İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

TÜRKİYE'NİN ULUSAL SİBER GÜVENLİK STRATEJİ VE POLİTİKALARININ OLUŞTURULMASI ÇERÇEVESİNDE CAYDIRICILIK

DOKTORA TEZİ

Mustafa ŞENOL

Bilişim Uygulamaları Anabilim Dalı

Bilgi Güvenliği Mühendisliği ve Kriptografi Programı

TEMMUZ 2020

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

TÜRKİYE'NİN ULUSAL SİBER GÜVENLİK STRATEJİ VE POLİTİKALARININ OLUŞTURULMASI ÇERÇEVESİNDE CAYDIRICILIK

DOKTORA TEZİ

Mustafa ŞENOL

(707152004)

Bilişim Uygulamaları Anabilim Dalı

Bilgi Güvenliği Mühendisliği ve Kriptografi Programı

Tez Danışmanı: Prof. Dr. Ertuğrul KARAÇUHA

TEMMUZ 2020

İstanbul Teknik Üniversitesi Bilişim Enstitüsü'nün 707152004 numaralı Doktora Öğrencisi Mustafa ŞENOL, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "TÜRKİYE'NİN ULUSAL SİBER GÜVENLİK STRATEJİ VE POLİTİKALARININ OLUŞTURULMASI ÇERÇEVESİNDE CAYDIRICILIK" başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı :	**Prof. Dr. Ertuğrul KARAÇUHA** İstanbul Teknik Üniversitesi	……..……
Jüri Üyeleri :	**Prof. Dr. Oğuzhan KÜLEKÇİ** İstanbul Teknik Üniversitesi	……..……
	Prof. Dr. Mustafa ALKAN Gazi Üniversitesi	……..……
	Prof. Dr. Şahin Serhat ŞEKER İstanbul Teknik Üniversitesi	……..……
	Prof. Dr. Şeref SAĞIROĞLU Gazi Üniversitesi	……..……

Teslim Tarihi : 07 Temmuz 2020

Savunma Tarihi : 30 Temmuz 2020

Değerli Eşime ve Sevgili Kızıma,

ÖNSÖZ

Doktora yapmam için isteklendiren, doktora eğitimim, tez konumun belirlenmesi, araştırılması ve yazımı sırasında değerli bilgilerini ve zamanını benden esirgemeyen ve tez sürecim boyunca sahip olduğu bilgi birikimi ve deneyimleri ile çalışmamı yönlendiren, her türlü desteği ve yardımı sunan değerli danışmanım Prof. Dr. Ertuğrul KARAÇUHA'ya sonsuz teşekkürlerimi ve şükranlarımı sunarım.

Doktora öğrencisi olarak derslerine katılma fırsatı bulduğum, bilgi ve deneyimlerini benimle paylaşan, görüş ve önerileriyle çalışmamalarımı yönlendiren başta değerli hocam Prof. Dr. Eşref ADALI olmak üzere, Doç. Dr. Enver ÖZDEMİR ve Dr. Nafiz ÜNLÜ ile Dr. Çiçek ERSOY'a, tezimin hazırlanmasında yol gösterici önerileri ile bazı çalışmalarımın yayımlanması sırasında her türlü destek, katkı ve yönlendirmeleri dolayısıyla Prof. Dr. Şeref SAĞIROĞLU'na çok teşekkür ederim.

Tez çalışmalarımın izlenmesinde ve yönlendirilmesinde değerli katkılarından dolayı Tez İzleme Komitesi Üyeleri Prof. Dr. M. Oğuzhan KÜLEKÇİ ile Prof. Dr. Mustafa ALKAN'a ve Tez Savunma Jüri Üyesi Prof. Dr. Ş. Serhat ŞEKER'e en içten teşekkürlerimi sunarım.

Ayrıca, doktora eğitimi almam için beni isteklendirmekle kalmayıp yönlendiren ve çalışmalarım boyunca her türlü destekleriyle beni hiçbir zaman yalnız bırakmayan değerli eşime ve sevgili kızıma sonsuz teşekkür ederim.

Temmuz 2020 Mustafa ŞENOL

İÇİNDEKİLER

Sayfa

KISALTMALAR

ABD : Amerika Birleşik Devletleri
AK : Avrupa Konseyi
Ar-Ge : Araştırma ve Geliştirme
ATM : Automated Teller Machine (Otomatik Vezne Makinesi)
BGYS : Bilgi Güvenliği Yönetim Sistemi
BM : Birleşmiş Milletler
BSO : Bilgi Sistem Olayı
BSTB : Bilim Sanayi ve Teknoloji Bakanlığı
BT : Bilgi Teknolojileri
BTK : Bilgi Teknolojileri ve İletişim Kurumu
CB : Cumhurbaşkanlığı
CCD COE : Cooperative Cyber Defence Centre of Excellence (Müşterek Siber Savunma Mükemmeliyet Merkezi)
CIA : Confidentiality, Integrity, Availability (Gizlilik, Bütünlük, Erişebilirlik)
CISA : Cybersecurity and Infrastructure Security Agency (Siber Güvenlik ve Altyapı Güvenliği Başkanlığı)
CİMER : Cumhurbaşkanlığı İletişim Merkezi
COBİT : Control Objectives for Information and Related Technology (Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri)
CSC : Cyber Security Coordinator (Siber Güvenlik Koordinatörü)
DDoS : Distributed Denial of Service (Dağıtık Servis Dışı Bırakma)
DHS : Department of Homeland Security (İç Güvenlik Bakanlığı)
DISA : Defence Information Systems Agency (Savunma Bilgi Sistemleri Başkanlığı)
DLP : Data Leakage Prevention (Veri Sızıntısı Önleme)
DNI : Director of National Intelligence (Ulusal İstihbarat Direktörü)
DNS : Domain Name System (Alan Adı Sistemleri)
DoD : Department of Defence (Savunma Bakanlığı)
DoS : Denial of Service (Servis Dışı Bırakma)
ENISA : European Union Agency for Cybersecurity (Avrupa Ağ ve Bilgi Güvenliği Ajansı)
FBI : Federal Bureau of Investigation (Federal Soruşturma Bürosu)
GA : God'sApstls (Tanrının Havarileri)
GoP : Guardians of Peace (Barışın Savunucuları)
GPS : Global Positioning System (Küresel Konumlama Sistemi)
ICI-IPC : Information and Communications Infrastructure Interagency Policy Committee (Bilgi ve İletişim Altyapısı Uyumluluk Politikası Komitesi)
IEC : International Electrotechnical Commission (Uluslararası Elektroteknik Komisyonu)
İHA : İnsansız Hava Aracı

IP : Internet Protocol (İnternet Protokolü)
ISO : International Organization for Standardization (Uluslararası Standartlar Teşkilâtı)
ITU : International Telecommunication Union (Uluslararası Telekomünikasyon Birliği)
KHK : Kanun Hükmünde Kararname
KVK : Kişisel Verileri Koruma Kurumu
MASAK : Mali Suçları Araştırma Kurumu
MEBS : Muhabere, Elektronik, Bilgisayar Sistemleri
MGK : Milli Güvenlik Kurulu
MGSB : Milli Güvenlik Siyaset Belgesi
MİT : Milli İstihbarat Teşkilatı
M.Ö. : Milattan Önce
M.S. : Milattan Sonra
MSG : Milli Siber Güvenlik
MSGB : Milli Siber Güvenlik Başkanlığı
NATO : North Atlantic Treaty Organization (Kuzey Atlantik Paktı Teşkilatı)
NCCIC : National Cybersecurity and Communications Integration Centre **(**Ulusal Siber Güvenlik ve İletişim Uyum Merkezi)
NCSS : National Cyber Security Strategy (Ulusal Siber Güvenlik Stratejisi)
NSA : National Security Agency (Ulusal Güvenlik Ajansı)
OECD : Organisation for Economic Co-operation and Development (Ekonomik Kalkınma ve İşbirliği Örgütü)
PDCA : Plan, Do, Check, Act (Planla, Uygula, Kontrol et, Önlem al)
POS : Point of Sale (Satış Noktası)
PUKÖ : Planla, Uygula, Kontrol et, Önlem al
RF : Rusya Federasyonu
SG : Siber Güvenlik
SGKK : Siber Güvenlik Koordinasyon Kurulu
SGUDK : Siber Güvenlik Uzmanları Danışma Kurulu
SGYS : Siber Güvenlik Yönetim Sistemi
SOME : Siber Olaylara Müdahale Ekibi
TBMM : Türkiye Büyük Millet Meclisi
TDK : Türk Dil Kurumu
TEİAŞ : Türkiye Elektrik İletim Anonim Şirketi
TİB : Telekomünikasyon İletişim Başkanlığı
TSK : Türk Silahlı Kuvvetleri
TUİK : Türkiye İstatistik Kurumu
TÜBİTAK : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UAB : Ulaştırma ve Altyapı Bakanlığı
UDH : Ulaştırma, Denizcilik ve Haberleşme
UDHB : Ulaştırma, Denizcilik ve Haberleşme Bakanlığı
UEKAE : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
US-CERT : United States Computer Emergency Readiness Team (ABD Siber olaylar Acil Durum Hazırlık Ekibi)
USCYBERCOM : United States Cyber Command (ABD Siber Komutanlığı)
USOM : Ulusal Siber Olaylara Müdahale Merkezi

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

TÜRKİYE'NİN ULUSAL SİBER GÜVENLİK STRATEJİ VE POLİTİKALARININ OLUŞTURULMASI ÇERÇEVESİNDE CAYDIRICILIK

ÖZET

Teknolojinin, özellikle bilgisayarların icadı sonrasında, her geçen gün daha hızlı gelişen bilgi sistemleri ve iletişim teknolojileriyle, internetin keşfi, gelişmesi ve yaygınlaşmasıyla, haberleşme, finans, enerji ve güvenlik gibi çok önemli faaliyetlerin bilgi sistemleri üzerinden yürütülmesi sonucu sağlanan kolaylıklar ve kazanımlarla bilişim sistemleri dünyada günlük yaşamın vaz geçilmez bir parçası olmuştur.

Bilişim sistemleri günlük yaşamın vaz geçilmezi olurken, siber ortamın önemi her geçen gün daha da artmış ve artmaya da devam etmektedir. Bu kapsamda siber ortamda bilgilere ve bilişim sistemlerine yönelik olarak başlayan kötü niyetli hareketlerin ve saldırıların da her geçen gün çeşitleri ve şiddetleri de artmaktadır. Devletler siber ortamı daha etkin kullanmanın yanında oluşan tehdit ve tehlikelere karşı koymak için strateji ve politikalar geliştirmeye ve bunları uygulamaya başlamışlardır.

Türkiye'de de bilgisayarların kullanımının artması ve internetin de yaygınlaşmasıyla, dünyadaki gelişmelere paralel olarak ortaya çıkan olumsuzlukların giderilmesi için başlatılan çalışmalarla geçmişten bugüne çok önemli mesafeler kat edilmiştir. Bu kapsamda oluşturulan ulusal siber güvenlik strateji ve politikalarıyla ilgili eksiklik ve yetersizliklerin giderilerek etkinliğinin artırılması yanında, siber caydırıcılık konusunun da siber güvenlik strateji ve politikaları ile birlikte bütüncül bir yaklaşımla ele alınmasının uygun olacağı değerlendirilmiştir.

Türkiye'de siber ortamda sahip olunan değerli varlıkların, bilgi ve iletişim sistemleri ile altyapılarının siber güvenliğinin etkinlikle sağlanabilmesi, ulusal siber güvenliğin Türkiye için öneminin ve ulusal güvenliğinin ayrılmaz bir parçası olduğunun ortaya konulması, siber savaş (savunma, taarruz ve caydırıcılık) için etkili bir güç olunabilmesi, ulusal siber gücün geliştirilerek, tek başına ve / veya diğer ulusal güç unsurlarıyla birlikte, caydırıcılık sağlayacak şekilde kullanılması ve siber alanda belirlenecek hedeflere ulaşılabilmesi maksatlarıyla ihtiyaç duyulan ulusal siber güvenlik strateji ve politikaların nasıl hazırlanması ve etkinlikle nasıl uygulanması gerektiği konusunda ilgili kişi, kurum ve kuruluşlara yol gösteren bir kaynak olarak yapılacak çalışmalara ışık tutulması amaçlanmıştır.

Bu amaç doğrultusunda; konuyla ilgili yapılan akademik çalışmalar, dünyada konuyla ilgili önde gelen devletlerin siber güvenlik strateji ve politikaları ile Türkiye'nin konuyla ilgili çalışmaları, uygulamaları ve sonuçları incelenmiş, geçmişten günümüze yaşanan olaylardan çıkarılan derslerle geleceğin ihtiyaç ve hedeflerine yönelik öngörülerde bulunularak, Türkiye'nin aynı zamanda caydırıcılık da sağlayacak siber

güvenlik strateji ve politikalarının bilimsel yaklaşım ve yöntemlerle oluşturulması ve uygulanmasına yönelik esas ve prensiplerin belirlenmesine çalışılmıştır.

Bu kapsamda, bilgi, bilgisayar ve iletişim sistemleri ve bu konulardaki gelişmeler tarihi bir bakış açısıyla incelenirken, bilişim sistemleri ve güvenliği ile ilgili teknik kavramlarla, siber uzay, siber saldırı, siber taarruz, siber suç, siber terörizm, siber güvenlik, siber savunma, siber savaş, siber istihbarat, siber güç vb. kavramlar, siber güvenlik strateji ve politikaları ile siber caydırıcılık konularında, yerli ve yabancı hakemli dergiler ve akademik yayınlar başta olmak üzere, konuyla ilgili kurum ve kuruluşların yayınları ve belgeleri, kitaplar, dergiler, kütüphane ve internet ortamları taranmış, gelişmelerin takibi bağlamında çeşitli konferans ve çalıştaylara katılım sağlanmış, konuyla ilgili kurum ve kuruluş yetkilileri ile görüşmelerde bulunulmuştur.

Bu çerçevede; Strateji ve Güvenlik konusunda 20'nin üzerinde kitap, doküman ve çalışma, Siber Güvenlik ve Stratejisi konusunda 30'un üzerinde kitap, doküman ve çalışma, Dünya Ülkeleri Siber Güvenlik Strateji Belgeleri ve Eylem Planları konusunda başta ABD, Çin, Rusya, Fransa, İngiltere, İsrail, Hindistan, Kuzey Kore, Almanya, Kanada, Hollanda, Finlandiya, Japonya, Avustralya ve İran olmak üzere 20'ye yakın ülkenin belgeleri, Türkiye Siber Güvenlik Stratejileri ve Eylem Planları konusunda başlangıçtan bugüne hazırlanarak uygulamaya konulan 17 strateji belgesi ve eylem planı, Caydırıcılık ve Siber Caydırıcılık konusunda 30'un üzerinde kitap, doküman ve çalışma incelenmiş, konuyla ilgili gelişmelerle ilgili seminer, sempozyum, panel, çalıştay ve konferanslar kapsamında 20'nin üzerinde etkinliğe katılım sağlanmıştır.

İncelemeler sonrası analiz ve düzenleme çalışmaları yapılarak, İstanbul Teknik Üniversitesi Lisansüstü Tez Yazım Kılavuzu ve Lisans Üstü Tez Şablonu esasları doğrultusunda hazırlanan tezin içeriği 7 ana bölümden oluşmuştur.

Giriş bölümünde; bilgi ve iletişim sistemleri konusunda gelişmeler ile yaşanan kötü niyetli hareket ve saldırılara karşı ulusal siber güvenliğin sağlanması için strateji ve politikaların geliştirilmesi önemi ve ihtiyacı açıklanmıştır.

Siber güvenlikle ilgili terim ve kavramlar bölümünde; siber güvenlik konusunun bütüncül bir yaklaşımla ele alınarak doğru anlaşılması için öncelikle terim ve kavram birliği sağlanması, ortaya çıkan kavramlarla ilgili gelişmelerin bilinmesinin önemi doğrultusunda, konuyla iç içe olan ve en çok kullanılan terim ve kavramlar tanımlanarak kısaca açıklanmıştır

Siber savaş bölümünde; siber ortamda yaşanan siber saldırılar ve taarruzlar sonucunda siber güvenliğin ulusal güvenlik sorunu ve ulusal güvenliğin ayrılmaz bir parçası olduğu görüşünü destekleyen, geçmişte başlayan, günümüzde devam eden ve gelecekte de artarak devam edecek olan siber saldırı ve savaşlarla ilgili bilgiler verilmiştir.

Siber caydırıcılık bölümünde; geçmişten günümüze siber olay, saldırı ve savaşlardan da örnekler verilerek, savaşlarda kazanmaktan çok caydırıcılığın daha iyisi olabileceği düşüncesi ile siber güvenlik uygulamalarında dünyada çok yeni olan, Türkiye'de ise yeterli önem ve önceliğin verilmediği görülen bu konuda yaklaşımlar ortaya konmuştur.

Ulusal siber güvenlik strateji ve politikaları bölümünde; strateji ve politika kavramları açıklanmış, kurumsal ve ulusal siber güvenlik stratejileri ile bu konuda önde gelen ülkelerin ve Türkiye'nin mevcut siber güvenlik strateji ve politikaları hakkında bilgiler verilmiştir.

Caydırıcılık sağlayacak siber güvenlik strateji ve politikalarının oluşturulması bölümünde; ulusal siber güvenlikte söz sahibi ülkelerin ulusal siber güvenlik strateji belgeleri ile bazı uluslararası kurumların çalışmalarından elde edilen bilgilerden hareketle, Türkiye için mevcut stratejiler ve eylem planları da dikkate alınarak, caydırıcılık da sağlayacak ulusal siber güvenlik stratejisi ve politikalarının hazırlanması ve uygulanması için bir yaklaşım tarzı ortaya konmuştur.

Sonuç ve öneriler bölümünde; tez konusu kapsamında yapılan çalışmanın sonuçları ve yapılan değerlendirme ile görüş ve öneriler sunulmuştur.

Bu tez ile ortaya konulan ve önerilen yaklaşım tarzı; bilimsel taktik ve teknikler çerçevesinde, mevcut durumun değerlendirilmesinden belirlenen hedefe ulaşılmasına kadar teşkilat, kapsam, planlama ve uygulama aşamaları ile süreç içerisinde kontrol ve denetim faaliyetleri ile geliştirme faaliyetlerini içeren 8 aşamalı "Ulusal Siber Güvenlik Stratejisi Oluşturma ve Uygulama Yaşam Döngüsü"dür.

Ayrıca bu yaşam döngüsü içerisinde, bu döngüden, yani 'Ulusal Siber Güvenlik Stratejisinden ve Siber Gücün Yönetiminden', ana sorumlu olarak ve 2016-2019 Ulusal Siber Güvenlik Stratejisinde vurgulanan ve Türkiye'de halâ eksikliği görülen "Siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesi" ihtiyacını da karşılamak üzere, mevcut yönetim sisteminde Cumhurbaşkanlığına bağlı, "Milli Siber Güvenlik Başkanlığı" yapılanması önerilmektedir.

DETERRENCE WITHIN THE FRAMEWORK OF CREATING TURKEY'S NATIONAL CYBER SECURITY STRATEGIES AND POLICIES

SUMMARY

With the rapid development of technology, especially computers and communication systems, with the discovery and widespread of the Internet, conveniences and achievements provided by the information and communication systems, that is, the informatics systems and infrastructures have made informatics systems and services indispensable in people's lives all around the world. The effectiveness and efficiency attained in the processing, transmission, sharing, using, storage, and protection of information, which is the most important asset for humanity since the beginning of history, has increased and continues to increase day by day.

Parallel to these developments, the improvements of government's powers, particularly in the economic, political, and military fields that have taken place in shortest time, have made the cyber space, which is a combination of physically and virtually valuable assets, more important. The cyber space has become to be referred to as the 5th operational domain after land, sea, air, and space operation domain. As the importance of cyberspace increases, malicious movements and attacks that have come with the development of information and informatics systems continue to increase rapidly today.

While the facilities and conveniences provided by the cyberspace with the developments in information and communication technologies make life more dependent on such facilities and conveniences every day, significant damages that individuals, societies, and countries have suffered as a result of the use of cyber space for threats, attacks, to harm life and property, and similar malicious purposes, have caused great changes in the understanding of the notion of security. In this context, it has started to be accepted that cyber security is a national security issue and an integral part thereof.

Measures are considered and strategies and policies are being developed to preventing cyber attacks initiated by using means of cyber power, informatics systems and infrastructures that are required for the initiation and maintenance of cyber war and are attained in cyberspace and the ability to use them effectively, and wars caused by cyber attacks, and to dissuade those who think about cyber attacks or war to pursue such thoughts and actions.

Governments are trying to carry out various works in the fields of cyber security, cyber warfare, and cyber deterrence, to evaluate the situation within the framework of technological developments, take measures by identifying risks and threats, make targets in line with their needs by making predictions for the future, develop strategies and policies and implement them effectively.

With the increase in the use of computers, and the widespread of the Internet, which is a constantly growing communication and information communication network

around the world, significant progresses have been attained in Turkey compared to the past with the works initiated to prevent and eliminate the risks, threats, dangers, etc. that occur in parallel with the developments in the world. In this context, besides increasing the efficiency by eliminating the deficiencies and inadequacies related to cyber security strategies and policies against cyber attacks and incidents, it is thought that it would be appropriate to address the issue of cyber deterrence, which is recently a hot topic of conversation and study, with a holistic approach along with cyber security strategies and policies.

Significant progresses have been made from the past to present with studies initiated to prevent and eliminate the negativity emerging in parallel with the developments in the world, and with the increasing use of computers and the Internet becoming more widespread in Turkey as well.

In addition to increasing the effectiveness by eliminating the deficiencies and inadequacies related to the national cyber security strategies and policies created within this scope, it was evaluated that it would be appropriate to address the issue of cyber deterrence with an integrated approach together with cyber security strategies and policies.

Based on the thoughts put forward, in this study it is aimed to answer what ways should be followed to develop a needed strategy and how this strategy should be developed in order to ensure effectiveness of the cyber security of assets, information and communication systems and infrastructures owned in a country in cyberspace, to become an effective power for cyber war and deterrence and to create a summary resource for the studies to be carried out.

As a method, to facilitate an understanding of the subject and to provide term unity, first, basic concepts related to the subject have been discussed, certain studies in Turkey and abroad are reviewed and brief samples are provided and discussed. Later, an approach regarding the guidelines, principles, and procedures for the establishment of a national cyber security strategy and the development and implementation of the existing one is presented and opinions are evaluated.

In this context, the information, computer and communication systems and developments in these issues are examined from a historical perspective; primarily peer-reviewed academic publications and journals, publications and documents of relevant institutions and organizations, books, magazines, library and internet environments were scanned about cyber space, cyber attacks, cyber crime, cyber terrorism, cyber security, cyber defence, cyber warfare, cyber intelligence, cyber power, etc. concepts, cyber security strategies and policies, and cyber deterrence with technical concepts related to information systems and security, for following of developments, various conferences and workshops were participated, and meetings were held with the relevant institutions and organizations.

In this context; on Strategy and Security, more than 20 books, documents and studies; on Cyber Security and Strategy over 30 books, documents and studies; on Cyber Security Strategy Documents and Action Plans documents of nearly 20 countries, primarily USA, China, Russia, France, England, Israel, India, North Korea, Germany, Canada, Netherlands, Finland, Japan, Australia and Iran; on Turkey's National Cyber Security Strategies and Action Plans, from beginning to present, preparing the implementation 17 strategy documents and action plans; on Deterrence and Cyber Deterrence, over 30 books, documents and studies have been examined; Seminars,

symposiums, panels, workshops and conferences related to developments on the subject, more than 20 events were participated.

After researching, analysing and editing studies have been made and the content of this thesis consists of 7 Main Sections stated below, which has been prepared in accordance with the principles of Istanbul Technical University Postgraduate Thesis Writing Guide and Postgraduate Thesis Template.

In the Introduction section, the importance and need to develop strategies and policies to provide national cyber security against malicious acts and attacks experienced with the developments in information and communication systems have been explained.

In Terms and Concepts Related to Cyber Security, the most used terms and concepts that are closely intertwined with the subject are defined and briefly explained in order to correctly understand the cyber security issue with a holistic approach providing a term and concept unity.

In Cyber War, information is provided on cyber attacks and wars that started in the past that continue today and will continue increasingly in the future, which support the view that cyber security is an integral part of national security, and national security as a result of cyber attacks and attacks in cyber environment.

In Cyber Deterrence, it is discussed that a common approach in terms of deterrence is very new in cyber security applications in the world, but adequate attention and priority was not given in Turkey; examples from wars from the past to present are given, explaining the idea that deterrence might be better rather than winning in wars

In National Cyber Security Strategy and Policies, strategy and policy concepts are explained, information is provided about current cyber security strategies and policies of leading countries in this regard and Turkey with intuitional and national cyber security strategies

In Creating Cyber Security Strategies and Policies to Provide Deterrence, an approach style has been put forward for the preparation and implementation of the national cyber security strategy and policies that will also provide deterrence for Turkey, considering existing strategies and action plans, based on the information obtained from the studies of some international institutions with national cyber security strategy documents of countries leading in national cyber security.

In Conclusions and Suggestions, results of the conducted study within the scope of the thesis topic, the evaluation, and opinions and suggestions were presented.

The approach presented and proposed with this thesis is, an 8-stage cycle; “Creating and Implementing the National Cyber Security Strategy Life Cycle”, beginning with the assessment of the current situation, followed by the achievement of the specified goal, organization, scope, planning and implementation stages including control and audit activities and development activities in the process, within the framework of scientific tactics and techniques.

Additionally in this life cycle, the structuring of “The National Cyber Security Presidency” is recommended, as the main body responsible for this cycle, 'for managing the National Cyber Security Strategy and the Cyber Power', and to meet the needs of “a strong central public authority to ensure coordination in the field of cyber security” emphasized in the 2016-2019 National Cyber Security Strategy and still seen to be deficient in Turkey.

1. GİRİŞ

Teknolojinin, bilgisayar ve iletişim sistemlerinin hızla gelişmesi, özellikle internetin keşfi ve yaygınlaşmasıyla, bilişim sistemleri ve altyapılarının sağladığı kolaylıklar ve kazanımlar bilişim sistemlerini ve hizmetlerini bütün dünyada yaşamın vazgeçilmezleri yapmıştır. İnsanlık için tarihin başlangıcından bugüne en önemli varlık olan bilginin, elektronik ve bilişim sistemlerinin sağladığı imkânlarla, işlenmesinde, iletiminde, depolanmasında, korunmasında ve kullanılmasında sağlanan etkinlik ve verim her geçen gün daha da artmış ve artmaya da devam etmektedir.

İnternet kullanımı, 2020 yılı itibariyle 4,5 milyar kullanıcıya ulaşmış ve yaklaşık 7,7 milyarlık dünya nüfusunun yaklaşık % 59'u internet kullanmaktadır. Dünya nüfusunun % 66'sının, yaklaşık 5 milyonunun mobil telefonu (% 76'sı akıllı telefon) bulunmakta ve internet kullanımının ve iletişimin % 52'si mobil telefonlar üzerinden yapılmaktadır [1].

Telli, telsiz ve uydu sistemleri üzerinden internet dâhil yerel ve geniş ağ sistemleri ile iletişim, akıllı cihaz ve sistemlerle duyargaların (sensörlerin) kullanımının artmasını, nesnelerin interneti, bulut bilişim sistemleri, büyük veri analizi ve yapay zekâ, otonom ve robotik sistemler, akıllı evlerin ve akıllı şehirlerin insan yaşamına dâhil olması izlemiştir. Bilgi ve iletişim sistem ve teknolojilerindeki gelişmeler ile sayısal (dijital) dönüşüm ve yenileşimle (inovasyonla) devletlerin özellikle ekonomik, politik ve askeri güçlerindeki kısa sürede meydana gelen olumlu yükselişler, 5'inci Harekât Alanı olarak da adlandırılan 'Siber Uzay (Siber Ortam)'ın önemini daha da artırmıştır. Siber ortamın önemi artarken, bilgilere ve bilişim sistemlerine yönelik olarak başlayan kötü niyetli hareketler ve saldırılar günümüzde de hızla artarak devam etmektedir. Teknoloji değerlendirmeleri ve geleceğe yönelik öngörüleriyle tanınan ABD'li yazar ve gelecek bilimci Alvin Toffler'ın "Teknolojik gücümüz artıyor ancak, yan etkileri ve olası tehlikeleri bundan çok daha hızlı büyüyor" [2] sözü, konuya dikkat çekmesi ve önemini vurgulaması yanında, içinde bulunulan durumu da tek cümleyle açıklamaktadır.

Bilgi ve iletişim teknolojilerindeki gelişmelerle siber ortamın sağladığı imkân ve kolaylıklar yaşamı her geçen gün kendisine daha bağımlı hale getirirken, bilgilere ve bilişim sistemlerine yönelik her türlü kötü niyetli hareketin, siber ortamın tehdit, saldırı, cana ve mala zarar verme vb. amaçlarla kullanılması sonucunda kişilerin, toplumların ve ülkelerin uğradığı büyük zararlar güvenlik anlayışında büyük değişikliklere yol açmıştır.

Siber ortamda karşı tarafın bilgilerine ve bilgi sistemlerine yönelik zarar verme veya olumsuz etkileme istek ve ihtiyaçları 'Siber Saldırı - Siber Taarruz', bilgi ve bilişim sistemlerinin kötü niyetli hareketlere ve saldırılara karşı korunması ihtiyacı ise 'Siber Güvenlik - Siber Savunma' kavramlarını ortaya çıkarmıştır. Devletler siber savunma ve siber taarruz konularında strateji ve politikalar geliştirmeye ve bunları etkinlikle uygulamaya başlamışlar, bunlarla birlikte de 'Siber Savaş' kavramı her geçen gün daha sık konuşulur olmuştur. Bu çerçevede siber güvenliğin ulusal güvenlik sorunu ve ulusal güvenliğin ayrılmaz bir parçası olduğu yaygın kabul görmeye başlamıştır.

Siber savaşın başlatılması ve sürdürülmesi için gerekli olan, siber ortamda sahip olunan bilgi sistemleri ve alt yapıları ile bunların etkin olarak kullanılması yeteneği 'Siber Güç' imkânları kullanılarak yapılan siber saldırıları ve siber saldırıların oluşturduğu savaşları önlemek, siber saldırıyı veya savaşı düşünenleri bu düşüncelerinden ve eylemlerinden vazgeçirmek için tedbirler düşünülmekte, strateji ve politikalar geliştirilmektedir. M.Ö. 500'lü yıllarda yaşamış olan ünlü Çinli filozof ve savaş stratejisti Sun Tzu'nun "En iyisi savaşmadan baş eğdirmektir" [3] özdeyişinde olduğu gibi, saldırganları isteklerinden, saldırılardan veya savaştan caydırmak, söz konusu siber savaş olduğuna göre de 'Siber Caydırıcılık' en iyisi olabilir.

Türkiye'de de bilgisayarların kullanımı artarken, dünya çapında sürekli büyüyen bilgi iletişim ve haberleşme ağı olan internet de yaygınlaşmış, internet kullanım sayısı, 2020 yılı itibariyle 77.048.026 (83.900.373 nüfusun % 91'i) ve mobil telefon sayısı ise 82.896.108 [4] olmuştur. Telli, telsiz ve uydu sistem ağlarının yaygınlaşması, kamu ve özel yapıların sayısal dönüşümlerinin hızlanması ve yenileşim çalışmalarıyla, bütün dünyadaki gelişmelere paralel olarak ortaya çıkan siber tehdit, risk, tehlike vb. olumsuzlukların önlenmesi ve giderilmesi için başlatılan çalışmalara benzer

çalışmalarda geçmişten bugüne çok önemli mesafeler kat edilmiştir. Ancak yeterli olduklarını söylemek çok zordur ve Gazi Mustafa Kemal Atatürk'ün dediği gibi; "Felaket başa gelmeden evvel önleyici ve koruyucu tedbirleri düşünmek gerekir, geldikten sonra dövünmenin yararı yoktur." [5]

Bu kapsamda siber saldırı ve olaylara karşı oluşturulan siber güvenlik strateji ve politikalarıyla ilgili eksiklik ve yetersizliklerin giderilerek etkinliğin artırılması yanında, son dönemde sıkça konuşulmaya ve çalışmalar yapılmaya başlanılan siber caydırıcılık konusunun siber güvenlik stratejileri ve politikaları ile birlikte bütüncül bir yaklaşımla ele alınmasının uygun olacağı değerlendirilmektedir.

Ortaya konulan bu değerlendirmeden hareketle, Türkiye'de siber ortamda sahip olunan varlıkların, bilgi ve iletişim sistemlerinin ve altyapılarının siber güvenliğinin etkinlikle sağlanabilmesi, siber savaş ve caydırıcılık için etkili bir güç olunabilmesi maksatlarıyla ihtiyaç duyulan strateji ve politikaların oluşturulması için gereken çalışmalara katkı sunulması düşüncesiyle Tez Konusu; "Türkiye'nin Ulusal Siber Güvenlik Strateji ve Politikalarının Oluşturulması Çerçevesinde Caydırıcılık" şeklinde belirlenmiştir.

Çin'in Vuhan şehrinde 12 Aralık 2019'da ortaya çıkan yeni tip koronavirüs (COVID-19) salgın hastalığı, çok hızlı bir küresel yayılım göstermesi sonucu bütün dünyayı etkilemiş ve 11 Mart 2020'de Türkiye'de ilk hasta tespit edilmiştir [6]. Salgın dolayısıyla başta sokağa çıkma kısıtlamaları olmak üzere bununla bağlantılı eğitimden sağlığa, ekonomiden ulaşıma ve dolayısıyla çalışma hayatına yönelik kısıtlamalar sürecinde özellikle internet kullanımı çok artmış, bilgi ve iletişim alanına yönelik pek çok yeni ihtiyaç ortaya çıkmış ve geliştirilen yeni bilişim teknolojileri ve sistemleri kullanılmaya başlanmıştır.

Bu çerçevede özellikle uzaktan eğitim ve çalışma, görüntülü görüşme ve toplantı vb. sistem ve yazılımları ile sayısal elektronik ortamda yapılan e-devlet, e-ticaret, e-bankacılık gibi işlemler yaygınlaşarak çok daha yoğun kullanılır olmuştur. Korkunun, belirsizliklerin ve kararsızlıkların yaşandığı dönem içerisinde, siber suçlar artarken siber saldırılar da durmamıştır. Ortaya çıkan yeni tür ihtiyaçlar ve yaygınlaşan yoğun kullanımlar siber güvenliğinin önemini daha da artırırken bu alanda yeni siber güvenlik ihtiyaçlarını da ortaya çıkarmıştır.

Bu gelişmeler, tespit ve değerlendirmeler doğrultusunda, Tez Çalışmasının temel amaç ve hedefi, tezin içeriğinde yanıtlanması planlanan soruların bazıları, tezin gerçekleştirilmesi sonucunda ekonomiye, toplumsal gönence (refaha), bilimsel birikime ve ulusal güvenliğe yapılabileceği öngörülen katkılar ve sağlanabileceği düşünülen yararlar aşağıda açıklanmıştır.

1.1 Tezin Temel Amacı ve Yapısı

Tez çalışması ile ulusal siber güvenliğin Türkiye için öneminin ve ulusal güvenliğinin ayrılmaz bir parçası olduğunun ortaya konulması, ulusal siber gücü meydana getiren varlıkların etkin güvenliği için gerekli önlemlerin alınmasını sağlayacak yetkinliğin kazanılması, ulusal siber gücün geliştirilerek, tek başına ve / veya diğer ulusal güç unsurlarıyla birlikte, caydırıcılık sağlayacak şekilde kullanılması ve siber alanda belirlenecek hedeflere ulaşılabilmesi maksatlarıyla ihtiyaç duyulan ulusal siber güvenlik strateji ve politikaların nasıl hazırlanması ve etkinlikle nasıl uygulanması gerektiği konusunda ilgili kişi, kurum ve kuruluşlara yol gösteren bir kaynak olarak yapılacak çalışmalara ışık tutulması amaç ve hedeflenmiştir.

Bu amaç ve hedef doğrultusunda yapılan incelemeler sonrası analiz ve düzenleme çalışmaları yapılarak hazırlanan tezin içeriği 7 ana bölümden oluşmaktadır.

- **Giriş**

Bilgi ve iletişim sistemleri konusunda gelişmeler ile yaşanan kötü niyetli hareket ve saldırılara karşı ulusal siber güvenliğin etkinlikle sağlanması için ulusal siber güvenlik strateji ve politikalarının geliştirilmesinin önemi ve ihtiyacı açıklanmıştır.

- **Siber güvenlikle ilgili terim ve kavramlar**

Siber güvenlik konusunun doğru anlaşılması için öncelikle terim ve kavram birliği sağlanması, ortaya çıkan kavramlarla ilgili gelişmelerin bilinmesinin önemi doğrultusunda, konuyla iç içe olan ve en çok kullanılan terim ve kavramlar tanımlanarak kısaca açıklanmıştır

- **Siber savaş**

Siber ortamda yaşanan siber saldırılar ve taarruzlar sonucunda siber güvenliğin ulusal güvenlik sorunu ve ulusal güvenliğin ayrılmaz bir parçası olduğu görüşünü

destekleyen, geçmişte başlayan, günümüzde devam eden ve gelecekte de artarak devam edecek olan siber saldırı ve savaşlarla ilgili bilgiler verilmiştir.

- **Siber caydırıcılık**

Geçmişten günümüze siber olay, saldırı ve savaşlardan da örnekler verilerek, savaşlarda kazanmaktan çok caydırıcılığın daha iyi olabileceği düşüncesi ile siber güvenlik uygulamalarında dünyada çok yeni olan, Türkiye'de ise henüz yeterli önem ve önceliğin verilmediği görülen bu konuda yaklaşımlar ortaya konmuştur.

- **Ulusal siber güvenlik strateji ve politikaları**

Strateji ve politika kavramları açıklanmış, kurumsal ve ulusal siber güvenlik stratejileri ile bu konuda önde gelen ülkelerin ve Türkiye'nin mevcut siber güvenlik strateji ve politikaları hakkında bilgiler verilmiştir.

- **Caydırıcılık sağlayacak siber güvenlik strateji ve politikalarının oluşturulması**

Ulusal siber güvenlikte söz sahibi ülkelerin ulusal siber güvenlik strateji belgeleri ile bazı uluslararası kurumların çalışmalarından elde edilen bilgilerden hareketle, Türkiye için mevcut stratejiler ve eylem planları da dikkate alınarak, caydırıcılık da sağlayacak ulusal siber güvenlik stratejisi ve politikalarının hazırlanması ve uygulanması için bir yaklaşım tarzı ortaya konmuştur.

- **Sonuçlar**

Tez konusu kapsamında yapılan çalışmanın sonuçları ve yapılan değerlendirme ile görüş ve öneriler sunulmuştur.

1.2 Yanıtlanan Sorular

Yukarıda belirtilen temel amaç ve hedef için bir kısmı aşağıda sıralanan soruların yanıtlanmasına ve bu konuda dikkate alınmasının uygun olacağı düşünülen esas ve prensiplerin ortaya konulmasına çalışılmıştır.

- Kişi, kurum, kuruluş, toplum veya devletlerin günümüzde en değerli varlıklarını oluşturan bilgi ve bilişim sistemleri ile altyapılarından oluşan siber gücüne yönelik kötü niyetli hareket ve tehlikeler olan tehditler ve saldırılar nelerdir?
- Bu saldırıların sonuçları veya oluşturabileceği hasar ve zararlar neler olabilir?

- Bunlara karşı korunmak için neler ve nasıl yapılmalı, hangi güvenlik veya savunma tedbirleri alınmalıdır?
- Saldırganları caydırarak kötü niyetli hareketlere ve saldırılara engel olmak, bu bağlamda risk ve tehditleri ortadan kaldırmak veya azaltmak mümkün olabilir mi?
- Ülkenin siber gücünü veya diğer güçlerini ve alanlarını hedef alan siber saldırıları ve savaşları siber güçle caydırmak mümkün müdür?
- Ulusal güvenlik ve kalıcılık (beka) için siber gücün caydırıcılık maksatlı tek başına veya diğer ulusal güç unsurlarıyla birlikte kullanılmasıyla caydırıcılık nasıl sağlanabilir?
- Dünyada önemli bazı devletlerin siber güvenlik / savaş stratejileri ve siber caydırıcılık konusunda yaklaşımları nasıldır?
- Türkiye'nin resmi belgelerinde siber güvenlik ve caydırıcılık konusunda belirlenen ve uygulanması öngörülen tedbirler ve planlamalar ile yapılan çalışmalar nelerdir?
- Gerek siber saldırılara / savaşa karşı ve gerekse ulusal güvenlik ve kalıcılık için aynı zamanda siber caydırıcılık da sağlamak maksadıyla strateji ve politikalar nasıl geliştirilmeli ve uygulanmalıdır?

1.3 Bu Tez Çalışmasıyla Sağlanabileceği Düşünülen Katkılar ve Yararlar

Konuyla ilgili yapılan akademik çalışmaların, dünyada önemli devletlerin siber güvenlik / caydırıcılık strateji ve politikaları ile Türkiye'nin konuyla ilgili çalışmalarının, uygulama ve sonuçlarını inceleyerek, geçmişten günümüze yaşanan olaylardan çıkarılan derslerle geleceğin ihtiyaç ve hedeflerine yönelik öngörülerde bulunularak Türkiye'nin aynı zamanda caydırıcılık da sağlayacak siber güvenlik strateji ve politikalarının bilimsel yaklaşım ve yöntemlerle oluşturulasına ve uygulanmasına yönelik esas ve prensiplerin belirlenmesine çalışılan bu tez çalışmasıyla;

- Türkiye'nin siber ortamında yer alan ve gelecekte yer alacak muhtemel kritik alt yapı bilişim sistemlerinin ve değerli varlıklarının siber güvenliğine önemli katkılar sağlanacağı,
- Ulusal Siber Güvenlik Strateji ve Politikalarının aynı zamanda caydırıcılık da sağlayacak şekilde nasıl hazırlanması gerektiği konusunda, konuyla ilgili çalışan kamu

/ özel sektör kurum ve kuruluşları ile akademisyenlere yol gösterici bilimsel bir kaynak oluşturulacağı,

- Ulusal siber güvenlik strateji ve politikalarından sorumlu yetkin bir teşkilatın ortaya konulmasıyla, kararlılıkla uygulandığı takdirde siber güvenlik konusunda etkinlik ve caydırıcılık sağlanması yanında ekonomik artırım (tasarruf) ve kazançlar da sağlanacağı değerlendirilmektedir.

1.4 Kullanılan Yöntemler

Bu Tezin hazırlanması kapsamında, bilgi, bilgisayar ve iletişim sistemleri ve bu konulardaki gelişmeler tarihi bir bakış açısıyla incelenmiştir. Bu kapsamda siber uzay (ortam), siber saldırı (taarruz), siber suç, siber terörizm, siber güvenlik (savunma, siber savaş, siber istihbarat (casusluk), siber güç vb. kavramlar, siber güvenlik strateji ve politikaları ile siber caydırıcılık konularında, Çizelge 1.1'de konusu, türü ve miktarı açıklanan, akademik yayınlar başta olmak üzere, konuyla ilgili kurum ve kuruluşların yayımları ve dokümanları, kitaplar, dergiler, kütüphane ve internet ortamları taranmış, seminer sempozyum ve konferanslara katılım sağlanmıştır.

Çizelge 1.1: İncelenen kitap, doküman, belge ve çalışmaların dökümü.

S.No	Konu	Türü	Miktarı
1.	Strateji ve Güvenlik	Kitap, doküman ve çalışmalar	23
2.	Siber Güvenlik ve Strateji	Kitap, doküman ve çalışmalar	32
3.	Ülkelerin Siber Güvenlik Stratejileri	Belgeler ve planlar (ABD, Çin, Rusya, Fransa, İngiltere, İsrail, vd.)	18
4.	Türkiye'nin Siber Güvenlik Stratejisi	Belgeler ve planlar	17
5.	Caydırıcılık ve Siber Caydırıcılık	Kitap, doküman ve çalışmalar	30
6.	Konuyla ilgili gelişmeler ve etkinlikler	Seminer, sempozyum ve konferanslar	35

Bilişim sistemlerindeki teknolojik gelişmelerle birlikte, bilginin her alanda işlenmesi, üretilmesi depolanması, iletilmesi ve kullanılması konularında etkinliğin ve verimin artması paralelinde, siber ortamda kötü niyetli hareketler ve saldırılar her geçen gün çeşitlenerek artmaya devam etmektedir. Bu bağlamda, ülkeler her geçen gün önemi daha da artan siber uzaylarının güvenliğini sağlamak için, kendilerine özgü

ulusal siber güvenlik strateji ve politikalarını oluşturularak uygulamaya koymaları kaçınılmaz zorunluluk olarak ortaya çıkmıştır.

Konuyla ilgili tespit edilen, yaygın kabul görmüş bazı uluslararası kurum ve kuruluşların (ITU, ENISA, NATO CCD COE vb.) çalışmaları ile bazı akademisyen ve uzmanların görüşlerinden dikkate ve incelemeye değer bulunanların bazıları aşağıda kısa yorumlarla sunulmuş ve tez içerisinde değerlendirilmiştir

F. Wamala tarafından hazırlanan Uluslararası Telekomünikasyon Birliği (ITU) Ulusal Siber Güvenlik Strateji Kılavuzu (The ITU National Cybersecurity Strategy Guide)'nda [7], modern yaşamın siber ortamda sağlanan hizmetlerin zamanında ve yeterli seviyede sağlanmasına bağlı olduğu, siber güvenliğin sadece bir bilgisayar güvenliği sorunu olmadığı ve ulusal bir politika meselesi olduğu belirtilmektedir. Bu nedenle, hükümetlerin siber riskleri uygun bir şekilde azaltmak ve saldırıları önlemek için tüm ulusal güç araçlarını kullanmaları önerilmekte ve ulusal liderlerin, bir siber güvenlik stratejisi hazırlama ve işbirliği konusunda sorumlu oldukları vurgulanmaktadır.

Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) tarafından yayımlanan Ulusal Siber Güvenlik Stratejileri (NCSS) İyi Uygulama Kılavuzu (Good Practice Guide)'nda [8], siber alanın güvence altına alınmasının 21. yüzyılın en önemli meselelerinden biri haline geldiği ve her toplumu etkileyen bir ulusal güvenlik meselesi olduğu vurgulanırken, siber güvenlik tehditlerini karşılamak için Avrupa Birliği Üye Devletlerinin, ulusal siber güvenlik stratejilerini hazırlamaları ve sürekli geliştirerek güncel bulundurmaları gerektiği belirtilmektedir. Bu kapsamda, bir siber güvenlik stratejisinin nasıl geliştirileceği, uygulanacağı ve sürdürüleceği ile ilgili uygulamalar açıklanmakta ve tavsiyelerde bulunulmaktadır.

NATO'nun siber savunma kapasitesinin artırımı amacıyla 14 Mayıs 2008 tarihinde Estonya'nın başkenti Tallinn'de kurulan, uluslararası bir askeri merkez olan NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCD COE)'nin ana görevi eğitim, araştırma ve geliştirme, alınan dersler ve danışmalar yoluyla NATO ülkeleri ve siber savunma alanındaki ortakları arasındaki yetenek, işbirliği ve bilgi paylaşımını güçlendirmektir. Merkezin resmi internet sitesinde [9] üye ülkelerin siber güvenlik strateji belgeleri yanında, ulusal siber güvenlik strateji ve politikalarının hazırlanması ve uygulanması öneri, eğitim, tatbikat, uzmanlık ve danışmanlık yardımları ile

uluslararası alanda siber ortama yönelik yasal düzenlemelerle ilgili çalışmalar yer almaktadır.

Geçmişten günümüze Türkiye'de devlet kurum ve kuruluşlarınca siber güvenlik stratejileri konusunda pek çok çalışma yapılmış, çalışmalarla ilgili hazırlanan resmi belgeler, onaylanması ve yayınlanması sonrasında uygulamaya konulmuştur. Söz konusu çalışma ve belgelerin içerik ve uygulamaları tez içerisinde incelenerek analiz edilmiştir. Konuyla bağlantılı elde edilen bazı akademik çalışmalar ve belgelerle ilgili tespitler de şu şekildedir.

H. Şentürk vd. tarafından yapılan 'Türkiye'nin Siber Güvenlik Analizi (Cyber Security Analysis of Turkey)' konulu çalışmada [10]; siber güvenliğin ulusal düzeyde en önemli boyutunun stratejik planlamaları da kapsayan stratejik yönetim olduğu, siber tehditlere karşı yapılması gereken ilk şeyin stratejik hedefleri ve bu hedeflere ulaşılırken alınması gereken tedbirleri kapsayan bir ulusal strateji belgesi hazırlanması gerektiği vurgulanmıştır.

U. Akyazı tarafından yapılan 'Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler' konulu çalışmada [11]; Siber uzayın diğer çatışma ve savaş alanlarından ayrı olarak ulusal gücün unsurlarının her birisi üzerinde etkili olduğu belirtilmiş, NATO'nun siber güvenlik politikası, ABD doktrinleri ve bazı ülkelerin stratejileri kısaca özetlenerek, bu kapsamda alınması gereken önlemler ortaya konmuştur

E. U. Küçüksille vd. tarafından yapılan 'Dünyada Siber Güvenlik Stratejileri ve Bir Siber Güvenlik Stratejisinin Oluşumu' konulu çalışmada [12]; dünyada internetin yaygın bir şekilde kullanılması ile beraber bilgi güvenliği kavramından daha çok bahsedilir olduğu, bu bağlamda devletler tarafından yasal düzenlemelerin yapılmaya ve siber güvenlikle ilgili stratejilerin oluşturulmaya başlandığı belirtilmiş ve bir siber güvenlik stratejisi oluşturulurken dikkate alınması gereken önerilerde bulunulmuştur

M. Güngör tarafından hazırlanan 'Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma' konulu çalışmada [13]; bilgi sistemleri ile kritik altyapılarını korumak amacıyla üretilen stratejilerin gerçekleştirilmesinin kamu ve özel sektörün koordineli çalışacakları bir kurumsal yapıdan geçmekte olduğu, Türkiye'de bu alanda yasal altyapı eksikliği bulunduğu, bilgi güvenliği kavramının tam olarak

anlaşılamaması ve yanlış bir kavramsal çerçeveye oturtulması nedeniyle bir türlü istenilen sonuca ulaşılamadığı belirtilmiştir.

V. Göçoğlu tarafından hazırlanan 'Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi' [14] konulu doktora tezinde, Siber güvenliğin kritik altyapı sistemleri yanında endüstriyel kontrol sistemleri güvenliğini de içeren bir alan durumuna geldiği, ulusal güvenliğin sağlanması ve kritik altyapı sistemlerinin korunmasında ülkelerin, alışılmış güvenlik yöntemleriyle birlikte gelişen teknolojilerle dönüşen kritik altyapılarla birlikte siber güvenlik konularında farkındalık kazanıldığı belirtilmektedir. Siber güvenliğin bir kamu politikası olarak ele alınması ve kamu politikası analizi çerçevesinde düşünülmesi gerektiği vurgulanmıştır. Çalışmada örnek olay ve bazı ülke inceleme sonuçlarıyla Türkiye'nin siber güvenlik ve kritik altyapı politikaları ile ilgili olarak kamu politikası analizi yaklaşımları ortaya konmuştur.

A. Şengönül, 'Dördüncü Nesil Savaş Kapsamında Türkiye İçin Strateji Tartışmaları' [15] konulu çalışmasında, dördüncü nesil savaşı, teknolojik ve askeri bakımdan üstün devletlerin, üstünlüklerini korumak, artırmak ve devam ettirmek isteklerine karşı tehditleri tespit etmek ve önlem almak üzere geliştirdikleri bir bakış açısı olarak değerlendirmektedir. Savaşın değişim süreci içerisinde, 20. yüzyılın sonlarında kullanılmaya başlanılan ve internetle birlikte ortaya çıkan, internet ağlarında savaş olarak da ifade edilen, bilişim teknolojilerinin kullanılmasıyla daha ölümcül olan siber savaşın dördüncü nesil savaş olarak bilindiğini vurgulamakta ve Türkiye'ye yönelik strateji önerilerinde bulunmaktadır.

Ulusal siber güvenlik strateji ve politikaları kapsamında, Türkiye'de 2003 yılında, '2003/10 Sayılı Başbakanlık Genelgesi [16] ile başlayan ve günümüzde de devam eden çalışmalarla ilgili belgeler ayrı ayrı incelenerek analiz edilmiştir. Türkiye'de siber güvenlik strateji ve politikalarıyla ilgili bu güne kadar hazırlanan ve uygulamaya konulan belgeler incelendiğinde, siber güvenlik (savunma) ayrıntılı olarak ele alınmıştır. Siber savaşın diğer ana boyutu siber taarruz boyutuna değinilmemiş, 'siber caydırıcılık' konusuna ise, siber suçlarla yasal olarak mücadele edilerek caydırıcılık sağlanması [17] konusu hariç açıkça hiç yer verilmediği görülmüştür. Bunun yanında siber savaş için gerekli olan ve diğer ulusal

güç unsurları arasında yer alması gereken ‘Siber Güç’ konusunun ele alınmadığı, siber gücün oluşturulması, geliştirilmesi ve kullanılması konularına değinilmediği tespit edilmiştir. Siber Güç ve caydırıcılık konularında temin edilerek incelenen bazı çalışmalardan önemli tespitler şunlardır.

J. Nye, ‘Siber Güç (Cyber Power)’ adlı eserinde [18]; ülkelerin siber ortamda sert ve yumuşak güç kullanma kapasitelerinin de mümkün olduğunu belirtmektedir. Bazı ülkelerin kara, deniz ve hava harekât alanlarında çok güçlü olmalarına karşın, aynı gücü ve etkiyi siber alanda gösteremeyebileceklerini ve asimetrik kullanım etkileri dolayısıyla devlet dışı aktörlerin de siber alanda etkili olabileceklerini vurgulamaktadır.

F. D. Kramer vd. ‘Siber Güç ve Milli Strateji (Cyberpower and National Security)’ isimli eserde [19]; siber alanın, siber uzay kullanıcıları için hem olağanüstü fırsatlar hem de büyük zorluklar sunan olağanüstü değişiklikler geçirdiği, zorlukların siber uzayı kullanan kötü niyetli aktörlerden ve bu alanı etkileyen birçok güvenlik açığından kaynaklandığı, fırsatlardan yararlanmak ve zorlukları aşmak için siber alanda dengeli bir bilgi birikimine ihtiyaç duyulduğu belirtilmektedir. “Siber Güç ve Ulusal Güvenlik” konusunda siber zorlukları gidermek için uluslararası ortaklıkların geliştirilmesi ve bu maksatla insan kapasitesinin oluşturulması ve kullanılması konularına dikkat çekmektedir.

C. Haley, ‘Siber Caydırıcılık Kuramı (A Theory of Cyber Deterrence)’ konulu eserinde [20]; siber caydırıcılığın nükleer caydırıcılıktan birçok temel yolla farklılık gösterdiği, uygulamanın ne kadar etkili olursa olsun tüm saldırıların ortaya çıkma olasılığını ortadan kaldırmasının pek mümkün olmadığı, bununla birlikte düşük maliyetle yönetilebilir bir düzeye indirmede kritik bir rol oynayabileceği belirtilmektedir.

ABD’li siber güvenlik uzmanı M.C. Libicki, askeri siber gücün önemini vurguladığı ‘Askeri Siber Güç (Military Cyberpower) isimli çalışmasında [21]; harekât alanlarında harekâtın ağ merkezli olarak icrasını siber gücün kullanımı olarak ifade etmektedir. Askeri siber gücün diğer klasik askeri güç unsurlarıyla birlikte kullanımı durumunda, o güçlerin etkinliğini daha da artırdığını iddia etmektedir. Libicki, ‘Siber Caydırıcılık ve Siber Savaş (Cyberdeterrence and Cyberwar)’ adlı eserinde [22]; siber ortamda caydırıcılık sağlamanın klasik veya nükleer harekâttan

farklı ve çok daha zor olmakla birlikte mümkün olduğunu ve işe yarayabileceğini belirtmekte, ancak bazı şartlara ve kurallara bağlamaktadır.

T.J. Mowbray yaptığı 'Siber Caydırıcılık İçin Çözüm Mimarisi (Solution Architecture for Cyber Deterrence)' adlı çalışmasında [23]; bir ülkenin siber caydırma stratejisinin etkili olabilmesi için, o ülkenin ağa sızma araçlarının yanı sıra, dağıtık servis dışı bırakma, paralel tarama, keşif, gözetleme ve diğer yetenekler için araçlara sahip olması gerektiğini belirtmektedir. Siber caydırıcılıkta en önemli konunun da, siber saldırıyı yapan ülkenin ya da hedefin hızlı ve kesin bir şekilde değerlendirilebilmesi olduğu vurgulanmaktadır.

C.F. Wrenn, Stratejik Siber Caydırıcılık (Strategic Cyber Deterrence) konulu Doktora Tez çalışmasında [24] siber caydırma teorisini geliştirmek için öncelikle siber savaşın doğasını ve amacını anlamak gerektiğini, bu kapsamda ilk zorluğun siber alandaki terim birliği ve tanımlarda tutarlılığın olmaması nedeniyle ortaya çıktığını, siber savaşın devlet politikasının siber vasıtalar ve yollarla devamı olarak tanımlanabileceğini, işbirliğinin siber caydırıcılıkta daha önceki caydırıcılık teorilerinden daha büyük bir rol oynadığını düşündüğünü belirtmektedir.

R.A. Clarke ve R.K. Knake, 'Siber Savaş (Cyber War)' adlı eserlerinde [25]; siber savaş, saldırı, savunma ve caydırıcılık konusundaki düşünce ve tespitlerini açıklamaktadır. Sağlıklı bir ölçüm yapılabilseydi, ABD siber saldırı yeteneği konusunda ilk sırada yer alabilirdi. Teknolojisi yetersiz ve hiçbir ağa sahip olmayan bir ülkeye siber saldırılarla zarar verilemez. Buna karşılık ileri seviyede teknolojiye sahip, ekonomisi ve endüstrisi internete bağımlı bir ülke ise siber saldırılara karşı yüksek duyarlılık taşır ve siber savunma maliyetleri de yüksek olacaktır. Bu düşünceye göre siber bağımlılık ne kadar yüksekse, siber savaş gücü o kadar olumsuz etkilenecektir.

E.T. Jensen, 'Siber Caydırıcılık (Cyber Deterrence)' konulu çalışmasında [26]; ulusların ağlarını ve altyapılarını savunmak için mücadele ederken, siber ortamda caydırıcılığın geleneksel misillemeye ek olarak, soğuk savaşın nükleer çağında geliştirilen geleneksel caydırma metotlarından daha fazla yasal işlemleri yapma, ağları görünmez, esnek ve birbirine bağlı hale getirme gibi seçenekleri de sunduğunu belirmektedir.

T. Thomasen, ‘Siber Caydırıcılık - 21. Yüzyıl Majino Hattı (Cyber Deterrence-A 21st Century Maginot Line)’ adlı çalışmasında [27]; siber güvenliğin sağlanmasının çağdaş devletlerin karşılaştığı en üst düzey tehditler arasında olduğunu, siber sistemlerin güvenli hale getirilmesi konusunun ulusal güvenliğin tam kalbi olarak kabul edildiğini, siber konularda uluslararası işbirliği sürdürülürken siber uzayda saldırı yeteneklerin geliştirilmesinin amaçlandığını, siber caydırıcılığın da bu yaklaşımlardan birisi olduğunu vurgulamaktadır.

A. Bendiek ve T. Metzger’in, ‘Siber Çağda Siber Caydırıcılık (Cyberdeterrence Theory in the Cyber-Century)’ isimli çalışmalarında [28]; siber saldırılardan korunmak için caydırıcılık kuramının uzun zamandır değerli bir kavram olarak düşünüldüğü ve siber uzayda uygulanabilir olduğunun tartışıldığı belirtilmektedir. Klasik caydırıcılığa dair ilkelerin siber caydırıcılıkta nasıl uygulanabileceği, sahip olunan siber yetenekler saldırgan düşmanları caydırmakta etkili olup olamayacağı, caydırıcılık için klasik misillemenin düşünülmesi gerektiği ve siber caydırıcılığın uygulama zorlukları konuları açıklanmaktadır.

P.K. Davis, ‘Caydırıcılık, Etki, Siber Saldırı ve Siber Savaş (Deterrence, Influence, Cyber Attack, and Cyberwar)’ konulu çalışmasında [29]; siber saldırıların ve siber savaşın ulusal güvenlik tehditleri olduğunu, caydırıcı çabaların geçmişte başarısızlıkla sonuçlandığını ancak bazen yararlı bir rol oynayabileceğini, akademisyenlerin ve politika yapıcıların, uluslararası ve yasal alanlardaki hangi eylemlerin yararlı olabileceği konusunda erken sonuçlardan kaçınmaları gerektiği üzerinde durmaktadır.

J.R. Lindsay, ‘Ölçeklerin ağır basması: Dayandırma problemi ve siber saldırıya karşı caydırmanın uygulanabilirliği (Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack)’ isimli çalışmasında [30]; siber saldırganların güvenlik açıklarını kullanırken, kimliklerini gizlemeye ve aldatmaya güvendiklerini, bunun da siber caydırıcılık konusunda başarı için kötümserliğe sevk ettiğini belirtmektedir. Özellikle misilleme cezasının etkisiz kaldığını ve aldatmacaya güvenin saldırgana bazı avantajlar sağladığını vurgulamaktadır.

P.W. Singer ve Alan Friedman’ın, ‘Siber Güvenlik ve Savaş (Cybersecurity and Cyberwar)’ isimli eserlerinde [31] belirttiklerine göre; caydırıcılık maliyet ve fayda

analizleri değiştirilerek bir düşmanın eylemlerinin değiştirilme yeteneğidir. Siber ortamda caydırıcılığın diğer ortamlardaki caydırıcılıktan en önemli farkı ise, "kime karşı caydırıcılık veya misilleme yapılacağı" problemidir.

P. Pernik'in, 'NATO'nun Siber Caydırıcılığı (NATO's Cyber Deterrence)' konulu çalışmasında [32]; NATO'nun siber uzayda görevinin sadece kendi ağlarının korunmasını ve müttefiklerine siber saldırılar çerçevesinde yardım etmesini içeren savunma amaçlı olduğu, siber saldırı yeteneklerini kullanma şansı olmadığı ve güvenilir bir caydırıcılığı sürdürmeyi başaramayacağı belirtilmektedir. Siber alanın harekât alanı olarak ele alınması ile NATO görevlerinin ve operasyonlarının daha iyi korunmasının sağlanabileceği, bu maksatla planların yapılması ve hazırlanılması önerilmektedir.

A. Wilner, 'Siber caydırıcılık ve kritik altyapı koruması: Beklenti, uygulama ve sınırlamalar (Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation)' konulu çalışmasında [33]; caydırıcılık kuramını siber güvenlik politikasına ve kritik altyapıların korumasına bağlamanın kolay olduğunu, ancak bunu uygulamanın daha zor olduğunu, caydırıcılık stratejisi mantığının siber güvenlik politikası ve stratejisine nasıl uygulanacağını belirlemek için klasik caydırıcılık teorisinden yararlanılabileceğini belirtmiştir. Bu maksatla dikkat edilmesi gereken yedi temel kuralı; Sayısal erişimi reddetme, Siber misillemeyi yönetme, Caydırıcılıkta başarısızlığı gözlemleme, Siber uyumsuzlukları engelleme, Zayıflığın siber gücünü ele alma, Siber saldırıları dayandırma ve Sınırlamaları kuvvetlendirme şeklinde sıralamıştır.

M. Taddeo, 'Siber Ortamda Dengeyi Güçlendirmek İçin Caydırıcılık ve Kurallar Deterrence and Norms to Foster Stability in Cyberspace)' konulu çalışmasında [34]; siber alanda caydırıcılığın mümkün olduğunu kabul etmekle birlikte, ayrıca bu alana özgü, kavramsal, uygulanabilir kurallar ve stratejik çerçeve geliştirilmesi ihtiyacını vurgulamaktadır. Ülkelerin siber caydırıcılıkta başarılı olmaları ve dengeyi sağlamaları için siber alanda devletlerin davranışlarını düzenleyen uluslararası kurallar sistemi ile stratejilerini tamamlamaları gerektiğini savunmaktadır.

S. Ünal'ın, 'Siber Uzamın Güvenlikleştirilmesi Söylemi: Türkiye, ABD ve Avrupa Birliği Örnekleri' [35] konulu doktora tezinde; haberleşme ve iletişim teknolojilerinin güvenliği konusunda sorunlar ve bu teknolojilerin toplumsal alanda etkisinin siber

uzayın güvenliğine yönelik yeni tehditleri ve riskleri de beraberinde getirdiği, bu tehdit ve risklerin ulusal güvenlik kapsamında ele alınmasıyla konunun siyasi alana taşındığı açıklanmıştır. Risk ve tehdit kavramlarından hareketle siber uzaya yönelik güvenlik sağlayıcı bir yöntemin oluşması ve böylece siber ortamın askeri alan olarak denetim ve gözetimin yasal hale getirilmesi sorunu kamu politikalarıyla etkileşim içerisinde ele alınmış, yapılan analiz çalışması sonunda Türkiye'nin yaklaşımının ABD ve Avrupa Birliği'nden benzerlikler içeren hibrit bir yapıya sahip olduğu ortaya konmuştur.

E. Gündoğdu, 'Caydırıcılık Teorisini Yeniden Düşünmek: Asimetrik Caydırıcılık ve Oyun Teorisi' konulu doktora tezinde [36]; soğuk savaş döneminde, caydırıcılık teorisinin nükleer silahlara ilişkin uluslararası güvenlik çalışmalarının odak noktası olduğu, soğuk savaş sonrasında ise caydırıcılık çalışmalarının devlet dışı aktörlerin ve haydut devletlerin caydırılması konusuna yöneldiği, askeri güce sahip olunmasının caydırıcılığın başarısı için tek başına yetersiz olduğunu ve caydırıcılığın karar alıcıların tercihleri ve algılamalarına dayandığını açıklamıştır. Bu nedenle caydırıcılık stratejisinin uygulanmasında hedef devletlerin kimliği ve stratejik kültürünün özelliklerinin dikkate alınması gerektiği ve uluslararası ilişkilerde bu bakış açısıyla hareket edilmesinin doğru olacağını vurgulamıştır.

Ulusal siber güvenlik strateji ve politikaların oluşturulması ve uygulanması konusunda, özellikle uygulama zorlukları ve maliyetleri nedeniyle; yazılı yayın ve eserlerde deneysel bir metodun bu güne kadar ortaya konulmadığı, kuramsal (teorik) olarak çalışmaların yapıldığı, yaşanan olaylardan edinilen tecrübeler ve öngörülerle bu çalışmaların geliştirilmekte olduğu görülmektedir. Siber güvenlik, siber savaş, siber caydırıcılık vb. konularda strateji ve politikaları ele alan kaynak niteliğindeki kuramsal çalışmaların dikkat çeken ortak özelliği, uygulamada test edilmemiş olmaları veya deneysel sonuç özellikleri taşımadıkları için, siber uzayda etkili olup olamayacakları konusunda belirsizliklerle kararsızlık ve tartışmaların devam etmesine yol açmalarıdır.

Taranan ve incelenen kaynaklarda, siber güvenlik strateji ve politikaları ile siber caydırıcılık konusunda akademik çalışmalar, çeşitli yayın ve kitaplar bulunmakla birlikte; aynı zamanda caydırıcılık da sağlanması hedef ve amaçlanan ulusal siber güvenlik strateji ve politikalarının nasıl oluşturulması ve uygulanması gerektiği

konusunda, açıkça esas, prensip, ilke, yol ve yöntemlerin ortaya konulduğu örnek bir çalışma tespit edilememiştir. Ayrıca siber güvenlik strateji ve politikalarının bir laboratuvar ortamında test ya da denemesi de mümkün olamadığı için, ülkelerin siber güvenlik strateji ve politikalarının test, deneme veya uygulama alanı, yine o ülkelerin siber uzaylarının yani günümüzdeki yaşamlarının kendisi olmaktadır.

Konuyla ilgili bütüncül çalışmalar olmamakla birlikte yaşanmışlıklar ve gerçek deneyim sonuçları bulunmaktadır. Stratejistlerin ünlü Alman devlet adamı Bismark'a dayandırdıkları bir söz vardır. Bismark, "Budalalar deneyerek öğrendiklerini söylerler. Bense, başkalarının deneyimlerinden yararlanmayı tercih ederim" [37] demiştir. Yine Türkiye cumhuriyetinin Kurucusu Gazi Mustafa Kemal Atatürk yaptığı köklü devrimleri ve yenileşmelerin başlangıcını ve gerekçelerini; "Biz, ilhamlarımızı gökten ve gaipten değil, doğrudan doğruya hayattan almış bulunuyoruz. Bizim yolumuzu çizen; içinde yaşadığımız yurt, bağrından çıktığımız Türk milleti ve bir de milletler tarihinin binbir facia ve ıstırap kaydeden yapraklarından çıkardığımız neticelerdir." [38] şeklinde açıklamıştır.

Bu sözlerden hareketle bu çalışmanın yolu ve yöntemi; "Biz, siber güvenlikle ilgili esinlerimizi gökten ve görünmez evrenden değil, doğrudan doğruya yaşamdan alacağız. Bizim siber güvenlik stratejisi ve caydırıcılık için yolumuzu çizen; içinde yaşadığımız yurt ve siber uzay, bağrından çıktığımız Türk ulusu ve bir de uluslar siber uzay tarihinin bin bir acı ve üzüntü kaydeden yapraklarından çıkardığımız sonuçlar olacaktır." sözleriyle belirlenmiştir. En önemli yol ve yöntemlerin, geçmişte ve günümüzde yaşanan olaylar ve uygulamalar ile bunlardan çıkarılan sonuçların geleceğe ve ihtiyaçlara yönelik tespit ve öngörülerle uygulamaya konulması olacaktır.

Bu açıklamalar çerçevesinde tezin hazırlanması için yapılan çalışmada; kütüphane, kitapçı ve internet ortamı araştırması, kitap, dergi, yayın, belge ve kayıt incelemesi, seminer, konferans ve çalıştay gibi etkinliklere katılım, görüşme, söyleşi, vb. sonucu elde edilen bilgilerin ortaya konması, analizi ve değerlendirilmesi şeklinde 'karma yöntemler' kullanılmıştır.

