebilecek siber tehditlerle karşılaşılması durumunda tehlikeyi ortadan kaldıracak çalışmalara USOM önderliğinde başlanarak diğer ilgili kamu kurumları ile irtibat halinde olunmalıdır. Afet ve Acil Durum Yönetim Başkanlığı, İçişleri Bakanlığı ve bağlı ilgili kurumlar, Milli Savunma Bakanlığı ve ona bağlı ilgili kurumlar acil olarak haberdar edilmelidir.

Kritik altyapılar konusunda öncelikli süreç kritik altyapı envanter bilgilerinin çıkarılması konusudur. Daha önce diğer kurumlar tarafından yürütülen çalışmaları bütünleştirecek bir kapsamlı çalışmanın yapılması ve sonuçlarının incelenmesi, risklerin değerlendirilerek sınıflandırılması, bir nevi ülke bazında risk haritasının çıkarılması oldukça önemli bir konudur.

Siber dünyanın risklerine karşı ülke olarak ne gibi açıklıklar ile karşı karşıya olduğumuz ve bu açıklıkların derecelendirilmesi konusu; bu açıklıkların oluşturacağı tehditleri nasıl, ne yöntemle karşılayabileceğimizi belirleyebilme noktasında özen gösterilmesi gereken bir konudur. Kuruluşlar siber uzayda risk teşkil edebilecek unsurları günlük hayatı ne derece etkileyebileceği doğrultusunda değerlendirmeli, derecelendirmelidir. Bu değerlendirme ve derecelendirme süreçleri, ortaya çıkacak olumsuz gelişmelerde siber güvenlik ekosisteminin savunma mekanizmasının işletilmesini sağlayacaktır.

Şekil 6.7. Kritik altyapılarla ilişkili kamu kurumları

Şekil 6.8'de tasnif edildiği gibi, kamu kurum ve kuruluşları kendi çalışma alanları ile ilgili konularda kritik kabul edilen iş süreçlerini belirleyerek siber güvenlik otoritesi ile paylaşmalıdır. Risklerin günlük hayatın akışını ne ölçüde etkileyebileceğinin proaktif

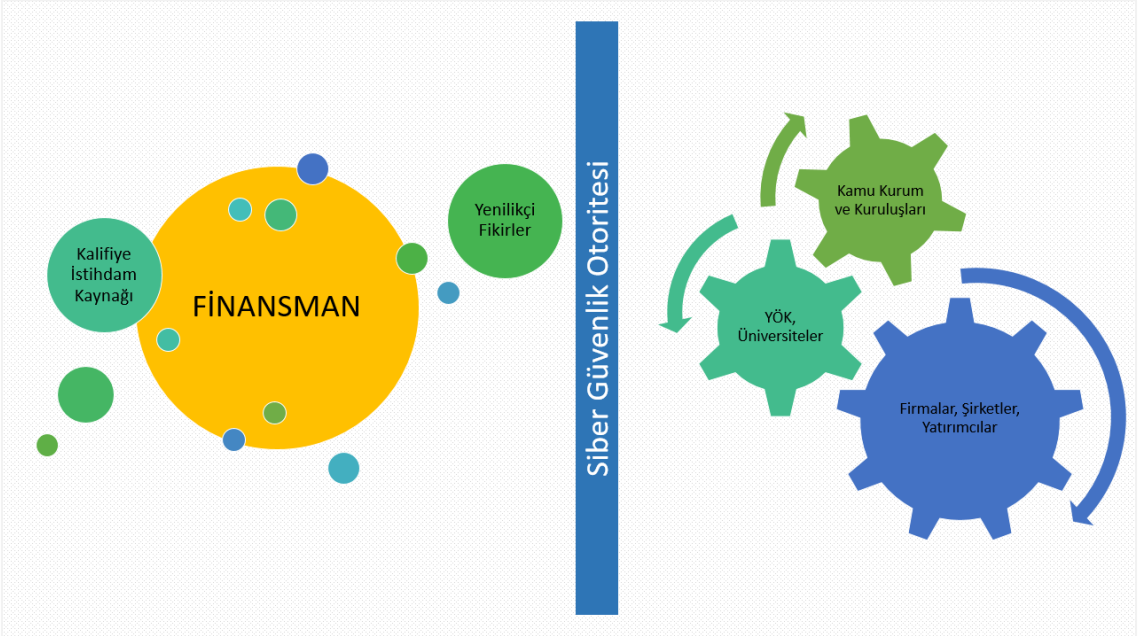
yaklaşımlarla tespit edilmesi, olası tehdit unsurlarıyla karşılaşma anlarında hızlı karşı cevaplar verilmesini kolaylaştıracaktır. Bu anlamda siber güvenlik otoritesinin tüm paydaşlarla sektörler bazında yürüteceği kritik altyapıların belirlenmesi ve korunması çalışmaları; toplumsal ihtiyaçların kesintisiz karşılanması, siyasi bütünlüğün korunması ve kamu düzeni ve otoritesinin devamı için ciddi öneme sahiptir.

Öte yandan dünya ülkeleri incelendiğinde kritik altyapıları hedef alan siber saldırıların yarattığı risk düzeyinin ciddi önem arzeden konular arasında sayıldığı görülmektedir. Bu bağlamda kritik altyapılara yönelik çeşitli kurum ve kuruluşların siber olayları da kapsayacak şekilde politiklar ürettiği ve uyguladığı gözlenmiştir. Ülkemizde de bu gibi çalışmaların arttırılması gerekmektedir.

6.1.7. Siber güvenlik kümelenmeleri

Siber güvenlik kümelenmesi; üniversiteler, özel sektör kuruluşları, kamu kurumları ve siber uzayda rolü olan her bir paydaşın, kendi çalışma alanlarına benzer alanlarda ortak hedefleri gerçekleştirmek üzere bir araya gelmesi, kümelenmesidir. Bu ortak hedefler gerçekleştirilirken paydaşların her biri kendi altyapılarının zenginliğini diğer paydaşın altyapı zenginlikleri ile birleştirerek siber güvenlik sorunlarına yönelik nitelikli çözümler üretebilecektir. Örneğin siber savunma alanında savunma sanayi teçhizatı imalatı yapan bir kuruluşun, diğer savunma sanayi kuruluşları ile kümelenerek ortak problemlere daha hızlı çözüm üretebilmesi buna örnek olarak gösterilebilir. Ek olarak aynı savunma sanayi teçhizat üreticisi kendi bünyesinde yazılım gücünü yetersiz görüyorsa iyi bir yazılım firması ile kümelenebilir, akademik çalışmalarla üretimini desteklemek veya öğrencileri hem yetiştirip hem iş fırsatı sağlamak için üniversitelerle kümelenerek iş birliği yapabilir. Özetlenirse; siber güvenlik kümelenmesi, geniş bir çalışma alanını kapsayan siber güvenlik konusunda, kuruluşların kümeler oluşturarak ortak amaçlar için güçlerini birleştirmesini; farklı disiplinler üzerine çalışan kuruluşların ortak paydada buluşarak üretim yapmasını ifade eder.

Siber güvenlik otoritesi yerli yazılım ve donanım üretimi konusunda siber güvenlik kümelenmelerini teşvikin faydalarına odaklanmalıdır. Küçük ve orta ölçekli işletmelerin bütçelerinin yetersiz olması, insan kaynağı gereksinimleri veya diğer hususlar gözetilerek güçlü yatırımcılarla eşleştirilmek suretiyle çeşitli projelerin üretilmesi kolaylaştırılmalıdır. Bu anlamda otorite benzer ilgi alanında olan işletmeler arasında bir iletişim köprüsü vazifesine bürünebilecektir.



Şekil 6.8. Kümelenme yapısında iletişim ve koordinasyon

Teknolojik olarak güçlü ülkelerin başında gelen ABD örneğinde bilgi sistemleri ile ilişkili olan kuruluşların sektörel olarak kümelendiği ulusal bir yapılanma örneği göze çarpmaktadır. Ulusal Bilgi Paylaşımı ve Analiz Merkezleri (National ISAC's) Konseyi [5], sektör olarak ortak alanlarda çalışan çeşitli teknoloji şirketlerinin bir araya geldiği bir platform sağlamaktadır. Bu gibi oluşumların ülkemizde de yaygınlaşmasının faydalı olacağı öngörülmektedir.

6.1.8. Yatırımcılar ile ilişkilerin güçlendirilmesi ve yerli üretimin teşviki

Bilgi güvenliği risklerinin farkında olunması ve bu alana yatırımın gerekliliğinin üst makamlar tarafından kabul edilmesinin elle tutulur göstergesi yerli yatırımın ve yatırımcının desteklenmesidir. Öncelikle, siber güvenlik konusunun, herhangi bir felaket ile karşılaşılmadığı sürece pek de önemsenmeyen bir konu olmaktan çıkarılması gerekmektedir. Siber güvenlik otoritesinin yatırımcılara, siber güvenliğin ve siber güvenlik alanında kalifiye personel çalıştırmalarının önemi ve değeri anlatılmalıdır. Bu alanda yerli yatırıma ne kadar fazla ihtiyaç olduğuna yönelik açıklayıcı çalışmaların yapılması ve çalışma sonuçlarının kamuoyu ile paylaşılması yoluyla yatırımcıların dikkatinin bu alana çekilmesi gerekmektedir.

Ülkemizde siber güvenliği sağlama amaçlı kullanılan uygulamaların yüksek oranda yabancı kaynaklı olmasının önemli problemlere yol açtığı bilinmektedir [166]. Siber güvenliği

sağlamak amacıyla satın alınan herhangi bir cihaz, içerisinde barındıracağı casus bir yazılım ile siber istihbarat sağlayan bir cihaza dönüşebilir. Bilgi sistemleri altyapısını oluşturan cihazların ve yazılımların, tedarik sağlanan ülke için siber istihbarat kaynağına dönüşme riskini ortadan kaldırmak ancak yerli üretimle gerçekleştirilebilir.

Yerli üretim dışa bağımlılığı azaltır. Üretim gücünü arttıran ülkenin diğer ülkelere bağımlılık düzeyi düşer. Dışa bağımlılığı azalan ve üreten ülke, politik anlamda söz söyleyebilen ülke konumuna ulaşır. Dolayısıyla bir ülkenin gelişmişlik seviyesini o ülkenin üretim gücü belirler.

Dışa bağımlılığı azaltmak ve milli ürünlerin yaygınlaşmasını sağlamak için yazılım ve donanım sektörü ile etkin bir iletişim kurulmalıdır. Yerli yatırımcıların teknolojik alanda üretim yapmaya teşviki, siber güvenlik otoritesinin bir takım düzenlemeler yapmasını gerektirebilecektir. Belirlenecek şartları sağlayan ve siber güvenlik sistemleri alanında yazılım veya donanım üretimi yapma hedefi olan yatırımcılar kamu tarafından yasalar çerçevesinde maddi olarak desteklenmelidir. Bu destek, siber güvenlik otoritesinin yatırımcının çalıştıracağı personele dönemsel eğitimler vermesi, personel giderlerinin bir kısmının kamu eliyle karşılanması, yatırımcının vergi giderlerine yönelik iyileştirmeler yapılması vb. şeklinde olabileceği gibi yatırımcıların ihtiyaçlarına göre de şekillenmesi önemli olacaktır. Yatırımcının kamu desteğinden beklentilerini anlayabilmek için yatırımcılara çağrılarda bulunularak dönemsel toplantılar düzenlenmelidir. Bu toplantılar teşvik mekanizmasının işlerliğine ve teşviklerin ihtiyaca binaen şekillenmesine katkı sağlayacaktır.

Üretilen yerli yazılım ve donanımların kurumlarda kullanımının yaygınlaştırılması, kamuya hizmet alımlarında yerli üretimin önceliklendirilmesi, üretimin devamlılığı açısından gereklidir. Kamu İhale Kurumu ile siber güvenlik otoritesi arasında bu anlamda bir çalışma yürütülmesi faydalı olacaktır. Ancak bu süreçler ilerletilirken ürünlerin belirlenecek olan kalite esaslarını karşılaması bakımından değerlendirilmesi konusuna özen gösterilmelidir. Ürünlerin uluslararası pazarda benzer diğer ürünlerle rekabet edebilecek seviyede hatta ithal ürünlerden daha yüksek kalite düzeyinde olması tercih edilirliği arttıracaktır.

Gelişmiş ülkelerin siber güvenlik alanında yapmış olduğu yatırımların irdelenmesi gelişmekte olan ülkemiz için vizyon oluşturacaktır. Bu nedenle dünyadaki teknolojik gelişmelerden uzak kalınmaması amacıyla siber güvenlik otoritesinin sürekli yeniliğe açık

olması gerekir. Yatırımcıları yeni alanlara sevk edilmesi süreci, otorite tarafından bu gelişmelerin takibi ve edinilen güncel yatırım fırsatlarının yatırımcılarla paylaşımıyla mümkün olacaktır.

Ülkelerin gelişmişlik düzeyi ile araştırma geliştirme faaliyetleri arasında sıkı bir ilişki vardır. Gelişmekte olan ülkeler arasında yer alan bir ülke olarak, bu düzeyi yükseltmeye katkı sağlayacak bir alan olan teknoloji dünyasına yatırım, araştırma geliştirme faaliyetlerinin inovasyon fikirlerini teşvik edici unsurlarla desteklenerek etkin olarak yürütülmesiyle birlikte sağlanabilecektir. Bu bağlamda, sanayi, endüstri ve akademik çevrenin çeşitli alanlarda ortaklaşa yürüteceği projeler yerli teknolojilerin üretimini arttıracaktır. Kamunun teşvik olarak kaynaklar oluşturması ve AR-GE faaliyetlerine yatırımlarını arttırmasının bir getirisi olarak ülke gelişmişlik düzeyinin yükseleceği açık bir gerçektir. Bu bağlamda siber güvenlik otoritesi, kümelenme yapılarının oluşmasında üstten bir göz olarak, teknolojik arz ve talepler doğrultusunda yatırımcıları odaklı olarak ilgili alanlara yönlendirebilmelidir. Örneğin, savunma sanayii alanında üretim yapan ancak kıt kaynakları olan bir yerli sanayi kuruluşunun finansmanı için bu alana yatırım yapabilecek yerli finansman kaynaklarını buluşturmak; güvenilir finansal tablo üretimini sağlayacak yazılımlar ve platformlar geliştirmeyi hedefleyen ancak kalifiye personel bulamayan bir yazılım firması ile, bu alanda çalışmalar yürüten ve bilgi düzeyi bu işe uygun olan akademik çevreyi buluşturmak siber güvenlik otoritesinin koordinasyonunu gerektirmektedir.

