# ULUSLARARASI GÜVENLİKTE SİBER DENGELEME

**Doktora Tezi**

**Nuray ALTINDAĞ**

**Eskişehir 2023**

# ULUSLARARARASI GÜVENLİKTE SİBER DENGELEME

**Nuray ALTINDAĞ**

**DOKTORA YETERLİK TEZİ**

**Siyaset Bilimi ve Uluslararası İlişkiler Doktora Programı**

**Danışman: Prof. Dr. Murat ERCAN**

**Eskişehir**

**Anadolu Üniversitesi**

**Sosyal Bilimler Enstitüsü**

**Temmuz 2023**

# JÜRİ VE ENSTİTÜ ONAYI

Nuray ALTINDAĞ'ın "Uluslararası Güvenlikte Siber Dengeleme" başlıklı tezi 23 Haziran 2023 tarihinde, aşağıdaki jüri tarafından Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğinin 37. Maddesi uyarınca ilgili maddeleri uyarınca Uluslararası İlişkiler Anabilim Dalı Siyaset Bilimi ve Uluslararası İlişkiler Bilim Dalında, Doktora tezi olarak değerlendirilerek kabul edilmiştir.

İmza

Üye (Tez Danışmanı) : Prof. Dr. Murat ERCAN

Üye :Prof. Dr. Selim BAŞAR

Üye :Prof. Dr. Cenap ÇAKMAK

Üye :Prof. Dr. Ali AYATA

Üye :Doç. Dr. Deniz TURAN

Prof. Dr. Saime ÖNCE
Anadolu Üniversitesi
Sosyal Bilimler Enstitüsü Müdürü

# ÖZET

## ULUSLARARASI GÜVENLİKTE SİBER DENGELEME

Nuray ALTINDAĞ

Siyaset Bilimi ve Uluslararası İlişkiler Anabilim Dalı

Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Temmuz 2023

Danışman: Prof. Dr. Murat ERCAN

Teknolojinin ilerlemesi ve internet kullanımının yaygınlaşmasıyla uluslararası platformdaki aktörlerden, gerek devletler gerekse uluslararası işbirlikleri siber alana yönelik yapılanmalar geliştirmeye ve politikalar üretmeye mecbur kalmışlardır. Kötü amaçlı kullanıldığında siber alan, devletler açısından hayati öneme sahip tehlikeler barındırmaktadır. Özellikle geleneksel savaşların devletler için ciddi maddi yükümlülükler gerektirmesine rağmen; çeşitli siber saldırılarla bir devlete zarar vermenin yolunun, son derece cüzi gereklilikler içermesi, siber saldırıları cazip hale getirmektedir. Üstelik kimi zaman bu asgari şartların sağlanmasıyla yapılacak siber saldırılar, devletler için geleneksel savaşlardan daha tehlikeli sonuçlar doğurabilmektedir. Bu tehlikeler zamanla siber alanda da devletler için büyük bir güvenlik endişesi yaratmıştır. Bu gelişmelerle siber alan, devletlerin egemenliklerini ve güvenliklerini korumaları gereken bir platform halini alarak uluslararası güvenliğin önemli konularından biri haline gelmiştir.

Bu çalışmada siber alan, güç dengesi kavramıyla beraber değerlendirilecek, uluslararası platformdaki aktörlerin, siber alandaki davranışları ve politikaları ele alınacaktır. Aktörlerin ülkeler ve işbirlikleri çerçevesinde temel yapılanmalarına yer verilecek; ardından siber alanda gerçekleşen temel olaylar ele alınacaktır. Nihai bir genel değerlendirme ile siber alanda aktörler arasında bir siber dengeleme arayışının olup olmadığına dair bir sonuca ulaşılacaktır.



**Anahtar Kelimeler:** Uluslararası güvenlik, Siber alan, Güç dengesi, Siber dengeleme.

## ABSTRACT

## CYBER BALANCING IN INTERNATIONAL SECURITY

Nuray ALTINDAG

Department of Political Science and International Relations

Anadolu University Institute of Social Sciences, July 2023

Advisor: Prof. Dr. Murat ERCAN

With the advancement of technology and the widespread use of the internet, both the states and international collaborations from the actors in the international platform were obliged to develop structures and produce policies for the cyberspace. When used maliciously, cyberspace contains vital dangers for states. Although traditional wars require serious financial obligations for states; The fact that the way to harm a state with various cyber-attacks contains extremely low requirements makes cyber-attacks attractive. Moreover, sometimes cyber attacks that will be carried out by providing these minimum conditions can cause more dangerous results for states than traditional wars. These dangers have created a great security concern for states in the cyber field over time. With these developments, cyber space has become one of the important issues of international security by becoming a platform where states must protect their sovereignty and security.

In this study, the cyber space will be evaluated together with the concept of balance of power, and the behaviors and policies of the actors in the international platform will be discussed. The basic structuring of the actors within the framework of countries and collaborations will be included; Then, the main events taking place in the cyber space will be discussed. With a final overall assessment, a conclusion will be reached on whether there is a search for cyber balancing among the actors in the cyber space.



**Keywords:** International security, Cyberspace, Balance of power, Cyber balancing.

# TEŞEKKÜR

Öncelikle saygıdeğer hocam Prof. Dr. Murat Ercan'a doktora sürecim boyunca sağlamış olduğu katkılar için teşekkürlerimi sunuyorum. Bu çalışmanın her aşamasında desteklerini esirgemeyen Prof. Dr. Selim Başar ve Prof. Dr Cenap Çakmak'a teşekkürlerimi sunuyorum. Lisans, yüksek lisans ve doktora hayatım boyunca ilgisini esirgemeden, her soruma cevap vererek beni yönlendiren, ufkumu genişleterek çalışmalarımın tüm aşamalarında bana rehberlik eden ve bu sürede bir usta çırak ilişkisiyle gelişmeme büyük katkı sağlayan Prof. Dr. Cengiz Dinç'e teşekkürlerimi sunuyorum. Ayrıca, lisans, yüksek lisans ve doktora öğrenimim boyunca ders aldığım tüm Eskişehir Osmangazi Üniversitesi ve Anadolu Üniversitesi öğretim üyelerine teşekkürlerimi sunuyorum.

Hiçbir zaman benden desteklerini esirgemeyen, tüm zor zamanlarımda maddi ve manevi varlıklarıyla yanımda olan, bana benden daha çok güvenerek, gösterdikleri ilgi, sevgi, sabır ve yaşama dair tüm paylaşımlarıyla her anımı güzelleştiren, hayatımın ve ideallerimin mimarları annem Hatice Altındağ ve babam Ahmet Altındağ'a minnet borçluyum. Bilginin sonsuzluğunu göstererek, gerektiğinde 'bilmiyorum' diyebilme erdemini öğreten, doğumumla beraber eğitim ve öğretim sürecimi başlatan, hayatımdaki en büyük şansım ailem, bu çalışmanın asıl sahipleridir. Hayatımı cennete çeviren can yoldaşım İlker Göktaş'ın sevgisi ve desteği olmasaydı böyle bir çalışmayı tamamlamak mümkün olmazdı. Beni bir an bile yalnız bırakmayan patili kızım Arwen'in varlığı, her zaman en büyük motivasyonlarımdan biri oldu. Elbette her çalışmada olduğu gibi bu çalışma süresince de hem akademik hem hayata dair türlü zorluklar yaşanmıştır. Tüm bu zorluklar içinde beni desteklemekten asla vazgeçmeyen başta Burcu Babayiğit, Barış Canbolat, Hülya Öztürk, Mehtap Altunel ve Meriç Yetik olmak üzere tüm can dostlarıma ve ne olursa olsun hayatımı dans tadında yaşamama vesile olan Tango26 aileme teşekkür ederim.

17/08/2023

## ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Bu tezin bana ait, özgün bir çalışma olduğunu; çalışmamın hazırlık, veri toplama, analiz ve bilgilerin sunumu olmak üzere tüm aşamalarında bilimsel etik ilke ve kurallara uygun davrandığımı; bu çalışma kapsamında elde edilen tüm veri ve bilgiler için kaynak gösterdiğimi ve bu kaynaklara kaynakçada yer verdiğimi; bu çalışmanın Anadolu Üniversitesi tarafından kullanılan "bilimsel intihal tespit programı"yla tarandığını ve hiçbir şekilde "intihal içermediğini" beyan ederim. Herhangi bir zamanda, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçları kabul ettiğimi bildiririm.

(Öğrencinin Adı Soyadı)

## İÇİNDEKİLER

**Sayfa**



## BİRİNCİ BÖLÜM

## ÜÇÜNCÜ BÖLÜM

## TABLOLAR DİZİNİ

**Sayfa**

## ŞEKİLLER DİZİNİ

**Sayfa**

## KISALTMALAR DİZİNİ

| | |
|---|---|
| AB | : Avrupa Birliği |
| ABD | : Amerika Birleşik Devletleri |
| APT | : Gelişmiş Siber Tehditler |
| ARPA | : Gelişmiş Araştırma Projeleri Ajansı |
| ARPANET | : Gelişmiş Araştırma Projeleri Ajansı Ağı |
| CERT | : Bilgisayar Olaylarına Müdahale Ekibi |
| ÇHC | : Çin Halk Cumhuriyeti |
| DCS | : Dağıtık Kontrol Sistemi |
| DDoS | : Dağıtık Hizmet Dışı Bırakma Saldırıları |
| DoS | : Hizmet Dışı Bırakma Saldırıları |
| ENISA | : Avrupa Şebeke ve Bilgi Güvenliği Ajansı |
| ICS | : Endüstriyel Kontrol Sistemleri |
| IP | : İnternet Protokolü |
| NATO | : Kuzey Atlantik Anlaşması Teşkilatı |
| NCI | : Kuzey Atlantik Anlaşması Teşkilatı Muharebe ve Bilgi Teşkilatı |
| NPC | : Çin Ulusal Kongresi |
| SCADA | : Merkezi Denetleme Kontrol ve Veri Toplama Sistemi |
| SSCB | : Sovyet Sosyalist Cumhuriyetler Birliği |
| TR-BOME | : Türkiye Bilgisayar Olayları Müdahale Ekibi |
| UEKAE | : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü |
| USCYBERCOM | : Amerika Birleşik Devletleri Siber Komutanlığı |

# GİRİŞ

İlk amacı kod çözme olan ve hacmi bir oda büyüklüğünde olan bilgisayarın zamanla gelişmesi, teknolojide yeni bir çığır açmıştır (Randell, 2012). Rusya'nın Ay'a uydu göndermesinin ardından, bir araştırma birimi kuran ABD, nükleer bir saldırı halinde tek bir merkeze bağlı kalmayarak ve iletişimin kesintiye uğramadan devam etmesine olanak tanıyacak bir yapı üzerinde çalışmaya başlamış (Weimann, 2006) ve bu çalışmalar internetin ortaya çıkmasını sağlamıştır. Başlangıçtaki temel amacı iletişim olan internetin temel felsefesi, bilgi paylaşımıdır ve tasarlanırken kullanım kolaylığı, maliyette düşüklük ve evrensel ulaşılabilirlik dikkate alınmış; internet kullanıcılarının zamanla bu sistem için tehdit haline gelebileceği düşünülmemiştir. (Goodman, 2008). Bu sebeple siber ortama dair güvenlik, bu ortamın önemli bir bölümünü oluşturan internetin tasarımından daha sonra dikkat çekmeye başlamış ve ancak bundan sonra inşa edilmeye çalışılmıştır.

Siber alana dair güvenlik endişeleri ilk zamanlarda internetin fiziki altyapısına gelebilecek tehditlerle sınırlıyken, zararlı kodlar ve virüslerin üretilmesi ve bunların yaygınlaşması, siber güvenlik endişesini hem dikey hem de yatay düzlemde artırmıştır. Başka bir ifadeyle siber güvenlik endişesi, hem yükselmiş hem de daha geniş bir alana yayılmıştır (Cridland, 2008).

İlk olarak 1990'larda sadece ağa bağlı bilgisayarların güvenlik sorunlarını ifade etmek için kullanılan (Hansen ve Nissenbaum, 2009) siber güvenlikte, tehdit oluşturan saldırı araçları oldukça fazla sayıda ve çeşitlidir. Kimi zaman virüs, solucan, kurtçuk, Truva atı ya da casus yazılım gibi siber silahlar saldırı aracı olurken, kimi zaman sahte ya da kopya internet siteleri tehdit oluşturabilmektedir. Dolayısıyla siber güvenlikte bireyler hem saldırı aracı hem de saldırı hedefi haline gelmektedir. Siber alandaki tehditlerin sadece yine siber alanda yer alan varlıklara yönelik olduğunu düşünmekse büyük bir yanılgıdır. Elbette siber saldırılarla, bu alanda bilgi hırsızlığı ve casusluk yapmak, kişisel bilgilerin çalınması, istenmeyen elektronik postalara, reklam ve propagandalara maruz kalınması gibi sonuçlar doğurabilmektedir. Ancak daha da önemlisi bu yolla devletin varlıklarına ciddi zararlar verilebiliyor olmasıdır.

Son derece ciddi sosyal, ekonomik, politik ve askeri tehditlerin yükselmesiyle siber güvenlik, devletler için çok daha büyük bir öncelik haline gelmiştir. Kötü niyetli

kullanıcılarla beraber teröristlerin de siber saldırılarla bir devlete ait kritik alt yapılara kasıtlı olarak zarar verebileceği gerçeği ortaya çıkmıştır. Teknolojinin çığır açan bir şekilde gelişip değişmesinin de büyük etkisiyle siber alanda güçlü ve etkin savunma sistemlerinin geliştirilmesi, kriz ve saldırı durumlarına hazırlık çalışmalarının yapılması, saldırıların engellenmesine yönelik bariyerlerin inşa edilmesi, ulusal ve bölgesel siber güvenlik politikalarının oluşturulması zorunlu hale gelmiştir (Goodman, 2008).

Siber saldırı araçlarından bir ya da birkaç tanesinin kullanılmasıyla dünya üzerindeki çok sayıda sistemden bilgi kopyalanabilmektedir. Dolayısıyla devletler için son derece kritik öneme sahip askeri ve politik bilgi, siber saldırıların hedefi olabilecek durumdadır (Geers, 2012). Zarar görmesi halinde son derece hayati sonuçlar doğurabilecek kritik alt yapılar içinde; su arıtma ve dağıtma sistemleri, elektrik üretim ve dağıtım sistemleri, petrol ve gaz tesisleri, ulusal enerji, ulaşım, haberleşme ve finans sistemleri, -e devlet uygulamaları, stratejik sanayi ve teknoloji alt yapıları ve ulusal savunma ve güvenlik alt yapılarını sıralamak mümkündür. Bu kabaca sıralamadan bile anlaşılacağı üzere, bu sistemlerin gelebilecek muhtemel saldırılardan korunması devletler adına hem vatandaşlarının hem de kendi güvenliğini sağlamak için son derece hayati bir önem taşımaktadır. Siber alanda bu duruma örnek verilebilecek çok sayıda olay meydana gelmiştir. Bu saldırıları tek tek ayrıntılı şekilde tek bir çalışma içinde incelemek mümkün olmasa da uluslararası ilişkiler ve siber güvenlik açısından tarihi öneme sahip siber olaylar üçüncü bölümde ele alınmıştır.

Küresel anlamda büyük kolaylık ve fayda sağlayan teknolojik gelişmelerin kötü niyetli kullanıcılar tarafından suistimal edilmesi, yaşanan siber saldırılar ve bu saldırıların doğurduğu sonuçlar güvenlik algısında büyük değişikliklere sebep olmuştur. Gelinen noktada bireysel, kurumsal, toplumsal, ulusal ve uluslararası güvenlik içinde siber güvenliğin yeri ve önemi artmış, özellikle devletlerin güvenlik ajandasında ilk sıralarda yer almaya başlamıştır. Nitekim ABD eski Başkanı Obama "siber güvenlik risklerinin 21. Yüzyılın en ciddi ekonomik ve ulusal güvenlik zorluklarının bir kısmını oluşturduğunu" dile getirmiş, Foreign Policy dergisi siber alanı "tek ve en büyük gelişmekte olan tehdit" olarak nitelendirmiş ve Boston Globe, geleceğin bu alanda olduğunu iddia etmiştir (Singer ve Friedman, 2014). Tüm bunların yanında siber suçların küresel ekonomiye verdiği zarar, her yıl 1 trilyon dolar civarında hesaplanmıştır (Kane, 2012).

ABD, İngiltere, Fransa, Almanya, Japonya, İtalya, Kanada, Danimarka, İsveç, İspanya, Estonya, Malezya gibi çok sayıda ülke, siber güvenlikle ilgili politikalar geliştirmekte ve ulusal kurumlar inşa etmeye çalışmaktadır. Türkiye'de de siber güvenlik alanında gerçekleştirilen faaliyet ve düzenlemeleri; Siber Güvenlik Eylem Planları, Ulusal Bilgi Güvenliği Programı, Ulusal Bilgi Güvenliği Kapısı, Siber Güvenlik Müdahale Ekipleri ve Birimleri, Siber Güvenlik Tatbikatları, konferans ve çalıştaylar ve Türk Silahlı Kuvvetleri ile TÜBİTAK çatısı altında yürütülen çalışmalar olarak sıralamak mümkündür.

Günümüzde internetin ve tüm bilişim sistemlerinin neredeyse hayatın bütün alanlarında kullanıldığı dikkate alındığında, siber güvenlik ulusal ve uluslararası güvenlik için son derece hayati bir önem taşımaktadır. Üstelik teknolojinin gün geçtikçe ilerlemesi, bu önemin de zamanla çok daha geniş bir alana yayılacağını göstermektedir.

Ulusal güvenlikleri adına son derece önemli hale gelen siber alanda riskler ve tehlikeler ise ulusal sınırlara hapsedilemez boyuttadır. Bu sebeple siber güvenliği sağlamak için ulusal çabaların yanında bölgesel ve küresel politikaların ve yapılanmaların varlığı devletler için hayati önem taşımaktadır.

Her ne kadar yeni bir alan olsa da siber güvenliğe dair çok sayıda çalışma bulunmaktadır. Ancak bu çalışmaların büyük kısmı, konunun doğası gereği, teknik ve mühendislik alanları içinde yer almaktadır. Bu çalışmada uluslararası ilişkiler disiplininin temel kavramlarından olan "güç dengesi" ile siber alan birlikte değerlendirilmeye çalışılmıştır. Uluslararası platformdaki aktörler siber alanda da denge arayışında mıdır? Siber alan, güç dengesi açısından uluslararası platformun bir uyarlanması mıdır? Siber saldırıya uğrayan bir aktör, saldırı sonrasında siber alandaki yapılanmalarını ve politikalarını değiştirmekte midir? Aktörler siber denge için ittifak arayışına girmekte midir? Soruları bu çalışmanın temel araştırma sorularını oluşturmaktadır. Çalışmanın ilk bölümünde kavramsal çerçeve içinde güvenlik algısı ve siber güvenlik, ikinci bölümde uluslararası ilişkilerde etki aracı olarak siber güvenlik başlığı altında siber silahlara, siber saldırı türlerine, siber savunma, korunma yöntem ve sistemlerine son olarak da siber aktörlere yer verilmiştir. Son bölümde literatürde uluslararası platformda siber alanda başat aktörler olarak kabul edilen devletlerin ve uluslararası işbirliklerinin siber alandaki

temel yapılanmaları ardından siber alanda tarihi öneme sahip olaylar ele alınmıştır. Son olarak genel değerlendirme ve sonuç bölümüyle çalışma tamamlanmıştır

# BİRİNCİ BÖLÜM

## 1. KAVRAMSAL ÇERÇEVE

### 1.1. Güvenlik Algısı:

#### 1.1.1. Kavramsal olarak güvenlik:

Uluslararası ilişkiler çerçevesinde "güvenlik" terimi, bu disiplinin temel ayaklarından birini oluşturmaktadır. Dolayısıyla bu bilim dalının dayanmış olduğu düşünsel temellerde, güvenlikle ilgili bakış açıları son derece önemli bir yere sahiptir. Hatta "güvenlik" teriminin boyutu ve önemi bazı yazarlar tarafından öylesine önemsenmiştir ki, terimin kimi zaman uluslararası ilişkilerin önüne geçtiği bile iddia edilmiştir (Çiçekçi, 2012: 6).

"Güvenlik" terimi, değişik sözlüklerde müşterek anlamlarla yer almaktadır ve genel olarak tehdit, korku ve tehlikelerden uzak olmak manasına gelmektedir (Karabulut, 2015: 7). Bir insanın veya departmanın güvenlik içinde olmasını, Benjamin Miller ise "The Concept of Secuirty: Should it be Redefined" başlıklı yazısında iki şarta bağlamaktadır. Bu şartlar; mevcut değerlerle ilgili bir tehdidin bulunmaması ve eğer bu tür bir tehdit bulunuyorsa, tehditle karşılaşanın akli bir maliyet ile söz konusu tehdidi savuşturma kapasitesine sahip olmasıdır (Miller, 2010: 26-27).

