Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü
Siyaset ve Sosyal Bilimler Anabilim Dalı
Siyaset Bilimi Programı

SİBER GÜVENLİK VE TÜRKİYE: ÖRGÜTSEL YAPI, UYGULAMALAR VE GELECEK

Doktora Tezi

İbrahim AKDAĞ

Ankara, 2021

SİBER GÜVENLİK VE TÜRKİYE: ÖRGÜTSEL YAPI, UYGULAMALAR VE GELECEK

İbrahim AKDAĞ

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü

Siyaset ve Sosyal Bilimler Anabilim Dalı

Siyaset Bilimi Programı

Doktora Tezi

Ankara, 2021

YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin tamamını veya herhangi bir kısmını, basılı (kağıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe Üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinleri yazılı izin alınarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim Kurulu tarafından yayınlanan ***"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"*** kapsamında tezim aşağıda belirtilen koşullar haricince YÖK Ulusal Tez Merkezi / H.Ü. Kütüphaneleri Açık Erişim Sisteminde erişime açılır.

- Enstitü / Fakülte yönetim kurulu kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren 2 yıl ertelenmiştir. (1)
- Enstitü / Fakülte yönetim kurulunun gerekçeli kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren ….. ay ertelenmiştir. (2)
- Tezimle ilgili gizlilik kararı verilmiştir. (3)

……/……/……

[İmza]

İbrahim AKDAĞ

"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"

*(1) Madde 6. 1. Lisansüstü tezle ilgili patent başvurusu yapılması veya patent alma sürecinin devam etmesi durumunda, tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulu** iki yıl süre ile tezin erişime açılmasının ertelenmesine karar verebilir.*

*(2) Madde 6. 2. Yeni teknik, materyal ve metotların kullanıldığı, henüz makaleye dönüşmemiş veya patent gibi yöntemlerle korunmamış ve internetten paylaşılması durumunda 3. şahıslara veya kurumlara haksız kazanç imkanı oluşturabilecek bilgi ve bulguları içeren tezler hakkında tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulunun** gerekçeli kararı ile altı ayı aşmamak üzere tezin erişime açılması engellenebilir.*

*(3) Madde 7. 1. Ulusal çıkarları veya güvenliği ilgilendiren, emniyet, istihbarat, savunma ve güvenlik, sağlık vb. konulara ilişkin lisansüstü tezlerle ilgili gizlilik kararı, **tezin yapıldığı kurum** tarafından verilir *. Kurum ve kuruluşlarla yapılan işbirliği protokolü çerçevesinde hazırlanan lisansüstü tezlere ilişkin gizlilik kararı ise, **ilgili kurum ve kuruluşun önerisi** ile **enstitü** veya **fakültenin** uygun görüşü üzerine **üniversite yönetim kurulu** tarafından verilir. Gizlilik kararı verilen tezler Yükseköğretim Kuruluna bildirilir.*
Madde 7.2. Gizlilik kararı verilen tezler gizlilik süresince enstitü veya fakülte tarafından gizlilik kuralları çerçevesinde muhafaza edilir, gizlilik kararının kaldırılması halinde Tez Otomasyon Sistemine yüklenir.

***** *Tez* ***danışmanının*** *önerisi ve* ***enstitü anabilim dalının*** *uygun görüşü üzerine* ***enstitü*** *veya* ***fakülte yönetim kurulu tarafından karar verilir.***

ETİK BEYAN

Bu çalışmadaki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi, görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, yararlandığım kaynaklara bilimsel normlara uygun olarak atıfta bulunduğumu, tezimin kaynak gösterilen durumlar dışında özgün olduğunu, Prof. Dr. Ali ÇAĞLAR danışmanlığında tarafımdan üretildiğini ve Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Yönergesine göre yazıldığını beyan ederim.

İbrahim AKDAĞ

ÖZET

AKDAĞ, İbrahim. *Siber Güvenlik ve Türkiye: Örgütsel Yapı, Uygulamalar ve Gelecek*, Doktora Tezi, Ankara, 2021.

Bu tezin ana amacı ülkemizdeki siber güvenlik uygulamaları ve örgütsel yapısının gelecekteki olası ulusal, bölgesel ya da küresel siber güvenlik krizlerinin yönetimi çerçevesinde analizinin gerçekleştirilmesidir. Bu amaca ulaşmak için tez çalışması beş ana bölümden oluşturulmuştur. Birinci bölümde araştırmanın amacı, konusu ve kapsamı, ikinci bölümde araştırmada kullanılan metod ve araştırma verilerinin nasıl analiz edildiği açıklanmıştır. Araştırmanın üçüncü bölümümde araştırmada yer alan temel kavramlar ve kuramsal çerçeve ortaya konmuştur. Araştırmanın dördüncü bölümünde tarihsel süreç içerisinde siber güvenlik kavramının nasıl genişlediği ve günümüzdeki durumu analiz edilmiştir. Araştırma bulgularının açıklandığı beşinci bölümde siber güvenlik krizleri ve Türkiye konusu tartışılmıştır. Araştırmamız, araştırma sonuçlarının ve geleceğe ilişkin değerlendirmelerin yer aldığı sonuç ve değerlendirme kısmı ile tamamlanmıştır. Bu tez çalışması ile şu sonuçlara ulaşılmıştır; ülkemizde siber güvenliğe olan yaklaşımın ülkemizin genel güvenlik algısından etkilendiği, ülkemizdeki siber güvenlik uygulamaları ve örgütsel yapısının siber olay yönetimi seviyesinde gelişme gösterdiği, ancak kapsamlı güvenlik krizlerinin çözümüne yönelik gerekli olgunluk seviyesinde olmadığı tespit edilmiştir. Araştırma bulguları neticesinde gelecekteki siber güvenlik uygulamaları içerisinde; insan gücünün yetiştirilmesi, siber uzayın yeni durumuna uygun gerekli hukuki düzenlemelerin gerçekleştirilmesi konularına daha fazla yer verilmesinin, gelecekteki olası siber tehdit ve risklere karşı olan dayanıklılık seviyesinin artırılmasını sağlayacağı değerlendirilmiştir. Ülkemizdeki siber güvenlik örgütsel yapılanmasının yönetiminin; gerekli hukuki yaptırım gücüne sahip, bağımsız denetim fonksiyonu ile donatılmış bir siber güvenlik otoritesi tarafından gerçekleştirilmesi sonucuna ulaşılmıştır.

Anahtar Sözcükler: Siber Güvenlik, Kriz Yönetimi, Güvenlikleştirme, Siber Uzay

ABSTRACT

AKDAĞ, İbrahim. *Cyber Security and Turkey: Organizational Structure, Applications and Future,* PhD Dissertation, Ankara, 2021.

The main purpose of this thesis is to analyze the cyber security practices - applications and organizational structure in Turkey within the framework of the management of possible future national, regional or global cyber security crises. In order to achieve this aim, the study is composed of five main parts. In the first part, the purpose, subject, aim and scope of the research are explained. In the second part, the method used, data collection and data analysis are explained. In the third part, the basic concepts and theoretical framework of the research are presented. In the fourth part, how the concept of cyber security has expanded in the historical process and its current situation are discussed. In the fifth chapter, the research findings are explained, discussed and analyzed. In addition, the cybersecurity crise in Turkey is discussed. This research has been completed with the conclusion and evaluation part, which includes the overall research results and proposals. It has been determined that the approach to cyber security in Turkey is affected by the general security perception of the country. The cyber security practices and organizational structure in Turkey are developed at the level of cyber incident management. But they are not at the required maturity level for the solution of comprehensive security crises. As a result of research findings, it has been evaluated that giving more space to the training of human power and the realization of the necessary legal arrangements in accordance with the new situation of cyberspace will increase the level of resilience against possible cyber threats and risks in the future. It has been concluded that the management of the cyber security organizational structure in Turkey should be carried out by a cyber security authority that has the necessary legal sanction power and should be equipped with an independent audit function.

Key Words: Cyber Security, Crisis Management, Securitization, Cyber Space

İÇİNDEKİLER

KISALTMALAR

USOM **:** Ulusal Siber Olaylara Müdahale Merkezi
SOME **:** Siber Olay Müdahale Ekibi
BTK **:** Bilgi Teknolojileri Kurumu
ENISA **:** European Union Agency for Cybersecurity
MSB : Milli Savunma Bakanlığı
TSK : Türk Silahlı Kuvvetleri
OHAL : Olağan Üstü Hal
BM : Birleşmiş Milletler
AGİT : Avrupa Güvenlik ve İşbirliği Teşkilatı
NATO : North Atlantic Treaty Organization
ABD : Amerika Birleşik Devletleri
LAN : Local Area Network
MAC : Media Access Control
DAC : Digital-To-Analog Converter
SSL : Secure Socket Layer
TCK : Türk Ceza Kanunu
APT : Advanced Persistent Threat
USB : Universal Serial Bus
OWASP : Open Web Application Security Project
DDoS : Distrubuted Denial of Service
GKÇ : Geleneksel Konvansiyonel Çatışma
DPT : Devlet Planlama Teşkilatı
BOME : Bilgisayar Olayları Müdahale Ekibi
TİB : Telekomünikasyon İletişim Başkanlığı
EPDK : Enerji Piyasaları Denetleme Kurumu
SPK : Sermaye Piyasası Kurulu
BDDK : Bankacılık Düzenleme ve Denetleme Kurumu
AFAD : Afet ve Acil Durum Yönetimi Başkanlığı

GAMER : Güvenlik ve Acil Durumlar Koordinasyon Merkezi Başkanlığı

EKS : Endüstriyel Kontrol Sistemleri

SCADA : Supervisory Control and Data Acquisition

DKS : Dağıtık Kontrol Sistemleri

DDO : Dijital Dönüşüm Ofisi

BTD : Bilgi Toplumu Dairesi

TUIK : Türkiye İstatistik Kurumu

NIST : National Institute of Standards and Technology

COMSEC : Communication Security

TABLOLALAR **Sayfa No**

ŞEKİLLER **Sayfa No**

GİRİŞ

Bu tezin ana amacı, siber alanın hızlı ve öngörülemeyen bir ivme ile büyümesi sonucunda ortaya çıkan yeni güvenlik tehditlerine karşı alınan tedbirler bütününden oluşan siber güvenlik kavram ve uygulamalarının Türkiye'deki izdüşümünün ulusal güvenlik kavramları çerçevesinde ortaya çıkarılmasıdır. Bu temel amaca ulaşmak için çalışma beş ana bölümden oluşturulmuştur. Araştırma bilgilerinin yer aldığı birinci bölümde araştırmanın konusu, amacı ve temel araştırma soruları açıklanmıştır. Ayrıca araştırmanın kapsamı ve sınırlılıkları belirlenmiştir. Araştırmanın kapsam ve sınırlılıkları belirlenirken siber uzayın hızlı gelişimi ve mevcut büyüklüğü göz önünde bulundurulmuştur. Bu çalışmanın başlangıcında COVID-19 krizi daha dünyayı sarmamış, beraberinde getirdiği dijital dönüşüm fırtınası başlamamıştı. Dünyadaki internet kullanıcı sayısı, çalışmanın sonuçlanma aşamasına geldiğinde başlangıca göre % 10'luk bir artış göstermiş, siber uzaya 500.000.000 yeni insan eklenmiştir. Bu istatistiği göz önünde bulundurarak araştırma kapsamı, ulusal siber güvenlik krizlerinin merkezi yönetimi olarak belirlenmiş; sağlık, enerji finans gibi kritik altyapı sektörlerine özel siber güvenlik kriz yönetimi faaliyetleri merkezi yönetimle olan ilişkileri ile sınırlandırılmıştır. Araştırmanın bir diğer sınırlılığı ise, araştırma verilerinin TASNİF DIŞI verilerden oluşması, ulusal siber güvenlik faaliyetlerine ilişkin bazı detayların HİZMETE ÖZEL ve üzeri gizlilik derecesinde ele alınması nedeniyle, bu verilerin çalışmaya dahil edilememesidir. Gerekli literatür taraması sonuçları değerlendirilmiş, siber güvenlik kriz yönetimi alanındaki akademik boşluk ortaya çıkartılarak alana ilişkin özgün değer katkı beklentisi sunulmuştur.

Araştırmanın çerçevesi belirlenirken siber alanın hızlı dönüşümü ve geniş kapsamı nedeniyle Türkiye'de kamuda siber güvenlik özeline indirgenmiş, bununla yetinilmeyerek araştırma esnasında analiz edilen iç hukuk mevzuatımızda siber güvenlikten sorumlu bakanlık olarak belirlenen T.C. Ulaştırma ve Altyapı Bakanlığı odağında ilerlenmiştir. Bu noktada çalışmanın tutarlı sonuçlara ulaşması için siber güvenlik krizlerinin yönetimi ikinci bir odak noktası olarak belirlenmiştir. Krizlerin olağan dışı bazı olaylar dışında

gerçekleşmesi ve bazı durumlarda olağanüstü tedbirlerle çözülmesi nedeniyle bir olayın hangi durumlarda kriz kabul edileceği, ne zaman olağanüstü tedbirler alınacağına ve normale dönüş kararının hangi aşamada verileceğine ilişkin sayısal bir değerlendirme yapmak olanaklı değildir. Bu nokta, araştırmanın kapsamı ve araştırma soruları göz önünde bulundurulduğunda; neden, nasıl, niçin sorularına cevap veren bir yöntemin belirlenmesi ihtiyacı, bizi nitel araştırma türüne yönlendirmiştir.

Araştırmanın ikinci bölümünde yukarıda yer alan sonuçlara nasıl ulaşıldığı açıklanmış, araştırmada uygulanan bilimsel metot ele alınmıştır. Ayrıca bu bölümde, araştırma-çalışma evreninin nasıl belirlendiği, çalışma için ne tür verilere gereksinim duyulduğu da açıklanmıştır. Elde edilen verilerin nasıl toplandığı, verilerin ne şekilde analiz edildiği konusu da bu bölümde açıklanmıştır.

Araştırmanın üçüncü bölümü, siber güvenlik krizlerinin çok boyutluluğu gözetilerek, araştırmanın kavramsal ve teorik çerçevesine ayrılmıştır. Başlangıçta ülkemizin temel güvenlik yaklaşımı ve nedenleri ele alınmıştır. Sonrasında araştırmanın teorik çerçevesini oluşturan siber güvenlikleştirme kavramı açıklanmış, siber güvenlik krizi ve siber güvenlikleştirme kavramları arasındaki bağlantı açıklanmıştır.

Araştırmanın dördüncü bölümü, siber güvenlik kavramına ayrılmıştır. Siber güvenlik kavramının tarihsel gelişimi, siber tehdit aktörleri ve tehdit çeşitleri açıklanmıştır. Siber çatışmaların kendine özgü durumu örneklerle açıklanmıştır.

Araştırmanın beşinci bölümü, Türkiye'deki siber güvenlik kriz yönetimi süreçlerinin analizine ayrılmıştır. Bu tarihi süreçte ülkemizin geçirdiği siber güvenlik dönüşümü analiz edilmiş tarihsel çerçevedeki ulusal konumumuz belirlenmiştir. Belirlenen kriz yönetimi aşamalarına göre ülkemizdeki siber güvenlik faaliyetlerinin analizi gerçekleştirilmiştir.

Araştırmanın değerlendirme ve sonuç kısmında, analiz çerçevesinde elde edilen temel sonuçların değerlendirilmesi gerçekleştirilmiştir. Türkiye'nin hızla büyüyen küresel siber uzaya uyum sağladığı ve ulusal siber uzayın benzer bir büyüme sürecinden geçtiği, aynı zamanda küresel alanda yaşanan siber güvenlik süreçlerinin ülkede paralel bir seyirde olduğu sonucuna ulaşılmıştır. Ülkede siber güvenlik alanında önemli gelişmeler yaşandığı ve küresel anlamda siber güvenlik gelişmişlik seviyesi olarak üst sıralarda olduğu tespit edilmiştir.

Siber güvenliğin Türkiye'de başlangıçta bilgi toplumu dönüşüm faaliyetleri kapsamında değerlendirildiği, ancak zaman içerisinde elektronik haberleşme kritik altyapısı çerçevesine kaydırıldığı tespit edilmiştir. Bu dönüşümün elektronik haberleşme ve siber uzayın teknik ve mantıksal boyutunun yönetimi için faydalı olduğu ancak siber uzayın insan boyutunu, yönetişim boyutunu kapsayamadığını, bu nedenle de sistemin bazı güvenlik sorunlarına açık olduğu tespit edilmiştir. Gerçekleştirilen analiz neticesinde siber güvenlik kriz yönetimi süreçlerinin parça parça karşılandığı sonucuna ulaşılmıştır. 2000'li yılların başında ortaya konan ulusal siber güvenlik kurulunun 2012'de hayata geçirilmesi, ancak zaman içerisinde aktif olarak çalışmaması nedeniyle USOM çerçevesinde bir siber güvenlik kriz yönetimine geçiş yapıldığı, USOM'un diğer kamu kurumlarını kapsayıcılığı ve teknik yönünün yüksek oluşunun idari süreçlerin kapsanmasında eksikliklere neden olması nedeniyle ulusal siber güvenlik ve kriz yönetimi otoritesi eksikliklerinin ortaya çıktığı sonucuna varılmıştır.

Cumhurbaşkanlığı hükümet sistemine geçişle beraber elektronik haberleşme kanununda yapılan değişiklik nedeniyle kaldırılan siber güvenlik kurulunun yine aynı kanunda yer alan yeni düzenlemeye göre Cumhurbaşkanlığı tarafından belirlenmesi ve ulusal bir siber güvenlik otoritesinin ortaya çıkarılmasının, teknik ve idari anlamda gerçekleştirilen başarılı çalışmaların karşılığının olası bir siber güvenlik krizinde kazanca dönüştürülmesi için gerekli olduğu değerlendirilmiştir.

I. BÖLÜM

ARAŞTIRMA BİLGİLERİ

Belirtilmiş olduğu üzere bu tez çalışmasının temel konusu “Türkiye ve Siber Güvenlik”tir. Diğer bir deyişle siber güvenlik açısından Türkiye’nin ne durumda olduğu, mevcut örgütsel yapılarının nasıl işlediği, eksiklik ve yetkinlikleri vb. konular açıklanmış, tartışılmış ve değerlendirilmiştir. Bu ana çerçeveden hareketle bu bölümde; araştırmanın konusu, amaçları, kapsamı temel soruları ile mevcut literatür durumu açıklanmıştır.

1.1 ARAŞTIRMANIN KONUSU, AMACI VE KAPSAMI

Günümüzde teknoloji gündelik yaşamın bir parçası olup ulusal kalkınma ve gelişmenin de temelini oluşturmaktadır. Kamu yönetiminde teknolojik dönüşüm, özel sektörün yüksek teknoloji üretmesi, teknoloji üretmeye yönelik bilimsel çalışmaların artırılması ülkelerin başlıca hedefleri arasında yer almaktadır. Teknolojik ilerlemenin bir ürünü olan bilgi ve iletişim teknolojilerindeki gelişim sonucunda, başlangıçta savunma amaçlı kapalı devre bir ağ olarak ortaya çıkan bilgisayar ağları kurulması fikri, günümüzde 4 milyar insanı çevrimiçi olarak birbirine bağlayan küresel bir ağ olan internete dönüşmüştür. İnternetin getirdiği avantajlar ve dönüşüm, konunun ekonomik ve sosyal bir boyutunun ortaya çıkmasına neden olmuştur. Günümüzde ise internetin ekonomik ve sosyal boyutu, fiziksel enstrümanlarla oluşan ekonomik ve sosyal faaliyetlerle aynı boyutlara ulaşmıştır.

İnternetin kullanım oranları üzerinden konuyu örneklendirdiğimizde Uluslararası Telekomünikasyon Birliği (ITU) verilerine göre;

“2019 yılı sonu itibarıyla dünya nüfusunun yaklaşık %53,6’sının, yani 4,1 milyar insanın, internet kullanıcısı olduğu değerlendirilmektedir. (ITU, 2019) Türkiye’deki

duruma bakıldığında; Bilgi Teknolojileri ve İletişim Kurumu (BTK) Türkiye Elektronik Haberleşme Sektörü 2020 yılı 2. Çeyrek Raporu'na göre 2008 yılında yaklaşık 6 milyon olan genişbant internet abone sayısı, 2020 yılı ikinci çeyreği itibarıyla 78,4 milyona ulaşmıştır. Türkiye İstatistik Kurumu (TÜİK) verilerine göre 2020 yılında ülkemizde 16-74 yaş arası bireylerde internet kullanım oranı %79 düzeyindedir (TUIK, 2020)."

Bilgi teknolojilerinin bu hızlı gelişimi beraberinde, aynı büyüklükte güvenlik sorunlarını getirmiştir. İnternetin ilk yıllarında bilgi güvenliğinin üç önemli bileşeni olan erişilebilirlik, gizlilik ve bütünlük kavramlarından erişilebilirlik ön plana çıkmış, önce internetin gelişmesi ve işletilmesi düşünülmüş, gizlilik ve bütünlük geri planda kalmıştır. Bu durumda internetin temel mimari ve servislerin zaman içerisinde gizlilik ve bütünlüğe ilişkin sorunlara neden olmasına sebebiyet vermiş, hızlı büyüme nedeniyle de erişilebilirlikle ilgili de sorunlar zaman içerisinde artmıştır. Bu durumda güvenlik kavramının her zaman bir adım geride kalmasına neden olmuştur. Günümüzde yaşanmış olan acı siber güvenlik olayları nedeniyle konuya ilişkin farkındalığın yüksek olması siber güvenliğe karşı hak ettiği ilginin sağlanmasını sağlamıştır. Ancak teknolojik gelişimden, tehditler de faydalanmış, çok karmaşık bir siber güvenlik tehdit evreni oluşmuştur. Bu tehditler günümüzde asimetrik etki sağlayabilecek bir boyuta ulaşmıştır. Stuxnet olayında görüldüğü üzere gerekli güvenlik tedbirlerinin alınmadığı, milyarlarca dolar harcanmış bir nükleer tesisin işlerliği USB bellek vasıtasıyla sisteme bulaşan bir zararlı yazılımla engellenebilmektedir (Masood, Samar, & Raja, 2019). 2020 yılında Amerika'da yaşanmış olan Sunburst siber güvenlik krizinde (Cuthbertson, 2020) ABD Savunma Bakanlığı, Hazine Bakanlığı ve Nükleer Silah Yönetim ağı gibi stratejik öneme sahip sistemlere sızılarak uzun bir dönem boyunca içeriden bilgi kaçırılmıştır.

Konuyu ülkemiz açısından değerlendirdiğimizde TSK başarılı bir şekilde teknolojik dönüşümünü sağlamış ve ağ tabanlı harp tekniklerini sahada uygulamıştır. Türk İHA'larının TSK'nın katıldığı operasyonlardaki başarısı, harekatların canlı olarak merkez karargahlardan yönetimi, ateş destek, hava

savunma sistemlerinin ağ tabanlı teknolojilere geçişi, deniz ve hava kuvvetleri unsurlarının ağ tabanlı yönetimi, teknolojik dönüşümün en önde gelen örnekleridir. Diğer stratejik öneme sahip ve kritik altyapı işleten ulusal kurum ve kuruluşlarda benzer bir dönüşüm geçirmiştir. Günümüzde enerji, finans, sağlık gibi kritik altyapılarımız ağ tabanlı bir yönetime sahiptir. Bu durumda beraberinde ülkemizin asimetrik harbin bir kuvvet çarpanı olan siber tehditlere karşı hassasiyetini artırmıştır.

Siber güvenlik kavramının önemi, COVID-19 pandemisi ile birlikte yaşanan kriz ortamından yararlanan siber güvenlik tehdit aktörlerinin faaliyetlerini artırması nedeniyle artış göstermiştir (Threat Landscape:Phising, 2020, s. 2). Kriz sürecinde hayatın tüm alanlarında teknolojik dönüşüm yaşanmış, pek çok sektör çevrim içi teknolojilere geçiş yapmıştır. Bu dönüşüm sürecinde daha önce de belirtilmiş olan erişilebilirlik kaygıları nedeniyle gizlilik ve bütünlük geri planda kalmış bu durumda, siber tehditler için elverişli bir ortam sağlamıştır.

Siber güvenliğin artan önemi bu alanda yapılması gereken akademik çalışmaların eksikliği ortaya çıkarmıştır. Türkiye'de siber güvenlik alanında yeteri kadar akademik çalışma bulunmamaktadır. Çalışmamızın temel amacı, bu alanda ortaya çıkan boşluğun doldurulmasına katkı sağlamaktır. COVID-19 Pandemisi, kriz yönetimi kavramının önemini artırmıştır. Ülkelerin olası krizlere hazırlık durumu, kriz esnasında belirleyici olmakta, krizin başarılı yönetimi ve en kısa sürede bitirilmesi, öncesindeki hazırlık ve planlamanın başarısına bağlı olmaktadır. Siber güvenlik krizleri ise ülkelerin gündeminde son on yılda yer almaya başlamış, pek çok ülkede siber olaylar yaşansa da birkaç örnek dışında ulusal seviyede krize dönüşmemiştir. Ülkemizde ise ulusal çapta bir siber güvenlik krizi yaşanmamış, doğal afet, terör olaylarının neden olduğu güvenlik krizlerinde tecrübeler yaşandığı için, bu tehditlere yönelik kriz yönetimi çalışmalarında gerek akademik olarak gerekse krizlerin devlet otoriteleri tarafından yönetimine ilişkin pek çok çalışma gerçekleştirilmiştir. Bu çalışmanın amacı, bu alandaki akademik boşluğu doldurarak ülkemizde yaşanabilecek olası bir siber güvenlik krizinin nasıl ele alınacağını ortaya çıkarmaktır.

Siber güvenlik, tanımlaması oldukça değişken, genellikle öznel ve bazen de bilgilendirici olmayan, yaygın olarak kullanılan bir kavramdır. Siber güvenliğin çok boyutluluğunu yakalayan özlü, geniş ölçüde kabul edilebilir bir tanımının zorluğu, siber güvenliğin ağırlıklı olarak teknik yönünü güçlendirirken aynı zamanda teknolojik siber güvenlik zorluklarını çözmek için birlikte hareket etmesi gereken disiplinleri ayırarak bu alandaki teknolojik ve bilimsel ilerlemeleri engellemektedir. Siber güvenlikle ilgili çalışmalar bilgisayar bilimi, mühendislik, siyasal çalışmalar, psikoloji, güvenlik çalışmaları, yönetim, eğitim ve sosyoloji gibi çok çeşitli akademik disiplinleri de içeren geniş bir kaynak yelpazesine yayılmıştır.

Siber güvenlik krizleri içerdiği tespiti zor teknik faktörler ve krizin olası sonuçlarının tahmininin zor olması nedeniyle genel kriz yönetimi esaslarına kıyasla ek zorluklar içermektedir. Siber krizlerin yönetimi için genel kriz durumlarından çok daha büyük ölçüde bilginin analizi ve farklı durumların koordinesi gereklidir. Etkili bir siber kriz yönetimi, yöneticilerin hem kriz olaylarının kaynaklarını (yani siber olaylar) hem de bunları belirlemek ve planlamak için gereken strateji ve taktikleri anlamasını gerektirir.

ITU (ITU, 2019) ve TUIK (TUIK, 2020) verileri Günümüzde küresel ölçekte dünya nüfusunun %60'ı, ülkemizde ise nüfusun %70'i aktif olarak interneti kullanmaktadır. Siber uzayın kendine özgü güvenlik problemlerinin genel bir güvenlik sorunsalına kimi durumlarda da ciddi güvenlik krizlerine dönüşme senaryoları, siber uzayın mevcut durumu nedeniyle bir olasılık durumundan bir realiteye dönüşmüştür. Çalışmanın temel amacı, bu yeni güvenlik alanında yaşanan krizlerin nasıl ele alındığını güvenlikleştirme teorisi argümanları ışığında analiz ederek siber güvenlik krizlerinin yönetimine ilişkin bilimsel çıkarımlar elde etmektir.

Çalışma esnasında cevabı aranan temel araştırma soruları şu şekilde verilebilir:

- Ulusal siber uzay nasıl yönetilmekte ve güvenliği nasıl sağlanmaktadır?
- Yeni bir güvenlik alanı olan siber güvenliğe ilişkin ülkemizde hukuksal, düzenlemeler nedir ve bu düzenlemeler mevcut siber güvenlik tehditlerine karşı yeterli güvenlik tedbirlerinin alınmasını sağlamakta mıdır?
- COVID-19 krizinin ele alınma biçimi ile daha çok belirginleşmiş olan güvenlikleştirme ve kriz yönetimi ilişkisinin siber alandaki karşılığı nedir?
- Genel kriz yönetimi kavramları ve siber güvenlik kriz yönetimi kavramları arasındaki benzerlik ve farklılıklar nelerdir?
- Kriz yönetimi kavramı, siber güvenlik krizlerinin ele alınışında nasıl yorumlanmalıdır?
- Siber Güvenlik krizlerinin yönetiminde odak noktası ve kapsam nedir?

Çalışmanın temel amacı kapsamında ikincil amaçları ise şu şekilde belirlenmiştir:

- Türkiye'de siber alan nasıl yönetilmektedir?
- Türkiye'de kamuda siber güvenlik yönetim organizasyonu nasıl yapılandırılmıştır?
- Türkiye'deki siber güvenlik mevzuatının durumu nedir?
- Türkiye'de siber güvenlik krizleri, hangi durumlarda güvenlikleştirme alanına dahil edilmektedir?

Kısacası, siber uzayın güvenliğinin sağlanması esnasında orta çıkmış olan ve gelecekte ortaya çıkması muhtemel güvenlik krizlerinin ülkemiz özelinde nasıl yönetildiği, bu çalışmanın konusunu oluşturmaktadır. Daha geniş ifade ile ülke nüfusunun büyük bir bölümünün etkileşim halinde olduğu, COVID-19 krizi ile birlikte artan bir ivmeyle ekonomi, eğitim, kamu yönetimi, hayatın hemen hemen tüm alanlarının siber uzayda geniş karşılık bulmasının getirdiği yeni güvenlik sorunları ve olası kriz durumlarına karşı nasıl tedbirler alındığı, bu alandaki tehdit evreninin nasıl tanımlandığı, kamu siber güvenlik hiyerarşisinin nasıl

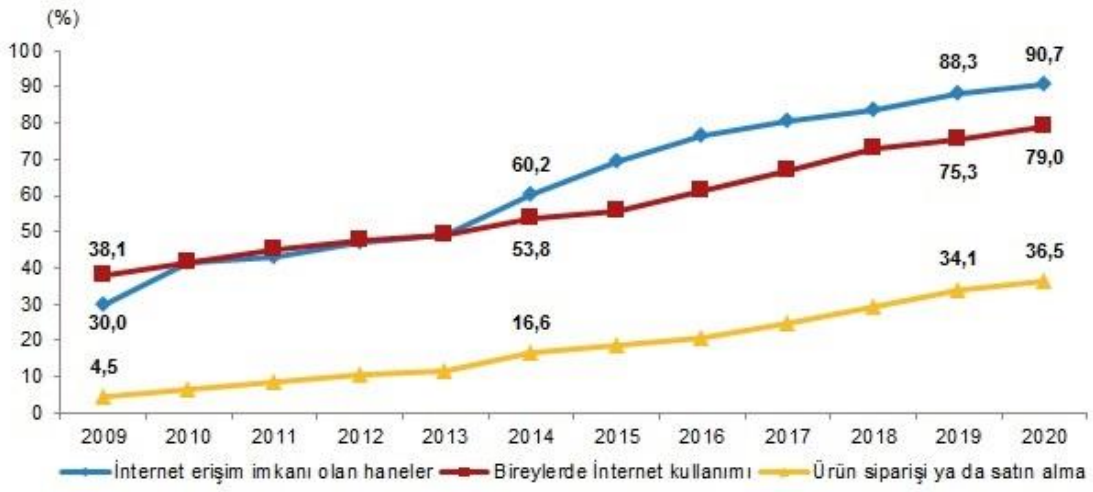
şekillendirildiğinin güvenlikleştirme teorisi ile analizi, ikincil konuları oluşturmaktadır.

Çalışma yukarıda yer alan sorulara aranan cevaplar ışığında yapılandırılmıştır. Bu temel soruların yanıtları elde edilen veriler sonucunda "Araştırmanın Bulguları" bölümde tartışılmış ve değerlendirilmiştir.

1.2 ARAŞTIRMANIN KAPSAMI VE SINIRLILIKLARI

Günümüzde siber alanın istatistiksel bir değerlendirmesini yaptığımızda, dünya nüfusunun % 60'a yakını internet kullanıcısı, % 49'u sosyal medya kullanıcısıdır. 2020 yılında bir önceki yıla göre aktif internet kullanıcı sayısı % 7, sosyal medya kullanıcı sayısı % 9 oranında artış göstermiştir. Aktif internet kullanıcılarının % 74'ü internet üzerinden alışveriş yapmaktadır (Digital 2020: Turkey, 2020). Ülkemizdeki rakamlar ele alındığında ülke nüfusunun % 74'ü aktif internet kullanıcısıdır, sosyal medya kullanım oranı ise % 64 seviyelerindedir. 2020 yılında bir önceki yıla göre aktif internet kullanıcısı % 4, sosyal medya kullanıcı sayısı % 4.2 artış göstermiştir. Aktif internet kullanıcılarının günlük internet kullanımı 7,5 saat dolaylarındadır (Digital 2020: Turkey, 2020). Bu zaman diliminin içinde 3 saatlik bir sosyal medya kullanımı yer almaktadır. Dikkat çekici bir diğer istatistik ise siber uzayın genişlemesinin bir sonucu olarak ortaya çıkan kripto para kullanımındadır. Aktif internet kullanıcıların % 10'luk bir kısmı kripto para sahibidir. Ülkede 770.000 evde akıllı ev cihazları mevcuttur. Sosyal medyanın iş maksatlı kullanımı % 44 seviyelerindedir (Digital 2020: Turkey, 2020). TUİK istatistiklerinin yer aldığı Şekil-5'te yer alan yıllara göre hane halkı internet kullanımı grafiği incelendiğinde internet kullanımın yaygınlaşmasındaki yüksek ivme ortaya çıkmaktadır.

Şekil-1: Hane halkı bilişim teknolojileri kullanımına ilişkin temel göstergeler, 2009-2020



Kaynak: TUIK Resmi İnternet Sitesi, https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2020-33679 Erişim Tarihi: 18 Mayıs 2021

Yukarıda yer alan istatistikler göz önünde bulundurulduğunda günümüzde insanların sanal alanda, fiziksel alanda aktif olarak yer aldığı zaman dilimine yakın seviyede vakit geçirdiği ortaya çıkmaktadır. Bu durum ise beraberinde, siber alana ilişkin çalışmaların kapsamının oluşturulmasında dar bir çerçevenin belirlenmesini getirmektedir. Siber alana ilişkin araştırma kapsamının geniş tutulması, beraberinde araştırma evreninin analiz edilebilmesini imkansız hale getirebilme tehlikesini barındırmaktadır. Bu çerçevenin kısıtlı tutulmasının bir diğer nedeni de bu alanda yaşanan hızlı gelişmedir. Sınırları geniş tutulmuş bir siber alan çalışması, sonuçlandırıldığında güncelliğini yitirmiş argümanlara sahip bir araştırma olarak karşımıza çıkabilir. Bu çalışmanın başlangıcında COVID-19 krizi daha dünyayı sarmamış, beraberinde getirdiği dijital dönüşüm fırtınası başlamamıştı. Dünyadaki internet kullanıcı sayısı, çalışmanın sonuçlanma aşamasına geldiğinde başlangıca göre %10'luk bir artış göstermiş ve siber uzaya 500.000.000 yeni insan eklenmiştir.

Bu kapsamda ülkemizde yeni başlayan siber güvenlik araştırmalarına[1] katkı sunmak maksadıyla, dünyada ve ülkemizde emekleme aşamasında olan "siber güvenlik kriz yönetimi konusu" çalışmanın ana odak noktası olarak belirlenmiştir. Ancak siber alanın büyüklüğü ve artan ivmeli büyüme hızı odak noktasının daha da küçültülmesini gerektirmiş, çalışma kamu özelinde bir siber güvenlik kriz yönetimi çalışmasına evrilmiştir. Bu noktada tüm kamu kurum ve kuruluşlarını kapsayan bir çalışma yapılması yine geniş bir kapsam olarak karşımıza çıkmış ve nihayetinde çalışma, kamuda siber güvenlikten sorumlu bakanlık olan T.C. Ulaştırma ve Altyapı Bakanlığı siber güvenlik faaliyetleri ve düzenlemeleri odağında gerçekleştirilmiştir. Ancak tüm kamu genelini ilgilendiren düzenlemeler yapan kamu kurum ve kuruluşlarının (Örn. Türkiye Dijital Dönüşüm Ofisi, Kişisel Verilerin Korunması Kurumu vd.) faaliyet ve düzenlemeleri, çalışmanın çerçevesi içerisine alınmıştır. Araştırma konusu kamu özelinde tutulduğu için "HİZMETE ÖZEL[2]" ve üstü gizlilik dereceli bilgilerin kamuoyu ile paylaşılmaması nedeniyle kamunun "TASNİF DIŞI" belgeleri ve uygulamaları üzerinden bir analiz gerçekleştirilmesi durumu söz konusu olmuştur.

1.3 LİTERATÜR TARAMASI

Tez çalışması sonucunda öncelikle kapsamlı bir literatür taraması yapılmıştır.[3] Tez çalışması, üç ana argümanın kesişim noktasında bulunmaktadır; Siber güvenlik, kriz yönetimi, güvenlikleştirme. "Siber güvenlik" kelimelerini içeren doktora tezleri araştırıldığında karşımıza bugüne kadar yayımlanmış 7 doktora tezi çıkmaktadır. Bu tezlerden ilki 2016 yılında yayımlanmış olup 4 tanesi sosyal

[1] Siber güvenlik konulu bir tezin ilk yayımı olan 2012 yılı ile siber güvenlik kavramının 40 yıllık geçmişi karşılaştırıldığında neden yeni ve oldukça geç kalınmış olduğu daha da belirginleşecektir.
"[2] Ek-3 Bilgi Varlıklarının Derecelendirilmesi Kılavuzu Gizlilik Dereceleri ilgili detaylı açıklamayı içermektedir. Günümüzde bu konuya kesin hatlarıyla açıklık getiren başka resmi bir kaynak mevcut olmaması nedeniyle belgelere gizlilik derecesi verilmesi konusunda uyuşmazlık yaşanmaktadır.
[3] Araştırma ile ilgili literatür taraması öncelikle YÖK Tez veri tabanı taranarak gerçekleştirilmiş, akabinde Hacettepe Üniversitesi Kütüphanesi vasıtasıyla yerli ve yabancı kitap, makale, rapor ve diğer akademik yayınlar incelenmiştir. Milli Kütüphane, yerli kitapevleri ve yabancı kitapların dijital kopyalarının yer aldığı internet siteleri gözden geçirilmiştir. Google vb. arama motorlarında akademik kaynakları ön plana çıkaran anahtar kelimeler vasıtasıyla aramalar gerçekleştirilmiş, erişilen yerli ve yabancı resmi ve özel internet siteleri, bloglar, akademik çalışmaların paylaşıldığı portallar konu kapsamında taranmıştır.

bilimler alanında, 3 tanesi ise fen bilimler alanında gerçekleştirilmiştir. İlk doktora tezinin 2016 yılında yayımlanmış olması ve sayısının 4 ile sınırlı olması alanın ülkemizde yeni ele alınmış olmaya başlandığının ve yeteri kadar çalışmanın gerçekleştirilmemiş olduğunun bir göstergesi niteliğindedir. Sosyal bilimler alanındaki tezler incelendiğinde, aşağıda yer alan çalışmalar ortaya çıkarılmıştır.

Güntay, tarafından kaleme alınmış olan “Uluslararası İlişkiler Temelinde Siber Güvenlik: Mikro Siber İttifak Teorisi Micro-CAT” konu başlıklı tez çalışmasında ülkelerin siber güç kapasiteleri analiz edilmiş ve mevcut siber güçlerine göre siber alanda geçici ittifaklar kurma yoluna gittiklerine ilişkin bulgular elde edilmiştir. Her ne kadar siber güvenlik üzerine bir başlık inşa edilmiş olsa da ülkelerin siber saldırı ve güç kapasiteleri, tezin ikincil araştırma sorunsalları arasındadır. Savunma ve saldırı kapasitesine göre ülkelerin ittifak kurma politikaları tezin genel çatısını oluşturmaktadır. Tez içerisinde ülkemizdeki siber güvenlik organizasyonları irdelenme aşamasında siber güvenlik kriz yönetiminde önemli bir bileşen olan USOM ve faaliyetlerine yönelik bulgulara yer verilmiştir. Tezde “mikro ittifak kurma kavramı” yeni bir teori olarak sunulmuştur. Ülkelerin siber güç kapasitelerine ilişkin özgün bulgulara da yer verilmiştir (Güntay, 2016).

Darıcılı, tarafından kaleme alınmış olan “Amerika Birleşik Devletleri ve Rusya Federasyonu’nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi” konu başlıklı tez çalışmasında ABD ve Rusya Federasyonu’nun ulusal siber güvenlik stratejileri karşılaştırılmıştır. ABD ve Rusya Federasyonu gibi alanın öncü ve güçlü iki ülkesinin siber güvenlik stratejilerindeki farklılıklar siber güvenlikleştirme kavramına ışık tutmaktadır. Metin içerisinde siber güvenlikleştirme kavramı doğrudan ele alınmamış olmasına rağmen aynı duruma her iki ülkenin farklı yaklaşım sergilemesi, ülkelerin siber güvenliğe olan yaklaşmışlarında kendilerine özgü siyasal argümanların hakim olduğu çıkarımı elde edilebilmektedir. ABD saldırgan yönünü gizli bir şekilde icra ederken Rusya Federasyonu siber uzaydaki etki gücünü dış politika olaylarında güçlü bir olasılık dahilinde doğrudan kullanmakta ancak siber alandaki teknik imkansızlıklardan dolayı tam olarak bu faaliyetler ispatlanamamaktadır. Ayrıca her iki ülkenin icra ettiği olası siber

saldırılar geleceğe ilişkin siber güvenlik olaylarının nasıl gerçekleşeceği yönünde önemli bulgular sunmaktadır (Darıcılı, 2017).

Bozgeyik, tarafından işletme anabilim dalında kaleme alınan "Gaziantep'te Faaliyet Gösteren Orta ve Büyük Ölçekli İşletmelerin Siber Güvenlik Yönetim Yaklaşımlarının Analizi" konulu çalışmada genel siber güvenlik kavramlarına değinilerek Gaziantep özelinde orta ölçekli firmaların siber güvenlik yönetim yaklaşımları analiz edilmiştir (Bozgeyik, 2018). Göçoğlu tarafından kamu yönetimi anabilim dalında kaleme alınan "Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi" konulu çalışmada ise siber alanda saldırgan faaliyetler icra etmekten çekinmeyen İran, ABD, Rusya Federasyonu, İsrail vd. ülkelerin siber güvenlik politikaları incelenmiş, ülkemizde mevcut siber güvenlik mevzuatı ve resmi düzenlemeleri üzerinden kamu politikası analizi yapılmıştır. Yazar "Türkiye'nin siber güvenlik politikalarının kamu politikası analizi yaklaşımları çerçevesindeki yönelimleri nelerdir?" sorusuna cevap ararken "*Türkiye'de hem karar verme açısından hem de siber güvenliğin sağlanmasına yönelik atılacak adımlar açısından bir belirsizlik ortamı var olduğu görülmüş, karar vericilerin bu alandaki teknik bilgilerinin yeterince kapsamlı olmadığı ve bu konuda diğer ülke uygulamalarına ilişkin raporlar oluşturma gibi araştırmalara yöneldikleri*" (Göçoğlu, 2018, s. 7) tespitinde bulunmuştur. Bu belirsizlik durumu araştırmamızın temel sorunsalları arasında olan karar verici aktörlerin siyasal olandan güvenlik alanına geçişteki muğlaklığın varlığının ispatına yönelik destekleyici bir argüman olarak karşımıza çıkmaktadır. Göçoğlu bu duruma karşın cevabı kamu politikaları geliştirilmesi kapsamında aramıştır, araştırmamızda bu cevaplar güvenlikleştirme teorisi ışığında aranmıştır (Göçoğlu, 2018).

Siber güvenlik kavramına ilişkin yüksek lisans tezleri ele alındığında ise 2012 yılında ilk tezin yayımlandığı günümüze kadar 57 tez çalışmasının görülmüştür. 16 farklı anabilim dalında çalışma yapıldığı tespit edilmiştir. Yelpazenin genişliği siber güvenlik kavramının multi-disipliner yapısını ortaya çıkarmaktadır. Uluslararası ilişkiler alanındaki siber güvenlik çalışmalarının baskınlığı siber alan

kavramının uluslararası niteliğinden kaynaklanmaktadır. Bu durum araştırma sayılarına doğrudan etkilemiştir. Fen bilimlerinde çalışmaların bir kısmı da sosyal bilimler alanında ele alınabilecek konuları araştırma sorunsalı olarak belirlemiştir. Ancak siber güvenliğin teknik boyutu kapsam dışı bırakıldığından siber güvenlik teknik terimleri üzerinden bir araştırma ile gerçekçi bir araştırma sayısına ulaşılabilecektir. Güvenlik duvarı, antivirüs sistemleri, log analiz, saldırı tespit ve önleme sistemlerine yönelik teknik araştırmalar kapsam içerisinde yer almamaktadır.

Şekil-2 Anabilim Dallarına Göre Tez Dağılımı

Sosyal Bilimler alanındaki tezler incelendiğinde, siber güvenlik krizlerinin güvenlikleştirilmesine ilişkin doğrudan bir tez bulunmamaktadır. Uluslararası alanda örnekleri bulunan ve yeni bir araştırma alanı olarak ortaya çıkan “siber-

güvenlikleştirme" üzerine ise bir adet tezin var olduğu tespit edilmiştir. Küçükaydın tarafından kaleme alınan "National and International Cybersecurity Strategies of The United States: A Securitizatıon Attempt" konulu tezde *"siber güvelik kavramı ABD tarafından nasıl ve neden ulusal güvenlik meselesi olarak ele alınmıştır?"* sorusunun cevapları aranırken, birincil kaynakların niteliksel incelemesi araştırma yönteminin odak noktası olarak belirlenmiştir. Bu incelemenin nedensellik bağını açıklayıcı gücünün Kopenhag Okulu'nun Güvenlikleştirme Teorisi ile desteklenmesi hedeflenerek siber güvenlik sorunlarının bir güvenlik meselesi haline nasıl getirildiği açıklanmaya çalışılmıştır. ABD'nin siber alandaki gri bölgelerden yararlanarak diğer alanlarda izlediği politikaları siber alandaki faaliyetleri ile desteklemeye çalıştığı ve bu duruma uluslararası kapsama sahip bir siber güvenlikleştirme hareketinin yokluğunun sebep olduğu çıkarımında bulunulmuştur (Küçükaydın, 2016).

Kurnaz tarafından kaleme alınmış olan "21. yüzyılda Ortodoks Güvenlik Paradigmasının Aşınımı: Uluslararası İlişkilerde Siber Güvenlik" konulu çalışmada 21. yüzyılda güvenlik kavramının dönüşümü odağına siber alanın beraberinde getirdiği güvenlik sorunlarını merkeze alan bir metod izlenmiştir. Çalışma sonucunda siber güvenlik sorunlarının klasik güvenlik yaklaşımları ile cevaplanamadığını, siber güvenlik tehditlerinin kaynağının muğlaklığı, asimetrik karakterinin uluslararası alanda yeni tehdit aktörlerinin varlığına sebebiyet verdiği tespitinde bulunulmuştur (Kurnaz, 2016).

Araştırmanın diğer argümanı olan kriz yönetimi kavramı üzerine ülkemizde 26 adet doktora tezi yapılmıştır. Güvenlik krizleri yönetimini doğrudan ele alan bir çalışmanın bulunmamasıyla birlikte bu alana yakınlaşan iki tez öne çıkmaktadır. Uysal tarafından kaleme alınmış olan "İnsani Müdahale Harekâtlarında Çatışma ve Kriz Yönetimi: Sivil-Asker İşbirliği Tartışmaları" konulu tez çalışmasında insan hakları güvenliğinin ihlali sonucu ortaya çıkan kriz durumlarında uluslararası müdahale ve kriz yönetimine ilişkin değerlendirmelere yer verilmiştir. Uysal, BM'nin, 20. yüzyıl sonları ve 21. yüzyıl da yaşanan askeri çatışmalar sonucu ortaya çıkan insan hakları krizlerinin yönetimine sistematik bir yaklaşım

sergileyemediğini ve krizlere zamanında müdahale edilemediği sonucuna ulaşmıştır. Soğuk savaş sonrasında güvenlik kavramının dönüşüme uğradığını ve BM'nin bu dönüşüme ayak uyduramayarak güvenlik olaylarına karşı soğuk savaş döneminden kalma bir yaklaşım sergilediği tespitine yer verilmektedir. Her ne kadar çalışma içerisinde güvenlikleştirme teorisinin temel argümanlarına yer verilmemiş olsa da güvenlikleştirme teorisinin çıkış noktasını oluşturan güvenlik kavramının dönüşümü ve askeri güvenlik kavramı dışına yayılımına ilişkin insani güvenlik krizleri bağlamında örnekler sunulmuştur. Aynı zamanda insan haklarına yönelik tehditlerin güvenlik krizi olarak belirlenmesinde BM çatısı altındaki ülkelerin konuya siyasi çıkarlar ve öncelikler bağlamında yaklaştığı değerlendirilmesinde bulunulmuştur. Güvenlik meselelerinin ele alınmasında reel tehditlerin analizi yerine siyasi bir değerlendirme yapıldığı önermesi tezimizin temel argümanları ile paralellik göstermektedir (Uysal, 2018).

Öztürk tarafından kaleme alınmış olan "Stratejik Halkla İlişkiler Kapsamında Kriz Yönetimi: Türkiye'de Krizlerin Algılanması Üzerine Bir Araştırma" konulu çalışmanın temel araştırma soruları arasında "*Kriz algılaması ile ilişkili unsurları tespit edebilmek ve bu yolla kriz yönetimi ve kriz iletişimi alanında fayda üretebilmek mümkün olabilir mi?"* sorusuna yer verilerek çevresel krizlerin algılamasında yaş, cinsiyet, eğitim, gelir düzeyi, meslek, çocuk sahibi olmak, otomobil sahibi olmak gibi değişkenlerin etkili olduğu çıkarımlarında bulunulmuştur. Başarılı bir güvenlikleştirme için güvenlikleştirici aktör ve dinleyici kitle ilişkisi ön plana çıkmakta ve güvenlikleştirici aktörün ortaya koyduğu olağan dışı güvenlik tedbirlerinin kabulü başarı kriteri sayılmaktadır. Bu anlamda kriz ve algı yönetimi başarılı bir güvenlikleştirme için temel argümanlar arasında yer almaktadır. Öztürk çalışmasında, kriz ve algı yönetimi arasındaki ilişkiyi Türk toplumunun geçmişte yaşadığı örnek krizlerin analizini yaparak ortaya koymaya çalışmış, Türk toplumunun krizleri algılamasına yönelik belli kategoriler ortaya koyarak gelecekte icra edilecek olan kriz yönetimi ve iletişim faaliyetlerine ışık tutmayı amaçlamıştır. Uysal çalışmasında belirli kategori ve hal tarzlarını ortaya çıkarırken güvenlik konularını siyasal (olağan) tedbirler ışığında ele almış ve

güvenlik tedbirlerini negatif bir bakış açısıyla olağan dışı bir yaklaşım olarak benimsemiştir (Öztürk, 2017).

Kriz yönetimine ilişkin yüksek lisans tezleri incelendiğinde siber güvenlik krizlerinin doğrudan ele alındığını görülmemektedir. Çatışma yönetimine ilişkin tezler bulunmakta ve askeri güvenlik meselelerine odaklanılmaktadır. Askeri çatışmaların ele alındığı tezler içerisinde Özocak'ın AB ve Kosova krizi odaklı çalışmasında kriz yönetiminin krizi önleme aşaması ele alınırken, askeri çatışmaların kriz durumuna evrilmesini önlemek için bazı olağan dışı tedbirlerin alınması gerekliliği vurgulanmaktadır. Özocak, olağandışı tedbirler alınarak krizin önlenebileceğini öne sürerken güvenlikleştirme argümanlarını kullanmamış olsa da olağan dışı tedbirlerle güvenlik sağlanmasına ilişkin önermesi, güvenlikleştirme argümanlarının sunduğu kavramlara karşılık sağlamaktadır. Güvenlik meseleleri kriz aşamasına tırmanmadan da güvenlikleştirmenin konusu olabileceği bu tez çerçevesinde örneklendirilmiştir (Özocak, 2019). Güvenlik krizlerini ele alan bir diğer önemli çalışma ise Dağar tarafından kaleme alınmış olan "Kriz Yönetiminde İstihbarat Birimlerinin Fonksiyonları ile Güvenlik Politikalar" konulu çalışmada güvenlik krizleri ve istihbarat örgütleri arasındaki ilişki incelenmiştir. Krizlerin güvenlikleştirilmesi için istihbarat örgütlerinin aldığı olağan dışı tedbirler ve olağandışı tedbir alabilme kabiliyetlerinin getirdiği avantajlar ele alınmıştır. Uluslararası siber güvenlik meselelerinde istihbarat örgütlerinin siber saldırıların gerçekleştirilmesindeki etkin rolü göz önünde bulundurulduğunda siber-güvenlikleştirme kavramının önemli bir aktörü olan istihbarat örgütlerinin temel güvenlik fonksiyonları kapsamlı bir şekilde değerlendirilmiştir. Çalışmada istihbarat örgütlerinin saldırgan ya da defansif siber alan faaliyetleri incelenmemekte ancak terör örgütlerinin siber alanı kullanımından nasıl bir fayda sağlandığı örneklendirilmektedir. FETÖ ve PYD terör örgütlerinin kullandığı mesajlaşma uygulamalarının deşifresinin örgütün çökertilmesinde nasıl kullanıldığı detayları ile birlikte ele alınmıştır (Dağar, 2019). Soy, kriz dönemlerinde başarılı bir yönetim için karizmatik bir liderin varlığının, krizin başarılı olarak yönetimine ilişkin katkılarını sorgulayan çalışmasında Recep Tayyip Erdoğan'ın kriz yönetimi süreçlerindeki katkılarının halk tarafından nasıl

karşılandığına ilişkin anket çalışmaları gerçekleştirerek; “Kriz öncesinde hedef kitlesinin güvenini almış, hedef kitle ile yakın ilişkiler geliştirmiş, ikna kabiliyeti güçlü, iletişimi etkili kullanan, hedef kitlesi ile güçlü bağlar kurmaya çabalayan bir liderin olası bir kriz anında kendi varlığının yegâne sebebi olan hedef kitlesini bu süreçte yanında tutarak krizi başarılı bir şekilde atlatabilmeye fayda sağladığı” (Soy, 2018, s. 23) tespitinde bulunmaktadır. Başarılı bir güvenlikleştirme için hedef kitlenin güvenlikleştirici aktörle hareket etmesi önemli bir güvenlikleştirme argümanı olup ülkemiz özelinde ise bu durumun mevcut uygulamalardaki karşılığına çalışmada yer verilmiş olması çalışmamız içerisinde siyasi liderliğe önem verilmesi gerekliliğini bizlere sunmaktadır (Soy, 2018).

Bu çalışmamızın bir diğer argümanı olan güvenlikleştirme kavramına ilişkin ülkemizde kaleme alınan doktora tezleri araştırıldığında, karşımıza 9 adet tez çalışması çıkmaktadır. Miş, tarafından kaleme alınmış olan “Güvenlikleştirme Teorisi ve Türkiye'de Güvenlikleştirme Siyaseti: 1923-2003” konulu tez çalışmasında, Kopenhag Okulu ve Schmitt ilişkisi üzerinde analizler gerçekleştirilmiş ve güvenlikleştirme siyasetinin Türkiye’de Schmityen bir çizgide olduğu önermelerinde bulunulmuştur (Miş, 2012). Küpeli tarafından kaleme alınan “Güvenlikleştirme Teorisi Bağlamında Kritik Altyapıların Terörist Saldırılardan Korunmasının ABD ve AB Güvenlik Politikalarındaki Rolü” konulu tez çalışmasında ise kritik altyapıların siber güvenliğinin sağlanmasının kritik altyapı güvenlikleştirilmesi süreci için önemli olgu olduğu tespiti yapılmış ancak bahse konu güvenlikleştirme faaliyetleri siyasal alan içerisinde tanımlanmış, olağanüstü tedbirler öngörülmemiştir. Güvenlikleştirmenin siyaset bilimi ile olan ilişkilerine değinilmeden güncel faaliyetlerin nasıl güvenli yönetileceğinin analizi yapılmıştır. (Küpeli, 2019) Doğan tarafından (Doğan, 2019) kaleme alınmış olan “Güvenlikleştirme Süreçlerinde Medyanın Rolü: 28 Şubat Örneği” konulu çalışmada güvenlikleştirme süreçlerine medyanın etkisi analiz edilmiştir. Doğan medya ve güvenlikleştirme ilişkisini çift taraflı olarak ele alarak medyanın sadece güvenlikleştirme aracı olmadığı, aynı zamanda siyasetin gündemine etki edebilme gücü sayesinde güvenlikleştirme süreci başlatabilme imkanına sahip olduğu önermesinde bulunmaktadır. Doğan önermesini şu şekilde açıklamıştır:

> Medya sadece güvenlikleştirici aktörlerce kullanılması hususunda değil aynı zamanda bu güvenlikleştirici aktörlerin bir meseleyi güvenlik sorunu olarak ele almasında da etkilidir. Zira hatırlanacağı üzere medyanın gündem belirleme özelliğinden bahsederken medyanın gündeminin siyasetin gündeminden beslendiğini ve bununla beraber meydanında siyasetin gündemine etki edebildiğini belirtmiştik. Bu açıdan güvenlikleştirici aktörler hem medyayı güvenlik söylemlerinin yaygınlaşması amacıyla kullanabilirken güvenlik söylemlerinin içeriği noktasında medyadan etkilenebilmektedirler (Doğan, 2019).

Siber güvenlik, güvenlikleştirme ve kriz yönetimi kapsamında kaleme alınmış bilimsel makaleler ele alındığında güvenliğin ve siber güvenliğin değişen boyutunu AB, BM ve NATO gibi uluslararası örgütler bazında, ABD, Rusya gibi siber alanda özellikle saldırgan anlamda önde olan ülkelerin politikalarına yönelik çeşitli araştırmalar karşımıza çıkmaktadır (Köksoy, 2020); (Bıçakçı, NATO'nun gelişen tehdit algısı: 21. Yüzyılda siber güvenlik, 2014). Güvenlikleştirme teorisi ve siber güvenlik ilişkisi özelinde ise kaleme alınmış bir makale ya da kitap, Türkçe eserler içinde bulunamamıştır. Yabancı kaynaklar ele alındığında ise Hansen & Nissenbaum'un siber güvenlikleştirme kavramının yeni bir güvenlik sektörü olarak ortaya çıkışının başlangıcını sağladığı tespit edilmiştir. Hansen ve Nissenbaum siber alanın güvenlikleştirme teorisisin ilk günlerindeki konumunda olmadığı, 2010 yılı itibari ile hayatın her alanında etki sahibi olduğu ve bu nedenle yeni bir sektör olarak ele alınması gerektiğini öne sürmektedir (Hansen and Nissenbaum, 2009).

Siber güvenlik krizlerinin yönetimine ilişkin makaleler incelendiğinde, siber güvenlik krizlerinin tekil olarak kurum bazında yönetimine ilişkin önermeler karşımıza çıkmaktadır. Bu önermeler ise siber güvenlik krizlerinin teknik yönü üzerine inşa edilmekte, siber olay tespit, engelleme ve müdahale süreç ve yazılımları üzerinden modeller sunulmaktadır. Ulusal boyutta siber güvenlik krizlerinin devlet kurumları tarafından yönetimi, ulusal bir organizasyonun nasıl olması gerektiğine ilişkin kapsamlı bir çalışma yapılmadığı tespit edilmiştir. Bu konuya en yakın çalışmanın 2014 yılında AB Siber Güvenlik Ajansı (ENISA) tarafından gerçekleştirildiği bu çalışmada siber güvenlik krizlerinin yönetimine ilişkin genel bir çerçeve çizildiği görülmüştür (Trimintzios, Holfeldt, Uckan, and

Gavrila, 2014). Ancak çalışma AB odaklı olarak ele alınmış sonrasında ulusal bazda bir çalışma gerçekleştirilmemiştir.

Literatür taraması neticesinde çalışmanın üç ana argümanı olan Siber güvenlik, kriz yönetimi, güvenlikleştirme kavramlarının literatürde nasıl yer aldığı belirlenmiş, çalışmanın özgünlüğünü ortaya çıkarmış olan boşluk analizi çalışmamıza ilişkin veriler toplanmış ve analiz edilmiştir.

1.4 ARAŞTIRMANIN ÖZGÜN DEĞER, KATKI ve BEKLENTİLERİ

Türkiye'den elde edilen verilere göre, nüfusunun %74'ü aktif internet kullanıcısıdır, sosyal medya kullanım oranı ise % 64 seviyelerindedir. 2020 yılında bir önceki yıla göre aktif internet kullanıcısı %4, sosyal medya kullanıcı sayısı % 4,2 artış göstermiştir. Aktif internet kullanıcılarının günlük internet kullanımı 7,5 saat dolaylarındadır. Bu zaman diliminin içinde 3 saatlik bir sosyal medya kullanımı yer almaktadır. (Kemp, 2020) Ülke olarak siber alandaki varlığımız karşısında bu alanın güvenliğine ilişkin çalışmalar yetersiz kalmaktadır. Bu durumda beraberinde her güvenlik krizinde çözümün bulunması, uzun bir dönem gerektirmektedir. Siber güvenlik kavramı ise kavramsal ve kuramsal çerçevenin çizildiği üçüncü bölümde ele alındığı üzere sadece teknik bir kavram değildir. Siber alanın bu geniş kullanımı toplumsal pek çok sorunun aynı zamanda siber güvenlik boyutunun olması durumunu beraberinde getirmektedir, Örneğin COVID-19 ile birlikte uzaktan eğitime geçişle beraber yaşanan internet erişimi sorunları, evinde bilgisayar olmayan çocukların bulunması konusu siber güvenlik alanının çalışma sahasına girmektedir. Üstelik bu durum sadece uzaktan eğitim platformlarına karşı siber saldırılarla sınırlı değildir, örnek durumda bilgi güvenliğinin ve siber alandaki bilgi güvenliğinin temel bileşenlerinden olan **erişilebilirlik** bu anlamda hasara uğramıştır. Türkiye'de çocukların bir kısmının siber uzayda yer alan eğitim faaliyetine erişim için fiziki olarak zor şartlara göğüs germesi sorunu (EBA'dan canlı derslere katılabilmek için her gün bir kilometre yürüyor, 2020) bilgiye erişim için yeterli kaynağın yaratılamaması (Bilgisayar

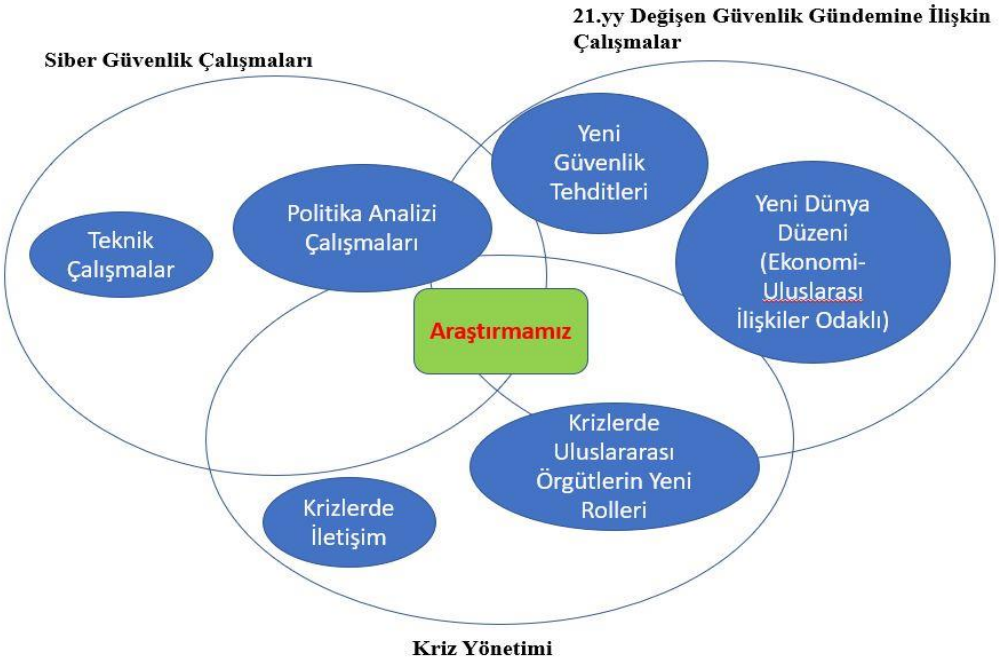
tedarik zincirinin sağlıklı kurulamaması, internet erişiminde yaşanan sıkıntılar vd.) nedeniyle siber güvenlik problemi ve krizi olarak ortaya çıkmaktadır. Siber güvenlik kavramına bu yelpazeden bakıldığında alandaki çalışmaların yetersizliğinin oranı çok daha artmaktadır.

Bir önceki bölümde ele alındığı üzere, siber güvenlik krizlerinin kamu genelinde ele alınmasına ilişkin doktora ve yüksek lisans seviyesinde bir çalışma ülkemizde mevcut değildir. Siber alanın kamu genelinde güvenliği kapsamı göz önüne alındığında bu kapsama karşılık gelen bir tezin yeterliliği sorusu akıllara gelecektir. Bu anlamda tezin kapsamı siber güvenliğin sağlanmasından sorumlu T.C. Ulaştırma ve Altyapı Bakanlığı faaliyetleri çerçevesinde ele alınmış, ülkemizin genel siber güvenliğine ilişkin düzenlemeler ve faaliyetler odağında ilerlenilmiştir.

Siber güvenlik krizlerinin yönetimi üzerine bir çalışma gerçekleştirirken işin teknik boyutuna saplanmadan, büyük resmi görebilmek için sosyal bilimler argümanlarından faydalanılması bir gereklilik olarak ortaya çıkmaktadır. Bu noktada güvenlik kavramının Türkiye'de ele alınış biçimi, krizlerin yönetimine ilişkin yaklaşımları kapsayan bir siber güvenlik kriz yönetimi çalışması sonucunda araştırmanın istenen seviyede olabileceği tespit edilmiştir. Alandaki bu boşluğu doldurmak için gerçekleştirilen literatür taraması ve analizler neticesinde güvenlikleştirme teorisi ve kriz yönetimi arasındaki yakın ilişki ortaya konmuştur. COVID-19 krizinin ele alınış biçimi kriz yönetiminde güvenlikleştirme argümanları ile hareket edildiğinin bir göstergesi olarak ortaya çıkmıştır. Durumun kriz olarak kabulü reel tehditlerin başlangıcı ile değil ilk vaka sayılarının ülkemizde artışa geçmesiyle olmuştur. Bu aşamada şu nokta da gözden kaçırılmamalıdır: Siyasal alanda bu konu, güvenlik tehdidi olarak reel tehditlerin başlangıcı ile olmuş, devlet mekanizması kendi içerisinde bazı tedbirler almıştır. Ancak güvenlikleştirme süreci olarak adlandırdığımız süreç olağanüstü tedbir alma kararlarının alınıp uygulanmasıyla başlamıştır. Yine krizin ilk dalgası olarak belirtilen dönemin bittiğinin kabulü de reel tehditler ışığında değil, güvenlikleştirme sürecinin ekonomi başta olmak üzere diğer güvenlikleştirme sektörlerinde yarattığı

tahribatla reel tehditler arasındaki denge gözetilerek gerçekleştirilmiştir. 2020 yaz döneminde halen reel olarak COVID-19 vakaları mevcutken güvenlikleştirme çabaları bu noktada düşürülmüş, güvenlikleştirmenin somut örnekleri olan sokağa çıkma yasağı, seyahat yasağı gibi güvenlikleştirici tedbirler bu aşamada kaldırılmıştır.

Şekil-3: Siber Güvenlik Krizlerinin Yönetimine İlişkin Gerçekleştirilen Araştırmaların Boşluk Analizi



Çalışma neticesinde, siber güvenlik ve güvenlikleştirme kavramı arasındaki ilişki ortaya çıkarılmıştır. Çalışmanın ilerleyen aşamalarında ele alınacak olan Cumhurbaşkanlığı siber güvenlik genelgesinde de belirtildiği şekilde[4] siber alandaki güvenlik olaylarının ve olası krizlerin ulusal bir güvenlik krizine dönüşme potansiyeli bir gerçeklik olarak karşımızda durmaktadır. Ancak bu durumun analizini gerçekleştiren bir çalışmanın bulunmaması ciddi bir kavramsal boşluk

[4] 2019 tarihli Cumhurbaşkanlığı Bilgi Güvenliği ve Siber Güvenlik genelgesi siber güvenlik kavramlarının açıkça ele alınıp kısa da olsa detaylandırıldığı hukuktaki normlar hiyerarşine göre en üstte olan hukuki düzenlemedir. Bu kapsamda tam metni Ek-5'te sunulmuştur.

yaratmaktadır. Bu çalışma ile bu boşluğun doldurulacağı düşünülmüştür. Güvenlikleştirme-Kriz Yönetimi, Siber Güvenlik-Güvenlikleştirme ilişkilerine ilişkin kavramsal bir çerçeve sunarak gelecekteki çalışmalara, bu alt alanlara ilişkin bir başlangıç noktası sunulmuş olacaktır. Çalışma neticesinde Kopenhag Okulu tarafından soğuk savaş sonrası dönemde dönüşüm geçiren güvenlik sorunlarına cevap olarak ortaya çıkartılan, güvenlikleştirme teorisinin önemli bir argümanı olan güvenlik sektörleri arasında siber uzayında yer alması gerektiği yine teorinin belirlediği analiz düzeylerinden ulusal analiz düzeyinde Türkiye örneği üzerinden ele alınarak ortaya konmuştur. Şekil-2 incelendiğinde, alandaki çalışmalar ve bu çalışmanın doldurmaya çalıştığı boşluk görülebilecektir.

Çalışmanın bu aşamasından sonra şimdi de çalışmanın metodu bölümü açıklanmıştır.

II. BÖLÜM

ARAŞTIRMANIN METODU

Bu bölümde araştırmanın metodolojisine yer verilmiştir. Diğer bir deyişle çalışmanın kapsamı, araştırmanın türü, araştırmanın ne tür verilere gereksinim duyduğu ve bu verilerin nereden ve ne şekilde hangi araştırma tekniği ile elde edildiği ve elde edilen verilerin ne şekilde analiz edildiği konularındaki açıklamalara bu bölümde yer verilmiştir.

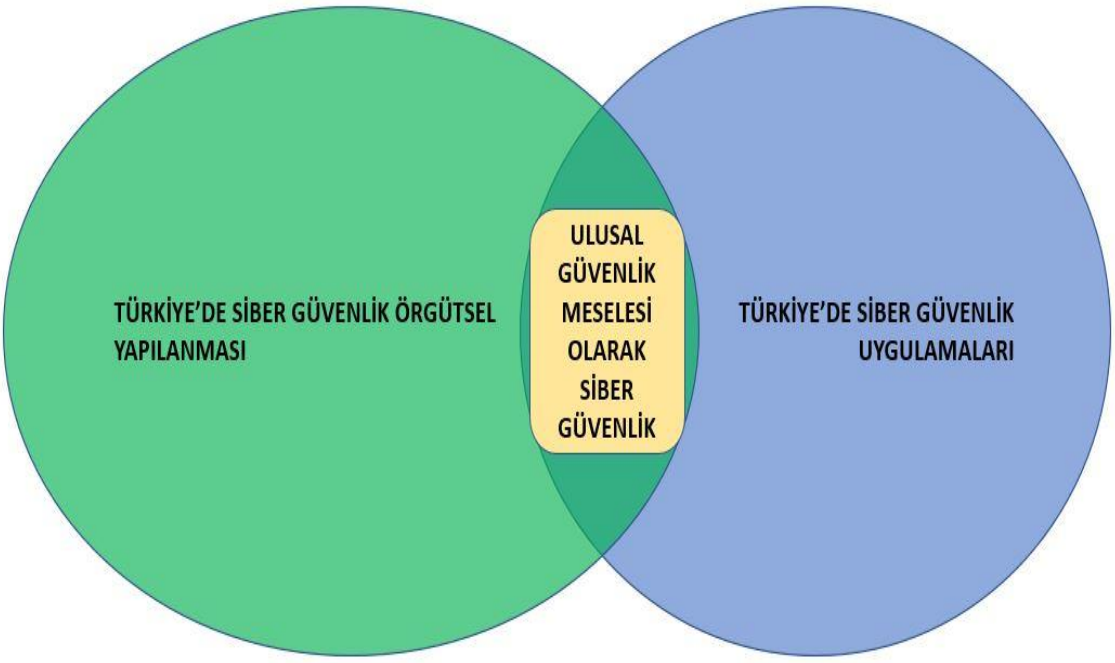
Bu araştırma, literatüre- ikincil verilere dayalı bir araştırmadır. Bu süreçte karşımıza verilerin nasıl toplanacağı ve analiz edileceği soruları çıkmaktadır. Bu noktada araştırmanın kapsamı ve araştırma soruları önem kazanmaktır. Araştırmanın kapsamı kamu genelini ilgilendiren ulusal ölçekteki siber güvenlik olaylarının ne zaman kriz olarak ele alındığı ve nasıl bir çözüm üretildiği ile sınırlıdır. Kriz kavramı ele alınırken, krizlerin siyasal boyutu kapsama alınarak güvenlikleştirme teorisi ve kriz yönetimi ilişkisi ele alınmıştır. Teori ve araştırma evreni tarafından sınırlandırılmış olan kapsam ve araştırma soruları ile kamuya odaklanmış olan bu araştırma için temel veri kaynağı olarak kamu idaresinin en temel dayanağı olan resmi dokümanlar seçilmiştir. Araştırmanın teorik ve kavramsal çerçevesini ele alırken detayları belirtilen güvenlikleştirme teorisinin kamunun yazılı metinleri ile olan doğrudan ilişkisinin de bu kararda etkisi bulunmaktadır. Araştırmanın temel dayanağının resmi dokümanlar olarak belirlenmesi sonrasında ikincil verilerin avantaj ve dezavantajları gözden geçirilmiş ve araştırma sonucu elde edilen verilerin analizi için, yazılı belgelerin içeriği titizlikle ve sistematik incelenmiş ve ileri veriler titizlikle derlenmiştir.

2.1 ARAŞTIRMA EVRENİ

Araştırma evrenini oluşturulurken temel kıstas olarak araştırmanın kapsamı belirlenmiştir. Dolayısıyla araştırma, Türkiye'de siber güvenlik[5], örgütsel yapılanma, uygulamalar ve geleceğe yönelik strateji ve politikalarını kapsayan bir çalışmadır. Bu nedenle çalışmanın evreni tüm Türkiye'dir denebilir.

Ek-1'de yer alan dokümanlar siber uzayın yönetimi ve genel kriz yönetimine ilişkin resmi düzenlemeleri içermektedir. Şekil-3'te sunulmuş olan modelde görüleceği üzere çalışmanın odağını; Türkiye'deki siber güvenliğe ilişkin örgütsel yapı ve mevcut uygulamaların, siber güvenlik krizlerini ulusal bir güvenlik meselesi eksenine alan bir analiz oluşturmuştur.

Şekil-4: Örneklemin Belirlenmesi



[5] Araştırma süresi olan 2 yıl zarfında siber uzay, yaklaşık olarak % 10'luk bir büyüme kaydetmiştir.

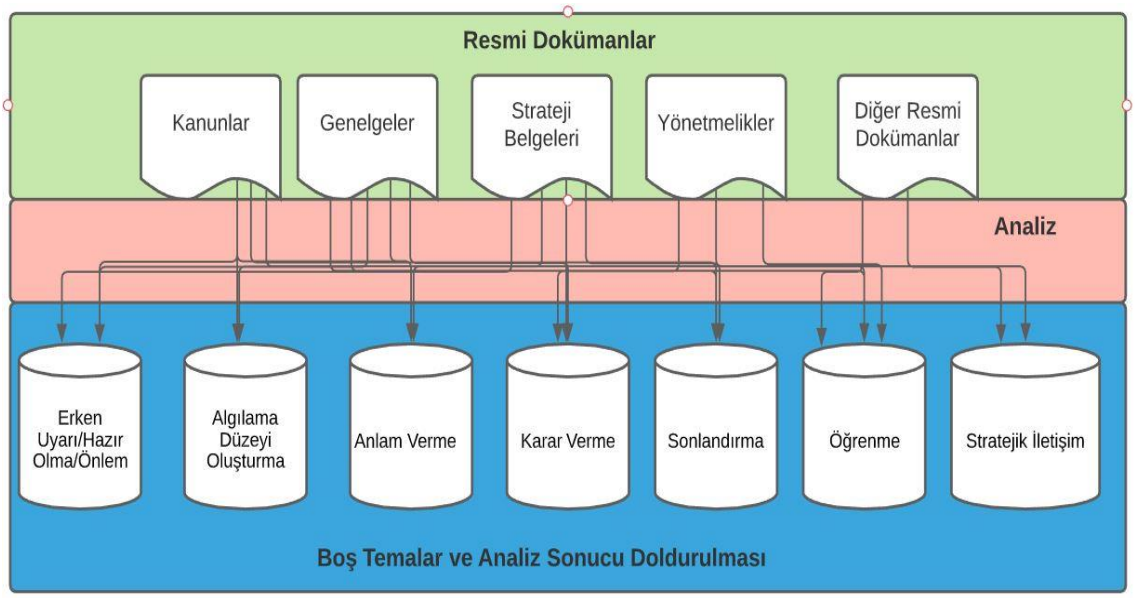
2.2 VERİLERİN TOPLANMASI ve ANALİZİ

Araştırmanın çıkış noktası, siber güvenlik krizlerinin ele alınışının teknik bir konunun yönetiminden ziyade siyasal bir süreç olduğu şeklindeki önermemizdir. Bu önermemizin teorik temelini güvenlikleştirme teorisi ve siber güvenlik kavramları arasında yer alan ilişki oluşturmaktadır. İkinci teorik dayanağımız ise güvenlikleştirme süreci ile kriz yönetimi kavramı arasındaki siyasal bağlantıdır. Teorik ve kavramsal çerçeve, resmi belgelerin toplanması için yeterli olsa da analiz için gerekli olan temalar ve kodlamaların ortaya çıkarılması için gerekli detaylar ve bilgiler için yeterli veri elde edilememektedir. Gerekli temaların oluşturulabilmesi için siber uzay, siber uzayın yönetimi ve güvenliği, ilgili siber uzay kavramlarının ülkemizdeki yansımasına ilişkin detaylı bir araştırma ve raporlama sürecinden geçilmiştir. Bu raporlama sürecinde, araştırmanın bulguları ve analizi gerçekleştirilmiş, kavramsal ve teorik çerçevenin pratikteki karşılığı ortaya konmuş ve bulguların analizi için gerekli temalar ve kodlamalar belirlenmiştir.

Araştırma sırasında elde edilen dokümanların içerik analizinin gerçekleştirilmesi için “örnekleyici yöntem” kullanılmıştır. Örnekleyici yöntem ile, araştırmacı kuramı somut bir tarihsel duruma veya toplumsal ortama uygular ya da verileri önceki kuramlara dayanarak düzenler. Önceden var olan kuram, boş kutular sağlar. Araştırmacı, onları dolduracak verilerin toplanıp toplanamayacağına bakar. Kutulardaki kanıtlar, araştırmacının toplumsal dünyayı yorumlamak için yararlı bir araç olarak kullandığı kuramı doğrular ya da reddeder. Kuram, genel bir model, bir benzeşim ya da bir dizi basamak biçiminde olabilir (Neuman, 2006, s. 659). Bahse konu boş kutular, örnekleyici yöntemin bir parçası olarak kullanılan kavramsal kategorilerdir.