Bu gibi çalışmalar, mevcut durum göz önüne alındığında, teknolojiyi ithal eden konumda olan ülkemizin, öz kaynaklarını doğru alana sevk etmesi suretiyle teknoloji ihracatı yapan bir konuma ulaşmasını sağlayacaktır. Türkiye'de devlet kurumlarına görevler verilmiş olsa da, özel sektördeki paydaşların belirlenmesi hususunda eksiklikler bulunmaktadır [51]. Başlangıçta yatırımcıların ve özel sektör girişimcilerinin çalışma alanlarının belirlenmesi sancılı bir süreç olmasına karşın, uzun vadede teknolojik özgürlüğün ve bağımsızlığın kapısı aralanacaktır.

Ayrıca yatırımcıların teşviki yerli üretimin gelişmesini beraberinde getirecektir. Yenilikçi yaklaşımların artması teknolojik gereksinimlerin milli olarak karşılanması dışa bağımlılığı azaltan bir unsurdur. Bu nedenle insan gücü ve maddi yatırımların odaklı olarak yönetilmesine, siber güvenlik otoritesinin bir üst bakış olarak etkisi yadsınamayacak ölçüde olacaktır. Siber güvenlik otoritesinin dolayısıyla kamu yönetiminin yatırımcılara desteği

gelişim için değerli olduğu bilinciyle bu doğrultuda çalışmalara ivme kazandırılması gerekecektir. Öte yandan kamu kurumlarının teknik hizmet alımlarına ilişkin ihalelerde yerli yazılım ve donanım firmalarına öncelik tanıması, ürettikleri ürünlerin kamuda diğer güçlü firmalarla yarışabilecek düzeye kavuşması uzun soluklu kontrollü bir çalışmayı gerektirebilir.

Devlet, dijital dönüşüm ile ilgili ulusal öncelikleri, stratejileri ve politikaları belirleyen, ekosistem paydaşlarını harekete geçiren, onlara yol gösteren ve iş birliği içinde çalışmalarını sağlayan en temel paydaştır [168]. Bu bağlamda, milli kabiliyetler ile hangi teknolojilerin geliştirilmesine ihtiyaç olduğu ve ihtiyaçların önceliklendirildiği konusunda oluşturulacak ulusal bir stratejinin kaynak israfını azaltacağı ifade edilmektedir [166].

Siber güvenlik otoritesinin, öncelikli girişim alanlarını belirledikten sonra, devlet kurumlarını bu girişimlerin her biri için görevli olarak tanımlaması, devlet kurumlarının kendilerine atanan her bir girişimin uygulanmasından sorumlu olarak uygulama sürecinin bir parçası halinde, diğer ilgili paydaşları koordine etmesi sağlanmalıdır. Yürütülecek bu çalışmaların sonucu ise insan kaynakları, uzmanlık ve finansman ihtiyaçlarını içerecek şekilde değerlendirilebilir [160]. Siber güvenliğe ilişkin yatırımcıların ne gibi gereksinimleri olacağı bu çalışmaların neticesinde daha net bir şekilde elde edilebilecektir.

6.1.9. Sivil toplum kuruluşlarıyla ilişkilerin güçlendirilmesi ve toplumsal bilincin arttırılması

Sivil toplum kuruluşları, toplumun herhangi bir konuda bilgi edinmesi hususunda elverişli ortam sağlayabilecek kuruluşlardır. Kamu otoritesinin bilgi sistemleri ve siber güvenlik alanında misyon ve vizyon belirleyen sivil toplum kuruluşları ile sıkı iletişimde olması, siber güvenliğe ilişkin gelişmelerden toplumun haberdar olmasına katkı sağlayacaktır.

Bu kuruluşlar kendi üyelerine en azından güncel siber tehditler ve korunma yöntemleri hakkında bilgi aktarabilse dahi toplumsal bilincin artması yönünde büyük bir ilerleme kaydedilecektir. Örneğin kamu otoritesinin, yayılım gösterdiğini tespit ettiği bir zararlı yazılıma ilişkin yaptığı duyuru akabinde, sivil toplum kuruluşlarının düzenleyeceği ilgili zararlı yazılımdan korunma yöntemleri konulu kısa bilgilendirme, seminer, konferans ve eğitim toplantıları, sivil toplum kuruluşuna bağlı olan üyelerin tehlikeden haberdar olmasını, korunmasını sağlayacaktır. Üyelerin kendi çevrelerinde bu tehdit hakkında paylaşacağı

bilgiler toplumsal bilincin artmasına ve bireysel savunma mekanizmasının güçlenmesine katkı sağlayacaktır. Devam edegelen bilgi akışıyla siber tehlikelere karşı toplum daha uyanık davranabilecektir.

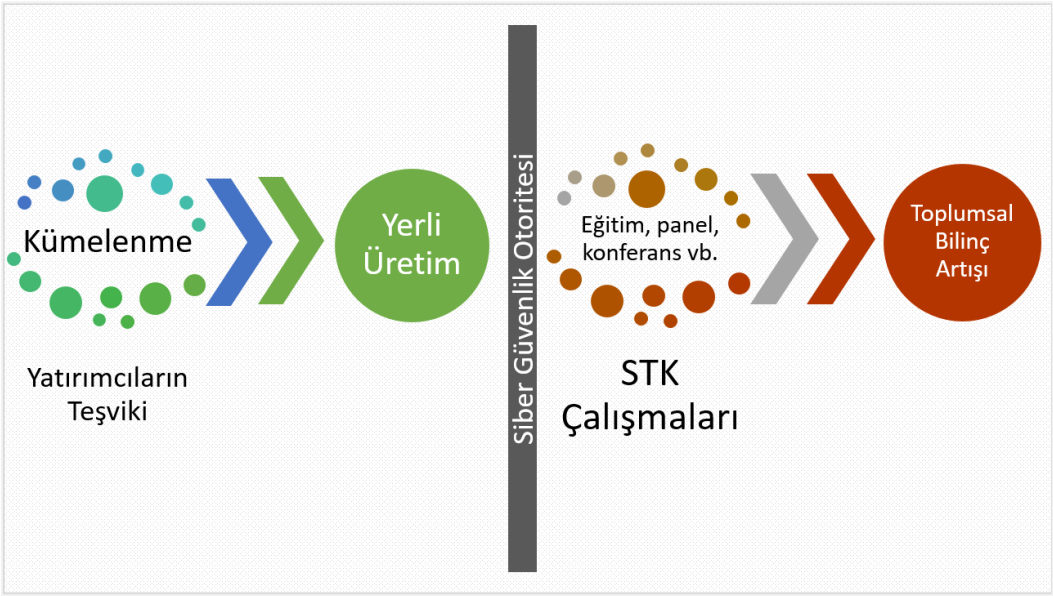
Benzer şekilde sivil toplum kuruluşlarının güncel teknolojiyi takip ederek, siber güvenliğe ilişkin sorunların çözümüne katkı sağlaması, strateji ve politikalar üreterek alanında yaptığı çalışmaları kamu otoritesi ile paylaşması siber güvenlikte kamu ve STK iş birliğini arttıracaktır. İyi ortaklık iyi kazanç demektir. Bir zinciri zorladığında en zayıf halkasından kopacaktır [165]. Siber güvenlik ekosisteminde zincirin her bir halkası, ekosistemde yer alan her bir bireydir. Bu anlamda zincirin her bir halkasını ayrı ayrı güçlendirmek şarttır.

Ülkelere göre internet kullanımı incelendiğinde, yapılan araştırmalar Türkiye'nin, ortalamanın üstünde, %67 seviyesinde internet kullanım oranına sahip olduğu görülmektedir [25]. İletişimin akıllı cihazlarla sağlandığı, mobilizasyonun arttığı, bilgi sistemleri kullanan bireyler ve kurumlardan oluşan yeni nesil toplum yapısında kötü niyetlilerin de yer aldığı unutulmamalıdır. Reel dünyada olduğu gibi siber dünya da iyilerin ve kötülerin bulunduğu bir ortamdır. Ülkemizde, internet ve sosyal medya kullanım oranları, siber uzayın barındırdığı riskler hakkında toplumsal bilincin artmasına yönelik seminerler, konferanslar, yürütülmelidir. Bu bağlamda kurulacak siber güvenlik otoritesinin basın yayın organları dahil tüm iletişim kanallarını kullanarak siber uzaydaki tehditlere ilişkin bilgilendirmeler yapması gerekmektedir.

Örneğin, Türkiye'den gençlerin de içinde yer aldığı ve dünya çapında onlarca gence, sosyal medya aracılığıyla ulaşan, önce çevrimiçi oyun daveti görünümüyle başlayıp daha sonra şantaja dönüşen ve gençlerin hayatlarına son vermelerine neden olan akıllı telefon uygulaması konusunda BTK'nın internet sitesinde bilgilendirme içerikli bir duyuru yayımladığını görüyoruz. Daha geniş kitlelere ulaşacak şekilde bu duyuruların yaygınlaştırılması için çalışılmalı, gerçek dünyada yapılmayacak şeylerin siber dünyada yapılmaması gerektiği hukuki gerekçelerle desteklenerek topluma açıklanmalıdır.

Bilinçli bir kullanıcı, diğer tüm siber tehdit mücadele unsurlarıyla kıyaslandığında en güçlü olan mücadele unsurudur. Büyük yatırımlar yapılarak alınan önemli teknolojik güvenlik tedbirleri bilinçsiz kullanıcıların yapacağı ufak bir hata ile kullanıma elverişsiz hale gelebilir.

Siber güvenlik otoritesinin Şekil 6.10'da ifade edildiği gibi, yatırımcıların kümelenmeler vasıtasıyla desteklenmesinin sonucu olarak yerli teknoloji üretimi ivme kazanacaktır. Benzer olarak, otoritenin STK'lar ile birlikte yürüteceği çalışmalar neticesinde düzenlenecek eğitim, panel, konferans vb. vasıtasıyla, toplumsal bilincin artması sağlanacaktır.



Şekil 6.9. Yerli üretim ve toplumsal bilinci arttırmaya yönelik çalışmalar

Siber ortamın riskleri ve güçlü olunması halinde sağlayacağı milli faydaların toplumu oluşturan bireylere daha kolay anlatılabilmesi ve toplum farkındalığının arttırılabilmesi sivil toplum kuruluşları vasıtasıyla sağlanabilecektir. Dolayısıyla siber güvenlik otoritesi eğitim, bilgilendirme toplantıları, çalıştaylar yoluyla halka daha kolay bilgi ulaştırabilecek olan sivil toplum kuruluşlarıyla ilişkilerini sıkı tutmak durumundadır. Ayrıca kamuoyunun beklentilerinin siber güvenlik otoritesi tarafından karşılanması için de STK'ların geri dönüşleri önemsenmelidir.

Farkındalık sahibi bireyler ve bilinçli toplum inşası için, siber güvenlik konusunda farkındalık sahibi kurumsal bakış açısı şarttır. Siber güvenlik risklerine odaklanarak çağın gereksinimlerini karşılayabilecek hizmetlerin sunulması kamu kurumlarının birincil hedefi olmalıdır.

6.1.10. Uluslararası iş birliği

Uluslararası iş birliklerinin arttırılması, yeni teknolojilerin takibi siber güvenlik otoritesi tarafından yürütülmesi gereken önemli iş kollarından biridir. Dünyadaki gelişmelere ve iş

birlikteliklerine kayıtsız kalınması gerçek dünyada olduğu gibi çıkar ilişkilerine dayalı olarak yürütülen bir dizi politikaya bağlı olarak siber uzayda tehlikelerin hedefi haline gelmeye ve savunmasız kalabilmeye neden olabilecek bir durumdur.

Dünya politik düzeninde ilişkiler, ülkelerin birbirleriyle olan gizli veya açık birliktelikler ile sürdürülmektedir. Kalıcı ve geçici çıkar ortaklıkları ülkeler arası dostlukların oluşmasını sağlarken çıkar çatışmaları ülkelerin karşı karşıya gelmelerine neden olmaktadır. Dünya hukuk literatüründe siber güvenliğe ilişkin gelişmeler göz önüne alınarak, "Yurtta Sulh, Cihanda Sulh" ilkesiyle siber silahsızlanma ve barışı destekleyen girişimlerde Türkiye olarak en ön saflarda yer alınmalıdır. Dünya barışına katkı sağlayıcı ortaklıklar için siber güvenlik otoritesinin öncülüğünde dış ülkeler ile antlaşmalar yapılmalıdır.

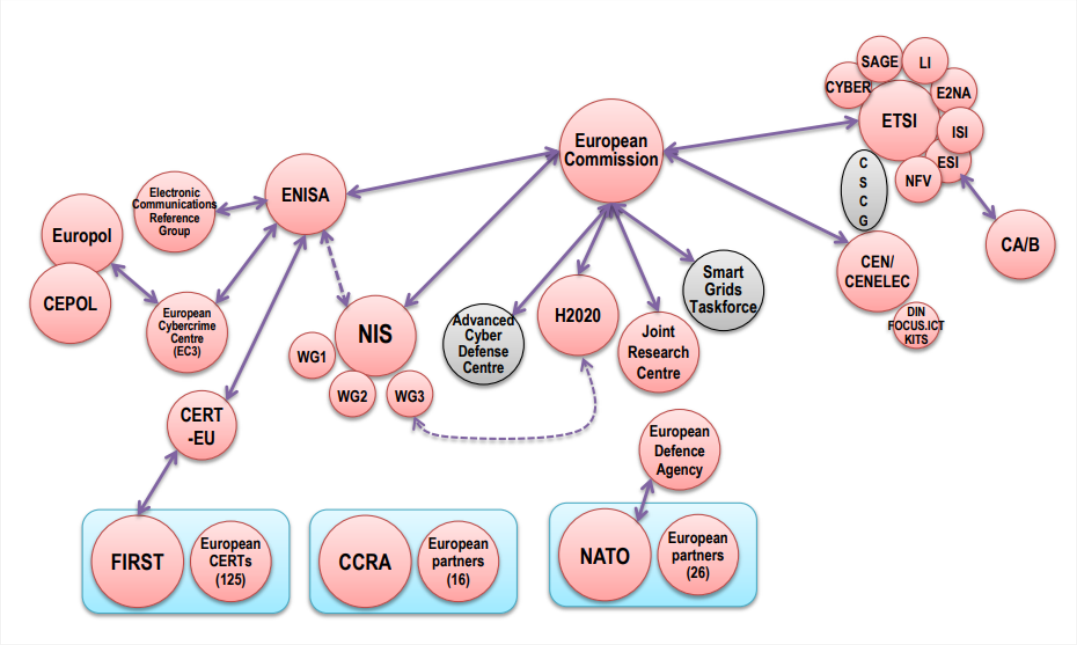
Siber savaşlara karşı dünyada barışçıl politika desteklenirken savaş nedeni sayılabilecek siber müdahalelere ve saldırılara karşı ortak savunma platformları sağlayacak uluslararası anlaşmalar yapılması gerekir.