Baldwin (2004: 1) geniş çerçeveli bir araştırma olan "Güvenlik Kavramı" isimli eserinde, terimin tekrar açıklanmasının disiplin içi bir gereklilik olduğunu ortaya koymaktadır. Bu tür gayretlerin önemli bir kısmı ise "güvenlik" teriminin kendisiyle alakalı olmasından ziyade, ulus devletlerin siyaset gündemlerinin tekrar tanımlanmasıyla alakalıdır.

"Güvenlik" terimi sorgulandığı zaman da milli güvenlikle ilgili olarak en önemli tehlike hala savaşlardır. Nükleer, kimyasal ve biyolojik kitle imha silahlarının yaygınlaştığı, ihtilaflarla sınırların, ırki ve dinsel güç, kaynak, mülteci, insan haklarıyla ticaretin dışındaki problemlerin yoğunluk kazandığı uluslararası sistemde, güvenlik tüm devletlerin programlarında üst sıralardadır. Bu çerçevede pek çok ülke, güvenliğine tehdit olacak ihtilafları sonlandırmak adına uluslararası örgütler kurmakta ve var olan örgütlere katılmaktadır. Elbette uluslararası sistemdeki çatışmaların birçoğunun nedeni

derinlerdedir ve bazı yazarlar çatışma nedeni ciddi ise uluslararası örgütlerin çözüm adına yararının olmayacağını dile getirmektedir (Roskin ve Berry, 2014: 277). Tartışmaların bir bölümünü de bu bağlamda, uluslararası yapılanmalar ile oluşabilecek güvenlik anlayışı veya "kolektif güvenlik" şeklinde belirtilen güvenlikçi yaklaşım temsil etmektedir ama bu hususta meydana gelebilecek güvenlik perspektifiyle ilgili oluşturulan uluslararası bir müşterek akıl da yoktur (McSweeney, 1999: 5).

Devletlerin ajandalarında üst sıralarda yer alan "güvenlik" terimi, bu perspektiften ele alındığı zaman, uluslararası ilişkiler faaliyetleri kapsamında pek çok yazar arasında da tartışmalı kalmaktadır. Ancak uluslararası ilişkiler disiplininde uzmanların pek çoğunun güvenliğin devletin temel değerlerine yönelik tehditlerden uzak/bağımsız olması manasına geldiği hususunda bir uzlaşı içinde olduğunu söylemek mümkündür. Yine de bu noktada da analizlerin merkezinin "bireysel", "ulusal" veya "uluslararası" güvenlik mi olması gerektiği konusunda farklılaşma olduğu gözlenmektedir. Ağırlıklı olarak askeri açıdan tanımlanmış "ulusal güvenlik", tarihi olarak da alan yazınına egemen olmuştur. Bu bakış açısının ana ilgi alanıysa, ülkelerin kendisine dönük tehditler ile başa çıkmak üzere geliştirmesi gereken askeri olanak ve yetenekler üstüne kurgulanmıştır (Baylis, 2008: 73).

Temelde söz konusu yeteneklerin güvenlikle ilgili algıdaki boyutu, nükleer silahların, haberleşme ve ulaşımla ilgili teknolojilerin, bilhassa savaşlar üstündeki tesiri üstüne gelişmiştir. Bu durum ise askeri açıdan "devrim" olarak görülmektedir. Savaşlar gün geçtikçe daha yoğun bir şekilde elektronik unsurlar ile donatılmaktadır. Nitekim bu anlamda çok önemli olan "cephe" terimi değişmiş, insansız hava araçları, hassas güdümlü mühimmatlar, global konum tespit sistemleri, haberleşme ağlarıyla bilgisayarlar sahada çok daha belirleyici bir hale gelmiştir. "Güvenlik" terimine dair algıdaki değişimi ve bahsi geçen teknolojik ögelerin baskınlığının artması ile değişik çalışma sahalarını ortaya çıkarmıştır. Elbette bu değişik çalışma sahalarının uluslararası ilişkiler içinde bölünmüşlüğü kuramsal alanı da zenginleştirmiştir.

### 1.1.2. Günümüzde güvenlik:

Güvenliğe dair algının değiştiği veya bazı bilim adamlarına göre değişik algılandığı artık bir realitedir. Çağımızda, temelde silahlar ve savaş ögelerinin değişmesiyle çağdaş politika teorileri de güvenlik algısının ögeleri üstünde durmaktadır.

Şekil 1.1'de Sun Tzu'nun modelinden de ilham alan Geeraertz ile Jing, "güvenlik" terimini "askeri olmayan" ile "askeri güvenlik" şeklinde iki biçimde incelemiştir. Bu bakış açısına benzeyen yaklaşımlardaki tasnifte uluslararası ilişkilerin doğasıyla ilgili yapılan askeri kavramsallaştırmayla ilgili iyi bir örnek teşkil etmektedir. Nitekim bu türden tipolojilerde devletlerin var olmalarıyla alakalı bir düşünce ortaya konmaktadır. Ancak bu tip tasniflerde çalışmanın da konusu içinde yer alan "siber güvenlik" teriminin nasıl ve nerede bulunabileceği konusu tartışmalı kalmaktadır.


**Şekil 1. 1.** *Kapsamlı güvenlik anlayışıyla sınıflandırma (Geeraerts, Jing, 1999)*

Soğuk Savaş'ın bitişinin, güvenlik algısıyla ilgili değişimin özünde ciddi bir dönüşümü beraberinde getirdiği görülmektedir. Söz konusu dönüşümün ise ne şekilde ve hangi cephede olduğuyla ve hangi şekilde ilerlediğiyle ilgili pek çok faktör ve teori ortaya çıkmıştır. Söz konusu faktörlerin baş döndürücü bir şekilde algıya dayalı değişimi Amerika'da İkiz Kuleler ile Pentagon'a çarpan uçakların ardından gündeme gelmiştir (Paker, 2012: 17). Devletler arasında devam eden mücadeleler legal olmayan yapılanmalara da sıçramış ve uluslararası aktörler arasındaki güvenlik algısı tabiri caizse artık bir algısızlık haline gelmiştir.

### 1.1.3. Güvenlik teorilerinin düşünsel temelleri:

"Güvenlik" terimiyle içinde barındırdığı bütünlük, insanın gelişimi ile beraber bireyin bulunduğu her noktada kullanılmış olan bir terimdir. Ayrıca mevcudiyetini koruma ve devam ettirme amacı taşıyan tüm davranışlarda karşılaşılan bir hadisedir. Bireyle ilgili söz konusu durum bütün sosyal, milli ve uluslararası kuruluşa da yayılmıştır. Bu durumun özünde tehdit olgusu ve insanın tabiatındaki bazı çatışmacı ögeler etkilidir.

Uluslararası ilişkilerde güvenliğe göre de aktörler amaçlarına dayalı olarak değişik güvenlik perspektifi sergilemektedir. Dedeoğlu (2003: 12) uluslararası ilişkilerde "güvenlik" teriminin esasında birkaç bağlamda belirtilebileceğini dile getirerek aşağıdaki tasnifi ortaya koymuştur:

- Uluslararası sistemin tamamı veya tamamına yakınının güvenliği,
- Coğrafi veya fonksiyonel alt-sistemlerin, bölgelerin güvenliği,
- Ülkenin güvenliği,
- Toplumsal güvenlik,
- Sosyal alt-grupların güvenliği,
- Fertlerin güvenliği.

Yaklaşımsal bağlamda farklı unsurlar ile incelenen "güvenlik" teriminin içinde "siber güvenlik" olgusunun da ele alınmasına dair öncelik, insanları yakın tarihe yaklaştırmış olsa da antik dönemden gelmiş olan güvenlik parametreleri belirli bir birikim ile de evrimini devam ettirmektedir. Devrimler, sınıf çatışmaları vb. unsurlar ile yoğrulmuş olduğu ve teknolojideki gelişmeler ile dünyanın algılanmasıyla alakalı değişimlerin güvenlik parametrelerinde hissedilmeye başlandığı global ortam kendi başına ciddi bir tartışma ve araştırma sahasıdır.

XX. yüzyılın başındaki gelişmeler, güvenlikle ilgili yaklaşımsal tavrı bilhassa uluslararası ilişkilerle ilgili olarak daha önemli bir yere taşımış ve çağımızdaki çalışmalar açısından temel mimariyi teşkil etmiştir. Uluslararası ilişkilerin çağdaş fikir adamlarından XX. yüzyılın başındaki gelişmeler ile yoğurmuş olduğu uluslararası sistem Machiavelli, Hugo Grotius, Thomas Hobbes, Hegel, Kjellen, Ratzel, Haushofer, Marx gibi pek çok fikir adamının düşünceleriyle temel eleştiri noktası olmuştur.

Söz konusu birikimle, yaklaşımsal bağlamda güvenlik uzun bir müddet realizmin hakimiyetinde gelişmiştir. Bu gelişim iki kutuplu sistemin SSCB'nin dağılmasından sonra ortadan kalkması ile beliren devlet-altı ve ötesi gelişmeler ile beraber yeni bir görünüm de kazanmıştır (Çiçekçi, 2012: 30). Globalleşen dünyanın getirdiği değişik parametreler realizm merkezindeki yaklaşımla tartışmaları kendi içinde eritmiştir. İktisadi unsurlar ve savaş stratejileri, gücün değişik biçimlerde ve tanımlar ile değerlendirilmesini zorunlu hale getirmiştir.

Colin Elman, "yükselen ve düşen" realizm tanımlaması ile gelişmekte ve değişmekte olan bu durumu incelemiştir. Uluslararası sistemin dinamikleri kendi içinde gücün döngüsünü iktisadi beklentilerle ve menfaatlerle kişileri ve kuruluşları da bazen en üst seviyeye taşır iken bazen kendi içerisinde menfaatler çerçevesinde ortadan kaldırmaktadır (Elman, 2007: 15). Bunu Gilpin'in 1981 senesinde yayımladığı yapıtı, "War and Change in World Politics"le de ilişkilendirmiş olan Elman'ın, uluslararası ilişkilerin temelde gerçekte hiç değişmediğini, sadece kabuğunun değiştirdiğini vurgulaması sebebiyle, çağımız siber güvenlik araştırmalarının özüne dair bir gönderme yaptığını da dile getirmek mümkündür.

İki kutuplu uluslararası sistemin yumuşadığı dönemlerde etkisini devam ettiren bir başka model olan neo-realist teori, değişen koşullarla ilgili durumu etkileyici bir biçimde ortaya koymaktadır. Bu teori, devletlerin uluslararası yapıda dış siyaset toplamı şeklinde görülmediği realitesini, kendi güvenliklerinden sorumlu olan devlet anlayışı ile çok taraflı biçimde ele almıştır. Uluslararası sistemin kuralının, bu durumu tesis edebilecek güce sahip aktör tarafından tespit ve tesis edileceği anlayışı etrafında, aktör çatışmacıysa sistemin kaotik, uyuşmacıysa barışçı olacağı dile getirilmiştir (Dedeoğlu, 2013: 45).

Güvenlikle ilgili öne çıkan başka bir teori olan liberalizm, felsefi ve farklı bir perspektifle, çok yönlülüğü artırarak, insanın tabiatını dikkate alıp bunu değiştirmeye çalışmaktansa, pozitif olarak yönlendirmeyi seçmektedir (Birdişli, 2016: 39). Liberalizm, güvenlik yaklaşımları bakımından, kendi içinde farklılıklar barındırmaktadır ve bu sebeple, siber güvenlik çalışmaları açısından kuramsal bir zeminde açıklanması da oldukça zor görülmektedir.

Kuramsal olarak uluslararası sistem bağlamında, güvenlik modellerinde benzer bir zorluk ve karmaşıklığa sahip bir başka teori de Marksizm'dir. Uluslararası çatışmaların kendi içindeki dinamiklerin bir ürünü olduğunu her zaman vurgulamış olan bu yaklaşımsal gelenek, hegemonik sistemin sorunsal bütünlüğünü sömürgeci gelenekle ve küreselleşmeyle bağdaştırmaktadır (Rupert, 2007: 42). Marksizm'de devletin, hakim sınıfın baskınlığının sürdürülmesinin bir aracı şeklinde görülmesi, güç münasebetini açıklama konusunda ve siber güvenlik gibi sahalarda kuramsal bir tavır oluşturmayı güçleştirmektedir. Bu çerçevede eleştiri temelinde baskın perspektif, güvenlik sahasının geneline dair, yalnızca ideolojik bir bakış açısı sunmaktadır (Wallerstein, 2004: 130).

Konstrüktivist (İnşacı) yaklaşımsa, kuramsal olmanın dışında, bilhassa liberalizmle Marksizm'den farklılaşıp analiz metodu olarak uluslararası sistemle ilgili çok boyutlu veya disiplinler arası bir perspektif getirmesi, bilhassa yeni güvenlikle ilgili algı bakımından önemli bir temel yaratmaktadır. Materyalizmle idealizmin bileşiminden oluşan çok cepheli bir modelin güvenliğe etkisi, söz konusu teori içerisinde ciddi bir yere sahiptir (Birdişli, 2016: 84).

Tablo 1.1'de değişik modellerin temel aktörler ile beraber değişkenler, davranış, analiz düzeyi ve yöntem açısından tasnif edilmiştir. Temel değişkenlerle beklenen davranışlar bakımından söz konusu teoriler arasındaki zenginlik ve farklılık, gerçekte güvenlikle ilgili tüm yaklaşımların kendine has duruşunu ortaya koymaktadır. Temel değişkenlerin arasında liberal ve Marksist teorilerin ağırlıklı olarak iktisada olan vurgusundan kaynaklanan farklılıkları göz ardı edilmemelidir.

**Tablo 1. 1.** *Güvenlik paradigmalarnnnn kıyaslanması (Buzan ve Hansen, 2009)*

| Fikir Okulu | TemelAktörler | Temel Değişkenler | Beklenen Davranışlar | Analiz Düzeyi | Yöntem (ler) |
|---|---|---|---|---|---|
| **Realizm** | Devlet | Şiddet/ Askeri Kuvvet | Çatışma/Rakip ile İş birliği | DevlettenDevlete | Tarihi/Analitik |
| **Neorealizm** | DevletlerSistemi | Şiddet/ Askeri Kuvvet | Çatışma/İş birliği Mümkün | Sistem | Tarihi/Analitik |
| **Liberal Kurumsalcı** | Öteki Oyuncularla Sınırlı Devlet | Şiddet/ Askeri Kuvvetle İktisadi | İş birliği | Devletten Devlete/ Milletleşen Kuvvet | Tarihi/ Bilimsel/ Analitik/ Davranışsal |
| **Geleneksel Liberalizm** | Birey (Birey/ Şirket) | Teknolojik/ İktisadi | İş birliği | Ferdi | Yöntem bilimsel |
| **Neomarksism** | Şirketler | Teknolojik/ İktisadi | Çatışma | Sistem/ Piyasalar | Tarihi/ Analitik |
| **İnşacı** | Toplumsal İnşacı Olarak Oyuncu | Düşünceler/ Değerler | İş birliği/ Çatışma (?) | Toplumsal İnşa ile Değişim | Toplumsal ve Sosyo-Psikolojik |
| **Davranışsal** | Araştırma Bağımlısı | Araştırma Bağımlısı | Çatışma/ İş birliği | Tüm Düzeyler | Modellemeye Ölçüm |

## 1.2. Uluslararası İlişkilerde Güç Dengesi:

### 1.2.1. Güç dengesi sisteminin temel kavramları:

Güç kavramı uluslararası ilişkiler alanında oldukça sık kullanılan kavramlardan biridir. Türk Dil Kurumu (TDK) güç kavramını "Fizik, düşünce ve ahlak yönünden bir etki yapabilme veya bir etkiye direnebilme yeteneği, kuvvet, efor. Zihin gücü. Yaşama gücü." şeklinde tanımlamaktadır.

Güç bir eylemi gerçekleştirme potansiyeli başka bir deyiş ile "yetenek" anlamında kullanılmasının yanı sıra bir eylemi gerçekleştirmeye bağlı olarak amaçlanan sonucu elde

edebilme yeteneği olarak da kullanılmaktadır. Bununla birlikte "ikna edici unsur" olarak da değerlendirilmektedir. Bu bağlamda güç ile bireyleri, grupları, toplumları, örgütleri ve devletleri tehdit, teşvik, ikna veya zor kullanma yöntemlerinden herhangi biri veya birkaçıyla istenilen eylemi gerçekleştirmesini sağlayan bir unsur ve çatışmaların ve engellerin üstesinden gelme yeteneği olarak da bahsedilmektedir (Viotti ve Mark, 1999: 65). Güç kavramı bireyler bazında fiziksel güç olarak değerlendirilmesine karşın devletler bazında askeri, ekonomik, sosyal, kültürel vb. açılardan bir devletin başka bir devlete karşı üstünlüğünü ifade eden bir unsur olarak geçmişten günümüze kadar olan süreçte güncelliğini koruyan bir anlam taşımaktadır. Güç kavramına ilişkin pek çok farklı tanımlama söz konusu olmasına karşın tanımlamalar genel olarak benzer bir anlamı ifade etmektedir.

Güç kavramı uluslararası düzeyde ilişkiler ve uluslararası politikalar açısından oldukça önemli bir kavram olarak öne çıkmaktadır. Tarihsel süreçte güç kavramı değerlendirildiğinde, ilkel toplumlarda, toplumlar arası çatışmaların açıklanmasında kullanılan bir kavram olarak gözlemlenmektedir. Toplumların devlete evrilme sürecinde en önemli etken olarak insanların şiddet eğilimi taşıması olduğu düşünülmektedir. Bu bağlamda Openheimer'ın öne sürdüğü çatışma teorisi toplumların devlete evrilmesinde en önemli faktörün çatışmalar olduğunu öne sürmektedir. Bu teoriye göre henüz ilkel toplumların devlete evrilmesinden öncesinde yer alan süreçte güce sahip olan toplumların kendisinden güç olarak zayıf olan toplumları himayesi altına alması, toprakları işgal etmesinin bir sonucu olarak çatışma ortamı ortaya çıkmış ve buna bağlı olarak toplumlar devletlere evrilmiştir. Hobbes da Openheimer'ın önermesine benzer şekilde devletlerin çatışmalardan ve savaşlardan ortaya çıktığını öne sürmektedir (Hobbes, 2017: 133). Bununla birlikte bireylerin kişisel menfaatleri doğrultusunda çatışma yaratmaya ve dolayısıyla dünya genelinde bir kaos ortamı hakimiyeti olduğunu ifade etmektedir. Devlet, toplumların ortak bir amaç bağlamında bir araya gelmesi ve belirli bir hukuki sistem kapsamında bireylerin haklarını koruyan bir güç olarak ifade edilebilir. Hobbes önermesi bağlamında, dünya genelinde var olan kaos ortamını ancak devletlerin kurulmasının önleyebileceğini ifade etmektedir.

Toplumların devletlere evrilmesinin ardından, bireylerin çıkar çatışmasına bağlı olarak bir başkasından zarar gelebileceği korkusu, toplumsal düzeyde en aza indirgenmiş

olmaktadır. Bu bağlamda bireylerin zarar görme korkusu azalmakta ve bireysel çıkarlarının korunması amacı doğrultusunda, bireyler güçlerini devlet otoritesinin hakimiyetine sunmaktadırlar. Toplumların devletlere evrilmesinin ardından sosyal anlamda pek çok değişiklik ortaya çıkmıştır. Bu bağlamda bireylerin, devletlerin oluşumundan önce var olan özgürlükleri, hukuki düzen kapsamında sınırlandırılarak devlet otoritesine devredilmiştir. Bununla birlikte hukuki düzenlemeler kapsamında sınırlandırılan özgürlük, bireylere tekrar teslim edilmemektedir. Hobbes tarafından yapılan önerme bağlamında, devletler ortaya çıkmasına karşın dünya genelinde hakim olan kaos ortamı devletlerin kurulmasıyla birlikte sonlandırılamamıştır (Hobbes, 2017: 134-137). Openheimer ve Hobbes'un görüşleri doğrultusunda devletlerin ortaya çıkmasında etken faktör olan bireylerin çatışma eğilimi, aynı devlet sınırlarında çatışmasızlığı sağlamasına karşın, devletler arasındaki çatışmaları önlemekte etki sağlayamamıştır. Toplumların devlete evrilmesi öncesinde güçlü toplumlar-zayıf toplumlar var iken devletlerin ortaya çıkmasıyla birlikte güçlü devlet-zayıf devlet değerlendirmesi ortaya çıkmıştır. Bu durum devletler arasında savaş çıkmasını tetiklemiştir. Devletlerin ortaya çıkışı ile birlikte devlete bağlı toplumlar düzeyinde barış ortamı sağlanmış olmakla birlikte devletler arasında bu barış ortamını korumak amacıyla savaşlar gelişmiştir. Buna bağlı olarak devletler arasında güçlenme yarışı ortaya çıkmıştır. Bu durum dünya genelinde devletler düzeyinde bir anarşi ortamı oluşmasına neden olmuştur (Gözen, 2016).