Araştırma neticesinde, siber güvenlik krizlerinin yönetimine ilişkin 7 tema belirlenmiş ve bazı temalar için alt kategoriler oluşturulmuştur. Analiz ilerledikçe her bir doküman incelenmiş ve ilgili temalara ait boş alanlar doldurulmuştur. Şekil-5’te de analiz süreci modellenmiştir.

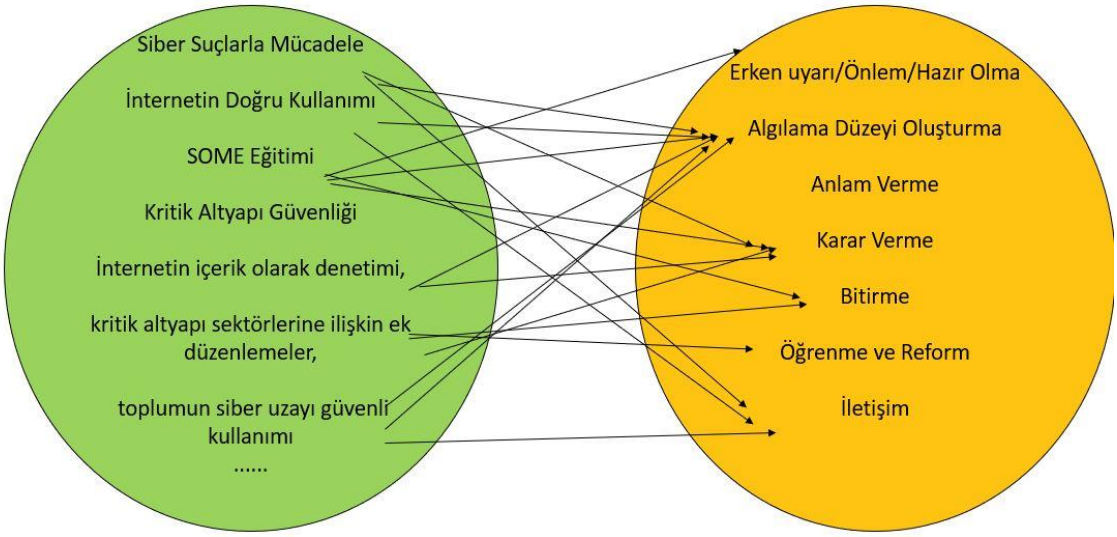
Şekil-5: Analiz Modeli



Analiz temaları oluşturulurken kavramsal çerçevede yer alan kriz yönetimi ve siber güvenlik ilişkisinden faydalanılmıştır. Belgelerin anlamlandırılması içinse, tarihsel süreç içerisinde Türkiye'deki siber güvenlik algısının gelişiminin analizinden elde edilen bulgulardan yola çıkılmıştır. Söz konusu bulgular neticesinde kritik altyapı güvenliği, yerli siber güvenlik teknolojisi geliştirme, siber olaylara zamanında müdahale, siber olay yönetimi, SOME ekiplerinin etkinliğinin artırılması, internet trafiğinin teknik denetimi, internetin içerik olarak denetimi, kritik altyapı sektörlerine ilişkin ek düzenlemeler, toplumun siber uzayı güvenli kullanımı, kamu kurum kuruluşlarında bilgi güvenliği kültürünün oluşturulması, çocukların siber ortamda korunması, insan kaynağının yetiştirilmesi, uluslararası faaliyetlere katılım, siber suçlarla mücadele ve internetin doğru kullanımına ilişkin alt kodlamalar belirlenmiştir. Kodlamalara ilişkin bulgular analiz edildiğinde ise kodlama kümesi ve tema kümesi arasında birebir bir ilişki yerine bire çok bir ilişki ortaya çıkmıştır. İlgili kodlamalarla tema ilişkisi ise kavramsal çerçeveye göre belirlenmiştir. İlgili kodlamanın tarihsel süreç içerisindeki gelişimi ve algılanış biçimine göre temalara dağılımı gerçekleştirilmiştir (Bknz. Şekil-5). Bahse konu tarihsel sonuca siber uzayın büyüme süreci ve insan-siber uzay etkileşim

düzeyinin dönüşümü de etkili olmuştur. Aşağıda kodlamalar ve temalar arasındaki ilişki verilmiştir:

Şekil-6: Kodlamalar ve Temalar Arası İlişki



Güvenlikleştirme teorisi beş analiz seviyesi öngörmüştür: İnsan, topluluk, ulusal, uluslararası/bölgesel ve küresel. (Buzan, Security: A New Framework for Analysis, 1997) Bu seviyelere göre kodlamalara yaklaşım sağlanmıştır. Bir kodlamanın insan seviyesinde olan tematik karşılığı algılama düzeyi oluşturma temasına karşılık gelirken, aynı kodlamanın ulusal seviyede analizi gerçekleştirildiğinde karşılığının anlam verme teması olarak belirlendiği analizler gerçekleştirilmiştir. Bu durumun temel nedeni ise siber güvenliğe olan yaklaşımının analiz seviyeleri değiştikçe farklı tanımlamalara sahip olmasıdır. Örneklendirecek olursak, kritik altyapı güvenliğine ilişkin dokümanlarda insan seviyesindeki tanımlamalar genellikle bireysel güvenlik tedbirleri ya da teknisyenlere ait görevlere yönelikken, ulusal seviye de teknik önlemlerden ziyade ülke güvenliğinin temelden sarsılabileceği bir güvenlik çıkmazına neden olunabileceği algısının oluşturulması çerçevesinde tanımlamalar gerçekleştirilmiştir. Sonuç olarak derlenen veriler araştırmanın temel sorularını

yanıtlayacak şekilde sınıflandırılmış ve araştırmanın amaçlarına ulaşma doğrultusunda analiz edilmiştir.

III. BÖLÜM

KAVRAMSAL ve KURAMSAL ÇERÇEVE

Bu bölümde; çalışmanın kavramsal ve kuramsal çerçevesine yer verilmiştir. Diğer bir deyişle araştırmada kullanılmış olan temel kavramların ne anlama geldikleri, çalışmada hangi anlamda kullanılmış oldukları konusu ile çalışmanın dayandığı kuramsal çerçeveye ilişkin açıklamalar ve değerlendirmeler sunulmuştur. Diğer bir ifade ile, çalışmaya ilişkin çeşitli kavramsal ve kuramsal bilgiler ele alınmış, araştırmanın merkezi konumunda yer alan siber güvenlik kavramının gelişimi üzerinde durulmuş, siber güvenlik kavramını ortaya çıkaran siber alan kavramı, gelişimi, yönetimi ve bu alandaki güvenlik tehditleri ele alınmış, tüm bunlara dahil olarak güvenlikleştirme kavramı ve siber güvenlik ilişkisi değerlendirilmiştir.

Araştırmanın ana odak noktası olan Türkiye'de siber güvenlik krizlerinin yönetiminin güvenlikleştirme kavramı bağlamında ele alınmasına yönelik olarak siber güvenlik, güvenlikleştirme, kriz yönetimi kavramlarının ilişkisine yönelik kavramsal çerçevenin oluşturulması amaçlanmıştır.

Bu çerçevede ilk önce "Türkiye ve Güvenlik" kavramına yer verilmiştir.

3.1. TÜRKİYE ve GÜVENLİK KAVRAMI

Türkiye'nin güvenlik sorunlarına, güvenlik politikası üretme süreçlerine ve güvenlik krizlerine olan yaklaşımını, tarihsel ve kültürel bağlam derinden etkilemektedir (Aydın & Eker, 2013, s. 2). Türk toplumu için diğer tüm kavramların ötesinde, önde tutulan bir güvenlik yaklaşımı mevcuttur. Bunun en temel nedeni ise tarihsel tecrübelerden kaynaklanan, sürekli olarak güvenlik krizleri ile karşılaşılmasıdır. Bu güvenlik krizlerine ek olarak ülkenin jeopolitik konumu

güvenlik kavramsallaştırmasına etki eden diğer temel etken olarak karşımıza çıkmaktadır.

Türkiye tüm güvenlik sorunları, avantaj ve dezavantajları ile Osmanlı İmparatorluğu jeopolitiğinin merkezini devralmıştır. Bu sebepten dolayı komşu ve müttefik devletlerle olan ilişkilerinde bu tarihsel arka plan kendisini hissettirmektedir. Bu tarihsel arka planın içerisinde devlet yönetiminde devletin bekasına verilen önem, uzun süren savunma savaşları, devleti korumak için güdülen denge politikaları, komşu ülkelerle kimi zaman savaşa varan güvenlik krizleri ve nihayetinde birinci dünya savaşı sonrasında topyekün olarak devletin ortadan kalkmasına neden olan bir işgal vardır.

Cumhuriyet Türkiye'si tarihsel ve coğrafi güvenlik sorunlarından sıklıkla etkilenmiştir. Küresel güvenlik krizlerinin (İkinci Dünya Savaşı, Soğuk Savaş vd.) tümü Türkiye'yi yakından etkilemiştir. Küreselleşmenin beraberinde ulus devletlere karşı getirdiği tehdit ve riskler, etkisini ülkemizde derinden göstermiştir. Küreselleşmeye tepki olarak gelişen mikro etnik ve dini yapılanmalar ve bunların oluşturduğu güvenlik tehditleri, doksanlı yıllarda ülkenin güvenlik bunalımları yaşamasına neden olmuştur. Ülkenin önemli kaynakları terörle mücadeleye ayrılmak zorunda kalmıştır.

Küreselleşmenin yaygınlaşması ve Soğuk Savaş'ın bitmesi berberinde güvenlik tehditlerinin çeşitlenmesini getirmiştir. İleride ele alınacağı üzere askeri güvenlik sektörüne ek olarak ekonomi, çevre, toplumsal ve siyasi güvenlik sektörleri ortaya atılmıştır. Türkiye tüm bu sektörlerde yer alan tehditlerle mücadele etmek zorunda kalmıştır. Geçmişte olduğu gibi günümüzde de ülkemizin bağımsız politikalar üretmesini engellemek için tüm sektörlerde güvenlik saldırıları yaşanmakta ve bunlara karşı güvenlik tedbirlerinin alınması gerekliliği ortaya çıkmaktadır. Türkiye, karşılaştığı güvenlik problemlerini siyasal alandan güvenlikleştirme alanına çıkararak çözmek zorunda kalmaktadır. Siyasal alandan güvenlikleştirme alanına çıkış çalışmanın ilerleyen aşamasında detaylı bir şekilde ele alınacaktır. En özet tanımı ise olağan siyasal süreçlerle ortaya çıkan güvenlik

risklerinin, tehditleri ve krizlerinin olağanüstü tedbirler alınarak çözümlenmeye çalışılmasıdır.

Türkiye'de devletin güvenliği kavramı, 20. Yüzyılda batı ile olan müttefiklik ilişkilerinin gelişmesiyle beraber gelişim göstermiştir. Soğuk savaş döneminde batı dünyasında içeriği genişletilen güvenlik kavramı, öncellikle askeri çevrelerde kullanılmaya başlanmış, sonrasında ise kamu geneline genişlemiştir. Güvenlik kavramının ülkemizde gelişmesinde, 1961 Anayasası ile birlikte kurulan Milli Güvenlik Kurulu, önemli bir etken olarak karşımıza çıkmaktadır. Bu gelişme ile başlayan güvenlik kavramının genişleme süreci zaman içinde salt askeri bir güvenlik kavramını aşarak devlet yönetiminin tüm kademelerinde ve fonksiyon alanlarında kendine geniş bir yer bulmuş vaziyettedir. Günümüzdeki resmi güvenlik kavramsallaştırmasını milli güvenlik kurulu üzerinden ele alacak olursak Cumhurbaşkanlığı hükümet sistemine geçişten sonra kurumu tekrardan düzenleyen "6 sayılı Millî Güvenlik Kurulu Genel Sekreterliğinin Teşkilat Ve Görevleri Hakkında Cumhurbaşkanlığı Kararnamesinde" milli güvenlik kavramı; "Millî güvenlik: Devletin anayasal düzeninin, millî varlığının, bütünlüğünün, milletlerarası alanda siyasi, sosyal, kültürel ve ekonomik dâhil bütün menfaatlerinin ve ahdi hukukunun her türlü dış ve iç tehditlere karşı korunması ve kollanmasını*",* şeklinde ifade edilmiştir (15 Temmuz 2018 Tarihli ve 30479 Sayılı Resmî Gazete). Bu tanımlamada yer aldığı üzere resmi güvenlik anlayışı, askeri güvenlik kavramının dışına çıkarılarak sosyal, kültürel ve ekonomik alanlarda da güvenlik tehditlerinin varlığına dikkat çekilmiştir.

Cumhurbaşkanlığına bağlı bakanlıkların güvenliğe olan yaklaşımı ele alındığında güvenlik kavramının genişlemesine karşılık gelen bir misyon üstlenildiği görülmektedir. Cumhurbaşkanlığı hükümet sistemi ile birlikte Genelkurmay Başkanlığı ve kuvvet komutanlıklarının bağlandığı T.C. Milli Savunma Bakanlığı kendi misyonunu; "Türkiye Cumhuriyeti'nin bekası ve güvenliğini sağlamak üzere, Millî Savunma Stratejisi doğrultusunda; Millî niteliğini koruyarak hızlı gelişen bilgi ve teknoloji çağına uyum sağlayan, güvenlik ortamında meydana gelen değişimlere bağlı olarak ortaya çıkan ve coğrafi sınırlara bağlı olmayan belirsizlik,

risk ve tehditlerle mücadele edebilecek niteliklere haiz Türk Silahlı Kuvvetlerinin ihtiyaçlarını dinamik ve proaktif bir kurum olarak karşılamaktır (T.C. MSB Resmi Web Sitesi, 2020).” şeklinde tanımlayarak bilgi ve teknolojideki hızlı değişimin güvenlik kavramında yaratığı dönüşüme dikkat çekmektedir. Güvenlik tehdit ve risklerinin ise günümüzde coğrafyadan bağımsız bir şekilde ortaya çıktığı gerçeği öne çıkarılmıştır.

İç güvenlik alanından sorumlu bakanlık olan[6] T.C. İç İşleri Bakanlığı kendi misyonunu; “Temel hak ve hürriyetleri esas alarak; iç güvenlik, kıyı ve karasularının emniyetini sağlama, etkili sınır yönetimi ve güvenliği, göç politikaları oluşturma, kamu hizmetlerinin koordinasyonu ile etkin il ve ilçe yönetimini tesis etme, afetlere dirençli toplum oluşturma, nüfus ve vatandaşlık hizmetlerini sunma ve sivil toplumu destekleme görevlerini insan odaklı ifa etmek (T.C. İçişleri Bakanlı Resmi Web Sitesi, 2020)*”* olarak tanımlamaktadır. Görüldüğü üzere iç güvenliğin sağlanması dışında pek çok görevi bulunan T.C. İç İşleri Bakanlığı kendi vizyonunu güvenlik odaklı belirleyerek “Güvenli Türkiye” olarak tanımlamıştır. T.C. Dış İşleri Bakanlığı ve güvenlik kavramı ele alındığında bakanlığın güvenliğe olan yaklaşımını 2019-2023 Stratejik Planı üzerinden okumak mümkündür. İlgili planda yer alan dış çevre tehdit analizinde, Dış tehditler şu şekilde ifade edilmiştir:

- “Yakın coğrafyamızda çatışma bölgelerinin artması ve güvenlik tehdidinin yükselmesi,”
- “Bölgesel kırılganlıkların ve zayıf devletlerin artması,”
- “Özellikle Orta Doğu’da ulus devletlerin yapısına yönelik tehditler,”
- “Belli ülkelerin uluslararası gündemi tek başlarına değiştirebilme kapasitesi,”
- “Terörizmin uluslararası sistemi temelden etkileyen ortak bir tehdit haline gelmesi,”
- “Çatışma bölgelerindeki sivil nüfusun olumsuz etkilenmesi sonucunda oluşan göç dalgaları ve ülkemiz açısından mülteciler konusunun öncelikli gündem haline gelmesi, Batı ülkelerinde artan aşırı milliyetçi, korumacı, yabancılara yönelik ayrımcı ve ırkçı yaklaşım ve uygulamalar, bunların iktidarlar tarafından yürütülen dış politikaya etkisi ve ülkemize yönelik yansımaları,”
- “Uluslararası örgütlerin karar alma mekanizmalarının yavaş olması/işlememesi nedeniyle etkilerinin azalması,”
- “Özellikle gelişmiş ülkelerin liderlik ve vizyon göstermeyi sürdürmemesi,”
- “Mültecilere yönelik toplumsal bakışın sertleşmesi,”
- “Küreselleşme karşıtlığı,”

[6] İleride ele alınacağı üzere aynı zamanda ulusal kriz yönetimi faaliyetlerini koordinasyon makamıdır.

- “Tek taraflı tasarruflarla uluslararası hukukun, anlaşmaların ortadan kaldırılmasına ilişkin emsaller oluşması,”
- “Küresel ısınma, iklim değişikliği ve buna bağlı olarak su kaynaklarının azalması,”
- “Jeopolitik mücadelelerin yeniden ve farklı yöntemlerle ortaya çıkması şeklinde belirlenmiştir.”

Bu tehditler incelendiğinde, klasik tehdit anlayışı ve güvenlik kavramsallaştırmasından ayrışan, tehditleri çok geniş bir yelpazede ele alan bir yaklaşım öne çıkmaktadır. Göç, Küreselleşme karşıtlığı, küresel ısınma gibi yeni güvenlik sorunsallarına değinilmiştir. Bakanlık vizyonu da diğer bakanlıklarda olduğu gibi güvenlik odaklı olarak belirlenerek “Güvenli bir gelecek için köklü, güçlü, girişimci ve insani diplomasi yürütmek (T.C. Dışişleri Bakanlığı 2019-2023 Dönemi Stratejik Planı, 2019)” olarak belirlenmiştir. Siber güvenlik alanında yetkili bakanlık olan T.C. Ulaştırma Bakanlığı kendi vizyonunu “Güvenli ulaştırma, hızlı erişim sağlama (T.C. Ulaştırma Bakanlığı Resmi Web Sitesi, 2020)” olarak tanımlamaktadır.

Soğuk savaş döneminde askeri tehditler odaklı bir tehdit evreninden ekonomi, sağlık, çevre gibi pek çok alanda yeni tehditler boy göstermiş ve güvenlik kavramı tehdit-tedbir dengesi doğrultusunda dönüşüme uğramıştır. Güvenliğin bu dönüşümü Türk kamu kurumlarını da etkilemiş ve TSK haricindeki kamu kurumları da güvenlik olgusu ile yakından ilgilenmeye başlamıştır. Yukarıda yer alan bulgular analiz edildiğinde günümüz Türkiye’sinde resmi güvenlik kavramsallaştırması, tehdit evreninin genişlemesi doğrultusunda hareket ederek genişlemiştir.

Güvenlik alanındaki genişlemeden kritik altyapı güvenliği meseleleri de etkilenmiş ve giderek artan bir öneme sahip olmuşlardır. Geçmiş dönemde yaşanan savaşlar ele alındığında birinci ve ikinci dünya savaşı ve sonrasında yaşanan savaşlarda ilk stratejik hedef olarak kritik altyapılar seçilmiştir. Silahlı saldırı ve stratejik bombardımanların ilk hedefleri bu altyapılar olmuştur. Günümüzde ise toplumun kritik altyapılara olan bağımlılığı üst seviyelere yükselmiştir. Enerji, finans, elektronik haberleşme gibi altyapılardaki krizler tüm toplumu derinden etkileyecek seviyeye ulaşmıştır. Siber güvenlik krizleri pek çok kritik altyapıyı

etkileyebilecek bir niteliğe bürünmüştür. Türkiye'deki siber güvenlik kavramsallaştırması da genel güvenlik kavramsallaştırmasına göre gelişerek kritik altyapı güvenliği üzerinden ele alınmıştır.

3.2 GÜVENLİKLEŞTİRME ve SİBER GÜVENLİK

3.2.1 Kopenhag Okulu ve Güvenlikleştirme

Güvenlik alanındaki çalışmalar, seksenli yıllara kadar realist teori tarafından çerçevelenmiştir. Realist teorinin merkezinde devletin güvenliği bulunmaktadır. Çıkış noktası ise İkinci Dünya Savaşı öncesi dönemdeki çalışmaların bu savaşı önleyememiş olmasıdır. Bu teoriye göre güvenliğe yönelik en büyük tehdit devletler üzerinden gelen tehditlerdir. Ancak bu yaklaşım soğuk savaşın sona ermesiyle birlikte sarsılmaya başlamıştır. Bunun en temel sebebi ise tehdit evreninin değişime uğraması sonucu devlet dışı aktörlerin tehdit unsuru olarak ortaya çıkması ve bunun yanında birey ve toplumu tehdit eden yeni güvenlik risklerinin belirmesidir ("The New World Order": An Outline of the Post-Cold War Era, 2008, s. 48) denebilir.

Realizme karşı çıkan yaklaşımların temel savı; güvenlik çalışmalarının devletin güvenliği kavramının yanı sıra toplum, grup ve birey güvenliği kavramlarına yer verilmesini, aynı zamanda askeri tehditlerin yanı sıra sosyal, çevresel ve insani alanda yaşanan sorunların ve tehditlerin göz önünde bulundurulması gerekliliğidir. Bu durum da beraberinde, güvenliği sağlayan aktörlere yeni aktörlerin eklenmesini getirmektedir. Devlet aktörünün dışında uluslararası kuruluşlar, sivil toplum kuruluşları gibi aktörlerde güvenlik sağlayıcısı sorumluluğunu üstlenmişlerdir. Realist okula karşı çıkışın başladığı bu dönemde ortaya çıkan "Kopenhag Okulu Ekolü" geleneksel güvenlik çalışmalarına karşı çıkarak güvenlik kavramını politik, askeri, toplumsal, ekonomik ve çevresel beş boyutta ele almıştır. Buna ilaveten sadece devlet odaklı bir çözümlemeye karşı

çıkmış uluslararası, bölgesel, ulusal, grup ve birey analiz düzeylerini gözeten bir güvenlik çözümlemesi önermişlerdir. Okul, güvenlik tanımlamasında dar kalıplarının dışına çıkılması ve geniş bir güvenlik tanımlamasının yapılmasından yanadır:

> [Geniş anlamda] güvenlik kavramı, bireylerin, sosyal grupların, ulusların ve insanoğlunun varlığı, refahı ve kalkınmasına yönelik her türlü tehdide karşı alınan önlemlerle özdeştir. Askeri tehditler, ekolojik tehditler, salgın hastalıklar ve zihinsel tehditler ötesinde bir tehdit türüdür. Açlık, yetersiz beslenme, suç, terörizm, sivil çatışma ve mücadele, kirlilik, trafik ve nükleer reaktör kazaları, hastalıklar, işsizlik, az gelişmişlik, geri kalmışlık, enerji ve diğer ekonomik kaynakların arzının tükenmesi, dini ve etnik zulüm, vb. tehditler de eklenebilir. Bu geniş anlamda, Avrupa güvenliği Avrupa'nın sosyal düzeni ve bireysel olarak Avrupalıların varlığına yönelik tehditlerin azaltılması çabasına işaret eder. Güvenlik, insan yaşamının hemen her boyutunu kapsayacak şekilde, sosyal veya insan güvenliği olarak anlaşılır (Buzan, The European Security Order Recast: Scenarios for the Post-Cold War Era, 1990, s. 4).

Kopenhag ekolünün güvenlik alanına getirdiği bir diğer öneri ise güvenlikleştirme modelidir. Kamusal alanda var olan sorunlar siyasallaşmamış, siyasallaşmış ve güvenlikleştirilmiş olmak üzere üç farklı şekilde kategorize edilebilir. Siyasetin konusu olmayan sorunlar devlet otoritesi tarafından ilgilenilmeyen kamusal alanda işlenmeyen sorunlardır, siyasallaşmış sorunlar ise devlet otoritesi tarafından ele alınan, karar alıcı organlar tarafından ele alınması gereken sorunlardır. Güvenlik sorunları ise acil önlemler gerektiren siyasetin olağanlığı dışında uygulamaları gerekli kılan tehdidin hayat verdiği sorunlardır. Siyasal bir sorun, eğer devlet otoritesi tarafından ele alınıp güvenlik sorunu olarak ele alınırsa bu sorun artık güvenlikleştirilmiş olmaktadır. Siyasal sorunla güvenlik sorunu ayrışımın en temel etkeni güvenlik sorununun olağan dışı önlemlere sebebiyet vermesidir. Bu ayrıma gidilmeden devletin tüm kaynaklarının güvenlik sorunlarına adanması bir yönetim krizine neden olacaktır.

3.2.1.1 Güvenlik Analiz Seviyeleri

Güvenlik analizinin hangi seviyelerde yapılacağı Kopenhag Okulu öncesi dönemde başlamış olan bir tartışmadır. Güvenlik için hangi nesnelerin referans gösterileceği (bireylere karşı devletler) ya da savaşın nedenlerine yönelik (sistem

yapısına karşı, devletlerin doğasına karşı ya da insan doğasına karşı) tartışmalar mevcut olmuştur. Güvenlik seviyeleri kendi içerisinde açıklama kaynakları olmaktan ziyade olayların nerede gerçekleştiğine dair basitçe ontolojik referanslardır. Bunlar sırasıyla;

- Küresel/Gezegensel
- Uluslararası/Bölgesel
- Ulusal/Birim
- Topluluk/Altbirim
- İnsan, olarak tespit edilmiştir (Buzan, Security: A New Framework for Analysis, 1997, s. 6) .

Küresel analiz seviyesi tüm gezegeni kapsayan üstünde bir sistem/organizasyon bulunmayan bir seviyeyi işaret etmektedir. Geçmişte küresel anamda birbiriyle etkileşimsiz ve bağımsız sistemlerin varlığından söz edilse bile günümüzün dünyasında tek bir küresel sistem var olmakta bu anlamda bu analiz seviyesi tüm gezegene karşılık gelmektedir. Bölgesel analiz seviyesi küresel sistemin içerisinde belirli bir bölgede var olan uluslararası organizasyonlar olabileceği gibi, bileşenlerinin coğrafi tanımlamalardan uzak belli bir ilişki nedeniyle bir araya gelen uluslararası organizasyonlar da olabilir. Ulusal/Birim analiz seviyesi genellikle ulus devlet seviyesini işaret etmektedir. Ayrıca bu analiz seviyesi küresel şirketleri de kapsamaktadır. Topluluk/Altbirim analiz seviyesi bir üst analiz seviyesi olan Ulusal/Birim kategorisinde yer alan ulus devlet, küresel şirket gibi oluşumları etki altına alabilecek organize olmuş oluşumları belirtmektedir. Bu kavrama örnek olarak lobiler gösterilebilir. İnsan/birey seviyesi ise en alt seviye analiz birim olarak belirlenmiştir.

Okulun öncülerinden olan Buzan'a göre teoriler kendilerini belirli bir analiz seviyesine indirgemişlerdir (Buzan, 1997, p. 6). Alana o güne kadar hakim olan realist teorinin ulusal analiz seviyesinde hareket ettiğini eleştirirken, en az konu edilen alanın insan/birey olduğu konusu eleştirmektedir. Ortaya koydukları

genişletilmiş güvenlik kavramı, analizi ile birlikte tüm seviyelerde analiz yapılmaktadır.

3.2.1.2 Güvenlik Sektörleri

Okul güvenlik tanımlamasının genişletilmesini savunurken bu genişlemenin sınırları olduğunu belirterek sınırsız bir güvenlik genişlemesi tanımlamasından sakınmaktadır. Bu durum okulun aslında realist teoriden tamamen farklı bir çizgi de hareket etmediğinin göstergesidir. Askeri nitelik taşımasa bile güvenlik sorunlarının askeri konulara dönüşebileceğini ve bu durumun bir güvenlik sorunu haline gelebileceğini belirterek realist çizgiye yaklaşmıştır (Buzan, 1990, p. 6). Okul askeri güvenlik sektörünü, devletlerin silahlı kuvvetinin savunma ve saldırı yeteneği ve birbirleriyle olan karşılıklı etki-tepki dengesinin değerlendirilmesi olarak tanımlamaktadır. Siyasi güvenlik ise devlet örgütünün istikrarı, hükümet sistemi ve meşruiyet kaynakları ve temel ideolojisine ilişkin analizleri içermektedir. Ekonomik güvenlik; devletin halkın refah seviyesini olumlu seviyede tutmasına yönelik gerekli kaynak, pazar ve finansmana sahip olması ile ilgilidir. Toplumsal güvenlik insanların kültür, dil, kimlik ile kabul edilebilir seviyede geleneklerin sürdürülebilmesine ilişkindir (Buzan, 1997, p. 7). Çevre güvenliği ise dünya ve gezegeni yaşanabilir kılınmasına yöneliktir.

Analiz düzeyleri ve güvenlik sektörleri arasındaki ilişki Şekil-7'de sunulmuştur. Askeri ve siyasi sektörler ulusal düzeyde ele alınırken, ekonomik, çevresel ve toplumsal sorunların küresel seviyeye kadar ulaşabildiği değerlendirilmiştir. İnsan analiz seviyesinin ekonomik, çevresel ve toplumsal sektörlerle etkileşim içerisinde olduğu, sosyal, enerji, gıda sağlık alanlarındaki tehditlerin ve diğer çatışma alanlarının birey seviyesinde güvenlik sorunlarına neden olduğu belirlenmiştir. Rekabetin hakim olduğu küresel sistemde ulusal güvenlik kavramı askeri ve siyasi sektörleri etkisi altına almaktadır. Çalışmanın ilerleyen bölümlerinde detaylı olarak ele alınacağı üzere yeni gerçekleştirilen çalışmalarda askeri ve siyasi güvenlik sektörlerine siber güvenlik sektörü eklemlenmiştir.

(Hansen and Nissenbaum, 2009) Siber güvenlik sektörü de da askeri ve siyasi sektör gibi ulusal güvenlik kavramları içerisinde değerlendirilmiştir.

Şekil-7: Güvenlik Analiz Seviyeleri ve Sektörleri Arasındaki İlişki

<table>
<tr><td>Güvenlik Boyutu ⇒
Etkileşim Düzeyi ⇓
(gösterilenler)</td><td>Askeri</td><td>Siyasi</td><td>Ekonomik</td><td>Çevresel
↓</td><td>Toplumsal</td></tr>
<tr><td>İnsan
→</td><td></td><td></td><td colspan="3">Sosyal, enerji, gıda, sağlık, geçim yollarına yönelik tehditler, çatışma alanları ve riskler, yüksek hassasiyet içeren alanlarda bir beka ikilemi ortaya koyabilir</td></tr>
<tr><td>Köy/Topluluk/Toplum</td><td></td><td></td><td></td><td>↓ ↑</td><td></td></tr>
<tr><td>Ulusal</td><td colspan="2">“Rekabet halindeki devletlerin güvenlik ikilemi” (Ulusal Güvenlik Kavramı)</td><td colspan="3">Tüm analiz ve etkileşim düzeylerini bir araya getiren “enerji, gıda, sağlık ve geçim yolları, vs güvenliğini sağlamak” (İnsan Güvenliği Kavramı)</td></tr>
<tr><td>Uluslararası/Bölgesel</td><td></td><td></td><td rowspan="2"></td><td rowspan="2">↓ ↑</td><td rowspan="2"></td></tr>
<tr><td>Küresel/Gezegensel</td><td>→</td><td></td></tr>
</table>

Kaynak: (Brauch, 2008, s. 8)

3.2.2 Güvenlikleştirme Kavramı ve Siyaset Teorisi

Güvenlikleştirme kavramını geliştirenler bu kavramın temeline siyasal kavramını yerleştirmişlerdir. Bu kavramsallaştırma esnasında bir sorunu güvenlikleştirme konusu haline getirmek için kullanılan tehdit olgusu, Carl Schmitt’in dost düşman ayrımı üzerinden gerçekleştirilen siyasal ilişkinin gerçekleşmesi düşüncesi temelli geliştirilmiştir. Schmitt’e göre herhangi bir dinsel, ahlaki, ekonomik, etnik veya başka bir karşıtlık, insanları dost ve düşman olarak ayırmaya muktedir ise bu karşıtlıklar siyasal bir karşıtlığa denk düşer. Schmitt için karşıtın ahlaken kötü olması bir kıstas değildir, her iyi dost ve her kötü düşman olarak tanımlanmamalıdır, önemli olan yabancılaşma diğer anlamıyla siyasal olarak karşıtlık halidir. Bir kere siyasal karşıtlık belirdiğinde bununla mücadele edilmelidir. Düşman bu nokta da ötekileştirilmektedir. Siyasal bir birlik olan devlet

ise öteki ile mücadele etmek zorundadır. Güvenlikleştirme sürecinde siyasal olarak öteki yada yabancı olanın yerini tehdit kavramı almaktadır (Açıkmeşe, 2011, s. 63). Tehditlerin algılanma biçimi doğrultusunda siyasal olarak ötekileştirilene karşı güvenlik kavramları gündeme alınmaktadır.

Güvenlikleştirme esnasında, bir aktörün kendi mevcudiyetine karşı kasti bir tehdidi öne sürüp bu tehdidi önlemek için olağanüstü tedbirler almasını onaylayan anlayışta Schmitt'in siyasal ve egemenlik kavramlarına olan yaklaşımının izleri görülmektedir. Schmitt'in egemenlik anlayışında egemenlik baskı ya da hakimiyet tekel değildir. Egemenlik bir karar alma tekelidir. Egemen istisnai durumlarda karar veren konumundadır. Egemen siyasi düzene yönelik tehditlere ne zaman tedbir alınacağına karar vericidir. (Huysmans, 2006, s. 134) Tedbir alma aşamasında normal düzenin nasıl askıya alınacağını egemen belirlemektedir. Bu noktada OHAL kararları örnek gösterilebilir. Egemen, güvenliği yeniden tesis için birey adına onun özgürlükleri kısıtlayıcı tedbirler alma özgürlüğüne sahiptir. Egemenin bu özgürlüğü güvenlikleştirmede karşımıza güvenlikleştirmeye yetkili aktörün aldığı olağanüstü tedbirlere, kitlenin uymasını beklemesi olarak çıkmaktadır. Bu anlamda güvenlikleştirme tıpkı Schmitt'e olduğu gibi istisnai politikaların uygulanmasıdır.

Schmitt'in bu belirgin etkisine rağmen tam anlamıyla güvenlikleştirme kavramını domine ettiği söylenmez. Güvenlikleştirmede Schmitt'in aksine dinleyicinin rolü karar verici aktör kadar yetkinidir. Eğer karar verici aktörün kararları dinleyici tarafından gerçekleştirilirse güvenlikleştirme kavramından söz edilebilir. Güvenlikleştirmenin kendi özgü bir siyasal edinim olarak ortaya çıkmasında Alman düşünür Arendt'in etkisi büyüktür. Okul düşünürleri bu durumu (Buzan, 1997, p. 142-143) eserlerinde satır aralarında belirtmektedir.

Arendt siyasal kavramını doğumluluk, anımsama, hergünkülük, umut, şiddetsizlik gibi argümanlara göre açıklar. O'nun için gerçek siyasal eylem, bahse konu argümanlar doğrultusunda tekçi iradeyi reddetmeye, çoğulcu karaktere ve deneyime açık olma durumudur. Bu kapsamda Arendt için siyaset Schmitt'in

aksine egemen aktörün tekelinde değildir, siyaset karşılıklı birlikteliğe, çoğulculuğa dayalıdır. Onun için çoğulcu olmayan siyaset dışıdır. Swift'in aktardığına göre Arendt, Yunan "Polis" düzeninin çoğulcu politik düzenine çokça gönderme yapar (Swift, 2009, s. 32-36). Siyaset herkesin söz hakkı olduğu bir Polis'te bireylerin tekil sözleri değil toplumun ortak ürettiği bir konuşmadır.

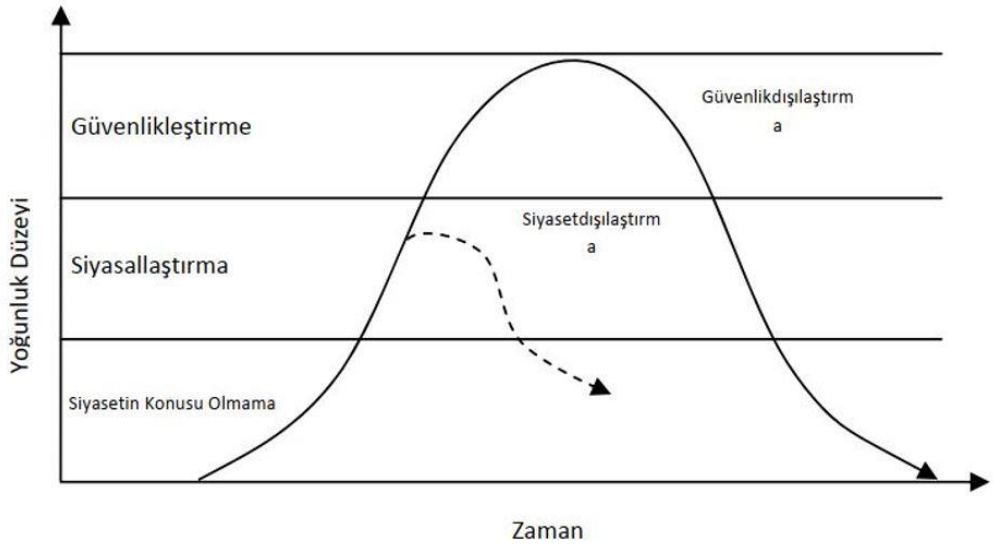
Okul tek egemen üzerinden hareketle güvenlikleştirme kavramına yaklaşmamaktadır. Güvenlikleştirme eylemi sadece devlet düzeyinde yapılmamakta başka düzeylerde de gerçekleştirilmektedir. Burada önemli olan tehdidin varlığının ortaya konmasıdır. Okul tehdidin varlığının ortaya konması sürecini sözdizimsel edinimle açıklar. Sözdizimsel edinim ise topluğun ortak konuşmasından hareketle elde edilir. Eğer sözdizimsel olarak bir mesele güvenlik tehdidi olarak ortaya konuyorsa bu mesele siyasalın dışına çıkarak güvenlik alanına girmiş olmaktadır. Güvenlikleştirme çalışmasıyla başarılı güvenlikleştirme ise aynı anlamda değildirler. Başarılı bir güvenlikleştirme için, meseleyi siyasalın dışına çıkarıp olağanüstü kararlar almayı meşru kılmak için, güvenlikleştirici aktör ve diğer kitle, ortak bir kararda buluşmalıdır. Güvenlikleştirme sürecinde güvenlikleştirici aktör tek başına etken değildir bu durum okul tarafından Arendt'in siyasal kavramına atıfla siyasalın birliktelik ve çoğulculuk üzerinden gerçekleşmesine uyumlandırılmaktadır (Buzan, 1997, p. 25).

Okul, güvenlikleştirme sürecindeki kavramların muğlaklığının farkındadır. Bunu gidermek için bazı kavramlara daha fazla açıklık kazandırmak için çeşitli tanımlamalar zaman içinde yapılmıştır. Kitle onay alınması gereken bir makamdır, kimi durumlarda toplum ya da gruptan öte, kitle onayı durumu resmileştiren bir grup olarak ortaya çıkar. Örneğin, ülkeler güvenliğe ilişkin askeri hareketlerde bulunurken çoğunlukla BM Güvenlik Kurulu onayını gerekli görmezler ancak hükümet kendi meclisinin onayını almak zorundadır. Bu noktada güvenlikleştirici aktör hükümet, onaylayıcı dinleyici kitle meclistir (Balzacq, 2010, p. 9). Güvenliğin kendine özgü siyah güvenlik alanlarının olabileceği ön kabulü de mevcuttur. Gelişmiş demokrasilerde askeri kurum ve istihbarat örgütleri

siyasal olanın dışındadır. Ancak güvenliğin kendine özgü kamuoyundan gizli kalması gereken, onaylayıcı kitle, siyah alanının mevcudiyeti nedeniyle bu siyah alanda güvenlikleştirme karar verici aktör tarafından onay süreci olmaksızın gerçekleştirilir (Buzan, 1997, p. 24). Okul bu noktalarda Arendt'in siyasal düşüncesinden uzaklaşarak Schmitt'in çizgisine yaklaşır. Bu kapsamda okulun siyasal olana yaklaşımının Arendt-Schmitt arasında kaldığından söz edilebilir.

Okul için güvenlikleştirilmiş sorunlar siyasal alana dönmeden önce uzun süre güvenlik alanında kalabilir. Güvenliğe ilişkin sorunlar kendiliğinden güvenlik tehdidi olarak algılanmazlar. Ancak aktörler tarafından güvenlikleştirildiğinde güvenlik konusu olurlar. Güvenlik siyasetini oluşturma da bu noktada siyasal bir harekettir. Sorun zamanla güvenlik dışından siyasal alana ve siyasetin konusu olmama durumuna evrilebilir (Miş, 2014, s. 355). Sorunun yoğunluk ve güvenliğe etki düzeyi burada etkinidir. Bu durum aşağıda Şekil-8'de sunulmuştur.

Şekil-8: Sorunların Güvenlikleştirme Süreci



Kaynak: (Miş, 2014, s. 347)

Okul, söylemin güvenlikleştirme için analizi kavramını ele alırken Derridda'nın asıl olan metindir önermesinden hareketle kendine söylem analiz kaynağı olarak egemen aktörün metinlerini esas alınmaktadır. Okul için esas kaynak metin kamu

metinleridir. Bu metinler analiz edilirken egemenin gizli niyet ve maksatları göz önünde bulundurulmaz bu durumlar güvenlikleştirmenin dışında yer alan konulardır, güvenlikleştirme bunlarla ilgilenmez (Buzan, 1997, p. 22). Okul bu noktada realist teoriden ayrışır. Realist teori, metin dışı kavramlarla yola çıkarak tehdidi belirlerken, güvenlikleştirme için sadece metin geçerlidir. Güvenlikleştirme teorisi bu nokta da realist teoriyi analizcilerin karar verici aktör yerine karar vererek tehditleri ve tedbirleri belirlemekle itham eder. Oysaki analizcinin görevi objektif tehditleri belirlemek değil, tehdidin inşa sürecini incelemektir. Bunun içinde esas olanın söylemin (metin) incelenmesi olduğu belirtilmektedir (Buzan, 1997, s. 204).

Okul, objektif tehditleri tümden görmezden gelmez. Sınırdaki tanklar, kirlenmiş nehirler genel kabul görmüş objektif tehditler olup, güvenlikleştirici aktör güvenlikleştirme sürecinde bu objektif tehditleri, kolaylaştırıcı etken olarak kullanabilir. Okul, kolaylaştırıcı etkenlerin varlığını ve güvenlikleştirmeye olan etkisini kabul eder (Buzan, 1997, p. 204). Metin dışı kavramları, verili kabulleri reddeden Derrida çizgisinden bu nokta da ayırılır. Bu nokta, realist teoriye kısmi bir yakınlaşma mevcuttur.

Sonuç olarak Kopenhag Okulu, güvenlik çalışması kavramını realist teorinin dar çerçevesinden uzaklaştırmış ancak, bütünü kapsayan, geniş bir güvenlik yelpazesi sunmaktan kaçınmıştır. Siyaset teorisinin sınırları dahilinde, güveliğin öz anlamını değiştirmeden söylemle inşa edilen güvenliğin inşa edilen sınırları içerisinde kalmıştır. Bu noktada yeni bir yol olarak ortaya çıkan Kopenhag Ekolü belli sınırlar içinde kalmış, realist teoriden tamamen uzaklaşmamıştır. Okul güvenlik aktörleri, tehditleri ve siyaseti anlamında realist teoriye benzer çıkarımlarda bulunmuştur.

3.2.3 Siber Güvenlikleştirme

Güvenlikleştirme teorisinin başlangıç evresinde beş güvenlik sektörü öne sürülmüştür. Bunlar; askeri, siyasi, toplumsal, ekonomik ve çevre sektörleridir.

Günümüzde tüm bu sektörler siber alanla doğrudan bağlantılıdır. Bu alanda yaşanan gelişmeler ve bu gelişmelerle beraber artan güvenlik tehditleri, varlığını tüm sektörlerde hissettirmektedir. Günümüzde harp araç ve gereçleri bilgisayar ağları üzerinden yönetilmekte, fiziki para akışı giderek yerini bilgisayar ağları üzerinde gerçekleştirilen para transferine bırakmış durumdadır. Siyasiler kitlelere sosyal medya üzerinden erişmekte, mitingler, televizyon tartışmaları yerini, Twitter üzerinden yollanan mesajlara bırakmaktadır. Önemli siyasi bir figürün sosyal medya hesabının ele geçirilmesi yeni güvenlik sorunu olarak karşımıza çıkmaktadır. Aynı zamanda askeri bilgi sistemleri yeni askeri alanda yeni bir saldırı alanı olarak belirmiştir. NATO 2014 yılında siber alanı, harbin beşinci boyutu olarak belirlemiştir (Wales Summit Declaration, 2014). Dünya üzerinde kaydedilen en büyük konvansiyonel patlamalar arasında yer alan 1982 Sibirya Petrol Boru Hattı patlamasının arka planında ABD'nin siber saldırısının mevcudiyeti şüphesi hiçbir zaman giderilememiştir (Hoffman, 2004). Bu saldırının beraberinde getirdiği çevre felaketi siber alanın, siber güvenliğin çevre sektörüne etkilerinin günümüzde başlayan bir sorun olmaktan ziyade siber alanın varlığının ortaya çıkmasından itibaren süre gelen bir ilişki olduğunun göstergesidir. Siber alanın bu yeni durumu, siber güvenlik kavramının güvenlikleştirme teorisinin çalışma alanına sokmaktadır. Siber güvenlikleştirme kavramını daha iyi anlayabilmek için siber uzay, siber güvenlik kavramlarını detaylı olarak ele almak, tarafımızca bütünsellik açısından gerekli görülmüştür.

3.2.3.1 Siber Uzay Kavramı

Günümüzde siber uzay kavramı, sadece bilgi teknolojilerini içermemektedir. İnsanların da artık bir parçası olduğu siber alan, kendi yarattığı ya da yine insanlar tarafından arka planda yaratılan siber kültür öğeleriyle birlikte fiziksel olarak yaşadığımız gerçek zaman ve mekanla tümleşik ve onunla etkileşimli bir kavrama dönüşmüştür. Günümüzdeki siber alan kavramını incelemek için zaman içindeki dönüşümünü ele alarak başlamak geleceğe ilişkin tespitlerimiz için kavramsal alt yapıyı sağlayacaktır.

Bilgisayarların gelişimi, mekanik tablolardan başlamış, günümüzde ise ağlarla birbirine bağlanmış dijital makinelere dönüşmüştür. Bilgisayarların gelişimini sağlayan en temel etkenlerin başında karmaşık güvenlik sorunlarının/problemlerinin bilgisayarlar yardımıyla çözümlenmesi düşüncesi gelmiştir. Birleşik Devletler ve Birleşik Krallık hükümetleri, İkinci Dünya Savaşı sırasında uçaksavar savunmasını ve kod kırmayı iyileştirmek için bilgisayarlarla ilgili erken araştırmalarını finanse etmiştir. İkinci Dünya Savaşı'nın ardından, ABD Savunma Bakanlığı, ABD'nin yeteneklerini ve gücünü artırmak için bilgisayar ve bilgisayar ağlarının geliştirilmesine yönelik erken araştırmaların çoğuna sponsor olmuştur. Devlet tarafından sağlanan finansman akışı, hükümet, akademi ve endüstrideki bilim insanlarının, kaynakları ve bilgileri paylaşmak için ortak bir araç olarak bilgisayar vasıtasıyla bilgi paylaşım ağı oluşturmaları ile ortaya çıkan ilk bilgisayar ağı, zamanla tüm dünyaya yayılarak bugün internet olarak adlandırdığımız küresel bir bilgisayar ağına dönüşmüştür (Banks, 2008, p. 5). Bu gelişme ise beraberinde, bilgisayar ağları üzerinde yaşanan etkileşimden doğan siber alan kavramını getirmiştir.

Siber uzay, günümüzün en popüler kavramları arasında yer almaktadır. Siber kelimesi sibernetik kökeninden gelmektedir ve yönetici anlamında kullanılan Yunanca “kybernetes”e kadar indirgenmektedir. Sibernetik kavramı ilk defa 1948 yılında Norbert Weiner tarafından hayvanlar ve makinelerde kontrol ve iletişim anlamında kullanılmıştır. Weiner makinelerle sağlanan otomasyonun gelecekteki olası faydalarını olumlu anlamda yorumlarken otomasyon sürecinin yoldan çıkarak makinaların insanları kontrol edebileceği bir geleceği öngörmüştür (Wiener, 1950, s. 23-25). Siber alan kavramı ise ilk kez William Gibson tarafından 1984 yılında yayımlanan “Neuromancer” romanında kullanılmıştır. Gibson için siber alan, yüzbinlerce bilgisayar teknisyenin iletişim halinde olduğu, bilgisayarlar ağları üzerinde gerçekleşen sanal bir dünyadır.

Gibson tarafından siber kelimesinin siber uzayı tanımlamak üzere kullanılmasının üzerinden geçen 35 yıl içerisinde siber uzay kavramı bilgisayar, bilgisayar ağları

ve bilgisayar kullanıcıları kavramlarını aşarak uluslararası bir fenomen haline gelmiştir. Siber ön eki kültür, savaş, terör, çatışma, güvenlik gibi pek çok kavramın siber alandaki izdüşümü olarak kullanılmasını sağlamıştır. Siber uzay bu süreçte teknik tanımlamalarının çok ötesine geçerek yeni bir yaşam alanı olarak karşımıza çıkmıştır.

Siber alanın zaman içindeki dönüşümünden günümüzdeki tanımlamasına dönecek olursak ABD Savunma Bakanlığı Siber Alan Operasyonları adlı yönergesinde siber alanı; birbiriyle bağlantılı üç farklı katmana ayırarak şu şekilde tanımlamıştır:

> “Siber uzay, birçok farklı ve çoğu zaman örtüşen ağların yanı sıra bu ağlardaki düğümlerden (İnternet protokol adresi veya başka bir benzer tanımlayıcıya sahip herhangi bir cihaz veya mantıksal konum) ve bunları destekleyen sistem verilerinden (yönlendirme tabloları gibi) oluşur. Siber uzay, üç katman olarak tanımlanabilir: fiziksel ağ, mantıksal ağ ve siber uzay-insan etkileşim katmanı. Siber uzayın fiziksel ağ katmanı, coğrafi bileşen ve fiziksel ağ bileşenlerinden oluşur. Verinin hareket ettiği ortamdır. Mantıksal ağ katmanı, fiziksel ağdan soyutlanmış bir şekilde birbiriyle ilişkili olan ağ öğelerinden oluşur, yani form veya ilişkiler, bireysel, belirli bir yol veya düğüme bağlı değildir. Basit bir örnek, tüm içeriğin tek bir tek tip kaynak konumlandırıcı aracılığıyla erişilebildiği birden çok fiziksel konumdaki sunucularda barındırılan herhangi bir Web sitesidir. Siber uzay-insan etkileşim katmanı, siber uzaydaki mantıksal ağın daha yüksek bir soyutlamasını temsil eder; siber uzayda bir birey veya varlık kimliğinin dijital bir temsilini geliştirmek için mantıksal ağ katmanında geçerli olan kuralları kullanır. Siber uzay-insan etkileşim katmanı, aslında ağdaki insanlardan oluşur (Puyvelde, 2020, p. 44) .”

Fiziksel katman, bilgisayar ağlarını oluşturan cihazlardan oluşurken, mantıksal ağ bilgisayarların birbiriyle iletişim kurmasını sağlayan ağ topolojisinin işlerlik kazandıran ağ yönetim ilişkileridir. Siber uzay-insan etkileşim katmanı ise ağda iletişim halinde olan insanlardan oluşmaktadır.

Ülkemizin resmi olarak siber uzay tanımlaması "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023)’’nda şu şekilde yer almıştır: “Siber uzay: Doğrudan ya da dolaylı olarak internete, elektronik haberleşme ve bilgisayar ağlarına bağlı olan tüm sistem ve hizmetlerdir.” Siber uzay kavramına, internet ağı dışında bağımsız sistemlerde var olan bilgi sistemleri de dahil edilerek derin ve karanlık internet ortamlarının da bu kavrama dahil edildiğini görmekteyiz. Ancak daha önce ele alınmış olan siber uzay-insan etkileşim katmanının siber uzay

kavramına dahil edilmediği görülmektedir. Bu tanımlama tesadüfi bir durum olmayıp ülkemizdeki siber güvenlik algısı üzerinden etkilenmektedir. Siber güvenlik kavramı, adı geçen stratejide bilgi sistemleri tabanlı bir tanımlamaya sahiptir. Siber güvenlik kavramı ülkemizde resmi olarak bu tanımlamalar çerçevesinde gelişmiş ve ele alınmıştır. Ancak günümüzdeki siber uzay ve insan etkileşimini göz önüne aldığımızda kapsamlı bir siber güvenlik kavramının siber uzayın insan boyutunu da ele alması gerektiği ortaya çıkmaktadır.

3.2.3.2 Siber Güvenlik Kavramı

Siber güvenlik, tanımlaması oldukça değişken, genellikle öznel ve bazen de bilgilendirici olmayan, yaygın olarak kullanılan bir kavramdır. Siber güvenliğin çok boyutluluğunu yakalayan özlü, geniş ölçüde kabul edilebilir bir tanımının zorluğu, siber güvenliğin ağırlıklı olarak teknik yönünü güçlendirirken aynı zamanda teknolojik siber güvenlik zorluklarını çözmek için birlikte hareket etmesi gereken disiplinleri ayırarak bu alandaki teknolojik ve bilimsel ilerlemeleri de engellemektedir. Siber güvenlikle ilgili çalışmalar; bilgisayar bilimi, mühendislik, siyasal çalışmalar, psikoloji, güvenlik çalışmaları, yönetim, eğitim ve sosyoloji gibi çok çeşitli akademik disiplinleri de içeren geniş bir kaynak yelpazesine yayılmıştır.

Siber güvenlik alanında birbirine bağlı çok sayıda söylem bulunmaktadır. Siber güvenlik kavramının yeniden yapılandırılması, tartışmanın hem "siber" hem de "güvenlik" alanlarında konumlandırılmasına yardımcı olacaktır. “Siber” ön eki daha önce ortaya çıkışı ve tanımlanması gerçekleştirilen siber uzayı, ilgili terimlerle birleştirmektedir. Güvenlik kavramının dönüşümü ve yeniden inşa edilmesine ilişkin bulgular, daha önceki değerlendirmelerde ele alınmıştır. Güvenlik kavramının yeni tanımlamasının önüne siber alanı temsilen siber ön eki getirilerek her iki alandaki yenilik ve sorunları birleştiren bir terim olan siber güvenlik kavramı ortaya çıkarılmıştır.

Siber güvenlik kavramının tanımlanması için güvenlikleştirme olgusundan yola çıktığımızda ortaya konan kavramın; referans nesneyle etkileşimli olan aktörlerin ortaya koymaya çalıştıkları yapı; bu yapıya yönelik amaçları ve eylemleri ile birlikte tehdit algısını çerçeveleyen bir kapsama sahip olması gerekliliğini ortaya çıkarmaktadır. Ulusal Siber Güvenlik Stratejisi 2020-2023'te yer alan resmi siber güvenlik tanımlaması,[7] öngördüğümüz tanımlamanın karşılığını sağlayamamaktadır. Siber uzayın insan boyutunu (siber uzay-insan etkileşim katmanı) yadsıyan bir tanımlama olması nedeniyle bu katmanda gerçekleştirilen faaliyetleri kapsayan bir güvenlik tanımlaması olamamaktadır.

Yeni bir siber güvenlik tanımlamasını ortaya çıkarmak araştırmanın kapsamında değildir. Teorik çerçeveye uygun bir tanımlama için gerçekleştirilen literatür taraması neticesinde Craigen ve arkadaşlarının (Dan Craigen, 2014) siber uzay insan etkileşim katmanı faaliyetlerini kapsayan, multidisipliner yeni bir siber güvenlik tanımlamasını ortaya koydukları çalışmanın ürünü olan siber güvenlik tanımlaması, çalışmamız için referans tanımlama olarak belirlenmiştir.

İlgili çalışmada yer alan siber güvenliğe ilişkin mevcut kavramsal kategoriler ve tanımlama süreçleri Ek-2'de sunulmuştur. Craig ve arkadaşları siber güvenlik kavramını sınırlandırmalardan uzak tutarak mülkiyet hakları tabanlı bir tanımlama yapmışlardır:

"Siber güvenlik, siber uzay ve siber uzay etkin sistemlerin fiili (de facto) mülkiyet haklarını, hukuki (de jure) mülkiyet haklarından saptıran herhangi bir olay veya faaliyetten korumak için kullanılan kaynakların, süreçlerin ve yapıların organizasyonu ve toplamıdır (Dan Craigen, 2014)." Bu tanıma bakıldığında konunun mülkiyet hakkı temelinde ele alındığı ve siber güvenlik kavramının teknik boyutuna siyasi bir boyut eklendiği söylenebilir.

[7] "**Siber Güvenlik:** Siber uzayı oluşturan **bilişim sistemlerinin** saldırılardan korunmasını, bu ortamda işlenen bilginin/verinin gizliliği, bütünlüğü ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber olayların tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber olay öncesi durumlarına geri döndürülmesini kapsayan faaliyetler bütünü." Kaynak: (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023), 2020)

3.2.3.3 Siber Güvenlikleştirme Kavramı

Kopenhag Okulu, soğuk savaş sonrası dönemde güvenlik kavramının askeri güvenliği aşarak genişlemesine karşı yeni bir güvenlik yaklaşımı olarak güvenlikleştirme kavramını öne sürmüştür. Doksanlı yılların güvenlik kavramsallaştırmasına göre beş güvenlik sektörü ve farklı güvenlik sektörü tanımlamışlardır, askeri, ekonomik, çevre, siyasi ve toplumsal sektör. Okul bilgisayar ağlarının yeni gelişmeye başladığı bu dönemde siber güvenlik alanının önemine kayıtsız kalmamış ancak bu alanını ayrı bir sektör olarak ele almamış, siber alanının güvenlikleştirici aktör tarafından referans obje olarak değerlendirilebileceği analizi yapılmıştır (Buzan, 1997, s. 25).

Aradan geçen 25 yıl içerisinde siber uzay küresel bir ağ ve ilişkiler bütününe dönüşmüştür. Güncel internet, sosyal medya kullanımını analiz ettiğimizde gelinen noktanın büyüklüğü daha iyi anlaşılacaktır.[8]

Günümüzde dünya nüfusunun %60'ı (5.5 milyar insan) aktif olarak internet kullanıcısıdır. Yine dünya nüfusunun %50'si (3.8 milyar insan) sosyal medya kullanıcısıdır. Ülkemizde durumu ele aldığımızda, Ocak 2020 itibarıyla Türkiye'de nüfusun %72'si (62 milyon insan) aktif internet kullanıcısıdır. Sosyal medya kullanım oranı ise %64 (54 milyon insan) seviyesindedir. İnternette bağlanan cihaz sayısı üzerinden bir analiz yaptığımızda, 16-64 yaş arası nüfusun %89'unun akıllı telefona sahip olduğu ve %67 oranında bilgisayara sahip olunduğu görülmektedir. Tablet bilgisayar sahiplik oranı da yaklaşık olarak %49 civarlarındadır. Aktif internet kullanıcıların (54 milyon insan) mobil cihaz ya da bilgisayarlar vasıtasıyla günde ortalama 7 saat 30 dakika internette vakit geçirdikleri tespit edilmiştir. Bu orana dahil olmak üzere sosyal medyada vakit geçirme süresi günlük ortalama 2 saat 52 dakikadır. İnternetin ekonomi alanına

[8] Çalışmanın bir sonraki bölümünde siber uzayın büyümesi ve güncel durumu daha kapsamlı olarak ele alınacaktır. Bu noktada kavramsal çerçeveye kaynaklık etmesi, günümüzde siber uzayın neden ayrı bir güvenlik sektörü olması gerekliliğini açıklamak maksadıyla güncel bazı veriler bu nokta da değerlendirilmiştir.

getirdiği bir yenilik olan ve sıklıkla siber saldırılara maruz kalan kripto paraya sahiplik oranı ise %10 seviyelerindedir.[9]

Eldeki veriler analiz edildiğinde, ülkemiz insanının internet ve sosyal medya üzerinde fiziki dünyadaki yaşamına eş değer sürelerde bir zamanı sanal dünyada geçirdiğini göstermektedir. Fiziki sınırlardan bağımsız olan bu yeni uzay, insanlık için yeni fiziki sınırlardan bağımsız yeni bir siyasal yaşam alanı yaratmıştır. Fiziki sınırlardan bağımsız olan bu sanal alan, fiziki sınırlara dayalı geleneksel güvenlik anlayışı ve teorilerinde dönüşümü zorunlu kılmaktadır. Güvenlikleştirme teorisi özelinde bir analiz yapacak olursak siber uzay güvenliği referans obje durumunun ötesine geçerek yeni bir güvenlik sektörü haline gelmiştir (Garcia, 2014, p. 1076).

Kopenhag Okulu, güvenlik sektörlerinin belirli alt konseptlerle tanımlanabileceğini öne sürmüştür. Bu önermeye göre bir sektörün tanımlanmasında farklı alt konseptler referans nesneleri, güvenlikleştirici aktör ve tehditleri bir araya getirmektedir (Buzan, 1997,p. 27). Siber güvenlikleştirme kavramının ortaya atılmasıyla beraber bu yeni alana özgü üç farklı kavram belirlenmiştir. Bu kavramlar farklı sektörler için de uygun olmasına rağmen siber alan sektörüne özgü birtakım özelliklere sahiptirler (Hansen and Nissenbaum, 2009, p. 1170). Ayrıca kendi aralarındaki etkileşim siber alana özgü farklılıklara da sahiptir.

3.2.3.3.1 Hiper Güvenlikleştirme

İlk kavram olan hiper güvenlikleştirme, normal bir tehdit ve tehlike seviyesinin ötesinde bir tehdit ve tehlike tanımlamasıyla birlikte bu olağanüstü tehdit ve tehlikelere karşı güvenlik tedbirlerinin artırılması olarak tanımlanabilir. Her ne kadar Güvenlikleştirme kavramının kendisi, olağanüstü tedbir almak olarak belirlenmiş olsa da siber alan için hiper güvenlikleştirme kavramı bu alandaki tehditlerin zamansız bir biçimde aniden ortaya çıkması ve siber alan dışına taşarak tüm sektörlerde yıkıcı etkiler bırakabilmesi olarak düşünülmüştür

[9] www.gloabalwebindex.com tarafından sağlanan verilerle hazırlanmıştır. Erişim tarihi:16 Kasım 2020

(Hansen and Nissenbaum, 2009, p. 1157). Örneğin bir devlet bankasının siber saldırı sonrasında ekonomik olarak yaşadığı büyük kayıplar sadece ekonomik sektörde değil, toplumsal alanda da ciddi zararlara neden olabilecektir. Siber alandaki tehditlerin bu etki seviyesi de beraberinde aşırı güvenlikleştirme tedbirlerini getirebilmektedir. Bu duruma örnek olarak stratejik iletişimden sorumlu bir kamu kurumu olan İletişim Başkanlığı'na dijital verilere erişim yetkisi sınırlamasının çok geniş tutulması gösterilebilir. İletişim başkanlığı görev ve sorumluluklarının tanımlandığı kararnamede iletişim başkanlığın veri taleplerine tüm kurumların uyması zorunlu tutulmuştur. (İletişim Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi, 2018) Bu durumdan sadece ticari veriler hariç tutulmuş, kişisel verilerin gizliliği gözetilmemiştir. Kişisel verilerin gizliliğinin özünde temel hak ve hürriyetinin korunması esasının yer aldığı göz ardı edilerek, reel bir tehdidin varlığı olmaksızın bir kamu kurumuna siber alanda geniş yetkiler tanımlanmıştır.

Güvenlikleştirme kavramı, hayata geçirilirken geçmişte yaşanmış felaketlerin boyutu ve yarattığı yıkıcı etkiler göz önünde bulundurularak tedbirler hayata geçirilir. Siber alanın yeni bir sektör olması ve sektörde yaşanmış felaket, olağanüstü hal durumlarının azlığının getirdiği belirsizlik durumu beraberinde daha fazla güvenlik endişesi getirmektedir. Bu öngörülemezlik durumunun önüne geçmek için dijital "Pearl Harbour" gibi benzetimlerde bulunularak (Goldman, 2018, s. 128) karşılaşılacak durumun yaşanmış felaketlere benzetimi yoluyla olası sonuçları değerlendirilmektedir. Tüm bu senaryolar da beraberinde daha yoğun bir güvenlikleştirme ihtiyacı getirmektedir.

3.2.3.3.2 Günlük Güvenlik Uygulamaları

Günlük güvenlik uygulamaları kavramı, özel sektördekiler de dahil olmak üzere güvenlikleştirici aktörlerin aldığı güvenlikleştirme önlemlerinin, daha önce vurgulanmış olan hiper güvenlikleştirme uygulamaları dahil, bireylerin gündelik olarak siber alanla olan ilişkisini düzenleyen uygulamalardır. Günlük güvenlik

uygulamaları kavramı klasik bireysel güvenlik kavramlarını öne çıkarmaz. Güvenlikleştirme teorisinin önemli bir sac ayağı olan güvenlikleştirme tedbirlerinin dinleyici (halk ya da bireyler) tarafından da kabul edilmesi aşamasını temsil eder. Örneğin, güvenlikleştirici aktör olarak devletin bazı web sitelerine ya da sosyal medya uygulamalarına erişimi engellemesi düzenlemesini, bireylerin uyum sağlaması başarılı bir siber güvenlikleştirmeyi sağlayacaktır. Teknik olarak erişim sağlamanın engellenmesini de içeren bu düzenlemelerin VPN vb. tekniklerin kullanılarak aşılması durumu ise başarılı bir güvenlikleştirmenin sağlanamaması ile sonuçlanacaktır. Bireylerin sanal dünya da kendine yeni bir siyasal yaşam alanı yaratmış olması, siber alana ilişkin olağanüstü güvenlik tedbirlerinin kişilerin temel hak ve özgürlüklerinin sınırlandırılması gibi tartışmaları da beraberinde getirebilecektir. Örneklendirecek olursak, güvenlik için kişilerin internet trafiğinin analizi beraberinde kişi mahremiyetinin ihlali durumlarını da doğuracağı aşikardır. Bu nokta da güvenlikleştirici aktör bilgilendirme ve onay alma süreci gibi ek hukuki önlemler almak zorunda kalacaktır. Siber güvenliğin kendine özgü durumu nedeniyle bütüncül bir siber güvenlik kavramı için günlük siber güvenlik uygulamaları başarılı bir güvenlikleştirme için kritiklik arz etmektedir. Nükleer savaş senaryoları doğrultusunda halkın nükleer saldırılara karşı eğitilmesi sonucu gündelik hayattaki uygulamalarda değişim sağlanmasının başarı seviyesi total güvenliğe kısmi etki sağlayacaktır. Gerekli siber güvenlik tedbirleri doğrultusunda kapalı bir ağla yönetilen nükleer santral ağında bir kullanıcının evinden getirdiği bir taşınabilir belleği bu ağdaki bilgisayarında kullanması dünya çapında nükleer bir felaketle sonuçlanabilecektir. Bu nedenlerden dolayı siber alanın güvenlikleştirilmesine yönelik günlük güvenlik uygulamaları siber alana özgü bir durum olarak karşımıza çıkmaktadır.

3.2.3.3.3 Zorunlu Teknikleştirme

Siber güvenlik alanının kendine özgü teknik boyutu aynı zamanda belirli bir eğitim ve süreç sonucunda ulaşılabilen bilgi sistemleri güvenliği uzmanlarının bu alanda söz sahibi olmasını sağlamıştır. Halkın ve güvenlik teorisyenlerinin bu teknik

bilgiden yoksun oluşu teknik uzmanların alanı domine etmesine neden olmaktadır. Siber saldırıların teknik karmaşıklığının her geçen gün artması bu durumu destekleyen bir diğer etkendir. Ayrıca siber güvenliğin teknik uzmanları kamuoyunu ve güvenlikleştirici aktörleri yönlendirmektedirler. Teknik uzmanlar tarafından dile getirilen tehditler ve güvenlik tedbirlerinin bilinmezliği ise beraberinde artırılmış bir güvenlikleştirmeyi getirebilmektedir. Kimi durumlarda teknik ütopik bir tehdit evreni ve güvenlikleştirme süreci ortaya çıkmaktadır. Salt teknik bilgi ile günlük siyasal alandan güvenlikleştirme aşamasına geçişte beraberinde güvenlikleştirme bunalımını getirebilmektedir. Kimi durumlarda ise güvenlikleştirici aktörün teknik gereklilik olarak ortaya çıkardığı güvenlikleştirme hareketinin arka planında politik bazı amaçlar yer alabilmektedir. Örneklendirecek olursak, güvenlik gerekçesiyle tüm çalışanlarının internet trafiğini analiz ettiren bir özel sektör yöneticisinin bu yaklaşımının arkasında çalışanların siber uzaydaki faaliyetleri takip etme dürtüsünün yer alması karşımıza her yerde çıkabilecek bir durumdur.

3.3 Siber Güvenlik Krizleri ve Siber Güvenlikleştirme İlişkisinin Kavramsal Analizi

3.3.1 Kriz Kavramı ve Güvenlikleştirme

Kriz kavramı araştırma alanı ve bağlamına göre farklı şekillerde tanımlanabilmektedir. Genel bir tanımlama ile kriz, olağan durumda belirleyici bir değişiklik yaratma olasılığı yüksek olan istikrarsızlık durumudur. Daha genel anlamda kriz; birey, grup, organizasyon veya topluluk düzeyinde kritik, tehlikeli ve istikrarsız bir durum yaratan, çoğunlukla ani ve beklenmedik olumsuz bir değişimdir. Krizler genellikle olağan olanın ve süreçlerin istikrarının bozulması ile karakterize edilir, böylece kriz çeşitli seviyelerde karmaşaya neden olur. Krizler çoğu zaman aniden ortaya çıkmasına rağmen, uzun dönem süren ve çözümü için uzun vadeli planlama ve uygulama gerektiren bir sürece dönüşebilmektedirler. Krizlerin getirdiği karmaşa durumu olağan durumlarda sahip olunan kapasite ve

yeteneklerin sınırlanmasına neden olabilmektedir. Krizlerin karmaşa ve aniden gelişme özelliği, beraberinde bir krizin başlangıç aşamasındaki bilinmezlik olgusunu da getirmektedir (Garayev, 2013, p. 187). Bilinmezlik durumunun bir diğer sonucu da karar verici aktörlerin karar almalarını güçleştirmesi ve kriz sürecinin uzamasıdır.

Karar alma mekanizmasını pek çok etken etkilemektedir. Zaman baskısı, bunlar arasında önemli olan etkenlerden birisidir. Karar verici aktörler kriz esnasında hızlı bir çözüme odaklanırlar çünkü krizin uzaması durumunda krizin kalıcı ya da çok uzun vadeli bir sürece dönüşme ihtimali mevcuttur. Kriz durumunda karar vericilerin çözüm üretici karar verebilmeleri için bilgi akışı önem arz etmektedir. Bilgi akışının sağlıklı olduğu kimi durumlarda sağlıklı karar alma kapasitesi, tek başına alınan kararların doğruluğunu yükselten etken olamamaktadır. Akan bilginin analizini yapabilmek için yeterli zamanın bulunmaması elde edilen yararlı bilgiden fayda sağlanmasını engellemektedir. Bu etkenlerden dolayı kriz zamanları yüksek risk dönemi olarak adlandırılır. Bu noktada yüksek riskin varlığı tutarlı karar almayı güçleştiren bir faktör olarak karşımıza çıkar. Bu durumun bir diğer sonucu da krizden etkilenen aktörlerin beklenmeyen ya da gerçekleşmesi istenmeyen kötü sonuçlarla karşı karşıya kalması durumudur.

Krizin getirdiği kötü sonuçlarla karşı karşıya kalma ihtimali, olağan zamanlarda değiştirilemeyen, yanlış uygulama ve düzenlemelerin değiştirilmesine fırsat yaratmaktadır. Pek çok kriz yönetimi uzmanı, krizlerin aynı zamanda bir öğrenme ve sistemi yenileme fırsatı sunduğunu öne sürmektedir. Aynı zamanda krizlerin toplumun ve karar verici mekanizmaların dayanıklılık kapasitesini ölçtüğü ve karar verici mekanizmaların karar alma gücünü test ettiği öne sürülmektedir (Garayev, 2013, p. 188).

Kriz kavramının yaşam döngüsünü üç aşamaya bölmek olanaklıdır. İlk aşamada kriz kavramı başlamış, ilk uyarıları ortaya çıkmış ancak karar verici aktörler bu yeni durum için henüz tedbir almamışlardır. Bu dönemi “Kriz Uyarılarının Oluşumu ve Gelişimi” aşaması olarak adlandırmak mümkündür. Bu aşama da

krizin “bilinmezlik” özelliği devrededir, bilinmezlik durumu içinde oluşan kriz sinyal ve uyarıları doğru okunur ve gerekli tedbirler zamanında alınırsa, kriz oluşmadan önlenebilir. Aksi durumlarda ise kriz aşaması artık başlamış olur. Kriz döneminde ise krizin varlığı kabul edilmiş olur ve gündemde olağanüstü tedbirler ve yönetim usulleri bulunur. Krizin aktif yönetimi aşaması da diyebileceğimiz döneme ilişkin güvenlikleştirme teorisine göre bir yaklaşım sergilediğimizde, krizin varlığının kabulü krize neden olan olayların güvenlik konusu olduğunun karar alıcı aktörler tarafından kabulüdür. Karar alıcı aktörler siyasal olanın dışına çıkarak olağan üstü tedbirler alınarak çözülmesi gereken bir olay/olayların olduğu öne sürerek bu durumu güvenlikdışlaştırmak[10] için olağan dışı olan çeşitli düzenlemelere başvuracaktır. Krizin aktif olarak yönetildiği bu dönemde kriz yönetimi sürecinin de aktif döneminin başladığını söylemek olanaklıdır. Güvenlikleştirme teorisi üzerinden bu dönemi ele aldığımızda; krizin başlangıç ve sonunun belirlenmesi reel tehdit ve tehlikelerin varlığı ile belirlenmez. Kriz yönetim sürecine reel tehditlerin varlığı ve sonlanması üzerinden yapılan kriz yönetimi yaklaşımları, güvenlikleştirme teorisi kapsamında geçerliliğini yitirmektedir. Son dönemde meydana gelen ve halen içerisinde bulunulan COVID-19 krizi üzerinden örnekleyecek olursak, durumun kriz olarak kabulü reel tehditlerin başlangıcı ile değil ilk vaka sayılarının ülkemizde artışa geçmesiyle olmuştur (Deutsche Welle,2020). Bu aşamada şu nokta da gözden kaçırılmamalıdır: Siyasal alanda bu konu güvenlik tehdidi olarak reel tehditlerin başlangıcı ile olmuş, devlet mekanizması kendi içerisinde bazı tedbirler almıştır (Sözcü,2020). Ancak güvenlikleştirme süreci olarak adlandırdığımız süreç olağanüstü tedbir alma kararlarının alınıp uygulanmasıyla başlamıştır. Yine krizin ilk dalgası olarak belirtilen dönemin bittiğinin kabulü de reel tehditler ışığında değil, güvenlikleştirme sürecinin ekonomi başta olmak üzere, diğer güvenlikleştirme sektörlerinde yarattığı tahribatla reel tehditler arasındaki denge gözetilerek gerçekleştirilmiştir. 2020 yaz döneminde halen reel olarak COVID-19 vakaları

[10] Güvenlikdışılaştırma; daha önce tehdit olduğu kabul edilen bir şeyin artık tehdit olarak inşa edilmemesidir. Kopenhag Okulu güvenlikleştirme kavramının olağan dışı durumlara nedeniyle demokratik siyasi bir rejim ortamına engel olarak görür (Hisarlıoğlu, 2019). Bu nedenle siyasalın inşasında güvenlikdışlaştırmayı savunur. Güvenlikdışlaştırma sayesinde sorunlar rutin siyasi süreçlerle çözülebilecektir. Güvenlikdışlaştırma rutin sorunları güvenlik dışına alarak daha çok siyaset ve daha az güvenlikleştirme öngörmektedir.

mevcutken güvenlikleştirme çabaları bu noktada düşürülmüş, güvenlikleştirmenin somut örnekleri olan sokağa çıkma yasağı, seyahat yasağı gibi güvenlikleştirici tedbirler bu aşamada kaldırılmıştır (Milliyet, 2020). Güvenlikleştirme gündemine alınan olay/olaylar dizisi, karar verici aktörler tarafından güvenlikdışılaştırıldığı sonrası dönemi, kriz sonrası aşama olarak ele almak olanaklıdır. Bu aşama da hasar tespiti, alınan dersler ışığında olağan tedbirler alınması, eğitim gibi siyasal olan içinde kalan süreçler işlemektedir.

3.3.2 Kriz Yönetimi Kavramı

Genel anlamda kriz yönetimi ile ilgili literatür kriz yönetimini zor koşullar altında karar verme ve kararların uygulanmasını sağlamak olarak tanımlamaktadır. Gerçekte neyin "zor koşullar" olarak kabul edildiğine dair nesnel ve öznel düşünce okulu arasında temel bir ayrım vardır. Bilişsel-kurumsal yaklaşım, algıların, politik ve örgütsel kısıtlamaların bir krizi “yaratan” olarak ele alır ve daha öznel bir bakış açısı sunar. Krizi sayısal bir gerçeklikten ziyade olayların bir yorumu olarak kabul eder. İkinci bakış açısının avantajı, hepsi aynı olayla ilgilenen, farklı durumlarda farklı aktörlerin daha kapsayıcı ve nüanslı bir resmine izin vermesidir. Bir aktörün ciddi bir kriz olarak algıladığı şey, diğeri için neredeyse günlük rutin olacaktır. Dolayısıyla öznel bir yaklaşım hem bakış açılarını ele almamıza hem de alınan kararları ve nihai bir karara varmada yer alan mekanizmaları analiz etmemizi ve açıklamamızı sağlar.