Teknik olarak daha gelişmiş ülkeler ile anlaşmalar sağlanarak siber savunma politikalarının milli savunma sistemlerine entegrasyonu konusunda tecrübelerinden istifade edilmelidir. Siber suçluların tespiti ve cezalandırılması süreçlerinde diğer ülkelerle iş birliği yapılması gerekmektedir. NATO üyesi olan ülkemizin de siber güvenliği sağlama noktasında uluslararası iş birliği amaçlı anlaşmalar yapması, siber uzayda olası tehditlere karşı savunma kabiliyetini güçlendirmesi bakımından önem arz etmektedir.

Küresel dünyada diğer konularda olduğu gibi siber güvenlik konusunda da uluslararası gelişmelerden ve politikalardan bağımsız hareket edilmesi düşünülemeyecek bir olgudur. Bu nedenle de siber güvenlik otoritesinin, kendi dış ilişkiler birimini örgütlenmesi, hem tehditleri karşılama bakımından hem de teknik gelişmeleri takip edebilme bakımından gereklidir.

Türkiye'de uluslararası iş birliği rutin gerçekleştirilen tatbikatlar seviyesinde gerçekleştirilmektedir [51]. Uluslararası çapta siber güvenliğe ilişkin çalışmalar yürüten bazı önemli kuruluşlara ilişkin kısa açıklamalara bu bölümde yer verilmiştir. Siber güvenlik ekosisteminin geliştirilmesi açısından ulusal kuruluşların, örneğin; Avrupa Komisyonu ve ona bağlı Siber Güvenlik Koordinasyon Grubu (Cybersecurity Coordination Group), ENISA (European Network and Information Security Agency), Avrupa Güvenlik Organizasyonu

(European Organization for Security), Elektronik İletişim Grubu (Electronic Communications Reference Group), Ağ ve Bilgi Güvenliği Grubu (Network and Information Security) ile EC3 gibi kuruluşların çalışmalarının takip edilmesi oldukça önemlidir. Bu gibi siber güvenlik alanında çalışan küresel kurumlarla siber güvenlik otoritesi ve ilgili diğer kurum ve kuruluşların sağlayacağı bağlantılar, uluslararası iş birliğinin geliştirilmesi bakımından önem arz etmektedir. Şekil 6.11'de Avrupa Birliği'nin siber güvenlik ekosisteminde yer alan kuruluşları görülmektedir.



Şekil 6.10. Avrupa siber güvenlik ekosistemi [38]

6.1.11. Eğitim sisteminde yenilikler

İnternete erişimin erken çocukluk döneminde sağlanabiliyor olması, teknolojinin olumsuz yanlarından biri durumundadır. Birçok siber tehdit unsurunu barındıran internete çocukların erişimi, ailelerinin gözetiminde olmalıdır. Okul çağına gelmiş çocuklar ise siber tehditlere karşı, siber güvenlik eğitimleriyle desteklenmelidir.

Clark, Çin eğitim sisteminde siber güvenliğe verilen önemi; "Çin'deki siber savaş birliklerinin komutanı bir yarbay. Bu hücrelerdeki birliklerin üyeleri daha ilkokul düzeyinde istihdam ediliyor. İlkokul sonrası ortaokul ve lisede çeşitli bilişim derslerine tabi tutularak direkt bir şekilde Otomasyon Üniversitesi Komutanlığı'na girmektedirler. Bu üniversitenin odaklandığı tek konu, düşmanların ağ şebeke sistemlerinin nasıl hack edileceği. Şu anda 700 kadar öğrenci burada okuyor. Birbirlerine karşı siber savaşçılık teknikleri tatbikatları

yürütüyorlar. Bazıları da Japonya'ya sızarak en son bilişim teknolojilerini öğreniyor." ifadeleriyle vurgulamaktadır [13].

Şimdilere kadar yalnızca temel bilgisayar dersleriyle yetinilen müfredatlar yenilenmelidir. Bu anlamda MEB ve siber güvenlik otoritesi iş birliği içerisinde olmalıdır. Yeni nesil teknolojiler ve teknolojinin doğru kullanımı ile siber tehditlerden korunma yöntemleri MEB'in ilgili birimleri ile paylaşılmalıdır. Siber tehditlere ve siber zorbalıklara karşı en savunmasız olan ve geleceğimizi inşa edecek çocuklarımızı, onların anlayabileceği düzeylerde siber güvenlik eğitimleri ile bilinçlendirmek MEB'in çalışma alanına girmektedir.

Zorunlu temel eğitim sonrası üniversitelerde verilen derslere de aynı şekilde siber güvenlik tehdit unsurlarını ve korunma yöntemlerini içeren dersler eklenmelidir. Temel bilgisayar kullanımı vb. öğretmeyi hedefleyen bilgisayar dersleri günümüz bilişim dünyası için güncelliğini kaybetmiştir. Bu nedenle özellikle ön lisans ve lisans düzeyindeki öğrencilerin siber güvenliğin temellerini içeren eğitimlerle bilgilendirilmesinde fayda vardır. Bu noktada siber güvenlik otoritesi ve YÖK arasında iş birliği gerekecektir. Ders içeriklerinin belirlenmesi amacıyla akademisyenlerle toplantılar düzenlenerek fikir alışverişinde bulunulabilir.

Ülkemizde siber güvenliğe ilişkin olarak eğitim ve istihdam kuruluşları arasında daha güçlü bir bağ kurulması ve siber güvenlik eğitimlerinde karşılaşılan açığın kapatılması gerektiği bilinmektedir [166]. Bu anlamda, üniversitelerde ön lisans, lisans, lisansüstü eğitimlerde siber güvenlik ile ilgili bölümlerin ve ana bilim dallarının kurulmasına ve geliştirilmesine yönelik olarak yine akademisyenler ile toplantılar düzenlenebilir. Ortak yürütülen çalışmalar neticesinde ihtiyaca binaen bu konuda üniversite eğitimli gençlerin yetişmesi için belirgin adımlar atılmış olacaktır. Yalnızca güvenlik eğitimlerine odaklı akademilerin kurulması konusu da gündeme getirilebilir. Nitelikli personelin sağlanması ancak uluslararası düzeyde geliştirilen ve geçerliliği olan programlar sayesinde gerçekleştirilebilecektir. Bu adımlar siber güvenlik alanında kalifiye eleman arayışının giderilmesine de katkı sağlayacaktır. Siber güvenliğe akademik desteğin artışının getirisi olarak bu alanda eğitimli, kabiliyetli, nitelikli ve daha donanımlı personeller kurumlarda yerini alacaktır. Bu da yerli üretimi ve milli güvenliğin sağlanmasında yerli ürünlerin kullanımının yaygınlaşmasını tetikleyecektir.

Siber güvenlik otoritesinin eğitim faaliyetlerinde öncelikli olarak Milli Eğitim Bakanlığı, üniversiteler ve YÖK ile diğer özel eğitim kuruluşlarıyla iş birliktelikleri, çalışma planları yapması gerekmektedir. Günün gereklerini karşılayabilecek siber dünyaya dair eğitim programları her yaştan birey için gereklidir. Bu anlamda ilk eğitim düzeyinden son eğitim düzeyine kadar siber güvenlik konularında bilincin arttırılması amacıyla eğitimler yaygınlaştırılmalıdır. Eğitim faaliyetlerinin yaygınlaştırılması toplumsal bilincin artmasını da sağlayacaktır. Türkiye'nin strateji belgesinde eğitim konuları dar kapsamlı olarak ele alınmıştır [51].

Şekil 6.11. Eğitim sisteminde yenilikler

Mesleki yetkinliklerin standart hale gelebilmesi ve üniversite eğitimlerinin gerçek iş hayatı ile daha uyumlu hale gelebilmesini sağlamak adına, Mesleki Yeterlilik Kurumu ile YÖK arasında çalışmaların koordinasyonu siber güvenlik otoritesi tarafından sağlanmalıdır.

6.1.12. Belgelendirme ve sertifikasyon mekanizması

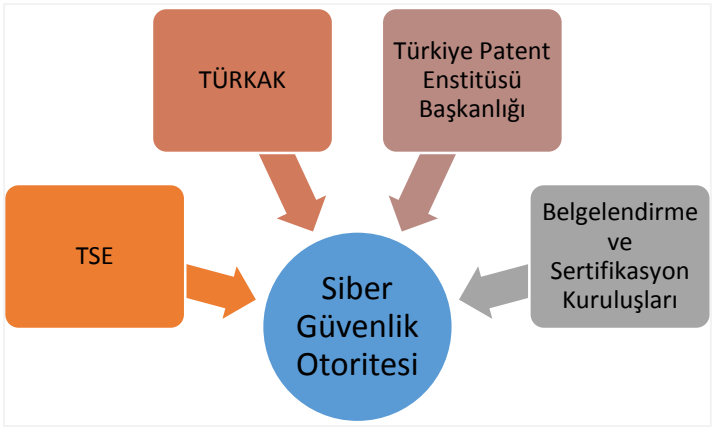
Kamu personelinin dönemsel olarak temel siber güvenlik eğitimleri verilmesi ve bu sürecin siber güvenlik otoritesi eliyle yürütülmesi gereklidir. KamuNet, internet ortamında yalıtılmış alan olarak sadece kamu kurumlarına özel bir altyapı sağlamaktadır. Bu özel TTVPN ağı, siber saldırılara karşı daha korumalı bir ortam olması bakımından eğitimlerde kullanılabilir. Bu teknolojiden faydalanmak kalabalık eğitimlerde kolaylık sağlayacaktır.

TSE ile iletişim halinde olunarak siber güvenlik ile ilgili dünya standartlarının Türkçeleştirilmesi ve yaygınlaştırılması konusunda adımlar atılmalıdır. TSE tarafından yürütülen kişilerin ve danışmanlık firmalarının sertifikasyon ve belgelendirme işlemlerinin siber güvenlik otoritesi tarafından takip edilmesi gerekmektedir. Çeşitli yarışmalar ile siber

güvenlik alanına merak duyan gençler teşvik edilmeli, başarılı gençler belgelendirilmeli ve ödüllendirilmelidir.

Kamu kurumlarının, uluslararası geçerliliği olan ISO/IEC 27032 gibi siber güvenliğe ilişkin standartlara uyumunun takibi siber güvenlik otoritesi tarafından yapılmalıdır. Standartlara uyum siber güvenlik otoritesinin koordinasyonunda, dönemsel olarak sızma testleri yapılmak suretiyle denetlenmeli ve bu konuda kurumlara yaptırımlara uygulanmadır. Düzenli ve sıkı denetimler kurumların bilgi sistemleri altyapısının bütüncül olarak güçlenmesini sağlayacaktır.

Yerli ve yabancı menşeili donanım ve yazılımların kullanıma uygunluk denetimleri otorite tarafından veya yetkilendirilmiş akreditasyon kurumlarının eliyle gerçekleştirilmelidir. Belgelendirme ve sertifikasyon süreçleri özenle yönetilmelidir. Yerli yazılım ve donanımların belgelendirilmesi ve sertifikasyonlar verilmek suretiyle sınıflandırılması, üretilen ürünlerin belirlenmiş özellikleri taşımasını şart koşması bakımından teknolojik ortamın belli bir kalite düzeyine çekilmesini sağlayacaktır. Bu anlamda, TSE ve TÜRKAK ile koordinasyon halinde çalışmalar yürütülmesi gerekecektir. TSE'de hazırlanan ürün geliştirme standartları, kullanılacak tüm yazılım ve donanım için geçerli olacak şekilde genişletilmelidir [51].



Şekil 6.12. Siber güvenlik otoritesi, belgelendirme ve sertifikasyon ilişkileri

Bilgi sistemlerinin istenilen düzeyde korunması, bu alanda eğitim görmüş kalifiye personelin istihdamını gerektirir. Yetkilendirme ve sertifikasyon mekanizmasının doğru işletilmesi alanında uzman kişilerin istihdamını beraberinde getirecektir. Böylece bilişim sektöründe yetkinliği eğitimi ile kanıtlanmamış kişilerin istihdamının önüne geçilebilecektir.

İzlenecek yetkinlik politikalarıyla bu alanda daha eğitimli kişilerin istihdamı desteklenerek daha nitelikli işlerin üretimi sağlanabilecektir.

Siber suçlar kapsamında hizmet veren laboratuvar ve birimlerin, akredite edilme faaliyetleri ile birlikte ülkemizde ve uluslararası platformlarda yapılan incelemelerin güven, saygınlık ve geçerliliği artacaktır [169]. Ürün kalitesinin artmasına katkı sağlayacak olan akreditasyon çalışmalarını yürütmek amacıyla ülkemizde de çeşitli faaliyetler yürütüldüğü bilinmektedir [166].

Başta ETSI, Uluslararası Telekomünikasyon Birliği (ITU), Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE), İnternet Mühendisliği Görev Grubu (IETF) ve Uluslararası Standartlar Teşkilâtı (ISO) olmak üzere dünyada yaygın olarak görevler yerine getiren kurum ve kuruluşların çalışmaları takip edilerek ülkemizde siber güvenliğe ilişkin standardizasyon çalışmalarının arttırılması gerekmektedir. İş birlikleri, dünya ile eş çalışmaların yürütülmesine katkı sağlayacaktır. Öte yandan Ortak Kriterler Tanıma Anlaşması (Common Criteria Recognition Agreement) gibi birçok ülkenin katılım sağladığı, teknolojik ürünlerin fonksiyonellik ve güvenlik açısından değerlendirildiği [5] global anlaşmaların incelenerek bu anlaşmalara dahil olunmasının, yerli teknolojik ürünlerin kalitesini arttıracağı düşünülmektedir.

6.1.13. Siber güvenlik ekosistemi paydaşlarıyla düzenli değerlendirme toplantılarının gerçekleştirilmesi

Siber güvenlik otoritesinin paydaşları siber dünyada iletişimde olunan her bir birey, her bir topluluk, her bir ülkedir. Bu nedenle siber güvenlik otoritesinin uzun vadede düzenli bir şekilde yürütmesi gereken en önemli çalışmalarda biri de, bu ekosistemi oluşturan paydaşların her biri ile iletişimde kalması, her bir paydaşın ihtiyacına cevap verecek politikalar üretmesidir. Dolayısıyla paydaşlarla düzenli değerlendirme toplantıları ekosistemin sürekliliği için gereklidir. İş süreçlerinde devamlılığın ve sürekli gelişimin esas alınması, siber güvenlik ekosistemini besleyecek önemli bir unsurdur. Paydaşlara, ekosistemin sağlayacağı faydalar ile siber güvenlik otoritesinin çalışmalarına ne kadar özen gösterdiği birbiriyle doğru orantılıdır. Bu anlamda ekosistemin faydalarına odaklanan her bir paydaş uzun ve kısa vadede siber güvenlik ekosisteminin gelişimine katkı sunacaktır.