2500 yıl önce yazılan "Savaş Sanatı" adlı eser o dönemde Çin'de yaşayan Sun Tzu tarafından kaleme alınmış olmakla birlikte bu eser günümüzde uluslararası ilişkiler açısından ilk çalışma olarak değerlendirilmektedir. Bu eserde yazar, askeri makamları savaşlarda etkili olmak amacıyla stratejilerden, savaş maliyetleri ve güç kapasitesi oranlamasından, gücün doğru kullanımından, güç algısı oluşturulmasından ve düşmanları analiz etmeye ilişkin hususlardan bahsetmektedir. Güç kavramına ilişkin olarak önemli eserlerden bir diğeri ise "Peloponnessos Savaşları" dır. Söz konusu eser ise M.Ö. 5. YY'da Atina'da general olarak görev yapan Thucydides tarafından yazılmıştır. Thucydides, bu eserdeki görüşleri dolayısıyla bazı yazarlar tarafından "realizmin babası" olarak nitelendirilmektedir. Söz konusu eserde şehir devletlerinin güç mücadelesi karşılaştırmalar yoluyla açıklanmakla birlikte kitabın adını veren Peleponez savaşları detaylı olarak incelenmektedir. Thucydides, kitabında yer alan görüşlerinde güçlülerin

güç kapasiteleri yettiği ölçü kapsamında yapmak istediklerini yapabileceğini ve güç kapasitesi daha zayıf olanın ise buna bir çözüm üretemeyeceğine vurgu yapmaktadır (Joshua vd., 2017).

Hindu bir devlet görevlisi olan ve aynı zamanda politika danışmanlığı yapan Kautilya, devletlerin mevcut güçlerini maksimize etme amacında olduğunu belirtmekle birlikte, uluslararası düzeydeki ilişkilerde ahlaki değerlerin gözetilmediğini ve dolayısıyla rasyonel koşullar ile ahlaki değerler arasında bir çatışma söz konusu olması durumunda rasyonel eylemin gerçekleştirilmesi gerektiğini önermektedir. Kautilya'nın dönemin Hindu kralına yapmış olduğu tavsiyeler içinde güç kavramı oldukça önemli bir yer bulmuştur. Kautilya, kralının gücünü arttırmaya yönelik politika önerilerinde bulunmuştur.

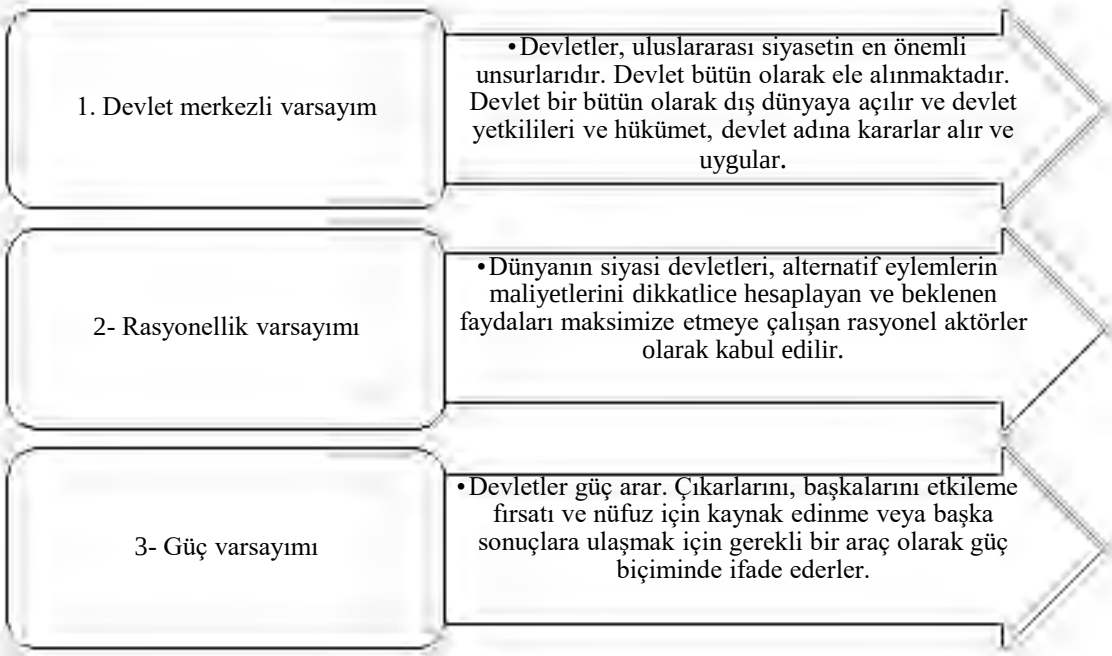
Güç kavramına ilişkin yapılan ilkel tanımlamalara ilk modern yorum ise Machiavelli tarafından getirilmiştir. Bu bağlamda Machiavelli, bireysel çıkarların ötesinde devlet çıkarlarının daha büyük önem arz ettiğini ifade etmiştir. Bununla birlikte gücün tanımlamasından daha çok gücün elde edilmesine yönelik görüşlerini ortaya koymuştur. Machiavelli gücün elde edilmesi bağlamında her türlü yöntemin kullanılabileceğini savunmaktadır. Dolayısıyla Makyavelist görüş gerektiği takdirde zor kullanılarak avantajların değerlendirilmesini ve kontrolün ele geçirilmesi olarak ifade edilebilmektedir.

#### 1.2.1.1. Uluslararası ilişkilerde güç kavramı:

##### 1.2.1.1.1. Realizme göre güç:

Realizme göre güç, insanları başkaları üzerinde güç ve hakimiyet arayan varlıklar olarak konumlandıran uluslararası bir politika görüşü olarak ifade edilmektedir. Realistler için çalışmalarının başlangıç noktası, insanların doğası gereği bencil oldukları düşüncesidir. Bu sebeple iş birliği yapacaklarına güvenilemez ve çıkarları çatıştığı takdirde iş birliği yapmayı bırakmaktadırlar.

Klasik realist yazarlardan Thucydides ve Hans Morgenthau'nun ortaya koydukları realizmin temel ilkeleri şu şekilde sıralanabilir:




**Şekil 1. 2.** Realizmin Temel İlkeleri *(Hornblower, 1992:170; Morgenthau, 1973:27)*

Realistler için rekabet halindeki ulus-devletler sistemi esasen anarşist bir sistem olarak kabul edilmektedir. Sistemi kontrol eden bir hükümet, kuralları belirleyen hiçbir üst otorite bulunmamaktadır. Devletler güç için rekabet eder ve nihayetinde kendi çıkarlarına ulaşmak için kendi kendine yardım ilkesine göre hareket etmektedir. Uluslararası hukukun uygulanması için daha yüksek bir organa başvurma imkanı bulunmamaktadır (Kinsella vd., 2012: 107).

Uluslararası kanunlar ve ulusötesi kurumların pekiştirilmesiyle realist görüşün güçsüz taraflarına değinilmiştir. Ulus devletler arasındaki ilişkiyi düzenleyen uluslararası yasalar, ilişkilerin çerçevesine bir öngörülebilirlik unsuru eklemiştir ve özellikle Amerika Birleşik Devletleri ile Rusya arasındaki Soğuk Savaş'ın sona ermesinden bu yana askeri boyutun önemi Avrupa'da büyük ölçüde zayıflatılmıştır.

Devletlerin uluslararası siyasette birçok hedefi bulunmaktadır. Birkaç devlet dünya hakimiyeti isteyebilir, diğeleri yerel hegemonya isteyebilir ve bazıları sadece barış isteyebilmektedir. Dünyayı kuşatmak isteyen bir devletin asgari hedefi bile kendi

devamlılığını garanti altına almak olmaktadır (Waltz, 2001: 203). Tüm bu isteklerin ortak noktası devletlerin varlığının korunmasıdır.

Morgenthau, uluslararası siyasetin de tümüyle bir güç mücadelesi olduğunu ifade etmiştir (Morgenthau, 1973: 27). Bu bağlamda uluslararası siyasetin nihai hedefleri arasında her zaman en önde gelen istağin de güç elde etme isteği olduğunu vurgulamıştır.

Bazı devletler diğerlerine karşı avantaj elde etmek istediğinde, ortak bir alanda toplanmaktadır. Diğerleri bu talebe direnmek istediğinde, bu duruma yanıt olarak katılmaktadır. Amaçlanan fayda, başka bir devleti yok edecek veya yaralayacak güç olarak ölçülürse, tehdit edilen devlet gücünü artırmaktan ancak istikrar pahasına kaçınabilmektedir. Burada temel kural oyunu kazanmak için her şeyin yapılmasıdır. Bazı devletler bu kurala göre hareket etmekteyken, diğer devletler stratejilerini değiştirmek zorunda kalmaktadır. Hobbes'un yaklaşımına göre güç, arzu edilen bir sonucu elde etme yeteneği olarak tanımlanabilmektedir (Waltz, 2001:203).

İktidarın kullanılması iç politikada genellikle bir devlet tekelinin konusu olmaktadır. Ancak uluslararası siyasette kuvvet kullanımını fiilen yasaklayabilecek bir ilke bulunmamaktadır. Güç dengesi, devletler arasında, devletlerin hedeflerine ulaşmak için kullanabilecekleri fiziksel güç de dahil olmak üzere tüm seçenekler arasında bir denge haline gelmektedir.

Güç, bir devletin komutasındaki finansal güç, diplomatik, askeri, teknik ve bilim, diğer yeteneklerin toplamı olarak anlaşılabilir veya bir devletin yetenekleri ile diğer devletlerin yetenekleri arasındaki oran olarak tahmin edilebilmektedir. Ancak her iki tanım da devletin kendi yeteneklerinin toplamı olarak ve diğerlerinin yetenekleriyle ilişkili olarak güç söz konusu olduğunda statik bir iktidar değerlendirmesini varsaymaktadır. Güç, devletin bir parçasıdır ve diğer devletlerle birlikte olsun veya olmasın, yeteneklerinin toplamı olarak bakılmaktadır. Alternatif olarak, gücün dinamik tanımı, devletler arasındaki etkileşime dikkat çekmektedir. Gücün belirlenmesindeki zorlukların yanı sıra gücün ölçülmesi de birçok tartışmaya ve fikir ayrılıklarına neden olmuştur. Bir devletin etkisi (etkileme veya kısıtlama yeteneği) yalnızca kapasitesi (veya diğer devletlere göre kapasitesi) tarafından değil, aynı zamanda; yeteneklerini kullanma isteği (ve istekliliğini diğer devletler tarafından nasıl algılandığı); ve diğer devletler üzerindeki etkisi ve kontrolü tarafından belirlenmektedir (Krippendorff, 1982:58). Bu

nedenle güç, karşılıklı şekilde devletlerin faaliyetlerindeki davranış kalıpları gözlemlenerek ölçülebilmektedir. Devletin dolaylı gücü, kendisini en açık biçimde faaliyetlerinin sonuçlarında göstermektedir.

Bazıları güce hesaplanmış bir bütün olarak bakmanın, becerilerin veya dolaylı becerilerin birleşiminin mantıklı olmayabileceğine inanmaktadır. Devletin gücü, neyle ilişkili olduğuna bağlı olarak ele alınmaktadır: örnek vermek gerekirse Japonya'nın gücüne bakıldığında askeri yönden zayıf olduğu ifade edilirken ekonomik konularda güçlü bir devlet olduğunu söylemek gerekmektedir.

Kenneth Waltz, devletin çeşitli kapasitelerinin desteklenmemesi durumunda, güçlü yönlerine odaklanmak ve zayıf yönlerinin görmezden gelinmesi gerektiğini ifade etmektedir (Waltz, 1979:129). Ancak bu anlayışa göre, yalnızca belirli sınıflandırmalar içindeki bazı devletlerin yanlışlıkla süper güç olarak kabul edilmesine yol açabilmektedir. Devletlerin güç hiyerarşisindeki konumu, nüfus, doğal kaynaklar, ekonomik fırsatlar, askeri güç, siyasi istikrar ve yüz ölçümü gibi tüm yönleriyle ele alınmalıdır. Dolayısıya, ülkelerin ekonomik, teknolojik, askeri ve diğer yetenekleri ayrı ayrı değerlendirilmemesi gerekmektedir.

Bir devletin gücünü veya kapasitesini hesaplama girişimi, bir devletin davranışını ve uluslararası sistemin savaş ve barış gibi gündemleriyle ilgili işleyişini açıklamada önemli bir bilgi vermektedir. Devletler tehdidi kendi güçlerini ve hasımlarının gücünü nasıl algıladıklarına göre değerlendirir ve buna göre denge, savunma, saldırı veya silahlanma gibi seçeneklerden bazı davranışlarla ilerlemektedir.

#### 1.2.1.1.2. Neorealizme göre güç:

Neorealist teoriye göre güç kavramı, devletler için güvenliklerini garanti altına almak, eylemlerini sistem içinde yürütmek, eylem alanı yaratmak veya egemenliklerini devam ettirmek adına önem arz etmektedir (Çıtak ve Şen, 2014: 36).

Devletler uluslararası yapıya ve sisteme önem verdiği kadar diğer devletlerin eylemlerini etkileme değiştirme konusuna da önem vermektedir (Waltz,1979:192). Fakat sistemde otokontrol sağlama adına güç mücadelesi vermek sadece devletlerin diğer devlet üzerinde kontrol mekanizması kurması anlamına gelmemektedir.

Hegemon olarak adlandırılan bir ülkenin sistemdeki en güçlü karakter olmasının sebebi, her şeyi ve herkesi kontrol etmesi değil, sistem üzerinde en çok hareket alanı bulunan ülke konumunda olmasıdır. Bir devletin diğer devlet ve devletler üzerindeki etkisine bakıldığında güçlü yapısı olduğunun bir sonucu olarak diğer devletin siyasi yapısını ve davranışlarında yön verme gibi yetenekleri olduğu sonuçları elde edilmektedir (Stephen, 1987: 22). Başka bir deyişle, devletin güç kapasitesi ne kadar büyük olursa, diğerlerini o kadar etkili bir şekilde koruyabilir, cezalandırabilir ve kısıtlayabilme gücünü de elde edebilmektedir

Güç eksikliği saldırganın cesaretini kırarken, aşırı güç kullanımı uluslararası sistemde bir güç mücadelesine yol açmaktadır. Güçlerini genişleten devletler, uluslararası sistemde de güvenlik sorunları yani güvenlik ikilemi (security dilemma) yaratmaktadır. Kenneth Waltz, uluslararası sistemdeki gücün kritik önemine değinmek için, dağılımını ve bu dağıtımın sisteme nasıl ayırt edici bir karakter kazandırdığını vurgulamaktadır (Aslanlı ve Memmedov, 2016:1523). Waltz, uluslararası gücün, güvenliğin bir amacı değil, bir aracı olarak ortaya çıktığını ifade etmektedir. Sistemde büyük güçlerin etkisi arttıkça gelişmekte olan ülkelerin bağımlılık derecesi de artmaktadır (Collins, 2022: 18). Güvenlik ikilemine gelince, devletlerin diğerlerinin niyetlerini anlama konusundaki belirsizliği, iş birliğini içine girmeyi güçlendirir ve bir güç arayışına yol açmaktadır.

Kontroller ve dengeler sistemi ile güç dengesi, bir devletin veya devletler grubunun güçlenmesini engelleyecek şekilde gücün dağılımından bahsetmektedir. Realizm kuramına göre, anarşist bir sistemde barış belli başlı koşullar altında kontrol edilmektedir. Uluslararası sistemde güç dengesi sağlandığında, çok dengesiz bir aktörün hegemonyası altında veya savaş sonrası muzaffer devletlerin etkisi altında arzu edilen dünya düzeni meydana gelebilmektedir (Sandıklı, vd., 2005:67). Uluslararası sistemde, güç dengesi, istikrarın korunmasında etkili bir oyunculuk sergilenmektedir. Tarih boyunca uluslararası ilişkilerde gücünü korumayı başaran devletlerin, hayatta kalma mücadelesini sürdürmüş ve sistem içindeki mevcut hakimiyetini artırmayı başardıkları görülmektedir. Sistemdeki diğer devletler, büyük güçler arasındaki güç dengesini korumak ve diğer devletin aşırı güçlenmesini önlemek için büyük güçlere karşı ittifaklar içine girmektedir. Örneğin Çin ile Rusya arasında çeşitli alanlarda iş birliği ve onlara karşı bir güç ittifakının oluşması, Amerikan etkisi de dikkate alınarak sistemdeki düzenin

devamlılığını garanti etmektedir. Çin ve Rusya arasında oluşan iş birliği anlayışına göre, ABD'nin uluslararası ağdaki hareket alanını sınırlandırmakta, ABD'nin gücünü sürekli her alanda artırmasını engellemekte ve aynı zamanda küçük devletlerin çıkarlarına da hizmet etmektedir.

Uluslararası sistemde devletlerin, güçlerini hayatta tutabilmek adına güç dengesini korumak için büyük çaba sarf ettikleri bilinmektedir. Devletler, güç hiyerarşisindeki konumlarını bildiklerinde daha temkinli davranmaya hazır bulunmaktadır. Uluslararası sistem içinde güvence altına alınan istikrar ve düzen sayesinde sistemde mevcut olan güç zayıflamasına giden devletler olduğunda veya sistemdeki zayıf bir devlet güç kazandığında güç dengesinde bozulmalar meydana gelmektedir (Roskin ve Berry, 2014:30). Sistem üstünde güç dengesi, revizyonist bir yaklaşım sergileyen bir devlete karşı güçlerini dengeleyen veya eylemlerinin kapsamını sınırlayan bir veya bir grup devletin ortaya çıkmasıyla sağlanmaktadır. Bölgesel bölünmeler ve böl ve yönet politikaları, askeri ittifaklar, güç dengesini korumanın ana yöntemlerinden bazıları ile sağlanmaktadır.

Kenneth Waltz'a göre, uluslararası düzeyde ikili koalisyonlarda istikrar sağlayan devlet, zayıf devletle birlikte olursa olası bir savaştan kaçınılabilmektedir. Uluslararası sistemde dengeli bir devlet güçlü olanın yanında yer alıp onu takip ettiğinde, güçlü ve zayıf devletler arasındaki mesafe artar, güç dengesi bozulur ve devletler savaşa teşvik edilmektedir. Devletler periyodik olarak sistemdeki güçlerini artırmakta ve bir güç mücadelesine girmektedir. Devletlerin birleşmesi ile meydana gelen güç dengesi, diğer devletler üzerinde olası bir hegemonyayı engellemekte ve ortaya çıkan gücün etkisini yok etmektedir.

Neorealizm kuramı çerçevesinde, güç kontrolü sağlamak adına güçlü bir yapıya sahip olan egemen bir devlet veya sistem içinde bulunan anarşist bir yapıda hegemonik devletin bulunması, sistem üzerinde hem düzen hem barışın sağlanmasına etkisi bulunmaktadır. Örneğin Soğuk Savaş'ta düzen ve istikrarın sebebi, oyuncuların iki süper güç arasında güç paylaşması ve iki devletin birbirini yok edecek ölçüde nükleer silaha sahip olmasının büyük etkisi bulunmaktadır. Neorealist teoriye göre, değişim sağlanması ancak savaş veya barış yoluyla gerçekleşmektedir. Barışçıl değişime giden yol, hegemonik gücün rıza ve şiddetin eşzamanlı kullanımından geçmektedir (Carr,

1946:218). Rızaya dayalı hegemonya, ortaya çıkma ihtimali bulunan yeni bir güç dengesini engellemektedir. Sistemdeki güç bileşenleri değiştiğinde, sistem içerisinde devletlerin uluslararası sistemdeki kutupların yapısı veya sayısı da değişmektedir (Waltz,1979:97).