2. SİBER GÜVENLİKLE İLGİLİ TERİM VE KAVRAMLAR

Bilgisayarın icadı sonrasında teknolojinin de gelişmesine paralel olarak bilişim sistemleri insan yaşamının bir parçası olurken siber uzay şekillenmiş, bunun yanında gelişmelerle birlikte ortaya çıkan ihtiyaçlar, risk, tehdit ve tehlikelere karşı korunma bağlantılı siber ortamın güvenliği çerçevesinde yeni terim ve kavramlar da kullanılmaya başlanmıştır. Terim ve kavramların yeni olmasından da kaynaklanan çok çeşitli ve farklı tanımlarının yapıldığı görülmektedir. Örneğin, Kramer tarafından yapılan bir çalışmada siber güvenliğin 28 farklı tanımının yapıldığı belirtilmiştir [19].

Siber güvenlik konusunun geniş ve ayrıntılı bir yaklaşımla ele alınarak, inceleme, analiz ve değerlendirmelerin doğru anlaşılması için, öncelikle terim birliği sağlamak ve ortaya çıkan kavramlarla ilgili gelişmeleri bilmek aynı dili konuşmak ve anlamak kadar önem arz etmektedir. Siber güvenlik konusu ile iç içe olan ve en çok kullanılan temel kavramlar, siber uzaydan başlayarak sırasıyla, siber tehdit / risk, siber saldırı, siber suç, siber terörizm, siber savaş, siber güvenlik, siber caydırıcılık, siber istihbarat ve siber güç terim ve kavramları kısaca açıklanmıştır.

2.1 Güvenlik Kavramı

Hassas ve değerli varlıkları kötülüğe, hasar veya zarara karşı koruma veya karşı koyma anlamında kullanılan ‘Güvenlik’ kavramı, TDK sözlüğünde “Toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet” [39] şeklinde açıklanmaktadır.

İnsanın varoluşundan başlayarak kişisel ve toplumsal yaşamının zorunluluğu olan güvenlik kavramı, insanın varlığını koruması ve sürdürebilmesi için her davranış biçiminde karşılaşılan bir olgu olarak kabul edilmektedir. Diğer bir tanımlamada güvensizlik olasılıklarının ortadan kaldırılması durumu olarak açıklanan güvenlik kavramı tehdit, risk ve tehlike sözcükleriyle birlikte ele alınmakta ve dördüncü bir faktör olarak amaç ya da hedefle bağlantılandırılmaktadır. Yani tehdit ve riskten söz

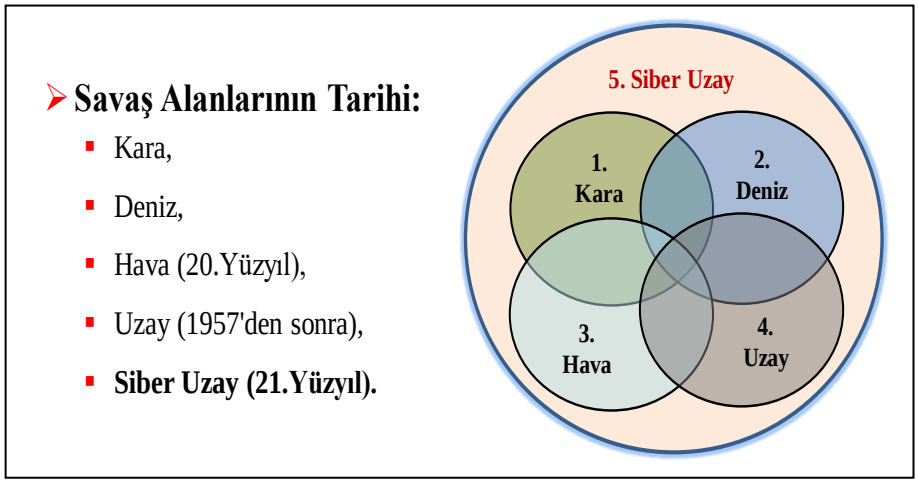
edebilmek için öncelikle tehlike ve o tehlikeyle ilişkili hedef veya amaç gerekmektedir [40].

Halk arasında saldırılara karşı koyma anlamına gelen ‘Savunma’ kavramı yerine de kullanılmakta olan güvenlik kişiden aileye, toplumdan devlete, devletten bölgeye ve uluslararasına kadar çok geniş seviyelerde söz konusudur. Geleceğe dönük neler olabileceği konusunda öngörülerde bulunarak planlamalar yapılmasını ve tedbirler alınması için yatırımlar yapılmasını gerektirir.

Güvenlik tanım ve yaklaşımlarından hareketle, ‘Siber Uzay’daki değerli varlıklara gelecek kötülük, hasar veya zararlara karşı korunma ve karşı koyma derecesi ile sağlanan düzenin aksaksız yürütülmesi, kişilerin, toplumların ve ulusların korku duymadan yaşayabilmesi hali siber güvenlik olarak karşımıza çıkmıştır.

2.2 Siber Uzay

İnsanoğlunun varoluşundan başlayarak zaman içerisinde kara, deniz, hava ve uzay gibi kendine has özellikleri ve gereklilikleri bulunan dört savaş alanına, 21’inci yüzyıla gelindiğinde bu alanları da içerisine alan ve 5’inci harekât alanı olarak ifade edilmeye başlanan ‘Siber Uzay’, siber ortam, sanal ortam, sayısal ortam, bilgi ortamı vb. terimlerle de adlandırılmaktadır (Şekil 2.1).



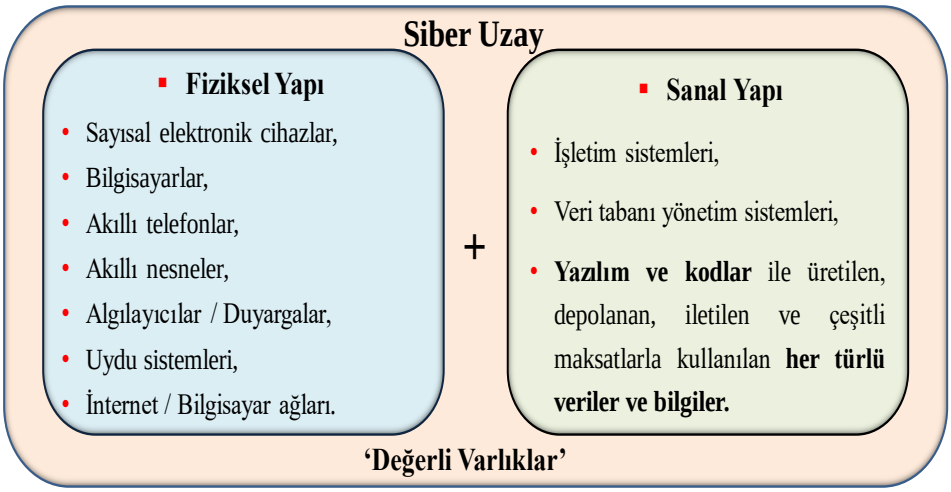
Şekil 2.1: Savaş (Harekât) alanları.

Tanım olarak bakıldığında, geçen yıllar süresince siber uzayın pek çok farklı şekilde tanımının yapıldığı görülmektedir. Kısaca “Bilgisayar ağları üzerinde sayısallaştırılmış bilginin iletildiği düşünsel ortam” olarak tanımlanan siber uzayın en kapsamlı tanımı Singer ve Friedman tarafından yapılan; “Bilgisayar ve füzelerden,

güneşten gelen ışınlara kadar elektronik ve elektromanyetik görüngenin kullanımı ile karakterize edilen alan" [31] şeklindedir.

Türkiye 2016-19 Ulusal Siber Güvenlik Stratejisi belgesinde siber uzay; "Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam" [41] olarak tanımlanmaktadır.

Tanımlar incelendiğinde siber uzayın fiziksel ve sanal olarak iki birleşik yapıdan oluştuğu görülmektedir (Şekil 2.2). Fiziksel yapı, sayısal elektronik cihazlarını, bilgisayarları, akıllı telefonları, akıllı nesneleri, algılayıcılar (detektörler) ve duyargaları (sensörleri), uydu sistemlerini ve internet dâhil bütün bilgisayar ağlarını içeren her türlü bilgi ve iletişim sistemlerini ve kullanıcılarını kapsamaktadır. Sanal anlamda ise, fiziksel ortamdaki işletim sistemleri başta olmak üzere yazılım ve kodlar ile üretilen, depolanan, iletilen ve çeşitli maksatlarla kullanılan her türlü verileri ve bilgileri kapsamaktadır. Siber uzayın bileşenlerini oluşturan varlıklar korunması ve güvenliğinin sağlanması gereken değerli varlıkları oluşturmaktadır.



Şekil 2.2: Siber uzayın bileşenleri.

Teknolojik gelişmeler sonrası içinde yaşadığımız bilgi çağında, elektronik, bilgi iletişim sistemleri ve ağları ile yaşamımızın, vücudumuzda beynimizle sinir sistemimiz gibi, bir parçası haline gelen siber uzay; siber tehdit ve risklere açık, siber saldırılar, suçlar ve terör olayları yanında siber savaş gibi pek çok tehlikeyi de üzerinde barındırmakta, bu tehlikeler de her geçen gün çeşitlenerek artmaktadır.

2.3 Siber Tehditler ve Riskler

Siber tehditler, siber ortamda bir kurumun / kuruluşun veya sistemin zarar görmesi ile sonuçlanabilecek istenmeyen olayların potansiyel nedenleri olarak tanımlanmaktadır [42]. Tehditler yönlerine göre iç ve dış tehditler şeklinde sınıflanırken, kaynaklarının insan olmasına göre; kötü niyetli olmayan (Eğitimsiz, bilinçsiz, dikkatsiz kullanıcılar tarafından yanlış veri girişi, zararlı yazılım yüklemesi vb.) ve kötü niyetli olan (Zarar vermek veya çıkar sağlamak amaçlı ağ saldırısı, zararlı yazılım yüklemesi, yetkisiz erişim vb.) şeklinde gruplanmaktadır. Ayrıca uzun süreli elektrik kesintileri, hava kirliliği, vb. çevresel tehditler ile deprem, sel, çığ, yıldırım düşmesi, toprak kayması vb. nedenlerle gerçekleşen doğa kaynaklı tehditler de bulunmaktadır.

Siber riskler ise, zarara ve kayba neden olacak bir olayın bilgi varlığı üzerinde gerçekleşme olasılığı, diğer bir ifadeyle de tehditlerin bilgi varlıkları üzerindeki açıklıkları kullanarak zarar yaratma potansiyeli şeklinde tanımlanmaktadır [43].

Ulusal siber güvenlik strateji belgelerinde yaygın olarak kabul edildiği görülen riskler [41]:

- Toplumun sosyal ağlara bağımlılığı,
- Kritik kurum ve kuruluşların siber uzaydaki konumları,
- Çeşitli siber casusluk çalışmaları ve hedefli saldırılar,
- Personel ve yetkinlik bağlamında yetersizlik,
- Kurumlar arası koordinasyon eksikliği,
- Siber uzayda faaliyet gösteren farklı ölçeklerdeki sektörlere yönelik ekonomik kaygılar şeklinde sıralanmaktadır.

2.4 Siber Saldırılar ve Olaylar

Kazanç sağlamak veya zarar vermek maksatlarıyla siber uzayda belirlenecek hedef ya da hedeflere yönelik gerçekleştirilecek faaliyetler siber saldırıları oluşturmaktadır. ABD Ulusal Araştırma Konseyi tarafından, 2009 yılında yapılan bir çalışmada siber saldırılar “Bilgisayar sistemleri, ağlar veya bilgiyi ve / veya bunlarda yerleşik olan ya da bunları taşıyan programları bozmak, aldatmak, küçük düşürmek veya yok etmek için yapılan kasıtlı hareketler” [44] olarak tanımlanmıştır.

Siber saldırılar, siber ortamdaki fiziksel veya sanal yapıyı, yazılım, donanım ve alt yapı sistemlerini, genellikle de bu sistemler üzerindeki bilgiyi ve kullanıcıları hedef almaktadır. Türkiye Ulusal Siber Güvenlik Stratejisi belgesinde bu düşünceden hareketle siber saldırıların tanımı, "Ulusal siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın her hangi bir yerindeki kişi ve / veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler" [41] şeklinde yapılmıştır.

Siber uzayın fiziksel ve sanal olarak bileşenlerini oluşturan değerli varlıkların korunması esas alındığında, bunların kasıtlı veya kasıtsız, bilerek veya bilmeyerek, ihlal, saldırı ya da başka niyet ve maksatlarla olumsuz olarak etkilenmeleri, zarar görmeleri ve üzerlerinde işlem yapılması durumları da genel anlamda siber olay olarak adlandırılmaktadır [45]. Bilgisayarlar, bilgisayar ağları ve donanımları kullanılarak işlenen politik amaçlar gütmeyen ve ulusal güvenlik açısından sorun teşkil etmemekle birlikte kişi, kişiler veya organize suç örgütleri tarafından gerçekleştirilen hukuka aykırı bu olaylar ise siber suçları oluşturmaktadır.

2.5 Siber Suçlar

Başlangıçta klasik suç tanımına uymayan ve bilgisayar veya bilişim suçları olarak ifade edilmeye başlanan suçlar, bilgisayarın iş hayatında ve internetin yaygınlaşarak sosyal hayatta da kullanılmasıyla birlikte siber suçlar kavramı ile ifade edilmeye başlanmıştır. Genel olarak, "Bilgisayarların kötüye kullanılması, bilgileri otomatik işleme tabi tutulmuş ve verilerin nakline ilişkin kanuna ve meslek hayatına aykırı davranışlar" [43] şeklinde ifade edilen ve uluslararası bir konu olan siber suçlar, Birleşmiş Milletler (BM) 10.Kongresi (2000)'nde "bilişim sistemi güvenliğini / veri işlemini hedef alan, bilişim sistemi / ağı marifetiyle gerçekleşen kanun dışı eylemler" [44] şeklinde açıklanmıştır.

Avrupa Konseyi (AK) Siber Suçlar Sözleşmesi (2004)'nde ise; yetkisiz erişim, sisteme ve veriye müdahale, bilişim sistemi aracılığıyla sahtekârlık ya da dolandırıcılık suçları yanında, bilgisayar ve veriye yönelik fiillere ilave olarak, bilişim sistemlerinin kullanılmasıyla ve özellikle internetin yaygınlaşması ile birlikte niceliksel olarak ortaya çıkan çocuk pornografisi, telif haklarına ilişkin ihlaller, yabancı düşmanlığının ve ırkçılığın önlenmesine ilişkin hükümler de siber suç kapsamına alınmıştır [45].

BM çalışmalarında ve AK sözleşmesinde farklı şekillerde yer aldığı görülen ve uluslararası alanda ortak bir tanımı bulunmayan, siber saldırılar gibi her geçen gün çeşitlenerek artan siber suçlarla ilgili yasalar ve düzenlemeler de ülkeden ülkeye değişmektedir.

Genel anlamda, bilişim sistemleri üzerinde kişi, kişiler veya organize suç örgütleri tarafından, politik amaçlar gütmeyen ve ulusal güvenlik açısından sorun teşkil etmeyen siber saldırılar ve hukuka aykırı fiiller siber suç olarak kabul edilmekte ve hukuk önünde ona göre işlem görmektedir. Her türlü siber saldırı ve olayların terör unsurlarınca veya terör maksatlarıyla gerçekleştirilmesi durumunda ise siber terörizm şeklinde ortaya çıktığı görülmektedir.

2.6 Siber Terörizm

En basit şekilde, siber uzay ile terörizm sözcüklerinin birleşiminden oluşan, terör gruplarının siber ortamı kullanarak terör faaliyetlerini icrası şeklinde açıklanabilecek olan siber terörizm, teknolojinin gelişmesine paralel olarak teknolojik araç ve sistemlerinin terör unsurlarınca kullanılmaya başlanmasıyla her geçen gün daha fazla yaşanır olmuştur.

Günümüzün modern terör örgütlerinin, örgütlerini yapılandırmak, eleman temin etmek, amaçları doğrultusunda organizasyon ve eylemlerini planlayarak gerçekleştirmek maksadıyla bilişim teknolojilerini yaygın olarak kullandıkları, kamu ve özel kurumların bilişim sistemlerine yönelik siber saldırı faaliyetleri gerçekleştirdikleri görülmektedir.

Ancak uluslararası ortamda, terörizmin olmadığı gibi, siber terörizmin de kabul görmüş ortak bir tanımı bulunmamaktadır. Siber terörizmin genel bir tanımı; politik veya sosyal hedefleri gerçekleştirmek, devleti ve vatandaşlarını korkutarak, aşağılayarak, baskı oluşturarak etkilemek ve hükümet politikalarını değiştirtmek maksadıyla, bilgisayarlara, ağ sistemlerine, veri tabanlarına bilişim teknolojisi yeteneklerini kullanarak yapılan yasadışı tehdit ve zarar verici saldırılar [45] şeklinde yapılmaktadır.

Tanımdan da anlaşılacağı üzere, siber terör olaylarında, silah olarak bilişim sistemleri kullanılarak, hedef olarak kişilere, kurumlara veya devlete ait bilgisayar ve

iletişim sistemleri alınarak yapılan siber saldırılar korku, şiddet içermesi yanında, can ve mal kaybına da sebep olabilmektedir.

2.7 Siber Güvenlik

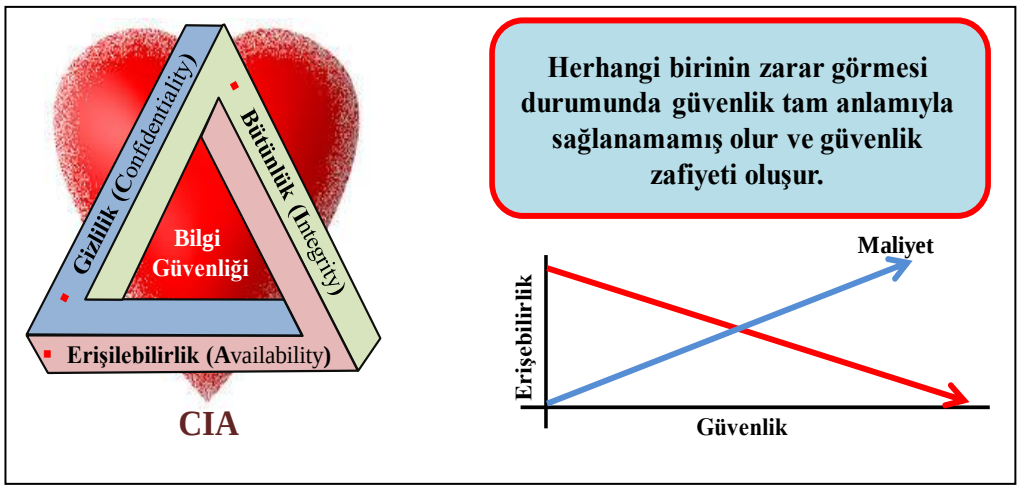
Siber saldırılarda ve olaylarda hedefin merkezinde bilginin olması nedeniyle, başlangıçta 'Bilgi Güvenliği' olarak kullanılan kavramın siber güvenliği de kapsadığına dair yaklaşımların olmasına karşın, bilgilerin sayısal ortama aktarılarak kâğıtsız ortamın hedeflendiği günümüzde, siber ortamın çok hızlı değişimi dolayısıyla yaşanan olayların da etkisiyle bunun tersinin yaygınlaştığı, siber güvenliğin bilgi güvenliğini de içerir şekilde kullanılmaya başlandığı görülmektedir.

Bu durum, "Konuyla ilgili farklı terimlerin ve tanımların ortak temalarından hareketle, siber güvenliğin devlet sırlarının korunması ve ulusal savunmanın sağlaması için temel esas olduğu…" şeklinde NATO Siber Güvenlik Çerçeve Kılavuzu'nda da açıkça vurgulanmıştır [46].

Uluslararası Telekomünikasyon Birliği (ITU) siber güvenliği "Siber uzayda kurum, kuruluş ve kullanıcıların varlıklarını korumak için kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, kuralları, risk yönetimi yaklaşımları, eylemleri, eğitimler, en iyi uygulamalar ve teknolojiler toplamıdır" [47] şeklinde tanımlanmaktadır.

Türkiye Ulusal Siber Güvenlik Stratejisi belgesinde ise siber güvenliğin; "Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi / verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini" [41] ifade ettiği belirtilmiştir.

Strateji belgesindeki bu tanımlamada görüldüğü üzere, temel amaç bilgiyi korumak ve sistemlerin devamlılığını sağlamak olup, bilgiyi, bilişim sistemlerini ve kullanıcılarını hedef alarak gerçekleştirilen siber saldırılarda kullanılan üç prensip bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması siber güvenliğin de temelini teşkil etmektedir (Şekil 2.3).



Şekil 2.3: Siber güvenliğin temel ilkeleri ve dengesi.

Siber risk ve tehditlere karşı korunmak için siber güvenliğin / savunmanın temel ilkeleri bilgi güvenliğinin kalbini oluşturmaktadır. İngilizce karşılıklarının baş harflerinden hareketle 'CIA üçgeni' (ABD Merkezi İstihbarat Teşkilatı 'Central Intelligence Agency' çağrışımı) olarak da bilinen bu ilkelerden herhangi birinin zarar görmesi durumunda güvenlik tam anlamıyla sağlanamamış olur, güvenlik zafiyeti oluşur. Maliyet ve etkinlik açısından her birinin dengesi de çok önemlidir. Diğer önemli ilkelerden bazıları da güvenilirlik, kimlik denetimi, inkâr edememe, sorumluluk, erişim denetimi ve emniyet şeklinde sıralanmaktadır.

"İşlediği bilginin 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 altyapılar olarak kabul edilmektedir. [41] Kritik altyapı bilişim sistemleri; Türkiye'de elektronik haberleşme, enerji, su yönetimi, kritik kamu hizmetleri, ulaştırma, bankacılık ve finans şeklinde 6 grupta toplanırken, Amerika Birleşik Devletleri (ABD)'nde 16 [48], Avrupa Birliği ülkelerinde ise 11 grupta [49] toplanmaktadır (Çizelge 2.1).

Siber saldırı ve olaylarının tespit edilerek engel olunması ve bilişim sistemlerinin saldırı / olay öncesi duruma döndürülmesi siber güvenliğin amaç ve hedefleri arasında yer almaktadır. Değişen ve gelişen siber saldırılara karşı aldatma teknik ve yöntemleri ile desteklenen savunma ve güvenlik tedbirleri yanında saldırganların saldırı öncesinde önleyici saldırılarla silahsızlandırılması, saldırıların yapılması durumunda misliyle

cezalandırma ve aktif savunma yani karşı saldırıların yapılması gibi seçenekler uygulanabilmektedir. [50]

Çizelge 2.1: Kritik Altyapıların Gruplanması [48, 49, 41].

ABD (16)	AB (11)	TÜRKİYE (6)
Kimyasal, Ticari tesisler, İletişim, Kritik üretim, Barajlar, Savunma sanayi, Acil servisler, Enerji, Finansal hizmetler, Gıda ve tarım, Devlet tesisleri, Sağlık ve halk sağlığı, Bilgi teknolojisi, Nükleer tesisler, Ulaşım sistemleri, Su.	Enerji, Bilgi ve iletişim teknolojileri, Su, Gıda, Sağlık, Finansal sistemler, Kamu düzeni ve güvenlik, Sivil yönetim, Ulaşım, Kimyasal ve nükleer endüstriler, Uzay ve araştırmalar.	1. Elektronik haberleşme, 2. Enerji, 3. Su yönetimi, 4. Kritik kamu hizmetleri, 5. Ulaştırma, 6. Bankacılık ve finans

Siber uzayın değişerek ve gelişerek artan tehlikelerinin farkında olan ülkeler siber güvenliği önemsemekte, siber tehditleri ulusal güvenliğe karşı en önemli tehdit unsurlarından biri olarak kabul etmekte ve başta ülkenin kritik altyapıları olmak üzere bireylerinin, kurum ve kuruluşlarının varlıklarını siber risklere, tehditlere ve saldırılara karşı korumak için çözümler üreterek uygulamaya koymayı zorunluluk olarak görmektedirler. Çünkü başlangıçta küçük çapta ve bir kısmı zararsız denebilecek seviyedeki tehditler, riskler ve saldırılar, teknolojinin gelişmesi ve internetin yaygınlaşmasıyla birlikte büyüyerek 'Siber Savaş' halini almıştır.

2.8 Siber Savaş

İnsanlık tarihi boyunca amacı, usulleri ve kullanılan silahları değişse de, var olduğu görülen savaşın devletler hukukuna göre tanımlarından birisi; "Bir toplumun, bir ulusun veya devletler topluluğunun isteklerini diğer bir ulus ve devletler topluluğuna zorla kabul ettirmek amacıyla giriştikleri bir mücadele, uluslararası hukuk kurallarına uygun şekilde devletlerarasında yürütülen silahlı bir çatışma, bir çekişme" [54] şeklinde ifade edilmektedir.

Türk hukukuna göre ise savaş; "Devletin bekasını temin etmek, milli menfaatleri sağlamak ve milli hedefleri elde etmek amacıyla, başta askeri güç olmak üzere, Devletin maddi ve manevi tüm güç kaynaklarının, hiçbir sınırlamaya tabi tutulmadan kullanılmasını gerektiren silahlı mücadele" [52] olarak tanımlanmaktadır.

Siber uzayın, kara, deniz, hava ve uzay savaş alanlarına, bu alanları da içerisine alacak şekilde 5'inci savaş alanı olarak eklenmesiyle, özellikle son on beş-yirmi yıllık zaman süresince, dünya kamuoyu siber saldırı ve siber suç terimlerine alışırken siber savaş terimi ile daha fazla meşgul olmaya başlamıştır. İlk yıllarda basit tekniklerle organize olmayan test saldırıları, kısa süre sonra ekonomik güdülerin de öne çıktığı ve komuta kontrol merkezleri aracılığıyla daha gelişmiş teknik ve taktiklerle gerçekleştirilen siber saldırılara dönüşerek siber savaşa doğru gelişim göstermiştir.

Ancak, siber savaşın geçmişte hiç olmadığını, günümüzde gerçekleşmediğini ve gelecekte de gerçekleşmesinin pek olası olmadığını, politik güdümlü siber saldırıların savaş kadar eski olan sabotaj, casusluk ve yılıcı faaliyetlerin karmaşık şekilleri olduğunu [53] savunanlar görülmektedir. Bu görüşü savunanlara karşın, savaşa yönelik stratejik kuramın kuvvet, şiddet ve ölümcüllük özelliğini taşıdığını, siber saldırıların ve siber savaşın da bu üç kavramı taşıması nedeniyle savaş eylemi olarak kabul edilmesi gerektiği [54] vurgulanmaktadır.

'Bilgi Güvenliği' ile 'Siber Güvenlik' kavramlarının iç içe olma durumunda açıklanmaya çalışıldığı gibi, önceleri bilgi savaşının bir alt bölümü olarak görülen siber savaşın, günümüzde bilgi savaşı ile aynı anlamda ve daha yaygın olarak kullanılmaya başlandığı görülmektedir. Nitekim bazı sözlüklerde olduğu gibi, Birleşmiş Milletler Terimler Sözlüğü'nde de 'Siber Savaş', 'Bilgi Savaşı'nın eş anlamlısı olarak gösterilmekte ve "Bilgisayar sistemlerinin düşman sistemlerine zarar vermek veya yok etme maksadıyla kullanıldığı bir savaş tipi" şeklinde tanımlanmaktadır. Yapılan tanıma ek olarak ta, "Düşmanın politik, askeri veya ekonomik bilgilerine ve bilgi sistemlerine zarar vermek veya kendi bilgilerini ve bilgi sistemlerini korumak için bilgi üstünlüğü sağlamaya yönelik faaliyetleri kapsayabileceği" [55] belirtilmektedir. Bu tanımlamada dikkat edilmesi gereken husus, devletler hukukuna göre savaşın tanımlamasında olduğu gibi, siber savaş kapsamına giren faaliyetlerin toplum, ulus veya devlet ya da devletler grubu tarafından icra edilen faaliyetler olmasıdır.

Bu kapsamda siber savaş, "Devletler veya devlet benzeri aktörler tarafından gerçekleştirilen, kritik ulusal altyapıları, askeri sistemleri veya ülke için önemli endüstriyel yapıyı tehdit eden, simetrik veya asimetrik, saldırı veya savunma maksatlı sayısal ağ faaliyetleridir" [51] şeklinde tanımlanmaktadır. Diğer bir tanımlamayla,

siber savaş, siber ortamdaki değerli varlıkları korumak için karşı tarafın bilişim sistemlerine zarar vermek, bilişim hizmetlerini yavaşlatmak, aksatmak, durdurmak, bozmak veya ele geçirmek maksatlarıyla yapılan saldırılardır [42].

Yapılan pek çok tanımdan hareketle siber savaş, siber ortamda bilişim sistemleri kullanılarak bilişim sistemlerine yönelik yapılan saldırılar ile bu saldırılara karşı alınan güvenlik tedbirlerinden oluşan faaliyet ve mücadeleler bütünüdür ve başlamış devam etmektedir. Savaşın klasik tanımında olduğu gibi, siber savaşın da maksatlarından birisi savaşı kazanarak istek veya istekleri diğer bir ulus ve devletler topluluğuna zorla kabul ettirmektir. Karşı tarafı yapmak istediğinden vaz geçirmek de buna dâhildir. Ancak savaşta en mükemmeli hep kazanmak olmayabilir. M.Ö. 500'lü yıllarda yaşamış olan ünlü Çinli filozof ve savaş stratejisti komutan Sun Tzu'nun dediği gibi "En iyisi savaşmadan baş eğdirmektir." [3] Yani bir anlamda saldırganı isteğinden, saldırıdan veya savaştan caydırmak, söz konusu siber savaş olduğuna göre 'Siber Caydırıcılık' en iyisi olabilir.

2.9 Siber Caydırıcılık

Halk arasında genellikle korkutarak cesaret kırmak ve vazgeçirmek anlamlarında kullanılan 'caydırmak' sözcüğünden türetilen 'Caydırıcılık' kavramı Türk Dil Kurumu (TDK) Sözlüğünde "Bir saldırganlığı önlemek ve engellemek için önlem alma işi" [56] olarak açıklanmaktadır.

İnsanların günlük yaşamda her an iç içe bulundukları caydırıcılık (Şekil 2.4); hukuksal alanda ceza veya hapis korkusuyla suç işlemekten kaçınma [57], uluslararası ilişkilerde yani diplomasi alanında karşıdaki devleti belirli politik davranışlara yönlendirme veya politik isteklerinden vazgeçirme davranışı [58] olarak ifade edilirken, askeri alanda ise düşmanı uyguladığı baskının veya silahlı çatışmanın olumsuz sonuçlarının kendisi için sağlayacağı kazançlardan daha ağır olacağına ikna etmek [59] olarak tanımlanmaktadır.

Bir saldırı veya savaş söz konusu olduğunda caydırıcılığın yaygın olarak kullanılan anlamı ise, bir düşmanın belirli bir eylemi gerçekleştirmesi durumunda, maliyetlerini artırıp faydalarını azalarak, maliyet / fayda hesaplamasına yönelik tahmini üzerinde yönlendirilmesidir [60]. Caydırıcılığı genel anlamda "Karşı tarafa düşmanca eylemleri yapmama konusunda gözdağı verme" şeklinde açıklayan Libicki, siber caydırıcılığı;

“Siber ortamda saldırganın eylemini boşa çıkarma veya cezalandırma (misilleme tehdidi) yoluyla saldırıdan vazgeçirme” [22] olarak tanımlamaktadır.

Şekil 2.4: Günlük yaşamda basit caydırıcılık uygulamaları.

Yukarıdaki açıklamalardan doğrultusunda kısaca; “Siber ortamda bilişim sistem ve altyapılarına saldırı başlatacak saldırganı saldırıdan vazgeçirmek” şeklinde tanımlanabilecek siber caydırıcılık, aynı zamanda bir siber güvenlik sağlama yöntemi olmaktadır. Siber caydırıcılıkta temel esas ve önemli olan ise, siber saldırıların / savaşın doğru zamanda, doğru hedefe, doğru teknik ve yöntemlerle icrasıdır.

Günlük yaşamda karşılaşılan caydırıcılık uygulamalarından da görüleceği üzere her türlü caydırıcılık stratejisinde en önemli esaslardan birisi caydırıcılık sağlayacak gücün belirgin şekilde inandırıcılığıdır. Siber caydırıcılıkta inandırıcılığın sağlanması için, diğer caydırıcılık alanlarında da olduğu gibi öncelikle üç koşulun yerine getirilmesi gerekir. Bunlar, saldırganı cezalandırmak için yapabilirlik yeteneği, yapmak için kararlılık iradesi ve yapabilirlik yeteneği ile kararlılık iradesinin saldırgana duyurulması için iletişimdir. [61] Bu üç koşulun yerine getirerek inandırıcılık sağlamak, belirsizlikleri en aza indirip siber saldırıların / savaşın zamanını ve hedefini doğru şekilde belirleyerek doğru teknik ve yöntemlerle icra etmek için ise en başta gelen ihtiyaçlardan birisi ‘Siber İstihbarat’ olarak ortaya çıkmıştır.

2.10 Siber İstihbarat

Hangi alanda olursa olsun savaşın vazgeçilmezi olan konu istihbarattır. Sun Tzu, zaferin önceden görülebileceğini, düşmanı ve kendini iyi bilenin hiçbir savaşta tehlikeye düşmeyeceğini, karşısındakini bilmeyen, sadece kendini bilenin bir kazanıp bir kaybedeceğini, karşısındakini de kendini de bilmeyenin her savaşta mutlaka

tehlikeye düşeceğini [3] belirterek önemini vurguladığı istihbarat, TDK Sözlüğünde "Yeni öğrenilen bilgiler, haberler, duyumlar" [62] şeklinde tanımlanmaktadır.

Zamanla ve günün şartlarına göre değişen, İngilizcede 'Intelligence' olarak ifade edilen istihbarat aynı zamanda 'Akıl' anlamına da gelmekte, pek çok sözlükte, kaynak ve dokümanda da faklı şekillerde tanımlanmaktadır. İstihbarat sözcüğünün özünde aklın yanında, 'Bilgi' bulunmaktadır. İstihbaratın temel hedefi de, ihtiyaç duyulan bilginin akılcı yöntemlerle, toplanması, analiz ve değerlendirmesinin yapılması ve zamanında kullanıma sunulmasıdır. Bu ifadelerden hareketle istihbarat, kişi, toplum, kurum, kuruluş, devlet veya devletler topluluğu, her seviyede oluşum açısından, başta güvenlik ve refahın sağlaması için olmak üzere, her maksatla önemlidir.

Ulusal güvenliğin sağlanması, ulusal çıkarların elde edilmesi ve diğer tanımların ortak yönleri de dikkate alınarak genel anlamda istihbarat; "Ulusal güvenliği tehdit edecek unsurlara karşı koruma sağlamak amaçlı yahut politika yapıcıların, ulus menfaatini olumlu şekilde etkileyecek kararların alınması hususunda ihtiyaç duyduğu bilgilerin açık, yarı açık ve gizli kaynaklardan elde edilip doğruluğuna göre sınıflandırılması, karşılaştırılması ve analiz edilmesi süreci sonunda ulaşılan bilgidir" [63] şeklinde tanımlanmaktadır.

Bu tanımlamadan da hareketle, siber saldırı ve olaylara karşı savunma yani siber güvenlik için, ulusal çıkarların korunması maksadıyla siber saldırıların / taarruzların yapılması veya siber caydırıcılık sağlanması, kısaca siber savaşın kazanılması için siber ortamda ihtiyaç duyulan bilgilere ulaşmak maksadıyla yapılan istihbarata siber istihbarat denir. Devlet olarak siber ortamda ihtiyaç duyulan bilgilerin elde edilmesi veya kendi bilgilerimizin başka devlet ya da oluşumları tarafından elde edilmesine karşı konulması için bütün faaliyetler de, aslında birer siber savaş olarak adlandırılmaktadır.

Teknolojinin ve siber ortamın sağladığı imkânların teknik ve insan istihbaratı ile birlikte kullanılmasıyla siyasi, askeri, ekonomik, sosyal vb. alanlarda kişi, grup, toplum, örgüt, firma ya da ülkeler tarafından icra edilen siber casusluk faaliyetleri ile kısa sürede çok az maliyetle çok önemli bilgiler elde edilebilmektedir. Genel anlamda istihbaratın stratejik, operatif veya taktik her seviyesinde icra edilebilen siber istihbarat faaliyetleri ile elde edilen bilgiler sadece siber savaş için değil her türlü savaşta, kişi, toplum veya devletlerin ülke içi ya da dışı her alanında kullanılabilmekte ve bunun

sonucunda sağlanan yüksek üstünlükler ve kazanımlar ile 'Siber Güç' daha da geliştirilerek artırılabilmektedir.

2.11 Siber Güç

Tarihin başlangıcından günümüze her alanda var olan güç kavramının anlamı, TDK sözlüğünde "Fizik, düşünce ve ahlak yönünden bir etki yapabilme veya bir etkiye direnebilme yeteneği, kuvvet" [64] şeklinde ifade edilmektedir. Diğer pek çok sözlükte de eş anlamı 'Kuvvet' sözcüğü gösterilmekte olan 'Güç' kavramı için kısaca "Etki yapabilme veya etkiye direnebilme kapasitesi / yeteneği" ortak tanımlamasında buluşulmaktadır.

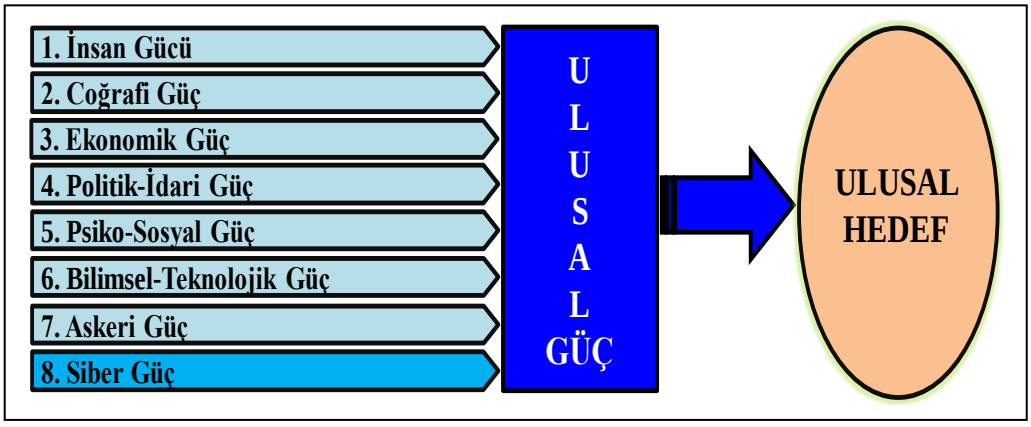
Güçlü olmak caydırıcı olmaktır. Genel anlamda, "Hedeflere ya da amaçlara erişme becerisi, daha belirgin olarak da arzulanan sonuçları elde etmek için başkalarını etkileme becerisi" [65] olarak da tanımlanan gücün ölçülmesi için çok çeşitli hesaplamalar ve ölçüm yöntemleri geliştirildiyse de mutlak olmadığı açıktır. Çünkü uluslararası ortamda bir devlet diğer devlete karşı güçlü iken başka bir devlete karşı güçsüz olabilmektedir.

Son yıllarda, güç konusunda yapılan stratejik çalışmalarda, Sert Güç (Zorlama, tehdit ya da rüşvet yoluyla arzulanan sonuçları elde etme becerisi), Yumuşak Güç (Çekicilik, cezbetme ya da ikna yoluyla arzulanan sonuçları elde etme becerisi) ve Akıllı Güç (Sert ve yumuşak güçlerin ustalıkla birleştirilmesi) [66] gibi çeşitli yaklaşımların uygulandığı ve sonuçları üzerinde durularak, yeni stratejiler geliştirilmeye çalışıldığı görülmektedir. Bütün yaklaşımların da ortak hedefi ulusal gücün, ulusal çıkarların elde edilmesi, ülkenin kalıcılığı ve gönenci için etkinlikle kullanılmasıdır.

Stratejik yaklaşımlarda kısaca "Bir ulusun maddi (maddesel) ve manevi (moral) değerleriyle toplam potansiyel gücü" olarak tanımlanan 'Ulusal Güç'; bir devletin ulusal çıkarlarını sağlamak ve ulusal hedeflerini elde etmek için kullanabileceği insan gücü, coğrafi güç, ekonomik güç, politik ve idari güç, psikososyal güç, bilimsel ve teknolojik güç, askeri güç şeklinde 7 ayrı güç unsurundan [67] oluşmaktadır (Şekil 2.5).

Teknolojinin gelişmesi, siber ortamın hayatın vazgeçilmezleri arasına girmesi ve 5'inci harekât alanı olarak kabul edilmesi sonrasında, varlığının her geçen gün

öneminin arttığı görülen ‘Siber Güç’, “Siber ortamda sahip olunan bilgi sistemleri ve altyapıları ile bunların etkin olarak kullanılması yeteneği” [18] olarak tanımlanmaktadır.



Şekil 2.5: Ulusal güç unsurları içerisinde ‘siber güç’.

Kısaca ‘Siber ortama hâkimiyet’ demek olan siber gücü, ulusal güç unsurlarından bilimsel ve teknolojik güç unsuru altında değerlendirmek yerine, 8’inci güç unsuru kabul etmek daha doğru olabilir. Çünkü siber güç oluşumu incelendiğinde, siber gücün diğer bütün ulusal güç unsurlarını etkilediği, onların etkilerini daha da artırılabildiği ve tek başına da etkin olarak kullanılabildiği görülmektedir.

Siber güç, gücün boyutları ve kullanılması yöntemleri açısından, temeli askeri ve ekonomik güce dayanan sert gücün yanında, teknolojinin ve bilişim sistemlerinin yaygın olarak kullanılmasıyla kendini gösteren yumuşak güç içerisinde yer almaktadır. Ülkelerin sahip oldukları siber gücün, hem saldırı aracı, hem de saldırı hedefi olabileceği, tarafların birbirine zarar vermek, siber güçlerini zayıflatmak veya bazı unsurlarını devre dışı bırakmak maksadıyla karşılıklı siber güçlerini kullanabilecekleri kararsızlığa meydan bırakmayacak şekilde ortadadır.

Bir ülkenin savaş alanında sert gücünün büyüklüğünü ölçerken, Taarruz (Saldırı) ve Savunma (Güvenlik) açısından değerlendirmek yeterli olurken, siber güç söz konusu olduğunda bu iki faktöre üçüncü bir faktör olarak ‘Bağımlılık’ faktörünün eklendiği görülmektedir. Bağımlılık bir ülkenin siber saldırılara (taarruzlara) açık sistemlere ve ağlara yani siber uzaya ne kadar gereksinim duyduğunun ölçüsü [25] olarak açıklanmaktadır.

Askeri silah, araç ve gereçlerin nitelik ve miktar olarak artırılması sert gücü artırırken, siber ortamda bilişim sistemlerinin yaygınlaşarak yaşamın her alanına

girmesi ve özellikle kritik altyapıların bilişim sistemlerine ve ağlarına bağımlılığının artmasına sebep olmaktadır. Bunun sonucunda bilişim sistem ve ağlarının güvenliğinin sağlanması daha zorlaşacağı (siber saldırılarda verilebilecek hasar ve zarar miktarı daha yüksek olabileceği) için siber ortama bağımlılığın, asimetrik bir etki sağlayacak olan siber gücü azalttığı değerlendirilmektedir.

Ülkelerin siber güçlerini ölçmek için açık ve somut yol ve yöntemler olmasa da, bu konuda çeşitli çalışmaların yapıldığı ve bazı tespitlerin ortaya konulduğu görülmektedir. Bu çerçevede yapılan ve Çizelge 2.2'de görüldüğü üzere, ABD, Rusya, Çin, İran ve Kuzey Kore'nin yer aldığı bir çalışmada, siber taarruz gücü düşük olmasına karşın savunma ve bağımlılık değerleri dolayısıyla siber gücü ve yeteneği en yüksek olan ülkenin Kuzey Kore olduğu değerlendirilmiştir [25].

Çizelge 2.2: Ülkelerin siber güç ve yeteneklerinin değerlendirilmesi [25].

Devlet	Siber Saldırı	Siber Savunma	Siber Bağımlılık	Toplam
ABD	8	1	2	11
Rusya	7	4	5	16
Çin	5	6	4	15
İran	4	3	5	12
Kuzey Kore	2	7	9	18

Siber güç, siber caydırıcılık demektir. Siber gücün artırılması ve etkin yönetimi etkin siber caydırıcılık sağlar. Siber gücün artırılması için siber ortama bağımlılığın azaltılması kolay ve basit bir çözüm gibi görülebilir, ancak siber ortamın sağladığı kazanım ve üstünlüklerden vazgeçilmesi doğru bir hareket tarzı olamaz. Doğru hareket tarzı, bütüncül bir yaklaşımla savunma, taarruz ve bağımlılık faktörlerinin birlikte ele alınması, özellikle bilişim sistemleri geliştirilirken ve yaygınlaştırılırken savunma boyutunun da mutlaka düşünülmesidir. Siber savaş durumunda, güçlü bir siber silahı dünyaya uygulamayı düşünen ülkelerin, o silaha karşı kendini savunmayı planlamadılarsa, o savaşı kaybetmeye mahkûm olacakları [25] unutulmamalıdır. Siber gücün üçüncü boyutu olarak kabul edilen 'Akılcı Güç' kapsamında değerlendirilerek oluşturulmalı, geliştirilmeli ve diğer güç unsurlarıyla koordineli olarak yönetilmelidir.

3. SİBER SAVAŞ

Bilgisayarın icadı sonrası, teknolojinin gelişmesine paralel olarak bilgi ve iletişim teknolojilerindeki gelişmelerle siber ortamın sağladığı imkân ve kolaylıklar daha da artmıştır. Süreç içerisinde bilişim sistemleri yaşamı her geçen gün kendisine daha bağımlı hale getirirken, bilgilere ve bilişim sistemlerine yönelik kötü niyetli hareketler ve saldırılar başlamış, saldırılar geçen her gün çeşitlenerek ve şiddetlenerek artışa devam etmektedir.

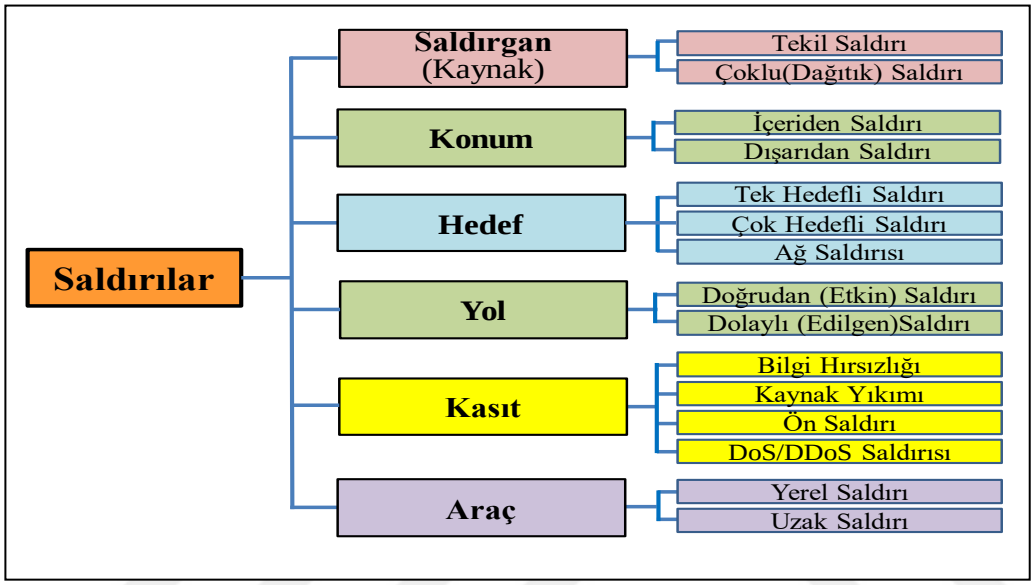
Siber ortamın tehdit, saldırı, cana ve mala zarar verme vb. amaçlarla kullanılması sonucunda kişilerin, toplumların ve ülkelerin uğradığı büyük zararlar güvenlik anlayışında büyük değişikliklere yol açarken savaşların şeklini, teknik ve yöntemlerini de değiştirmiştir. Bu çerçevede siber saldırıların ve taarruzların sonucunda, siber güvenliğin ulusal güvenlik sorunu ve ulusal güvenliğin ayrılmaz bir parçası olduğunun kabul edilmesine sebebiyet veren, "bir devletin başka bir devletin bilgisayar sistemlerine ve ağlarına sızarak hasar veya kesinti yaratmak üzere hareket etmesi" [25] şeklinde de tanımlanan siber savaşlar ortaya çıkmıştır.

Bilgi Güvenliği Derneği Yönetim Kurulu Başkanı ve Gazi Üniversitesi Teknoloji Fakültesi Öğretim Üyesi Prof. Dr. Mustafa Alkan'ın 09 Mayıs 2012'de TBMM Bilişim ve İnternet Araştırma Komisyonu'na **"**İnternette Bilgi Güvenliği" konusunda yapığı sunum sırasında belirttiği gibi; dünya artık 'siber saldırılar ve siber savaş' olgusuyla karşı karşıya bulunmakta, Türkiye siber saldırılarla en yoğun maruz kalan ülkeler arasında olup, bazen ilk 3 ve bazen de ilk 10 içinde yer almaktadır. [68]

3.1 Siber Saldırıların Çeşitleri ve Yapılması

Siber savaşlara temel teşkil eden siber saldırı ve olaylar pek çok şekilde sınıflandırılmakta, çeşitlere ve gruplara ayrılarak tanımlanmaktadır. Saldırıların en yaygın sınıflandırması Şekil 3.1'de toplanmıştır.

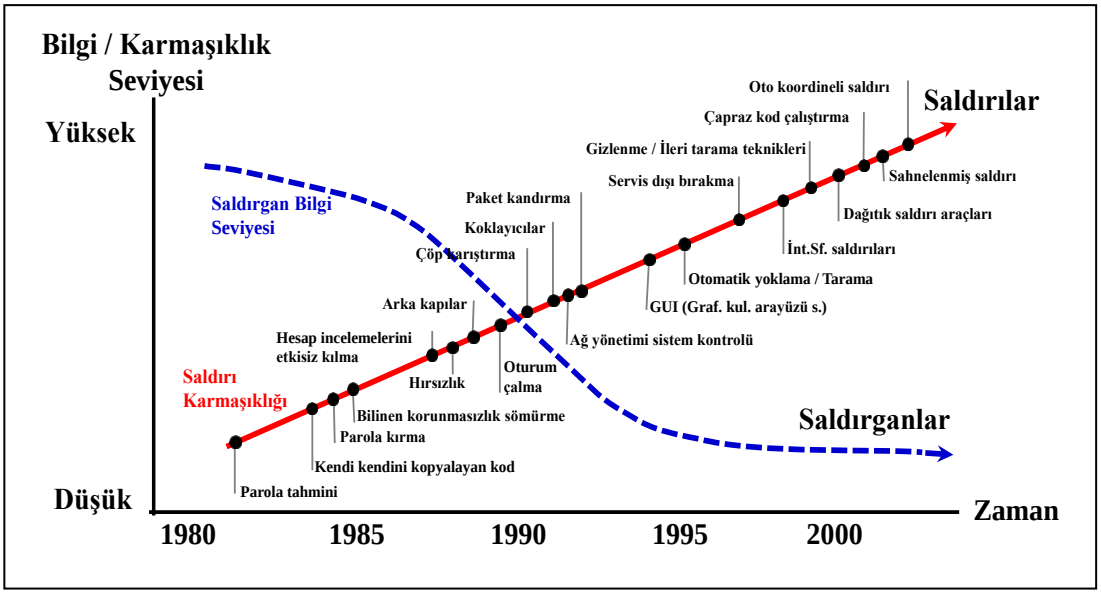
Saldırılar yapıldığı kaynağa yani gerçekleştiren saldırganın sayısına göre tekil veya çoklu (dağıtık) saldırı, yapıldığı konuma göre içeriden veya dışarıdan saldırı, saldırı hedefine göre tek / çok hedefli veya ağ saldırısı, saldırı yol ve yöntemine göre doğrudan (etkin) veya dolaylı (edilgen) saldırı, saldırının kasıt veya maksadına göre bilgi hırsızlığı, kaynak yıkımı, ön saldırı ve servis dışı / dağıtık servis dışı bırakma (DoS / DDoS) saldırıları, saldırı sırasında kullanılan araçlara göre yerel veya uzak saldırı şeklinde sınıflandırılmaktadır [69].



Şekil 3.1: Siber saldırıların sınıflandırılması / çeşitleri [69].

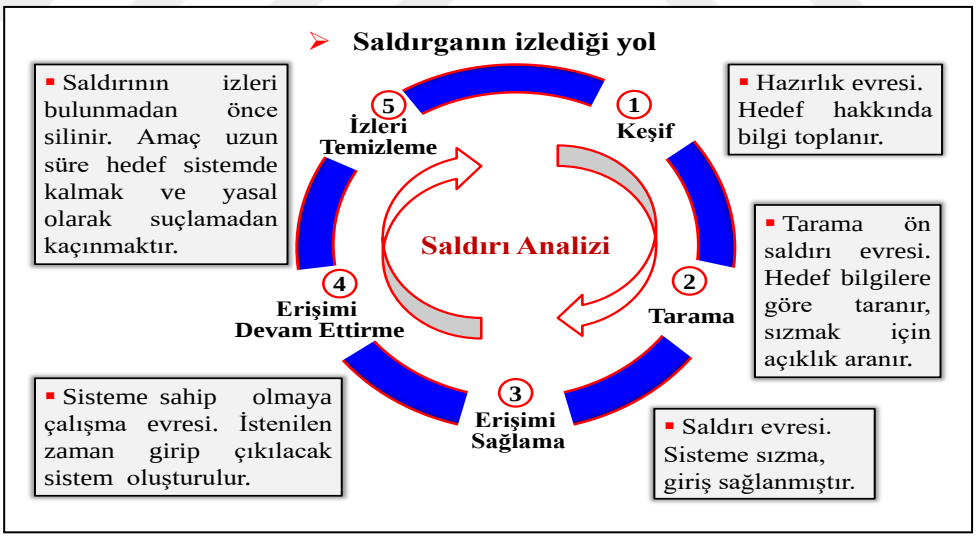
Saldırganlar bilgiyi ve kullanıcıları hedef alarak eylemlerini gerçekleştirirken temel olarak üç prensibe göre hareket etmektedirler. Bunlar, gizli bilgilerin elde edilmesi veya bilginin gizliliğinin açık edilmesi, bilgiye zarar verilerek değiştirilmesi yani bütünlüğünün bozulması ve bilgiye kullanıcıların erişiminin engellenmesi yani kullanılabilirliğinin önlenmesidir.

Ülke veya kurum içinden veya dışından, suç örgütleri, teröristler, bilgisayar korsanları, casuslar vb. saldırı düzenleme kapasitesine sahip kişi, grup ve devletler tarafından yapılabilen siber saldırıların teknoloji geliştikçe çeşitleri, şiddeti ve sayıları ile teknik açıdan karmaşıklığı artarken, saldırı yapma uzmanlığı ve becerisi diğer bir ifadeyle saldırganların bilgi seviyelerinin ve uzmanlıklarının ise gittikçe azaldığı, buna paralel olarak tehdit kaynakları ve risklerin yanında saldırılar sonucunda verilebilecek zararların daha da arttığı ve saldırıları tespit ve önleme tedbirlerinin ise zorlaştığı gözlenmektedir (Şekil 3.2) [69, 70].



Şekil 3.2: Süreç içerisinde saldırganların bilgi seviyesi ve siber saldırılar [69, 70].

Siber savaşlara temel oluşturan ve planlanarak gerçekleştirilen siber saldırı ve olaylarda, saldırganların izlediği yol incelendiğinde genel olarak birbirini takip eden beş safhada gerçekleştirildikleri gözlenmektedir. Bu safhalar Şekil 3.3'de de görüleceği üzere; keşif, tarama, erişimi sağlama, erişimi devam ettirme ve izleri temizleme safhalarıdır. [71]



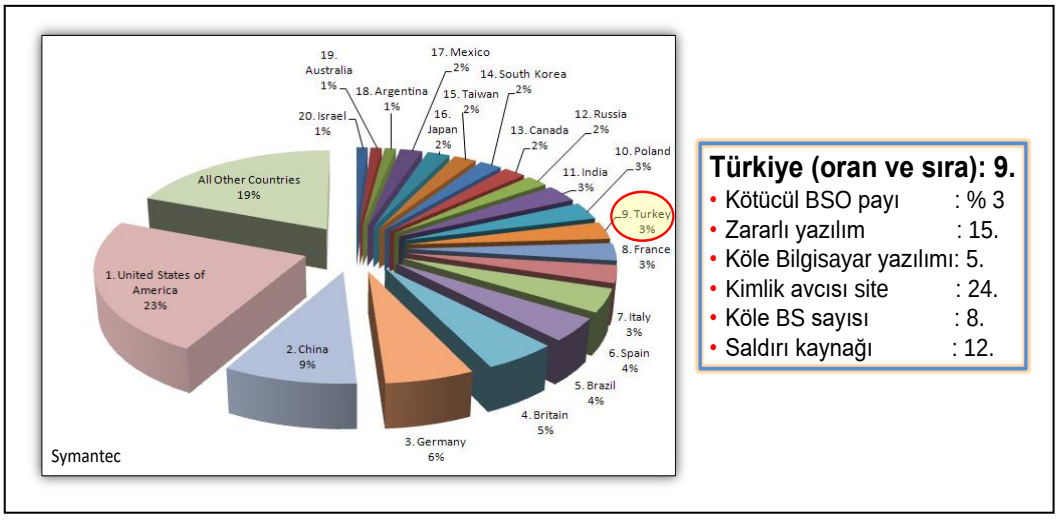
Şekil 3.3: Siber saldırıların gerçekleştirilmesi safhaları [71].

- **Keşif safhası:** Bu safha hazırlıkların yapıldığı evredir. Siber ortamda saldırının gerçekleştirileceği hedefle ilgili olarak istihbarat çalışmaları yapılır ve ihtiyaç duyulan bilgiler toplanır.

- **Tarama safhası:** Ön saldırı evresi olarak da adlandırılan bu safhada hedef keşif safhasında elde edilen bilgilere göre taranır ve saldırının gerçekleştirilmesi için hedefe erişim sağlamak maksadıyla açıklıklar aranarak tespit edilmeye çalışılır.
- **Erişimi sağlama safhası:** Saldırı evresi başlar ve bu safhada hedef bilişim sitemine sızma girişimi başlatılarak giriş sağlanır.
- **Erişimi devam ettirme safhası:** Bu safha sızmanın sonucu giriş yapılan hedef sisteme sahip olmaya çalışma evresidir. Bu safhada hedefe istenilen zamanda girip çıkılacak yapısal bir sistem oluşturulur. Oluşturulan bu yapı içerisinde hedeflenen eylemler gerçekleştirilir.
- **İzleri temizleme safhası:** Saldırının tamamlanması ve sonuçlandırılması safhası olan son safhada, saldırının izleri bulunmadan önce silinir. Bu safhada amaç, uzun süre hedef sistemde kalmak ancak herhangi arama tarama sırasında tespit edilmekten kaçınarak yasal olarak suçlanmaktan kurtulmaktır.

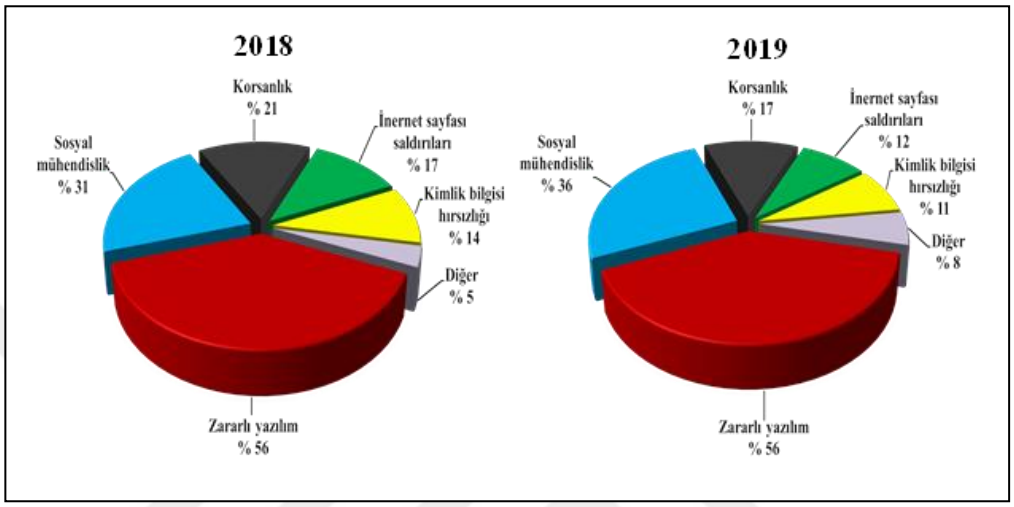
3.2 Siber Saldırıların İstatistiksel Durumu

Siber saldırı ve olayların çeşit ve yöntemleri ile şiddetleri ve verilen hasar ve zararlar yıldan yıla, aydan aya ve hatta günden güne artarak değişmektedir. Konuyla ilgili yapılan tespitlerde rakamsal olarak toplamlar çeşitli kaynaklarda farklılıklar göstermekle birlikte istatistiksel sonuçlarda benzerlikler bulunmaktadır. 2015 yılına ait bir çalışma sonuçlarına göre, Şekil 3.4'de görüldüğü üzere, dünyada siber saldırı ve olayların en çok yaşandığı ilk 20 ülke içerisinde bulunan Türkiye, hem saldırılan hem de saldıran ülke olarak ilk 10 ülke arasında yer almaktadır. [72].



Şekil 3.4: Dünyada siber saldırı ve olayların ülkelere göre dağılımı [72].

Dünyada 2018 ve 2019 yıllarına ait siber saldırılara ait çeşitli kaynaklardan derlenerek elde edilen tespitlerin analiz edilen sonuçları ile ilgili veriler [73] şu şekildedir. 2018 yılında ortalama 702,06 milyon siber saldırı yapılırken, 2019 yılında % 15,75 artarak 812,67 milyon saldırı yapılmıştır. Saldırıların türlerine bakıldığında, her iki yılda da kötücül yazılımlar (% 50 üzeri) ve sosyal mühendislik saldırıları (% 30 üzeri) üst sıralarda yer almaktadır (Şekil 3.5).



Şekil 3.5: 2018-2019 Siber saldırıların dağılımı [73].

Bütün dünyada siber saldırı ve olayların iş alanlarına dağılımına bakıldığında, sırasıyla kamu kurumları ile endüstri, sağlık ve finans iş kolları en üst sıralarda yer almaktadır (Çizelge 3.1). Siber saldırlar sonucu iş alanlarının ortalama finansal kayıpları 20118 yılında 11 milyon ABD dolarından 2019 yılında % 18 artarak 13 milyon ABD dolarına yükselirken, 2018 yılında 608 milyar ABD doları olan toplam evrensel zarar 2019 yılında % 64'ün üzerinde artarak bir trilyon ABD dolarını geçmiştir.

Türkiye'de 2018 yılında 72.975 siber saldırı yapılırken, 2019 yılının ilk yarısında bu sayı 95.202 olmuş [74] ve yıl bazında toplamda bir önceki yıla göre % 105'ten fazla artış yaşanarak 150.000'i bulduğu [75] belirtilmiştir. Türkiye'de siber saldırıların çoğunlukla elektronik haberleşme altyapıları ve kamu kurumları başta olmak üzere, enerji, bankacılık ve sağlık gibi kuruluşları hedef aldığı görülmektedir. Bu saldırıların % 90'ından fazlasını dağıtık servis dışı bırakma (DDoS) ve Oltalama (Phishing) saldırıları oluşturmaktadır.

Çizelge 3.1: Siber saldırı ve olayların iş alanlarına dağılımı ve zarar durumu [73].

2018 Yılı		İş Alanları	2019 Yılı	
2018 Zararı Ortalama 11 milyon $	% 19	Kamu Kurumları	% 16	2019 Zararı Ortalama 13 milyon $ (% 18,2 artış)
	% 11	Sağlık	% 10	
	% 10	Finans - Bankacılık	% 6	
	% 7	Eğitim	% 6	
	% 5	Bilişim Teknolojileri	% 4	
	% 4	Perakende Satış	% 4	
Evrensel Toplam 608 milyar $	% 4	Endüstriyel Kuruluşlar	% 10	Evrensel Toplam 1 Trilyon $ (% 64,5 artış)
	% 4	Eğlence	% 6	
	% 4	Kripto Para	% 4	
	% 3	Çevrimiçi Servisler	% 6	
	% 2	İletişim	-	
	% 1	Ulaşım	-	
	% 26	Diğer	% 28	

Geçmişten günümüze dünyada ve Türkiye'de yaşanan, bir kısmı saygınlık kaybı vb. nedenlerle gizlenmekle birlikte yazılı ve görsel basın dâhil açık kaynaklara da yansıyan, sonuçları incelendiğinde ciddi hasar ve zararlara sebebiyet verdiği anlaşılan önemli siber olayların ve saldırıların bazıları M.Şenol'un "Siber güçle caydırıcılık ama nasıl?" konulu çalışmasında [76] incelenmiş ve yeni ilavelerle müteakip maddelerde sunulmuştur.

3.3 Dünyada Yaşanan Önemli Siber Saldırılar ve Olaylar [76]

- **2000'de Avustralya'da arıtma tesisi bilgi sistemlerine saldırı ve pis suların şehre bırakılması:** 28 Şubat-23 Nisan 2000 tarihleri arasında, Avustralya'nın Maroochy bölgesinde, arıtma tesisi bilgi sistemlerine müdahale sonrasında pis kanalizasyon suları, en az 40 defa, parklara, nehirlere hatta turistik bir otelin zeminine bırakılmıştır.

- **2003'te ABD'nin sekiz eyaletinde 2 gün süren, ölümlere ve zarara yol açan elektrik kesintisi:** 14 Ağustos 2003'te ABD'nin sekiz eyaletinde 50 milyon kişiyi etkileyen, bazı şehirlerde 2 gün süren, 11 kişinin ölümüne ve 6 milyar dolar zarara yol açan ve tarihe 'Kuzey Doğu Kesintisi' olarak geçen ABD tarihinin en önemli elektrik kesintisinin nedenlerinden birisinin enerji yönetim sisteminde kullanılan bir yazılımdan kaynaklandığı saptanmıştır.

- **2007'de Estonya bilgi sistemlerine yapılan saldırıların ülke çapında faaliyetleri durma noktasına getirmesi:** 2007 yılı Nisan ve Mayıs aylarında, Rus bilgisayar

korsanlarının Estonya bilgi sistemlerine sızması, özellikle internet ve bankacılık hizmetlerini durma noktasına getirmiş, ülke çapında ciddi ekonomik ve toplumsal zararlar yaşanmıştır.

- **2007'de İsrail savaş uçaklarının Suriye nükleer tesisini imha ederek zayiatsız dönmesi sırasında Suriye hava savunmasının hiçbir hedef görememesi:** 6 Eylül 2007'de İsrail savaş uçakları Türkiye-Suriye sınırını takip ederek hiçbir engelle karşılaşmadan Suriye topraklarına girmiş, nükleer tesisi yerle bir ederek, en ufak bir zayiat vermeden evlerine dönmüşlerdir. İsrail uçaklarının saldırıları sırasında Suriye hava savunması siber saldırılarla desteklenen karma saldırılar nedeniyle hiçbir hedef görememişlerdir.

- **2008'de Gürcistan'a yapılan siber saldırılar sonucu ciddi sıkıntılar yaşanması:** 2008 yılı Ağustos ayında, Rusya-Gürcistan savaşında, başta devlet başkanlığı internet sitesi olmak üzere Gürcistan'ın neredeyse tüm internet sayfaları ele geçirilmiştir. Finans merkezleri, haberleşme sistemleri ve elektrik santralleri ciddi sıkıntılar yaşamıştır.

- **2010'da İran nükleer sistemlerine ciddi sorunlara sebep olan 'Stuxnet' yazılımı saldırısı:** 2010 yılı Temmuz ayında keşfedilen, endüstriyel kontrol sistemlerini hedefleyen ve bilinen en tehlikeli zararlı yazılım olduğu düşünülen 'Stuxnet' yazılımı ile İran nükleer zenginleştirme programına saldırıldığı ve ciddi zararlar verildiği ortaya çıkmıştır. Bu saldırı, yazılım sistemlerine fiziksel zarar vermesi ile de bir ilk olmuştur.

- **2010'da WikiLeaks'in yayınladığı belgeler ile diplomasiyi etkilemesi:** İsveç merkezli uluslararası bir oluşum olan WikiLeaks, siber ortamda yayımladığı diplomatik belgeler ile dünya çapında ses getirmiş ve şimdiye kadar açıkladığı toplam bir milyon civarında gizli yazışma ile diplomaside depreme yol açmıştır.

- **2010 ve 2011 yıllarında Tunus, Mısır, Libya ve Yemen'de yaşanan 'Arap Baharı' olayları:** Bu süreçte, insanların ve toplumların çeşitli olaylarla zamanla biriken öfkelerinin bilişim sistem ve teknolojileri üzerinden sosyal ağlar yoluyla etkilenmesi ve yönlendirilmesi sonucunda gelişen ve genelde başarıyla sonuçlanan isyan ve devrim hareketlerinin ilki 17 Aralık 2010 tarihinde Tunus'ta başlamıştır. [77] Tunus'tan sonra özellikle Mısır, Libya ve Yemen gibi ülkelerde yönetimlerin değişmesine neden olan siyasi, silahlı, bölgesel ve toplumsal bir halk hareketine

dönüşmüştür. Olaylar hemen hemen tüm Arap ülkelerinde görüldüğü ve etkilediği için Arap Baharı olarak adlandırılmıştır. Bazı Arap ülkelerinde küçük çaplı halk ayaklanmaları, protestolar, vb. yürüyüşler ve toplantılar şeklinde görülmekle birlikte etkileri çeşitli şekillerde hala devam etmektedir.

- **2011'de İran'ın ABD insansız hava aracının kontrolünü ele geçirerek yere indirmesi:** 2011 yılı Aralık ayında, İran Silahlı Kuvvetlerinin İran'ın doğusunda, ABD'ye ait insansız casus uçağının kontrolünü ele geçirip sapasağlam yere indirerek el koyması, bütün dünyanın ilgisini çeken ve siber harekât açısından incelenmeye değer bir olay olmuştur.