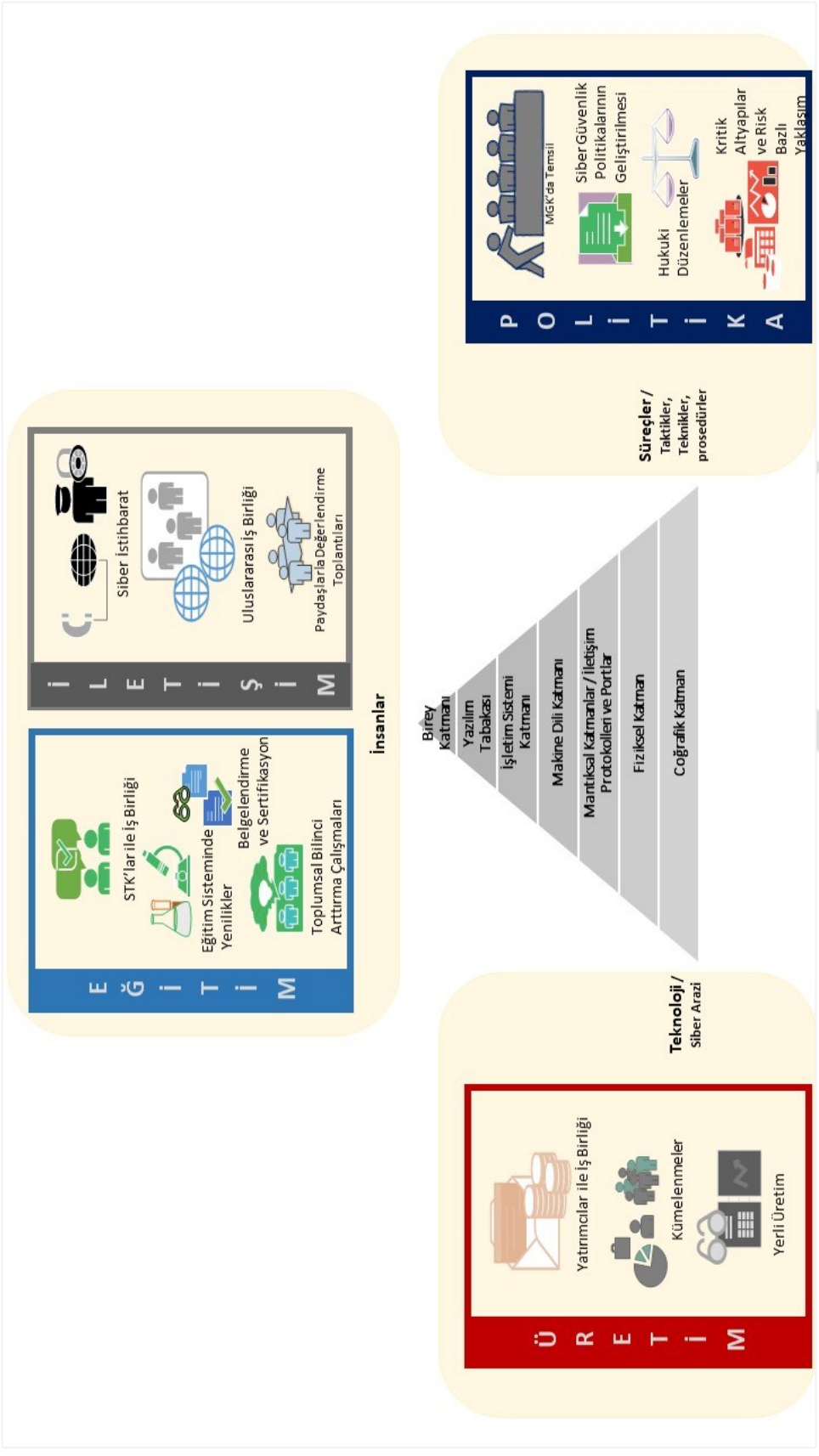
Kurulacak kamu otoritesi, siber güvenlik ekosisteminin paydaşlarıyla, düzenli aralıklarla toplanarak, değişen ve gelişen dünyaya paralel olarak ihtiyaçların belirlenmesi ve bu ihtiyaçlara çözümler üretilmesi üzerine çalışmalar yapmalıdır.

Siber güvenlik ekosisteminde her sektörün kendine göre ihtiyaçları olması bakımından, her paydaşın kendi sektörüne yönelik eksiklere odaklanarak kamu otoritesini bilgilendirmesi beklenmektedir. Kamu otoritesi, paydaşların önerilerine istinaden çeşitli çalışmalar yürüterek siber sürekliliği sağlayacaktır. Stratejik planlama kapsamında vatandaş, özel sektör, kamu kurum ve kuruluşların üzerlerine düşen görevlerin açıklanmadığı [51] gözlenmiştir.

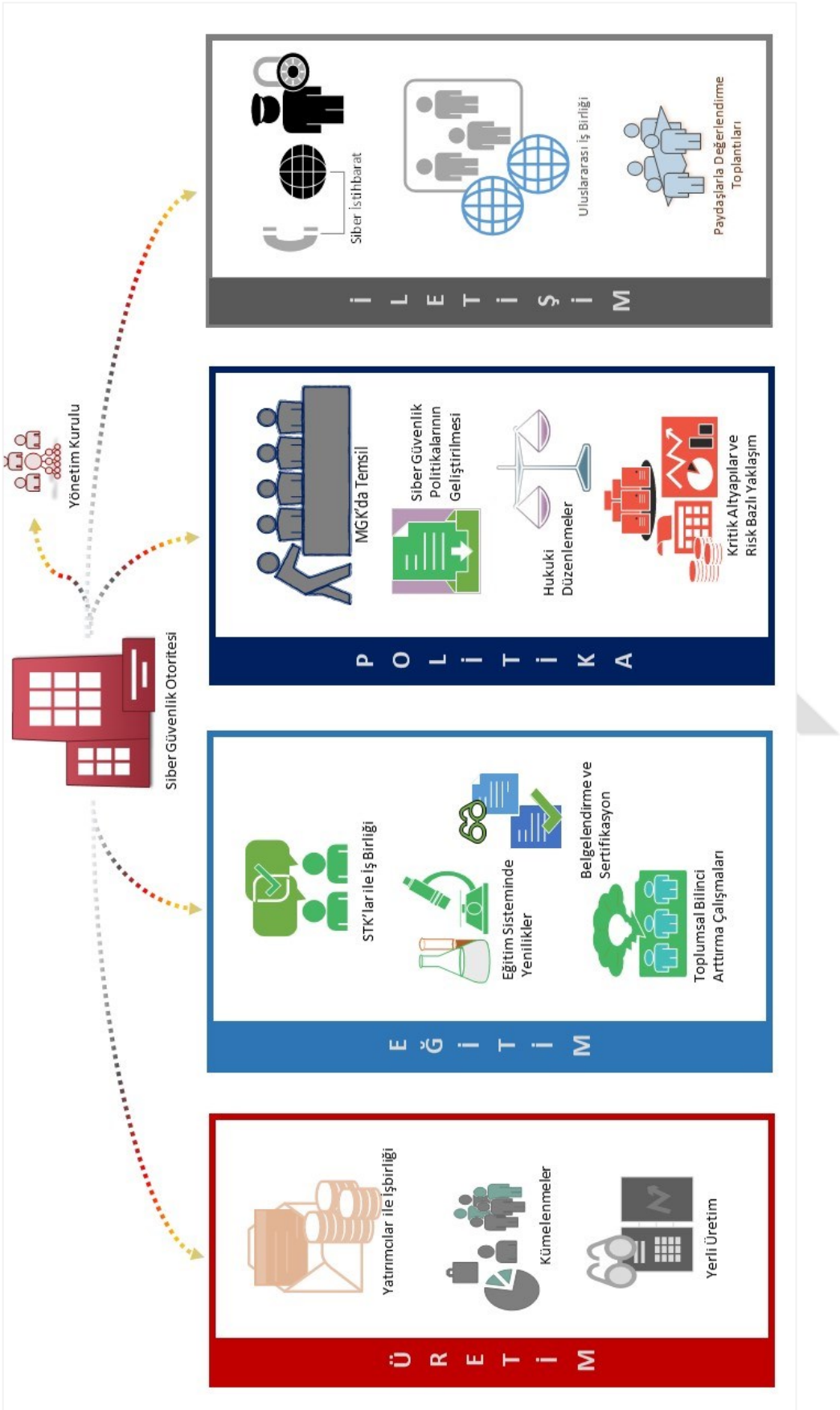
ITU'nun yayımladığı raporda, siber güvenlik stratejilerinin geliştirilmesinde olduğu gibi, uygulanması aşamasında da tek bir otoritenin sorumluluk sahibi olarak görülmesi yanlış bir yaklaşımdır. Bunun yerine, sivil toplumdan ve özel sektörden destek alınması, hükümet genelinde bir dizi farklı paydaşın katılımının sağlanması ve bu katılımcıların koordinasyonunun gerektiği ifade edilmiştir [160].

6.2. Siber Güvenlik Ekosistemi Model Önerisi

Siber güvenlik ekosisteminin geliştirilmesini hedefleyen temel süreçleri içeren Şekil 7.1'in hazırlanmasında, Riley'nin siber güvenlikte esas aldığı üç ana başlık [41] referans alınmıştır. Bu anlamda üretim bandı, teknolojileri; eğitim ve iletişim bantları insanları, politikalar bandı ise süreçleri temsil etmektedir. Ekosistemin sürekliliği sağlayan koordinasyon ve iş birliğini sağlayan otorite ise Şekil 7.2'de ifade edildiği gibi temel olarak belirlenen süreçlerin yürütülmesinden ve ekosistemin işlerliğini takipten sorumludur.



Şekil 6.13. Ekosistem geliştirme kıstaslarının sınıflandırılması



Şekil 6.14. Otoritenin yönetmesi öngörülen temel alanlar

Ülkemizde devlet organizasyonunun yeniden yapılanması süreçleri neticesinde Cumhurbaşkanlığı'na bağlı olarak kurulan iki önemli kurumun bilgi teknolojileri alanında çalışmalar yürüteceği bilinmektedir. Bu kurumlardan biri olan Bilim, Teknoloji ve Yenilik Politikaları Kurulu'nun Cumhurbaşkanı'na teknoloji alanında üretilecek politikaların belirlenmesini sağlayacak çalışmalar sunacağı beklenmektedir. Bir diğer kurum olan Dijital Dönüşüm Ofisi'nin ise siber güvenlik, büyük veri, yapay zeka vb. teknik konular baz alınarak ülke çapında dönüşüm çalışmaları yürüteceği ifade edilmektedir. Siber Güvenlik Kurulu'nın icrai görevlerinin iptal edilmesi neticesinde siber güvenlik alanında karşılaşılan yönetimsel eksikliklerin oluşturulan bu kurumlar veya yeni bir güçlü otorite ile giderilmesi gerekmektedir.

Çalışma kapsamında incelenen ülkelere bakıldığında; siber güvenlik konulu süreçlerin yönetiminin, çalışma alanı özellikle siber güvenlik veya bilgi güvenliği olan ajanslar tarafından yerine getirilmektedir. Bu ülkelerde siber güvenliğe ilişkin çalışmaların genellikle bakanlıklar düzeyinde yönetim organları tarafından özellikle desteklenmektedir, devletin en üst merciine karşı sorumlulukları olan konseyler bulunmaktadır. Bu konseyler, politika ve projelerin üretiminden ve bu politikların yürütülmesinden sorumludur. Ayrıca bu konseyler, kilit kamu kuruluşları ve özel sektör temsilcilerini de kapsayacak şekilde oluşturulmuştur. Danışma kurulları ve uzman konferansları (Uzman konferansları, belirli bir alana yönelik olarak uzmanlık gerektiren bir husus mevcut ise, bu alanda bilgi düzeyini arttırma amaçlı yapılan, alanında uzman olan kişilerin bilgisinden istifade edilebilecek kongre, toplantı, konferans vb. anlamında kullanılmıştır.) yoluyla siber güvenlik konseylerinin bilgi yönünden desteklendiği gözlenmiştir. Ülke örnekleri arasında, kritik altyapıların korunması amacına yönelik çalışmalar yürüten ayrı kurumlar oluşturulduğu, kritik altyapıların korunması hedefiyle diğer strateji belgelerine ek olarak ulusal politikalar yayımlandığı gözlenmiştir. Standardizasyon çalışmalarını yürüten standart organizasyonlarının siber güvenliğe ilişkin çalışmalar yürütmektedir. Bu kurumlar, standartlaşma konusunda küresel organizasyonlarla iş birliği halindedir. Ülkemizde olduğu gibi, siber olaylara müdahale merkezlerinin ve müdahale ekipleri siber tehditlere karşı görevler yerime getirmektedir. Ek olarak bu ekipler, küresel müdahale ekipleri ile iş birliği ve dayanışma halindedir, çeşitli anlaşmalar doğrultusunda siber tehlikelere karşı ortak çalışmalar yapmaktadırlar. Üniversitelerde araştırma geliştirme laboratuvarları kurulmuştur, mükemmeliyet merkezleri oluşturulmuştur ve bu merkezler maddi anlamda devlet tarafından önemli ölçüde desteklenmektedir.