Uluslararası yapıda devletler arasındaki güç dağılımı, değişikliği ifade etmektedir. Güç dağılımı uluslararası yapıdaki güvenlik kapsamına bakış açısının değerlendirilmesi açısından önem teşkil etmektedir. Sistemdeki baskın güçlerin sayısına bağlı olarak dünya tek kutup, iki kutup ya da çok kutuplu olarak ifade edilmektedir. Kenneth Waltz, güvenlik açısından iki kutuplu bir yapının çok kutuplu bir yapıdan çok daha güvenilir olduğunu belirtmektedir. İki kutuplu bir yapıda iki baskın gücün birbirlerinin davranışlarını daha kolay tahmin edebildiği ve çatışmaya girme olasılıklarının daha düşük olduğu vurgulanmaktadır. İki kutuplu bir yapıda, devletler başkalarının davranışlarını veya tepkilerini daha kolay şekilde öngörmektedir. Uluslararası sistemdeki iki rakibin yer aldığı bloğun birbirlerinin hareketlerini dengelediği veya kontrol ettiği zamanlar aslında daha az savaş dönemi olarak görülmektedir. Örneğin Soğuk Savaş sonrası iki kutuplu yapıda oluşturulan güç dengesi, yeni dönemde uluslararası sistemde barışçıl dönüşümlere geçişi kolaylaştırmıştır. İki büyük güç arasında uluslararası sistemde müzakere imkânı çok faktörlü sistemlere göre daha kolay ve ucuz maliyet sağlamaktadır. Uluslararası sistemde birden fazla sesin varlığı, tehdidin kaynağı ve aktörlerin gerçek niyetlerinin anlaşılması konusunda belirsizlik yaratmaktadır. Çok kutuplu bir yapının daha fazla kafa karışıklığı yaratması uluslararası sistemi de istikrarsız hale getirmektedir. Uluslararası siyasetin yapısına etki eden güçlü yapıların dengesinde yükseliş veya düşüşlerin yaşanması, devletler arasındaki denge kontrolünün raydan çıkmasına neden olmaktadır.

Devletler, uluslararası sistem üzerinde, mutlak üstünlük ilkesi yerine göreceli üstünlük ilkesini tercih etme eğiliminde olmaktadır (Waltz,1979:106) Uluslararası sistem içinde hükümetler arası ilişkilere dayanan bu anarşik düzende, devletler arasında bulunan güç dengesinde sarsılmalar ve sistemdeki kutupların sayısını değiştirme olasılığı her daim bulunmaktadır. Kenneth Waltz'un ifadesine göre; devletlerin temel kaygısı, güçlerini maksimize etmek değil, sistemdeki konumlarını sağlamlaştırmaktır. (Waltz,1979:126).

### 1.2.1.1.3. Realizme Göre Uluslararası Sistemin Yapısı:

İnsanların ilişkileri ile birlikte devletlerin de çalışmalarını düzenleyen belirli bir yapı ve sistemin olduğu anlaşılmaktadır. Uluslararası sistem ise, ana unsurları belirli sınırlarla ayrılmış, aralarında düzenli ve bağımlı ilişkilerin bulunduğu devletlerden oluşmaktadır. Morton A. Kaplan'a (Arı, 2010) göre bir sistem, "*kendi davranış kalıpları ile dış çevredeki farklı ve ilgili değişkenler kümesi*" olarak görülmekteyken, McClelland'a göre sistem "*bir bütün olarak dış çevreden farklıdır ve belirli sınırlar içinde etkileşim içinde yer almaktadır*". Arı (2004) ise uluslararası sistem olarak adlandırılan bu mekanizmanın ana unsurları birbirinden belirli sınırlarla ayrılmış, birbirleriyle kalıcı ve bağımlı ilişkiler sürdüren devletlerin oluşturduğu bir yapı şeklinde görülmektedir. Arı'nın uluslararası sistem tanımında, devletler arasındaki tutarlı ve bağımlı ilişkilerin olduğu anlaşılmıştır. Ancak Holsti (1983) uluslararası sistemi bağımsız bir siyasi birimler kümesi olarak yorumlamıştır. Holsti'ye göre, uluslararası sistemin tarihsel verileri, tutarlı ve sistematize edilmiş bir yapı içinde analiz edilmelidir. Bu çalışma ile birlikte aşiretlerden şehir devletlerine, imparatorluklardan ulus devlet yapılarına kadar uluslararası sistemin bir bütün olarak incelenmesi gerektirdiğini vurgulamıştır.

Uluslararası sistem teorisinin önemli kurucularından biri Morton A. Kaplan olarak görülmektedir. Kaplan (2005), uluslararası sistemi, tanımlanmış davranış kalıplarıyla dış çevreden ayrılan ve aralarında bir ilişkiler ağıyla donatılmış değişkenler olarak düşünmektedir. Kaplan, organizasyonel statülerine ve sayılarına göre altı uluslararası sistem modeli geliştirmesine rağmen, bunlardan ikisine odaklanmış ve geri kalanın bu iki sistemin yansımaları olduğunu ifade etmiştir. Kaplan'ın geliştirdiği altı uluslararası sistem modeli ise şunlardır:


**Şekil 1. 3.** *Altı uluslararası model (Kaplan, 2005).*

Kaplan, her sistemin durumunu incelemek ve açıklamak için kullanılan beş değişken kümesini ortaya çıkarmaktadır. Sistemi dengelemek için gereken davranışı ifade eden temel kurallar, sistemin değişmesine neden olan girdilerle ilgili değişim kuralları, faktörlerin yapısal özellikleri ile ilgili değişkenler, güç unsurlarına ilişkin yetenek değişkenleri faktörlerin sınıflandırılması, aktörler arası iletişim, teknolojik gelişme, ekonomik durum, aktörler arası iletişim, değişkenler hakkında bilgi düzeyi içerisinde yer almaktadır. Temel kurallar, sistem durumları içinde yer alan devletlerin karakteristik davranışını anlatmaktadır.

Waltz'un uluslararası sisteminin içeriği "*anarşist*" olarak bilinmektedir. Birimlerin konumlarının kendi aralarında hiyerarşik olduğu ulusal sistemlerden farklı olarak, uluslararası sistemde yapıyı oluşturan birimler arasında hiyerarşi olmadığı için devletlerin temel düşünceleri içerisinde "*hayatta kalmak*" yer almaktadır Her varlık sadece kendi bekası ile ilgilendiğinden, bu bir "*kendi kendine yardım*" sistemi halinde olup kendi kendine yardım uluslararası sistemin düzenleyici ilkesi halindedir.

#### 1.2.1.2. Güç dengesi sistemi:

Daha önce de belirtildiği üzere, güç kavramının pek çok farklı tanımlaması bulunmakla birlikte bu durum güç dengesi için de geçerli olmaktadır. Bu bağlamda güç dengesinin, güç kavramına benzer şekilde pek çok tanımlaması bulunmaktadır. Güç dengesi uluslararası ilişkiler için temel bir kavram niteliği taşımaktadır. Güç dengesine ilişkin olarak pek çok araştırma yapılmıştır. Tarihsel süreçte incelendiğinde güç dengesi kavramına ilişkin olarak farklı açıklama ve yorumlarda bulunulduğu bilinmektedir (Morgenthau, 2006). Güç dengesi realizm akımı açısından oldukça önemli bir kavram niteliği taşımaktadır. Bu bağlamda uluslararası sistemin temel aktörü niteliğinde olan devletler anarşik bir düzen içerisinde varlığını koruyabilmesi için güçlerini arttırmak durumundadır. Dolayısıyla uluslararası sistem içerisinde rekabet ortamı söz konusu olmaktadır (Sheehan, 2004). Söz konusu açıklamalar doğrultusunda güç dengesi, bir denge durumunu ifade etmekte iken gücün kullanım faydası, gücün dağılımını veya bir durumun açıklamasını yapmak amacıyla kullanılmaktadır. Bu tanımların yanı sıra güç üstünlüğünün devamı veya bir eylemin meşru kılmak amacıyla kullanılan bir kavram olarak da öne çıkmaktadır.

Güç dengesi kavramının tanımı kişiden kişiye farklılık göstermekle birlikte kişiler tarafından farklı anlamları açıklamak amacıyla da kullanıldığı bilinmektedir (Arı, 2006: 279-282) . Bu bağlamda Ernst Haas'ın güç dengesi kavramını birbirinden farklı anlamları açıklamak amacıyla kullandığı bilinmektedir. Bu bağlamda Haas, güç dengesi kavramını şu açıklamalar kapsamında kullanmıştır:

- Güç dağılımı
- Denge durumu
- Üstünlük
- İstikrar
- Barış
- İstikrarsızlık
- Savaş
- Güç politikası
- Evrensel tarih yasası
- Sistem
- Politika belirleyicisi

Güç kavramını birden çok durumu açıklamak amacıyla kullanan kişilerden bir diğeri ise Morgenthau'dur. Morgenthau ise güç dengesi kavramını şu açıklamalar için kullanmıştır:

- Devletlerin hedeflerine ulaşmak amacıyla uygulamış olduğu politika
- Devletlerin mevcut ilişkileri
- Uluslararası düzeyde gücün eşit dağılımı
- Gücün herhangi bir şekilde dağılım göstermesi

Yazarların tanımlamalarından da anlaşılacağı üzere güç dengesi kavramına ilişkin bir çok farklı tanımlama söz konusu olmaktadır. Bu araştırmada güç dengesi bir ya da birden çok devletin başka bir devlet ya da bir araya gelen birden çok devleti dengelemek

amacıyla kullanmış olduğu gücü tanımlamak amacıyla kullanılmaktadır. Bu bağlamda güç dengesi devletler ya da ittifak oluşturan devletler arasında gücün eşit kapasitede oranlaması olarak ifade edilebilmektedir. Güç dengesi temel olarak devletlerin fiziksel nüfuzunun yanı sıra mevcut tüm olanakları (örneğin: teknolojik gelişmişlik, doğal kaynaklar vb.) dengelemesini ifade etmektedir (Başaran, 2017). Denetimsiz bir uluslararası ortamda yer alan bir devletin gücünün kontrol edilebilmesi açısından, en önemli faktör bu ortamda yer alan diğer devletlerin güçleri olmaktadır. Bu doğrultuda söz konusu durumda bir devlet bir bölgeyi kontrol altına alma amacı doğrultusunda eylemler gerçekleştirmesi durumunda diğer devlet bunu gerçekleştiren devlet ya da ittifaklara karşı tek başına ya da ittifak halinde müdahale ederek engel olmaktadır. Bu durum tarihsel süreçte pek çok kez görülen bir olgu niteliğini taşımaktadır. Güç dengesi teorisi ise söz konusu sürecin düzenli bir süreçte geliştiğini ve bir devlet ya da ittifakın uluslararası sistemin istikrarının bozulmasını önlemek amacıyla müdahalede bulunduğunu öne sürmektedir (Pevehouse, 2017).

#### 1.2.1.2.1. Morton Kaplan ve klasik güç dengesi sistemi:

Güç dengesini bir sistem olarak öne süren Morton Kaplan, bu sistemi oluştururken 18. ve 19. Yüzyıl Avrupasını temel almıştır. Bu bağlamda Morton Kaplan tarafından önerilen güç dengesi sistemi, güçleri birbirine yakın en az beş devletin oluşturduğu bir uluslararası sistemde devletlerin ya da ittifakların birbirlerine karşı üstünlük kurmasını önleyen bir sistem olarak tanımlanmaktadır. Söz konusu sistemde yer alan her bir devlet mevcut koşullarını geliştirme ve diğer devletlere karşı üstünlük kurma amacı taşıması nedeniyle diğer devletler buna müdahale ederek kendilerine karşı üstünlük kurulmasını önlemektedir.

Morton Kaplan bir güç dengesinden söz edebilmek için belirli temel kurallar öne sürmüştür. Bu kurallar ise şunlardan oluşmaktadır:

1. Uluslararası sistemde yer alan her devlet mevcut imkânlarını geliştirme güdüsünde hareket etmektedir. Ancak bu amaç doğrultusunda savaşmak yerine diplomasiyi tercih etmektedir.
2. Sistemde yer alan her bir devlet mevcut imkânlarını geliştirme konusunda başarısız olmak yerine savaşa girmeyi tercih etmektedir.

3. Sistemde yer alan aktörlerden birinin ortadan kaldırılması söz konusu olması durumunda ise savaşa son verilmektedir.
4. Sistemde yer alan aktörlerden birinin veya birkaçının bir araya gelerek oluşturduğu ittifakın üstünlük kurma durumunda diğer aktörler bunu önlemek amacıyla harekete geçmektedirler.
5. Sistemde yer alan devletlerin uluslarüstü bir organizasyon oluşturma eğilimi söz konusu olması durumunda diğer devletler bu durumu sınırlandırmak amacıyla harekete geçmektedirler.
6. Sistemde yer alan devletlerden birinin yenilmesi ve/veya yıkılması durumunda söz konusu devletin sisteme tekrar bir aktör olarak katılabilmesi ya da sistemde daha önce temel aktör konumunda bulunmayan bir devletin sisteme dahil olabilmesi için çaba vermektedirler.

Morton Kaplan, güç dengesi sistemine göre sistemde yer alan temel aktör sayısının beşin altına düşmesi durumunda, istikrarsızlık probleminin ortaya çıkacağını ve sistemin yıkılabileceğini öne sürmektedir. Temel aktör sayısının azalması durumunda sistemde yer alan devletlerin, bazılarının çıkarlarına aykırı olsa bile bir ya da birkaç devletin temel aktör statüsüne getirilmesi için yardım etmesi gerektiğini belirtmektedir.

Morton Kaplan oluşturmuş olduğu güç dengesi sistemini 18. ve 19. Yüzyıl dönemlerini temel alarak oluşturması sebebiyle bu dönemlerde gerçekleşen olaylardan örneklendirme yapmaktadır. Kaplan'ın güç dengesi teorisine göre ittifakların dışında kalan devlet sayısının çok olması istikrar için belirleyici bir faktör niteliği taşımaktadır. Bu durum ittifakların gevşek bir yapıya sahip olması ve ittifakta devlet sayısının çok olması durumunda da geçerli olmaktadır. Bu önermeleri karşı ittifaka katılımı dengeleme ve dengeleyicinin işlevini gösterebilmesinin kolay olması ile ilişkilendirmektedir. Ancak aksi bir durum oluştuğu takdirde yani sistemde yer alan devlet sayısının az olması dengeleyici rolünde olan unsurun dengeyi bozmasına neden olabilecek ve sistem çökebilecektir (Kaplan, 1969).

Kaplan'a göre sistemin istikrarını tehlikeye atan durumlar şunlardan oluşmaktadır:

- Temel kurallara uygun davranmayan devletler

- Devletler arasında iletişim eksikliği
- Sistemde yer alan aktörlerin kapasite farklarının büyümesi
- Sistem içerisinde devletlerin rollerin tanımlanması hususunda anlaşmazlık oluşması
- Sistemin dengeleme mekanizmasının işlevini kaybetmesi

Tarihsel süreçte dünya geneli değerlendirildiğinde uluslararası sistemde dengeleme rolünde en başarılı olan devletlerden biri İngiltere'dir. Bu durum ise İngiltere'nin savaş bölgelerinden uzak olması, Avrupa kıtası içerisinde toprak elde etme amacı söz konusu olmaması ve donanma kuvvetinin yüksek olması ile açıklanmaktadır (Kaplan, 1969). Bu durumu İngiltere'nin dengenin dengeleyicisi olarak nitelendirilmesine sebep olmuştur.

Morton Kaplan'ın güç dengesi sistemi genel olarak değerlendirildiğinde sistemde oluşturulan ittifaklar kısa süreli olmakla birlikte özel amaçlar taşımaktadır. Ayrıca bu ittifaklar ideolojik bir nitelik taşımamaktadır. Bununla birlikte savaşlar ise sınırlı amaçlar doğrultusunda ortaya çıkmaktadır. Sistem içerisinde üstünlük kurmaya çalışan devlet veya ittifaklar, her bir devletin üstünlük kurma amacı taşıması nedeniyle amaçlarına ulaşamamaktadır. Söz konusu sistemlerde uluslararası hukuk uygulaması önemli bir araç olarak kullanılmaktadır. Temel kurallara uygun davranmayan devletlerin sayısının artması, devletlerin uluslarüstü bir organizasyon oluşturmak amacıyla bir araya gelmesi ve uluslararası ideolojilerin gelişmesi güç dengesi sisteminin istikrarsızlığına ve dolayısıyla çöküşüne neden olabilecek faktörler olarak öne çıkmaktadır.

#### 1.2.1.2.2. Hans J. Morgenthau ve güç dengesi sistemi:

Uluslararası politikada modern realizmin en önemli temsilcilerinden birisi Hans J. Morgenthau'dur. Uluslararası politikalara ilişkin olarak 2. Dünya Savaşı akabinde 1948 yılında "Uluslararası Politika" adlı eseri kaleme almıştır. Morgenthau'nun bu eseri modern realizmin temeli olarak da nitelendirilmektedir. Söz konusu eserde Machiavelli ve Thucydides gibi realizm akımının öncü düşünürlerin görüşlerini de temel almıştır (Antunes ve Camisao, 2017). Morgenthau bu eserde modern realizmin temelini oluşturan siyasal gerçekçiliği işlemektedir. Bu bağlamda 6 ilke öne sürmüştür. Söz konusu ilkeler şu maddeler kapsamında özetlenmektedir (Morgenthau, 2006):

- Modern realizmin temeli olarak nitelendirilen siyasal gerçekçilik Morgenthau'ya göre objektif yasalar doğrultusunda yönetilmektedir. Morgenthau siyasal gerçekçilik ile toplumun yönetimini benzeştirmektedir. Bu bağlamda toplumun geliştirilebilmesi için toplumsal yasaların anlaşılması gerektiğini savunmaktadır.
- Uluslararası politikalarda siyasal gerçekçiliğin istikrar sağlayabilmesi için yegane unsur güç olarak nitelendirilen çıkar olmaktadır. Söz konusu kavram uluslararası siyasetin anlaşılması hususunda işlev göstermektedir. Bu bağlamda Morgenthau, siyaseti diğer toplumsal kavramlar olan ekonomi, din ve ahlak gibi kavramlardan ayrı bir kavram olarak nitelendirmektedir.
- Morgenthau'nun modern realizmin temeli olarak gösterdiği siyasal gerçekçilik gücün evrensel olarak geçerli olduğunu öne sürmektedir. Fakat gücü tek bir anlam ile ilişkilendirmemekle birlikte kişiden kişiye de farklılık gösteren tanımlamalar için kullanmaktadır. Güç ve menfaat politika için belirleyici unsurlar olmakla birlikte zaman ve mekân koşullarından etkilenmemektedir.
- Siyasal gerçekçilik, siyasi ahlâkı önemsemektedir fakat siyasette başarı sağlayabilmek için ahlâki normlar ile siyasî başarı arasında çatışma olabileceğini de dikkate almaktadır. Bu sebeple realizm siyasî başarıya önem veren bir yapıya sahip olması nedeniyle siyasal gerçekçilik ile ahlâkı bağdaştırmamaktadır.
- Siyasal gerçekçiliğe göre bir toplumun ahlâki normları ile evrensel olarak geçerli olan ahlâki normların özdeşleştirilmemesi gerekmektedir. Bu durumun gerekçesi ile tüm toplumların evrensel ahlâki normların toplumların çıkarları doğrultusunda şekillendirme çabasına gireceği varsayımı ile açıklanmaktadır.
- Siyasal gerçekçiliğe göre siyaset diğer toplumsal unsurlardan bağımsız bir olgu niteliğindedir. Bu nedenle siyaset diğer toplumsal alanlardan bağımsız kabul edilmektedir. Bu durum ise toplumsal alanların işlevlerinin

farklılık göstermesi ile ilişkilendirilmektedir.

Devletlerin uluslararası düzeyde anarşik bir ortamda varlığını sürdürmeye çalıştığını öne süren reailizm, bu bağlamda uluslararası sistemde bir merkezi otoritenin söz konusu olmadığı ve her devletin bu sistemde var olmaya veya varlığını sürdürmeye çalıştığını varsaymaktadır. Dolayısıyla devletler anarşik bir uluslararası sistemde temel olarak şu amaçları taşımaktadır (Mearsheimer, 2006):

- Devletin çıkarlarına uygun hareket etmek
- Devletin güvenliğini sağlamak
- Devletin gücünü maksimize etmek

Yukarıda yer alan maddeler ile Morton Kaplan'ın güç dengesi teorisi benzerlik göstermektedir. Realizm akımında güç kavramı genel olarak askeri nüfuzu açıklamak amacıyla kullanılmaktadır. Morgenthau ise realist düşünürlerin genelinden farklı olarak güç kavramını pek çok farklı anlamı açıklamak amacıyla kullanmıştır. Bu bağlamda güç kavramını bir ilişki türü ile uluslararası politikaların temel amacı olarak nitelendirmektedir. Bununla birlikte uluslararası amaçların gerçekleştirilebilmesi için gerekli bir amaç olarak da tanımlamaktadır. Dolayısıyla Morgenthau güç kavramını çok boyutlu bir kavram olarak değerlendirmektedir (Aydoğan ve Aydın, 2011). Morgenthau bu sebeple güç kavramını maddi unsurlar ile ilişkilendirmiştir. Bu unsurlar şunlardan oluşmaktadır:

- Doğal kaynaklar
- Coğrafi koşullar
- Nüfus
- Teknolojik gelişmişlik
- Askeri güç

Morgenthau'ya göre bu unsurlar arasında istikrar için en belirleyici faktör olarak askeri güç öne çıkmaktadır. Realizme göre güç kavramı caydırıcı bir kuvvet olarak da değerlendirilmektedir. Realizme göre uluslararası sistemde anarşik bir ortamda varlığını sürdüren devletler, ulusal menfaatlerini koruyabilmek için rekabet halinde oldukları

devletlerin müdahalesini caydırıcılık ile önleyebilmektedir (Özdemir, 2008). Bu nedenle Morgenthau, uluslararası düzeyde askeri gücün istikrar sağlayabilmek için en önemli faktörlerin başında geldiğini savunmaktadır. Bu bağlamda askeri güç ile caydırıcılık arasındaki ilişkiye vurgu yapmaktadır.