Boin vd. tarafından gerçekleştirilen, kriz yönetimini siyaset bilimi argümanları ile ele alan ufuk açıcı çalışmada kriz; yüksek derecede belirsizlik veya belirsizlik yaratan, büyük bir aciliyet duygusu uyandıran ve yüksek değer verilen varlıkları tehlikeye atan bir olay olarak tanımlanmış, bir krizin öznel bir tanımı sunulmuştur (Boin, Stern, and Sundelius, 2005). Krizin tanımlanmış olan öznel nitelikleri arasındaki denge, krizin gelişimine göre öngörülemez bir şekilde değişebilir. Gerçekte ne olduğuna dair bir belirsizlik meydana gelebilir, aynı zamanda önerilen bazı eylemler dizisinin sonuçlarına yönelik belirsizlik durumu ortaya

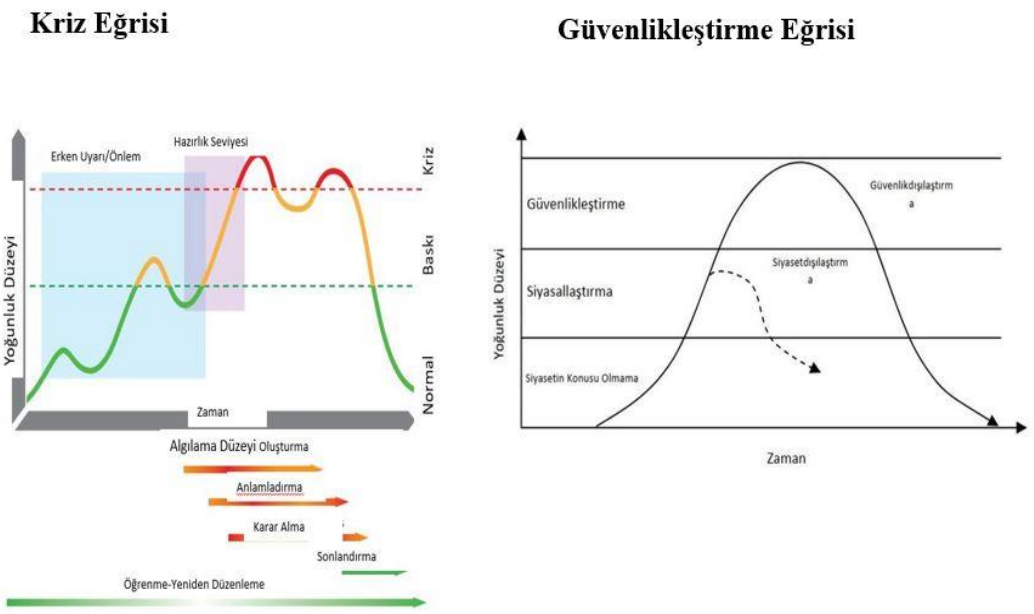
çıkabilir. Kriz durumunda tehdit altında olan yalnızca insan hayatı veya maddi varlıkları değil, aynı zamanda güven, itibar veya güç gibi daha soyut değerler de olabilir.

Kriz sürecinin yönetimini sağlayan karar verici aktörlerdir. Her ne kadar kriz durumunda olağan durumun ötesine geçilse de bu olağan durumdaki siyasal statüko bu aşama da karar vericileri etkileyecektir. Kamu genelini değerlendirdiğimizde üst kademelerden itibaren kamudaki kriz yöneticileri hükümetin belirlediği politikaya göre hareket edecektir. Güvenlikleştirme teorisi ele alınırken belirlenen politikaların uygulayıcılarının, bu noktada kamu hükümet ve kamu bürokrasisi bu misyondadır. Dinleyici kitle (halk) ile ilişkisi vurgulanmıştır. Başarılı bir güvenlikleştirme ya da kriz yönetimi için alınan kararlara halk tarafından uyulması gerekmektedir. Kriz yönetiminde sürecin yönetiminde lider kadro ve teşkilatının krizi yönetirken halkın sürece uyumu kapsamında daha önce ele alınmış olan kriz aşamalarına uygun bir hiyerarşide hareket etmesi gereklidir. Krizin ve kriz yönetimin politik yönünü gözeten bir kriz yönetim çerçevesi Boin ve arkadaşları tarafından orta konmuştur (Boin, Stern, and Sundelius, 2005, p. 1). Kriz yönetiminin politik durumunu öne çıkaran bu çerçeve kriz yönetimi süreci ile güvenlikleştirme teorisi argümanları paralellik içermektedir (Trimintzios, Holfeldt, Uckan, and Gavrila, 2014). İleri de ele alınacağı üzere bu çerçeve aynı zamanda siber güvenlik krizlerinin kendine özgü durumunu kapsayabilecek bir konumdadır.

Boin, bu tür kriz durumlarının çözümünde yer alan beş temel aşama veya zorluğu tanımlamaktadır. Aşamalar, kronolojik sırayla şunlardır: algılama düzeyi oluşturma, anlam verme, karar verme, sonlandırma ve öğrenme (Boin, Stern, and Sundelius, 2005, p. 10). Bu aşamalar (eşit olmayan bir şekilde) kriz öncesi-sırasında-sonrasında şeklinde ayrılabilir. Kriz yönetimi fiili olarak büyük oranda kriz sırasında gerçekleşir. Bu beş aşama ayrı olaylar olarak görülmemelidir. Aksine, üst üste gelirler ve birbirlerine geçiş yaparlar. Kriz döneminde karar verici aktörler tarafından krize anlam verme aşaması devam ederken buna paralel yeni bir algılama düzeyi oluşturma ve acil karar verme durumu gelişebilir.

Kriz çözümü için belirlenen bu beş görev, güvenlikleştirme argümanları ile örtüşmektedir. Karar verici aktör dinleyici onayına sunmak için tehditleri, algılama düzeyi oluşturma aşamasında gündeme getirir. Anlam verme aşamasında dinleyici kitleye belirlenen tehditler ve alınan kararlar bildirilir. Karar verme aşamasında güvenlikleştirme için belirlenen olağan dışı tedbirler uygulanır. Tekrar olağan olana dönme aşamasında ise sonlandırma ve öğrenme aşamasına geçilir. Zaman ve yoğunluk derecesine göre kriz durumu ve güvenlikleştirme eğrilerinin paralelliği kriz yönetimi ve güvenlikleştirme kavramı arasındaki ilişkiyi göstermektedir. Şekil-9 incelendiğinde kriz eğrisi ve güvenlikleştirme eğrisinin aşamalar arası geçiş noktalarının birbiriyle olan örtüşmesi görülmektedir.

Şekil-9 Kriz ve Güvenlikleştirme Eğrilerinin Karşılaştırılması



Kaynak: a) Kriz Eğrisi (Williams, 2016) b) Güvenlikleştirme Eğrisi (Miş, 2014).

Algılama düzeyi oluşturma, neyin neden olduğunu bulmayı içerir. Algılama, krizin "öncesi" ve "sırasında" sınırlarını aşar ve erken uyarı ve tespit ile karıştırılmamalıdır. Algılama düzeyi erken uyarı ve tespit, anlamlandırma aşamasını tetikleyen etkinliklerdir. Bu faaliyetler ne kadar iyi ele alınırsa,

anlamlandırma o kadar kolay olur. Krizin belirsizliği burada zirve yapar. Olağan dışı olaylar meydana gelmektedir ancak olası olaya yol açan nedensel zincir ve krizin sonuçları henüz belirsiz durumdadır. Mevcut konuyla başa çıkmak için tam olarak ne yapılması gerektiğini anlamak ve ikincil olaylardan etkilenmemek, kritik öneme sahiptir. Konunun asıl özünü belirlemek, kriz yöneticilerinin kararlı ve yapıcı bir şekilde ilerlemesini sağlayan şeydir. Modern krizlerin ortak bir özelliği, muazzam bir veri akışına sahip olmasıdır. Ancak verinin işlenerek değerlendirilmesinde sorunlar yaşanmaktadır. Bu noktada algılama düzeyi oluşturma sürecinin çoğu, hangi verinin krizin özüyle ilgili olduğunu değerlendirmekle ilgilidir ve aynı zamanda gereksiz bilginin, durumun özünü ele alınış biçiminin engellememesi gereklidir (Boin, Stern, and Sundelius, 2005, p. 20).

Algı düzeyi oluşturulduktan sonra, anlam oluşturma yeni sorun haline gelir. Karar verici aktör tarafından, güvenlikleştirme nedeni olan durumun anlaşılması (bu duruma neden olduğu belirlenen tehdidin dinleyici kitle tarafından anlaşılmasını sağlamak için) yeni algı düzeyi halka aktarılarak neyin kriz olduğu ve neden bazı önlemlerin alınması gerektiği anlamı oluşturulmalıdır. Güven tesis etmek ve inandırıcılık düzeyini yükseltmek amacıyla olaylar için bir arka plan oluşturma sembolik mesajlar verme aşaması sürece dahil edilir (Boin, Stern, and Sundelius, 2005, p. 69). Örneğin bir ülkenin neden terörizm için hedef alındığını yanıtlayabilmek veya felaket esnasında toplumsal gücü ortaya çıkarabilmek için güçlü sembolik bileşenlere ihtiyaç vardır.

Anlam verme aşaması bir sonraki aşama olan karar verme için fikir birliği ve anlayış temeli oluşturur. Karar verme, mevcut kaynaklar, lojistik ve zaman kısıtlamaları yasal ve demokratik kısıtlamalar göz önüne alındığında durumu çözmek için fiilen harekete geçmeyi gerektirir. Karar verici aktörün ortaya koyduğu karar uygulayıcı organizasyondaki üst düzey yönetimden alt düzeyde gerçekleştirilen eylemelere kadar bir rehber olarak ele alınır. Kriz yönetimi yönetim organizasyonunu işler kılmakla ilgilidir.

Bu noktada karar vericiler, alt seviyelerde yapılan işlerin delegasyonunu iyi bir strateji ile sağlamak yerine mikro seviyedeki işleri yönetebilmek için detaylı bir koordinasyon sağlama yoluna gitme hatasına düşebilirler. Karar verme aşaması, sistem üzerinden verilecek başka karar kalmayana kadar ve operasyonel konular normale dönmeye başlayıncaya kadar sürer (Boin, Stern, and Sundelius, 2005, p. 42). Bu nedenle, gelecekteki operasyonel kararların sorumluluğu, bu noktada normal, günlük yetkililere geri verilebilir.

Sonlandırma aşaması, beş aşamadan belki de en farklı olanıdır. Ancak aynı zamanda, diğer aşamaların yerine getirilmesinin en kritik hale geldiği aşamadır. Karar vericilerin krizin nihayet bittiğine ve kriz yönetimi organizasyonunun (şimdilik) dağıtılabileceğine karar verdikleri yer burasıdır. Bu, mutlaka krizin her ayrıntısının tam olarak çözüldüğü anlamına gelmez, bunun yerine geriye kalanların normal, kriz dışı araçlar ve yöntemler kullanılarak ele alınabileceği anlamına gelir. Yapacak hiçbir şey kalmadığından dair bir beyandan ziyade normalliğe dönüştür. Güvenlikleştirme aşamasından siyasal olana ya da güvenlik dışsallaştırma kararı bu noktada verilir. Artık olağan dışı tedbirlerin alınmasına gerek kalmamıştır. Ancak öznel kriz anlayışı burada öne çıkmaktadır. Krizin bittiğine dair değerlendirmeye dinleyici kitlenin katılmama durumu ortaya çıkabilecektir. Karar verici aktörler anlam oluşturmayı başarılı bir şekilde yönetemezlerse fikir ayrılıkları ortaya çıkacaktır. Siyasi bir ortamda ise krizin nedenine ilişkin suçlayıcı ifadeler bu aşamada ortaya çıkacaktır. Alınan önlemlerle birlikte muhtemel sorumlularda sorgulanacaktır.

Operasyonel kriz yönetiminin sona ermesinden çok sonra bile, siyasi veya sembolik yönetim bir sonraki aşamaya hazırlanmak için ek güçlü eylemlerden faydalanabilir. Alt seviye yönetim bile bu uzanımdan yararlanabilir. Kriz sırasında, karar verici aktörlerle ile uygulamalı işi yapan alt seviye yönetim arasında hızlı ve doğrudan iletişim yolları kurulmuş olabilir (Boin, Stern, and Sundelius, 2005, p. 112). Kriz devam ettiği sürece, karar verici aktörlerin kriz sona erdiğinde hangi reformlara ihtiyaç duyulacağı konusunda etkileme, hatta bazı kriz önlemlerinin günlük bazda yararlı olabileceğini öne sürme imkanları vardır.

Öğrenme ve reform, en azından retorik olarak, bitirme muammasının çıkış yoludur. Bir araştırma, politika ve uygulamada değişiklik vaat ederek, siyasal olan alana geri dönüş cazip hale getirilebilir. Bununla birlikte, sembolik bir hareket olmanın ötesinde, öğrenme ve reform görevi işlevsel bir amaca hizmet eder. Gerçek iyileştirmeler yapma ve krizin ortaya çıkardığı sistemdeki hataları düzeltme fırsatı sunar. Tarihsel olarak, krizlerin çok ihtiyaç duyulan değişimler için büyük bir katalizör olduğu tespit edilmiştir. Bazı durumlarda dengeyi parçalayan bu olaylar olmadan, sistem durgunluk ve hantal hale gelme ve ayrıntılarla aşırı yüklenme riski taşır. Kriz, siyasal düzeni sarsar ve neyin işe yarayıp neyin yaramadığına yeni bir bakış atmaya zorlar. Kriz son seferden beri yapılan siyasal düzenlemelerin bir testidir. Böylece öğrenme, bir sonraki kriz beklentisindeki döngüyü kapatır. Yeni olayları anlamlandırmayı besleyen erken uyarı ve tespit mekanizmalarını üretir (Boin, Stern, and Sundelius, 2005, p. 136). Sadece karar verme için değil, aynı zamanda tarihsel benzetmelerin diğerlerinin, ortaya çıkan yeni tehditleri anlamasına yardımcı olduğu gelecekteki anlam oluşturma çabaları için bir temel sunan deneyimleri korur.

3.3.3. Siber Güvenlik Kriz Yönetimi

Bu tez çalışmasının odak noktası olan Türkiye'de, Kamu'da, siber güvenlik krizlerinin yönetimi sorunsalı üzerinden kriz yönetimini ele aldığımızda, Cumhurbaşkanlığı sistemine geçildikten sonra "Güvenlik ve Acil Durumlar Koordinasyon Merkezi" kurulmasına ilişkin yayımlanan Cumhurbaşkanlığı kararnamesinde ilgili kurumun görevleri arasında, "teknoloji kaynaklı acil durumlarda" ortaya çıkabilecek güvenlik riskleri yer almaktadır. Bu durum şu şekilde ifade edilmiştir:

> "Kamu düzeni ve güvenliğini, bireylerin temel hak ve hürriyetlerini, toplumun huzur ve güvenini temin etmeye yönelik faaliyetler ile doğa, insan ve **teknoloji** kaynaklı acil durumlarda ortaya çıkabilecek her türlü güvenlik riskinde, güvenlik odaklı olarak Bakanlık merkez birimleri, bağlı kuruluşlar, valilikler, mahalli idareler, diğer bakanlıklar, kurum ve kuruluşlar, özel sektör ve sivil toplum kuruluşlar arasında koordinasyon ve işbirliğini sağlamak (32 Numaralı Cumhurbaşkanlığı Kararnamesi, 2019, s. 1). "

Siber güvenlikle ilgili alınan tedbirlerin ana hatlarını ortaya koymak üzere 2019 yılında yayımlanan Cumhurbaşkanlığı Siber Güvenlik Genelgesi'nde siber güvenlik risklerinin ulusal bir güvenlik meselesi haline gelebileceği hususu vurgulanmaktadır. Diğer bir deyişle;

Güvenlik risklerinin gözden geçirilerek azaltılması, etkisiz kırılması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla tedbirler alınması öngörülmüştür.

Siber güvenlik kriz yönetimi özelinde ilerleyecek olursak, siber krizler içerdiği tespiti zor teknik faktörler ve krizin olası sonuçlarının tahmininin zor olması nedeniyle genel kriz yönetimi esaslarına kıyasla ek zorluklar içermektedir. Siber krizlerin yönetimi için genel kriz durumlarından çok daha büyük ölçüde bilginin analizi ve farklı durumların koordinesi gereklidir (Golandsky,2016, p. 1). Etkili bir siber kriz yönetimi, yöneticilerin hem kriz olaylarının kaynaklarını (yani siber olaylar) hem de bunları belirlemek ve planlamak için gereken strateji ve taktikleri anlamasını gerektirir.

Siber alanın büyüme hızına siber alanın getirdiği yenilikleri ve değişimi anlamlandırma çalışmaları yetişmekte zorlanmaktadır. Diğer güvenlik sektörlerinin siber alanla olan ilişkisinin de bu hıza dahil olmasıyla birlikte çok faktörlü bir tehdit evreni ortaya çıkmaktadır. Reel olarak siber alandaki iletişim altyapılarına yönelik saldırılarda bu paralelde ilerleyerek büyük bir artış göstermektedir. Dünyanın en büyük ve en iyi organize olmuş güvenlik örgütleri arasında olan NATO, siber alana ilişkin tehditleri ortaya çıkarmakta büyük güçlükler çektiğini itiraf etmektedir (Arts, 2019). BM tarafından da benzer bir yaklaşım sergilenerek siber alanın büyümesinin getirdiği pek çok avantajın yanında yeni tehditleri de getirdiği istatistiksel çalışmalarla ortaya konarken ve bu tehditlere karşı siber güvenlik normlarının geliştirilmesi çalışmalarına başlanmıştır (Roadmap to Digital Cooperation, 2020, p. 2).

Siber güvenlik kavramını, siber uzayda insanların varlığını bu alandaki mülkiyet hakları üzerinden tanımlamıştık. Siber krizlerde tam bu noktada etkisini hissettirmektedir. Hayatın tüm alanları ve yönetim ilişkilerinin siber alana karşı bağımlılık hızla artarken insan siber alan etkileşiminin sekteye uğraması ya da istismar edilmesi siber güvenlik olaylarını beraberinde getirmektedir.

Siber güvenlik krizini daha önce açıklanmış olan kriz tanımlamaları üzerinden ele aldığımızda, siber alandaki güvenlik krizlerini siber birey, grup, organizasyon veya topluluk düzeyinde kritik, tehlikeli ve istikrarsızlık olaylarına neden olan olay/olaylar dizisi olarak tanımlayabiliriz. Finans sistemlerini etkileyen bir siber olay ülke güvenliğine yönelik bir siber olaya dönüşebilir (Mee, 2018, p. 1). Söz konusu siber olay finans sistemi ile sınırlı kalmayıp enerji, sağlık sektörünü de etkisi altına alabilir (Williams, 2016, p. 3). Siber-insan etkileşiminin boyutu değerlendirildiğinde tüm toplumu derinden etkileyecek bir kriz senaryosu ortaya çıkabilecektir.

Literatürde siber güvenlik kriz yönetimine yönelik kendine geniş bir yer bulmuş olan siber olay müdahale süreci (Williams, 2016, p. 3-4) siber güvenlik kriz yönetimini ele alırken birincil başvuru argümanı olarak bu süreç ele alınmamıştır. Bunun en temel nedeni ise bu sürecin siber güvenliğin teknik boyutunun önemli bir ayağı olmasıdır. Ancak daha önce açıklanmış olan siber güvenlikleştirme aşamaları ile bu süreç arasında dolaylı bir ilişki bulunmaktadır. Türkiye'de siber güvenlik kriz yönetimi süreci daha önce ortaya konmuş olan siber güvenlikleştirme ve kriz yönetimi ilişkisi üzerinden ele alınarak irdelenmiştir.

Araştırmanın kavramsal ve kuramsal kısmı burada tamamlanmıştır. Bir sonraki bölümde siber güvenlik olgusunun analizi gerçekleştirilmiş, tarihsel süreçteki dönüşümü ve günümüzdeki karşılığı açıklanmıştır.

IV. BÖLÜM
SİBER GÜVENLİK

Bu bölümde; siber güvenlik olgusunun kavramsal ve tarihsel gelişimi kronolojik olarak açıklanmıştır.

4.1. SİBER GÜVENLİĞİN KAVRAMSAL VE TARİHSEL GELİŞİMİ

Günümüzde siber alan kavramı içerisinde sadece bilgi teknolojileri yer almamaktadır. İnsanların da artık bir parçası olan siber alan, kendi yarattığı ya da yine insanlar tarafından arka planda yaratılan siber kültür öğeleriyle birlikte fiziksel olarak yaşadığımız gerçek zaman ve mekanla tümleşik ve onunla etkileşimli bir kavrama dönüşmüştür.

4.1.1 Siber Uzay Kavramının Ortaya Çıkması ve Eşzamanlı Olarak Siber Güvenlik Kavramı ile Birlikte Genişlemesi Süreci

Siber alan kavramı ilk kez karşımıza William Gibson'a ait olan Neuromancer romanında çıkmaktadır. Gibson Neuromancer'de bilgisayarlar ve onları yöneten ajanlardan oluşan bir dünya betimlenmektedir (Gibson, 1984). Dönemin internet şartları düşüldüğünde, bilgisayarların henüz kolay kullanılan makinalar olmadığı bir dönem, ajanlar tarafından yönetilen bir ağ fikri olsa da arkasındaki temel düşünce Platon'dan beri süre gelen yeni ideal bir dünyanın kurulmasıdır. Teknolojinin gelişmesiyle ortaya çıkan bu alana ilk bakış açısı kültürel bir devrim sağlayacağı, özgürlüklerin artacağı, insanlık için bir umut şeklidedir. İlk çalışmalarda yer alan bakış açısı devrimci bir yapıdadır ve tabi ki bu ideal dünya da kötülük çok az olacağı gibi güvenliğe gereksinim de yoktur. Hobbes'un İngiltere'sindeki insanlar dışarıda kötülük kol gezdiği için evlerinin kapılarını kilitlerken bu yeni dünyada buna gerek yoktur. Çalışmanın genel problematiğini oluşturan siber güvelik kavramının önemi de bu çıkış noktasından gelmektedir.

Çünkü internetin ilk çıkış noktası her şeyi paylaşılabilir kılmak ve veri çıkışını özgür kılmak olduğu için güvenlik ön plana çıkmamıştır. Temellerinde güvenlik olmayan bu mimari, gerçek dünyadaki kötülükle yüz yüze gelince devasa bir güvenlik probleminin doğmasına neden olmuştur. 1990'lı yılların başındaki çalışmalarda siber alan yeni bir dünya olarak ele alınırken tüm internete hakim olabilecek bir güç, bilgisayar tanrı, gibi kavramlar üzerinden siber alanın nasıl bir evrim geçireceği tartışılmıştır (Benedikt, 1991). Tartışmanın günümüzde geldiği nokta, internete hakim olan bir bilgisayar tanrıdan onu hakimiyet altına almaya çalışan devletler ve şirketlerin durumudur. Siber güvenliğe ilişkin en keskin problemler ve tartışmalar da bu noktada çıkmaktadır. Küresel güç mücadelesinin yeni oyun alanı siber alan olmuştur.

Siber güvenlik tarihi, 1960'larda ana bilgisayarlarla başlar. İşletmeler için yeterince uygun olan ilk bilgisayar türleri bu dönemde ortaya çıkar. Bu bilgisayarların kapasitesi, elektronik veri işleme sistemlerinden yatırım getirisini görmekle sınırlıdır. Bu zamana kadar, "bilgisayar" kelimesi hesaplama yapan kişilerle ilgili bir kavram olup, "siber" kelimesi bilim kurgu dünyasına ait bir kavramdı. Bu dönemde, bilgisayarlar gardiyanlar ve kapılarla güvenlik altına alınmaktaydı. Fiziksel güvenlik prosedürleri, yalnızca yetkili kişilerin bilgisayarlarda çalışması için onlara fiziksel erişimine izin vermekteydi. Bilgisayarlar çok büyüktü ve yüzlerce metre kare alanın içerisinde özel güvenlik personeli tarafından korunmaktaydı. Zamanla bu güvenlik fonksiyonu iş kontrol teknisyeni adı verilen bilgisayar operatörünün rolü ile birleştirildi. Bilgisayarı kullanması gereken kişiler, verilerini ve programlarını delikli kart destesinde operatörlere teslim ederek operatör vasıtasıyla kartlardaki delinmiş deliklerin otomatik olarak bitlere ve baytlara çevirecek bir kart okuyucuya iletilmesi sağlandı. (Bayuk, 2012, s. 15)

1960'ların sonralarına doğru delikli kartlardaki verilerin ofislerdeki kart okuyucular sayesinde kablolarla ana bilgisayara aktarılması uygulamasına geçilmiştir. Bu durum beraberinde güvenlik personeline, ortaya çıkan bu yeni kablo ağının fiziksel güvenliğini sağlama görevini getirmiştir. Ancak bu dönemde bilgi

güvenliğinin temel bileşenleri olan gizlilik, bütünlük ve erişilebilirlik, endüstri standardı olarak kabul edilmediği için askeri ve istihbarat birimlerine ait birkaç istisna dışında gizliliğin önemi bulunmamaktadır. Bu dönemde sistemin sürekli olarak arıza vermesi ve yazılan kodların düzgün çalışmaması nedeniyle işlenen verinin bütünlüğünün bozulması daha ön planda olan bir güvenlik gereksinimiydi.

1970'li yıllarda delikli kartların yerini klavye ve terminalden veri girişi teknolojileri almaya başlamıştır. Bu durum delikli kartla veri giriş sisteminin güvenliğine dayanan güvenlik modelinde değişimi beraberinde getirmiştir. Kablo ve bina güvenliğine ilişkin fiziksel tedbirler devam ederken bunlara elektronik veri girişi için oluşturulan kullanıcılar için özelleştirilmiş mantıksal arayüzler eklenmiştir. Her kullanıcının yetkisine göre ayrı tasarlanan bu mantıksal arayüzlere kullanıcı adı ve şifrelerle erişilerek oturum açıldıktan sonra kullanıcıların yetkilerine göre verilere erişim sağlanmaktaydı. Klavye teknolojisi ile birlikle bilgisayarların kullanımı yaygınlaşmaya başlamıştır. Bu durum beraberinde gizliliğe ilişkin endişeleri de getirmiş ve özellikle askeri çevrelerde verilerin yetkisiz erişimini engelleyen kriptoloji algoritmaları geliştirilmeye başlanmıştır.

Bilgisayarlarda kişisel verilerin gizliliğe dikkat edilmeden depolanıp işlenmesi hususu ABD adalet çevrelerinin dikkatini çekmiş ve bilgi teknolojilerinde depolanan verilerin mahremiyetinin sağlanması için 1974 Gizlilik Kanunu kabul edilmiştir. Bu kanun ABD vatandaşların verilerini işleyip depolayan resmi kurumlar için veri gizliliğine ilişkin yaptırımlar içermektedir (Privacy Act of 1974).

1970'lerin sonlarına doğru ortaya çıkan kablo göbeği (hub) teknolojisi bilgisayarlar için yerel alan ağı oluşturmayı sağlamıştı. Bu yeni teknolojide oluşturulan yerel alan ağındaki (Local Area Network, LAN) veriye ağdaki bilgisayar sahibi herkes erişebilmekteydi. Ortaya çıkan bu güven açığının giderilmesi için MAC ve DAC protokolleri geliştirilmiştir. MAC protokolü zorunlu erişim kontrolünü sağlarken DAC ise herkese, erişime açık verilerin ayrımını sağlıyordu. Ancak bu protokoller kimin erişim sağlayabileceğini donanım seviyesinde belirlemekteydi. Bilgisayar kullanıcıların yaptıkları işlemleri takip

etmek, ilk LAN teknolojileri ile birlikte daha da güçleşmiştir (Canteaut, 2011, s. 314). Ayrıca ağ trafiğini şifreleme gibi bir teknoloji olmadığı için ağ trafiğini dinlemek, araya girmekte mümkün olabilmekteydi.

Bilgisayar teknolojilerindeki olası güvenlik ihlallerinin önüne geçmek için 1983 yılında daha sonra kapağının rengi nedeniyle turuncu kitap olarak adlandırılacak "Güvenilir Bilgisayar Sistemi Değerlendirme Kriterleri" ABD Savunma Bakanlığı'nca yayınlanmıştır. Bu yayında bilgi sistemleri güvenliği için zorunlu kurumsal politikaların belirlenmesi gerekliliği, ilgili politikanın içeriğinin nasıl olması gerektiği, erişim listesi mantığına göre hareket edilerek kullanıcı yetkilerinin sınıflandırılması ve hangi verilere ulaşabileceğinin belirlenmesi, hassas verilerin kriptolojik şifreleme yöntemleri ile şifrelenmiş bir şekilde işlenmesi hususları gibi günümüzde de halen geçerli olan güvenlik ilklerini içermekteydi (Trusted Computer System Evaluation Criteria, 2020). Bu yayın daha sonra yerini "Bilgi Teknolojileri Güvenlik Değerlendirmesi için Ortak Kriterler" dokümanına bırakmış olup, söz konusu doküman günümüzde bir siber güvenlik cihazı satın alımı işleminde ya da bilişim projelerinin güvenlik gereksinimlerinde göz önünde tutulan endüstri standarttı haline gelmiştir.

İnternetin başlangıç noktası olan daha önce ele almış olduğumuz ARPANET projesinde bilgisayarlar ağ üzerinden çevrimiçi olarak etkileşim halinde olmaktaydı. Bu dönemin temel servisi ise kullanıcıların birbirlerine eposta gönderdiği eposta servisiydi. 1988 yılında babası AT&T Bell Laboratuvarlarında araştırmacı olan, küçük yaşta bilgisayar teknolojileriyle tanışan ve onların güvenlik açıklıklarını sorgulayan Robert Morris, internetin ilk kurtçuk türü zararlı yazılımını geliştirerek ARPANET üzerinden yaymaya başladı. Bu yazılım kendini eposta hizmetinin açıklığından yararlanarak bu hizmeti kullanan bilgisayarlara kopyalayarak bilgisayarların temel servislerinin çalışmasını engelliyordu. Bu saldırıdan sadece AT&T Bell Laboratuvarları etkilenmemişti. Bunun nedeni eposta hizmetini daha güvenli hale getirmeye yönelik bir güvenlik tedbiri almış olmaları değildi. Gelen internet trafiğini analiz eden yeni bir teknoloji olan "güvenlik duvarı" sistemini test ediyor olmalarıydı. Bu saldırı ARPANET güvenliği

konusunda yeni politikaların üretilmesine neden oldu. Güvenlik duvarı teknolojisi yaygınlaştırılarak erişim politikaları güvenlik duvarı üzerinden yürütülmeye başlandı. Bu uygulama günümüzde benzer bir şekilde devam etmektedir. ARPANET içerisinde "Bilgisayar Olayları Müdahale Ekibi" kurularak bu gibi durumlara müdahale için uzmanlaşmış ekipler kurulmuştur. Temel siber güvenlik fonksiyonu olarak tespit ve geri kurtarma anlayışı geliştirilmiştir (Bayuk, 2012, s. 22). İleride ele alacak olduğumuz, Ulusal Siber Güvenlik Strateji Belgelerinde yer alan politikaları gerçekleştirmek üzere ülkemizde Kamu ve özel sektör genelinde benzer işlevleri yerine getirmek üzere Siber Olaylara Müdahale Ekipleri kurulmuştur.

1990'lı yılların başlarından itibaren internet ve günümüzdeki taşınabilir belleklerin öncüleri olan disklerin yaygınlaşması ile beraber zararlı yazılımların yayılımı ve etkileri artmaya başlamıştır. Bu duruma bir diğer etken ise, kullanıcıların ihtiyaçlarına yönelik yazılımların artmaya başlaması ve bu yazılımların gerekli güvenlik ilkelerine göre geliştirilmemesi nedeniyle açıklıklara sahip olmasıdır. Zararlı yazılımlara karşı yazılımların açıklıklarını kapatmak için yama güncellemeleri bu dönemde başlamıştır. Ayrıca her zararlı yazılımın gerçekleştirdiği faaliyetin işletim sistemi ve ağda kendine özel bir iz bilgisi bırakmasından yola çıkılarak zararlı yazılıma ait bu bilgiler, imza adı altında kategorize edilmeye başlanmıştır. Bu imzaların bir veri tabanında toplanarak işletim sistemlerini alt süreç ve işlemlerini, ağ trafiğini analiz edip bu imza veri tabanıyla karşılaştırıp zararlı yazılımları tespit eden anti virüs yazılımları geliştirilmeye başlanmıştır. Yine bu dönemde internet üzerinden alışveriş, kredi kartı bilgilerinin kullanılarak işlem yapılması uygulamalarının öncüleri gerçekleştirilmeye başlanmıştır. Bu durum beraberinde kullanıcı bilgisayarı ve sunucu bilgisayar arasında şifreli haberleşme ihtiyacını getirmiştir (Bayuk, 2012, s. 25). Bunu sağlamak için uçtan uca şifreleme sağlayan güvenli soket katmanı (Secure Socket Layer SSL) teknolojisi geliştirilerek kullanıcı ve sunucu tarafında oluşturulan SSL anahtarlarının değiş tokuşu mantığına dayanan uygulama katmanı şifrelemesi sağlanmıştır.

Siber güvenliğin gelişiminin erken evresine baktığımızda temel sorunun güvenliğin arka planda tutularak erişilebilirliğin öne çıkarılması olduğu karşımıza çıkmaktadır. İnternet ve bilgisayar teknolojilerinin hızlı gelişimi ve bu teknolojilere olan talep nedeniyle pek çok internet protokolü ve servisi güvenlik gereksinimleri gözetilmeden geliştirilerek ortaya çıkmıştır. Bu durum saldırganlar için elverişli bir ortam yaratmış ve bilgisayarların ilk çıktığı günlerden itibaren bilgi sistemlerine saldırılar gerçekleştirilmeye başlanmıştır. Günümüzde de devam eden temel sorun aslında budur, erişilebilirliği öne alarak güvenliğin arka planda tutulması güvenliğin ancak bir saldırı halinde düşünülmeye başlanması bilgisayarların ilk günlerinden itibaren ortaya çıkan güvenlik politikası uygulamasının geri planda tutulması, beraberinde, günümüze kadar gelen büyük siber güvenlik problemleri getirmiştir.

4.1.2 Günümüzde Siber Tehditler ve Siber Saldırılar

Siber tehditler siber alanın gelişimi ile birlikte ortaya çıkmış bir kavram olup, 1990'lı yılların başında ulusal güvenlik ve güvenlik önlemleri için yeni bir tür tehdit olarak değerlendirilmekteydi (Cavelty, 2008, s. 38). Siber tehdit kavramı, günümüzde bu yeni özelliğinden sıyrılıp ulusal güvenlik meselelerinin her alanında karşımıza çıkan bir olguya dönüşmüştür. Siber tehdit olgusunu bilgi ve iletişim teknolojilerinin kötü amaçlı olarak kullanımı potansiyeli şeklinde tanımlamak mümkündür. Bilgi ve iletişim teknolojilerinin kötü amaçlı kullanımı potansiyeline sahip aktörler, siber tehdit tanımlamasında başat rolü oynamakta, kötü amaçlarına ulaşmak için kullandıkları yöntemler siber tehditlerin sınıflandırılmasında etkin rol almaktadır. Siber alandaki tehditlerin doğru şekilde tespiti geliştirilecek olan siber güvenlik tedbirlerini doğrudan etkilemektedir. Bu nedenle tehdit tespiti güvenlikleştirme sürecinde kritik öneme sahip bir aşama olarak karşımızda durmaktadır.

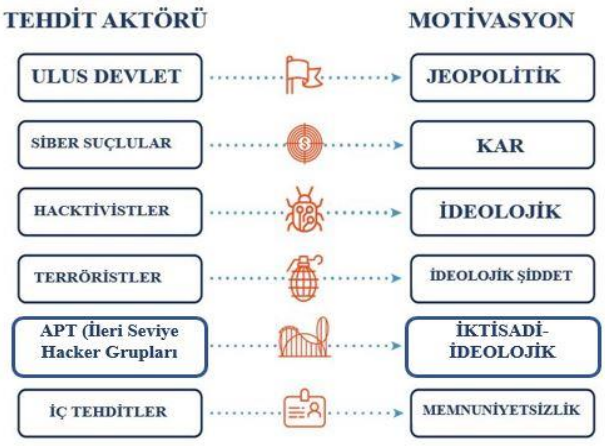
Tehdit kavramı; "hayata, bilgiye, her türlü faaliyete, çevreye ve/veya mülkiyete zarar verme potansiyeline sahip ve tehlike oluşturacağını işaret eden doğal veya insan yapımı olay, birey, tüzel varlık veya eylem" şeklinde tanımlanmaktadır

(Wikipedia, 2020). Siber tehditleri bu tanım üzerinden değerlendirdiğimizde siber tehditler dolaylı olarak insanların hayatını kaybetmesine neden olabilmektedir. Bu durum siber alanın ilk gelişimini sağladığı dönemlerden itibaren bir realite olarak karşımıza çıkmaktadır.

4.1.2.1 Siber Tehdit Aktörleri

Siber tehdit aktörleri, kötü niyetli olarak, mağdurların verilerine, cihazlarına erişmek veya başka bir şekilde etkilemek amacıyla bilgi sistemlerine yetkisiz erişim elde etmek için güvenlik açıklarından, düşük siber güvenlik bilincinden ve teknolojik gelişmelerden yararlanmayı amaçlayan devletler, gruplar veya bireylerdir. Siber tehdit aktörleri motivasyonlarına ve bir dereceye kadar karmaşıklıklarına göre kategorize edilebilir. Tehdit aktörleri, farklı nedenlerle aygıtlara, işlem gücüne, bilgi işlem kaynaklarına ve bilgilere erişime değer verir. Genel olarak, her tür siber tehdit aktörünün birincil motivasyonu vardır. Bu durum Şekil-10'da belirtilmiştir.

Şekil-10: Siber Tehdit Aktörleri ve Motivasyon Kaynakları



Kaynak: (CIS,2021).

Siber tehdit aktörleri yetenek ve gelişmişlik açısından eşit değildir ve faaliyetleri için bir dizi kaynak, eğitim ve desteğe sahiptir. Siber tehdit aktörleri kendi

başlarına veya daha büyük bir örgütün (yani bir ulus-devlet istihbarat programı veya organize suç grubu) bir parçası olarak faaliyet gösterebilir. Bazen, sofistike aktörler bile daha az sofistike ve kolay ulaşılabilir araçlar ve teknikler kullanır, çünkü bunlar belirli bir görev için hala etkili olabilir ve / veya savunucuların aktiviteyi ilişkilendirmesini zorlaştırabilir. Şimdi sırasıyla siber tehdit aktörleri açıklanmıştır.

4.1.2.1.1 Ulus Devletler

Özel kaynaklar, personel, kapsamlı planlama ve koordinasyon ile en karmaşık tehdit aktörüdür. Ulus Devlet Aktörünün "Hacking Lisansı" vardır. Bir hükümet, değerli verilere veya istihbarata erişmek için hedef hükümetleri, kuruluşları veya bireyleri bozmak veya tehlikeye atmak için çalışmalar içerisinde olabilir ve uluslararası öneme sahip olaylar yaratabilir.

Bir hükümet veya otoriter yönetim amaçlarına ulaşmak için yarı gizli bir siber orduyu veya kiralık bilgisayar korsanlarını kullanabilir. Elindeki bu kaynakları endüstriyel sırları çalmak, kritik ulusal altyapıyı bozmak, politika tartışmalarını dinlemek, ülke sınırları içinde ve dışında propaganda veya dezenformasyon kampanyaları yürütmek için kullanabilir (Güngör ve Güney, 2017, s. 142). Tüm bunlara ek olarak, ulus devletler, ellerindeki siber gücü devletin güvenlik aygıtının bir uzantısı olarak, muhalifleri veya aktivistleri izlemek ve engellemek için kimi zamanda Gürcistan örneğinde olduğu gibi elindeki gücü politik hedeflerini gerçekleştirebilmek için askeri güç ile birlikte kullanabilmektedirler.

4.1.2.1.2 Siber Suçlular

Siber suçluların, ulus-devletlere kıyasla genellikle orta derecede karmaşıklığa sahip oldukları anlaşılmaktadır. Bununla birlikte, çok sayıda kurbanı etkileyen özel teknik ve yeteneklere sahiptirler. Siber suçlu kavramının kısa tanımı bilişim

suçu işleyen kişi olarak yapılabilir. Bilişim suçu kavramının ise geniş bir karşılığı bulunmaktadır. Bilişim suçları, genel olarak bilgisayarın, bilgisayar ağlarının ya da elektronik ortamların araç olarak kullanıldıkları ya da bir hedef olarak maruz kaldıkları hukuka aykırı fiiller olarak tanımlanabilmektedirler (Turan, 2017, s. 64). Avrupa Komisyonu'nun 2007 tarihli bir tebliğinde yer alan tasnif esaslarına göre bilişim suçları;

- Elektronik ağlar vasıtasıyla işlenen klasik suçlar
- Elektronik medya üzerinde yayınlanan yasa dışı içeriğe ilişkin suçlar
- Elektronik ağlara has suçlar şeklinde (Hekim & Başıbüyük, 2013, s. 135) kategorilere ayrılmıştır.

Siber suçlular, gündelik hayattaki güvenlik krizlerini ve açıklıklarını kullanmak için siber alanı ikinci bir saldırı vektörü olarak kullanmaktadırlar. EUROPOL İnternet Ortamında İşlenen Suçlar ve Tehditler 2020 yılı raporuna göre, COVID-19 krizinin getirdiği zafiyetler siber suçlular tarafından istismar edilmektedir. Oltalama saldırılarından fidye şifreleme saldırılarına kadar tüm atak vektörlerinde COVID-19 teması masum insanları kandırmak için bir yem olarak suçlular tarafından kullanılmıştır. Çocuk cinsel istismarı gibi yüz kızartıcı suçların siber alanda işleme oranı 2020 yılında dramatik bir artış göstermiştir. Bu durumun en temel nedeni ise kolluk kuvvetlerinin suçluları takip ve tespit kapasitesinin pandemi nedeniyle düşüş göstermesidir.

Ülkemizdeki uygulamalar üzerinden bilişim suçlarına yaklaşıldığında bilişim suçları Türk Ceza Kanunu kapsamında tanımlanarak cezai müeyyideleri bulunmaktadır. TCK'da tanımlanan bilişim suçlarını doğrudan ve dolaylı bilişim suçları şeklinde tasnif edip gerçekleşme sıklıklarını ele aldığımızda karşımıza aşağıdaki tablo çıkmaktadır. Bankacılık sistemine yönelik suçlar başı çekerken bir diğer önemli oran "sistemi engelleme, bozma, verileri yok etme veya değiştirme suçuna" aittir.

Tablo-1: TCK Kapsamında Bilişim Suçlarının Dağılımı

TCK Bilişim Suçları İhlal Maddeleri	**Gerçekleşme %si**
Doğrudan Bilişim Suçları	
TCK 243 Bilişim Sitemine Girme	1
TCK 244 Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme	25
TCK 245 Banka veya Kredi Kartlarının Kötüye Kullanılması	62
TCK 245 (Teşebbüs)	1
Dolaylı Bilişim Suçları	
TCK 136 Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme	1
TCK 142 Nitelikli Hırsızlık	2
TCK 158 Nitelikli Dolandırıcılık	5
TCK 158 Nitelikli Dolandırıcılık (Teşebbüs)	1
TCK 226 Müstehcenlik	2

Kaynak: (Turan, 2017, s. 71).

Siber uzayın genişlemesi ve insanlar tarafından kullanım amaçlarının çeşitlenmesi siber suçların çeşitliliğini de beraberinde getirmiştir. Gelecekte ortaya çıkacak olan yeni kullanım alanları farklı siber suçları ortaya çıkaracaktır. Dolaylı bilişim suçları da bu kapsamda genişleyecek ve TCK'nın diğer maddelerinde dolaylı suç kapsamına girmeye başlayacaktır.

4.1.2.1.3 Hacktivistler

"Hacktivizm" kelimesi "hacking ve activism" kelimelerinin birleşimi ile birlikte ortaya çıkmıştır. Hacktivizm, hedef web sitesine hasar vermekten ziyade web sitesi sahiplerine karşı tepki ve rahatsızlığı belirtmek için siber saldırı düzenlenmesini ifade eder (Yegen, 2014, s. 119). Ancak günümüzde hacktivizm ve siber terörizm veya siber suçlar birbirine karışmış durumdadır. Kendilerini hacktivist olarak tanımlayan kişi ya da gruplar bir terör örgütünün uzantısı olabilmektedirler. Gerçekleştirilen eylemler ise TCK'da tanımlanan bir suça karşılık gelmektedir. Hacktivizm için en basit ifade yolu olan bir web sitesinin ele

geçirilip bu sitede propaganda yapılması aslında, “TCK 244 Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme” kanun maddesinde tanımlanan suça karşılık gelmektedir.

4.1.2.1.4 Siber Teröristler

Siber teröristleri, hacktivistler ve siber suçlulardan ayıran bir tanımlama için öncelikle terör tanımını hatırlamakta fayda vardır. 3713 sayılı Terörle Mücadele Kanunu’nda terör;

“Terör; cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir.” şeklinde tanımlanmaktadır. Görüldüğü üzere terörizm de yöntem olarak suç ve aktivizme konu olan eylemler, paralellik göstermekte ancak eylemin gerçekleşme amacı suç işleme, propaganda ya da tepki göstermekten ziyade anayasal düzeni değiştirme paralelinde yer almaktadır. Suç ve aktivizmin siber alandaki uzantısı konumunda olan siber suçlar ve hacktivizm ve yine terörizmin siber alan uzantısı olan siber terörizm arasındaki temel fark, eylemlerin anayasal düzeni bozma amacıyla yapılmasından kaynaklanmaktadır. Terörle mücadele kanunu da bu minvalde hareket ederek düzenlenmiştir. İlgili kanunun dördüncü maddesinde, TCK’nın bazı maddeleri sıralanmış ve terör örgütünün faaliyeti çerçevesinde işlendiği takdirde, terör suçu sayılacağı belirtilmiştir. Bu maddeler arasında doğrudan bilişim suçlarını tanımlayan TCK 243 Bilişim Sitemine Girme ve TCK 244 Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme maddeleri yer almaktadır.

Aşağıdaki suçlar 1'inci maddede belirtilen amaçlar doğrultusunda suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlendiği takdirde, terör suçu sayılır:

a) Türk Ceza Kanunu'nun 79, 80, 81, 82, 84, 86, 87, 96, 106, 107, 108, 109, 112, 113, 114, 115, 116, 117, 118, 142, 148, 149, 151, 152, 170, 172, 173, 174, 185, 188, 199, 200, 202, 204, 210, 213, 214, 215, 223, 224, 243, 244, 265, 294, 300, 316, 317, 318 ve 319 uncu maddeleri ile 310 uncu maddesinin ikinci fıkrasında yer alan suçlar (3713 Sayılı Terörizmimle Mücadele Kanunu).

Siber uzaya terörizm bağlamı özelinde yaklaşıldığında, teröristlerin bilişim ve iletişim teknolojilerini propaganda, örgüte üye kazanma, terörist eylemleri planlama, terörizm maksadıyla kullanılacak olan araç ve gereçlerin kullanımına ilişkin eğitim verilmesi, finansal kaynak temini gibi amaçlarla kullandığı belirtilebilir (Sönmez, 2017, s. 70). Finansal kaynak elde etme bağlamında değerlendirildiğinde siber teröristler siber suçluların kullandığı benzer yöntemlerle para elde etmeye çalıştığı ve insan, silah ve uyuşturucu ticareti gibi illegal faaliyetlerinin ödemelerini yine siber enstrümanlar (kripto para vb.) vasıtasıyla temin ettikleri söylenebilir. Günümüzde bu yasadışı, siber suç teşkil eden teşkil eden eylemler tür ve biçim olarak her geçen gün daha da çeşitlenmekte ve artmaktadır.

4.1.2.1.5 APT Grupları (İleri Seviye Hacker Grupları)

APT kelimesi İngilizce "Advanced Persistent Threat" kelimelerinin baş harflerinden oluşan, siber uzaydaki en tehlikeli siber tehdit unsurunu tanımlamaktadır. Türkçeye gelişmiş kalıcı tehdit olarak çevrilebilecek olan APT'ler ileri seviye hackerların bir araya geldiği grupları tanımlamak amacıyla kullanılmaktadır. APT grupları diğer siber tehdit unsurlarının aksine, teknik bilgi olarak üst seviye ve her biri farklı alt teknik alanlarda (zararlı yazılım geliştirme, web hacking olarak adlandırılan web siteleri, uygulamaları web hizmetleri üzerinden hedef sisteme sızma, ağ bileşenlerine saldırı vd.) uzmanlaşmış

kişilerden oluşur ve metodolojik olarak sürekli, gizli ve gelişmiş korsanlık tekniklerini kullanarak bir sisteme erişir ve burada, yıkıcı sonuçlar yaratmaya yetecek kadar uzun bir süre boyunca kalırlar. APT grupları genellikle Ulus Devlet tehdit aktörlerinin amaçlarına hizmet ederler. Ulus devletler APT gruplarını genellikle istihbarat örgütleri vasıtasıyla kullanırlar. Teknik yetkinlik seviyesi üst seviye olan bu gruplar sadece istihbarat örgütleriyle çalışmazlar, kimi durumlarda terörist örgütler yeterli teknik yetkinliğe sahip olamadıkları için amaçlarını gerçekleştirmek için APT gruplarına başvurabilmektedir (Evan, ve diğerleri, 2017). Bu amaç için terör örgütleri 'dark web'i kullanmaktadırlar. APT grupları ellerindeki teknik kapasiteyi siber suç işlemek içinde kullanmaktadırlar. Özellikle finans sektöründe gerçekleştirilen büyük çaplı başarılı siber saldırılar ve siber soygunlar, APT grupları tarafından gerçekleştirilmektedir.

4.1.2.1.6 Kurum İçi Tehditler

İçeriden gelen tehditler, kuruluşlarında çalışan ve güvenlik çevreleriyle korunan iç ağlara erişimleri nedeniyle özellikle tehlikeli olan kişilerdir. Erişim, kötü niyetli tehdit aktörleri için önemli bir bileşendir ve ayrıcalıklı bir erişimin olması, diğer uzak yolların kullanılması ihtiyacını ortadan kaldırır. İçeriden gelen tehditler, listelenen diğer tehdit aktörlerinin herhangi biriyle ilişkilendirilebilir. Ancak güdüleri olan hoşnutsuz çalışanları da içerebilir.

Kurum içi çalışanlar, zarar verme konusunda eşsiz bir yeteneğe sahiptir, çünkü bir kurumun iç güvenlik önlemlerini atlatmak genellikle sertleştirilmiş çevre savunmalarından daha kolaydır. Bir kurumun ofisleri ve ağlarındaki konumlarından, içeriden gelenler yalnızca hedeflerine daha fazla erişime sahip olmakla kalmazlar, aynı zamanda teknolojik koruma ve politika uygulamalarındaki herhangi bir tedbiri saptama ve böylece kritik bilgi varlıklarının nerede olduğunu keşfetme fırsatlarını arttırırlar. Bazı durumlarda kurum çalışanları farkında olmadan bir güvenlik olayına neden olan veya katkıda bulunan iyi niyetli çalışanları bir iç tehdit olarak ortaya çıkabilmektedir. Özelikle

kolay tahmin edilebilen parola kullanan kurumsal e-posta kullanıcıları büyük bilgi güvenliği ihlallerine neden olabilmektedirler.

4.1.1.2.2 Siber Saldırı Türleri

Siber saldırılar genellikle siber alanın teknik boyutunun zafiyetlerini hedef alır, ancak oltalama saldırılarında olduğu gibi insanların zafiyetlerini içeren karma saldırılar da bulunmaktadır. Siber saldırıların teknik detayları bu çalışmanın kapsamı dışında olup en etkili ve güncel siber saldırılar, kavramsal bütünlüğü sağlamak maksadıyla teknik detaylarından arındırılarak mantıksal metodolojileri üzerinden ele alınmıştır.

4.1.2.2.1 Zararlı Yazılımlar

Zararlı yazılımlar, bilgisayar virüsü, fidye yazılımları, casus yazılımlar ve diğer kötücül amaçlarla kodlanmış betik kodlar ya da yazılımlardır. Zararlı yazılımlar siber saldırganlar tarafından çeşitli amaçlar gözetilerek geliştirilirler. Bu amaçlar hedef sisteme girme, veri kaçırma, hedef sistemi çökertme veya zarar verme, hedef sistemi şifreleme ve akabinde fidye talebi gibi geniş bir yelpazeye dağılmaktadır. Zararlı yazılımın saldırılan sistemde aktive edilebilmesi için hedef sistem kullanıcıları hedef alınmakta ve bu amaç için sıklıkla oltalama eposta saldırıları kullanılmaktadır. Iran nükleer programını hedef alan “Stuxnet” siber saldırısı bir dizi zararlı yazılımın kombinasyonundan oluşmaktaydı ve kapalı bir ağda çalışan sistemlere erişim için farkındalığı az personel hedef alınarak, hedef personelin bahçesine atılan USB belleğin nükleer tesis ağında kullanımı sonrasında zararlı yazılımlar santral sistemlerine bulaştırılmıştı (Zaheer Masood, 2019). Bu anlamda en tehlikeli siber saldırı türü zararlı yazılımlardır. Zararlı yazılımlar gerekli siber güvenlik tedbirlerinin alınmadığı sistemlerde ciddi zararlara neden olabilmekte ve hayati sonuçlar yaratabilmektedirler.

4.1.2.2.2 Uygulama ve İnternet Sitelerinde Yer Alan Açıklıklara Yönelik Saldırılar

Bu tip saldırılarda internet uygulamaları ve sitelerinin geliştirilmesi esnasında gerekli güvenli önlemlerinin alınmamasından kaynaklanan açıklıklar kullanılmaktadır. Bu tip saldırıların iç ağa sızma, veri tabanlarında yer alan verilerin çalınması, internet sitelerinin yönetiminin ele geçirilmesi gibi ciddi sonuçları bulunmaktadır. Açık Ağ Uygulama Projesi Kuruluşu (Open Web Application Security Project OWASP) bu tür saldırıların sınıflandırılması ve alınacak önlemlerin belirlenmesi konularında dünya çapında kabul görmüş bir kuruluş olup, yayınlamış olduğu "OWASP Top Ten" açıklık listesi alandaki geçerli web ataklarını içermektedir. Bu önemli listenin açıklamaları Ek-6'da sunulmuştur.

4.1.2.2.3 Oltalama ve Kimlik Avı Saldırıları

Oltalama saldırıları hedef alınan kişinin parolasını, banka hesabını veya kredi kartı bilgilerini ele geçirmek amacıyla kullanılır. Saldırgan tarafından saldırı amacına özel olarak hazırlanan oltalama e-postası gerçek bir kurumdan geliyormuş gibi ya da gerçek bir eposta şeklinde görülür. Hazırlanan e-posta vasıtasıyla kullanıcılar sahte sitelere yönlendirilerek parolalarını girmeleri sağlanır. Bir diğer senaryo da ise epostalara eklenen dosyaların çalıştırılması ile kurbanların bilgisayarları ele geçirilerek saldırganın kontrolü altına girebilir (BGA Security, 2020). Bu tür saldırılar özelikle bilişim alanında yeterli bilgi ve farkındalığa sahip olmayan kullanıcılarda etkin olmaktadır.

4.1.2.2.4 Dağıtık Servis Dışı Bırakma Saldırıları

İnternet sitelerinin, uygulamalarının ya da hizmet ve servislerinin gelen aşırı istekler sonucunda hizmet veremez hale getirilmesi, saldırıları servis dışı bırakma saldırıları olarak tanımlanmaktadır. Servis dışı bırakma saldırıları, tek kaynaktan gelen servis dışı bırakma saldırılarını engelleme günümüzde basit güvenlik tedbirleri ile sağlanabildiği için, dağıtık servis dışı saldırılara evrilerek karmaşık

güvenlik tedbirlerini gerektiren kimi zamanda tüm bu tedbirlere rağmen gerekli başarının sağlanamamasına neden olan siber saldırı türüne dönüşmüştür. Saldırının dağıtık olarak adlandırmasının nedeni dünya genelinde zararlı yazılımlar sayesinde ele geçirilmiş bilgisayarların komuta kontrol merkezinden gönderilen komutlarla hedef sisteme saldırı düzenlemesidir. 2007 yılında Estonya'ya karşı gerçekleştirilen ve Estonya'nın sağlık, bankacılık, e-devlet gibi kritik sistemlerini kullanılamaz hale getiren siber saldırıların arka planında DDoS[11] saldırıları bulunmaktadır (Atasever, Özçelik ve Sağıroğlu, 2019). Gerekli önlemler alınmadığında çok vahim sonuçlarla karşılaşmak kaçınılmazdır.

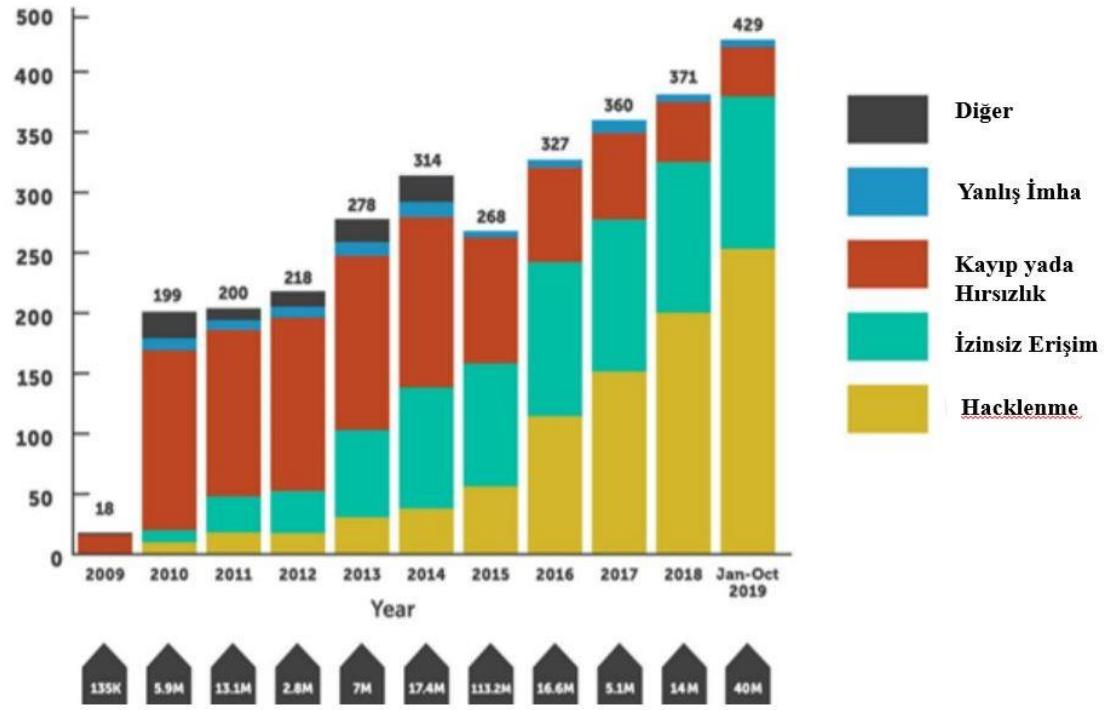
4.1.2.2.5 Veri Hırsızlığı Saldırıları

Veri hırsızlığı saldırısı, bir bilgi sistemine yetkisiz erişim sonucu elde edilen bilgilerin kötü amaçlı kullanım için sistem dışına çıkarılması olarak tanımlanabilir. Bu durum aynı zamanda sistem kullanıcıların kişisel hataları nedeniyle de yaşanmaktadır. Veri hırsızlığına neden olan bilgi güvenliği ihlali, genellikle çok geç anlaşılır ya da kimi durumlarda anlaşılamaz. Son araştırmalara göre ortalama veri ihlali tespit süresi ihlal başlangıcından itibaren 206 gündür. Son 10 yılda yaşanan veri ihlalleri incelendiğinde hacklenme yoluyla veri ihlallerinde ciddi bir artış olduğu gözlenmektedir. Veri işlemek için bilgi sistemlerine olan bağımlılığın artması ve artan bu talebe karşılık yeterli güvenlik tedbirlerinin alınmaması bu oranın arkasındaki temel nedendir (Bknz. Şekil-11 Son 10 Yılın Veri Kaçağı İhlalleri).

2010'lu yılların başında veri ihlalleri bilgi sistem malzemelerinin kaybedilmesi yada hırsızlık gibi fiziksel nedenlerle yaşanırken, yıllar içerisinde hacklenme, izinsiz erişim gibi ağ üzerinden gerçekleştirilen zararlı eylemler nedeniyle yaşanan veri hırsızlığı oranları artış göstermiştir. Veri hırsızlığı saldırısı verinin değerine göre milyar dolarlar seviyesinde maddi kayba neden olabilmektedir.

[11] Distrubuted Denial of Service.

Şekil-11: Son 10 Yılın Veri Kaçağı İhlalleri



Kaynak: (ENISA Data Breach Report, 2020)

4.1.3 Siber Uzayda Güç Mücadelesi: Siber Çatışmalar

Siber alan, küresel güç mücadelesinde önemli bir oyun alanını temsil etmektedir. Uluslararası aktörlerin güç mücadelesi siber alana sirayet etmekte ve siber alan güç mücadelesinin yeni bir cephesi olarak karşımıza çıkmaktadır. Siber alandaki güç mücadelesi, diğer alanlarda yaşanan (ekonomik, askeri, sosyal vb.) güç mücadelelerinden bağımsız olmamakta onlara paralel bir minvalde gerçekleşmektedir. Siber alan bir anlamda küresel politikaların bir uzantısı haline gelmektedir.

Siber alandaki mücadeleyi ele alırken siber savaş kavramını mı yoksa siber çatışma kavramı mı ön planda tutulmalıdır sorunsalı, bu kavramlara uluslararası hukuk normları üzerinden yaklaşımı gerekli kılmaktadır.

Öğretide savaş biri objektif diğeri de sübjektif olmak üzere iki unsur üzerinden tanımlamaktadır. Savaşın bu iki ana unsuru şu şekilde belirtilebilir:

-Taraf devletler arasında silahlı çatışmalar olgusunun varlığı,
-Taraflardan en az birisinin bu silahlı eylemleri savaş niyetiyle gerçekleştirmesi (animus belligerandi) durumlarıdır (Pazarcı, 2013).

Savaşa varmayan, devletlerarası sınırlı nitelikteki silahlı çatışmalar ve eylemler farklı yöntemler üzerinden yürütülebilmektedir. Bir silahlı çatışmanın ya da eylemin savaş olarak değerlendirilmesinde objektif bir ölçüt bulunmamasından dolayı bahse konu eylemleri savaştan ayıran temel ölçüt söz konusu devletlerin niyetidir. Taraf devletlerden hiçbiri bahse konu eylemleri veya çatışmaları savaş amacı ile gerçekleştirilmiş eylem veya çatışma olarak değerlendirmedikleri durumlarda uluslararası hukuk açısından bunlar savaşa varmayan silahlı zorlama yolları ya da silahlı karışma olarak ele alınmaktadır. Çatışan tarafların dışında üçüncü aktörlerin bu durumu savaş olarak ele alması bu çatışmalara hukuksal olarak savaş tanımlaması yapılması için yeterli sayılmamaktadır (Pazarcı, 2013, s. 536).

Savaşı bir çatışmanın varlığı olarak ele alan önermeler devletlerin bu eylemlerindeki amaçlarına önem vermektedirler. Bu anlayışa göre savaş diğer devletin dayanma kapasitesine ortadan kaldırmak ve öne sürülen barış şartlarının kabul ettirilmesine yönelik bir çatışmadır. Sonuç olarak ortada bir kuvvet kullanma faaliyeti ve aynı zamanda kuvvet kullanma faaliyetinin genel bir maksatla yapılması söz konusudur. “Dolayısıyla amacı daha sınırlı, belirli bir amaç olan ve tarafların savaşma niyetine sahip olmadıkları bir çatışma, hukuksal anlamda savaş olmayacaktır” (Ata, 2014, s. 84). Bu çerçevede literatürde siber savaş olarak geçen pek çok durum hukuki açıdan siber çatışma olarak var olmaktadır.

Siber çatışmalarda temel hedef, etki sağlanmak istenen hedef sistemdeki bilgilerin gizliliğini, bütünlüğünü veya kullanılabilirliğini engellemektir. Siber

güvenlik kavramına bilgi güvenliği temelli bir tanımlama getiren bu yaklaşıma göre hedef sistemlerdeki bilgilerin gizliliği “kritik veri kaçağı ihlali” olarak kabul edilirken, bilginin bütünlüğünü veya kullanılabilirliğini bozan etkinlik “siber saldırı” olarak adlandırılır. Bu kapsamda siber çatışma kavramını siber yeteneklerin ulusal amaçları gerçekleştirebilmek için hedefin bilgi teknolojisi sistemlerinin veya ağlarının gizliliğini, bütünlüğünü veya kullanılabilirliğini engellemek için ortaya konan saldırgan eylemler olarak tanımlayabiliriz. (Lin, The Strategic Dimensions of, 2018, s. 21).

Siber çatışmalar pek çok konuda fiziksel çatışmalardan farklılık göstermektedir. Bazı temel farklıkları detaylandıracak olursak şunlar söylenebilir (Lin, 2012, s. 521):

a. Çatışma alanı; Geleneksel konvansiyonel çatışmada (GKÇ devlet tarafından kontrol edilen konvansiyonel silahlarla gerçekleşen askeri faaliyetler) çatışmalar kara, deniz ve hava harekat alanlarında icra edilmektedir ve çatışmaların sınırı konvansiyonel silahların menzilini bazı gayri nizami harp durumları dışında aşmamaktadır. Ancak siber çatışmalarda harekat alanı tüm dünyayı kapsayan siber uzay olup, dünya üzerindeki herhangi bir bilgi sistemi siber saldırıya maruz kalabilmektedir.

b. Hücum savunma dengesi; GKÇ’de saldırgan teknolojiler ve savunma teknolojileri genellikle bir denge halindedir. Örneğin, anti tank füzeleri ne kadar gelişmişse zırh teknolojilerinde benzer bir gelişmişliğe sahiptir. Ancak siber çatışmalarda çatışmanın dengesi saldırgan tarafın lehinedir. Siber çatışmada saldırı doğal olarak savunmadan daha üstündür, çünkü saldırının sadece bir kez başarılı olması gerekirken, savunanın her seferinde başarılı olması gerekmektedir. Konvansiyonel caydırıcılık bir realite iken siber caydırıcılık pek çok durumda geçerli değildir. Dünyanın en gelişmiş siber savunma sistemlerine sahip ülkeler aynı zamanda en çok siber saldırı alan ülkeleridir. Oysaki dünyanın en büyük konvansiyonel güçleri sahip oldukları caydırıcılık nedeniyle konvansiyonel bir saldırı altında değildirler.

c. İlişkilendirme ve Devlet dışı aktörler; GKÇ ülkelerin elinde bulundurduğu varsayılan askeri kuvvetler tarafından yürütülmektedir. Ancak siber çatışmalarda ülkeler evinde geliştirdiği zararlı yazılımı hedef ülke bilgi sistemlerine yönlendiren vatandaşlarını kontrol edemezler. Her ne kadar internet erişim sağlayıcıları vasıtasıyla ülkeler internet trafiğini kontrol etmeye çalışsa da VPN vb. teknolojiler sayesinde bu kontrolleri aşmak mümkündür. Etkili bir zararlı yazılım geliştirme teknik yetkinliğine sahip vatandaşlar için bu kontrolleri aşmak çok daha kolaydır. Kimi durumlarda ise ulus devlet aktörleri siber saldırıların arkasında filli olarak yer almakta istihbarat örgütleri vasıtasıyla hedef ülke sistemlerine saldırıda bulanabilmektedir. Ancak internet protokollerinin zafiyetleri nedeniyle genellikle bu ilişki ortaya net kesin bir şekilde çıkartılamamaktadır.

d. Maliyet; Konvansiyonel harp oldukça maliyetli bir iştir. Ancak siber çatışmalarda kimi durumlarda bu çok düşük maliyetlerle istenen etki sağlanabilir. Ancak bu durum sanılanın aksine her zaman geçerli değildir. Öncelikle siber savunma faaliyeti maliyetli bir iştir ve ciddi insan gücü ve yatırım gerektirmektedir. Ancak tüm emek ve yatırımlara rağmen gerekli güvenlik güncellemelerinin yapılmadığı bir bilgi sisteminin varlığı ya da kolay şifre kullanıcı adı kullanan bir personel, tüm bu savunma sistemlerinin niteliksiz saldırganlarca aşılmasını sağlayabilecektir.

Bu bölümde siber güvenlik kavramının tarihsel gelişimi ve günümüzdeki karşılığı analiz edilmiştir. Analiz sonucunda siber güvenlik kavramının günümüzde askeri, ekonomik, çevre gibi güvenlik sektörlerinde karşılığı olduğu ve siber alanın güvenliğinin sağlanmasının kendi başına bir güvenlik sektörü haline geldiği sonucuna ulaşılmıştır. Araştırmanın bundan sonraki bölümünde “Türkiye’de Siber Güvenlik ve Kriz Yönetimi” konusu ele alınmıştır. Araştırmanın beşinci bölümü olan bu bölümde, içinde bulunduğumuz bölümden elde edilen bulgular çerçevesinde ülkemizdeki siber güvenlik örgütsel yapısı ve uygulamaları açıklanmıştır.

V. BÖLÜM

ARAŞTIRMANIN BULGULARI: TÜRKİYE'DE SİBER GÜVENLİK ve KRİZ YÖNETİMİ

Çalışmanın bu bölümünde ülkemizde siber güvenlik kavramının gelişimi üç aşamada ele alınmıştır. “Kamu kurumlarının bilgi ve iletişim teknolojisi yatırımları arasında eşgüdüm sağlamak, e-Dönüşüm Türkiye Projesi'nin koordinasyonunu yürütmek ve bilgi toplumu olma yolunda atılması gereken adımlara ilişkin stratejileri belirlemek üzere, 2003 yılında DPT bünyesinde kurulmuş olan Bilgi Toplumu Dairesi tarafından 2006-2010 Bilgi Toplumu Stratejisi hazırlanmıştır. Bu önemli gelişme öncesi dönem birinci aşamayı oluşturmuştur. 11/6/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar kurulu kararının üçüncü maddesi gereği, “ulusal siber güvenlik politikalarının, strateji ve eylem planlarının hazırlanması, kamu kurum ve kuruluşlarına ait bilgi ve verilerin güvenliği ile mahremiyetinin güvence altına alınmasını sağlamaya yönelik usul ve esasların hazırlanması” sorumluluğu T.C. Ulaştırma Bakanlığı’na verilmiştir. Bu bağlamda 2006-2012 arası dönem ikinci aşama olarak ele alınmıştır. 2012 ve günümüze kadar olan dönemde üçüncü aşama olarak incelenmiştir. Olası siber güvenlik krizlerine karşı alınan önlemler, krizin yönetimine ilişkin süreçler ve uygulamalar kavramsal çerçevede ele alınmış olan siber güvenlik krizlerinin yönetimi esaslarına göre analiz edilmiştir.

5.1 Türkiye’de Siber Güvenlik

Siber güvenlik kavramının siber uzay kavramı ile birlikte ortaya çıkıp geliştiği daha önce incelenmiştir. Ülkemizdeki siber güvenlik faaliyetleri ele alındığında da bu durum üzerinden hareket etmek bizi tutarlı sonuçlara götürecektir. 1993 yılında internetle tanışan ülkemizde internet ve siber uzayın büyümesi dünya ile parelel bir gelişme göstermiştir. Günümüz verilerine göz atıldığında;

Ülke nüfusunun %74'ü aktif internet kullanıcısıdır, sosyal medya kullanım oranı ise % 64 seviyelerindedir. 2020 yılında bir önceki yıla göre aktif internet kullanıcısı %4, sosyal medya kullanıcı sayısı % 4.2 artış göstermiştir. Aktif internet kullanıcılarının günlük internet kullanımı 7,5 saat dolayındadır. Bu zaman diliminin içinde 3 saatlik bir sosyal medya kullanımı yer almaktadır. Dikkat çekici bir diğer istatistik ise siber uzayın genişlemesinin bir sonucu olarak ortaya çıkan kripto para kullanımındadır. Aktif internet kullanıcıların %10'luk bir kısmı kripto para sahibidir. Ülkede 770.000 evde akıllı ev cihazları mevcuttur. Sosyal medyanın iş maksatlı kullanımı %44 seviyelerindedir (Kemp, 2020).

Yukarıda yer alan verilere göre ülke nüfusunun önemli bir bölümü günün aktif olarak geçirilen saatlerinin neredeyse yarısını siber uzayda geçirmektedir. Ülkemizdeki e-devlet kullanıcı sayısı 51 milyon dolaylarındadır. Siber uzayın hayatın her alanına nüfuz ettiği günümüz Türkiye'si için siber güvenlik kavramı ciddi bir önem arz etmektedir.

5.1.1 2006 Öncesi Türkiye'de Siber Güvenlik

Siber kelimesinin, sibernetik bilimi üzerinden gelişerek günümüze geldiği, daha önceki bölümlerde ele alınmıştır. Ülkemizde bilgi sistemlerinin gelişimi ve siber uzay kavramına dönüşümünden önce sibernetik kavramına olan yaklaşımları irdelemek yararlı olacaktır. Ülkemizde bu alandaki ilk çalışmalar 1960 yılında Tıp fakültelerinde başlamış sonrasında alana ilişkin pek çok çalışma gerçekleştirilmiştir. 1972 yılında konuyu hukuk bilimi açısından ele alan uluslararası bir sempozyum gerçekleştirilmiştir. Bu dönem için sibernetik kavramı insan makine ilişkisi ve gelecekte makine insan kombinasyonları gibi kavramlar üzerinden ele alınmıştır. Aynı zamanda bilgisayarların ortaya çıkarak kısıtlı yaygınlaşması da bu dönemde yaşanmış ve otomasyon sistemlerine yönelik ilgi artış göstermiştir.

Ülkemizde bilgi güvenliğine ilişkin erişilebilen en eski belge Türkiye ve Dünya Bankası iş birliği ile hazırlanan "Bilişim ve Ekonomik Modernizasyon Raporu" 'dur

(Güngör M. , 2015, s. 92). Bu rapora göre Türkiye'nin Türkiye'de bilgi toplumuna dönüşüm sürecinde ortaya çıkacak temel ihtiyaçlara ilişkin tespitlere yer verilmiştir. Raporda bu dönemde Ülkemizdeki; bilgisayar kullanımı, yazılım pazarı, bilgi ekonomisinde insan kaynağı, iletişim ağları, bilişim güvenliği alanındaki yasal altyapı gibi konulara açıklık getirilmiştir. Raporda yer alan eylem planlarında bilgi teknolojilerinden kaynaklanabilecek olan güvenlik risklerine dikkat çekilmekte ve kullanıcıların bu risklere karşı korunması için yasal düzenlemelerin gerekliliğine verilmektedir.

"7'nci beş yıllık plan 1996-2000", 17 Temmuz 1995 tarihinde onaylanmıştır. Bu plan dahilinde enformatik çalışma grubu oluşturulmuştur. Bu çalışma gurubunun çalışmaları kamu kurumları, sanayi ve akademik çevrelerinden kişilerin katılımıyla geniş bir alana yayılmış ve saha çalışmalarıyla desteklenmiştir. Sonucunda, "Türkiye Ulusal Enformasyon Altyapı Anaplanı" ortaya çıkmıştır. Bu planda ağ güvenliği ve bilgi güvenliğine ilişkin tespitler yer almaktadır. Ağ güvenliği ürünlerinin artık bir realite olduğu ve bu alanın gelişmeye çok uygun olduğu, bu alanda yatırım yapılması gerekliliği öne sürülmüştür. Geleceğe yönelik planlamalarda, Ulusal Bilgi Güvenliği Kurulu'nun kurulması öngörülmüştür. Ancak o günün Türkiye'sinde, hane halkı internet kullanımının %1,5 dolaylarında olması ve bu oranın büyük bölümünün üst gelir grubuna üye haneleri kapsaması gerçeği vurgulanarak topluma yayılmamış bir bilgi sistem ağı olmadan bu kurulun varlığına gerek olmadığı, gerçek sorunun internete erişimdeki adaletsizliğin ortadan kaldırılması olduğu vurgulanmıştır (Türkiye Ulusal Enformasyon Ulusal Altyapı Anaplanı, 1999).

2000'li yılların başındaki Türkiye için temel sorun bilgisayar ağlarının güvenliğinden ziyade yeni bir suç alanı olan internetin bilinmezliği ve beraberinde getirdiği yeni hukuki sorunlardır. Bu sorun Emniyet Genel Müdürlüğü Organize Suçlar Daire Başkanlığının 2000 yılı raporunda açıkça gözlenmektedir (EGM, 2000, s. 92). İlgili raporda internet yeni bir suç alanı olarak tanımlanmaktadır. Bu dönemde internetin yaygınlaşmasından önce de bilgisayar kullanımındaki artışa paralel olarak bilgisayar suçları olarak nitelenen bazı davranış şekilleri ortaya

çıkmış ve yasa koyucu tarafından düzenlenerek yaptırıma bağlanmıştır (Özbek, 2001, s. 107). TCK'na 1991 yılında 3756 sayılı yasa ile eklenen m.525a, m.525b, m.525c ve m.525d bilgisayar programlarını hukuka aykırı olarak ele geçirme, bilgisayar sisteminde yer alan verileri tahrip etme, silme, değiştirme, bilgisayar sistemini kullanarak haksız çıkar sağlama ve sahtekarlık gibi fiilleri suç haline getirmiştir.

Sivil toplum açısından konuya yaklaşıldığında hacker kavramı daha internetin ilk günlerinden itibaren özelikle gençler arasında bilinen ve sempati duyulan bir kavramdır. Bu dönemde günümüzde de popüler olan exploit, açıklık gibi siber güvenlik kavramları bilinir durumdadır (İnternetin Karanlık Yüzü, 1997). 1995 yılından itibaren düzenli olarak Türkiye İnternet Kullanıcıları konferansları düzenlenmiş ve ağ, internet güvenliği kavramları bu konferanslarda ele alınmıştır (Akgül, 1996). İnternetle beraber gündelik hayata çevrimiçi sohbet programları girmeye başlamış ve kullanıcılar kendilerine internetin bu ortamında yeni bir kimlik yaratmaya başlamışlardı. Sosyal medyanın ilk pratikleri bu platformlarda yaşanmaktaydı (Bayar, 1999). İnternet ortamının bu kontrolsüzlüğü evinde internet olan aileler içerik filtreleme gibi siber güvenlik ürünlerini kullanmaya başlamışlardır (Siber Bebek Bakıcısı, 1999).

2000 yılı sonrasında kamu siber güvenlik çalışmaları daha görünür bir hal almıştır. 1997 yılında TUBITAK çatısı altında kurulan "Ağ Güvenliği Grubu" tarafından kapsamlı bir test laboratuvarı kurulmuştur. "Laboratuvar ortamında Microsoft ve açık kaynak kodlu işletim sistemleri, bunların üzerinde çalışan e-posta sunucu, veri tabanları gibi popüler uygulamalar, aktif ağ cihaz ve kutuları, saldırı tespit sistemleri gibi savunma ürünleri güvenlik bakış açısı ile değerlendirildi." 2001 yılında Genelkurmay Başkanlığı desteğiyle ülkemizin ve o dönem için dünyanın sayılı laboratuvarları arasında yer alan "Ortak Kriterler Laboratuvarı" kurulmuştur. Burada, kripto cihazlarının gereksinimlerinin karşılanıp karşılanmadığına yönelik gerçekleştirilen COMSEC (Haberleşme Güvenliği) testleri icra edilmeye başlanmıştır (TUBİTAK BİLGEM, 2020).

5.1.2 2006-2012 Dönemi

2006 yılı, ülkemizde siber güvenliğin gelişiminde önemli bir dönüm noktasıdır. E-Dönüşüm Türkiye Projesi'nin koordinasyonunu yürütmek, ve bilgi toplumu olma yolunda atılması gereken adımlara ilişkin stratejileri belirlemek üzere 2003 yılında DPT bünyesinde kurulmuş olan Bilgi Toplumu Dairesi tarafından hazırlanan 2006-2010 Bilgi Toplumu Stratejisi bu yıl itibari ile devreye girmiştir. Bilgi Toplumu Stratejisi Eylem Planı'nın 88. maddesinde yer alan Ulusal Bilgi Sistemleri Güvenliği Programı (UBGP) gereği yapılması gereken faaliyetler şu şekilde belirtilmiştir:

"Siber alemdeki güvenlik tehditlerini sürekli olarak takip edecek, uyarılar yayınlayacak, bu risklere karşı ne şekilde tedbir alınabileceğine dair bilgilendirme yapacak, risklerin ortaya çıkması durumunda karşı tedbirleri koordine edebilecek bir "bilgisayar olaylarına acil müdahale merkezi (CERT) kurulacaktır. Kamu kurumları için gerekli minimum güvenlik seviyeleri kurum ve yapılan işlem bazında tanımlanacak, kurumlar tarafından kullanılan sistem, yazılım ve ağların güvenlik seviyeleri tespit edilecek ve eksikliklerin giderilmesi yönünde öneriler oluşturulacaktır"

Bu programdan sorumlu makam olarak TUBİTAK belirlenmiş ve ulusal siber güvenliğin sağlanmasından asıl sorumlu kuruluş olarak bu görevini 2012/3842 sayılı Bakanlar Kurulu Kararı ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na devredene kadar sürdürmüştür.