- **2014'te Sony Şirketinin siber saldırılar sonucu Kuzey Kore Lideriyle ilgili filmi gösterimden kaldırması:** Aralık 2014'te, Kuzey Kore liderine suikast girişimini konu alan komedi filmi Kuzey Kore tarafından tepkiyle karşılanmış, yapımcı Sony Pictures Şirketi yoğun siber saldırılara uğramış, şirket bilgisayarlarından çekimine başlanmamış film senaryoları ve personel bilgileri dâhil pek çok gizli bilgi / belge sızdırılmış, tehditler ve siber saldırılar sonucu film gösterimden kaldırılmıştır. Saldırılardan Kuzey Kore Cumhuriyeti sorumlu tutulmuş ancak kanıtlanamamıştır.

- **2016'da ABD'de yapılan saldırılarla internet bağlantısının engellenmesi:** 21 Ekim 2016'da, ABD'nin doğu yakasına hizmet sunan alan adı sistemleri (DNS) altyapılarına yönelik olarak başlayan saldırılar ülke geneline yayılarak internet bağlantısının yüzde 90'ını engellemiş ve Türkiye'nin de aralarında bulunduğu birçok ülkede etkisini göstermiştir. Özellikle sanal ticareti olumsuz etkileyen saldırıların, ABD ekonomisine maliyetinin 7 milyar doları bulduğu belirtilmiştir.

- **2017'de Fidye Yazılımı Saldırıları' ile sayısız kurum ve kuruluş ile kullanıcıya zarar verilmesi:** 150'den faza ülkede, başta bankacılık olmak üzere, sağlık, haberleşme ve lojistik sektörleri çok sayıda kurum ve kuruluşun bilişim sistemlerine zarar veren WannaCry isimli fidye yazılımları ile 4 milyar ABD Dolarına yakın zarar verilmiştir. Saldırılar sonrasında, İspanya'da Telefonica ve Renault otomobil fabrikalarının çalışmayı durdurması ve İngiltere'de 600'den fazla ulusal sağlık tesisinin etkilenmesi, binlerce doktorun randevularının ve ameliyatlarının iptal edilmesi olayları yaşananların bazılarıdır.

Ukrayna merkezli, 65 ülkeyi etkileyen Petya / NotPetya zararlı yazılımları ile de 300 milyondan fazla kullanıcıya 1,2 milyar ABD Dolara yakın zarar verilmiştir.

Saldırılar sonrasında Ukrayna'da TNT Express (FedEx - Avrupa) bilgi sistemlerinin yeniden kurulması bir aydan fazla sürmüş, Danimarka'da Maersk Gemicilik bilgi sistemlerinin (4.000 sunucu, 45.000 sistem) yeniden kurulması on gün ve Almanya'da Merck (ilaç) ve İngiltere'de Reckitt Benckiser (sağlık) tesislerinde iki aydan fazla üretim ve arz kesintileri yaşanmıştır [78].

- **2020'de Ukrayna yolcu uçağının İran tarafından düşürülmesi:** Ukrayna Hava Yollarına ait yolcu uçağı, 8 Ocak sabahı Tahran Havalimanı'ndan havalandıktan kısa süre sonra düşmüş, uçakta bulunan 176 kişi hayatını kaybetmiştir. Ukrayna uçağının İran resmi makamlarınca düşürüldüğü başlangıçta kabul edilmemiş, 11 Ocak'ta yapılan açıklamada ise 'hassas askeri bir noktanın' üzerinden geçerken 'insani hata' sonucu hava savunma sistemi tarafından yanlışlıkla düşürüldüğü açıklanmıştır [79].

Daha sonra yapılan açılamalarda ise Ukrayna uçağının seyir (Cruise) füzesi olarak algılandığı, o anlarda iletişim hatlarında yaşanan sorunlar nedeniyle hava savunma biriminin gerekli izni alamadan verilen hatalı kararı sonrası uçağın füzeyle düşürüldüğü açıklanmıştır [80].

Olayın insan hatasından kaynaklandığına dair resmi açıklamalara karşın, bu hatanın nedenleri arasında doğrulanmış tespitler ve kesin raporlar olmamakla birlikte, siber saldırıların da yer aldığına dair açık kaynaklarda varsayımlar ve önemli iddialar yer almıştır [81, 82].

3.4 Türkiye'de Yaşanan Önemli Siber Saldırılar ve Olaylar [76]

- **2008'de Bakü-Tiflis-Ceyhan boru hattına saldırı yapılması:** 5 Ağustos 2008'de Bakü-Tiflis-Ceyhan petrol boru hattındaki 1,768 kilometrelik hat üzerinde Erzincan'ın Refahiye ilçesi yakınlarında bir patlama meydana gelmiş, Türk makamların sabotajdan şüphelenmesi ile PKK terör örgütü saldırıyı üstlenmişti. Araştırma sonucunda ise patlamanın nedeninin teknik arızadan kaynaklandığı belirtilmişti. Ancak sonradan elde edilen bilgilere göre, bu patlamanın bir siber saldırı sonucunda gerçekleştiği anlaşılmıştır.

- **2009'da zararlı bir yazılımın Atatürk Havalimanı bilgisayarlarını etkilemesi:** 30 Ocak 2009 tarihinde birçok ülkenin bilgisayar sistemine yayılan ve önemli zararlar veren 'Conficker' virüsü İstanbul'da Atatürk Havalimanı'nın dış hatlar terminalinde çalışan bilgisayarları ciddi şekilde etkilemiştir.

- **2011'de saldırılar sonrasında TİB'in sitesinin devre dışı kalması:** 9 Haziran 2011'de 'İnternete Filtre Uygulamasının karşısında temel hak ve özgürlüklerin ihlal edileceğini savunan 'Anonymous' adlı Uluslararası Bilgisayar Korsanları Topluluğu akşam saatlerinde BTK Telekomünikasyon İletişim Başkanlığının internet sitesine saldırmış, devre dışı kalan site çalışmaya gece yarısından sonra ancak başlayabilmiştir.

- **2015'te 79 ili etkileyen elektrik kesintisi:** 31 Mart 2015 günü Türkiye'de elektriğini İran'dan alan Van ve Hakkâri hariç 79 ilde elektrik kesintisi yaşanmıştır. Elektrik kesintisinin nedeniyle ilgili uzmanların görüşü; "Yüklü bir hattın devre dışı kalmasının tüm sistem dinamiğini bozması, ardından diğer hatların bir arıza olduğunu düşünerek kademeli olarak kendilerini kapatması…" şeklinde olmuştur. Elektrik kesintisi olayından kısa süre sonra, Türkiye Elektrik İletim A.Ş. (TEİAŞ)'nin elektrik kesintilerini engellemek için bilgisayar sistemleri ve ağları ihalesine çıktığı öğrenilmiştir.

- **2015'te, 10 gün süreli saldırılar sonucu birçok internet sitesine ve mobil uygulamalara erişim sağlanamaması:** 14 Aralık 2015 tarihinde başlayan ve yaklaşık 10 gün süreli, özellikle 'tr' uzantılı alan adlarının yönetildiği sunucuları hedef alan saldırılar sonucu birçok banka, noter ve devlet kurumunun internet sitesine ve mobil uygulamalarına erişim sağlanamamıştır. İnternet trafiğini büyük ölçüde etkileyen bu toplu saldırıların, bugüne değin dünya üzerinde yaşanmış en yoğun siber saldırılardan birisi olduğu ifade edilmiştir.

- **2016'da Sağlık Bakanlığı hastanelerine siber saldırılar yapılması:** 18 Mayıs 2016 günü sabah saatlerinde, 33 devlet hastanesinin veri tabanlarında bulunan bilgilerin kopyalandıktan sonra silindiği, saldırıları 'Anonymous' adlı bilgisayar korsanları grubunun üstlendiği belirtilmiştir. Sağlık Bakanlığı sistemin kısmen etkilendiğini ve yedekleme mekanizması sayesinde olası veri kayıplarının önüne geçildiğini duyurmuştur.

- **2018'de bazı bankaların internet bankacılığı döviz uygulamalarına saldırılar yapılması:** 31 Ağustos 2018 tarihinde Halk Bankası'nın, 09 Eylül 2018'de de Vakıf Katılım'ın döviz kurlarının sisteme aktarılmasında kullanılan yazılımlarına yönelik saldırılar sonrasında internet sayfalarında değişiklikler yapılmış ve hatalı döviz alım satım işlemleri sonrası, saygınlık kaybı düşüncesiyle miktarı açıklanmamakla birlikte, işletmelerin zarara uğratılmasına sebebiyet verilmiştir [83, 84].

3.5 Siber Saldırıların Genel Sonuçları

1990'lı yıllardan başlayarak internetin yaygınlaşmasından sonra, özellikle 2000 yılından bu güne yaşanan, bir kısmı yukarıda açıklanan siber saldırı ve olayların açık kaynaklara yansıdığı kadarıyla içerik ve sonuçlarına bakılarak, siber saldırılar ile;

- İletişim ağlarının devre dışı bırakılarak askeri haberleşme dâhil aksatılabileceği,
- Bankacılık ve finans iş alanlarının çökertilebileceği,
- Ulaşım ve su sistemlerinin bozulabileceği,
- Elektrik ve doğal gaz sistemlerinin kapatılabileceği ya da tahrip edilebileceği,
- Baraj kapaklarının açılarak şehirlerin sular altında bırakılabileceği,
- Nükleer santrallerin kontrolü ele geçirilerek potansiyel birer atom bombasına dönüştürülebileceği,
- Toplumsal olaylar çıkarılabileceği, halkın yönlendirilebileceği, kargaşa ve karışıklıklar yaratılabileceği, bütün bunların sonucunda klasik savaşın verdiği zararlara benzer hatta daha ağır zararlar verdirilebileceği anlaşılmaktadır.

Bu sonuçlara bakıldığında ise bilinen, geçmişte yaşanan ve günümüz de yaşanmakta olan klasik savaşların sebebiyet verdiği yıkımlar, hasar ve zararlar akla gelmektedir. Bu da siber saldırılarla savaşı yani siber savaşı akla getirmektedir. Kısaca, siber savaşlar başlamış ve günümüzde de devam etmektedir.

3.6 Siber Savaşın Kapsamı, Silahları ve Yöntemleri

Bilgisayarların icadı sonrası, özellikle internetin de icadı ve yaygınlaşması sonrasında, zaman ve mekân kavramı ortadan kalkmış, kıtalararası iletişim ve bilgi aktarımı bir tuşa basmaktan ibaret hale gelirken, siber saldırılar için küçük bir ağ sistemi ve bağlantısı yeterli hale gelmiştir. Bilgi ve iletişim sistemlerinde gelişmeler ile ilgili örgütsel yenilikler çatışmaların doğasını ve ihtiyaç duyulacak askeri yapıları, doktrinleri ve stratejileri değiştirmektedir. Siber savaş 'Ağ savaşı' olarak ta tanımlanırken iletişim ve zekânın önemi artmış, gelecekteki çatışmaların ve savaşların ağlar üzerinde olacağı ve üstünlüğün ağlara hâkim olanda olacağı görüşleri ortaya çıkmıştır.[85]

Yaklaşık 50 - 100 Amerikan dolarlık bir sistemle milyonlarca dolarlık füze ve uçakların verebileceği zarar etkisi yaratılabilir. Klasik bombalı saldırılarda olduğu gibi

olay yerinde olmaya da gerek yoktur. Bu konuda “Bit ve baytlar, mermiler ve bombalar kadar tahrip edici olabilir” [86] sözü siber saldırı ve dolayısıyla siber savaş gerçeğini çok anlamlı bir şekilde özetlemektedir.

‘Bilgi Savaşı’ ile eş anlamlı olarak kullanılan, devletler tarafından kendi bilgilerini ve bilgi sistemlerini korurken karşı tarafın bilgilerine ve bilgi sistemlerine zarar vermek için yapılan faaliyetler şeklinde yapılan ‘Siber Savaş’, siber saldırılar ve suçlar ile siber terörizm ve siber casusluk / istihbarat faaliyetleri ile tek başına veya diğer savaş türleriyle birlikte, hibrit savaş / çok katmanlı savaş içerisinde gerçekleştirilerek etkin sonuçların alınmasını sağlayabilmektedir.

Klasik savaşta taarruz ve savunma teknik ve yöntemleri kullanılırken, benzer şekilde siber savaşta da bunların karşılığı olarak siber saldırı / taarruz ve siber güvenlik / savunma teknik ve yöntemleri kullanılmaktadır. Siber ortamda yapılan saldırılar taarruz, güvenlik tedbirleri savunma harekâtına karşılık gelmekte ve her iki harekât türü birlikte siber harekâtı veya savaşı oluşturmaktadır. Klasik harekâtta kullanılan silahın siber harekâtta yerini siber silah olarak bilişim sistem ve teknolojileri, merminin yerini ise zararlı yazılım ve kodlar alırken kullanıcı değişmemektedir (Çizelge 3.2).

Çizelge 3.2: Klasik / Siber savaş temel harekât çeşitleri ve özellikleri.

Klasik Savaş	Siber Savaş (Harekât)
• Taarruz	• Saldırı, Taarruz
• Savunma	• Güvenlik, Savunma
• Silah	• Bilişim sistem ve teknolojisi
• Mermi	• Yazılım (Zararlı yazılım, kod, komut, bilgi vb.)
• Kullanıcı	• Kullanıcı

‘Siber silah’ tanımına ilişkin şu anda uluslararası bir fikir birliği olmamakla birlikte, genel anlamda bir silah alt kümesi olarak görülmekte, yapılara fiziksel, işlevsel veya zihinsel zararlar vermek için tehdit etmek veya bunlara neden olmak amacıyla kullanılan veya kullanılmak üzere tasarlanmış bilgisayar kodları, sistemleri veya canlılar (kullanıcılar) şeklinde yapılan tanım yaygın kabul görmektedir. Geliştirme ve dağıtım için kaynakları, istihbaratı ve zamanı artırırken hedef sayısını ve riskleri azaltarak siber silahların etkilerini daha da artırmak mümkündür. [87]

Siber silahın tanımından siber gücün tanımına da açıklık gelmektedir. Siber savaş gücü yani siber güç ile siber silah yaklaşımından, siber gücün eldeki bilişim sistem ve teknolojileri, yazılım ve kodlar ile kullanıcılardan oluştuğu görülmektedir. Siber savaşta kullanılan silah ve mühimmat kavramlarında en önemli husus, klasik savaşta silahının üreteni kim olursa olsun kullanıcı buna eğitimler soncunda her bakımdan kolaylıkla hâkim olup etkinlikle kullanabilirken, siber silah ve savaşlarda bu mümkün görülmemektedir. Siber silah ve mühimmatlarda üreticinin başkası olması durumunda kullanıcının buna her zaman tam anlamıyla hâkim olamayabileceği, bilişim sistem ve yazılımlarının üretene her zaman bir açık, arka kapı ve kazanım imkânı sağlayabileceği riski bulunmaktadır.

Siber gücün artırılması ve geliştirilmesi için siber silah ve mühimmatın yani bilişim sistem ve teknolojileri ile yazılımların geliştirilmesi zorunluluktur. Ancak bilişim sistem ve teknolojileri ile yazılımları üretenler ve kullanıcılar da insandır. Dolayısıyla insan faktörü ve gücün kullanıcı unsuru çok önemlidir. Silah ve mühimmatın etkin üretimi yanında savaşta etkinliği, sonuç alıcılığı ve başarısı kullanıcıya bağlı olmaktadır. Bu düşüncelerden hareketle siber savaşlarda hedef her zaman bilişim sistemleri ve yazılımlar yanında onları kullananları hedef alıp etkileyip yönlendirerek te sonuç alınabilmektedir. İnternet ortamında sosyal ağların kullanılarak kişilerin, grupların ve toplumların çeşitli psikolojik harekât teknikleri ve algı yöntemleri ile yönlendirilmesi de bu kapsamda ele alınarak siber savaş kapsamında değerlendirilmesi gerekir.

Unutulmaması ve her zaman hatırda tutularak uygulamalara yansıtılması gereken ise; “Henüz en güçlü ülkelerin en gelişkin siber silahlarını kullandığı tür bir siber savaş henüz gerçekleşmediği” gerçeğidir. Ayrıca siber savaş durumunda, güçlü bir siber silahı dünyaya uygulamayı düşünen ülkelerin, o silaha karşı kendini savunmayı planlamadılarsa, o savaşı kaybetmeye mahkûm olmalarının kaçınılmaz olacağıdır [25].

3.7 Klasik Savaş ve Siber Savaş Karşılaştırması

Siber savaş alanı klasik savaşların yapıldığı kara, deniz, hava ve uzayı da içerisine alan siber uzaydır. Ayrıca günümüzde yaşanan klasik savaşlarda hangi alanda yapılırsa yapılsın hepsinde mutlaka bilişim sistem ve teknolojileri de kullanılmaktadır. Yani

klasik savaşın içerisinde siber güç de kullanılmakta ve genellikle aynı anda siber muharebeler ve siber harekât da yapılmaktadır. Ayrıca unutulmaması gereken hususlarda birisi siber harekât sırasında icra edilen siber saldırılar ya da taarruzlar, her ne kadar siber ortamda yapılsa da etkileri ve sonuçları fiziksel ortamda da görülebilmekte, klasik savaşta olduğu gibi can ve mal kaybına da sebep olabilmekte ve ülkeler için büyük tehditler oluşturabilmektedir.

ABD eski Savunma Bakanlarından Leon Panetta, 11 Ekim 2012 tarihinde New York'ta işadamlarına yaptığı konuşmasında, "ABD Siber-Pearl Harbor olasılığı ile karşı karşıya olduğu" sözüyle, benzer hususları belirtmiş ve siber savaşın ulusal güvenlik için büyük bir tehdit olduğunu vurgulamıştır [51]. Klasik savaş ve siber savaşın temel bazı özellikleri karşılaştırıldığında, Çizelge 3.3'te de görüleceği üzere, ilginç sonuçlar ortaya çıkmaktadır.

Çizelge 3.3: Klasik Savaş - Siber Savaş karşılaştırması [88].

Özellikler	Klasik Savaş	Siber Savaş
Saldırı Kaynağı	Bulması kolaydır.	Tespit etmek çok zor, hatta imkânsız olabilir.
Hızı	Silahın / sistemin hızı kadardır.	Işık hızındadır.
Etkisi	Çoğunlukla fiziksel alanda etkilidir.	Çoğunlukla bilişim sistemleri alanında etkilidir.
Savaşanlar	Tarafların silahlı kuvvetleri.	Kişi, grup, örgüt veya devlet savaşabilir.
Maliyeti	Kullanılan silah / sistemlerin maliyeti - Pahalıdır.	Genelde ucuzdur. Bazen bir bilgisayar yeterlidir.
Saldırı Belirtileri	Farkına varılır.	Saldırının farkına varılmayabilir.
Hasar Tespiti	Fiziksel etkiler nedeniyle oldukça kolaydır.	Nerede ne kadar hasar oluştuğunu tespit etmek çok zor, çoğu zaman imkânsızdır.

Saldırı kaynağı klasik savaşta kolaylıkla bulunabilirken, siber savaşta saldırı kayağını tespit etmek çok zor, hatta imkânsız olabilmektedir. Klasik silahların hızı silah sisteminin hızı ile sınırlı kalırken, siber savaşın hızı ışık hızında gerçekleşmektedir. Klasik savaşta saldırıların etkisi fiziksel alanla sınırlı kalırken, siber saldırıların etkisi bilişim sistemlerinin bulunduğu her alanı kapsamaktadır.

Klasik savaşta tarafların silahlı kuvvetleri askeri birlikleri savaşırken, siber savaşta sivil asker, kişi grup, örgüt veya devlet savaşabilir. Klasik savaşın silah ve sistemlerinin yüksek maliyetlerine karşın, siber savaşın maliyeti çok ucuz kalmakta,

bazen bir bilgisayar bile yeterli olabilmektedir. Klasik saldırılar hemen farkına varılırken, siber saldırıların farkına varılmayabilmektedir. Siber savaşlarda saldırıların sebep olduğu hasar ve zararların tespiti fiziki etkiler nedeniyle kolaylıkla yapılırken, siber savaşlarda nerede ne kadar hasar ve zarar oluştuğunun tespiti çok zor, çoğu zaman imkânsız olabilir [88].

Bilgisayar ve iletişim sistemlerinin gelişmesi, insanların internetinden nesnelerin internetine, akıllı cihazlardan akıllı evlere - şehirlere, insansız hava araçlarından insansız kara / deniz araçlarına, duyargaların, mikro - nano robotların, nano - biyo vb. teknolojilerin de birlikte kullanılmasıyla siber uzayda sınır tanımayan ve insanın hayalinde canlandırma sınırlarını zorlayan gelişmeler yaşanmaktadır. Böyle bir ortamda, çoğu ülke tarafından siber saldırı tehditleri ve riskleri gerçeği ile tehlike boyutu dikkate alınarak, siber savaşın hem taarruz ve hem de savunma boyutu ile ilgili yasa, politika ve stratejiler üreterek uygulamaya konulmakta, bu çalışmalara 'Siber Caydırıcılık' da dâhil edilerek konu geniş kapsamlı bir yaklaşımla ele alınmaktadır.

Siber savaşı küçümseyip bu konuda ciddi çalışmalar içerisinde olmayan ülkeleri çok zor bir gelecek beklemektedir. Çünkü siber savaş gerçektir ve saldırganlar şimdiye kadar gerçek yeteneklerini ortaya çıkmaması için en gelişmiş siber silahlarını yani bu konudaki gerçek yeteneklerini kullanmamışlardır. Tam ölçekli bir siber savaşın, yani gerçek yeteneklerin kullanıldığı saldırıların yapıldığı bir siber savaşın sonuçlarının tahmin edilemeyeceği ve olabileceklerin modern bir ülkeyi mahvedebileceği yorumları yapılmaktadır [25].

Bu düşüncelerin çerçevesinde ülkeler arayışlarını ve çalışmalarını sürdürmektedir. Son birkaç yıldır siber saldırılara ve siber savaşa karşı uluslararası işbirliği girişimlerinin de olduğu ancak bu konudaki başarıların sınırlı kaldığı görülmektedir. Baram ve Menashri bu konuda başarı için üç büyük zorluğun aşılması gerektiğini vurgulamaktadır. Bu zorluklar; Güven sorunu, Değişen tehdit algılamaları ve Devlet egemenliğinin farklı tanımlarıdır. 'Küresel Siber Denge Kararlılığı' gibi aşağıdan yukarıya bir çözümün görüş ayrılıklarına karşın bu zorlukların aşılmasını sağlayacağı belirtilmektedir. [89]

Sun Tzu'nun "En iyisi savaşmadan baş eğdirmek" [3] ve Belisarius'un "Kendiniz bir zarar görmeden, düşmanı amacından vazgeçmek zorunda bırakmak" [37] sözleri yanında Atatürk'ün "…Savaş zorunlu ve hayati olmalıdır. Ulusun hayatı tehlikeye

girmedikçe, savaş bir cinayettir.” [38] sözlerini unutmadan, siber savaşa her zaman hazır olunmalı, ancak savaşmadan kazanmak için yani siber caydırıcılık için de azami çaba ve gayretle çalışılmalıdır.

4 SİBER CAYDIRICILIK

4.1 Caydırıcılık

Geçmişten günümüze bakarak, hukuk alanında bireylerin çeşitli cezalar ile suç işlemelerinin önlenmesine, diplomasi alanında devletlerin çeşitli yaptırımlarla ilişkilerinin yönlendirilmesine ve askeri alanda savaşmadan karşı tarafın farklı davranmasının sağlanmasına, yani bu alanlarda caydırıcılık uygulamalarına yönelik yaşanmış pek çok örnek olay sıralanabilir. Adli olaylarda para ya da mahkûmiyet cezaları, uluslararası ortamda devletlere çeşitli yaptırımların uygulanması, klasik savaşta güçlü ordularla karşı tarafa misilleme tehdidi, güç gösterisi, tatbikatlar, vb.

Potansiyel faydaları azaltarak ya da olası masrafları artırarak (ya da her ikisini de birden), diğer bir ifadeyle saldırı veya eylemin bedelinin sağlayacağı kazancın çok üzerinde ve kabul edilemeyecek seviyede yüksek bir zarar şeklinde olacağına düşmanı inandırarak saldırı veya eylemden kaçınmaya ikna etmek, yani düşmanı eylemeden vaz geçirmek veya caydırmak için stratejik bir yaklaşım gerekmektedir. Caydırıcı olmak ve caydırıcılığın sağlanması için 'Saldırganın eylemini boşa çıkarma' ve 'Cezalandırma (misilleme tehdidi)' yoluyla saldırıdan veya eylemden vazgeçirilmesine dayanan iki yöntem uygulanır. Bu yöntemlerden, özellikle soğuk savaş döneminde ön planda kullanılan ve nükleer caydırıcılığın esasını teşkil eden cezalandırma yoluyla caydırıcılığın başarıyla sağlanması için ise üç temel koşul bulunmaktadır. Bunlar caydırıcının yetenekleri, misilleme tehdidinin güvenilirliği ve tehdidin saldırgana iletilmesidir [90].

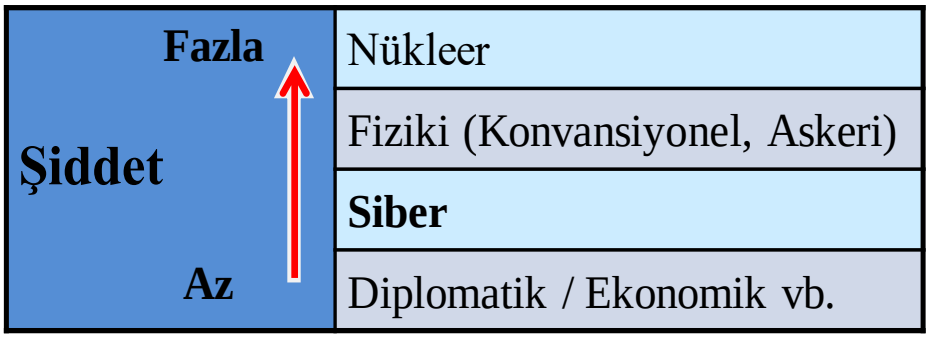
Siber savaşın da maksatlarından birisi, askeri anlamda savaşın klasik tanımında olduğu gibi, istek veya istekleri diğer bir ulus veya devletler topluluğuna zorla kabul ettirerek, icra edeceği harekâttan vaz geçirterek savaşı kazanmaktır. Ancak M.Ö. 500'lü yıllarda Sun Tzu'nun dediği gibi "Savaşmadan baş eğdirmek" [3] ya da M.S. 500'lü yıllarda Belisarius'un dediği gibi "Kendiniz bir zarar görmeden, düşmanı amacından vazgeçmek zorunda bırakmak" [37] savaşı kazanmaktan daha iyisi olabilir.

Yani saldırganı isteğinden, saldırıdan veya savaştan caydırmak, benzer şekilde siber savaşta da en iyisi ve en mükemmeli 'Siber Caydırıcılık' olabilir.

4.2 Siber Caydırıcılık Yaklaşımları

Saygınlık kaybı, gizlilik, kamu yararı, ulusal ve uluslararası güvenlik vb. nedenlerle açıklanmayanlar yanında, yazılı ve görsel basın, medya gibi açık kaynaklarda da yer alan siber saldırı olaylarına ve bunların olumsuz sonuçlarına rağmen, siber savaşın bir savaş olup olmadığı tartışmalarının devam ettiği gibi, siber alanda siber güçle bir caydırıcılığın mümkün olup olmadığı konusunda da tartışmaların başlamış ve devam etmekte olduğu görülmektedir.

ABD'li bilişim ve ulusal güvenlik uzmanı akademisyen Libicki siber caydırıcılığı; "Siber ortamda saldırganın eylemini boşa çıkarma veya cezalandırma (misilleme tehdidi) yoluyla saldırıdan vazgeçirme" olarak tanımlamaktadır. Bu konuda, Şekil 4.1'de görüleceği üzere, siber güç ve siber savaş kapsamında misillemenin etkisinin de, nükleer ve klasik (konvansiyonel) savaş kapsamında caydırıcılıktan sonra, diplomatik ve ekonomik yaptırımlarla sağlanan caydırıcılıktan ise önce geldiğinin kabul edilebileceğini belirtmektedir [22].



Şekil 4.1: Caydırıcılıkta misillemenin etki seviyeleri [22].

ABD eski Genelkurmay Başkan Yardımcılarından (2007-2011) Orgeneral J. Cartwright siber caydırıcılığı, "Siber ortamda başkalarının bize yapmak istediklerinin aynısını onlara yapma yeteneği" [27] olarak tanımlamıştır. Yani sen bana siber ortamda saldırır zarar verirsen, ben de sana aynı şekilde saldırır zarar veririm. Bu tanımlamanın nükleer veya konvansiyonel caydırıcılık için karşılık bulduğu kabul edilmekle birlikte, siber gücün ve kullanılmasının özellikleri dolayısıyla, siber caydırıcılık için yeterli olup olmayacağı tartışılmaktadır.

İstihbarat yetenekleri bu sorunun çözümünü kolaylaştırsa da, genelde saldırıya karşılık verileceği zaman daha geniş bir potansiyel tehdidi kapsayacak şekilde değerlendirilmelidir. Soğuk savaş döneminde her iki tarafın da yetenekleri açıkça bilinirken, bilgi çağında olası saldırganların sayısının artması ve güçlerinin de belirsizliği, caydırıcılık mesajının kime ve nasıl iletileceğinin zorlukları istikrarlı ve inanılır caydırıcılık sunma olasılığını düşürmüştür.

Siber saldırılara karşı caydırıcılığın zorlukları nedeniyle; nükleer savaşı önlemenin olmazsa olmazı olan caydırıcılık kuramının, günümüzde siber savaşı durdurmakta önemli bir rol oynayamadığı [25] ve ABD'nin nükleer ve konvansiyonel anlamda sağladığı caydırıcılığı, tüm çabasına rağmen siber alanda sağlayamayacağı ileri sürülmektedir [60]. Bu düşünce, 2011 yılında ABD Savunma Bakanlığınca hazırlanan raporlardan sızan bilgilerden, "Siber saldırıların savaş sebebi sayılacağının ve askeri operasyonlarla karşılık verilebileceğinin açıklanması" [91] ile desteklenmektedir.

Ancak ABD'nin siber saldırılara karşı caydırıcılık çalışmaları daha önceye dayanmakta, siber güvenlikte önde gelen ülkelerin ulusal siber güvenlik stratejilerinin incelendiği bölümde (5.4) görüleceği üzere, kararlılıkla sürdürülmektedir. ABD'de 2008 yılında siber alanda kalıcı siber caydırma stratejileri ve programlarının tanımlanması ve geliştirilmesi kararı uygulamaya konulmuştur. 2011 yılında siber savunmada vaz geçirme ve caydırıcılığın esas alınacağı vurgulanırken; Ülkeye karşı diğer tehditlerde olduğu gibi, siber uzayda düşmanca eylemlerin tehdit oluşturması durumunda karşılık verileceği, siber saldırılara karşı da tüm devletlerin öz savunma hakkı olduğu, bu kapsamda, ulusu, müttefikleri ve ortakları savunmak için gerekli tüm uygun yöntemleri (diplomatik, bilgi amaçlı, askeri ve ekonomik) uluslararası hukuka uygun olarak kullanma hakkının saklı tutulduğu açıklanmıştır. 2015'te ABD çıkarlarına karşı siber saldırıları engellemek için kapsamlı bir siber caydırıcılık stratejisinin geliştirilmesinin ve uygulanmasının ABD güç ve eylemlerinin toplamı yoluyla sağlanacağı belirtilmiş, 2018'de Barışın Güçle Korunması gerektiği, sorumlu devlet davranışı değerleriyle siber kararlılığının artırılması ve Siber değerlerle evrensel bağlılığın özendirilmesi, Siber alanda kabul edilemez davranışların tespiti ve caydırılması için 'Siber Caydırıcılık Girişimi' oluşturulması kararları alınarak uygulamaya konulmuştur.

ABD ulusal siber güvenlik stratejisi çalışmaları ve uygulamalarına benzer şekilde Rusya Federasyonu, Fransa ve İngiltere'nin de siber alanda yapılacak saldırılara karşı caydırıcılık sağlanması konusunu strateji belgelerine ve çalışmalarına dâhil ettikleri, önemli kararlar aldıkları ve uygulamaya koydukları görülmektedir.

Siber silahlar nükleer silahlara benzemez ve bireyler, küçük gruplar ve devletler tarafından kolayca geliştirilip konuşlandırılırlar. Kolayca çoğaltılır ve ağlar arasında dağıtılırlar [92]. Siber alanda bilgisayar ve iletişim teknolojileri kullanarak elde edilen imkân ve kolaylıkların bir güç (siber güç) olduğu, bu gücün hem saldırı aracı, hem de saldırı hedefi olabileceği, tarafların birbirine zarar vermek, siber güçlerini zayıflatmak veya bazı unsurlarını devre dışı bırakmak maksadıyla karşılıklı siber güçlerini kullanabilecekleri tereddüde meydan bırakmayacak şekilde ortadadır. Bu arada, güçlü ülkelerin en gelişmiş siber silahlarını kullandığı türden bir siber savaşın henüz gerçekleşmediği [25] öne sürülmektedir. Bu nedenle gelişmiş ve kullanılmayı bekleyen siber silahların kullanılacağı bir savaşı kimin kazanacağı, bu savaşın sonuçlarının ne olacağı şu anda tahmin edilse de tam olarak bilinmemektedir. Kesin olarak bilinen ise, siber silahların artan kullanımının uluslararası dengeyi ve toplumların güvenliğini tehlikeye atabileceği, yeni siber çatışmaların kıvılcımına yol açabilecek sürtünmeleri ve gerilimleri tırmandırarak büyük hasar ve zararlara sebep olabilecek siber savaşlara yol açacağıdır.

Siber caydırıcılığı, "Savunan bir devletin, daha büyük bir karşılık verilmesi korkusu nedeniyle yıkıcı siber saldırılardan kaçınmak için, düşmanın karar verme organını hedeflemek suretiyle, siber eylemini caydırma niyetlerini bildirerek ve onu etkileyerek mevcut durumu korumaya çalıştığı strateji" şeklinde tanımlayan Iasiello'ya göre [93]; nükleer silah kullanımı, terörizm ve kural tanımaz devlet davranışlarına karşı kullanılanlar gibi caydırıcı stratejiler siber ortam için uygun örnekler değildir. Soğuk savaş sırasında nükleer silahların kullanımının caydırılmasında başarıya ulaştıran ilkeler, şiddetli misilleme (karşılık verme) tehdidi gibi, siber alanda uygulanamaz. Saldırganın kimliğinin tespiti ve dayandırma (isnad) zorlukları nedeniyle, siber alanda caydırıcılık için gerekli olan hızlı ve etkili bir şekilde karşılık verme ve tekrarlanabilirliği sürdürme sağlanamaz.

Libicki'ye göre ise, siber caydırıcılık işe yarayabilir. Ancak bunun için, siber caydırıcılığı nükleer ve klasik askeri caydırıcılıktan ayıran, siber caydırıcılığın

aleyhinde olan ve problemli yanlarını ortaya koyan üçü asıl, altısı yardımcı olmak üzere dokuz soruyu cevaplamak gerekmektedir [22].

Asıl sorular:

- Kimin yaptığı biliniyor mu?
- Onların değerli varlıkları risk altında tutulabilir mi?
- Aynı şey art arda tekrarlanabilir mi?
- Yardımcı sorular:
- Eğer misilleme caydırıcılığı sağlamazsa, en azından silahsızlandırmayı sağlayabilir mi?
- Üçüncü gruplar mücadeleye katılır mı?
- Misilleme kendi tarafımıza doğru mesajı verir mi?
- Saldırıya karşılık vermek için bir eşik var mıdır?
- Tırmanmadan kaçınılabilir mi?
- Saldırgan tarafa vurmaya değmediği durumda ne olur?

Nükleer caydırıcılıkta cevaplanması kolay olan bu soruların, siber caydırıcılık söz konusu olduğunda cevaplanması zorlaşmakta ve bazen de imkânsızlaştığı görülmektedir. Ancak siber ortamda siber güç kullanılarak siber güvenlik ve caydırıcılık sağlanması düşünülüyorsa bu soruların cevaplanması ve bu cevaplar doğrultusunda stratejilerin oluşturulması, planlamaların yapılması ve daha sonra eyleme dönüştürülmesi gerekmektedir.

W. Goodman, çalışmasında [94] siber caydırıcılığın teoride uygulamadan daha mı zor olduğunu sorarken, siber caydırıcılık üzerine geliştirilen teorik yaklaşımları sorgulamış, teoride kasıtsız olarak abartıldığını belirtirken uygulamada etkili bir siber caydırıcılığın zorluklarını vurgulamıştır. Tespitlerini de 2007 yılında Estonya'da ve 2008 yılında da Gürcistan'da yaşanan siber saldırı olaylarını inceleyerek somutlaştırmaya çalışmıştır. Goodman'ın, belirlediği esaslar Libicki'nin belirlediği esaslara benzer şekilde olup, siber caydırıcılığın sağlanabilmesi "Çıkar, Duyurma, Engelleme, Cezalandırma, İnandırma, Güven verme, Korku ve Kar-zarar durumu" başlıklarıyla sıralanan sekiz temel esasa göre hareket edilmesine bağlıdır.

Tarihsel olarak yeni ve daha etkili silahların tasarımı sonrasında, genellikle onların konuşlandırılmasını ve kullanımlarını caydırmak için yeni stratejiler tanımlama ihtiyacı doğduğunu, bu durumun siber silahlar düşünüldüğünde de geçerli olduğunu

belirten Taddeo; caydırıcılık teorisini analiz ettiği çalışmasında [95], caydırıcılığın siber uzaya uygulanabilirliğinin sınırlı olduğunu ve bu sınırların önemli olduğunu vurgulamaktadır. Caydırıcılığın siber çatışmaların ve bunların tırmanmasının önlenmesinde önemli bir rol oynayabileceğini, ancak caydırıcılık teorisi ile siber çatışmaların ve siber uzayın doğası arasındaki temel farklılıkların sonucu olarak bazı zorluklar ve sınırlamalar söz konusudur. Caydırıcılık teorisinin ana unsurları olan dayandırma, savunma / karşılık verme ve iletişimden her birinin siber alanda uygulanmasında ciddi zorlular bulunmaktadır. Bunların başında da teknik yetersizlikler nedeniyle tehditlerin ve saldırıların kaynağının kimliğine yönelik belirsizlikler gelmektedir.

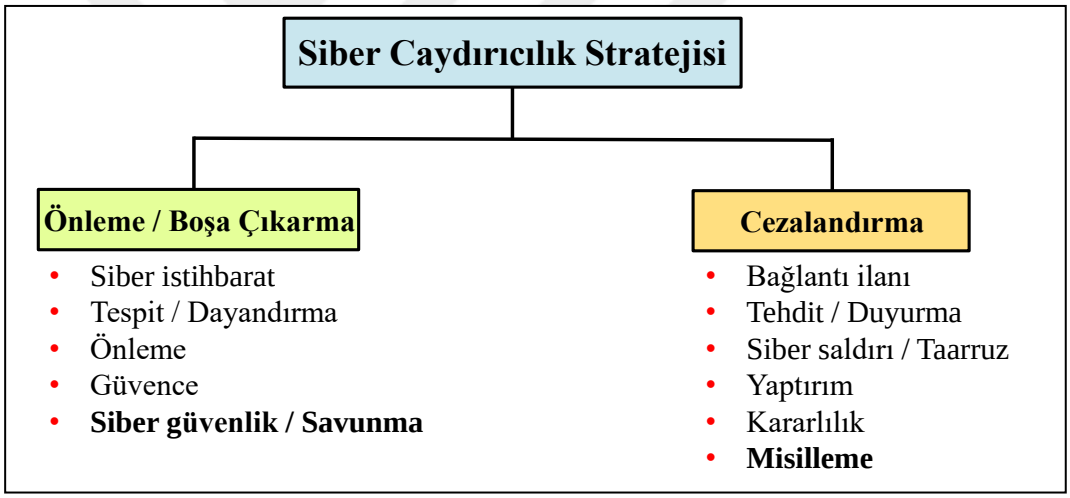
Haley ise [20], caydırıcılık teorisinde amacın, maliyetleri ve sonuçları avantajlardan ağır basarak saldırıları gidermek olduğunu belirtmekte ve bu stratejiyi uygulamak için öncelikle güçlü bir savunmaya sahip olmanın gerektiğini (saldırganı durmaya zorlamak için) vurgulamakta, ikinci yöntem olarak da, misilleme üzerine odaklanmakta ve bazı başarılı saldırganların eylemlerini takiben ağır cezalandırma ile karşı karşıya kalındığında, diğer istekli saldırganların hiç saldırmamayı seçebileceği üzerinde durmaktadır. Üçüncü bileşen olarak da, Taddeo'nun görüşlerine benzer şekilde, saldırının saldırgan tarafa dayandırılması (saldırgana isnat) yaklaşımlarının zorluğu ve önemi üzerinde durmaktadır.

Jensen "Siber Caydırıcılık" konulu çalışmasında [96], Haley'in vurguladığı cezalandırma konusunda siber saldırganlara karşı yasal işlemlerin önemine işaret ederken, ulusların ağlarını ve altyapılarını savunmak için mücadelede, caydırıcılık ilkelerini siyasal etkinliklere uygulayabilme becerilerinin daha da önem kazanmakta olduğunu ve siber ortamda caydırıcılığın, geleneksel misillemeye ek olarak, soğuk savaşın nükleer çağında geliştirilen geleneksel caydırma metotlarından daha fazla yasal işlemleri yapma ve ağları görünmez, esnek ve birbirine bağlı hale getirme gibi seçenekleri sunduğunu belirmiştir. Siber yetenekler ulusal hedefleri gerçekleştirmek için benzersiz ve yenilikçi araçlar sağlarken, aynı şekilde "Misilleme gibi geleneksel caydırma metotları ve yenilmezlik, görünmezlik, esneklik ve karşılıklı bağımlılık gibi" yeni ve yenilikçi bazı caydırıcılık yöntemleri de sunmaktadır.

Yaptığı "Siber Savaş ve Caydırıcılık" konulu çalışmada, siber uzayda devletler tarafından caydırıcılığın sağlanıp sağlanamayacağını sorgulayan Lupovici'nin de

belirttiği [90] gibi, siber saldırganın eylemini boşa çıkarma ve cezalandırma (misilleme) yöntemlerinden cezalandırma yoluyla caydırıcılığın başarılı olabilmesi için caydırıcının yetenekleri (kapasitesi), misilleme tehdidinin güvenilirliği ve misilleme tehdidin saldırgana başarılı bir şekilde duyurulması şartlarının sağlanması gerekmektedir.

Siber caydırıcılık konusunda yukarda değinilen çeşitli düşünce ve yaklaşımlar ile uygulamalardan da hareketle bu konudaki stratejinin iki temel yöntemde birleştiği görülmektedir (Şekil 4.2). Bunlardan birincisiyle, öncelikle saldırı ve eylemleri önlemeye ve boşa çıkarmayı amaçlamakta, istihbarat, tespit ve isnat, önleme ve güvence vb. çalışmalarıyla siber güvenlik ve savunma kapasitesi daha da artırılmaktadır. İkincisiyle de, bağlantı (angajman) ilanı ve tehditler ile yetkinlikler saldırgana duyurulmakta, siber saldırı / taarruz, çeşitli yaptırımlarla cezalandırma için misillemede kararlılık gösterilmektedir.

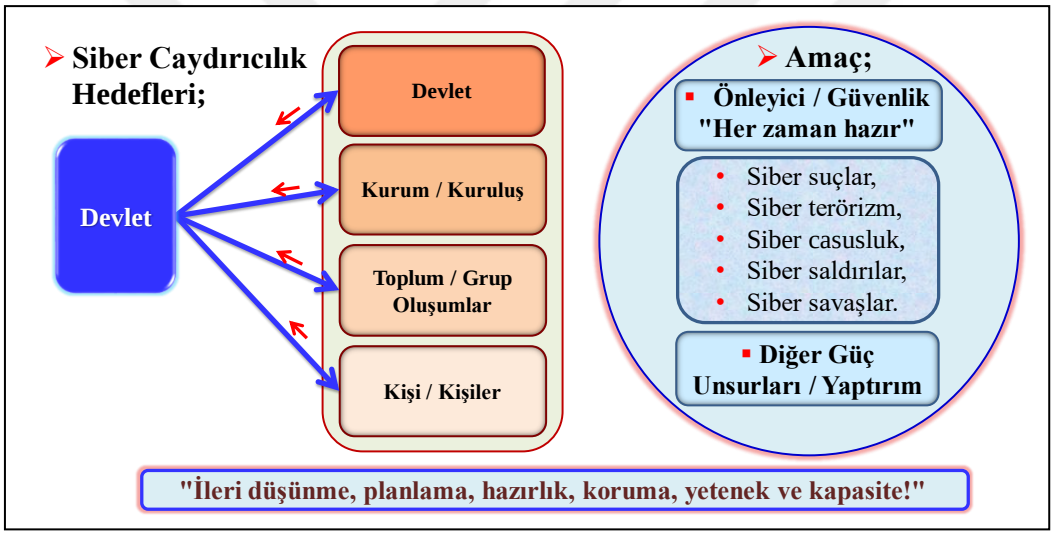


Şekil 4.2: Siber caydırıcılık stratejisi yöntemleri ve teknikleri.

Bu şartlardan yetenek veya kapasite konusunun asimetrik bir etki doğurmasından dolayı göreli olarak küçük olan devletler, klasik savaş maliyetlerinin çok azıyla siber uzayda önemli bir saldırı kapasitesi oluşturabilmektedir. Buna karşın büyük ve gelişmiş devletler saldırı yeteneklerini geliştirmelerine rağmen, siber ortama bağımlı yapılarından dolayı savunma kapasitelerini aynı oranda geliştiremediklerinden ve caydırıcılıklarını sağlamak için yapacakları siber misilleme tehditleri saldırganın bilgi ve iletişim sistemleri altyapıları yetersizlikleri ile ağsız yapısı nedeniyle etkisiz kalmaktadır.

Geçmişten günümüze, saygınlık kaybı, gizlilik, kamu yararı, ulusal ve uluslararası güvenlik vb. nedenlerle açıklanmayanlar yanında, yazılı ve görsel basın, medya vb. açık kaynaklarda yer alan, bir kısmı devlet destekli bile olmayabilecek, kurum/kuruluş, toplum / grup, kişi/kişiler gibi küçük saldırı gruplarınca gerçekleştirilmiş olan siber saldırı ve olayların kullanılmasıyla siber ortamda caydırıcılık sağlanabileceği açıkça ortaya konulabilir.

Siber suçluları, teröristleri ve casusları veya siber saldırı / savaş hazırlığında olan saldırganları siber güvenlik / savunma ile veya karşı siber saldırılarla / savaşla caydırmak yanında, devlet veya devlet benzeri sivil ya da askeri oluşumların siber ortam dışındaki faaliyetlerinin diğer ulusal güç unsurları ve yaptırımlarla birlikte ya da sadece siber güç ile durdurulması veya yönlendirilmesi konuları da siber caydırıcılık kapsamında değerlendirilebilir (Şekil 4.3).



Şekil 4.3: Siber caydırıcılık hedef ve amaçları.

Bu açıklamalar ışığında, siber caydırıcılığı desteklemek için dikkate alınması, tanımlanması ve başarılması gereken bir takım önemli esas ve prensipler kendiliğinden öne çıkmaktadır.

- Siber saldırganlar başta olmak üzere olası hedeflerin güçlü siber istihbaratla takibini sağlamak,
- Saldırganları saldırı öncesinde tespit etmek, siber güç ve caydırıcılıkta inandırıcı olarak saldırganların cesaretlerini kırmak,
- Siber alanda herhangi bir saldırıyı yapılmadan önce durdurmak,
- Saldırganlara korku verirken kullanıcılara güven vermek,

- Değerli varlıkları savunmak için doğru teknik ve yöntemleri uygulamak,
- Gelişmiş koruma sistemlerine ve alt yapılarına sahip olmak ve onları etkin kullanmak,
- Caydırıcılık ve yaptırım için siber gücü artırmak, geliştirmek ve diğer güç unsurlarıyla birlikte her an kullanıma hazır olmak,
- Siber savunmayı ve siber saldırıları doğru zamanda, doğru hedefe, doğru teknik ve yöntemlerle yapmak.
- Belirsizlikleri en aza indirmek için siber güvenlik stratejileri ve politikaları geliştirmek ve uygulamak,
- Değerli varlıkları ve sistemleri savunmak için herhangi bir saldırıya ve saldırganı cezalandırmak için karşı saldırıya her an hazır olmak.

Konuyla ilgili olarak askeri ve akademisyen araştırmacı, yazar ve düşünürlerin görüş birliği sağladığı husus; saldırıların bir kısmının devlet destekli olduğu bilinse de, daha önce açıklandığı üzere, bazıları küçük saldırı gruplarınca gerçekleştirilen siber saldırıların ve olayların sadece bilinen sonuçlarına bakmanın bile, 'siber alanda siber güç kullanılarak caydırıcılık (siber caydırıcılık) sağlanabilir' sonucuna ulaşmak için yeterli olduğudur.

Ortaya konulan inceleme ve analizlerde açıkça görülen husus; siber caydırıcılığın mümkün olduğu ve ileri düşünme, planlama, hazırlık, koruma, yetenek ve kapasite gerektirdiğidir. Bunun başarılması ve ulusal bilişim varlıklarının korunması, siber uzayın stratejik doğasını ve özellikle bilişim teknolojilerinin sağladığı yetenekleri dikkate alarak geliştirilecek stratejilerle siber gücün tek başına veya diğer ulusal güç unsurlarıyla birlikte etkin kullanımına bağlıdır.

4.3 Siber Caydırıcılık Uygulaması Örnekleri

Uygulanması büyük zorlukların aşılmasını gerektiren siber caydırıcılıkta saldıranın gücü, saldırı sonrası verilebilecek hasar ve zararlar konusunda da önceden net tespitlerde bulunmak günümüz şartlarında mümkün görülememektedir. Bu belirsizlik özelliği, siber caydırıcılığa asimetrik saldırı / savaş (zayıf tarafın daha güçlü tarafa karşı onun zayıf taraflarından da istifade ederek farklı taktik veya rastgele / belirsiz yöntemlerle yürüttüğü mücadele) [97] imkânı sağlamakta ve saldırının etkisini daha da artırmaktadır.

Saldırılar sonucu istekler tam olarak yerine getirilmese ve hedeflenen sonuçlara ulaşılmasa bile, saldırgana karşı saygınlık ve korku yaratılmakta, karşı tarafa verilen hasar ve zararlar ile saldırgan yararına hareketleri kısıtlanmakta, davranışları değiştirilmekte ve saldırganın diğer harekât şekillerinin başarıları olumlu şekilde etkilenmektedir.

Dünyada ve Türkiye'de geçmişte yaşanan siber saldırı ve olaylar incelendiğinde bunlardan hangilerinin caydırıcılık özellikleri içerdiği kolaylıkla görülebilmektedir. 2014 yılında Sony Şirketine yapılan siber saldırılar, sonuçları açısından siber caydırıcılığa somut ve güzel bir örnek teşkil etmesi nedeniyle aşağıda ayrıntılı olarak incelenmiştir.

4.3.1 Dünyada Siber Saldırılar ve Olaylarda Caydırıcılık

- **2007 yılında Estonya sistemlerine yapılan saldırılar**

2007'de, Estonya yönetimince Estonya'nın 2.Dünya Savaşı sırasında Rus askeri tarafından Alman işgalinden kurtarılmasını temsil eden anıtın kaldırılması üzerine, anıtın kaldırılmasına tepki ve tekrar yerine konması talepleriyle Estonya'ya yönelik siber saldırılar başlamıştır. Rus bilgisayar korsanları Estonya bilgi sistemlerine sızmış, özellikle internet ve bankacılık hizmetlerinin yaklaşık bir ay süresince durma noktasına getirilmesi neticesinde ülke çapında ekonomik ve toplumsal zararlar yaşanmıştır.

Rusya'da internet sitelerinde Estonya internet sitelerinin nasıl çökertileceğine yönelik bilgiler yer almış ve uzman korsanların yanında amatör bilgisayar kullanıcıları da saldırılara katılmıştır. Bazı kuruluşlar kendi sitelerini ve Estonya yurt dışından gelen internet hatlarını kapatmıştır. Saldırıda kullanılan köle bilgisayarların kontrol merkezi Rusya'da ve programın Kiril alfabesi ile yazıldığı tespit edilmiştir.

Rusya siber saldırı iddialarını kabul etmemiş ve sorumlularla ilgili işlem yapmamıştır. Estonya'nın başlangıçta Birleşmiş Miletler ve NATO'dan saldırıların durdurulması için yardım talebi reddedilmekle birlikte daha sonra Estonya'nın internet altyapısı onarılmış ve 14 Mayıs 2008'de Tallin'de 'NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defence Centre of Excellence, CCD COE)' kurulmuştur. [98, 99]

Günümüz de siber savaş denince akla gelen Estonya saldırılarında, saldırıların Rusya'dan devlet destekli olarak gerçekleştirildiği geniş kabul görmekle birlikte, doğrulama ve kanıt olmadığı için de Rusya'ya yönelik herhangi bir yaptırım uygulanamamıştır.

Saldırılarla Estonya'ya anıtın tekrar yerine konması kabul ettirilememekle birlikte, ciddi zarar verdirilmiş ve büyük bedel ödettirilmiş, dünyaya da Rusya merkezli siber saldırı gücünün böyle bir olayda bile ne kadar şiddetli olabileceğinin mesajı verilmiş, müteakip durumlar için yaptırım gücü - caydırıcılık gösterisi yapılmıştır.

- **2007 yılında İsrail savaş uçaklarının Suriye nükleer tesisine saldırısı:**

İsrail savaş uçaklarınca 6 Eylül 2007'de gece yarısından sonra "Operation Orchard (Meyve Bahçesi Harekâtı)" kod adıyla Suriye nükleer tesislerine gerçekleştirilen harekâtın en önemli özelliği saldırılar sırasında Suriye hava savunmasının hiçbir hedef görememesi olmuştur. Harekât başlangıçta Suriye tarafından kabul edilmemiş, daha sonra önemsiz bir saldırı gibi gösterilmiştir. İsrail tarafından yaklaşık bir yıl sonra açıklanmakla birlikte, nasıl yapıldığı hakkında bilgi verilmemiştir.

İsrail Hava Kuvvetlerine ait çok sayıda hava aracının katıldığı harekâtta Suriye hava savunma unsurlarının aldatılması, görüntü verilmemesi ve kayıp verilmeden dönülmesi konusunda bazı varsayımlar ve iddialar şu şekildedir. [25]

- Heron İHA ile aldıkları sinyalleri aynı frekansta geriye göndererek Suriye radar sistemlerini etkisiz hale getirilmesi.
- Suriye hava savunma sistemlerine yerleştirilen 'arka kapı' yazılımının Heron İHA ile etkinleştirilmesi ve radar sisteminin körleştirilmesi.
- İsrail ajanlarının Suriye hava savunma sistemlerinin fiber optik kablolarına 'saplama girerek' ve 'arka kapı' yazılımını etkinleştirerek sistemi körleştirmesi.

Türkiye sınırı takip edilerek gerçekleştirilen harekâtla ilgili olarak, İsrail savaş uçaklarının menzillerini uzatmak için kullandığı, atış altında uçuş durumunda ya da hafiflemek için bıraktıkları ve daha sonra İsrail F-15 savaş uçaklarına ait olduğu anlaşılan iki adet boş yakıt tankı Hatay'ın Hassa ve Gaziantep'in Oğuzeli ilçeleri arazisinde çobanlar tarafından bulunmasıdır [100].

İsrail siber güç destekli bu harekâtıyla, klasik savaş gücünün yanında siber savaş gücünü sadece Suriye'ye değil başta bölge ülkeleri olmak üzere bütün dünyaya

göstermiştir. Suriye hava savunmasının aldatılması, Rus hava savunma silah ve sistemlerine karşı güvensizlik yanında Rusya desteğinin sorgulanmasını da sağladı. Bu sorgulamayı o sıralarda Rusya'dan hava savunma silah ve sistem tedarik etme çalışmaları sürdüren İran'ı da olumsuz etkilemiş [25], böylece İsrail siber güç ve caydırıcılık desteğiyle ile çok yönlü bir kazanım sağlamıştır.

- **2008 yılında Gürcistan'a yapılan siber saldırılar**

2008'de, Gürcistan'ın Güney Osetya'ya saldırısı sırasında ve sonrasında Rusya-Gürcistan savaşında devlet başkanlığı internet sitesi dâhil tüm internet sayfaları engellenmiş, finans merkezleri, haberleşme sistemleri ve elektrik santrallerinde ciddi sıkıntılar yaşanmıştır.

Rus askeri harekâtı öncesinde, 19-20 Temmuz 2008 gecesi Gürcistan internet sitelerine yönelik saldırılar başlamış, uzman siber saldırgan ve korsanların yanında sıradan gönüllü kullanıcıların da saldırılara katılabilmesini sağlamak amacıyla siteler ve programlar kullanıma açılarak saldırılar yoğunlaşmış, birçok siteye erişim engellenmiş ve sayfaların içerikleri değiştirilmiştir. Gürcistan Rusya'dan gelen internet trafiğini engellemiş, ancak Rusya kaynaklı saldırılar özellikle Çin, Kanada, Türkiye ve Estonya'daki köle bilgisayarlar kullanılarak devam etmiştir. Siber saldırı olayları yoğunlaşması sonrasında Gürcistan'a yardım maksadıyla Estonyalı ve Polonyalı uzmanlar ile NATO Acil Müdahale Ekibi (NATO Rapid Response Team) Gürcistan'a gidip bilgi birikimlerini aktarmışlar ve teknik destek sağlamışlardır. [99, 101]

Siber saldırı olayları ile Gürcistan'a Güney Osetya'da geri adım attırılamamakla birlikte, bu saldırıların Gürcistan'a yönelik Rus askeri harekâtının kısa sürede hedefine ulaşmasına ve sonrasında Rusya'nın talep ve isteklerinin yerine getirilmesi büyük katkı sağladığı görülmüştür. Yani siber saldırılarla sağlanan caydırıcılık gücü ve etkisi askeri harekâtı kolaylaştırarak başarıyı artırmıştır.

- **2010 yılında İran nükleer programını hedefleyen saldırılar**

2010'da keşfedilen ve İran nükleer zenginleştirme programını hedefleyen 'Stuxnet' yazılımı ile (endüstriyel kontrol sistemlerini hedeflediği bilinen en tehlikeli zararlı yazılım) ciddi sıkıntılara sebep olunmuştur.

'Stuxnet' ABD'li ve İsrailli uzmanlar tarafından üretilmiş olan, 'en karmaşık virüs (500 KB)' ve 'ilk siber silah' olarak kabul edilmektedir. Yazılım bir çalışan tarafından

taşınabilir bellek ile kasıtlı veya kasıtsız olarak diğer çalışanların bilgisayarlarına bulaşmış, 30 bine yakın bilgisayarı ve özellikle Siemens ürünü kontrol sistemlerini etkilemiştir. Saldırı ile İran'ın 9.000 merkezkaç sisteminden (santrifüjünden) 5.300'ünün etkilendiği ve bunun sonucunda İran nükleer programının iki yıla yakın geciktirildiği iddia edilmektedir. [102]

ABD öncülüğünde İsrail ve AB ülkeleri ile BM'nin de isteğiyle İran'ın nükleer programını durdurması konusundaki yaptırımlarla birlikte uygulanan siber saldırılarla, uluslararası yaptırımlardan çok daha sonuç alıcı bir eylem başarıyla gerçekleştirilmiş, program fiziksel zararlar da verdirilerek iki yıl geciktirilmiştir. Programdan tamamen vaz geçirme sağlanamasa da yavaşlatılmıştır. Stuxnet yazılımı siber caydırıcılık gücü de veren bir siber silah olarak bütün dünya tarafından da yaygın kabul görmüş durumdadır.

- **2010 yılında WikiLeaks'in internette yayınladığı belgeler**

Kasım 2010'da, merkezi İsveç'te bulunan uluslararası bir internet oluşumu olan WikiLeaks (2006'da dünya çapında yozlaşma ve kötüye kullanmayı açıklama amacıyla açılan site) internette yayınladığı, ABD kaynaklı belgeler başta olmak üzere pek çok ülkeyle ilgili diplomatik belgeler ile dünya çapında ses getirmiş ve şimdiye kadar açıkladığı toplam bir milyon civarında gizli yazışma ile diplomaside depreme yol açmıştır [37].

Siber istihbarat ve casusluk da dâhil olmak üzere sayısal ortamdaki gizli bilgi ve belgelerin çalınarak internet ortamında yayımlanması olayı şeklinde özetlenebilecek olan bir siber saldırı olayı olan WikiLeaks olayı, ilgili ülkelerin iç yasalarına aykırılıklar yanında uluslararası anlaşma, sözleşme ve yasalara aykırılıkları, ihlalleri, vb. kural tanımazlıkları ortaya dökmesi açılarından benzerlerinin yaşanmamasına yönelik ciddi caydırıcı bir etki yaratan olay olarak tarihte yerini almıştır.

- **2010 ve 2011 yıllarında yaşanan ve "Arap Baharı" olarak adlandırılan olaylar**

Sosyal ağların, maliyetsiz veya maliyeti çok düşük olması, kullanım kolaylıkları ve sınırlama olmaksızın paylaşım sağlama özellikleri dolayısıyla, doğru ve zamanında kullanıldığında bireyler ve toplumlar üzerinde gücü ve etkisi çok yüksek seviyede, kontrolü ve engellenmesi çok zor olmaktadır. Bu tespiti dünyada en iyi destekleyen olay, 2010 ve 2011 yıllarında Tunus, Yemen, Mısır ve Libya'da yaşanan ve "Arap Baharı" olarak adlandırılan olaylar olmuştur. İnsanların ve toplumların çeşitli olaylarla

zamanla biriken öfkelerinin bilişim teknolojileri ve sosyal ağlar yoluyla etkilenmesi ve yönlendirilmesi sonucunda gelişen isyan ve devrim hareketleri genelde başarıyla sonuçlanmıştır. Araştırmacı gazeteci ve yazar Banu Avar; ABD Dışişleri Bakanı Clinton'a atfen "Hedefimiz insanlara interneti değil, meydanları nasıl kullanacaklarını öğretmek!", "Mısır'da Facebook ve Twitter an be an olayları izledi.", "Protestoların bir sonraki adımları koordine edildi. Halk korku ve umutlarını bu yolla paylaştı…" tespitleri ile "Arap Baharı" olaylarının "Facebook Devrimi" [103] olarak adlandırıldığına dair görüşleri bu sonucu teyit etmektedir.

Toplumsal olaylarda etkisini gösteren ve olumlu sonuçlar alınmasını sağlayan sosyal ağlar, süreç içerisinde siyasi parti yöneticilerinin daha geniş kitlelere ulaşmak ve onları amaçları doğrultusunda yönlendirmek için kullandıkları vazgeçilmez araçlar olmuştur. Özellikle 2016 yılı İngiltere Brexit oylamalarında ve ABD Başkanlık seçimlerinde sosyal ağların gerçekleri yalan haberlerle çarpıtarak halkın yönlendirilmesi maksatlı kullanıldığı ve önemli sonuçlar alındığı [104] görülmüştür.

Türkiye'de de bazı toplumsal olaylarda, 2013 yılında "Gezi Parkı Olayları"nda ve sonrasında yapılan seçimler döneminde sosyal ağlar yoğun olarak kullanılmış ve benzer süreçler yaşanmıştır. Özellikle Gezi olayları sürecinde, sosyal ağlarla halkın etkilenmesi ve yönlendirilmesi, getirilen yasaklar ve engellemelerin birçok yöntemle kırılması, sosyal ağların engellenmesinin çok zor olduğunu ispatlamıştır.

Son yıllarda yaygınlaşmaya başlayan ve etkileriyle de dikkat çeken sosyal ağların Türkiye'de kullanım oranları yükselmeye devam etmektedir. 2020 yılı Şubat ayı rakamlarıyla nüfusunun %74'si (yaklaşık 62,07 milyon) internet kullanan Türkiye'de; aktif sosyal medya kullanıcı sayısının önceki yıla göre 2,2 milyon kişi artarak 54 milyon (%64), sosyal medyaya mobilden bağlanan toplam kullanıcı sayısının ise 53 milyon (%99) olduğu, bu rakamların da her yıl arttığı görülmektedir [105].

Olayların siber caydırıcılık yönü, sosyal ağların gücü siber gücü direk olarak etkilemektedir. Kullanıcıların eğitimleri, bilinçlendirilmesi ve doğru yönlendirilmesi sonucunda içerden veya dışardan sosyal ağlar üzerinden gelen saldırılar başarılı olamayacak, diğer taraftan bu güç ihtiyaç duyulduğunda, siber savaşta veya caydırıcılıkta hedefe karşı etkin bir şekilde kullanılabilecek ve başarılı sonuçlar alınabilecektir.

- **2011'de İran Silahlı Kuvvetlerinin ABD İHA'sını ele geçirmesi**

2011 yılı Aralık ayında, İran Silahlı Kuvvetlerinin, Kaşmir bölgesinde ABD'ye ait gizli harekât yapan RQ-170 model İHA'sının kontrolünü ele geçirip sapasağlam yere indirerek el koyması olayı ABD'li yetkililerce başlangıçta reddedilmiş, ancak daha sonra kabul edilmiş ve hatta aracın geri iadesi istenmiştir [106]. Bu olaya öncesinde çok sayıda İHA'nın elektronik karıştırma, klasik silahlarla ateş vb. çeşitli saldırı yöntemleriyle düşürülmesine karşın ilk defa başkası tarafından kontrolü sağlanarak ve sağlam olarak ele geçirilme olayı yaşanmıştır. Ancak kesin yöntemi her iki taraf tarafından açıklanmamıştır. İHA'ların kontrolünün genelde telsiz frekans sistemleriyle sağlanması nedeniyle elektronik savaş teknik ve yöntemleriyle karıştırılarak düşürülmesi sağlanabilirken, bu olayda küresel konumlama sistemi casusluğu (GPS - Global Positioning System) ile birlikte karma yöntemler kullanılarak olayın gerçekleştirildiği değerlendirilmektedir. Bu varsayım bazı araştırmacılar tarafından da gerçeklenmiştir. [107]

Olayın siber caydırıcılık yönü ise; İran'ın siber gücünün varlığını ve seviyesini teyit etmesi, ABD'nin siber gücünün sorgulanması yanında ABD İHA'larının ilave tedbirler almadan İran ilgi ve etki sahasında hareketinin sınırlandırılmasının sağlanması olmuştur. Ayrıca siber ortamda bu başarıyı gösteren İran'ın siber gücünün diğer yetkinlikleri de düşünülmeye ve incelenmeye başlanmıştır.

- **2020'de Ukrayna yolcu uçağının İran tarafından düşürülmesi**

İran hava savunma unsurlarınca 8 Ocak'ta düşürülen Ukrayna yolcu uçağının, 11 Ocak ve sonrasında yapılan resmi açıklamalarda, uçağın 'hassas askeri bir noktanın' üzerinden geçerken 'insani hata' sonucu yanlışlıkla düşürüldüğü belirtilmişti. Olayın kısa ayrıntısında, Ukrayna uçağının seyir (Cruise) füzesi olarak algılandığı, o anlarda iletişimde yaşanan sorunlar nedeniyle hava savunma birimin gerekli izni beklemeden acele ve hatalı kararlar vererek füzeyle düşürdüğü açıklanmıştı. [80]

Olayın temel noktası insan hatasından kaynaklanmasıydı. Bu hatanın nedenleri arasında yer alan siber saldırılarla ilgili varsayımlar ve iddialar resmi makamlar tarafından doğrulanmamış ve herhangi bir rapor da bulunmamaktadır. Ancak olay öncesinde sırasında yaşananlarla ilgili tespitler siber saldırılar ve benzeri tespitleri düşündürmektedir.

İran'ın Kudüs Gücü Komutanı General Kasım Süleymani'nin de aralarında bulunduğu 10 kişinin 3 Ocak'ta Bağdat Havalimanı'nda ABD unsurlarınca düzenlenen hava saldırısında öldürmesine [108] misilleme olarak İran tarafından 8 Ocak'ta ABD'nin Irak'taki iki hava üssüne füze saldırısı düzenlemesi sonrasında ABD'nin olası misillemesine karşı İran birlikleri alarm hazırlık seviyelerini yükseltmişti [109]. Misilleme beklentileri ve ABD'nin her bakımdan yetenekleri personel üzerinde baskılar oluşturmuştu. ABD savaş uçağının sivil yolcu uçağını taklit ederek uçabileceği, İran hava savunma birimlerinin iletişiminin aksatılabileceği ve radarlarının körleştirilerek aldatılabileceği bölgede kullanılabilecek bir ABD seyir füzesinin radarda sivil yolcu uçağı gibi görünmesi vb. yetenekler bunlardan bazılarıydı.

Bütün bu belirsizliklerin sorgulanarak doğrulanması ve doğru karar verilerek uygulanması için zaman çok kısaydı. Hava savunma sisteminin Ukrayna yolcu uçağını kimlik tanımlama sorgulamasında ve birimler arasında iletişim aksaklıkları elektronik ve siber savaş karması saldırılarla kolaylıkla gerçekleştirilebilmektedir.

ABD unsurlarının bu yetenekleri kullanarak bir eylemi olmadıysa bile, ABD siber savaş gücü İran unsurlarına çok ciddi bir zarar vermiştir. Gelecekte sivil yolcu uçağı yerine gerçek durumla karşılaşıldığında yaşanacak belirsizlik ve karasızlıklar saldırıdan vazgeçme sonucu daha ciddi hasar ve kayıplara sebep olabilecektir. Kısaca siber gücün varlığı ve psikolojik harekât destekli sağlanan algılar siber caydırıcılık sağlayabilecektir.