#### 1.2.1.2.3. Kenneth Waltz ve güç dengesi sistemi:

Realizm akımı kapsamında sınıflandırılan önemli temsilcilerden biri olan Kenneth Waltz klasik realizm ile bağdaştırılmamakta ve dolayısıyla bu kapsamda sınıflandırılmamaktadır. Kenneth Waltz realizmi farklı bir bakış açısıyla değerlendirmekle birlikte neorealizmin kurucusudur (Brown, 2009). Klasik realizmin varsaydığı anarşik uluslararası sistemi Waltz ise farklı bir biçimde tanımlamaktadır. Waltz, diğer realist düşünürlerin de savunduğu uluslararası ortamın anarşik bir ortam olduğu görüşüne katılmakla birlikte realist düşünürlerden farklı olarak uluslararası sistemdeki anarşik ortamın devletlerin davranışları açısından belirleyici olduğunu öne sürmektedir. Bu bağlamda uluslararası yapının, devletlerin ideolojileri ve siyasal rejimleri farklılık göstermesine karşın uluslararası yapıya bağlı olarak devletlerin benzer davranışlar sergileyebileceğini öne sürmektedir (Efegil ve Erol, 2012). Neorealizmin kurucusu olarak nitelendirilen Waltz, klasik realist düşünürlerden farklı olarak güç kavramını istikrarı sağlamak yerine devletin gerek duyması halinde kullanabileceği bir araç olarak nitelendirmektedir. Bu doğrultuda güç kullanımının sadece gerek duyulması halinde söz konusu olabileceğini öne sürmektedir (Arı, 2004).

Neorealizm akımının kurucusu Waltz'a güç kavramını bir amaç olarak görmemekte ve araç olarak nitelendirmektedir. Bununla birlikte güç kavramını yetenek dağılımı ile açıklamaktadır. Bu bağlamda devletlerin yetenekleri birbirinden farklılık göstermekte ve dolayısıyla bir uluslararası sistemde devletlerin yetenekleri eşit dağılım göstermemektedir. Bu doğrultuda gücün tanımlaması bu dağılım açısından belirleyici faktör niteliği taşımaktadır. Yetenek dağılımı ise uluslararası sistemde devletlerin hareket kapasitesini belirlemektedir (Waltz, 1979).

#### 1.2.1.2.4. Hedley Bull ve güç dengesi sistemi:

Hedley Bull, İngiliz Okulu'nun temsilcilerinden biridir. İngiliz Okulu realizm, rasyonalizm ve devrimcilik akımlarından etkilenmiş bir yapıya sahip olmakla birlikte bu akımları sentezleyen bir yaklaşımdır. Uluslararası ilişkiler disiplininde İngiliz Okulu tarafından öne sürülen "uluslararası toplum" önemli bir kavram olarak nitelendirilmektedir. Uluslararası toplum önermesinin temelini ise şu düşünürlerin görüşlerinin etkisinde sentezlemişlerdir:

- Niccolo Machiavelli
- Thomas Hobbes
- Hugo Grotius
- Immanuel Kant

Politika biliminin kurucusu olarak kabul edilen Machiavelli ve Hobbes uluslararası ilişkileri, devletlerin birbirleri ile savaş halinde olduğu bir yapı olarak tanımlamaktadır. Hobbes doğayı kaotik olarak nitelendirmekte ve dolayısıyla toplumsal unsurların belirleyici bir faktör olmadığını öne sürmektedir. Hobbes kaosun ancak kontrat ile devletin kurulması ile sonlandırılabileceğini düşünmektedir. Fakat Sosyal Kontrat imzalanması anarşik ortamı önleyebilmek açısından yeterli olmamaktadır. Bu bağlamda uluslararası düzeyde devletler arasında güvensizlik olduğunu varsaymaktadır. Uluslararası ilişkilerin kurulması ve sürdürülebilmesi için oluşturulan kural, kurum ve hukukun kurgusal bir ürün olduğunu ve devletlerin buna rağmen çıkarları doğrultusunda hareket edeceğini öne sürmektedir. Bu nedenle uluslararası sistemi anarşik olarak nitelendirmektedir.

Hugo Grotius ise uluslararası topluluğun devletlerden meydana geldiğini öne sürmektedir. Devletlerin her birini bir bütün olarak değerlendirmektedir. Uluslararası topluluğu oluşturan unsurlar olan devletlerin sürekli etkileşim halinde olduğunu öne sürmektedir. Grotius'a göre devletlerin ortak menfaatleri ve değerleri bulumaktadır. Bu doğrultuda devletler arasında ilişkiler kurulmaktadır. Grotius'un önermesine göre devletler bu ortak çıkar ve değerlerin bilincindedirler. Grotius'a göre devletler bağımsız olsa dahi bu bağımsızlık ancak devlet içerisinde geçerli olmaktadır. Bu nedenle devletlerin uluslararası sistemde bir toplum üyesi olduğunu ve bu nedenle belirli

sorumluluklara ve haklara sahip olan bir siyasi unsur olarak değerlendirmektedir. Grotius buna ilişkin olarak uluslararası düzeyde oluşturulan hukuk esas alınarak uluslararası bir toplum oluşturulması gerektiğini savunmaktadır. Genel olarak değerlendirildiğinde uluslararası ilişkilerde anarşik bir yapı söz konusu olduğunu kabul etmesine karşın uluslararası düzeyde anarşinin sonlandırılması gerektiğini öne sürmektedir.

İngiliz Okulu'nun temsilcilerinden olan Hedley Bull, güç dengesi kavramını uluslararası toplum için başat bir kurum olarak nitelendirmektedir. Bull, güç dengesini açıklarken Emerich de Vattel'in güç dengesi tanımlamasını temel almaktadır. Uluslararası hukuk alanında çalışmalar yapan Vattel güç dengesini "hiçbir gücün ağır basar ve diğerleri için kanun koyar pozisyonda olmadığı bir ilişkiler durumu" şeklinde tanımlamaktadır. Bull, uluslararası toplumda herhangi bir devletin bir başka devletleri baskı altına almasını önlenmesi noktasında güç dengesinin belirleyici olduğunu öne sürmektedir. Bull'a göre güç dengesi devletlerin bağımsızlığının tanınmasını ve bir devletin uluslararası sistemin işleyişini sekteye uğratmasını engellemektedir. Bununla birlikte güç dengesi uluslararası toplum ve kurumların işleyişini sağlaması açısından önem arz etmektedir. Bu durumu ise şu şekilde açıklamaktadır (Bull, 2012):

"Uluslararası hukuk, diplomatik sistem, savaş ve uluslararası sistemin büyük güçler tarafından yönetimi, güç seviyesi olarak hiçbir mevcut gücün baskın olmadığı durumda işlevseldir. Tüm bu kurumların [işlerliği], büyük ölçüde, bir devletin kuralları çiğnediği zaman diğerlerinin misilleme yapabilmesine dayanmaktadır…baskın güç sahibi olan bir devlet, uluslararası hukuku, kuralları ve diplomatik münasebetleri tanımayabilir…"

Bull, güç dengesi kavramını açıklarken İngiliz yazar Lord Acton'un görüşlerinden faydalanmaktadır. Bu bağlamda Lord Acton'un şu sözlerine vurgu yapmaktadır: "güç yozlaşma eğilimindedir, mutlak güç ise mutlak olarak yozlaşır" (Acton, 1907). Bull, burdan yola çıkarak uluslararası düzenin işleyişini tehdit edebilecek potansiyele sahip bir gücün uluslararası antlaşmalar ile kontrol altına alınamayacağını düşünmektedir (Bull, 2012). Bu nedenle uluslararası sistemin sürdürülebilmesi için sistemi tehdit eden güce karşılık direnç gösterebilecek bir gücün bulunması ile sistemin dengelenebileceğini savunmaktadır.

Bull'a göre uluslararası toplumda güç dengesinin kendiliğinden oluşacağı görüşüne katılmamaktadır. Bu bağlamda uluslararası toplumda güç dengesini ancak devletlerin bilinçli ve gönüllü olarak oluşturabileceğini öne sürmektedir (Bull, 2012). Bull bu görüşünü uluslararası sistemin istikrarını koruyabilmek için iradi olarak oluşturulan güç dengesine dayandırmaktadır.

Bull güç dengesini uluslararası toplum düzeyinde kurumların işleyişinin sağlanması açısından belirleyici faktör olarak konumlandırmakla birlikte güç dengesinin amacının uluslararası toplumun tek bir gücün egemenliği altına girmesini önleyen bir mekanizma olarak tanımlamaktadır. Böylece yerel ve bölgesel düzeyde güç dengesinin işleyişi sağlanarak üstünlük kurmayı amaçlayan aktörler önlenerek uluslararası sistemde yer alan devletlerin bağımsızlıkları teminat altına alınmış olmaktadır. Bull'un güç dengesi tanımlaması değerlendirildiğinde güç dengesi temel olarak uluslararası toplumun varlığını sürdürmesini temin eden bir mekanizma niteliği taşımaktadır. Uluslararası toplumda bir başat gücün diğer devletlere üstünlük sağlamasını önlemek için savaş dışında bir çözüm kalmadığı takdirde güç dengesi mekanizması savaş için de işlev göstermektedir (Bull, 2012). Bull'a göre uluslararası sistemin işleyişini ve devletlerin bağımsızlığını teminat altına alan güç dengesi savaşlarda da işlev gösteren bir mekanizma niteliğindedir. Bu nedenle güç dengesi kavramını tanımlarken askeri gücü de açıkladığı ifade edilebilir.

Güç dengesi kavramı içerisinde yer alan "güç" kavramına ilişkin pek çok farklı tanımlama söz konusu olması nedeniyle karmaşık bir yapıya sahip olduğu ifade edilebilir. Bull bu unsuru uluslararası politikalarda söz konusu olan "satranç tahtası" olarak nitelendirmektedir. Uluslararası politikalarda güç ve etki kavramlarının çıkarımları bağdaştırılarak farklı satranç tahtalarında uygulanmaktadır. Yani Bull, gücü uluslararası politikalar için bir strateji faktörü olarak görmekte ve bunun uygulama alanına göre farklı işlevlere sahip olduğunu öne sürmektedir. Bull buna ilişkin olarak şu ifadelere yer vermektedir (Demirel, 2017):

"Açıkçası, uluslararası siyasetteki hamleler birden çok satranç tahtası üzerinde yapılır. Stratejiknükleer caydırıcılık satranç tahtasında, Amerika Birleşik Devletleri ve Sovyetler Birliği'nin öncü oyuncular olduğu, Çin'in çıraklık seviyesinde bulunduğu, Japonya'nın ise bu tabloda bulunmadığı görülür. Konvansiyonel askeri güç satranç

tahtasında ise, nükleer olmayan askeri güçlerini yakın çevresine konuşlandırma kapasitesine sahip olan Amerika Birleşik Devletleri ile Sovyetler Birliği yine başat oyuncular iken, Japonya ise bu alanda daha küçük bir oyuncudur. Uluslararası parasal işler ile uluslararası ticaret ve yatırım satranç tahtasında ise Amerika Birleşik Devletleri ile Japonya'nın başat oyuncular olduğu, Sovyetler Birliği'nin daha az önem arz ettiği ve Çin'in neredeyse önemsiz sayılabileceği söylenebilir. Eğer ideolojik cazibeden kaynaklanan etki satranç tahtası göz önüne alınırsa, Çin'in üstün bir oyuncu olduğu iddia edilebilir."

Bull'un güç dengesi sistemi temel olarak uluslararası toplumda bir devletin diğer devletlere üstünlük kurmasını önleyen bir mekanizma olmakla birlikte diğer devletlerin eylemlerini de sınırlandırmaktadır. Bu doğrultuda başat güç olarak bir imparatorluk kurulması önlenmektedir. Bununla birlikte Bull, güç dengesinin devletlerin iradesi dışında bu kurumun otomatik olarak oluştuğu görüşüne katılmamaktadır. Bull'a göre güç dengesi üstünlük kurma eylemlerini karşı eylemler ile dengelemektedir.

#### 1.2.1.3. Tarihsel açıdan güç dengesi:

Güç dengesi kavramına ilişkin tanımlamalar değerlendirildiğinde tanımlamaların olaylar ile ilişkilendirildiği gözlemlenmektedir. Morgenthau'nun tanımına uygun olarak nitelendirilebilecek klasik güç dengesi Avrupa devletler sistemini tanımlamaktadır. Bu bağlamda sistemde beş ve/veya daha fazla devletin yer aldığı çok kutuplu bir yer yapı söz konusu olmaktadır. Bu sistemde devletler güç kapasitesi olarak birbirine çok yakındır. Bu nedenle sistem istikrarlı bir yapıya sahiptir. Ancak bu durum güç dengesinin sağlanabilmesi için devletler arasında savaşlar çıkmasına neden olmaktadır.

1648 yılında imzalanan Vestfalya Barış Antlaşması, klasik güç dengesinin başlangıcı olarak kabul edilmektedir. 1618 ile 1648 yılları arasında Avrupa'da yer alan Habsburg ve Bourbonlar arasında Katolik ve Protestan çatışması temelinde 30 Yıl Savaşları olarak adlandırılan bir süreç meydana gelmiştir. Söz konusu savaş sonucunda Protestan devletler yenilgiye uğramıştır. Savaşın sonunda ise 1648 yılında Vestfalya Barış Antlaşması imzalanmıştır. Söz konusu antlaşma uluslararası ilişkiler disiplini için oldukça önem arz eden bir konuma sahiptir. Bunun nedeni ise antlaşmanın uluslararası sistem için oluşturulan kuralları içermesi olmaktadır. Bu bağlamda antlaşma uyarınca antlaşmanın tarafları devletlerin bağımsızlığını, toprak bütünlüğünü tanımaktadır.

Bununla birlikte taraflar birbirlerinin içişlerine müdahale etmemeyi taahhüt etmektedir. Antlaşma sonrasında 30 Yıl Savaşları sonucunda yenilgiye uğrayan devletler güç dengesinin sağlanması ile birlikte bazı toprakların kontrolünü kaybetmiş olmasına karşın bağımsızlıklarını, toprak bütünlüğünü ve iç işlerin yürütülmesini teminat altına almıştır (Pevehouse, 2017). Klasik güç dengesi sistemi 1648 ile 1945 yılları arasında geçerli olmuştur (Mearshimer, 2006). Söz konusu süreçte devletler çok kutuplu bir sistem içerisinde varlığını sürdürmüşlerdir.

Vestfalya Antlaşması'nın imzalanmasının akabinde devletler arasında din temelli olarak meydana gelen savaşlar sona ermiştir. Bu süreç sonrasında devletler ulusal menfaatleri doğrultusunda politikalar geliştirerek bu politikalara uygun şekilde hareket etmişlerdir. Bu bağlamda Fransa'nın çıkarları gözetilerek dönemin Fransa Kralı 14. Louis ile başlayarak 16. Louis'e kadar Fransa, uluslararası sistemde egemenlik kurma çabası vermiştir (Aydın ve Bakıncak, 2016). Ancak güç dengesi mekanizması Fransa'nın bu çabasını önlemek üzere işlev göstermiş ve bu bağlamda İngiltere önderliğinde Avrupa'da yapılan ittifak ile Fransa'nın başat olması engellenmiştir. Bunun sonucunda 1713 yılında Utrecht Antlaşması imzalanmıştır. Bu antlaşma Avrupa'da klasik güç dengesinin tekrar tesis edildiği bir antlaşma olarak önem taşımaktadır. Güç dengesinin değişimi ile birlikte İngiltere ise "dengenin dengeleyicisi" niteliğini kazanmıştır (Sönmezoğlu, 2011). Yeniden tesis edilen güç dengesi ise 1789'da gerçekleşen Fransız İhtilali ile tekrar sona ermiştir.

Fransız İhtilali sonrasında Fransa, Avrupa üzerinde hâkimiyet sağlamayı amaçlamıştır. Bu bağlamda ortaya çıkan Napolyon Savaşaları 1803 ile 1815 yılları arasında gerçekleştirmiştir. Savaş sonucunda Fransa "Kutsal İttifak" olarak adlandırılan ittifaka yenilmiştir.

Napolyon Savaşları sonrasında Avrupa'da güç dengesini yeniden sağlamak amacıyla Viyana Kongresi'nde taraf devletler tekrar bir araya gelmiştir (Sönmezoğlu, 2011). Viyana Kongresi ile birlikte güç dengesi yeniden tesis edilmiş olmakla birlikte uluslararası sistem açısından önemini vurgulamıştır.

1815 yılında gerçekleşen Viyana Kongresi itibariyle 1871 yılına kadar geçen süreç "Avrupa Uyumu" olarak adlandırılmaktadır. Söz konusu dönemde Avrupa'da devletlerin diğer devletler üzerinde hâkimiyet kurma çabası söz konusu olmamıştır. Bahsi geçen

süreçte devletler Fransız İhtilali'nin etkisiyle ortaya çıkan başta milliyetçilik akımı olmak üzere, liberalizm, demokrasi ve özgürlükçü düşüncelere karşı mücadele etmek durumunda kalmıştır (Aydın ve Bakıncak, 2016).

Avrupa Uyumu olarak adlandırılan süreç ise 1871 ile 1918 yılları arasında gerçekleşen olaylar sonucunda sona ermiştir. Askerî teknolojilerin gelişmesi ile birlikte Avrupa ülkeleri silahlanma yarışına girmiştir. Böylece askeri güç olarak başat bir konuma geçmeyi hedeflemişlerdir. Bununla birlikte 19. Yüzyılda ortaya çıkan düşünce akımlarından biri olan sosyalizm akımının güç kazanması, Avrupa Uyumu'nu tehdit eden bir diğer faktör olarak öne çıkmıştır (Sönmezoğlu, 2011). 1871 ile 1890 yılları arasında Alman İmparatorluğu'nun ilk şansölyesi olarak da bilinen Otto von Bismarck önderliğinde Alman İmparatorluğu oldukça önemli bir güç kazanmıştır. Daha sonrasında Bismarck, Rusya Çarlığı ve Avusturya-Macaristan İmparatorluğu ile antlaşmalar imzalamıştır. Söz konusu antlaşmalar sonucunda Üç İmparatorlar Birliği olarak adlandırılan bir ittifak kurulmuştur (Healy ve Stein, 1973). Bismarck böylece Alman İmparatorluğu'nun gücünü arttırmıştır. Alman İmparatorluğu'nda monarşinin kaldırılması ile birlikte Alman İmparatorluğu'nun son imparatoru niteliği taşıyan II. Wilhelm ise Bismarck'ın politikasına uygun hareket etmemiştir (Nye, 2003). Napolyon'a benzer şekilde uluslararası sistem üzerinde hâkimiyet kurmaya çalışmış ve buna bağlı gelişen olaylar sonucunda 1. Dünya Savaşı başlamıştır. Almanya'nın üstünlük kurma çabası "İttifak Devletleri" olarak adlandırılan ittifak grubu tarafından önlenmiştir. I. Dünya Savaşı'ndan sonra uluslararası platformdaki güç dengesi bu savaşın topyekün bir savaş olması sebebiyle sona ermiştir.

1918 yılında 1. Dünya Savaşı'nın sona ermesiyle birlikte Almanya savaştan mağlup ayrılmış ve ağır şartlar içeren antlaşmalar imzalamak durumunda kalmıştır. Söz konusu antlaşmaların bağlayıcılığı İttifak Devletleri tarafından muhafaza edilmeye çalışılmıştır. Fakat söz konusu süreçte 1929 yılında gerçekleşen ve dünya ekonomisini oldukça olumsuz etkileyen Büyük Buhran, özellikle Almanya ve İtalya'da etkisini arttıran faşizm akımıyla birlikte güç dengesi tekrar bozulmuş ve 2. Dünya Savaşı başlamıştır. Söz konusu süreçte neo-faşist bir ideolojiye sahip Adolf Hitler önderliğinde Almanya diğer Avrupa ülkeleri üzerinde hâkimiyet kurmayı amaçlamıştır. Fakat güç dengesi

mekanizması tekrar devreye girerek bunu önlemiştir (Aydın ve Bakıncak, 2016). Ancak 2. Dünya Savaşı tüm taraflar açısından oldukça ağır sonuçlar ile sona ermiştir.