TUBITAK tarafından UBGP kapsamında "ülkemizin bilgi sistem güvenliği ile ilgili bilgi ihtiyacını karşılamak ve kamu bilgi sistemlerinin güvenliğinin sağlanması ile ilgili etkin önlemler alınmasına ön ayak olmak amacıyla Türkiye Bilgisayar Olayları Müdahale Ekibi Koordinasyon Merkezi (TR-BOME)" faaliyete geçirilmiştir. Yine bu faaliyet kapsamında kamu kurumları içerisinde kurum BOME'leri faaliyete geçmiştir. BOME faaliyetleri Tablo-3'te sunulmuştur.

Tablo-2: BOME Faaliyetleri

Tepki Servisleri	Önleyici Servisler	Güvenlik Kalite Yönetim Servisleri
• Alarm ve Uyarılar	• Duyuru	• Risk Analizi
• Olay Müdahale	• Teknoloji Takibi	• İş Sürekliliği ve Felaket Kurtarma
o Olay Analizi	• Güvenlik Denetleme ve Değerlendirme	
o Olay Yerinde Müdahale		• Güvenlik Danışmanlığı
o Olay Müdahale Destek	• Güvenlik Araçlarının, Uygulamalarının ve Altyapısının Yapılandırılması ve Bakımı	• Bilinçlendirme
• Açıklık Müdahale		• Eğitim
o Açıklık Analizi		• Ürün Değerlendirme ve Sertifikasyonu
o Açıklık Müdahale		
o Açıklık Müdahale Koordinasyonu	• Güvenlik Araçlarının Geliştirilmesi	
• Saldırı Araçları Müdahale	• Saldırı Tespit Servisleri	
o Saldırı Araçları Analizi	• Güvenlik ile İlgili Bilgi Yayınlanması	
o Saldırı Araçları Müdahale		
o Saldırı Araçları Müdahale Koordinasyonu		

Kaynak: (Türkiye 2008 Yılı BOME Faaliyetleri Raporu, 2008).

1 Haziran 2006 tarihinde yürürlüğe giren 5237 sayılı yeni Türk Ceza Kanunu" da eski kanunda yer almayan yeni düzenlemeler yapılarak bilişim suçlarını tekrar düzenlemiştir. Yeni Türk Ceza Kanunu'nda bilişim güvenliği ile ilgili olarak bilişim sistemine girme, sistemi engelleme, bozma, yok etme veya değiştirme (m.243-245) gibi eski kanunda yer alan bilgisayar suçlarına ek olarak;

"banka veya kredi kartlarının kötüye kullanılması, nitelikli hırsızlık, dolandırıcılık, kişisel verilerin kaydedilmesi ve hukuka aykırı olarak verme veya ele geçirme , kişisel verileri yok etme, haberleşmenin engellenmesi, hakaret, haberleşmenin gizliliğini ihlal, kişiler arasındaki konuşmanın dinlenmesi ve kayda alınması, özel hayatın gizliliğini ihlal, müstehcenlik " (Güngör M. , 2015, s. 99) gibi suçların bilgi sistemleri vasıtasıyla işlenebileceği ve bilişim suçu olarak kabul edilebileceği belirtilmiştir.

10 Kasım 2008'de yayımlanan "Elektronik Haberleşme Kanununda" bilgi güvenliği temel ilkeler arasında sayılmış ve Kanunun 4'üncü maddesinin (l) numaralı bendinde elektronik haberleşme hizmetinin sunumu ile bu alanda yapılacak ikincil düzenlemelerde bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi hüküm altına alınmıştır (Güngör M. , 2015, s. 101). Diğer yandan aynı Kanunun 12'nci maddesinde de işletmecilere bilgi güvenliğinin temel öğeleri olan haberleşmede gizliliğin sağlanması, kesintisiz hizmet sunumu ve şebeke bütünlüğünün idame ettirilmesi görevleri verilmiştir.

4 Mayıs 2007 tarihinde yayımlanan "5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" ile içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usuller düzenlenmiştir. Bu kanun zaman içerisinde değişikliklere uğrayarak günümüzde internet ağındaki faaliyetleri düzenleyen önemli bir belge haline gelmiştir.

5.1.3 2012 Sonrası Gelişmeler ve Günümüz Türkiye'si

20 Ekim 2012 tarihli ve 28447 sayılı resmi gazetede yayımlanarak yürürlüğe giren 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin" Bakanlar Kurulu Kararı ile birlikte siber güvenlik alanına ilişkin çeşitli düzenlemeler yapılmış ve geleceğe ilişkin planlamalara yer verilmiştir. Bu kararın üçüncü maddesi gereği, ulusal siber güvenlik politikalarının, strateji ve eylem planlarının hazırlanması, kamu kurum ve kuruluşlarına ait bilgi ve verilerin güvenliği ile mahremiyetinin güvence altına alınmasını sağlamaya yönelik usul ve esasların hazırlaması sorumluluğu T.C. Ulaştırma Bakanlığı'na verilmiştir. Bu karar neticesinde siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla Siber Güvenlik Kurulu kurulmuştur. Kurul; Ulaştırma, Denizcilik ve Haberleşme

Bakanı'nın başkanlığında (Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı, 2012):

- "Dışişleri Bakanlığı Müsteşarı,
- İçişleri Bakanlığı Müsteşarı,
- Milli Savunma Bakanlığı Müsteşarı,
- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Müsteşarı,
- Kamu Düzeni ve Güvenliği Müsteşarı,
- Milli İstihbarat Teşkilatı Müsteşarı,
- Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı,
- Bilgi Teknolojileri ve İletişim Kurumu Başkanı,
- Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı,
- Mali Suçları Araştırma Kurulu Başkanı,
- Telekomünikasyon İletişim Başkanı ile
- Ulaştırma, Denizcilik ve Haberleşme Bakanı"nca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşmaktadır.

Kurulun görevleri ise şu şekilde belirlenmiştir:

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

Adı geçen bakanlar kurulu kararının üçüncü maddesi gereği ulusal siber güvenlik politikalarının, strateji ve eylem planlarının hazırlanması, kamu kurum ve kuruluşlarına ait bilgi ve verilerin güvenliği ile mahremiyetinin güvence altına alınmasını sağlamaya yönelik usul ve esasların hazırlaması sorumluluğu T.C. Ulaştırma Bakanlığı'na verilmiştir. Böylece Ulusal siber güvenlik sorumluluğu TUBİTAK'tan T.C. Ulaştırma ve Altyapı Bakanlığı'na geçmiştir. 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun 5 inci maddesinin birinci fıkrasına eklenen h bendi ile Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na

siber güvenlik alanında aşağıdaki görev ve yetkiler verilmiştir (10377 Sayılı Elektronik Haberleşme Kanunu, Md. 6):

- Ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek
- Kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirlemek, eylem planlarını hazırlamak,
- İlgili faaliyetlerin koordinasyonunu sağlamak, kritik altyapılar ile ait oldukları kurumları ve konumları belirlemek, gerekli müdahale merkezlerini kurmak, kurdurmak ve denetlemek,
- Her türlü siber müdahale aracının ve millî çözümlerin üretilmesi ve geliştirilmesi amacı ile çalışmalar yapmak, yaptırmak ve bunları teşvik etmek ve siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek,
- Siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlamak.

Ulaştırma bakanlığı koordinesinde icra edilen siber güvenlik faaliyetlerini açıklamadan önce, ilgili bakanlık teşkilatında yer alan ve ülkemiz siber güvenlik yönetiminde önemli bir aktör olan Bilgi Teknolojileri Kurumunun (BTK) görev ve sorumlulukları ile faaliyet alanlarını kısaca açıklamak konu bütünlüğü açısından faydalı olacaktır. Elektronik haberleşme kanununda yukarıda adı geçen düzenleme esnasında BTK içinde düzenleme yapılarak aşağıda yer alan değişikle birlikte siber güvenlik için ek görevler verilmiştir. BTK görev ve yetkileri şu şekilde açıklanmıştır:

> Siber güvenlik ve internet alan adları konularında Bakanlar Kurulu, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri Telekomünikasyon İletişim Başkanlığı veya diğer birimleri marifetiyle yerine getirmek (10377 Sayılı Elektronik Haberleşme Kanunu, Md. 6).

5.1.3.1 Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı ve Kapsamında İcra Edilen Siber Güvenlik Faaliyetleri

Siber Güvenlik Kurulu ilk toplantısı, 21/12/2012 tarihinde; Ulaştırma, Denizcilik ve Haberleşme Bakanı Binali Yıldırım'ın başkanlığında yapılmıştır. Söz konusu Siber Güvenlik Kurulu kararında “Siber Güvenlik Kurulunun Görevleri, Çalışma Usul ve Esasları Yönergesi” ve “Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı” kabul edilmiştir. İlgili strateji belgesi ve eylem planında kamu

kurumların bilgi sistemlerine olan bağımlılığının her geçen gün artığı, bu nedenle bahse konu hızlı gelişime uygun siber güvenlik faaliyetlerinin icra edilmesi gerekliliği ortaya konmuştur. Bilgi ve iletişim teknolojilerin güvenliğinin ulusal bir güvenlik meselesi olduğu, söz konusu sistemlerdeki güvenlik zafiyetleri sonucu oluşabilecek siber güvenlik olaylarının can kaybına, büyük ölçekli ekonomik zarara, kamu düzeninin bozulmasına ve/veya ulusal güvenliğin ihlaline neden olabileceği belirtilmiştir.

5.1.3.1.1 USOM, Kamu ve Sektörel SOME'lerin Kurulumu ve İşleyişi

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın "Ulusal Siber Olaylara Müdahale Merkezinin (USOM) Kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) Oluşturulması" başlıklı 4. eylem maddesi uyarınca, Telekomünikasyon İletişim Başkanlığı (TİB) bünyesinde USOM kurulmuştur. USOM'un ulusal siber güvenlik faaliyetleri içerisindeki temel fonksiyonu, ulusal ve uluslararası seviyede siber ortamda ortaya çıkan tehditler ile ilgili kendisine ulaştırılan ihbarları da değerlendirerek, söz konusu tehditlerin tespit ve bertaraf edilmesi için Kamu Kurumları ve özel kişiler ile koordinasyonunu sağlamak olarak belirtilmiştir.

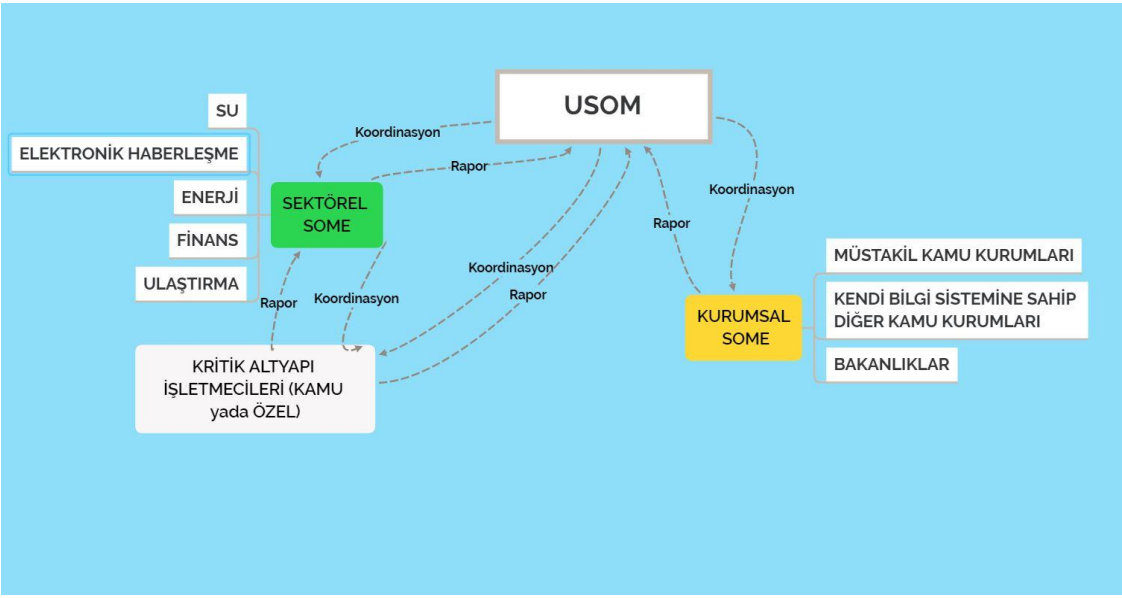
İlgili eylem planı gereği "siber ortamda ortaya çıkan tehditlerin hızla belirlenmesi, yaşanabilecek olayların etkilerini azaltmaya veya ortadan kaldırmaya yönelik önlemlerin geliştirilmesi ve paylaşılması için ulusal düzeyde etkin bir şekilde çalışacak Siber Olaylara Müdahale Organizasyonu" oluşturularak Türkiye'deki kurum ve kuruluşların siber güvenlik olaylarına müdahale yeteneği kazanması hedeflenmiştir. Bu kapsamda Ülkemizi etkileyebilecek tehditlere karşı 11 Kasım 2013 tarihli resmi gazete yayımlanan "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ" gereği kurumsal ve sektörel SOME'lerin nasıl kurulacağı, faaliyet alanları ve işletme esasları belirlenmiştir.[12]

[12] Bu tebliğ çevresinde belirlenen, kurumsal SOME'lerin görev ve sorumlukları Ek-7'de sunulmuştur.

Yukarıda belirtildiği üzere kurumsal SOME'ler kendi kurumlarındaki bilgi sistemlerinin güvenliğini mevcut standart ve mevzuatlara göre sorumluluğunu üstlenmişlerdir. Böylece kamu genelinde her kurumun siber güvenlik yaklaşımı ve seviyesi gerek teknik gerekse idari anlamda belirli bir standarda bağlanmıştır. Siber olayların siber suç boyutu gözetilerek SOME'lerin gerektiğinde kolluk kuvvetleri ile birlikte hareket etmesi sağlanmıştır. Yeni çıkan siber tehditlere karşı bir tehdit istihbarat paylaşımı ağı oluşturularak kamu genelinde mevcut tehditlere karşı koordineli olarak önlem alınmasına ilişkin bir organizasyon oluşturulmuştur.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı gereği Kritik altyapı sektörlerine özel sektörel SOME'lerin kurulması öngörülmüştür. Bu kapsamda kurumsal SOME'ler kurulurken benzer bir yapı, görev ve fonksiyonlara sahip kritik altyapı sekörlerine yönelik sektörel SOME'ler kurulmuştur. Sektörel ve Kurumsal SOME'lerin USOM ile olan bağlantı ve ilişikleri Şekil-12'de sunulmuştur.

Şekil-12: USOM, Sektörel SOME ve Kurumsal SOME İlişkisi



Kaynak: (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014).

5.1.3.1.2 Kritik Altyapı Sektörlerinin Siber Güvenliğinin Sağlanması

Kritik altyapı sektörlerinin siber güvenliğinin sağlanması eylem planının önemli hedefleri arasında yer almaktadır. Bu kapsamda Siber Güvenlik Kurulu tarafından ülkemizin kritik altyapı sektörleri "Ulaştırma, Enerji, Elektronik Haberleşme, Finans, Su Yönetimi, Kritik Kamu Hizmetleri" olarak belirlenmiştir. Tablo-4'te sunulan Kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlara çeşitli görevler verilmiştir. Adı geçen kurumlar kendi sektörlerindeki risklere özel risk analizi yöntemlerini belirleme sorumluluğu verilmiştir. Diğer görev ve sorumluluk ise; Sektörel acil eylem planlarının gereksinimlerinin belirlenmesi, Sektörel güvenlik önlemlerinin belirlenmesi ve uygulanması, Sektörel iş sürekliliği planlarının gereksinimlerinin belirlenmesi ve uygulanması şeklinde belirlenmiştir.

Tablo-3: Kritik Sektörleri Denetlemek ve Düzenlemekle Sorumlu Kurumlar

Kritik Altyapı	**Kurum**
Enerji	EPDK
Elektronik Haberleşme	BTK
Finans	SPK, BDDK
Su Yönetimi	Orman ve Su İşleri Bakanlığı
Kritik Kamu Hizmetleri	"İç İşleri, Adalet, Maliye, Çevre ve Şehircilik, Çalışma ve Sosyal Güvenlik, Gıda Tarım ve Hayvancılık, Sağlık Bakanlıkları"
Ulaştırma	"Karayolu Düzenleme Genel Müdürlüğü, Demiryolu Düzenleme Genel Müdürlüğü, Deniz ve İç sular Düzenleme Genel Müdürlüğü, Sivil Havacılık Genel Müdürlüğü, Tehlikeli Mal ve Kombine Taşımacılık Düzenleme Genel Müdürlüğü"

5.1.3.1.3 Diğer Hedefler ve Faaliyetler

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı gereği Siber Güvenlik Kurulunun faaliyete geçmesi, USOM'un kurulumu ve kritik altyapı güvenliğine ek olarak aşağıda sunulan konu başlıklarına ilişkin planlamalar ve öngörüler mevcuttur. Ancak bu hedef ve planlamalar 2016-2019 Ulusal Siber Güvenlik Stratejisi ile birlikte güncellenerek günümüzdeki mevcut yapısına ulaştığı için ayrı bir başlık olarak 2016-2019 Ulusal Siber Güvenlik Strateji başlığı altında değerlendirilmiştir. 2013-2014 Eylem planındaki diğer konu başlıkları ise şu şekildedir:

- Siber güvenlik konusunda mevzuat çalışmalarının yapılması
- Siber olayların delillendirilmesi
- Kamu Bilgi Güvenliği Programı ve
- Siber güvenlik eğitim altyapısının güçlendirilmesi şeklinde belirlenmiştir.

5.1.3.2 2016-2019 Ulusal Siber Güvenlik Stratejisi

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

gerçekleştirmesi gereken eylemler belirlenmiştir (2016-2019 Ulusal Siber Güvenlik Stratejisi). Bir önceki strateji planının eylem planı kamuoyu ile paylaşılırken 2016-19 Strateji Planının eylem planı ise paylaşılmamıştır. Strateji belgesi kapsamında belirlenen amaçların mevcut durumunun analizi yapılarak kamu ve özel sektörde ilgili amaçlara ilişkin gerçekleştirilen siber güvenlik faaliyetlerinin analizi yapılmıştır.

5.1.3.2.1 Kritik Altyapıların Korunması

Bir önceki strateji dokümanında olduğu gibi 2016-2019 Strateji Planında da kritik altyapı güvenliğine önem verilmiştir. T.C. Ulaştırma Bakanlığı tarafından TUBITAK'a "Kritik Altyapı Bilgi Sistemleri için Asgari Güvenlik Önlemleri Dokümanı" hazırlatılmıştır. Bu kapsamda ilgili dokümanda kritik altyapılar için asgari güvenlik kriterleri belirlenmiştir. Kritik altyapı güvenliği ilkelerine uyulup uyulmadığının kontrolünün bağlı oldukları düzenleyici kurumlar[13] tarafından denetlenmesi amaçlanmıştır.

5902 sayılı kanun gereğince; afet ve acil durumlar ile sivil savunmaya ilişkin hizmetlerin ülke düzeyinde etkin bir şekilde gerçekleştirilmesi için gerekli önlemlerin alınması ve olayların meydana gelmesinden önce hazırlık ve zarar azaltma, olay sırasında yapılacak müdahale ve olay sonrasında

[13] Kritik Altyapıları Düzenleyici ve Denetleyici Kurumlar şu şekildedir:

> "Bankacılık Düzenleme ve Denetleme Kurumu (BDDK)
> Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı (BTK)
> Enerji Piyasası Düzenleme Kurumu Başkanlığı (EPDK)
> Hâkimler ve Savcılar Yüksek Kurulu Başkanlığı (HSYK)
> İstanbul Tahkim Merkezi Başkanlığı
> Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumu Başkanlığı
> Kamu İhale Kurumu Başkanlığı (KİK)
> Radyo ve Televizyon Üst Kurulu Başkanlığı (RTÜK)
> Rekabet Kurumu Başkanlığı
> Şeker Kurumu Başkanlığı
> Sermaye Piyasası Kurulu Başkanlığı (SPK)
> Türkiye Cumhuriyeti Merkez Bankası Başkanlığı (TCMB)
> Tütün ve Alkol Piyasası Düzenleme Kurumu Başkanlığı (TAPDK)
> Yüksek Seçim Kurulu Başkanlığı (YSK)
> Yükseköğretim Kurulu Başkanlığı (YÖK)"

gerçekleştirilecek iyileştirme çalışmalarını yürüten kurum ve kuruluşlar arasında koordinasyonun sağlanmasından ve bu konularda politikaların üretilmesinden, uygulanmasından AFAD sorumlu kılınmıştır.

AFAD'ın yukarıda sayılan yetki ve görevleri kapsamında, kurum ve kuruluşların koordinasyonu ve teknolojik afetlerin etkin yönetimi amacıyla "Kritik Altyapıların Korunması Yol Haritası Belgesi" hazırlaması ihtiyacı ortaya çıkmış ve bu belge sadece AFAD tarafından değil aynı zamanda diğer kurum, kuruluşlar ve Türkiye çapındaki faydalanıcı grupların yetkililerinin de katılımıyla hazırlanmıştır.

İlgili yol haritasında AFAD kendisini kritik altyapılara yönelik Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı çerçevesinde kritik altyapılardan sorumlu kurumların ve konu ile ilgisi olan diğer kurumların koordinasyonunun da yetkili kurum olarak konumlandırmaktadır. AFAD siber tehditleri insan kaynaklı tehditler kapsamında terörist eylemler kategorisinde değerlendirmektedir. Siber tehditler teknolojik afetler kapsamında değerlendirilmekte ve siber güvenlik kaynaklı acil olaylar siber tehditler ışığında değerlendirilerek "haberleşme" kritik altyapısına yönelik bir tehdit olarak algılanmaktadır. AFAD'ın ulusal çapta bir siber güvenlik krizinin yönetimine ilişkin ne gibi faaliyetleri icra edeceğine ilişkin somut bilgiler yer almamaktadır. 2019-2023 AFAD Stratejik Planı incelendiğinde 2014 yılında belirlenmiş olan kritik altyapı güvenliğine risk azaltma ve yönetimi kapsamındaki yaklaşıma yönelik somut bir hedef tespit edilememiştir. Yine aynı belge de siber tehditler ve yönetimi, olası etkilerine yönelik bir planlama bulunmamaktadır. AFAD projeleri kapsamında siber güvenlik kaynaklı kriz durumlarının yönetimine ilişkin bir faaliyet bulunmamaktadır.

5.1.3.2.2 Siber Güvenlik Alanında Denetim Yaklaşımını da İçeren Uluslararası Standartlara Uygun Mevzuatın Oluşturulması Çalışmaları

2012 sonrası dönemde ülkemizde siber güvenlik mevzuatının düzenlenmesine yönelik önemli gelişmeler yaşanmıştır. 2012 öncesi dönemde siber alanın

düzenlenmesine yönelik çıkarılan kanunlarda değişiklikler yapılarak güncel sorunlara çözüm aranmıştır. Daha öncede incelendiği üzere Elektronik haberleşme kanununda düzenleme yapılarak ulusal siber güvenliğin sağlanmasına yönelik gerekli faaliyetlerin icrası ve koordinasyonu görevi T.C. Ulaştırma Bakanlığı ve BTK'ya verilmiştir. Cumhurbaşkanlığı hükümet sistemine geçişle beraber Siber Güvenlik Kurulu yapısında Cumhurbaşkanınca değişiklik yapılmasının önü açılarak ilgili kanunda siber güvenlik kurulu cumhurbaşkanınca belirlenen kurul olarak değiştirilmiştir. Ancak cumhurbaşkanlığınca güncel olarak ayrıca açıklanmış bir kurul bulunmamaktadır.

4 Mayıs 2007 tarihinde yürürlüğe giren "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun", internetin kullanımına ilişkin mevcut mevzuattaki en kapsamlı ve belirleyici kanundur. Zaman içerisinde internet ortamına ilişkin tedbirler bu kanun üzerinde yapılan değişikliklerle sağlanmıştır. 6 Şubat 2014 tarihinde yapılan değişikle erişimin engellenmesi kavramına kanunda açıklık getirilmiştir. İlgili değişikle erişimin engellenmesi kavramı, "Alan adından erişimin engellenmesi, IP adresinden erişimin engellenmesi, içeriğe (URL) erişimin engellenmesi ve benzeri yöntemler kullanılarak erişimin engellenmesi" olarak belirlenerek geniş bir tanımlama yapılmıştır. Kanunun ilk halinde IP adresi gibi daha teknik bir kapsam belirlenmemiş daha çok alan adlarının erişimi üzerinde durulmuştur. Teknik detayların artırılması, erişime engellenecek sistemlerin kapsamını da doğal olarak artırmıştır. Aynı tarihte gerçekleştirilen bir değişiklik ise içerik sahiplerine, içeriğe yönelik şikayet ve içeriğin kaldırılmasına ilişkin vatandaşların e-posta yoluyla da başvuru yapabilmeleri ve bu başvurunun resmi başvuru kapsamında değerlendirilmesi konusu eklenerek vatandaşların özel hayatının gizliliğinin ihlaline yönelik alabileceği önlem ve tedbirler hızlandırılmıştır. Aynı değişiklikler kapsamında yer sağlayıcılarına ek yükümlük getirilerek kanunda belirtilen yollar vasıtasıyla kendilerine bildirilen zararlı içerikleri sunucular üzerinden kaldırma yükümlülüğü getirilmiştir. Kanun toplu erişim sağlayıcılarına da çeşitli zorunluluklar getirmiştir. Yapılan değişikle beraber toplu kullanım sağlayıcılarına belirlenen müeyyideleri yerine getirmedikleri

takdirde mülki amir tarafından cezai işlem uygulanabileceği hükmü eklenmiştir. Kanunun ilk halinde BTK başkanının erişimi engelleme yetkisi yokken yapılan değişiklerle BTK başkanının bazı durumlarda resen erişimi engelleme kararı verebileceği hükmü eklenmiştir. Bu hüküm şu şekildedir:

> "Yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması sebeplerinden bir veya bir kaçına bağlı olarak hâkim veya gecikmesinde sakınca bulunan hâllerde, Cumhurbaşkanlığı veya millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması ile ilgili bakanlıkların talebi üzerine Başkan tarafından internet ortamında yer alan yayınla ilgili olarak içeriğin çıkarılması ve/veya erişimin engellenmesi kararı verilebilir." (Madde 8/A- (Ek: 27/3/2015-6639/29 md.).

2020 yılında Sosyal medya kuruluşlarına yönelik getirilen yeni yaptırımlar[14], ülke gündeminde kendisine sıklıkla yer bulmuş ve pek çok platformda tartışılmıştır. Sosyal medya yasası olarak adlandırılan bu değişikler, 5651 sayılı yasada yapılarak, hükme bağlanmıştır. Sosyal medya yasası gibi ayrı bir yasa bulunmamakta tüm bu düzenlemeler 5651 sayılı kanun vasıtasıyla gerçekleştirilmektedir. İlgili değişikle beraber uluslararası sosyal medya uygulamalarını yöneten şirketlerin Türkiye'de resmi temsilci bulundurması zorunluluğu getirilmiştir.

24 Mart 2016 tarihinde kişisel verilerin işlenmesinde "başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek amacıyla" "Kişisel Verilerin Korunması Kanunu" yürürlüğe girmiştir.

---

[14] EK MADDE 4 – (Ek:29/7/2020-7253/6 md.)
"Türkiye'den günlük erişimi bir milyondan fazla olan yurt dışı kaynaklı sosyal ağ sağlayıcı; Kurum, Birlik, adli veya idari makamlarca gönderilecek tebligat, bildirim veya taleplerin gereğinin yerine getirilmesi ve kişiler tarafından bu Kanun kapsamında yapılacak başvuruların cevaplandırılması ve bu Kanun kapsamındaki diğer yükümlülüklerin yerine getirilmesini temin için yetkili en az bir kişiyi Türkiye'de temsilci olarak belirler ve bu kişinin iletişim bilgilerine kolayca görülebilecek ve doğrudan erişilebilecek şekilde internet sitesinde yer verir. Sosyal ağ sağlayıcı bu kişinin kimlik ve iletişim bilgilerini Kuruma bildirmekle yükümlüdür. Temsilcinin gerçek kişi olması hâlinde Türk vatandaşı olması zorunludur…" (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,2020).

Bu kanun gereği kişisel veriler aşağıda yer alan şartlar neticesinde bilişim sistemlerinde işlenebilecektir. Bu şartlar şunlardır;

“Hukuka ve dürüstlük kurallarına uygun olma.
Doğru ve gerektiğinde güncel olma.
Belirli, açık ve meşru amaçlar için işlenme.
İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza
edilme” (Kişisel Verilerin Korunması Kanunu, 2016).

Cumhurbaşkanlığı hükümet sistemine geçişle birlikte bilginin dijital ortamlara taşınması, bilgiye erişimin kolaylaşması, altyapıların dijital hale gelmesi ve bilgi yönetim sistemlerinin yaygın olarak kullanılması, ciddi güvenlik risklerini beraberinde getirmektedir. Karşılaşılan güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla bir dizi tedbiri içeren “2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi” yayımlanmıştır. “Güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla ulusal ve uluslararası standartlar ve bilgi güvenliği kriterleri çerçevesinde, kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerde uygulanmak üzere farklı güvenlik seviyeleri içeren “Bilgi ve İletişim Güvenliği Rehberi” Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı koordinasyonunda, ilgili kamu kurum ve kuruluşları tarafından gereken katkı sağlanarak hazırlanması” öngörülmüştür. İlgili rehber 24 Temmuz 2020 tarihinde yayımlanmıştır. Rehber kurumsal siber güvenlik faaliyetlerinin yürütülmesine ilişkin pek çok idari ve teknik düzenlemeyi içermektedir. İlgili cumhurbaşkanlığı genelgesi gereği Tüm kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerde yeni kurulacak bilgi sistemlerinde, Rehberde yer verilen usul ve esaslara uyulması zorunludur. Rehberde yer alan düzenlemeler ileride daha detaylı olarak incelenmiştir.

5.1.3.2.3 Güvenli Kamu-Net Ağının Kurulması

Kamu kurum ve kuruluşlarının daha güvenli bir ağ üzerinden haberleşmesine yönelik gerçekleştirilen çalışmalar kapsamında kurumlar arası internete açık olmayan gerekli güvenlik gereksinimleri kapsayan bir kamu ağı kurulması kararlaştırılmış, bu maksatla Kamu Sanal Ağı (KamuNet) kurulmasına karar verilmiştir. (Kamu Kurum ve Kuruluşlarının KamuNet'e Dahil Edilmesi, 2016). "KamuNet ağına bağlanma ve KamuNet ağının denetimine ilişkin usul ve esaslar hakkında tebliğ" 21 Haziran 2017 tarihinde yayımlanarak yürürlüğe girmiştir. İlgi tebliğ gereği KamuNet ağında hizmet veren tüm kamu kuruluşlarının Uluslararası Bilgi Güvenliği Yönetim Sistemi standardı olan TS ISO/IEC 27001 veya ISO/IEC 27001 standartlarına uygun hareket etmesi zorunlu kılınmıştır. Bunlara ek olarak bir dizi siber güvenlik uygulaması belirtilerek uygulanması zorunlu tutulmuştur. (Kamunet Ağına Bağlanma ve Kamunet Ağının Denetimine İlişkin Usul Ve Esaslar Hakkında Tebliğ, 2017)

5.1.3.2.4 Türkiye Siber Güvenlik Kümelenmesi

"Türkiye Siber Güvenlik Kümelenmesi", 2017 yılında ilgili tüm kamu kurum/kuruluşlar, özel sektör ve akademi temsilcilerinin katılımlarıyla ortaya çıkan, "Savunma Sanayii Başkanlığı ve Dijital Dönüşüm Ofisi Başkanlığı" tarafından desteklenen ve SSTEK A.Ş.[15] tarafından yürütülen bir projedir. Kümenin uzun vadeli hedeflerinin belirlenmesi ve yönetilmesi "Savunma Sanayii Başkanı Başkanlığında, Sanayi ve Teknoloji Bakanlığı, Ulaştırma ve Altyapı Bakanlığı, Dijital Dönüşüm Ofisi Başkanlığı ve Savunma Sanayi Başkanlığı üst düzey temsilcilerinin katılımıyla oluşturulmuş Danışma Kurulu" vasıtasıyla yapılır.

[15] "SSTEK Savunma Sanayi Teknolojileri AŞ, 2016 yılında T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı'nın %100 iştiraki olarak kurulmuştur"

Siber güvenlik kümelenmesi faaliyetleri arasında şu konular yer almaktadır (Türkiye Siber Gvüenlik Kümelenmesi Resmi İnternet Sitesi, 2021):

> "Üye siber güvenlik firmaların ürün ve hizmetlerini kataloglamak,
> Yerli ürünlerin kullanımı için teşvik mekanizmaları oluşturmak,
> Siber güvenlik konusuna ilgi duyan kişilerin kendilerini geliştirebileceği, kabiliyetlerini belgelendirebileceği eğitim, yarışma grup çalışmaları gibi etkinlikler düzenlemek, eğitim tesisi kurmak, kurulmasına destek olmak,
> Firmaların yararlanabileceği destek, teşvik, proje gibi kaynakları tespit etmek ve üyelerin erişimini kolaylaştırmak amacıyla danışmanlık ve lobi faaliyetleri yapmak,
> Ulusal/Uluslararası konferans, eğitim, seminer, panel, fuar gibi etkinlikler düzenlemek,
> Siber güvenlik sektörüne girme niyetinde olan Türk veya Yabancı işletme ve yatırımcılara; mesleki, sosyal, teknik ve ekonomik yönlerden rehberlik etmek gibi konular yer almaktadır."

Türkiye siber güvenlik kümelenmesi faaliyetleri sayesinde yerli siber güvenlik firmalarının desteklenmesi ve yerli siber güvenlik yazılımlarının geliştirilmesi, yetişmiş insan gücünün oluşturulması, siber güvenlik tatbikatlarının icra edilmesi, siber güvenlik alanındaki lisansüstü çalışmaların desteklenmesi gibi bugüne kadarki siber güvenlik düzenlemelerinde yer verilen hedeflere yönelik ciddi sonuçlar elde edilmiştir.

5.1.4 Ulusal Siber Güvenlik ve Eylem Planı (2020-2023)

Ulusal Siber Güvenlik ve Eylem Planı (2020-2023) 29 Aralık 2020 tarihli Resmi Gazetede yayımlanarak yürürlüğe girmiştir. Daha önce yayımlanmış olan siber güvenlik strateji belgelerine benzer bir kavramsallaştırmaya sahip olup Ulusal Siber Güvenlik olaylarından sorumlu olarak belirlenen siber güvenlik kurulunun mülga olduğunu belirterek bu alandaki ana sorumlu kurum olarak T.C. Ulaştırma ve Altyapı bakanlığı odaklı bir yaklaşım belirlenmiştir. Ülkenin kalkınma girişimlerinde teknolojinin önemi ve bu öneminde beraberinde getirdiği teknolojik risklere vurgu yapılmakta ve siber güvenlik kavramının önemi bu kapsamda belirlenmiştir. Bu durum, ilgili eylem planında şu şekilde ifade edilmiştir:

> "Milli birlik ve beraberlik içerisinde sürdürdüğümüz kalkınma ve büyüme yolundaki mücadelemizde teknoloji alanında yaşanan gelişmeler önemli bir yer tutuyor. Bu gelişmeler; ekonomiden sağlığa, eğitimden ulaşıma kadar kamu

> hizmetleri de dâhil olmak üzere hayatın her alanında büyük bir hızla gerçekleşiyor. Sürekli gelişim ve değişim kaydeden, yaygınlaşarak yaşamımızın ayrılmaz bir parçası haline gelen bilgi ve iletişim teknolojileri bizlere birçok imkân sunarken siber güvenlik risklerini de beraberinde getiriyor. Siber tehditlere karşı, milli güvenliğimizin önemli bir parçası olan ulusal siber güvenliğimizin sağlanması en öncelikli konulardan biri haline gelmiş olup buna yönelik çalışmalarımızı büyük bir azimle sürdürmekteyiz. Bu çerçevede, ortaya çıkan ulusal ihtiyaçlar ile teknolojide yaşanan gelişmeler dikkate alınarak Ulaştırma ve Altyapı Bakanlığınca, kamu, özel sektör, sivil toplum kuruluşları ve üniversitelerle iş birliği içinde Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023) hazırlanmıştır." (Cumhurbaşkanın önsözünden alıntılanmıştır).

İlgili stratejik planda; "2013-2014 dönemi ile 2016-2019 döneminde gerçekleştirilen ve süreklilik arz eden eylemler, mevcut durum ve planlanan çalışmalar kapsamında gözden geçirilmiş ve gerekli iyileştirmelerin yapılması" sağlanmıştır. Bu çerçevede, belirlenen stratejik amaçlar 8 ana başlıkta toplanmıştır. Bunlar şunlardır:

> "Kritik Altyapıların Korunması ve Mukavemetin Artırılması
> Ulusal Kapasitenin Geliştirilmesi
> Organik Siber Güvenlik Ağı
> Yeni Nesil Teknolojilerin Güvenliği
> Siber Suçlarla Mücadele
> Yerli ve Milli Teknolojilerin Geliştirilmesi ve Desteklenmesi
> Siber Güvenliğin Milli Güvenliğe Entegrasyonu
> Uluslararası İş Birliğinin Geliştirilmesi"

Bundan sonraki alt başlıkta tez çalışmasının bir anlamda ikinci ana konusu olan "siber alanda güvenlik krizi ve yönetimi" konusu açıklanmış ve tartışılarak analiz edilmiştir.

5.1.5 TSK Siber Savunma Komutanlığı'nın Kuruluşu ve Faaliyetleri

TSK'da siber güvenlik faaliyetleri ülkemizdeki siber güvenlik faaliyetleri ile paralel bir yolda ilerlemiştir. Ulusal siber uzayının korunumunun nasıl sağlanacağına yönelik 2000'li yılların başlarında icra edilen ulusal çalışmalara TSK tarafından katkı sağlanmıştır. (Güngör M. , 2015) Çalışmada ele alındığı üzere ülkemizdeki erken dönem siber güvenlik çalışmaları TUBİTAK çatısı altında gerçekleştirilmeye başlamıştır. Bu dönemde TSK ve TUBİTAK, Ortak Kriterler

Test Merkezi, Haberleşme Güvenliği (COMSEC) test laboratuvarı gibi önemli çalışmalar gerçekleştirilmiştir.

2012 yılından itibaren siber güvenlik alanında yaşanan gelişmelerden TSK'da etkilenmiş ve 2013 yılında TSK'ın siber güvenlik faaliyetlerini yönetmek gerek ulusal gerekse başta NATO olmak üzere TSK'nın uluslararası arenadaki faaliyetlerinin siber alandaki izdüşümünü takip ve yönetimi sağlamak için TSK Siber Savunma Komutanlığı kurulmuştur (Darıcılı A. , 2019). Bu komutanlık ayrıca ulusal olarak ve NATO tarafından icra edilen tatbikatlara iştirak etmek, TSK çapında bilinçlendirme ve eğitim faaliyetleri yürütmek, TSK tarafından kullanılan ağlarda düzenli olarak siber güvenlik denetlemeleri ve testleri yapmak faaliyetlerini icra etmektedir.

5.2 Siber Alanda Güvenlik Krizi ve Yönetimi

2016-2019 Ulusal Siber Güvenlik Strateji belgesinde belirtildiği üzere "siber güvenlik, risk yönetimini esas alan etkin ve sürekli değerlendirmeye ve iyileştirmeye dayalı yöntemler aracılığıyla sağlanır. Oluşturulan risk yönetimi metotlarının tehdit ve açıklıkları ele alarak bunlardan dolayı ortaya çıkacak riskleri belirlemesi, bu riskleri kabul edilebilir düzeye indirmek için yöntemler sunması hedeflenir" (2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2016) şeklinde bir açıklama yapılmıştır.

Araştırmanın bir önceki aşamasında ele alınan siber tehditler göz önüne alındığında ise siber tehdit aktörlerinin kurum içi tehditler hariç tutulduğunda kurumun yönetim alanı dışında yer aldığı belirtilmiştir. Risk ve tehdit arasında yönetilebilirlik anlamında bir ilişki bulunmaktadır. Tehditler bir güvenlik riskine sebebiyet vermekte ancak yönetimi kurum kapsamı dışında yer almaktadır. Örneklendirecek olursak, yangın vb. fiziksel riskleri bertaraf etmek için ana veri merkezinde gerekli yangın söndürme tedbirlerini alarak ve uzak lokasyonda bir yedek veri merkezi kurmak, bu fiziksel riski yönetmeyi sağlarken, kurumunu hedef almış bir APT grubunun faaliyetlerini yönetmek mümkün olmayacaktır. Bu

durumda ancak ilgili tehdidin potansiyel etkilerine karşı bazı ön alıcı güvenlik tedbirleri alınarak kurumun olası tehditlere karşı korunması sağlanabilir.

Görüldüğü üzere risk ve tehdit arasında yönetilebilirlik anlamında hiyerarşik bir ilişki mevcuttur. Tehdit kavramı yönetilemez bir olgu olarak karşımıza çıkmakta tehdidin potansiyel etkileri bir gerçek durum olarak karşımıza çıktığında ise ortaya bir güvenlik krizi durumu çıkmaktadır (Demir, 2019, s. 33). Kapsamlı bir siber güvenliğin sağlanması için siber güvenlik kavramına kriz yönetimi tabanlı bir yaklaşım sergilenmesi gerekliliği ortaya çıkmaktadır. Siber olayların yönetimi, engellenmesi ve siber risk yönetimi tabanlı bir siber güvenlik yönetimi yaklaşımı, tehdit ve siber güvenlik krizi yönetimini mümkün kılamazken kriz yönetimi temelli bir yaklaşım, bütüncül bir siber güvenlik yönetimi sağlayacaktır.

5.2.1 Kriz ve Kriz Yönetimi

Çalışmanın daha önceki bölümlerinde kriz yönetimine ilişkin kavramlar açıklanmıştır. Çalışmanın bu aşmasında ise kriz yönetiminin aktif aşamalarından ziyade kriz kavramına kapsamlı bir yaklaşımla kriz yönetimi arasındaki ilişki ele alınmış, krizlerinin önlenmesine ilişkin planlama faaliyetleri değerlendirilmiş, izleme, tespit, önlem alma gibi kavramların kriz yönetimindeki önemleri ve kriz yönetimi aşamaları ile olan ilişkisi belirlenmeye çalışılmıştır. Stratejik iletişim ve kriz yönetimine değinilerek kriz yönetimine proaktif ve kapsamlı bir yaklaşım sergilenmiştir.

Kriz kavramının evrensel tek bir tanımlaması yoktur. Sosyoloji, ekonomi, tıp, siyaset, yönetim bilimleri, psikoloji gibi pek çok farklı disiplinde farklı tanımlamalar ve yaklaşımlar mevcuttur. Kriz Yunanca “karar”, “ayrılmak” anlamına gelen “Krisis” kavramından gelmektedir. Bu öznel bir karar anı değil, bir sürecin içinden bir sürecin içine veya bir sürecin içinde bir duruma geçiş başlarken ortaya çıkan bir karar ya da kararsızlık anını belirtmektedir (Çapar ve Koca, 2017, s. 1). Krizin genel anlamda ifadesi aniden ortaya çıkan bir durum, kötüye gidiş ve içinden

çıkılması güç bir durumu ifade etmektedir (Akkuş, 2020, s. 103). Krizin bu genel tanımına her disiplin kendi öz kavramları ile bir yaklaşımda bulunarak kriz tanımlamasında bulunmaktadır. İnsan ve toplum yaşamında görülen sosyal, psikolojik, ekonomik, mali, siyasi, tıbbi ve doğal krizlerin yanı sıra, çalışma ve yönetim yaşamında da örgütsel krizler görülebilmektedir (Çapar ve Koca, 2017, s. 1). Bu nedenlerden dolayı, kamu kurumlarının da kriz kavramının özüne farklı bir yaklaşımda bulunması her kurumun kendine özgü kavramlarının diğerlerinden farklılıklar içermesi nedeniyle gayet doğal bir hal olarak karşımıza çıkmaktadır.

Daha önce de incelendiği üzere, Boin vd. tarafından gerçekleştirilen, kriz yönetimini siyaset bilimi argümanları ile ele alan ufuk açıcı çalışmada kriz; yüksek derecede belirsizlik veya belirsizlik yaratan, büyük bir aciliyet duygusu uyandıran ve yüksek değer verilen varlıkları tehlikeye atan bir olay olarak tanımlanmış, bir krizin öznel bir tanımını sunulmuştur (Boin, Stern, & Sundelius, 2005). Krizin tanımlanmış olan öznel nitelikleri arasındaki denge krizin gelişimine göre öngörülemez bir şekilde değişebilir. Gerçekte ne olduğuna dair bir belirsizlik meydana gelebilir, aynı zamanda önerilen bazı eylemler dizisinin sonuçlarına yönelik belirsizlik durumu ortaya çıkabilir. Kriz durumunda tehdit altında olan yalnızca insan hayatı veya maddi varlıkları değil, aynı zamanda güven, itibar veya güç gibi daha soyut değerlerde olabilir.

Kriz kavramının belirsizlik üzerine temellendiren siyaset bilimi yaklaşımı köklerini, modern devletin formüle eden iki siyaset felsefecisi Hobbes ve Locke'tan alır. Locke "Yönetim Üzerine İnceleme" adlı eserinde devleti iki yönlü bir görev üzerine temellendirir: Güvenliğin üretilmesi ve belirsizliğin azaltılması. Hobbes içinse yönetimin olmadığı doğa hali bir kriz durumudur ve güçlü olanın kazandığı doğa durumunu belirsizlik olarak tanımlar. Her iki düşünür için belirsizlik dışında önemli olan bir diğer şey ise bireyin yaşam hakkı ve mülkiyettir (Rosanvallon, 2003, s. 22). 17. Yüzyıl'dan günümüze gelindiğinde, belirsizliğin karşılığı halen bir kriz durumudur. Siber alana baktığımızda belirsizlik durumu her an karşımıza çıkabilecek olası bir durumdur. Bu anlamda siber güvenlik alanında proaktif bir güvenlik anlayışı sergilenirken daha önceki tanımlamamızda belirtildiği üzere

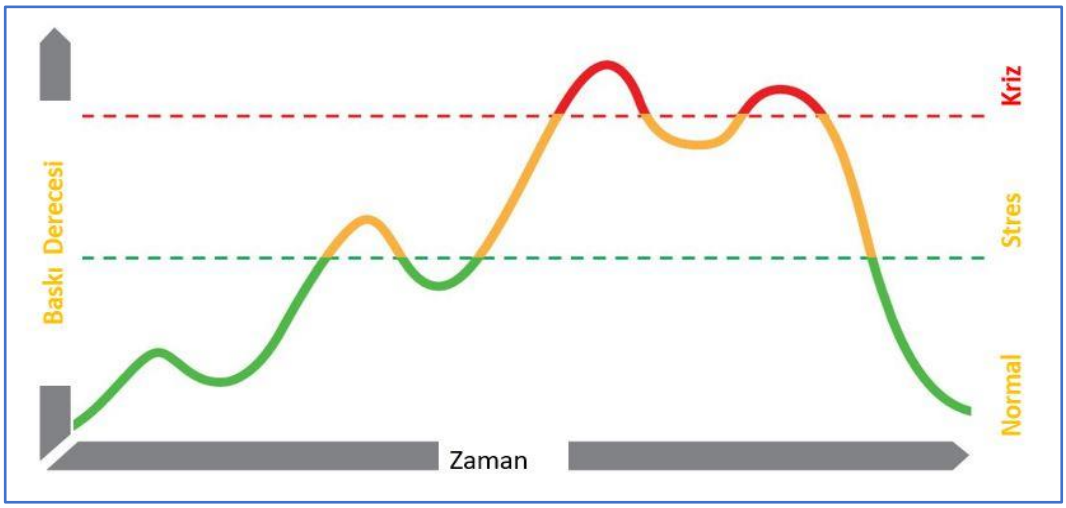
siber uzaydaki mülkiyet hakkının ihlalinin engellenmesi siber güvenliğin önemli bir bileşenidir. Devletin siber uzaydaki hukuki sorumluluğu ve egemenlik hakkını kullanımı yine kendi sınırları üzerindeki egemenlik hakkı ile aynı doğrultudadır. Devlet kendi sınırları üzerindeki siber uzayın fiziki, mantıksal ve siber insan etkileşim katmanlarındaki tüm bileşenler üzerinde kendi iç hukuku kapsamında yetkilidir (Schmitt, 2017). Devletin siber uzaydaki yetki sınırı kendi iç hukuku doğrultusunda belirlenmektedir. Türkiye'de siber güvenlik elektronik haberleşme kapsamında değerlendirilip, ulusal çaptaki siber güvenlik faaliyetleri bu eksende belirlenmekte ve icra edilmektedir. Haberleşme güvenliği anayasanın 22. maddesi[16] ile düzenlenmiş olup, Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması kapsamında haberleşme özgürlüğü devlet tarafından kısıtlanabilmektedir. Bu kısıtların dışında herkes haberleşme özgürlüğüne sahip olup, devletin haberleşme özgürlüğüne müdahale sınırı belirlenmiştir.

Krizler acil hareket etme hissi uyandırır. İlkim değişikliği, küresel ısınma, ormanların azalması vb. sorunlar bazı çevrelerde endişe ile karşılanıp kriz durumu olarak algılansa da genellikle kamuoyu ve politikacılar tarafından kriz olarak algılanmazlar. Fakat tehlikenin ciddiyetinin hissedildiği veya yaşanıldığı olaylar esnasında politikacılar aniden zaman baskısı altında kalırlar ve krize acil çözüm bulma baskısıyla karşılaşırlar. Belirsizlik, aciliyet ve risk altında olan varlıkların miktarı zamanla hem yukarı hem aşağı doğru değiştikçe, bir olay "yönetilebilir" bir kriz durumuna girip çıkabilir. Bu durum özellikle güvenlik yönetiminin genelinde sıkça rastlanan bir durumdur. Sahip olduğunuz risklerin değerlemesi dinamik bir haldedir ve orta düzey riskleriniz aniden kritik bir değerlemeye sahip olurken kritik riskleriniz zaman içinde orta ve düşük bir değerlemeye sahip olabilirler. Yönetim kavramı hiçbir zaman düz bir çizgide

[16] Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır. Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar. İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir.

yönetim demek değildir. Aynı zamanda normal olandan kriz durumuna geçiş çizgisinde uzun süre stres altında çalışmak zorunda kalınabilmektedir. Bu durum aşağıda verilen Şekil-13'de açıklanmıştır:

Şekil-13: Baskı Derecesi ve Kriz İlişkisi



Kaynak: (Trimintzios, Holfeldt, Uckan, & Gavrila, 2014).

5.2.1.1. Kriz Yönetimi ve İzleme/Tespit/Önlem Alma/ Hazır Olma İlişkisi

Kriz yönetiminin temel özelliklerinden biri de kriz sinyallerinin belirmesi veya sezilmesi durumunda, krizi mümkün olduğunca engellemek olmalıdır. Bir kurum önceliği, mümkünse kriz durumuna hiç girmemektir. Şekil-13'de tarif edilen baskı ve kriz arasındaki ilişki de baskının yükselmesi sonucu olağan yönetimden kriz yönetimine geçiş aşaması başlamış olur. Ancak bir güvenlik olayının getirdiği baskıyı azaltıcı tedbirlerin alınması proaktif bir kriz yönetimi için elzemdir. Bu noktada erken uyarı ve korunma tedbirlerini almak olası baskıları azaltarak krize neden olabilecek olayları yönetilebilir kılabilecektir. Baskı durumuna hazırlık ise olayların yönetilebilir seviyede kalmasına yardımcı olacak bir diğer önemli unsurdur.

Krizlere hazır olmanın bir diğer önemli bileşeni stratejik planlamadır. Strateji örgütün amaçlarına ulaşmak amacıyla yaptığı ve çevre ile olan etkileşimini belirleyen geniş kapsamlı planlar olarak tanımlanabilir. Makro düzeyde yapılacak olan planlamalarla örgütün zayıf ve güçlü yanları görülerek, uzun vadede ulaşılması istenen amaçlar, seviyelere yönelik bir dizi planlama ile örgütün gelecekteki olası kriz durumlarına karşı hazır olması sağlanabilir. Stratejik planlamaya öncelikle değerler ve ilkelerin belirlenmesi ile başlanır. Değerler ve ilkeler örgütün sağlıklı bir biçimde varlığını sürdürmesini sağlar. Örgüt üyelerinde ortak bir düşünce oluşmasını ve olaylara karşı nasıl bir reaksiyon gösterileceğini belirleyen özellikler arasında yer almaktadırlar. Vizyon ve misyonun belirlenmesi bir diğer önemli aşamadır. Vizyon mevcut durum, umutlar, hayaller, tehlike ve fırsatlar bağlamında örgütün bir bütün olarak bilinenden bilinmeyene doğru zihinsel bir süreç, istenilen duruma ulaşmak için yapılacakları ifade eden niteliksel bir tasarım olarak tanımlanabilir. Misyon ise örgüte ve örgüt üyelerine istikamet veren ve onu benzerlerinden ayıran, anlamlı, uzun dönemli görev ve ortak değerler bütünüdür.

Stratejik planlama sürecinin ilk aktif aşaması durum analizidir. Yönetim tarafından amaç ve hedeflerin tespiti için mevcut durumun belirlenmesi gereklidir. Durum analizi, örgütün güçlü ve zayıf yönlerinin belirlenmesi ve dış çevreden kaynaklı fırsat ve tehditlerin tespitini içerir. Durum analizi örgütün kendisini tanımasını sağlarken stratejik planlamanın yorumlanmasını beraberinde getirir. Bu dönemde gerek örgüt içi gerekse örgüt dışı faktörler doğrultusunda izlenecek alternatif stratejiler belirlenir ve alternatifler arasında bir değerlendirme yapılır. Eylem planlarının ortaya çıkarılmasıyla belirlenen hedeflere nasıl ulaşılacağı ortaya konmuş olur. Bu bağlamda eylem planları; örgütün amaç hedef ve misyonları doğrultusunda, örgüt fonksiyonlarının ve alt programlarının başarıya ulaşması için kullanılan yöntemleri ve stratejileri ayrıntılı bir biçimde açıklayan ifadeler olarak tanımlanır (Akkuş, 2020, s. 116-121).

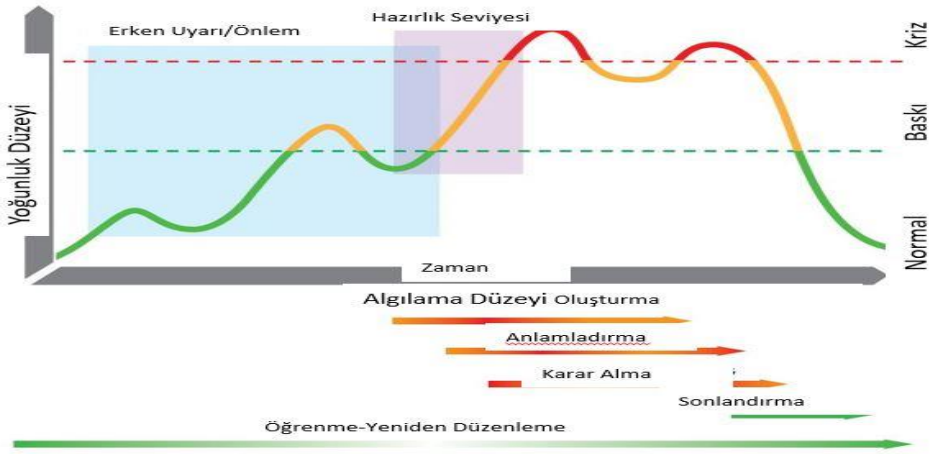
Krizi önlemek veya krize hazır olabilmek için krize neden olan iç ve dış nedenlerin devamlı olarak izlenmesi ve alınan sinyallerin her birinin dikkatle analiz edilmesi

gerekmektedir (Çapar ve Koca, 2017, s. 5). Aynı şekilde gerek "bölgesel" ve gerekse "küresel" seviyede meydana gelen olaylara bağlı olarak ortaya çıkması muhtemel olan ve olumsuz etkiler yapabilecek gelişmeler de takip edilmelidir. Krizin meydana gelmesini engellemedeki önemli bir unsur doğru ve sürekli bilgi akışıdır. Bu durum tespit kabiliyetini artırıcı bir unsur olacaktır. Doğru bilginin doğru zamanda doğru kişiye ulaşmasının sağlanmasıyla, bilgi eksikliği veya yanlış anlamalar sebebiyle risk unsurlarının krize dönüşmesi önlenmiş olur.

Dikkat edilmesi gereken bir diğer nokta da, daha önce de belirtildiği gibi, "erken uyarı", "önleme" ve "hazırlıklı olma" gibi kavramların kriz yönetiminin aktif beş aşamasının biraz dışında kalmasıdır. Erken uyarı[17] süreci, sistem üzerindeki olağandışı basınç artışlarını tespit eden ve böylece ilk anlam oluşturma çabalarını tetikleyen bir unsurdur. Bu durum erken aşamada krizin patlak vermesini önlemek olarak da düşünülebilir. Benzer şekilde, hazırlık süreci, anlam verme ve karar verme süreçlerini başlatan şeydir. Çünkü burada kilit karar vericilerle bağlantı kurulur ve krizi açıklamak için bir mesaj formüle etmeye yönelik ilk girişimler yapılır. "Önleme" ve "hazırlıklı olma" arasındaki ayrım, özellikle dikkat çekicidir. Çünkü tamamen analitik alanın dışında bile, iki terim arasında bazı karışıklıklar vardır. Yapılandırılmış kriz planlamasının çoğu örneğinde olduğu gibi burada da, hazırlık kavramı, gelecekteki bir olası olay için herhangi bir ön planlama veya genel zihinsel hazırlığı içermez. Daha ziyade, yakın gelecekte ortaya çıkması çok muhtemel görünen bir krizin aktif yönetimi için hazırlanmanın spesifik faaliyetini ifade eder. Bu, acil durum önlemlerini harekete geçirmek, ilgili karar vericileri aramak vb. anlamlara karşılık gelir (Bknz. Şekil-14).

[17] "Erken uyarı sistemleri oluşturmada krizden kaçınmada önemli bir tedbir olarak karşımıza çıkmaktadır. Erken uyarı sistemleri sayesinde krizin varlığı, şiddeti ve yoğunluğu tespit edilebilir."

Şekil-14: Kriz Yönetimi Aşamaları ve Erken Uyarı/Önlem/Hazırlık Seviyesi İlişkisi



Kaynak: (Trimintzios, Holfeldt, Uckan, & Gavrila, 2014)

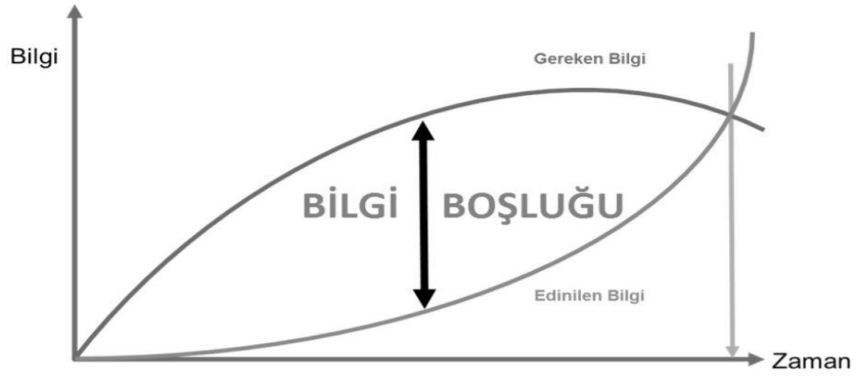
5.2.1.2 Krizlerde İletişim

Büyük çaplı krizler, toplumun ve medyanın yoğun ilgisini çekebilir bazı durumlarda siyaset konusu olabilirler. Kriz yönetimi aşamaları, kriz öncesi tespit/izleme/hazır olma gibi kriz yönetimi kavramları her zaman iletişim kavramı ile ilişki halindedir. Ayrıca iletişim kriz yönetiminin en kritik kaynaklarından olan bilginin etkin yönetiminde başrolde yer almaktadır.

Kriz yönetimindeki önemli risklerden biri, ortaya çıkan bilgi boşluğu nedeniyle kriz hakkında yayılan bilgilerin dolaylı olarak da aktarılan hikâyenin kontrolünün kaybedilmesidir. Şekil-14'de görülen bilgi boşluğu ani gelişen olayların krize dönüşmesinde ve krizin süresi, boyutu ve etkisi üzerinde rol sahibidir. Gerek bilgi gerek zaman boyutunda krizin başlangıç dönemindeki hızlı ilerleyişin zamanı durdurarak kontrol edilememesi nedeniyle kriz hızla kontrol edilemez bir vaziyete dönüşme riskini içermektedir. Doğrulanmış bilginin doğru zamanda ve doğru paydaşlara iletilmesi bilgi boşluğunu azaltacaktır. Bu amaca ulaşmanın en iyi yolu bilgiyi sistematik olarak toplamak ve paylaşmaktır. Sistematik olarak bilgi toplama ve paylaşma özellikle coğrafi olarak geniş yayılımlı krizlerde kritik önem

taşımaktadır. (Karaağaç, 2013, s. 122) Şekil-15 incelendiğinde kriz esnasında zaman ilerledikçe gereken bilgi ihtiyacı artış gösterirken edinilen bilgi miktarı aynı seviyede artış gösterememekte ve bilgi boşluğu oluşmaktadır.

Şekil-15: Krizlerde Bilgi Boşluğu



Kaynak: (Karaağaç, 2013, s. 122).

Günümüzde teknoloji, iletişimi dönüştürmüş toplumun haber alma beklentisi yükseltmiştir. Ortaya çıkan yeni durumlarla ilgili gerekli açıklamaların zamanında yapılmaması, ortaya büyük bir bilgi boşluğu çıkarmaktadır. Bu durum ise kriz durumu algısının yükselmesine neden olmaktadır. Mevcut durumu açıklamak gizlilik, durum hakkında yetersiz bilgi vb. nedenlerle mümkün olmasa dahi bilgi kirliğini önlemek maksadıyla tutarlı ve basit bir açıklama ile zaman kazanılmalıdır. İletişimi güvenli bir temele oturtmak kriz iletişiminin yönetimini kolaylaştıracaktır. Aksi durumlarda ise toplumsal algı, medyanın konuya yaklaşımı ve iletişim eksikliği hızlı itibar kaybına ve kurumun başarısızlığına yol açacaktır (Karaağaç, 2013, s. 124). Bu gibi algı operasyonlarının önüne geçmek için krizin medya ve sosyal ağlarda ciddi bir şekilde takip edilmesi gereklidir ayrıca krizin toplum tarafından nasıl algılandığı da yakından takip edilmelidir.

Bu nedenle gerek kurum içi gerekse kurum dışı iletişimin sağlıklı bir şekilde sağlanması maksadıyla krizlerde iletişim stratejisine ihtiyaç duyulmaktadır. İletişim stratejisinin sorun yönetimi, paydaşların katılımı ve risk iletişimi şeklinde üç sacayağının olduğu varsayılmaktadır. Sorunların yönetimi kapsamında olağan

dışı durumlara ilişkin belirtilerin izlenmesi gerekli reaksiyon alınabilmesini sağlayan önemli bir çözümdür. Bu durum aynı zamanda ortaya çıkabilecek muhtemel risklerin değerlendirilmesi ve gerekli tedbirlerin alınabilmesini sağlayacaktır.

"İngiliz Standartları Enstitüsü" tarafından 2011 yılında çıkarılan "PAS200 – Kriz Yönetimi Rehberi"'nde söz konusu iletişim stratejisinin ortaya konmasında sorun yönetimi, risk iletişimi ve paydaşların katılımının oynadığı role dikkat çekilmektedir. İyi bir kriz yönetimi iletişim stratejisi, "hangi paydaşın ne zaman ve nasıl bilgi alacağını" belirtmeli ve öncelikleri belirlenmelidir. Bilginin "çalışanlar, tedarikçiler, müşteriler, ortaklar, toplum ve medya" gibi farklı çevrelerde farklı algılanabileceği göz önünde bulundurulmalıdır. Bu nedenle iletilecek mesajların içeriği ve iletim şekli hedef kitleye uygun olarak belirlenmeli, ancak aktarılacak temel mesajlar her zaman birbirleriyle tutarlı olmalıdır (Karaağaç, 2013, s. 126).

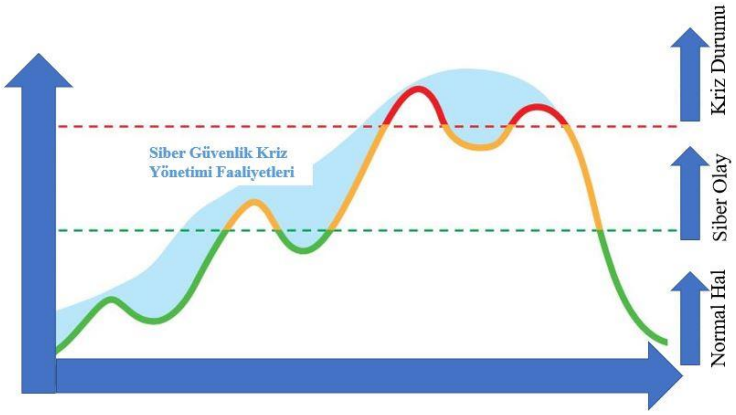
Örgütün yapısı ve konumuna bakılmaksızın iletişim stratejisinde açıklık ve güvenilirlik her zaman ön planda tutulmalıdır. Açıklık ve güvenilirlik etkin bir kriz iletişiminin temel kavramları arasındadır. Kriz sırasında bilginin dönüşüme ve değişime uğramadan, hızla tüm paydaşlara ulaşması kritik önem arz etmektedir. Geleneksel yapılarda bilgi hiyerarşik düzen içerisinde, yönetim kadrosuna doğru tek yönlü bir çizgi izler. "*Hiyerarşi katılaştıkça bilginin ilerleyiş hızı düşer, darboğazlar oluşur, bilgi filtrelenir, deformasyona uğrar, hatta kaybolur*." (Karaağaç, 2013, s. 126). Bu durum bir kriz anında kurum içerisinde paylaşılması gereken bilginin, yeterli hız ve etkinlikte yayılamaması riskini beraberinde getirmektedir. Kriz anında bilginin yatay ve dikey eksende yayılımının yeterli seviyede olmasının sağlanması krizin yönetimi için gerekli bir eylemdir. Bilgi günümüz sosyal medyasında çok hızlı bir şekilde herhangi bir yön takip etmeksizin orantısız ve kontrolsüz bir dağılım gösterir. Bu durumda beraberinde bilgi kirliğini getirerek olumsuz algı oluşmasına neden olabilmektedir. Bu nedenle, kurumların krizi yönetme becerilerinden ziyade, krizin ortaya çıkmasını önleyici tedbirler üzerinde durmaları daha sağlıklı olacaktır.

5.2.2. Siber Güvenlik Kriz Yönetimi

Siber olay kavramını resmi olarak tanımlanan şekliyle "*Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilgi/verinin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya teşebbüste bulunulması*" (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023), 2020) olarak tanımlayabiliriz. Siber uzayın fiziksel, mantıksal, insan ve siber uzay etkileşim katmanlarında yer alan bilişim sistemleri, siber uzay insan etkileşimini sağlayan uygulamalar, hesaplar ve hizmetlere yönelik gerek teknik gerekse içerik yönetimi ile algı oluşturma saldırıları neticesinde hedef sistem ve sistemin bağlı olduğu ekosistemin geneli yada diğer bileşenlerinin gizlilik, bütünlük ve erişilebilirlik işlevlerini yerine getirmesinde ciddi sorunlarla karşılaşılması ve bu durumun kalıcı olma yönünde eğilime sahip olması durumlarını siber güvenlik krizi olarak tanımlayabiliriz. Siber güvenlik krizleri, sahip olduğu geniş etki alanı nedeniyle siber güvenlik olaylarından ayrışmaktadır (Golandsky, 2016, s. 1). Aynı paralelde hareket ettiğimizde siber güvenlik kriz yönetimi, siber olay yönetimini de kapsayan geniş çaplı bir önleme, yönetim ve öğrenme sürecidir.

Çalışmanın önceki bölümünde ele alınmış olan kriz yönetimi faaliyetleri ve aşamaları siber güvenlik kriz yönetimi için analitik bir çerçeve sunmuştur. Siber güvenlik kriz yönetimi süreçleri ele alınırken bu çerçeve ışığında değerlendirmeler yapılmıştır. Bu aşamalara ek olarak siber güvenlik için olmazsa olmaz olan kavramlar olan izleme, tespit ve dayanıklılık hususlarına ek olarak stratejik planlama ve stratejik iletişim kavramları ışığında siber güvenlik krizleri değerlendirilmiştir. Siber güvenlik krizlerini, genel güvenlik krizi yönetimi esaslarından ayıran temel ayrım, genel kriz yönetimi süreçleri kriz ve kriz olmama durumu olarak ayrımlarken, siber güvenlik krizleri siber olayların yönetiminin getirdiği baskı ve etki seviyesine göre şekillenmesidir. Siber olayların meydana gelmesi öncesi başlayan siber kriz yönetimi faaliyetleri olayların meydana gelmesi ve getirdiği stresin yükselmesi ile birlikte devam etmekte ve kriz durumundan normale dönüş ve olay yönetiminden normale dönüş döneminde daha fazla yoğunluk göstermektedir. Bu durum Şekil-16'te gösterilmiştir.

Şekil-16: Siber Güvenlik Kriz Yönetimi Faaliyetleri Yoğunluğu



Kaynak: (Trimintzios, Holfeldt, Uckan, & Gavrila, 2014).

5.2.2.1 Hazır Olma/Erken Uyarı/Önlem Alma

Siber güvenlik kriz yönetimini diğer kriz yönetimi safhalarından ayrıştıran önemli aşamalardan birisi erken uyarı sistemlerine sahip olma ve önceden önlem alma aşamasıdır. Ulusal ya da kurumsal siber uzay tehdit ve risk evreni global ölçekte olabilmektedir. Ülkemizden binlerce kilometre uzaklıktaki bir APT siber tehdidi, ulusal düzeyde siber güvenlik ve siber güvenlik kaynaklı kriz yaratma potansiyeline sahiptir. Bu durum da beraberinde gerekli siber güvenlik önlemlerinin alınmasını getirmektedir. Bu önlemler gerekli teknik altyapının oluşturulmasından personelin eğitimi, siber tehdit istihbaratı gibi geniş bir skalaya dağılmaktadır. Bu aşamanın sürdürülebilir bir başarıya sahip olması stratejik planlama ile doğru orantılıdır. Gelecekteki siber tehdit ve risk evrenini hesaplayıp bu minvalde planlama yapan kurum ve kuruluşlar gerekli teknik altyapı ve idari hazırlığı zamanında yaptığı için yeni gelişen durumlara karşı daha hızlı reaksiyon gösterebilecektir (Boeke, 2018, s. 452).

Siber güvenlik olaylarının krize dönüşümünü engellenmesini sağlayan en önemli aşama bu aşamadır. Gerekli tespit, hazırlık ve dayanıklılığa sahip kurum

kuruluşlar siber olay yönetimini daha kolay ve etkin gerçekleştirerek siber olayların kriz durumuna yükselmesini engelleyecektir. Bu noktada kurumların gerekli önlem ve hazırlığı yaptıklarını düşünerek kendilerini güvende hissetmeleri yanıltıcı olacaktır. Günümüz siber güvenlik olayları siber uzayda, yüzde yüz güvenlik olmadığını açıkça ortaya koymuştur. Günümüzde siber güvenlik "2015-2019 Ulusal Siber Güvenlik Stratejisi'nde" vurgulandığı üzere risk yönetimi odaklı sağlanmalıdır. Risk yönetimi ise risklerin tamamen ortadan kaldırılmasından ziyade risk işleme ve azaltma süreçlerine dayandırılmaktadır. Özellikle risk azaltma süreci alınan güvenlik tedbirleri ile doğrudan orantılıdır. Elde bulunan siber güvenlik enstrümanlarının tespit edilen riskleri nasıl azaltacağını belirleyerek risk seviyeleri azaltılmaktadır. Bu süreçte ISO 27001 Bilgi Sistemleri Güvenliği Yönetim Standardı kurumlar için en geçerli çerçevelerden birisini sunmaktadır (Önder, 2018, s. 90). Bu konularda, hızlı teknolojik gelişimlere yanıt verebilecek hazırlıklar büyük önem taşımaktadır. (KAMUNET ağının farklı bir ağa bağlanması senaryosuna göre hazırlanmış örnek bir risk analizi Ek-10'da sunulmuştur.)

5.2.2.2 Algılama Düzeyi Oluşturma

Kriz yönetiminde aşamaların birbirleri arasında olan geçişkenliği ve iç içeliği, araştırmanın önceki safhalarında belirtilmiştir. Siber güvenlik, kriz yönetiminde algılama düzeyi oluşturma, tespit ve önlem aşamaları birbirleri arasında girişkenliklere sahiptir. Olayların tespiti, önleme ve hazır olma durumu algılama düzeyi oluşturma safhasını beslemektedir (Backman, 2020, s. 5). Gerekli hazırlık ve dayanıklılıkla siber olaylar tırmanışa geçmeden bertaraf edildiği durumlar genellikle siber güvenlik krizi olarak algılanmazlar. Ancak kimi durumlarda olayın nevi ve kurumun ya da ulusal düzeydeki politik atmosferin durumuna göre zamanında önlenebilmiş olan siber olaylar, siber güvenlik krizi olarak stratejik yönetim tarafından gündeme getirilebilir. ABD hükümetinin Kuzey Kore tarafından gerçekleştirilen olası siber saldırıları ulusal bir siber güvenlik krizi seviyesinde olmamasına rağmen stratejik seviyede ele alması (Sevestapolo, 2018) ve benzer saldırılar, Batı Avrupa ya da ABD içeresinden geldiğinde farklı

reaksiyon gösterilmesi ülke yöneticilerin Kuzey Kore kaynaklı siber tehditlere karşı algı düzeyinin olağan seviyeden daha yoğun olduğunun göstergesidir. Şekil-17'de yer alan günlük siber saldırı haritasında görüleceği üzere AB üzerinden ABD'ye doğru ciddi miktarda siber saldırı düzenlenmektedir.

5.2.2.3 Anlam Verme

Siber krizlerin teknik yönü anlam oluşturma aşamasını, diğer krizlere göre karmaşıklaştırmaktadır. Tüm yönetim seviyelerindeki karar vericiler için siber güvenlik krizinin kavranması bazı güçlükleri içerir. Siber krizlerin etkin bir yönetimi için yaşanan gelişmelerin, anlamlandırılabilir bir formata dönüştürülmesi gerekir. Bu dönüşüm teknik uzmanlar ve idari yöneticiler arasında kriz yönetimi sürecini başarıyla ele almalarını sağlayacak olan uyumu beraberinde getirir. Bu uyumunun sağlanamaması ise kriz yöneticilerini besleyen bilginin sağlıklı adreslenmesini engelleyerek çözüm sürecini uzatacaktır (Trimintzios, Holfeldt, Uckan, & Gavrila, 2014, s. 38). Teknik hususların yöneticiler için anlaşılabilir hale getirilmesi için gerekli formatlamayı sağlayacak bir birimin oluşturulması bu alandaki başarıyı artıracaktır.

Şekil-17: 21 Aralık 2020 Günlük Siber Saldırı Haritası

Kaynak: (Digital Attack Map, 2020)

Hukuki ve idari düzenlemelerle anlam verme, bu aşamanın bir diğer ögesidir. Yaşanacak olası siber güvenlik olayları (siber suçlar ve siber saldırılar vd.) esnasında kurum ve kuruluşlarının hareket tarzlarını belirleyecek olan çerçeveyi hukuki ve idari düzenlemeler belirlemektedir. Bu noktada kanunlar, bakanlar kurulu kararları ya da kanun hükmünde kararnameler vb. hukuki düzenlemeler kuruluşların kendi iç idari düzenlemelerinden daha fazla yaptırım gücüne sahiptirler. Güvenlikleştirme teorisi üzerinden siber alanın güvenlikleştirilmesine doğrudan ve yaptırım gücü yüksek etki anlam verme aşamasında gerçekleştirilir. Hükümetler kanun yapıcı organları etkileyerek güvenlikleştirilecek alanı ve konuları belirleyerek hukuki yaptırımlar getirme yoluna gitmektedirler. Araştırmanın daha önceki bölümlerinde siber alandaki algı operasyonlarının siber güvenlik meselesi olarak ele alınmasının gerekliliği belirtilmiştir. Bu konuyu örneklendirecek olursak, ABD'de sosyal medyanın algı yönetimi maksatlı olarak kullanımını engellemek için sosyal medya platformlarını (Twitter, Facebook vd.) platform statüsünün değiştirilerek, yayımcı olarak belirlenmesini sağlayan başkanlık kararnamesinin beraberinde getirdiği tartışmalar, güvenlikleştirme kavramına karşılık gelmektedir. Bu kararname ile sosyal medya platformu yöneticilerine yeni sorumluluklar, yaptırımlar ve kısıtlamalar getirilerek siber uzayın ilgili bölümü güvenlikleştirilmeye çalışılmıştır.[18]

5.2.2.4 Karar Verme

Siber güvenlik krizleri, stratejik seviyede diğer kriz yönetimi faaliyetleri ile aynı karar vericiler tarafından yönetilir. Stratejik seviyedeki karar vericileri yönlendiren algı ve anlam verme aşamasındaki verilerden oluşan durumsal farkındalık raporları, analizler, etki-tepki mekanizmalarının işleyişi, karar verici aktörleri karar verme aşamasında etkilemektedir. Algı ve anlam verme süreçleri, kararları doğrudan etkilemektedir. Karar verme aşamasında siber güvenlik krizlerini diğer

[18] Başkan tarafından da mevcut durumun müdahale edilmesi gereken ciddi bir güvenlik ihlali olduğu belirtilerek gelecekteki olası krizlerinde önüne geçmek için bu düzenleme savunulmakta, siber güvenlik kriz yönetiminin anlam verme aşaması faaliyetleri icra edilmektedir. (BBC Resmi İnternet Sitesi, 2020)

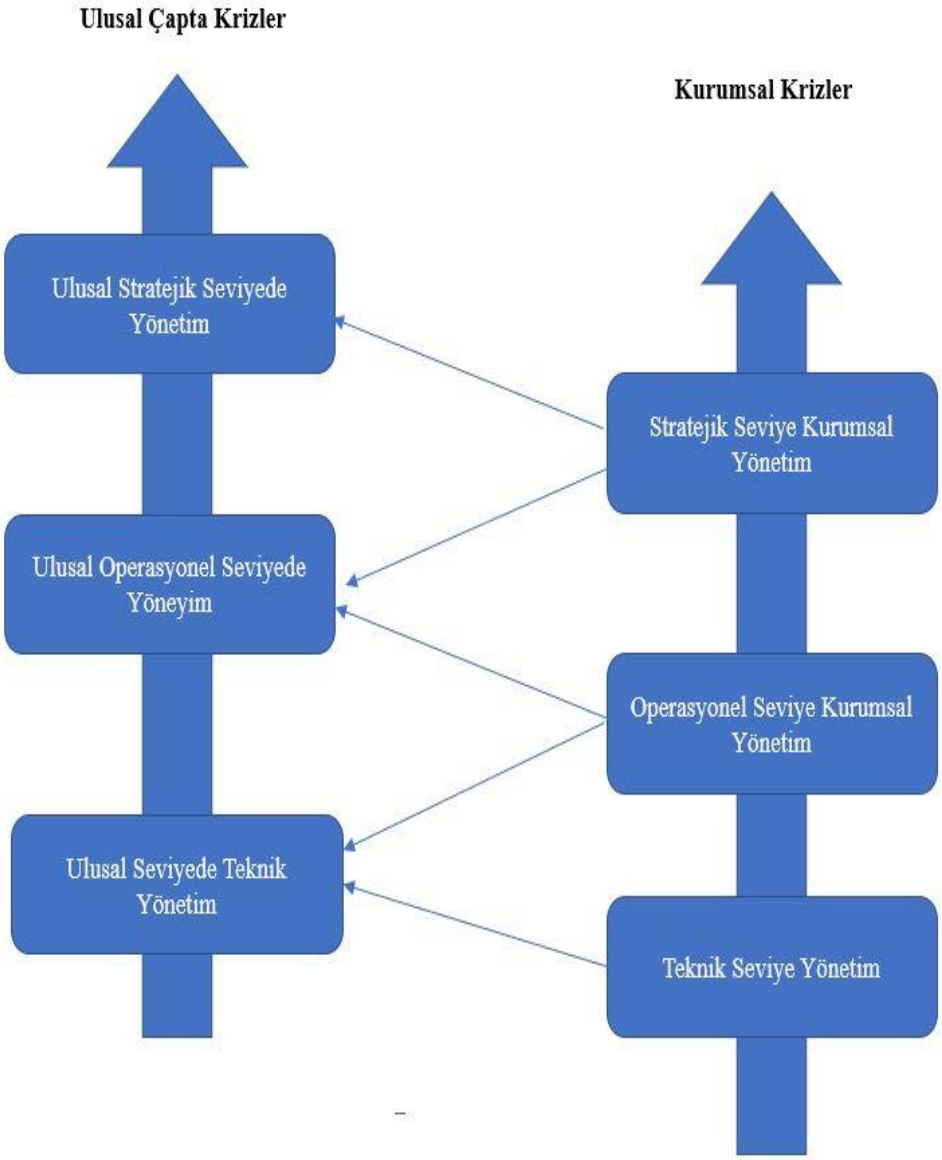
kriz alanlarından ayıran temel husus, bu alandaki krizlerin diğer finans, çevre, askeri vd. alanlardaki karar vericileri doğrudan ya da dolaylı olarak etkilemesidir. Çalışmada daha önce örnek gösterilmiş olan Amerikan kamu kurum ve kuruluşlarının etkilendiği Sunburst siber saldırısı ve sonrasında yaşanan kriz durumu hazine, silahlı kuvvetler, ulusal güvenlik departmanı ve bileşenleri (nükleer silah fırlatma sistemleri güvenliği vb.) gibi pek çok farklı alanlarda krize neden olmuştur (Cuthbertson, 2020).