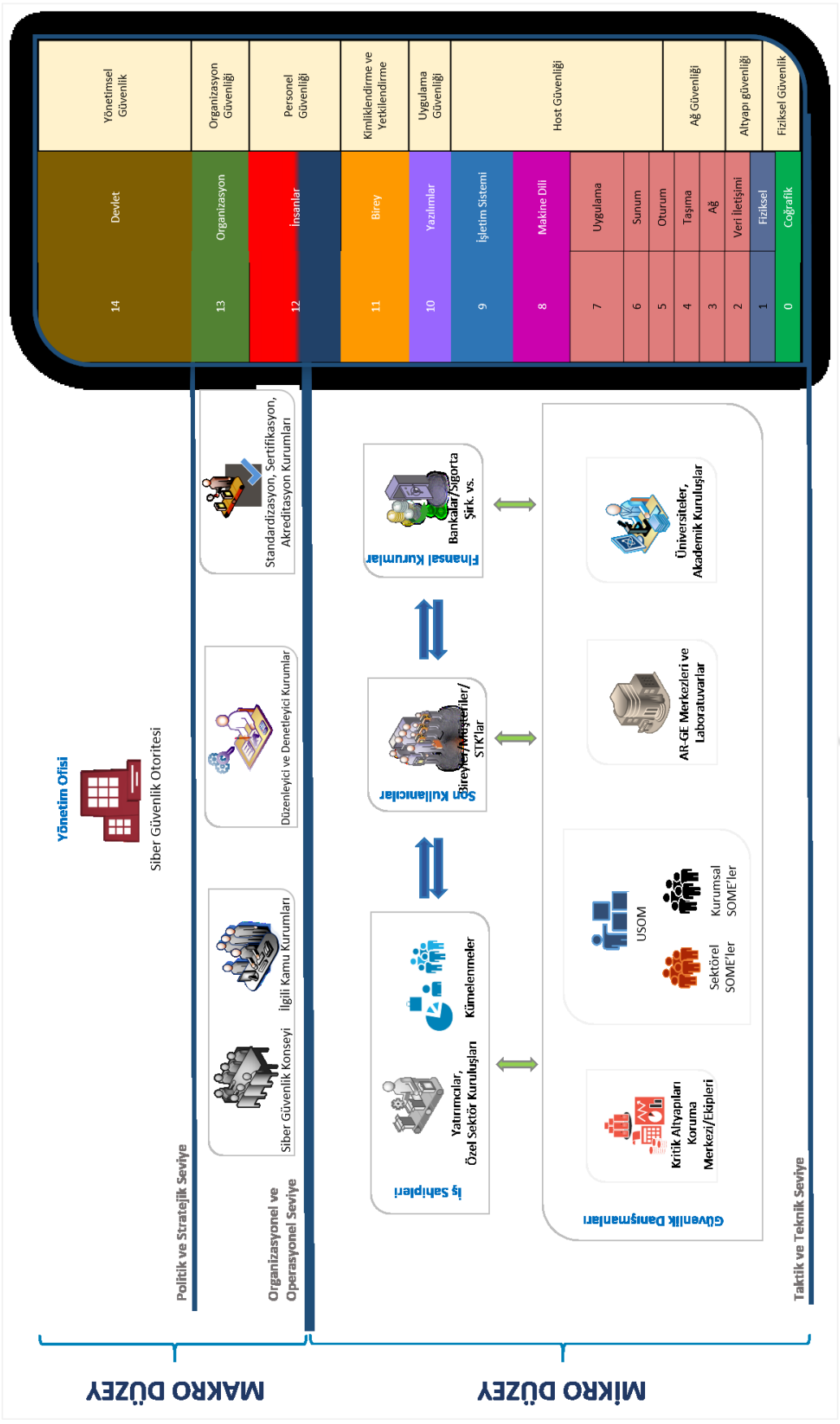
Raghu, siber güvenlik ekosistemini (Bkz. Şekil 2.11), iki ana başlık olarak mikro ve makro düzeyde sınıflandırmıştır [38]. 2016-2019 Ulusal Siber Güvenlik Stratejisi incelendiğinde, siber güvenlik organizasyonunda, Siber Güvenlik Kurulu'nun yer aldığı, düzenleyici denetleyici kurumların kendi çalışma alanları ile ilgili siber güvenliğe ilişkin riskleri minimize etmek için denetimler yürütmesi gerektiği ifade edilmiştir. Aynı belgede, siber olayların sektörel ve kurumsal siber olaylara müdahale ekipleri tarafından takibi konularının stratejik siber güvenlik amaçları ve eylemleri arasında sayıldığı görülmektedir. Ayrıca ilgili belgede, merkezi bir kamu otoritesinin koordinasyon amacıyla oluşturulması gerektiği de hedefler arasında yer almaktadır [16]. Ulaştırma ve Altyapı Bakanlığı internet sitesinde yer alan şekliyle ülkemizde mevcut siber güvenlik yapılanması [140] incelendiğinde, çalışmanın "6.1. Siber Güvenlik Ekosisteminin Geliştirilmesinde Önemli Kıstaslar" bölümünde detaylı olarak açıklandığı üzere, koordinasyonun daha merkezi bir otorite terafından sağlanması gerektiği görülmektedir. Ülkemizdeki mevcut siber güvenlik organizasyonu incelendiğinde, makro düzeyde, düzenleyici otoritelerin ve standardizasyon kuruluşlarının da ekosistemde yer almadığı görülmektedir. Öte yandan Riley'nin (Bkz. Şekil 2.12 ve Şekil 2.13) katmanlı modelleri baz alındığında, devlet yönetimi veya yönetişim katmanında kabul edebileceğimiz kurumlar ile siber güvenliğe ilişkin süreçleri organize edecek kurumların birbirinden ayrılmış olması, siber güvenlik konusunun daha doğru bir şekilde ele alınabilmesine katkı sağlayacaktır.

Çalışma neticesinde Raghu (Bkz. Şekil 2.11) ve Riley'nin (Bkz. Şekil 2.12 ve Şekil 2.13) oluşturduğu katmanlı yapılar hibrit bir şekilde ele alınarak Şekil 6.15'de yer alan siber güvenlik ekosistemi modeli oluşturulmuştur. Önerilen siber güvenlik ekosistemi modeli, Makro Düzey ve Mikro Düzey olmak üzere iki esas düzeye ayrıştırılmıştır. Makro Düzey, Politik ve Stratejik Seviye ve Organizasyonel ve Operasyonel Seviye olmak üzere iki alt seviyeye daha ayrılmıştır. Mikro Düzey ise, Teknik ve Taktik Seviye'de görev ifa eden paydaşların yer aldığı topluluğu ifade etmektedir.

Önerilen siber güvenlik ekosisteminde Makro Düzey, siber güvenliğe yön verici kurumlardan oluşan bir topluluktur. Bu düzey, Riley'nin siber alan detaylı katmanlı modelinde [40] ifade edilen 12. Katmanın bir kısmı ve 13-14. katmanlara ilişkin politik, stratejik, organizasyonel ve operasyonel iş süreçlerini yürüten kurum ve kuruluşlara karşılık gelmektedir. Bu düzeyde, Politik ve Stratejik Seviye'de, siber güvenliğe ilişkin yasa gereksinimlerini belirleyen, düzenlemelerin yapılmasında ve politikaların geliştirilmesinde

ve uygulanmasında en üst seviye olan, siber güvenlik konusunda yönetişimi sağlayacak siber güvenlik otoritesi yer almaktadır. Organizasyonel ve Operasyonel Seviye, Raghu'nun ifade ettiği (Bkz. Şekil 2.11) politika üretici, düzenleyici ve standart koyucu kurumlardan oluşmaktadır. Bu seviye; siber güvenliğe yön verecek önemli kurum ve kuruluşları bulundurması bakımından ikincil yönetim mekanizması olarak işlemektedir. Bu seviyede, siber güvenlik politikalarının belirlenmesi, oluşturulması süreçlerinde karar alabilecek bir siber güvenlik kuruluna yer verilmiştir. Siber güvenliğe ilişkin düzenleyici kararların alınması, uygulanması ve alana ilişkin denetimlerin yapılması açısından düzenleyici denetleyici kuruluşların organizasyonel ve operasyonel olarak çalışmalar gerçekleştirmesi gerekmektedir. Bilginin daha doğru ve güvenilir kullanımına ilişkin çalışmaların yürütülmesi, yerli yazılım ve donanım üretimi, üretilen ürünlerin belirlenen standartlara uygunluğunun kontrolü ile bu ürünlere ilişkin belgelendirme ve akreditasyon süreçlerini yürütmek üzere, konuyla ilgili standardizasyon ve akreditasyon kurum/kuruluşlarının organizasyonel ve operasyonel seviyede sorumlulukları bulunmaktadır.

Modelde yer alan Mikro Düzey; Taktik ve Teknik Seviye'de görevler yerine getiren kurum, kuruluş ve bireylerin bütünüdür. Mikro düzeyde yer alacak kurum ve kuruluşlar tarafından, Riley'nin çalışmasında yer alan [40] 0-11. katmanlar ve 12. katmanı da kısmen kapsayan katmanlarda teknik ve taktik seviyede iş süreçlerinin işletilmesi gerekmektedir. Bu bağlamda Taktik ve Teknik Seviye, Raghu'nun ifade ettiği (Bkz. Şekil 2.11) iş sahipleri, tüketiciler/son kullanıcılar ve finansal kuruluşlardan oluşmaktadır. İş sahipleri, son kullanıcılar ve finansal kuruluşlar güvenlik danışmanları tarafından siber güvenliğe ilişkin konularda bilgi ve beceri bakımından teknik ve taktik seviyede beslenmekte ve desteklenmektedir. Güvenlik danışmanı olarak sayılabilecek paydaşlar ise, araştırma geliştirme merkezleri, siber olaylara müdahale merkezleri ve ekipleri, kritik altyapıların korunmasını amaçlayan merkezler ve ekipler ile akademik çevre ve bu alanda görev yerine getirebilecek diğer paydaşlardır. Bu şekilde değerlendirildiğinde Taktik ve Teknik Seviye; bireyleri, finans kuruluşlarını, yatırımcıları, özel-ticari kurum ve kuruluşları, kümelenmeleri, sayılan bu paydaşlarla iş birliği yaparak siber olaylara karşılık veren siber olaylara müdahale merkezlerini, akademik kurumları ve araştırma geliştirme merkezlerini de içine alacak şekilde, nicelik ve nitelik olarak genişletilebilecek diğer paydaşları kapsamaktadır.



Şekil 6.15. Siber güvenlik ekosistemi model önerisi

7. SONUÇ VE ÖNERİLER

Siber güvenlik, bir bütün halinde düşünülmesi gereken yeni ve çok hızlı gelişir yapıda bir çalışma alanıdır. Siber güvenlik politikalarının uygulanması ve takibi için ciddi emek sarf edilmesi gerekmektedir. Ülkemizde bu alana ilişkin çeşitli çalışmalar yürütülmüştür. İşletilmesi gereken bir takım yeni süreçlerle beraber daha donanımlı bir siber güvenlik organizasyonu elde edileceği düşünülmektedir.

Siber güvenlik ekosistemi, siber uzayın getirdiği yenilik ve kolaylıkların arkasına saklanan siber tehditleri bertaraf etmek, siber riskleri asgari düzeye çekebilmek amacıyla sürekli olarak işletilmesi gereken bir iş birlikteliğini ifade etmektedir. Bu çalışmada detaylarına yer verilen siber güvenlik ekosistemi, devlet hiyerarşisinin en üst seviyesinden başlanarak, toplumu meydana getiren en temel unsur olan her bir bireyin ekosisteme dahil edilerek işletilmesi gereken bir yapıdır. Bu bağlamda, siber güvenlik ekosisteminin geliştirilmesi için ilk olarak siber alanı koordine edecek otoritenin belirlenmesi gerekmektedir. Öncü otoritenin belirlenmesi paydaşlar arasında koordinasyonun sağlanmasında en önemli konulardan biridir.

İncelenen ülkeler göz önünde bulundurulduğunda, siber güvenliğe ilişkin konuların tek yönetim otoritesi tarafından koordine edilmesi gerekmektedir. Ülkemizde devlet yönetiminin yeniden yapılandırıldığı da göz önüne alındığında, Siber Güvenlik Kurulu'nun görevlerinin iptali durumuyla birlikte siber güvenlik alanında yönetimsel bir takım eksikliklerin oluştuğu açıktır. Bu durum fırsat bilinerek böylesine önemli olan bir alanda siber güvenlik konusunun daha sağlam bir zemine oturtulması ve geleceği öngören bir yaklaşımla hareket edilmesi gerekmektedir. Cumhurbaşkanlığı'na bağlı olarak kurulan Dijital Dönüşüm Ofisi ve Bilim, Teknoloji ve Yenilik Politikaları Kurulu'nun siber güvenlik ekosisteminde yönetim pozisyonlarında roller alması durumunda, siber güvenliğe ilişkin devlet hiyerarşisinde üst seviyede ve merkezi bir yönetim sağlayanabileceği düşünülmektedir. Bu sayede, siber güvenlik risklerinin sebep olacağı aksaklıkların ve siber tehditlerin tetikleyeceği kamu düzeninin bozulması, toplumsal kaos ortamının yaşanması gibi büyük risklerin etki düzeyine ilişkin üst yönetim kademelerinin daha detaylı bir şekilde bilgilendirilmesi, siber güvenlik ekosistemini oluşturan diğer paydaşların ise daha kolay bir şekilde yönetilmesi sağlanacaktır.

Siber güvenlik konusunda geliştirilecek politikalar olabildiğince geniş olarak ele alınmalıdır. Yapılacak yatırımlar ise geleceği de öngörecek şekilde planlanmalıdır. Siber güvenlik ekosisteminin doğru ve aktif bir şekilde işletilmesi, ekosistemin canlı tutulması siber güvenlik risklerine bir bütün olarak cevap verilmesine olanak tanır. Siber güvenlik otoritesinin, siber güvenlik politikalarını günün gereklerini karşılayacak şekilde geliştirmesi, uygulaması, yapılan uygulamaların yeterliliğine yönelik değerlendirmeleri takip etmesi ve dönemsel denetimler yapması gerekmektedir.

Siber güvenlik konusunda organizasyonel ve operasyonel olarak politika üretmek amacıyla ikincil bir yönetim mekanizması işletilmelidir. Önerilen siber güvenlik ekosistemi modelinde detaylı olarak açıklandığı üzere bu seviyede, kilit kurum ve kuruluşlardan oluşan yeni bir konsey veya kurul oluşturulmalıdır. Oluşturulacak konsey, uzmanlık gerektiren konularda bilgi yönünden desteklenmelidir. Öte yandan sektörel alanlarda politikalar üretilebilmesi, bunların denetlenebilmesi amacıyla düzenleyici ve denetleyici kuruluşlara bu seviyede görevler verilmelidir. Siber güvenliğe ilişkin ürünlerde standartlaşmaya gidilmesi, siber güvenliğe ilişkin yeterliliğin belirlenmesi amacıyla kurumların akredite edilmesi ve belgelendirilmesi amacıyla standardizasyon, akreditasyon ve belgelendirme kuruluşlarına da bu seviyede yer verilmesi gerekmektedir.

Ülkemizde siber güvenlik risklerine karşı yürütülen işlerden sorumlu olan USOM-SOME yapılarının tüm siber güvenlik ekosistemi paydaşlarını besleyecek şekilde geri bildirimlerde bulunması gereklidir. Önerilen siber güvenlik ekosistemi modelinde teknik anlamda bilgi aktarımı sağlayan güvenlik danışmanı konumundaki siber olaylara müdahele ekipleri/merkezleri, ekosistemde siber risklerin yayılımını engellemeye odaklanmalıdır. Bu ekiplerin/merkezlerin güçlendirilerek benzer göreve sahip uluslararası çalışmalar yürüten kurumlarla iş birliği noktasında çalışmalarını arttırması gerekmektedir.