2. Dünya Savaşı'ndan itibaren 1991 yılına kadar olan süreç "Soğuk Savaş" olarak adlandırılmaktadır. 2. Dünya Savaşı'nın sonucu olarak klasik güç dengesi sisteminde etkin olan çok kutuplu yapı iki kutuplu bir yapıya dönüşmüştür. Bu bağlamda 2. Dünya Savaşı sonrasında dünya genelinde en önemli iki güç olarak ABD ve SSCB öne çıkmıştır. ABD'yi destekleyen ülkeler "Batı Bloku" ve SSCB'yi destekleyen ülkeler ise "Doğu Bloku" olarak adlandırılmaktadır. Bununla birlikte 2. Dünya Savaşı sonrasında Almanya'nın toprakları ABD, İngiltere, Fransa ve SSCB'nin kontrolüne geçmiştir. Fransa ve İngiltere, ABD'yi desteklemesi nedeniyle Almanya Batı ve Doğu olarak ikiye ayrılmış ve Batı'da Federal Almanya, Doğu'da ise Doğu Almanya kurulmuştur (Pevehouse, 2017). Klasik güç dengesi sisteminden farklı olarak Soğuk Savaş döneminde ABD ve Rusya arasında meydana gelen yarış nükleer caydırıcılık ekseninde sürmüştür. Bu sürecin Soğuk Savaş olarak adlandırılmasının sebebi ise SSCB ve ABD'nin nükleer bir savaşa girme çekincesi dolayısıyla sıcak bir çatışma içerisine girmemesi olmuştur.

SSCB'nin 1991 yılında yıkılması ile birlikte Soğuk Savaş sona ermiş ve savaşı ABD kazanmıştır. Bu bağlamda ABD'nin tek başına süper güç olması güç dengesi sisteminin yeniden tesis edilmesini gerekli kılmıştır. Böylece ABD önderliğinde dünya düzeni değiştirilmeye başlamıştır. 11 Eylül 2001 tarihinde gerçekleşen "11 Eylül Saldırıları" olarak da adlandırılan olay ile birlikte ABD uluslararası politikalarında değişikliğe gitmiştir. Bununla birlikte askeri güç kazanmaya oldukça önem vermiştir. Fakat bu durum uluslararası düzeyde ABD'ye olan desteğin azalmasına neden olmuştur. Bununla birlikte SSCB'nin yıkılmasının ardından yeni adı ile Rusya, Çin, Hindistan ve Pakistan uluslararası düzeyde nüfuz kazanmaya başlamış ve güç dengesi sistemi tekrar değişerek çok kutuplu bir yapı haline gelmiştir (Aydın ve Bakıncak, 2016).

### 1.3. Siber Güvenlik:

#### 1.3.1. Siber uzay:

Yaşamın tüm alanlarında olduğu gibi teknolojinin uluslararası ilişkilerdeki tesiri zaman geçtikçe artmaktadır. Globalleşmenin geldiği evre ile beraber internet teknolojisinin gelişmesi, siber alanın oluşmasında son derece önemli bir kilometre taşını

oluşturmaktadır. İnternet teknolojisinin ortaya çıkışıyla birlikte bilgi sistemlerinin kullanımının artması, insanların hayatında ciddi değişimlere yol açmıştır. Söz konusu değişimler çerçevesinde, ticaretle ilgili de pek çok engel ortadan kalkmıştır. Bunlara ek olarak; sınıf, coğrafi konum ve devrin getirmiş olduğu klasik engeller ne olursa olsun dünyadaki her yerden insanlar birbirleriyle iletişime geçme, iş birliğinde bulunma ve düşünce alışverişi yapma imkanına sahip olmuştur. Bu da, beşinci operasyonel saha şeklinde belirtilen siber uzayda global rekabetin artması sonucunu doğurmuştur. Bu çerçevede uluslararası politikada hükümetler, özel firmalar, uluslararası örgütler ve bireyler siber uzay teknolojilerini giderek daha çok benimser hale geliniştir. Girilen söz konusu rekabetin arkasında, üretkenlik sahibi olmak ve kâr sağlama amaçları bulunmaktadır. Örneğin; siber alan araştırmaları, geliştirmeleri ve inovasyonlarıyla ilgili olarak pek çok avantaj vardır; bir taraftan ekonomik büyüme ve refaha giden bir yol ortaya çıkmaktadır, diğer taraftansa süratle ilerleyen bir şekilde bilgi toplumları inşa edilmektedir (Mbanaso ve Dandaura, 2015: 17).

Endüstri 4.0, uzay madenciliği, dijitalleşme, 3D yazıcılar, yapay zekâ gibi pek çok yeniliğin ortaya çıkması ve giderek süratli bir şekilde gelişen teknoloji dünyayı farklı bir boyutta biçimlendirmeye devam etmektedir. Beraberindeyse bu yeni dünyaya karmaşıklığı ve belirsizliği getirmektedir. Siber uzaydaki popülasyon arttığı müddetçe, rekabet de artmaktadır. Yani siber uzay, oyuncularla paydaşlar için cazip bir saha durumuna gelmiştir. Bu noktadan yola çıkarak, siber uzayla beraber birçok işlevin fiziki dünyadan sanal dünyaya geçmeyi temin eden bir portalla açıldığını ve teknolojideki ilerlemelerle söz konusu portalın giderek büyüdüğünü iddia etmek mümkün hale gelmiştir.

Siber uzayın kilidini açabilmek için öncelikle, internet teknolojisinin geçmişi hususundaki süreçten bahsedilecek ve sonra bu sahanın anahtar sözcüğü olan internet teknolojisinin gelişiminden söz edilecektir. İnternet teknolojisinin tanımlanmasıyla ilgili araştırmalar, genel olarak bu kavramı bir donanımla yazılım grubu şeklinde teknik olarak tanımlama eğilimindeyken; Janet Abbate de,internete dair tek bir doğru tanımın olmadığını kabul etmekte ama yine de uzmanları kullanmış oldukları tanımlar hususunda dikkatli olmaya ve terimin çıkış noktasının Amerika merkezli olarak çerçevelendirilmesi hususunda ayrıntılı bir incelemeye davet etmektedir (Abbate, 2017: 1). Bir ağ şeklinde

belirtilen ve tarihi İkinci Dünya Savaşı'ndan sonraki senelere dek uzanmış olan internet teknolojisinin dönüşümünü; askeri bir deneyden başlayıp sivil bir hizmet kurumu olmasını içeren süreçle, ağın ticarileştirilmesine evirilmiş olan süreç biçiminde iki adımda incelemek mümkündür (Naughton, 2016: 7). İnternet teknolojisinin ikinci aşaması ise Naughton'a göre (2016: 12) 1995'ten bugüne dek geçen süreçtir.

1967-1995 yıllarındaki süreci ifade eden ilk evreye geçmeden önce, arka planda söz konusu sürecin oluşmasına giden altyapıdan bahsetmek gerekmektedir. İnternet teknolojisinin Soğuk Savaş çerçevesinde ortaya çıktığı realitesinden hareketle, ilk aşamanın Amerika ve Sovyetler Birliği arasındaki nükleer sahada gerçekleşen ilişkileri yönetmekte olan "karşılıklı kesin yıkım doktrini" stratejisiyle yakından ilgili olduğunu dile getirmek mümkündür. Söz konusu strateji, tarafların birisinin nükleer bir saldırı başlatması halinde, ötekinin misillemeyle karşılık vereceğini garanti altına alıp, milli güvenliği temin etmeyi amaçlayan bir muhtevaya sahip olsa da mantıki olarak kusurlu bir strateji olduğu ortadadır. Zira saldırıları başlatmış olan tarafın önlemeye dönük saldırısı (preemptive strike) misillemede bulunacak tarafın komuta ve kontrol sistemini etkisizleştirecek denli yıkıcı ise karşı taraftan herhangi bir saldırının gelmesi mümkün değildir.

Bunun için Soğuk Savaş evresinde tarafların gereksinimi olan şey, yıkıcı bir nükleer saldırının sonunda, zarar görmeyecek bir iletişim sisteminin tasarlanmasıdır. RAND Corporation'dan Paul Baran, yüksek düzeylerde çoklu bağlantıya dayanan bir örgüsel ağla çoklu iletişim aletleri arasındaki bağlantıyı temin etmenin yanında veri iletimi hususunda da daha başarılı olan "paket anahtarlama" ismi verilen bir dijital iletişim teknolojisinin tasarımını yapmıştır. Ancak Baran, analog sistemli iletişim ağlarının baskın olduğu ve anahtarlama şekli olarak devre anahtarlamanın tercih edildiği bir devirde radikal düşüncelere sahip olarak değerlendirilmiş ve bürokrasi engeline takılan düşünceleri uygulamaya dökülememiştir.

Diğer taraftan, söz konusu dönemde "İngiltere Ulusal Fizik Laboratuvarı"nda görevli Donald Davies de paket değiştirme hususunda çalışmalar yapmıştır. Davies, sivil uygulamalarla ilgili yeni bir iletişim ağı üstünde çalışmıştır. Araştırmadaki bulgular çerçevesinde, analog telefonların bu ağ için yeterli olmadığı hususunda farkındalık ve bu sistemden ayrı bir paket tasarlama düşüncesi oluşmuştur (Naughton, 2016: 7). Söz konusu

düşüncenin ardındaki amaçsa, büyük mesafelere duyarlı, interaktif zaman paylaşımlı bir bilgi işleme sistemine sahip olmaktır.

1957 yılındaysa Rusya'nın Sputnik uydusunu başarılı olarak fırlatması ve ardından 1958'de Amerika Savunma Bakanlığında "Gelişmiş Araştırma Projeleri Ajansı (ARPA)"nın oluşturulması bu konuda son derece önemli gelişmelerdir. Söz konusu ajans, daha sonra Pentagon'daki bir birim haline gelmiştir. ARPA, ajans ile araştırma sözleşmeleri bulunan kimi üniversitelerin bilgisayarlarına finansman sağlamıştır. Fakat söz konusu bilgisayarlar birbiri ile uyumsuz olduğunda araştırmacılara kaynakların paylaşımı hususunda sıkıntı yaşatmıştır. Bu noktada, söz konusu kaynakların paylaşılmasını temin edecek bir ağ düşüncesi üretilmiştir: ARPANET (Gelişmiş Araştırma Projeleri Ajansı Ağı). ARPANET ile tümü bir ana bilgisayara bağlanan özdeş küçük bilgisayarlardan müteşekkil bir alt ağın oluşturulması düşüncesi gündeme gelmiştir (Naughton, 2016: 8). Bu düşüncenin uygulamaya dökülmesi teknik olarak çok zor görülse de süratli bir şekilde kurulması sağlanmıştır. 1972 yılına gelindiği zaman; daha önce düşünsel temelleri atılmış olan ağ, 15 özgün sitenin tamamının birbirine bağlı ve çalışır duruma ulaşması ile tamamlanmıştır. Kullanıcılar ağın dizaynına etkin olarak katıldıklarından hem tasarımcı hem de kullanıcı halini almışlardır. Öte taraftan, ağın bir kaynak paylaşım birimi olması hedeflense de kişiler sistemi daha ziyade dosyaları paylaşmak, elektronik posta yollamak ve almak vb. iletişimleri kurmak için kullanmıştır. Aslında buradaki önemli nokta, kullanıcıların ağ oluşturmanın anlamı hususunda yeni bir anlayış geliştirmesidir. Kullanıcılarca oluşturulan bu anlayış çerçevesinde, ARPANET bir bilgi işlem sistemi olarak değil, bir iletişim sistemi olarak görülmüştür (Abbate, 1999: 108-111).

"Siber uzay" kavramını ise 1980'li senelerde, yazar William Gibson yazdığı "Neuromancer" isimli eserde, bilgisayar ekranının arka kısmındaki sanal dünyayı tanımlamak üzere kullanmıştır (Gibson, 1984). Bu aşamada iki temel gelişme vardır: Siber uzayla fiziki dünya arasındaki ayrım aşındırılmış ve birleşmiştir. Söz konusu gelişmelerden ilki, "ABD Ulusal Bilim Vakfı"nın, ağın ticarileştirilmesine yönelik karar alarak ağı İnternet Servis Sağlayıcılarına devretmiş olmasıdır. Söz konusu karar, sıradan insanların ağa erişebilmesi anlamına gelmektedir. Gelişmelerden ikincisiyse, CERN'de görevli fizikçi ve bilgisayar bilimcisi Tim Berners-Lee'nin 1989'da "World Wide Web"i

yaratmasıyla ortaya çıkmıştır. Düşüncenin altındaki husus, dünyanın her tarafındaki internet sunucularında depolanmış olan dokümanları yayımlamanın, yerini belirlemenin ve bunlara erişmenin bir yolunu bulmaktır. İsviçre'de bulunan Avrupa Fizik Laboratuvarı CERN'de araştırmalarını sürdürürken, dokümanların kontrolünü sağlamanın yararlı olacağına inanılmıştır. Berners-Lee ise söz konusu kontrolü yapmak üzere bir metot geliştirmiştir: bir metnin ilgili bölümleriyle ve o bölümler ile ilgili grafikler arasında, çapraz referansla kapsamlı bir biçimde belgeler yaratan yerleşik bir teknoloji olan hypertext'i alarak internetten çalışmasını sağlamak (Naughton, 2016: 13).

Hypertext teknolojisini internet teknolojisine adapte eden Bernes-Lee; 1990 senesinin sonlarında, 3 ay içerisinde "World Wide Web" ismini verdiği bir prototip yaratmıştır. Eskiden çok ciddi heyecan uyandırmayan bu proje, 1991'in Mart ayında CERN'den gereken izinlerin alınmasının ardından Berners-Lee info.cern.ch adresinde sunucuyu topluma açmıştır. Fakat bütün bu gelişmelere karşın, 1991-1992 yıllarında Web'in yayılma sürati düşük seyretmiştir. 1993 yılının bahar aylarına gelindiğindeyse, Illinois Üniversitesi'nde görevli Marc Andreessen ile Eric Bina Web için yazdıkları grafikleri satır içinde görüntüleyebilen ilk tarayıcı olan Mosaic'i üretmiştir. Mosaic'in üretilmesi, Web'in ve internet teknolojisinin dönüşümünde oldukça önemli olmuştur (Naughton, 2016: 14). Bunun yanı sıra Web'i kullanmak üzere internet gerektiği için, toplum arasında evine ya da iş yerine internet bağlatmak isteyenlerin sayında artış yaşanmıştır; bu da Web'in ticari potansiyelinin varlığını gözler önüne sermiştir.

### 1.3.2. Siber saldırı:

Önemli altyapılara saldırı yapma, bunları çalışamaz duruma getirme, yemleme yapma, kötücül yazılımlar ile zararlar verme, toplumsal mühendislik, iletişimi dinleme, verileri çalma ve değiştirme vb. yöntemlerle devlete ait ya da ticari kurumların web sayfalarını bozmak, sistemde bulunan gizli bilgileri çalmak, silmek, ifşa etmek ya da değiştirmek için hedef şahıs, firma ya da örgütün iletişim altyapısına ya da bilgi sistemine siber uzayda gerçekleştirilen genel olarak planlı ve koordineli saldırılar "siber saldırı" olarak tanımlanmaktadır (Çakmak ve Demir, 2009: 29-30).

"2016-2019 Ulusal Siber Güvenlik Stratejisi"ne (2016: 7) göre siber saldırı, milli siber uzaydaki bilgi ve iletişim teknolojilerinin gizliliğini, bütünlüğünü ya da erişilebilirliğini yok etmek üzere, siber uzayın belli bir yerindeki şahıs ya da sistemlerce

kasti olarak gerçekleştirilen işlemlere denilmektedir.

Siber saldırılar, kişisel bilgisayar korsanları, organize suç örgütleri, casusluk çalışmaları gerçekleştiren şahıslar, teröristler, dış istihbarat örgütleri ya da düşman devlet tarafından planlı ve koordinasyon içinde yapılabilmekte ya da sistem içindeki bilinçsiz kullanıcılarca farkında olmaksızın da gerçekleştirilebilmektedir.

Günümüzde bilgi, süratli bir biçimde yayılmaktadır, siber uzayı teşkil eden unsurların kullanımıysa hızlı bir biçimde yaygınlaşmaktadır. Bunların sonucunda bilgi, bilgi ve iletişim teknolojileri, önemli altyapı sektörlerine karşı gerçekleştirilen saldırılar da artmaktadır. Diğer taraftan son dönemlerde, saldırganların gereksinim duyduğu teknik bilgiler gün geçtikçe azalır iken siber saldırı yöntemlerinin karmaşıklığı ve saldırıların sebep olduğu zararlar da artmaktadır. Aşağıda yer alan şekilde de söz konusu ilişki verilmiştir.

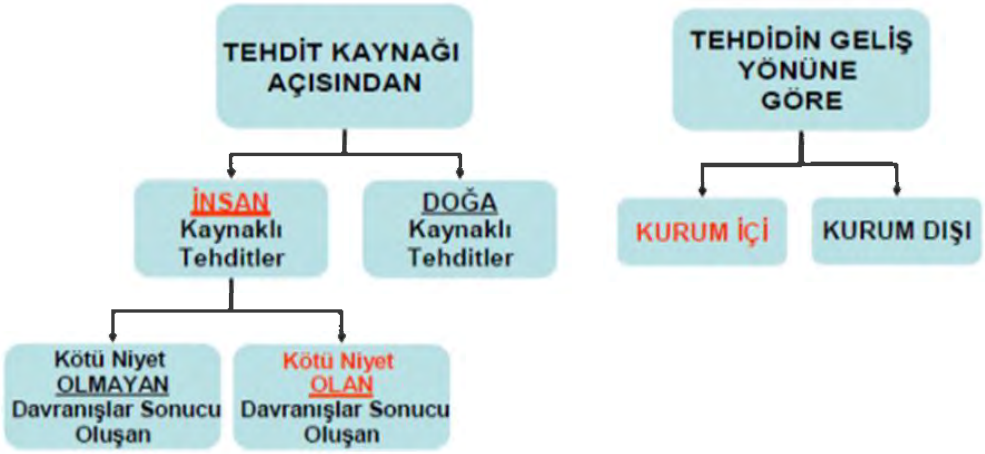

**Şekil 1. 4.** *Siber saldırıların gelişim süreci (Sağıroğlu, 2013).*

Şekildeki grafikten de anlaşılacağı üzere, günümüzde siber saldırı gerçekleştirmek için ihtiyaç duyulan teknik bilgi düzeyi ve saldırıların verdiği hasar ters orantılıdır. Bu da siber saldırıların cazip hale gelmesinde etkili bir rol oynamaktadır.

### 1.3.3. Siber tehdit:

Siber uzayla ilgili tüm "yıkıcı, bozucu, engelleyici ve ele geçirici" niteliklere sahip girişimlerle siber saldırıların farklı araçlar ve yöntemlerle siber uzayda kullanılmasına "siber tehdit" adı verilmektedir. Siber tehditler, bunların dışında geleneksel suçların siber uzaya adapte edilmiş durumlarını ve bilgi-iletişim teknolojilerinden yararlanılarak türetilen, tamamıyla yeni suç tanımlarını da içermektedir (Bilgi Teknolojileri ve İletişim Kurumu (BTK), 2009: 8).

Siber tehditler, kaynağıyla geliş yönüne dayalı olarak ikiye ayrılır. Kurum içerisinden küskün ve art niyetli kişilerden kaynaklı tehditlerin kurum dışı düşman güçlerden kaynaklı tehditlere nazaran daha başarılı ve tehlikeli olduğu da bilinmektedir. Siber tehditler, siber saldırılarda söz konusu olduğu gibi kişisel bilgisayar korsanları, casusluk çalışmaları yapanlar, organize suç örgütleri, terörist kurumlar, dış istihbarat teşkilatları, düşman ülkelerce planlı ve koordinasyon içerisinde yapılabileceği gibi bilinçsiz kullanıcılarca farkında olmaksızın da yapılabilmektedir. Siber tehditlerde tercih edilen yöntemlerle amaçlar, siber saldırıların yöntemleriyle ve hedeflerle benzerlik göstermektedir. Şekil 1.5.'te siber tehditlerin kaynaklarına göre sınıflandırılması şematik olarak gösterilmiştir.




**Şekil 1. 5.** *Siber tehdit kaynakları (Kılıç, 2012).*

Siber tehditlerin ana hedeflerini, sisteme yetki olmadan erişim, bilgilerde değişiklik yapılması ya da bilgilerin yok edilmesi, çalınması, ortaya çıkarılması, sistemin bozulması ve hizmetlerin sekteye uğratılması şeklinde sıralamak mümkündür (Atalay, 2012: 42).

### 1.3.4. Siber suç:

Bilişim çağında teknolojideki çok süratli ilerlemeden dolayı sınırlarını açık bir biçimde çizemediğimiz siber suçu, öteki suç türlerinden ayıran ana faktör; bilgisayar, bilgisayar sistemleri ve bilgisayar ağlarının suçların işlenmesi noktasında kullanılıyor olmasıdır. Müşterek bir fikir olarak bilgisayarların suçlarda bir vasıta olarak kullanılmasıyla bilgisayarsız da söz konusu suçların işlenebilmesi realitesi siber suçlarla klasik suçların farklılığının özünü teşkil etmektedir (Çakmak ve Demir, 2009: 34).