Siber güvenlik krizlerinde karar vericileri etkileyen bir diğer faktör, krizin hızla gelişimi ve nereden kaynaklanabileceğinin öngörülememesidir. Sunburst olayında saldırganlar kurumların siber güvenliğini sağlayan güvenlik ürünlerini hedef almışlar ve saldırıların aslında aylar öncesinde başarılı olduğu ve kritik sistemlere sızılarak bilgi hırsızlığı yapıldığı belirlenmiştir. Bu gibi krizlerde kriz bir anda büyüyerek, gün geçtikçe orantısız bir artış gösterebilir. Karar vericiler bu noktada hızlı kararlar alabilmek için teknik seviye yönetiminin verilerine ve görüşüne ihtiyaç duyarken, ulusal seviyede bir kriz ortaya çıktığında stratejik seviyedeki karar vericiler operasyonel seviyedeki yöneticilerin bilgi akışına ihtiyaç duyarlar. Çünkü elde veri olmadan teknik alanda doğan bu krizi çözümleyemezler. Krizin yoğunluğu ve kurumsal teknik seviyeden ulusal stratejik seviyeye bilgi akışı ve krizin sıçraması Şekil-18'de gösterilmiştir. Görüldüğü üzere krizin yoğunluğu artıkça ulusal bir krize dönüşmekte ve stratejik seviyede karar alıcılar krizle yüzleşmek zorunda kalmaktadırlar. Bu durum Şekil-18'de açıklanmaya çalışılmıştır.

Siber güvenlik kriz yönetiminde karar vericileri etkileyen bir diğer önemli girdi elde mevcut olan yetkin ve yetişmiş teknik insan gücü faktörüdür. Krize müdahale edebilecek, gerekli girdileri sağlayabilecek insan gücünün mevcudiyeti karar vericileri doğrudan etkileyecektir. Bazı durumlarda bu durum siber güvenlik krizlerini ele almak için uluslararası yardım çağrısına neden olabilecektir. Estonya siber saldırıları üzerinden durumu örneklediğimizde 2007 yılında gerçekleştirilen geniş kapsamlı siber saldırıya karşı yeterli teknik personele sahip olmayan Estonya hükümeti NATO'dan bu konuda yardım talebinde bulunmuştur (Bıçakçı,

2014, s. 121). Sorunun çözümü içi dışarıdan yardım alınmak zorunda kalınmıştır. Dışarıdan yardım alarak siber güvenlik sorunlarının çözümü de kendi başına başka sorunlar oluşturmaktadır.

Şekil-18: Siber Güvenlik Krizlerinin Yoğunluk Seviyesi ve Yönetim Seviyeleri İlişkisi



Kaynak: (Trimintzios, Holfeldt, Uckan, & Gavrila, 2014).

5.2.2.5 Sonlandırma

Siber güvenlik kriz yönetiminde sonlandırma aşaması, kendine özgü farklılıklara sahiptir. Bunlardan en önde geleni krizin bitip bitmediğine karar verilmesindeki güçlüklerdir. Siber uzayın kompleks yapısı bu durumu güçleştiren en temel etkendir. Siber güvenlik kriz yönetiminin önceki aşamalarında da kendisini gösteren bilinmezlik durumu karar vericileri, krizin bitip bitmediğine dair karar alırken zor durumda bırakmaktadır. Siber güvenlik krizlerinin politik tarafı krizin sonlandırılması sürecine etki eden bir diğer etkendir. ABD 2016 başkanlık seçimlerine siber saldırı yapılmasının politik etkilerinin 2020 yılı itibariyle devam etmesi ve yeni yönetimini geçmişe yönelik saldırı analizlerinde bulunma ihtimali, konuyla ilgili siber güvenlik otoritelerince krizin yönetimi süreçlerine devam edilmesini zorunlu kılmaktadır (Mehrotra, 2020).

Siber güvenlik krizlerinin ulusal stratejik seviyede ele alınışının bir diğer politik boyutu saldırgan tarafın hareketlerinin yorumlanmasıdır. Krize neden olan saldırıların bir çatışma durumu olduğu, espiyonaj faaliyeti ya da normal bir kriz durumu olduğuna karar verilmesindeki güçlüktür. Bu güçlük beraberinde krizin nasıl sonlandırılacağı sorununu getirmektedir. Krizleri fırsat olarak değerlendiren görüşlere göre ise krizin sonlandırılması krizle beraber gelen fırsatların değerlendirilmesini engellemektedir. Krizin bir süre daha devamının kriz sonrası reform ve öğrenme süreçlerine katkı sağlayacağını belirten görüşlerde (Trimintzios, Holfeldt, Uckan, & Gavrila, 2014) mevcuttur.

Siber güvenlik krizine neden olan problemin tam olarak belirlenmesi krizin sonlandırılmasında etken durumdadır. Problemin tam olarak ortaya konmaması durumu problemin devam edip etmediğinin belirlenmesini engellemektedir. Krizin teknik yetersizlikler nedeniyle mi yoksa teknik alanı çevreleyen karar mekanizmalarındaki problemlerden mi kaynakladığının belirlenmesi krize neden olan problemi ortaya çıkartacaktır. Dolayısıyla konuya hakimiyet, sorunun daha kolay çözümünü sağlayacaktır.

5.2.2.6. Öğrenme ve Reform

Öğrenme ve reform aşaması kriz yönetiminin önemli bir parçasıdır. Krizler doğası gereği öngörülemeyen nedenlere sahip olduğu için krizlerin sonlanması sonrasında bir önceki krizin nedenleri artık belirgin durumdadır. Siber güvenlik krizlerinde kriz sonrası detaylı bir dijital kayıt bilgisi analizi, hem krizin zararlarının boyutlarını ortaya çıkartacaktır hem de aynı nedenlerden dolayı krizin oluşmasını engellemek için gerekli düzenlemelerin yapılmasını sağlayacaktır. Kimi durumlarda kurum ve kuruluşlarda reform yapma isteksizliği görülebilir. Siber güvenlik alanında krize neden olan süreçlere ilişkin düzenlemenin yapılmaması ise bir diğer krizin kapısını aralayacaktır. İngiltere'de 2017 yılında sağlık sektöründe yaşanan kriz değerlendirildiğinde krizin temel sebebinin o dönemde ortaya çıkan işletim sistemi açıklıklarının zamanında giderilmemesi olduğu tespit edilmiştir (Dunton, 2020). Kriz sonrasında açıklık giderme planının düzenlenmemesi aynı krizin tekrar yaşanmasına neden olacaktır. Bu örnek diğer tüm siber güvenlik krizleri için geçerli bir durumu ifade etmektedir. Temel sebebi ise saldırganların denenmiş yöntemleri tekrar denemekteki ısrarı ve ikinci saldırı düzenleme için gerekli olan teknik bilgininin ilk kez düzenlenecek olan saldırılara göre çok daha az teknik kapasite ve beceri gerektirmesidir.

Kurum ve kuruluşlarının krizler sonucunda alınan dersleri paylaşımına yönelik bir alınan dersler platformunun oluşturulması krizlere hazır olma aşamasına olumlu katkı sağlayacaktır. Alınan derslerden öğrenme süreci ulusal çapta sınırlı kalmamalı siber uzayın tüm dünyayı kapsayan yapısı göz önünde bulundurularak küresel bazda araştırmalar yapılarak elde edilen bilgilerden faydalanılmalıdır. Siber alandaki geniş çaplı ve kapsamlı saldırılar, çoğu durumda belli bir zafiyet üzerinde inşa edilmekte ve ilgili zafiyet devam ettiği sürece, coğrafi sınırlardan bağımsız olarak bu saldırılara devam edilmektedir. Bu süreçte alınan dersler vasıtasıyla tecrübe paylaşımı saldırıların başarılı olma ihtimalini azaltacaktır.

Tatbikatlar vasıtasıyla süreçlerin test edilmesi bir diğer önemli öğrenme metodudur. Siber güvenlik kriz yönetimi özelinde daha hayati bir önem arz etmektedir. Olası bir siber güvenlik krizinin çıkış noktası teknik süreçlerin iyi organize edilmemesi ve uygulamalardaki eksiklikler olacaktır. Teknik bir faaliyetin testini ise yine teknik bir sorun yaratarak gerçekçi bir düzlemde test edebilir ve sonrasındaki süreçlerin işleyişini analiz edebilirsiniz. Siber güvenlik tatbikatlarında saldırgan rolünü üstlenen kırmızı takımlar oluşturularak mavi takım olarak adlandırılan kurum ve kuruluşların siber güvenlik birimleri ve altyapılarına kontrollü siber saldırılar düzenlenmekte, saldırıların başlamasıyla birlikte mavi takımlardan gelen bilgi akışına göre operatif ve stratejik seviyedeki süreçler başlatılarak analiz edilmektedir. Bu tarz tatbikatlara yönelik iyi bir örnek olarak NATO tarafından her yıl üye ülkelerin mavi takımları ve NATO genelinden katılımla oluşturulan kırmızı takım oluşturularak gerçekleştirilen Kilitli Kalkan Tatbikatı (NATO Resmi İnternet Sitesi, 2019) gösterilebilir. Bu tatbikatta sadece siber güvenlik personeli yer almakta ülkelerin stratejik iletişimden sorumlu birimleri, elektronik haberleşme gibi kritik altyapı yöneticileri ve hukuk uzmanları da katılım sağlamaktadır.

5.2.2.7. Siber Güvenlik Krizlerinde İletişim

Kriz yönetiminde iletişimin sahip olduğu özel durum, çalışmanın önceki aşamalarında belirtilmiştir. Ulusal çapta yaşanan siber güvenlik olaylarına yönelik gerekli şeffaflık ve bilgilendirmenin yapılmaması kamuoyunun yönlendirilmesine açık ve bilgi kirliliğinin hızla büyümesine neden olmaktadır. Bu durum siber saldırıların temel hedeflerinden olan itibar kaybettirme ile sonuçlanabilecektir (Zhan & Borden, 2019, s. 1336). Siber güvenlik krizinin teknik, operatif ve stratejik seviye yöneticilerine aktarılan bilginin akışkanlığının sağlanması ve idari seviyelere bilgi aktarılırken teknik bir dil yerine süreçlere olan etkilerin ve olası sonuçların yer aldığı bir tanımla gerçekleştirilmesi gerçekçi çözümlerin bulunmasını destekleyecektir.

Ulusal siber güvenlik krizlerinin yönetiminde, stratejik seviyedeki iletişim önem arz etmektedir. Krizin teknik boyutu ve tehdit aktörü belirlenmeden stratejik seviyede gerçekleştirilen açıklamalarda dikkatli olunmalıdır. Örneğin tehdit aktörü yabancı ülke vatandaşı siber suçlularsa ve ulus devlet aktörü ile bağı kanıtlanamıyorsa bu durumda ülkeler arası ikili hukuk devreye girmekte,[19] resmi siber etki güçleriyle karşılık vererek krizi siber çatışma seviyesine yükseltmek uluslararası hukuk açısından mümkün olamayacaktır. Askeri ve ekonomik güvenlik sektörlerinde siber alanda yaşanmayan diğer krizlerle eş zamanlı olarak siber krizlerin baş gösterdiği durumlarda benzer bir durum söz konusu olacaktır. Krizin yaşandığı tüm sektörlerin kendine özgü tehdit analizi, saldırı vektörü ve tehdit aktörlerin niyet ve maksadının belirlenmesi için stratejik seviyede çok boyutlu bir iletişim ihtiyacını ortaya çıkaracaktır. Gerçekleştirilecek olan ulusal seviyedeki kriz yönetimi tatbikatlarında iletişim organizasyonu ve altyapısının testine yönelik özel senaryolar geliştirmeli ve kriz öncesi dönemde iletişim organizasyonu ve altyapısının eksikleri tespit edilmelidir.

Siber güvenlik krizinden etkilenen ya da krizin derinleşmesi ile etkilenme potansiyeline sahip kritik kamu ve özel sektör kuruluşlarının koordinasyon içerisinde olması krizin çözümünde ve ilerlemesinin engellenmesi için önemlidir. Teknik anlamda karşılıklı iletişim ve bilgi paylaşımı yoluyla krize neden siber saldırı türünün diğer ülke içerisinde yayılması engellenebilir. Zararlı yazılım, sıfırıncı gün saldırısı gibi ileri seviye saldırıların etkisini azaltmak içinse ulusal çapta konunun uzmanlarından oluşan heyetler tarafından gerekli teknik analizler gerekebilir. Bu durumda bilgi paylaşımının hızlı, doğru ve tam olması gereklidir. Saldırıya uğrayan kurumun gerekli bilgileri eksik paylaşması konun çözümlenmesini engelleyecek ve zaman içerisinde ilgili saldırının diğer kurumlarda etkili olmasına neden olacaktır.

[19] Estonya'da 2007 yılında yaşanan siber güvenlik krizlerinin sonrasında NATO tarafından Estonya'nın başkenti Tallin'de Siber Savunma Mükemmellik Merkezi kurulmuştur. Bu merkez çatısı altında siber güvenlik alanına ilişkin önemli çalışmalar gerçekleştirilmektedir. Gerçekleştirilen önemli çalışmalardan bir tanesi de "Tallin Manual" olarak adlandırılan derleme kitap çalışmasıdır. Bu kitap NATO üyesi ülkelerin silahlı çatışma hukuku alanındaki uzmanlarının katkısıyla oluşturulmuş olup, zaman içerisinde siber çatışma hukuku konularında temel başvuru kaynağı haline gelmiştir.

5.3 TÜRKİYE'DE SİBER GÜVENLİK KRİZLERİ VE YÖNETİMİ

Kriz yönetimi kavramı yeni bir kavram değildir. Tarihin her evresinde yönetici ve askeri kesim ülke güvenliğine ilişkin belirsizlikleri azaltacak tedbirler almışlar ve belirsizlik durumunu azaltacak bilginin peşinde olmuşlardır. Ülkelerin dış ve iç güvenliğini tehdit edebilecek olan krizlerin oluşmadan önlenmesi, en az zararla atlatılması devletler için bir beka meselesi olmuştur. Soğuk savaş sonrası dünyanın değişen güvenlik gündemi ve teknolojik ilerlemeler yeni güvenlik sorunlarını beraberinde getirmiştir. Siber uzay güvenliği söz konusu güvenlik sahalarından birisi olarak belirmiştir.

Ülkemizdeki siber güvenlik faaliyetlerini daha önce ele alınmıştı. 2006 yılı sonrasında ülkemizde artan bir ivme ile siber güvenlik tedbirlerinin alınmasında, kurumlar kendi sorumluluk sahalarına göre kendilerini konumlandırarak gerekli gördükleri aksiyomları almaya çalışmışlardır. Siber güvenlik alanında yaşanan krizler siber uzayın kapsamını ele aldığımızda, kamu siber güvenliğini tehdit eden krizler zamanında önlenemez veya süreç düzgün yönetilemez ise bu krizlerin sosyal, siyasal, ekonomik, sağlık gibi pek çok alanda başka krizleri tetikleyeceği ve ülke genelinde topyekün bir güvenlik krizine neden olabileceği düşüncesi, gerek ülkemizdeki resmi belgelerde ve cumhurbaşkanlığı dahil olmak üzere ülkenin stratejik yönetim seviyelerinin beyanlarında kendine yer bulmuştur.

Çalışmanın bu aşamasında siber güvenlik krizlerinin yukarıda ele alınan önemine binaen kamu kriz yönetimi faaliyetlerindeki konumu ve günümüze kadar ki icraatlar analiz edilmiştir. Siber güvenlik kavramının kriz yönetimi amaçlı analizinin yapılacağı bu aşamada, siber güvenlik krizlerinin sadece kriz anındaki yönetimi yerine daha proaktif bir bakış açısıyla kriz öncesi dönemdeki önleyici faaliyetler ve sonrasında yapılması gereken geri besleme faaliyetleri kapsamlı olarak analiz edilmiştir. Bunun için öncelikle etkin, kapsamlı ve proaktif bir siber güvenlik kriz yönetiminin kendine özgü aşamaları belirlenmiş, ortaya çıkan

kategorilere göre kamu genelini ilgilendiren resmi düzenlemeler analiz edilerek ilgili kategorilerin altı doldurulmaya çalışılmıştır.

5.3.1 Kamuda Kriz Yönetimi

Ülkemizde afet yönetimine ilişkin ilk çalışmalar 1939 Erzincan Depremi sonrası başlamış kriz yönetimine yönelik kapsamlı ilk çalışmalar ise 1997 yılında başlamıştır (Çapar ve Koca, 2017, s. 7). 1997 yılında ülke genelinde meydana gelen krizleri yönetmek maksadıyla başbakanlığa bağlı olarak Başbakanlık Kriz Yönetim Merkezi oluşturulmuştur. 17 Ağustos 1999'da meydana gelen deprem afet ve afet kaynaklı krizlerin yönetimine ilişkin mevcut mevzuatın eksiklikleri ortaya çıkarmıştır. 2009 yılında yayımlanan 5902 sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanun gereği Başbakanlığa bağlı Afet ve Acil Durum yönetimi başkanlığı oluşturulmuştur.

2011/1377 sayılı Bakanlar Kurulu kararı ile yürürlüğe giren "Afet ve Acil Durum Yönetim Merkezleri Yönetmeliği", Başbakanlık Kriz Yönetim Merkezleri Yönetmeliğini yürürlükten kaldırmıştır. 2011 yılında Başbakanlık AFAD Başkanlığınca "Afet ve Acil Durum Yönetim Merkezleri Yönetmeliğinin" yürürlüğe konulması ile birlikte, "Başbakanlık Kriz Yönetim Merkezleri Yönetmeliği" yürürlükten kaldırılarak, kriz yönetiminden risk yönetimine geçiş süreci tamamlanmıştır" (GAMER El Kitabı, 2018, s. 11).

"Başbakanlık Kriz Yönetim Merkezi Yönetmeliğinin yürürlükten kaldırılmasıyla; terör olayları, yaygın şiddet hareketleri, ağır ekonomik bunalımlar, siber saldırılar, enerji arz güvenliği, Milli güvenliğimiz ile hak ve menfaatlerimizi tehdit eden yurt dışı kaynaklı gelişmeler, deniz/çevre kirliliği alanlarında; koordinasyonun nasıl ve hangi kurum tarafından sağlanacağı konusunda, yöntem ve yönetim boşlukları ortaya çıkmıştır (GAMER El Kitabı, 2018, s. 12)." Ortaya çıkan bu ihtiyaç çerçevesinde, Başbakanlıkça çıkarılan (2014/18) genelge ile Afet ve Acil Durum Yönetimi Başkanlığının görev alanına giren koordinasyon hizmetlerinden ayrı olarak, Başbakanlık Müsteşarı veya görevlendireceği Müsteşar Yardımcısının üst

koordinasyonunda, yurt içinde kamu düzenini ve güvenliğini ciddi şekilde bozucu nitelikte olayların yol açtığı acil durumlarda koordinasyon sağlama görevi İçişleri Bakanlığına verilmiştir.

Bu doğrultuda, "İçişleri Bakanlığı tarafından, ortaya çıkan boşlukların doldurulması amacıyla kendi teşkilat kanunu ile verilen görev ve 2014/18 sayılı Başbakanlık Genelgesi hükümleri doğrultusunda, güvenlik ve asayiş alanında faaliyet gösteren birim ve kuruluşlar arasında koordinasyon ve iş birliğini sağlamak üzere, Bakanlık merkez ile 81 ilde Güvenlik ve Acil Durumlar Koordinasyon Merkezleri (GAMER)" teşkil edilerek faaliyete geçirilmiştir. (GAMER El Kitabı, 2018, s. 14) Şekil-19'da görüleceği üzere GAMER güvenlik olayları odaklı bir görev tanımına sahip olup güvenlik olaylarının koordinasyonu ve çözümü üzerine kendisini konumlanmıştır. AFAD ise afet ve acil durum odaklı bir görev tanımına sahip olup, afet ve acil olaylarda risk yönetimi, müdahale, olay yönetimi, insani yardım konularının koordinasyonu ve çözümü üzerine kendisini konumlandırmıştır.

Şekil-19: GAMER ve AFAD Farklılıkları

5.3.2 Kamuda Siber Güvenlik Kriz Yönetimi

Çalışmanın daha önceki aşamalarında, Türkiye'de siber güvenlik faaliyetleri ele alınmıştır. Bu analiz esnasında ülkedeki siber güvenlik faaliyetlerinin kamu genelini ilgilendiren stratejik bir faaliyet olarak başlangıcının Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı olduğu tespit edilmiştir. İlgili doküman gereği, kritik altyapı sektörlerine özel sektörel SOME'lerin kurulması öngörülmüştür. Sonrasında gelişen faaliyetler neticesinde siber güvenliğin sağlanması gereken kritik altyapılar Enerji, Elektronik Haberleşme, Finans, Su Yönetimi, Kritik Kamu Hizmetleri, Ulaştırma şeklinde belirlenmiş ve ilgili sektörleri regüle eden resmi kurum kuruluşlara ilişkin uyulması gereken siber güvenlik tedbirleri belirlenmiştir. Düzenli olarak ilgili alt paydaşların denetlenmesini ve ilgili kritik altyapı sektörüne yönelik SOME ekipleri kurularak hiyerarşik olarak ulusal SOME görevini yürüten USOM altında birleştirilmiştir. Tüm bu gelişmeler Elektronik Haberleşme Kanunu gereği ülkemizde siber güvenlikten sorumlu bakanlık olan T.C. Ulaştırma Bakanlığı çatısı altında gerçekleşmiştir. 10 Temmuz 2018 tarihli ve 30474 sayılı Resmî Gazete'de yayımlanan 1 no'lu Cumhurbaşkanlığı Kararnamesi ile kurulan Dijital Dönüşüm Ofisi'ne (DDO) *"*Bilgi güvenliğini ve siber güvenliği artırıcı projeler geliştirmek*"* görevi verilmiştir. Bu çerçevede, 2019/12 sayılı Cumhurbaşkanlığı Genelgesi ile Bilgi ve İletişim Güvenliği Tedbirleri yayımlanmıştır. İlgili dokümanda kritik altyapı güvenliğinin sağlanmasına ilişkin minimum teknik isterler ve süreçler belirlenmiştir.

5 Ağustos 2016 tarihinde 5809 sayılı Elektronik Haberleşme Kanunu'na eklenen hükümler ile BTK'ya siber saldırıların engellenmesi ve caydırıcılığın sağlanması görevleri ile bu görevler kapsamında yükümlülüklerini yerine getirmeyen ilgili taraflara yaptırım uygulama yetkisi verilmiştir. Ayrıca 2013 yılında, "BTK bünyesinde faaliyetlerini sürdüren Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuş, belirlenen kritik altyapı sektörleri başta olmak üzere kurum ve kuruluşlarda Siber Olaylara Müdahale Ekipleri (SOME) faaliyetlerine başlamıştır (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023), 2020, s. 13-14)."

Ulusal siber güvenlik organizasyonunun oluşturulmasıyla ülkemizde kurumsal ve organizasyonel yapıların kurularak güçlendirilmesi sağlanmıştır.

Ulusal çaptaki krizlerin yönetiminden sorumlu olan iki temel kuruluş olan GAMER ve AFAD çalışmalarını siber güvenlik özelinde incelediğimizde siber güvenlik meselelerini kendi misyon vizyonları kapsamında ele aldıkları ve kendilerini bu alanda koordinatör makam olarak belirledikleri ortaya çıkmaktadır. GAMER bünyesi içerisinde yer alan Siber Güvenlik ve Bilgi Sistemleri Çalışma Grubu'nun görev tanımı incelendiğinde GAMER bünyesine yönelik sorumluluklar öne çıkmakta ulusal bazda siber güvenlik kriz yönetimi ve koordinasyonuna yönelik görevlendirmeden ziyade sorumlu kurumlara atıfta bulunularak alandaki alt paydaşlık belirlenmektedir.

Siber Güvenlik ve Bilgi Sistemleri Çalışma Grubu'nun görevleri şu şekilde açıklanmıştır;

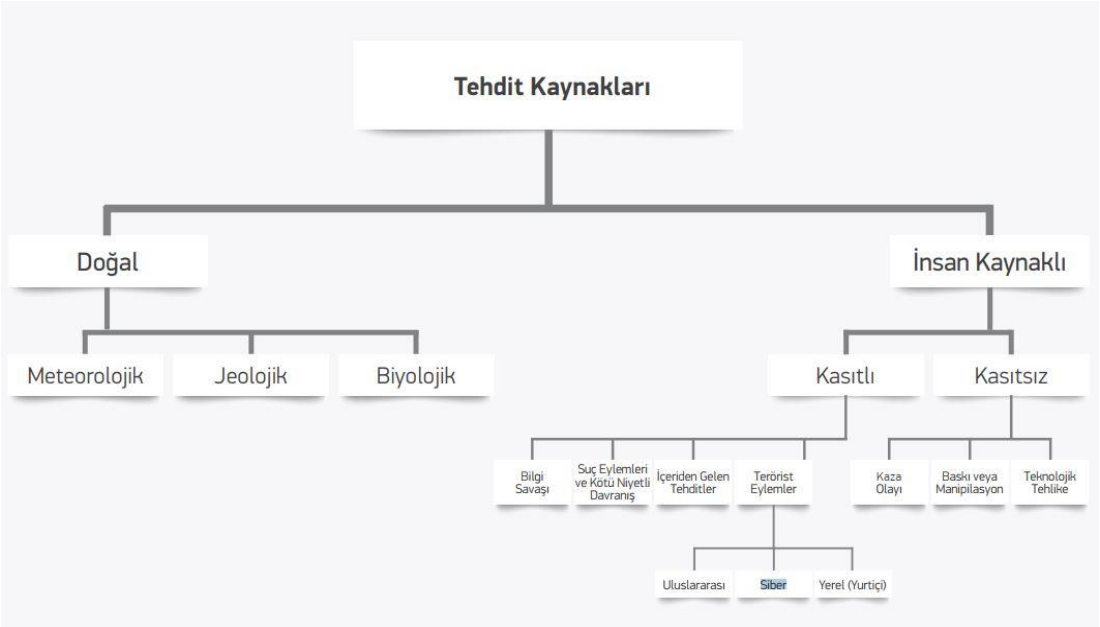
> "Siber güvenlik ihlal ve saldırılarına yönelik sorumlu kuruluşlar tarafından alınan kararları Başkanlıkta uygulamak,
> Siber güvenlik alanında görev yapan diğer kurumlarla irtibat sağlamak,
> GAMER Merkezinde bulunan bilgi sistemleri aktif bulunmasını sağlamak.
> GAMER Başkanı tarafından verilen benzer görevleri yapmak" (GAMER El Kitabı, 2018, s. 79).

Bir diğer kriz yönetim kuruluşu olan AFAD'ın yaklaşımı ise siber olayları teknolojik bir afet olarak ele almak ve kritik altyapı özelinde değerlendirmektir. Kritik altyapılara yönelik siber tehlikelerin ulusal çapta teknolojik afetlere neden olabileceği değerlendirilmektedir. AFAD tarafından tanımlanan kritik altyapı tehditlerinde siber alandaki tehditler, insan kaynaklı kasıtlı tehditlerin altında terörist eylemler başlığı altında sınıflandırılmaktadır (Bknz. Şekil-20).

Yukarıda ele alınan bilgiler ışığında siber uzayda meydana gelebilecek krizler, Türkiye'de elektronik haberleşme kritik altyapısının hasara uğraması odağında ele alınmakta ve elektronik haberleşme kanunundan alınan yetki doğrultusunda

gerekli sorumluluk Ulaştırma ve Altyapı Bakanlığı'na verilmektedir. Çalışmanın son döneminde çıkarılmış olan 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nda da bakanlığın bu misyonu açıkça belirtilmiş ve Cumhurbaşkanlığınca gelecekteki siber güvenlik faaliyetleri için temel doküman olarak belirlenmiştir. Çalışmanın bundan sonraki bölümünde ülkemizdeki siber güvenlik faaliyetleri, çalışmanın daha önceki aşamalarında ele alınmış olan siber güvenlik ve kriz yönetimi kavramları çerçevesinde incelenecektir.

Şekil-20: AFAD Kritik Altyapılara Yönelik Tehditler



Kaynak: (Kritik Altyapıların Korunması Yol Haritası Belgesi, 2014, s. 29).

5.3.2.1 Hazır Olma/Erken Uyarı/Önlem Alma

Siber güvenlik krizleri yönetiminin önemli aşamaları arasında hazır olma, erken uyarı ve önlem alma aşaması yer almakta ve en belirgin aksiyomlar bu aşamada gözlemlenmektedir. Siber güvenlik kavramı dünyada ve ülkemizde siber uzayın genişlemesi ile birlikte ilerleme kaydetmiştir. Önemli siber olaylar yaşandıkça siber güvenlik tedbirleri artan bir ivme ile anılmaya başlanmıştır. 1999 Kosova Savaşı esnasında NATO'ya karşı gerçekleştirilen siber saldırılar, ilk siber savaş denemesi olarak tarihe geçmiştir. Bu savaş esnasında yoğun bir hava

bombardımanı gerçekleştiren ABD kuvvetleri sahip olduğu siber saldırı kapasitesini konvansiyonel gücünü kullandığı ölçüde kullanmaktan çekinmiştir. ABD askeri birimleri, siber savaşta pandoranın kutusunu açan taraf olmaktan çekinmiştir. Bunun en temel nedeni ise konvansiyonel bir savaşa göre çok az maliyetle ciddi etki sağlanmasına neden olan siber saldırılara karşı kendi ve müttefik bilgi sistemlerinin mevcut zayıflıklarıdır. (The Guardian Resmi İnternet Sitesi, 1999) Bu dönemle beraber siber saldırılara karşı hazır olma durumu giderek artan bir öneme sahip olmaya başlamıştır.

2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı proaktif bir siber güvenlik yaklaşımı sunmaktadır. Belirlenen ulusal hedefler arasında siber olaylara müdahalenin olay öncesi, esnası ve sonrasını kapsayan bir bütün olmasından hareketle; proaktif siber savunma anlayışının geliştirilmeye devam edilmesi ilkesi eklenmiştir. Proaktif siber güvenlik tanımlamasının içerisine siber caydırıcılık kavramı da eklenerek hazır olma kavramı genişletilmiş ve askeri caydırıcılık kavramına benzetilmiştir. Gerçekleştirilecek çalışmalarla, proaktif savunmanın pekiştirilmesi, siber caydırıcılığın sağlanması ve saldırıların oluşmadan tespit edilerek önlem alınması sağlanacak ve siber uzayda birlikten doğan kuvvetle, güç artırımı hedeflenmiştir.

İlgili strateji belgesi öncesi dönemi ele aldığımızda siber güvenlik alanında 2006 yılında yaşanan dönüşümle beraber siber olaylara müdahele öncesinde gerekli tedbirlerin alınması, hazırlığa ilişkin gerekli teşkilatlanma gibi kavramlar öne çıkmaya başlamıştır. Devlet Planlama Teşkilatı Bilgi Toplumu Dairesi'nin 2005 yılında başlattığı **Bilgi Toplumu Stratejisi** çalışması içerisinde bilgi sistem güvenliği ile ilgili bir program da yer almıştır. Bu programı yürütmekle görevli TUBITAK BİLGEM Ağ Güvenliği Grubunun temel hedefi kamu kurum ve kuruluşları ile birlikte ülkemizde yer alan bilgi sistemlerinin güvenlik ihtiyaçlarının yürütülmesi olarak belirlenmişti. Bilgi Sistemleri Güvenlik Programı'nın önemli hedeflerinden birisi de ülkemizde bilgisayar ortamlarında yaşanabilecek bilgi güvenliği olaylarına doğru ve sağlıklı müdahaleyi gerçekleştirmek adına gerekli altyapıyı oluşturmaktı. Bu amaçla yine "TÜBİTAK BİLGEM"

bünyesinde “Bilgisayar Olaylarına Müdahale ekibi (TR-BOME)”[20] kuruldu. TR-BOME kritik kamu kurumlarında BOME yapılanmasının kurulabilmesi için gerekli eğitim ve koordinasyon faaliyetlerini yürüttü. Aktif olarak faaliyete geçtiği 2009 yılı ilk döneminde yurt dışından 258, yurt içinden 15 olmak üzere toplam 273 siber saldırı ihbarı TR-BOME’ye ulaştırılmıştır (Devlet Bilgisayarlarını Siber Ordu Koruyor, 2009). Ülkemiz zaman içerisinde alınan siber güvenlik önlemlerini daha üst seviyelere çıkarmıştır.

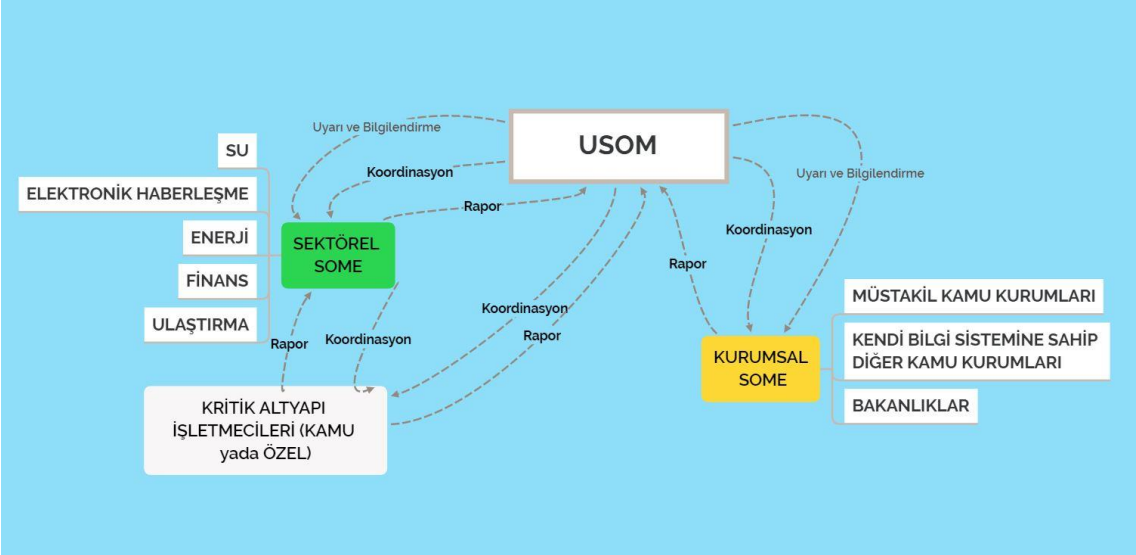
5.3.2.1.1 T.C. Ulaştırma ve Altyapı Bakanlığı Faaliyetleri

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın dördüncü maddesinde “Ulusal Siber Olaylara Müdahale Merkezinin (USOM) Kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) oluşturulması hedefi bulunmaktadır. Söz konusu eylem planı kapsamında temel görevi koordinasyon ve işbirliği olan Ulusal Siber Olaylara Müdahale Merkezi (USOM)” 27 Mayıs 2013 tarihinde kurularak, faaliyetlerine başlamıştır. Aynı eylem planı dahilinde kamu kurum ve kuruluşları organizasyonu içerisinde Siber Olaylara Müdahale Ekipleri (Kurumsal SOME, Sektörel SOME) oluşturulması belirlenmiştir. USOM ve SOME’ler siber olayları yönetme, oluşması muhtemel zararları önlemede veya azaltmada, siber olay yönetiminin ulusal düzeyde koordinasyon ve işbirliği içerisinde gerçekleştirilmesinde temel resmi organizasyonlardır (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014, s. 2). Siber olaylara müdahale organizasyonundaki üç temel bileşen USOM, Sektörel SOME’ler ve Kurumsal SOME’lerdir. Ülkemiz kamu kurumlarını ve kritik

[20] “Devlet Planlama Teşkilatı Müsteşarlığı (DPT) Bilgi Toplumu Dairesi Başkanlığı tarafından hazırlanan Bilgi Toplumu Stratejisi Eylem Planı'nın 88 inci maddesinde yer alan Ulusal Bilgi Sistemleri Güvenliği Programında BOME ile ilgili aşağıdaki ifadeler yer almaktadır.”
“Kurulacak olan BOME;
- Siber âlemdeki güvenlik tehditlerini sürekli olarak takip edecek,
- Uyarılar yayınlayacak,
- Tespit edilen risklere karşı ne şekilde tedbir alınabileceğine dair bilgilendirme yapacaktır.
- Risklerin ortaya çıkması durumunda karşı tedbirleri koordine edebilecek bir “bilgisayar olaylarına acil müdahale merkezi (CERT) olarak gerekli müdahaleleleri gerçekleştirecektir. Ayrıca, Kamu kurumları için gerekli minimum güvenlik seviyeleri kurum ve yapılan işlem bazında tanımlanacak. kurumlar tarafından kullanılan sistem. Yazılım ve ağları güvenlik seviyeleri tespit edilecek ve eksikliklerin giderilmesi yönünde öneriler oluşturulacaktır.”

altyapıları içine alan siber olaylara müdahale organizasyonu Şekil-21'de sunulmuştur.

Şekil-21: Ulusal Siber Olaylara Müdahale Organizasyonu



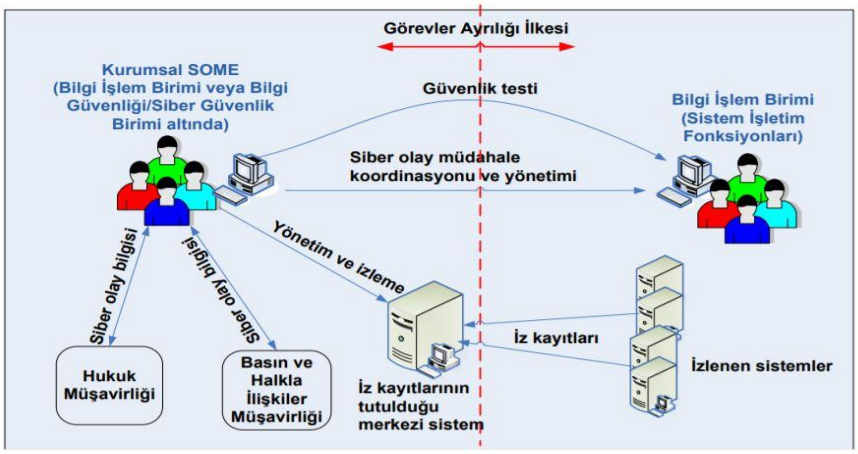
Kaynak: (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014).

Şekil-21 incelendiğinde ulusal siber güvenlik olayları yönetiminin uyarı, koordinasyon ve iletişim üzerine kurulduğu görülecektir. USOM bilgi kaynaklarından aldığı bilgiyi yukarıdan aşağıya doğru gönderirken SOME'ler tarafından bildirilen siber olayları diğer paydaşlarla paylaşmakta ve koordinasyonunu sağlamaktadır. Şekil'de şu bilgiler yer almıştır (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014):

"**Uyarı ve bilgilendirme:** Siber olay öncesinde USOM tarafından hazırlanan bülten, duyuru gibi bilgileri,
Koordinasyon: Siber olay esnasında USOM ve varsa bağlı olduğu Sektörel SOME tarafından yapılan koordinasyonu,
Rapor, form ve bilgilendirme: Siber olay öncesi, esnası ve sonrasında USOM ve varsa bağlı olduğu Sektörel SOME tarafından talep edilen ve Kurumsal SOME'ler tarafından iletilen bilgileri, ifade etmektedir."

Kurumsal SOME'ler siber olay öncesinde erken uyarı sistemleri kurup işletirler. Bunun için bilgi sistemleri tarafından oluşturulan iz bilgilerini kayıt altına alırlar ve gelen bilgileri analiz ederek saldırının başladığı andan itibaren saldırıdan haberdar olmaya ve gerekli aksiyomları almaya çalışırlar. Kurumsal SOME'ler siber olay öncesi, esnası ve sonrasında, siber güvenliği yönetmek amacıyla kurumdaki bilgi işlem birimi ve varsa hukuk ve basın / halkla ilişkiler müşavirlikleri ile birlikte çalışır. Ulusal siber olay müdahale ve yönetim teşkilatı kurulurken siber güvenlik olaylarının hukuk ve halkla ilişkiler boyutu düşünülerek gerekli teşkilatlanma gerçekleştirilmiştir. Bu konu Şekil-22'de verilirmiştir.

Şekil-22: Kurumsal SOME'nin Kurum İçindeki Paydaşları ve Temel Fonksiyonları

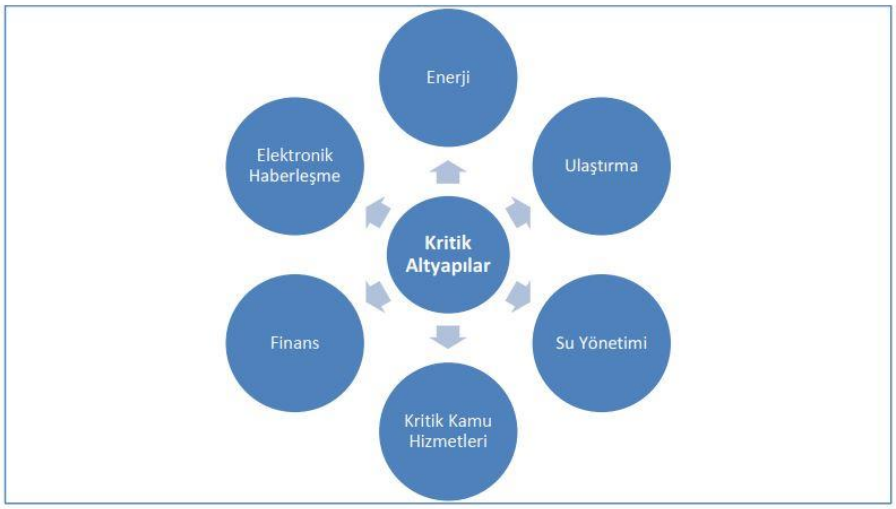


Kaynak: (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014).

Kalkınma Bakanlığı 2012 Yatırım Programı içerisinde yer alan "Kritik Altyapılarda Bilgi Güvenliği Yönetimi Projesi" doğrultusunda kritik altyapıların ve kritik altyapıları barındıran kritik sektörlerin ortaya çıkarılması için çalışmalar gerçekleştirilmiştir. Bu çalışmalar neticesinde Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın 5 numaralı eylem maddesi kapsamında Siber Güvenlik Kurulu'nca ilk etapta "Ulaştırma, Enerji, Elektronik Haberleşme, Finans, Su Yönetimi, Kritik Kamu Hizmetleri" ülkemizin kritik sektörleri olarak belirlenmiştir (Bknz. Şekil-23). Bu kritik sektörlerin düzenleyicisi konumunda bulunan ve Sektörel SOME kurma yükümlülüğüne sahip olan kurum ve bakanlıkların faydalanması, Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ'de yer alan hükümlerin

açıklanması ve kurumlara yardımcı olması maksadıyla “Sektörel SOME Kurulum ve Yönetim Rehberi” dokümanı T.C. Ulaştırma ve Altyapı Bakanlığı’nca hazırlanmıştır.

Şekil-23: Türkiye’nin Kritik Altyapı Sektörleri



Kaynak: (Sektörel SOME Kurulum ve Yönetim Rehberi, 2014).

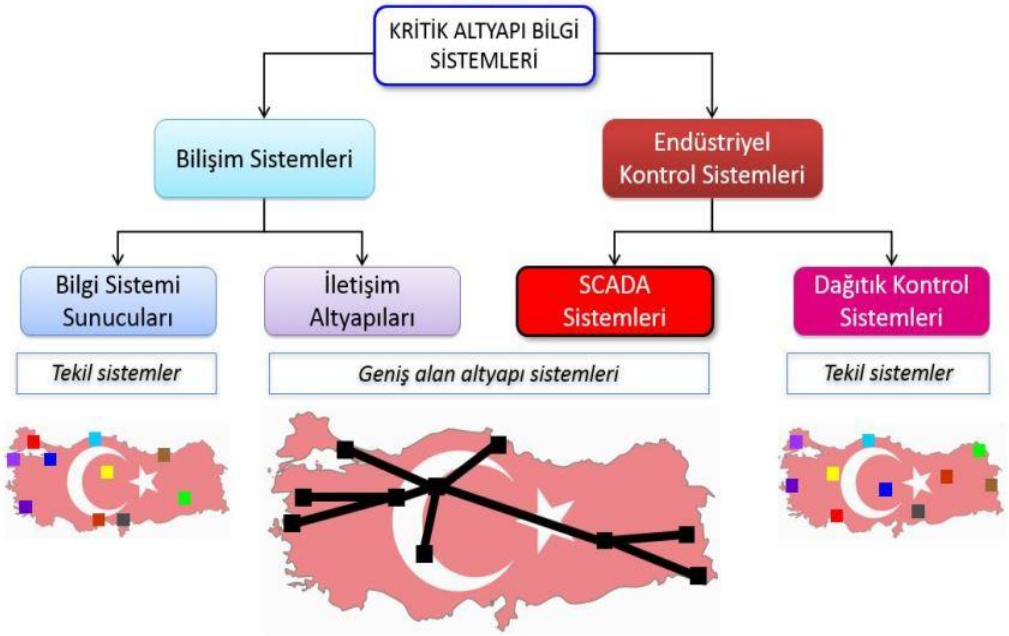
Sektörel SOME’ler sektöre yönelik siber güvenlik ilkeleri gerekli olduğu durumlarda USOM ile işbirliği içerisinde belirlemekte ve bu ilkelerin uygulandığını kontrol etmektedir. Siber Güvenlik Kurulunun aldığı stratejik kararın sektörel seviyedeki karşılığı Sektörel SOME’ler tarafından yerine getirilmesi esası benimsenmiştir. Sektörel SOME’ler, sorumluluk alanındaki sektörde faaliyet gösteren kurum ve kuruluşları bilgilendirme ve başlıca siber güvenlik çözümleri hakkında bilgi sağlama hizmeti vermektedir. Aynı zamanda kendi sorumluluk sahasında yer alan kritik sektörü kapsayacak şekilde siber saldırı uyarısı ve güvenlik açığı duyurusu yayınlarlar (Sektörel SOME Kurulum ve Yönetim Rehberi, 2014, s. 13).

Sektörel SOME’ler tarafından alınacak kritik altyapı önlemlerine yönelik Kritik Altyapı Asgari Güvenlik Dokümanı, T.C. Ulaştırma ve Altyapı Bakanlığı

tarafından yayımlanmış, asgari siber güvenlik tedbirleri belirlenmiştir. İlgili dokümanda kritik altyapılara siber güvenlik odaklı bir tanımlama yapılarak Kritik altyapı kavramı; "işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim veya endüstriyel kontrol sistemlerini barındıran sistemler" olarak tanımlanmıştır. Kritik altyapılar üç ana katmana ayrıştırılmıştır. Bunlar genel olarak fiziksel varlıklar, insan kaynakları, bilişim sistem ve varlıkları şeklinde belirlenmiştir. Kritik altyapıların belli bir bölümü sadece bilişim sistemlerinden oluşmaktadır. Kritik altyapıların bazı hizmetleri bilinen bilişim sistemleri üzerinden gerçekleştirilirken bazı hizmetler de Endüstriyel Kontrol Sistemleri (EKS) olarak adlandırılan özel bilişim sistemleri tarafından gerçekleştirilmekte ve gözlem altında tutulmaktadır. Endüstriyel Kontrol Sistemleri, topolojilerine ve içerdikleri bileşenlere göre SCADA ve DKS olarak ikiye ayrılmaktadır. Bu durumda, bilişim sistemleri açısından, kritik altyapı bilgi sistemlerini dört farklı kategoride ele alınması mümkün olmaktadır (Bknz. Şekil-24).

T.C. Ulaştırma ve Altyapı Bakanlığı tarafından, kurumların kendi güvenlik sistemlerini test etmeleri maksadıyla Kurumlar İçin Siber Güvenlik Önlemlerini Ölçme Testi Dokümanı hazırlanarak yayımlanmıştır. Bahse konu doküman incelendiğinde yüzeysel bir çalışma göze çarpmaktadır. Yayımlandığı günün, halen de yayımda olması nedeniyle günümüz, siber güvenlik ihtiyaçlarının test edilmesinden uzak bir görüntü çizmektedir. Bu kapsamda aşağıda ele alınacak olan Bilgi ve İletişim Güvenliği Rehberi alınması gereken önlemlerin belirlenmesinde daha kapsayıcı bir doküman olarak karşımıza çıkmakta ve Cumhurbaşkanlığı genelgesi ile uygulanmasının zorunluluk haline getirilmesi nedeniyle hukuken de daha zorlayıcı bir konumda yer almaktadır.

Şekil-24: Kritik Altyapı Bilgi Sistemleri



Kaynak: (Kritik Altyapı Bilgi Sistemleri için Asgari Güvenlik Önlemleri Dokümanı, 2015, s. 6).

Ulaştırma Bakanlığı tarafından belirlenen önleyici, siber olaylara hazır olma ve siber olay yönetim süreçleri özetlendiğinde, SOME organizasyonu temelli bir yaklaşım sergilendiği ve gerekli düzenlemelerin bu organizasyonun verimli ve çağın gereklerini yerine getirmesine yönelik gerçekleştirildiği tespit edilmiştir. Ancak elde edilen bulgularda günümüz siber güvenlik tehdit ve risklerine cevap veren genel teknik ve idari hususlarının tümünü kapsayan, yaptırım gücü yüksek bir düzenleme bugüne kadar gerçekleştirilmemiştir. Güvenli KamuNet Ağı, çalışmanın önceki bölümlerinde ele alınmıştır. İlgili düzenlemeler güvenli, bir kamu ağını ortaya çıkarmıştır. Ancak resmi düzenlemelerde kapsamlı bir teknik ister belirlenmemiş gerekli gereksinimler uluslararası bir bilgi güvenliği standardı olan 27001 Bilgi Güvenliği Yönetim Sistemi vasıtasıyla giderilmeye çalışılmıştır. Bilgi ve İletişim Güvenliği Rehberi'nin yayımlanması ile bu alanda yer alan boşluklar doldurulmaya çalışılmıştır.

5.3.2.1.2. Dijital Dönüşüm Ofisi Faaliyetleri

Türkiye'deki siber güvenlik gelişimlerini ele alırken, T.C. Dijital Dönüşüm Ofisi'nin siber güvenlik faaliyetlerini ele alınmıştır. Siber güvenlik krizlerinin önlenmesine yönelik alınan tedbirler, dayanıklılık ve hazır olmaya yönelik faaliyetler söz konusu olduğunda DDO önemli bir aktör olarak karşımıza çıkmaktadır. 2019 yılında DDO faaliyetleri kapsamında yayımlanan Cumhurbaşkanlığı Siber Güvenlik genelgesi temel siber güvenlik tedbir ve uygulamalarını tanımlamıştır. Bahse konu genelge de ayrıca "güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla ulusal ve uluslararası standartlar ve bilgi güvenliği kriterleri çerçevesinde", kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerde uygulanmak üzere farklı güvenlik seviyeleri içeren "Bilgi ve İletişim Güvenliği Rehberi" Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı koordinasyonunda, ilgili kamu kurum ve kuruluşları tarafından gereken katkı sağlanarak hazırlanacak ve www.cbddo.gov.tr adresinde yayımlanması öngörülmüş ve ilgili rehber 10 Temmuz 2020 tarihinde yayımlanarak yürürlüğe girmiştir.

Rehber, "bilgi güvenliği risklerinin azaltılması, ortadan kaldırılması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik bilgi/verinin güvenliğinin sağlanması için asgari güvenlik tedbirlerinin belirlenmesi ve belirlenen tedbirlerin uygulanması için yürütülecek faaliyetlerin tanımlanması" amacıyla yayımlanmıştır. Rehber, geniş bir kapsama sahip olup, bilgi işlem birimi barındıran veya bilgi işlem hizmetlerini sözleşmeler çerçevesinde üçüncü taraflardan alan, devlet teşkilatı içerisinde yer alan kurum ve kuruluşlar ile kritik altyapı hizmeti veren işletmeleri kapsamaktadır. Rehber kapsamına giren tüm kurum ve kuruluşlar ilgili Cumhurbaşkanlığı genelgesi gereği rehbere uyum sağlamakla mükelleftirler. Rehber kapsamında 12 hedef planlanmıştır. İlgili

hedefler incelendiğinde önlem alma ve dayanıklılığa ilişkin maddeler öne çıkmaktadır: İlgili durum aşağıda Şekil-25'te açıklanmıştır.

Şekil-25. Bilgi ve İletişim Güvenliği Rehberinin Hedefleri

Kaynak: (Bilgi ve İletişim Güvenliği Rehberi, 2020).

Rehber, risk yönetimi odaklı bir yaklaşım içerisindedir. Bu kapsamda risklerin bilgi sistem varlıkları bazında tek tek ele alınması öngörülmektedir. Bilgi sistem varlıkları sınıflandırılırken sadece bilgisayar, ağ cihazı gibi donanımsal varlıklar tanımlanmamış, kurum binaları, personel, uygulamalar gibi varlıklarda tanımlanarak varlık grupları çeşitlendirilmiştir. Personel varlık gurubuna ilişkin kamu için kritik faaliyette bulunan personelin güvenlik soruşturmasının gerçekleştirilmesi ön şart olarak belirlenmiştir. Varlık gruplarının belirlenmesinin ardından bu varlık gruplarının hangi kritiklik derecesine sahip olduğunun belirlenmesi ön görülmüştür. Her bir varlık grubunun kritiklik derecesinin, işlenen verinin gizlilik, bütünlük ve erişilebilirlik açısından kritikliği ile oluşabilecek güvenlik ihlallerinin etki alanları dikkate alınarak belirlenmesi gerektiği değerlendirilmiştir. Bu durum Şekil-26'te verilmiştir.

Şekil-26: Kritiklik Derecesi Belirlemek İçin Kullanılan Boyutlar

Kaynak: (Bilgi ve İletişim Güvenliği Rehberi, 2020, s. 24).

Olası güvenlik krizlerine hazır olmak için gerekli insan gücünün yetiştirilmesi rehberde öne çıkan bir diğer kıstastır. Bilgi güvenliğinin sağlanmasında en zayıf halkanın insan faktörü olduğu belirtilerek kurum personelinin gerekli yetkinliğe sahip olması öngörülmüştür. Personelin gelişimini ölçecek gerekli mekanizmaların kurulumunun yapılması ve bilginin beceriye dönüştürülmesi için eğitimlerin sadece teorik bilgi vermekten ziyade, personelin ilgili alanda pratik becerisini arttıracak uygulamaları içermesi önerilmektedir (Bilgi ve İletişim Güvenliği Rehberi, 2020, s. 29).

5.3.2.2. Algılama Düzeyi Oluşturma

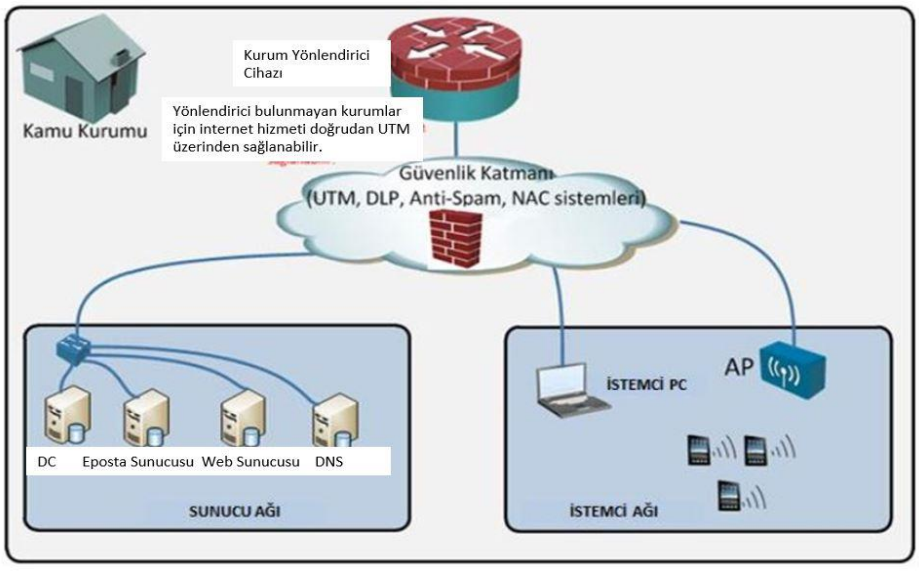
Siber güvenlik krizlerinin yönetiminde bir diğer önemli aşama, algılama düzeyi oluşturma aşamasıdır. Bu aşama kendisinden önceki ve sonrasındaki aşamalara geçişkenliğe sahip olup bu aşamalarda belirleyici özelliğe sahiptir. Bir önceki aşamada açıklanan güvenlik önlem ve tedbirleri, siber güvenlik olay yönetimi, hazır olma faaliyetlerini, oluşturulan algılama düzeyi yakından etkilemektedir. Güvenlikleştirme teorisinin siber güvenlik alanına uygulanmasında algılama düzeyi oluşturulması hangi risk ve tehditlerin siber güvenlikleştirme meselesi olarak ele alınacağının belirlenmesinde kritik öneme sahiptir. Olayların tespiti ve önleme, hazır olma durumu algılama düzeyi oluşturma safhasını beslemektedir (Backman, 2020, s. 5). Gerekli hazırlık ve dayanıklılıkla siber olaylar tırmanışa geçmeden bertaraf edildiği durumlar, genellikle siber güvenlik krizi olarak algılanmazlar ancak kimi durumlarda olayın nevi ve kurumun ya da ulusal düzeydeki politik atmosferin durumuna göre zamanında önlenebilmiş olan siber olaylar siber güvenlik krizi olarak stratejik yönetim tarafından gündeme getirilebilir.

Ülkemiz üzerinden örneklendirecek olursak, yukarıda ele alınmış olan USOM'a verilen görevler, izleme ve koordinasyon şeklinde icra edilmektedir. Teknik kapasite ve işleyişte bu yönde mimarilendirilmiş ve USOM tarafından aktif bir siber güvenlik tedbiri alınmamıştır. Yine yayımlanan resmi KamuNet güvenlik mimarisi ele alındığında aktif güvenlik tedbirleri, kurumlar tarafından alınmaktadır (Bknz. Şekil-27). Olası bir siber saldırıda aktif savunma, kurumların güvenlik birimleri tarafından gerçekleştirilecektir. USOM tarafından gerçekleştirilen faaliyetler sadece erken uyarı ve tespit seviyesinde kalacaktır. USOM bu anlamda koruma sağlayan bir kale olmaktan ziyade bir gözetleme kulesi görevi görmektedir. Teknik olarak konu değerlendirildiğinde de tek bir merkezden siber güvenlik koruması gerçekleştirilmesi imkansızdır. Ancak basın kuruluşları tarafından USOM faaliyetleri için farklı bir algı oluşturularak, aktif güvenliğinde sağlandığı bir merkez kuruldu algısı oluşturulmaktadır. Bu merkez de işletilen milli yazılımlara ilişkin bu algı oluşturma sürecinden etkilenerek aktif siber savunma

ürünü olarak öne çıkarılmaktadırlar (Ünal, 2020). Örneklendirecek olursak zararlı yazılım analizi bir sistemin zararlı bir yazılımdan etkilenmesinin tespitinden sonra gerçekleştirilen bir faaliyettir (Souppaya, 2013, s. 10), etkili bir zararlı yazılım analizi ile aktif önleyici bir tedbir alınmaktan ziyade zararlı yazılımın yayılımı önlenebilir.

Siber güvenlik krizlerinin boyutunun tespiti, gelişimi ve olası etkilerini kestirmek teknik boyutunun her geçen gün değişmesi ve genişlemesi ve bu gelişime paralel olarak bireylerin, kamu kurum ve kuruluşlarının siber uzaya bağımlılığının artması nedeniyle güçleşmektedir. Algılama düzeyinin bir diğer önemli fonksiyonu da, bu noktada ortaya çıkmaktadır. Krizin odağının belirlenmesi ve hangi sektörlere sıçrayabilmesini öngörebilmek için siber güvenliğe ilişkin güncel tehditleri ön görebilen bir algılama düzeyinin oluşturulması gereklidir. Bu kapsamda gerçekleştirilen düzenlemelerde yer alan siber güvenlik tanımlamaları siber güvenlik algı düzeyinin seviyesini ölçmekte yol gösterici olacaktır. Bir diğer önemli başvuru noktamız da daha önce ele alındığı üzere ülkemizdeki erken dönem siber güvenlik çalışmalarının başlatıldığı bilgi toplumu dairesi faaliyetleri olacaktır.

Şekil-27 KamuNet Güvenlik Mimarisi



Kaynak: (Kamu Kurum ve Kuruluşlarının KamuNet'e Dahil Edilmesi, 2016).

Kalkınma Bakanlığı bünyesinde, Bilgi Toplumu Dairesinin kurulması "2002 yılında 58. Hükümet tarafından hazırlanan Acil Eylem Planına" dayanmaktadır. "E-Dönüşüm Türkiye Projesi'nin koordinasyonunu yürütmek, kamu kurumlarının bilgi ve iletişim teknolojisi yatırımları arasında eşgüdüm sağlamak ve bilgi toplumu olma yolunda atılması gereken adımlara ilişkin stratejileri belirlemek" üzere, 2003 yılı Mart ayında Devlet Planlama Teşkilatı bünyesinde Bilgi Toplumu Dairesi (BTD) kurulmuştur (Bilgi Toplumu Dairesi Hakkında, 2020). İlgili daire başkanlığı tarafından koordine edilerek yayımlanan E-Türkiye Girişimi Raporunda, dönemdeki siber güvenliğe bakış açısının bilgi sistem güvenliği temelli olması nedeniyle bilgi sistem güvenliğine ilişkin önemli planlamalar ve öngörüler mevcuttur. İlgili rapor incelendiğinde bu dönemde ortaya konan algı düzeyinin etkilerinin günümüzü halen etkilediği pek çok kavramın algı biçiminin aynı kaldığı görülmektedir. Bilgi güvenliği ve bilgi sistem güvenliğinin kamu kurum kuruluşları için kritik öneme sahip olduğu bu dönemde gündemde yer almakta ve gerekli düzenlemelerin yapılmasının elzem olduğu belirtilmektedir. Aynı rapor içerisinde göze çarpan bir diğer nokta, ulusal bilgi güvenliği kanunu taslağıdır (e-Türkiye Girişimi I. Ara Rapor, 2002). İlerleyen dönemde siber güvenlik yasa tasarısına dönüşecek bu taslak günümüzde artık gündemde bulunmamakta ulusal siber güvenlik stratejilerinde kendisinden bahsedilmemektedir. Çalışma boyunca göze çarpan bir unsur olarak beliren siber güvenlik yönetimi için merkezileşmiş, ulusal bir güvenlik kurumu yokluğu erken dönem siber güvenlik çalışmalarında öngörülmüş ancak dönem içinde değişen siber güvenlik algı düzeyi, önce siber güvenlik kurulunu[21] ortaya çıkarmış, son dönemde ise bu kurulu mülga ederek T.C. Ulaştırma ve Altyapı Bakanlığı'nı siber güvenlikten sorumlu merkezi kurum olarak belirlenmesini sağlamıştır. Adı geçen kanun tasarısı incelendiğinde, o dönemki siber güvenlik algısının daha çok devlet odaklı ve devlete ait bilginin güvenliği ön planda tutulurken daha önce ele alınan 2020 tarihli Bilgi ve İletişim Güvenliği rehberinde özel sektör ve bireysel siber güvenlik

[21] Adı geçen kanun tasarısında ayrıca bir ulusal bilgi güvenliği kurulu kurulması öngörülmüştür. Sonrasında kurulan Siber Güvenlik Kurulu'na Ulaştırma Bakanı başkanlık ederken tasarıda kurul başkanı olarak Başbakan belirlenmiştir. Sadece bakanlık düzeyinde bir yaklaşım yerine Başbakanlık seviyesinde tüm hükümet organlarını harekete geçirebilecek bir yapı öngörülmüştür.

konuları da kritik bir siber güvenlik faaliyeti olarak değerlendirilmiştir (Bilgi ve İletişim Güvenliği Rehberi, 2020).

“Bu Kanun; ulusal güvenliği ilgilendiren, çok gizli, gizli, özel ve hizmete özel gizlilik dereceli askeri, istihbari, dış ilişkiler, ekonomik, teknolojik, bilimsel, ticari ve diğer alanlardaki bilgilerin korunması, Devletin bilgi güvenliği faaliyetlerinin geliştirilmesi, gerekli politikaların üretilmesi ve belirlenmesi, kısa ve uzun dönemli planların hazırlanması, kriter ve esasların saptanması, ihracat ve ithalat izinleri ile ilgili görüş ve sertifikaların verilmesi, uygulamanın takip ve denetimi, kamu kurum, kurul ve kuruluşları ile özel kuruluşlar arasında koordinasyonun sağlanması için teşkilatın kurulması ve görevlerine ilişkin usul ve esasları düzenler.”

“Ulusal bilgi güvenliği: Ulusal güvenliği ilgilendiren, yetkisiz ellere geçtiği takdirde, Devlet, kamu kurum, kurul ve kuruluşları ile özel kuruluşlar ve diğer gerçek ve tüzel kişilerin faaliyet alanlarında güvenliklerini ve güvenilirliklerini tehlikeye sokabilecek, aleyhlerine kullanılabilecek, bunlar tarafından, çok gizli, gizli, özel ve hizmete özel gizlilik derecelerinde tasnif edilen, belirlenen ve işaretlenen bilginin; üretilmesi, kullanılması, işlenmesi, saklanması, nakledilmesi ve imhasında içeriğinin ve bütünlüğünün korunmasına, yetkisiz kişilerin erişimine ve olası her türlü fiziksel ve elektronik müdahaleye karşı korunmasına, bilgiye erişim ve kullanılmasına ait usullerin açık şekilde belirlenmesine ve bilginin istenilen yer ve zamanda hazır bulundurulmasına yönelik tedbirleri ifade eder” (e-Türkiye Girişimi I. Ara Rapor, 2002, s. 138).

Yukarıda taslak kanunda yer alan bazı öngörüler, 11/6/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar kurulu kararı neticesinde gerçekleştirilmiştir. Adı geçen kararda resmi bir siber güvenlik tanımlaması yapılarak ulusal siber güvenlik; Bilgi ve iletişim teknolojileriyle vasıtasıyla sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda alan sistem güvenliği şeklinde tanımlanmıştır. 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında

siber güvenlik kavramı; “Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesin” şeklinde tanımlanarak bilgi sistemleri güvenliği ve siber olay yönetimi odaklı bir tanımlama gerçekleştirilmiştir. Daha sonra yayımlanan strateji planlarında da aynı tanımlama gerçekleştirilmiş, bilgi sistem ve siber olay yönetimi odaklı bir siber güvenlik tanımlaması ortaya konmuştur. Bu tanımlamanın etkisini bir önceki aşama olan siber olay tespit, erken uyarı ve hazır olma aşamasında görmek mümkündür. Söz konusu aşamada belirlenen düzenlemelerin önemli bir kısmının bu tanımlamaya uyumlu olduğu bir sonraki aşama olan anlam verme aşamasının da benzer bir uyum içerisinde olduğu tespit edilmiştir.

5.3.2.3. Anlam Verme Aşaması

Anlam verme aşaması algılama düzeyi oluşturma aşamasının etkisiyle şekillenen olay tespit süreciyle ortaya konan güvenlik olaylarının değerlendirilmesi ve nasıl yönetileceğine ilişkin esasların belirtileceği aşamadır. Türkiye’nin güvenlik algılamasındaki hassasiyetlerinin tarihsel arka planı ve günümüzdeki durumu çalışmanın bir önceki bölümünde ele alınmıştır. Bir hukuk devleti olan Türkiye’nin güvenlik algısının anlamlandırılması başta T.C. Anayasası olmak üzere resmi dokümanlar yoluyla gerçekleştirilmiştir. Stratejik seviyedeki planlamalar da yine güvenlik algısı doğrultusunda hareket ilgili bakanlık ve kamu kuruluşlarının stratejik planlama dokümanlarında güvenlik konularına yer verilmiştir. Çalışmanın bu bölümünde daha önce analiz edilmiş olan ulusal güvenlik algısının nasıl şekillendiği ve siber alana olan etkileri doğrultusunda oluşan güvenlik anlamlandırma süreç ve uygulamaları analiz edilmiştir. Anlam verme aşaması güvenlikleştirme kavramı içerisinde olağan dışı olandan olağan üstü duruma geçiş olarak açıklanmıştı. Ülkemizdeki durum analiz edilirken bu doğrultuda

bulgular analiz edilmiş, başlangıç noktası olarak T.C. Anayasasında yer alan OHAL durumu ve siber uzaydaki karşılığı analiz edilmiştir.

5.3.2.3.1. OHAL Durumunun Değerlendirilmesi

Siber güvenlik özelinde ülkemizdeki duruma yaklaştığımızda siber güvenlik olaylarının en üst seviye güvenlik reaksiyonu olarak gösterebileceğimiz OHAL şeklinde olarak anlamlandırılması için OHAL durumunun anayasal karşılığını ele almak, tutarlı bir başlangıç noktası olacaktır. Anayasamızda OHAL 119. Md. esaslarınca düzenlenmiştir. OHAL kavramı bu maddede "savaş, savaşı gerektirecek bir durumun baş göstermesi, seferberlik, ayaklanma, vatan veya Cumhuriyete karşı kuvvetli ve eylemli bir kalkışma, ülkenin ve milletin bölünmezliğini içten veya dıştan tehlikeye düşüren şiddet hareketlerinin yaygınlaşması, anayasal düzeni veya temel hak ve hürriyetleri ortadan kaldırmaya yönelik yaygın şiddet hareketlerinin ortaya çıkması, şiddet olayları nedeniyle kamu düzeninin ciddî şekilde bozulması, tabiî afet veya tehlikeli salgın hastalık ya da ağır ekonomik bunalımın ortaya çıkması hallerinde" şeklinde tanımlanarak bazı durumların ortaya çıkması şartına bağlanmıştır. Ülkemizde bugüne kadar OHAL durumunu gerektirecek bir siber güvenlik olayı ya da krizi yaşanmamıştır. Ancak araştırmanın bu noktaya kadar olan bölümlerinde yer alan siber güvenlik kavramları ve ülkemizde siber güvenlik yapılanması üzerinden olası senaryolara göre bir analiz gerçekleştirilebilir.

5.3.2.3.1.1. Ayaklanma, Vatan veya Cumhuriyete Karşı Kuvvetli ve Eylemli Bir Kalkışma ve Şiddet Hareketleri Durumu

İlgili maddede yer alan güvenlik olayları, siber uzayda başlayan güvenlik olaylarının fiziki güvenlik olaylarına dönüşmesi neticesinde gerçekleşebilecektir. Örneklendirecek olursak 2010'nun sonlarında Tunus'ta başlayan halk isyanları, 2011 Ocak itibari ile Mısır'a sıçramış ve başlayan isyanlar, 33 yıllık Mübarek rejimine son vermiştir. Bu isyanlarda halkın organize olmasında sosyal medyanın rolü çok fazladır. Bir anlamda isyan siber uzayda başlayarak fiziki alana

sıçramıştır. Bu durum da, beraberinde OHAL uygulamalarına varacak tedbirleri getirmiştir. Sosyal medya üzerinden halkın kışkırtılarak bir kalkışma girişimi, ülkemizde gerçekleşmesi senaryosunda durumu fiziki alana sıçramadan kontrol altına almak için "5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu"'nda yer alan sosyal medya uygulamalarına erişimin engellenmesi tedbirleriyle, olayların yoğunluğuna göre mümkün olabilecektir. Ancak günümüzde bahse konu erişimin engellenmesi düzenlemelerini aşmak için kullanılan sanal özel ağ teknolojileri (VPN Virtual Private Network), alınan teknik tedbirleri kolaylıkla aşabilmekte ve bu teknolojinin kullanımı için ileri seviye teknik bilgi gerekmemektedir. Bu nedenle erişimi engelleme tedbirleri kimi durumlarda yeterli olamayacak ve diğer OHAL tedbirlerinin alınması kaçınılmaz hale gelebilecektir.

Siber zorbalık, kavramı fiziksel şiddet olaylarına ek olarak sanal ortamda şiddet uygulanması durumunu ortaya çıkarmıştır. Siber zorbalıkla mücadele için[22] günümüz şartlarında 5651 sayılı kanun ve diğer TCK hükümleri yeterli olarak değerlendirilebilir. Ancak iyi kontrol edilemeyen siber suçluların engellenemediği bir internet ortamının mevcut büyüklüğü göz önüne alındığında siber alanda şiddet olaylarının ulusal çapta bir krize neden olması potansiyeline sahip olacaktır.

[22] "Siber zorbalık, bilgi ve iletişim teknolojilerini kullanarak bir birey ya da gruba yapılan teknik ya da ilişkisel tarzda zarar verme davranışlarıdır. Bir bireyin bir başkasını kasıtlı olarak rahatsız etmesi, kötü davranmak ya da dalga geçmek için dijital iletişim araçlarını, akıllı telefonları ya da diğer elektronik aygıtları kullanması ve bunu tekrar etmesidir."
"İki çeşit siber zorbalık bulunmaktadır: Birincisi daha çok teknik yönünü içeren elektronik zorbalık (electronic bullying), diğeri ise psikolojik yönünü içeren elektronik iletişim (e-iletişim) zorbalığıdır (e-communication bullying).""Elektronik zorbalık kişilerin şifrelerini ele geçirmek, web sitelerini heklemek, spam içeren mailler göndermek ya da bulaşıcı e-postalar göndermek gibi teknik olayları içerir. Elektronik zorbalık, bireysel yapılabileceği gibi birçok kişi tarafından organize bir şekilde aynı anda da yapılabilir. DDoS denilen bu tür saldırıların hedefi sistemi kullanılamaz hale getirmektir. Bu tür saldırılar kişilerin sahip olduğu web sitelerine yapılabildiği gibi büyük kurum ya da devletlere ait yazılım ya da sitelere de yapılmaktadır. Bu saldırılar donanım ve yazılımlara direkt olarak etkide bulunurken, dolaylı olarak kişilerin duygularına da etki etmektedir" (Siber Zorbalık,2020)

5.3.2.3.1.2. Savaş, Savaşı Gerektirecek Bir Durumun Baş Göstermesi, Seferberlik Durumu

Savaş, gerginlik ve seferberlik ilanına siber uzaydan kaynaklanan siber güvenlik olaylarının neden olması durumu, günümüze kadar ki dönemde gerçekleşmemiş olsa da Estonya ve Gürcistan örnekleri siber uzay yaşanabilecek siber saldırıların silahlı çatışmalara eş değer etki yaratabileceğini göstermiştir. Estonya'ya karşı gerçekleştirilen siber saldırılar ülkenin tüm kritik altyapı sektörlerinde büyük krizlere neden olmuş, krize NATO müdahil olmak zorunda kalmıştır. NATO yaşanan olaylar sonrasında bir dizi düzenlemeye gitmiş, 2014 Galler Zirvesinde siber uzaydan gelecek saldırıların NATO Antlaşması'nın beşinci maddesi kapsamında değerlendirileceği ve saldırıya maruz kalan ülkenin konvansiyonel güç kullanımı dahil olarak NATO tarafından savunulacağı kararı alınmıştır (Burkadze, 2018, s. 20-22). 2016 Varşova zirvesinde ise siber uzay, harbin beşinci boyutu olarak kabul edilmiştir.

Konu kapsamında ülkemizdeki durumu ele aldığımızda "697 sayılı Ulaştırma ve Haberleşme Hizmetlerinin Olağanüstü Hallerde ve Savaşta Ne Suretle Yürütüleceğine Dair Kanun"'da yer alan düzenlemeler gereği haberleşme hizmetlerinden yararlanma önceliği Genelkurmay Başkanlığı'na geçmektedir. Aynı zamanda harekatın gerektirdiği durumlarda harp alanının haberleşme yönetimi, Genelkurmay başkanlığına geçmektedir. Ülkemizde siber uzayın yönetimi, elektronik haberleşme kanunu üzerinden gerçekleştirilmekte bu anlamda elektronik haberleşme hizmetleri de ilgili kanuna tabi olmaktadır. Gerek ulusal siber güvenlik tatbikatları (Siber Güvenlik Tatbikatları, 2017) gerekse NATO tarafından icra edilen siber güvenlik tatbikatları incelendiğinde (Locked Shields, 2019) siber savaşın silahlı kuvvetlerin yönetimi şeklinde değil, ilgili tüm paydaşların koordinesiyle icra edileceği düşüncesi öne çıkmaktadır. Bu anlamda kanunda yer alan işletme devri yerine yaşanabilecek olası kapsamlı siber çatışma ya da savaş durumunda harekat kontrolü maddesi ön plana çıkmaktadır. Bu madde ilgili kanunda şu şekilde açıklanmaktadır:

> Madde 2 – “Olağanüstü hallerde ve savaşta uygulanacak ulaştırma ve haberleşme planları Türk Silahlı Kuvvetlerinin ihtiyaçları önceliğe alınmak suretiyle, Türk Silahlı Kuvvetlerinin ihtiyaçları bakımından Genelkurmay Başkanlığınca, diğer Devlet daire ve müesseseleri ile halk ihtiyaçları bakımından Genelkurmay Başkanlığının mütalaası alınmak ve ilgili makamlarla iş birliği yapılmak suretiyle Ulaştırma Bakanlıklarınca ve müştereken barıştan itibaren hazırlanır.”
> Madde 3 – “Yukarıdaki maddeye göre hazırlanan planların aksatılmadan yürütülebilmesini sağlamak için, lüzumlu görülecek araç, malzeme, tesis, fabrika ve atölyelerin bu kanun kapsamına giren daire, teşekkül, müessese ve ortaklıklar elinde bırakılması veya lüzumlu görülecek araç, malzeme, tesis, fabrika, atölye ve personelin bunların emrine tahsisi için yapılacak işlem Genelkurmay Başkanlığının mütalâası alınmak şartı ile Milli Savunma, İçişleri ve Ulaştırma Bakanlığınca müştereken tespit olunur.”
> Madde 4 – “Olağanüstü hallerde ve savaşta kritik harekat alanlarının bir kısmının veya tamamının ulaştırma ve haberleşme harekat kontrolü veya gereğinde özel birlikler vasıtası ile işletme yetkisi, Genelkurmay Başkanlığının istemi üzerine Ulaştırma Bakanlığınca Türk Silahlı Kuvvetlerine verilir.” (Ulaştırma ve Haberleşme Hizmetlerinin Olağanüstü Hallerde ve Savaşta Ne Suretle Yürütüleceğine Dair Kanun)

Ulusal Siber Güvenlik Stratejisi 2020 2023’e “Siber Güvenliğin Milli Güvenliğe Entegrasyonu” hedefi eklenmiştir. Siber güvenlik kavramının, ulusal siber güvenlik kavramının ayrılmaz bir parçası olduğu belirtilmiş, üst düzey milli politikalarımızda siber güvenliğe ilişkin hususların azami derecede dikkate alınması, bu politikalara kara, hava, deniz ve uzay güvenliğinin yanında siber savunmanın da yerini alması, ülkemizin diğer unsurlarla birlikte siber unsurları da içeren hibrit tehditlerden koruması ve caydırıcılığının artırılması hedeflendiği vurgulanmıştır (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023), 2020, s. 23). Detayları Hizmete Özel gizlilik derecesinde olan eylem planında E39 numaralı eylem planı, bu hedefin gerçekleştirilmesi için planlanmıştır.