Siber istihbarat amaçlı çalışmalar, ekosistemde hem organizasyonel ve operasyonel seviyede hem de teknik ve taktik seviyede yürütülmelidir. Siber güvenlik otoritesinin, oluşturulacak siber güvenlik konseyinin ele aldığı konular ve kararlar neticesinde belirleyeceği politikaların ülke genelinde karşılık bulabilmesi için ülke milli güvenlik politikalarının belirlendiği Milli Güvenlik Kurulu'nda temsili sağlanmalıdır.

Hukuki gereksinimlerin uygulamaya geçirilmesi amacıyla organizasyonel ve operasyonel seviyede ilgili kamu kurumlarından ve uzman görüşlerinden faydalanılarak politikalar

belirlenmeli, ayrıca gerekli görülen alanlarda kanuni düzenlemeler için öneriler sunulabilmelidir. Siber güvenlik ekosisteminde yeni teknolojilerin kullanımından kaynaklanan hukuk problemlerinin çözümü için hem bilgi teknolojileri hem hukuk alanında belirli seviyede bilgi birikimine sahip kişilere ihtiyaç vardır. Bu anlamda dünyada bilgi teknolojilerine ilişkin yeni hukuki düzenlemeler ve ülke içinde karşılaşılan siber güvenlik ihlalleri, hem hukuk hem bilgi teknolojileri konusunda bilgi birikimine sahip uzman kişiler tarafından özenle takip edilmelidir. Siber güvenlik otoritesi, hukuki sorunların çözümüne katkı sağlamak amacıyla disiplinler arasında iş birliğini teşvik eden mekanizmaları kurmalıdır.

Kritik altyapıların korunmasına daha fazla önem gösterilmelidir. Bu anlamda çeşitli ülke örneklerinde olduğu gibi yalnızca bu konu ile ilgilenen ayrı bir kuruluş oluşturulabilir. Böyle bir yaklaşımın benimsenmesi, kritik altyapıların korunması amacıyla çıkarılması gereken strateji belgelerinin daha kapsamlı hazırlanmasına olanak tanıyacaktır. Öte yandan, siber güvenlik ekosisteminde, oluşturulması halinde, kritik altyapıları koruyan ekiplerin/merkezlerin, ekosistemin diğer paydaşlarını teknik anlamda beslemesi gerekmektedir.

Yatırımcıların, kümelenmeler yoluyla iş ve istihdam ağlarını genişletme süreçleri siber güvenlik ekosisteminde, desteklenmesi ve kapsamlı çalışmalar yapılması gereken bir alandır. Yerli üretimin siber güvenlik ekosisteminde desteklenmesi için bireyler, finans kuruluşları ve yatırımcılar arasında bir sinerji oluşturulması gerekmektedir. Bu amaca yönelik siber güvenlik otoritesi tarafından yapılacak çalışmalar, konseyin, düzenleyici ve denetleyici kuruluşlar ve standardizasyon, akreditasyon ve belgelendirme kuruluşlarının geliştireceği politikalarla şekillendirilmelidir. Güvenlik danışmanı konumundaki siber olaylara müdahale ekipleri/merkezleri, araştırma geliştirme merkezleri, üniversiteler ve akademik çevre, yatırımcıları, bireyleri ve finans kuruluşlarını teknik olarak beslemelidir. Böylelikle geliştirilecek politikalara ve standartlara uygun, teknik anlamda güvenilir yerli ürünlerin üretilmesi sağlanabilecektir.

Toplumu oluşturan bireyler, siber güvenlik ekosisteminin merkezinde yer almaktadır. Bu anlamda bireylerin bilgi seviyesini arttırmak amacıyla sivil toplum kuruluşlarının desteği siber güvenlik ekosisteminde önemsenmesi gereken bir diğer konudur. Siber güvenlik ekosisteminde makro düzeyde geliştirilen tüm politikalar, esasında, bireylere ait bilgi

varlıklarının güvenilir bir şekilde korunduğu güvenli bir toplumda yaşayabilmesini amaçlayacak şekilde üretilmelidir. Bireyler teknik anlamda güvenlik danışmanı konumundaki siber olaylara müdahele ekipleri/merkezleri, araştırma geliştirme merkezleri, üniversiteler ve akademik çevre tarafından bilgi bakımından beslenmelidir.

Siber güvenlik ekosisteminde, her kurum ve kuruluş, uluslararası boyutta görev alanına karşılık gelen kurum ve kuruluş ile iş birliğine giderek çalışmalarını yerine getirmelidir. Uluslararası iş birliği, siber olayların yönetiminde güncel kalabilmeye, savunma mekanizmalarının daha doğru işletilmesine, hukuki süreçlerin günün gereklerini karşılayacak şekilde revize edilebilmesine ve siber güvenlik konusunda yeni gelişmelerin takibine katkı sağlayacaktır.

Eğitim sisteminin geliştirilmesi amacıyla siber güvenlik ekosisteminin makro ve mikro düzeyinde bir takım iyileştirme çalışmalarının yürütülmesi gerekmektedir. Bu anlamda yine ilgili görülen kamu kuruluşları ile irtibat halinde olunması gerekmektedir. Araştırma geliştirme merkezleri ve üniversitelerin siber güvenliğin gelişmesini sağlamak amaçlı çalışmaları, yatırımcılar tarafından desteklenmelidir. Bu ilişkilerin kurulması için siber güvenlik otoritesinin, uygun iş birliği politikalarını geliştirmesi ve bu ilişkilerde koordinasyon sağlaması gerekmektedir.

Siber güvenlik ekosistemi, kamu kurumlarından özel sektöre, sivil toplum kuruluşlarından yatırımcılara, öğrencilerden akademisyenlere, kamu kurumu personelinden sade vatandaşa kadar uzanan, siber uzaya dahil olan her bireyi kapsamaktadır. Siber güvenlik ekosisteminin işleyişinde koordinasyon makamı olan siber güvenlik otoritesinin nispeten fazla sorumlulukları vardır. Ancak, ekosistemin tüm paydaşları aktif olarak kendisine düşen -en azından bilginin gizliliği, bütünlüğü ve erişilebilirliği temelinde- güvenlik gereklerini yerine getirmelidir. Dolayısıyla siber güvenlik ekosisteminin, tüm paydaşların katılımı ile birlikte her zaman aktif ve canlı tutulması gerekmektedir. Siber güvenlik ekosisteminin paydaş temsilcileri düzenli aralıklarla bir araya gelerek değerlendirmeler yapabilmelidir. Siber güvenlik otoritesi, bu amaçlarla uygun platformlar oluşturarak paydaşlar arasında iletişim ve iş birliğinde sürekliliği sağlamalıdır.

Araştırma esnasında, seçilen ülkelerin çoğunda dökümantasyon eksikliği, var olan dokümanların ülkelerin kendi anadillerinde yayımlanmış olması, ülke anadilinden İngilizce'ye çevirilmiş dokümanların az olması ve ülkelerde siber güvenlik konulu görev

yürüten kurum internet sitelerinin güncel ve İngilizce olmaması gibi zorluklarla karşılaşılmıştır.

Literatür taraması yoluyla elde edilen tüm bu bilgiler ve bu doğrultuda oluşturulan Şekil 6.15'te yer alan siber güvenlik ekosistemi model önerisinin konuyla ilgili daha kapsamlı çalışmalar için temel bilgilerin yer aldığı bir başvuru kaynağı olabileceği öngörülmektedir. Var olan bilgi birikimini arttırmayı amaçlayan bu tez çalışmasından, konuyla ilgili çalışma yapmak isteyen diğer araştırmacıların istifade edebileceği ve çalışmanın uygulamalı araştırmalarda kaynak olarak kullanılabileceği düşünülmektedir.

KAYNAKLAR

1. İnternet: Okten, Ayşe Nur. Araştırmanın Çeşitli Boyutları. 2019-01-11. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.yildiz.edu.tr%2F%7Eokten%2Fimages%2FDy_2%2520Arastima%2520turleri_07.10.09.pdf&date=2019-01-11, Son Erişim Tarihi: 11.01.2019.

2. İnternet: Doğan, Güleda. Araştırma Yöntemleri. 2019-01-11. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fyunus.hacettepe.edu.tr%2F%7Eumutal%2Flesson%2Fbby606%2F2018%2Fbby606-2018-02.pdf&date=2019-01-11, Son Erişim Tarihi: 11.01.2019.

3. İnternet: Vikipedi. Siber uzay. www.wikipedia.org. 2018-09-16. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.wikizero.co%2Findex.php%3Fq%3DaHR0cHM6Ly90ci53aWtpcGVkaWEub3JnL3dpa2kvU2liZXJfdXpheQ&date=2018-09-16, Son Erişim Tarihi: 16.09.2018.

4. İnternet: Ceylan, H. Siber Alan (Siber uzay) Nedir?. halukceylan.wordpress.com. 2018-09-16. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fhalukceylan.wordpress.com%2F2014%2F11%2F13%2Fsiber-alan-siber-uzay-nedir%2F&date=2018-09-16, Son Erişim Tarihi: 16.09.2018.

5. European Telecommunications Standard Institute. (2017). Cyber: Global Cyber Security Ecosystem; ETSI, TR 103 306 V1.2.1 (2017-03). *France.*

6. Akyazı, U. (2013). *Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler.* 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı. 216-220.

7. Deloitte Touche Tohmatsu Limited. (2014). Global Siber Güvenlik Yönetici Bilgilendirme Raporu; Deloitte Türkiye. *İstanbul.*

8. İnternet: Passeri, P. August 2018 Cyber Attacks Statistics. www.hackmageddon. 2018-09-28. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.hackmageddon.com%2F2018%2F09%2F21%2Faugust-2018-cyber-attacks-timeline%2F&date=2018-09-28, Son Erişim Tarihi: 28.09.2018.

9. İnternet: Akçay, E. Siber Suç Nedir?. www.erdemakcay.av.tr. 2018-09-16. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.erdemakcay.av.tr%2Fsiber-suc-nedir%2F&date=2018-09-16, Son Erişim Tarihi: 16.09.2018.

10. İnternet: Emniyet Genel Müdürlüğü. Siber Suç Nedir?. URL : http://www.istanbul.pol.tr/sibersuclarlamucadele/Sayfalar/Siber_Suclar.aspx, Son Erişim Tarihi: 16.09.2018.

11. Keleştemur, A. (2015). *Siber İstihbarat* (Birinci Baskı). İzmit: Level Yayınevi.

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

13. Clarke, R. A.; Knake, R. K. (2011). *Siber Savaş* (Birinci Baskı). (çev. M. Erduran). İstanbul: İKÜ Yayınevi. (Eserin orijinali 2010'a yayımlandı), 29,53,140.

14. Özdağ, Ü.; Önenli Güven, M. (2015). *Teşkilat'ı Mahsusa'nın 100. Yılında Türk İstihbaratı* (Birinci Baskı). Ankara: Kripto Yayınları, 328.

15. İnternet: Ünver, M; Canbay, C; Mirzaoğlu, A. G. Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler. BTK. 2018-09-16. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.academia.edu%2F24841538%2FUlusal_Siber_G%C3%BCvenli%C4%9Fin_Sa%C4%9Flanmas%C4%B1&date=2018-09-16, Son Erişim Tarihi: 16.09.2018

16. T.C. Ulaştırma ve Altyapı Bakanlığı. (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi. *Ankara.*

17. Can, Ö.; Akbaş, M. F. (2014). Kurumsal Ağ ve Sistem Güvenliği Politikalarının Önemi ve Bir Durum Çalışması. *Tübav Bilim Dergisi*, 7(2), 16-31.

18. İnternet: Vikipedi. Bilgi güvenliği. www.wikipedia.org. 2018-09-16. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.wikizero.co%2Findex.php%3Fq%3DaHR0cHM6Ly90ci53aWtpcGVkaWEub3JnL3dpa2kvQmlsZ2lfZ8O8dmVubGnEn2k&date=2018-09-16, Son Erişim Tarihi: 16.09.2018.

19. İnternet: Kaya, M. Bilişim Güvenliği Prensipleri. www.mustafakaya.com.tr. 2018-09-17. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.mustafakaya.com.tr%2Fbilisim-guvenligi-prensipleri.html&date=2018-09-17, Son Erişim Tarihi: 16.09.2018.

20. Ünver, M; Canbay, C. (2010). Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik. *Elektrik Mühendisliği*, 438, 94-103.

21. İnternet: Karabacak, B. Kritik Altyapılara Yönelik Siber Tehditler Ve Türkiye İçin Siber Güvenlik Önerileri. www.academia.edu. 2018-09-16. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.academia.edu%2F9599603%2FKritik_altyap%C4%B1lara_y%C3%B6nelik_siber_tehditler_ve_T%C3%BCrkiye_i%C3%A7in_siber_g%C3%BCvenlik_%C3%B6nerileri&date=2018-09-16, Son Erişim Tarihi: 16.09.2018.

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

23. Milli Güvenlik Kurulu Genel Sekreterliği. (2017). 21. Yüzyılda Küresel Ekonomiyi Şekillendirecek Temel Eğilimler; MGK. *Ankara,* 1-21.

24. Karakuş, C. (Ekim, 2011). *Kritik alt yapılara siber saldırı.* TMMOB Makina Mühendisleri Odası, Geleceğin Teknolojileri Sempozyumunda sunuldu. İstanbul.

25. İnternet: Kemp, S. Digital In 2018: World's Internet Users Pass the 4 Billion Mark. www.wearesocial.com. 2018-09-28. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwearesocial.com%2Fblog%2F2018%2F01%2Fglobal-digital-report-2018&date=2018-09-28, Son Erişim Tarihi: 28.09.2018.

26. İnternet: Babayigit, S. (2017). İnternet, Sosyal Medya ve Mobil Kullanım İstatistikleri 2017. www.sosyalmedyakampusu.com. URL: https://www.sosyalmedyakampusu.com/internet-sosyal-medya-ve-mobil-kullanim-istatistikleri-2017/ , Son Erişim Tarihi: 16.09.2018.

27. İnternet: Bıçakcı, S. Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.uidergisi.com.tr%2Fp%2F3010%2Fyeni-savas-ve-siber-guvenlik-arasinda-natonun-yeniden-dogusu&date=2018-09-14, Son Erişim Tarihi:14.09.2018.

28. İnternet: Shea, J. Esneklik: toplu savunmanın temel unsurlarından biri. Nato Dergisi. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.nato.int%2Fdocu%2Freview%2F2016%2FAlso-in-2016%2Fnato-defence-cyber-resilience%2FTR%2Findex.htm&date=2018-09-14, Son Erişim Tarihi: 14.09.2018.

29. Milli Güvenlik Kurulu Genel Sekreterliği. (2017). Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı; MGK. *Ankara.* 1-15.