Sistemin sahibinin rızası olmadan sisteme girilmesi, sistemdeki verilere yetkisiz şekilde erişilmesi, verilerde değişiklik yapılması, silinmesi, sistemin kullanılmasının önlenmesi, iletişimin izin alınmadan takip edilmesi, kaydedilmesi vb. hukuk kurallarına aykırı fiiller siber suçlar arasında yer almaktadır. Netice olarak siber suç, sayısal verilerin ya da bilgi akışının kasti olarak yanlış amaçlar çerçevesinde kullanılmasıdır ve ağ sistemleri içinde ya da ağ sistemlerine karşı işlenebilmektedir (Corell, 2000: 8)

### 1.3.5. Siber terörizm:

Terörizm, en temel tanımıyla zaman ve yer kısıtlaması olmayan, hedefinin genel olarak siyasi ve ilk amacının korku oluşturmak olan, içerisinde genel olarak şiddet barındıran, insanlığın ayrılmaz bir parçasıdır ve ne yazık ki yaşamımızın bir realitesidir. Siber terörizmse, terörizmin tanımından hareketle, organize suç örgütleri, gizli ajanlar, terörist gruplar ya da kişileirn kasti ve politik bir amaç çerçevesinde, belli bir toplumda belirsizlik ve karmaşa oluşturup gündelik hayatın gidişatını bozmak için, hükümetler ve toplumları belli bir siyaset ya da ideolojiye adapte olmaya mecbur edip, milyonların davranışlarını etkileyip, sivil, kamusal ya da askeri hedeflere karşı şiddete, yıkıma ya da hizmetlerin sekteye uğramasına neden olan bilgisayar, bilgisayar ağları ya da iletişim altyapısını kullanmak suretiyle işlenen suçlardır (Colarik, 2006: 45-47).

Genel olarak kabul edilen açık bir tanımının bulunmamasına karşın siber terörizmi; sınırlı insan kaynağıyla maliyeti en düşük saldırıyı gerçekleştirilen, birçok

amacı aynı anda etkileyebilen ve iletişim imkanlarının gelişmişliğine koşut olarak, önemli organizasyonlara ihtiyaç hissettirmeyen, yüksek mobiliteyle süratli reaksiyon kabiliyeti bulunan, asimetrik olmasından dolayı kaynağında yok edilmesi çok güç; bağlantılarının ispatlanmaması ve gizliliği bakımından bir devletle ilişkilendirilmesi hemen hemen olanaksız, milli ve uluslararası hukuktaki boşluklardan yararlanan çağdaş savaş yöntemi şeklinde de tanımlamak mümkündür (Çitlioğlu, 2008: 14-15). Weimann'a (2004: 4) göre siber uzayla terörizmin kesişmiş olduğu noktada siber terörizm ortaya çıkmıştır.

Siber terörizmle ilgili eylemler, bilgisayarları, sanal ağları, bilgi, iletişim ve depolama sistemlerini hedeflerine alan kanun dışı eylemlerdir ve söz konusu eylemleri yapanların temel amacı siyasi, sosyal, dinsel ve düşünsel hedeflerini kabul etmeye zorlamak ve bu amaçla beraber korkuyla panik havası yaratmaktır (Güneştaş vd., 2015: 88-89). Bundan dolayı, siber terörizm, yalnızca bireylerin canla mal güvenliğini tehdit etmemekte, aynı zamanda da hedef kitle üzerinde toplumsal, politik, dinsel, düşünsel ve bilhassa psikolojik tesir oluşturmak için bilgisayar, bilgisayar ağlarıyla iletişim altyapısına karşı gerçekleştirilen terör eylemleri olarak tanımlanmaktadır (Çifçi, 2013: 6).

Bu noktada dikkat edilmesi gereken husus, siber saldırı ve siber terörizm ile klasik terörizm arasındaki ince çizgiyi fark etmektir. Geleneksel terörizmin oluşturduğu korku ve kaygı bilgisayarla internet vasıtasıyla oluşturuluyorsa ve hedef kişi, grup ya da devlet iktisadi ya da maddi olarak zarara uğratılıyorsa "siber saldırı", "siber terörizm" şeklinde adlandırılabilmektir (Altunok ve Kaya, 2009: 153,154).

### 1.3.6. Siber caydırıcılık:

Caydırıcılığı bir devletin ya da topluluğun diğer bir devlet ya da toplulukça kendi aleyhine yapılabilecek askeri güç kullanımına kadar uzanan hareketlerden sakınması için gereken önlemleri alması olarak tanımlamak mümkündür (İduğ ve diğerleri, 2013: 287).

Caydırıcılığı uygulama konusundaysa temel olarak iki öge bulunmaktadır. Birincisi, muhtemel saldırılarla tehditlere karşı kuvvetli bir savunma mekanizması kurmak, ikincisiyse belli bir durumda belli bir kaynaktan gelen bir saldırıya misillemede bulunma kapasitesi ve kabiliyetine sahip olmaktır (Haley, 2013).

Devletlerle toplumların şiddet oranlarına dayalı olarak başvurduğu caydırıcılık metotlarına Şekil 1.6.'da yer verilmiştir.


**Şekil 1. 6.** *Şiddet oranlarına göre caydırıcılık yöntemleri (Libicki, 2009: 29).*

Prof. Dr. Martin C. Libicki'ye (2009: 29-30) göre tek başına kullanıldığı zaman siber güçlerin şiddeti, diplomatik ve iktisadi yaptırımlardan daha fazlayken, klasik ve nükleer güçlerin şiddetinden daha azdır. Kısacası, siber caydırıcılık tek başına etkili olmasına rağmen, diplomatik ve iktisadi yaptırımlar, klasik ve nükleer kabiliyetlerle beraber ortak olarak kullanıldığı zaman daha etkili olmaktadır.

Soğuk Savaş devrinde klasik silahlar caydırıcılığının yerini nükleer caydırıcılığa terk etmiştir. Bu dönemin uzun soluklu olması ve caydırıcılık siyasetlerinin sıkça kullanılması caydırıcılık ve nükleer caydırıcılık terimlerinin birbirinin yerine kullanılmasına sebep olmuştur. Bunların yanı sıra muhtemel bir nükleer saldırının sonucunca dünyadaki hayatın ortadan kalkacağı fikri, nükleer caydırıcılığın çok daha etkili görülmesine yol açmıştır. Fakat siber silahların, nükleer silahlarda olduğu gibi geniş coğrafyalara yayılan tesiri olmadığı için, siber caydırıcılığın önemi konusunda günümüzde de düşünce birliği yoktur.

Nükleer silahlara sahip olmak, diğer devletler ya da topluluklar üstünde caydırıcılık tesiri oluşturmaktadır. Siber silahlara sahip olmaksa düşman ülke ya da toplulukların söz konusu teknolojileri elde etmesi ya da silahlara karşı savunma yeteneklerini geliştirip siber saldırıları boşa çıkartmaları durumda etkisiz hale gelmektedir. Bunun yanı sıra nükleer caydırıcılık daha ziyade misilleme odaklıyken; siber saldırıların nereden geldiği net olarak belirlenemediği için siber caydırıcılık savunma

merkezlidir. Bundan dolayı siber caydırıcılıkta, kuvvetli savunmadan kaynaklı potansiyel saldırganların hedeflerine ulaşmaksızın, başarısız olacakları hususunda ikna edilip harekete geçmesinin engellenmesi amaçlanmaktadır (Lupovici, 2011: 51).

Siber savunma yetenekleri üst düzeyde olduğu sürece, siber saldırı kaynakları gerçekleştirecekleri siber saldırılarının boşa çıkacağını düşünerek bu yola başvurmayacaktır ve siber savunma tek başına caydırıcılık temin edecektir (İduğ ve diğerleri, 2013: 288). Fakat siber saldırıların maliyetleri siber savunmayla siber güvenlik maliyetlerinden daha düşük olduğu için kimi ülkeler, kritik altyapılarının savunmasını daha güvenli duruma getirmektense, siber saldırganları misillemeyle ya da cezalandırmayla ortadan kaldırmaya çalışmaktadır.

### 1.3.7. Siber istihbarat ve siber casusluk:

İstihbarat ve casusluk, insanlığın tarihte hasım devlet, ülke ya da topluluklar üstünde avantaj ve üstünlük sağlamak için yürütülen çalışmalardır. Bu iki terimin önemi değişmemiş olsa da uygulama metodu teknolojik gelişmelerle doğru orantılı olarak farklılaşmıştır (Çifçi, 2013: 289).

Siber saldırıyla ve siber tehdit tanımlarıyla yakın münasebetli olan siber istihbarat, dijital bağlamda sistemin siber saldırılarla tehdit değerlendirmelerini gerçekleştirmek ve karşı siber saldırılar yapıp sisteme ilişkin istihbaratlar sağlamaktır (Keleştemur, 2015: 90). Siber saldırılarda bulunup ülkenin bekası için ehemmiyeti olan bilgilerin sağlanması konusu siber istihbaratın en önemli niteliğidir.

Teknoloji henüz bu kadar gelişmemişken casusluk ve istihbarat yoluyla düşmanlara karşı avantaj ve üstünlük oluşturacak bilgileri sağlamak daha zor, daha maliyetli ve tehlikeliyken, teknolojideki gelişmeyle beraber içerisinde bulunduğumuz bilişim çağında siber casusluk ve siber istihbarat çalışmaları, daha kolay, daha ucuz, daha az tehlikeli hale gelmiştir (Clarke ve Knake, 2010: 120-127). Üstelik bu yolla elde edilen bilgi de düşünülemeyecek kadar büyüktür.

Siber casusluk, hasım üstünde iktisadi, siyasi ya da askeri üstünlük temin etmek üzere, iletişim ağları ya da bilişim sistemlerine kanun dışı yollarla sızıp, rızaları olmaksızın şahsın, grubun veya devletin bekasına yönelik olarak çok önemli bilgilerin sağlanma çalışmalarıdır (Çifçi, 2013: 291). Siber istihbaratla siber casusluk sonucunca

ulaşılan önemli bilgiler ileride karşılaşılabilecek konvansiyonel ya da siber savaştan önce düşmana karşı bilgi üstünlüğü ve avantajlar verecektir (Singer ve Friedman, 2015: 130,131). Bundan dolayı, siber istihbarat ve siber casusluk, devletlerin bekaları için geleneksel ya da siber savaş öncesinde ve esnasında kullanılması şart olan çok önemli kozlar olarak karşımıza çıkmaktadır (Keleştemur, 2015: 162). Bu sebeplerle farklı bilgisayar korsanlığı metotları kullanılmak suretiyle hedef şahıs, firma, kuruluş ya da ülkeden bilgi sızdırmak için bilhassa istihbarat örgütlerinin sık sık başvurduğu metotlardan birisi de siber casusluktur.

### 1.3.8. Siber savaş ve bilgi savaşı:

Uluslararası sahada siber savaşın benimsenen bir tanımı olmamakla beraber en fazla kabul gören model Richard A. Clarke ile Robert K. Knake'e aittir. Buna göre siber savaş, bir ülkenin, diğer bir ülkenin bilgisayar ya da iletişim ağlarına zarar vermek veya kesinti oluşturmak üzere yaptığı sızma çalışmalarıdır (Clarke ve Knake, 2010: 8). Carr'a (2011: 2) göreyse siber savaş, kavga etmeden savaşmayla düşmanı kanını dökmeden yenme sanatı ve bilimidir.

Siber savaş, Türkiye'de ise sivil, askeri ve hükümete ait bilgilerle iletişim teknolojilerinin düşmanın siber saldırılarına karşı savunulmasıyla iktisadi, siyasi ya da askeri nedenler ile hedefteki devlete, bilgi ve iletişim teknolojileri aracılığıyla düzenli saldırı çalışmalarının gerçekleştirilmesi şeklinde de tanımlanmıştır (Yazıcı, 2011).

Bilgi savaşının ise bilgisayarlar, bilgisayar ağları ya da sistemlerini de içine alan siber savaştan daha geniş bir tanımı vardır (Denning, 1999: 9-12). Bilgi savaşları tüm bilgilerle ilgilenir iken, siber savaşın ilgi alanı siber uzaydır (Çakmak ve Demir, 2009: 45). Bundan dolayı, bilgi savaşıyla siber savaş terimlerini birbiriyle karıştırmamak gerekmektedir.

### 1.3.9. Siber güvenlik ve siber savunma:

#### *1.3.9.1. Siber güvenlik kavramının ortaya çıkışı:*

Bilginin yaşamımızdaki yerinin vazgeçilmez ve yaşamsal olduğu tartışılmaz bir gerçektir. İçerisinde olduğumuz bilişim çağında, teknolojinin çok süratli bir ivmeyle gelişim göstermesi, yaşamımıza sunduğu kolaylık ve yeniliklerinin tesirlerini çok zor gözlemleyebilmemize sebep olmuştur. Teknolojik gelişmelere bağımlılık arttığında da

teknolojinin neden olacağı zaafiyetleri, açıklıklar ve dezavantajları da bir o kadar artmaktadır (Cavelty, 2008: 12,13). Bilgi ve iletişim teknolojilerindeki süratli gelişimle söz konusu sistemlerce sunulmuş olan hizmetlerin tüm sahalarda yaygınlaşmasının neticesinde, bilgi ve iletişim teknolojilerinin politik, toplumsal, iktisadi ve askerî sahadaki işlevi de artmıştır. Tüm bu gelişmeler çerçevesinde pek çok insan, kurum ve kuruluş, bilgi ve iletişim teknolojilerini en üst düzeyde kullanmış, bütün faaliyetlerin ayrılmaz bir parçası olmuştur. Bunun neticesinde de bilgi ve iletişim teknolojileri devletlerin önemli altyapı alanları için hayati bir hale gelmiştir.

Son dönemlerde, organize suç ve terör örgütleri, girişimlerini planlama, eğitim, bilgi paylaşma ve propaganda çalışmalarını siber uzaya kaydırmakta, bilgi ve iletişim teknolojisini amaçlarına ulaşmak üzere kullanmaktadır. Meydana gelen saldırılar ve tehditlerden dolayı da siber güvenlik ve siber savunmaya yönelik çalışmalar, bireyler, kurumlar, kuruluşlar ve devletler nezdinde son derece önemli bir noktaya gelmiştir.

Siber saldırılar ve tehditlerin hedeflerinde, zarar görmesi ya da ortadan kalkması durumunda, yurttaşların mal ve can güvenliğine, sağlık, ekonomik refah ya da kamusal hizmetlerin sunulmasında negatif tesir oluşturacak, yaşamsal önemi bulunan tesis, şebeke, hizmet ve varlıklar bulunmaktadır. Bunlar devletten devlete değişmekle beraber, genel olarak "savunma, finans, enerji, ulaşım, elektronik haberleşme, sağlık, eğitim, nükleer tesisler ve temel kamu hizmetlerine" dönük altyapılardır ve bütün bu ögeler kritik altyapılar olarak tanımlanmaktadır (Cavelty, 2008: 91-121).

"2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" ve "2016-2019 Ulusal Siber Güvenlik Stratejisi" kritik altyapıları "işlediği 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" şeklinde tanımlamaktadır. 20 Haziran 2013 tarihli Siber Güvenlik Kurulu Kararına göre ise kritik altyapılarla ilgili sektörler, "Ulaştırma, Enerji, Bankacılık ve Finans, Elektronik Haberleşme, Kritik Kamu Hizmetleri ve Su Yönetimi" şeklinde belirlenmiştir. Kritik altyapıların tespiti ve iş birliği için görevlendirilen "T.C. Başbakanlık Afet ve Acil Durum Yönetim Başkanlığı (AFAD)" tarafından da çerçevesi ilerleyen süreçte genişletilmiştir. Bu çerçevede ülkemizde önemli kritik altyapı sektörleri

şunlardır (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2013:4890; 2016-2019 Ulusal Siber Güvenlik Stratejisi, 2016: s.8; T.C. Başbakanlık AFAD, 2014: s.34);

i. "Ulaştırma
ii. Su Yönetimi
iii. Tarım ve Gıda
iv. Elektronik Haberleşme
v. Kritik Kamu Hizmetleri
vi. Kültür ve Turizm
vii. Bankacılık ve Finans
viii. Kritik Üretim Ticari Servisleri
ix. Enerji
x. Sağlık"

Avrupa Birliğine göre ise kritik altyapı sektörleri şöyledir (Alcaraz ve Sherali, 2015: 53);

i. "Enerji
ii. Sağlık
iii. Ulaşım
iv. Bilgi ve İletişim Teknolojileri
v. Finans
vi. Kimyasal ve Nükleer Endüstri
vii. Su
viii. Nakliye
ix. Uzay ve Araştırmalar
x. Gıda ve Tarım
xi. Kamu-Hukuk Düzeni ve Emniyeti"

Amerika İç Güvenlik Bakanlığına (DHS) göre kritik altyapılar şöyledir (Alcaraz ve Sherali, 2015: 54);

i. "Enerji
ii. Nakliye
iii. Ticari Tesisler
iv. Bilgi ve İletişim Teknolojileri
v. Kamu-Hukuk Düzeni ve Emniyeti
vi. Kritik Üretim
vii. Su
viii. Ulaşım
ix. Savunma Sanayi
x. Gıda ve Tarım
xi. Kimyasal ve Nükleer Endüstri
xii. Barajlar
xiii. Sağlık
xiv. Uzay ve Araştırmalar
xv. Acil Servisler
xvi. Bankacılık ve Finans
xvii. Milli Heykel ve Semboller
xviii. Sivil Yönetim"

Görüleceği üzere, kritik altyapıların belirlenmesinde ülkeler ya da uluslararası teşkilatlar nezdinde küçük farklılıklar bulunmasına rağmen, değişim yaşamayan tek nitelikleri hemen hemen hepsinin siber uzay ile irtibatı bulunan ve bilişim sistemlerince denetlenen yapılar olmasıdır.

Kritik altyapıların karmaşıklığının çözümlenebilmesine yönelik olarak, söz konusu sektörlerin operatörlerce uzaktan gözlemlenmesi, kontrol ve kumanda edilmesi gerekmektedir. Günümüzde ağ sistemleri, operatörler ya da yetkililere kritik altyapıları uzaktan kontrol etme, takip etme ve yönetme imkanı vermektedir. Bugünün teknolojisinde söz konusu sistemler "Merkezi Denetleme Kontrol ve Veri Toplama

Sistemi (SCADA - Supervisory Control and Data Acquisition)" ile "Dağıtık Kontrol Sistemi (Distributed Control System - DCS)" şeklinde ikiye ayrılmaktadır. Söz konusu sistemlerle genellikle, elektrik üretim ve dağıtımı sistemleri, barajlar ve sulama sistemleri, fabrikalar, doğal gaz sistemleri, petrol rafinerisi vb. endüstriyel, altyapı ya da tesis tabanlı süreçleri takip ve kontrol eden "Endüstriyel Kontrol Sistemleri (Industrial Control Systems - ICS)" belirtilmektedir (Karabacak, 2011). SCADA sistemleriyle DCS arasındaki ana farklılık, SCADA sistemlerinin DCS'ye göre daha geniş coğrafi sahaya yayılmasıdır (Peterson, 2013: 120).

Endüstriyel Kontrol Sistemleri (Insdustrial Control Systems - ICS), sadece bir merkezden bilgisayar, akıllı telefon ya da tablet vb. cihazlar yardımıyla kritik altyapı sektörlerinin takip edilmesini temin etmektedir. Yalnızca bir cihazla kullanılacağı gibi ağ bağlantılarıyla birden çok bilgisayarla ve taşınabilen cihaz ile kontrol ve takip edilebilmektedir. Bu özellik, sitemin kontrol edilmesini, denetlenmesi ve yönetilmesini kolaylaştırsa da önemli düzeyde güvenlik sorunlarını da beraberinde getirmektedir (Karakuş, 2013: 6). Bağlı bulunduğu ağda yer alan ICS'lere gerçekleştirilebilecek saldırılar, yazılım, donanım ya da insanlardan kaynaklanan hatalar, ağdaki bütün sistemi de etkileyebilmektedir. Buna karşın kritik altyapı sektörleri ve ICS'lerin karşılaştığı söz konusu tehditlerle, sadece dikkatli tasarlanan ve iyi bir şekilde uygulanan korunma ve savunma stratejileriyle mücadele edilebilmektedir (Alcaraz ve Sherali, 2015: 54, 55).