5.3.2.3.1.3. Doğal ya da İnsan Kaynaklı Afetler ve Kritik Altyapı Güvenliğinin Değerlendirilmesi

Çalışmanın daha önceki aşamasında afet ve olağanüstü hal yönetiminde siber güvenlik olaylarının insan kaynaklı afet kapsamında değerlendirilerek teknolojik afet olarak sınıflandırıldığı belirtilmiştir. Siber uzay kaynaklı afetler günümüzde sadece elektronik haberleşme kritik altyapısını etkilememektedir. Sağlık sistemlerine yapılacak bir siber saldırı ulusal elektronik haberleşme altyapısına

zarar vermekten ziyade sağlık kritik kamu hizmetini sekteye uğratacaktır (Massive WannaCry/Wcry Ransomware Attack Hits Countries, 2017). Enerji altyapısına yapılan saldırılar da benzer şekilde enerji altyapısını derinden etkileyecek potansiyele sahiptir, kimi durumlarda ise enerji altyapısına gerçekleştirilen bir saldırı, çevre krizlerine neden olabilecektir. Duruma ilişkin somut örnek olarak Sibirya petrol boru hattına düzenlenen siber saldırının getirdiği çevre krizi gösterebilir. Bir başka olası örnek de, İran nükleer tesislerine gerçekleştirilen Stuxnet siber saldırısı üzerinden verilebilir (Hoffman, 2004). Stuxnet saldırısı sonucunda İran nükleer tesislerinde oluşmuş olacak olası bir patlamanın sınırları aşan bir çevresel felakete neden olması durumu kaçınılmaz gerçeklik olarak karşımıza çıkmaktadır (Masood, Samar, and Raja, 2019, p. 2).

Finans kritik altyapısına yönelik saldırıların genel bir güvenlik krizine neden olması olasılığı günümüz finans sisteminin siber uzaya olan bağımlılığı göz önüne alındığında gerekli tedbirler alınmadığı takdirde, kesin seviyesine yakındır. Estonya saldırılarında finans sistemi derinden etkilenmiş, ülkede ekonomi durma noktasına gelmiştir. Günümüzde ise siber saldırı sonucu elde edilecek kazancın büyüklüğü büyük ve gelişmiş saldırıların bu sektörü hedef almasına neden olmaktadır. Kripto para sektörünün giderek büyümesi, bu alanın hedef alınmasına neden olan bir başka etkendir. Kripto para sektörünü hedef alan başarılı saldırıların etkileri giderek artan bir grafik sergilemektedir. Forbes verilerine göre 2018 yılında 1.8 milyar dolarlık bitcoin hırsızlığı yaşanırken 2019 yılında bu rakam 4 milyar dolar seviyelerine yükselmiştir (Su, 2019).

Finans kritik altyapısını hedef alan saldırıların amacı ve saldırı tekniği krizin çözüm aktörünü belirlemektedir. Bankacılık sektörünü işleyemez hale getirmeyi amaçlayan bir saldırı, bankacılık bilgi sistemlerinin çalışamaz hale getirebilecektir. Ülkemizde son dönemde Garanti Bankasını hedef alan saldırılar bu türden bir saldırı olup, elektronik haberleşme kritik altyapısındaki aktörler tarafından saldırılarla mücadele edilmiştir (Bıktım, 2019). Para hırsızlığına yönelik saldırılar ise sistemi işleyemez hale getirmekten ziyade sitemin açıklıklarını istismar eden teknik saldırılar olacaktır. Bu gibi saldırılara, ekonomi

kritik altyapısından sorumlu sektörel SOME tarafından karşılık verilecektir. Sektörel SOME'nin sorunu çözemediği durumlarda ise ülke genelini etkileyen bir finans krizi ortaya çıkacaktır. Bu nokta da ülkemizde siber güvenlikten sorumlu birincil makam olarak belirlenen Ulaştırma ve Altyapı Bakanlığı'nın elektronik haberleşme sektörü üzerinden gerçekleştireceği düzenlemeler yetersiz kalacaktır.

5.3.2.3.2 Stratejik Planlamalarla Anlam Verme

Ulusal çapta siber güvenlik krizlerinin görülmeye başlaması sıklığının artması ülkeleri ulusal siber güvenlik stratejileri üretmeye zorlamıştır. Günümüz dünyasında siber güvenlik stratejileri dijital toplum, ekonomi, erişilebilirlik, e-devlet, e-ticaret hatta e-demokrasi gibi toplumun siber uzayla olan etkileşiminin temelini oluşturmakta ve inşa etmektedir (Akyeşilmen, 2018, s. 110). Ülkemizde bu gelişmelerden etkilenmiş ve ilk ulusal siber güvenlik strateji belgesini 2013 yılında yayımlamıştır.

Siber güvenlik kriz yönetiminde stratejik planlama algı düzeyi oluşturma aşamasında siber güvenlik kavramsallaştırmasını ortaya koyarak anlam verme aşamasına geçiş için hangi olayların siber güvenlikle ilgili olduğunu belirler. Anlam verme aşamasında ise siber güvenlik olayı olarak belirlenen gelişmelerin nasıl ele alınacağı değerlendirilir. 2013-2014 ulusal siber güvenlik stratejisi ile birlikte ulusal siber güvenliğin nasıl sağlanması gerektiğine ilişkin ilkeler belirlenmiştir.

Siber güvenlik kavramının risk yönetimi temelli ele alınması gerekliliği öne çıkarılmıştır. Risk yönetimi süreci ise sadece risklerin tespit edildiği bir süreç olarak değil, riskleri giderici sürekli iyileştirmeye dayalı bir süreç olarak tanımlanmıştır. Siber güvenlik için teknik boyutta analizin yetersizliği belirtilmiş ve hukuki, idari, ekonomik, politik ve sosyal boyutlarda güçlü ve zayıf yönlerin, tehditlerin ve fırsatların belirlenmesini içeren bütüncül bir yaklaşım sergilenmesi ilke olarak belirlenmiştir. Kritik altyapıların güvenliği için sadece kamu genelinde

alınan tedbirlerin yetersiz olacağı özel sektörü kapsayan bir yaklaşımın benimsenmesi gerekliliği ortaya konmuştur. Uluslararası iş birliği, mevzuat geliştirme, insan gücü yetiştirme, kamu, akademi ve özel sektör işbirliği ve koordinasyonu, temel hak ve hürriyetlerin korunması hususları da diğer önemli ilkeleri oluşturmaktadır.

2016-2019 Ulusal Siber Güvenlik Strateji belgesinde yukarıda belirlenmiş olan ilkelere ek olarak siber güvenlik olaylarının etkilerinin düşük seviyede kalması için stratejik seviyede önlemler alınması, siber suçlara daha etkin müdahale yurtdışından ithal edilmek zorunda kalınan bilgi sistemlerinin güvenli kullanımı, Uluslararası Siber Güvenlik Operasyon Merkezleri arasında gelişmiş siber olay yönetimi işbirliği ilkeleri belirlenirken risk yönetimi sürecine ilişkin yukarıda yer alan ilkelere ek olarak risk yönetiminde kabul edilebilir risklerin varlığı belirtilmiştir. Riskin tamamen giderildiği bir siber güvenlik ütopyası yerine gerçekçi bir hedef belirlenmiştir.

Ulusal Siber Güvenlik Stratejisi 2020 2023 ile birlikte önümüzdeki döneme ilişkin yeni amaç ve ilkeler belirlenerek 2023 yılına kadarki dönemde siber uzaydaki faaliyetlerin nasıl anlamlandırılacağı ortaya konmuştur. Cumhurbaşkanının yorumlarının yer aldığı bölümde, odak noktası kalkınma ve ekonomik gelişme üzerine kurulmuş, bu gelişmenin beraberinde, teknolojik gelişme ve büyümeyi getirdiği belirtilmiştir. Teknolojik gelişmişliğin siber güvenlik risklerini tetiklediği ve günümüzde siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olduğu ifade edilmiştir. Geçen yıllarda yayımlanan belgelerde yüzeysel olarak var olan dijital hayat kavramı, COVID-19 krizinin getirdiği dijitalleşme içerisinde değerlendirilmiş ve bu değerlendirmeye göre risk tanımlamaları gerçekleştirilmiştir. Ortaya çıkan her yeniliğin beraberinde yeni bir riski doğurduğu analizi yapılmıştır.

5.3.2.3.3 Hukuki Düzenlemelerle Anlam Verme

E-Türkiye çalışmalarının başladığı 2001 yılından günümüze kadarki stratejik seviye çalışmaların tümünde gerekli hukuki mevzuatın eksikliğine dikkat

çekilmiştir. Zaman içindeki hukuki düzenlemeler ülkemizdeki siber güvenlik gelişmelerinin ele alındığı bölümde açıklanmıştır. Bu bölümde ise siber uzayda yaşanan güvenlik olaylarının siber güvenlik krizi çerçevesinde değerlendirilmesine neden olacak hukuki düzenlemeler ele alınarak güncel mevzuatın siber güvenlik kriz yönetimi boyutu ortaya çıkartılacaktır.

Temel hak ve hürriyetlerin yok edilmeye çalışması, pek çok kanunda ciddi bir güvenlik sorunu olarak ele alınmıştır. Ülkemizdeki güvenlik olaylarının koordinasyonundan sorumlu merkez olan GAMER'in kurulmasını öngören 32 numaralı Cumhurbaşkanlığı kararnamesinde de temel hak ve hürriyetlerin teminini riske atan güvenlik olaylarını koordinasyon görevi GAMER'e verilmiştir. Ülkemizde siber güvenlik, elektronik haberleşme sektörü üzerinden ele alınmaktadır. Siber uzayın teknik ve mantıksal katmanının elektronik haberleşme altyapısı üzerinde yer alması bu kavramsallaştırmanın nedenini açıkça ortaya koymaktadır. Siber güvenlik ve haberleşme arasındaki ilişkiyi haberleşme temel hak ve hürriyeti ile ilişkilendirmek gerekliliği gün geçtikçe artmaktadır. En önemli nedeni ise insanlarımızın fiziki alanda olduğu kadar siber uzayda da varlık göstermesi dijital kimlik, dijital vatandaş gibi kavramların karşılığının genişlemesidir. Anayasanın 22. Maddesi[23] haberleşme hakkını düzenlemektedir. Haberleşmenin gizliliği esasını yerine getirmek için alınan önlem ve tedbirler daha önceki aşamalarda ele alınmıştır. Haberleşme altyapısı kullanılarak siber suç işlenmesi durumunda haberleşmeye müdahale edilmesi ise 5651 sayılı kanun, TCK ve Terörle Mücadele Kanunu ele alınırken tartışılmıştır. Bu noktada analiz edilmemiş olan ve siber güvenliğin erişilebilirlik boyutuyla bağlantılı olan esas, herkesin haberleşme hürriyetine sahip olmasıdır. Günümüzde siber uzaya sağlıklı erişim sağlama haberleşme hürriyetiyle bağlantılı olmaktadır. 5369 sayılı Evrensel Hizmet Kanunu, bu bağlamda kişilerin siber uzaya erişiminin sürekliliğini

[23] "Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır. Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar."

sağlayarak haberleşme özgürlüğünün erişilebilirlik boyutunu şekillendirmektedir. Kanunda evrensel hizmet; Türkiye Cumhuriyeti sınırları içinde coğrafi konumlarından bağımsız olarak herkes tarafından erişilebilir, önceden belirlenmiş kalitede ve herkesin karşılayabileceği makul bir bedel karşılığında asgari standartlarda sunulacak olan, internet erişimi de dahil elektronik haberleşme hizmetleri olarak tanımlanmaktadır. Görüleceği üzere vatandaşların makul bir internet hizmetine sahip olması hakkı olduğu, bu kanunla ortaya konmakta ve bu durumun sürekliliğine dikkat çekilmektedir.

5.3.2.4 Karar Verme ve Krizlerin Sonlandırılması Aşaması

Karar verme aşamasında, karar verici aktörler tarafından oluşturulan algılama düzeyi oluşturma ve anlam verme çalışmaları çerçevesinde gelişen siber olayların nasıl ele alınacağının kararı verilmektedir. Anlam verme aşamasında krizlerin nasıl ele alınacağı hangi durumlarda nasıl bir müdahale yöntemi izlenebileceği değerlendirilmiştir. Ancak karar verme aşaması sadece matematiksel bir süreç değildir. Krize konu olabilecek verilerin algılanması ve gelen veriler doğrultusunda hangi anlamlar içereceği önceden belirlenmiş olsa da krizin yönetim biçimini, karar verici aktörler belirleyecektir. Bu durum kriz yönetimi ve liderlik arasındaki bağlantıdan kaynaklanmaktadır.

E-Türkiye çalışmalarında ulusal bilgi güvenliğinin sağlanması maksadıyla “Ulusal Bilgi Güvenliği Üst Kurulu”[24] ile kamu tüzel kişiliğine haiz, idari ve mali özerkliğe

[24] İlgili kurul şu şekilde ifade edilmiştir: **“**Kurul; ulusal bilgi güvenliği alanında en yetkili organdır. Kurulun Başkanı, Başbakandır. Kurul; Başbakan, yokluğunda görevlendireceği devlet bakanının başkanlığında, Adalet, Milli Savunma, İçişleri, Dışişleri, Ulaştırma, Sanayi ve Ticaret Bakanları ile Milli Güvenlik Kurulu Genel Sekreteri, Genelkurmay Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Milli İstihbarat Teşkilatı Müsteşarı, Türkiye Bilimsel ve Teknik Araştırma Kurumu Başkanı ile Kurum Başkanından oluşur. Kurul Başkanının talebi üzerine, ihtiyaç duyulduğu hallerde diğer bakanlar ile kamu kurum, kurul ve kuruluşları ile özel kuruluş temsilcileri de Kurul toplantılarına çağrılabilir. Kurul üye tam sayısının üçte ikisi ile toplanır. Kararlar, toplantıya katılan üyelerin oy çokluğu ile alınır. Oyların eşitliği halinde Kurul Başkanının oyu yönünde karar alınır. Toplantılara katılmaları uygun görülen diğer kişilerin oy hakkı yoktur. Kurul, nisan ve ekim aylarında olmak üzere, yılda iki defa olağan olarak toplanır. Kurulun gündemi

sahip Ulusal Bilgi Güvenliği Kurumunun kurulması öngörülmüştür. Bu taslak kurul, 2012 yılında yayımlanan 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" ile kurulan Siber Güvenlik Kurulu olarak mevcudiyet kazanmıştır. Dönem içerisinde kurulun faaliyetleri incelendiğinde ise somut bir faaliyet bulunmamaktadır. Taslak tasarıda kurulun yılda iki kez düzenli olarak toplanması öngörülürken mevcut siber güvenlik kurulu zaman içerisinde 4 kez toplanabilmiştir. (Ulaştırma ve Altyapı Bakanlığı Resmi İnternet Sitesi, 2020)

Elektronik haberleşme kanununda gerçekleştirilen düzenlemeler sonucunda Ulaştırma ve Altyapı Bakanlığı siber güvenlikten sorumlu kurum olarak belirlenmiş ve bağlısı olan BTK'ya bu alanda görevler verilmiştir. Günümüze kadarki gelişmeleri ele aldığımızda, ülkemizdeki siber güvenlikleştirme aktörü karşılığını, tek başına Ulaştırma ve Altyapı Bakanlığı karşılamaktadır. Araştırmanın bu noktasına kadarki analizlerde kullanılan resmi düzenlemelerde bu tespiti doğrular nitelikte olup önemli siber güvenlik düzenlemeleri, ilgili bakanlıkça ya da koordinesinde gerçekleşmiştir. Ayrıca siber uzayın yönetimi de elektronik haberleşmeden sorumlu bakanlık olarak bu bakanlıkça gerçekleştirilmekte internet altyapısının düzenlenmesi, tarifeler, internet içeriğinin denetlenmesi, gerekli işletme izinlerinin verilmesi ve esaslarının belirlenmesi ve denetimi gibi pek çok yönetimsel ve idari faaliyet ilgili bakanlıkça yerine getirilmektedir.

Cumhurbaşkanlığı hükümet sistemine geçişle beraber T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin kurulmasıyla yeni bir güvenlikleştirici aktör ortaya çıkmıştır. Bu kuruma Cumhurbaşkanlığı teşkilatı oluşturulurken çeşitli siber güvenlik görevleri verilmiştir[25]. Ulusal Siber Güvenlik Stratejisi 2020-2023'te dijital

Başbakan tarafından belirlenir. Başbakan, gerek gördüğünde veya üyelerden birisinin talebi üzerine Kurulu olağanüstü toplantıya çağırabilir. Kurulun sekreterya hizmetleri, Kurum tarafından yerine getirilir."

[25]" Dijital dönüşüm ofisine aşağıda yer alan görev ve sorumluluklar 1 Sayılı Cumhurbaşkanı kararnamesi gereğince tevdi edilmiştir;

dönüşüm ofisinin temel görevi, siber güvenlik projeleri geliştirmek olarak belirtilmiştir. T.C. Dijital Dönüşüm Ofisi, gerçekleştirdiği somut siber güvenlik faaliyetleri nedeniyle Cumhurbaşkanlığı Hükümet Sistemi'ne geçişle birlikte proje geliştirme faaliyetlerinin ötesine geçerek önemli bir siber güvenlikleştirici aktör olarak belirmiştir.

5.3.2.5 Öğrenme ve Reform

Ülkemiz bugüne kadar kriz seviyesinde ele alınan bir siber güvenlik olayı ile karşılaşmamıştır. Bu anlamda Estonya krizi özelinde bu ülkenin yaşadığı kriz sonrası reform, ülkemizde henüz yaşanmamıştır. Ancak NATO üyesi bir ülke olarak, NATO tarafından Estonya krizi sonrasında geliştirilen reform hareketleri ülkemizde de takip edilmektedir. Siber uzayın yeni bir harekat alanı olması tespiti 2020-2023 Ulusal Siber Güvenlik Stratejisinde kendisine yer bulmuştur. COVID-19 kriziyle berber ortaya çıkan yeni güvenlik riskleri göz önünde bulundurularak ilgili strateji belgesinde ortaya çıkan yeni risklerin analizi gerçekleştirilmiş, bu risklere cevap verecek şekilde geleceğe ilişkin amaçlar optimize edilmiştir. Kurumlar arası koordinasyonun önemi, sürekli bilgi paylaşımına önem verilmesi, bir diğer öne çıkan öğrenme metodu olarak belirlenmiştir. Tatbikatlarla öğrenme yönetimine ilişkin gerekli altyapı Ulaştırma ve Altyapı Bakanlığı'nca sağlanmış,

---

"1) Cumhurbaşkanınca belirlenen politikalar kapsamında kamu kurumları ve kritik altyapılara yönelik siber güvenlik stratejileri geliştirmek.
2) Ulusal siber güvenlik ve bilgi güvenliğini destekleyici projeler geliştirmek.
3) Siber güvenlik ile ilgili politika, strateji ve eylem planlarının ülke çapında etkin şekilde uygulanmasına yönelik gelişmeleri takip etmek.
4) Kritik altyapıların belirlenmesine yönelik çalışmalar yapmak.
5) Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşlar konusunda ilgili kurumlara önerilerde bulunmak.
6) Kamu, özel sektör ve üniversiteler arasındaki işbirliğinin artırılması suretiyle ulusal siber güvenlik ekosisteminin oluşturulmasına katkı sağlamak.
7) Özel sektörün kapasitesinin kritik alanlara yönlendirilmesi ve mükerrer yatırımların önlenmesi için öncelikli siber güvenlik alanlarını belirlemek.
8) Kritik altyapılar başta olmak üzere her alanda, yerli ve milli siber güvenlik ürünlerinin geliştirilmesine ve bu çözümlerin kullanımının kamuda yaygınlaştırılmasına yönelik çalışmalar yapmak.
9) Kritik teknoloji ve bilgi varlıklarını korumak amacıyla önleyici ve koruyucu faaliyetler konusunda çalışmalar yürütmek.
10) Kamu kurumlarında ve kritik altyapı işleten kuruluşlarda bilgi güvenliği yönetim sisteminin kurulup işletilmesi, teknik standartlar ile usul ve esasların belirlenmesi, uygulamanın izlenmesi ve yönlendirilmesi konularında çalışmalar yürütmek.
11) Başkan tarafından verilen diğer görevleri yapmak."

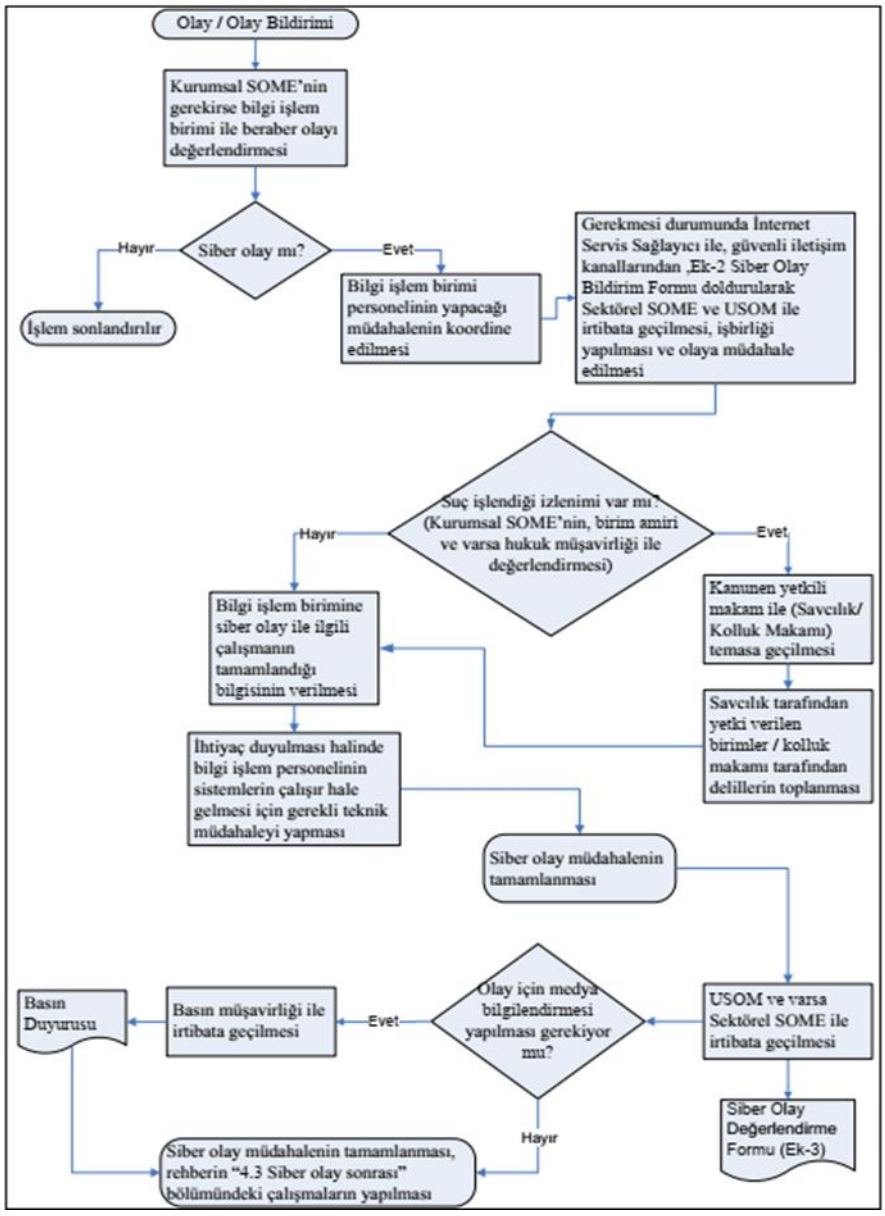
belirli periyotlarla ulusal siber güvenlik tatbikatları icra edilmiştir. Ancak tatbikatlarının azlığı ve katılım yelpazesinin düşüklüğü (Siber Güvenlik Tatbikatları, 2017) göz önüne alındığında gerekli verimin sağlanamadığı değerlendirilmiştir.

5.3.2.6 Kriz Durumlarında İletişim

Siber güvenlik krizlerinde iletişim için temel sorun krize neden olayın boyutu ve tam nedeninin bilinememesi ve teknik boyutu nedeniyle teknik jargonun kamuoyu ve üst yönetimin anlayacağı şekle çevrilmesi sorunudur. 2020 Aralık ayında ABD'de yaşanan Sunburst siber güvenlik krizinde, ulus devlet kaynaklı saldırıyı ilk ortaya çıkaran Fireeye siber güvenlik şirketi kendi sistemlerinin etkilendiğini ve araştırmayı derinleştireceği açıklamasıyla kriz başlamıştı. Başlangıçta kamuoyu ve hükümet Fireeye gibi küresel bir şirketin zafiyetlerini önceden tespit etmediği için hatalı olduğunu ve saldırganların bunları istismar ettiğini düşündü. Ancak kriz ilerledikçe ve araştırmalar derinleşince siber saldırıların başarılı olmasına neden olan olayın başka bir küresel ABD şirketi olan Solarwinds siber güvenlik firmasının açıklıklarının kullanıldığı ve pek çok ABD resmi kurumuna sızıldığı ortaya çıktı. Krizin sonunda başlangıçta suçlanan Fireeye olayı tespit eden kurum olarak ortaya çıktı.

Yukarıda yer alan örnekten yola çıktığımızda Türkiye'de siber olay iletişim ağı, USOM ve paydaşları olan kurumsal SOME'ler arasında tesis edilmiştir. Teknik iletişim ağı USOM'un kuruluş dokümanlarında belirlenmiştir. Siber olay esnasında USOM'un bilgilendirilmesi için ilk olay tespit raporu siber olay sonrasında gerekli incelemenin yapıldığı siber olay değerlendirme formu doldurularak USOM'a iletilmektedir. Siber olay müdahale akışı içinde suç unsuruna rastlanması halinde savcılık, kolluk makamı vb. makamlara haber verilmesi sürecini de içermektedir (Bknz. Şekil-28).

Şekil-28: Siber Olay Bildirimi Akış Şeması



Kaynak: (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2014)

Ulusal çapta meydanda gelebilecek siber güvenlik krizlerinin bir diğer önemli boyutunu stratejik iletişim oluşturmaktadır. Cumhurbaşkanlığı hükümet sistemine geçişle beraber stratejik kriz yönetimi iletişimi görevi 18 Eylül 2020 tarihinde Cumhurbaşkanlığı iletişim başkanlığına bu alanda görev tevdi edilerek ilgili başkanlığa bağlı olacak şekilde "Stratejik İletişim ve Kriz Yönetimi Dairesi

Başkanlığı" kurulmuştur. Kurulan bu yeni dairenin görev ve sorumlulukları[26] arasında kamu kurum kuruluşları arasında koordinasyon, tehdit analizi, olağanüstü hallerde stratejik iletişimin yönetilmesi gibi siber güvenlik kriz yönetimine ilişkin görevler yer almaktadır.

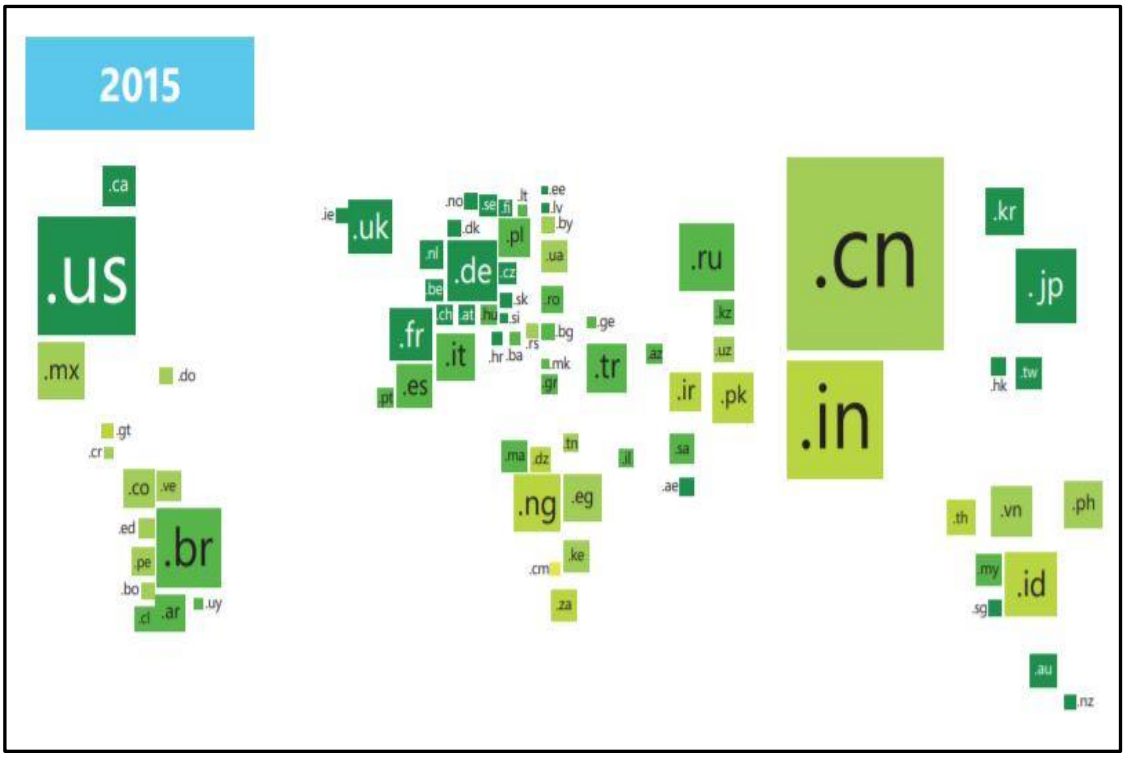
5.4 Türkiye, Siber Güvenlik ve Gelecek

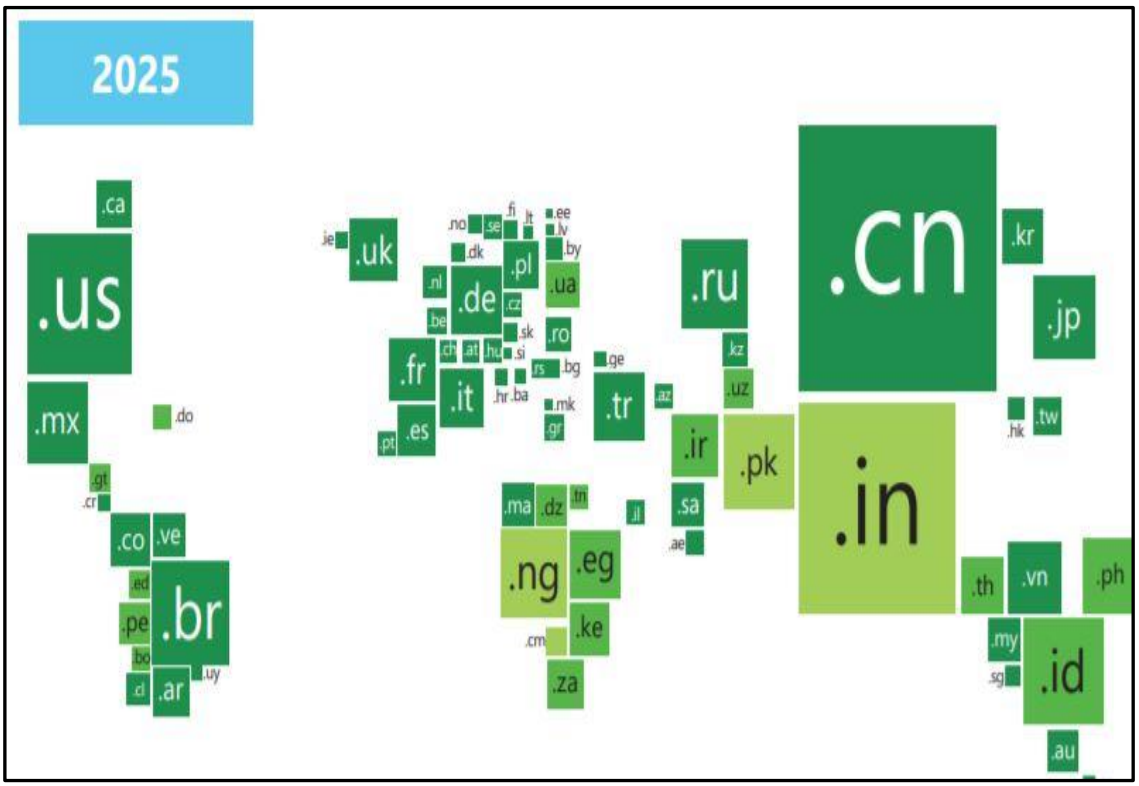
Siber güvenlik kavramının siber uzayla beraber olan genişleme süreci çalışmanın önceki bölümlerinde açıklanmıştır. Siber uzay gelecekte mevcut büyümesini sürdürürken yatay eksende de genişlemeye devam edecektir. Siber uzayı kullanan kişi sayısı artarken gündelik hayatta siber uzayın kullanım alanları genişleyecek ve günlük internet kullanım süresi uzayacaktır. Ülkemizde bu süreçten olumlu etkilenecek ve ulusal siber alan büyüyecek ve genişleyecektir. Şekil-29'da Unesco tarafından gerçekleştirilen Siber Uzay Raporu'ndan alınan 2015 ve 2025 yıllarında siber uzay grafiği sunulmuştur. Şekil incelendiğinde ulusal siber alanın 2025 yılında küresel siber uzayda daha fazla oranda yer kaplayacağı görülecektir. Ulusal siber güvenlik sorunları da bu büyümeden etkilenerek mevcut sorunlara eklenmelerle genişleyecektir. Bu sorunların çözümü ise günümüzden itibaren eldeki veriler ışığında analizler gerçekleştirilerek mümkün olacaktır. Araştırma bulgularına göre analizlerimiz aşağıda sunulmuştur.

---

[26] "Stratejik İletişim ve Kriz Yönetimi Dairesi Başkanlığının görevleri;
Devletin stratejik amaç ve hedefleri ile devletin ve milletin menfaatleri doğrultusunda gerektiğinde ilgili kurum ve kuruluşlarla iş birliği yaparak ulusal ve uluslararası alanda yürütülecek faaliyetlerde uygulanacak stratejik iletişim politikalarını belirlemek.
Ulusal ve uluslararası alanda stratejik iletişim ve kriz yönetimi faaliyetlerini yürütmek ve bu kapsamda ilgili kurum ve kuruluşlarla iş birliği yapmak.
Türkiye Cumhuriyeti'ne yönelik iç ve dış tehdit unsurlarını analiz ederek stratejik iletişim ve kriz yönetimi açısından gerekli tedbirleri uygulamak.
Türkiye Cumhuriyeti'ne karşı yürütülen psikolojik harekat, propaganda ve algı operasyonu faaliyetlerini belirleyerek her tür manipülasyon ve dezenformasyona karşı faaliyette bulunmak.
Kriz, afet, olağanüstü hal dönemleri ile yakın savaş tehdidi, seferberlik ve savaş halinde, devletin belirlediği amaç ve hedeflere ulaşmak için stratejik iletişim ve kriz yönetimi faaliyetlerinde bulunmak.
Görev alan kapsamında tüm kamu kurum ve kuruluşları arasında koordinasyonu sağlamak." (İletişim Başkanlığı Resmi İnternet Sitesi,2020)

Şekil-29: 2015 ve 2025 Yıllarında Siber Uzay





Kaynak: (2025 Cyberspace, 2015).

5.4.1 Gelecekte Siber Güvenlik

Ne kadar güvenlik alınacağı sorunsalı içerisinde maliyet analizini barındırır. Güvenliği sağlanacak nesne ya da sistemin zarar görmesinin getireceği maliyetin büyüklüğü güvenlik için ayrılacak kaynaklarında miktarını ve nevini belirler. Bu durum siber güvenlik alanında da geçerlidir. Güvenliği sağlanacak olan siber uzay elemanının değerine göre siber güvenlik tedbirleri alınır. Ülke güvenliğini etkileyecek bir bilgilerin işlendiği bir ağın güvenliği için yüksek seviyede ve maliyetli güvenlik tedbirleri alınırken, sıradan bilgilerin yer aldığı sistemlerde orta düzey güvenlik tedbirleri yeterli görülmektedir. Bazı durumlarda siber uzay elemanın değerini artıran şey bilginin muhteviyatı olmaktadır. Endüstriyel sırlar gibi edinimi maliyetli bilgilerin değerini bilginin işlendiği sistemlerin maliyeti değil bilgi elde etme sürecindeki maliyet belirlemektedir. Ulusal siber güvenlik söz konusu olduğunda da benzer durumlar söz konusu olmaktadır. Ülke insanın mahremiyetinin korunması için kişisel verilerin korunması kapsamında maliyetli güvenlik tedbirleri zorunlu hale getirilmekte, kritik kamu kurum kuruluşlarının siber güvenlik tedbirleri üst seviyede alınmaktadır.(Kişisel verilerin korunması kanunu kapsamında alınması gereken tedbirler Bilgi ve İletişim Güvenliği rehberi baz alınarak Ek-9'da sunulmuştur.)

Yukarıda yer alan nedenlerden dolayı, siber güvenlik kavramının gelecekteki durumu ele alınırken maliyet olarak siber güvenlik segmentlerinin büyüme ivmesi baz alınmıştır. Uluslararası bir siber güvenlik kuruluşu olan Gartner'a ait 2021 yılı siber güvenlik harcamaları raporunda büyüme gerçekleştiren siber güvenlik segmentleri belirtilmiştir. Şekil-29 incelendiğinde bulut güvenliği ve uygulama güvenliği gibi güvenlik segmentlerinin öne geçtiği görülmektedir. Şekil-30'da yer alan TUIK Bulut kullanım raporu analiz edildiğinde bulut teknolojilerinin kullanım hacminin arttığı görülmektedir. Her iki şekil karşılıklı olarak değerlendirildiğinde kullanım hacmi büyüyen bir siber uzay elemanının benzer oranda bir güvenlik büyümesine sahip olduğu görülmektedir. Siber güvenlik harcamalarının dağıldı alandaki bileşenlerin çeşitliliği beraberinde güvenlik yönetimi sorunlarını getirmektedir. Ulusal güvenlik üzerinden konuyu ele aldığımızda, gelecekte kritik

altyapılar ve kamu kurumlarının güvenliğinin sağlanabilmesi için bu karmaşık güvenlik ortamının belli bir model üzerinden yönetimi zorunluluğu karşımıza çıkmaktadır. Siber güvenlikte en önemli yönetimsel uygulama derinliğine savunmadır. Ulusal anlamda derinliğine savunma ise her bir kurum ve kuruluşun siber güvenliğinin kendi sınırları içerisinde tutarlı ortak bir modele göre sağlanmasıdır. Böylece operatif seviyede alınmış olan sıkı güvenlik tedbirleri olası siber olayların krize dönüşmesine engel olacaktır.

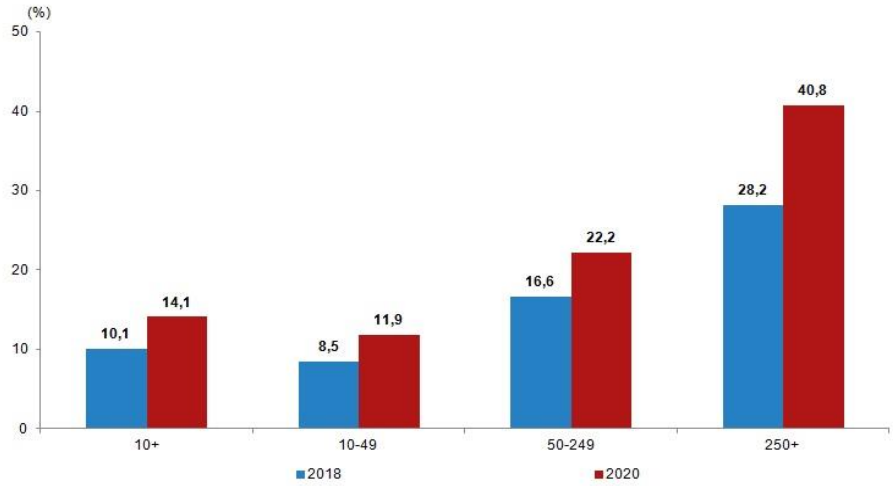
Gelecekte stratejik seviyede alınması gereken siber güvenlik tedbirlerine yönelik analizler, AB Siber Güvenlik Ajansı (ENISA) tarafından kapsamlı bir araştırma sonrasında ortaya çıkarılmış olan Ulusal Siber Güvenlik Yeteneklerinin Analizi Çerçevesi kapsamında gerçekleştirilmiştir. Analiz sonucunda grafiksel bir model ortaya çıkartılarak önceki bölümlerde ortaya çıkarılmış olan mevcut durumumuz ve geleceğe ilişkin değerlendirilmeler model üzerinde sunulmuştur. (Bknz. Ek-7)

Şekil-30: 2020-2021 Siber Güvenlik Harcamalarının Oransal Değişimi

Segment	2020	2021	Büyüme %
Uygulama Güvenliği	3,333	3,738	12.2
Bulut Güvenliği	595	841	41.2
Veri Güvenliği	2,981	3,505	17.5
Hesap ve Erişim Güvenliği	12,036	13,917	15.6
Altyapı Güvenliği	20,462	23,903	16.8
Risk Yönetimi	4,859	5,473	12.6
Ağ Güvenliği	15,626	17,020	8.9
Diğer Siber Güvenlik Ürünleri	2,306	2,527	9.6
Güvenlik Servisleri	65,070	72,497	11.4
Tüketici Güvenliği	6,507	6,990	7.4
Total	**133,776**	**150,409**	**12.4**

Kaynak: (Gartner Forecasts Worldwide Security, 2021).

Şekil-31: Türkiye'de Ücretli Bulut Kullanım Oranları 2019-2020

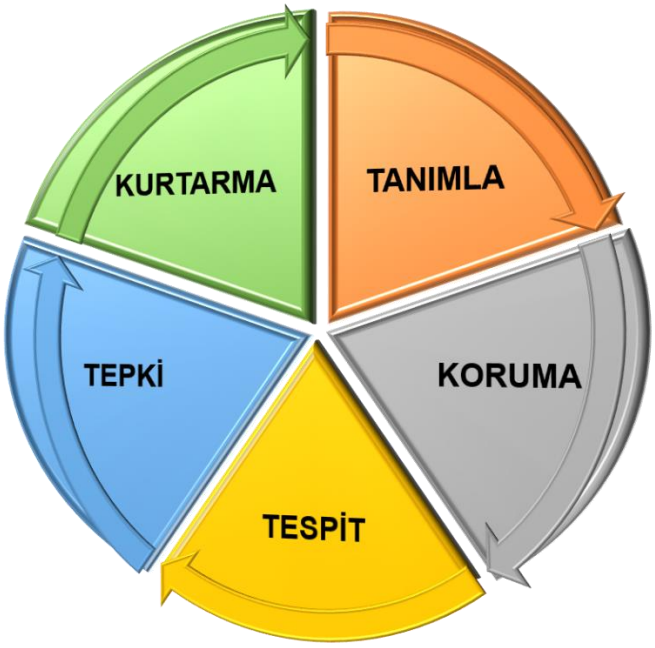


Kaynak: (Girişimlerde Bilişim Teknolojileri Kullanım Araştırması,, 2020)

5.4.2 Gelecekte Operatif Seviyede Siber Güvenlik

Siber güvenlik alanında yeni bir model çıkarmak çok uzun ve maliyetli bir süreçtir. Bu anlamda ülkeler yeni bir model ortaya çıkarmak yerine, uluslararası standartlara uyum sağlama yönetimini seçmektedirler. Bu durum NATO, BM, AGİT gibi uluslararası kuruluşlar içinde geçerli olup belli başlı standartlara uyum sağlanmaktadır. Şekil-32'de yer alan NIST Siber Güvenlik Çerçevesi uluslararası kabul görmüş ve sıklıkla uygulanan bir model olarak karşımıza çıkmaktadır. Model teknik detaylardan yerine yönetimsel fonksiyonları ortaya koymakta, kurumlar ellerindeki teknik envantere göre bu modele uyum sağlamaktadırlar. Bir önceki başlıkta çalışmanın amacı doğrultusunda stratejik seviyedeki siber güvenlik uygulamaları ve örgütsel yapılanması analizleri sunulmuştur. Çalışmanın amacının tamamlanabilmesi için gelecekte operatif seviyede uyulması gereken temel güvenlik tedbirleri bu model doğrultusunda ele alınmıştır. Model'in aşamaları aşağıda açıklanmıştır.

Şekil-32: NIST Siber Güvenlik Çerçevesi



Kaynak: (NIST Cybersecurity Framework, 2018)

5.4.2.1 Tanımlama

Tanımlama aşamasında sistemlere, insanlara, varlıklara, verilere ve yeteneklere yönelik siber güvenlik risklerini yönetmek için kurumsal bir anlayış geliştirmelidir. Tanımlama Fonksiyonundaki faaliyetler, çerçevenin etkin kullanımı için temel teşkil eder. (NIST Cybersecurity Framework, 2018) İş bağlamını, kritik işlevleri destekleyen kaynakları ve ilgili siber güvenlik risklerini anlamak, bir kuruluşun risk yönetimi stratejisi ve iş gereksinimleriyle tutarlı olarak çabalarına odaklanmasına ve öncelik vermesine olanak tanır. Bu Fonksiyon kapsamındaki kategoriler şu şekildedir; varlık yönetimi, iş çevresi; yönetim, risk değerlendirmesi ve risk yönetimi stratejisi. Bu aşamalar aşağıda özetlenmiştir, aşamaların alt maddeleri Şekil-33'de sunulmuştur.

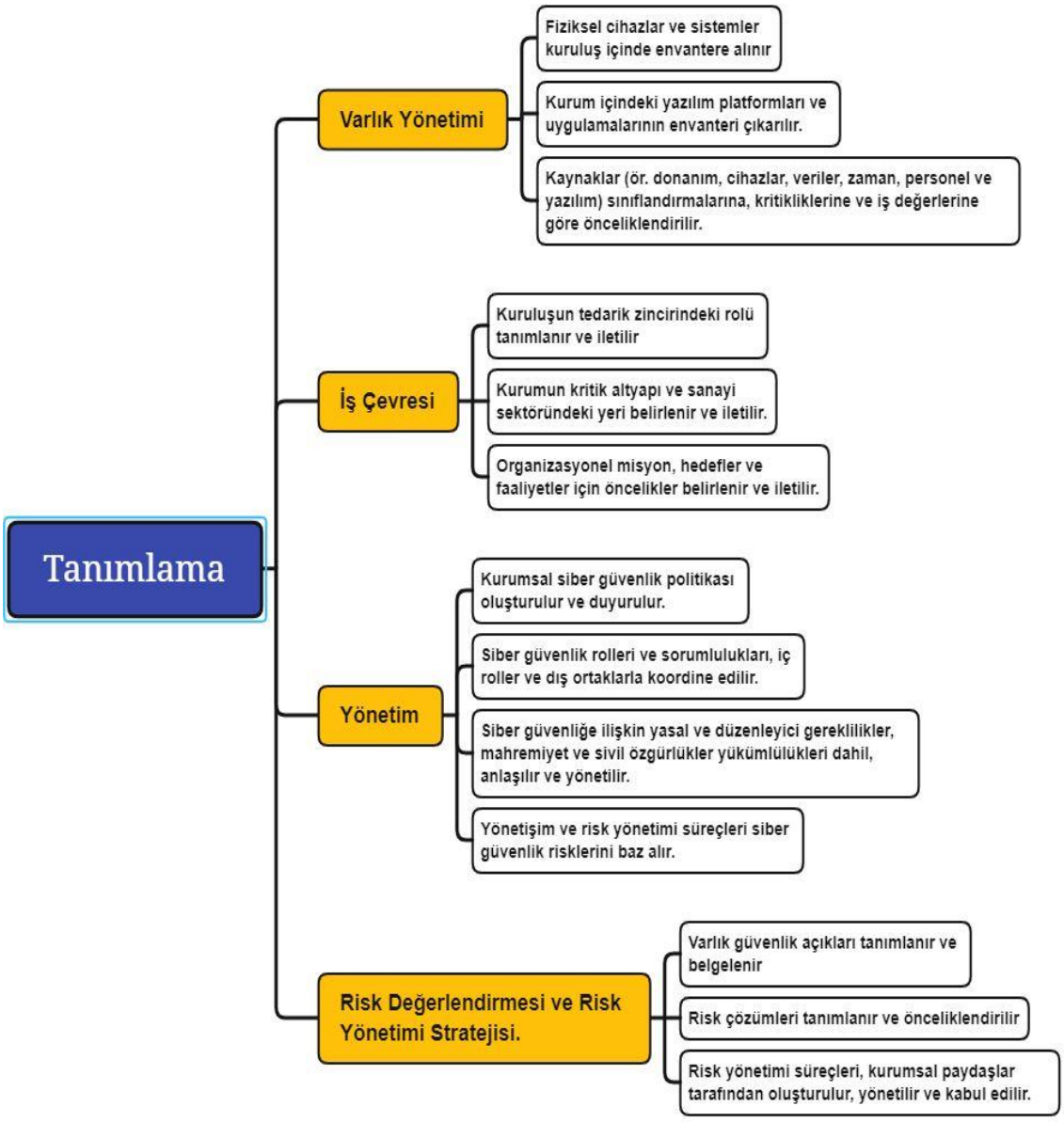
Varlık Yönetimi sürecinde Kuruluşun iş amaçlarına ulaşmasını sağlayan veriler, personel, cihazlar, sistemler ve tesisler, kuruluş hedeflerine ve kuruluşun risk stratejisine göreli önemleriyle tutarlı olarak tanımlanır ve yönetilir. Kaynaklar (ör. donanım, cihazlar, veriler, zaman, personel ve yazılım) sınıflandırmalarına, kritikliklerine ve iş değerlerine göre önceliklendirilir.

İş çevresi oluşturmaya yönelik faaliyetler esnasında; Kuruluşun misyonu, amaçları, paydaşları ve faaliyetleri anlaşılır ve önceliklendirilir; bu bilgiler siber güvenlik rollerini, sorumluluklarını ve risk yönetimi kararlarını bildirmek için kullanılır. Kurumun kritik altyapı ve sanayi sektöründeki yeri belirlenir ve iletilir. Tüm çalışma durumları için kritik hizmetlerin sunulmasını desteklemek için esneklik gereksinimleri belirlenir (ör. baskı/saldırı altında, kurtarma sırasında, normal operasyonlar).

Yönetim sürecinde; kuruluşun düzenleyici, yasal, risk, çevresel ve operasyonel gereksinimlerini yönetmek ve izlemek için politikalar, prosedürler ve süreçler anlaşılır ve siber güvenlik riski yönetimi birimi bilgilendirilir. Kurumsal siber güvenlik politikası oluşturulur ve duyurulur. Siber güvenliğe ilişkin yasal ve düzenleyici gereklilikler, mahremiyet ve sivil özgürlükler yükümlülükleri dahil, anlaşılır ve yönetilir.

Risk değerlendirmesi ve Risk Yönetimi Stratejisi belirlenirken; Kuruluşun öncelikleri, kısıtlamaları, risk toleransları ve varsayımları belirlenir ve operasyonel risk kararlarını desteklemek için kullanılır. Risk yönetimi süreçleri, kurumsal paydaşlar tarafından oluşturulur, yönetilir ve kabul edilir.

Şekil-33: Tanımlama Şeması



Kaynak: (NIST Cybersecurity Framework, 2018)

5.4.2.2 Koruma

Koruma İşlevi, olası bir siber güvenlik olayının etkisini sınırlama veya içerme yeteneğini destekler. Bu İşlev içinde şunları içerir: Kimlik Yönetimi ve Erişim

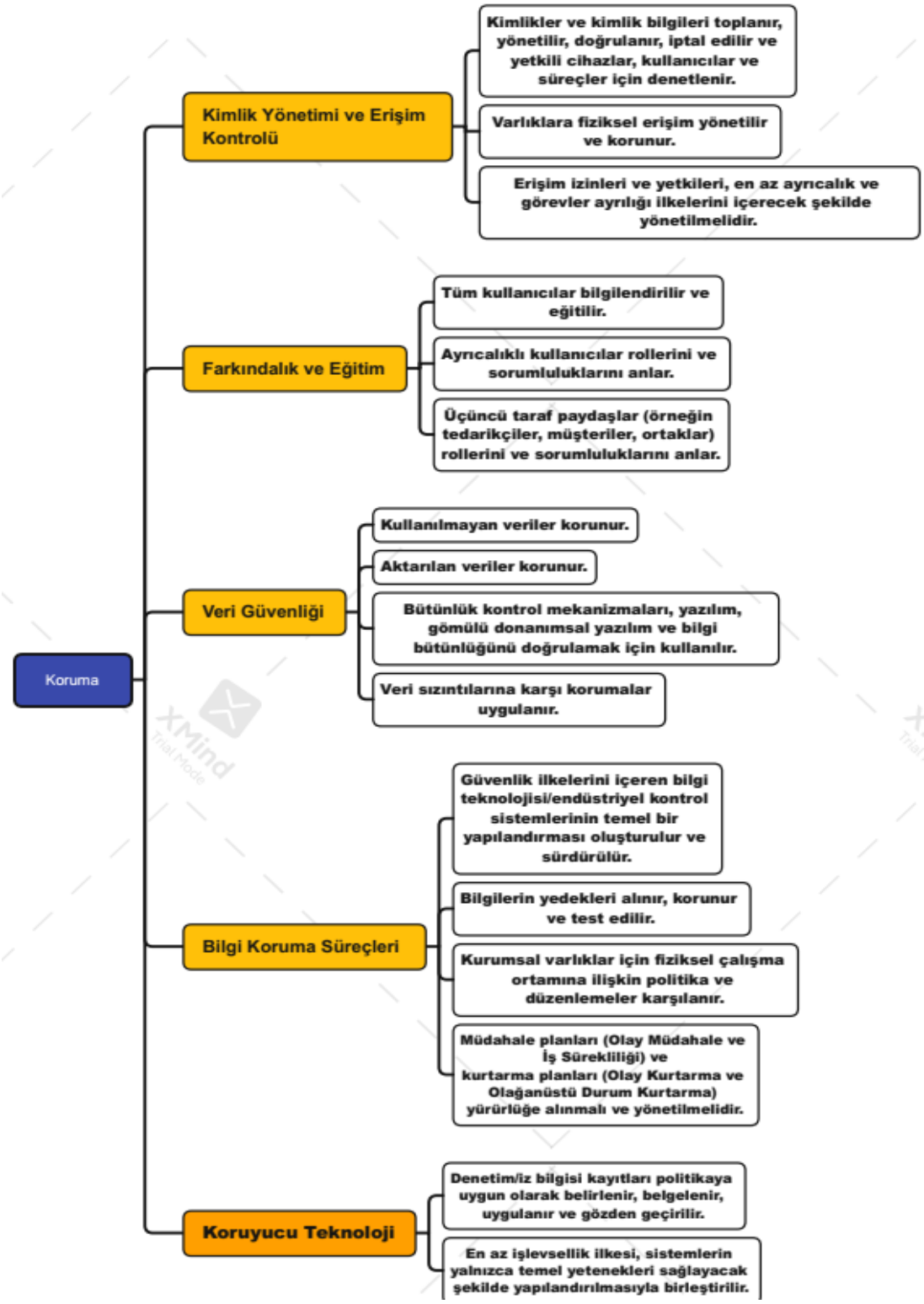
Kontrolü; Farkındalık ve eğitim, veri güvenliği; bilgi koruma süreçleri ve prosedürleri, bakım ve koruyucu teknoloji. İlgili süreçlere yönelik şema ve açıklamalar Şekil-33'de sunulmuştur.

Fiziksel ve mantıksal varlıklara ve ilgili tesislere erişim, yetkili kullanıcılar, süreçler ve cihazlarla sınırlıdır ve yetkili faaliyetlere ve işlemlere yetkisiz erişim olarak değerlendirilen riskle tutarlı bir şekilde yönetilir. Kuruluşun personeline ve ortaklarına siber güvenlik farkındalık eğitimi verilir ve ilgili politikalar, prosedürler ve anlaşmalarla uyumlu olarak siber güvenlikle ilgili görev ve sorumluluklarını yerine getirmeleri için eğitilir. Bilgi ve kayıtlar (veriler), bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak için kuruluşun risk stratejisiyle tutarlı bir şekilde yönetilir.

Güvenlik politikaları (amaç, kapsam, roller, sorumluluklar, yönetim taahhüdü ve kurumsal varlıklar arasındaki koordinasyonu ele alan), süreçler ve prosedürler sürdürülür ve bilgi sistemleri ve varlıklarının korunmasını yönetmek için kullanılır. Teknik güvenlik çözümleri, ilgili politikalar, prosedürler ve anlaşmalarla tutarlı olarak sistemlerin ve varlıkların güvenliğini ve esnekliğini sağlamak için yönetilir.

Kuruluşun personeline ve ortaklarına siber güvenlik farkındalık eğitimi verilir ve ilgili politikalar, prosedürler ve anlaşmalarla uyumlu olarak siber güvenlikle ilgili görev ve sorumluluklarını yerine getirmeleri için eğitilir. Üçüncü taraf paydaşlar (örneğin tedarikçiler, müşteriler, ortaklar) rollerini ve sorumluluklarını anlar.

Şekil-34: Koruma Şeması



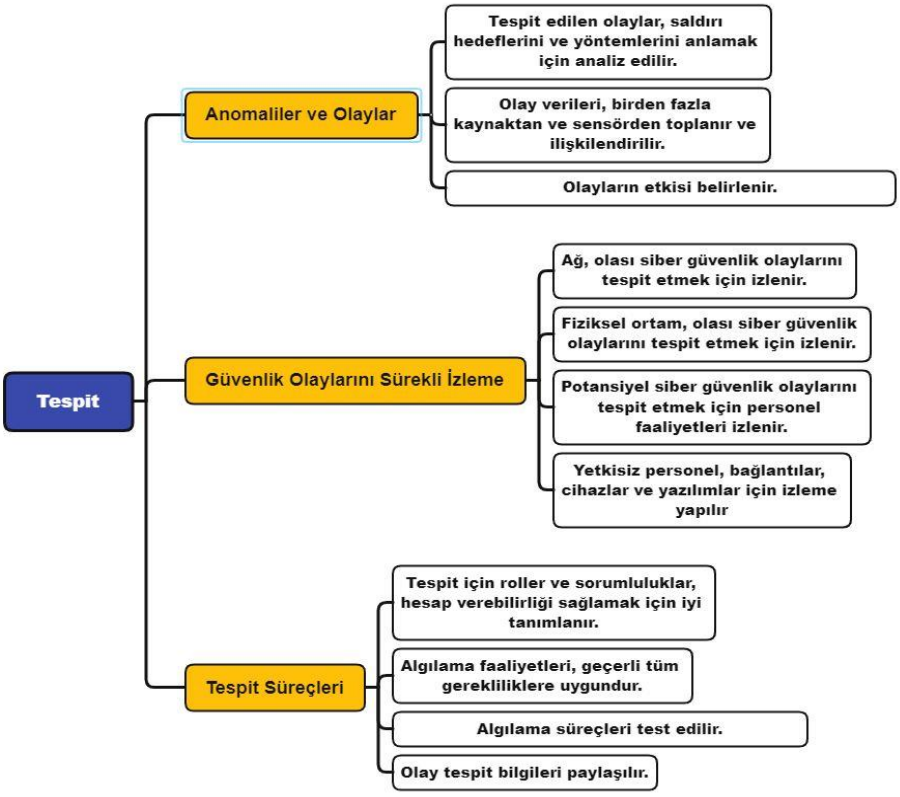
Kaynak: (NIST Cybersecurity Framework, 2018)

5.4.2.3 Tespit

Tespit işlevi, siber güvenlik olaylarının zamanında keşfedilmesini sağlar. Bu İşlev şunları içerir: Anomaliler ve Olaylar; Güvenlik Olaylarını Sürekli İzleme, Tespit Süreçleri. Aşamanın akış şeması Şekil-35'te sunulmuş, şema aşağıda açıklanmıştır.

Anormal olayların farkındalığını sağlamak için algılama süreçleri ve prosedürleri korunur ve test edilir. Tespit edilen olaylar, saldırı hedeflerini ve yöntemlerini anlamak için analiz edilir. Olay verileri, birden fazla kaynaktan ve sensörden toplanır ve ilişkilendirilir. Olayların etkisi belirlenir. Tespit için roller ve sorumluluklar, hesap verebilirliği sağlamak için iyi tanımlanır. Algılama faaliyetleri, geçerli tüm gerekliliklere uygundur. Algılama süreçleri test edilir. Olay tespit bilgileri paylaşılır.

Şekil-35: Tespit Şeması



Kaynak: (NIST Cybersecurity Framework, 2018).

5.4.2.4 Tepki

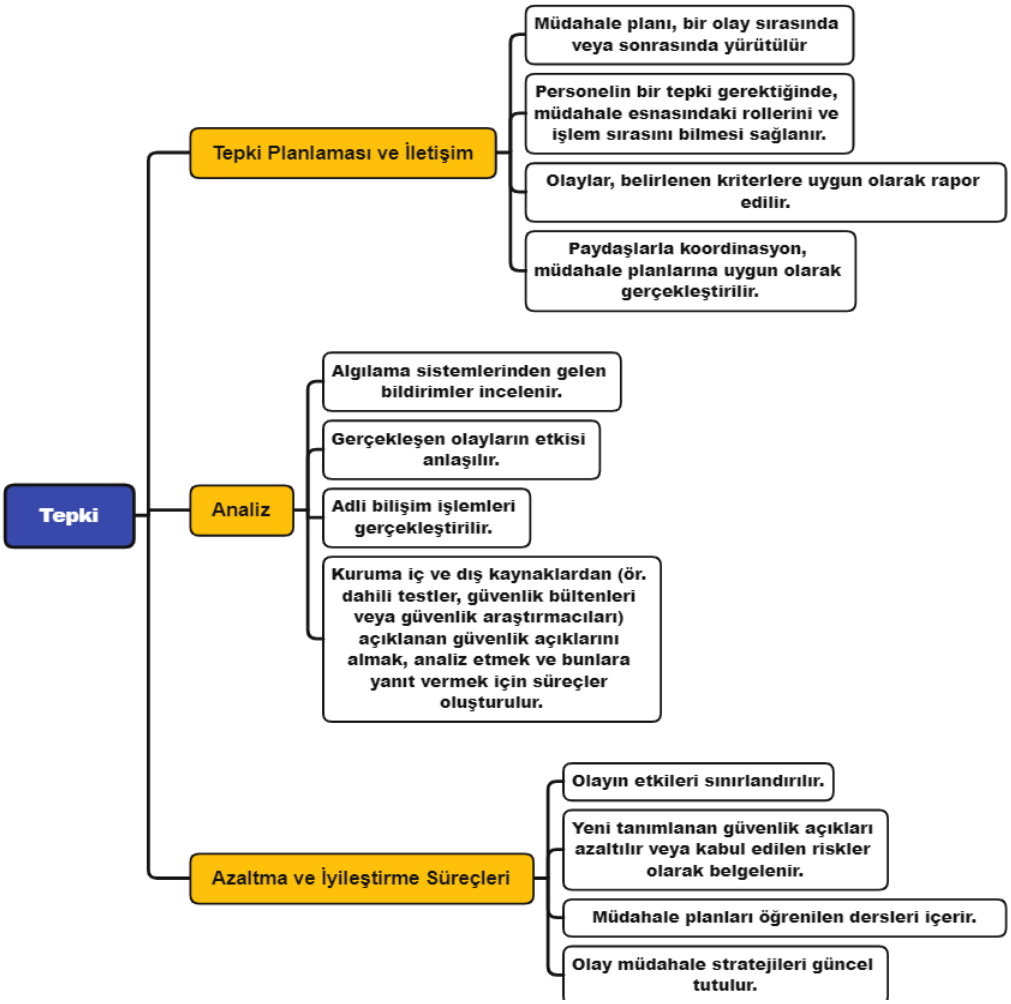
Bu aşamada tespit edilen bir siber güvenlik olayıyla ilgili önlem almak için uygun faaliyetleri geliştirilir ve uygulanır. Tepki İşlevi, olası bir siber güvenlik olayının etkisini kontrol altına alma yeteneğini destekler. Bu işlev şunları içerir: tepki planlaması ve iletişim, analiz; azaltma, iyileştirmeler. Aşamanın akış şeması Şekil-36'da sunulmuş, şema aşağıda açıklanmıştır.

Bu aşamada, Tespit edilen siber güvenlik olaylarına müdahale edilmesini sağlamak için müdahale süreçleri ve prosedürleri yürütülür ve sürdürülür. Müdahale faaliyetleri, iç ve dış paydaşlarla koordine edilir (örneğin, kolluk kuvvetlerinin dış desteği). Etkili müdahaleyi sağlamak ve kurtarma faaliyetlerini desteklemek için analiz yapılır. Bir olayın yayılmasını önlemek, etkilerini azaltmak ve olayı çözmek için faaliyetler gerçekleştirilir. Organizasyonel müdahale faaliyetleri, mevcut ve önceki tespit/cevap faaliyetlerinden öğrenilen dersler dahil edilerek geliştirilir.

Aşamanın analiz safhasında, algılama sistemlerinden gelen bildirimler incelenir. Gerçekleşen olayların etkisi anlaşılır. Kuruma iç ve dış kaynaklardan (ör. dahili testler, güvenlik bültenleri veya güvenlik araştırmacıları) açıklanan güvenlik açıklarını almak, analiz etmek ve bunlara yanıt vermek için süreçler oluşturulur.

Olayların etkilerinin azaltılması ve süreçlerin iyileştirilmesi aşamasında, gerçekleşen olayın etkileri sınırlandırılır. Risk analizinin güncel tutulması için, yeni tanımlanan güvenlik açıkları azaltılır veya kabul edilen riskler olarak belgelenir. Müdahale planları sürekli güncellenir ve daha önceki olaylardan öğrenilen dersleri içerir. Olay müdahale stratejileri sürekli olarak gözden geçirilerek güncel tutulur.

Şekil-36: Tepki Şeması



Kaynak: (NIST Cybersecurity Framework, 2018).

5.4.2.5 Kurtarma

Bu aşamada esneklik planlarını sürdürmek ve bir siber güvenlik olayı nedeniyle bozulan yetenekleri veya hizmetleri geri yüklemek için uygun faaliyetler geliştirilir ve uygulanır. Kurtarma İşlevi, bir siber güvenlik olayının etkisini azaltmak için normal işlemlere zamanında kurtarmayı destekler. Bu işlev şunları içerir: Kurtarma planlaması; iyileştirmeler ve iletişim. Aşamanın akış şeması Şekil-37'de sunulmuş, şema aşağıda açıklanmıştır.

Kurtarma süreçleri esnasında; siber güvenlik olaylarından etkilenen sistemlerin veya varlıkların geri yüklenmesini sağlamak için kurtarma süreçleri ve prosedürleri yürütülür ve sürdürülür. Kurtarma planlaması ve süreçleri, öğrenilen derslerin gelecekteki faaliyetlere dahil edilmesiyle iyileştirilir. Geri yükleme faaliyetleri, iç ve dış taraflarla (örn. koordinasyon merkezleri, İnternet Servis Sağlayıcıları, saldırı sistemlerinin sahipleri, kurbanlar, diğer SOME'ler ve vendor) koordine edilir.

Şekil-37: Kurtarma Şeması

Kaynak: (NIST Cybersecurity Framework, 2018).

Bir kuruluş, sunulan modeli siber güvenlik riskini belirleme, değerlendirme ve yönetmeye yönelik sistematik sürecinin önemli bir parçası olarak kullanabilir. Model, mevcut süreçlerin yerini alacak şekilde tasarlanmamıştır; bir kuruluş, mevcut siber güvenlik risk yaklaşımındaki boşlukları belirlemek ve iyileştirmeye yönelik bir yol haritası geliştirmek için mevcut sürecini kullanabilir ve model üzerine yerleştirebilir. Modeli bir siber güvenlik risk yönetim aracı olarak kullanan bir kuruluş, kritik hizmet sunumu için en önemli olan faaliyetleri belirleyebilir.

Bu bölümde ulusal güvenlik algımızı oluşturan tarihsel arka plan ve günümüz uygulamaları çerçevesinde, siber güvenlik kavramının ülkemizde stratejik seviye ’de nasıl algılandığı, araştırma esnasında elde edilen bulgular neticesinde analiz edilmiştir. Bu analiz sonrasında bir güvenlik sorununun siyasal alandan güvenlikleştirme alanına geçiş aşamasını oluşturan anlam verme aşamasının ülkemizdeki karşılığı analiz edilmiştir. Kriz yönetiminin diğer aşamaları olan karar verme, öğrenme, iletişim aşamaları mevcut uygulamalara göre tartışılmış, bulgular neticesinde değerlendirilmiştir.

Değerlendirme ve sonuç kısmında, araştırma neticesinde elde edilen sonuçlar açıklanmış, tespit edilen eksiklerinin giderilmesi, gelecekteki olası tehdit ve risklere yönelik alınması gereken tedbirler ve uygulamalar değerlendirilmiştir.

5.4.3 Gelecekte Siber Güvenlik Pazarı ve Yerli Siber Güvenlik Sanayi

HAVELSAN tarafından sunulan verilere göre 2020 yılında 184 milyar dolar olarak ölçülen küresel siber güvenlik pazarı 2023 yılında 248 milyar dolar, 2025 yılında ise 290 milyar dolar civarında olması öngörülmektedir. Türkiye açısından elde edilen veriler analiz edildiğinde 2019 yılında 120 milyon dolar seviyesinde olan siber güvenlik pazarının 2025 yılında 260 milyon dolar seviyesinde olacağı öngörülmektedir (Özarar, 2021).

Bir diğer önemli savunma sanayi firması olan STM, siber güvenlik ürün üreticisi ve hizmet sağlayıcısı konumundadır. STM verilerine göre yerli siber güvenlik pazarının %90’lık bir bölümü yabancı menşei ürünlere aittir (Korkut, 2020). Eldeki veriler analiz edildiğinde siber güvenlik alanındaki yerlilik oranın %10 seviyelerinde olduğu ve yakın gelecekte bu seviyede bir değişim yaşanmayacağı görülmektedir. Çalışma esnasında analizi gerçekleştirilen, Türkiye’deki siber güvenlik ürünü üretim faaliyetlerini koordine etmek üzere Savunma Sanayi Başkanlığı çatısı altında kurulan Türkiye Siber Güvenlik Kümelenmesi’ne kayıtlı yerli üreticilerin faaliyet alanları incelendiğinde “Gelecekte Operatif Seviyede Siber Güvenlik” başlığı altında incelenmiş olan siber güvenlik faaliyetlerini

karşılayabilecek ürün çeşitliliğinin mevcut olduğu görülmektedir. Ancak gerek ihracat verileri gerekse yerli pazardan alınan pay göz önüne alındığında yerli ürünlerin rakip yabancı ürünlerden geride kaldığı görülmektedir. Siber güvenliğin her alanında üretim yapmak yerine belli alanlara yoğunlaşarak o alanda uzman personel sayısının artırılması ulusal siber güvenlik endüstrisinin gelişimi için tercih edilen bir yöntemdir (Carr, 2018). Bu yöntemden yola çıkarak ortaya çıkartılacak bir Ulusal Siber Güvenlik Ürünü Üretim Kapasitesinin Artırımı Stratejisinin belirlenmesi gerek yetişmiş insan gücüne sahip olunması gerekse yerli siber güvenlik ürünlerinin kalitesinin artırımı sorunlarına çözüm olacaktır.

Günümüzde açık kaynak yazılım teknolojisi bilişim dünyasının tüm alanlarında yaygın bir şekilde kullanılmaktadır. Pek çok yeni start-up firması açık kaynak yazılımları özgünleştirerek büyümekte ve küresel bir üreticiye dönüşebilmektedir. Siber güvenlik sektöründe de benzer senaryolar yaşanmaktadır. Türkiye'nin gelecekteki yerli siber güvenlik ürün ihtiyacının karşılanması ve siber güvenlik ürünlerinin ihracatının artırılması için açık kaynak ürünlerden faydalanılması önemli bir girişim olacaktır. Bu alanda başarılı bir örnek olarak TUBİTAK tarafından geliştirilen "Açık Kaynak Kodlu Bütünleşik Siber Güvenlik Projesi" AHTOPOT sistemi gösterilebilir. Halen TSK gibi kritik kamu kurumları tarafından kullanılan AHTOPOT sistemi, Derinlemesine savunma için ihtiyaç duyulan siber güvenlik bileşenlerinin entegre edildiği bir sistemdir. İşletim sistemi olarakta yine TUBİTAK tarafından geliştirilen PARDUS işletim sistemini kullanmaktadır. (PARDUS ve AHTOPOT projeleri için Bknz. Ek-8) AHTOPOT sistemi siber güvenlik ekosistemini yerli ve milli ürünlerle tesis etmek isteyen kritik kamu ve özel sektör kurum ve kuruluşları için önemli bir alternatiftir.

DEĞERLENDİRME VE SONUÇ

Araştırma neticesinde, Türkiye'nin son yirmi yılda siber alanda gerçekleştirdiği faaliyetlerin siber alanın pek çok alt kapsamını kapsadığı, ilk siber güvenlik çalışmalarının başladığı 1990'lı yıllardan bugüne kayda değer pek çok gelişme yaşandığı tespit edilmiştir. Uluslararası Telekomünikasyon Birliğinin (ITU) tarafından 2021 yılında yayımlanan Global Siber Güvenlik Endeksi Raporu'nda Türkiye 11. sırada yer almıştır. Elde edilen bu başarının temelinde araştırma esnasında doğrulaması gerçekleştirilen siber güvenlik çalışmaları yer almaktadır.

Tez süreci sonucunda elde edilen sonuçların açıklanmasına geçmeden önce tezin bölümleri hakkında özet bir değerlendirme yapılmıştır. Tezin amacı olan Türkiye'de siber güvenlik kriz yönetimi süreçlerini ele almak için belirlenen kavramsal çerçeve neticesinde, siber güvenlikleştirme kavramlarının ülkemizdeki siber güvenlik mimarisinin inşası ve siber güvenlikle ilgili algı ve anlam verme aşamalarındaki karşılığına yönelik bulgu ve tespitlerin kısa bir analizi gerçekleştirilmiştir. Ayrıca Türkiye'nin güvenlik algısının nasıl şekillendiği ve bu algının siber güvenlik süreçlerine olan etkisi de değerlendirilmiştir.

Türkiye, konumu ve tarihsel geçmişi nedeniyle bölgemizdeki ve dünyadaki güvenlik krizlerinden etkilenmektedir. Soğuk savaşın bitmesiyle beraber güvenlik riski artan ülkeler grubunda yer almıştır. Soğuk savaş sonrası değişen güvenlik gündeminden, askeri güvenlik kavramı dışında ortaya çıkan yeni güvenlik kavramlarından etkilenmiştir. Bu etkenlerden dolayı ülkemizdeki resmi kurum ve kuruluşların kendi alanlarına yönelik güvenlik kaygısı, güvenlik misyonu olduğu tespit edilmiştir.

Bu kapsam da tezin kavramsal altyapısının oluşturulduğu üçüncü bölüme Türkiye'nin güncel resmi güvenlik algısının kısa gelişim tarihi ve önemli kurumların güvenlik kavramsallaştırılması üzerinden bir tespitle başlanmıştır. Bu yöntemin seçilmesinin temel nedeni ise kamu kurumları, özel sektör ve halkın temel gündelik işlemlerinin önemli bir kısmının siber uzaya bağlı bilgi sistemleri

vasıtasıyla yürütülmesidir. Bir diğer yorumla günümüzde gerek gündelik hayat pratikleri gerekse resmi işlemler, kamu yönetimi faaliyetleri, askeri güvenlik sistemleri vb. pek çok faaliyet, fonksiyon, işlem bilgi sistemlerine bağımlı durumdadır. Bu bağımlılık durumu, ülkemizin temel güvenlik meselelerinden siber uzayında etkilenmesi gerçekliğidir. Siber uzaydaki faaliyetler ülkelerin temel politikalarından bağımsız gelişmemekte, ülkelerin ekonomi, güvenlik, dış politika bakışları siber uzaya sirayet etmektedir. Bu sirayet durumu sadece resmi kurumlarda yaşanmamakta sivil toplumda bu sürecin bir parçası olmaktadır. İki ülke arasında yaşanan dış politika gelişmeleri, milli bilgisayar korsan gruplarını da etkilemekte, bu grupların faaliyetlerini yönlendirmesine neden olmaktadır.

Tezin teorik çerçevesi oluşturulurken güvenlikleştirme teorisi ve siyaset bilimi arasındaki ilişkiye dikkat çekilmiştir. Güvenlikleştirme teorisi, kamusal alandaki sorunları siyasallaşmamış, siyasallaşmış ve güvenlikleştirilmiş olmak üzere üç farklı şekilde ele almaktadır. Güvenlikleştirme sürecinde güvenlik sorunları güvenlikleştirici aktör olan devlet yönetimi tarafından güvenlikleştirme alanına alınarak siyasal süreçlerin dışında olağanüstü tedbirlerin alınması şeklinde tanımlanmaktadır. Bu süreç işletilirken, Schmitt çizgisinde bir hareketle dost düşman ayrımı penceresinden hareket edilmektedir. Schmitt'in (Schmitt, 2014) öne sürdüğü siyasal karşıtlığı belirleme ve bununla mücadele edilmesi süreci, güvenlikleştirme sürecinde benzer bir yoldan ilerleyerek siyasal olarak öteki, yabancı olanın yerine tehdit kavramını geçirmektedir.