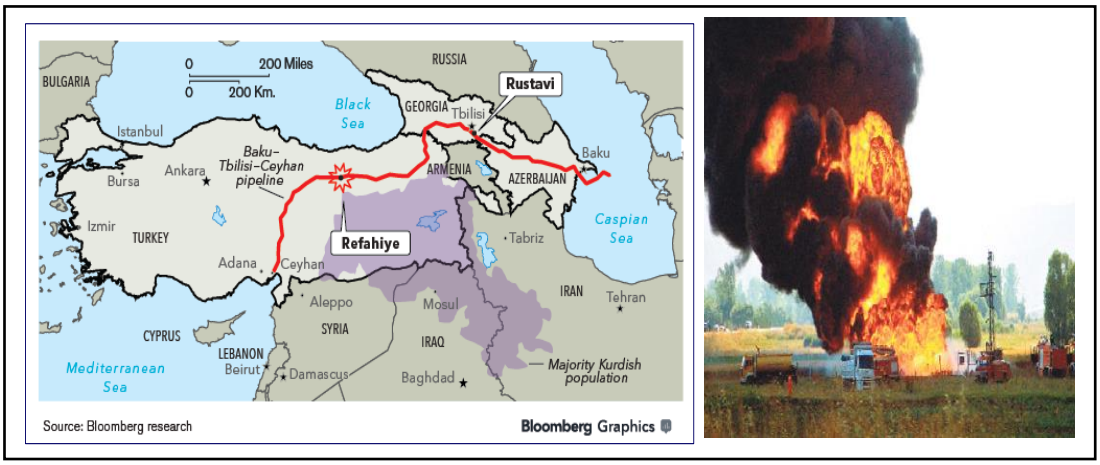
4.3.2 Türkiye'de siber saldırı ve olaylarda caydırıcılık

- **2008 yılında Bakü-Tiflis-Ceyhan boru hattına yapılan siber saldırı**

5 Ağustos 2008'de Bakü-Tiflis-Ceyhan boru hattında meydana gelen patlamada sabotajdan şüphelenilmiş, PKK bölücü terör örgütünün saldırıyı üstlenmesine karşın araştırma sonucunda patlamanın teknik arızadan kaynaklandığı belirtilmişti (Şekil 4.4)

Olaydan 6 yıl sonra, ABD merkezli Bloomberg haber sitesi, dört farklı Batılı kaynağa dayanarak "Patlamanın sebebi karmaşık bir 'siber saldırı', Patlamadaki 'silah' bir klavye" açıklaması yapmış, yine aynı haberde ABD'li Prof. D. Reveron "Saldırının Büyüklüğü 'Siber Savaşın Tarihi'ni tekrar yazıyor" söyleminde bulunmuştur [111,

112]. Söz konusu haber sitesince yapılan ve diğer açık kaynaklarda da yer alan açıklamalarda saldırının şu şekilde yapıldığı iddia edilmiştir.



Şekil 4.4: Bakü-Tiflis-Ceyhan boru hattına saldırı [111, 112].

Saldırganlar doğal gaz boru hattının işletme sistem ağına güvenlik kameraları bağlantısından girmiş, Windows işletim sisteminde çalışan ve alarm sistemlerini yöneten bilgisayara zararlı yazılım yerleştirmişti. Alarmı harekete geçirmeden petrol üzerindeki basınç artırılarak boru hattı patlatılmıştı. Patlama zamanı dâhil 60 saate yakın güvenlik kamerası görüntüleri silinmişti. Alarm sisteminin neden çalışmadığının araştırılması sırasında sisteme dışarıdan giriş yapıldığı anlaşılmıştı. Uydulara bilgi akışının kesilmesi kuvvetli bir 'sinyal karıştırma' faaliyetini gösteriyordu. Aynı ağa bağlı kızılötesi bir kamera, patlamadan günler önce boru hattı yakınında dizüstü bilgisayarlarla yürüyen siyah üniforma benzeri kıyafetli iki kişinin görüntüsünü kaydetmişti.

Saldırı sonrası 30 bin varilden fazla petrol çevreye saçıldığı, Türkiye'nin 7,5 milyon dolar, BP petrol şirketi ve ortaklarının 75 milyon dolar ve Azerbaycan'ın 1 milyar dolardan fazla para kaybettiği belirtilmiştir. [111]

Saldırının yapıldığı tarihlerde Abhazya ve Güney Osetya sorunları dolayısıyla Rusya ile Gürcistan arasında bir savaş yaşanmaktaydı. Gürcistan Rusya kaynaklı ciddi siber saldırılarla da karşı karşıya kalmıştı. Türkiye ve Azerbaycan savaşla ilgili tarafsız görünmekle birlikte iki ülkenin de kamuoyu Gürcistan'ın yanında yer almaktaydı. Saldırıya uğrayan boru hattı Azerbaycan, Gürcistan ve Türkiye ile BP dolayısıyla İngiltere için de önem taşımaktaydı. Türkiye Gürcistan'ın egemenliğinin ve toprak bütünlüğünün korunması ve sorunlarına bu ilkeler çerçevesinde çözüm bulunmasını istemekle birlikte, siber caydırıcılık konusunda bir yorum da bulunmak için bu

saldırının öncesinde ve sonrasında ilgili ülke makamları arasında politik ve diplomatik neler yaşandığı bilinmemektedir.

Ancak boru hattı saldırısının Rusya ile Gürcistan arasındaki olaylarla bağlantısının bulunması olasılığı çok yüksektir. Konuyla ilgili T.C. Cumhurbaşkanlığı İletişim Merkezi (CİMER)'ne kişisel olarak müracaat edilerek konuyla ilgili açık kaynaklarda yer alan iddiaların doğruluğu ile ilgili bilgi istenmiş, 'Boru Hatları ile Petrol Taşıma Anonim Şirketi Genel Müdürlüğü' tarafından 05.08.2019 tarih ve 00:24 saatli e-mesaj ile "…..Bu itibarla, ilgili birimlerimiz tarafından, başvurucunun talep ettiği bilgi ve belgelerin milli güvenliğimiz açısından önem arz eden bilgiler içermesi nedenine bağlı olarak verilmesinin uygun olmadığı…" [113] bilgisi verilmiştir.

- **2011 yılında Telekomünikasyon İletişim Başkanlığı (TİB)'na yapılan siber saldırılar**

İnternet ortamında yer alan yayınlara erişimle ilgili özel nitelikli kanun olan 5651 sayılı kanunun, internete filtre uygulaması olduğu ve temel hak ve özgürlüklerin ihlal edileceğini savunan 'Anonymous' adlı Uluslararası Bilgisayar Korsanları Topluluğu, 09 Haziran 2011 günü akşam saatlerinde, BTK - Telekomünikasyon İletişim Başkanlığının internet sitesine saldırmış, erişim engellenerek devre dışı bırakılmıştır. Ancak siteye erişim ancak gece yarısından mümkün olabilmiştir. Saldırıdan '.gov' uzantılı başka siteler de etkilenmiş, Devlet Meteoroloji İşleri ve Sosyal Sigortalar Kurumu gibi birçok siteye daha aynı saatlerde ulaşılamamıştır [114].

Saldırıların maksadı internetle ilgili kısıtlamaların kaldırılmasına yönelik olarak geri adım atılmasını sağlamak olmakla ve bu konuda geri adım attırılamasa, yani siber caydırıcılık sağlanamasa da, konu yazılı ve görsel basında geniş yer bularak kamuoyunun dikkatinin çekilmesi sağlanmıştır.

- **2015 yılında elektrik enerji sistemlerine yönelik saldırı**

31 Mart 2015'de saat 10:36'da, Türkiye'de elektriğini İran'dan alan Van ve Hakkâri illeri hariç 79 ilde 10 - 18 saat süreli elektrik kesintisi yaşanmıştır. Aynı gün 'Karanlıkta' İstanbul Adliye Sarayı'na teröristler sızarak bir savcıyı rehin aldıktan sonra katletmişlerdir.

Arızanın nedeni yetkililer tarafından başlangıçta anlaşılamadı ve açıklanamadı. Enerji Bakanı; "…Operasyonel hata mı yoksa siber saldırı mı? Bu az mı çok mu ihtimal bunu söyleyemem, takipteyiz." şeklinde açıklamada bulunmuştur. [115]

Elektrik kesintisi nedeniyle ilgili uzmanların daha sonraki saatlerde görüşü; "Yüklü bir hattın devre dışı kalması sonucu Ana Kontrol Merkezlerinin (Gölbaşı / Ankara ve Adapazarı) hatlardaki elektrik frekansında 50 Hz. - 0 Hz. arasındaki dalgalanmayı düzeltememesi nedeniyle tüm sistem dinamiğini bozması, ardından diğer hatların bir arıza olduğunu düşünerek kademeli olarak kendilerini kapatması" şeklinde açıklanmıştır [116].

Bir Hafta sonra ise; "İyileştirme ve yeni devreye girecek santrallerin bağlantı hatları çalışmaları sebebiyle Türkiye doğusunu batısına bağlayan eksende 5 iletim hattının devre dışı kalması, hatların aşırı yüklenmesi, oluşan salınımlar nedeniyle bağlantının kopması" şeklinde açıklamalar yapılmıştır.

Konuyla ilgili olarak bilgi edinme kanunu kapsamında Cumhurbaşkanlığı İletişim Merkezi (CİMER)'ne yapılan bilgi edinme başvurusuna cevap olarak, basın yoluyla yapılan açıklamaları doğrular bir teknik rapor gönderilmiştir [117]. Kıta Avrupa'sında son 15 yılın üçüncü en önemli arızası olduğu, anormal frekans sapmalarına bağlı olarak yüksek koridor yüklenmeleri, düşük frekanslı yük atlamaları ve uygun olmayan elektrik santrali davranışı gibi nedenlerle meydana geldiği belirtilen "Türkiye 31 Mart 2015 Sistem Çökmesi Raporu"nda, olayın nedenleri arasında siber saldırı kaynaklı bir bulgu yer almamıştır.

Ancak olayın temel nedeni olarak, Türkiye elektrik sisteminde başlıca Doğu - Batı koridorunun aşırı yüklenmesinin önlenmesinde teknik yetersizlikler ile arıza ve bakım planlarının koordinasyon eksiklikleri açıklanırken ana iletim hatları için mesafe koruma ayarları analizi ile ilgili SCADA sistem veri tabanıyla koordinasyonun sağlanmasının gereği vurgulanmıştır.

Raporda belirtilen teknik eksiklikler ve yetersizlikler yanında personel hataları ve kusurları da bulunmaktadır. Nitekim olay sonrası günlerde TEİAŞ Genel Müdürü istifa etmiş ve bazı görevliler açığa alınmıştır. Aradan yaklaşık 6 ay kadar sonra 06 Eylül 2015 günü TEİAŞ'ın bilgisayar sistem ve ağları ihalesine çıkması [118], elektrik kesintisi olayının nedenleri arasında siber saldırı olmasa bile, bilişim sistem ve

altyapıları eksikliği ve siber güvenlik zafiyeti nedeniyle bir siber olay yaşanmış olabileceğini düşündürmektedir.

Yaşanan arıza olayının başlangıç nedeni bağlantı hatları çalışmaları olarak açıklanmakla birlikte, ortaya çıkan hasar ve zararlarla ilgili başka bir açıklama yapılmamış ve siber saldırı olamadığına dair tereddütler bu güne kadar giderilmemiştir. Sadece elektriği İran'dan sağlanan Van ve Hakkâri illerinin olaydan etkilenmemesi, saldırıların İran kaynaklı olabileceği şüphesi de yaratmıştır.

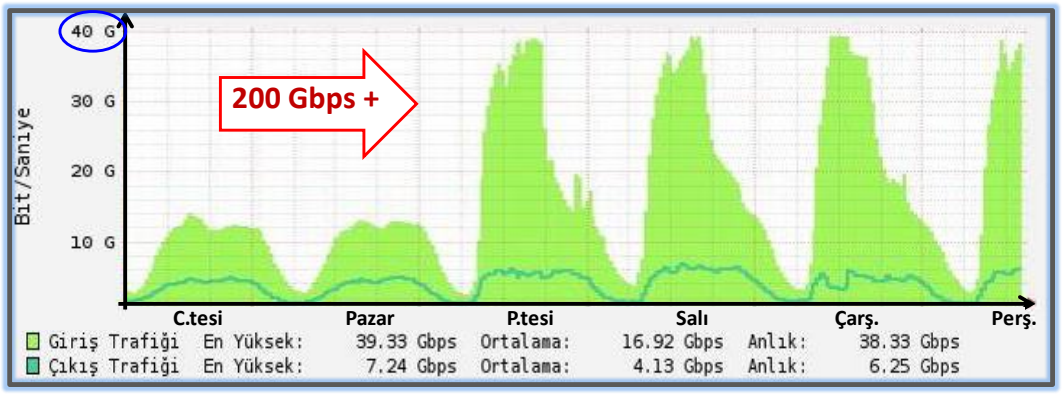
Olayın görünen ve açıklanan nedenleri teknik yetersizlikler ve personel hataları görünmekle birlikte, siber olay veya saldırı bağlantısı hiç yoktur demek zordur. Gerçek nedeni siber olay veya saldırı olmasının düşüncesi bile endişeye sevk eden ve korkutan bir siber caydırıcılık özelliği taşımaktadır.

- **2015 yılında internet sistemlerine yönelik saldırılar**

14-24 Aralık 2015 tarihlerinde, özellikle 'tr' uzantılı alan adlarının yönetildiği sunuculara saldırılar yapılmış, birçok banka, noter ve devlet kurumunun internet sayfasına ve mobil uygulamalarına erişim engellenmiştir.

Saldırı 14 Aralık Pazartesi günü sabahı başlamış, '.tr' uzantılı alan adlarını yöneten ODTÜ Bilgisayar Merkezi'ndeki NIC.TR yoğun saldırılara hedef olmuştur. Ağ ve Alan Adı (DNS) sistemleri ve sunucuları, dünyanın çeşitli bölgelerinden gelen ve saniyede milyonlarca sahte mesajla veya sorguyla sistemi devre dışı bırakmak amacı güden dağıtık servis dışı bırakma (DDoS) saldırısına uğramış ve saldırı nedeniyle ya çok yavaşlamış ya da tıkanıp cevap veremez hale gelmiştir Şekil 4.5'te 12-17 Aralık 2016 tarihleri arasında sistemlerde ki trafik yoğunluğu görülmektedir. [119, 120]

'.tr' DNS sunucularına erişildiği durumlarda DNS sunucularının verdiği yanıtların isteği yapan noktalara gidişi yönünde ciddi gecikmeler olmuştur. Diğer bir deyişle, saldırganlar tarafından ana iletişim ana yollarında oluşturulan yapay ve yoğun trafik, ülke ağının önemli merkezi noktalarında tıkanmalara ve yavaşlamalara sebep olmuştur. Olayı inceleyen uzmanlar tarafından saldırılarda amacın ulusal siber sistemi yavaşlatmak, durdurmak, mümkünse çökertmek olduğu, aynı zamanda Türkiye'nin siber altyapısının da test edildiği değerlendirmeleri yapılmıştır [121].



Şekil 4.5: 12-17 Aralık 2016 tarihlerinde sistemdeki trafiğin durumu [119].

Türkiye'ye dönük bu saldırılarda, daha önce ele geçirilen bazı bilgisayarların (Köle bilgisayar, botnet) da sahiplerine fark ettirmeden kullanıldığı tespit edilmiştir. Saldırılar sırasında, başta Garanti, Akbank, Ziraat ve İş Bankası olmak üzere birçok bankanın internet sitesi, mobil uygulamaları, POS cihazları ve ATM'si belli sürelerle devre dışı kalmıştır. Noter sistemi çökmüştür. E-Devlet uygulamalarında sorunlar yaşanmıştır. Ulaştırma, Denizcilik ve Haberleşme Bakanı (UDHB) yurtdışı kaynaklı olan ve kaynağı tam olarak belirlenemeyen saldırıların 14 Aralık'tan itibaren etkili olduğunu, hemen karşı önlemlerin devreye alındığını söylemiştir [122].

Rus savaş uçağının Türk savaş uçakları tarafından 24 Kasım 2015 tarihinde düşürülmesi nedeniyle Rusya'dan yapılan çeşitli tehditler nedeniyle saldırlar ile ilgili şüpheler Rusya'ya yönelmiş [123], ayrıca saldırıların boyutu ve dünyanın her yerinden gelmesi, kesin bir delil elde edilememekle birlikte, etkin bir saldırı ağı olan Rusya'nın bu işin arkasında olduğu iddiasını daha da güçlendirmiştir. Buna karşın ilk başta herkesin Rusya'dan şüphelendiği bu saldırıları, saldırıdan bir hafta sonra kendilerini Anonymous olarak adlandıran ve Türkiye'de 50 bine yakın bilgisayarı ele geçirdikleri iddia edilen, siber saldırı grubu üstlenmiştir [124, 125].

Rus televizyonu, "Türkiye'ye son günlerde yapılan siber saldırıların Rusya ile hiç bir bağlantısı yok" iddiasında bulunurken, Televizyona konuşan bir Anonymous üyesi, Türkiye'ye 'kötü sonuçlar' armağan edeceklerini ileri sürerek "Biz Türkiye'nin banka sistemini çökerteceğiz. 5 büyük bankaya, 40 binden fazla Türk sitesine saldırı yaptık. Bunlar daha başlangıç" tehditlerinde bulunmuştur. Amaç ülkenin kritik altyapılarını hizmet veremez duruma getirip sokaktaki vatandaşın hayatına dokunacak kadar bir kargaşa ve karışıklık ortamı oluşturmak olduğu, bunun için de ülkenin özellikle finans

altyapısına yapılacak bir saldırının hem çok ses getireceği hem de ciddi manada maddi zararlara sebep olabileceği düşünülerek seçildiği değerlendirilmiştir [126].

14 Aralık saat 16.20'de Türkiye'de yetkililer saldırıyı önlemek için NIC.TR sunucularına erişimi yurt dışına kapatmıştır. Böylece Türkiye'de içindeki kurumlar arasında iletişim yeniden sağlanmıştır. Ancak Türkiye'deki yaklaşık 400 bin kadar '.tr' uzantılı şirket ve resmi kurumun sitesine yurt dışından erişim kesilmiştir. Özellikle yurt içinden köle bilgisayarlar dolayısıyla saldırılar tamamen durdurulamamış ve sonrasında dağıtık konumlara yerleştirilmiş daha fazla sunucu ile hizmet verilmeye başlanmış ve bu sayede saldırı bertaraf edilmeye çalışılmıştır. [124, 125, 127]

Saldırı sonuçları ile ilgili zararlar ve kayıplar konusunda herhangi bir resmi ya da kurumsal açıklama yapılamamakla birlikte, kişisel kullanıcıların veya kurumların finans, bankacılık, noter, vb. işlerde işlemlerini zamanında yapamadıkları için maddi, işgücü, zaman vb. kayıplara uğramıştır. Saldırılarda yurt içinde ele geçirilmiş köle bilgisayarların etkisinin de yüksek olduğu anlaşılmış ve siber güvenlik açısından önemli bir sorun olarak ortaya çıkmıştır.

2014-15 istatistiklerine göre Türkiye'nin internete bağlı bilgisayar miktarına göre oranlamada (% 5), 2 milyona yakın bilgisayar ile İngiltere, ABD, Almanya, ve Rusya'dan sonra, dünyada 5'inci sırada olduğu belirtilmiştir [72, 128]. Saldırıları kendilerinin yaptığını iddia eden gruplar tarafından da bu konunun vurgulanması dikkat çekicidir. En önemli kayıplardan birisi de, saldırılar karşısında işlemlerdeki aksamalar nedeniyle dış dünyaya internetin kapatılması sonucu, hem Türkiye ve hem de ilgili kurum ve kuruluşlar açısından saygınlık kaybı yaşanması olmuştur.

Olayın tarafsız ve geniş bir yorumla Rus uçağının Türk Hava Kuvvetleri tarafından düşürülmesi nedeniyle bir cezalandırma yanında diğer diplomatik ve ekonomik yaptırımlarla birlikte Türkiye'ye bir boyun eğdirme bazı talep ve istekleri yerine getirtmek için caydırıcılık maksatlı bir hareket olduğu açıktır.

4.3.3 2014 yılında Sony şirketine yapılan siber saldırıların siber caydırıcılık açısından incelenmesi

Siber caydırıcılıkta, askeri yeteneklerin ve güç gösterilerinin aksine, bir ülkenin büyüklüğü pek önemli değildir. Bir siber savaşın yapıldığı savaş alanı tüm dünya olup, nitelik, girişim ve konum özellikleri genellikle nicelikten daha önemlidir [129].

Bunun daha iyi anlaşılmasını sağlamak için, siber saldırılarla caydırıcılığın nasıl sağlandığı ve hedeflenen sonuçlara nasıl ulaşıldığı açıkça görülen ve açık kaynaklarda da geniş yer tutan, "Aralık 2014'te Kuzey Kore Lideriyle ilgili film nedeniyle Sony Şirketinin yoğun siber saldırılara maruz kalması ve filmin gösterimden kaldırılması" olayı örnek alınmış ve konuyla ilgili açık kaynaklara yansıyan bazı bilgi ve haberler incelenmiştir.

ABD'de Sony Pictures şirketinin yapımcısı olduğu, 'Röportaj (The Interview)' isimli filmde, Kuzey Kore Lideri Kim JONG-UN ile röportaj yapmaya hazırlanan bir muhabirin ABD Merkezi İstihbarat Teşkilatı (CIA) tarafından Kim'e suikast düzenlemek için eğitilmesi ve ardından Kuzey Kore'de yaşadıkları anlatılmaktadır [130].

Film, Kuzey Kore'de büyük öfkeyle karşılanmış ve "Yüce lideri aşağılıyorlar" yorumları yapılmıştır. Bu yorumların ardından, Sony kendilerini 'Tanrının Havarileri (God'sApstls, GA)' ve 'Barışın Savunucuları (Guardians of Peace, GoP)' olarak tanımlayan kimliği belirsiz bilgisayar korsan grupları tarafından başlatılan yoğun siber saldırılara maruz kalmış ve düzenlenen siber saldırılar sonrasında, Sony şirketine ait, aralarında çekimine başlanmamış film senaryoları dâhil, pek çok film çalınarak internet ortamında yayımlanmıştır. Şirket içindeki pek çok gizli bilgi ve belgeler ile tüm özel elektronik posta ve yazışmalar da bu arada internet ve açık kaynak ortamlarında görülmüştür. Sony Pictures şirketi, yaklaşık 100 TB büyüklüğünde verilerin çalındığı bu saldırılar nedeniyle milyonlarca dolar zarara uğratılmıştır. [131-133]

Filme tepki olarak gönderilen ve Sony çalışanlarının bilgisayar ekranlarına "11 Eylül 2001'de neler olduğunu hatırlayın. Size tavsiyemiz bu filmi gösterime sokan sinemalardan uzak durmanız!" denilen mesajlar düşmüştür. Gönderilen e-postalarla filmi göstermeyi planlayan sinema salonları da açıkça tehdit edilmiştir [134].

Sony şirketinin bilgisayarlarına sızan zararlı yazılımın Destover adında yeni bir zararlı yazılım türü olduğu tespit edilmiş ve ABD Federal Soruşturma Bürosu (FBI), bu saldırılardan Kuzey Kore'yi sorumlu tutmuştur. FBI'nın, "Siber saldırıların ardındaki yazılımların Kuzey Kore ile bağlantılı olduğunu ve filmle bağlantılı şirketlerin risk altında olabileceğini…" duyuran açıklaması yayımlanmıştır. 15 bine yakın Sony çalışanı kişisel bilgilerinin açık edilmesi nedeniyle Sony Firmasına dava

açarken, ülkenin en büyük sinema zincirleri filmi göstermekten vazgeçtiklerini açıklamıştır [130, 132, 134].

Gelişmeler üzerine Sony şirketi, 44 milyon dolara mal olan filmi geri çektiklerini belirten açıklamasında "Ortaklarımızın kararını anlıyor ve saygı duyuyoruz ve tabii çalışanların ve sinemaseverlerin güvenliğine verdikleri değeri paylaşıyoruz." denilmiştir. Filmin sadece ilk hafta sonu 30 milyon dolar gişe yapması ve Sony'nin filmden toplam 120 milyon dolar kazanabileceğinin beklendiği de raporlanmıştır [130].

ABD yönetimi, Sony'ye yapılan saldırıların 'ulusal güvenlik meselesi' olarak değerlendirildiğini duyurmuştur. ABD Başkanı Barack Obama, söz konusu filmin gösterime çıkmasının engellenmesine neden olan siber saldırıların ardında Kuzey Kore'nin olduğuna inandıklarını belirtmiştir. Kuzey Kore tarafından yapılan açıklamalarda, siber saldırılardan sorumlu oldukları iddiaları yalanlanmış ve bunun 'terbiyesizce yapılan dedikodular' olduğu belirtilerek konunun ortak soruşturulması teklifinde bulunulmuştur. [135]

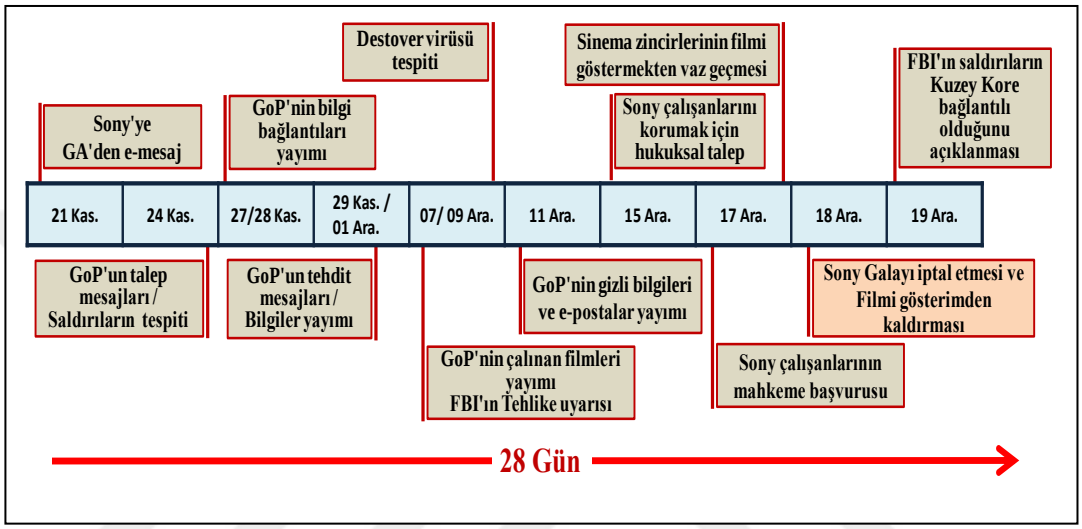
"Kuzey Kore liderine yönelik saldırıyı konu alan 44 milyon dolarlık filmin, 'siber korku' nedeniyle geri çekildiği, Sony Pictures'ın, kendi halkını öldüren zalim bir diktatörün baskılarına boyun eğdiği, bu olayın ifade özgürlüğüne bir tehdit olduğu…" haber ve yorumları yapılmıştır. ABD Beyaz Saray Basın Sözcüsü'nün 'önemli bir ulusal güvenlik meselesi olduğunu' açıkladığı saldırı olayıyla ilgili olarak, Temsilciler Meclisi'nin eski başkanı Newt Gindrich, 'Sony'nin kararı ile ABD'nin ilk siber savaş yenilgisini aldığını' belirtmiştir [133].

Sonuçta; Kuzey Kore lideriyle ilgili komedi filminin gösterimden kaldırılmasıyla bu ülke tarafından devlet destekli (direk / dolaylı) siber saldırılar hedefe ulaşmış, bir ülke veya devlete karşı olmasa da Sony gibi uluslararası, küresel dev bir şirkete karşı, yapılan siber saldırılar ile caydırıcılık sağlanmış ve geri adım attırılmıştır.

Saldırıların başarılı olmasında;

- Siber istihbarat,
- Teknolojik güç,
- İnternet başta olmak üzere yazılı ve görsel iletişimin ile psikolojik harekâtın etkin kullanılması,

- Saldırıların çok iyi düşünülüp hedef odaklı olarak yönlendirilmesi ve yönetimi,
- Devlet desteğinin gizliliği,
- Diplomatik destek ve
- Misillemeye karşı hazırlık gibi faktörler önemli rol oynamıştır. Bu olayda, nükleer güce ve caydırıcılığa sahip bir ülke olan Kuzey Kore'nin, sahip olduğu kısıtlı siber güç yeteneklerini caydırıcılık maksadıyla etkinlikle kullanarak, 28 günlük bir eylem aktif eylem süreci içerisinde, hedefine ulaştığı anlaşılmaktadır (Şekil 4.6).



Şekil 4.6: Sony Pictures Şirketine yapılan siber saldırılar süreci.

Saldırıdan kısa süre sonra Başkan Obama siber saldırıların ivedi ve büyüyen bir tehdit oluşturduğuna dikkat çekerek Kongre'ye hükümet ile özel sektör arasında işbirliği ve iletişim sağlayacak yeni siber güvenlik yasa tasarısı getireceğini duyurmuştur. Kamu veya özel sektörün siber tehditlerle tek başına başa çıkamayacağını vurgulayan Obama, tasarının "siber tehditle ilgili bilgileri paylaşan şirketlerin korunmasının sağlanması, kişilerin özel yaşamları ve özgürlüklerinin koruma altına alınması" gibi hususları da içereceğini dile getirmiştir. [136]

Kısaca, Sony Pictures şirketine yapılan saldırılar, olayın ulusal bir güvenlik sorunu olarak ele alınmasını sağlamış, değişen düşünceler ve bakış açılarıyla alınan tedbirler ve hareket tarzları 2015 - 2016 yıllarında geliştirilen siber güvenlik stratejisi ve eylem planlarına yansımıştır.

Elbette ki siber caydırıcılık, klasik askeri caydırıcılık veya nükleer caydırıcılık kadar kolay ve kesin kural veya esaslarla açıklanamaz. En basit açıklama olarak, nükleer caydırıcılık, 'nükleer silahlara sahip taraflar arasında, hedeflerin ve saldırı

etkileriyle sonucunun belli olduğu' bir durumda söz konusudur [86]. Buna karşın siber caydırıcılıkta; güvenlik ve savunmanın yüksek maliyeti yanında, saldırı ve taarruz yetenekli siber güce sahip olmak kolay ve maliyeti düşük olmakla birlikte, günümüz şartlarında hedefin belirlenmesinin çok büyük zorluklarının bulunduğu, misilleme saldırısının başarısızlıkla sonuçlanmasının ve aynı saldırı eyleminin tekrarlanmasının zorlukları gibi olumsuzluklar yadsınamaz gerçeklerdir.

Yine siber caydırıcılıkta saldıranın gerçek gücü bilinememekte, karşı tarafın değerli varlıklarının risk altında tutulup tutulamayacağı yani saldırı sonrası verilebilecek hasar ve zararlar konusunda da önceden belirgin tespitlerde bulunmak günümüz şartlarında mümkün görülememektedir. Bu ve benzeri konularda belirsizliklerin olması, siber caydırıcılığa asimetrik saldırı / savaş özelliği ve imkânları sağlamakta ve caydırıcılığın etkisini daha da artırmaktadır.

5. ULUSAL SİBER GÜVENLİK STRATEJİ VE POLİTİKALARI

5.1 Strateji ve Politika Kavramları

Geçmişten günümüze anlamı genişleyen, savaş sanatı olarak askeri alanlarda kullanılması yanında, siyasal, ekonomik, kültürel vb. her alanda kullanılmaya başlanan strateji kavramı sözlüklerde, "Bir amaca ulaşmak için izlenmesi gereken ana yol" [67] olarak tanımlanmaktadır. Günümüzde strateji savaş sanatı tanımlamasının ötesinde bir bilim dalı olarak kabul edilmiş, üniversitelerde örgütler ve toplumlar başta olmak üzere, iş ve sosyal yaşamı oluşturan bütün unsurlara stratejik bilinç ve yaklaşım becerisi kazandırmaktan, devlet yönetimlerinin yapılanması ve faaliyetlerinin belirlenmesine kadar çeşitli eğitimler verilmeye başlanmıştır.

TDK Sözlüğünde stratejinin tanımı, bilim ve sanat yönü de vurgulanarak, "Bir ulusun veya uluslar topluluğunun, barış ve savaşta benimsenen politikalara destek vermek amacıyla politik, ekonomik, psikolojik ve askerî güçleri bir arada kullanma bilimi ve sanatı" [137] şeklinde yapılmıştır. Bu tanımdan hareketle ulusal stratejinin tanımı da, "Ulusal gücü oluşturan unsurların, ulusal politikaların desteklenmesi amacıyla birlikte kullanılması bilim ve sanatı" şeklinde yapılabilir.

TDK Sözlüğünde 'Politika' ise; "Belirlenen amaç veya hedeflere ulaşmaya yönelik karar ve eylemler bütünü" [138] olarak açıklanmaktadır. Devletler özellikle ülkelerinin güvenliklerini sağlamak için, ulusal güvenlik stratejileri doğrultusunda belirledikleri politikaları gerçekleştirmek maksadıyla, bazen gizli bazen de açık olarak, ulusal güvenlik siyaset ve politikalarını belirlemekte ve uygulamaya koymaktadır. Türkiye'de Milli Güvenlik Kurulu (MGK) tarafından her beş yılda bir iç ve dış tehditler ile bu tehditlere karşı mücadele esaslarını içeren, 'Çok Gizli' gizlilik dereceli, 'Milli Güvenlik Siyaset Belgesi (MGSB)' hazırlandığı ve eklerinin de her yıl güncellendiği bilinmektedir.

Ülkeler ve devletler gibi, ülke ve devletleri meydana getiren toplum, kurum, kuruluş, şirket, örgüt, vb. birimlerin de faaliyetlerini düzenleyerek geleceğe dönük

yönlendirmek ve başarılarını artırmanın yanında, olası tehditlere, risklere ve karşılaşılacak her türlü olumsuzluklara karşı tedbirlerin alınmasını sağlamak maksatlarıyla kurumsal strateji ve politikaların geliştirilmesi gerekir. Siber güvenlik boyutunda bu strateji ve politikaların adı da 'Kurumsal Siber Güvenlik Strateji ve Politikaları' olmaktadır. Kurumsal siber güvenlik strateji ve politikalarının zamanında ve doğru olarak hazırlanıp eksiksiz ve kararlılıkla uygulanması, ülkenin ulusal siber güvenlik strateji ve politikalarının başarısını da artıracaktır.

5.2 Kurumsal Siber Güvenlik Strateji ve Politikaları

Dışarıdan ya da içeriden günden güne artarak ve çeşitlenerek devam eden siber tehditlere, risklere ve saldırılara karşı bilginin ve bilişim sistemlerinin korunmasının daha da zorlaşması kapsamında, kurumların güvenlik ihtiyaçları da artmakta ve daha fazla önlem alınması zorunluluk halini almaktadır. Çünkü bireysel veya kurumsal olsun, en önemli değerlerden olan bilginin korunması gereken temel nitelikleri olarak gizliliğinin açığa çıkarılmaması yani gizliliği, bütünlüğünün korunması ve kullanım ihtiyacı durumunda erişilebilir olması gerekmektedir. Bu üç temel gerekliliğin yanında; kurumsal bilgiler için de güvenilirlik, kimlik denetimi, inkâr edememe, sorumluluk, erişim denetimi ve emniyet gibi destekleyici unsurların sağlanması da büyük önem arz etmektedir.

Bu nedenle günümüz dünyasındaki bütün kurum, kuruluş ve şirketler tehlike altındadır. İnternet servis sağlayıcı firmaları, ortakları ve müşterileri için erişim sağlarken aynı zamanda milyonlarca kötü niyetli saldırgana ve suçluya da erişim imkânı vermektedirler. Saldırganlar fiziki olarak şirketlerin bulunduğu ülkeye girmeden, internet sayfalarına, veri tabanlarına ve kritik altyapı bilişim sistemlerine saldırabilmekte ve zarar verebilmektedirler [139]. ABD FBI Direktörü James Comey'in, 2014 yılında söylediği "Günümüzde iki türlü kurum var. Siber saldırıya uğrayanlar ve siber saldırıya uğradığını bilmeyenler…" [140] sözü bu acı gerçeği çok iyi açıklamaktadır.

Bu doğrultuda, kurumlar için bilgiyi ve bilişim sistemlerini korumak çok önemlidir ve bu maksatla kurulan güvenlik sistemleri her geçen gün daha da önem kazanmaktadır. Ancak kurumlar için kurulan güvenlik sistemleri daha çok kurum dışından gelen saldırıları önlemek amacıyla kullanılmakta ve genellikle kurum içi

güvenlik ve kontrol göz ardı edilebilmektedir. Bilişim varlıkları üzerinde yer alabilen bir açıklığın / zafiyetin kullanılması ya da kullanıcıların farkında olmadan yaptıkları hatalar sonrasında, içeriden veya dışarıdan yapılan saldırılarla, kurum için kritik olan değerli bilgilerin yetkisiz kişiler tarafından okunması ya da değiştirilmesi, kurumun fiziki ve sanal yapılarının zarar görmesi söz konusu olabilmektedir. Bu durumda da, kurumlar ciddi saygınlık kaybına uğramakta, mali kayıplar ve yasal yaptırımlar gibi tekrar yerine konulması güç sonuçlarla karşılaşabilmektedirler.

Bu çerçevede karşılaşılan sorunlara karşı, başta bilginin ve bilişim sistemlerinin güvenliğinin sağlanmasının önemi daha da artmakta, siber güvenlik ihtiyaçlarının değerlendirilmesi ve yönetilmesi daha da karmaşık hale gelerek zorlaşmaktadır. Özellikle kurumlarda tüm bu sorunların çözümü için, kurumlara ait bilgilerin, bilgi ve bilişim sistemlerinin ve alt yapılarının korunması, kayıpların en aza indirilmesi veya hiç yaşanmaması, yaşandığı takdirde kısa sürede önceki normal durumuna getirilmesi için sadece bilgi güvenliğinin değil, tam kapsamlı siber güvenliğin etkinlikle sağlanması için çeşitli kurallar ve yöntemler uygulanabilir.

Bu kural ve yöntemler, kurumun tehdit ve açıklarını analiz ederek, risklerinin ortaya konularak farkına varılmasından, güncel teknik güvenlik çözümlerin sistemle bütünleştirilmesine, anlaşma ve sözleşmelerde siber güvenliği de ele alan düzenlemelerin yapılmasından, kullanıcıların siber güvenlik konusunda bilinçlendirilerek farkındalıklarının arttırılmasına kadar çok çeşitli alanlarda uygulanabilir. Bu kurallardan ve yöntemlerden en önemlisi, kurumun siber güvenlik hedefini ve bu hedefe ulaşılması için uygulamaya konulacak kuralların, esasların ve prensiplerin çerçevesini çizen etkin kurumsal siber güvenlik strateji ve politikalarının oluşturulması ve kararlılıkla uygulanmasıdır.

Kurumsal siber güvenlik strateji ve politikaları, kurum yapısındaki bilişim kaynaklarının güvenli bir şekilde nasıl kullanılması gerektiğine yönelik bir plan ortaya koymakta ve kurumun siber güvenliğini tehdit eden durumların önüne geçilebilmesi için izlenmesi gereken kuralları ve esasları belirlemektedir. Kurumsal siber güvenlik yönetim sistemi karmaşık süreçlere sahip olduğundan, yaygın ve kabul görmüş bilgi güvenliği ölçünlerini (standartlarını) de esas alarak yapılandırılmalı ve yürütülmelidir.

5.2.1 Kurumsal siber güvenlik tanımı ve önemi

Siber güvenlik kişide başlar ve kişiler için siber güvenlik önemlidir, ancak bundan daha önemlisi ve önceliklisi, kişilerin güvenliğini doğrudan etkileyen çalışanı ve üyesi oldukları kurumların sadece bilgi güvenliği değil, bilgi güvenliğini de içine alan kurumsal siber güvenliktir. Toplumdaki her kişi, çalışan veya kullanıcı olarak, bilgi ve iletişim sistemleri üzerinden hizmet alırken veya verirken kurumsal bilişim sistem ve altyapılarını kullanmak durumundadır. Bu kapsamda sağlanan hizmetler kurumsal anlamda hizmet alımı, finans ve bankacılık işlemleri ya da bir kurum içerisinde kişisel işlemler vb. olabilir. Kuruma ait bilgi ve bilişim varlıklarının siber ortamda etkin korunması sağlanmadıkça, kişisel işlemlerin gerçekleştirilmesinde siber güvenlik te sağlanamaz.

Bilgiye devamlı olarak erişilebilirliğin sağlandığı bir ortamda, bilgiyi gönderenden alıcısı olana kadar gizliliği korunarak, herhangi bir değişikliğe uğramadan ve başkaları tarafından ele geçirilmesine engel olunarak bütünlüğünün sağlanması ve güvenli şekilde iletilmesi bilgi güvenliğiyle birlikte siber güvenlik sürecini meydana getirir. Kurumlar için bu süreci oluşturan 'Kurumsal Siber Güvenlik'; 'Kurumsal Bilgi Güvenliği' tanımından [139, 141] hareketle (kurumsal bilgi güvenliğini de kapsayacak şekilde), kurumların siber ortamda bulunan kritik bilgi ve bilişim varlıklarının tespit edilerek açıklıklarının belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması maksadıyla gerekli güvenlik inceleme ve analizlerinin yapılması, önlemlerin alınması ve sürdürülmesi şeklinde tanımlanabilir.

Öncelikle bu tanımda geçen bilgi ve bilişim varlıkları teriminin içerdiği anlam çok önemlidir. Bilgi ve bilişim varlıkları, kurumun sahip olduğu, kurumun işlerinin aksaksız yürütülebilmesi için önemli ve kritik değerde varlıklarını ifade etmektedir. Bu değerli varlıklar, çalışanların veya yöneticilerin masasının üzerinde veya çekmecelerinde bulunan kâğıtlarda ya da bilgisayarlarında veya sunucularında dosyalarda bulunan bilgiler yanında her türlü sanal verileri ve personel dâhil fiziksel oluşumları da içermektedir.

Bir kurum için siber güvenlik sadece Bilgi Teknolojisi ya da yaygın ifadeyle Bilişim Teknolojileri (BT) işi değildir; kurumun en üst yöneticisinden en alt çalışanına kadar bütün çalışanlarının katkılarını ve katılımlarını gerektirir. Bu durum kurum kültürü gerektirdiği için, öncelikle üst yönetimin kabul ve onayı, katılımının

sağlanması ve desteklenmesi şarttır. BT bölümünün teknik olarak gerekli olduğunu belirlediği ve uygulamaya koyduğu teknolojik güvenlik çözümleri, kurumun iş süreçleri ve politikalarıyla desteklenmemiş ve kabul görmemiş ise etkisiz kalacaklar ve beklenen verim sağlanamayacaktır.

Kurum personelinde gerekli inanç ve isteklendirme yaratılamamışsa, çalışanlar şifrelerini saklamakta özensiz, hassas bölgelerde gördükleri yetkisiz kişilere umursamaz, gerekli imha işlemlerini yapmadan çöpe atacakları bilgilerin önemi ve değeri konusunda dikkatsiz davranabilecek, güvenlik konusunda yatırımlara karşın büyük açıklar ve riskler oluşmasına sebep olmaya devam edebileceklerdir.

Bu açıklamalar doğrultusunda, Doğantimur'un bilgi güvenliği için sıraladığına [142] benzer şekilde, kurumsal siber güvenliğin sağlanmasının önemli gerekçeleri kısaca şöyle sırlanabilir;

- Konuyla ilgili tehdit ve risklerin belirlenerek etkin bir siber risk yönetiminin sağlanması ve kurumsal saygınlığın korunması,
- İş devamlılığının sağlanması,
- Bilgi kaynaklarına erişimin eksiksiz kontrol ve denetimi,
- Çalışanların ve iş ortaklarının güvenlik konusunda bilinç seviyesinin yükseltilmesi ve önemli güvenlik konularında bilgilendirilmelerinin sağlanması,
- Değerli bilgi varlıklarının gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması,
- Kurumsal bilgi ve bilişim varlıklarının kötü amaçlı olarak ve / veya kötüye kullanılmalarının engellenmesi,
- Bilgi ve iletişim sistemlerini kullanan kişilerin, umursamazlığından, bilinçsiz, yanlışlıkla veya görev ve yetkileri kötüye kullanma gibi nedenlerle oluşabilecek yazılım, donanım altyapısı veya bilgisayar ağlarında meydana gelebilecek arızalara karşı konulmasıdır.

Kişilerin ve kurumlarının siber güvenlik eksikliklerinin yanında saldırganların saldırı için ihtiyaç duydukları yazılımlara internet üzerinden kolaylıkla ulaşabilmeleri için yüksek eğitim seviyesine ve fazla bilgi birikimine ihtiyaç duyulmaması, kişisel ve kurumsal bilgi varlıklarına yapılan saldırılardaki artışlar, kişisel ve kurumsal siber güvenliğe daha fazla önem verilmesi, yeni yaklaşımların ve ölçünlerin kurumlarda titizlikle uygulanması zorunluluğunu ortaya çıkarmıştır

Kurumlar için önemli ve değerli bilgilerle bilgi ve iletişim sistemlerinin korunabilmesi, risklerin en düşük seviyeye indirilmesi ve iş devamlılığının sağlanması, Siber Güvenlik Yönetim Sistemi (SGYS)'nin kurumlarda üst yöneticiler dâhil bütün kurum personeli tarafından sahiplenilerek eksiksiz uygulanmasıyla mümkün olabilir.

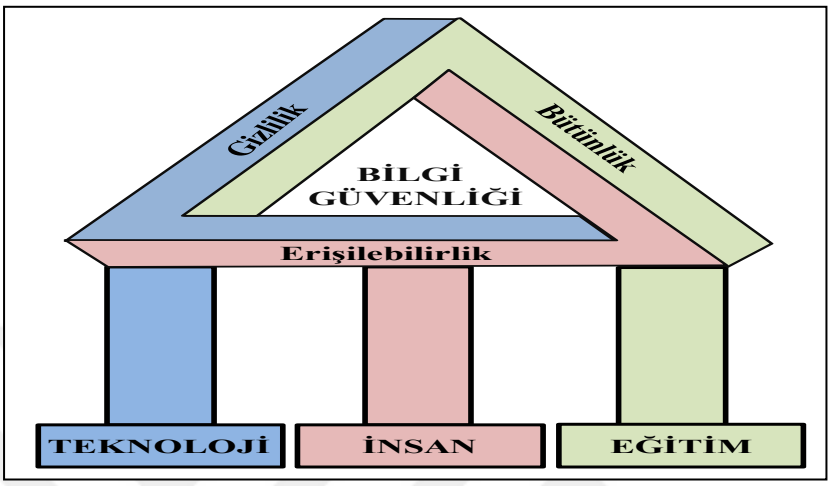
5.2.2 Siber güvenlik yönetim sistemi

Bilgi Güvenliği Yönetim Sistemi (BGYS) için "Bilgi güvenliğini sağlamak, planlamak, tasarlamak, gerçekleştirmek, işletmek, izlemek, denetlemek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası" [143] şeklinde yapılan tanımın, benzer şekilde Siber Güvenlik Yönetim Sistemi (SGYS) için de yapılması yanlış olmaz. Ancak sadece alınacak teknik tedbir ve önlemlerle (güvenlik duvarları, saldırı tespit ve önleme sistemleri, anti virüs yazılımları, şifreleme, vb.) siber güvenliğin sağlanması mümkün değildir. SGYS; insanları, süreçleri, siber ortamın sanal ve fiziki yapısını oluşturan bilgi ve iletişim sistemleri ile yazılım, donanım ve altyapılarını da içine alan ve üst yönetim tarafından da desteklenen bir sistemdir.

Kurumlar tarafından önemli bilgilerin ve bilişim sistemlerinin korunabilmesi, risklerin en aza indirilmesi ve iş sürekliliğinin sağlanması, SGYS'nin kurumlarda hayata geçirilerek uygulanmasıyla mümkün olur. SGYS'nin kurulması; ulusal siber güvenlik strateji ve politikalarıyla uyumlu, olası tehditlerin ve risklerin tespit edilmesi, siber güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü, uygun yöntemlerin geliştirilmesi, yönetimsel yapıların kurulması ve yazılım / donanım işlerliğinin sağlanması gibi bir dizi kontrol ve denetimin birbirini tamamlayacak şekilde gerçekleştirilmesi anlamına gelir.

Kurumsal siber güvenlik, kurumlar için siber güvenliğin sağlanmasında çalışanlar yani insan faktörü, başta eğitim ve farkındalık olmak üzere, teknoloji ve verim gibi birçok faktörün etki ettiği ve kurum içerisinde bir bütün olarak titizlikle yönetilmesi gereken iç içe geçmiş süreçlerden meydana gelir. Bu kapsamda, SGYS ile oluşturulacak kurumsal siber güvenlik tedbirleri kapsamında alınması gereken önlemlerin fiziki ve sanal ortamı da kapsayacak şekilde "İnsan odaklı Yönetimsel önlemler, Teknolojik önlemler ve Eğitim" şeklinde üç başlık altında toplanabilir.

Kurumsal siber güvenlik yönetim sisteminde başarı için, siber güvenliğin temel ilkeleriyle, kurum içerisinde bu üç unsuru oluşturan yönetim (insan), teknoloji ve eğitim yapısında birbirini tamamlayıcılık ve devamlılık olmalıdır. (Şekil 5.1) Bu esas prensibin, kurumun fiziksel ve sanal olarak bütün siber alanını kapsayacak şekilde sağlanamadığı kurumda etkin bir siber güvenlikten söz edilemez.



Şekil 5.1: SGYS için alınması gereken önlemler ve temel ilkeler.

- **Yönetimsel önlemler**

Yönetimsel önlemler kısaca, güvenlik yönetimi ile ilgili kuralların insan odaklı olarak ortaya konulması ve uygulanması şeklinde açıklanabilir. Kurumsal siber güvenliğin yönetiminde başarı için, iyi bir planlama, yönetim politikalarının doğru ve tutarlı bir şekilde belirlenmesi ve yazıya dökülerek kararlılıkla uygulanması gerekir.

Yalnız teknolojik önlemlerle (anti-virüs, güvenlik duvarı sistemleri, şifreleme, vb.) iş süreçlerinde siber güvenliğin sağlanması mümkün değildir. Kurumsal siber güvenlik, iş süreçlerinin bir parçası olmalı ve iş anlayışına göre yönetimsel ve kültürel sorun bakış açısıyla uygulanmalıdır. Devlet tarafından her seviyede eğitimde konu ele alınırken, kurumlar tarafından bir plan dâhilinde çalışanlarına yönelik olarak mutlaka kişisel ve kurumsal anlamda bir güvenlik politikası oluşturulmalı, bunun yazılı olarak çalışanlarına ve iş ortaklarına aktarılması sağlanmalıdır.

Bütün çalışanlar siber güvenlik konusunda bilinçlendirilmeli, bilgilerine sahip çıkmalı, üst yönetim tarafından yayımlanan 'Siber Güvenlik Politikası' siber güvenliğin önemini ortaya koymalı, yapılandırmayı sağlamalı, sorumlulukları belirlemeli, çalışanları bilgilendirmeli ve iş ortaklarını (müşteri, tedarikçi, taşeron, ortak firma vb.) da kapsamalıdır. Özellikle siber güvenlik yapılandırması konusunda,

bilgi, iletişim ve teknolojileri ile siber güvenliğin sağlanması faaliyet ve çalışmalarının yürütülmesi ve koordinasyonu için personel, birim, kurul ve benzeri güvenlik yönetimi yapılandırmaları mutlaka sağlanmalıdır. Bu konuda Kurum ve kuruluşlarda "İş Sağlığı ve Güvenliği Kanunu" [144] kapsamında 'İş Güvenliği Uzmanı' benzeri bir zorunluluk 'Siber Güvenlik Uzmanı' personel için de getirilmelidir.

Üst yönetimin desteklemediği kurumsal bir işi gerçekleştirmek zor olacağı için, üst yönetim ile güvenlik yönetimi arasında güçlü bir iletişim kurulmalı ve çift yönlü kusursuz bir bilgi akışı sağlanmalıdır. Bu şekilde, uygulanan güvenlik yönetim programı üst yönetimden yeterli desteği alır, üst yönetim de gerektiğinde uygun kararları kolaylıkla verir.

- **Teknolojik önlemler**

Siber güvenliğe ilişkin kurumsal bir politika oluşturmanın temel esaslarından birisi, bilgi ve iletişim teknolojilerinde yaşanan gelişmelerin bilinmesi ve kullanılan teknolojilerin sahiplenilmesidir. Bu nedenle, konuyla ilgili teknolojik gelişmelerin ne olduğunun ve hangi yönde olacağının doğru anlaşılması, ihtiyaçların içeriğinin doğru belirlenmesi, ihtiyaçlara uygun temin edilen teknolojilerin etkin kullanılmasının sağlanması çok önemlidir.

Kurumsal siber güvenliğin önemli bir kısmı sayısal ortamdaki bilgilerin saklanmasını içermektedir. Sayısal ortamdaki bilgilerin korunması için "Şifre bilimi (Kriptoloji), Güvenlik Duvarı (Firewall), Saldırı Tespit ve Önleme Sistemleri Kurulması, Yedekleme, vb." teknolojik önlemlerin alınması gerekmektedir [142].

- **Siber güvenlik eğitimi**

Siber güvenlik bilinci ve farkındalığı olmayan çalışanların güvenlik sürecini aksatacakları için siber güvenliğin sağlanmasında insan faktörüne gerekli önem verilmeli ve eğitimleri kesinlikle göz ardı edilmemelidir. Çünkü tarihte bilginin korunmasına başlandığı günden bu yana insanlar, güvenlik zincirinin en zayıf halkasını oluşturmuşlardır. Çok sayıda teknik ve yönetimsel güvenlik tedbiri alınsa bile, bu tedbirler saldırganlarca, özellikle çalışanların eksiklikleri, hataları ve yanlışlarından kaynaklanan açıklıklar kullanılarak, çeşitli teknik ve yöntemlerle kolaylıkla aşılabilmektedir. Bu nedenle, "Bir zincirin en zayıf halkası kadar güçlü

olduğu" söylemini siber güvenliğe uygulayarak "Güvenlik sadece en zayıf halka kadar iyidir" kavramını [145] unutmamak gerekir.

Tehditlerin çoğunun dış kaynaklı olduğu düşünülmesine karşın, yapılan araştırmalar siber tehditlerin çoğunun iç kaynaklı olduğunu, siber güvenlik ihlali olaylarının genellikle kurum çalışanları tarafından yapıldığını ve saldırıların %80'inine yakınının görevli personel tarafından gerçekleştirildiğini ortaya koymaktadır [146]. Bunların büyük bir kısmı bilgisayarına zararlı yazılım bulaşmış ama farkında bile olmayan vb. bilgisiz ve bilinçsiz kullanım ve davranışların sonucudur. Az da olsa çalışanların kötü niyet ve amaçlarla bilgiyi dışarıya sızdırması veya yok etmesi de söz konusu olmaktadır.

Yeterli bilinç, farkındalık ve eğitim seviyesine sahip olmayan kurum personeli ile kurumsal bilişim sistemleri üzerinde yetkili ama iyi niyetli olmayan yüksek önemde bilgiye sahip çalışanlar kurumsal siber güvenlik içerden tehdit oluşturan faktörlerdir. Bu nedenlerle çalışanların siber güvenlik konusunda eğitimleri şarttır. Siber güvenlik konusunda farkındalık ve bilinçlendirme sağlayacak bu eğitimler, kurumun yaşamsal işlevlerini yerine getirebilmesini sağlayan bilgilerin neden ve nasıl korunacağını öğretmeli, çalışanların hatalı davranışlarının kurumun siber güvenliği üzerinde yaratabileceği olumlu ya da olumsuz etkileri anlamalarını sağlamalıdır.

Kurumsal siber güvenlikte eğitimin ana hedefi, çalışanların siber güvenlik görev ve sorumlulukları konusunda bilinçlendirilmesi, güvenlik kontrollerinin önemi hakkında ortak bilinç ve farkındalık sağlanması olmalıdır. Kurumlarda siber güvenlik sadece bilgi işlem veya bilişim işi olarak algılanmakta, çalışanlar siber güvenliğin bilişimcilerin sorunu olduğuna inanmakta ve bu konuda kendi sorumlulukları olmadığını düşünmektedirler. Doğrusu ve olması gereken, siber güvenlik sadece bilgi teknolojileri ve bilgi işlem çalışanlarının değil bütün personelin sorumluluğudur. Teknolojinin çok hızlı ilerlediği günümüzde, bazen de yeni teknolojilerin eğitimden bağımsız olarak kullanıma alınması söz konusu olduğunda siber güvenlikte bir açıklık oluşması kaçınılmaz olmaktadır.

Bu görüşlerden ve düşüncelerden hareketle, siber güvenlik eğitimlerine gerekli önem ve öncelik verilerek bir defaya özgü bir çalışma olmadığı anlayışı yerleştirilmeli, çalışanların ihtiyaçları ve beklentileri doğrultusunda uygun programlar oluşturulmalı ve sürekliliği sağlanarak karalılıkla uygulanmalıdır. Bu süreçte unutulmaması gereken

konu, eğitimle ancak iyi niyetli ve bilinçsiz kullanıcıların sebep olabileceği siber güvenlik olaylarının önüne geçilebileceği, kötü niyetli ve amaçlı çalışanlara karşı güvenlik riskinin ise tamamen yok edilemese bile iyi planlanmış bir eğitim uygulamasıyla kabul edilebilir alt seviyelere indirilmesinin sağlanabileceğidir.

5.2.3 Kurumsal siber güvenlik politikası oluşturulması

Kurumsal siber güvenlik strateji ve politikaları, bilgi güvenliği strateji ve politikalarını da kapsayacak şekilde, bir kurumun değerli bilgilerinin yönetimini, korunmasını, dağıtımını ve önemli işlevlerinin yerine getirilmesini düzenleyen planlamalar, kurallar ve uygulamaların bütünüdür [139]. Bu çerçevede, kurum veya kuruluşlarda kabul edilebilir güvenlik seviyesinin tanımlanmasını sağlayan, bütün çalışanların ve iş ortamlarının uyması gereken kuralları kapsayan ve yönlendiren, esas ve prensipleri açıklayan talimatlar olup kurumsal bilgi kaynaklarına erişim yetkisi olan çalışanların uymaları gereken kuralları ve uygulamaları içeren resmi belge özelliğindedir [141].

Bu kural ve uygulamaları tanımlayan politikalar kurum ve kuruluşlar içerisinde çeşitli seviyelerde hazırlanabilir. Politikalar, genel bir siber güvenlik politikası ve belirli alanlara ait politikalardan (Parola politikası, Erişim kontrol politikası, Uzaktan erişim politikası, Kullanıcı politikası, E-posta kullanım politikası, Sunucu Güvenlik Politikası, Yedekleme politikası, Bakım ve onarım politikası, vb.) oluşur ve uygulamaları tanımlayan yordam (kılavuz) ve talimatlarla tamamlanır. Diğer bir ifadeyle, belli konularda çalışanların daha fazla bilgilendirilmesi, dikkat etmeleri gereken hususlarla ilgili konuların ayrıntılı olarak açıklanması istendiğinde alt politikalar geliştirilmesi gerekir.

Örneğin kullanıcı hesaplarının oluşturulması ve yönetilmesi, şifre / parola unutulması, şifrelerin yeniden tanımlanması veya değiştirilmesi gibi durumlarda uyulacak kurallar, kurumsal e-posta gönderme ve alma konusunda üst yönetimin kararları, hakları, kullanıcının sorumlulukları, uyması gereken kuralları vb. kurallar alt politikalar içerisinde açıklanabilir.

Her seviyedeki politikanın tek bir belgede bulunması yerine, en üst seviyede temel ilkeleri, esas ve prensipleri içeren bir Siber Güvenlik Politikası Belgesi'nin oluşturulması ve bu belgeyle diğer ayrıntılı alt politikaların bağlantılandırılması uygun

olur. Kurumsal siber güvenlik politikası, bu alt politikalar doğrultusunda uygulanacak yordamları ve amaçlarını tanımlayan en üst düzey genel belge olarak kullanılır.

Kurumsal siber güvenlik politikaları, kurum ve kuruluşların görevleri ve ihtiyaçları doğrultusunda bilginin korunmasıyla ilgili temel güvenlik ilkelerinin (gizlilik, bütünlük ve erişilebilirlik) bazıları üzerinde ve farklı önem ve önceliklerle yoğunlaşabilir. Örneğin askeri kurumlarda, siber güvenlik politikalarında genellikle öncelikli olarak gizlilik ve bütünlük konusunda kötü niyetli ve amaçlı kullanımların önlenmesi ele alınmaktadır. Erişilebilirlik ise ikinci planda gelir.

5.2.4 Kurumsal siber güvenlik politikaları yaşam döngüsü

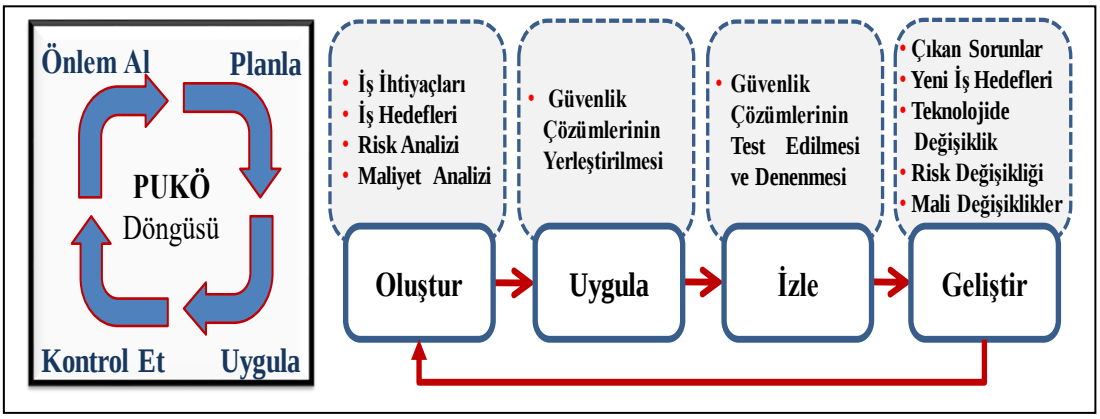
Kurumsal siber güvenlik politikaları, kurumun üst düzey yönetimi ve yöneticilerince desteklenmeli ve bütün çalışanları tarafından benimsenmeli, uygulanabilir, kullanıcılar tarafından anlaşılır, yapılabilir ve ilgili yöneticileri tarafından kolaylıkla yönetilebilir olmalıdır. Siber güvenlik politikaları her kurum ve kuruluş için farklılık gösterse de, genel olarak çalışanların sorumluluklarını, kontrol ve denetim yapılarını, amaç ve hedefleri içeren genel açıklamalardan oluşur.

Teknolojinin gelişmesine paralel olarak her gün yeni tehditlerin ve risklerin ortaya çıkmasıyla, daha önce güvenli olarak kabul edilen bilişim sistemleri güvensiz hale gelebilmektedir. Bu nedenle, kurumlar tarafından SGYS siber ortamda güvenli yaşam süreci olarak ele alınmalı ve BGYS için olduğu gibi, günümüzde uygulamalarda onun yerini alan SGYS için de, "Planla - Uygula - Kontrol Et - Önlem Al (PUKÖ / PDCA - *Plan, Do, Check, Act)* döngüsü [147, 148] benimsenmelidir. Politikalar kurumlara özgü özel kanunlar olarak da düşünülmekle birlikte, her kurum içinde genel olarak politikaların oluşturulması, uygulanması, izlenmesi ve geliştirilmesi aşamalarını izleyen bir süreç işletilmelidir [149]. PUKÖ döngüsüne benzer bir bakış açısıyla düşünülen SGYS döngüsü süreci Şekil 5.2'de görülmektedir.

SGYS süreçlerine uygulanabilecek PUKÖ modeli aşamaları şu şekilde özetlenebilir

- **Planla;** Kurumun SGYS politikası, amaçları, hedefleri, süreçleri ve yordamları oluşturulur.
- **Uygula;** SGYS politikası, iş süreç ve yöntemleri gerçekleştirilerek işletilir.
- **Kontrol et;** SGYS politikasını amaçları ve kullanım deneyimlerine göre iş süreci verimi ölçülür ve sonuçların değerlendirilmek üzere yönetime rapor edilir.

- **Önlem al**; Yönetimin değerlendirme sonuçlarına göre düzeltici ve önleyici çalışmalar gerçekleştirilerek SGYS'nin devamlılığı ve iyileştirilmesi sağlanır.



Şekil 5.2: PUKÖ ve SGYS döngüsü [147, 149].

- İyi bir kurumsal siber güvenlik politikasının sahip olması gereken asgari özellikler aşağıda sıralanmıştır [143]**;**

- Politika metni çok uzun olmamalı, açık ve basit olmalıdır.
- Özel ve teknik tanımlamalar içermemeli, dili kolay anlaşılabilmelidir.
- Politika ve yordam kavramları birbirinden kolay ayırılabilmelidir.
- Kullanıcıların gerektiğinde sorularını sorabilecekleri güncel iletişim bilgileri yer almalıdır.
- Güvenlik hedefleri açık şekilde belirtilmeli ve metin maddeler ile açıklanmalıdır.
- Politika belgesine, kurumun bütün çalışanları kolaylıkla erişilebilmelidir.
- Politikada, bütün kurum çalışanlarının siber güvenlik görev ve sorumluluklarına yer verilmelidir.
- Politikaya uygun hareket edilmeyen durumlarda ne yapılacağı açıklanmalı ve politikada yer almayan konularda kurumun hareket tarzı açıklanmalıdır.

5.2.5 Kurumsal siber güvenlik politikaları bileşenleri

Kurumsal siber güvenlik politikası, kurumun siber güvenlik ihtiyacının ve siber güvenlik kavramının kurumun bilgi varlıklarını kullanan her personele anlatılması amacıyla hazırlanır. Kurumdaki siber güvenlik ihtiyacı, kurumun yaptığı işlerin gerekliliği olarak ortaya çıkmış veya ilgili yasalar ve düzenlemelerle belirlenmiş olabilir. Bu iş gereklilikleri ve varsa yasal zorunluluklar bu politika belgesinde açıkça ortaya konulmalıdır.

Kurumsal siber güvenlik politikası, kurum yönetiminin siber güvenliğe yönelik yaklaşımını, sözünü, desteğini gösterir ve siber güvenliğin kurumun belirlemiş olduğu amacına ulaşabilmesi için önemini ve destekleyici yönünü tanımlar.

Siber güvenlik politikası ile ilgili ISO/IEC 27001 Ölçünü esaslarına [150] ve Bilgi Güvenliği Politikası Oluşturma Kılavuzu'na göre bir Siber Güvenlik Politikasında en azından aşağıdaki hususlar yer almalıdır [151].

- Siber güvenliğin tanımı, kapsamı ve hedefi,
- Siber güvenliğin kurum için önemi, amacı ve ilkeleri, bu amaç ve ilkeler için yönetimin desteği,
- Kontrol ve denetim hedefleri, kontrollerin seçimi için risk değerlendirmesi ve yönetimi,
- Güvenlik politikaları, ilkeleri, ölçünleri ve uyum gereksinimleri,
- Siber güvenlik ile ilgili bütün görev ve sorumluluklar,
- Diğer kurumsal politikalar ve bilgi sistemleri için yordamlar veya kullanıcıların uyması gereken kuralları destekleyen belgeler.

Konuyla ilgili diğer bir yaklaşıma göre politikalar; tehdit ve risklerin tanımlandığı, değerli bilgi varlıklarının ve sorumluların belirlendiği, yapılması ve uyulması gereken kuralların, kuralların yerine getirilmemesi durumunda uygulanacak cezalandırma yaptırımları ile teknik terimlerin açıklamalarının ve yapılan değişiklik / düzeltme çizelgelerinin yer aldığı 7 bölümden oluşmaktadır [141].

Açıklanan esaslar ve prensipler doğrultusunda, Kurumsal Siber Güvenlik Politikasını oluşturan ve yaygın kabul gören bölümler kısa başlıklar halinde aşağıda sıralanmıştır.

- Genel açıklama,
- Amaç,
- Kapsam,
- Politika,
- Cezai yaptırımlar,
- Tanımlar,
- Düzeltme tarihçesi.

Türkiye'de kurumsal siber güvenlik politikaları genellikle TS ISO/IEC 27000, COBIT vb. ölçünlere uygun olmadan, yazılı veya sözlü, onaylı veya onaysız bir biçimde kuruluşlar tarafından uygulanmakta ve çoğu kurum tarafından ise sadece 'Siber Güvenlik Yönetimi' yeterli görülmektedir. Bu ve benzeri yanlış anlamaların giderilmesi için dünya genelinde kabul görmüş ve uygulanabilirliği denenmiş siber güvenlik ölçünleri esas alınarak kuruluşların, siber güvenlik yönetimi konusunda eksikliklerini gidererek SGYS kurmaları, uygulamaları ve belgelendirmeleri gerekmektedir.

Bu kapsamda, son yıllarda özellikle bilgi ve bilgisayar güvenliğini zayıflatan, hatta ortadan kaldırmaya çalışan, kurumlar üzerinde maddi ve manevi büyük zararlara yol açan, kişi, kurum ve kuruluşları tehdit ederek zararlara uğramasına yol açan siber güvenlik tehditlerinin önlenmesi için kurumsal siber güvenlik mutlaka sağlanmalıdır.

SGYS çerçevesinde oluşturulacak kurumsal siber güvenlik politikalarına, üst yönetim ve tüm çalışanların destek vermesi ve kararlı bir şekilde uygulanması, iş birliğinde bulunulan tüm kişi ve kuruluşların da bu politikalara uyma zorunluluğu, kurumsal siber güvenliğinin üst düzeyde sağlanmasında önemli bir faktördür.

Kurumsal siber güvenliğin sağlanması amacıyla, siber saldırıların takip edilmesi, saldırganların kullandığı yöntemlerin saptanması, Türkiye'de ve dünyada bu konuda yapılan araştırmaların, raporların ve çalışmalar ile tespit edilen açıkların takip edilmesi ve giderilmesi, siber güvenlik ihlalinin yaşanmaması için gerekli önlemlerin zamanında alınması, güvenlik ihlallerine anında müdahale edilerek saldırıların zararlarından en az şekilde etkilenme, felaket anında uygulanabilecek felaket ve iş sürekliliği planlarının uygulanması gibi stratejiler, kurumlar tarafından gecikmeksizin uygulamaya konulmalıdır.

Bunun ötesinde de; yeni eğilim ve yaklaşımların keşfedildikçe kurumsal güvenliğinin arttırılması yönünde sahiplenilerek hayata geçirilmesi gerektiği ve Kurumsal Siber Güvenlik Strateji ve Politikalarında başarının, Ulusal Siber Güvenlik Strateji ve Politikalarında başarıyı olumlu yönde etkileyen en önemli unsurlardan birisi olduğu ve bir kuvvet çarpanı etkisi yaratacağı asla unutulmamalıdır. Çünkü siber güvenlikte kurumların başarısı ülkenin ulusal siber güvenlikte başarısını getirecektir.

5.3 Ulusal Siber Güvenlik Strateji ve Politikaları

Ülkelerin ulusal siber güvenlik strateji ve politikaları genel anlamda ve kısaca; "Devletin milli varlığına, bekasına ve güvenliğine yönelik tehditlere karşı tedbirler almak için bölgesel ve küresel ortamın izlenerek tehdit ve fırsatların tespit edilmesi ile bu hususlara uygun siyasetin belirlenmesini ve en uygun politikaların uygulanmasını sağlayacak süreç ve unsurlar" [152] şeklinde tanımlanmaktadır.