30. The North Atlantic Treaty Organization. Cooperative Cyber Defence Centre of Excellence. (2008). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations; The NATO CCD COE. *Tallinn.*

31. İnternet: Bıçakcı, S.; Ergun, D.; Çelikpala M. Türkiye'de Siber Güvenlik. Türkiye'de Siber Güvenlik ve Nükleer Enerji. 2018-09-14. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fedam.org.tr%2Fdocument%2FCyberNuclear%2FSiberKitapTR%2Fedam_siber_guvenlik_b2.pdf&date=2018-09-14, Son Erişim Tarihi: 14.09.2018.

32. Öğün, M. N.; Kaya, A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. *Güvenlik Stratejileri Dergisi*, 18, 103-144.

33. İnternet: Ermiş, U. "Geleneksel caydırıcılığın siber alanda uygulanabilirliği" üzerine bir inceleme. www.siberbulten.com. 2018-09-16. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fsiberbulten.com%2Fmakale-analiz%2Fgeleneksel-caydiricilik-kavramlarinin-siber-alanda-uygulanabilirligi-uzerine-bir-inceleme%2F&date=2018-09-16, Son Erişim Tarihi: 16.09.2018.

34. İnternet: Sağıroğlu, Ş. 3. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu Sonuç Bildirgesi. http://bigdatacenter.gazi.edu.tr. 2018-09-16. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fbigdatacenter.gazi.edu.tr%2Fisdfs-2015-sonuc-bildirgesi%2F&date=2018-09-16, Son Erişim Tarihi: 16.09.2018.

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

36. Department of Homeland Security. (2011). Enabling Distributed Security in Cyberspace- Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action; DHS. *Washington.*

37. İnternet: Raghu, A. The Cyber Security Ecosystem: Collaborate or Collaborate: It's Your Choice. 2019-01-09. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.linkedin.com%2Fpulse%2Fcyber-security-ecosystem-collaborate-its-your-choice-arun-raghu%2F&date=2019-01-09, Son Erişim Tarihi: 09.01.2019.

38. İnternet: Potii, O. Cybersecurity Ecosystem. 2019-01-09. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.itu.int%2Fen%2FITU-D%2FRegional-Presence%2FCIS%2FDocuments%2FEvents%2F2018%2F05_Kiev%2FITU%2520Seminar%252015.05.18%2520-%2520Oleksandr%2520Potii.pdf&date=2019-01-09, Son Erişim Tarihi: 09.01.2019.

39. Tagarev, T., Sharkov, G., Stainov, N. (2017). Cyber Security and Resilience of Modern Societies: A Research Management. *Information & Security: An International Journal,* 93-108.

40. İnternet: Riley, S. Science of Security: Cyber Ecosystem Attack Analysis Methodology. 2019-01-09. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.slideshare.net%2Fshawnriley2%2Fcs1-2-riley&date=2019-01-09, Son Erişim Tarihi: 09.01.2019.

41. İnternet: Riley, S. "Cyber Terrain": A Model for Increased Understanding of Cyber Activity. 2019-01-09. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fcscss.org%2FCS%2F2016%2F08%2F20%2Fcyber-terrain-a-model-for-increased-understanding-of-cyber-activity%2F&date=2019-01-09, Son Erişim Tarihi: 09.01.2019.

42. Türkiye Büyük Millet Meclisi. (2007). İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun; TBMM. *Ankara.*

43. İnternet: Telekomünikasyon İletişim Başkanlığı. 5651 Sayılı Kanun Erişim ve Yer Sağlayıcıların Yükümlülükleri. www.ulakbim.tubitak.gov.tr. 2018-09-16. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fulakbim.tubitak.gov.tr%2Fsites%2Fimages%2FUlakbim%2F5651.pdf&date=2018-09-16, Son Erişim Tarihi 17.09.2018.

44. İnternet: Ulaştırma Bakanlığı. Türkiye Ulusal Enformasyon Altyapısı Ana Planı (TUENA) (1996-1999). www.edevlet.gov.tr. 2018-09-17. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.edevlet.gov.tr%2F2015%2F10%2F13%2Fturkiye-ulusal-enformasyon-altyapisi-ana-plani-tuena-1996-1999%2F&date=2018-09-17, Son Erişim Tarihi: 17.09.2018.

45. Ulaştırma Bakanlığı. (1999). Türkiye Ulusal Enformasyon Altyapısı Anaplanı Sonuç Raporu. *Ankara.*

46. İnternet: Devlet Planlama Teşkilatı. Bilgi Toplumu Stratejisi (2006-2010). www.bilgitoplumu.gov.tr. 2018-09-17. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.bilgitoplumu.gov.tr%2FDocuments%2F1%2FBT_Strateji%2FDiger%2F060500_BilgiToplumuStratejisi.pdf&date=2018-09-17, Son Erişim Tarihi: 17.09.2018.

47. İnternet: T.C. Kalkınma Bakanlığı. 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı. www.trakyaka.org.tr. 2018-09-17. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.trakyaka.org.tr%2Fupload%2FNode%2F36836%2Fxfiles%2FBilgi_Toplumu_Stratejisi_ve_Eylem_Plani.pdf&date=2018-09-17, Son Erişim Tarihi: 17.09.2018.

48. İnternet: Türkiye Büyük Millet Meclisi. Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ. www.resmigazete.gov.tr. 2018-09-16. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.resmigazete.gov.tr%2Feskiler%2F2013%2F11%2F20131111-6.htm&date=2018-09-16, Son Erişim Tarihi: 17.09.2018.

49. İnternet: Bilgi ve İletişim Teknolojileri Kurumu. USOM ve Kurumsal Siber Olaylara Müdahale Ekibi. www.btk.gov.tr. 2018-09-16. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.btk.gov.tr%2Fusom-ve-kurumsal-siber-olaylara-mudahale-ekibi&date=2018-09-16, Son Erişim Tarihi: 17.09.2018.

50. Ulaştırma ve Altyapı Bakanlığı. (2013). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. *Ankara*.

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

52. T.C. Ulaştırma ve Altyapı Bakanlığı. (2016). 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı. *Ankara.*

53. İnternet: T.C Ulaştırma ve Altyapı Bakanlığı. Kamu-NET. 2019-01-10. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.hgm.gov.tr%2Ftr%2Fsayfa%2F45&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

54. İnternet: IT Planing Council. Tasks of the IT Planning Council. 2019-01-09. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.it-planungsrat.de%2F&date=2019-01-09, Son Erişim Tarihi: 09.01.2019.

55. İnternet: IT Planing Council. Organisation and Tasks. 2019-01-09. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.it-planungsrat.de%2FEN%2Fit-planing-council%2FOrganisation%2FOrganization_node.html&date=2019-01-09, Son Erişim Tarihi: 09.01.2019.

56. İnternet: Deutsches Institut für Normung. Koordinierungsstelle IT-Sicherheit. 2019-01-09. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.din.de%2Fde%2Fdin-und-seine-partner%2Fdin-e-v%2Forganisation%2Fkoordinierungsstellen%2Fkits&date=2019-01-09, Son Erişim Tarihi: 09.01.2019.

57. Deutsches Institut für Normung. (2014). German Standardization Roadmap IT Security; DIN/DKE. *Germany.*

58. İnternet: Kritische Infrastrukturen. Critical Infrastructure Protection. 2019-01-09. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.kritis.bund.de%2FSubSites%2FKritis%2FEN%2FHome%2Fhome_node.html&date=2019-01-09, Son Erişim Tarihi: 09.01.2019.

59. İnternet: Bundesministerium des Innern, für Bau und Heimat. LÜKEX. 2019-01-09. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.bmi.bund.de%2FDE%2Fthemen%2Fbevoelkerungsschutz%2Fkrisenmanagement%2Fluekex%2Fluekex-node.html&date=2019-01-09, Son Erişim Tarihi: 09.01.2019.

60. Kritische Infrastrukturen. (2017). UP KRITIS Public-Private Partnership for Critical Infrastructure Protection; KRITIS (BBK&BSI). *Germany.*

61. İnternet: Cyber Security Cluster Bonn. Bonn - Der Führende Security Standort Europas. 2019-01-09. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fcyber-security-cluster.eu&date=2019-01-09, Son Erişim Tarihi: 09.01.2019.

62. International Telecommunication Union. (2017). Global Cybersecurity Index (GCI); ITU. *Switzerland.*

63. İnternet: KoSIT. Koordinierungsstelle für IT-Standards. 2019-01-09. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww1.osci.de%2Fsixcms%2Fdetail.php%3Fid%3D1181&date=2019-01-09, Son Erişim Tarihi: 09.01.2019.

64. Güngör, M.(2015). *Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma,* Uzmanlık Tezi, T.C. Kalkınma Bakanlığı, Ankara.

65. Türkiye Büyük Millet Meclisi. (2012). TBMM Bilgi Toplumu Olma Yolunda Bilişim Sektöründeki Gelişmeler İle İnternet Kullanımının Başta Çocuklar, Gençler ve Aile Yapısı Üzerinde Olmak Üzere Sosyal Etkilerinin Araştırılması Amacıyla Kurulan Meclis Araştırması Komisyonu Raporu; TBMM. *Ankara.*

66. The North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence. (2016). National Cyber Security Organisation: Unıted States; The NATO CCD COE. *Tallinn.*

67. The White House. (2018). The National Cyber Strategy of the United States of America. *Washington.*

68. İnternet: Australian Signals Directorate. Australian Cyber Security Center. 2019-01-09. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fcyber.gov.au%2Fabout-this-site%2Fabout-acsc%2F.&date=2019-01-09, Son Erişim Tarihi: 09.01.2019.

69. İnternet: Australia Cyber Security Center. CERT Australia. 2019-01-09. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.cert.gov.au&date=2019-01-09, Son Erişim Tarihi: 09.01.2019.

70. Austrailan Government/The Australian Trade and Investment Commission. (2017). Cyber Security. *Australia.*

71. İnternet: CERT Australia. Australian Internet Security Initiative. 2019-01-09. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.cert.gov.au%2Faisi&date=2019-01-09, Son Erişim Tarihi: 09.01.2019.

72. Çakır, H. ve Kılıç, M. S. (Editörler). (2014). *Güncel Tehdit: Siber Suçlar*. Ankara: Seçkin Yayıncılık, 44-61.

73. İnternet: Australia TISN. Trusted Information Sharing Network for Critical Infrastructure Protection. 2019-01-09. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.tisn.gov.au%2FPages%2FPublications-by-topic.aspx&date=2019-01-09, Son Erişim Tarihi: 09.01.2019.

74. Australian Government, Federal Attorney-General's Department. (2009). Critical Infrastructure Protection Modelling and Analysis Program; AGD. *Australia.*

75. Australia Trusted Information Sharing Network for Critical Infrastructure Protection. (2015). Critical Infrastructure Resilience strategy: PLAN; Australia TISN. *Australia.*

76. İnternet: Data61. Data61-CSIRO. 2019-01-09. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.data61.csiro.au&date=2019-01-09, Son Erişim Tarihi: 09.01.2019.

77. İnternet: Department of Communications and the Arts. Building cyber safe communities. 2019-01-09. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.communications.gov.au%2Fdepartmental-news%2Fbuilding-cyber-safe-communities&date=2019-01-09, Son Erişim Tarihi: 09.01.2019.

78. İnternet: eSmart.org. Smart Safe Responsible. 2019-01-09. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.esmart.org.au%2Fwhat-is-esmart%2F.&date=2019-01-09, Son Erişim Tarihi: 09.01.2019.

79. İnternet: IRAP. Information Security Registered Assessors Program. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Facsc.gov.au%2Finfosec%2Firap%2Findex.htm&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

80. The North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence. (2015). National Cyber Security Organisation in UK; The NATO CCD COE. *Tallinn*.

81. The North Atlantic Treaty Organization Cyber Defence Centre of Excellence. (2015). National Cyber Security Organisation in China; The NATO CCD COE. *Tallinn.*

82. İnternet: Ministry of Defence. The Security Committee. . 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.defmin.fi%2Fen%2Foverview%2Fministry_of_defence%2Fdepartments_and_units%2Forganisations_accountable_to_the_ministry_of_defence%2Fsecurity_committee&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

83. İnternet: Ministry of Finance. Information security and cybersecurity. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fvm.fi%2Fen%2Finformation-security-and-cybersecurity&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

84. İnternet: VAHTI. VAHTI. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.vahtiohje.fi%2Fweb%2Fguest%2Fhome&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

85. The Security Committee of Finland. (2017). Security Strategy for Society, Government Resolution. *Finland.*

86. The Security Committee of Finland. (2017). Implementation Programme for Finland's Cyber Security Strategy for 2017–2020. *Finland.*

87. İnternet: JYVSECTEC. Specializing in cyber security expertise. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fjyvsectec.fi%2Fabout%2Foverview%2F&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

88. İnternet: Agence Nationale de la Sécurité des Systèmes d'Information. The French CIIP Framework. 2019-01-10. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.ssi.gouv.fr%2Fen%2Fcybersecurity-in-france%2Fciip-in-france%2F.&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

89. Ministry of Public Administration and Security. (2009). Ministry of Public Administration and Security Republic of Korea Introductory Brochure; MOPAS. *Seoul*.

90. Ministry of Science and ICT. (2017). 2017 Annual Report on the Promotion of the Korean ICT Industry. *Korea.*

91. İnternet: Forum of Incident Response and Security Teams. KN-CERT. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.first.org%2Fmembers%2Fteams%2Fkn-cert&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

92. İnternet: NIS. National Intelligence Service. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Feng.nis.go.kr%2FEAF%2F1_7.do&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

93. İnternet: KOTRA. Korea Trade-Investment Promotion Agency. 2019-01-10 URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.korusevent.org%2Fhome3.html&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

94. İnternet: MeitY. Vision & Mission. 2019-01-10. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fmeity.gov.in%2Fabout-meity%2Fvision-mission&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

95. Ministry Of Electronics And Information Technology. (2017). Unstarred Question No. 3697. *India.*

96. İnternet: NCPIIC. National Critical Information Infrastructure Protection Centre. 2019-01-10. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fnciipc.gov.in&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

97. Ministry of Electronics and Information Technology, Government of India. (2017). Indian-Computer Emergency Response Team; MeitY. *India.*

98. Ministry of Electronics and Information Technology, Government of India. (2017). CISOs Top Best Practices for a Safe & Secure Cyber Environment; MeitY. *India*.