Siber güvenlik alanında süreçler belirlenirken tehdit kavramı önemli girdiler sağlamaktır. Kurum/kuruluştaki işlerin sürekliliğinin sağlanması, meydana gelebilecek aksaklıkların azaltılması amacıyla bilginin tehditlerden korunmasını sağlamaktadır (Çağlar ve Özbilen, 2020, s. 89). Siber güvenlik süreçleri risk yönetimi temelinde geliştirilmekte, risk yönetimini ise tehditler, bu tehditlerin istismar edebileceği açıklıklar ve açıklarla etki sağlanabilecek varlıklar üzerinden gerçekleştirilmektedir. Siber güvenlik teknik süreçleri de, tehdit kavramından derinden etkilenmekte, siber tehdit istihbaratı, tehdit analizi, tehdit avcılığı faaliyetleri önemli siber güvenlik faaliyetleri arasında yer almaktadır. Siber

güvenlik stratejileri, politikaları da oluşturulurken de tehditler önemli bir yer tutmakta tehdit kavramsallaştırılmasına göre politikalar inşa edilmektir. Schmitt üzerinden örneklendirildiğinde öncelikle siyasal olarak öteki belirlenmekte ve bununla mücadele edilmektedir. Siber güvenlik alanında paralel sürecin izlenmesi ise, siber tehdit analizinin gerekli teknik yetkinliğe sahip kişilerin görüşleri alınmadan gerçekleştirildiği, siber güvenliğin stratejik yönetiminden sorumlu birimlerin kapsamlı bir teknik görüş almadığı için bazı reel tehditler, güvenlik gündemine alınmamakta bu tehditlere karşı gerekli tedbirler alınamamaktadır. Bir diğer sorun ise tespit edilen tehditler güvenlik gündemine alınırken yanlış değerlendirilmekte ve aşırı güvenlikleştirme kavramı ortaya çıkmaktadır. Siber güvenlik alanındaki aşırı güvenlikleştirme ve güvenlik dışı kalma sorunsallarının ülkemizdeki varlığı tez süresince gözetilmiş, gerçekleştirilen analizlerde ön planda tutulmuştur. Kapsamlı bir siber güvenlik politikasının belirlenmesi ve güvenli bir siber uzay için güvenlikleştirme sürecinin yanlış güvenlikleştirme ve hiper güvenlikleştirme süreçlerinden arındırılması gerekliliğine ilişkin önerme tez süresince test edilmiştir.

Güvenlikleştirme sürecinin bir diğer önemli önermesi olan “güvenlik sektörleri kavramları arasına zaman içerisinde yeni sektörlerin eklenmesi” ve bu “yeni sektörler arasında siber uzayın yer almasının gerekliliğine” ilişkin çalışmalar analiz edilmiştir. Siber uzayın mevcut büyüklüğü ve birey düzeyinden uluslararası organizasyonlar düzeyine kadar tüm düzeylerle etkileşim seviyesinin yüksekliği, siber uzayda yaşanan güvenlik olaylarının etkisinin büyüklüğü ve niteliğinin analizi sonucunda, siber uzayı yeni bir güvenlik sektörü olarak ele alan çalışmaların doğrulanmasını sağlamıştır.

Araştırmanının dördüncü bölümünde, Siber güvenlik kavramının tarihsel süreci analiz edilmiş, analiz sonucunda başlangıçta askeri bir faaliyet olarak ortaya çıkan bilgisayar ağları kurma düşüncesinin hızla gelişerek zaman içerisinde küresel bir ağla sonuçlanmasının, bu hızlı gelişmeler neticesinde güvenlik sorunlarını doğurduğu sonucuna ulaşılmıştır. Bu gelişimin ülkemizdeki iz düşümü de benzer bir durum sergilemektedir. Nedeni ise, siber uzayın fiziksel, mantıksal

ve insan-siber uzay etkileşim katmanlarındaki süreçlerin, cihazların, uygulamaların, protokollerin uluslararası karşılıklarına uyumlu olmak zorunda olması ve bu alandaki dışa olan bağımlılıktır. Son dönemde gerçekleştirilen yerli ağ cihazları, güvenlik ürünleri, yazılım teşviklerinin çıkış noktasında dışarıdan alınan sistemlerde yer alan güvenlik açıklıklarının yeteri kadar tespit edilememesi nedeniyle sahip oldukları potansiyel güvenlik risklerinin farkındalığının artması olduğu değerlendirilmektedir. Araştırma içerisinde örneklendirilen siber olaylarda ülkelerin ithal sistemler nedeniyle yaşadığı somut siber güvenlik olayları, ülkemizdeki bu endişeleri destekler niteliktedir.

Araştırmanın beşinci bölümünde, siber güvenlik kavramlarının ülkemizdeki karşılığının analizi gerçekleştirilmiştir. Siber güvenlik kavramının ülkemizde güvenlik gündemine girişi, bilgisayar kullanımının artışa geçtiği 90'lı yılların başlangıç döneminde gerçekleşmiştir. Bu dönemde henüz internet kullanımı yaygınlaşmamış olup, bilgisayar kullanımındaki artışa paralel olarak bilgisayar suçları olarak nitelenen bazı davranış şekilleri ortaya çıkmış ve yasa koyucu tarafından düzenlenerek yaptırıma bağlanmıştır. TCK'na 1991 yılında 3756 sayılı yasa ile eklenen "m.525a, m.525b, m.525c ve m.525d" bilgisayar programlarını hukuka aykırı olarak ele geçirme, bilgisayar sisteminde yer alan verileri tahrip etme, silme, değiştirme, bilgisayar sistemini kullanarak haksız çıkar sağlama ve sahtekarlık gibi fiilleri, suç haline getirmiştir. Siber suçlar, internetin yaygınlaşması ve bilgi toplumuna dönüşüm projelerinin başlamasıyla birlikte 2000'li yılların başından itibaren kapsamlı bir niteliğe bürünmüştür. Ülkenin siber güvenlik politikalarını, bilgi toplumuna dönüşümle beraber ortaya çıkacak olan dijitalleşmenin getireceği yeni güvenlik sorunları belirlemiştir. İlgili gelişmelerin ulusal güvenliğe zarar vereceği endişesinin politikalara hakim olduğu tespit edilmiştir. O dönemden bugüne kadarki gelişmeler izlendiğinde siber güvenlik sorunlarının ulusal güvenliğe zarar verebileceği düşüncesinin korunduğu görülmüş, 2020 yılında yayımlanan ulusal siber güvenlik stratejisinde de aynı düşüncenin korunduğu tespit edilmiştir. Siber güvenlik kavramsallaştırması bu nedenle ülkemizde ulusal güvenliğe yönelik tehditler üzerinden inşa edilmiştir.

Siber tehditler ulusal siber güvenliğe yönelik tehdit aktörleri üzerinden ele alınmıştır.

Beşinci bölümde ele alınan bir diğer kavram da siber güvenlik krizlerinin yönetimi olmuştur. Kriz yönetimi kavramı ve siber güvenlik kavramlarının kendine özgü durumu karşılaştırılarak, Boein ve arkadaşları (Boin, Stern, & Sundelius, 2005) tarafından ortaya konan dört aşamalı kriz yönetimi faaliyetlerinin AB Siber Güvenlik Ajansı (ENISA) tarafından AB siber güvenlik kriz yönetimi süreçleri analiz edilirken kullanıldığı tespit edilmiştir. Adı geçen aşamaların siber güvenlikleştirme üzerinden siber güvenlik krizlerinin analizine uygun olduğu belirlenmiştir. Söz konusu aşamaların siber güvenlik faaliyetlerine uyumluluğunu araştıran çalışmalar analiz edilerek ilgili aşamaların esasları, siber güvenlik kriz yönetimi faaliyetleri doğrultusunda belirlenmiştir. Bu aşamada ayrıca güvenlikleştirme kavramları ve kriz yönetimi arasındaki ilişki analiz edilmiş, siber güvenlikleştirme süreçleri ile kriz yönetimi faaliyetleri arasındaki paralellikler ortaya çıkarılmıştır. Başarılı bir siber güvenlik için siber olay yönetim, risk analiz süreçlerinin yetersiz kaldığı, ulusal seviyede oluşabilecek kapsamlı siber güvenlik olaylarının güvenlik krizine dönüşmesinin ancak siber güvenlik kriz yönetimi süreçlerinin kriz öncesi dönemde işetilmesi ile engellenebileceği sonucuna ulaşılmıştır.

Türkiye'de siber güvenlik faaliyetlerinin stratejik seviyede önemsenmesi, bilgi toplumuna dönüşüm süreçleri içerisinde ele alınmasıyla başlanmıştır. 2006 yılında, bu çalışmalar neticesinde alınan kararlar doğrultusunda Bilgisayar Olaylarına Müdahale ekiplerinin kurulması kararlaştırılmıştır. Ayrıca TUBİTAK tarafından başlanmış olan siber güvenlik faaliyetlerinin artırılması yönünde kararlar alınmış ve bu alanda somut adımlar atılmıştır. Siber güvenlik kavramı, bu gelişmelerden sonra 2010'lu yılların başından itibaren elektronik haberleşme ekseninde değerlendirilmiş, ulusal siber güvenlik politikalarının kritik altyapı güvenliği üzerinden inşası düşüncesi ortaya çıkmıştır. Bu alandaki ilk somut adım 2012'de atılmış, "Ulusal Siber Güvenlik Kurulu" kurulmuş, bu alandaki temel sorumluluk Ulaştırma ve Altyapı Bakanlığı ve bağlı kurumu olan BTK'ya

verilmiştir. 2014, 2016 ve 2020 yıllarında yayımlanan siber güvenlik strateji belgelerinde de elektronik haberleşme kritik altyapısı üzerinden sergilen bu yaklaşıma devam edildiği sonucuna ulaşılmıştır.

Siber güvenlik kriz yönetimi süreçleri üzerinden ülkemiz faaliyetleri analiz edildiğinde, ülkemizde kriz yönetiminden sorumlu iki ana kurum olan GAMER ve AFAD'ın da benzer bir yaklaşım içerisinde olduğu, siber güvenliği teknoloji kaynaklı güvenlik ve afet olayları kapsamında değerlendirdikleri sonucuna ulaşılmıştır. Türkiye'de siber güvenlik faaliyetleri, elektronik haberleşme odağında ele alınmakta, Ulaştırma ve Altyapı Bakanlığı'nca gerekli hukuki düzenlemeler gerçekleştirilmektedir. İlgili bakanlık teşkilatında yer alan USOM'un siber güvenlik olaylarının yönetimde öne çıktığı sonucuna ulaşılmıştır. USOM çatısı altında siber olay müdahale, tespit, erken uyarı, siber olaylara hazır olma süreçlerinde çağın gereklerini karşılayan bir yapılanmanın mevcut olduğu değerlendirilmiştir. Ancak siber güvenlik kriz yönetiminin diğer aşamalarında da teknik yorum bakış açısı korunduğu için sadece teknik bir yönetim mimarisinin çizildiği, diğer güvenlik sektörlerine yönelik idari ilişkilerin gözetilmediği, bu durumun da kriz esnasında yönetim krizlerine neden olacağı sonucuna ulaşılmıştır.

Kriz yönetimi süreçlerinde kriz yönetici aktörün güvenlikleştirme bakış açısıyla, güvenlikleştirici aktörün belirleyici bir önemi vardır. 2000'li yılların başında kurulması öngörülen "ulusal bilgi güvenliği kurulu ve kurumunun" kuruluşunun hayata geçirilemediği tespit edilmiştir. Süreç içerisinde bu kurumun yerine, yetki kapsamı daha dar olan "Siber Güvenlik Kurulu", Ulaştırma ve Altyapı Bakanı başkanlığında kurulmuştur. Kurulması öngörülen "Bilgi Güvenliği Kurumu" yerine, teknik bir kurum olan BTK'ya ilgili kurumun görev ve yetkileri verilmiştir. BTK süreç içerisinde siber uzayın teknik yönetimi ve güvenliğinin sağlanması alanlarında önemli bir aktöre dönüşmüştür. Ancak siber güvenlik kurulu zaman içerisinde istenen faydayı sağlayamamış, ulusal çapta güvenlikleştirici aktör rolünün gereklerini yerine getirememiştir. Cumhurbaşkanlığı hükümet sistemine geçişle beraber bu kurul "Elektronik Haberleşme Kanunu"nda değişiklik yapılarak

kaldırılmış ve Cumhurbaşkanının belirleyeceği kurul olarak değiştirilmiştir. Ancak şu ana kadarki dönem içerisinde bu kurulun belirlenmediği, Ulusal Siber Güvenlik Stratejisi, 2020 2023'te kurula yer verilmediği sonucuna ulaşılmıştır. İlgili strateji belgesinde Ulaştırma ve Altyapı Bakanlığı temel güvenlikleştirici aktör olarak belirlenmiştir.

Siber güvenlik kavramının ülkemizde bilgi toplumuna dönüşümle beraber ulusal çerçevede ele alınması sürecine Cumhurbaşkanlığı Hükümet Sistemi'ne geçişle beraber devam edildiği, bu sürecin önemli adımlarından olan dijital dönüşüm sürecinin yeni kurulan Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yönetildiği ve ilgili ofise siber güvenlikle ilgili önemli görevler verildiği tespit edilmiştir.

Araştırma bulgularına göre siber güvenlik kavramı ve siber tehditlerin boyutu siber uzayla eşzamanlı olarak genişlemiştir. Siber uzayın sahip olduğu büyüme ivmesi, gelecekte günümüzdekine oranla çok daha fazla siber güvenlik tedbir ve uygulaması ihtiyacı doğuracaktır. Ulusal güvenliği tehdit eden siber tehditler de bu eksenden hareketle çoğalacak ve siber güvenlik kavramı, ulusal güvenlik meselelerinde daha hayati bir konuma erişecektir. Araştırmada elde edilen bulgular neticesinde siber güvenlik krizlerinin ulusal güvenlik krizlerine neden olabileceği ve ülkemizin olası siber güvenlik krizlerine ilişkin hazırlık seviyesinde eksiklikler olduğu soncuna ulaşılmıştır. Tezin amaçları arasında yer alan "ulusal siber güvenlik uygulamaları gelecekte nasıl olmalı" sorunsalının çözümü yine araştırma bulguları neticesinde elde ettiğimiz siber uzay ve insan-toplum etkileşimi, siber tehditler, siber güvenlik uygulamaları analizlerinin değerlendirmesi ile sağlanmıştır.

Siber uzayın yönetimi ve güvenliğinin sağlanmasının temel kaynakları arasında uluslararası standartlar bulunmaktadır. Siber güvenliğinin eksiksiz sağlanabilmesi için sahip olunan bilgi sistemlerinin yapısına uygun politika ve standartlara uyum sağlanmalıdır. Araştırmanın dördüncü bölümünde açıklanan elektronik haberleşme kanunu da, elektronik haberleşmede uluslararası

standartlara uyulması gerektiğini belirtmektedir. AB genelinde siber güvenlik uygulamalarını belirleyen kuruluş olan AB Siber Güvenlik Ajansı'nın ortaya koyduğu Ulusal Siber Güvenlik Uygulamaları Çerçevesi'ne göre oluşturulan model EK-8'de sunulmuştur. AB Siber Güvenlik Ajansı, gelecekteki bu siber güvenlik uygulamalarının bu çerçevenin analizi neticesinde şekillenmesi gerektiğini belirtmektedir. Gelecekte ülkemizdeki ulusal siber güvenlik uygulamalarının nasıl olmasına ilişkin değerlendirmeler bu çerçeve kapsamında gerçekleştirilmiştir.

Ulusal acil durum planlaması, olası krizler öncesinde gerçekleştirilmelidir. Türkiye'deki siber güvenlik uygulamaları incelendiğinde ulusal acil durum planlamasının bulunmadığı tespit edilmiştir. Araştırma esnasında analiz edilen USOM'un "siber olay yönetim çerçevesi" ve AFAD'ın siber kriz öngörüleri ulusal acil durum planlaması kapsamında olmadığı sonucuna ulaşılmıştır. Tüm güvenlik sektörlerini etkileyebilecek kriz senaryolarına göre, ulusal acil durum planlamalarının yapılması olası güvenlik krizlerinde krizin boyutunun ortaya çıkarılması ve krize yönelik çözümlerin üretilmesi için yol gösterici olacaktır. Acil durum planlaması olmaksızın gerçekleştirilecek bir kriz yönetimi süreci, krizin uzamasına neden olacak, krizin boyutuna göre can ve mal kaybına neden olacaktır. Kurumların kendi siber güvenlik kriz acil durum planlamalarına sahip olması ulusal çaptaki planlamalara katkı sağlayacaktır.

Bu kapsamda Türkiye'de güvenlikleştirici aktör olarak belirlenmiş olan Ulaştırma ve Altyapı Bakanlığı öncülüğünde ulusal siber güvenlik acil durum planlamasının çeşitli senaryolara göre taktik seviyeden stratejik seviyeye kadarki tüm süreçleri içerecek şekilde ulusal siber güvenlik acil planının oluşturulması gereklidir. Dijital Dönüşüm Ofisi'nin gerçekleştirmeyi planladığı denetimlerin kontrol listelerine acil durum planına olan uyum maddeleri eklenmelidir. Her planın gerçek olaylar meydana gelmeden, tatbikatlarla test edilmesi gereklidir. Bu kapsamda güvenlikleştirici aktörlerin koordinasyonunda acil durum planının ulusal tatbikatlarla test edilmesi, planın eksiklerinin ortaya çıkarılmasını sağlayacaktır.

Ulusal siber güvenlik ortak kriterlerinin belirlenmesi, ülke genelindeki siber güvenlik faaliyetlerinin koordine halinde icra edilmesi için elzem durumdadır. 2020 yılının ortalarında yayımlanan Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi öncesindeki çalışmaların yetersiz olduğu sonucuna ulaşılmıştır. Bilgi ve İletişim Güvenliği Rehberi, alandaki bazı boşlukları doldurmuştur. Ancak siber güvenliğin alt kırılımlarına yönelik standartların belirlenmesine ilişkin eksiklikler devam etmektedir. Siber güvenlik kavramın bütüncül bir kavram olduğu ve bazı alanlarda gerekli tedbirlerin alınmasının yeterli olmadığı değerlendirilmiştir. Bu kapsamda siber güvenlikle ilgili teknik detayların yer aldığı kapsamlı ulusal kriterlerin belirlenmesi gelecekteki siber güvenlik uygulamalarını şekillendirecek ve olası krizlere karşı olan hazırlık seviyesini artıracağı düşünülmektedir.

Dijital kimliğin korunması ve siber uzaydaki resmi faaliyetlere olan güvenin inşası, bir diğer ulusal siber güvenlik faaliyetidir. Siber uzaya olan resmi yaklaşımın “siber-persona”, insan - siber uzay etkileşim katmanını gözetmediği görülmüştür. Dijital kimlik kavramı da bu durumdan etkilenmektedir. Kişinin dijital kimliğinin korunması, siber uzaydaki mülkiyet haklarının gözetilmesi başta olmak üzere T.C. Anayasası'nda yer alan temel hak ve özgürlüklerinin dijital alanda korunması ile olanaklıdır. Siber alana özgü kanun ve normların azlığı, dijital kimliğin korunmasına yönelik boşluklara neden olmaktadır. Fiziksel dünyayı düzenleyen tüm hukuki uygulamaların siber uzaydaki karşılığını belirleyen çalışmaların Adalet Bakanlığı öncülüğünde gerçekleştirilmesi ulusal siber güvenlik çalışmalarına katkı sağlayacaktır.

Kapasite ve farkındalık artırımı, siber güvenlik faaliyetlerin başarısında önemli rol oynamaktadır. Gelinen nokta değerlendirildiğinde kapasite artımının gelişmiş insan gücü boyutunda, eksiklikler göze çarpmaktadır. Gerek resmi eğitim kurumları gerekse özel eğitim kurumları pek çok siber güvenlik eğitim programına sahiptir. Ancak verilen eğitimlerin içeriği ve kapsamı başlangıç seviyesinde kalmaktadır. Temel siber güvenlik eğitimi almış insan gücü çok fazlayken, bu gücün ileri seviyeye dönüşmesini sağlayacak olan, işte yaparak öğrenme

aşamasında büyük eksiklikler vardır. Belirli iş kollarını icra ederken gerekli görülen uzman bulundurma zorunluluğu, siber güvenlik alanında mevcut değildir. Kimi durumlarda onlarca kişinin çalıştığı bilgi teknolojileri firmalarında tek bir siber güvenlik personeli bulunmamaktadır. Benzer bir durum, kamu kurumları içinde geçerlidir. Ülkemizde sadece bankacılık alanı geçmiş dönemde yaşadığı büyük maddi kayıpların neticesinde yeterli güvenlik personeli bulundurmaya başlamış ve pozitif olarak ayrışmıştır. Bilgi teknolojileri alanında gerçekleştirilen hizmet ya da üretime oranla siber güvenlik personelinin bulundurulmasına ilişkin hukuki zorunluluk sağlanması başlangıç seviyesindeki siber güvenlik iş gücünün tecrübe edinerek gelişimi sağlaması ve ileri seviye siber güvenlik işgücünün beyin göçü şeklinde yurtdışına gidişine engel olunmasına büyük katkı sağlayacaktır. Gelecekte gerçekleştirilecek olan tüm eğitim faaliyetleri planlamaları ile eşzamanlı olarak yetişmiş personelin istihdamına ilişkin planlama gerçekleştirilmelidir. Günümüzde gelişmiş ülkelerin hemen hepsi yetişmiş siber güvenlik işgücüne ihtiyaç duymakta ve bu ihtiyacını beyin göçü vasıtasıyla gidermektedir. Bu anlamda siber güvenlik uzmanlarının ülkelerine yerleşmelerinde kolaylıklar sağlanmaktadır. Ülke imkanları ile yetiştirilen işgücünün dışarıya kaçmasının engellenmesi için gerekli istihdam politikalarının stratejik seviyede planlanması gerekmektedir.

Ülke genelinde siber tehditlere yönelik farkındalığın artırılması olası siber güvenlik olaylarının önüne geçilmesini sağlayacaktır. Milyonlarca lira harcanan bir siber güvenlik sistemi, yeterli farkındalığa sahip olmayan bir personelin basit parola kullanımı yada kontrolsüz taşınabilir bellek kullanımı gibi nedenlerle kolayca aşılabilmektedir. Araştırmanın dördüncü bölümünde ele alına ABD tarihindeki en büyük siber olay olan “Sunburst” olayı basit parola kullanımı nedeniyle, İran nükleer tesislerini hedef alan Stuxnet olayı ise kontrolsüz taşınabilir bellek kullanımı nedeniyle gerçekleşmiştir. İlkokuldan itibaren eğitimin her aşamasında zorunlu siber güvenlik seminerlerinin verilmesi, öğrencilerin farkındalık seviyesinin sürekli olarak test edilip farkındalığı düşük öğrenciler için ek önlemler alınması gelecekte gerçekleşmesi muhtemel pek çok siber olayın önüne geçecektir. Kamu ve özel sektör çalışanlarının farkındalığının artırılmasına

yönelik eğitim ve tatbikatların icrası, bu kurum ve kuruluşların siber güvenlik seviyesini yükseltecektir. Kamu denetimlerinde farkındalık testine yer verilmesi de, geleceğe ilişkin bir diğer önemli uygulama olacaktır.

Kapasite artırımının bir diğer önemli adımı, yerli siber güvenlik teknolojileri ile alanda ileri teknoloji üretimidir. Aslında Türkiye'de, yerli siber güvenlik teknolojilerine yönelik devlet desteğinin yeterli seviyede olduğu rahatlıkla söylenebilir. Siber kümelenme altındaki yerli firmalar siber güvenliğin alt alanlarına yatırım yapmakta ve ürün geliştirmektedir. Ancak siber güvenlik alanında ileri teknoloji üretilemediği durumlarda bu çalışmalar eksik kalmaktadır. Türkiye'de dünya çapında rekabet edebilecek kapsamlı bir siber güvenlik firması bulunmamaktadır. Bu durum alanda eksikliklere neden olmakta katma değeri yüksek ürün üretimini engellemektedir. Resmi düzenlemelerle bu ürünlerin alımının zorunlu tutulması yerine, bu ürünlerin yurtdışına satış yapma kapasitesi artırılmasına yönelik politikalar üretilmelidir.

Siber uzay insan etkileşimin boyutları çalışma esnasında analiz edilmiş, günümüz insanı için sanal alandaki varlığının, fiziki alandaki varlığına eşdeğer bir anlam taşıdığı sonucuna ulaşılmıştır. Siber uzayda yer alan kişisel verilerin gizliliğinin ve mahremiyetinin sağlanmasının önemi, bu büyüme ve genişleme ile paralel olarak artmaktadır. Türkiye'de gerçekleştirilen kişisel verilerin korunması faaliyetlerinin analizi sonucunda bu faaliyetlerin dünyadaki örneklerine göre geç başladığını ancak Kişisel Verilerin Korunması Kanunu'nun çıkarılması ile birlikte alanda gelişme sağlanmaya başlandığı sonucuna ulaşılmıştır. Cezai müeyyide uygulanması ve sıkı denetimler bu alandaki başarıyı artıracaktır. Günümüzdeki uygulamalarda kanunu ihlal eden firmalara cezai müeyyide uygulanmakta ancak ceza miktarlarıyla alınması gereken güvenlik tedbirlerinin miktarı karşılaştırıldığında cezalar caydırıcı olamamaktadır. Denetim faaliyetleri kapsamında bir denetim mekanizması bulunmakta, şikayet ve başvuru yoluyla ihlaller tespit edilmektedir. Cezaların caydırıcılığın artırılması, bağımsız ve nitelikli bir denetim mekanizmasının kurulması gelecekteki ihlalleri engelleyecektir.

Tez çalışması boyunca gerçekleştirilen analizler, siber uzayın karmaşıklığını ve siber güvenlik kavramının ulusal güvenlik için olan önemini ortaya koymuştur. Geleceğe ilişkin analizler, bu önemin artan bir ivme ile büyüyeceğini ve gerek uluslararası güvenlik gerekse iç güvenlik sorunları içerisindeki ağırlığının hayati seviyelere ulaşacağını göstermektedir. Geleceğe ilişkin değerlendirmelerin uygulama aşamasına geçebilmesi için bağımsız ve nitelikli ulusal siber güvenlik otoritesine gerek duyulmaktadır. Türkiye'de siber güvenlik kavramı, son 25 yılda elektronik haberleşme ve dijital dönüşüm çerçevesinde ele alınmıştır. Siber uzayın genişleyen yapısının beraberinde getirdiği güvenlik sorunlarının çözümünü kapsayan bir ulusal siber güvenlik otoritesi ortaya çıkartılamamıştır. Elde edilen bulgular bu kapsamda değerlendirildiğinde, mevcut yapı ile devam edilmesi durumunda krize varmayan siber olaylarda başarı sağlanabileceği ancak olası ulusal siber güvenlik krizlerinde ciddi yönetim sorunlarının çözümünde ciddi sıkıntılar yaşanabileceği, siber uzayın kriz yönetimi esaslarına göre tam olarak güvenlikleştirilemediği sonucuna ulaşılmıştır. Gelecekteki tehdit ve riskler göz önünde bulundurulduğunda; siber güvenlik kavramının tüm alt alanlarında uzmanların bulunduğu nitelikli ve bağımsız bir ulusal otoritenin, gerekli hukuki yaptırım gücüyle donatılarak tesis edilmesi gerektiği sonucuna ulaşılmıştır.

KAYNAKÇA

A Glossary of Common Cybersecurity Terminology. (2014). Department of Homeland Security.

Açıkmeşe, S. A. (2011). Algı mı, Söylem mi? Kopenhag Okulu ve YeniKlasik Gerçekçilikte Güvenlik Tehditleri. Uluslararası İlişkiler, 43-73.

Akgül, M. (1996, Aralık 14). Doğru Bilinen Yanlışlar. Milliyet.

Akkuş, A. (2020). COVID-19 Sürecinde Kriz Yönetimi ve Stratejik Planlama. E. Şen, D. Hıdıroğlu, & O. Yılmaz (Dü) içinde, COVID-19 Pandemisinde Yönetim ve Ekonomi. Ankara: Gazi Kitapevi.

Akyeşilmen, N. (2018). Disiplinler Arası Bir Yaklaşımla Siber Politika ve Güvenlik. Ankara: Orion.

Arts, S. (2019). Offense as the New Defense: New Life for NATO's Cyber Policy. GMF.

Ata, F. K. (2014). Uluslararası Hukukta Savaş ve Barış. Mülkiye Dergisi, 83-89.

Atasever, S., Özçelik, İ., & Sağıroğlu, Ş. (2019). Siber Terör ve DDoS. Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 238-244.

Aydın, M., & Eker, F. (2013). Türkiye'de Güvenlik: Algı, Politika,Yapı. istanbul: İstanbul Bilgi Üniversitesi Yayınları.

Backman, S. (2020). Conceptualizing cyber crisis. Contingencies and Crisis Management, 1-10.

Balzacq, T. (2010). Securitization Theory. Oslo: PRIO.

Banks, M. A. (2008). On the Way to the Web: The Secret History of the Internet and Its Founders. New York: Apress.

Bayar, A. (1999, ocak 24). Siber Uzay'da Herkes Travesti. Milliyet.

Bayuk, J. L. (2012). Cyber Security Policy Guidebook. John Wiley & Sons, Inc.

Benedikt, M. (1991). Introduction. M. Benedikt içinde, Cyberspace: First Steps (s. 1-27). London: The MIT Press.

BGA Security. (2020, Aralık 15). www.bgasecurity.com adresinden alındı

Bıçakçı, S. (2014). NATO'nun gelişen tehdit algısı: 21. Yüzyılda siber güvenlik. Ulusarası İlişkiler, 101-130.

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

Biden'dan Rusya'ya siber savaş sinyali. (2020, Aralık 28). Sözcü Gazetesi İnternet Sitesi: https://www.sozcu.com.tr/2020/dunya/bidendan-rusyaya-siber-savas-sinyali-6178972/ adresinden alındı

Bıktım, E. (2019). Garanti Bankası ve Türk Telekom siber saldırıya maruz kaldı. Hürriyet Gazetesi: https://www.cnnturk.com/teknoloji/garanti-bankasi-ve-turk-telekom-siber-saldiriya-maruz-kaldi adresinden alındı

Bilgi Toplumu Dairesi Hakkında. (2020, Aralık 29). T.C. Strateji ve Bütçe Başkanlığı Resmi İnternet Sitesi: http://www.bilgitoplumu.gov.tr/bilgi-toplumu/bilgi-toplumu-dairesi-hakkinda/ adresinden alındı

Boeke, S. (2018). National cyber crisis management: Different Europe Approaches. Governance, 449-464.

Boin, A., Stern, E., & Sundelius, B. (2005). The Politics of Crisis Management. New York: Cambridge University Press.

Bozgeyik, A. (2018). Gaziantep'te Faaliyet Gösteren Orta ve Büyük Ölçekli İşletmelerin Siber Güvenlik Yönetim Yaklaşımlarının Analizi(Yayılanmamış Doktora Tezi). Gaziantep: Hasan Kalyoncu Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilimdalı.

Brauch, H. G. (2008). Güvenliğin Yeniden Kavramsallaştırılması: Barış,Güvenlik, Kalkınma ve Çevre Kavramsal Dörtlüsü. Uluslararası İlişkiler, 1-47.

Burkadze, K. (2018). A Shift in NATO's Article 5 in the Cyber Era? Fletcher Forum of Worl Affairs, s. 215-226.

Buzan, B. (1990). The European Security Order Recast: Scenarios for the Post-Cold War Era.

Buzan, B. (1997). Security: A New Framework for Analysis. UK: Lynne Rienner Publishers.

Canteaut, A. (2011). Encyclopedia of Cryptography and Security. Springer.

Cavelty, M. D. (2008). Cyber-Security and Threat Politics: US efforts to secure the information age. New York: Routledge.

Common Criteria. (2020). 07 17, 2020 tarihinde https://www.wikiwand.com/en/Common_Criteria adresinden alındı

Corona virüsü: Son yılların en büyük sağlık krizine karşı Türkiye ne yaptı? (2020, Mart 14). Sözcü: https://www.sozcu.com.tr/2020/gundem/son-dakika-

corona-virusu-son-yillarin-en-buyuk-saglik-krizine-karsi-turkiye-ne-yapti-5679069/ adresinden alındı

Cuthbertson, A. (2020, Aralık 18). Solarwınds Hack: How Sunburst Hackers Infıltrated Hıghest Levels Of Us Government. Independent: https://www.independent.co.uk/life-style/gadgets-and-tech/solarwinds-hack-how-russia-us-government-b1776034.html adresinden alındı

Cyber Threats. (20121). CIS: https://www.cisecurity.org/spotlight/cybersecurity-spotlight-cyber-threat-actors/#:~:text=A%20Cyber%20Threat%20Actor%20(CTA,devices%2C%20systems%2C%20or%20networks. adresinden alındı

Çapar, S., & Koca, M. (2017). Güvenlik ve Kriz Yönetimi. İdarecinin Sesi dergisi(179).

Dağar, O. (2019). Kriz Yönetiminde İstihbarat Birimlerinin Fonksiyonları ile Güvenlik Politikalar (Yayımlanmamış Yüksek Lisans Tezi). Konya: Selçuk Üniversitesi İBBF Siyaset ve Kamu Yönetimi Anabilimdalı.

Dan Craigen, N. D. (2014). Defining Cybersecurity. Technology Innovation Management Review, 13-21.

Darıcılı, A. B. (2017). Amerika Birleşik Devletleri Ve Rusya Federasyonu'nun Siber Güvenlik Politikalarının Karşılıklı Analizi (Yayımlanmamış Doktora Tezi). Bursa: Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Anabilimdalı.

Demir, T. (2019). Güvenlik Kavramı İle Kriz Yönetimi Arasındaki Epistemolojik İlişki ve Türkiye. Turkish Studies - Economics, Finance, Politics, 14(1), 31-43.

Devlet Bilgisayarlarını Siber Ordu Koruyor. (2009, Eylül 1). Hürriyet.

Digital 2020: Turkey. (2020). https://datareportal.com/reports/digital-2020-turkey?rq=turkey adresinden alındı

Digital Attack Map. (2020, 12 21). https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18617&view=map adresinden alındı

Doğan, Z. (2019). Güvenlikleştirme süreçlerinde medyanın rolü: 28 şubat örneği (Yayımlanmamış Doktora Tezi). ankara: Polis Akademisi Güvenlik Bilimleri Enstitüsü Uluslararası Güvenlik Anabilim Dalı.

Dunton, J. (2020, Eylül 7). UK's 'next cyber crisis' likely to come from mistake or misfortune. Public Technology: https://www.publictechnology.net/articles/news/uk%E2%80%99s-

%E2%80%98next-cyber-crisis%E2%80%99-likely-come-mistake-or-misfortune-%E2%80%93-outgoing-ncsc-head adresinden alındı

EBA'dan canlı derslere katılabilmek için her gün bir kilometre yürüyor. (2020, Mayıs 19). Anadolu Ajansı Resmi İnternet Sitesi: https://www.aa.com.tr/tr/yasam/ebadan-canli-derslere-katilabilmek-icin-her-gun-bir-kilometre-yuruyor/1845996 adresinden alındı

Evan, T., Leverett, E., Ruffle, S. J., Coburn, A. W., Bourdeau, J., Gunaratna, R., & Ralph, D. (2017). Cyber Terrorısm:Assessment of the Threat to Insurance. University of Cambridge.

Garayev, V. (2013). Crisis Defination. B. Penuel içinde, Encyclopedia of crisis management. SAGE.

Garcia, S. M. (2014). Reflections on Virtual to Real: Modern Technique, International Security Studies and Cyber Security Environment. J. F. Kremer içinde, Cyberspace and International Relations (s. 1076). London: Springer.

Gartner Forecasts Worldwide Security. (2021) GARTNER.

Gibson, W. (1984). Neuromancer. New York: Ace Books.

Girişimlerde Bilişim Teknolojileri Kullanım Araştırması,. (2020) TUIK.

Golandsky, Y. (2016). Cyber Crisis Management, Survival or Extinction. Las Vegas: Information Institute Conferences.

Golandsky, Y. (2016). Cyber Crisis Management, Survival or Extinction? 2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment.

Goldman, E. (2018). Why Digital Pearl Harbour Makes Sense. G. Perkovich içinde, Understanding Cyber Conflict: Fourteen Analogies (s. 128). GeorgetownUniversityPress.

Göçoğlu, V. (2018). Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi Yayımlanmamış Doktora Tezi). Ankara: Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilimdalı.

Güngör, M. (2015). Ulusal Bilgi Güvenliği: Strateji Ve Kurumsal Yapılanma. Ankara: T.C. Kalkınma Bakanlığı.

Güngör, U., & güney, O. (2017). Uluslararası İlişkilerde Güvenliğin Dönüşümü Çerçevesinde Bilgi Güvenliği Ve Siber Savaş. Journal of Black Sea Studies, 131-146.

Güntay, V. (2016). Uluslararası ilişkiler temelinde siber güvenlik: Mikro siber ittifak teorisi (Micro-CAT) / International relations and cyber security: Micro cyber alliance theory. Karadeniz Teknik Üniversitesi (Yayımlanmamış Doktora Tezi).

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 1155-1175.

Hekim, H., & Başıbüyük, O. (2013). Siber Suçlar Ve Türkiye'Nin Siber Güvenlik Politikaları. Uluslararası Güvenlik ve Terörizm Dergisi, 135-158.

Hisarlıoğlu, F. (2019). Güvenlikleştirme. Uluslarası İlişkiler Konseyi. https://trguvenlikportali.com/wp-content/uploads/2019/11/Guvenliklestirme_FulyaHisarl%C4%B1oglu_v.1.pdf adresinden alındı

Hoffman, D. (2004, 27 Feburary). Reagan Approved Plan to Sabotage Soviets. The Washington Post.

Huysmans, J. (2006). The Politics of Insecurity. New York: Routledge.

ITU. (2019). Measuring digital development: Fact and Figures. ITU.

İletişim Başkanlığı'na yeni görev. (2020, Eylül 18). T.C. Cumhurbaşkanlığı İletişim Başkanlığı Resmi İnternet Sitesi: https://www.iletisim.gov.tr/turkce/haberler/detay/iletisim-baskanligina-yeni-gorev#:~:text=Ulusal%20ve%20uluslararas%C4%B1%20alanda%20stratejik,y%C3%B6netimi%20a%C3%A7%C4%B1s%C4%B1ndan%20gerekli%20tedbirleri%20uygulamak. adresinden alındı

İnternetin Karanlık Yüzü. (1997, Kasım 30). Milliyet.

Kamu Kurum ve Kuruluşlarının KamuNet'e Dahil Edilmesi. (2016). Başbakanlık.

Karaağaç, t. (2013). Kriz Yönetimi ve İletişim. İ.Ü. Siyasal Bilgiler Fakültesi Dergisi(49), 117-132.

Köksoy, F. (2020). Avrupa Birliği'nin Siber Güvenlik Politikası:Kurumsalcılık mı Tutarlılık mı ? Güvenlik Stratejileri Dergisi, 635-674.

Kurnaz, İ. (2016). 21. Yüzyılda Ortodoks Güvenlik Paradigmasının Aşınımı: Uluslararası İlişkilerde Siber Güvenlik. Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Anabilimdalı.

Küçükaydın, D. (2016). National And International Cybersecurity Strategies Of The United States: A Securitizatıon Attempt (Yayımlanmamış Yüksek

Lisans Tezi. Ankara: Orta Doğu Teknik Üniversitesi Uluslararası İlişkiler Anabilimdalı.

Küpeli, H. (2019). Güvenlikleştirme teorisi bağlamında kritik altyapıların terörist saldırılardan korunmasının Abd ve Ab güvenlik politikalarındaki rolü. Ankara: Polis Akademisi.

Lewis, J. (2006). Cybersecurity and Critical Infrastructure Protection. Washington, DC: Center for Strategic and International Studies.

Lin, H. (2012). Cyber conflict and international humanitarian law. International Rewiev of Red Cross, 515-531.

Lin, H. (2018). The Strategic Dimensions of. Washington: THE BROOKINGS INSTITUTION.

Locked Shields. (2019). NATO Cooperative Cyber Defence Centre of Excellence Resmi İnternet Sitesi: https://ccdcoe.org/exercises/locked-shields/ adresinden alındı

Masood, Z., Samar, R., & Raja, M. A. (2019). Design of a mathematical model for the Stuxnet virus in a network of critical control infrastructure. Computers & Security, 1-15.

Massive WannaCry/Wcry Ransomware Attack Hits Countries. (2017, Mayıs 7). Trendmicro: https://www.trendmicro.com/en_us/research/17/e/massive-wannacrywcry-ransomware-attack-hits-various-countries.html adresinden alındı

Mee, P. (2018). How a Cyber Attack Could Cause the Next Financial Crisis. Oliver Wyman.

Mehrotra, K. (2020, Kasım 2). U.S. Fires Up ‘All Government’ War on Cyber Election Threats. Bloomberg: https://www.bloomberg.com/news/articles/2020-11-02/u-s-fires-up-all-government-war-on-election-cyber-threats adresinden alındı

Miş, N. (2012). Güvenlikleştirme teorisi ve Türkiye'de güvenlikleştirme siyaseti: 1923-2003 (Yayımlanmamış Doktora Tezi). Sakarya: Sakarya Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı.

Miş, N. (2014). Güvenlikleştirme Teorisi ve Siyasal Olanın Güvenlikleştirilmesi. Akademik İncelemeler Dergisi, 345-381.

NATO. (2014). Wales Summit Declaration. NATO.

NATO team takes part in one of the world’s most challenging cyber exercises. (2019, Nisan 9). NATO Resmi İnternet Sitesi:

https://www.nato.int/cps/en/natohq/news_165640.htm?selectedLocale=en adresinden alındı

Neuman, L. (2006). Toplumsal Araştırma Yöntemleri (Cilt 2). (S. Özge, Çev.) İstanbul: Yayın Odası.

NIST Cybersecurity Framework. (2018). NIST.

Overview of Cybersecurity. (2009). International Telecommunication Union.

Oxford Online Dictionary. (2014). Oxford University Press.

Önder, Ş. (2018). Iso 27001 Standardı Kapsamında Kurumsal Bilgi Güvenliği ve İşletme Performansı Arasındaki İlişki. Ekonomik ve Sosyal Araştırmalar Dergisi, 89-100.

Özbek, V. Ö. (2001). İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları. Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 107-157.

Özbilen, T. ve A. Çağlar, (2020). Türk Kamu Sektöründe Bilgi ve Bilişim Güvenliği. *Kamu Yönetimi ve Teknoloji Dergisi*, 2020, 72-93.

Özocak, T. (2019). AB ve Kriz Yönetimi: Kosova Örneği (Yayımlanmamış Yüksek Lisans Tezi). İzmir: Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü AB Anabilimdalı.

Öztürk, İ. D. (2017). Stratejik Halkla İlişkiler Kapsamında Kriz Yönetimi: Türkiye'de Krizlerin Algılanması Üzerine Bir Araştırma (Yayımlanmamış Doktora Tezi). İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Halkla İlişkiler Anabilimdalı.

Pazarcı, H. (2013). Uluslararası Hukuk. Ankara: Turhan Kitapevi.

Pentagon kept the lid on cyberwar in Kosovo. (1999, Kasım 9). The Guardian Resmi İnternet Sitesi: https://www.theguardian.com/world/1999/nov/09/balkans adresinden alındı

Privacy Act of 1974. (tarih yok). ABD. https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf adresinden alındı

Puyvelde, D. v. (2020). Cybersecurity: Politics, Governance and Conflict in Cyberspace. Polity.

Roadmap to Digital Cooperation. (2020). UN.

Rosanvallon, P. (2003). Refah Devletinin Krizi. Ankara: Dost Kitabevi.

Sağıroğlu, Ş. (2019). Siber Güvenlik ve Savunma:Standartlar ve Uygulamalar. Ş. Sağıroğlu (Dü.) içinde, Siber Güvenlik ve Savunma:Standartlar ve Uygulamalar (s. 54). Grafiker Yayınları.

Satter, R. (2020, Aralık 14). IT company SolarWinds says it may have been hit in 'highly sophisticated' hack. Reuters Resmi Web Sitesi: https://www.reuters.com/article/us-usa-solarwinds-cyber-idUSKBN28N0Y7 adresinden alındı

Schmitt, C. (2014). Siyasal Kavramı. Metis Yayıncılık.

Sevestapolo, D. (2018, Eylül 18). US accuses North Korea over global cyber crime wave. Aralık 14, 2020 tarihinde Financial Times Resmi İnternet Sitesi: https://www.ft.com/content/91453da8-b1de-11e8-99ca-68cf89602132 adresinden alındı

Siber Bebek Bakıcısı. (1999, Mayıs 15). Milliyet.

Siber Güvenlik Kurulu Toplantısı gerçekleştirildi. (2016). Ulaştırma ve Altyapı Bakanlığı Resmi İnternet Sitesi: https://www.uab.gov.tr/haberler/siber-guvenlik-kurulu-toplantisi-gerceklestirildi adresinden alındı

Siber Güvenlik Tatbikatları. (2017, Aralık 15). BTK Resmi İnternet Sitesi: https://www.btk.gov.tr/siber-guvenlik-tatbikatlari adresinden alındı

Siber Güvenlik Tatbikatları. (2017). BTK Resmi İnternet Sitesi: https://www.btk.gov.tr/siber-guvenlik-tatbikatlari adresinden alındı

Son dakika haberi: Yasaklar tek tek kalkıyor! İşte kritik tarih... (2020, Mayıs 29). Milliyet: https://www.milliyet.com.tr/galeri/son-dakika-haberi-yasaklar-tek-tek-kalkiyor-iste-kritik-tarih-6221805/1 adresinden alındı

Souppaya, M. (2013). Guide to Malware Incident Response. NIST.

Soy, S. (2018). Kriz Yönetiminde Karizmatik Liderliğin Önemi: Recep Tayyip Erdoğan Örnekliğinde Teorik Ve Uygulamalı Bir Çalışma (Yayımlanmamış Yüksek Lisans Tezi). Kayseri: Erciyes Üniversitetesi Sosyal Bilimler Enstitüsü Halkla İlişkiler Anabilimdalı.

Sönmez, G. (2017, Ocak-Şubat). Siber Alanda Yükselen Terör Tehdidi ve Siber Güvenlik.

Su, J. (2019). Hackers Stole Over $4 Billion From Crypto Crimes In 2019 So Far, Up From $1.7 Billion In All Of 2018. Forbes Resmi İnternet Sitesi: https://www.forbes.com/sites/jeanbaptiste/2019/08/15/hackers-stole-

over-4-billion-from-crypto-crimes-in-2019-so-far-up-from-1-7-billion-in-all-of-2018/?sh=5e5651ed55f5 adresinden alındı

Swift, S. (2009). Hannah Arendt. New York: Routledge.

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Resmi İnternet Sitesi. (2020, Aralık 13). https://cbddo.gov.tr/hizmet-birimlerimiz/siber-guvenlik-dairesi-baskanligi/ adresinden alındı

Threat Landscape:Phising. (2020). ENISA.

Trimintzios, P., Holfeldt, R., Uckan, B., & Gavrila, R. (2014). Report on Cyber Crisis Cooperation and Management. European Union Agency for Network and Information Security.

Trump 'Twitter kararnamesini' imzaladı, ABD'de sosyal medya şirketleri daha sıkı denetlenecek. (2020, Mayıs 29). BBC Resmi İnternet Sitesi: https://www.bbc.com/turkce/haberler-dunya-52844303 adresinden alındı

Trusted Computer System Evaluation Criteria. (2020). 07 12, 2020 tarihinde https://www.wikiwand.com/en/Trusted_Computer_System_Evaluation_Criteria adresinden alındı

TUBİTAK BİLGEM. (2020, Aralık 15). https://sge.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce adresinden alındı

TUIK. (2020). Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması. TUIK.

Turan, M. (2017). Bilişim Hukuku. Ankara: Seçkin Yayıncılık.

Türkiye 2008 Yılı BOME Faaliyetleri Raporu. (2008). Ulusal Elektronik Ve Kriptoloji Araştırma Enstitüsü.

Türkiye Siber Gvüenlik Kümelenmesi Resmi İnternet Sitesi. (2021, Mayıs 25). Türkiye Siber Gvüenlik Kümelenmesi Resmi İnternet Sitesi: https://www.siberkume.org.tr/Index adresinden alındı

Türkiye'de alınan ilk koronavirüs önlemleri. (2020, mart 12). Deutsche Welle: https://www.dw.com/tr/t%C3%BCrkiyede-al%C4%B1nan-ilk-koronavir%C3%BCs-%C3%B6nlemleri/a-52736132 adresinden alındı

US cyber-attack: US energy department confirms it was hit by Sunburst hack. (2020, Aralık 18). BBC Resmi İnternet Sitesi: https://www.bbc.com/news/world-us-canada-55358332 adresinden alındı

USOM ve Kurumsal Siber Olaylara Müdahale Ekibi. (2020, Aralık 15). BTK Resmi İnternet Sitesi: https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi adresinden alındı

Uysal, H. (2018). İnsani Müdahale Harekâtlarında Çatışma ve Kriz Yönetimi: Sivil-Asker İşbirliği Tartışmaları (Yayımlanmamış Doktora Tezi) . İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Anabilimdalı.

Ünal, A. Y. (2020, Şubat 16). Türkiye'nin siber kalesinde' anlık 16 milyon IP taranıyor. Anadolu Ajansı Resmi Sitesi: https://www.aa.com.tr/tr/bilim-teknoloji/turkiyenin-siber-kalesinde-anlik-16-milyon-ip-taraniyor/1735490 adresinden alındı

Wiener, N. (1950). The Human Use of Human Beings. London: Eyre & Spottiswoode.

Williams, C. (2016). Cyber Crisis. Trustee, 1-11.

Yıldız, MEte (2020). "Yeni Teknoloji ve İş Yapış Biçimlerinin Kamu Politikalarına Etkileri: Genel Bir Çerçeve", MEte Yıldız ve Cenay Babaoğlu(der.) Teknoloji ve Kamu Politikaları: Yeni Teknoloji ve İş Yapma Biçimlerinin Kamu Yönetimi ve Politikalarına Etkisi. Ankara: Gazi Kitapevi, s4

Yılmaz, M.E, (2008)The New World Order": An Outline of the Post-Cold War Era. (2008). Alternatives: Turkish Journal of International Relations, 7(4), 44-59.

Yegen, C. (2014). Dijital Aktivizmin Bir Türü Olarak Hacktivizm Ve "Redhack". E-journal of Intermedia, 118-132.

Zaheer Masood, R. S. (2019). Design of a mathematical model for the Stuxnet virus in a network of critical control infrastructure. Computers & Security.

Zhan, X. A., & Borden, J. (2019). How to communicate cyber-risk? An examination of behavioral recommendations in cybersecurity crisis. Journal of Risk Research, 23(10), 1336-1352.

Wikipedia: (2020, Haziran 2). https://tr.wikipedia.org/wiki/Tehdit adresinden alındı

The Open Web Application Security Project: (2020, Aralık 15). https://owasp.org/ adresinden alındı

2025 Cyberspace. UNESCO. Mayıs 20, 2021 tarihinde http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/Events/netconference_march2015_submissions/C/reference_from_microsoft_cyberspace2025.pdf adresinden alındı

Resmi Kurum Belgeleri

2014-2023 Teknolojik Afetler Yol Haritası Belgesi. (2014). AFAD.

Kişisel Verilerin Korunması Kanunu. (2016, Mart 24).

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı. (2016). Ulaştırma ve Haberleşme Bakanlığı.

Kamunet Ağına Bağlanma Ve Kamunet Ağının Denetimine İlişkin Usul Ve Esaslar Hakkında Tebliğ. (2017, Haziran 27)T.C. Ulaştırma Bakanlığı.

Millî Güvenlik Kurulu Genel Sekreterliğinin Teşkilat Ve Görevleri Hakkında Cumhurbaşkanlığı Kararnamesi. (2018). Resmi Gazete-30479

T.C. MSB Resmi Web Sitesi: (2020, 11) 11https://www.msb.gov.tr/Bakanlik/Misyon adresinden alındı

T.C. İçişleri Bakanlı Resmi Web Sitesi: (2020, 11 11). https://www.icisleri.gov.tr/hakkimizda adresinden alındı

T.C. Ulaştırma Bakanlığı Resmi Web Sitesi: (2020, 11 11). https://www.uab.gov.tr/kurumsal adresinden alındı

32 Numaralı Cumhurbaşkanlığı Kararnamesi. (2019).

Ulaştırma ve Haberleşme Hizmetlerinin Olağanüstü Hallerde ve Savaşta Ne Suretle Yürütüleceğine Dair Kanun. (tarih yok).

Türkiye Ulusal Enformasyon Ulusal Altyapı Anaplanı. (1999). TUBİTAK.

T.C. Dışişleri Bakanlığı 2019-2023 Dönemi Stratejik Planı. T.C. Dışişleri Bakanlığı. (2019).

Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ. (2013, Kasım 11). Ulaştırma, Denizcilik ve Haberleşme Bakanlığı.

Sektörel SOME Kurulum ve Yönetim Rehberi. T.C. Ulaştırma ve Altyapı Bakanlığı. (2014).

Kurumsal SOME Kurulum ve Yönetim Rehberi. T.C. Ulaştırma ve Altyapı Bakanlığı. 2014).

Kritik Altyapı Bilgi Sistemleri için Asgari Güvenlik Önlemleri Dokümanı. T.C. Ulaştırma ve Altyapı Bakanlığı. (2015).

Ankara: İç İşleri Bakanlığı. (20 GAMER El Kitabı. (2018).

EGM. (2000). Kaçakçılık ve Organize Suçlar Daire Başkanlığ 2000 Raporu. EGM.

ENISA Data Breach Report. ENISA. (2020).

Bilgi ve İletişim Güvenliği Rehberi. T.C. Dijital Dönüşüm Ofisi. (2020).

Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Genelgesi. (2019).

e-Türkiye Girişimi I. Ara Rapor. T.C. Başbakanlık.14). Kritik Altyapıların Korunması Yol Haritası Belgesi. AFAD. (2002).

Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı. (2012).

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023). Ulaştırma ve Altyapı Bakanlığı. (2020).

EKLER:

Ek-1: Araştırmada Kullanılan Resmi Dokümanlar

Resmi Dokümanlar			
S. No	**Belge Adı**	**Türü**	**Çıkaran Makam**
1	"Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar"	Bakanlar Kurulu Kararı	Bakanlar Kurulu
2	"Ulaştırma ve Haberleşme Hizmetlerinin Olağanüstü Hallerde ve Savaşta Ne Suretle Yürütüleceğine Dair Kanun"	Kanun	TBMM
3	"Evrensel Hizmet Kanunu"	Kanun	TBMM
4	"İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"	Kanun	TBMM
5	"Elektronik Haberleşme Kanunu"	Kanun	TBMM
6	"Elektronik Ticaretin Düzenlenmesi Hakkında Kanun"	Kanun	TBMM
7	"Fikir ve Sanat Eserleri Kanunu"	Kanun	TBMM
8	"Elektronik İmza Kanunu"	Kanun	TBMM
9	"Kişisel Verilerin Korunması Kanunu"	Kanun	TBMM
10	"Türk Ceza Kanunu"	Kanun	TBMM

11	“Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği”	Yönetmelik	T.C. Ulaştırma Bakanlığı
12	“Evrensel Hizmet Gelirlerinin Tahsili ve giderlerin Yapılmasına İlişkin Usul ve esaslar Hakkında Yönetmelik”	Yönetmelik	T.C. Ulaştırma Bakanlığı
13	“İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik”	Yönetmelik	T.C. Ulaştırma Bakanlığı
14	“Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı”	Strateji Planı	T.C. Ulaştırma Bakanlığı
15	“2016-2019 Ulusal Siber Güvenlik Stratejisi”	Strateji Planı	T.C. Ulaştırma Bakanlığı
16	“T.C. Ulaştırma Bakanlığı Bilgi Teknolojileri Kurumu 2019-2023 Stratejik Planı”	Strateji Planı	T.C. Ulaştırma Bakanlığı Bilgi Teknolojileri Kurumu
17	“Bilgi Teknolojileri ve İletişim Kurumu 2016-2018 Dönemi Stratejik Planı”	Strateji Planı	T.C. Ulaştırma Bakanlığı Bilgi Teknolojileri Kurumu
18	“KAMUNET Ağına Bağlanma ve KAMUNET Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ”	Tebliğ	T.C. Ulaştırma Bakanlığı
19	“Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve	Tebliğ	T.C. Ulaştırma Bakanlığı

	Çalışmalarına Dair Usul Ve Esaslar Hakkında Tebliğ”		
20	“Bilgi Varlıklarının Derecelendirilmesi Kılavuzu”	Rehber/Kılavuz	T.C. Ulaştırma Bakanlığı Bilgi Teknolojileri Kurumu
21	“Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı”	Rehber/Kılavuz	T.C. Ulaştırma Bakanlığı
22	“Kurumlar İçin Siber Güvenlik Önlemlerini Ölçme Testi Dokümanı”	Rehber/Kılavuz	T.C. Ulaştırma Bakanlığı
23	“Kurumsal SOME Kurulum ve Yönetim Rehberi”	Rehber/Kılavuz	T.C. Ulaştırma Bakanlığı Haberleşme Genel Müdürlüğü
24	“Sektörel SOME Kurulum ve Yönetim Rehberi”	Rehber/Kılavuz	T.C. Ulaştırma Bakanlığı Haberleşme Genel Müdürlüğü
25	“Bilgi ve İletişim Güvenliği Rehberi”	Rehber/Kılavuz	T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
26	“Kamu Kurum ve Kuruluşlarının KAMUNET’e dâhil edilmesi”	Genelge	T.C. Başbakanlık
27	“Siber Güvenlik Genelgesi”	Genelge	T.C. Cumhurbaşkanlığı

28	“Developments in the field of information and telecommunications in the context of international security-2012”	BM Rapor	BM
29	“Developments in the field of information and telecommunications in the context of international security-2017”	BM Rapor	BM
30	“Developments in the field of information and telecommunications in the context of international security-2019”	BM Rapor	BM
31	“Developments in the field of information and telecommunications in the context of international security-2013”	BM Rapor	BM
32	“National Views And Assessments Of Turkey-2017”	BM Rapor	BM
33	“National Views and Assessments Of Turkey on Developments In The Field Of Information and Telecommunıcatıons In The Context of International Security and On The Reports of The Un Group of Governmental Experts” 10.05.2019	BM Rapor	BM
34	“İletişim Başkanlığı ‘na yeni görev”	Resmi İnternet Sayfası	T.C. Cumhurbaşkanlığı İletişim D.Bşk.lığı

35	“32 Numaralı Cumhurbaşkanlığı Kararnamesi” (GAMER Kuruluşu)	Genelge	T.C. Cumhurbaşkanlığı
36	GAMER Genelgesi	Genelge	T.C. İç İşleri Bakanlığı
37	GAMER Yönergesi	Yönerge	T.C. İç İşleri Bakanlığı

Ek-2: Siber Güvenlik Kavramsal Kategorileri ve Tanımları (Dan Craigen, 2014)

Kategori	Tanım
Varlık	Genel olarak, "faydalı veya değerli bir şey veya kişi" olarak tanımlanır. Burada tanımı, "siber uzay ve siber uzayın etkin olduğu sistemlere" gönderme yapacak şekilde indirgiyoruz.
Kapasite	Kaynakların, süreçlerin ve yapıların organizasyonu ve birleşimi
Yanlış Konumlandırma	Konumlandırma, "(kavramları) doğru veya uygun göreceli konumlara yerleştirmek" olarak tanımlanır; dolayısıyla yanlış konumlandırma, yanlış veya uygun olmayan konumlara neden olur.
Oluşum	Bir kaza ya da olay.
Organizasyon	Kurumlar.
Proses	Bir eylem veya eylemler dizisi olarak devam etme veya devam etme olgusu; ilerleme, süreç.
Mülkiyet hakkı	Belirli alanlarda belirli eylemleri üstlenmek için uygulanabilir bir otorite. Erişim, geri çekme, yönetim, hariç tutma ve devretme haklarını içerir.
Koruma	Zarar görmekten koruma.

Siber Güvenlik Tanımları ve Kavramsal Kategorilerdeki Karşılığının Analizi

Siber Güvenlik Tanımları	Analiz (Anahtar Terimler → Önerilen Tanımdaki İlgili Terimler)
Elektronik verilerin yasadışı veya yetkisiz kullanımına karşı korunma durumu veya bunu başarmak için alınan önlemler. (Oxford Online Dictionary, 2014)	"Korunma" → KORUMA “Yasadışı veya yetkisiz kullanım” → YANLIŞ KONUMLANDIRMA

	“Elektronik veriler” → VARLIKLAR ve MÜLKİYET HAKLARI “Alınan önlemler ...” → KAPASİTE
"Bilgi ve iletişim sistemlerinde yer alan bilgilerin hasar, yetkisiz kullanım veya değiştirme veya istismara karşı korunduğu ve / veya bunlara karşı savunulduğu faaliyet veya süreç, yetenek veya kabiliyet veya durum." (A Glossary of Common Cybersecurity Terminology, 2014)	"Etkinlik veya süreç, yetenek veya yetenek veya durum" → KAPASİTE "Bilgi ve iletişim sistemleri ve burada bulunan bilgiler" → VARLIKLAR ve MÜLKİYET HAKLARI "Korunan ve / veya savunulan" → KORUMA "Hasar, yetkisiz kullanım veya değiştirme veya istismar" →YANLIŞ KONUMLANDIRMA
Siber güvenlik, yazılımlara, bilgisayarlara ve ağlara kötü amaçlı saldırı riskini azaltmayı içerir. Bu, izinsiz girişleri tespit etmek, virüsleri durdurmak, kötü niyetli erişimi engellemek, kimlik doğrulamasını zorunlu kılmak, şifreli iletişimi etkinleştirmek ve devam etmek için kullanılan araçları içerir. (Lewis, 2006)	"Riski azaltmayı içerir" → YETENEK "Kötü niyetli saldırı" → OLUŞUM “Yazılım, bilgisayarlar ve ağlar” → VARLIKLAR ve MÜLKİYET HAKLARI "İzinsiz girişleri tespit etmek, virüsleri durdurmak, kötü niyetli erişimi engellemek, kimlik doğrulamasını zorunlu kılmak, şifrelenmiş iletişimi etkinleştirmek ve devam ettirmek için kullanılan araçları içerir" → KAPASİTE
Siber güvenlik, siber ortamı, organizasyonu ve kullanıcı varlıklarını korumak için	"Araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitim, en iyi

kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitim, en iyi uygulamalar, güvence ve teknolojilerin toplamıdır. (Overview of Cybersecurity, 2009)	uygulamalar, güvence ve teknolojilerin toplamı" → KAPASİTE "Korumak için" → KORUMA “Siber ortam ve organizasyon ve kullanıcının varlıkları” → VARLIKLAR ve MÜLKİYET HAKLARI

Ek-3: Siber Güvenlik Tanımları

Kaynak: (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023), 2020)

"Çok paydaşlı ve disiplinler arası bir konu olan siber güvenliğin sağlanmasında anahtar noktalardan bir tanesi, ortak dilin konuşulmasıdır. Siber güvenlik alanında
ortak tanımlamaların yapılması, paydaşlar arası iletişimin gelişmesine katkı sağlamaktadır. Bu doğrultuda, Strateji ve Eylem Planı kapsamındaki tanımlar aşağıda yer almaktadır:"

Adli Bilişim: "Bilişim suçları davalarında, olay kapsamında suça konu olan dijital delillerin zarar görmeyecek şekilde toplanması, değerlendirilmesi, belgelendirilmesi, sınıflandırılması ve bu verilerin yargı sürecinde kullanılabilmesini
kapsayan bilim dalı."

Balküpü: "Siber saldırıları gerçek sistem sunucularına benzer mimarideki tuzak sistemlere yönlendirerek tehdit ve saldırıları tespit etmek için kullanılan donanım ve yazılım altyapısı bütünü."

BGYS (Bilgi Güvenliği Yönetim Sistemi): "Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak üzere sistemli, kuralları koyulmuş, planlı, yönetilebilir, sürdürülebilir, dokümante edilmiş, kurumun/kuruluşun yönetimince kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütünü."

Bilgi Güvenliği: "Bilişim sistemlerinin ve bilgilerin izinsiz kullanımını, yetkisiz kişilerce erişilmesini ve ifşa edilmesini, silinmesini, değiştirilmesini ve zarar görmesini, engellemek, bu sistem ve bilgilere yetkili kişiler ve işlemlerin ihtiyaç duyulan zamanda ve kalitede erişebilmesini sağlamak için yürütülen faaliyetler bütünü."

Bilgi Varlığı: "Kişi veya organizasyon için kıymetli olan veriler ile bu verilerin taşındığı, saklandığı, aktarıldığı veya işlendiği sistemler, yazılımlar, BT donanımları
ve iş süreçleri."

Bütünlük: "Bilginin/verinin doğruluğunu ve tamlığını koruma özelliği.
EKS (Endüstriyel Kontrol Sistemi): Geleneksel bilişim teknolojileri dışında, programlanabilir mantıksal denetleyiciler aracılığı ile üretim, ürün işleme ve dağıtım kontrolleri gibi endüstriyel işlemler için kullanılan, SCADA (Supervisory Control and Data Acquisition) ve Dağınık Kontrol Sistemleri şeklinde gruplanan bilgi sistemleri."
Erişilebilirlik: "Bilginin/verinin yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliği."
Gizlilik: "Bilginin/verinin yetkisiz kişiler, varlıklar ya da süreçler tarafından erişilememesi, kullanılamaması, depolanmaması, başka bir ortama kaydedilmemesi veya ifşa edilmemesi özelliği."
İDN (İnternet Değişim Noktası): "İnternet trafiğinin değişimine imkân veren en az iki bağımsız otonom sistemin birbirine bağlanmasını sağlayan ağ altyapısı."
İleri Düzey Kalıcı Tehdit (APT): "İleri seviyeli bilgi birikimiyle ve tekniklerle geliştirilmiş ve amaçlarını gerçekleştirebilmek için çoklu vektör ataklarını kullanabilen tehdit."
KamuNet (Kamu Sanal Ağı): "Kamu kurum ve kuruluşları tarafından özel ağ ile internet ortamından yalıtılmış şekilde hizmet, işlem ve veri trafiğinin aktarılacağı, fiziksel ve siber saldırılara karşı daha güvenli kapalı devre ağ altyapısı."
Kritik Altyapı: "İşlediği bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar."
Kritik Altyapı Sektörleri: "Mülga Siber Güvenlik Kurulu'nun 20 Haziran 2013 tarihli ve 2 sayılı kararı uyarınca kritik altyapıları barındırmakta olan "Elektronik Haberleşme", "Enerji", "Finans", "Ulaştırma", "Su Yönetimi" ve "Kritik Kamu Hizmetleri" sektörleri."
Risk Yönetimi: "Kuruluşun iş süreçlerini etkileyecek risklerin belirli standart ve metodolojilere uygun olarak belirlenmesi, değerlendirilmesi, ihtiyaç duyulan kontrollerin, politika ve prosedürlerin hayata geçirilmesi ile olası kayıpların önlenmesi ya da azaltılması, izlenmesi ve gözden geçirilmesi."
SCADA: "Denetimsel Kontrol ve Veri Toplama."

SGOM: “Siber Güvenlik Operasyon Merkezi.”

Sıfırıncı Gün (Zero-Day) Zafiyeti: “Donanım, işletim sistemleri veya uygulamalarda
yeni ortaya çıkmış, henüz herhangi bir yaması veya güncellemesi geliştirilmemiş bir açıklıktan kaynaklanan ve kullanılan saldırı yöntemi ortaya çıkana kadar bilinmeyen zafiyet türü.”

Sızma Testi (Pentest): “Bilişim sistemlerinin veya ağın güvenlik önlemlerini atlatmanın yollarını belirleme, sisteme sızma ve bu şekilde öncelikli sistem zafiyetlerini ve açıklıklarını belirlemeye yönelik test.”

Siber Güvenlik: “Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin/verinin gizliliği, bütünlüğü ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber olayların tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber olay öncesi durumlarına geri döndürülmesini kapsayan faaliyetler bütünü.”

Siber Olay: “Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından
işlenen bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliğinin ihlal edilmesi.

Siber Risk: Siber tehditlerin bir veya birden çok bilgi varlığındaki açıklığı kullanarak
zarar yaratma potansiyeli. Siber olayın olumsuz sonuçlarına ilişkin olasılıklar kombinasyonu.”

Siber Saldırı: “Siber uzaydaki bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kişi ve/veya bilişim
sistemleri tarafından kasıtlı olarak yapılan işlemler.”

Siber Suç: “Bir bilişim sisteminin güvenliğini ve/veya buna bağlı verileri ve/veya kullanıcısını hedef alan ve bilişim sistemi kullanılarak işlenen suçlar.”

Siber Tehdit: “Bir kurumun veya sistemin zarar görmesi ile sonuçlanabilecek istenmeyen bir siber olayın potansiyel nedeni.”

Siber Uzay: “Doğrudan ya da dolaylı olarak internete, elektronik haberleşme ve bilgisayar ağlarına bağlı olan tüm sistem ve hizmetler.”

SOME: “Siber Olaylara Müdahale Ekibi.”

USOM: “Ulusal Siber Olaylara Müdahale Merkezi.”

Zafiyet: “Siber uzayda yer alan varlıkların herhangi bir siber tehdit tarafından kullanılabilecek zayıflıkları ifade eder.”

Ek-4: Bilgi Varlıklarının Derecelendirilmesi Kılavuzu Gizlilik Dereceleri

“Kurumlardaki bilgi varlıklarının belirlenmesi, gizlilik derecelerine göre sınıflandırılarak kurumlar arası bilgi paylaşımı esnasında bilginin gizliliğinin güvence altına alınması maksadıyla Ulaştırma ve Altyapı Bakanlığı öncülüğünde oluşturulan teknik çalışma gurubunun oluşturduğu Bilgi Varlıklarının Derecelendirilmesi Kılavuzu MSB vb. kurum ve kuruluşların kendi özel düzenlemeleri saklı kaydıyla kamu genelinde geçerli gizlilik derecelendirme resmi dokümanıdır. Bu dokümanda yer alan tanımlamalar aşağıda sunulmuştur. “

ÇOK GİZLİ: “İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda kişi güvenliği veya milli güvenlik açısından saygınlık ve çıkarlarımıza hayati derecede zararlar verebilecek, yabancı bir devlet için faydalar temin edebilecek ve güvenlik bakımından olağanüstü sonuçlar doğurabilecek bilgi için kullanılır.”

GİZLİ: “İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda, kişi güvenliği veya milli güvenlik açısından, saygınlık ve çıkarlarımıza büyük zarar verebilecek, yabancı bir devlet için faydalar temin edebilecek özellikler taşıyan bilgi için kullanılır.”

ÖZEL: “İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda, kişi güvenliği veya milli güvenlik açısından saygınlık ve menfaatlere zarar verebilecek, yabancı bir devlet için faydalar temin edebilecek bilgi için kullanılır.”

HİZMETE ÖZEL: “İçerdiği bilgi itibarıyla ÇOK GİZLİ, GİZLİ veya ÖZEL gizlilik dereceleriyle korunması gerekmeyen, ancak bilmesi gerekenler dışındaki kişiler tarafından bilinmesi durumunda gerçek ve tüzel kişilerin itibarını sarsacak bilgi için kullanılır.”

TİCARİ GİZLİ: “İzinsiz açıklanması durumunda, haksız rekabete yol açabilecek veya aynı konuda hizmet veren diğer firmalara avantaj sağlayabilecek olan bilgi için kullanılır.”

TİCARİ ÖZEL: “İçerdiği bilgi itibarıyla TİCARİ GİZLİ derecesiyle korunması gerekmeyen, ancak bilmesi gerekenler dışındaki kişiler tarafından bilinmesi istenmeyen bilgi için kullanılır.”

KİŞİYE GİZLİ: “Kişisel Verilerin Korunması Kanunu çerçevesinde özel nitelikli kişisel veri kapsamına giren bilgi için kullanılır.”

KİŞİYE ÖZEL: “İçerdiği bilgi itibarıyla KİŞİYE GİZLİ derecesiyle korunması gerekmeyen, ancak ait olduğu kişi ve bilmesi gerekenler dışındaki kişiler tarafından bilinmesi istenmeyen bilgi için kullanılır.”

TASNİF DIŞI: “Gizlilik derecesi olmayan ve özel olarak korunması gerekmeyen bilgi için kullanılır.”

Ek-5: OWASP Top 10 Listesi (The Open Web Application Security Project, 2020)

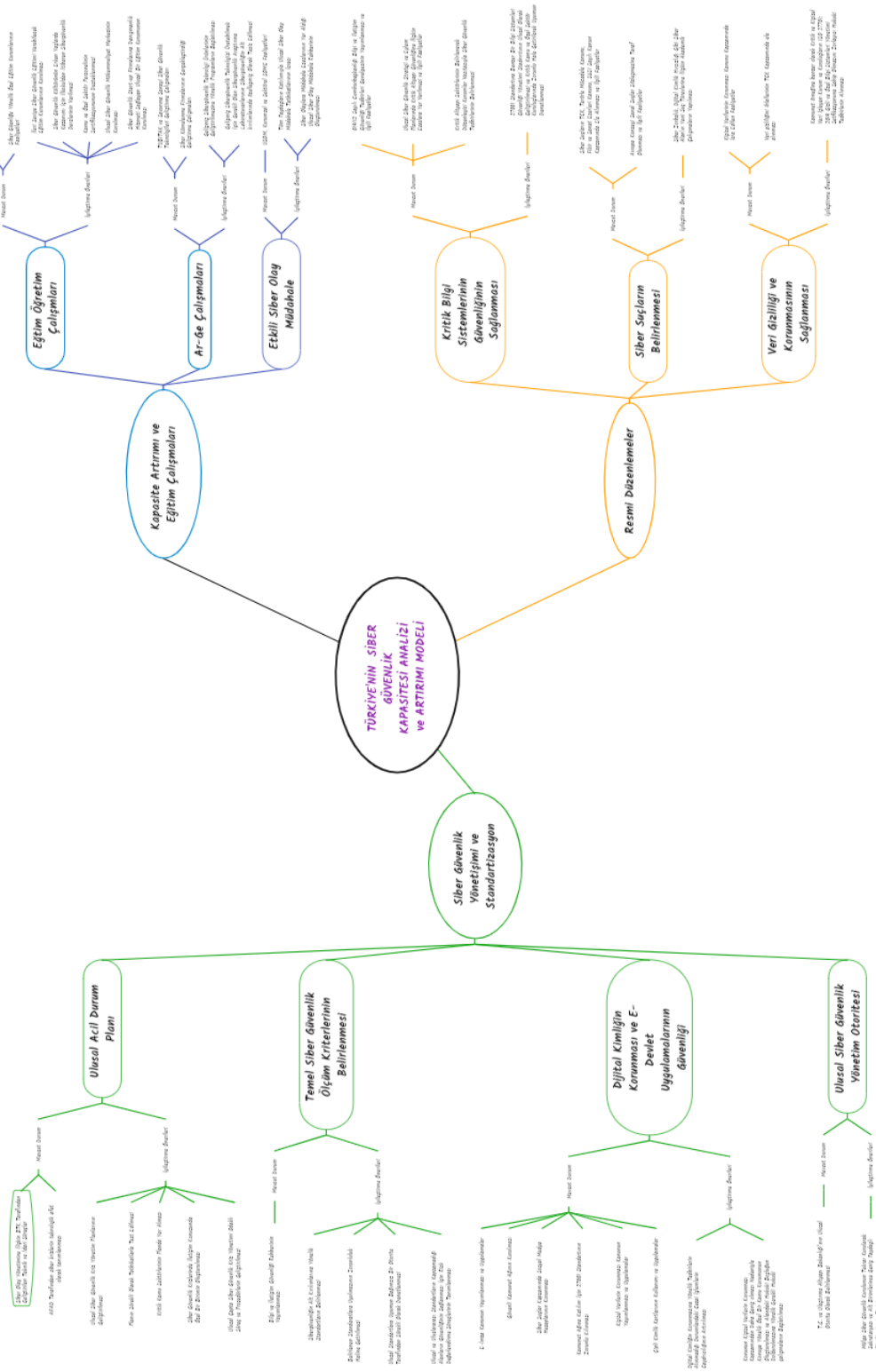
OWASP Top 10 Listesi	
Saldırı Türü	**Açıklama**
Enjeksiyon	"SQL, NoSQL, OS ve LDAP enjeksiyonu gibi enjeksiyon kusurları, güvenilmeyen veriler bir komutun veya sorgunun parçası olarak bir yorumlayıcıya gönderildiğinde ortaya çıkar."
Bozuk Kimlik Doğrulama	"Kimlik doğrulama ve oturum yönetimi ile ilgili uygulama işlevleri genellikle yanlış uygulanır ve saldırganların parolalardan, anahtarlardan veya oturum belirteçlerinden ödün vermesine veya diğer kullanıcıların kimliklerini geçici veya kalıcı olarak varsaymak için diğer uygulama hatalarından yararlanmasına olanak tanır."
Hassas Veri İfşası	"Birçok web uygulaması ve API, finansal, sağlık ve kişisel bilgi gibi hassas verileri düzgün bir şekilde korumaz. Saldırganlar, kredi kartı sahtekarlığı, kimlik hırsızlığı veya diğer suçları yürütmek için zayıf korunan bu verileri çalabilir veya değiştirebilir. Hassas veriler, beklemede veya geçişte şifreleme gibi ekstra koruma olmadan tehlikeye girebilir ve tarayıcıyla değiştirilirken özel önlemler gerektirir."
XML Harici Varlıklar	"Birçok eski veya kötü yapılandırılmış XML işlemci XML belgeleri içindeki harici varlık referanslarını değerlendirir. Harici varlıklar, dosya URI işleyicisi, dahili dosya paylaşımları, dahili bağlantı noktası taraması, uzaktan kod yürütme ve hizmet reddi saldırılarını kullanarak dahili dosyaları ifşa etmek için kullanılabilir."
Bozuk Erişim Kontrolü	"Kimliği doğrulanmış kullanıcıların ne yapmasına izin verildiğine ilişkin kısıtlamalar genellikle uygun şekilde uygulanmaz. Saldırganlar, diğer kullanıcıların hesaplarına erişme, hassas dosyaları görüntüleme, diğer kullanıcıların verilerini değiştirme, erişim haklarını değiştirme gibi yetkisiz

	işlevlere ve / veya verilere erişmek için bu kusurlardan yararlanabilir.”
Güvenlik Yanlış Yapılandırması	“Güvenlik yanlış yapılandırması en sık görülen sorundur. Bu genellikle güvenli olmayan varsayılan yapılandırmaların, eksik veya geçici yapılandırmaların, açık bulut depolama alanının, yanlış yapılandırılmış HTTP üstbilgilerinin ve hassas bilgiler içeren ayrıntılı hata iletilerinin bir sonucudur.”
Siteler Arası Komut Dosyası Oluşturma XSS	“XSS kusurları, bir uygulama doğru doğrulama veya kaçmadan yeni bir web sayfasına güvenilmeyen veriler eklediğinde veya HTML veya JavaScript oluşturabilen bir tarayıcı API'sı kullanarak mevcut bir web sayfasını kullanıcı tarafından sağlanan verilerle güncellediğinde ortaya çıkar. XSS, saldırganların kurbanın tarayıcısında kullanıcı oturumlarını ele geçirebilecek, web sitelerini tahrif edebilecek veya kullanıcıyı kötü amaçlı sitelere yönlendirebilecek komut dosyaları yürütmesine izin verir.”
Güvensiz Veri Dönüşü	“Genellikle uzaktan kod yürütülmesine neden olur, uzaktan kod yürütülmesine neden olmasa bile, tekrar saldırıları, enjeksiyon saldırıları ve ayrıcalık yükseltme saldırıları da dahil olmak üzere saldırılar gerçekleştirmek için kullanılabilir.”
Bilinen Güvenlik Açıklarına Sahip Bileşenleri Kullanma	“Kitaplıklar, çerçeveler ve diğer yazılım modülleri gibi bileşenler, uygulama ile aynı ayrıcalıklarla çalışır. Savunmasız bir bileşenden yararlanırsa, bu tür bir saldırı ciddi veri kaybını veya sunucunun ele geçirilmesini kolaylaştırabilir.”
Yetersiz Kayıt ve İzleme	“Yetersiz günlük kaydı ve izleme, olay yanıtı ile eksik veya etkisiz bir entegrasyon ile birleştiğinde, saldırganların sistemlere daha fazla saldırmasına, kalıcılığını korumasına, daha fazla sisteme dönmesine ve verileri kurcalamasına, ayıklamasına veya yok etmesine olanak tanır.”