Ülkeler, ulusal güvenlik strateji ve politikalarını oluşturdukları gibi, siber güvenlik strateji ve politikalarını da oluşturmakta ve uygulamaktadırlar. Bu strateji ve politikalarda temel ve ortak amaç, ülkelerin siber uzaydaki değerli varlıklarının, bilişim sistemlerinin ve altyapılarının siber tehditlere ve saldırılara karşı güvenliğinin yani savunmasının sağlanmasıdır.

Güvenliğin anlam ve tanımında da olduğu gibi siber güvenlik strateji belgelerinde, siber ortamda karşılaşılacak kötülük ve saldırılara karşı eksiklikleri, olumsuzları ve yetersizlikleri, tehditlere ve risklere karşı tedbirleri içeren sorumlukların ortaya konması, koordinasyon ve işbirliği esaslarının belirlenerek yönetilmesi kapsamlı emniyet ve savunmayla ilgili hususların yer alması gerekmektedir.

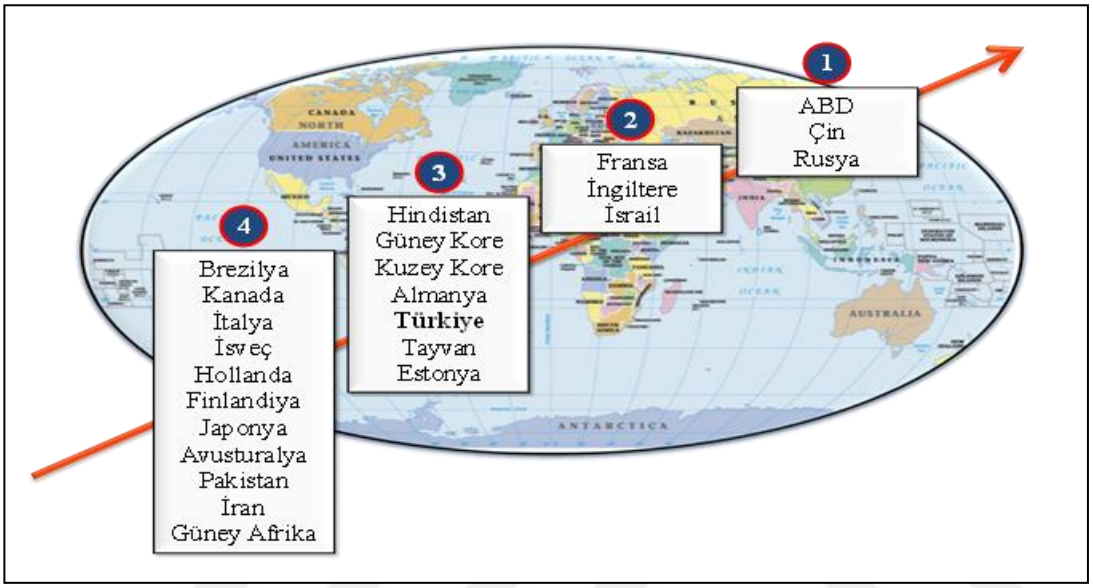
Ulusal stratejinin tanımlamasında ki, ulusal politikalar için bütün güç unsurlarının birlikte kullanılması esasından hareket edilmesine benzer şekilde, bir ülkenin sahip olduğu siber gücün oluşturulması, geliştirilmesi, etkinlikle korunması ve kullanılmasının sağlanması esas alınarak geniş kapsamlı strateji ve politikaların oluşturulmasının uygun olacağı ortaya çıkmaktadır. Bu kapsamda dünyada ulusal siber güvenlik ve politikaları yaklaşımları ile siber uzayda ön planda olan bazı ülkelerin siber güvenlik strateji ve politikaları incelenerek tespit edilen esas ve prensipler ortaya konmaya çalışılmıştır.

5.4 Dünyadan Siber Güvenlik Strateji ve Politikaları Örnekleri

Dünyada ülkeler ulusal çıkarlarını sağlamak ve ulusal hedeflerini elde etmek için kullanabileceği insan gücü, coğrafi güç, ekonomik güç, politik ve idari güç, psiko sosyal güç, bilimsel ve teknolojik güç ile askeri güçlerinden oluşan ulusal güçlerine siber gücü de dâhil ederek bu konuda strateji ve politikalarını her geçen gün daha da geliştirmeye ve güçlendirmeye devam etmektedirler. Ülkelerin siber güçlerini ölçmek

için açık ve somut yol ve yöntemler olmasa da bu konuda çeşitli çalışmaların yapıldığı ve bazı tespitlerin ortaya konulduğu görülmektedir.

Bu konuda çalışmalardan birisi Dennesen tarafından iDefense 2011 Trends Report'tan da alıntı yapılarak ortaya konmuştur [153]. Çalışmada siber güvenlik strateji ve politikaları da dikkate alınarak siber güç ve yeteneklerine göre ülkeler Şekil 5.3'te gösterildiği gibi 4 grupta incelenmiş ve belirgin özellikleri yorumlanmıştır.



Şekil 5.3: Ülkelerin siber güç ve yeteneklerine göre gruplanması [153].

- **1'inci grup ülkeler (ABD, Çin ve Rusya);**

- Siber güvenlik / savunma geliştirme çabaları üzerine uluslararası politika uygulama yeteneğine sahip,
- Siber güvenlik politikaları ve siber savunma çalışmalarına en fazla kaynak ve insan desteği sağlayan,
- Çok sayıda iyi tanımlanmış ve uzmanlaşmış askeri ve istihbari kurumlara sahip,
- Diğer ülkelere karşı kapsamlı, devamlı ve karmaşık saldırı ve savunma eylemleri uygulama yeteneği olan ülkelerdir.

- **2'nci grup ülkeler (Fransa, İngiltere ve İsrail);**

- Birinci gruptaki ülkeleri yakından izleyen ve daha az personel ve daha sınırlı altyapıya sahip,
- Çok sayıda, iyi tanımlanmış ve uzmanlaşmış askeri ve istihbari kurumları olan ancak daha az kaynak sağlayan,

- Sınırlı sayıda ülkelere karşı kısıtlı miktarda, sürekli ve karmaşık saldırı ve savunma eylemleri uygulama yeteneği olan ülkelerdir.

- **3'üncü grup ülkeler (Hindistan, Güney Kore, Kuzey Kore, Almanya, Türkiye, Tayvan ve Estonya);**

- Siber güvenlik politikaları ve savunma yeteneklerinin geliştirilmesi için önemli ölçüde kaynak ayıran,
- Birçok durumda birinci ve ikinci gruptaki ülkeleri taklit eden,
- Birkaç iyi tanımlanmış kuruma sahip fakat kurumsallaşmanın yeterli olmadığı,
- Siber savunma yetenekleri kapsamlı ve devamlı olan fakat siber saldırı yetenekleri zayıf olan ülkelerdir.

- **4'üncü grup ülkeler (Brezilya, Kanada, İtalya, İsveç, Hollanda, Finlandiya, Japonya, Avusturalya, Pakistan, İran, Güney Afrika);**

- Siber güvenlik politikaları ve savunma yetenekleri geliştirilmesi için kısıtlı kaynak ayıran,
- Az sayıda ve geliştirilmesi gereken kuruma sahip,
- Siber savunması güçlü ama yetersiz, siber saldırı faaliyetleri kısıtlı olan,
- Kendi iç kaynaklarını korumaya odaklanmış olan ülkelerdir.

Ülkelerin, siber güçleri ile siber güvenlik strateji ve politikaları açısından değerlendirilmesi konusunda önemli diğer bir çalışma Uluslararası Telekomünikasyon Birliği (ITU) tarafından yapılmıştır. ITU siber güvenlik alanındaki uluslararası çok paydaşlı işbirliği çerçevesinde ülkeler için mevcut ve gelecekteki girişimler arasında bir görevdeşlik kurmayı amaçlayarak aşağıdaki beş ana esası önemsemiştir [7].

- **Yasal:** Siber güvenlik ve siber suçla ilgili yasal kurumların ve çerçevelerin varlığına dayanan önlemler.

- **Teknik:** Teknik kurumların varlığına ve siber güvenlik ile ilgili çerçeveye dayalı önlemler.

- **Yapısal:** Koordinasyon kurumlarının varlığına ve ulusal düzeyde siber güvenlik geliştirme stratejilerine ve politikalarına dayanan önlemler.

- **Kapasite geliştirme:** Araştırma ve geliştirme, eğitim ve öğretim programları, sertifikalı uzmanlar ve kapasite geliştirmeyi destekleyen kamu sektörü kuruluşlarının varlığına dayalı önlemler.

- **İşbirliği:** Ortaklıklar, işbirlikçi oluşumlar ve bilgi paylaşım ağlarının varlığına dayalı önlemler.

ITU tarafından yapılan araştırma sonucunda ülkeler bu esaslar doğrultusunda değerlendirilerek sıralanmıştır. Dünya değerlendirmesinde ilk onda sırasıyla İngiltere, ABD, Fransa, Litvanya, Estonya, Singapur, İspanya, Malezya, Kanada ve Norveç ile Avusturya'nın yer aldığı görülen listede, bölgesi Avrupa'da 11'inci sıradaki Türkiye dünyada 20'nci sırada yer almaktadır (Çizelge 5.1) [154].

Çizelge 5.1: ITU - Siber güvenlik alanında ülkelerin derecelendirmesi [154].

Ülke	Puanı	Bölge Sıra	Dünya Sıra	Ülke	Puanı	Bölge Sıra	Dünya Sıra
İngiltere	0.931	1.	1.	Güney Kore	0.873	5.	15.
ABD	0.926	1.	2.	Umman	0.868	2.	16.
Fransa	0.918	2.	3.	Katar	0.860	3.	17.
Litvanya	0.908	3.	4.	Gürcistan	0.857	9.	18.
Estonya	0.905	4.	5.	Finlandiya	0.856	10.	19.
Singapur	0.898	1.	6.	**Türkiye**	**0.853**	**11.**	**20.**
İspanya	0.896	5.	7.	Danimarka	0.852	12.	21.
Malezya	0.893	8.	8.	Almanya	0.849	13.	22.
Kanada,	0.892	2.	9.	Mısır	0.842	4.	23.
Norveç	0.892	6.	9.	Hırvatistan	0.840	14.	24.
Avusturalya	0.890	3.	10	İtalya	0.837	15.	25.
Lüksemburg	0.886	7.	11.	Rusya	0.836	1.	26.
Hollanda	0.885	8.	12.	Çin	0.828	6.	27.
Sudi Arabistan	0.881	1.	13.	Avusturya	0.826	16.	28.

Dennesesn ve ITU tarafından yapılan bu iki ayrı çalışma arasında, zamansal olarak 10 yıla yakın bir süre olmakla birlikte ülkelerin değerlendirme ölçekleri ve bazı ülkelerin değerlendirme sonuçları benzerlikler taşımaktadır. Bu değerlendirme sonuçlarından da hareketle sırasıyla Amerika Birleşik Devletleri (ABD), Çin, Rusya Federasyonu (RF), Fransa, İngiltere, İsrail'in siber güvenlik strateji ve politikaları ayrıntılı olarak incelenmiştir.

5.4.1 Amerika Birleşik Devletleri siber güvenlik stratejisi

Dünya genelinde ulusal siber güvenlik stratejileri ve politikalarının oluşturulması ve geliştirilmesi çalışmaları ABD'nin öncülüğünde olmuştur. ABD'de siber ortama yönelik olası tehdit ve tehlikelere karşı konulması ve güvenliğin sağlanmasına yönelik çalışmaların 1960'lı yıllarda başladığı ve 1990'lı yıllardan sonra da hız kazandığı görülmektedir.

ABD Savunma Bakanlığınca 1967 yılında bilgisayarların açıklıklarını incelemek için 'Savunma Bilim Kurulu Bilgisayar Güvenliği Görev Kuvveti' adı altında bir birim

kurulmuş, bu birim 1970 yılında askeri sistemlerdeki gizli bilgilerin korunmasına ilişkin bulgularını ve önerilerini içeren bir rapor yayımlamıştır. 1990'da Ulusal Araştırma Konseyi "Amerika'nın giderek daha fazla bilgisayara bağımlı olmaya başladığını, yarının teröristinin bir klavyeyle bombaya kıyasla daha fazla zarar verebileceğini, bu nedenle güvenli ve güvenilir bilgisayar sistemleri kurulmasının gerektiğini..." belirten bir rapor yayımlanmıştır.

1997 yılında Beyaz Saray'a sunulan diğer bir raporda ise "Bugün, İnternete yapılacak sürekli bir saldırının ABD'de kritik altyapılar üzerinde ciddi bir etkiye sahip olabileceği, bu saldırılara direnilebilmesi ve İnternetin kritik işlevleri yerine getirmeye devam edebilmesi için şimdiden gerekli adımların atılmasının şart olduğu…." [155] belirtilmiştir.

ABD'nin Ulusal siber güvenlik konusundaki mevcut belgelerinin çoğunda öncelikler ve yapı bakımından farklılıklara yol açan hususlar bulunmakta, diğer politika belgelerine nasıl bağlanılacağını veya uyum sağlanacağının belirlenemediği ve siber güvenlik alanlarından daha dar olarak ulusal önceliklerin ele alındığı görülmektedir [156].

ABD'de geçmişten günümüze siber güvenliğin sağlanmasına yönelik, Başkanların yürütme emirleri de dâhil, yapılan idari ve yasal düzenlemelerin her biri çeşitli faaliyetlere yönelik olup temel amaçları;

- Ulusal kritik altyapıların korunması,
- Devletin bilgisayar sistemlerinin ve ağlarının güvenliğin sağlanması,
- Kamu / Özel sektör için görevlerin, sorumlulukların belirlenmesi ve işbirliğinin geliştirilmesi,
- Ulusal ve uluslararası güvenlik, savunma ve karşı istihbarat konularındaki siber güvenlik birimlerinin faaliyetleri şeklinde sıralanmaktadır.

Bu çerçevede belgeler genel olarak üç ana bölümde gruplanmaktadır.

- Kamu ağlarının siber güvenlik özelliklerini düzenleyen belgeler,
- Kritik altyapıların korumasına ilişkin belgeler,
- Ulusal güvenlik ve savunma kapsamında siber güvenlik unsurlarına ilişkin askeri belgeler.

ABD'nin ulusal siber güvenlik stratejileri ve politikaları kapsamında geçmişten bugüne önemli belgeleri ve kısaca içerikleri aşağıda sunulmuştur.

- **Siber Uzay Güvenliği İçin Ulusal Strateji (2003)** [157]

Siber uzayın güvenliğini sağlamak maksadıyla üç ulusal stratejik hedef belirlenmiştir:

- Ulusal kritik altyapılara karşı siber saldırıların önlenmesi,
- Siber saldırılara karşı ulusal duyarlılığın azaltılarak dayanıklılığının artırılması,
- Meydana gelen siber saldırılardan kaynaklanan hasarı ve hasarı giderme süresini en aza indirilmesi.

Bu hedeflere ulaşmak için ise beş ulusal öncelik belirlenmiştir:

- Federal bilgisayar sistemlerini ve ağlarını güvence altına almak,
- Bir karşı koyma sistemi geliştirmek,
- Bir güvenlik açığı ve tehdit azaltma programı oluşturmak,
- Siber güvenlik için bir farkındalık ve eğitim programı başlatmak,
- Uluslararası bir işbirliği sisteminin geliştirilmek.

- **Kapsamlı Ulusal Siber Güvenlik Girişimi (2008)** [156, 158]

Siber güvenlik çalışmalarının halkın anlamasını ve kavramasını artırmak ve çalışmaların koordinasyonunu sağlamak amacıyla, özellikle gelişmiş bilgi paylaşımı, Amerikan halkının mahremiyeti ve medeni özgürlüklerinin korunması konularında hükümler ortaya konmuştur. Girişimle ilgili olarak 2008 yılında gizlilik dereceli olarak hazırlanan kararlar 2010 yılında kamuya açıklanmıştır.

ABD'yi siber alanda güvenceye almak için hazırlanan girişimin üç ana hedefi bulunmaktadır.

- Ağ girişlerine karşı bir ön savunma hattı oluşturarak güvenlik açıklarını azaltmak, tehditler ve olaylarla ilgili durumsal farkındalığı artırmak ve izinsiz girişleri önlemek için hızlı hareket etme yeteneği kazanmak,

- ABD'deki karşı istihbarat yeteneklerini ve temel bilgi teknolojileri için tedarik zincirinin güvenliğini artırarak her türlü tehdide karşı savunma yapmak,

- Siber eğitimi genişleterek, araştırma ve geliştirme çabalarını koordine ederek ve yönlendirerek, siber uzayda düşmanca veya kötü niyetli faaliyetleri engellemek için stratejiler tanımlayıp geliştirerek gelecekteki siber güvenlik ortamını güçlendirmek.

Konuyla ilgili olarak daha sonraki çalışmalara yön veren bu girişimle; Ar-Ge çabalarının koordine edilmesi ve yönlendirilmesi, mevcut siber operasyon merkezlerinin birbirine bağlanması, devlet çapında bir siber karşı istihbarat planı geliştirilmesi ve uygulanması, kritik altyapılarının siber güvenliğinin sağlanmasında devletin rolünün belirlenmesi, siber güvenlik kapsamında kalıcı caydırma stratejilerinin tanımlanması ve geliştirilmesi konuları başta olmak üzere 12 ana karar uygulamaya konulmuştur.

- **Siber Uzay Politikaları İncelemesi (2009)** [159]

ABD Başkanı tarafından verilen bir direktifle, uzman bir ekip tarafından siber güvenlik politikaları ve yapılanmaları incelenerek geleceğe yönelik sağlam, güvenli ve güvenilir bir siber uzayın nasıl oluşturulması gerektiği konusunda görüş ve öneriler ortaya konmuştur.

Ülkenin sayısal altyapısının ve büyük ölçüde internete dayanan mimarisinin güvenli ve esnek olmadığı, ülkenin artan siber suçlar, devlet destekli saldırı ve operasyon tehditlerinden korunabileceğinin şüpheli olduğu, bunun ekonomik ve ulusal güvenlik çıkarların bilgi sistemlerine duyduğu güveni zedelediği belirtilmekte, olumsuzluklar yetersizlikler ve ihmaller açıklanarak alınması gereken tedbirler kapsamında özetle;

- Siber güvenliği geniş kapsamlı ele alan uygun örgütlenme ve planlama yapılmasının,

- Siber güvenlikle ilgili risklerin azaltılması için gereken politikaların, süreçlerin ve teknolojinin geliştirilmesinin,

- Tehdit ve risklere karşı etkin bir mücadele için siber güvenlik konusunda ulusal birliktelik sağlanmasının,

- Bilişim ağlarının ulusal ve uluslararası özelliği nedeniyle başta ağ güvenliği olmak üzere siber güvenliğin kamu ve özel ortaklık yanında uluslararası işbirliğinin,

- Bilgi ve iletişim altyapılarında güvenlik ve esnekliğe ulaşmak için yeni yaklaşımların geliştirilmesinin, ekonomik ve ulusal güvenlik gereksinimleri karşılanırken siber güvenlik açıklarını gidermeye yardımcı olacak araştırmalara yatırım yapılmasının kaçınılmaz olduğu belirtilmiştir.

- **Siber Uzay İçin Uluslararası Strateji (2011)** [48]

Siber güvenlik ABD'nin en ciddi ekonomik ve ulusal güvenlik mesellerinden birisi olarak tanımlanırken, güvenliğin artırılması, ekonomik faaliyetler için uygun bir ortamın sağlanması ve kullanıcıların özgürlüğünün korunması gibi temel esaslarla internet ile ilgili stratejilerin belirtildiği belgede; Beyaz Saray'ın siber uzayda başarmayı hedeflediği amaçlar 4 ana başlıkta toplanmıştır.

- Siber uzay politikasının oluşturulması: Zorlukların tanımlaması ve prensiplere dayanma esaslarını ortaya koyan bir stratejik yaklaşım benimsenmiştir.

- Siber uzayın geleceği: Açık, birlikte çalışılabilir, güvenli, kalıcı ve kararlı bir şekilde kuralların uygulandığı, diplomaside ortaklıkları güçlendirecek bir siber uzay hedeflenmiştir.

Savunmada vaz geçirme ve caydırıcılık esas alınacaktır. Ulusal ve ekonomik güvenliği tehdit edecek suçlular ve diğer devlet dışı aktörler söz konusu olduğunda, ülke içi caydırıcılık, tüm devletlerin, yurtiçinde veya yurtdışında ağlara yönelik saldırıda bulunanların soruşturulmasına, yakalanmasına ve kovuşturulmasına izin veren süreçlere sahip olunması gerekir. Ülkeye karşı diğer tehditlerde olduğu gibi, siber uzayda düşmanca eylemlerin tehdit oluşturması durumunda karşılık verilecektir. Bu kapsamda, Ulusu, müttefikleri ve askeri anlaşmalara dayanan ortakları savunmak için gerekli tüm uygun yöntemleri (diplomatik, bilgi amaçlı, askeri ve ekonomik) uluslararası hukuka uygun olarak kullanma hakkı saklı tutulmuştur. Bunu yaparken eylemsizlik maliyetlerine karşı eylem maliyetleri ve riskleri dikkatlice tartılacak, askeri güçten önce tüm seçenekler tüketilecek, mümkün olduğunca geniş uluslararası destek ve haklılığı güçlendirecek şekilde hareket edilecektir.

- Politika öncelikleri: Ekonomi ağlarını korunması, yasaların uygulanması, askerlik, internet yönetişimi, uluslararası gelişme ve internet özgürlüğü şeklinde sıralanmıştır.

- Geleceğe yönelik adımlar: Ağ teknolojisinin yararları, ağ bağlantıları konusunda dünya üzerinde birlikte çalışılması, yeniliklere açık olunması, insanların güvenini kazanacak ve işlerini destekleyecek kadar güvenilir bir siber alanın oluşturulmasının desteklenmesi vurgulanmıştır.

- **Savunma Bakanlığı Siber Uzayda Harekât Stratejisi (2011)** [160]

Siber alanda güvenli ve etkin çalışması gereken ABD kritik altyapı sistemlerinin bozulmaya veya istismara maruz kalabilecek bilgi teknolojilerine dayandığı, binlerce ağ ve bilgisayar sistemleriyle ABD Savunma Bakanlığı askeri istihbarat, personel, lojistik ve harekât faaliyetleri için komuta kontrol sistemlerinin kullanıldığı siber uzayın öneminin her geçen gün daha da arttığı vurgulanmaktadır. Bakanlığın ve ulusun siber alanda hem dışardan hem de içerden gelen, ülkeler, terörist gruplar ve siber korsanlar tarafından yapılan ve giderek artan saldırılara karşı zayıflıklar bulunmaktadır.

Bu kapsamda Savunma Bakanlığının özellikle veri hırsızlığı, bilişim sistemlerinin çalışmasının engellenmesi ve bilgilerin bütünlüğünün sağlanmasına karşı gerekli tedbirlerin alınmasına odaklanılan strateji belgesinde ortaya konulan beş temel stratejik girişim (G) görev olarak ortaya konmuştur.

G1. Siber uzay, bütün potansiyelinden tam olarak yararlanabilmek için düzenlenecek, eğitim ve donanım için harekât alanı olarak değerlendirilecektir.

G2. Ağları ve ağ sistemlerini korumak için yeni savunma anlayış ve çözümleri uygulanacaktır.

G3. Ortak bir siber güvenlik stratejisinin etkinleştirilmesi için diğer bakanlıklar, kamu kurumları ve özel sektör ile ortak çalışmalar yapılacaktır.

G4. Siber güvenliği güçlendirmek için müttefikler ve uluslararası ortaklarla güçlü ilişkiler kurulacaktır.

G5. Olağanüstü bir siber işgücü ve hızlı teknolojik yenileşimcilik yoluyla ülkenin ulusal yetenekleri güçlendirilecektir.

- **Kritik Altyapı Siber Güvenliğinin Geliştirilmesi Konusunda Başkanlık Yönergesi (2013)** [48]

ABD Başkanı B. OBAMA imzası ile 12 Şubat 2013'te yayımlanan, siber güvenliğin önemini vurgulayan, siber güvenlik politikaları ile ilgili sorumluluklar ve uygulamaları konusunda esas ve prensipleri ortaya koyan yönerge 12 Bölümden (B) oluşmaktadır.

B1. Politika: Ülkenin kritik altyapısının güvenliğini ve esnekliğini artırmak ve güvenliği, güvenilirliği, gizliliği, mahremiyet ve medeni özgürlükleri teşvik ederken verimliliği, yenileşimi ve ekonomik gönenci teşvik eden siber bir ortamın sürdürülmesi.

B2. Kritik altyapılar: ABD için hayati önem taşıyan fiziksel, sanal sistemler ve varlıkların tanımlanması (16 grup: Kimyasal, Ticari Tesisler, İletişim, Kritik Üretim, Barajlar, Savunma Sanayi, Acil Servisler, Enerji, Finansal Hizmetler, Gıda ve Tarım, Devlet Tesisleri, Sağlık ve Halk Sağlığı, Bilgi Teknolojisi, Nükleer Tesisler, Ulaşım Sistemleri, Su.).

B3. Politika koordinasyonunun sağlanması.

B4. Siber güvenlik bilgi paylaşımı: Siber güvenlik tehditleri ve istihbaratı ile alınacak tedbirler ve yardımlar konusunda işbirliği esasları.

B5. Kişisel gizlilik, hak ve özgürlüklerin korunması.

B6. Danışma süreci: Siber güvenlik konusunda danışmanlık hizmeti vermesi ve tavsiyelerde bulunmak üzere, Başkanlık Sekreterliği tarafından Kamu kurum ve kuruluşları, Özel sektör kuruluşları, Bağımsız düzenleyici kurumları, Yerel ve bölgesel yönetimler, Üniversiteler, Kritik altyapı sahipleri vb. kurumlar ile uzmanlardan oluşan Kritik Altyapı Ortaklığı Danışma Konseyi oluşturulacaktır.

B7. Kritik altyapıya siber riskini azaltmak için temel çerçeve: Siber Güvenlik Çerçevesi, siber riskleri ele almak için politika, işletme ve teknolojik yaklaşımları düzenleyen bir dizi standart, yöntem, talimat ve süreçleri içerecek, kritik altyapı için geçerli sektörler arası güvenlik standartlarını ve kılavuzlarının belirlenmesi.

B8. Gönüllü kritik altyapı siber güvenlik programı: Sekreterlik tarafından ilgili kurum, kuruluş ve yapılanmaların iş birliği ve koordinasyonu konusunda bir program belirlenmesi.

B9. En büyük risk altında kritik altyapıların belirlenmesi: Oluşturulan danışma kurulunun çalışmaları ile kritik altyapıların önem ve öncelikleri ortaya konularak en yüksek risk altında olanların tespit edilmesi.

B10. Çerçevenin Kabulü: Kritik altyapının güvenliğini düzenleme sorumluluğuna sahip olan kuruluşlarca, Ön Siber Güvenlik Çerçevesinin gözden geçirilmesi ve mevcut siber güvenlik düzenlemelerin ön çerçevesinin yayımlanmasından itibaren 90

gün içerisinde İç Güvenlik ve Terörle Mücadele başta olmak üzere ilgili başkanlık ve direktörlükler koordinesinde başkana sunulacak raporlar doğrultusunda hazırlanan çerçevenin onaylanması.

B11. Tanımlar.

B12. Genel hükümler: Yönergenin yürürlükteki yasalara uygun olarak ve ödeneklerin mevcudiyetine bağlı olarak uygulanmasına yönelik esaslar.

- **Savunma Bakanlığı Siber Stratejisi (2015)** [161]

Strateji belgesinde Savunma Bakanlığı'nın üç ana siber görevi; Bakanlığın kendi ağlarını, sistemlerini ve bilgilerini savunması, ülkeyi ve çıkarlarını, önemli sonuçlara sahip siber saldırılara karşı korumaya hazırlıklı olması, askeri harekâtları ve acil durum planlarını desteklemek için bütünleşmiş siber yetenekler sağlayabilmesi şeklinde sıralanmıştır.

Siber alandaki riskleri azaltmak için karşı koymak ve gerekirse ve yıkıcı saldırılara dayanmak için kapsamlı bir strateji gerektiği vurgulanarak Bakanlığın siber görevleri kapsamında belirlenen stratejik hedefler beş grupta toplanmıştır.

- Siber operasyonları yürütmek için hazır kuvvetler ve yetenekler oluşturulması ve sürdürülmesi.

- Savunma Bakanlığı bilgi ağının korunması, verilerin güven altına alınması ve görevlere yönelik risklerin azaltılması.

- Anavatanı ve hayati öneme sahip çıkarları, önemli sonuçlara yol açan zararlı ve / veya yıkıcı siber saldırılardan korumak için hazırlıklı olunması.

- Bu seçenekleri çatışma tırmanışını kontrol etmek ve çatışma ortamını her aşamada şekillendirmek için kullanmanın planlanması.

- Ortak tehditleri caydırmak, uluslararası güvenliği ve istikrarı artırmak için sağlam uluslararası ittifakların ve ortaklıkların kurulması ve sürdürülmesi.

Gelecekteki güvenlik ortamında artacak tehditler karşısında, Savunma Bakanlığı, kilit durumdaki ve devlet dışı aktörlerin ABD çıkarlarına karşı siber saldırılar yapmalarını engellemek için kapsamlı bir siber caydırıcılık stratejisinin geliştirilmesine ve uygulanmasına katkıda bulunmalıdır**.** Siber uzayda caydırıcılık için Savunma Bakanlığının tek başına gücünü ve genel yeteneklerini siber politikalarını

uygulayarak sağlanamayacağını, ancak açıklama politikası, önemli göstergeler ve uyarı yetenekleri dâhil olmak üzere ABD güç ve eylemlerinin toplamı yoluyla sağlanacağını varsaymaktadır.

Caydırıcılığın kısmen algı işlevi olduğu, ülkeye bir saldırının kabul edilemez maliyetlere sebep olabileceği, öncelikle etkili savunma yetenekleri geliştirmek suretiyle potansiyel bir düşmanı ikna ederek saldırısının başarılı olma olasılığını azaltılabileceği belirtilmiştir. ABD'nin siber uzayda caydırıcılık sağlaması için, gizliliği azaltmak ve güveni artırmak için güçlü istihbarat, yasal takip ve bağlantılı uyarı yeteneklerini geliştirmesi, yanıt, inkâr ve dayanıklılık temel esaslarını uygulaması gerekmektedir.

- **Siber Güvenlik Ulusal Eylem planı (2016)** [162]

'Günümüz sayısal dünyasında Amerikalıları korumak için cesur adımlar atmak' başlığıyla yayımlanan planda, siber güvenliğin karşılaşılan en önemli zorluklardan biri olduğu, bugüne kadar yapılanlardan daha fazlasının yapılması gerektiği, siber güvenlik bilincini artırarak, ekonomik ve ulusal güvenliğin yanı sıra, Amerikalıların sayısal güvenliklerini ve kamu güvenliğini daha iyi sağlamak için uzun vadeli bir ulusal strateji ve eylem planının uygulamaya konduğu vurgulanmıştır.

Bilgi ve iletişimde özellikle çevrimiçi dünyadaki gelişmeler günlük hayatı temelden yeniden şekillendirdiği ve sürekli gelişen sayısal çağ ekonomi, işletmeler ve insanlar için sınırsız fırsatlar sunarken, aynı zamanda karşı konulması gereken yeni nesil tehditler de sunmaktadır. Her geçen gün daha hassas veriler çevrimiçi depolandığından, bu saldırıların maliyetlere yansıyan sonuçları her yıl daha da artmaktadır. Ağlara güvenle bağlanılacaksa korunmaları gerektiği düşüncesinden hareketle, Amerika'yı her zaman büyük yapan ruhu sürdürmek için Hükümet, işletmeler ve bireyler iş birliği ve güç birliği yaparak birlikte hareket etmelidirler.

Bu düşüncelerle oluşturulan Eylem Planının öne çıkan özellikleri arasında aşağıdakiler yer almaktadır:

- Ulusal Siber Güvenliği Geliştirme Komisyonu kurulması

Siber güvenlikle ilgili inceleme ve faaliyetleri koordine ederek yürütmek için hükümet içinden ve dışından gelen en önemli stratejik, ticari ve teknik düşünürlerden oluşan Komisyon; siber güvenlik bilincini ve korunmayı artırmak, gizliliği korumak,

kamu güvenliğini, ekonomik ve ulusal güvenliği sağlamak için gelecek on yılda gerçekleştirilebilecek eylemler için bir yol haritası sağlamakla görevlidir. Komisyon tarafından 3.1 milyar dolarlık Bilgi Teknolojisi Modernizasyon Fonu oluşturulması ve 2017 yılı Başkanlık Bütçesinde siber güvenlik için 19 milyar $ 'dan fazla yatırım yapılması için planlama yapılması öngörülmüştür.

- Ülke genelinde siber güvenlik seviyesini yükseltilmesi.

2015 Siber Güvenlik Stratejisi ve Uygulama Planında yer alan eylemler kapsamında Siber Güvenlik strateji ve politikalarının planlamasını, koordinesini, uygulamasını sağlamak ve yönetmek üzere Federal Baş Bilgi Güvenliği Görevlisi (Federal Chief Information Security Officer) konumu oluşturulmuştur.

Ülke genelinde siber risk ve tehditlere karşı sürekli teşhis ve azaltma programlarını genişleterek Devlet genelinde bilgi teknolojilerini ve siber güvenlik için ortak hizmetlerin kullanılabilirliğini ve siber güvenliğini arttırmak için İç Güvenlik Bakanlığına ek görevler verilmiş, Federal sivil siber savunma ekiplerinin sayısı ve siber güvenlik personeline ayrılan bütçe artırılmıştır. Siber güvenlik alanında bireylerin güçlendirilmesi yanında, kritik altyapı güvenliğinin ve esnekliğinin artırılması ve güvenli teknolojilerin geliştirilmesi ilave tedbirler ve hareket tarzlarıyla yol haritaları belirlenmiştir.

- Siber alanda kötü amaçlı hareketlerin durdurulması, vazgeçirilmesi ve caydırılması.

Sorumlu devlet davranış ilkelerini benimseyerek uluslararası çabalara öncülük edilmeli dünyadaki ortaklar ve müttefiklerle birlikte, ikili ve çok taraflı taahhütler ve güven artırıcı önlemler yoluyla kurumsallaşarak ve uygulamayı amaçlayarak belirlenen hedeflere yürünmesine önem verilmelidir.

- Siber olaylara müdahalenin geliştirilmesi.

Kötü niyetli siber olayların önlenmesinde ve caydırılmasında geçmiş olaylardan öğrenilen dersleri de uygulayarak gelecekteki siber olayların yönetiminin iyileştirilmesi ve ülkenin siber dayanıklılığını artırılması için kamu kurumları ve özel sektörün etkili bir şekilde iletişim kurabilmeleri ve uygun ve tutarlı bir tepki düzeyi sağlayabilmeleri için ulusal siber olayların değerlendirilmesi ve koordinasyonu için yapılanmanın ve yönetiminin geliştirilmesi sağlanmalıdır.

- **İç Güvenlik Bakanlığı Siber Güvenlik Stratejisi (2018)** [163]

Strateji ile Bakanlığa, zayıf noktaları azaltarak ve esnekliği artırarak gelişen siber risk manzarasına ayak uydurmak için gelecek beş yıl boyunca siber güvenlikle ilgili sorumlulukları yerine getirecek bir çerçeve sunulması, siber alanda kötü niyetli oyunculara karşı konulması, olaylara cevap vermek ve siber ekosistemin daha güvenli ve esnek hale getirilmesi amaçlanmıştır.

Bakanlık ulusal siber güvenlik risklerini stratejik olarak yönetmek için beş ana bölümden (B) oluşan ve yedi hedefi (H) öngören bir risk yönetimi yaklaşımı belirlemiştir.

BI. Risk Tanımlama.

H1. Gelişen siber güvenlik risklerini değerlendirilmesi.

BII. Güvenlik Açığı Azaltma.

H2. Federal Hükümet Bilgi Sistemlerinin korunması.

H3. Kritik altyapıların korunması.

BIII. Tehditlerin Azaltılması.

H4. Siber alanın suç maksadıyla kullanımının önlemesi.

BIV. Sonuçta Hasar ve Zararı Azaltma.

H5. Siber olaylara etkili bir şekilde yanıt verilmesi.

BV. Siber Güvenlik Tedbirlerinin Etkinleştirilmesi.

H6. Siber ekosistemin güvenliğinin ve güvenirliğinin güçlendirilmesi.

H7. Siber güvenlik faaliyetlerinin yönetiminin geliştirilmesi.

- **Ulusal Siber Strateji (2018)** [164]

ABD Başkanı tarafından onaylanan belgenin önsözünde; siber güvenliğin ekonomi ve savunma dâhil tüm Amerikan yaşamının ayrılmaz bir bileşeni olduğu, kamu ve özel kurumların hala sistemlerini güvence altına almakta zorlandıkları ve rakiplerin kötü niyetli siber faaliyetlerinin sıklığını ve karmaşıklığını arttırdıkları, Amerika'nın interneti yarattığı ve dünyayla paylaştığı, şimdiyse gelecek nesiller için siber alanın güvenliğinin ve korunmasının sağlanacağı belirtilmiştir.

Stratejinin yönetim ilkeleri üç başlıkta toplanmıştır.

- Ağları, sistemleri ve verileri koruyarak vatanı savunmak, güvenli, gelişen bir sayısal ekonomiyi besleyerek ve güçlü yerel yenileşimi teşvik ederek Amerikan gönencini teşvik etmek,

- ABD’nin müttefikleri ve ortaklarıyla birlikte siber araçları kötü niyet ve maksatla kullananları caydırma ve cezalandırma yeteneğini güçlendirerek barışı ve güvenliği sağlamak,
- Açık, birlikte çalışabilir, güvenli ve güvenilir bir internetin temel ilkelerini genişletmek için Amerika'nın yurtdışındaki etkisini artırmak.

Ulusal Siber Güvenlik Stratejisinin temel amacı ve önceliği; Amerikan halkını, vatanını, yaşam tarzını ve çıkarlarının korunması olarak belirlenmiş, kamu ağlarının, kritik altyapılarının korunması ve siber suçlarla mücadeleyle ilgili eylemlerin uygulanarak siber güvenliğin güçlendirilmesi için acil ve kararlı olarak atılacak adımlar dört ana bölüm (B) ile alt ve yardımcı eylemler şeklinde sıralanmıştır.

B1. Amerikan halkının, anavatanının ve yaşam tarzının korunması.
- Kritik altyapıların güvenliğinin sağlanması.
- Siber suçlar ile mücadele ve olay raporlamasının iyileştirilmesi.

B2. Amerikan gönencinin teşvik edilmesi.
- Canlı ve esnek bir sayısal ekonomi geliştirilmesi.
- Amerika'nın yetkinliğinin güçlendirilmesi ve korunması.

B3. Barışın güçle korunması
- Sorumlu devlet davranışı değerleriyle siber kararlılığının artırılması
- Siber değerlerle evrensel bağlılığın özendirilmesi,
- Siber alanda kabul edilemez davranışların tespiti ve caydırılması
- Tarafsız ve iş birliğine dayalı zekâ ile liderlik edilmesi,
- Sonuçların dayatılması,
- Siber caydırıcılık girişimi oluşturulması,
- Kötücül siber etkilere ve bilgi işlem faaliyetlerine karşı konulması,

B4. Amerika’nın Yüksek Güç Etkisi
- Açık, birlikte çalışabilir ve güvenli internet tanıtımı yapılması.
- Uluslararası siber kapasitenin oluşturulması

- **ABD siber güvenlik / savunma teşkilat yapısı**

ABD’de siber güvenlik strateji ve politikaları ile ilgili sorumluluklar geniş oranda dağılmış olsa da, en üst seviyede koordinasyon sorumluluğu Başkanlık Ulusal Güvenlik Konseyi’ne bağlı Bilgi ve İletişim Altyapısı Uyumluluk Politikası Komitesi (ICI-IPC) tarafından yerine getirilmekte, Ulusal Güvenlik Konseyi ve Siber Güvenlik

Koordinatörü (CSC) tarafından yönetilmektedir. CSC, ulusal siber güvenlik stratejisi ve politikasının bütünlüğünün geliştirilmesine öncülük eder ve kurumların bu politikaların uygulanmasını denetler. Ulusal Güvenlik Konseyi Başkanının Baş Danışmanı olarak görev yapan CSC, konseye rapor verir, Beyaz Saray'da danışma sürecini yönetir ve ABD'nin siber güvenlikle ilgili politika ve faaliyetlerini koordine eder [165, 166].

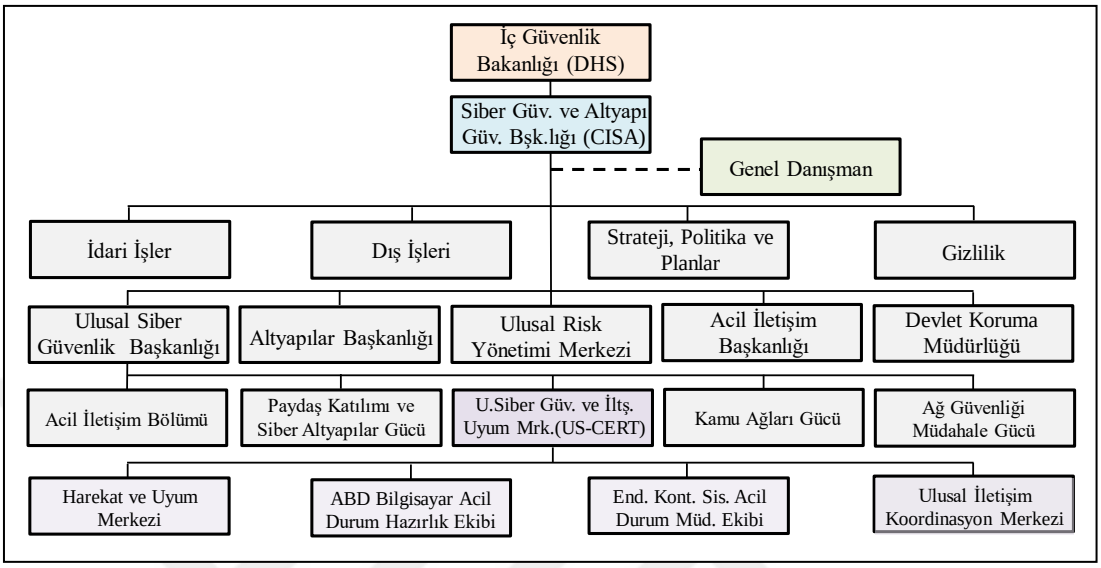
İç Güvenlik (Anavatan Güvenliği) Bakanlığı (DHS) ABD sınırları içindeki siber güvenlikten sorumlu birincil kurumdur. DHS'nin temel görevlerinden birisi olarak siber alanı korumak ve güvenliğini sağlamak için öncelikli alanlar şunlardır:

- Kritik altyapının güvenliğini ve esnekliğini güçlendirmek,
- Siber güvenlik projeleriyle ilgili federal sivil kuruluşlara yardım etmek,
- Ortak risklerle ilgili politikaların ve en iyi uygulamaların benimsenmesini teşvik etmek,
- Kanun uygulama, olay tepkisi ve raporlama yeteneklerini geliştirmek,
- Sağlıklı bir siber ekosistemi sağlamak.

İç Güvenlik Bakanlığının bu görevleri Siber Güvenlik ve Altyapı Güvenliği Başkanlığı (CISA) tarafından yerine getirilmektedir (Şekil 5.4). Bu başkanlığın ana unsurlarını Ulusal Siber Güvenlik, Altyapılar, Ulusal Risk Yönetimi Merkezi, Acil İletişim Başkanlıkları ve Devlet Koruma Hizmetleri Müdürlüğü oluşturmaktadır. Siber güvenlik ile ilgili siber olaylara müdahale başta olmak üzere kamu ağlarının güvenliği ile işbirliği ve koordinasyon görevlerini yerine getiren Ulusal Siber Güvenlik Bölümü ise Ulusal Siber Güvenlik ve İletişim Uyum Merkezi (NCCIC), Acil İletişim, Paydaş Katılımı ve Siber Altyapıları Gücü, Kamu Ağları ve Ağ Güvenliği Müdahale birimlerinden oluşmaktadır.

Ülkenin siber savunması için en önemli birimlerinden birisi olan Ulusal Siber Güvenlik ve İletişim Uyum Merkezi siber olaylara müdahale ve operasyonel uyum merkezi (US-CERT) olarak görev yapar, siber güvenlik ve iletişim bilgileri, teknik uzmanlık ve operasyonel bütünleşme için 7/24 durumsal farkındalık, olay analiz ve müdahale görevleri için ulusal bir merkez olarak hizmet vermektedir. Kritik altyapı sahiplerinin ve operatörlerinin yasal olarak siber güvenlik olaylarını belirlenmiş bir devlet otoritesine bildirmek zorunluluğu olan birçok Avrupa ülkesinin aksine, ABD'de hükümet ile özel sektör arasındaki güvenlik açığı ve risk değerlendirmeleri hakkında

bilgi paylaşımı isteğe bağlıdır. Benzer şekilde, kritik altyapıyı hedef alan siber saldırılardan korunma, müdahale ve kurtarma için birincil sorumluluk bu varlıkların sahiplerine ve operatörlerine aittir. ABD hükümetinin politikası özel sektörle bilgi paylaşımını artırmayı hedeflemektedir.



Şekil 5.4: ABD Siber Güvenlik ve Altyapı Güvenliği Başkanlığı teşkilatı [156,162].

ABD'de bütün ülke için siber güvenlik görevleri üslenen ve yerine getiren diğer iki bakanlık Dış İşleri ve Adalet Bakanlıklarıdır. Dış İşleri Bakanlığı ABD Başkanının uluslararası alanda başta güvenlik, ekonomi ve insan hakları konularının siber yönleri ve internet özgürlüğü olmak üzere siber güvenlik strateji ve politikalarının uygulanmasını koordine etmekten birinci derecede sorumludur. Adalet Bakanlığı ise, siber suçları ve suçluları önleme, araştırma, soruşturma ve kovuşturma, bu konuda siber istihbarat çalışmaları da dâhil olmak üzere siber güvenlik ile ilgili yasaların uygulanmasından sorumludur.

İç Güvenlik Bakanlığı devlet ağları ve altyapısını korurken, Savunma Bakanlığı (DoD), askeri alanı ve bakanlığın küresel bilgi altyapısını siber saldırılara karşı korumakla görevlidir. Ayrıca yabancı siber tehdit bilgilerinin toplanması, ulusal güvenlik ve askeri sistemlerin güvence altına alınması ve siber suçların askeri yargı alanındaki soruşturulması konusunda da sorumlulukları bulunmaktadır. Bu görevlerin üç ana başlıkta toplandığı görülmektedir.

- Savunma Bakanlığı bilgilerinin, sistemlerinin ve ağlarının korunmasına yönelik siber güvenlik ve operasyonel kapasite geliştirme,
- Ulusu hedef alan siber saldırılara karşı sonuç alıcı aktif savunma,

- Askeri harekâtların ve acil durum planlarının desteklenmesi.

Bakanlık bu temel görevleri ABD Stratejik Komutanlığı bağlısı Siber Komutanlık (USCYBERCOM) ile Ulusal Güvenlik Ajansı (NSA) / Merkezi Güvenlik Hizmet Merkezi, Savunma Siber Suç Merkezi ve Savunma Bilgi Sistemleri Başkanlığı (DISA) aracılığıyla gerçekleştirilmektedir. Siber Komutanlık görevlerini Kara, Deniz, Hava ve Sahil Güvenlik Komutanlıkları bünyesinde bulunan siber güvenlik birimleri ile işbirliği ve koordinasyon içerisinde yürütmekte olup temel görevleri altı başlık altında toplanmıştır.

- Bakanlık ağlarının bilgi güvencesini sağlamak ve siber güvenlik harekâtını icra etmek,
- Siber savunma harekâtını desteklemek,
- Siber harekâtın uyumunu ve koordinasyonunu desteklemek için personeli yetiştirmek ve güçlendirmek;
- Siber araştırma ve teknoloji projelerini desteklemek,
- Siber harekât için Ar-Ge'nin öncelikle geliştirilmesini desteklemek,
- Bakanlığın büyük bilişim teknolojileri bütçesinde devam eden yatırımları desteklemek.

Savunma Bakanlığının 6.000'den fazla sivil ve askerden oluşan siber görev gücünün dört farklı yapıda oluşması hedeflenmiştir.

- Ülkeye yönelik önemli siber saldırılara karşı destek sağlayan Ulusal Görev Ekipleri,
- Bakanlığın öncelikli ağlarını ve sistemlerini savunmak ve dünya çapında askeri harekâtları desteklemek için Siber Savunma Ekipleri,
- Harekât planları ve acil durum operasyonlarını destekleyen Mücadele Görev Ekipleri
- Analitik ve planlama desteği sağlamak için Destek Ekipleri.

ABD'de ülke çapında siber güvenlikle ilgili olaylarda kriz müdahale koordinasyonu, İç Güvenlik Bakanlığı sorumluluğunda 'Ulusal Siber Olay Müdahale Planı'na göre yürütülmektedir. Planda İç İşler Bakanlığına Ek olarak, Başkanlık, Savunma Bakanlığı, Ulusal Güvenlik Başkanlığı, Adalet Bakanlığı, Federal Soruşturma Bürosu (FBI), Dış İşleri Bakanlığı, özel sektör temsilcileri, diğer devlet birimleri ve hükümet dışı sektörler ve uluslararası işbirliği unsurları yer almaktadır.

Siber savunmada siber istihbarat desteği ise Ulusal İstihbarat Direktörü (DNI) başkanlığındaki İç Güvenlik Bakanlığı, Savunma Bakanlığı, Dış İşleri Bakanlığı, Federal Soruşturma Bürosu vb. birimlerin koordinesi ve güç birliğinden oluşan ABD İstihbarat Topluluğunca sağlanmaktadır. ABD Siber Komutanlığı ve Merkezi Güvenlik Hizmeti Komutanı olan NSA Direktörü de Ulusal İstihbarat Direktörüne rapor vermekten sorumludurlar. [156]

5.4.2 Çin Halk Cumhuriyeti siber güvenlik stratejisi

Nüfusuyla dünyanın en kalabalık ülkesi olan, ekonomik ve siyasi alanda da kilit bir konuma gelen Çin, 2016 yılına ait istatistiklere göre dört milyara yakın internet kullanıcısının bulunduğu dünyada bir milyara yakın [166] internet kullanıcısıyla da en üst sırada yer almaktadır. İnternetin sağladığı fırsatlardan yararlanırken siber uzaya bağımlı bir hale gelen Çin'in teknolojisi ve büyük bir uzman havuzuna sahip olan insan kaynağına karşın ulusal siber güvenliğe yönelik tehditlere cevap vermede strateji geliştirme konusunda yavaş kaldıkları, kısa süre öncesine kadar bu konuda kapsamlı ve etkin bir yaklaşım oluşturamadıkları görülmektedir.

Çin'in siyasi, ideolojik ve kendine özgün yapısından kaynaklanan belirsizlikler yanında özellikle sanayi ve devlet tesislerini hedef alan eylemleri dolayısıyla siber alanda uluslararası iş birliği ve koordinasyon çalışmalarında da güvensizlik söz konusu olmaktadır. Bu olumsuzluk ve belirsizliklere karşın 2012 yılında başlayarak dikkate değer bir atılım gerçekleştirdiği anlaşılmaktadır. Açık kaynaklardan resmî belgelere ulaşılmasının zorlukları nedeniyle, Çin'in siber güvenlik strateji ve politikalarının tam olarak neye dayandığını anlamak kolay değildir. Ancak devletin siber alanla ilgili düzenleme sağlamak maksatlı bazı yayımları ile kurum ve kuruluşların uygulamalarından hareketle bazı analizler yapılabilmekte ve kısmen de olsa bazı sonuçlara ulaşılabilmektedir.

Çin'in siber güvenlik konusunda ilk çalışmaları; 1986 yılında 'Devlet Ekonomik Bilgi Yönetimi Liderliği' grubunun kurulmasıyla bilgi teknolojisine ulusal yönelim başlanması, 1999 ve 2001 yıllarında Devlet Bilişim Liderliği Grubunun geliştirilmesi, 2003 yılında, Devlet Ağı ve Bilgi Güvenliği Koordinasyon Grubu'nun kurularak çalışmalarına başlaması şeklinde sıralanmaktadır. Kurulan bu grupların hedefleri, yerli bilgi teknolojilerini geliştirmek ve onları ulusal bir güvenlik bağlamına yerleştirmek şeklinde belirlenmiştir. 2000'li yılların başlarından itibaren de, bilişim teknolojilerinin

gelişimi devlet yöneticilerini ekonomi ile ulusal güvenliğin birlikte ele alınmasına yöneltmiştir [167].

- **Belge 27 ile yayımlanan bilgi güvenliği güvence çalışmasının güçlendirilmesine yönelik görüşler (2003)**

2003 yılında, felaket kurtarma, olay yönetimi ve e-devlet güvenlik planları dâhil olmak üzere siber güvenlikle ilgili temel politikaları ve ulusal stratejileri uygulayan 'Belge 27' yayımlanmıştır. Belge 27'nin temel dayanağının; 'aktif savunma' kavramı olduğu ve kritik altyapıların korunması, şifrelemelerin ve dinamik izlemenin arttırılması, yerli yenileşimin iyileştirilmesi ve siber güvenliğe yüksek önem verilmesi, daha iyi koordinasyon ve finansman konularına değinmek için çeşitli politikalar hazırlanması şeklinde sıralanmaktadır. [168]

- **Ulusal Orta ve Uzun Vadeli Bilim ve Teknoloji Geliştirme Planı - 15 yıllık strateji (2006)**

Çin'de Şubat 2006'dan bu yana, bilgi güvenliği ile ilgili strateji ve politikalardaki gelişmeler ile geleceğe yönelik yenileşim faaliyetlerinin tamamı Devlet Konseyi tarafından yayımlanan, 'Orta ve Uzun Vadede 2006-2020 Bilim ve Teknolojinin Gelişimi Ulusal Programı' belgesine dayanmaktadır.

Belgede, Çin'in teknolojik yerli yenileşim konusundaki hedefleri listelenirken araştırma ve geliştirmeye daha fazla yatırım yapılmasının gerekli olduğu, gelecek nesil internet teknolojileri, sayısal olarak kontrol edilen üretim tesisleri ve yüksek çözünürlüklü dünya gözlem sistemleri de dâhil olmak üzere, yurt dışından "Ulusal ekonominin ve ulusal güvenliğin canlanmasını etkileyen kilit alanlarda çekirdek teknolojiler" temin edilmesi vurgulanmıştır. [169]

15 Yıllık Strateji, askeri savunma ve güvenlik konularının yanında, teknolojik gelişmeler, enerji ve su temini konuları ile fikri mülkiyet hakları konusu dâhil önceliklendirmeler, Çin'in dünya pazarlarında rekabetini de güçlendirecek esasları ortaya koymuştur.

Planın uygulanması yenileşim Çin'in teknolojisi ve küresel standartları açık pazarları ve uluslararası bağları güçlendirirken, yavaş yavaş dünya pazarlarına girilirken, yabancı teknoloji firmalarının Çin'de faaliyetleri kısıtlanmakta, yabancı şirketlerin bankacılık ve ulaştırma başta olmak üzere kritik altyapı şirketlerine temel

ürünleri satmalarını yasaklayarak ulusal güvenliğin korunmasını amaçlamıştır. Özellikle bilgi güvenliği programlarını Çin hükümetine satmak isteyen yabancı firmaların, ürünlerinin kaynak kodlarını paylaşmaları gerekebileceği belirtilmiş ve fikri mülkiyet haklarını hükümete vermeleri zorunlu kılınmıştır. [170]

- **Devlet Konseyi'nin Bilgi Bürosu'nun Yeni Politika Görüşü (2012)**

Devlet Konseyi Bilişim Bürosu tarafından 2012 yılında Devlet Konseyi'nin bilişim teknolojilerinin gelişimini özendirmek ve bilgi güvenliğinin bilinçli olarak sağlanmasına yönelik olarak 'Yeni Politika Görüşü' yayımlanmıştır. Daha önceki belgelerde yer alan genel kaygılar devam ederken belirlenen hedeflerin tamamına ulaşılamadığı vurgulanmıştır. Siber güvenliğin temel alanlarının çoğunu kapsayan belgede Çin'in bilgi güvenliği modelinin temel zayıf yönleri gösterilmiş ve internete bağımlılıkların arttığına dikkat çekilmiştir.

Bilgilerin elde edilmesi, kullanılması ve kontrol edilmesi konusundaki uluslararası pazardaki rekabette karşılaşılan zorluklar ısrarla belirtilirken, sayısal altyapıdaki Batı ve Çin arasındaki eşitsizlik, hükümet ve sanayi arasında yetersiz bilgi alışverişi, zayıf siber güvenlik planlaması, yetersiz savunma yeteneği ve çekirdek teknolojiler üzerinde yabancılar tarafından sürekli olarak kontrol edilen alanlara dikkat çekilmiştir. Hızlı ekonomik kalkınma ile sosyal uyuma dikkat edilirken bilgilerin güvenliği ve siber güvenlik konusu ön plana çıkmıştır. Bu kapsamda sivil siber savunmaya odaklanan dört politika yetkisi belirlenmiştir. [171]

- Bilgi ağlarına odaklanarak, tüm kritik bilgi sistemlerinin ve altyapının güvenliğine büyük önem verilmesi, özellikle haberleşme, enerji ve finans ağlarının güvenliğinin sağlanması,

- Bilgisayar korsanları için çekici hedefler olan devlet ve gizlilik dereceli bilgilerin güvenlik sistemlerinin güçlendirmesi,

- Petrol ve doğal gaz boru hatları, nükleer ve elektrik altyapıları gibi tesislerin endüstriyel kontrol sistemlerinin, ulaşım ve kentsel tesislerin korumasının arttırılması,

- Ülkenin genel gönencini sağlayacak hassas verilerinin ve Çin vatandaşlarının kişisel bilgilerinin korunması.

- **Yeni ulusal bilgi güvenliği stratejisinin oluşturulması (2014)**

27 Şubat 2014'te 'Merkezi Öncü İnternet Güvenliği ve Bilgilendirme Merkezi' kurulmuş, Devlet Başkanı tarafından Çin'in Batı'nın yenileşim konusunda bulunduğu noktaya yetişmesine dikkat çekilirken 'İnternet güvenliği, bilginin elde edilmesi, modernleşme ve ulusal güvenlik' konularında yetersizliklere dikkat çekilmiştir. Bizzat Devlet Başkanı tarafından "İnternet Güvenliği ile Bilgi Yönetimi bir kuşun iki kanadına benzetilerek" siber egemenliğin önemi vurgulanmıştır.

İnternetin yönetişimi ve teknolojinin yenileşiminin sağladığı güce vurgu yapılırken interneti kullanmak için, internette ne ifade edilirse söylensin, yedi unsura saygı gösterilmesi gerektiği belirtilen Yedi Temelli Doktrin hazırlanmıştır. Devletin karalılıkla denetleyeceği belirtilen bu doktrin 'Kanun ve yönetmelikler, sosyalist sistem, ülkenin ulusal çıkarları, vatandaşların yasal hakları ve çıkarlar, kamu düzeni, ahlak ve doğruluk' esasları üzerine oluşturulmuştur.[167]

- **Çin Siber Güvenlik / Savunma Teşkilat Yapısı**

Siber güvenliğin sağlanması, bu konuda strateji ve politikaların oluşturularak uygulanması konusundaki yapılanmanın Devlet Konseyi tarafından 2006'daki 15 Yıllık Plan ve 2012'deki Yeni Politika Görüşü esaslarına göre gerçekleştirildiği görülmektedir [169-171].

- Sanayi ve Bilgi Teknolojileri Bakanlığı, 2008 yılında bilgi teknolojisi gelişiminin merkezileştirilmesi amacıyla kurulmuştur ve Çin'in siber alanının somut ilerlemesini gerçekleştirmenin arkasındaki ana güçtür. Tüm Devlet Konseyi'nin bilgi yönetimi konusundaki çalışmalarını üstlenir ve bu konudaki standartları belirler, ağ güvenliğini denetler ve özel bir bölüm aracılığıyla bilgi ve telekomünikasyon güvenliğini koordine eder, konuyla ilgili tatbikatları yapar.

2002 yılında kurulan ve ana görevi siber saldırılara cevap vermek olan Ulusal Bilgisayar Ağı Acil Müdahale Teknik Ekibi / Koordinasyon Merkezi'nin virüs ve güvenlik açığı veri tabanları oluşturmasına yardımcı olarak, zararlı internet protokolü (IP) ve etki alanı adı sağlayıcılarını bulmasına ve uluslararası iş birliğine girmesine rehberlik ederek çalışmalarını desteklemektedir. Bakanlık ayrıca, ulusal savunma için bilim, teknoloji ve endüstri ile ilgili kılavuz ilkeleri, politikaları, yasaları ve

düzenlemeleri hazırlayan Ulusal Bilim, Teknoloji ve Ulusal Savunma Sanayi İdaresi'nde yer almaktadır.

- Kamu Güvenliği Bakanlığı, siber suçları araştırmakta ve geniş kapsamlı araştırma laboratuvarları ağı aracılığıyla geliştirme çalışmaları ile birlikte kritik altyapıların korumasını sağlamaktadır. Ayrıca, devlet tarafından kullanılan ticari ürünlerin denetlenmesinden ve tüm ticari bilgi güvenliği şirketlerinin kontrol edilmesinden sorumludur. En önemli görevlerinden birisi de aynı zamanda yerel istihbarat yönetimini de kapsayan Çin Büyük Güvenlik Duvarı'nı işletmektir.

- Devlet Güvenlik Bakanlığı, karşı casusluk, karşı istihbarat, yabancı istihbarat ve yerel istihbarat görevlerini yerine getirmekte, ayrılıkçılık, terörizm ve aşırı dincilikle mücadele görevleri yanında, siber yeteneklerini yabancı hükümetler, sivil toplum kuruluşları ve yerel muhalifler hakkında daha fazla siyasi ve ekonomik veri toplamak için de kullanmaktadır.

- Milli Savunma Bakanlığı

Çin'in ulusal savunmasında siber güvenliğe önem verilmekte, doküman ve belgelerinde de bu konu açıkça vurgulanmaktadır. Çin'in 2010 Savunma Belgesinde ulusal savunmasında siber güvenliğin önemi vurgulanırken siber savaş yeteneklerinin olası askeri harekâta üç kilit alanda hizmet verebileceği belirtilmiştir. Bunlar, sızma yoluyla veri toplanması, ağ tabanlı lojistik, iletişim ve ticari faaliyetlerinin hedeflenerek düşmanın eylemlerinin sınırlandırılması ve kuvvet çarpanı olarak kullanılması şeklinde sıralanmıştır. [172]

Bilgi güvenliği de dâhil olmak üzere savaşın her alanında savunma yapısını her zaman ön planda vurgulayan Çin'in 2013 yılında yayımlanan Savunma Beyaz Kitabı'nda, Çin'in ulusal güvenlik çıkarlarını koruma hakkı ilan edilmekte ve siber uzay da dâhil olmak üzere saldırıya uğramadıkça saldırmayacağına dair söz verildiği görülmektedir. [173] Çin'in bu görüşünde, Belge-27'de de belirtildiği gibi ancak saldırıdan sonra saldırılacağı askeri strateji belgelerinde de yer almakta ve siber uzayda da benzer şekilde 'aktif siber savunma' anlayışı yaygınlaştırılmaktadır.

Çin Milli Savunma Bakanlığı'nca, savaşın bilgilendirilmesine yoğunlaşan ve buna ek olarak Çin'in siber güç ve siber durum farkındalığı, siber savunma, ülkenin siber alandaki çabalarına destek ve uluslararası siber iş birliğine katılım yeteneklerini içeren

gelecekteki bilgilendirilmiş savaşları kazanabilmek için bilgili bir ordu oluşturma hedefini öngören Çin'in Askeri Stratejisi Mayıs 2015'te yayımlanmıştır. Ordunun siber faaliyetlerinin ardında siber uzayda üstünlük kazanma yanında ekonomik ve politik hedefler vardır.

Orduda siber güvenliğe yönelik yapılanmada Genelkurmay Başkanlığına bağlı teknolojik keşif ve istihbarat desteğini sağlayan 3'ncü Başkanlık ve özellikle siber alan da dâhili elektronik keşif ve istihbarat sağlayan 4'ncü Başkanlık önemli görevler üslenmiş bulunmaktadır. Ayrıca 2014'te özellikle siber alanda orduya destek sağlamak üzere Siber Stratejik İstihbarat Araştırma Merkezi kurulmuştur.

Paralel olarak kurulan Stratejik Destek Gücü, 3 ve 4'üncü Başkanlık ile Siber Stratejik İstihbarat Araştırma Merkezi desteğinde Çin'in asimetrik savaş ve önleyici saldırı hakkındaki stratejik düşüncesinin merkezinde bulunan istihbarat, teknik keşif, siber savaş ve elektronik savaş dâhil her türlü bilgi savaşından sorumlu olarak görev yapmaktadır. [174]

5.4.3 Rusya Federasyonu (RF) siber güvenlik stratejisi

Rusya'nın son 20 yıllık geçmişine bakıldığında strateji ve doktrinlerinde eski Sovyet döneminden kalma yaklaşımların devam ettiği kolaylıkla görülmektedir. Siber güvenlik strateji ve politikalarında NATO ve diğer Batı ülkelerinin teknik ağ merkezli siber güvenlik yaklaşımlarından ve bakış açılarından farklı olarak teknik ağ merkezli siber güvenliğe odaklanma yerine, özellikle bilgi güvenliğinde daha farklı, kapsamlı ve bütünleşik bir yaklaşım benimsediği, internet, sosyal medya ve kitle iletişim araçlarının kullanılmasında bilginin kontrolüne odaklanıldığı ve kitlelerin biçimlendirilerek yönlendirilmesine önem verildiği görülmektedir.

Kontrolsüz bilginin hükümet ve toplum için bir tehdit oluşturduğu görüşü, ulusal strateji ve politikaları ile bilişim teknolojileri ve askeri doktrinlerin oluşturulmasında ve uygulanmasında etkili olmaktadır.

- **RF Bilgi Güvenliği Doktrini (2000)** [175]

Siber güvenlik konusunda açık kaynaklara yansıyan ilk resmî belgelerden birisi olan Doktrinde, bilgi dünyasına uygulandığı şekliyle ulusal güvenlik konsepti açıklanmış, RF'de bilgi güvenliğinin sağlanmasında ana hedefler ve temel ilkeler ortaya konmuştur. Doktrinde bilgi güvenliğine yönelik ana hedefler üç başlıkta toplanmıştır.

- Bilgi güvenliği hakkındaki hükümet politikasının şekillendirilmesi,
- Bilgi güvenliğini sağlamak için yasal, yöntemsel, bilimsel, teknik ve örgütsel çerçeveyi iyileştirmeye yönelik önerilerin hazırlanması,
- Hedeflenen ulusal bilgi güvenliği programlarının geliştirilmesi.

Genel yönelimlerine göre, RF'nin bilgi güvenliğine yönelik tehditler dört gruba ayrılmıştır.

- Vatandaşların anayasal hak ve özgürlüklerine, bireysel, toplumsal, kamu bilincine ve Rusya'nın toplumsal canlanmasına yönelik tehditler,
- Rusya Federasyonu devlet politikasına bilgi desteğine yönelik tehditler,
- Rus bilgi endüstrisinin (bilgi, iletişim ve haberleşme tesisleri dâhil) gelişimine, ürünlerin iç pazar gereksinimlerini karşılanmasına ve dünya pazarına girişleri ile ulusal bilgilerin üretimine, depolanmasına güvenilirliğine ve etkin kullanımına yönelik tehditler,
- Rusya topraklarında konuşlu olsun veya olmasın, bilgi ve iletişim sistemlerinin ve tesislerinin güvenliğine yönelik tehditler.

Bilgi güvenliğinin sağlanmasında özellikle dış politika alanında ulusal nitelikli bilgilere yönelik dış tehditlerin en büyük tehlike grubunu oluşturduğu kabul edilerek bunlara dikkat çekilmiştir.

Bu kapsamda kabul edilen tehlikeler;

- Dış politik, ekonomik, askeri ve bilgi kuruluşlarının, Rusya Federasyonu'nun dış politika stratejisinin açığa çıkarılması ve uygulanması konusunda sahip olunabilecek bilgilere yönelik tehlikeler,
- Rusya Federasyonu'nun deniz aşırı yayılması konusunda dış politikası hakkındaki bilgilere yönelik tehlikeler,
- Yurtdışındaki bilgi alanındaki Rus vatandaşlarının ve tüzel kişilerin haklarının ihlal edilmesi,
- Rusya Federasyonu dış politikasını uygulayan federal yürütme organları ile yurtdışındaki uluslararası kuruluşlardaki temsilcilerinin bilgi kaynaklarına saldırı girişimleri.

- **RF Bilgi Güvenliği Doktrini (2016)** [176]

Devlet Başkanı tarafından, bugünkü gerçeklerin göz önünde bulundurularak, bilgi alanındaki Rus ulusal çıkarlarının korunmasına yönelik mevcut yaklaşımları güncellemek, bilgi güvenliği alanındaki devlet politikasının ve halkla ilişkilerin

geliştirilmesinin yanı sıra bilgi güvenliği sistemini iyileştirmeye yönelik tedbirlerin geliştirilmesine de temel oluşturma maksatlarıyla hazırlanan ve 6 Aralık 2016'da onaylanarak 01 Ocak 2017'den itibaren uygulamaya konulan Doktrin, 2000 yılında kabul edilen eski doktrinin yerine geçmiştir.

Doktrinde görünüşe göre demokratik bir tavır ve Rusya'nın Rus vatandaşlarının 'anayasal haklarını ve özgürlüklerini koruma' ihtiyacına ve 'demokratik kurumlar için güvenli bilgi desteği' ihtiyacı vurgulanmasına karşın, Eski Sovyet ideolojisinin kullandığı yöntem ve kalıpları yeniden düzenlemenin amaçlandığı görülmektedir.

Siber güvenlik, gizlilik ve bilgi güvenliğini Rusya'nın ulusal çıkarları için yaşamsal öneme sahip esasların belirlenerek kamu politikaları ve halkla ilişkilerde daha ileri gelişmelerin temelini oluşturmaya yönelik sistemlerin geliştirilmesi amaçlanan Doktrinde ulusal çıkarlar beş ana grupta sıralanmıştır.