99. Ministry of Electronics and Information Technology, Government of India. (2013). National Cyber Security Policy; MeitY. *India.*

100. İnternet: STPI. Software Technology Parks of India. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.stpi.in&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

101. Ministry of Electronics and Information Technology, Government of India. (2018). Public Procurement (Preference to Make in India) Order 2018 for Cyber Security Products; MeitY. *India.*

102. İnternet: Standardizasyon, Test ve Kalite Belgelendirme Ofisi. Standardisation Testing and Quality Certification. 2019-01-10. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.stqc.gov.in%2Fcontent%2Fabout-stqc&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

103. İnternet: Autorità per le Garanzie nelle Comnicazioni. Che cos'è l'autorità. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.agcom.it%2Fche-cos-e-l-autorita&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

104. İnternet: Sistema De Informazione Per La Sicurezza Della Republica. Italy's Intelligence System for the Security of the Republic. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.sicurezzanazionale.gov.it%2Fsisr.nsf%2Fenglish.html&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

105. The North Atlantic Treaty Organization Cyber Defence Centre of Excellence. (2015). National Cyber Security Organisation in Italy; The NATO CCD COE. *Tallinn.*

106. İnternet: URL: AgID. Agenzia per l'ıtalia digitale. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.agid.gov.it%2Fit&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

107. Presidenza del Consiglio dei Ministri of Italy. (2017). Piano nazionale per la protezione cibernetica e la sicurezza informatica. *Italy.*

108. İnternet: CERT-N Italy. CERT Nazionale. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.certnazionale.it%2Fchi-siamo%2F&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

109. İtalya Bakanlar Kurulu Başkanlığı. (2013). Siber Uzayı Koruma ve Bilgi Güvenliği Ulusal Planı. *İtalya.*

110. İnternet: Commissariato di P.S. CNAIPIC. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.commissariatodips.it%2Fprofilo%2Fcnaipic.html&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

111. İnternet: AEPD. Bienvenida a la Agencia. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.aepd.es%2Findex.html&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

112. The North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence. (2016). National Cyber Security Organisation in Spain; The NATO CCD COE. *Tallinn.*

113. İnternet: Spanish National Cybersecurity Institute. Incibe. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.incibe.es&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

114. İnternet: İspanya Siber Güvenlik Araştırmaları Mükemmeliyet Ağı (RENIC). History and Background. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.renic.es%2Fen%2Fabout-us&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

115. İnternet: Cyber Security Incident Response Teams-Spain (CSIRT-ES). Spanish Cybersecurity and Incident Management Teams. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.csirt.es%2Findex.php%2Fen%2F&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

116. İnternet: Centro Criptológico Nacional-Cyber Emergency Response Team (CCN-CERT). Misión y Objetivos. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.ccn-cert.cni.es%2Fsobre-nosotros%2Fmision-y-objetivos.html&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

117. İnternet: Spanish National Cybersecurity Institute Computer Emergency Response Team. What incibe cert. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.incibe-cert.es%2Fen%2Fwhat-incibe-cert&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

118. İnternet: Departamento de Seguridad Nacional. Consejo Nacional de Ciberseguridad. 2019-01-10. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.dsn.gob.es%2Fsistema-seguridad-nacional%2Fcomit%C3%A9s-especializados%2Fconsejo-nacional-ciberseguridad%23collapseTwo&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

119. İnternet: CNPIC. El Centro Nacional de Protección de Infraestructuras y Cibersegurida. . URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.cnpic.es&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

120. Tobal, J. (2017). *An ICT Pole in Cyber Security with the Support of All.* 3RD International Cyber Warfare and Security Conference. Ankara.

121. İnternet: Agenda Digital. Agenda Digital. 2019-01-10. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.agendadigital.gob.es%2Fplanes-actuaciones%2FPaginas%2Fplan-impulso-contenidos-digitales.aspx&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

122. National Information Security Center. (2017). Japanese Govenrment's Efforts to Address Information Secuirty Issues; NISC. *Japan.*

123. Center for International Public Policy Studies. (2012). Cyber Security in Japan (v.2); CIPPS. *Japan.*

124. İnternet: IPA. Information Technology Promotion Agency. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.ipa.go.jp%2Fenglish%2Fabout%2Fabout.html&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

125. İnternet: AIST. The National Institute of Advanced Industrial Science and Technology. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.aist.go.jp%2Faist_e%2Fdept%2Fen_dithf.html&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

126. İnternet: National Institute of Information and Communications Technology. National Institute of Information and Communications Technology. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.nict.go.jp%2Fen%2Fdata%2Fpublications.html&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

127. İnternet: Secom Trust Systems. Japan Computer Emergency Response Team/Coordination Center. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.secomtrust.net%2Fsecword%2Fjpcertcc.htm&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

128. Asia Pacific Computer Emergency Response Team. (2018). Asia Pacific Computer Emergency Response Team (Apcert) Operational Framework; APCERT.

129. The Association of Southeast Asian Nations. (2018). Overview of ASEAN-Japan Dialogue Relations; ASEAN. *Jakarta.*

130. ICT-ISAC JAPAN. (2016). Trend of Cyber Attacks and Introduction of Cyber Security Activities in ICT-ISAC Japan; ICT-ISAC JAPAN. *Hong Kong.*

131. Milli Güvenlik Kurulu Genel Sekreterliği. (2017). Japonya Ulusal Güvenlik Stratejisi; MGK. *Ankara.*

132. National Information Security Center. (2018). Cybersecurıty Strategy; NISC. *Japan.*

133. National Information Security Center. (2018). Summary of the Japan's Cybersecurity Strategy; NISC. *Japan.*

134. Cybersecurity Strategic Headquarters Government of JAPAN. (2018). The Cybersecurity Policy for Critical Infrastructure Protection.

135. İnternet: ANO Digital Economy. Data Economy Russia 2024. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fdata-economy.ru%2F2024&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

136. ANO Digital Economy. (2018). Data Transformation in Action. *Russia.*

137. ANO Digital Economy. (2018). Directions of the program "Digital Economy". *Russia.*

138. İnternet: FinTsert. FinTsert. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.cbr.ru%2Ffincert%2F&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

139. İnternet: Public Governance Improvement. Public Governance Improvement. 2019-01-10. URL: http://www.webcitation.org/query?url=http%3A%2F%2Far.gov.ru%2Fru-RU%2Fmenu%2Fdefault%2Fview%2F88&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

140. İnternet: T.C. Ulaştırma ve Altyapı Bakanlığı. Siber Güvenlik. URL: http://www.udhb.gov.tr/h-12-siber-guvenlik.html , Son Erişim Tarihi: 23.01.2019.

141. İnternet: T.C. Emniyet Genel Müdürlüğü. Siber Suçlarla Mücadele Daire Başkanlığı. www.egm.gov.tr. 2018-09-16. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.egm.gov.tr%2Fsayfalar%2Fsibersuclarlamucadeledairebaskanligi.aspx&date=2018-09-16, Son Erişim Tarihi: 17.09.2018.

142. İnternet: Vikipedi. Kamu Düzeni ve Güvenliği Müsteşarlığı. www.wikipedia.org. 2018-09-16. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.wikizero.co%2Findex.php%3Fq%3DaHR0cHM6Ly90ci53aWtpcGVkaWEub3JnL3dpa2kvS2FtdV9Ew7x6ZW5pX3ZlX0fDvHZlbmxpxJ9pX03DvHN0ZcWfYXJsxLHEn8Sx&date=2018-09-16, Son Erişim Tarihi: 17.09.2018.

143. İnternet: Milli İstihbarat Teşkilatı Başkanlığı. Mit'in Görev Yetki ve Sorumlukları. www.mit.gov.tr. 2018-09-16. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.mit.gov.tr%2Fgorev.html&date=2018-09-16, Son Erişim Tarihi: 17.09.2018.

144. İnternet: Türk Silahlı Kuvvetleri. Kuvvet Yapısı. www.tsk.tr. 2018-09-16. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.tsk.tr%2FSayfalar%3FviewName%3DKuvvetYapisi&date=2018-09-16, Son Erişim Tarihi: 17.09.2018.

145. İnternet: Ulusal Siber Olaylara Müdahale Merkezi. Usom Hakkında. www.usom.gov.tr. 2018-09-16. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.usom.gov.tr%2Fhakkimizda.html&date=2018-09-16, Son Erişim Tarihi: 17.09.2018.

146. Türkiye Büyük Millet Meclisi. (1963). Türkiye Bilimsel ve Teknolojik Araştırmalar Kurumu Kurulması Hakkında Kanun; TBMM. *Ankara.*

147. Mali Suçlar Araştırma Kurulu. (2015). Faaliyet Raporu 2015; MASAK. *Ankara*.

148. İnternet: Vikipedi. Telekomünikasyon lletişim Başkanlığı (Türkiye). www.wikipedia.org. 2018-09-16. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.wikizero.co%2Findex.php%3Fq%3DaHR0cHM6Ly90ci53aWtpcGVkaWEub3JnL3dpa2kvVGVsZWtvbcO8bmlrYXN5b25fxLBsZXRpxZ9pbV9CYcWfa2FubMSxxJ_EsV8oVMO8cmtpeWUp&date=2018-09-16, Son Erişim Tarihi: 17.09.2018.

149. İnternet: Bankacılık Düzenleme ve Denetleme Kurumu. URL: http://www.bddk.org.tr/, Son Erişim Tarihi: 17.09.2018.

150. İnternet: Devlet Personel Başkanlığı. Devlet Teşkilatı. www.dpb.gov.tr. 2018-09-16. URL: http://www.webcitation.org/query?url=http%3A%2F%2Feuygulama.dpb.gov.tr%2Fdevletteskilati%2Fkontrollu%2FButce.aspx&date=2018-09-16, Son Erişim Tarihi: 17.09.2018.

151. İnternet: Hakimler ve Savcılar Kurulu. Hakkımızda. www.hsk.gov.tr. 2018-09-17. URL: http://www.webcitation.org/72UiZkX41, Son Erişim Tarihi: 17.09.2018.

152. İnternet: İstanbul Tahkim Merkezi. Hakkımızda. www.istac.org.tr. 2018-09-17. URL: http://www.webcitation.org/72Uj6D7Um, Son Erişim Tarihi: 17.09.2018.

153. Türkiye Büyük Millet Meclisi. (2014). İstanbul Tahkim Merkezi Kanunu; TBMM. Ankara.

154. Kamu İhale Kurumu. (2015). Kamu İhale Kurumu Faaliyet Raporu 2015; KİK. *Ankara.*

155. İnternet: Vikipedi. Radyo ve Televizyon Üst Kurulu. www.wikipedia.org. 2018-09-16. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.wikizero.co%2Findex.php%3Fq%3DaHR0cHM6Ly90ci53aWtpcGVkaWEub3JnL3dpa2kvUlTDnEs&date=2018-09-16, Son Erişim Tarihi: 17.09.2018.

156. Türkiye Büyük Millet Meclisi. (1994). Rekabetin Korunması Hakkında Kanun; TBMM. *Ankara.*

157. İnternet: Tarım ve Orman Bakanlığı. Şeker Dairesi Başkanlığı. www.tarim.gov.tr. 2018-09-16. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.tarim.gov.tr%2FSDB&date=2018-09-16, Son Erişim Tarihi: 17.09.2018.

158. İnternet: Türkiye Cumhuriyet Merkez Bankası. Sıkça Sorulan Sorular. www.tcmb.gov.tr. 2018-09-16. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.tcmb.gov.tr%2Fwps%2Fwcm%2Fconnect%2FTR%2FTCMB%2BTR%2FMain%2BMenu%2FBanka%2BHakkinda%2FSikca%2BSorulan%2BSorular&date=2018-09-16, Son Erişim Tarihi: 17.09.2018.

159. İnternet: Bilim ve Teknoloji Yüksek Kurulu. www.tubitak.gov.tr, URL: https://www.tubitak.gov.tr/tr/kurumsal/icerik-bilim-ve-teknoloji-yuksek-kurulu, Son Erişim Tarihi: 17.09.2018.

160. International Telecommunication Union. (2018). Guide to Developing a National Cybersecurity Strategy; ITU. *Switzerland.*

161. İnternet: Milli Güvenlik Kurulu Genel Sekreterliği. URL: https://www.mgk.gov.tr/index.php/kurumsal/hakkimizda, Son Erişim Tarihi: 17.09.2018.

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

163. İnternet: abhaber.com. AB siber güvenlik politikaları arayışında. 2019-01-10. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.abhaber.com%2Fab-siber-guvenlik-politikalari-arayisinda%2F.&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

164. İnternet: govtrack.usa. H.R. 2807 (115th): To amend title 10, United States Code, to require congressional notification concerning sensitive military cyber operations and cyber weapons, and for other purposes. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.govtrack.us%2Fcongress%2Fbills%2F115%2Fhr2807%2Ftext&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

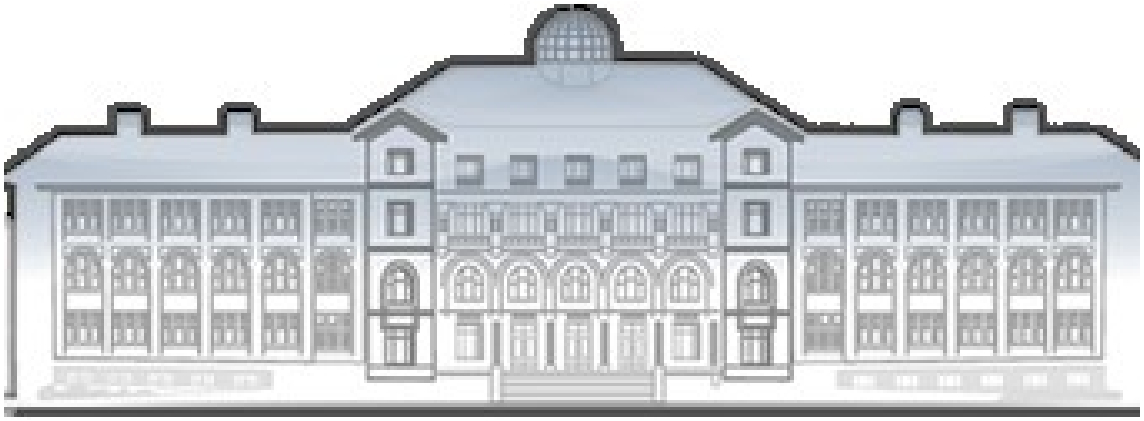
165. Sait Y., Olcay S. (2008). *Siber uzayda Güvenlik ve Türkiye* (Birinci Baskı). Ankara: Milenyum Yayınları. 35,107.

166. Türkiye Bilişim Derneği. (2018). TBD Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi Sonuç Bildirgesi. *Ankara.*

167. Afet ve Acil Durum Yönetim Başkanlığı (2014). 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi; AFAD. *Ankara.*

168. İnternet: The German Federal Office for Information Security. BSI. 2019-01-10. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.bsi.bund.de%2FEN%2FTheBSI%2Fthebsi_node.html&date=2019-01-10, Son Erişim Tarihi: 10.01.2019.

169. Sanayi ve Teknoloji Bakanlığı. (2018). İmalat Sanayinin Dijital Dönüşümü Raporu ve Yol Haritası. *Ankara.*



GAZİLİ OLMAK AYRICALIKTIR…