Ek-6: Kurumsal SOME'lerin Görev ve Sorumlulukaları

- "Kurumsal SOME'ler kurumlarına doğrudan ya da dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemleri alma veya aldırma, bu tür olaylara karşı müdahale edebilecek mekanizmayı ve olay kayıt sistemlerini kurma veya kurdurma ve kurumlarının bilgi güvenliğini sağlamaya yönelik çalışmaları yapmak veya yaptırmakla yükümlüdürler."
- "Kurumsal SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik olarak, kurumlarının bilişim sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda teknik ve idari tedbirler konusunda öneri sunarlar."
- "Kurumsal SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik faaliyetlerini varsa birlikte çalıştığı sektörel SOME ile eşgüdüm içerisinde yürütürler. Durumdan gecikmeksizin USOM'u haberdar ederler."
- "Kurumsal SOME'ler bir siber olayla karşılaştıklarında, USOM ve birlikte çalıştığı sektörel SOME'ye bilgi vermek koşulu ile öncelikle söz konusu olayı kendi imkân ve kabiliyetleri ile bertaraf etmeye çalışırlar. Bunun mümkün olmaması halinde varsa birlikte çalıştığı sektörel SOME'den ve/veya USOM'dan yardım talebinde bulunabilirler."
- "Kurumsal SOME'ler siber olaya müdahale ederken suç işlendiği izlenimi veren bir durumla karşılaştıklarında gecikmeksizin durumu kanunen yetkili makamlara bildirirler. Durumu gecikmeksizin USOM'a da bildirirler."
- "Kurumsal SOME'ler kurumlarına yapılan siber olayları raporlar ve gecikmeksizin USOM ve birlikte çalıştığı sektörel SOME'ye bildirirler."
- "Kurumsal SOME'ler USOM ve/veya birlikte çalıştığı sektörel SOME tarafından iletilen siber olaylara ilişkin alarm, uyarı ve duyuruları dikkate alarak kurumlarında gerekli tedbirleri alırlar."
- "Kurumsal SOME'ler 7/24 erişilebilir olan iletişim bilgilerini belirleyerek birlikte çalıştığı sektörel SOME'lere ve USOM'a bildirirler." (Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, 2013)

Ek-7 Türkiye'nin Siber Güvenlik Kapasitesi ve Artırımı Modeli

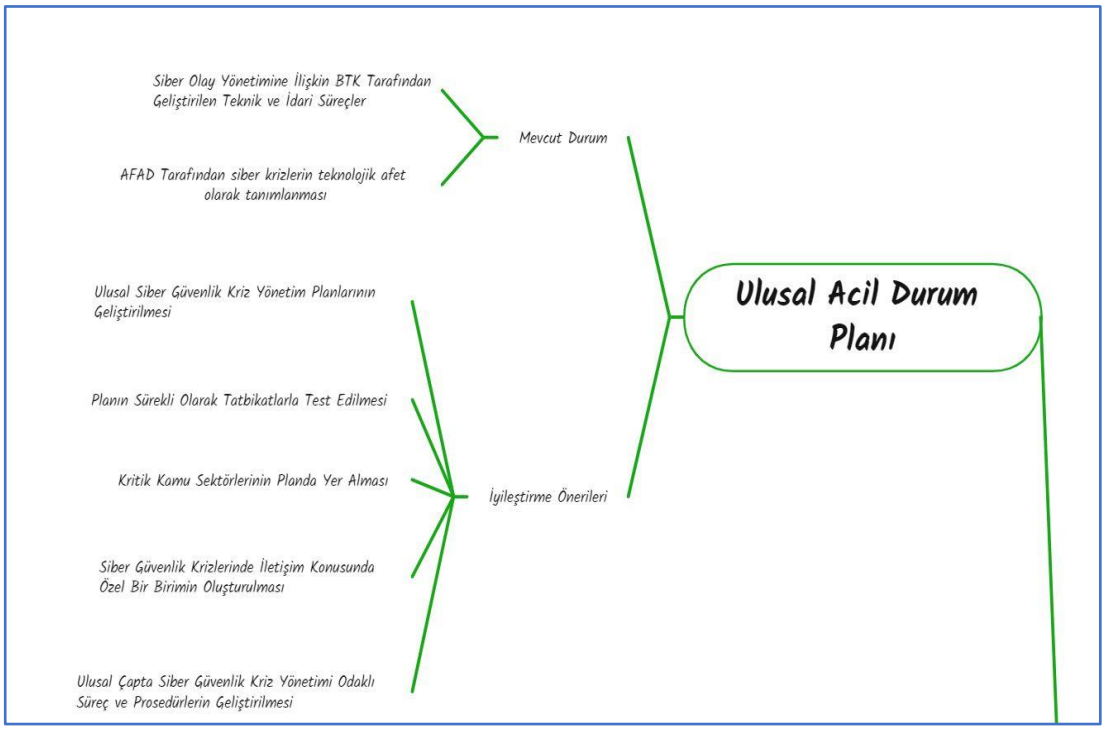


1. Siber Güvenlik Yönetişimi ve Standardizasyon

a. Ulusal Acil Durum Planı

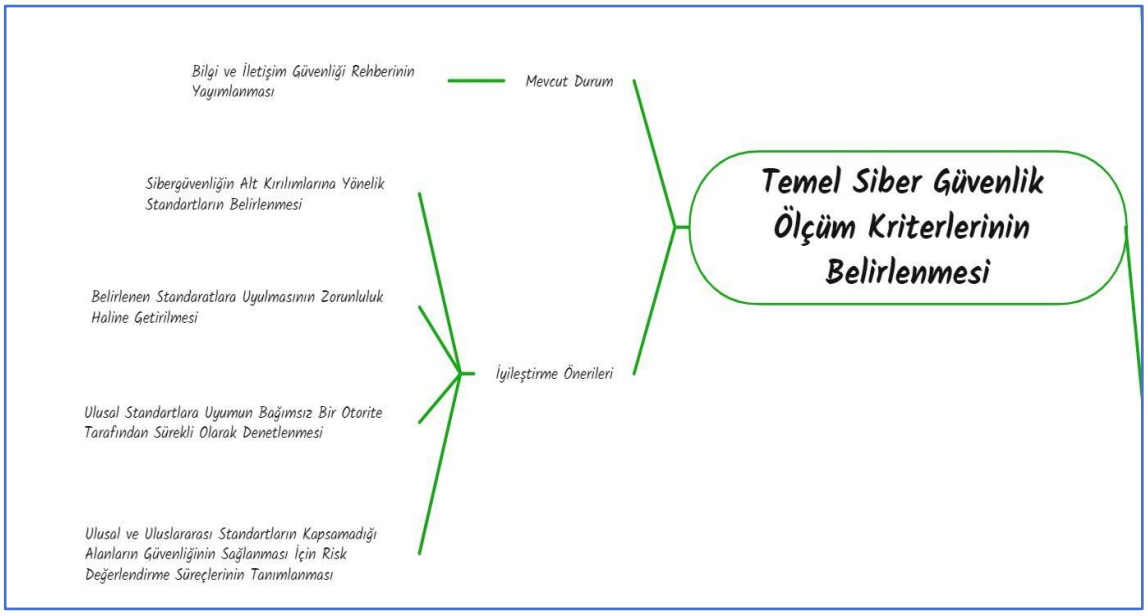
Mevcut ulusal acil durum planlarına siber güvenlik odaklı Ulusal Siber Güvenlik Kriz Yönetimi Planı'nın eklenmesi gelecekteki olası siber güvenlik krizlerinin yönetimi için önemli bir çerçeve sunacaktır. Ortaya çıkarılacak ola planın tüm paydaşların katılımıyla sürekli olarak test edilmesi gelecekte ortaya çıkacak olan yeni tehditlere karşı planın güncel kalmasını sağlayacaktır. Plan ortaya çıkarılmadan önce çalıştaylar gerçekleştirilerek kritik kamu kurumlarının planda yer alması ve kendi alanlarına yönelik tedbirlerin plana dahil edilmesi sağlanarak kapsayıcı bir plan ortaya çıkarılabilecektir. Siber güvenlik krizlerinde iletişiminin önemi çalışmada ortaya çıkarılmıştır. Bu kapsamda siber güvenli krizlerinde ve kriz öncesi süreçlerde iletişimin sağlanmasına yönelik uzmanlaşmış bir kadronun bulunduğu bir iletişim birimi tesis edilmelidir.

Şekil-38 Model'de Ulusal Acil Durum Planı



b. Kamu ve özel sektörde uygulanması gereken temel siber güvenlik tedbirleri T.C. Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi'nde yer almaktadır. Ancak siber alanın çok fazla teknik alt kırılımı mevcut olup daha kapsamlı bir standardizasyon çalışması bu alt alanlarda gerekli siber güvenlik tedbirlerinin ulusal çapta alınmasına katkı sağlayacaktır. Belirlenen standartlara uyumun bağımsız bir otorite tarafından denetlenmesi yaptırım gücü oluşturarak belirlenen standartlara uyumu hızlandıracaktır. Siber güvenliğin doğasında yer alan teknik güvenliğin uyumdan hızlı olması gerçeği gereği ortaya çıkan yeni tehditlere hızlı teknik güvenlik tedbirleri alınmakta uyum bu süreçte sonradan gelmektedir. Ortaya çıkan boşluk ise ancak etkili risk yönetimi süreçleri ile doldurulabilmektedir. Bu kapsamda ulusal çapta geçerliliği olan risk yönetimi süreçlerinin belirlenmesi ve ekosistemdeki tüm kurum kuruluşlarda uygulanması ortaya çıkan boşluğun doldurulmasını sağlayacaktır.

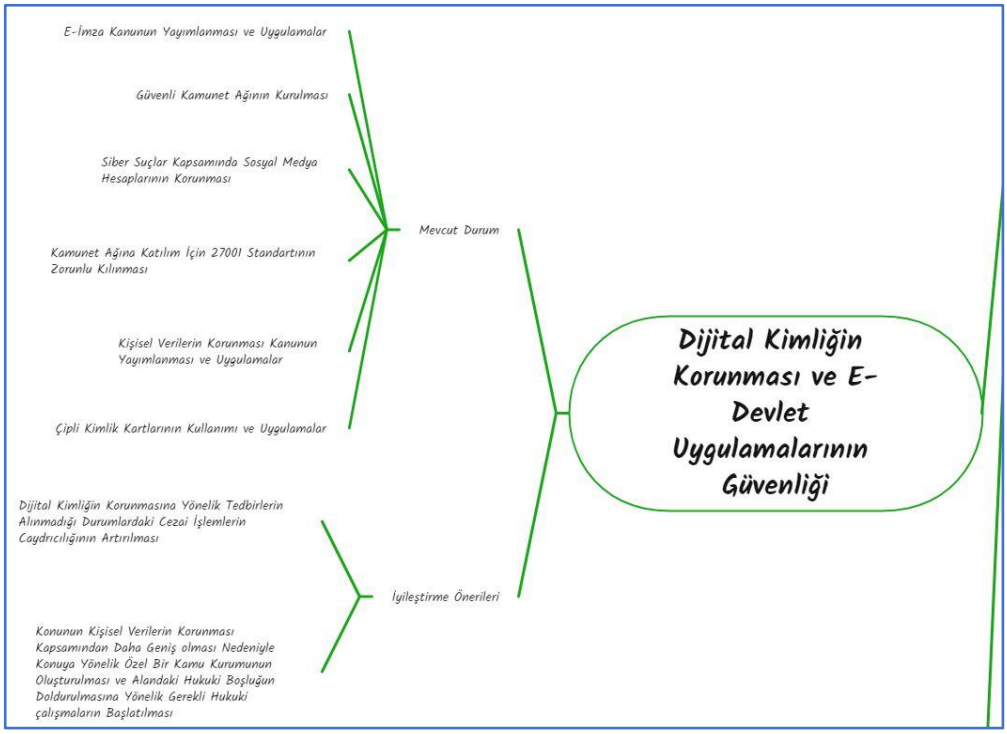
Şekil-39 Model'de Temel Siber Güvenlik Ölçüm Kriterlerinin Belirlenmesi



c. Dijital Kimliğin Korunması ve E-Devlet Uygulamalarının Güvenliği

Siber uzayın gerek gündelik hayatta gerekse kamusal işlemlerde karşılığın genişlemesi dijital kimliğin kapsamını genişletmiş, korunması gereken temel bir hakka dönüşmüştür. Dijital kimlik hırsızlığı, siber uzayın doğası gereği saldırganlar için başarıya ulaşılması daha kolay ve kapsamlı bir suç türüne dönüşmüştür. Bu yeni suç türü ile mücadele için TCK ve diğer ilgili kanunlarda yer alan cezai müyedilerin artırılması ve suçun tanımlanabilmesi için gerekli teknik ve idari araştırma süreçlerinin belirlenmesi gerekmektedir. Bu süreçlerin kendi özgü durumu nedeniyle alana odaklanmış ve uzmanlaşmış bir kurumun ortaya çıkarılması ortaya konan çabalardan maksimum faydanın sağlanmasını sağlayacaktır.

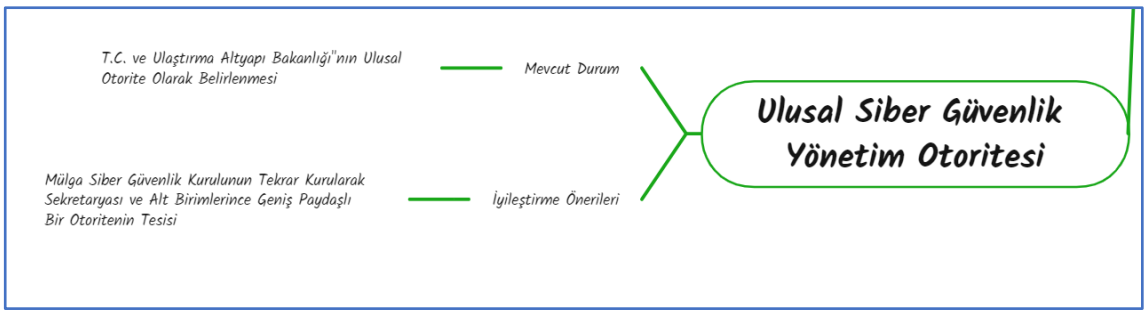
Şekil-40 Model'de Dijital Kimliğin Koruması ve E-Devlet Uygulamalarının Güvenliği



ç. Ulusal Siber Güvenlik Yönetim Otoritesi

Siber güvenliğin çok paydaşlı yapısı nedeniyle konunun ulusal çapta ele alınması T.C. Ulaştırma ve Altyapı Bakanlığı'nın yetki ve faaliyet kapsamını aşmaktadır. Bu nedenle Elektronik Haberleşme Kanununda Cumhurbaşkanı tarafından kurulması öngörülen Siber Güvenlik Kurulu'nun oluşturulması ve işler bir sekretaryaya sahip olması ulusal çaptaki siber güvenlik faaliyetlerindeki sinerjiyi artıracaktır.

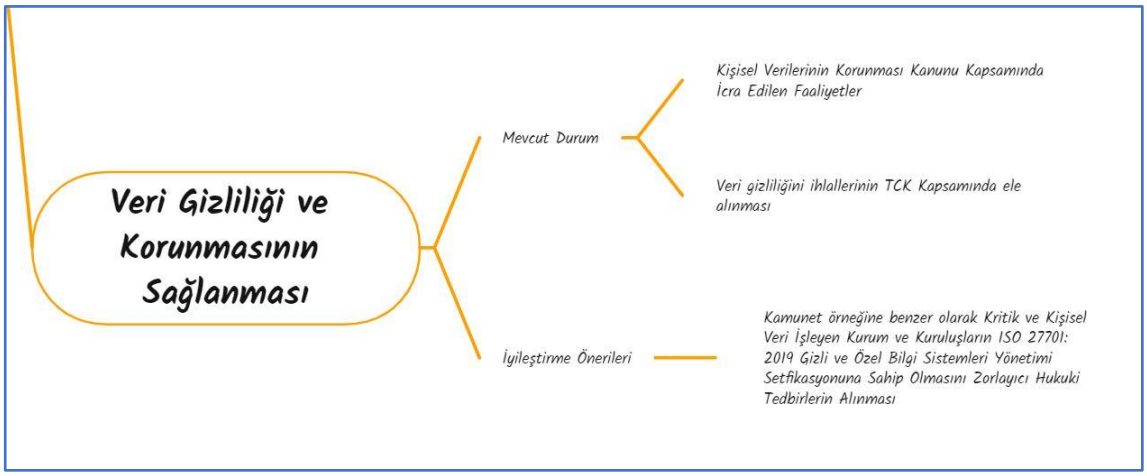
Şekil-41 Model'de Ulusal Siber Güvenlik Yönetim Otoritesi



d. Veri Gizliliği ve Korunmasının Sağlanması

Kamunet güvenliği için belirlenen 27001 Bilgi Güvenliği Yönetim Sistemi standartına uyum uygulamasına benzer bir sürecin veri gizliği ve korunması alanında belirlenmesi gerekmektedir. Alana en uygun standart olan ISO 27701:2019 Gizli ve Özel Bilgilerin Güvenliği standartına uyum alana yönelik gerekli tedbirlerin toplu bir şekilde alınmasını sağlayacaktır.

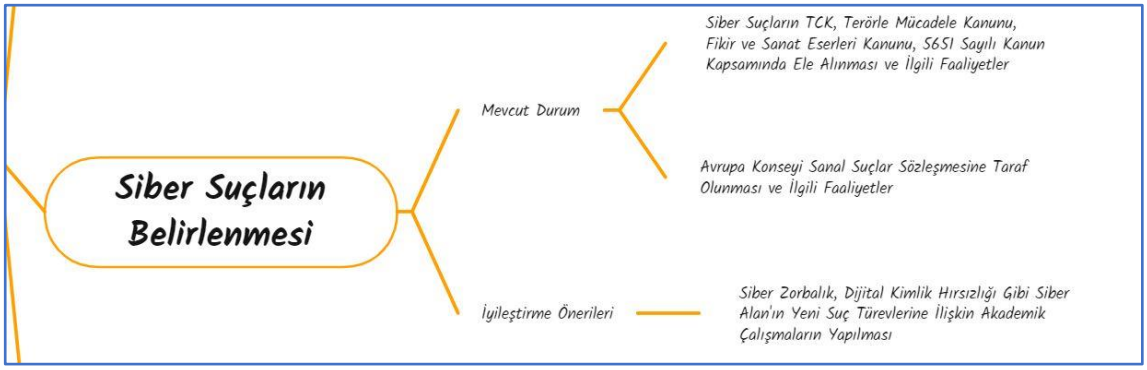
Şekil-42 Model'de Veri Gizliliği ve Korunmasının Sağlanması



e. Siber Suçların Belirlenmesi

Siber uzay beraberinde sanal suç kavramını da getirmiştir. Siber uzayda ortaya çıkan yeni suç türlerine yönelik akademik çalışmaların teşvik edilmesi ve alanın sürekli ve yakından incelenmesi siber suçlarla olan mücadeleye katkı sağlayacaktır.

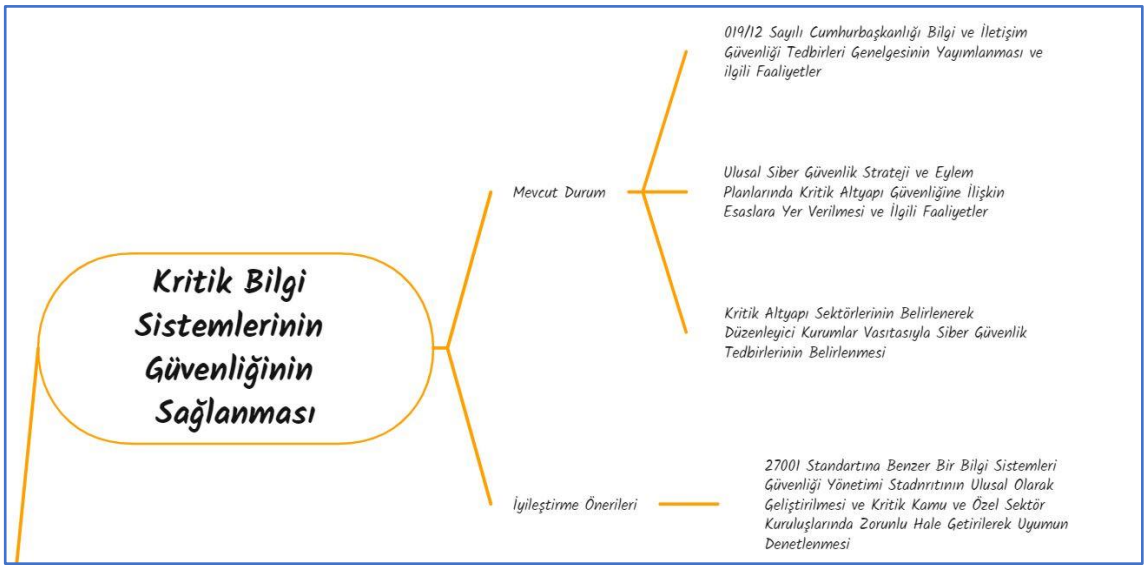
Şekil-43 Model'de Siber Suçların Belirlenmesi



f. Kritik Bilgi Sistemlerinin Güvenliğinin Sağlanması

Ulusal siber güvenlik standartlarına kritik bilgi sistemlerinin güvenliğine ilişkin özel standartların belirlenip uyum denetimimin sağlanması kamu ve özel sektörde yer alan kritik bilgi sistemlerinin güvenliğinin sağlanmasına katkı sağlayacak ulusal çapta güçlü bir siber güvenlik ekosisteminin oluşturulmasına neden olacaktır.

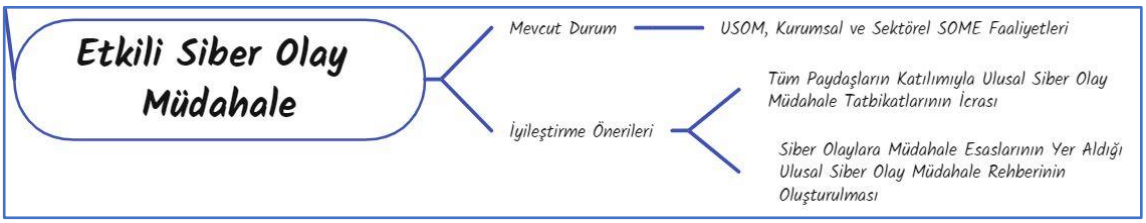
Şekil-44 Model'de Kritik Bilgi Sistemlerinin Güvenliğinin Sağlanması



g. Etkili Siber Olay Müdahale

USOM çatısı altında teşkilatmış olan Ulusal Siber Müdahale organizasyonun işlerliğinin test edilmesi için tüm paydaşların katılımıyla düzenli olarak Siber Olay Müdahale tatbikatlarının icra edilmesi ortaya çıkan yeni tehditlere karşı mücadele faaliyetlerine katkı sağlayacak ve faaliyet sonu inceleme süreci ile sistemin iyileştirilmesi sağlanabilecektir.

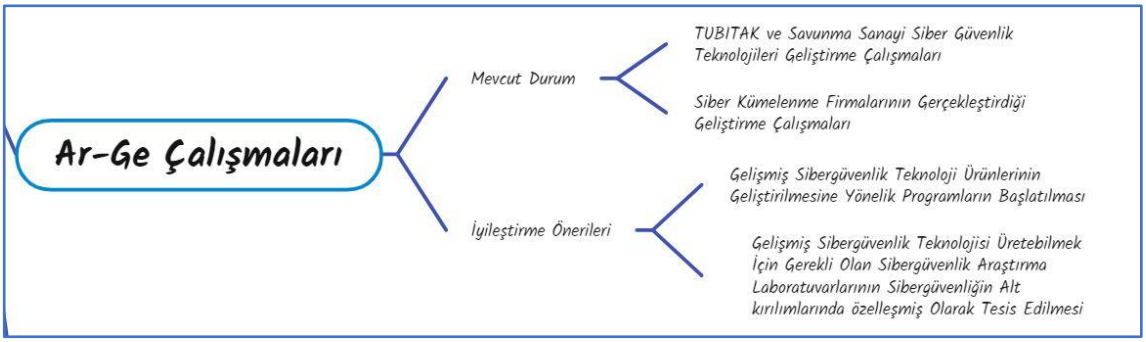
Şekil-45 Model'de Etkili Siber Olay Müdahale



h. Ar-Ge Çalışmaları

Siber uzayla beraber siber saldırı türleri de gelişim göstermektedir. Yeni siber saldırı türlerine karşı mücadele için yapay zeka, büyük veri analizi, makine öğrenmesi gibi yeni teknolojileri barındıran yüksek teknoloji ürünü siber güvenlik sistemlerine ihtiyaç duyulmaktadır. Ulusal güvenlik için son derece önemli olan bu sistemlerde yerli ve milliğinin artırılması için gerekli olan siber güvenlik araştırma enstitüleri ve laboratuvarlarının devlet destekli olarak kurulması alandaki değişim ve büyümenin yakalanmasına katkı sağlayacaktır.

Şekil-46 Model'de Ar-Ge Çalışmaları



i. Eğitim Öğretim Çalışmaları

Türkiye'de siber güvenlik eğitim çalışmaları ulusal siber güvenlik stratejisi geliştirme çalışmalarında kendisine yer bulmuş kısa süreli sertifika programlarından siber güvenlik lisesi, siber güvenlik yüksek lisans ve doktora programlarının geliştirilmesi gibi uzun süreli eğitim öğretim faaliyetleri icra edilmektedir. Ancak sektörde ileri seviye siber güvenlik personeline olan ihtiyacın artış göstermesi alanın alt dallarına yönelik siber güvenlik uzmanlık eğitimlerini gerekli kılmaktadır. Bu kapsamda üst seviye eğiticilerin yer aldığı ulusal çapta ileri seviye siber güvenlik eğitimi verebilecek eğitim öğretim kurumların kurulması ileri seviye siber güvenlik uzmanı ihtiyacının karşılanmasına katkı sağlayacaktır.

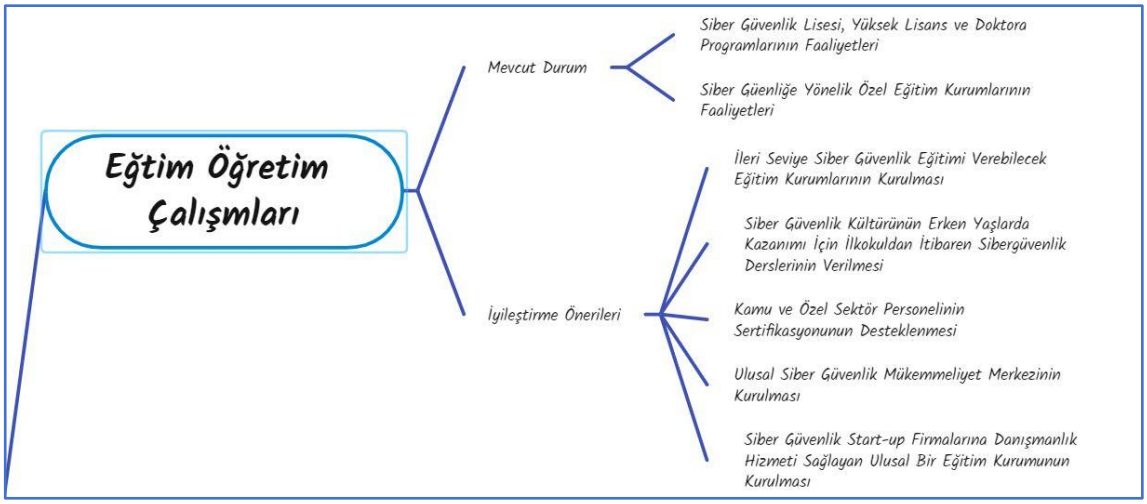
Çalışma esnasında ele alınan siber güvenlik olaylarının önemli bir bölümünde kullanıcı kaynaklı hata ve ihmaller yer almaktadır. Güvenliği için milyonlar harcanan bir sistem, kullanıcının, kurumun parola politikalarına aykırı olarak basit parola kullanması nedeniyle saldırganların hedeflerine ulaşmasına neden olabilmektedir. Ulusal çapta siber güvenlik bilincinin erken yaşlarda yerleşmesini sağlamak için Milli Eğitim Bakanlığı'nca ilköğretimden itibaren siber güvenlik derslerine yer verilmesi, gelecekte çeşitlilik ve kapsam bakımından artışa geçecek olan siber saldırılara karşı ulusal siber uzayın korunması faaliyetlerinin başarısını artıracaktır.

Siber güvenliğin alt alanlarındaki uzmanlık seviyelerindeki yetkinliğin önemli bir göstergesi olan siber güvenlik sertifikalarına kamu ve özel sektör personelinin görev alanı kapsamına göre sahip olmasının desteklenmesi personelinin kendisini bu alanda yetiştirmesine neden olacaktır. Söz konusu sertifikasyonları elde etmek için sunulan eğitim programları ilgili personele bir kılavuz görevi görmekte ilgili program takip edildiğinde gerekli uzmanlaşma sağlanabilmektedir. Kurumların kendi görev alanlarına göre bir sertifikasyon yol haritası belirlemesi

personel için siber güvenlik kariyer programının oluşturulmasına katkı sağlayacaktır.

Siber güvenlik faaliyetlerine ulusal çapta sinerji ve orkestrasyon kazandırılması maksadıyla Ulusal Siber Güvenlik Mükemmeliyet Merkezi kurulmalıdır. Alandaki yeniliklerin bu merkez üzerinden takip edilerek, ulusal çapta eğitim öğretim ve araştırma faaliyetlerinin bu merkez vasıtasıyla icra edilmesi alana ayrılan kaynaklardan maksimum faydanın elde edilmesini sağlayacaktır.
Siber güvenlik start-up firmaları günümüzde siber güvenlik ürünü geliştirimesinde önemli bir yere sahiptir. Yeni teknolojilerde üretim yapılmasını hızlı ve az maliyetle sağlayan bu oluşumlar zaman içerisinde katma değeri yüksek kurumlara dönüşebilmektedirler. Dünya ve ülkemizdeki gelişmeleri takip ederek ilgili firmalara yön gösterebilecek, gerekli başlangıç sermayesini sağlayabilecek bir kamu kurumunun kurulması yerli olarak siber güvenlik ürünü üretebilme faaliyetlerine katkı sağlayacak ayrıca önemli bir ihracat kalemi oluşturulabilecektir.

Şekil-47 Model'de Eğitim Öğretim Çalışmaları



Tablo-4 Eylem Maddeleri ve Aktörler Matrisi[27]

Aktör	Devlet							Özel Sektör
	Ulaştırma ve Altyapı Bakanlığı	Milli Eğitim Bakanlığı	Adelet Bakanlığı	YÖK	Dijital Dönüşüm Ofisi	Bilim Sanayi ve Teknoloji Bakanlığı	Kritik Altyapıları Düzenleyici Kurumlar	
Eylem Maddesi								
Ulusal Acil Durum Planı	Planın oluşturulması için genel koordinasyon görevi				Kamu ve özel sektör paydalarının belirlenmesi	TUBITAK tarafından gerekli akademik çalışmaların icrası	Plana kendi sorumluluk sahalarına göre katkı sağlamak	
Temel Siber Güvenlik Ölçüm Kriterlerinin Belirlenmesi	Elektronik Haberleşme İçin Gerekli Standartların Belirlenmesi				Bilgi ve İletişim Güvenliği Rehberi Çalışamlarının Geniletilmesi	TUBITAK tarafından belirlenen ölçütlerin genişletilmesi	kendi sorumluluk sahalarına göre ölçüm kriterlerini belirlemek	Belirlenen Kriterlere Uyum
Dijital Kimliğin Korunması ve E-Devlet Uygulamalarının Güvenliği			. Bu yeni suç türü ile mücadele için TCK ve diğer ilgili kanunlarda yer alan cezai müyedilerin artırılması ve suçun tanımlanabilmesi için gerekli teknik ve idari araştırma süreçlerinin belirlenmesi					Belirlenen Kriterlere Uyum
Veri Gizliliği ve Korunmasının Sağlanması	ISO 27701:2019 Gizli ve Özel Bilgilerin Güvenliği standartına uyum alana yönelik gerekli tedbirlerin toplu bir şekilde alınmasını sağlanması							Belirlenen Kriterlere Uyum
Siber Suçların Belirlenmesi			Siber uzayda ortaya çıkan yeni suç türlerine yönelik akademik çalışmaların teşvik edilmesi ve alanın sürekli ve yakından incelenmesi	Siber uzayda ortaya çıkan yeni suç türlerine yönelik akademik çalışmaların teşvik edilmesi ve alanın sürekli ve yakından incelenmesi				
Kritik Bilgi Sistemlerinin Güvenliğinin Sağlanması					Bilgi ve İletişim Güenliği Rehberinin İlgili Maddelerinin Artırılması ve Uyumun Denetlenmesi			
Etkili Siber Olay Müdahale	USOM çatısı altında teşkilatmış olan Ulusal Siber Müdahale organizasyonun işlerliğinin test edilmesi için tüm paydaşların katılımıyla düzenli olarak Siber Olay Müdahale tatbikatlarının icra edilmesi							
Ar-Ge Çalışmaları						Ulusal güvenlik için son derece önemli olan bu sistemlerde yerli ve milliğinin artırılması için gerekli olan siber güvenlik araştırma enstitüleri ve laboratuvarlarının devlet destekli olarak kurulması		
Eğitim Öğretim Çalışmaları	Siber güvenliğin alt alanlarındaki uzmanlık seviyelerindeki yetkinliğin önemli bir göstergesi olan siber güvenlik sertifikalarına kamu ve özel sektör personelinin görev alanı kapsamına göre sahip olmasının desteklenmesi faaliyetlerinin koordinasyonu	. Ulusal çapta siber güvenlik bilincinin erken yaşlarda yerleşmesini sağlamak için Milli Eğitim Bakanlığı'nca ilköğretimden itibaren siber güvenlik derslerine yer verilmesi		Lisansüstü eğitimde siber güvenlik bölümlerinin artırılması	Siber güvenlik faaliyetlerine ulusal çapta sinerji ve orkestrasyon kazandırılması maksadıyla Ulusal Siber Güvenlik Mükemmeliyet Merkezinin kuırulması	Siber güvenlik Start-Up firmalarına destek sağlanması Dünya ve ülkemizdeki gelişmeleri takip ederek ilgili firmalara yön gösterebilecek, gerekli başlangıç sermayesini sağlayabilecek bir kamu kurumunun kurulması		Özel eğitim merkezlerinin uzmanlık eğitimlerini artırması

[27] Tablo oluşturulurken (Yıldız ve Babaoğlu,2020) kaynağında yer alan Teknoloji Politikaları ve Aktörler tablosundan yararlanılmıştır.

EK-8 AHTOPOT ve PARDUS PROJELERİ

AHTAPOT PROJESİ

Siber güvenlik önlemlerinin başarıya ulaşabilmesi için uyulması gereken önemli kurallardan biri, bilişim sistemi içinde yer alması gereken tüm siber güvenlik bileşenlerinin sisteme dahil edilmesidir. Derinlemesine savunma için ihtiyaç duyulan siber güvenlik bileşenlerinin entegre edildiği bir sistemdir. Açık Kaynak Kodlu bileşenler kullanılmaktadır; bu sayede denetlenemeyen ve arka kapı bulundurması muhtemel olan, bununla birlikte pahalı olan siber güvenlik çözümlerine bağımlılığı azaltmaktadır. Türkçe ve kolay anlaşılır kurulum ve kullanım dokümanları ile, bileşenlerin kullanılması için gerekli bilgi birikiminin ve destek ihtiyacının azaltılması sağlanmaktadır. Merkezi yönetim sistemi ile, bilişim sisteminin farklı noktalarında dağıtık olarak yerleştirilecek siber güvenlik çözümlerinin yönetimi ve yapılandırılmasını kolaylaştırmaktadır.

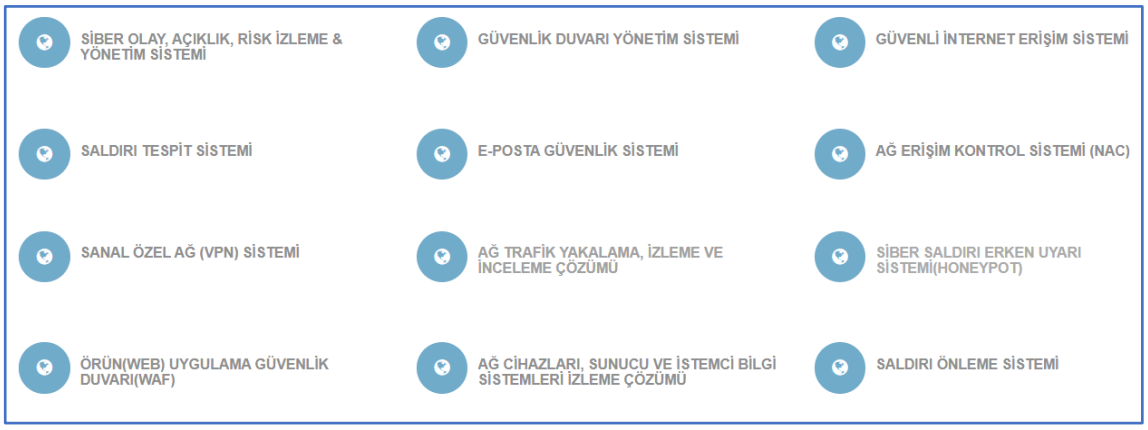
Ahtapot, şu özellikleri taşır;

- İşletim Sistemi Pardus'tur; bu sayede siber güvenlik bileşenlerinde de açık kaynak kodlu milli işletim sistemi dağıtımı kullanılmaktadır.
- Açık kaynak kodlu bileşenlerden oluşur; bu sayede denetleyemediğimiz, kimlerle hangi bilgileri paylaştığını bilemeyeceğimiz sistemlerden uzak durulur.
- Ahtapot; kurulumların, yapılandırmaların ve güncellemelerin kolaylaştırılması için bir merkezi yönetim sistemi barındırır.
- Türkçe ve kolay anlaşılır kurulum ve kullanım kılavuzlarına sahiptir.

BİLEŞENLER

Açık kaynak kodlu bileşenlerden oluşur; bu sayede denetleyemediğimiz, kimlerle hangi bilgileri paylaştığını bilemeyeceğimiz sistemlerden uzak durulur.

Şekil-48 AHTOPOT Sistemi Bileşenleri



Kaynak: (AHTOPOT Projesi Resmi İnternet Sitesi, 2021)

PARDUS PROJESİ

Pardus işletim sistemi dağıtımının adı, Anadolu Parsı'nın bilimsel adı olan "Panthera Pardus Tulliana"dan gelecek şekilde seçilmiştir. Pardus projesine yönelik ilk çalışmalar 2003 yılında Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) bünyesinde başlamıştır. Öncelikle gereksinimler, dünyadaki benzer uygulamalar, ülkenin bilgi teknolojisi alanındaki insan kaynağı, yerel yazılım sanayinin yetenekleri ve rekabet unsurları incelenmiştir. Elde edilen bulgular ışığında, 2003 yılı yazında, somut planlamalara başlanmıştır. Mevcut işletim sistemleri, başta Linux olmak üzere incelenmiş, açık kaynak yazılım metodolojisi ve özgür yazılım felsefesi incelenmiş. Bu incelemeler sonucunda, 2003 yılı güzünde, Linux temelli, açık kaynak kodlu, olabildiğince GPL lisanslama yöntemini kullanan bir işletim sistemi dağıtımı oluşturulmasına karar verilmiştir.

Pardus projesinin hayata geçmesi ise 2004 yılı başında TÜBİTAK BİLGEM Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) bünyesine oluşturulan ekip ile başlamıştır. Hedef; Pardus'un "bilişim okur-yazarlığına sahip bilgisayar

kullanıcılarının temel masaüstü ihtiyaçlarını hedefleyen" bir işletim sistemi olması olarak belirlenmiştir. 1 Şubat 2005 tarihinde ilk ürün olan Pardus Çalışan CD 1.0 yayımlanmıştır.

2012 yılı itibariyle Pardus projesinin hedefi öncelikle KAMU'da açık kaynak/özgür yazılımların yaygınlaştırılmasının sağlanması olacak şekilde güncellenmiş ve 2004-2011 yılları arasında UEKAE bünyesinde yürütülen projenin yönetimi Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM)'e devredilmiştir. Günümüzde işletim sisteminin yanı sıra PARDUS çatısı altında KAMU'nun ihtiyaçları doğrultusunda geliştirilen alt projelerde yer almaktadır. (PARDUS Projesi Resmi İnternet Sitesi, 2021)

PARDUS DÖNÜŞÜM

Pardus kullanmak isteyen küçük veya büyük ölçekli kamu kurum ve kuruluşlarında Pardus Dönüşüm için analiz çalışması yapılmaktadır. Bu analiz çalışmasında, kurum tarafından kullanılan yazılımların platform-bağımsız olup olmadıkları ve platform-bağımlı uygulamalarda verimli çalışılabilecek alternatifler varsa incelenerek, kurumun bilişim altyapısının Pardus dönüşümüne uygunluk durumu tespit edilmektedir. Ulus ekonomisi ve performans gözetilerek Kurumun Pardus Dönüşüm yapmasına yönelik karar sonrası dönüşüm çalışmalarına başlanmaktadır. Platform bağımlı bir uygulama var ise dönüşüm yapılmayarak, kurumun yazılımını platform bağımsız hale getirmesi beklenmektedir. Pardus Dönüşüm için TUBİTAK ULAKBİM'den destek alınabileceği gibi TÜBİTAK ULAKBİM tarafından yetkilendirilmiş İş Ortağı ve Kurumsal Göç Ortağı firmalardan da destek alınabilmektedir.

Ek-9 KİŞİSEL VERİLERİN KORUNMASI TEDBİRLERİ DENETİM MADDELERİ

Kayıt Yönetimi

Tedbir Adı	Denetim Sorusu	Açıklama
Kişisel Veri İşleme Envanterinin Hazırlanması ve Yönetimi	Veri Sorumluları Sicili Hakkında Yönetmelik'e uygun kişisel veri işleme envanteri hazırlanmış mıdır? Envanter belirli periyotlarda güncellenmekte midir?	
Kişisel Veri Saklama ve İmha Politikasının Hazırlanması	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'e uygun kişisel veri saklama ve imha politikası hazırlanmış, ilgili taraflara duyurulmuş ve uygulanıyor mu?	
Kişisel Verilerin Veri Tabanlarında Birincil Anahtar Olarak Kullanılmaması	Veri tabanı tablolarının tasarımında kişisel veriler (T.C. kimlik numarası, pasaport numarası vb.) birincil anahtar olarak kullanılmakta mıdır?	
Veri Tabanının Dışarıya Aktarımının Yetkili Kullanıcı Tarafından Yapılması	Veri tabanı işlemlerinde kullanılan hesaplarda minimum yetki prensibi uygulanmakta mıdır? Veri tabanının kısmen/tamamen dışa aktarımı için hangi hesap(lar) kullanılmaktadır?	
Kişisel Verilerin Güvensiz Ortamlarda Saklanmaması	Kişisel verinin hangi ortamlarda saklanabileceği tanımlanmış mıdır? Tanımlanan ortamlarda ulusal/uluslararası standartlara uygun güvenlik önlemleri alınmakta mıdır?	

Kişisel Veri Üzerinde Girdi/Çıktı Denetimi Yapılması	Uygulamanın girdi olarak kullandığı kişisel veri üzerinde girdi/çıktı doğrulama eksikliğinden kaynaklı zafiyetlere karşı güvenlik kontrolleri uygulanmakta mıdır?	
Kişisel Verinin Gizli Alanlarda Saklanmaması	Kişisel veriler web sayfalarının gizli alanlarında ya da web depolama özelliği üzerinde saklanmakta mıdır? Kişisel veriler tarayıcı ön belleğinde saklanmakta mıdır? Çerezlerde bulunan kişisel verinin güvenliği nasıl sağlanmaktadır?	
Hata Mesajlarında Mahremiyetin Korunması	Hata mesajlarında mahremiyetin korunması amacı ile hangi önlemler alınmaktadır?	
Özel Nitelikli Kişisel Verinin Saklanması	Özel nitelikli kişisel veri barındıran kayıtların güvenliği için ne gibi önlemler alınıyor? Alınan önlemler ulusal ve/veya uluslararası kabul görmüş uygulamalar mıdır?	
Geçici Olarak Tutulan Kişisel Verinin Yok Edilmesi	İstemci ve sunucu uygulamalarında kişisel verinin geçici kopyalarının yok edilmesi (geri getirilemeyecek, tekrar elde edilemeyecek vb. şekilde silme) amacıyla yöntemler/süreçler belirlenmiş midir? Belirlenen yöntemler/süreçler uygulanmakta mıdır?	

Erişim Kayıtları Yönetimi

Tedbir Adı	Denetim Sorusu	Açıklama
Erişimlerin Kayıt Altına Alınması	Kişisel veri barındıran ortamlara yapılan başarılı ve başarısız erişimler kayıt altına alınmakta mıdır? Alınan kayıtlar hangi periyotlarda gözden geçirilmektedir?	
Erişim Kayıtlarının Arşivlenmesi	Kişisel verilere gerçekleştirilen erişim kayıtları ilgili mevzuatlara ve ikincil düzenlemelere uygun şekilde arşivlenmekte midir?	
Erişim Kayıtlarının Güvenliğinin Sağlanması	Kişisel veriye gerçekleştirilen erişim kayıtlarının güvenliği nasıl sağlanmaktadır?	
Erişim Kayıtlarının Aktarımı	Erişim kayıtlarının dışarı/içeri aktarılması için bir mekanizma mevcut mudur? Erişim kayıtlarının dışarı/içeri aktarılması için kullanılan mekanizmada mevcut kayıtların güvenliğini sağlamak için ne gibi önlemler alınmaktadır?	
Yetkisiz Erişimlerin Tespiti	Erişim kayıtları üzerinden yetkisiz işlemleri tespit edebilmek amacıyla analiz faaliyetleri gerçekleştirilmekte midir?	
Erişim Kayıtlarında Özel Nitelikli Kişisel Veri Bulundurulmaması	Erişim kayıtlarının hangi bilgileri içereceği tanımlanmış mı? Erişim kayıtları özel nitelikli kişisel veri barındırıyor mu?	

Yetkilendirme

Tedbir Adı	**Denetim Sorusu**	**Açıklama**
Yetkilendirme Mekanizmasının Kullanılması	Kişisel veriye erişim istekleri için yetkilendirme mekanizması kullanılmakta mıdır? Kişisel veriye erişim isteklerinde kullanılan yetkilendirme mekanizmasında hangi kurallar uygulanmaktadır? Kişisel veriye yetkisiz erişimi engellemek amacıyla hangi önlemler alınmaktadır?	
Kimlik Doğrulama Mekanizmasının Kullanılması	Kişisel veri barındıran ortamlara (web sayfası, dosya vb.) erişimde kimlik doğrulama mekanizması kullanılıyor mu?	
Erişimin Sınırlandırılması	Kişisel veri barındıran ortamlara hangi yöntemlerle erişim sağlanmaktadır? Belirlenen yöntemler kullanılmadan gerçekleştirilmek istenen erişimlerin engellenmesi amacıyla hangi önlemler alınmaktadır?	
Erişim Denetim Politikalarının Oluşturulması	Kişisel verilerin bulunduğu ortamlara/kaynaklara yapılacak erişimleri denetlemek amacıyla politika oluşturulmuş mudur? Belirlenen politika hangi hususları içermektedir?	
Çok Faktörlü Kimlik	Özel nitelikli kişisel veri barındıran ortamlara erişim	

Doğrulama Mekanizmasının Kullanılması	için kullanılan kimlik doğrulama mekanizmaları nelerdir?	
Dış Sistemler / Uygulamalar Arası Veri Akışı için Erişimlerin Doğrulanması	Dış sistemler/uygulamalar arası kişisel veri akışı için erişim doğrulama kontrolü yapılmakta mıdır? Erişim ile ilgili girdi parametreleri ve sonuçlar kayıt altına alınmakta mıdır?	
Alt Bileşenler Arasında Veri Akışı için Erişimlerin Doğrulanması	Sistem içi kişisel verinin akışı için erişim doğrulama kontrolü yapılmakta mıdır?	

Şifreleme

Tedbir Adı	Denetim Sorusu	Açıklama
İletişimin Şifrelenmesi	Kişisel verinin paylaşımında sistemler arası iletişim şifreli olarak gerçekleştirilmekte midir?	
Verinin Maskelenmesi	Kişisel veri üzerinde işlem yapılması ana amaç olmayan durumlarda verinin mahremiyeti için hangi önlemler alınmaktadır? Alınan önlemlerde maskeleme yöntemleri kullanılmakta mıdır? Kullanılan maskeleme yöntemleri nelerdir?	
Verinin Bütünlüğünün Korunması	Kişisel verinin yetkisiz bir şekilde değiştirilmesini	

	engellemek için hangi yöntemler kullanılmaktadır? Kullanılan yöntemlerde kriptografik kontroller yer almakta mıdır?	
Sistemin Alt Bileşenleri Arasındaki İletişimin Şifreli Yapılması	Uygulama sunucuları ile bağlantı kurduğu sunucular arasındaki iletişim şifreli olarak sağlanmakta mıdır?	

Yedekleme, Silme, Yok Etme ve Anonim Hale Getirme

Tedbir Adı	Denetim Sorusu	Açıklama
Sistem Yedeklerinin Yetkili Kullanıcılar Tarafından Alınması	Kişisel veri barından sistem yedeklerini almak amacıyla yetkilendirilmiş kullanıcılar bulunmakta mıdır? Yedekleme işlemlerine ait iz kayıtları tutulmakta mıdır? Tutulan kayıtlar ne kadar süre ile muhafaza edilmektedir?	
Kişisel Verilerin Silinmesi	Kişisel verilerin silinmesine yönelik süreç tanımlanmış ve uygulanmakta mıdır?	
Kişisel Verilerin Yok Edilmesi	İşleme süresi biten kişisel veriler nasıl belirlenmektedir? Kişisel verilerin saklanmasına ve imhasına yönelik politika oluşturulmuş ve uygulanmakta mıdır?	
Kişisel Verilerin Anonim Hale Getirilmesi	Anonim hale getirilmesi planlanan kişisel veriler nasıl belirlenmektedir? Kişisel verileri anonim hale getirmek amacıyla hangi Yöntemlerden faydalanılmaktadır?	

	Test, geliştirme vb. ortamlarda kullanılan kişisel veriler anonim hale getirilmekte midir?	
Kişisel Veri Barındıran Yedeklerin Güvenliğinin Sağlanması	Kişisel veri barındıran yedeklerin güvenliğinin sağlanması için uygulanacak faaliyetler/süreçler belirlenmiş midir? Yedeklere yapılan erişimlerin iz kayıtları tutulmakta mıdır?	
Kişisel Veri Barındıran Yedeklerin Yok Edilmesi	Kişisel veri barındıran yedeklerin güvenli şekilde yok edilmesi amacıyla bir mekanizma/süreç uygulanmakta mıdır?	

Aydınlatma Yönetimi

Tedbir Adı	Denetim Sorusu	Açıklama
Aydınlatmanın Doğru Zamanda Yapılması	İlgili kişilere aydınlatmanın doğru zamanda yapılması amacıyla bir süreç oluşturulmuş mudur?	
Aydınlatmanın Yerine Getirildiğinin İspat Edilmesi	Aydınlatmanın yerine getirildiğini ispat edecek bir mekanizma oluşturulmuş mudur?	
Uygulama Üzerinden Aydınlatma Metninin Güncellenmesi	Aydınlatma metni uygulama üzerinden güncellenebilmekte midir? Aydınlatma metninin güncelleme işlemi öncesi durumu kayıt altına alınmakta mıdır?	

Açık Rıza Yönetimi

Tedbir Adı	Denetim Sorusu	Açıklama
Açık Rıza Unsurlarının Belirlenmesi	Kişisel verilerin işlenmesi amacıyla açık rıza alınması gereken durumlar belirlenmiş midir? Açık rıza alınması amacıyla aydınlatma metni hazırlanarak ilgili kişilere sunulmakta mıdır?	
Açık Rızanın Kayıt Altına Alınması	Açık rızanın kayıt altına alınması için bir mekanizma/süreç işletilmekte midir?	
Açık Rıza Durumunun Sorgulanması	İlgili kişiye ait açık rıza metninin onay durumu, onay tarihi saklanmakta mıdır? İlgili kişi tarafından açık rıza durumu sorgulanabilmektemidir? Yetkili kişi(ler)ce hangi kullanıcılardan açık rıza alındığı sorgulanabilmekte midir?	
Uygulama Üzerinden Açık Rıza Alınması	Uygulama üzerinden açık rızanın alınması ve açık rıza beyan durumunun sorgulanması için bir mekanizma/süreç işletilmekte midir?	
Açık Rıza Metninin Güncellenmesi	Uygulama üzerinde açık rıza metninin güncellenebilmesi için bir mekanizma/süreç tanımlanmışmıdır? Güncelleme öncesindeki açık rıza metinleri saklanmaktamıdır? Güncellenen açık rıza metinleri için kullanıcılardan tekrar açık rıza alınmakta mıdır?	
Açık Rıza ile İlgili Taleplerin Yönetilmesi	Uygulama üzerinden açık rıza ile ilgili taleplerin yönetimi sağlanabilmekte midir?	
Islak İmzalı Açık Rıza Metninin Saklanması	Islak imzalı açık rıza metinlerinin taranmış halinin saklanması amacıyla bir süreç işletilmekte midir?	

Kişisel Veri Yönetim Sürecinin İşletilmesi

Tedbir Adı	Denetim Sorusu	Açıklama
İlgili Kişinin Başvuru Hakkının Yönetilmesi	İlgili kişinin veri sorumlusuna başvuru hakkının yönetilmesi amacıyla bir süreç işletilmekte midir? Bu süreç yürürlükte olan ilgili mevzuata uygun mudur?	
Kişisel Veriye Yapılan İşlemlerin Elde Edilmesi	İlgili kişinin verisine yapılan işlemler kayıt altında tutulmakta mıdır?	
Güncelleme, Anonimleştirme, Silme ve Yok Etme İşlemlerinin Gerçekleştirilmesi	İlgili kişi tarafından talep edilen güncelleme, anonimleştirme, silme ve yok etme işlemlerinin yapılabilmesi amacıyla bir süreç işletilmekte midir? Tanımlanan süreç yürürlükte olan mevzuata uygun mudur?	
Kişisel Verinin Aktarıldığı Üçüncü Tarafların Tespit Edilmesi	Kişisel veriler üçüncü taraflara aktarıldığında aktarım işlemi ile ilgili hangi bilgiler kayıt altına alınmaktadır?	

Ek-10 ÖRNEK RİSK ANALİZİ VE YÖNETİM RAPORU

XYZ Kurumu Bölge Ofisi Veri Giriş İstasyonu İle ve KAMUNET Ağı Hizmet Sunucusunun Bağlantı Mimarisi Güvenlik Risk Analizi ve Yönetim Raporu

1. GENEL

a. Özet

Risk analizi ve Yönetim Raporu dokümanı XYZ Kurumu bölge ofisi veri giriş istasyonu ile ve KAMUNET ağı hizmet sunucusunun bağlantı mimarisi ve bileşenlerinin öngörülen risklerinin incelenmesini, tespit edilen risklerin giderimlerini içermektedir.

b. Amaç

XYZ Kurumu bölge ofisi veri giriş istasyonu ile ve KAMUNET ağı hizmet sunucusunun bağlantı mimarisi ve ilişkili alt bileşenlerde bulunan eksiklikleri ve açıklıkları belirlemek, bu açıklıklardan kaynaklanan riskleri ifade etmektir. Bununla birlikte risk çözümlemesi sonucu alınacak teknik ve operasyonel güvenlik tedbirlerini belirlemek ve bu tedbirlerin alınması halinde kalan riskleri ortaya koymaktır.

c. Kapsam

Yapılan çalışma, XYZ Kurumu bölge ofisi veri giriş istasyonu ile ve KAMUNET ağı hizmet sunucusunun bağlantı mimarisi ve ilişkili alt bileşenlere yönelik riskleri kapsamaktadır. XYZ Kamu Kurumu Ağı ve KAMUNET ağında yer alan diğer hizmet, servis ve uygulamalar kapsam dışında tutulmuştur.

ç. Tanımlar

Dokümanda yer alan tanımlamalara ilişkin başvuru kaynakları;

1) 2020 2023 Ulusal Siber Güvenlik Stratejisi
2) KAMUNET Ağı Bağlantı Esasları Yönetmeliği'dir.

d. Kısaltmalar

UDP	User Datagram Protocol
SIEM	Security Information Event Management
VLAN	Virtual Local Area Network

2. RİSK ANALİZİ METODU

Açıklık, bir Varlık'ı Tehditlere karşı korumasız hale getiren kusurlardır. Tehditler, Açıklıkları kullanarak Varlıklara zarar verirler. Bu nedenle, Açıklıklar, Risk'in asıl nedenidir.

Risk, Varlık'taki bir Açıklık'ın bir Tehdit tarafından kullanılma ihtimalidir. Risk'i ifade etmekte kullanılan temel formül,

Risk = Tehdit'in etki değeri * Tehdit'in gerçekleşme ihtimali şeklindedir.

Bu formül sayısal (quantitative) risk analizi yöntemlerinde, Risk'i numerik olarak ifade etmek amacıyla kullanılır.

Sistem'de Açıklıklardan doğan Riskleri ifade etmek ve sıralamak amacıyla bu temel formül kullanılmıştır. Böylece hem Risk miktarlarının sayısal olarak ifade edilmesi sonucunda anlama kolaylığı sağlanmış hem de Risklerin sıralanması gerçekleştirilmiştir.

Her bir Açıklık'tan doğan Risk miktarını sayısal olarak ifade etmek amacıyla, Açıklık'ı kullanan Tehdit'in etki değeri ve olma ihtimali değerleri de sayısal olarak ifade edilmiştir. Bunun için iki temel Risk tablosu kullanılmıştır.

Bu tablolardan ilki, Tablo 2-1, Tehdit'in etki değeri parametresini; ikincisi ise, Tablo 2-2, Tehdit'in gerçekleşme ihtimali parametresini sayısal olarak ifade etmekte kullanılmıştır. **Olasılık değerleri hesaplanırken geçmiş dönemde XYZ Kamu Kurumu Ağı ve KAMUNET ağında yaşanmış olan güvenlik olaylarının sıklığı, oluşum nedenleri göz önünde bulundurulmuştur.**

Risk tabloları düzenlenirken, “IS Standards, Guidelines and Procedures for Auditing and Control Professional” standardının “IS risk assesment & measurement” bölümünde bulunan tablo değerlerinden faydalanılmıştır.

Tablo 2-1 Etki Değeri için Kullanılan Değerler

ETKİ DEĞERİ	**AÇIKLAMA**
5	Sistemde ve sistem dışında kullanılan pek çok kaynağa ciddi zarar verir, Organizasyon durumunu ve ününü çok kötü etkiler.
4	Sistemde ve sistem dışında kullanılan birkaç kaynağa çok ciddi zarar verir.
3	Sistemde ve sistem dışında kullanılan bir ya da birkaç kaynağa ciddi zarar verir, yapılan iş olumsuz etkilenir.(tabloda orta zarar olarak işaretlenmiştir.)
2	Sistemde ve sistem dışında kullanılan bir kaynağa önemsiz zarar verir.
1	Sistemde ve sistem dışında kullanılan bir kaynağa çok az zarar verir ya da hiçbir zarar vermez.

Tablo 2-2 Riskin Gerçekleşme İhtimali için Kullanılan Değerler

OLASILIK DEĞERİ	**AÇIKLAMA**
5	Kesinlikle (Güvensiz, erişime açık sistem, bilinen zafiyetler)
4	Büyük İhtimalle
3	Orta İhtimalle
2	Az İhtimalle
1	Çok Az İhtimalle (Güvenli, Erişim kontrollü sistem, bilinen zafiyetler)

Belirli bir Açıklık’ı etkileyen Tehdit için Tablo 2-1 ve Tablo 2-2’deki değerler seçilirken, Varlık’ın değeri, görevi, kritikliği, Açıklık’ın derecesi ve Tehdit’in nereden geldiği göz önünde bulundurulmuştur. Belirlenen bu iki değerin Risk formülüne göre çarpılması sonucunda, belirli bir Açıklık için Risk değeri bulunur. Bir Risk değeri en küçük “1” en yüksek “25” çıkabilir. Ortaya çıkan Risk değerlerinin en yüksekten en düşüğe doğru sınıflandırılması ve nitel olarak ifade edilmesi sağlıklı bir analiz için gerekir. Bunun için, Tablo 2-3 kullanılmıştır. Tablo 2-3’te farklı renklerdeki hücreler içerisinde, formülün uygulanması sonucunda bulunan Risk miktarı ve Risk’in hangi nitel ölçeğe düştüğü

gösterilmiştir. Bu değerler, risk analizi raporunun sonuç kısmında Risk'i ifade etmek ve sıralamak amacıyla kullanılmıştır.

Risk Değeri = Olasılık * Etki	Çok Az Zarar	Önemsiz Zarar	Orta Zarar	Ciddi Zarar	Çok Ciddi Zarar
Çok Az İhtimalle	Düşük(1)	Düşük(2)	Düşük(3)	Orta(4)	Orta(5)
Az İhtimalle	Düşük(2)	Orta(4)	Orta(6)	Yüksek(8)	Yüksek(10)
Orta İhtimalle	Düşük(3)	Orta(6)	Yüksek(9)	Yüksek(12)	Kritik(15)
Büyük İhtimalle	Orta(4)	Yüksek(8)	Yüksek(12)	Kritik(16)	Çok Yüksek(20)
Kesinlikle	Orta(5)	Yüksek(10)	Kritik(15)	Çok Yüksek(20)	Çok Yüksek(25)

2. KRİTİK VARLIKLAR, AÇIKLIKLAR, TEHDİTLER

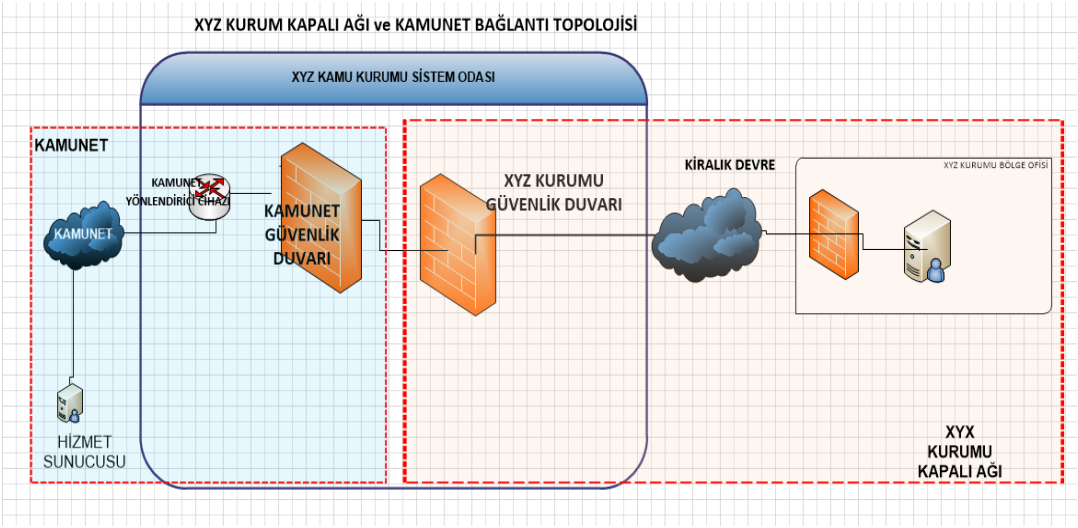
Bu kısımda XYZ Kurumu bölge ofisi veri giriş istasyonu ile ve KAMUNET ağı hizmet sunucusunun bağlantı mimarisi ve ilişkili alt bileşenlerinde yer alan kritik öneme sahip Varlıklar, Tehditler ve bu Tehditlerin gerçekleşmesine sebep olabilecek Açıklıklar belirlenmiştir.

İlgili mimari ve bileşenlerine ilişkin topoloji tablo 3-1 'de sunulmuştur.

XYZ Kurumu bölge ofisi veri giriş istasyonu ile ve KAMUNET ağı hizmet sunucusunun bağlantı mimarisi ve ilişkili alt bileşenleri;

- KAMUNET Ağı Hizmet Sunucusu
- KAMUNET Ağı Güvenlik Duvarı
- XYZ Kurumu Güvenlik Duvarı
- XYZ Kurumu Bölge Ofisi Güvenlik Duvarı

Tablo 3-1 XYZ Kurumu bölge ofisi veri giriş istasyonu ile ve KAMUNET ağı hizmet sunucusunun Bağlantı Mimarisi ve ilişkili alt bileşenleri mimarisi



a. Varlıklar

(1) Fiziksel ve Donanımsal Varlıklar

	Fiziksel ve Donanımsal Varlıklar	Değeri[28]		
		G	B	E
V1	KAMUNET Ağı Güvenlik Duvarı	NA	NA	5
V2	XYZ Kurumu Güvenlik Duvarı	5	5	5
V3	XYZ Kurumu Bölge Ofisi Güvenlik Duvarı	NA	NA	5
V4	KAMUNET Ağı Hizmet Sunucusu	NA	NA	5
V5	XYZ Kurumu Bölge Ofisi Veri Giriş Bilgisayarı	5	5	5
V6	XYZ Kurumu Ağı Kiralık Hattı ve Ağ Cihazları	NA	NA	5

(2) Bilgi Varlıkları (Bütünlük, Gizlilik, Kimlik Doğrulama ve İnkar Edememe)

	Bilgi Varlıkları (Bütünlük, Gizlilik, Kimlik Doğrulama ve İnkar Edememe)	Değeri[29]		
		G	B	E

[28] Varlığın değeri belirlenirken sisteme olan etkisi göz önüne alınmıştır. Bu etki 1 – 5 arasında belirlenmiş olup 1 en az etkiyi, 5 ise en çok etkiyi temsil etmektedir. (G: Gizlilik, B: Bütünlük, E: Erişilebilirlik, NA: Etkisi yok)

[29] Varlığın değeri belirlenirken sisteme olan etkisi göz önüne alınmıştır. Bu etki 1 – 5 arasında belirlenmiş olup 1 en az etkiyi, 5 ise en çok etkiyi temsil etmektedir. (G: Gizlilik, B: Bütünlük, E: Erişilebilirlik, NA: Etkisi yok)

V8	KAMUNET Ağı	5	5	NA
V9	XYZ Kurumu Ağı	5	5	NA

b. Tehditler

Riskin oluşması için olası bir tehlikenin ya da tehdidin gerçekleşmesi gerekir. Genel olarak bilgi varlıklarına zarar verebilecek her türlü olay ya da tehlike tehdit olarak tanımlanır. Tehditler genel olarak iş süreçleri ve varlıklar temelli oluşur.

T1	XYZ Kurumu Sistem Odası Sistemlerine Fiziksel Olarak Yetkisiz Erişim Gerçekleştiren Saldırganlar
T2	XYZ Kurumu Sistemlerine XYZ Kurumu Ağı Üzerinden Yetkisiz Erişim Gerçekleştiren Saldırganlar
T3	XYZ Kurumu ana merkezi ile Bölge Ofisi arasındaki VLAN'nın yer aldığı kiralık hatta şebek üzerinden sızan saldırganlar
T4	XYZ Kurumu Erişime Yetkili İç Tehditler
T5	KAMUNET Ağı Yetkili Erişim Sahibi İç Tehditler
T6	XYZ Kurumu Sistem Odası Sistemlerine Fiziksel Olarak Erişim Yetkisi Olan Ancak Mevcut Topoloji Bileşenlerine Erişim Yetkisi Olmayan Saldırganlar

Sistem bileşenlerine yönelik hazırlanan tehditler dışında kalan diğer fiziksel, personel, doğal vb. tehditler kapsam dışı bırakılmıştır. Bahse konu tehditlere ilişkin tedbirler XYZ Kurumu Güv. Talimatında yer almaktadır.

c. Açıklıklar (Zafiyetler)

Açıklık (zafiyet) tehditlerle birlikte risklerin oluşmasına etki eden diğer bir unsurdur. Tehditlerden etkilenen varlıklar riski doğurmakta, varlıkların tehditlere karşı zayıf yönlerini açıklıklar oluşturmaktadır.

A1	Sistem yöneticilerinin yanlış konfigürasyonu/Güncelleme geçilmemesi/sıfırıncı gün atakları sonucu XYZ Kurumu güvenlik duvarına ağ üzerinden yetkisiz erişim sağlanması

A2	Sistem yöneticilerinin yanlış konfigürasyonu/Güncelleme geçilmemesi/sıfırıncı gün atakları XYZ Kurumu ana merkezi ile Bölge Ofisi arasındaki VLAN'nın yer aldığı kiralık hatta sızma
A3	XYZ Kurumu Bölge Ofisinde yer alan XYZ Kurumu ağı sistemlerine gerekli fiziki/bilgi sistem güvenlik tedbirlerinin uygulanmaması sonucu yetkisiz kişilerce fiziksel erişim sağlanması
A4	XYZ Kurumu sistem odasında yer alan XYZ Kurumu Ağı bileşenlerine XYZ Kurumunca belirlenen ve işletilen fiziksel güvenlik tedbirlerinin dikkatsizlik/tedbirsizlik/bilerek eksik uygulanması sonucu fiziksel erişim sağlanarak sisteme müdahale edilmesi
A5	Sistem yöneticilerinin yanlış konfigürasyonu/Güncelleme geçilmemesi/sıfırıncı gün atakları sonucu XYZ Kurumu Bölge Ofisi Güvenlik Duvarına ağ üzerinden yetkisiz erişim sağlanması

3. RİSK SENARYOLARI ve RİSK ÇÖZÜMLEMELERİ

Senaryo-1 XYZ Kurumu sistem odasında yer alan sistem bileşenlerine fiziksel olarak yetkisiz yada fiziksel olarak yetkili ancak mevcut topolojiye erişim yetkisi olmayan kişilerce fiziksel erişim sağlanması

Kullanılan Açıklıklar	**A4** XYZ Kurumu sistem odasında yer alan XYZ Kurumu Ağı bileşenlerine XYZ Kurumunca belirlenen ve işletilen fiziksel güvenlik tedbirlerinin dikkatsizlik/tedbirsizlik/bilerek eksik uygulanması sonucu fiziksel erişim sağlanarak sisteme müdahale edilmesi
Etkilenen Varlıklar	V1 KAMUNET Ağı Güvenlik Duvarı V2 XYZ Kurumu Güvenlik Duvarı V8 KAMUNET Ağı V9 XYZ Kurumu Ağı

<table>
<tr><td>Tehidler</td><td colspan="7">T1 XYZ Kurumu Sistem Odası Sistemlerine Fiziksel Olarak Yetkisiz Erişim Gerçekleştiren Saldırganlar

T4 XYZ Kurumu Erişime Yetkili İç Tehditler

T6 XYZ Kurumu Sistem Odası Sistemlerine Fiziksel Olarak Erişim Yetkisi Olan Ancak Mevcut Topoloji Bileşenlerine Erişim Yetkisi Olmayan Saldırganlar</td></tr>
<tr><td>Risk Senaryosu</td><td colspan="7">T1,T4,T6 tarafından XYZ kurumunca belirlenen ve işletilen fiziksel güvenlik tedbirlerinin dikkatsizlik/tedbirsizlik/bilerek eksik uygulanması V1,V2,V8,V9’a fiziksel erişim sağlanması sonucu sistemin gizilik, bütünlük ve erişilebilirliğinin engellenmesi.</td></tr>
<tr><td rowspan="2">Risk Değeri=Olasılık X Etki Değeri</td><td colspan="3">Etki Değeri</td><td>Olasılık Değeri</td><td colspan="3">Risk Değeri</td></tr>
<tr><td>G</td><td>B</td><td>E</td><td rowspan="2">Çok Az İhtimalle (1)</td><td>G</td><td>B</td><td>E</td></tr>
<tr><td>5</td><td>5</td><td>5</td><td>5</td><td>5</td><td>5</td></tr>
<tr><td>Risk Çözümleme</td><td colspan="7">Risk senaryosunun gerçekleşmesi durumunda saldırganlar sistemlerin yönetim portlarına bağlanması durumunda ilgili portların MAC adresi kilitlenmesi ile korunması nedeniyle erişim sağlanamayacaktır. Bahse konu sistem de aşıldığında sistem kullanıcı arayüzleri karmaşık parola ve kullanıcı adı ile korunduğundan sisteme erişim engellenecektir. Sistemin hasara uğratılması ise sistem odaları nöbetçi personel tarafından 7/24 izlenmesi nedeniyle tespit edilecektir. Ayrıca ilgili sistemler PRTG ve SIEM ürünleri ile izlenmekte erişilebilirliğin kesilmesi durumunda ilgili sistem yöneticileri uyarılmaktadır.</td></tr>
<tr><td rowspan="3">Çözümleme Sonrası Artık Risk Değeri=Olasılık X Etki Değeri</td><td colspan="3">Etki Değeri</td><td>Olasılık Değeri</td><td colspan="3">Risk Değeri</td></tr>
<tr><td>G</td><td>B</td><td>E</td><td rowspan="2">Çok Az İhtimalle (1)</td><td>G</td><td>B</td><td>E</td></tr>
<tr><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td></tr>
</table>

Senaryo-2 Sistem yöneticilerinin yanlış konfigürasyonu/Güncelleme geçilmemesi/sıfırıncı gün atakları XYZ Kurumu ana merkezi ile Bölge Ofisi arasındaki VLAN'nın yer aldığı kiralık hatta sızma

<table>
<tr><td>Kullanılan Açıklıklar</td><td colspan="7">A2 Sistem yöneticilerinin yanlış konfigürasyonu/Güncelleme geçilmemesi/sıfırıncı gün atakları XYZ Kurumu ana merkezi ile Bölge Ofisi arasındaki VLAN'nın yer aldığı kiralık hatta sızma</td></tr>
<tr><td>Etkilenen Varlıklar</td><td colspan="7">V1 KAMUNET Ağı Güvenlik Duvarı
V2 XYZ Kurumu Güvenlik Duvarı
V8 KAMUNET Ağı
V9 XYZ Kurumu Ağı</td></tr>
<tr><td>Tehidler</td><td colspan="7">T2 XYZ Kurumu Sistemlerine XYZ Kurumu Ağı Üzerinden Yetkisiz Erişim Gerçekleştiren Saldırganlar
T3 XYZ Kurumu ana merkezi ile Bölge Ofisi arasındaki VLAN'nın yer aldığı kiralık hatta şebek üzerinden sızan saldırganlar</td></tr>
<tr><td>Risk Senaryosu</td><td colspan="7">T2,T3 tarafından kiralık hattın bileşenlerinin güncellemlerin yapılmaması, yanlış konfigürasyonu, sıfırıncı gün atakları, hattın kiralandığı şirket personelinin hatası yada bilerek gerçekleştirdiği faaliyetler sonucu V1,V2,V8,V9'a erişim sağlanarak sistemin gizilik, bütünlük ve erişilebilirliğinin engellenmesi.</td></tr>
<tr><td rowspan="3">Risk Değeri=Olasılık X Etki Değeri</td><td colspan="3">Etki Değeri</td><td rowspan="2">Olasılık Değeri</td><td colspan="3">Risk Değeri</td></tr>
<tr><td>G</td><td>B</td><td>E</td><td>G</td><td>B</td><td>E</td></tr>
<tr><td>5</td><td>5</td><td>5</td><td>Çok Az İhtimalle (1)</td><td>5</td><td>5</td><td>5</td></tr>
<tr><td>Risk Çözümleme</td><td colspan="7">Kiralık hattın her iki ucunda da fiziksel güvenlik duvarları mevcut olup gelen zararlı trafik engellenecektir. Tüm güvenlik bileşenleri merkezi olarak izlenmekte güvenlik olayları için gerekli alarmlar üretilmektedir.</td></tr>
</table>

Çözümleme Sonrası Artık Risk Değeri=Olasılık X Etki Değeri	Etki Değeri			Olasılık Değeri	Risk Değeri		
	G	B	E	Çok Az İhtimalle (1)	G	B	E
	3	3	3		3	3	3

Tehdit, Açıklık ve Varlık Etkileşim Tablosu

Tehdit	**Kullandığı Açıklık**	**Etkilenen Varlıklar**
T1	A2,A4,A6,A10	V1,V2V3,V4,V5,V6,V8,V9
T2	A1,A2,A4,A6,A10	V1,V2,V8,V9
T3	A1,A3,A5,A7,A8,A9,A11	V1,V2,V3,V4,V5,V6,V8, V9
T4	A1,A3,A5,A7,A8,A9,A11	V1,V2,V3,V4,V5,V6, V8,V9
T5	A1,A2,A4,A6,A10	V1, V2, V3,V4,V5,V6,V7
T6	A1,A3A5,A7,A8,A9,A11	V1,V2, V3,V4,V5,V6,V7,V8,V9
T7	A1,A3,A5,A7,A8,A9,A11	V1,V2, V3,V4,V5,V6,V7,V8,V9
T8	A2,A4,A6,A10	V1,V2,V3,V4,V5,V6,V8,V9

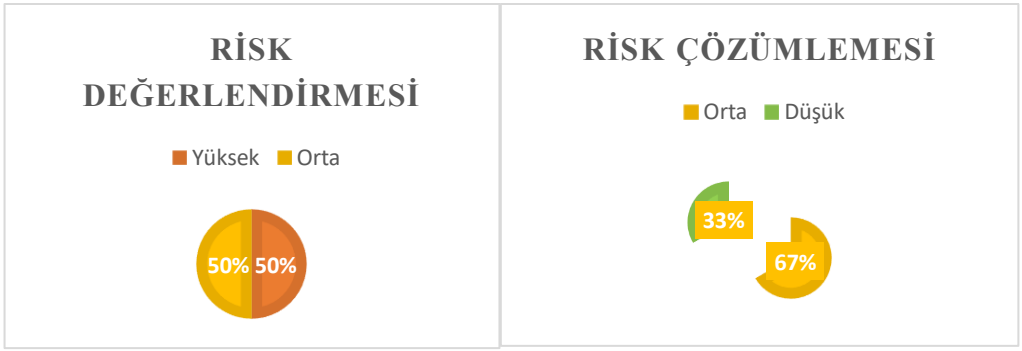
Risk Çözümlemesi Özet Tablosu

Riskler	Etkilenen Varlık	Risk Değeri	Çözümleme Risk Değeri
Senaryo-1 XYZ Kurumu sistem odasında yer alan sistem bileşenlerine fiziksel olarak yetkisiz yada fiziksel olarak yetkili ancak mevcut topolojiye erişim yetkisi olmayan kişilerce fiziksel erişim sağlanması	V1 KAMUNET Ağı Güvenlik Duvarı V2 XYZ Kurumu Güvenlik Duvarı V8 KAMUNET Ağı V9 XYZ Kurumu Ağı	Orta(5)	Düşük(3)
Senaryo-2 Sistem yöneticilerinin yanlış konfigürasyonu/Güncelleme geçilmemesi/sıfırıncı gün atakları XYZ Kurumu ana merkezi ile Bölge Ofisi	V1 KAMUNET Ağı Güvenlik Duvarı V2 XYZ Kurumu Güvenlik Duvarı V8 KAMUNET Ağı	Yüksek (8)	Orta(4)

arasındaki VLAN'nın yer aldığı kiralık hatta sızma	V9 XYZ Kurumu Ağı		

4. SONUÇ

Mevcut topolojiye yönelik 6 adet risk tespit edilmiştir. 3 Adet yüksek ve 3adet orta seviye risk bulunmaktadır. Risk Çözümlemesi sonucunda 3 adet yüksek risk orta seviyeye azaltılmış, 2 adet orta seviye risk düşük seviye azaltılmış, 1 adet orta seviye risk puanı düşmesine rağmen (5'ten 4'e) orta seviyede kalmıştır.



ETİK KURUL/KOMİSYON MUAFİYET FORMU

ORJİNALLİK RAPORU