- Bilgi gizliliği konusunda insan ve vatandaşların anayasal hak ve özgürlüklerinin desteklenmesi ve korunması, demokratik kurumların, devlet ile sivil toplum arasındaki etkileşim mekanizmalarının desteklenmesi, halkın kültürel, tarihi, manevi ve ahlaki değerlerinin korunması,
- Barış zamanı ve savaş zamanlarında ve yabancı saldırganlık eylemlerine cevap olarak kritik ulusal bilgi altyapısının sürdürülebilir ve kesintisiz çalışmasının sağlanması,
- RF'nin bilişim teknolojileri alanındaki gelişiminin sağlanması,
- Rus hükümetinin siber güvenlik ve savunma ile ilgili politikalarının ulusal ve uluslararası alanda tanıtılması,
- RF'nin bilgi egemenliğini korumak için bilgi teknolojilerinin kullanımına yönelik tehditleri önlemeyi amaçlayan uluslararası siber güvenlik alanında stratejik işbirliğinin geliştirilmesi ve ortaklıkların güçlendirilmesi.

Doktrinde, bilgi güvenliği üzerindeki etkileri dikkate alınmadan bilgi teknolojilerinin benimsenmesinin bilgi tehditlerinin olasılığını önemli ölçüde arttırdığı belirtilerek Rusya'nın bilgi altyapısını askeri amaçlar için etkilemek isteyen yabancı ülkelerden algılanan tehditlere göre belirlenen karşı tedbirlerle ilgili esaslar konmuştur.

Siber güvenlik kapsamında ülke güvenliğini de olumsuz yönde etkileyen ve tedbir alınması gerektiği belirtilen önemli risk ve tehditler şunlardır.

- Bazı devletlerin istihbarat servislerinin, dünyadaki çeşitli bölgelerdeki iç politik ve sosyal durumu istikrarsızlaştırmak, egemenliğini baltalamak ve diğer Devletlerin toprak bütünlüğünü ihlal etmek amacıyla bilişim teknolojileri ve psikolojik harekât araçlarını giderek daha fazla kullanmaları, bu faaliyetlere dini, etnik ve insan hakları örgütleri yanı sıra çeşitli toplulukların ve örgütlerin de bilgi teknolojilerini yoğun bir şekilde kullanarak bu faaliyetlere katılmaları,

- Çeşitli terörist ve aşırılık yanlısı örgütler, etnik ve toplumsal gerilimleri tetiklemek, etnik veya dini nefreti veya düşmanlığı kışkırtmak, aşırılık yanlısı ideolojiyi yaymak, terörist faaliyetlerin yeni destekçilerini işe almak için bireysel, grup ve halk bilincini etkilemek için yaygın olarak bilgi araçlarını kullanmaları, kritik bilgi altyapı nesnelerini yasa dışı amaçlarla etkilemek için yıkıcı araçlar geliştirmeleri,

- Bilgisayar suçlarında, özellikle kredi ve finansal alanda bir artış olması, bilgi teknolojilerinin kullanımıyla kişisel verilerin işlenmesinde gizlilik, kişisel ve aile hayatı da dâhil olmak üzere anayasal hak ve özgürlüklerin ihlaliyle ilgili suçların sayısının artması, bu tür suçları işlemek için kullanılan araç ve yöntemlerin gittikçe daha karmaşık hale gelmesi,

- Yerli sanayinin elektronik bileşenleri olan yazılımlar, bilgisayarlar ve iletişim cihazları gibi konularda yabancı bilgi teknolojilerine bağımlılığının yüksek düzeyde olması, bunun da RF'nin sosyoekonomik gelişimini yabancı ülkelerin jeopolitik çıkarlarına bağımlı kılması,

- Bilim, teknoloji ve eğitim alanındaki bilgi güvenliği kapsamında, gelişmiş bilgi teknolojileri oluşturmak için tasarlanmış bilimsel araştırmalarda, ulusal teknolojilerin sınırlı kullanımı ve bilgi güvenliği alanındaki personel eksikliğinin yanı sıra daha fazla etkinliğe ihtiyaç duyulması, kişisel bilgi güvenliği ile ilgili kamuoyu bilincinin düşük olması, aynı zamanda, iç bilgi teknolojisi ve ürünleri kullanılarak bütünlüğü, kullanılabilirliği ve erişebilirlik dâhil olmak üzere bilgi altyapısının güvenliğini sağlamak için kapsamlı bir çerçeve olmaması,

- Bazı Devletlerin bilgi üstünlüğüne hükmetmek için teknolojik üstünlüklerini kullanma isteklerinin stratejik istikrar ve adil stratejik ortaklık alanındaki bilgi güvenliğinin sağlanması konusunda RF ve müttefikleri için uluslararası barış, küresel ve bölgesel güvenlik için bir tehdit oluşturması.

İnternet'in güvenli ve istikrarlı bir şekilde çalışmasını sağlamak için gereken kaynakların mevcut küresel dağılımı göz önüne alındığında, bunların ortak ve adil bir şekilde yönetilmesi mümkün değildir. Ayrıca vatandaşların haklarının ve özgürlüklerinin korunması ve gizliliği ilkelerinin korunması yanında, RF bilgi altyapısının sürdürülebilir ve kesintisiz işleyişine olan ihtiyacı ve özellikle hem barış zamanında hem de doğrudan tehdit ve saldırganlık dönemlerinde olduğu gibi, birleşik iletişim ağının kurularak emniyetle işletilmesi, siber suçlarla mücadelenin güçlendirilmesi gibi önemli hedefler belirlenmiştir.

RF askeri politikası, ulusal savunma alanında bilgi güvenliğinin sağlanmasında kilit durumunda alanlar aşağıdaki şekilde sıralanmıştır.

- Bilgi teknolojilerinin kullanılmasıyla stratejik caydırıcılığı sağlamak ve askeri çatışmaları önlemek,
- RF silahlı kuvvetlerinin, diğer askeri oluşumların ve organların bilgi güvenliği sisteminin iyileştirilmesi,
- Bilgi alanındaki RF silahlı kuvvetlerine yönelik tehditler dâhil olmak üzere bilgi tehditlerini tahmin etmek, tanımlamak ve değerlendirmek,
- RF müttefiklerinin bilgi alanındaki çıkarlarını korumak,
- Vatanı savunmaya, tarihi vakıflara ve yurtsever geleneklere zarar vermeyi amaçlayanlar da dâhil olmak üzere bilgi harekâtını ve psikolojik harekâtı önlemek.

RF devlet ve kamu güvenliği ile ilgili bilgi güvenliğinin ana itici güçleri on maddede sıralanmıştır.

- Aşırılık yanlısı ideolojileri ve eylemleri desteklemek için bilgi teknolojilerinin kullanılmasının engellenmesi,
- RF'nin ulusal güvenliğine zarar veren, yabancı devletlerin özel hizmetleri ve kuruluşları ile teknik araç ve bilgi teknolojilerini kullanan bireyler tarafından yürütülen faaliyetlerin bastırılması,
- Kritik altyapı bilgilerinin korunmasının ve işleyişinin güvenilirliğinin arttırılması,
- RF'nin birleşik iletişim ağının güvenliğinin sağlanması da dâhil olmak üzere, Hükümet organları arasında düzenli ve güvenli bir etkileşimin sağlanması,
- Silahların, askeri ve özel teçhizatın ve otomatik kontrol sistemlerinin güvenli ve emniyetli bir şekilde çalışmasının geliştirilmesi,

- Bilgi teknolojilerinin kullanılmasını içeren suçların önlenmesinin etkinliğinin arttırılması,
- Devlet sırrını oluşturan bilgileri ve ilgili bilgi teknolojilerinin güvenliğini artırmak da dâhil olmak üzere diğer sınırlı erişim ve yayma bilgilerinin korunması,
- Sanayide imalat ve güvenli kullanım yöntemlerinin ve tekniklerinin geliştirilmesi ve bilgi güvenliği gerekliliklerine uygun yerli bilgi teknolojilerine dayalı hizmetlerin sağlanması,
- RF devlet politikasını uygulamak için bilgi destek faaliyetlerinin geliştirilmesi,
- Rusya'nın geleneksel manevi ve ahlaki değerlerini aşındırmaya yönelik bilgi harekâtının etkisiz hale getirilmesi.

Ekonomi alanında bilgi güvenliğinin sağlanmasının ana itici güçleri ise şu şekilde sıralanmıştır.

- Bilgi teknolojileri ve elektronik sektörünün yenileşimci gelişimini desteklemek ve ürünlerinin yurtiçi gayri safi hâsıla ve ihracat içindeki payının artırılması,
- Rus çözümlerinin yaratılması, geliştirilmesi ve yaygınlaştırılması ve yerli sanayilerin yabancı bilgi teknolojilerine ve bilgi güvenliği araçlarına bağımlılığının ortadan kaldırılması,
- RF bölgesinde bilgi güvenliği araçları üretim ve işletimi konusunda uygun çalışma ortamı oluşturarak bilgi güvenliği hizmetleri sağlayan elektronik şirketlerinde çalışan Rus şirketlerinin yarışabilirliğinin arttırılması,
- Elektronik bileşenlerin üretilmesi yarışmacı bir yerli elektronik bileşen tabanı ve teknolojileri geliştirilmesi, bu tür ürünlerdeki iç pazarın ihtiyaçlarının karşılanması ve bunların küresel pazarda tanıtımı.

RF'de bilim, teknoloji ve eğitimde bilgi güvenliğini sağlamanın stratejik amacı, bilgi güvenliği sisteminin yanı sıra bilgi teknolojileri ve elektronik sektörünün yenilikçi ve hızlandırılmış gelişimini desteklemek olarak kabul edilmiştir. Bu çerçevede bilim, teknoloji ve eğitimde bilgi güvenliğinin sağlanmasının ana itici güçleri şu şekilde belirlenmiştir.

- Rus bilgi teknolojilerini rekabetçi kılmak ve ülkenin bilgi güvenliğinin bilimsel ve teknolojik yeteneğini geliştirmek,
- Çeşitli etki türlerine dirençli olan bilişim teknolojilerini geliştirmek ve uygulamak,

- İleriye dönük bilgi teknolojileri ve bilgi güvenliği araçları üretmek amacıyla araştırma ve geliştirme yapmak,
- Bilgi güvenliği ve bilgi teknolojilerinin kullanımı alanında insan kaynakları geliştirmek,
- Kişisel bilgi güvenliği kültürünü teşvik etmek de dâhil olmak üzere vatandaşları bilgi tehditlerinden korumak.

Stratejik istikrar ve eşit stratejik ortaklık alanındaki bilgi güvenliğinin stratejik hedefi, bilgi alanında çatışmasız bir devletlerarası ilişkiler sistemi oluşturmaktır. Stratejik istikrar ve eşit stratejik ortaklık alanında bilgi güvenliğinin sağlanmasının ana itici güçleri şunlardır.

- Ulusal ve bağımsız politika yoluyla Rusya Federasyonu'nun bilgi alanındaki ulusal çıkarları takip etmek ve bilgi alanındaki egemenliğini korumak,
- Uluslararası hukuka aykırı olarak siyasi, askeri veya terörist, aşırılık yanlısı vb. yasa dışı amaçlarla bilgi teknolojilerinin kullanımını engellemek için uluslararası bir oluşum kurmak,
- Bilişim teknolojilerinin kendine özgü doğasını göz önünde bulundurarak ve Devletlerarasındaki anlaşmazlıkları önlemek ve bilgi alanlarına yerleştirmek amacıyla uluslararası yasal düzenler geliştirmek,
- Uluslararası örgütlerde RF için tüm ilgili taraflara bilgi alanındaki eşit ve karşılıklı yarar sağlayan işbirliğini savunan konumlarını desteklemek,
- Rus Ulusal İnternet sistemini geliştirmek.

- **RF siber güvenlik / savunma teşkilat yapısı** [175, 176]

RF'de ulusal güvenlik sisteminin önemli bir parçası olarak kabul edilen bilgi güvenliği sistemi strateji ve politikalarının oluşturulması ve etkinlikle uygulanması için yapılanma, yetki, görev ve sorumluluklar da RF Başkanlığınca belirlenmiştir. Bilgi güvenliği bu bakış açısıyla yasama, adli, gözetim, kolluk kuvvetleri ve yerel yönetimler ile kuruluşlar ve vatandaşlar işbirliğiyle çalışan devlet organlarının faaliyetlerinin bir araya getirilmesiyle sağlanmaktadır.

Bilgi güvenliği sisteminin kurumsal çerçevesinin strateji belgesinde şu şekilde oluşacağı belirtilmiştir.

RF Meclisi Konseyi, Devlet Duması, Hükümet, Güvenlik Konseyi, Yürütme organları, Merkez Bankası, Askeri-Sanayi Komisyonu, Başkanlık ve Hükümet tarafından kurulan kurumlar arası organlar, Kurucu kuruluşların yürütme organları, Yerel yönetimler ve adli organlar yasalarına uygun olarak bilgi güvenliği faaliyetlerinde bulunmaktadır.

RF Bilgi Güvenliği Sistemi kritik altyapı nesnelerinin ve bu nesneleri işleten organizasyonların sahipleri, kitle iletişim sistemi ve araçları, para, döviz, bankacılık ve diğer finansal kuruluşlar, İletişim işleticileri, bilgi sistemi işleticileri, bilgi ve iletişim sistemleri yaratan ve işleten kuruluşlar, bilgi güvenliği araçları geliştiren, üreten ve işleten kuruluşlar, bilgi güvenliği hizmetleri sunan kuruluşlar, bu alanda eğitim hizmeti veren kuruluşlar, kamu dernekleri ve bilgi güvenliği konusunda kanunlar uyarınca çalışan diğer kuruluşlar ve bireylerden oluşmaktadır.

Devlet kurumlarının bilgi güvenliği faaliyetlerinin dayandığı ilkeler;

- Halkla ilişkilerin bilgi alanındaki yasallığı ve vatandaşların anayasal haklarından kaynaklanan her türlü katılımcının yasal eşitliği, hukuki yollarla serbestçe bilgi alma, alma, iletme, üretme ve yayma,
- Bilgi güvenliği görevleriyle uğraşırken devlet kurumları, kuruluşlar ve vatandaşlar arasında yapıcı etkileşim,
- Vatandaşların bilgi alışverişinde serbest bırakılma talebi ile bilgi güvenliği dâhil olmak üzere ulusal güvenlikle ilgili kısıtlamalar arasında bir denge sağlamak,
- Bilgi güvenliği güçlerinin ve diğerlerinin yanı sıra, bilgi tehditlerinin sürekli izlenmesi yoluyla belirlenen araçların yeterliliği,
- Evrensel olarak kabul görmüş uluslararası hukuk ilkeleri ve değerlerine, RF'nin taraf olduğu uluslararası anlaşmalara ve RF yasalarına uymak şeklinde tanımlanmıştır.

Hükümet organlarının bilgi güvenliği alanındaki hedefleri;

- Bilgi alanındaki vatandaşların ve kuruluşların haklarını ve meşru çıkarlarını korumak,
- Bilgi güvenliği durumunu değerlendirmek, bilgi tehditlerini tahmin etmek ve tanımlamak, önlenmesi için öncelikli alanları belirlemek ve etkilerini gidermek,
- Bilgi güvenliği önlemlerinin etkinliğini planlamak, uygulamak ve değerlendirmek,

- Faaliyetleri düzenlemek ve bilgi güvenliği güçlerinin etkileşimini koordine etmek ve yasal, örgütsel, operasyonel araştırma, istihbarat, zekâ, bilimsel ve teknik, bilgi ve analitik, personel ve ekonomik desteklerini geliştirmek,
- Bilgi güvenliği araçlarını geliştiren, üreten ve işleten kuruluşlara, bilgi güvenliği hizmeti veren kuruluşlara ve bu alanda eğitim hizmeti veren kuruluşlara devlet desteği önlemleri geliştirmek ve uygulamak şeklinde belirlenmiştir.

Hükümetin bilgi güvenliği sistemini geliştirme ve iyileştirme hedefleri ise;

- Dikey yönetim sisteminin güçlendirilmesi ve bilgi güvenliği güçlerinin federal, bölgeler arası, bölgesel ve yerel yönetim seviyelerinin yanı sıra bilgi teknolojileri nesneleri ve bilgi sistemleri ve iletişim ağı işletmecileri düzeyinde merkezileştirilmesi,
- Düzenli tatbikatlar dâhil olmak üzere bilgi tehditlerine karşı hazırlıklı olmalarını geliştirmek için bilgi güvenliği güçleri arasındaki etkileşimin formlarını ve yöntemlerini geliştirmek,
- Bilgi güvenliği sisteminin işleyişinin bilgiyi, analitik ve bilimsel ve teknik yönlerini geliştirmek,
- Bilgi güvenliği görevlerini yerine getirmek için devlet kurumları, yerel yönetimler, kuruluşlar ve vatandaşlar arasındaki etkileşimin etkinliğini artırmak şeklinde sıralanmıştır.

Doktrin, RF'nin sektörel stratejik planlama dokümanlarına uygun olarak uygulanır. RF Güvenlik Konseyi, RF için stratejik görünümün hükümlerini dikkate alarak orta vadeli öncelikli bilgi güvenliği alanlarının bir listesini oluşturarak belgenin güncel tutmasını sağlar. Doktrinin uygulanmasının izlenmesinin bulguları, ulusal güvenlik raporuna Güvenlik Konseyi Sekreteri tarafından RF Başkanına sunulan iyileştirme önlemlerine dâhil edilir.

5.4.4 Fransa siber güvenlik stratejisi

Casusluk, propaganda, terörizm ve bilgi çarpıtma konularında yeni suç alanları ile haksız bir mücadele ortamı durumuna gelen siber uzayda Fransız Hükümetinin temel amacının sayısallaşan Cumhuriyet değerleri ile vatandaşların ve ekonominin korunması olduğu belirtilmiştir. Sayısal güvenliği pekiştirerek, Fransız şirketleri için sürdürülebilir bir büyüme ve fırsat kaynağı sağlayan bir siber ortamın gelişmesinin desteklenmesi, böylece demokratik değerlerin ortaya konularak vatandaşların kişisel verileri ile sayısal yaşamları da korunmuş olacaktır. Bu çerçevede Fransa'nın ulusal

sayısal güvenlik stratejisinde, özellikle eğitim ve uluslararası işbirliği sağlanması konuları önemsenmektedir. [177]

Kamu makamlarınca Fransa'nın bilişim teknolojilerine bağımlılığının ele alınarak çözümler üretilmesi çerçevesinde siber alan açısından kapsamlı bir strateji görevi gören üç adet üst düzey strateji ve politika belgesi hazırlandığı görülmektedir. [178]

- **Ulusal savunma ve güvenlikle ilgili Beyaz Kitap (2008)** [179]

Ulusal güvenlik kapsamında siber uzay ve siber güvenlik konusunun ilk önce 2008 yılında yayınlanan Savunma ve Ulusal Güvenlik Beyaz Kitabında yer aldığı görülmektedir. Bu resmi belgede siber tehditler devlet dışı aktörler, bilgisayar korsanları veya suç örgütleri tarafından yapılan saldırılar olarak ele alınmış ve bu tehditlere karşı geliştirilmesi gereken tedbirler ile atılması gereken adımlar belirtilmiştir. Güvenlik boyutuyla stratejinin, bilgi ve öngörü, caydırıcılık, korunma, önleme ve müdahale başlıkları altında oluşturularak uygulanacağı vurgulanmıştır. Belirlenen eylemler doğrultusunda ilk adım olarak, 2009 yılında, Fransız hükümetinde siber güvenlik için merkezi koordinasyon otoritesi olarak siber saldırıların ele alınması, devlet bilgi sistemlerinin ve kritik altyapıların korunması için görev yapmak üzere Başbakana bağlı, Savunma ve Ulusal Güvenlik Genel Sekreteri denetiminde 'Ulusal Ağ ve Bilgi Güvenliği Ajansı' kurulmuştur.

- **Fransa'nın siber stratejisi (2011)** [180].

Savunma ve Ulusal Güvenlik Genel Sekreterinin denetiminde Ulusal Ağ ve Bilgi Güvenliği Ajansına verilen görevlerden biri bir siber güvenlik stratejisi hazırlanması olmuştur. 2010 yılından hazırlanan 'Fransa'nın Bilgi Sistemleri Savunma ve Güvenlik Stratejisi' Şubat 2011'de, ana odak noktasının ulusal bilgi varlıklarının ve kritik altyapıların korunmasının olduğu vurgulanarak dört ana hedef başlığı altında yayımlanmıştır.

- Siber savunmada bir dünya gücü olunması,
- Fransa'nın egemenliğine ilişkin bilgilerin korunması yoluyla karar alma yeteneğinin güvenceye altına alınması,
- Ulusal kritik altyapıların siber güvenliğinin güçlendirilmesi,
- Siber alanda güvenliğin sağlanması.

- **Ulusal savunma ve güvenlikle ilgili Beyaz Kitap (2013)** [181]

Fransa Cumhurbaşkanı tarafından 2012'de Fransa'nın siber uzaydaki güvenlik durumu da dâhil olmak üzere jeopolitik zorlukları ve mali kısıtlamaları içeren bir çalışma yapılması isteği doğrultusunda, 29 Nisan 2013 tarihinde ulusal savunma ve güvenlik üzerine yeni bir Beyaz Kitap yayımlanmıştır. Beyaz Kitapta, güvenli bir siber alan elde etmek için yapılması gereken çalışmalar ortaya konmuş ve bu alana tahsis edilecek kaynaklar belirtilmiştir.

Bu kapsamda ilk önce Ekonomi Bakanlığınca Eylül 2013'te 'Sanayileşmiş Fransa'yı Yeniden Fethetmek' için başlatılan bir projeyle Ulusal Bilgi Sistemleri Güvenlik Kurumu Direktörlüğünün öncülüğünde Fransa'da siber güvenliğin geliştirilmesini hedefleyen bir plan hazırlanmıştır. Planda, Fransız toplumunun sayısallaşmasının, artan ve büyüyen sayısal hizmetler, ürünler ve işlerle gittikçe hızlandığı, sayısallaşmaya geçişin yenileşim ve büyümeyi desteklediği, ancak aynı zamanda devlet, ekonomik paydaşlar ve vatandaşlar için riskler taşıdığı, siber suçların, casusluk, propaganda, sabotaj ve kişisel verilerin aşırı kullanımının sayısal güvenliği ve güvenilirliği tehdit ettiği hususları vurgulanarak, bu tehditlere karşı koymak için beş stratejik amaç (A) belirlenmiştir.

A1. Devletin siber alandaki rolü, Fransa'nın düşünce fikir ve eylem özgürlüğünün yanı sıra, büyük bir siber saldırı durumunda kritik altyapılarının güvenliğinin sağlanması,

A2. Vatandaşların ve işletmelerin sayısal yaşamlarını korumak ve siber suçlarla mücadele edilmesi,

A3. Sayısal güvenlik için gerekli eğitim ve öğretimin sağlanması,

A4. Sayısal teknolojiye güvenmek için elverişli bir ortamın geliştirilmesine katkıda bulunulması,

A5. Sayısal stratejik özerkliğinin ortaya çıkmasına elverişli bir şekilde, ulusal değerlerden daha güvenli ve daha saygılı bir siber alanın uzun vadeli garantörü bir Avrupa Birliği için Üye Devletlerarasında işbirliğinin teşvik edilmesi.

Belgede konuyla ilgili olarak dikkat çeken en önemli bölüm ise Fransız siber savunma stratejisinin bir parçası olarak taarruzi siber yeteneklerin geliştirilmesinin açıkça belirtilmiş olmasıdır. Belgede belirtilen esaslar doğrultusunda Savunma

Bakanlığınca 7 Şubat 2014 tarihinde altı hedefi (H) içeren ‘Siber Savunma Paktı’ yayımlanmıştır.

H1. Bakanlığın ve ortaklarının savunma ve müdahale olanaklarını güçlendirerek bilgi sistemlerinin güvenliğinin artırılması,

H2. Fransa’nın sanayi temelini desteklerken, teknik, akademik ve operasyonel alanlarda araştırma çabalarının yoğunlaştırılması yoluyla geleceği hazırlayarak siber güvenlik araştırmalarının artırılması,

H3. Siber savunmaya adanmış insan gücünün güçlendirilmesi ve ilgili kariyer yollarının geliştirilmesi için eğitim ve öğretim hizmeti verilmesi,

H4. Bakanlığın ve ulusal siber savunma topluluğu için siber savunma merkezinin geliştirilmesi,

H5. Avrupa'da, NATO içinde veya stratejik ilgi alanlarında yabancı ortaklar ağı kurarak uluslararası işbirliğinin geliştirilmesi,

H6. İş birliğine ve yedek ağlara dayanan ulusal bir siber savunma topluluğunun ortaya çıkmasının sağlanması.

- **Fransa siber güvenlik / savunma teşkilat yapısı** [178]

Fransa’nın siber güvenlik strateji ve politikalarının oluşturulması ve uygulanması görevi Başbakana bağlı, Savunma ve Ulusal Güvenlik Genel Sekreteri denetiminde, siber alanda olumsuzlukları ile kritik altyapı bilişim sistemlerine yönelik saldırıları tespit etmek ve önlemek, servis sağlayıcılarını sistemlerinde bulunan güvenlik açıkları konusunda uyarmak amacıyla kurulan Bilgi Sistemleri Güvenliği Operasyon Merkezi'ni de işleten Ulusal Ağ ve Bilgi Güvenliği Ajansı ile Bilgi Sistemleri Güvenliği Stratejik Komitesi tarafından yürütülmektedir.

Bilgi Sistemleri Güvenliği Stratejik Komitesi, Bakanlıklar arası koordinasyonu sağlayan Savunma ve Ulusal Güvenlik Genel Sekreteri gözetiminde bilgi sistemlerinin güvenliği ile ilgili önlemleri koordine etmekten ve uygulamaktan sorumludur ve aşağıdaki üyelerden oluşturulur.

- Genelkurmay Başkanı,
- İçişleri Bakanlığı Genel Sekreteri,
- Dış İşleri ve Avrupa Bakanlığı Genel Sekreteri,

- Savunma Tedarik Ajansı Direktörü,
- Dış İstihbarat Direktörü,
- Savunma Bilgi ve İletişim Sistemleri Direktörü,
- Devletin Bilgi ve İletişim Sistemlerinin Bölümler arası Direktörü,
- Kamu Politikalarının Modernizasyonu ve Halkla İlişkiler Direktörü,
- İç İstihbarat Daire Başkanı,
- Ekonomi, Endüstri, Enerji ve Teknoloji Ulusal Konseyi Eş Başkanı,
- Ağ ve Bilgi Güvenliği Ajansı Direktörü.

Ayrıca Fransa Savunma Bakanlığı, bilgi egemenliğini garanti altına alarak ulusal savunma sistemlerinin bütünlüğünü ve güvenilir bilgilere dayanarak etkin karar verme kapasitesini korumak için savunma ağlarının ve bilgi sistemlerinin savunmasından sorumludur.

Bakanlık saldırı tespiti ve önleme görevleri yanında siber harekâta yönelik görevlerle birlikte bu sorumluluğunu Genelkurmay Muhabere ve Bilgi Sistemler Başkanlığına bağlı Siber Savunma Müdürlüğü ve taktik birimleri ile yerine getirmektedir.

5.4.5 İngiltere siber güvenlik stratejisi

İngiltere Kabinesi, siber alanda güvenlik, güvenilirlik ve esnekliğin sağlanması maksadıyla 2009 yılında ilk Ulusal Siber Güvenlik Stratejisini Kabul ederek uygulamaya koymuştur. Stratejide siber saldırıların olasılığını ve etkisini dikkate alarak, siber alanda yaşanması olası riskleri en yüksek ulusal güvenlik risklerinden biri ve siber tehditleri de nükleer saldırı tehdidinden daha yüksek bir sınıflandırma olarak değerlendirmiştir.

Ulusal Siber Güvenlik stratejisi, 2011 ve 2015 yıllarında siber güvenlik için stratejik bakış açısıyla ana ilkeler ile birlikte somut hedefler ve gerekli eylemler, grev ve sorumluluklar belirlenerek yenilenmiştir. [182]

- **Ulusal Siber Güvenlik Stratejisi (2016-21)** [183]

Ulusal Siber Güvenlik Stratejisi, bilişim sistemlerini ve altyapılarını savunmak, saldıranları caydırmak ve büyük şirketlerden bireysel vatandaşlara tüm toplumun siber alandaki yeteneklerini geliştirmek için İngiltere'yi hızlı ve hareketli bir sayısal dünyada kendinden emin, yetenekli ve esnek kılma planını belirlemeyi amaçlamıştır.

Strateji belgesinde tehditler ve güvenlik açıkları tanımlanırken Uygulama Planı savunma, caydırma ve geliştirme başlıkları altında ele alınmıştır.

- Savunma;
  - Aktif siber savunma,
  - Daha güvenli bir internet oluşturma,
  - Hükümeti koruma,
  - Ulusal kritik altyapıyı ve diğer öncelikli sektörleri koruma,
  - Kamu ve iş davranışlarını değiştirme,
  - Olayları yönetmek ve tehdidi anlama.
- Caydırma;
  - Siber ortamda caydırıcılık,
  - Siber suçu azaltma,
  - Terörizmi önleme,
  - Düşman aktörler,
  - Siber taarruz yeteneklerinin geliştirilmesi,
  - Şifreleme yeteneklerin geliştirilmesi,
- Geliştirme
  - Siber güvenlik becerilerinin güçlendirilmesi,
  - Siber güvenlik sektöründe büyümeyi teşvik etme,
  - Siber güvenlik bilimini ve teknolojisini teşvik etme,
  - Etkili ufuk taraması.

Strateji, Hükümet'in yetkilerinin siber alanda hareket etmede sınırlı olduğunu ve bu nedenle sanayi ve akademi ile yakın işbirliğinin gerekli olduğunu vurgulamakta ve dört ana hedefi (H) içermektedir.

H1. Siber suçlarla mücadele etmek ve siber alanda iş yapmak için dünyanın en güvenli yerlerinden biri olmak,

H2. İngiltere'yi siber saldırılara daha dayanıklı kılmak ve siber alandaki çıkarları daha iyi koruyabilmek,

H3. İngiltere halkının güvenle kullanabileceği, açık, dengeli ve canlı bir siber ortamın oluşturulmasını sağlamak,

H4. Tüm siber güvenlik hedeflerinin temelini oluşturmak için ihtiyaç duyulan en üst düzeyde bilgi, beceri ve yetkinliğe sahip olmak,

Stratejide yerine getirilmesi öngörülen politikalar şöyle sınırlanmıştır.

- Uluslararası siber güvenlik kapasitesinin artırılması,
- Tehditlerin tespit ve analiz edilerek ağları güçlendirilmesinin sağlanması
- Ulusal Siber Suçlarla Mücadele Biriminin kurulması,
- Siber beceri, eğitim ve mesleki fırsatların geliştirilmesi,
- Siber güvenlik sektöründe ekonomik büyümenin özendirilmesi,
- Asgari standart ve ilkelere göre sanayinin geliştirilmesi,
- Siber güvenlik bilgi paylaşım ve işbirliğinin sağlanması,
- İşletmeler ve halk için siber güvenlik desteği sağlanması.

- **İngiltere siber güvenlik / savunma teşkilat yapısı** [182, 183]

Siber güvenlikle ilgili örgütsel reformların ve yapılanmaların çoğu, 2009 ulusal siber güvenlik stratejisinin kabul edilmesinden sonra gerçekleştirilmiştir. Netlik açısından, siber güvenlik strateji ve politikalarının oluşturulması ve uygulanması üç temel iş akışına ayrılmıştır.

- Stratejik bilgi varlıkları önceliklerin belirlenmesi ve politikaların koordinasyonu (Kabine, Siber Güvenlik ve Bilgi Güvencesi Ofisi)

Ulusal Güvenlik Konseyi'ne siber alanın korunmasına ilişkin öncelikleri belirleme konusunda destek verilmesi, stratejik hedeflerin belirlenmesi ve siber güvenlik ve bilgi güvencesini arttırmaya yönelik eylemlerin koordine edilmesi görevlerini içermektedir.

- Ulusal güvenlik istihbaratları (Devlet İletişim Karargâhı)

Devletin siber tehditlere ve saldırılara karşı korumak amacıyla hükümet tarafından görevlendirilen güvenlik ve istihbarat kurumu görevleri ile siber güvenlik ve istihbarat konusunda danışmanlık faaliyetlerini içermektedir.

- Siber savunma (Savunma Bakanlığı)

Askeri siber savunma iş akışı, savunma politikası ve doktrin dâhil olmak üzere siber alanın askeri maksatlı kullanımı faaliyetleri Savunma Bakanlığı tarafından yönetilmektedir. Bakanlığın siber politikası, Siber Güvenlik Stratejisinin yol gösterici ilkelerini izler ve uygun olduğunda, uyumlu yaklaşımlarını sağlamak için, Siber

Güvenlik ve Bilgi Güvencesi Ofisi ile Devlet İletişim Karargâhı ve diğer bakanlıklarla koordineli olarak hareket eder. Savunma Bakanlığı bünyesinde aktif siber savunma dâhil siber güvenlik faaliyetlerinin yürütülmesinde, siber yeteneklerin test edilmesi ve geliştirilmesi Genelkurmay Başkanlığı içerisindeki 'Siber Savunma Operasyon Grubu' sorumludur.

5.4.6 İsrail siber güvenlik stratejisi

Siber güvenlik, Kasım 2010'da Başbakan'ın Bilim Bakanlığı bünyesindeki Ulusal Araştırma ve Geliştirme Konseyi'nin himayesinde bir 'Ulusal Siber Girişim' tanıtımı ile açık ve belirgin bir ulusal hedef haline gelmiştir.

Bu girişimle, Ulusal Araştırma ve Geliştirme Konseyi Başkanı tarafından yönetilen, silahlı kuvvetler, bakanlıklar, üniversiteler ve özel sektörden yaklaşık seksen uzman temsilciden oluşan çok disiplinli görev gücü oluşturulmuştur. 'Girişim' görev gücü Başbakan tarafından küresel düzeyde siber güvenlik alanında İsrail liderliğini teşvik etmek için önlemler önermekle görevlendirilmiş, altı aylık yoğun çalışmanın ardından sunulan önerilerle Ağustos 2011'de 'Ulusal Siber Yeteneklerin Geliştirilmesi' başlıklı 3611 sayılı Hükümet Kararı yayımlanmıştır.

Bu karar çerçevesinde, siber güvenlik için danışma ve geliştirme kurumu olarak görev yapacak 'Ulusal Siber Güvenlik Bürosu', daha sonra 'Ulusal Siber Güvenlik Gücü' ve bunların üzerinde Başbakanlığa bağlı olarak 'Siber Savunma Direktörlüğü' kurulmuş ve 2016 yılının sonlarına doğru siber alanda aşağıda sıralanan dört ulusal önceliği vurgulayan ulusal siber güvenlik strateji ve politikaları uygulamaya konulmuştur. [184]

- Ulusal kapasitelerin, mevcut ve gelecekteki siber alan zorluklarının yönetiminin geliştirilmesi,
- Dengeli ve üretken bir yaşam sürdürmek için gerekli olan ulusal altyapıların savunmasının geliştirilmesi,
- Ülkenin bilgi teknolojilerinin geliştirilerek küresel bir merkez durumuna getirlmesi,
- Bakanlıklar, üniversiteler, özel sektör ve sanayi kurumları arasında disiplinler arası işbirliğinin koordinesi ve desteklenerek geliştirilmesi.

Oluşturulan siber güvenlik strateji ve politikaları doğrultusunda savunma ve silahlı kuvvetler birimlerinde siber güvenlik ve savunma yapılanmasına gidilmiş ve Genelkurmay Başkanlığına siber savunma yanında siber taarruz yetenekleri de bulunan birimler oluşturulmuştur.

İsrail Savunma Kuvvetleri on yıllardır siber güvenlik sorunları ve siber tehditlerle ilgilenmekle birlikte, askeri alandaki güvenlik hususları ve politikaları kamuoyu ile paylaşılmadığı için ulusal siber güvenlik konularında ve politikalarındaki yaklaşımları tutarlı bilgiler azdır. Ağustos 2015'te Genelkurmay Başkanlığınca yayımlanan siber güvenlik strateji belgesinde, siber alanın askeri bir bölge olduğu, kamuoyu şeffaflığı gerektiği, kurumsal yenilikçilik ve devlet yatırımlarına teşvik sürecinin başlatılması vurgulanarak yapılması gerekenler;

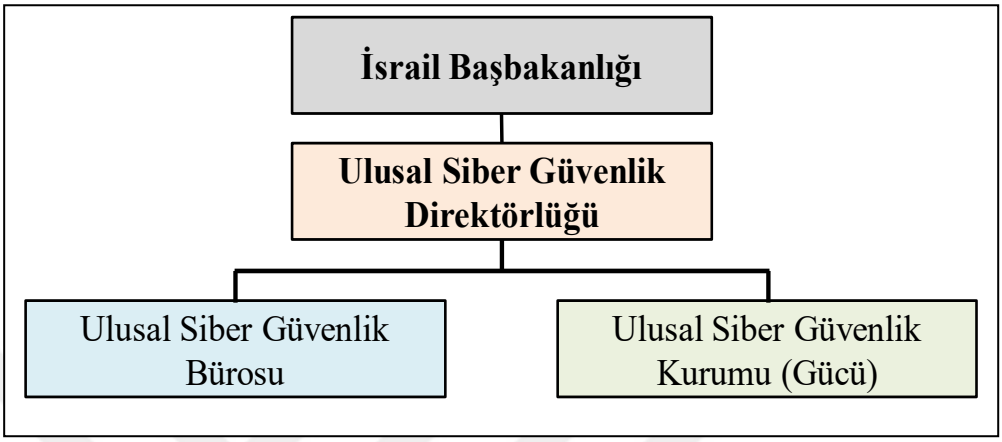
- Stratejik, operatif ve taktiksel seviyelerde siber savunma ve taarruz kapasitesinin geliştirilmesi,
- Siber tehdit farkındalığı yaratılması,
- Kurumsal düzeyde savunma gücü içerisinde siber güvenlik yönetim yapısını kurmak için bir sürecin başlatılması,
- Savaş ve acil durumlarda etkin bir siber savunmanın sağlanması şeklinde sıralanmıştır.

Aralık 2015'te, Siber Güvenlik Bürosu siber güvenlik mesleklerinin düzenlenmesi hakkında; politikanın temeli, İsrailli şirketlerin, devlet kurumlarının ve diğer kuruluşların belirli bir uzmanlık derecesine sahip güvenilir personeli kullanarak yüksek düzeyde siber güvenlik sağlayabilmelerinin gerekli olduğu vurgulanmış, ihtiyaç duyulan mesleklerde yetiştirilmesi gereken personel ve bunlarla ilgili ölçünler, esaslar ve yol haritalarını içeren bir politika belgesi yayımlanmıştır.

İsrail Avrupa Konseyi'nin 2001 Siber Suçlar Sözleşmesi'ne 1 Eylül 2016 tarihinde resmi olarak katılmış, birkaç ülke ve bazı uluslararası kuruluşlar ile siber güvenliğin teşvik edilmesi için iki taraflı işbirliğine dayanan ikili anlaşmalar imzalamıştır. Ulusal Siber Güvenlik Bürosu ile koordineli olarak, Dışişleri Bakanlığı iki ve çok taraflı düzeylerde siber güvenlik için temas ve işbirliği geliştirmekten sorumlu koordinatör olarak belirlenmiştir.

- **İsrail siber güvenlik / savunma teşkilat yapısı**

İsrail'in siber güvenlik strateji ve politikaları Başbakanlık ve direk bağlısı olan Ulusal Siber Güvenlik Direktörlüğü tarafından yürütülmektedir (Şekil 5.5). Direktörlüğün iki bağlısı 2011 yılında 3611 sayılı hükümet kararı ile kurulmuş olan İsrail Ulusal Siber Güvenlik Bürosu ile Şubat 2015'te kurulan Ulusal Siber Güvenlik Kurumudur.[184]



Şekil 5.5: İsrail ulusal siber güvenlik yönetimi.

Ulusal Siber Güvenlik Bürosu'nun görevi; siber güvenliği ulusal düzeyde pekiştirmek amacıyla Başbakan, bakanlıklar ve diğer resmi makamlara danışma organı olarak hizmet etmektir. Ulusal siber güvenlik politikasını önermekte ve hükümet genelinde uygulanmasını desteklemekte ve koordine etmektir.

Ulusal Siber Güvenlik Kurumu (Gücü) ise siber saldırılara karşı tam ve sürekli bir savunma sağlamak amacıyla, ulusal düzeyde siber alandaki tüm operasyonel savunma çabalarını bütünsel bir bakış açısıyla işleterek ve uygulayarak siber alanı savunmakla görevlendirilmiştir. Siber tehditleri ve olayları gerçek zamanlı olarak ele alarak analiz etmek, sürekli bir durumsal farkındalık oluşturmak, gerekli tedbirleri alarak geliştirmek ve pekiştirmekle görevlendirilmiştir.

Diğer görevleri Siber Olaylara Müdahale Merkezinin işletilmesi ve timlerinin görevlerini yapmalarının sağlanmasıdır. Bu kapsamda ülkenin hazırlıklılığını ve esnekliğini arttırmak, ulusal siber doktrin geliştirmek, mevcut yasaları değiştirecek ve yeni düzenlemeler getirerek siber güvenlik yasa ve politikalarının uygulanmasını sağlamaktır. Ayrıca diğer bakanlıklar da kendi görev sahalarıyla ilgili siber güvenlik düzenlemelerini yaparak kapasiteleri doğrultusunda uygulanmasını sağlamaktan sorumludurlar.

5.5 Türkiye'nin Siber Güvenlik Strateji ve Politikaları

Bilişim sistemlerinin etkinliğini ve sağladığı kazanımları artırmak, siber ortamdaki kritik altyapı bilişim sistemleri ile değerli varlıkların korunmasını ve siber gücün daha etkin kullanılmasını sağlamak için bütün dünyada strateji ve politikalar geliştirilmesi konusunda yapılan çok yoğun çalışmalara paralel olarak Türkiye'de de çalışmalara başlanmış ve günümüzde de sürdürülmektedir. Geçmişten bugüne konuyla ilgili yapılan önemli strateji ve politika çalışmaları ile planların bazıları Çizelge 5.2'de sunulmuştur.

Çizelge 5.2: Türkiye'nin önemli siber güvenlik stratejileri ve eylem planları.

S.No	Konu	Sorumlu Makam	Tarihi
1.	Bilgi Toplumu Stratejisi ve Eylem Planı	Kalkınma Bakanlığı	2006-10
2.	Ulusal Sanal Ortam Güvenlik Politikası	Sanayi ve Teknoloji Bakanlığı	2009
3.	Türkiye Siber Güvenlik Organizasyonu ve Yol Haritası	Sanayi ve Teknoloji Bakanlığı	2012
4.	Siber Güvenlik Kurulu Oluşumu	Ulaştırma ve Altyapı Bakanlığı	2012
5.	Ulusal Siber Güvelik Strateji ve Eylem Planı	Ulaştırma ve Altyapı Bakanlığı	2013-14
6.	Bilgi Toplumu Stratejisi ve Eylem Planı	Kalkınma Bakanlığı	2015-18
7.	Kişisel Verilerin Korunması Kanunu	Adalet Bakanlığı	2016
8.	Ulusal e-Devlet Stratejisi ve Eylem Planı	Ulaştırma ve Altyapı Bakanlığı	2016-19
9.	Ulusal Siber Güvenlik Strateji ve Eylem Planı	Ulaştırma ve Altyapı Bakanlığı	2016-19
10.	BTK'ya siber caydırıcılık sağlamak için her türlü tedbiri alma veya aldırma görevi verilmesi KHK	Ulaştırma ve Altyapı Bakanlığı	2016
11.	Türkiye Yazılım Sektörü Stratejisi ve Eylem Planı	Sanayi ve Teknoloji Bakanlığı	2017-19
12.	CB Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi	CB Dijital Dönüşüm Ofisi Bşk.lığı	2019

5.5.1 2003/10 Sayılı Başbakanlık Genelgesi (2003)

Türkiye'de siber güvenlikle ilgili faaliyet ve çalışmalar 17 Şubat 2003 tarihinde yayımlanan '2003/10 Sayılı Başbakanlık Genelgesi' [185] ile başlamıştır. Söz konusu genelgede, güvenlik kültürünü oluşturmayı amaçlayan ve OECD üyesi ülkelerin ortak tutumunu yansıtan rehber ilkelerin bilgi sistem ve ağlarına yönelik tehditler karşısında, her düzeydeki kullanıcılar tarafından benimsenip uygulanmasının yararlı olacağı belirtilerek, başta kamu kurum ve kuruluşları olmak üzere, bilgi sistem ve ağlarının korunması için yürütülen çalışmalarda göz önünde bulundurulması istenmiştir.

Bu genelgeyi, Devlet Planlama Teşkilatı tarafından 'E-Dönüşüm Türkiye Projesi (2003)' [186], Kalkınma Bakanlığı koordinasyonunda 'Bilgi Toplumu Stratejisi (2006)' [187], TÜBİTAK koordinasyonunda hazırlanan 'Ulusal Sanal Ortam Güvenlik Politikası (2009)' [188] takip etmiştir. Bu çalışmaların içeriğinde, siber güvenlikle

ilgili tespitler ve yol haritaları ortaya konmakla birlikte siber caydırıcılıkla ilgili dikkat çekici hususların bulunmadığı görülmektedir.

5.5.2 Bilişim suçları ve cezalarıyla ilgili yasal düzenlemeler

Bilgi ve iletişim sistemlerinde gelişmeler, bilişim sistemlerinin kullanımı ve internetin de yaygınlaşması zaman içerisinde suçların da cins, nitelik ve içeriklerinde değişikleri zorunlu kılmıştır. Bu kapsamda AB uyum yaslarının da getirdiği zorunlulukla Türkiye hukuk sisteminde ve ceza kanunlarında bilişim ve bilişimle ilintili alanlarda işlenen suçlarla ilgili olarak önce mevcut yasalara ek maddeler eklenmiş, daha sonra ihtiyaç durumuna göre özel yasalar çıkarılmış, suçların bilişim destekli ve internet ortamında işlenmesi durumunda niteliği yüksek kabul edilerek cezaları da artırılmıştır. Bu kapsamda değişiklik ve düzenleme yapılan yasalar aşağıda sıralanmıştır [189].

- Fikir ve Sanat Eserleri Kanunu (5846),
- Elektronik İmza Kanunu (5070),
- Türk Ceza Kanunu'nda bilişimle ilgili maddeler (TCK-5237)
- İnternet Kanunu (5651),
- Ceza Muhakemesi Kanunu ilgili maddeleri (CMK-5271),
- Kişisel verileri koruma kanunu (6563).

Yukarıda sıralanan yasalardan bilgisayar programlarının ilim ve edebiyat eserleri arasında olduğunun kabul edildiği Fikir ve Sanat Eserleri Kanunu (5846) değişikliği 2001 yılında, diğerleri 2004 yılı sonrasında yapılmıştır. Yasalarda bilişim ve bilişimle bağlantılı alanlarda suçların yeniden tanımlanması ve bilişim desteği ve bağlantısı dikkate alınarak cezaların artırılması siber suçlulara ve saldırganlara karşı önemli caydırıcılık sağlamıştır.

Ancak siber suçluların takibi, yakalanmaları, araştırma, sorgulama ve yargılama süreçleri ile ilgili yeni eğitim, teknoloji ve personel ihtiyaçlarını ortaya çıkarmıştır. Bu kapsamdaki eksiklik ve yetersizliklerin giderilmesi siber saldırılar ve suçlarla mücadelede başarıyı ve caydırıcılığı daha da artıracaktır.

5.5.3 Milli Güvenlik Kurulu Bildirisi (2010)

27 Ekim 2010 tarihli Milli Güvenlik Kurulu (MGK) Bildirisinde; "Siber tehdidin küresel düzeyde ulaştığı boyut ve bu tehdidin ulusal güvenliğe etkileri kapsamlı surette ele alınmıştır. Bu bağlamda, siber tehdidin engellenebilmesi için milli düzeyde

yürütülen çalışmalar değerlendirilmiştir. Siber tehditlere karşı önlem almaya yönelik kararlılık ve irade ortaya konmuştur" [190] ifadeleri yer almıştır. Ülkenin en üst ulusal güvenlik kurulunun bildirisinde yer alan bu ifadeler, siber tehditlere karşı önlem alınmasına yönelik kararlılık ve iradenin ortaya konduğunun vurgulanması ve bunun duyurulması, siber güvenliğin sağlanması yanında siber caydırıcılık açısından da önemlidir.

5.5.4 UDHB teşkilat ve görevleri (Bilgi toplumu stratejileri) KHK (2011)

Bakanlar kurulunun '26 Eylül 2011 tarih ve 655 sayılı Kanun Hükmünde Kararnamesi' ile Ulaştırma Denizcilik ve Haberleşme Bakanlığı (UDHB)'nın teşkilatı ile görev ve yetkileri düzenlenmiştir [191]. Yapılan düzenleme ile Bakanlığa verilen görevlerden birisi (Md.2, f): "Bilgi toplumu politika, hedef ve stratejileri çerçevesinde;

- İlgili kamu kurum ve kuruluşlarıyla gerekli işbirliği ve koordinasyonu sağlayarak e-Devlet hizmetlerinin kapsamı ve yürütülmesine ilişkin usul ve esasları belirlemek,
- Bu hizmetlere ilişkin eylem planları yapmak, koordinasyon ve izleme faaliyetlerini yürütmek, gerekli düzenlemeleri yapmak ve bu kapsamda ilgili faaliyetleri koordine etmek." şeklinde belirlenmiştir.

Bilgi toplumu politikaları, hedef ve stratejilerinden sorumlu bir makamın belirlenmesinin, bu konularda eksikliklerin giderileceğini düşündürmesi açısından olumlu bir adım atılmıştır. Müteakiben siber güvenlik konusunda çalıştay ve tatbikatların yapılması, kamu kurumlarında yapılanmaya gidilmesi ve 2012 yılında siber güvenlik yol haritasının ortaya konması bu tespiti destekler niteliktedir.

5.5.5 Türkiye Siber Güvenlik Organizasyonu ve Yol Haritası (2012)

TÜBİTAK tarafından hazırlamış ve TBMM Bilişim ve İnternet Araştırma Komisyonuna sunulan belgede siber güvenliğe yönelik teşkilatlanma ve yol haritası beş ana başlıkta toplanmıştır [88].

- Ulusal Siber Güvenlik Kurulunun kurulması,
- Siber güvenlik konusunda yasal düzenlemelerin yapılması,
- Ulusal siber güvenlik altyapısının güçlendirilmesi,
- Ulusal siber güvenlik yeteneklerinin geliştirilmesi,
- Siber güvenlikte ulusal işbirliğinin sağlanması.

5.5.6 Ulusal siber güvenlik çalışmalarının yürütülmesi, yönetilmesi ve koordinasyonuna ilişkin Bakanlar Kurulu kararı (2012)

Bakanlar Kurulunun 'Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin' 20 Ekim 2012 tarih ve 2012/3842 sayılı kararı [192] ile Siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla; UDH Bakanı başkanlığında 'Siber Güvenlik Koordinasyon Kurulu' kurulmuş ve bu kapsamda siber güvenliğe yönelik ilkeler, teşkilat, görev ve sorumluluklar belirlenmiştir.

Siber güvenlik konusunda dünyada öncü ve ileri seviyedeki devletlere benzer şekilde, ilgili bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşan 12 kişilik Siber Güvenlik Kurulu en önemli stratejik adımlardan birisi olarak hayata geçmiştir. Ayrıca UDHB'nin siber güvenlik konusundaki görev ve yetkileri de aşağıda sıralandığı şekilde yeniden belirlenmiştir.

- Ulusal Siber Güvenliğin sağlanması için politika, strateji ve eylem planlarını hazırlamak,
- Kamu kurum ve kuruluşlarına ait bilgi ve verilerin güvenliği ile mahremiyetinin güvence altına alınmasını sağlamaya yönelik usul ve esasları hazırlamak,
- Ulusal Siber Güvenliğin sağlanmasında kamu kurum ve kuruluşlarında teknik alt yapının oluşturulmasını takip etmek, uygulamaların etkinliğinin doğrulanmasını ve test edilmesini sağlamak,
- Ulusal bilgi teknolojileri ve iletişim alt yapısı ve sistemleri ile veri tabanlarının güvenliğini sağlamaya, kritik alt yapılan belirleyerek bunlara yönelik siber tehdit ve saldırı izleme, müdahale ve önleme sistemlerini oluşturmaya, ilgili merkezleri kurmaya, kurdurmaya, bu sistemlerin denetimi, işletimi ve sürekli güçlendirilmesine yönelik çalışmaları yapmak,
- Ulusal Siber Güvenliğin sağlanmasında her türlü milli çözümlerin ve siber saldırılara müdahale araçlarının geliştirilmesi ve üretilmesini teşvik etmek, kullanımını sağlamak,
- Ulusal Siber Güvenlik açısından kritik kurum ve konumlar için gerekli ve yeterli sayıda uzman personelin temini, eğitimi ve gelişimini planlamak, koordine etmek ve yürütmek,

- Bu Karar çerçevesinde diğer ülkeler ve uluslararası kuruluşlarla işbirliği yapmak,
- Ulusal Siber Güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek,
- Bilgi güvenliği alanında eğitim, test ve çözüm üretme alanında çalışan gerçek ve tüzel kişilere usul ve esaslarını belirleyerek güvenlik belgesi vermek,
- Siber Güvenlik Kurulunun sekretarya hizmetlerini yürütmek.

Bakanlar kurulunun 'Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin' kararları 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununa Ek Madde 1 ve 5'inci maddesinin birinci fıkrasına h bendi eklenerek kanunlaşmıştır [193].

5.5.7 TSK Siber Savunma Komutanlığının kurulması (2012)

Türk Silahlı Kuvvetleri bilişim sistemlerinin siber savunmasını sağlamak maksadıyla, 2012 yılında, Genelkurmay Muhabere Elektronik ve Bilgi Sistemler Komutanlığına bağlı olarak TSK Siber Savunma Merkez Başkanlığı kurulmuş, 30 Ağustos 2013'te TSK Siber Savunma Komutanlığı olarak yapılandırılmıştır [194].

Siber Savunma Komutanlığının kurulmasında hedeflenen temel amaç, siber ortamda öncelikle TSK unsurlarına yönelik tehditleri önleyerek gelişmiş siber savunma uyarı ve karşı koyma sistemlerine sahip güçlü bir merkezi siber savunma, siber istihbarat ve gerektiğinde siber taarruz yeteneği kazanılması ve siber caydırıcılığa yönelik yerli ve milli teknolojilerle ürün geliştirilmesi amaçlı Ar-Ge çalışmalarına öncülük etmektir.

Siber Savunma Komutanlığı, Ulaştırma ve Altyapı Bakanlığı, Dışişleri Bakanlığı, Savunma Sanayi Başkanlığı (SSB), TÜBİTAK ve diğer kamu kurumları ile koordineli olarak ve NATO ile koordineli ve işbirliği içerisinde faaliyetlerini yürütmektedir. Bu kapsamda;

- TSK karargâh, birlik ve unsurları tarafından kullanılan tüm bilgi ve iletişim sistemlerinin siber güvenliği sağlanmakta,
- TSK'nın ilgili birimleri ile koordine ve işbirliği içerisinde hareket edilerek, 7 gün 24 saat esasına göre, siber saldırı ve olaylar için gerekli tedbirler alınmakta, karşı konulmakta, saldırı ve olayların etkilerinin en aza indirilmesi ve izlerinin takip edilmesi sağlanmakta,

- Ulusal ve NATO siber tatbikatlarına katılınmakta,
- TSK bilişim sistemlerinde ve ağlarında siber güvenlik kontrol ve denetim faaliyetleri sürdürülmektedir.
- TSK personeline yönelik siber güvenlik eğitim, bilinçlendirme ve farkındalık yaratma faaliyetleri yürütülmekte,

TSK'ya ait bilgi sistemlerinin siber güvenliğinin milli yazılımlar vasıtasıyla güçlendirilmesi, siber savunma faaliyetlerinin tek bir noktadan koordine edilmesi ve siber olaylara anında tepki vererek söz konusu olayların olası etkilerinin azaltılması amacıyla TSK Siber Savunma Merkezi (SİSAMER) 2017 yılı içerisinde kurulmuş, 2020 yılı başlarında milli olarak geliştirilen siber güvenlik yazılımları kullanılmaya başlanmıştır [195].

TSK Siber Savunma Komutanlığının varlığı bile siber ortamda hem içeriye hem de dışarıya karşı bir siber caydırıcılık etkisi sağlar. Bu etkinin uygulamalarla gösterilerek duyurulması büyük önem taşımaktadır. Bunun gösterilmesinin en öncelikli yol ve yöntemlerinin başında, belirlenen görevlerinin etkinliğinin eğitim ve tatbikatlarla artırılması, planlanacak ulusal ve uluslararası tatbikatlara diğer kamu kurum ve kuruluşlarının da katılımının sağlanarak yaygınlaştırılması gelmektedir.

Dünyada icra edilen benzerlerine göre en kapsamlısı olan ve karmaşık teknikleri içeren canlı mücadelelerle geçekleştirilen bir uluslararası siber savunma tatbikatı kabul edilen, NATO Siber Güvenlik Mükemmeliyet Merkezi (CCDCOE, Tallin / Estonya) tarafından planlanıp yönetilen, yaklaşık 30 ülkeden 1200'den fazla uzmanın katıldığı, "Kilitli Kalkanlar (Locked Shields)-2019" Tatbikatı'nın, 11 Nisan 2019 tarihinde, Seçkin Gözlemci Günü bölümüne TSK MEBS ve Siber Savunma Komutanlığı (Ankara)'nda katılım sağlanmıştır.

Türkiye'den ilgili kurum ve kuruluşların temsilcilerinin de katılım sağladığı tatbikatın başarıyla icra edildiği ve her bakımdan faydalı olduğu gözlenmiştir. Tatbikat dolayısıyla komutanlık görev ve çalışmaları hakkında görüşme ve bilgi alma fırsatı da bulunmuş ve açık kaynaklara da yansıyan bilgiler doğrulanmıştır. [196]

5.5.8 Ulusal Siber Güvenlik Strateji ve Eylem Planı (2013-14)

UDHB koordinesinde kamu ve özel kurum/kuruluşlarının katılımları ile başta Bilgi Güvenliği Derneği (BGD) [197] olmak üzere bu konuda çalışmalar yapan benzer sivil

toplum kuruluşlarının da katkıları ile hazırlanan ‘Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı’ Siber Güvenlik Kurulu tarafından [198] kabul edilerek 20 Haziran 2013 tarihinde yayımlanmıştır.

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

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

Plan içeriğinde ve eylemlerde siber güvenlikle ilgili esaslar, prensipler ve görevler yer almasına karşın siber caydırıcılık konusu açıkça yer almamıştır. Bunula birlikte, eylemlerden güdülen niyet ve maksatlarla ulaşılması öngörülen hedeflerin kısmen de olsa siber caydırıcılık sağlama sonucuna götürebileceği düşünülebilir.

- **Planda siber caydırıcılığa katkı sağlayacağı düşünülen hususlar;**

- Siber güvenlik konusunda yasal düzenlemelerin yapılması ve adli süreçlere yardımcı olacak çalışmaların yürütülmesi siber saldırganların siber ortamda işledikleri suçlar nedeniyle cezalandırılacak olmaları,
- Ulusal Siber Olaylara Müdahale Merkezi (USOM)'nin oluşturulması ile Siber Olaylara Müdahale Ekipleri (SOME)’nin faaliyete başlaması, siber olayların tespitini, duyurulmasını, gerekli tedbirlerin alınarak saldırganlarla ilgili gerekli yasal işlemlerin de kısa sürede başlatılmasın sağlanabilecek olması,
- Ulusal siber güvenlik altyapısının güçlendirilmesinin siber saldırıların başarılı olmasını zorlaştırması ve daha masraflı hale getirmesi,
- Siber güvenlik alanında insan kaynağının yetiştirilmesi ile başta kullanıcıları siber güvenlik farkındalığının artırılmasıyla güvenlikte ihmallerin ve yanlışların azalması, bu konuda strateji ve politikaların geliştirilmesi,

- Siber güvenlikte yerli teknolojilerin geliştirilmesi ile daha güvenli donanım ve yazılımların kullanılmaya başlanması,
- Ulusal güvenlik mekanizmalarının kapsamının genişletilmesi ile koordinasyon ve işbirliğin artırılması siber caydırıcılık sağlanmasında temel yapı taşlarını oluşturan önemli eylem ve faaliyetlerdir.

5.5.9 Bilgi Toplumu Stratejisi ve Eylem Planı (2015-18)

Avrupa Birliğinin sosyal, siyasal ve ekonomik birikimlerini daha ileri düzeye çıkarılması ve bilginin üretimde kullanıldığı bilgi toplumuna geçiş sürecinin hızlandırılması, özellikle bu alanda birikimlerin artırılmasını ve daha etkin kullanılmasını sağlayan "sayısallaşma" kavramına odaklanma ihtiyacı duyulmuştur.

Bu bağlamda bilişim teknolojileri alanında birbirinden kopuk olarak ilerleyen çabaların birleştirilmesi, uygulamada eşgüdümün sağlanarak daha etkin çözümler üretilmesi adına strateji, eylem planı ve programlar oluşturma için sırasıyla e-Avrupa Girişimi (1999), Avrupa Birliği Lizbon Stratejisi (2000), e-Avrupa 2005 (2002) ve i2010 Büyüme ve İstihdam için Bilgi Toplumu Stratejisi (2005) çalışmaları yapılmıştır. Tüm bu çalışmaların da devamı olarak 2010 yılında Avrupa Komisyonu tarafından "Avrupa İçin Sayısal Gündem" (Digital Agenda for Europe) girişimi hayata geçirilmiştir [199]. Avrupa için Sayısal Gündem, AB'nin yeni ekonomik dönüşüm stratejisini ve 2020 yılı için hedeflerini ortaya koymak maksadıyla 3 Mart 2010 tarihinde açıklanan "Avrupa 2020 Stratejisi"nin 7 alt başlığından birisidir [200].

Küresel ölçekte ve bölgede yaşanmakta olan bu dönüşüme daha fazla dâhil olmak ve Türkiye'nin bu süreçten mümkün olduğunca faydalanmasını sağlamak amacıyla, T.C. Kalkınma Bakanlığı sorumluluk ve koordinesinde ilgili tüm tarafların katkılarının da alındığı kapsamlı çalışmalar sonucunda, 2006-2010 dönemine ait strateji belgesi ve eylem planı güncellenerek, 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı hazırlanmış ve 6 Mart 2015 tarihli ve 29287 sayılı (mükerrer) Resmi Gazete'de yayımlanarak yürürlüğe girmiştir [201].

- **Bilgi Toplumu Stratejisi Stratejisinin,** Türkiye'nin önemli gündem maddelerinden olan büyüme ve istihdamı odak alarak, bilgi toplumunun ülke açısından dikkate alınması çerçevesinde sekiz ana hedefi;

- Güçlü bir bilgi teknolojileri sektörü oluşturulması,
- Genişbant altyapılarının sağlıklı bir sektör yapılanmasıyla tesisi,

- İnsan kaynaklarının bilgi toplumu gündeminin ihtiyaçları doğrultusunda organizasyonu,
- Toplumun farklı kesimlerinin bilgi ve iletişim teknolojilerinin sağladığı olanaklardan istifadesinde etkinliğin artırılması ve eşitsizliklerin azaltılması,
- Bilgi güvenliği ve kullanıcı güveninin tesisi,
- Çeşitli toplumsal sorunlarla mücadele noktasında bilgi ve iletişim teknolojileri destekli yenilikçi çözümlerden üst düzeyde yararlanılması,
- İnternet girişimciliği ve e-ticaret alanında ekonomik kalkınmaya katkı sunacak bir ekosistem oluşturulması ve
- Kamu hizmetlerinin sunumunda kullanıcı odaklılığın ve etkinliğin sağlanması öngörülmüştür

'Bilgi Toplumu Stratejisi ve Eylem Planı' bilişim teknolojileri alt yapılarının geliştirilmesi, kullanıcıların eğitimlerinin artırılması, sektörlerin desteklenmesi vb. nedenlerle siber güvenliğe ve caydırıcılığa önemli katkılar sağlayacaktır.

5.5.10 Kişisel Verileri Koruma Kanunu (2016)

6698 sayılı Kişisel Verilerin Korunması Kanunu, AB uyum yasaları çerçevesinde 24 Mart 2016 tarihinde TBMM'de Kabul edilmiş ve 7 Nisan 2016 tarihli Resmi Gazetede yayımlanarak yürürlüğe girmiştir [202]. Kanunun amacı 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 düzenlemektir.

Kanun kapsamında uygulamaları ve gelişmeleri takip etmek, değerlendirmek, önerilerde bulunmak, araştırma ve incelemeler yapmak veya yaptırmak maksadıyla Kişisel Verileri Koruma Kurumu (KVKK) kurulmuştur.

Bilgi ve iletişim sistemlerinde gelişmeler ve internetin yaygınlaşmasıyla başta e-ticaret ve bankacılık hizmetleri olmak üzere günlük yaşamın sağladığı kolaylıklar kişisel bilgilerin kullanılmasını ve paylaşılmasını artırmış, kişisel verilerin kullanımının artması bu verilerin kötü niyet ve maksatlarla siber suç ve saldırılarda kullanılarak vatandaşların maddi ve manevi zarar görmesine yol açmıştır. Bu nedenle konunun tanımlanması, sorumlulukların belirlenmesi ve uyulmaması durumunda

yaptırım ve cezaların uygulanması caydırıcılık sağlarken vatandaşların da korunmasını sağlamıştır.

5.5.11 Ulusal e-Devlet Stratejisi ve Eylem Planı (2016-19)

Türkiye'nin kamu kurum / kuruluşlarının kurumsal süreçlerinin elektronik ortama taşınması ve organizasyon yapılarının güncellenmesi kapsamında, vatandaş odaklı e-dönüşüm, sosyal ağlar, yönetişim ve şeffaflık ile hesap verebilirlik kavramlarını öne çıkartarak, e-Devlet alanındaki planlama, karar verme ve uygulama süreçlerinde rol oynayan tüm paydaşlar ile devlet arasındaki ilişkilerin yeniden tanımlanmasını gerektirmiştir.

2016- 2019 Ulusal e-Devlet Stratejisi ve Eylem Planı bu doğrultuda, somutlaşan e-Devlet politikasının şekillendirilmesinde ve uygulanmasında kapsamlı ve sürdürülebilir bir "e-Devlet Ekosistemi" stratejik bakış açısı benimsenerek hazırlanmış, Yüksek Planlama Kurulu'nun 13 Temmuz 2016 tarihli kararı ile kabul edilmiş ve 19 Temmuz 2016 tarihinde Resmi Gazete'de yayımlanmıştır [203].

Belirlenen 4 stratejik amaç;

- E-Devlet ekosisteminin etkinliğinin ve sürdürülebilirliğinin sağlanması,
- Altyapı ve idari hizmetlere yönelik ortak sistemlerin hayata geçirilmesi,
- Kamu hizmetlerinde e-dönüşümün sağlanması,
- Kullanım, katılım ve şeffaflığın artırılması şeklinde sıralanmıştır.

Kamu kurum / kuruluşlarının kurumsal süreçlerinin elektronik ortama taşınması ve organizasyon yapılarının güncellenmesi yanında vatandaşın da sürece katılımının sağlanması koordinasyon ve işbirliğinde etkileşimi ve verimi artırarak sorunların çözümünde sürat ve elastikiyet sağlanmış ve hizmet kalitesi de artırılmıştır. Bu gelişmeler ve kazanımlar siber güvenliğin sağlanmasında caydırıcılık sağlanmasına da katkı sağlayacaktır.

5.5.12 Ulusal Siber Güvenlik Strateji ve Eylem Planı (2016-19)

Türkiye '2016 - 2019 Ulusal Siber Güvelik Strateji ve Eylem Planı' 09 Eylül 2016'da açıklanmıştır. Türkiye'nin siber güvenlik konusunda izleyeceği yolu belirleyen Strateji ve Eylem Planında, siber güvenliğin, ulusal güvenliğin ayrılmaz bir parçası olduğu anlayışının tüm kesimlerde yerleşmesi, ulusal siber uzayda bulunan sistem ve paydaşların tamamının güvenliğini sağlamak üzere idari ve teknolojik önlemlerin alınmasını sağlayacak yetkinliğin eksiksiz bir şekilde kazanılması amacıyla, 5 ana

eylem ve 41 alt eylemin gerçekleştirilmesi öngörülmektedir. Dört yıllık siber güvenlik yol haritasını oluşturan ana eylem maddeleri aşağıda sunulmuştur [17].

- Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması,
- Siber Suçlarla Mücadele,
- Farkındalık ve İnsan Kaynağı Geliştirme,
- Siber Güvenlik Ekosisteminin Geliştirilmesi,
- Siber Güvenliğin Milli Güvenliğe Entegrasyonu.

Bu strateji ve eylem planının ana metin ve ana eylem maddelerinde siber caydırıcılık konusunda açık ifadeler bulunmamakla birlikte, ana eylem maddelerinde planlanmakta olduğu belirtilen hususların doğru planlanarak zamanında da uygulamaya konulmasının siber güvenlik ve caydırıcılık konusunda ciddi ilerlemeler sağlayabileceği düşünülebilir. Bununla birlikte siber caydırıcılık konusundaki öngörü ve beklentinin, sadece 'Siber suçlarla mücadele' eyleminin alt maddelerinde, siber saldırganların tespiti ve suçlarının kanıtlanması sağlanarak caydırıcılık sağlanmasının hedeflenen kazanımlar arasında yer aldığının vurgulandığı görülmektedir.

5.5.13 Türkiye Yazılım Sektörü Stratejisi ve Eylem Planı (2017-19)

Bilim, Sanayi ve Teknoloji Bakanlığı koordinatörlüğünde üniversiteler, iş dünyası, kamu kurum ve kuruluşları ile ilgili sivil toplum kuruluşlarının katılımlarıyla hazırlanan "Türkiye Yazılım Sektörü Stratejisi ve Eylem Planı (2017-2019)" [204] 5 Ocak 2017 tarihinde Resmi Gazetede yayımlanarak yürürlüğe girmiştir. Stratejinin genel amacı; yazılım pazarını büyütmek, ihracatı ve sektörün istihdamını artırmak amacıyla yazılım ve bilgi teknolojileri alanlarında uluslararası standartlarda ürünler ve hizmetler üreten söz sahibi ülke konumuna gelmek olarak belirlenmiştir.

Stratejinin 4 temel amacı;

- Ulusal bilinci artırma ve altyapıyı güçlendirmek,
- Hukuki ve idari düzenlemeleri yapmak,
- Nitelikli insan kaynağı geliştirmek,
- Uluslararası rekabet gücünü artırmak şeklinde belirlenmiştir.

Yazılım sektöründe hem üretici hem de kullanıcıların ulusal bilincin artırılması ve altyapıların güçlendirilmesi caydırıcılığın temel şartlarından birisidir. Nitelikli insan gücü yetiştirilmesi ve ürünlerin uluslararası piyasada da görünürlüğünün artması

dışarıdan saldırıları ilave tedbirler almaya zorlayacak ve doğal olarak güvenliği artırıcı olumlu bir etki yapacaktır.

5.5.14 Siber Güvenlik Kurulu'nun kaldırılarak görevlerinin Cumhurbaşkanlığına devredilmesi (2018)

04 Temmuz 2018 tarihli ve 30468 sayılı Resmi Gazetede yayımlanan 477 numaralı KHK doğrultusunda Bakanlar Kurulunun yetkileri Cumhurbaşkanına devredilmiş [205], yeni Hükümet Sistemi'nin hukuki altyapısını oluşturacak düzenlemeler 9 Temmuz Pazartesi günü Resmi Gazetede yayımlanan 703 numaralı Kanun Hükmünde Kararname'yle yürürlüğe girmiştir.

Bu kapsamda; Bakanlar Kurulunca alınan 11/6/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Kararın 20 Kasım 2012 tarihli ve 28447 sayılı Resmî Gazetede yayımlanarak yürürlüğe girmesiyle oluşturulan ve Ulaştırma, Denizcilik ve Haberleşme Bakanlığı sorumluluk ve koordinesinde faaliyet gösteren 'Siber Güvenlik Kurulu' görevleri Cumhurbaşkanlığının 2018/3 numaralı [206] genelgesi ile Cumhurbaşkanlığına devredilerek kaldırılmıştır.

5.5.15 Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi (2019)

Cumhurbaşkanının 05 Temmuz 2019 tarihli imzasıyla, 'Kamu düzenine' ve 'Milli güvenliğe' etki edebilecek kritik verilerin güvenliğinin sağlanması amacıyla alınması gereken tedbirler, 06 Temmuz 2019 tarihli ve 30823 Sayılı Resmî Gazetede yayımlanan 2019/12 Numaralı Genelgede yayımlanmıştır [207]. Tamamı 21 madde altında toplanan 'önlemler paketinde' vatandaşlara ait kritik bilgiler ile kamu kurum ve kuruluşlarına ait verilerin hangi şartlarda nerelerde saklanacağına dair kararlar belirtilmiştir. Genelgede öne çıkan önemli hususlar aşağıda sunulmuştur.

- Nüfus, sağlık, iletişim bilgileri, biyometrik ve genetik verilerin kritik bilgi olarak tanımlandığı genelgede bu verilerin güvenli bir şekilde yurt içinde depolanması,
- Kamu kurum ve kuruluşlarında yer alan kritik verilerin depolanacağı ağların;
  - İnternete kapalı,
  - Fiziksel güvenliği sağlanmış,

- Güvenli olması şartı konulması,
- Bu ağlara erişimin kontrollü sağlanması ile log kayıtlarının değiştirilmesine karşı önlemler alınması.

• Genelgede ayrıca; Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı koordinasyonunda, ilgili kamu kurum ve kuruluşlarının katkılarıyla 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, 'Bilgi ve İletişim Güvenliği Rehberi' hazırlanacağı belirtilmiştir. 10 Temmuz 2020 tarihinde yayımlanan söz konusu rehberle ilgili önemli esaslar aşağıdadır.

- Rehberin ihtiyaçlar, gelişen teknoloji, değişen şartlar ile Ulusal Siber Güvenlik Stratejisi ve eylem planlarında yapılacak değişiklikler göz önünde bulundurularak güncellenecek,
- Tüm kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerin de yeni kurulacak bilgi sistemlerinde, rehberde yer verilen usul ve esaslara uyulması zorunlu olacak,
- Milli güvenliğin sağlanması ve gizliliğin korunması kapsamında yürütülen görev ve faaliyetler hariç olmak üzere kurum ve kuruluşlar, rehberin uygulanmasına ilişkin denetim mekanizmalarını oluşturacak ve yılda en az bir defa uygulamayı denetleyecektir.
- Denetim sonuçları ile yapılan düzeltici ve önleyici faaliyetler, rehberde belirtilen usul ve esaslara göre bir rapor halinde Dijital Dönüşüm Ofisine iletilecektir.

Bilgi ve İletişim Güvenliği Tedbirleri Genelgesine caydırıcılık açışından bakıldığında, 21 maddenin gereği yapıldığında siber güvenlik ve savunma konusunda güçlenme sağlanacağı, saldırganları siber ortamda kötü niyetli hareketlerinden ve saldırı eylemelerinden vaz geçmeleri konusunda olumlu katkılar sağlayabileceği düşünülmektedir.

Türkiye'de bu güne kadar ulusal siber güvenlik konusunda hazırlanan stratejiler ve eylem planları ile politikalar çerçevesinde çalışmalara devam edilmektedir. Bu çalışmaların etkinliği ve hedeflerine başarıyla ulaşılması, bu kapsamda özellikle caydırıcılık da sağlanması için siber güvenlik strateji ve politikalarının oluşturulması ile uygulanmasının esas ve prensipleri belirlenmesi çok büyük önem taşımaktadır.

5.5.16 Siber saldırılara karşı caydırıcılık çalışmaları

Türkiye'de siber güvenlik strateji ve politikalarıyla ilgili bu güne kadar hazırlanan ve uygulamaya konulan belgeler incelendiğinde, siber caydırıcılık konusuna, siber suçlarla yasal olarak mücadele edilerek caydırıcılık sağlanması konusu hariç yer verilmediği görülmektedir.

09 Kasım 2016 tarihli ve 6757 numaralı Kanun Hükmünde Kararname ile 5 Kasım 2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun 60'ıncı maddesinde değişiklik yapılarak Bilgi Teknolojileri ve İletişim Kurumuna; "Kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alma veya aldırma" [208] görevi verilmiştir.

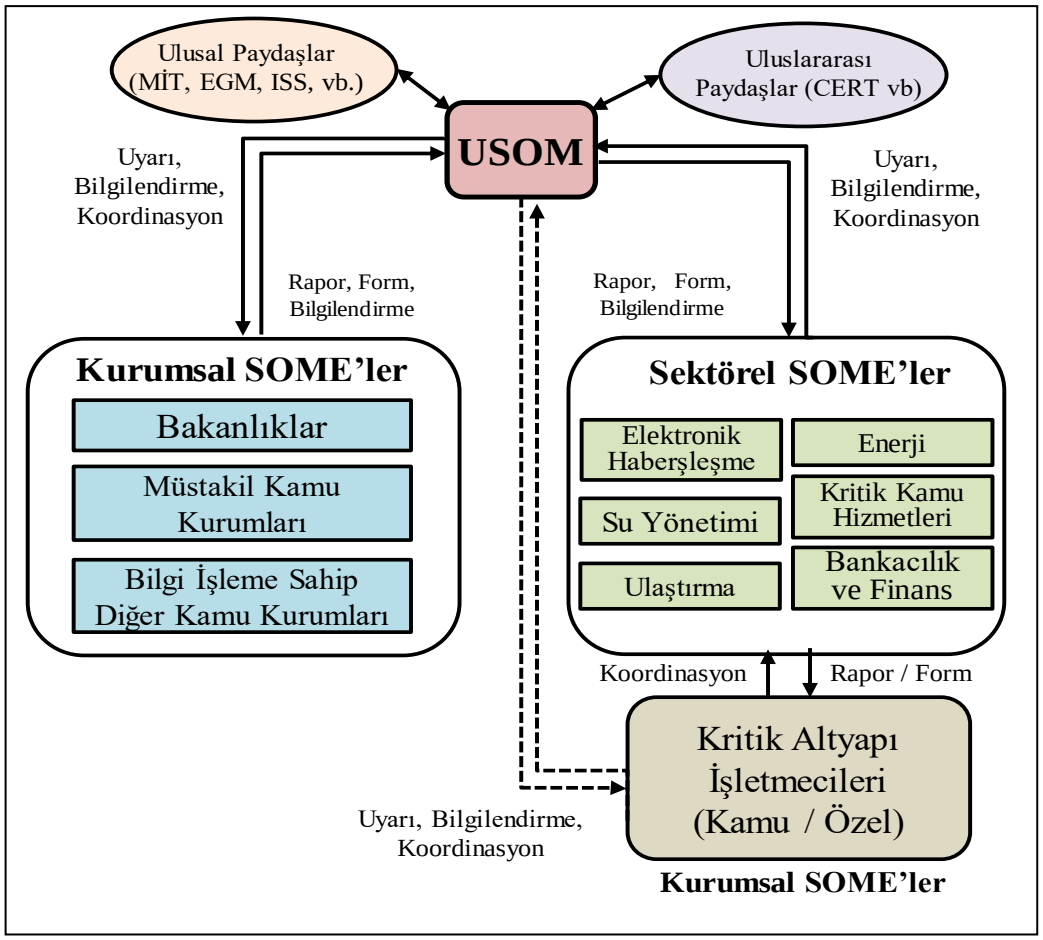
Türkiye Cumhuriyeti Başbakanının, 22 Kasım 2016 günü Bilişim Zirvesi'nde, siber güvenlikle ilgili yaptığı ve basına da yansıyan açıklamasında "Siber saldırılarda caydırıcılığın arttırılacağını, saldırılardan sadece korunulmayacağını, ayrıca caydırıcılık için ek önlemler alınacağını…" [209] ifade etmesi Türkiye'de siber güvenlik yanında siber caydırıcılık konusunda da umut verici çalışmaların başladığını göstermiştir.

BTK Bilgi Teknolojileri Dairesi Başkanlığı ziyaret edilerek BTK'nın siber güvenlik kapsamında görev ve faaliyetleri ile ilgili olarak Ekim 2018'de görüşmelerde bulunulmuş, Ulusal Siber Olaylara Müdahale Merkezi (USOM) gezilerek bilgiler alınmıştır [210].

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın "Ulusal Siber Olaylara Müdahale Merkezinin Kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) Oluşturulması" başlıklı 4.eylem maddesi uyarınca kurulan USOM ve SOME yapılanması ve işletimi [211] Şekil 5.6'da görülmektedir. Bilgilendirmede, USOM ile birlikte ilgili içerisinde siber saldırılara karşı mücadele edildiği belirtilmiştir.

Siber güvenlik denetim ve kontrolleri kapsamında özellikle kritik kurumlarda olay müdahale ve güvenlik testlerinin sayı ve niteliklerinin her geçen gün artırıldığı vurgulanmıştır. Kamu kurum ve kuruluşlarda siber güvenlik ve SOME yapılanmasının hemen hemen tamamlanmakla birlikte, özel kurum ve kuruluşlarda halen eksiklikler

ve yetersizlikler olduğu ve karşılıklı bilgi alışverişinde sorunlar yaşanmakta olduğu anlaşılmıştır.



Şekil 5.6: USOM / SOME yapılanması ve iletişimi [211].

BTK'nın 6757 sayılı KHK ile siber saldırılara karşı caydırıcılık sağlanması görev ve sorumluluğu hakkında bugüne kadar neler yapıldığı ve bundan sonra yapılması planlanan konularda bilgi alınmıştır. Kamu kurum ve kuruluşlara yönelik siber saldırılara karşı caydırıcılık sağlanması için özellikle siber güvenlik tedbirlerinin ve USOM faaliyetlerinin etkinliğinin artırılması konularında yeni projeler geliştirildiği, yeni yetenekler kazanıldığı ve hareket tarzlarının belirlendiği öğrenilmiştir.

Siber saldırıları ve zafiyetleri tespit etmek, siber güvenliğe yönelik tehlikelerin daha oluşmadan kaynağında yok edilmesini sağlamak ve yapılan tespitleri ilgili kurumlara iletmek için tamamen yerli, milli ve kurumsal imkânlarla geliştirilen yazılımları arasında; AVCI, AZAD ve KASIRGA isimleri verilen dağıtık mimaride çalışan, makine öğrenmesi ve büyük veri analitiği imkânlarını kullanan altyapıları ile USOM ile SOME'ler arasında siber tehdit, zafiyet ve saldırıların güvenli ve hızlı bir biçimde paylaşımını sağlayan SOME İletişim Platformu altyapısı bunlar arasındadır.

BTK İdari Yaptırımlar Yönetmeliği'nde yapılan değişiklikle [212] yasal dayanağı da bulunan ulusal siber güvenlikle ilgili yaptırımların tanımlandığı, yapılan düzenlemeyle siber güvenlik alanında önemli ölçüde caydırıcılık sağlanacağı, özellikle firmaların hizmet olarak sunduğu altyapılarda, sistemlerde, yazılım ve donanımlarında zafiyet bulunması ve bildirilen önlemleri almamaları durumunda BTK bünyesinde bulunan USOM'a Bin TL'den bir milyon TL'ye kadar para cezası verme yetkisi verildiği belirtilmiştir. Yapılan görüşmelerde kurum ve kuruluşların eksikleri nedeniyle para cezası henüz uygulanmadığı öğrenilmiştir.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanı, Ekim 2019'da basına verdiği bir söyleşide, siber saldırıların savaşa dönüşmesinin ülkelerin tıpkı sınırları gibi verilerini ve dijital altyapılarını da korumasını zorunlu kıldığını belirterek, veri güvenliğinin yabancı çözümlerle sağlamaya çalışmanın, sınır güvenliğini yabancı askerlere emanet etmeye eşdeğer olduğunu, siber güvenlikte caydırıcı olmanın yolunun bu alanda mevcut teknolojilere eşdeğer milli ürün ve çözümler geliştirmekten geçtiğini vurgulamıştır [213].

Bu tespit ve bilgilerin sonucu olarak, Türkiye'de siber güvenlik strateji belgeleri ve politikaları ile süreç içerisinde yapılan çalışmalara siber güvenliğin sağlanarak saldırıların engellenmesi ve saldırıların boşa çıkarılması açısından bakıldığında, siber caydırıcılık dolaylı ve kısmen sağlanabilir görünse de, yeterli olmadıkları düşünülmektedir.

6. CAYDIRICILIK SAĞLAYACAK SİBER GÜVENLİK STRATEJİ VE POLİTİKALARININ OLUŞTURULMASI

Bilgisayarın icadı sonrasında teknolojinin gelişmesine de paralel olarak bilgi ve iletişim sistemlerinde hayal sınırlarını zorlayan hızlı gelişmeler, bunların sonucunda da yaşamın her alanında her gün artan göz alıcı kazanımlar sağlanmıştır. Bu çerçevede belirlenen yeni hedeflere ulaşılması sırasında karşılaşılan veya karşılaşılması olası tehditler, riskler ve tehlikeler de her geçen gün çeşitlenerek ve şiddetlenerek artmaktadır. Kişileri, kurum ve kuruluşları, dolayısıyla devletleri olumsuz etkileyen bu tehlikelere karşı kapsamlı ulusal siber güvenlik stratejileri oluşturulması yaşamsal bir zorunluluk halini almıştır.

Devletler tarafından ulusal hedeflerine ulaşmalarında siber uzayın daha güvenli hale getirilmesi için farklı yol ve yöntemlerle ulusal siber güvenlik stratejileri oluşturulurken, çeşitli uluslararası kurum ve kuruluşlar da bu konularda çalışmalar yapmakta ve ulusal siber güvenlik stratejisi oluşturulması için çalışmalara yönelik görüş ve önerileri içeren rehberler hazırlayarak yayımlamaktadırlar.

Yayımlanan rehberlerde ortak yaklaşımın Deming tarafından sürekli iyileştirme faaliyetleri için geliştirilen, kurumsal siber güvenlik bölümünde de açıklanan PUKÖ / PDCA *(Planla, Uygula, Kontrol et* ve *Önlem al* / *Plan, Do, Check, Act)* döngüsü [148] modelini izlemektedir. PUKÖ yaklaşımı siber güvenlik stratejileri ve politikaları ile süreçlerini oluşturmak, kontrol etmek ve sürekli iyileştirmek için kullanılabilmektedir.

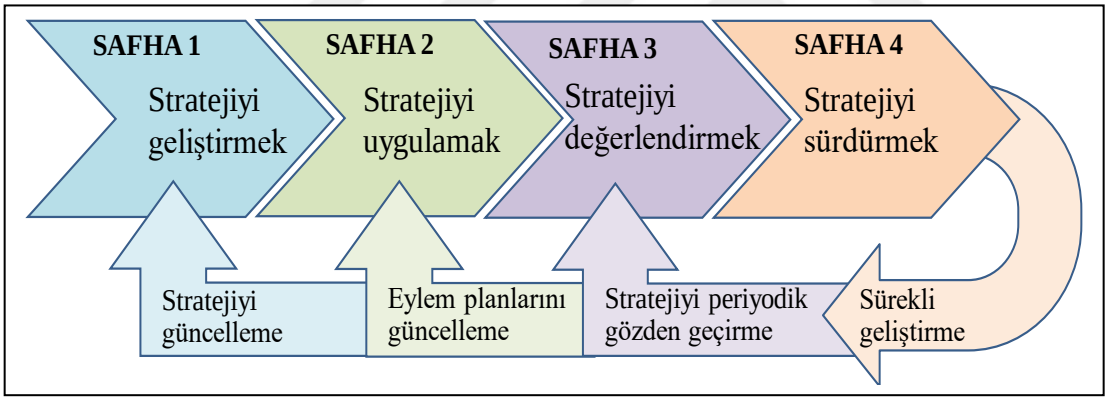
Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) tarafından hazırlanan rehberde, bu yaklaşımdan hareketle, bir ulusal siber güvenlik stratejisini oluşturarak yönetmenin iki temel aşaması olduğu belirtilmiştir [214].

- Stratejiyi geliştirmek ve uygulamak,
- Stratejinin değerlendirilmesi ve sürdürülmesi.

Ayrıca bir ulusal siber güvenlik stratejisini oluşturmak için üç ayrı yaklaşım benimsenebilir. Bunlar;

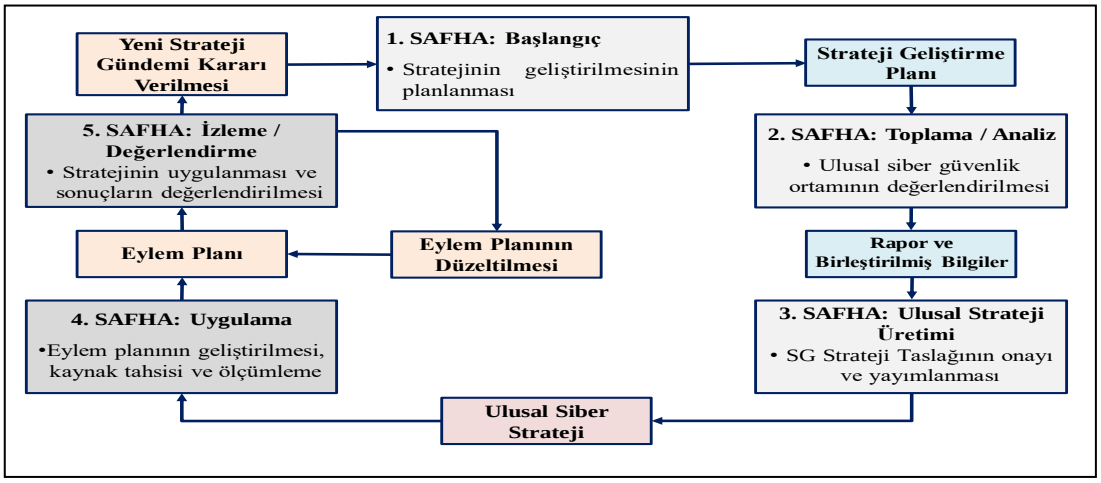
- **Doğrusal Yaklaşım:** Strateji geliştirilir, uygulanır, değerlendirilir ve sona erdirilir veya değiştirilir.
- **Yaşam Döngüsü Yaklaşımı:** Değerlendirme aşamasının çıktısı stratejinin kendisini korumak ve ayarlamak için kullanılır.
- **Karma Yaklaşım:** Farklı seviyelerde her iki yaklaşımı da içeren sürekli iyileştirme döngüleri olabilir.

Ulusal siber güvenlik stratejilerinin hazırlanmasında en yaygın kabul gören yaklaşımın ise Yaşam Döngüsü yaklaşımı olduğu görülmektedir. Bu çerçevede stratejiyi, ilgili politikaları ve bunun yanı sıra önlem, eylem ve süreçlerle uygulanmasını kontrol etmek ve sürekli iyileştirmek için ENİSA tarafından formüle edilerek önerilen yaşam döngüsü yaklaşımı Şekil 6.1'de sunulmuştur. [8] Şekilde görüldüğü gibi, Ulusal Siber Güvenlik Stratejisi Yaşam Döngüsü 4 safhadan oluşmakta, 1. ve 2. Safhada strateji geliştirilerek uygulamaya konulmakta, 3. ve 4. Safhalarda ise değerlendirilerek sürdürülmesi sağlanmaktadır. Faaliyetler hem bir defalık hem de devam eden / periyodik değerlendirmeleri içermektedir.



Şekil 6.1: ENISA - Ulusal siber güvenlik stratejisi yaşam döngüsü [8].

Son yıllarda, siber güvenlik stratejilerinin uygulanmasına ilişkin yayın ve çalışmalarda Uluslararası Telekomünikasyon Birliği (ITU)'nin yaklaşım ve önerilerini içeren bir rehber de kullanılmaktadır. Ulusal siber güvenlik stratejisi için bir ülkenin atacağı adımların, özel ihtiyaçlarına göre uygulanması için olası yapılar ve kapsayıcı ilkeler ile iyi uygulaması için gerekli olan esasların açıklandığı ITU'nun Ulusal Siber Güvenlik Stratejisi Geliştirme Rehberinde yer alan Strateji Yaşam Döngüsü yaklaşımı Şekil 6.2'dedir [215].



Şekil 6.2: ITU - Ulusal siber güvenlik stratejisi yaşam döngüsü [215].

Şekilde görüleceği üzere, ulusal düzeyde siber güvenlik hakkında stratejik düşünmeye odaklanma konusunda yönlendirme amaçlanan Strateji Yaşam Döngüsünün safhaları; Başlatma, Toplama ve analiz, Üretim, Uygulama, İzleme ve değerlendirme şeklinde 5 safhadan oluşmaktadır. 5.Safhada izleme ve değerlendirme süreci sonrasında yeni bir strateji hazırlanması kararı verilmediği takdirde mevcut strateji düzeltmelerle sürdürülmektedir.

Ulusal siber güvenlikte söz sahibi ülkelerin ulusal siber güvenlik strateji belgeleri ile bazı uluslararası kurumların çalışmalarından elde edilen bilgilerden hareketle Ulusal Siber Güvenlik Stratejisinin, ulusal siyaset / strateji esaslarına göre uyumlu ve mantıklı bir sıraya göre yapılandırılması ve bilimsel yöntemlerle çalışılarak ortaya konması gerektiği açıkça ortaya çıkmaktadır. Bu Tez çalışmasıyla, Türkiye için, mevcut stratejiler ve eylem planları da dikkate alınarak, bir yaklaşım tarzı olarak ulusal siber güvenlik stratejisinin temel yapısının, Şekil 6.3'de de görüleceği üzere, bir yaşam döngüsü şeklinde, 8 aşamada oluşturulması önerilmektedir.

Bu aşamalar aşağıda sıralanmıştır.

1.Aşama: Durum (Durumun Değerlendirilmesi),

2.Aşama: Teşkilat (Teşkilat, Görev, Yetki ve Sorumlulukların Belirlenmesi),

3.Aşama: Kapsam (Kapsam, Görev ve Sorumlulukların Belirlenmesi),

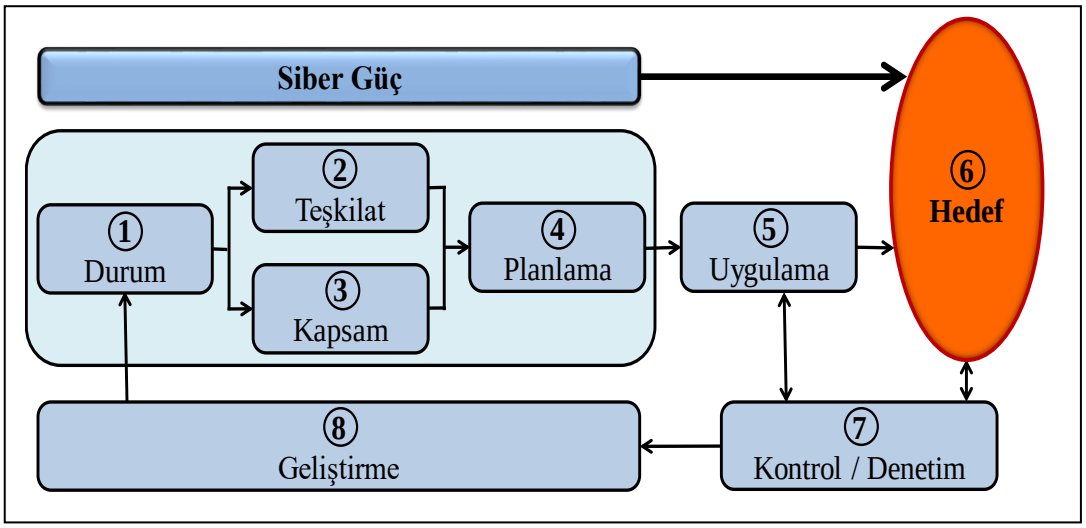
4.Aşama: Planlama (Planlamaların Yapılması),

5.Aşama: Uygulama (Stratejinin Uygulanması),

6.Aşama: Hedef (Hedefin Belirlenmesi ve Belirlenen Hedefe Ulaşılması),

7.Aşama: Kontrol / Denetim (Kontrol ve Denetimlerin Yapılması),

8.Aşama: Geliştirme (Stratejinin Geliştirilmesi).



Şekil 6.3: Ulusal siber güvenlik stratejisi oluşturma ve uygulama aşamaları önerisi.

6.1 Durum Değerlendirmesi

Siber güvenlik stratejisinin başlangıç bölümü olan bu aşama, askeri strateji de vazifenin en iyi şekilde yerine getirilmesi için ilgili bütün faktörlerin incelenerek en uygun hareket tarzını tespit etmek maksadıyla yapılan durum muhakemesi benzeri bir çalışmanın yapılmasını içerir. Geçmişten günümüze siber ortamda yaşananlar incelenir ve geleceğe bakılarak öngörülerde bulunulur.

Durum değerlendirmesi sırasında ülkenin siber ortamıyla ilgili durumu, öncelikle siber güvenlik boyutuyla geçmiş, güncel ve geleceğe dönük olasılıkları da içerecek şekilde, çeşitli ülkelerin belgeleri, uygulamaları, bölgesel ve uluslararası çalışmalar ile karşılaştırılarak incelenmeli, analiz edilmeli, siber güvenlik ve savunma konusunda başarılı ülke ulusal planları, programları ile bu konuda strateji ve politika geliştirmiş olan ülkelerin örnek uygulamalarından yararlanılmalıdır. Siber gücün aynı zamanda siber caydırıcılık olduğu düşüncesinden hareketle ana düşünce siber gücün değerlendirilmesi olmalıdır.

- Bu kapsamda incelenmesi ve yapılması gereken önemli çalışmaların bazıları önceliklerine göre aşağıda sıralanmıştır.

- Başta ulusal siyaset ve stratejinin siber güvenlik boyutunu ilgilendiren konular olmak üzere ulusal siber güvenlik stratejisine tesir eden hususlar,
- Ulusal siber gücün yapılandırılması,
- Ulusal güç unsurlarının siber güçle ve siber güvenlikle bağlantıları,

- Siber ortamda geçmişte ve halen yaşanan önemli siber güvenlik olayları ve sonuçları,
- Siber ortamda teknolojik gelişmeler dâhil siber güvenlik kapsamlı geleceğe yönelik öngörüler,
- Ulusal siber gücün güçlü ve zayıf yönleri ile hassas tarafları,
- Siber güvenlikle ilgili fırsatların, risklerin ve tehditlerin değerlendirilmesi ve ihtiyaçların belirlenmesi,
- Siber güvenlikle ilgili mevcut ulusal ve uluslararası yasalar ve politikalar,
- Siber gücün kullanılmasıyla ilgili verilen ve / veya durumdan çıkarılan vazifenin (görevlerin ve görevlerden güdülen maksatların) analizi.
- Siber gücün siber güvenlik ve savunma yanında siber ortam dışı da dâhil olmak üzere yaptırım ve caydırıcılık maksatlı kullanılmasının değerlendirilmesi,

Değerlendirmenin başarısı bütün ilgili faktörlerin belirlenmesine, bu faktörlerin mantıki bir sıra içerisinde gerçekçi olarak ve ayrıntılı bir şekilde incelenmesine bağlıdır. İncelemelerde anayasa, kanunlar ve uluslararası anlaşmalar, insan hakları ve özgürlükleri vb. hususlar göz önünde bulundurulmalıdır. Çalışmaları etkileyen faktörler değiştikçe ve yeni gerçekler ortaya çıktıkça, durum yeniden gözden geçirilerek yeni değerlendirmeler ve düzeltmeler yapılmalıdır.

6.2 Hedefin Belirlenmesi ve Belirlenen Hedefe Ulaşılması

Fiziksel olarak varılacak yer, ulaşılacak nokta anlamında kullanılan hedef [216], stratejide vazifenin veya belirlenen amacın gerçekleştirilmesi için ulaşılması veya elde edilmesi gereken kazanımlardır. Ulusal stratejide bir devletin bekası ve ulusunun refahının sağlanması [217] şeklinde belirlenen ulusal hedefine ulaşılması için pek çok alana yönelik görevler, amaçlar ve bunlara yönelik pek çok hedef belirlenebileceği gibi, belirlenecek her hedefe ulaşmak için de çok sayıda farklı yol ve yöntem olabilir.

Benzer şekilde ulusal siber güvenlik stratejisinde de durum değerlendirmesi sonucunda belirlenen vazife sonrasında pek çok görev ve amaçlar ortaya konabilir ve bunların her birinin gerçekleşmesi için farklı hedefler olabilir. Ancak diğer güç unsurlarında da olduğu gibi siber güç te sınırlıdır ve etkin kullanılması için farklı hedeflerin elde edilmesi için parçalanarak kullanılması yerine, vazifeyi gerçekleştirecek veya vazifenin gerçekleşmesi için en fazla kazanımın elde edilmesini

sağlayacak hedefe yönlendirilmelidir. Bunun için de esas dayanak durum değerlendirmesi ile sonucundaki görev ya da görevlerden güdülen maksadın ifadesi olan vazifenin analizidir. Belirlenecek hedef, vazifenin analizi sonrasında ortaya konulan açık ya da kapalı görevlerin tamamının veya tamamına yakının ve bunların amaçlarının gerçekleşmesini direk ya da dolaylı olarak sağlıyor veya destekliyor olmalıdır.

Bu düşüncelerden hareketle bir ulusal siber güvenlik stratejisinde hedef; "Siber gücü korumak ve geliştirmek, diğer güç unsurlarıyla birlikte veya gerektiğinde tek başına siber ortamın her boyutunda caydırıcılık da sağlayacak seviyede etkin ve başarılı olmak" şeklinde belirlenebilir. Böyle bir hedef ulaşılamaz veya elde edilemez, ulaşılıp ulaşılmadığı ölçülemez gibi görünmekle birlikte, önemli olan hususun oluşturulacak teşkilat ve kapsama dâhil edilen unsurlarla siber güç tarafından aşamalar halinde ve çeşitli sürelerde elde edilebilecek kazanımlar olacağı unutulmamalıdır. Ancak burada dikkat edilmesi gereken konu, böyle bir hedefin geçen zaman içerisinde devamlı olarak şekil ve konum değiştirecek olması nedeniyle, stratejinin de devamlı geliştirilmesinin gerekeceğidir. Konuyla ilgili belirsizlikler, sınırlama vb. olumsuzluklar ise planlama aşamasında giderilebilecektir.

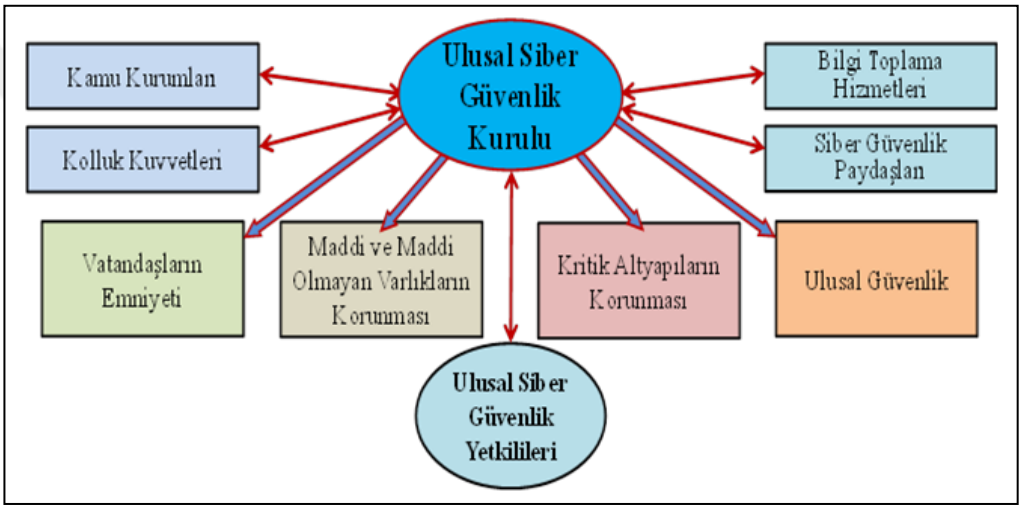
6.3 Teşkilat, Görev, Yetki ve Sorumlulukların Belirlenmesi

Ulusal siber güvenlik stratejisi oluşumları incelendiğinde, ülkelerin siber güvenliğin sağlanması için koordinasyon sistemleri için çalışmalar yaptığı ve belirledikleri yapıları uygulamaya koyduğu görülmektedir. Ülkelerin yönetim sistem ve yapıları ile işleyişlerinde olduğu gibi, bilişim sistemleri ve altyapıları ile bu kapsamdaki ihtiyaçları ve beklentilerindeki farklılıklar dolayısıyla, başta siber güvenliğin sağlanmasının koordinasyonu olmak üzere siber güvenlik strateji ve politikalarında da farklılıklar olmaktadır. Aralarında en büyük benzerlik ise izlenen yol ve yöntemlerin güçlü bir koordinasyonun sağlanmasını hedeflemesidir.

Ülkenin en değerli varlıkları bilgi, bilişim sistem ve altyapılarının öncelikle korunması, hayati önemde bir konu olması yanında aynı zamanda maliyeti de çok yüksektir. Siber güvenlik kapsamına, siber ortamın daha güvenilir olmasının sağlanması, siber gücün daha aktif ve etkin kullanılması boyutları da düşünüldüğünde güçlükler ve maliyetler daha da artacaktır. Ayrıca siber güvenliğin sağlanması yanında

siber savaşta başarı ve caydırıcılık sağlanması için koordinasyon ve işbirliği sadece ülke içinde değil uluslararası alanda da gerekli olmaktadır.

Ancak ulusal siber güvenlik çalışmalarının sadece koordinasyonu değil, aynı zamanda bu çalışmaların yönetilmesi için kurumsal bir teşkilatın kurulması ve siber gücün tek bir elden sevk ve idare edilerek etkinlikle kullanılmasının sağlanması düşünülmelidir. Uluslararası İletişim Birliği (ITU) tarafından 2008 yılında hazırlanan raporda bu görevin, Şekil 6.4'de görülen 'Ulusal Siber Güvenlik Kurulu' adı altında oluşturulacak, mevcut ilgili kurumlar arasında koordinasyon sağlayabilecek ve liderlik edebilecek üst seviyede bir devlet otoritesi tarafından yerine getirilebileceği [218] ifade edilmektedir.



Şekil 6.4: Ulusal Siber Güvenlik Kurulu koordinasyonu (218).

Amerika Birleşik Devletleri'nde siber güvenlik strateji ve politikaları sorumlulukları geniş oranda dağılmış olsa da, en üst seviyede koordinasyon sorumluluğu Başkanlık Ulusal Güvenlik Konseyi'ne bağlı Bilgi ve İletişim Altyapısı Uyumluluk Politikası Komitesi (ICI-IPC) tarafından yerine getirilmekte, Ulusal Güvenlik Konseyi ve Siber Güvenlik Koordinatörü (CSC) tarafından yönetilmektedir [156]. RF'de ulusal güvenlik sisteminin önemli bir parçası olarak kabul edilen siber güvenlik strateji oluşturulması ve uygulanması için yapılanma, yetki, görev ve sorumlulukları bizzat Rusya Federasyonu Başkanlığınca, RF Meclisi Konseyi, Devlet Duması, Hükümet, Güvenlik Konseyi, Yürütme organları, Merkez Bankası, Askeri-Sanayi Komisyonu yetki ve sorumlulukları çerçevesinde yürütülmektedir [176]. Çin'de siber güvenliğin koordinesi ve uygulanması görevleri ise Kamu Güvenliği,

Devlet Güvenlik ve Milli Savunma bakanlıkları tarafından yerine getirilmektedir [172].

Bu kapsamda, Türkiye'de siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla, 2012 yılında Ulaştırma, Denizcilik ve Haberleşme Bakanının başkanlığında, Bakanlıklar ile diğer ilgili kamu kurum ve kuruluşlarının aşağıda sıralanan 11 üst düzey yöneticinin katılımıyla 'Siber Güvenlik Kurulu' kurulmuştur [192].

Anayasada Yapılan Değişikliklere Uyum Sağlanması Amacıyla Bazı kanun ve KHK'larda Değişiklik Yapılması Hakkında 09 Temmuz 2018 tarih ve 703 Sayılı KHK ile 'Siber Güvenlik Kurulu' görevleri Cumhurbaşkanlığına devredilerek kaldırılmıştır [206]. Siber güvenlikle ilgili bazı görev ve sorumluluklar Cumhurbaşkanlığına bağlı 'Dijital Dönüşüm Ofisi' tarafından yürütülmektedir.

- **Kuruluşundan 6 yıl sonra kaldırılan Ulusal Siber Güvenlik Kurulunun yapısı;**

Başkan: Ulaştırma Denizcilik ve Haberleşme Bakanı
Üye : Dışişleri Bakanlığı Müsteşarı,
Üye : İçişleri Bakanlığı Müsteşarı,
Üye : Milli Savunma Bakanlığı Müsteşarı,
Üye : UDHB Müsteşarı,
Üye : Genelkurmay MEBS Başkanı,
Üye : MİT Müsteşarı,
Üye : Kamu Düzeni ve Güvenliği Müsteşarı,
Üye : TÜBİTAK Başkanı,
Üye : BTK Başkanı,
Üye : Mali Suçları Araştırma Kurumu (MASAK) Başkanı,
Üye : Telekomünikasyon İletişim Başkanlığı (TİB) Başkanı (TİB 15 Ağustos 2016'da kapatıldı).

- **Siber Güvenlik Kurulunun görev ve yetkileri;**

- 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 şeklinde belirlenmiştir. [193]

Etkinliği tartışılmakta olan söz konusu kurulun 4'üncü toplantısı 2016 yılında yapılabilmiş ve toplantı sonrasında yayımlanan 2016-19 Ulusal Siber Güvenlik Strateji ve Eylem planında "Siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesi oluşturulması" [17] ihtiyacının vurgulandığı görülmektedir.

Ulusal Siber Güvenlik Kurulunun bir kısım görevlerini de üslenen Dijital Dönüşüm Ofisinin alt hizmet birimleri ve görevleri, Cumhurbaşkanlığı teşkilatı hakkında cumhurbaşkanlığı kararnamesinde değişiklik yapılmasına dair, 24 Ekim 2019 Tarihli ve 30928 Sayılı Resmî Gazetede yayımlanarak yürürlüğe giren 48 Numaralı Cumhurbaşkanlığı Kararnamesi ile ayrıntılı olarak belirlenmiştir [219].

- Başkanının aynı zamanda 'Türkiye Dijital Dönüşüm Lideri' olduğu belirtilen Dijital Dönüşüm Ofisi'nin görevleri özetle;

- 'Dijital Türkiye' (e-Devlet) hizmetlerinin sunumuna aracılık etmek, kurumlar arası iş birliğini artırmak ve bu alanlarda koordinasyonu sağlamak ve kamu dijital dönüşüm yol haritasını hazırlamak,
- Bilgi güvenliğini ve siber güvenliği artırıcı projeler geliştirmek,
- Kamuda öncelikli proje alanlarında yapay zekâ uygulamalarına öncülük etmek ve koordinasyonu sağlamak,
- Görev alanına giren konularda politika ve strateji önerilerinde bulunmak.

- Dijital Dönüşüm Ofisi'nin Teşkilatı aşağıdaki birimlerden oluşmaktadır.

- Dijital Dönüşüm Koordinasyon Dairesi Başkanlığı,
- Dijital Teknolojiler, Tedarik ve Kaynak Yönetimi Dairesi Başkanlığı,
- Dijital Uzmanlık, İzleme ve Değerlendirme Dairesi Başkanlığı,
- Siber Güvenlik Dairesi Başkanlığı,
- Büyük Veri ve Yapay Zekâ Uygulamaları Dairesi Başkanlığı,
- Uluslararası İlişkiler Dairesi Başkanlığı,
- Bilgi Teknolojileri Dairesi Başkanlığı,
- Yönetim Hizmetleri Dairesi Başkanlığı,
- Hukuk Müşavirliği.

- Siber güvenlik ile ilgili faaliyetlerden sorumlu birim olan 'Siber Güvenlik Dairesi Başkanlığı'nın Görevleri ise şu şekilde belirlenmiştir.

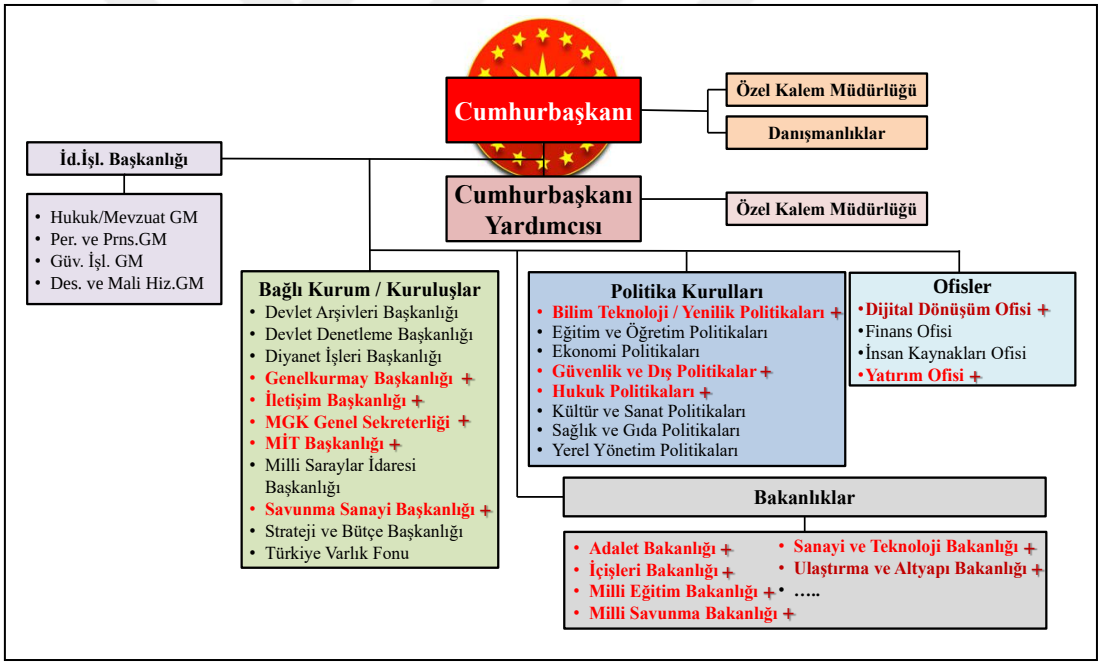
- Cumhurbaşkanınca belirlenen politikalar kapsamında kamu kurumlan ve kritik altyapılara yönelik siber güvenlik stratejileri geliştirmek.
- Ulusal siber güvenlik ve bilgi güvenliğini destekleyici projeler geliştirmek.
- Siber güvenlik ile ilgili politika, strateji ve eylem planlarının ülke çapında etkin şekilde uygulanmasına yönelik gelişmeleri takip etmek.
- Kritik altyapıların belirlenmesine yönelik çalışmalar yapmak.
- Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşlar konusunda ilgili kurumlara önerilerde bulunmak.
- Kamu, özel sektör ve üniversiteler arasındaki iş birliğinin artırılması suretiyle ulusal siber güvenlik ekosisteminin oluşturulmasına katkı sağlamak.
- Özel sektörün kapasitesinin kritik alanlara yönlendirilmesi ve mükerrer yatırımların önlenmesi için öncelikli siber güvenlik alanlarını belirlemek.
- Kritik altyapılar başta olmak üzere her alanda, yerli ve milli siber güvenlik ürünlerinin geliştirilmesine ve bu çözümlerin kullanımının kamuda yaygınlaştırılmasına yönelik çalışmalar yapmak.
- Kritik teknoloji ve bilgi varlıklarını korumak amacıyla önleyici ve koruyucu faaliyetler konusunda çalışmalar yürütmek.
- 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.

Belirlenen yeni teşkilat ve görevlendirmelere karşın, Ulusal Siber Güvenliğin yönetimi konusunda siber güvenlikte koordinasyonu sağlayacak güçlü bir kamu otoritesi yerine çok başlılık ve kaldırılan Siber Güvenlik Kurulu'nun görevlerinin tamamının yerine getirilmesi konusunda belirsizlikler devam etmektedir.

Halen Türkiye Cumhuriyeti Cumhurbaşkanlığı yönetim yapısında görev ve sorumluluk alanları dolayısıyla, 6 Bakanlık, 5 Başkanlık, 3 Kurul ve 2 Ofis ulusal siber güvenlik konusuna dâhil olup yetki ve görevleri çerçevesinde yönetim ve katılım sağlamaktadırlar (Şekil 6.5).

- **T.C. Yönetiminde siber güvenlikle ilgili görevli yapılar;**

- Bakanlıklardan Adalet (Kişisel Verileri Koruma Kurumu, Siber suçlar, Adli Bilişim ve Bilişim Hukuku), İçişleri (Siber Suçlar, Siber Terör ve Siber İstihbarat), Milli Eğitim Bakanlığı (Siber Güvenlik Eğitimi), Milli Savunma (Siber Güvenlik ve Savunma), Sanayi ve Teknoloji (Eğitim, Denetim, Ar-Ge ve Yatırım) ve Ulaştırma ve Altyapı (Strateji, Bilişim, Haberleşme ve Ulusal Siber Olaylara Müdahale) Bakanlıkları,
- Cumhurbaşkanlığı bağlısı kurum ve kuruluşlardan Genelkurmay, İletişim, Milli İstihbarat Teşkilatı (MİT), Savunma ve Sanayi Başkanlıkları ve Milli Güvenlik Kurulu Sekreterliği,
- Cumhurbaşkanlığı Kurullarından Bilim Teknoloji/Yenilik Politikaları, Güvenlik ve Dış Politikalar ile Hukuk Politikaları,
- Cumhurbaşkanlığı Ofislerinden Dijital Dönüşüm ve Yatırım Ofisleri.



Şekil 6.5: T.C. Yönetiminde siber güvenlikle ilgili görevli yapılar (+) işaretli.

Her seviyedeki kurum ve kuruluşların asli görev alanları, yetki ve sorumlulukları kanun ve yönetmeliklerle belirlenmiş olmakla birlikte, siber güvenlik konusunda esas ve prensipler ile sınırlar tam belirlenmediği için, tekrarlar ve karışıklıklar olmasının yanında ulusal güvenlik açısında eksik bırakılan ve etkinlik sağlanamayan alanlar bulunmaktadır. 2016-19 Ulusal Siber Güvenlik Strateji ve Eylem Planında yer alan beş önemli eylemden birisi ve ülke güvenliği için yaşamsal önem de olan 'Siber

Güvenliğin Milli Güvenliğe Entegrasyonu' [17] konusu da bunların başında gelmektedir.

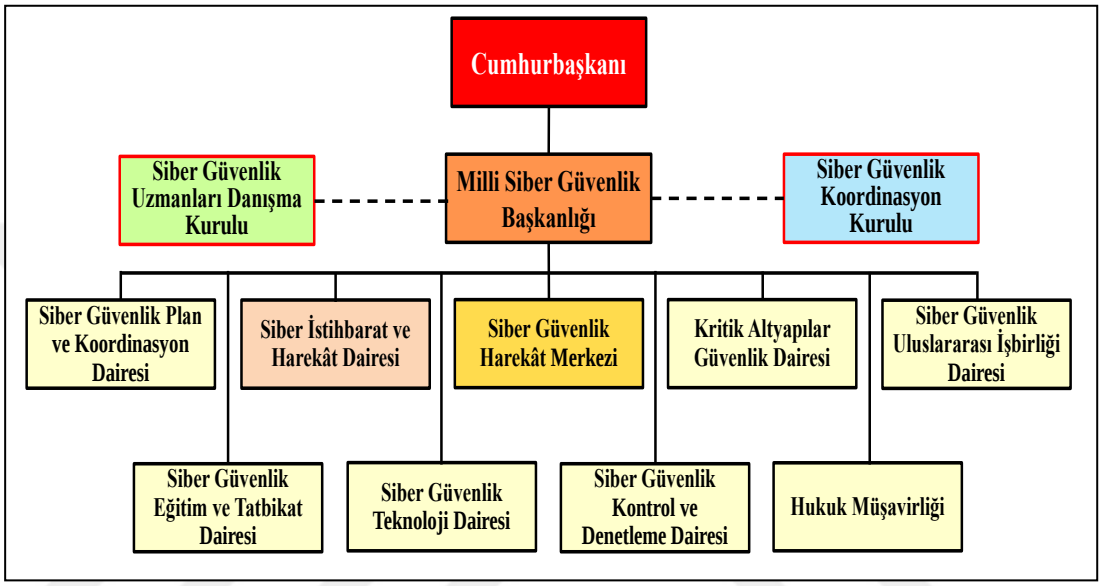
2016-19 Ulusal Siber Güvenlik Strateji ve Eylem Planının süresi geçmesine rağmen halen güncellenememiştir. 2020 - 2023 Ulusal Siber Güvenlik Strateji ve Eylem Planının hazırlanması çalışmaları Ulaştırma ve Altyapı Bakanlığı (UAB) sorumluluk ve koordinesinde devam etmekte ve 2020 yılı sonuna kadar yetiştirilmesi hedeflenmektedir. Bir konferansta açılış konuşması sırasında yeni strateji ve eylem planı hazırlıkları ile ilgili bilgi veren UAB Bakan Yardımcısı, Türkiye'de siber güvenlikten UAB (BTK, Haberleşme Gn.Md.lüğü), Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Adalet Bakanlığı (KVKK) ve Savunma Sanayi Başkanlığı (Siber Güvenlik Kümelenmesi)'nın sorumlu olduğunu ve yeni ulusal siber güvenlik stratejisi ve eylem planının da bu yapıların ana sorumluluk ve koordinesinde devam ettiğini belirtme ihtiyacı duymuştur [220].

Ulusal Siber Güvenliğin yönetimi konusunda, siber güvenlikte koordinasyonu sağlayacak güçlü bir kamu otoritesi ihtiyacını karşılamak ve konuyla ilgili belirsizlikleri gidermek maksadıyla, ülkenin siber güvenliğinden her bakımdan sorumlu olacak ve ülkenin 5'inci Harekât Alanı olan siber uzayında 'Siber Ordu Komutanlığı Karargâhı' olarak görev yapacak olan etkili bir teşkilat kurulmalıdır. Böyle bir teşkilatın kurularak ulusal siber güvenliğin yönetim ve koordinasyonunun tek elden sahiplenilmesi bile stratejide etkinlik yanında aynı zamanda caydırıcılık sağlayıcı bir rol oynayacaktır.

Bu Tez çalışmasında bu maksadın yerine getirilmesi için uygun bir hal tarzı olarak, Cumhurbaşkanlığına bağlı 'Milli Siber Güvenlik (MSG) Başkanlığı' kurulması önerilmiştir. Bir hal tarzı olarak önerilen MSG Başkanlığının ana teşkilat yapısı Şekil 6.6'da sunulmuştur

Ulusal Siber Güvenlik Başkanlığı 7 Daire Başkanlığı, bir Harekât Merkezi ve bir Müşavirlikten oluşmaktadır. Başkanlık bu yapılanmasıyla, siber güvenlikle ilgili ulusal politika ve stratejilerin geliştirilmesi, planlama ve koordinasyon çalışmalarının yürütülmesi (Plan ve Koordinasyon D.), siber istihbarat dâhil siber ortamda icra edilecek savunma, taarruz ve caydırıcılık vb. bütün harekât çeşitlerinin icrası (İstihbarat ve Harekât D.), siber güvenlik kriz yönetimi dâhil siber olaylara müdahale (Harekât Merkezi), kritik altyapıların siber güvenliği (Kritik Altyapılar Güvenlik D.),

uluslararası işbirliği ve koordinasyonun sağlanması (Uluslararası İşbirliği D.), eğitim ve tatbikat ihtiyaçlarının giderilmesi ve siber güvenlik uzmanlarının yetiştirilmesinin koordine ve yönlendirilmesi (Eğitim ve Tatbikat D.), siber güvenlik teknoloji araştırma ve geliştirme çalışmalarının yönlendirilmesi (Teknoloji D.), siber güvenlikle ilgili her türlü destek, kontrol ve denetim faaliyetlerinin yürütülmesi vb. (Kontrol ve Denetleme D.) ile başkanlığın faaliyetleri ve siber güvenlik ile ilgili adli görevlerin yerine getirilmesinden (Hukuk Müşavirliği) sorumlu olacaktır.



Şekil 6.6: Milli Siber Güvenlik Başkanlığı yapılanması önerisi.

MSG Başkanı, daha önce 2012'de kurulan ve 2018'de kapatılan Siber Güvenlik Kuruluna benzer şekilde ilgili kamu kurum ve kuruluşların yetkili temsilcilerinin katılımıyla oluşturulacak, Siber Güvenlik Koordinasyon Kuruluna (SGKK) da başkanlık edecektir. SGKK karar alma organından çok bir onay ve koordinasyon kurulu olarak görev yapacak olmakla birlikte gerektiğinde ve MSGB tarafından talep edildiğinde, siber güvenlik alanında stratejik hedefler oluşturma ve politika belirmek için de çalışmalar yapacaktır.

Danışmanlık hizmeti ve desteği vermek üzere, üniversitelerden akademisyenler arasından, kamu kurumlarından, özel sektör ve sivil toplum kuruluşlarından siber güvenlik konusunda uzmanlardan ve bilim adamlarından oluşan Siber Güvenlik Uzmanları Danışma Kurulu (SGUDK) oluşturulacaktır. SGUDK başlangıçta dokuz uzmandan oluşturulacak, uzmanların dördü MSG Başkanının, beşi SGKK önerisiyle belirlenecek ve Cumhurbaşkanının onayıyla görevlendirilecektir. Bu kurul üniversitelerde görev yapan danışma kurulları benzeri görev yapacaklar, MSG

Başkanlığının çalışmaları ve uygulamaları, siber güvenlik konusunda geleceğe dönük ihtiyaçlar ve hareket tarzları ile ulusal siber güvenlik stratejisi ve eylem planları hakkında değerlendirmeler yapacak, görüş ve önerilerde bulunacaktır.

MSG Başkanlığı sorumluluğu ve koordinesinde hazırlanacak siber güvenlik strateji ve politikalarının SGKK tarafından incelenip görüşülerek onayı sonrasında uygulamaya konulması ve etkinlikle uygulanması, denetimi ve kontrolü ile ihtiyaç durumunda günün koşullarına göre geliştirilmesi sağlanacaktır.

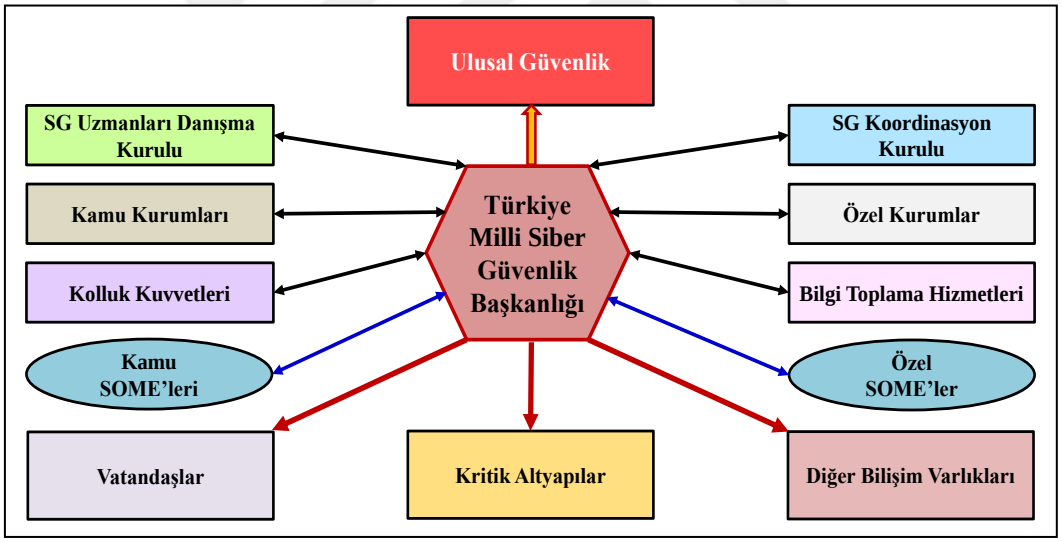
Siber Güvenlik Harekât Merkezi aynı zamanda Ulusal Siber Olaylara Müdahale (USOM) ve kriz yönetim merkezi olarak görev yapacaktır. MSG Başkanlığı Siber İstihbarat ve Harekât Dairesi ile Türk Silahlı Kuvvetleri (Siber Savunma Komutanlığı), MİT Başkanlığı, Jandarma Genel Komutanlığı ve Emniyet Genel Müdürlüğü birimleri ile tam koordinasyon içerisinde, birlikte veya yalnız, siber güvenlik ve savunma dışında da, gerektiğinde her türlü siber saldırı, taarruz ve caydırıcılık harekâtı planlayıp icra edilmesini sağlayabilecektir.

Mevcut durumda Dijital Dönüşüm Başkanlığı, siber güvenlikle ilgili bazı yetki, görev ve sorumlulukları üstlenmiş olsa da, başta oluşumun ismi olmak üzere ülkenin kurum ve kuruluşlarının sayısal dönüşümünün sağlanması ve bu konudaki Ar-Ge çalışmalarının koordinasyonu kapsamındaki çoklu görev ve sorumlulukları ile diğer kamu kurum ve kuruluşlarla bağlantıları dolayısıyla ulusal siber güvenlik strateji ve politikalarının oluşturulması ve uygulanmasında verimli ve yeterli seviyede etkin olması mümkün görülmemektedir.

6.4 Kapsam, Görev ve Sorumlulukların Belirlenmesi

Ulusal Siber Güvenlik Stratejisi, bir ülkedeki tek bireyden başlayarak, bütün özel (gerçek) ve tüzel kişilere, kamu ya da özel bütün kurum ve kuruluşlara, siber ortamı kullanan bütün varlıkları ve bileşenlerini kapsamaktadır. Siber ortamda mutlak güvenlik yani yüzde yüz güvenlik mümkün olamayacağı gibi, bütün varlıkların ve bileşenlerin siber güvenliklerinin aynı seviyede sağlanması da mümkün değildir. Siber güvenlik gücünün ve kapasitesinin etkin kullanılması için önem ve önceliklerin belirlenmesi gerekmektedir.

Siber güvenlik stratejisinin bu bölümünde, ulusal güvenlik ile tam bir bağlantı ve uyum içerisinde kapsama alanına giren bütün kişi, kamu / özel kurum ve kuruluşlar dâhil bütün devlet kademeleri, genel anlamda görev ve sorumlulukları belirtilerek ortaya konmalıdır. Temel hedef kritik altyapı bilişim sitemlerinin korunması başta olmak üzere vatandaşlar dâhil bütün bilişim sistemlerinin ve değerli varlıklarının korunmasıdır. Bu nedenle ülkenin siber güvenliği ve savunması için en tepedeki kamu oluşumundan en alttaki tek vatandaşa kadar bütüncül bir koruma yaklaşımı izlenmelidir. Siber ortamı kullanan birey için kişisel siber güvenlik öncelikle kendi sorumluluğudur. Ancak bu konuda eğitimi ve farkındalığının sağlanması için devletin görev ve sorumluluğu da bulunmaktadır. Ülkenin siber savunması söz konusu olduğunda tek bireyin bile yapması gereken eylemler ve katkıda bulunabileceği hususlar olabilir. Bu bağlamda, Türkiye'nin siber güvenlik yapılanması, yönetim ve koordinasyonu ile bağlantıları ve bütünleşimi için, bu Tez çalışmasıyla önerilen Şekil 6.7'de görülen düzenlenme ve çalışmaların bu bakış açısıyla sürdürülmesi kısa sürede başarılı sonuçlar alınmasını sağlayacağı değerlendirilmektedir.



Şekil 6.7: Ulusal siber güvenlik yönetimi, koordinasyonu ve bütünleşimi.

Ülkenin kritik altyapılarının bilişim sistemlerinin korunması, devletin siber güvenlik önceliklerinde en üst sıralarda yer almalıdır. Ancak bu altyapıların sahipleri olan kamu / özel sektörlerin de yerine getirmeleri gereken görevleri ve sorumlulukları olacaktır. Bu konuda görev ve sorumluluk paylaşımları belirlenmeli, bunların yerine getirilmesinin kontrol ve denetim esasları ile yaptırımları ortaya konmalı, bu maksatla planlamalar ve yasal düzenlemeler yapılmalıdır.

6.5 Planlamaların Yapılması

Ulusal siber güvenlik stratejisinin bu bölümünde, durumun değerlendirilmesi aşamasında vazifenin analizinde ortaya konulan açık ya da kapalı görevlerin yerine getirilmesine ve hedefin belirlenmesi aşamasında ulaşılması gerektiği düşünülen hedef ve / veya hedeflere yönelik hareket tarzları ortaya konularak incelenir. İncelemeler sonrası varılan kararları uygulamak için siber güvenlikten sorumlu teşkilat tarafından ya da onun sorumluluk ve koordinesinde ilgili devlet kademeleri, kamu / özel kurum ve kuruluşlar tarafından gerekli planlar yapılır. Gerçek verilere dayalı ve gerçekçi kararların plana dönüştürülmesi sırasında en basit tanımlamayla, "Kim / Kimler, Ne maksatla, Ne zaman / Ne Kadar Sürede, Nerede, Nasıl ve Ne / Neler Yapacak" sorularına cevap verilmelidir.

Askeri faaliyetlerde ve halk arasında özellikle tehlikeli iş alanlarında çok sık kullanılan "Önce Emniyet, Sonra Hareket!" özdeyişi, siber güvenlikte önemli bir prensiptir. Bu prensipten hareketle, planlamada öncelik savunmadadır. Siber saldırı ve olaylara karşı koymak için ulusal siber olaylara müdahale sistemlerinin (Siber Olaylara Müdahale Merkezi / Ekipleri vb.) kurulması ve işletilmesine yönelik planlamalar öncelikli olarak yapılır. Bu kapsamda ülkenin siber gücünün en büyük ve önemli kısmını oluşturan kritik altyapılarının bilişim sistemlerinin dökümleri (envanterleri) çıkarılarak bunların siber güvenliğinin sağlanmasına yönelik ayrıntılı planlar öncelikle yapılmalıdır.

Siber saldırılara karşı korunma, kriz yönetimi, gerektiğinde misilleme, siber istihbarat ve istihbarata karşı koyma, siber savunma, taarruz ve caydırıcılık vb. her türlü siber harekât türüne yönelik planlar hazırlanmalıdır. Planlar siber gücün tek başına kullanımın yanında, diğer güç unsurlarının yönetiminden sorumlu devlet kademelerinin, kamu veya özel kurum / kuruluşlarının planlarıyla koordineli ya da onları desteklemeyi içerecek şekilde seçenekli olmalıdır. Strateji ve politikaların uygulanması sırasında, yapılacak kontrol ve denetim faaliyetlerinin etkinliğini artırmak için, denetim ve kontrollere başlamadan önce stratejik planlarda belirlenen bütün hedeflerin tarafsız ve ölçülebilir göstergeler ile bağlantılandırılması gerekir. Planların ve belirlenen hedeflerin anayasa ve kanunlara, uluslararası anlaşmalar ve yükümlülüklere aykırı olmamasına dikkat edilmelidir.

6.6 Stratejinin Uygulanması

Bütün stratejilerde olduğu gibi, siber güvenlik stratejisinin de en önemli bölümü ve aşamalarından birisi uygulama aşamasıdır. Çünkü planlar kusursuz ve en iyi hareket tarzını içeren en mükemmel çalışmalar olsa da başarısı uygulanmasına bağlıdır. Tarihte kâğıt üzerinde veya düşünce de başarı ve zafer vaat eden çoğu plan ya uygulanmadığı için, ya da doğru uygulanmadığı için sonuçta beklenen amaçlar gerçekleştirilememiş ve hedeflere ulaşılamamıştır.

Planlar merkezi olarak yapılıp ayrı ayrı ellerle uygulanabileceği gibi, görev ve sorumluluğu olan kademelerce yapılıp aynı ellerle de uygulanabilir. Planların uygulanmasında diğer önemli hususlar gizlilik kurallarına ve zamanlamasına uyulması, uygulamadan doğan aksaklıkların giderilmesi için zamanında gerekli düzeltme ve değişikliklerin yapılması, uygulanacak planların güncellemelerin aksatılmaması vb. sıralanabilir.

Siber güvenlikte başarı ayrıntılı, geniş kapsamlı, bütüncül yaklaşım ve uygulamadadır. Planı uygulayan kademe, kurum / kuruluşun başta yönetim kademesi olmak üzere bütün unsurları planı sahiplenmeli, her çalışanı üzerine düşen görev ve sorumlulukları eksiksiz yerine getirmelidir. Bütün bilişim sistemlerinde olduğu gibi, bütün siber güvenlik planları da insan içerdiği için uygulanmasında, güvenlik zincirindeki en zayıf halkanın insan olduğu ilkesi unutulmamalıdır.

Planların uygulamasında görev ve sorumlulukların yerine getirilmesi için gerekirse kişi, sistem ve hatta cihaz bazında ayrıntılı olarak takip ve kontrol maksatlı faaliyetler icra edilmelidir. Faaliyetlerin belirlenen ilgili kişi / kişiler tarafından, yöntem ve zamanlarda gerçekleştirilip gerçekleştirilmediği yakından izlenmeli ve sonuçları mutlaka takip edilmeli, anlık ve periyodik değerlendirmelere göre gerekli tedbirler alınmalı, aksaklıklar gecikmeksizin düzeltilmeli, varsa eğitim eksiklikleri giderilmeli, başarılarda ödüllendirme, başarısızlık yetersizlik ve ihmal vb. durumlarda cezai yaptırımlar uygulanmalıdır.

6.7 Kontrol ve Denetimlerin Yapılması

Planların planlandığı şekilde uygulanıp uygulanmadığı, planlanan hedeflere ulaşılıp ulaşılmadığı veya ne kadar ulaşıldığı, ne kadar kazanç elde edildiği veya verim alındığı

bu aşamada yapılacak kontrol ve denetim faaliyetleri ile belirlenir. Bu bölüm kısaca stratejik plan uygulamasının sistematik olarak izlenmesi, kontrol edilmesi, denetlenmesi ve raporlanması aşamasıdır.

Bilimsel anlamda yapılacak kontrol ve denetim faaliyetleri, gelişmiş istatistiksel verilere ve ISO / IEC 27000, COBIT vb. ulusal / uluslararası ölçünlere dayanarak hazırlanan denetim listelerine yapılmalı, planın uygulama sonuçları amaç ve hedeflere göre kıyaslanarak ölçülmeli ve söz konusu amaç ve hedeflerin tutarlılık ve uygunluğu analiz edilmelidir. Bu konunun önemi, Avusturyalı yönetim bilimi uzmanı Peter Drucker tarafından "Ölçemediğiniz şeyi kontrol edemezsiniz, kontrol edemediğiniz şeyi yönetemezsiniz!" [221] sözüyle vurgulanmıştır.

Kontrol ve denetim faaliyetleri iç ve dış denetim ve kontrol faaliyetleri şeklinde yapılır. İç denetim ve kontrol faaliyetleri planları uygulayan kademelerin üst yönetimlerince, dış denetim faaliyetleri ise ulusal siber güvenlik strateji yönetiminin ilgili kurulları veya belirlediği yetkili birimler tarafından önceden hazırlanacak eylem planlarına göre yapılmalıdır.

Kontrol ve denetim eylem planları, sorumlu kişi, grup, kurum / kuruluş vb. yapısal birimleri, stratejik planda yerine getirilecek görevleri, amaçları ve ulaşılacak hedefleri içeren kontrol formlarını, takip edilecek ve kullanılacak ölçünleri içermelidir. Denetim faaliyetleri tarafsız olarak yapılmalı, sonuçları önceki denetim ve kontrol faaliyetleri sonuçları ile kıyaslanarak objektif raporlar halinde ortaya konmalıdır. İlerleme sağlanan ve sağlanamayan alanlar, ulaşılan ve ulaşılamayan hedefler belirtilmeli ve müteakip aşamada iyileştirme ve geliştirme faaliyetlerinde kullanılmak üzere gerekli değerlendirmeler yapılmalıdır.

6.8 Stratejinin Geliştirilmesi

Ulusal siber güvenlik stratejisi oluşturulmasının ve uygulanmasının son bölümü olan geliştirme aşaması, bütün aşamaların gözden geçirilerek başta yapılan ve uygulamaya konulan planlar olmak bütün sürecin iyileştirilmesi ve geliştirilmesi aşamasıdır. Süreç içerisinde, kontrol ve denetim faaliyetleri sonucunda hazırlanan raporlardaki bilgiler ve tespitler kullanılarak, başta planlar olmak üzere bütün strateji gözden geçirilir, hedeflenenlerle sonuçlar ve elde edilen kazanımlar karşılaştırılır.

Planlanan faaliyetler ile yapılan uygulamalar arasında ortaya çıkan farklılıkların, olumsuzlukların ve sapmaların nedenleri araştırılır. Uygulamada tespit edilen hatalar, kusurlar, yanlışlar, eksiklikler ve yetersizlikler ile olumlu görülen bütün hususlar denetim uzmanlarının değerlendirmeleriyle birlikte incelenir. İncelemeler ile öncelikle olumsuzlukların ortadan kaldırılmasına, olumlu hususların ise planlamalara dâhil edilerek daha da geliştirilmesine yönelik çalışmalar başlatılır.

Bu çalışmalar stratejinin oluşturulmasındaki ilk dört aşamada yer alan durum, teşkilat, kapsam ve planlama bölümlerindeki çalışmaların gözden geçirilmesi, yeniden düzenlenmesi ve güncellenmesi faaliyetlerinden oluşur. Ulusal siber güvenlik stratejisi, bir yaşam döngüsü şeklinde sürdürülmesiyle iyileştirilerek geliştirilir. İlgili bütün sıralı yönetim ve kurullarca, geliştirme çalışmalarının gerekli önem verilerek ve aksatılmadan yürütülmesi, bu konuda aynı zamanda eğitimler verilmesine, dersler çıkarılmasına ve kurumsal olarak bir kültürün oluşmasına da büyük katkılar sağlamış olur.

7. SONUÇLAR

Çağımızda bilgisayar ve iletişim teknolojilerindeki gelişmelere paralel olarak, ülke veya kurum içinden veya dışından, suç örgütleri, teröristler, bilgisayar korsanları, casuslar vb. saldırı düzenleme kapasitesine sahip kişi, grup ve devletler tarafından yapılabilen siber saldırıların, teknoloji geliştikçe çeşitleri, şiddeti ve sayıları ile teknik açıdan karmaşıklığı artarken, saldırı yapma uzmanlığı ve becerisi diğer bir ifadeyle saldırganların bilgi seviyelerinin ve uzmanlıklarının ise gittikçe azaldığı, buna paralel olarak tehdit kaynaklarının ve risklerin yanında saldırılar sonucunda verilebilecek zararların daha da arttığı ve saldırıları tespit ve önleme tedbirlerinin ise zorlaştığı açıkça gözlenmektedir

Çok sayıda ülkede yaşanan siber saldırılar ve olaylar analiz edildiğinde, etkilerinin ve verilen zararların yüksek olmasında ortak temel nedenler;

- Siber güvenlikle ilgili yasa ve politikaların yeterli olmaması veya etkin uygulanmaması
- Teknoloji ve altyapı yetersizlikleri, saldırılara karşı bilgi sahibi ve hazırlıklı olmama,
- Kullanıcıların eğitim ve farkındalık eksikleri, kurum ve kuruluşlar arasında koordinasyon ve iş birliğinin olmaması vb. şeklinde yaygın kabul görmektedir.

Bilişim teknolojilerinin geliştiği ve hızla gelişmeye de devam ettiği günümüzde, bilgisayar ve iletişim teknolojilerinin sağladığı imkân ve kolaylıklardan etkin şekilde yararlanmak ve yukarıda da kısaca sıralanan olumsuzlukları gidermek için siber güvenliğin önemi her geçen gün daha iyi anlaşılmakta ve ihtiyaçlar artmakta, etkin siber güvenlik ve savunmanın da her şeyden önce, Ulusal Siber Güvenlik Stratejisi oluşturulması ve uygulanması ile sağlanacağı görülmektedir. Çünkü siber saldırı olayları analiz edildiğinde, başarılarının, etkilerinin ve verilen zararların yüksek olmasında temel nedenlerinin başında savunmaya yönelik yerel ve ulusal stratejilerin bulunmaması ya da bulunsa bile bunların yeterli olmaması veya etkin uygulanmaması gelmektedir.

Ulusal siber güvenlik stratejisi ve politikaları oluşturulurken, öncelikle siber ortamla ilgili temel kavramlar doğru anlaşılmış ve bu konuda terim birliği sağlanmış olmalıdır. Ulusal Siber Güvenlik Stratejisi, ulusal siyaset / strateji esaslarına göre yapılandırılmalı, dünyada uygulanan kuramsal yaklaşımlar ve teknolojik gelişmeler dikkate alınarak, bunlardan azami yararlanılarak ve bilimsel yöntemlerle çalışılarak ortaya konmalıdır.

Yapılan bu Tez çalışmasıyla, Ulusal siber güvenlik stratejisi ve politikalarının oluşturulması ve uygulanması konusunda bir yaklaşım tarzı olarak; bilimsel taktik ve teknikler çerçevesinde, mevcut durumun değerlendirilmesinden belirlenen hedefe ulaşılmasına kadar teşkilat, kapsam, planlama ve uygulama aşamaları ile süreç içerisinde kontrol ve denetim faaliyetleri ile geliştirme faaliyetlerini içeren 8 aşamalı "Ulusal Siber Güvenlik Stratejisi Oluşturma ve Uygulama Yaşam Döngüsü" önerilmiştir.

Durum ayrıntılı olarak değerlendirilmeli, vazifeler ulusal yasalara, politikalara ve stratejiye göre analiz edilmeli, stratejik hedef / hedefler nesnel (objektif) olarak belirlenmelidir. Her şeyden önce, ülkenin haberleşme, enerji, su yönetimi, kritik kamu hizmetleri, ulaştırma, bankacılık ve finans gibi kritik altyapılarına yönelik siber saldırılara karşı korunması için siber gücün öncelikle savunma maksatlı olarak artırılması ve kritik altyapılar başta olmak üzere, ülkenin kamu, özel ve bireysel bütün bilişim varlıklarının etkinlikle savunulması gerekmektedir.

Tarihte sadece savunmayla hiçbir zafer kazanılmamış, karşı saldırı ve taarruz yeteneğinin de kazanılmasının ve kullanılmasının gerekli ve kaçınılmaz bir zorunluluk olduğu anlaşılmıştır. Siber güvenlikte de sadece güvenlik tedbirlerini artırarak başarılı olmak mümkün değildir. Türkiye'de geçmişten bugüne siber güvenlik strateji ve politikaları incelendiğinde, siber caydırıcılık konusuna gereken önemin verilmediği ve siber saldırılara karşı doğrudan veya dolaylı olarak caydırıcılık sağlanması için yapılan çalışmaların da yetersizliği de ortaya çıkmıştır. Siber ortamda güvenlik için savunma yanında mutlaka taarruz da düşünülmeli, savunma veya taarruz şeklinde icra edilecek mücadele ve savaşlarda, maksat istek veya istekleri karşı tarafa zorla kabul ettirmek ve temel amaç kazanmak olsa da, Sun Tzu'nun "En iyisi savaşmadan baş eğdirmektir" özdeyişinden de hareketle, siber savaşta saldırganı saldırıdan veya savaştan

caydırmak, yani siber caydırıcılığın en iyisi olabileceği esas ve prensip olarak kabul edilmelidir.

Siber saldırılarda caydırıcılığı sağlamak için; saldırılara karşı önceden etkili bir siber savunmaya hazır olarak karşı konulmalı, etkin bir karşı saldırı ve taarruzla hedefe ulaşma gücüne, ancak hem savunmada ve hem taarruzda, kısaca savaşta başarının vazgeçilmezi olan etkin siber istihbarat yeteneğine sahip olunmalıdır. Siber caydırıcılıkta en büyük zorluklardan birisi olan saldırganın kimliğinin tespiti ve dayandırma (isnat) güçlü istihbaratla sağlanabilecektir.

Siber ortamda savunma, taarruz, caydırıcılık ve istihbarat yetenekleri bilgi, bilgisayar ve iletişim konularında ulusal teknolojilere sahip olunarak desteklenmeli, ulusal teknolojilere sahip olunamayan alanlarda sahip olunan teknolojilere hâkim olunmalıdır. Siber güvenlik, savaş ve caydırıcılık için teknik yetersizliklerin giderilmesi, saldırıların tespiti ve önlenmesi yanında, güçlü saldırı silahı, teknik ve yöntemlerinin geliştirilerek etkin misilleme ile saldırganın cezalandırılması teknolojik yetkinlik ile mümkün olabilecektir.

Yerli ve ulusal olmayan bilişim sistem ve teknolojileri ile ulusal siber ortamın güvenliğini gerçek anlamda sağlamanın mümkün olmayacağı açıktır. Bu kapsamda bilişim ve siber güvenlik konusunda, güvenli yazılım başta olmak üzere, Ar-Ge, üretim, yerli ve ulusal ürünlerin kullanımının yaygınlaşması büyük önem taşımaktadır. Bu konuda, 2016-19 Ulusal Siber Güvenlik Strateji ve Eylem Planında belirlenen ana eylemlerden birisi olan 'Siber Güvenlik Ekosisteminin Geliştirilmesi' kapsamında oluşturulan 'Türkiye Siber Güvenlik Kümelenmesi' çalışmaları yerli ve ulusal siber güvenlik ürünleri geliştirilmesi için etkili olabilir.

Türkiye'de bilgi güvenliğinin sağlanmasında şifreleme alanında oldukça olumlu gelişmelere karşın, yaygın bir ulusal işletim sisteminin bulunmaması, TÜBİTAK tarafından geliştirilen ve büyük ümitler beslenen PARDUS işletim sisteminin istenen ve beklenen hedefe ulaştırılamamış olması, bunun için gerekli çabaların gösterilerek atılması gereken adımların atılmaması öncelikle siber güvenlik açısından büyük bir eksiklik ve olumsuzluktur. PARDUS işletim sistemi gibi yine TÜBİTAK tarafından geliştirilen 'Ahtapot Bütünleşik Siber Güvenlik Sistemi' ve TSK Güçlendirme Vakfına bağlı savunma sanayi şirketi HAVELSAN tarafından geliştirilen PARDUS ile uyumlu 'Bariyer Veri Sızıntısı Önleme (Data Leakage Prevention - DLP) Sistemi'

gibi siber güvenlik sistemleri ve ürünleri daha da geliştirilip yaygınlaştırılırken, yeni ve daha güçlü saldırı saptama ve önleme, virüse karşı koyma sistemleri, açıklık tarama ve önleme, arama motoru vb. alanlarda yerli ve ulusal sistem ve yazılımların gecikmeksizin geliştirilmesi ve uygulamaya konularak yaygınlaştırılması yaşamsal önemdedir. Söz konusu yazılım ve sistemlerin yaygınlaştırılmasında özellikle internet altyapı ve hizmet sağlayıcı kurum ve kuruluşlara da gerekli görev ve sorumluluklar verilerek uygulanması sağlanmalıdır. Siber güvenlik ve savunma yazılım ve sistemleri geliştirilirken caydırıcılık maksatlı siber saldırı ve taarruz yazılım ve sistemlerine de gereken önem ve öncelik verilmeli, bu konuda yazılım, donanım ve personel kapsamlı adımlar gecikmeksizin atılmalıdır.

Siyasi, askeri, ekonomik, coğrafik, demografik, bilimsel, teknolojik, sosyal ve kültürel güçten oluşan Milli Güç unsurlarının her biri uluslararası ortamda ve ilişkilerde aynı zamanda birer caydırıcılık unsuru oluşturmaktadır. Bilimsel ve Teknolojik Güç içerisinde kabul edilen, ancak ayrı bir ulusal güç unsuru olarak ele alınması gereken 'Siber Güç (siber savunma, taarruz ve caydırıcılık gücü)*'* ile de, tek başına veya diğer milli güç unsurlarıyla birlikte siber alanda, uluslararası hukuk ilkelerine bağlı kalarak, kendine özgü kural, esas ve stratejiler doğrultusunda yaptırım uygulamak ve belirlenecek amaçlar doğrultusunda tespit edilecek talep ve isteklerin gerçekleştirilmesi için strateji ve politikalar geliştirerek daha güçlü ve etkin 'caydırıcılık' sağlamak mümkündür.

Siber caydırıcılıkta temel esas ve önemli olan siber saldırıların / savaşın doğru zamanda, doğru hedefe yönelik, doğru teknik ve yöntemlerle yapılmasıdır. Bu kapsamda, 'Siber Güçle Caydırıcılık'; üzerinde düşünülmesi, daha fazla önem verilmesi, diğer alanlardaki caydırıcı gücün bu alanda da oluşturulması için ciddi ve ayrıntılı olarak çalışılması, konuyla ilgili doktrinler üretilmesi, mevcut stratejilerin bu yönde güncellenmesi, yeni stratejiler geliştirilmesi ve geleceğe dönük planlamalar yapılarak gecikmeksizin uygulamaya konulması gereken çok önemli bir konudur. Türkiye'de 6757 numaralı KHK ile verilen "….siber saldırılara karşı korunma ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alma veya aldırma" görevinin BTK tarafından etkinlikle yerine getirilmesinin gerek ve yeter koşulları halen oluşturulamamıştır. Kurum ve kuruluşlara gerekli siber güvenlik önlemlerini almadıkları için yasal para cezaları bile henüz uygulanamamıştır.

Siber güvenliğin öneminin anlaşıldığı gibi, siber gücün önemi de anlaşılmalı ve doğru şekilde yapılandırılması amaç edinilmelidir. Bu amacın başarısı ise, ulusal ve yerli üretim iş alanlarına gereken önem verilerek caydırıcılık sağlayacak şekilde yönlendirilmesi ve desteklenmesi yanında bilişim ve siber güvenlik uzman personeli ve kullanıcılarının yetiştirilmesinden geçmektedir. Kurum ve kuruluşlar siber güvenliğin sağlanması, yönetimi ve koordinasyonu ile ilgili yapılanmalarını mutlaka kurmalı, 'Siber Güvenlik Uzmanı' personel görevlendirmelerini yapmalı ve siber güvenlik yönetimi sistemlerini geliştirerek etkinlik ve kararlılıkla uygulamalıdır.

Siber gücün artırılması ve siber saldırılara karşı caydırıcılık da sağlayarak etkin güvenlik ve korunma için her alanda koordinasyon ve iş birliği gerekir. Bunun için bütün devlet kurum ve kuruluşları ile özel sektör arasında etkin iş birliği ve koordinasyon sağlanarak siber güç geliştirilmelidir. Çünkü siber güvenlik stratejisinde hedefe siber güçle ulaşılabilir. Bu bağlamda, ulusal güvenlik stratejisi ile siber güvenlik stratejisinin bağlantısı ve uyumu da mutlaka sağlanmalıdır. Siber gücün geliştirilerek artırılması ve her maksatla etkin şekilde kullanılması için uygulayıcıların yetiştirilmesi ve farkındalıklarını artıracak eğitimler verilmesi, bu maksatla özellikle siber güvenlik konularında uzman kadroların oluşturulması, her seviyede eğitim ve öğretimin planlanması ve yaygınlaştırılması gerekmektedir.

Oluşturulacak stratejinin aynı zamanda gelişmeye açık döngüsel başarısını sağlayacak en önemli hususlardan birisi olarak, siber güvenlik başta olmak üzere, siber gücün artırılması, etkin bir yönetim ve denetim sağlanması için yeniden yapılanmaya gidilmesi, 2016-2019 Ulusal Siber Güvenlik Stratejisinde belirtildiği gibi "Siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesi oluşturulması" ve siber gücü kullanma yetkilerinin tek bir merkezde toplanması kısa sürede olumsuzlukların en aza indirilerek başarının artırılmasını da sağlayacaktır.

Siber güvenlik stratejisini oluşturarak uygulayacak, siber gücü yönetecek, siber ortamda icra edilecek savunma, taarruz ve caydırıcılık vb. bütün siber harekât türleri ile siber güvenlikle ilgili ulusal ve uluslararası her türlü iş birliği, koordinasyon, destek, kontrol ve denetim faaliyetlerinin yürütülmesi vb. görevlerin yerine getirilmesinde yetkili ve sorumlu olacak olan bu teşkilatın, dünyadaki örneklerinden de yararlanılarak, bir ordu yapılanması gibi düşünülerek hayata geçirilmesi teşkilatın etkinliğini ve başarısını daha da artıracaktır.

Bu Tez çalışmasıyla önerilen, Türkiye için mevcut yönetim sisteminde Cumhurbaşkanlığına bağlı 'Milli Siber Güvenlik Başkanlığı' bu konudaki eksikliği giderecek ve ihtiyacı beklenen seviyede başarıyla ve kolaylıkla karşılayabilecektir. Ancak, Milli Siber Güvenlik Başkanlığının görev ve sorumluluklarını beklenen seviyede başarıyla gerçekleştirmesinin, büyük ölçüde bünyesinde oluşturulacak 'Siber Güvenlik Koordinasyon Kurulu' ile 'Siber Güvenlik Uzmanları Danışma Kurulu'nun etkin çalışmasına bağlı olacağı değerlendirilmektedir.

Ulusal Siber Güvenlik Stratejisi uygulanması ve yönetimi, bu Tez çalışmasıyla önerildiği şekilde, bir ülkedeki tek bireyden başlayarak, bütün özel ve tüzel kişileri, kamu ya da özel bütün kurum ve kuruluşları ve bileşenlerini kapsayacak şekilde etkin bir koordinasyon, işbirliği ve bütünleşim içerisinde gerçekleştirilmelidir. Siber güvenliği hukuki, teknik, idari, ekonomik, politik ve sosyal boyutları ile ele alan ayrıntılı ve geniş kapsamlı bir hareket tarzının benimsenmesi, gerekli yasal mevzuatın mutlaka oluşturulması ve etkinlikle uygulanması gerekmektedir. Ulusal güvenlikle bütünleşmiş Ulusal Siber Güvenlik, Mustafa Kemal Atatürk'ün "Hattı müdafaa yoktur sathı müdafaa vardır. O satıh bütün vatandır…" özdeyişinde olduğu bütün ulusal siber ortamı kapsamalıdır.

Bilişim teknolojileri ve özellikle internet sayesinde ülkelerarası etkileşimin boyutunun da derinleşmesi nedeniyle, diğer ülkelerle siber saldırılara karşı iş birliği yapılması, suçluların yakalanması ve haklarında gecikmeksizin yasal işlem yapılarak cezalandırılması, aynı zamanda caydırıcılık sağlaması yanında saldırıların azalmasını da sağlayacaktır. Yine Atatürk'ün "Yurtta barış, dünyada barış" sözünde olduğu gibi "Yurtta siber güvenlik, dünyada siber güvenlik" prensibi esas alınmalıdır. Bu konuda görev ve sorumluluklar belirlenmeli, bu maksatla planlamalar, idari ve yasal düzenlemeler yapılmalıdır.

Planlar merkezi olarak yapılıp ayrı ayrı ellerle uygulanabileceği gibi, görev ve sorumluluğu olan kademelerce yapılıp aynı ellerle de uygulanabilir. Planlar kusursuz ve en iyi hareket tarzını içeren en mükemmel çalışmalar olsa da başarısı doğru uygulanmasına bağlı olduğu unutulmamalıdır.

Süreç içerisinde çalışmalar sık sık kontrol edilmeli ve denetlenmeli, hedeflenen ve ulaşılan sonuçlar karşılaştırılarak gerekli değerlendirmeler yapılmalı, planlar yenilenerek güncel tutulmalı ve strateji devamlı geliştirilmelidir.

Sonsöz olarak; saldırganların şimdiye kadar gerçek güçlerin ve yeteneklerinin ortaya çıkmaması için en gelişmiş siber silahlarını kullanmadıkları, tam ölçekli bir siber savaşın sonuçlarının tahmin edilemeyeceği ve olabileceklerin modern bir ülkeye çok büyük hasar ve zararlar verebileceği düşüncesinin artık gerçek olduğunun tartışmasız kabul edilmesinin gerektiği günümüzde, bir ülkede savunması güçlü ve güvenli bir siber ortama, aynı zamanda caydırıcılık sağlayacak bir siber güce sahip olmak ve siber savaş durumunda zafer kazanmak isteniyorsa, siber güvenliği bütün boyutları ile ele alan ulusal güvenlikle tam bağlantılı bütüncül bir yaklaşım benimsenerek, daha kapsamlı ve etkin bir 'Ulusal Siber Güvenlik Stratejisi' oluşturulmalı, uygun ve doğru politikalar ile kararlılıkla uygulanmalıdır.

KAYNAKLAR

[1] **Wearesocial - Hootsuite** (2020). Digital Global Statshot Report in April 2020. *https://wearesocial.com/blog/2020/04/digital-around-the-world-in-april-2020, (Erişim: 05 Mayıs 2020).*

[2] **Goodman, M.** (2016). *Geleceğin Suçları Dijital Dünyanın Karanlık Yüzü.* TİMAŞ Yayınları, İstanbul.

[3] **Tzu, S.** (2016). *Savaş Sanatı.* (Çev.: P. Otkan ve G. Fidan), T. İş Bankası Kültür Yayınları, İstanbul.

[4] **TUİK** (2020). Sabit telefon, cep telefonu ve internet abone sayısı. *http://tuik.gov.tr/VeriBilgi.do?alt_id=1062, (Erişim 15 Nisan 2020).*

[5] **Atatürk, M.K.** (2008). *Nutuk, Söylev*. Türk Tarih Kurumu Yayını. Cilt II, Ankara.

[6] **Koca, F.** (2020). Sağlık Bakanı Koca Türkiye'de ilk koronavirüs vakasının görüldüğünü açıkladı. *https://www.aa.com.tr/tr/koronavirus/saglik-bakani-koca-turkiyede-ilk-koronavirus-vakasinin-goruldugunu-acikladi/1761466, (Erişim: 20 Mart 2020).*

[7] **Wamala, F.** (2012). *The ITU National Cybersecurity Strategy Guide-2011*. ITU Press, Cenevre, İsviçre.

[8] **ENISA** (2016). *NCSS Good Practice Guide, Designing and Implementing National Cyber Security Strategies.* ENISA Press, Heraklion, Yunanistan.

[9] **NATO CCD COE** (n.d.). Cyber Security Strategy Documents. *https://ccdcoe.org/cyber-security-strategy-documents.html, (Erişim: 05 Temmuz 2017).*

[10] **Şentürk, H. vd.** (2012). Cyber Security Analysis of Turkey. *UBGMD, 1(4), 112-125, Gazi Üniversitesi Yayını, Ankara.*

[11] **Akyazı, U.** (2016). Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler. *6.Uluslararası Siber Güvenlik ve Kriptoloji Konferansı, http://www.iscturkey.org/assets/files/2016/03/2013-paper105.pdf, (Erişim: 05 Temmuz 2017).*

[12] **Küçüksille, E.U. vd.** (2013**).** Dünyada Siber Güvenlik Stratejileri ve Bir Siber Güvenlik Stratejisinin Oluşumu. *1st International Symposium on Digital Forensics And Security, http://isdfs.firat.edu.tr/Upload/ISDFS2013_Proceeding _Book.pdf, (Erişim: 15 Temmuz 2017).*

[13] **Güngör, M.** (2015). Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma *(Uzmanlık Tezi). Bilgi Toplumu İdaresi Bşk.lığı Yayını, Ankara.*

[14] **Göçoğlu, V.** (2018)**.** Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi. *(Doktora Tezi). Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.*

[15] **Şengönül**, **A.** (2018). Dördüncü Nesil Savaş Kapsamında Türkiye İçin Strateji Tartışmaları. *(Doktora Tezi). Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü, Konya.*

[16] **T.C. Başbakanlık** (2003). Bilgi Sistem ve Ağları İçin Güvenlik Kültürü. *2003/10 sayılı Başbakanlık Genelgesi, Ankara.*

[17] **T.C. UDHB** (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı. *UDHB Yayını, Ankara.*

[18] **Nye, J.S**. (2010). *Cyber Power*. Belfer Center for Science and International Affairs, Masaçuset, ABD.

[19] **Kramer, F.D. vd.** (2011). *Cyberpower and National Security*. NDU Press, Washington, ABD.

[20] **Haley, C.** (2013). A Theory of Cyber Deterrence. *https://www.georgetown journalofinternationalaffairs.org/online-edition/a-theory-of-cyber-deterrence-christopher-haley, (Erişim:10 Nisan 2018).*

[21] **Libicki, M.C.** (2014). Military Cyberpower. *http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-11.pdf, (Erişim: 15 Temmuz 2017).*

[22] **Libicki, M.C.** (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation, Kaliforniya, ABD.

[23] **Mowbray, T.J.** (2010). Solution Architecture for Cyber Deterrence. *https://www.sans.org/reading-room/whitepapers/legal/solution-architecture-cyber-deterrence-33348, (Erişim: 15 Temmuz 2017).*

[24] **Wrenn, C.F.** (2012). Strategic Cyber Deterrence. *(Doktora Tezi). Tufts University, the Fletcher School, Masaçuset, ABD.*

[25] **Clarke, R.A.** ve **Knake, R.K.** (2010). *Siber Savaş.* (Çev.: M. Erduran). İstanbul Kültür Üniversitesi Yayınları, İstanbul.

[26] **Jensen, E.T.** (2012). Cyber Deterrence. *Emory International Law Review 773, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2070438, (Erişim: 15 Temmuz 2017).*

[27] **Thomasen, T.** (2011). Cyber Deterrence - A 21st Century Maginot Line. *http://fak.dk/biblioteket/publikationer/Documents/Cyber%20Deterrence.pdf (Erişim: 15 Temmuz 2017).*

[28] **Bendiek, A. ve Metzger, T.** (2015). Cyberdeterrence Theory in the Cyber-Century. *https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/Bendiek-Metzger_WP-Cyberdeterrence.pdf, (Erişim: 12 Nisan 2018).*

[29] **Davis, P.K**. (2015), Deterrence, Influence, Cyber Attack, and Cyberwar. *Internatıonal Law And Politics, 47(2), 327-355, New York, ABD, 2015.*

[30] Lindsay, J.R. (2015). Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity, 1(1), 53-67, https://doi.org/10.1093/cybsec/tyv003, (Erişim: 20 Temmuz 2017).*

[31] Singer, P.W. ve Friedman, A. (2015). *Siber Güvenlik ve Savaş*. (Çev.:A. Atav), Buzdağı Yayınları, Ankara.

[32] Pernik, P. (2016)**.** NATO's Cyber Deterrence. *https://www.icds.ee/publications/article/natos-cyber-deterrence/, (Erişim: 12 Nisan 2018).*

[33] Wilner, A. (2017). Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation. *Comparative Strategy Journal, 36(4), 309-318, https://doi.org/10.1080/01495933.2017.1361202.*

[34] Taddeo, M. (2018). Deterrence and Norms to Foster Stability in Cyberspace. *Philosophy and Technology Journal, Volume 31 Issue 3, Sf.:323–329, https://doi.org/10.1007/s13347-018-0328-0.*

[35] Ünal, S. (2015). Siber Uzamın Güvenlikleştirilmesi Söylemi: Türkiye, ABD ve Avrupa Birliği Örnekleri. *(Doktora Tezi). Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.*

[36] Gündoğdu, E. (2018). Caydırıcılık Teorisini Yeniden Düşünmek: Asimetrik Caydırıcılık ve Oyun Teorisi. *(Doktora Tezi). Akdeniz Üniversitesi, Sosyal Bilimler Üniversitesi, Antalya.*

[37] Hart, B.H.L. (1973). *Strateji Dolaylı Tutum*. (Çev.: C. Enginsoy), Gnkur. ATASE Bşk.lığı Yayını, Ankara.

[38] Atatürk, Kültür, Dil ve Tarih Yüksek Kurumu (1997). *Atatürk'ün Söylev ve Demeçleri.* Atatürk Araştırma Merkezi Yayını, Cilt II, Ankara.

[39] TDK Sözlükleri (t.y.). Güvenlik. *https://sozluk.gov.tr/?kelime=güvenlik (Erişim: 20 Mart 2019).*

[40] Dedeoğlu, B. (2014). *Uluslararası Güvenlik ve Strateji.* Yeniyüzyıl Yayınları, İstanbul.

[41] T.C. UDHB (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı. *T.C. UDHB Yayını, Ankara.*

[42] Sağıroğlu, Ş. (2018). Siber Güvenlik ve Savunma: Önem, Tanımlar ve Önlemler. *Siber Güvenlik ve Savunma - Farkındalık ve Caydırıcılık* (Ed.: Sağıroğlu, Ş. ve Alkan, M.), Grafiker Yayınları Kitap Serisi 1, 19-45, Ankara.

[43] Ocak, M.A. vd. (2014). *Güncel Tehdit Siber Suçlar.* Seçkin Yayınları, Ankara.

[44] Turhan, O. (2015). Bilgisayar Ağları İle İlgili Suçlar. (Planlama Uzmanlığı Tezi). *http://www.bilgitoplumu.gov.tr/wp-content/uploads/2015/01/Bilgisayar_Aglari_ile_ilgili_Suclar_OguzTurhan.pdf, (Erişim: 19 Temmuz 2016).*

[45] Yayla, M., (2014). Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı. *Hacettepe Hukuk Fakültesi Dergisi, 4(2), 181-200, Ankara.*

[46] Klimburg, A. (2012). National Cyber Security Framework Manual. *NATO Yayını, Estonya.*

[47] **ITU-T.** (2009), Overview of cybersecurity, *Recommendation ITU-T X.1205, Cenevre, İsviçre.*

[48] **The White House** (2013). Executive Order - Improving Critical Infrastructure Cybersecurity, *https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cyber security, (Erişim: 15 Temmuz 2018).*

[49] **E. M. Brunner ve M. Suter** (2008), International CIIP Handbook 2008/2009 An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies. *ETH Library, Zürih, İsviçre.*

[50] **Gartzke, E. ve Lindsay, J. R.** (2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Taylor & Francis and Routledge Group,* Journal of *Security Studies, 24(2), 316–348, DOI:10.1080/09636412.2015.1038188.*

[51] **Yayla, M.** (2013). Hukuki Bir Terim Olarak Siber Savaş. *Türkiye Barolar Birliği Dergisi, 104, 177-201, Ankara.*

[52] **Resmi Gazete** (1983). 2941 Sayılı Seferberlik ve Savaş Hali Kanunu**.** *https://www.resmigazete.gov.tr/arsiv/18215.pdf. (Erişim: 01 Şubat 2018).*

[53] **Rid, T.** (2012). Cyber War Will Not Take Place. Journal of Strategic Studies, 35(1), 5-32. https://doi.org/10.1080/01402390.2011.608939.

[54] **Stone, J.** (2013). Cyber War Will Take Place. Journal of Strategic Studies, *36(1), 101-108, https://doi.org/10.1080/01402390.2012.730485.*

[55] **UNTERM** (t.y.). Cyber Warfare. *https://unterm.un.org/UNTERM/display/Record/UNHQ/NA/c263537, (Erişim: 25 Temmuz 2017).*

[56] **TDK Sözlükleri** (t.y.). Caydırıcılık. *https://sozluk.gov.tr/?kelime=caydırıcılık, (Erişim: 29 Mart 2019).*

[57] **Kızmaz, Z**. (2005). Ceza veya Kriminal Yaptırımın Suç Oranları Üzerindeki Caydırıcı Etkisi. *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi, 7, 221-245, Afyonkarahisar.*

[58] **Özdemir, H.** (2008). Uluslararası İlişkilerde Güç-Çok Boyutlu Bir Değerlendirme. *Ankara Üniversitesi SBF Dergisi, 63(3), 128-139, Ankara.*

[59] **MS 76-3 TSK Müşterek Askeri Terimler Sözlüğü** (2010). Caydırıcılık. *Genelkurmay Basımevi, Ankara.*

[60] **Long, A.** (2008). *Deterrence From Cold War to Long War.* RAND Corporation, Kaliforniya, ABD.

[61] **Kane, T.M. ve Lonsdale, D.J.** (2016). *Çağdaş Stratejiye Anlamak.* (Çev.: A.T.Büyükkonat). Doruk Yayınları, İstanbul.

[62] **TDK Sözlükleri** (t.y.). İstihbarat. *https://sozluk.gov.tr/?kelime=istihbarat, (Erişim: 29 Mart 2019).*

[63] **Keleştemur A.** (2015). *Siber İstihbarat.* Level Kitap-Umuttepe Yayınları, İstanbul.

[64] TDK Sözlükleri (t.y.). Güç. *https://sozluk.gov.tr/?kelime=güç, (Erişim: 29 Mart 2019).*

[65] Nye, J.S. ve **Welch, D.A.** (2010). *Küresel Çatışmayı ve İşbirliğini Anlamak.* T.İş Bankası Kültür Yayınları, İstanbul.

[66] Armitage, R.L. ve **Nye, J.S.** (2007). *CSIS Commission on Smart Power: A Smarter, More Secure America.* CSIS Press, Washington, ABD.

[67] Mütercimler, E. (2006). *Geleceği Yönetmek ve Kazanmak İçin Stratejik Düşünme.* Alfa Yayınları, İstanbul.

[68] TBMM (2012). Türkiye Büyük Millet Meclisi Basın Açıklamaları - TBMM Bilişim ve Internet Araştırma Komisyonu. *https://www.tbmm.gov.tr/develop/owa/haber_portal.aciklama?p1=121672, (Erişim: 25 Temmuz 2017).*

[69] Canbek, G. ve **Sağıroğlu, Ş.** (2006*).* Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme*. Politeknik Dergisi, 9(3), 165-174, Ankara.*

[70] ITU (2008) Global Cybersecurity Agenda High-Level Experts Group Global Strategic Report. *ITU Press, Cenevre, İsviçre.*

[71] Burlu, K. (2015). *Bilişimin Karanlık Yüzü.* Nirvana Yayınları. Ankara.

[72] *EnigmaSoft* *(n.d.).* Top 20 Countries Found to Have the Most Cybercrime. *https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/, (Erişim: 20 T3mmuz 2017)*

[73] Özden, D. vd. (2019). 2018 ve 2019 Siber Saldırı Verileri. *HAVELSAN Dergisi, HAVELSAN A.Ş. Yayını, 3, 58-59, Ankara.*

[74] Sayan, Ö. F. (2019). Türkiye Global Siber Güvenlik İndeksinde Yükselişte. *HAVELSAN Dergisi, HAVELSAN A.Ş. Yayını, 3, 6-15, Ankara.*

[75] Ünal, A.Y. (2020). Türkiye'nin siber saldırıları önleme merkezi kapılarını AA'ya açtı. *https://www.aa.com.tr/tr/turkiye/turkiyenin-siber-saldiri lari-onleme-merkezi-kapilarini-aaya-acti/1727981, (Erişim: 18 Şubat 2020).*

[76] Şenol, M. (2016). Siber Güçle Caydırıcılık Ama Nasıl. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi (UBMGD), 2(2), 10-17, Gazi Üniversitesi Yayını, Ankara, https://doi.org/10.18640/ ubgmd.303581.*

[77] Kırık, A.M. (2012). Arap Baharı Bağlamı'nda Sosyal Medya-Birey Etkileşimi ve Toplumsal Dönüşüm. *21. Yüzyılda Eğitim ve Toplum Eğitim Bilimleri ve Sosyal Araştırmalar Dergisi, 1(3), 87-98, Ankara.*

[78] Republic of Estonian Information System Authority (2018). Annual Cyber Security Assessment 2018. *https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria-csa-2018.pdf, (Erişim: 25 Ekim 2018).*

[79] Güler, B. ve Dursun, A. (2020). İran'ın düşürdüğü yolcu uçağının karakutuları Ukrayna'da açılacak. *https://www.aa.com.tr/tr/dunya/iranin-dusur dugu-yolcu-ucaginin-karakutulari-ukraynada-acilacak/1763757, (Erişim: 18 Mart 2020).*

[80] **Dursun, A.** *(2020).* İran Devrim Muhafızları Komutanı Hacızade: Ukrayna uçağı yanlışlıkla seyir füzesi olarak tanımlandı. *https://www.aa.com.tr/tr/dunya/iran-devrim-muhafizlari-komutani-hacizade-ukrayna-ucagi-yanlislikla-seyir-fuzesi-olarak-tanimlandi/169957, (Erişim: 18 Mart 2020)*

[81] **Dilek, B. D.** (2020). ABD İran Füzelerini Neden Önleyemedi, Ukrayna Uçağı Yanlışlıkla Nasıl Vuruldu. *https://21yyte.org/tr/merkezler/islevsel-arastirma-merkezleri/milli-guvenlik-ve-dis-politika-arastirmalari-merkezi/abd-iran-fuzelerini-neden-onleyemedi-ukrayna-ucagi-yanlislikla-nasil-vuruldu, (Erişim: 18 Mart 2020)*

[82] **Aslan, Y.** (2020). Tahran Üniversitesi'nden Ukrayna uçağı raporu: İnsani hata değil, siber saldırı. *https://www.aydinlik.com.tr/haber/tahran-universitesi'nden-ukrayna-ucagi-raporu-insani-hata-degil-siber-saldiri-199862, (Erişim: 18 Mart 2020).*

[83] **Hürriyet Gazetesi** (2018), Halkbank'tan çok önemli 'ucuz dolar' açıklaması. *http://www.hurriyet.com.tr/ekonomi/son-dakika-halkbanktan-cok-onemli-ucuz-dolar-aciklamasi-40943969, (Erişim: 03 Eylül 2018)*

[84] **Türkiye Gazetesi** (2018). Katılım Bankası'na siber saldırı! Dolar kuru 4,58 bandına düştü. *https://www.turkiyegazetesi.com.tr/ekonomi/579795.aspx (Erişim: 13 Eylül 2018).*

[85] **Arquilla, J. ve Ronfeldt, D.** (1993). Cyberwar is coming, Comparative Strategy Journal, 12(2), 141-165, Published Online: 24 Sep 2007 https://doi.org/10.1080/01495939308402915.

[86] **Werner, D.** (2011). Cyber Alert. *C4ISR Journal, Army Times Publishing, Virjinya, ABD.*

[87] **Rid, T. ve McBurney, P.** (2012). Cyber-Weapons, *The RUSI Journal, 157(1), 6-13. https://doi.org/10.1080/03071847.2012.664354*.

[88] **Çiftçi, H.** (2013). *Her Yönüyle Siber Savaş.* TÜBİTAK Yayınları, Ankara.

[89] **Baram, G. ve Menashri, H** (2019). Why can't we be friends? Challenges to international cyberwarfare cooperation efforts and the way ahead. *Comparative Strategy Journal, 38(2), 89-97, https://doi.org/10.1080/01495933.2019.1573069.*

[90] **Lupovici, A.** (2011). Cyber Warfare and Deterrence. *Military and Strategic Affairs. 3(3), 49-62, İsrail.*

[91] **Gorman, S. ve Barnes, J. E.** (2011). Cyber Combat: Act of War. *http://www.wsj.com/articles/SB10001424052702304563104576355623135782718, (Erişim: 29 Temmuz 2017).*

[92] **Denning, D.** (2016). Cybersecurity's Next Phase: Cyber-deterrence. *The Conversation, https://theconversation.com/cybersecuritys-next-phase-cyber-deterrence-67090, (Erişim: 15 Temmuz 2018).*

[93] **Iasiello, E. (**2014). Is Cyber Deterrence an Illusory Course of Action. *Journal of Strategic Security, 7(1), 54-67, http://dx.doi.org/10.5038/1944-0472.7.1.5.*

[94] Goodman, W. (2010). Cyber Deterrence Tougher in Theory than in Practice. *http://www.au.af.mil/au/ssq/2010/fall/goodman.pdf, (Erişim: 17 Temmuz 2018).*

[95] Taddeo, M. (2018). The Limits of Deterrence Theory in Cyberspace. Philosophy and Technology Journal, 31(3), 339-355, https://doi.org/10. 1007/s13347-017-0290-2.

[96] Jensen, E.T. (2012). Cyber Deterrence. Emory International Law Review 773. *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2070438, (Erişim: 18 Temmuz 2018).*

[97] Akad, M.T. (2011). *Modern savaşın Temel Kavramları*. Kitap Yayınevi, Ankara.

[98] Ottis, R. (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. *https://ccdcoe.org/uploads/2018/ 10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspecti ve.pdf, (Erişim: 20 Temmuz 2018).*

[99] Tikk, E. vd. (2010). International Cyber Incidents: Legal Considerations. *NATO CCD COE Publications, Tallin, Estonya.*

[100] Hürriyet Gazetesi (2007). İsrail tepemize 'tank' bıraktı. *https://www. hurriyet.com.tr/gundem/israil-tepemize-tank-birakti-7245193, (Erişim: 20 Temmuz 2017).*

[101] Carr, Jeffrey (2009). Inside Cyber Warfare: Mapping the Cyber Underworld. *https://www.academia.edu/10861174/Inside_Cyber_Warfare_2nd_ Edition_Mapping_the_Cyber_Underworld, (Erişim: 10 Ağustos 2018).*

[102] Farwel, J.P. ve **Rohozinski R. (**2011). Stuxnet and the Future of Cyber War. *53(1), 23-40, https://doi.org/10.1080/00396338.2011.555586, (Erişim: 10 Ağustos 2018).*

[103] Avar, B. (2011). *Kaçın 'Demokrasi' geliyor.* Remzi Kitabevi Yayınları, İstanbul.

[104] Atmaca, A. Ö. (2016). Olay İncelemesi ABD'nin Hakikat Ötesi Başkanı-Donald Trump. *The Turkish Yearbook of International Relations, Cilt:47, Sf.:105-11, Ankara.*

[105] Wearesocial–Hootsuite (2020). Digital 2020: Turkey. *https://datareportal.com /reports/digital-2020-turkey, (Erişim: 05 Mayıs 2020).*

[106] Keller, J. (2016). Iran–U.S. RQ-170 incident has defense industry saying 'never again' to unmanned vehicle hacking. *https://www.militaryaero space.com/computers/article/16715072/iranus-rq170-incident-has-defense-industry-saying-never-again-to-unmanned-vehicle-hacking, (Erişim: 10 Mayıs 2018).*

[107] Hartmann, K. ve Giles, K. (2016). UAV Exploitation: A New Domain for Cyber Power. *https://ccdcoe.org/uploads/2018/10/Art-14-Assessing-the-Impact-of-Aviation-Security-on-Cyber-Power.pdf, (Erişim: 15 Mayıs 2017).*

[108] Anadolu Ajansı (2020). İranlı General Süleymani ve Haşdi Şabi Başkan Yardımcısı el-Mühendis öldürüldü. *https://www.aa.com.tr/tr/dunya/iranli-general-suleymani-ve-hasdi-sabi-baskan-yardimcisi-el-muhendis-olduruldu/1690687, (Erişim: 15 Şubat 2020).*

[109] Dursun, A. (2018). İran Devrim Muhafızları Ordusu ABD'nin Irak'taki üslerini füzelerle vurdu. *https://www.aa.com.tr/tr/dunya/iran-devrim-muhafizlari-ordusu-abdnin-iraktaki-uslerini-fuzelerle-vurdu/1695598, (Erişim: 15 Şubat 2020).*

[110] War News Updates (2014). Was This The World's First Cyber Attack. *http://warnewsupdates.blogspot.com/2014/12/was-this-worlds-first-cyber-attack.html, 10 Şubat 2017).*

[111] Milliyet Gazetesi (2014). Siber savaşın miladı. *http://www.milliyet.com.tr/dünya/siber-savasin-miladi-1982549com/hackerlar-in-en-buyuk-darbesi-erzincan-da-olmus-705841-teknoloji/, (Erişim: 20 Şubat 2017).*

[112] Robertson, J. ve Riley, M. (2014). Cybersecurity - Mysterious'08 Turkey Pipeline Blast Opened New Cyberwar. *https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar, (Erişim:20 Şubat 2020).*

[113] CİMER (2019). Boru Hatları ile Petrol Taşıma Anonim Şirketi Genel Müdürlüğü'nün Mustafa Şenol CİMER Başvurusuna 05.08.2019 tarih ve 00:24 saatli cevabi bilgi e-mesajı.

[114] CNN Türk TV (2011). Anonymous TİB'e saldırdı. *https://www.cnnturk.com/2011/bilim.teknoloji/teknoloji/06/09/anonymous.tibe.saldirdi/619484.0/index.html, (Erişim: 15 Şubat 2017).*

[115] NTV (2015). Elektrik kesintisinin nedeni siber saldırı mı. *https://www.ntv.com.tr/turkiye/elektrik-kesintisinin-nedeni-siber-saldiri-mi,6I9YdXkmvE6aewbUxSm0TA, (Erişim: 15 Şubat 2017).*

[116] Başaran, E. (2015). Elektrik Kesintisi Gerçekten Siber Saldırı İşi mi. *http://www.radikal.com.tr/yazarlar/ezgi-basaran/elektrik-kesintisi-gercekten-siber-saldiri-isi-mi-1326537/, (Erişim: 19 Şubat 2017).*

[117] CİMER (2019). TEİAŞ Gn.Md.lüğü'nün Mustafa Şenol CİMER Başvurusu konulu, 09.10.2019 tarih ve 6585913-622.03-E.409540 sayılı yazısı Eki Türkiye 31 Mart 2015 Sistem Çökmesi Raporu.

[118] Karanfil, N. (2015). TEİAS Elektrik Kesintilerini Engellemek İçin İhaleye Çıkıyor. *http://www.hurriyet.com.tr/teias-elektrik-kesintilerini - engellemek-icin-ihaleye-cikiyor-30001794, (Erişim: 20 Şubat 2017).*

[119] Hürriyet Gazetesi (2015). Türkiye'deki internet siteleri saldırı altında. *https://www.hurriyet.com.tr/gundem/turkiyedeki-internet-siteleri-saldiri-altinda-40028331, (Erişim: 26 Mart 2017).*

[120] BBC (2015). Türkiye'ye siber saldırının 10 günü: Ne oldu. *http://www.bbc.com/turkce/haberler/2015/12/151224_siber_saldiri_arslan, (Erişim: 26 Mart 2017).*

[121] Topal, A. (2016). Siber saldırıların ana hedefi ulusal system. *http://www.sabah.com.tr/gundem/2016/01/01/siber-saldirilarin-ana-hedefi-ulusal-sistem, (Erişim: 26 Mart 2017).*

[122] Hürriyet Gazetesi (2015). Bakan Yıldırım ODTÜ'yü suçladı. *http://www.hurriyet.com.tr/suclu-odtu-40031062, (Erişim: 26 Mart 2017).*

[123] Haberler.com (2015). Türkiye'ye Siber Saldırının Arkasında Ruslar Var. *http://www.haberler.com/turkiye-ye-siber-saldirinin-arkasinda-ruslar-var-8006069-haberi/, (Erişim: 26 Mart 2017).*

[124] Milliyet Gazetesi (2015). Anonymous, Türkiye'deki 50 bin bilgisayarı ele geçirdi. *http://www.milliyet.com.tr/turkiye-ye-turk-vatandaslarinin-teknoloji-2169676/, (Erişim: 26 Mart 2017).*

[125] Milliyet Gazetesi (2015). Türkiye'ye şok tehdit: Bunlar daha başlangıç. *http://www.milliyet.com.tr/turkiye-ye-sok-tehdit-bunlar-daha-gun dem-2170870/, (Erişim: 26 Mart 2017).*

[126] Hürriyet Gazetesi (2016). Anonymous bizi nasıl vurdu. *http://yeni.hurriyet.com.tr/anonymous-bizi-nasil-vurdu-40036254, (Erişim: 26 Mart 2017).*

[127] Hürriyet Gazetesi (2015). Onlar saldırdı biz fişi çektik. *http://www.hurriyet.com.tr/teknoloji/onlar-saldirdi-biz-fisi-cektik-40030151 (Erişim: 26 Mart 2017).*

[128] Trend Micro (2014). Turning the Tables on Cyber Attacks Responding to Evolving Tactics. *https://www.itu.int/en/ITU-D/Cybersecurity/Documents/rpt-turning-the-tables-on-cyber-attacks-itu.pdf (Erişim:20 Mart 2017)*

[129] Veebel, V. (2017). Baltic States and Cyber Deterrence: Taking or Losing Initiative against Russia. *http://www.fpri.org/article/2017/01/baltic-states-cyber-deterrence-taking-losing-initiative-russia/, (Erişim: 26 Mart 2017).*

[130] Milliyet Gazetesi (2014). Kuzey Kore'yi kızdıran Sony filmi geri çekildi. *http://www.milliyet.com.tr/kuzey-kore-yi-kizdiran-sony-filmi/dünya/detay/1986604/default.htm, (Erişim: 15 Şubat 2017).*

[131] Bicchierai, L. F. ve Warren C. (2014). Hackers sent extortion email to Sony executives 3 days before attack. *https://mashable.com/2014/12/08/hackers-emailed-sony-execs/, Erişim: 15 Şubat 2017).*

[132] Mancar. B. (2014) Sony Pictures Hack Skandalı ve Saldırı Süreci. *https://webmasto.com/sony-pictures-hack-skandali-ve-saldiri-sureci, (Erişim: 15 Şubat 2017).*

[133] Ünal, S. (2015). Siber Uzama Yönelik Güvenlikçi Söylemin İnşası: Sony Pictures'a Yönelik Siber Saldırı Haberlerinin Analizi. *Uluslararası Sosyal Araştırmalar Dergisi, 8(41), 1308-1320, Samsun.*

[134] BBC (2014). Kuzey Kore-ABD arasında siber saldırı gerilimi. *http://www.bbc.com/turkce/haberler/2014/12/141219_kuzey_kore_obama, (Erişim: 15 Şubat 2016).*

[135] BBC (2014) Kuzey Kore'den ABD'ye: Siber saldırıları ortak soruşturalım *https://www.bbc.com/turkce/haberler/2014/12/141220_sony_obama_yanit, (Erişim: 20 Şubat 2017).*

[136] Habertürk (2015). Obama siber güvenlik paketi açıkladı. *https://www.haberturk.com/dunya/haber/1030206-obama-siber-guvenlik-paketi-acikladi, (Erişim: 25 Şubat 2017).*

[137] TDK Sözlükleri (t.y.). Strateji. *https://sozluk.gov.tr/?kelime=strateji (Erişim: 20 Mart 2019).*

[138] TDK Sözlükleri (t.y.). Politika. *https://sozluk.gov.tr/?kelime=politika (Erişim: 20 Mart 2019).*

[139] Boyle, R. J. ve Panko, R. R. (2013). *Corporate Computer Security*. Pearson Press, 3.Baskı, New Jersey, ABD.

[140] Walters, R. (2014). Cyber Attacks on U.S. Companies in 2014. *https://www.heritage.org/defense/report/cyber-attacks-us-companies-2014#_ftn1, (Erişim. 20 Mart2019).*

[141] Vural, Y. ve Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. *Gazi Üniv. Müh. Mim. Fak. Der., 23(2), Ankara.*

[142] Doğantimur, F. (2009). ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği. *Mesleki Yeterlik Tezi, Maliye Bakanlığı Str. Glş. Bşk.lığı, Ankara.*

[143] Can, Ö. ve Akbaş, M. F. (2014). Kurumsal Ağ ve Sistem Güvenliği Politikalarının Önemi ve Bir Durum Çalışması. *TÜBAV Bilim Dergisi, 7(2), 16-31, Ankara.*

[144] Resmi Gazete (2012. İş Sağlığı ve Güvenliği Kanunu. *https://www.resmigazete.gov.tr/eskiler/2012/06/20120630-1.htm. (Erişim: 201 Mart 2017)*

[145] Arce, I. (2003). The weakest link revisited [information security]. *IEEE Security & Privacy Magazine, 1(2), 72-76, DOI:10.1109/MSECP.2003.1193216.*

[146] Garuba, **M. vd.** (2008). Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems. *5th International Conference on Information Technology: New Generations, 592 - 598, Nevada, ABD.*

[147] Şen, Ş. ve Yerlikaya, T. (2013). ISO 27001 Kurumsal Bilgi Güvenliği Standardı. *AÜ Akademik Bilişim Konferansı, http://ab.org.tr/ab13/kitap/AB2013_Bildiri_Kitap.pdf, (Erişim:21 Mart 2016).*

[148] Moen, R. (2010) Foundation and History of the PDSA Cycle. *https://deming.org/uploads/paper/PDSA_History_Ron_Moen.pdf, (Erişim: 21 Mart 2016).*

[149] Tekerek, M. (2008). Bilgi Güvenliği Yönetimi. *KSÜ Fen ve Mühendislik Dergisi, 11(1), 132-137, Kahramanmaraş.*

[150] Ottekin, F. (2008). TS ISO/IEC 27001 Denetim Listesi. *TÜBİTAK UEKAE Yayınları, Ankara.*

[151] Öztürk, G. (2008). Bilgi Güvenliği Politikası Oluşturma Kılavuzu, TÜBİTAK UEKAE Yayınları, Ankara.

[152] T.C. MGK Gn.Sekreterliği (2018) Milli Güvenlik Kurulu ve Milli Güvenlik Kurulu Genel Sekreterliği Hakkında Genel Bilgi. *https://www.mgk.gov.tr/index.php/kurumsal/hakkimizda (Erişim: 15 Temmuz 2018).*

[153] Dennesen, K. (2011). Latin American Cyber Threat Landscape and 2011 Trends. iDefense 2011 Trends Report. *http://www.cu.ipv6tf.org/ lacnic15/LACNICV3.pdf, (Erişim: 20 Mart 2016).*

[154] ITU (2019). Global Cybersecurity Index 2018. *Studies & research ITU Publications, Cenevre, İsviçre.*

[155] The White House (2003). The National Strategy to Secure Cyberspace. *https://www.us-cert.gov/sites/default/files/publications/cyberspace_ strategy.pdf. (Erişim: 15 Temmuz 2018).*

[156] Peritz, A.J. ve Sechrist, M. (2010). Protecting Cyberspace and The US National Interest. *Belfer Center for Science and International Affairs, Masaçuset, ABD.*

[157] Pernik, P. vd. (2016). National Cyber Security Organisation: United States. *https://www.us-ert.gov/sites/default/files/publications/cyberspace_ strategy.pdf (Erişim: 15 Temmuz 2018).*

[158] The White House (2008). The Comprehensive National Cybersecurity Initiative. *http://www.whitehouse.gov/issues/foreign-policy/cyber security/national-initiative, (Erişim: 15 Temmuz 2018).*

[159] The White House (2011). USA International Strategy for Cyberspace - Prosperity, Security, and Openness. *https://obamawhitehouse.archives. gov/sites/default/files/rss_viewer/international_strategy_for_cyberspa ce.pdf, (Erişim: 15 Temmuz 2018).*

[160] U.S. Department of Defense (2011). The Department of Defense Strategy for Operating in Cyberspace. *http://www.defense.gov/news/d20110714 cyber.pdf, (Erişim: 15 Temmuz 2018).*

[161] U.S. Department of Defense (2015). U.S. Department of Defense Cyber Strategy. *https://archive.defense.gov/home/features/2015/0415_ cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf, (Erişim: 15 Temmuz 2018).*

[162] The White House (2016). U.S. Cybersecurity National Action Plan. *https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/ fact-sheet-cybersecurity-national-action-plan, (Erişim: 15 Temmuz 2018).*

[163] U.S. Department of Homeland Security (2018). U.S. DHS Cybersecurity Strategy. *https://www.dhs.gov/sites/default/files/public cations/DHS-Cyber security-Strategy_1.pdf, (Erişim: 15 Mart 2019).*

[164] The White House (2018). U.S. National Cyber Strategy. *https://www.white house.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, (Erişim: 20 Mart 2019).*

[165] U.S. Department of Homeland Security (2018). US National Protection and Programs Directorate Organziation Chart. *https://www.dhs.gov/sites/default/files/publications/19_0226_cisa_org-chart-02252019.pdf, (Erişim: 15 Mart 2019).*

[166] The World Bank (2016). Digital Dividends - world development report. *http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf, (Erişim: 15 Mart 2019).*

[167] Raud, M. (2016). China and Cyber: Attitudes, Strategies, Organisation. *NATO CCD COE Publications, Tallin, Estonya.*

[168] Yuxiao, L. ve Lu, X. (2015). Cyberspace Security and International Cooperation. *In Lindsay, J. R. vd. (Eds.), China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, Oxford University Press, New York, ABD.*

[169] Ernst, D. (2010). Indigenous Innovation and Globalization - the Challenge for China's Standardization Strategy. *Report by the East-West Center, https://www.eastwestcenter.org/sites/default/files/private/ernstindigenousinnovation.pdf, (Erişim: 15 Temmuz 2018).*

[170] Segal, A. (2015). What to Do About China's New Cybersecurity Regulations. *Council on Foreign Relations. https://www.cfr.org/blog/ what-do-about-chinas-new-cybersecurity-regulations, (Erişim: 15 Temmuz 2018).*

[171] Giles, K. ve Hagested, W. (2013). Divided by a Common Language: Cyber Definitions in Chinese. *Russian and English, https://ccdcoe.org/uploads/2018/10/22_d3r1s1_giles.pdf, (Erişim: 15 Temmuz 2018).*

[172] The U.S China Economic and Security Review Commission (**2011).** Report to Congress. *https://www.uscc.gov/annual-report/2011-annual-report-congress, (Erişim: 20 Temmuz 2018).*

[173] The People's Republic of China Information Office of the State Council (2013). The Diversified Employment of China's Armed Forces. China Defense White Paper, *https://media.nti.org/pdfs/China_Defense_ White_Paper_2013.pdf, (Erişim: 20 Temmuz 2018).*

[174] The U.S China Economic And Security Review Commission (2019). Report to Congress, *https://www.uscc.gov/annual-report/2019-annual-report-0, (Erişim: 20 Temmuz 2019).*

[175] Presidency of the Russian Federation (2000). Information Security Doctrine of The Russian Federation. *https://www.itu.intm /en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository /Russia_2000.pdf, (Erişim: 20 Temmuz 2018).*

[176] Security Council of the Russian Federation (2016). Doctrine of Information Security of the Russian Federation. *http://www.scrf.gov.ru/security/information/DIB_engl/, (Erişim: 20 Temmuz 2018).*

[177] French Prime Ministry (2015). National Digital Security Strategy. *https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf, (Erişim: 20 Ağustos 2018).*

[178] Brangetto, P. (2015). National Cyber Security Organisation: France. *NATO CCD COE Publications, Tallin, Estonya.*

[179] Presidency of the French Republic (2008). The French White Paper on defence and national security. *http://responsibilitytoprotect.org/Livre_blanc_Press_kit_english_version.pdf, (Erişim: 20 Ağustos 2018).*

[180] French Prime Ministry (2011). Information System Defence and Security – France's Strategy. *https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy. Pdf, (Erişim: 20 Ağustos 2018).*

[181] Presidency of the French Republic (2013). French White Paper on Defence and National Security. *https://ccdcoe.org/uploads/2018/10/White-paper-on-defense-2013-1.pdf, (Erişim: 20 Ağustos 2018).*

[182] Osula, A.M. *(2015).* National Cyber Security Organisation: United Kingdom. *NATO CCD COE Publications, Tallin, Estonya.*

[183] The U.K. Government (2016). National Cyber Security Strategy (2016-2021). *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf , (Erişim: 20 Nisan 2019)*

[184] Housen-Couriel, D. (2017). National Cyber Security Organisation: Israel. *NATO CCD COE Publications, Tallin, Estonya.*

[185] T.C. Başbakanlık (2003). Bilgi Sistem ve Ağları İçin Güvenlik Kültürü Genelgesi (2003/10). Başbakanlık Per.ve Pren. Gn.Md.lüğü, 17 Şubat 2003, Sayı: B.02.0.PPG.0.12-320-2789, Ankara.

[186] DPT Müsteşarlığı (2003), e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı (2003-2004). *DPT Yayınları, Ankara.*

[187] DPT Müsteşarlığı (2006), Bilgi Toplumu Stratejisi ve Eylem Planı (2006-2010). *DPT Yayınları, Ankara.*

[188] Ünver, M. vd. (2009). Siber Güvenliğin Sağlanması- Türkiye'de Mevcut Durum ve Alınması Gereken Tedbirler. *BTK Yayını, Ankara.*

[189] Adalı, E. (2017). *Bilişim Etiği ve Hukuku.* İTÜ Ulusal Yazılım Sertifikasyon Merkezi Yayını, İstanbul.

[190] T.C. MGK Sekreterliği (2010). 27 Ekim 2010 Tarihli Toplantı, *http://www.mgk.gov.tr/index.php/27-ekim-2010-tarihlitoplanti, (Erişim: 25 Şubat 2017).*

[191] Resmi Gazete (2011). UDHB'nin Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname, *http://www.resmigazete.gov.tr/eskiler/2011/11/20111101M1-1.htm, (Erişim: 01 Şubat 2017).*

[192] Resmi Gazete (2012). Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar. *Bakanlar Kurulu Kararı:2012/3842, https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm, (Erişim: 05 Şubat 2017).*

[193] Resmi Gazete (2014). Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun. *https://www.resmigazete.gov.tr/eskiler/2014/02/20140219-1.htm, (Erişim: 05 Şubat 2017).*

[194] Uslu, S. (2016). Türk ordusunun yeni "kuvveti" siber savunma. *https://www.aa.com.tr/tr/turkiye/turk-ordusunun-yeni-kuvveti-siber-savunma/584061, (Erişim: 10 Şubat 2017).*

[195] T.C. Cumhurbaşkanlığı SSB (2020). TSK Sİber Savunma Merkezi Projesi. *https://www.ssb.gov.tr/Website/contentList.aspx?PageID=1083& LangID=1, (Erişim: 10 Mayıs 2010).*

[196] TSK Siber Savunma Komutanlığı (2019). 'Kilitli Kalkanlar (Locked Shields)-2019 Tatbikatı' Seçkin Gözlemci Gününe Katılım ve Görüşme. 11 Nisan 2019, Ankara.

[197] Alkan, M. vd. (2012). Ulusal Siber Güvenlik Stratejisi. *https://www. bilgiguvenligi.org.tr/wp-content/uploads/2016/03/Ulusal_Siber_ Guvenlik_Stratejisi.pdf, (Erişim: 10 Şubat 2017).*

[198] T.C. UDHB (2013). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. *T.C. UDHB Yayını, Ankara.*

[199] T.C. Kalkınma Bakanlığı (2011) Avrupa Birliğinin Bilgi Toplumu Politikaları ve Avrupa İçin Sayısal Gündem Girişimi. (Çalışma Raporu-3). *Kalkınma Bakanlığı Bilgi Toplumu Dairesi Yayını, Ankara.*

[200] Akses, S. (2014). Avrupa 2020 Stratejisi. *İktisadi Kalkınma Vakfı Yayınları, İstanbul.*

[201] T.C. Kalkınma Bakanlığı *(2015).* 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı. *KB Bilgi Toplumu D.Yayınları, Ankara.*

[202] Resmi Gazete (2016). 6698 sayılı Kişisel Verilerin Korunması Kanunu. *https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf, (Erişim: 20 Şubat 2017).*

[203] T.C. UDHB (2016). 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı. *T.C. UDHB Yayını, Ankara.*

[204] T.C. BSTB (2017). Türkiye Yazılım Sektörü Stratejisi ve Eylem Planı (2017-2019). *https://www.resmigazete.gov.tr/eskiler/2017/01/20170105-9-1.pdf, (Erişim: 20 Şubat 2017).*

[205] Resmi Gazete (2018). 477 Sayılı Kanun İle Bazı Kanunlarda Değişiklik Yapılması Hakkında 703 Numaralı KHK. *https://www.resmigazete. gov.tr/eskiler/2018/07/20180709M3.pdf (Erişim: 05 Ağustos 2018).*

[206] Resmi Gazete (2018). 703 Numaralı KHK İle Kaldırılan Kurulların Görevlerinin Cumhurbaşkanlığına Devredilmesi. *CB Genelgesi: 2018/3, https://www.resmigazete.gov.tr/eskiler/2018/08/20180802-2.pdf, (Erişim: 05 Ağustos 2018).*

[207] Resmi Gazete (2019). Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri. *CB Genelgesi (2019/12), https://www.resmigazete.gov.tr/eskiler/2019/ 07/20190706-10.pdf, (Erişim:06 Ağustos 2019).*

[208] Resmi Gazete (2016). Olağanüstü Hal Kapsamında Bazı Kurum ve Kuruluşlara İlişkin Düzenleme Yapılması Hakkında KHK Değiştirilerek Kabul Edilmesine Dair Kanun. *2016/6757, https://www.resmigazete.gov.tr/eskiler/2016/11/20161124-4..htm (Erişim: 01 Şubat 2017).*

[209] BTK (2016). Bilişim Zirvesi'16 "No Way Out!" Dedi. *https://www.btk.gov.tr/tr-TR/Ulusal-Etkinlik/Bilisim-Zirvesi16-No-Way-Out-Dedi, (Erişim: 01 Şubat 2017).*

[210] BTK (2018). BTK Ziyaret ve Görüşmeleri. *17-18 Ekim 2018, Ankara.*

[211] UDHB (2014). Sektörel SOME Kurulum ve Yönetim Rehberi. *https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi, (Erişim: 10 Mart 2017).*

[212] Resmi Gazete (2018). BTK İdari Yaptırımlar Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik. *https://www.resmigazete.gov.tr/eskiler/2018/09/20180929-4.htm. (Erişim: 01 Ocak 2019).*

[213] Şimşek, B. (2019). Cumhurbaskanlıgı'nda Siber Teyakkuz. *https://www.sabah.com.tr/ekonomi/2019/10/30/cumhurbaskanliginda-siber-teyakkuz. (Erişim: 11 Kasım 2019).*

[214] ENISA (2012). National Cyber Security Strategies Practical Guide on Development and Execution. *ENISA Publications, Heraklion, Yunanistan.*

[215] ITU (2018). Guide to Developing a National Cybersecurity Strategy. *ITU Publications, Cenova, İsviçre.*

[216] TDK Sözlükleri (t.y.) Hedef. *https://sozluk.gov.tr/?kelime=hedef (Erişim: 20 Mart 2019).*

[217] Erendil, M. (1980). Milli Strateji ve Milli Güç. *Slh.Kuv.Dergisi Eki, 274, Gnkur.ATASE Yayınları, Ankara.*

[218] ITU (2018). ITU Global Cybersecurity Agenda High-Level Experts Group Global Strategic Report. *https://ccdcoe-admin.aku.co/wp-content/uploads/2018/11/ITU-080801-HLEGreport.pdf, (Erişim: 20 Mart 2019).*

[219] Resmi Gazete (2019). Cumhurbaşkanlığı teşkilatı hakkında cumhurbaşkanlığı kararnamesinde değişiklik yapılması. *CB KHK:48, https://www.resmigazete.gov.tr/eskiler/2019/10/20191024-1.pdf, (Erişim: 01 Kasım 2019).*

[220] Sayan, Ö. F. (2020). 3. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi Protokol Konuşması. *20 Şubat 2020, BTK Konferans Salonu, Ankara.*

[221] Weber, A. ve Thomas, R. (2005). Key Performance Indıcators. *http://www.plant-aintenance.com/articles/KPIs.pdf, (Erişim:12 Ağustos 2016).*

ÖZGEÇMİŞ

Ad-Soyad : Mustafa ŞENOL

Doğum Tarihi ve Yeri: 01 Ocak 1961, Kocaeli

E-posta : senolm15@itu.edu.tr

ÖĞRENİM DURUMU:

- **Lisans** : 1981, Kara Harp Okulu, Elektrik ve Elektronik Mühendisliği
- **Yükseklisans :** Kara Harp Akademisi, Silahlı Kuvvetler Akademisi ve Milli Güvenlik Akademisi, Yüksek sevk ve idare, Strateji, Uluslararası ilişkiler ve güvenlik.

MESLEKİ DENEYİM VE ÖDÜLLER:

- 1982 yılında Kara Kuvvetleri Muhabere (MEBS) Okulu'nu bitirdikten sonra Kara Kuvvetlerine ve Genel Kurmay Başkanlığına bağlı birlik ve karargâhlarda çeşitli görevlerde bulundu.
- 1991-1992 yıllarında A.B.D.'de Muhabere, Elektronik Bilgi Sistemleri ve Haberleşme Eğitimi gördü, ayrıca 'IBM Bilgisayarları Oryantasyonu', 'Bilgisayar Programlama' ve 'İleri Seviye Amerikan İngilizcesi' konularında eğitimler aldı.
- 2011-2014 yıllarında Kara Kuvvetleri Muhabere Elektronik ve Bilgi Sistemleri (MEBS) Başkanı olarak görev yaptı ve Tuğgeneral rütbesinde 2014 yılında kadrosuzluk nedeniyle emekli oldu.
- 2018-2020 yıllarında HAVELSAN Hava Elektronik Sanayi Ticaret A.Ş. Yönetim Kurulu Başkan Vekilliği görevinde bulundu.
- 2020 yılında İstanbul Teknik Üniversitesi Bilişim Enstitüsü'nde doktorasını tamamladı.

DOKTORA TEZİNDEN TÜRETİLEN YAYINLAR, SUNUMLAR VE PATENTLER:

- **Şenol, M.** (2016). Siber Güçle Caydırıcılık Ama Nasıl? *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:2, No:2, Gazi Üniversitesi Yayını, Sf.:10-17, Ankara. DOI:10.18640/ubgmd.303581.*
- **Şenol, M. (**2017). Ulusal Siber Güvenlik Stratejisi Oluşturma ve Uygulama İçin Bir Yaklaşım. 2.*Uluslararası Bilgisayar Bilimleri ve Mühendisliği Konferansı Elektronik Kitabı. Sf.:189-194, https://ieeexplore.ieee.org/document/8093373/, DOI:10.1109/UBMK.2017.8093373.*
- **Şenol, M.** (2017). Türkiye'de Siber Saldırılara Karşı Caydırıcılık. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:3, No:2, Sf.:1-9, Gazi Üniversitesi Yayını, Ankara. DOI:10.18640/ubgmd.373193.*
- **Şenol, M.** (2018). Hibrit Savaş Kapsamında Siber Savaş ve Siber Caydırıcılık. *Siber Güvenlik ve Savunma - Farkındalık ve Caydırıcılık (Ed.: Sağıroğlu, Ş. ve Alkan, M.), Bilgi Güvenliği Derneği Siber Güvenlik ve Savunma Kitap Serisi-1, Sf.:179-221, Grafiker Yayınları, Ankara.*
- **Şenol, M. (2019).** Siber Güvenlik, Savaş ve Caydırıcılık. *BTK - HAVELSAN Teknoloji Sohbetleri 5 Siber Savaşlar ve Geleceği, 25 Eylül 2019, BTK Konferans Salonu, Ankara.*
- **Şenol, M.** ve Karaçuha, E. (2020). Creating and Implementing an Effective and Deterrent National Cyber Security Strategy. *Journal of Engineering, Hindawi Publishing Corporation, Volume:2020, Sf.:1-19, https://doi.org/ 10.1155/2020/5267564.*

DİĞER YAYINLAR, SUNUMLAR VE PATENTLER:

- **Şenol, M.** (2012). Siber Savaş. *Silahlı Kuvvetler Dergisi, Sayı:413, Sf.:34-51, Gnkur. ATASE Yayınları, Ankara.*
- **Şenol, M.** (2012). Atatürk'ün Askerlik ve Liderlik Anlayışı. *Atatürk Haftası Armağanı Dergisi, 10 Kasım 2012, Genelkurmay ATASE Başkanlığı Yayını, Ankara.*
- **Şenol, M.** (2019). Sayısal Dönüşüm ve Yenileşim. *HAVELSAN Dergisi, Sayı:2, Sf.:30-38, HAVELSAN A. Ş. Yayını, Ankara.*
- Sağıroğlu, Ş. ve **Şenol, M**. (2019). *Siber Güvenlik ve Savunma - Farkındalık ve Caydırıcılık (Editör), Bilgi Güvenliği Derneği Siber Güvenlik ve Savunma Kitap Serisi-2, Grafiker Yayınları, Ankara.*