Son zamanlarda dünyadaki kurumlar, kuruluşlar, uluslararası örgütler ve devletler kendi kritik altyapı sektörleri ve ICS'leri söz konusu tehditler karşısında koruyabilmek üzere, siber güvenlik ve savunma hususundaki çalışmalarına sürat vermiştir. Siber güvenlik ve savunmanın temin edilmesi için ulusal ölçekte yönetsel, teknik ve hukuksal kapasitenin artırılması, ulusal yazılımlar ve donanımların üretilmesi, kritik altyapı sektörlerinde imkan dahilinde ulusal kaynaklı güvenlik ürünlerinin tercih edilmesi önemli hale gelmiştir. Dolayısıyla siber uzaya yönelik saldırıların etkisini minimuma indirgeyebilmek üzere, kritik altyapı sektörlerinin belirlenmesi, güvenliklerinin temin edilmesi, alınan teknolojik ve hukuksal önlemlerin geliştirilmesi gibi konular gündeme gelmektedir.

#### *1.3.9.2. Uluslararası ilişkilerde siber güvenliğin yeri ve önemi:*

Fiziksel dünyada, sanal dünya aracılığıyla gerçekleştirilebilecek yeni siber saldırı

taşıyıcılarından kaynaklı artışa geçen bir duyarlılıkla karşılaşılmaktadır. Nitekim günümüzde savaşlar, yalnızca askerlerle ve askeri teknolojilerle gerçekleştirilmemektedir. Kamusal hizmetler, ulaşım, iletişim ve enerji gibi önemli alanları aksatan ya da ortadan kaldıran özenli bir biçimde silahlandırılan bilgisayar programlarını, fiziki olarak uzak mesafeden aktif hale getiren bir müdahaleyle gerçekleştirmek mümkün hale gelmiştir. Bu tür saldırılara ek olarak askeri ögelerin hareketleri, savaş uçaklarının rotaları ve gemilerinin komuta denetimi gibi ulusal güvenlik açısından hayati öneme sahip sistemleri de etkisiz hale getirmek siber alanda gerçekleştirilebilecek faaliyetler arasında yer almaktadır.

Söz konusu alanlarda etkisizleştirebilme veya süreci aksatabilen ögelerin ortaya çıkması, kendilerine mücadele sahası arayan aktörlerin de zaman içinde iştahlarını artırmıştır. Böylelikle siber teknolojilere dair bilgi ve bu alanı etkin bir şekilde kullanabilmek için gerekli olan bilgilere sahip olma arzusu, "siber güvenlik" terimini uluslararası siyaset sahasında daha belirgin hale getirmiştir. Siber saldırılarla terörizmin verdiği avantaj uluslararası güvenlikle ilgili sorunları ve faaliyetleri de artırmıştır. Dolayısıyla "siber güvenlik" terimi, siyasi bir düzlemde ilerler iken uluslararası bir boyut kazanmasıyla ilgili sorun, uluslararası güvenlik çalışmalarında da artan bir öneme sahip olmuştur. Söz konusu sorunun gelişimindeki, tarihsel arka planı ise teknolojiyle sibernetiğe dair gelişmelerin özellikle Soğuk Savaş dönemi ile beraber bir devinim elde etmesiyle başlamıştır.

Soğuk Savaş dönemindeki çekişmeler uluslararası ilişkilerin tüm alanlarında kendisini hissettirirken gelecekle alakalı sibernetiğe dair düşünsel tartışmalar da söz konusu mücadelenin içerisinde yerini bulmuştur. Soğuk Savaş'ın sonra ermesiyle bilhassa hegemonik bir güç olarak Amerika'nın siber uzayla ilgili faaliyetleri baş döndürücü bir biçimde gelişmiş ve günümüzdeki siber politikalarla alakalı faaliyetlerin özünü teşkil etmiştir.

Uluslararası ilişkiler başta, hakim ve eşit konumdaki devletler arasında gerçekleşmekte ve devletlerin yalnızca sahip oldukları sınırlarda yaptırım kuvvetleri vardı. Günümüzdeyse sınırların belli olmadığı ve belli bir fiziki kısıtlamanın bulunmadığı siber uzay içinde, egemenlik ve yaptırım erkinin kimde bulunacağı konusu tartışmalı bir hal almıştır. Devletler, fiziki sınırları içindeki güvenliklerini temin etmelerinin yanı sıra,

sınırların belli olmadığı siber uzayda da gerçekleştirilen siber saldırılara karşı savunma sistemlerini kurmaları gerekmektedir.

İçerisinde yer aldığımız bilişim çağında, kullanılan teknolojinin çok süratli bir biçimde gelişmesi, devletlerin fiziki olarak sınırlarının belirsizleşmesi, siber saldırı ve tehditler ve bunların oluşturduğu problemler, ülkelerin güvenlikle ilgili endişelerine yenilerini eklemiştir ve geleneksel güvenlik anlayışını değiştirmiştir (Güntay, 2015: 477). Bunların yanı sıra siber saldırılar ve tehditlerin, bunlarla karşılaşan coğrafyalar haricindeki coğrafyaları da etkileyebilmesi, siber uzay sınırlarının tespit edilmesini daha da güçleştirmektedir (Gürkaynak ve İren, 2011: 275-276).

Devletlerin siber saldırı ve tehditlere karşı bakış açıları da farklılık göstermektedir. Kimi devletler siber uzayı daha az ya da hiç kullanmaz iken, kimileriyse kendi çıkarları doğrultusunda sıkça kullanmaktadır. Pek tabii siber çalışmaları fazlaca kullanan devletler, teknolojik alanda daha gelişmiştir. Söz konusu çalışmalardan çıkar sağlamaları sebebiyle de global düzeyde bir siber güvenlik anlayışının oluşmasına genel olarak sıcak bakmamaktadırlar. Siber saldırıların, son derece az bir bilgiye sahip kötü niyetli kişiler ve örgütler tarafından kullanılabilmesi ve bu durumdan büyük devletlerin daha çok zarar görmesi, siber uzaydaki gelişmelerin geleneksel uluslararası ilişkilerle ilgili faaliyetlerin içine alınmasını gerektirmiştir. Çünkü siber uzaydaki gelişmeler, bu ilişkilerde yeni aktörlerin ortaya çıkmasını sağlamış ve güvenlikle ilgili yeni riskleri gün yüzüne çıkarmasına sebep olmuştur (Gürkaynak ve İren, 2011: 265). Bilhassa devletler için hayati öneme sahip, siber saldırı ve tehditlerin hedefinde bulunan kritik altyapılar, takip edilecek diplomaside ve siyasette ciddi bir yere sahip olmuştur. Siber uzayın aktörleri, artık uluslararası gündemi meşgul ederek, doğrudan etkileyebilecek "siber saldırı, siber tehdit, siber terörizm, siber caydırıcılık ve siber savaş vb." mekanizmaları ellerinde tutmaktadır.

Globalleşmenin son senelerde insanlığın geçmişinde eşi benzeri bulunmayan bir biçimde sürat kazanmasıyla beraber uydu, akıllı telefonlar, bilgisayarlar, internet ağı, bilgi ve iletişim teknolojileri de hayal dahi edilemeyecek derecede gelişmiştir. Devletleri birbirlerine yaklaştırmış ve adeta dünyayı elektronik otoyollar ile birbirlerine bağlamıştır (Henderson, 2010: 20,21). Bu sebeple uluslararası sahada yapılan ticaret faaliyetlerinde, iktisadi, politik, kültürel münasebetlerde, uluslararası suçlar, tabiat hadiseleri, sağlık

problemleri, siber saldırılar ve siber suçlar da dâhil daha pek çok alanda uluslararası iş birliği kaçınılmaz bir hale gelmiştir. Böylelikle söz konusu sahalarda uluslararası toplumun bir arada hareket etmekten başka çaresi olmamıştır (Aksar, 2013: 34,35).

Bahsi geçen sebeplerle de devletler, artık uluslararası alanda tek önemli aktör olmaktan çıkmıştır. Ulus ötesi firmalar, hükümet dışı kuruluşlar, uluslararası örgütler ve devlet dışı sistemler de artık uluslararası politikada söz sahibi olan yeni aktörler olarak yerini almıştır (Heywood, 2014: 28-31).

Uluslararası ilişkiler bağlamında, "siber güvenlik" teriminin yeri ve önemi gün geçtikçe arttığı düşünülür ise, dünya barış ve güvenliğinin temin edilebilmesine yönelik olarak, "siber suç, siber saldırı, siber tehdit, siber terörizm ve siber savaş vb." terimlerin tanımlanması, üstüne anlaşmaların yapılabilmesi, uluslararası hukuki kurallar içindeki yerlerinin netleştirilmesi son derece önemli bir hal almıştır (Gürkaynak ve İren, 2011: 275, 276). Uluslararası toplum söz konusu tanımlara ilişkin belli bir uzlaşmaya varamamıştır ve yakın gelecekte de böylesi bir uzlaşının sağlanacağı mümkün görülmemektedir.

Uluslararası ilişkilerin tabiatı temelde uluslararası sahadaki hadiselerin belirme biçimleri ve nedenleri üstünde durmaktadır. Birçok kuramcı da hakim devletler arasındaki ilişkilere dair düşünceler iddia etmişlerdir. Temelde amaçları, devletler arasındaki ve devletlerin kendi içlerindeki politik etkileşim yaklaşımlarını anlayabilmektir. Söz konusu kuramcılardan kimisi geçmişteki hadiseleri açıklamak ve gelecek ile alakalı öngörülerde bulunup, kuramsal modellemeler oluşturma ve söz konusu modellerle genel prensipler çıkarma gayreti içerisine girmiştir.

Söz konusu modellemeler tartışılırken savaş ve barış, sınırlar ve güç ilişkilerindeki ana paradigmalara dair bazı sorular uluslararası ilişkilerin tabiatını yoğurmuştur. Teknolojik gelişmelerdeki süratli değişim, devletler arası ilişkilerde ciddi gelişmelere neden olmuştur. Söz konusu süreç uluslararası sahada savaş ve siyaset şekillerinin de değişmesine yol açmıştır (Knutsen, 2006: 346). Bu değişimle beraber, "Digital-age Security" teriminin kendi kendine tartışıldığı yeni devirde, teknolojinin özel bir tesirinin olduğu yeni modellere gereksinim duyulduğu kaçınılmaz bir realite olmuştur (Dunn, 2007: 86).

Uluslararası ilişkilerle siber güvenlik ikilisi için, 1991'den sonra sivilleşmiş olan ve dünyanın kullanımına açılmış olan internet, uluslararası sistemin aktörleri olan devlet, toplumlar ve bireyleri birbirine daha aktif biçimde bağlamıştır. Bu çerçevede, internet teknolojisinin uluslararası arenadaki hadiselerin katalizörü olduğunu ifade etmekte yarar bulunmaktadır. İnternet, belleklerdeki Soğuk Savaş tansiyonunun düşmesiyle, değişik kamplardaki bireyler arasındaki perdelerin kalkmasında ciddi bir role sahip olmuştur. 1991 Körfez Savaşı'nın ayrıntılarının internetle basın yayın üstünden canlı şekilde izlenmesi, yeni devrin farklılık arz edeceğinin en önemli göstergesi haline gelmiştir (Bıçakçı, 2012: 207). Uluslararası ilişkilerin doğasıyla siber güvenliğin kesiştiği nokta da işte bu noktada başlamıştır. Bu hususlar bütün dünyada iletişimin ötesine geçerek verilerin nakledilmesini temin eden ve manipülasyon kuvveti bulunan bir ağ (www) ile devletler arası menfaatler şeklinde karşımıza çıkmıştır (O'Connell, 2012: 191).

Uluslararası ilişkilerin kalbindeki devletlerin, siber uzayın aktörü olmasıyla devletler, mevcut güç potansiyellerini siber güvenlik sahasına kaydırmıştır. Devletlerin siber uzayın bir aktörü olması, siber suçların tesir sahasının genişlemesi ve oluşturduğu tehdit potansiyelinin artmasına yol açmıştır. Bu da uluslararası ilişkilerde devletlerin "siber güvenlik" terimini daha önemli bir biçimde ele alması mecburiyetini getirmiştir. Siber güvenlik, iki önemli dünya savaşındaki gibi askeri ve jeopolitik üstünlüğü öne çıkaran taarruzlar yerine, bilgi sistemleri üstünden gerçekleştirilen, siber uzayın arz ettiği sınırsız hürriyet ortamı içerisinde daha kolay ve kısa süre içinde yapılan saldırıları olanaklı kılmıştır (Bayraktar, 2015: 24). Söz konusu gelişmelerin sonucunda, geleneksel olarak güç algısının yerine, değişik yöntemler ile güç çerçevesini arttırma ve global boyutta aktif olabilmek için değişik kuramsal modellerin çıkış noktası oluşturulmuştur. Uluslararası ilişkilerin aktörleri arasındaki mücadelelerin de teknolojik bir devrimden sonra kuramsal tartışmalar ile yeni bir boyutta tartışılması kaçınılmaz hale gelmiştir.

Değişmekte ve gelişmekte olan dünyanın ortaya çıkardığı bu tip girişimler ve yenilikler, teknolojik bağlamda uluslararası aktörlerin saldırı ve savaş stratejilerine de elbette etkide bulunmuştur. Literatürde tartışılmakta olan ve tam olarak yerinin belirlenemediği boyutsa, yaşanılanların tek yanlı bir saldırı olduğu mu savaş kavramı ile birlikte hatırlanan bir öge mi olduğu noktasındadır. Bu bağlamda uluslararası ilişkilerde

bir zemine oturtulmuş olan siber güvenlik ve beraberinde getirmiş olduğu algısal seviye, siber uzayı çatışma sahasına dönüştürüp kuramsal bir zemin oluşturmuştur.

Uluslararası ilişkilerde, siber güvenlikle etkileşim içinde olan kuramsal girişimlerin oluşturulması için, Amerika'da konuyla ilgili faaliyetler önemli görülmekte ve özel sektör de desteklenmektedir. Bilgi teknolojileri ve bu sahanın getirdiği yenilikler ile beraber yoğrulan devletlerin kurumsal çerçevede yaptıkları çalışmalar ve üniversitelerin bu hususstaki faaliyetlere olan destekleri karar alıcılara genellikle raporlar şeklinde sunulmaktadır. Bu tip gelişmeler, elbette uluslararası ilişkiler kuramlarının siber güvenlik zemininde gelişmesini mümkün hale getirmektedir (Choucri ve diğerleri, 2013: 97).

Uluslararası ilişkilerle ilgili olarak, uluslararası aktörlerin de etkilenmiş olduğu ve çalışmanın konusunu teşkil eden siber güvenlik, bilimsel ve profesyonel çerçevede, değişik sahalarda da gelişmesini devam ettirmiştir. Şekil 3.6'da görüleceği gibi siber güvenliğin çalışılmasıyla ilgili genel araştırma sahalarında, teknik başlıklarda bir baskınlık dikkati çekmektedir. Uluslararası ilişkilerdeki araştırmalar ise disiplinler arası boyutta incelenmekte ve konunun doğru anlaşılması için teknik boyuttan hiçbir zaman uzak durulmamaktadır. Bilhassa bilişim suçlarıyla ilgili artışlar dikkate alındığı zaman siber güvenliğin hukuki çalışmalar boyutundaki eksikliği dikkat çekmektedir.

# İKİNCİ BÖLÜM

## 2. ULUSLARARASI İLİŞKİLERDE ETKİ ARACI OLARAK SİBER GÜVENLİK

### 2.1. Siber Silahlar:

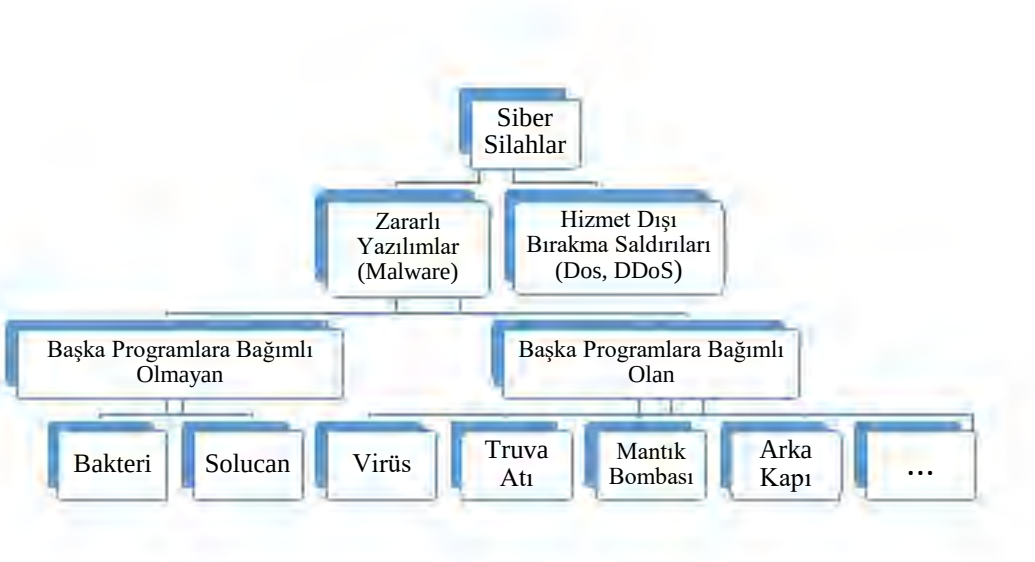
Genel olarak; insanlara, suni yapılara veya sistemlere zarar vermek ya da hasara uğratmak amacıyla kullanılan her türlü araç olarak tanımlanan silahlar; öldürme, sakatlama veya düşmanı mağlup etme ve düşmana karşı üstünlük kurma amacıyla kullanılmaktadır (Brown ve Metcalf, 2014, 131). Türk Dil Kurumu'na göre ise savunma ya da saldırı amaçlı kullanılan araçlara silah denilmektedir (TDK). Bu tanımlamalardan da anlaşılacağı üzere, bir aracın silah olarak tanımlanmasında belirleyici unsur, hangi amaca yönelik kullanılıyor oluşudur. Örneğin; bir bıçak nesneleri veya yiyecekleri kesmek için üretilmiş bir araçken, kimi zaman bir insana ya da canlıya saldırı amacıyla da kullanılabilmektedir. Söz konusu araç, burada kullanıldığı amaca göre silah olarak kabul edilmektedir.

Kara, hava, deniz ve uzay alanlarından sonra devletlerin beşinci harekat alanı olarak ortaya çıkan siber alanda ise siber silahlara dair uluslararası düzenlemeler ya da yasalarla belirlenmiş, uluslararası uzlaşının sağlandığı bir tanım yapılamamıştır. Devletler ve devlet dışındaki aktörler tarafından geliştirilen ve kullanılan siber silahların son derece çeşitli olması da siber silahlar için uluslararası platformda ortak kabul gören bir tanım yapılamamasında yaşanan zorluklardan biri olarak karşımıza çıkmaktadır (Arimatsu, 2012, 100). Ancak genel olarak siber silahları, hasmın bilişim sistemlerini veya bunlar içindeki bilgilerin gizliliğini, bütünlüğünü ya da erişilebilirliğini hedef alan, bilgi ve iletişim teknolojileriyle sayısal sistemleri etkisiz hale getirmek, bozmak, sekteye uğratmak veya tahrip etmek için kullanılan yazılım veya yöntemler (Çifçi, 2017, s. 168) olarak tanımlamak mümkündür. Ayrıca saldırı, insan öldürme, yaralama ya da siber ortamı tahrip etme veya yok etme aracı olarak tasarlanan ya da kullanılan tüm siber etkinlikler de siber silah olarak kabul edilmektedir (Schmitt, 2013, ss. 141-142).

Tanımlardan da anlaşılacağı üzere, tıpkı geleneksel silahlarda olduğu gibi, herhangi bir siber etkinliğin siber silah olarak nitelendirilmesinde en büyük kıstas amaçtır. Dolayısıyla, bir siber etkinlik önemli, fark edilebilir ya da somut bir hasara sebep olmadıkça siber silah olarak değerlendirilmemelidir (Mele, 2013, s.13).

Kabaca düşük potansiyelli ve yüksek potansiyelli olarak iki gruba ayrılabilecek siber silahlardan, düşük potansiyele sahip olanlar, bir sisteme teknik olarak doğrudan zarar verme kabiliyeti olmayan; fakat dolaylı yollarla sızması durumunda etkisini göstererek amacına yönelik faaliyetlerde bulunan yazılımlarken; yüksek potansiyele sahip siber silahlar, tıpkı bir istihbarat görevlisi gibi, korunaklı ve hatta fiziksel açıdan izole edilmiş sistemlere bile sızabilen ve doğrudan söz konusu sistemler içinde amacına yönelik istihbarat faaliyetlerinde bulunabilen yazılımlardır (Rid ve McBurney, 2012, s. 8). Siber silahlara yönelik bir başka sınıflandırma da aşağıdaki tabloda verilmiştir:

**Tablo 2. 1.** Siber silah türleri (Çifci, 2017: 168)




Tabloda da görüldüğü üzere bu sınıflandırmada siber silahlar öncelikle zararlı yazılımlar ve hizmet dışı bırakma saldırıları olarak genel itibariyle ikiye ayrılmıştır. Ardından zararlı yazılımlar da kendi içnde başka programlara bağımlı olma hallerine göre sınıflandırılmaya tabi tutulmuştur.

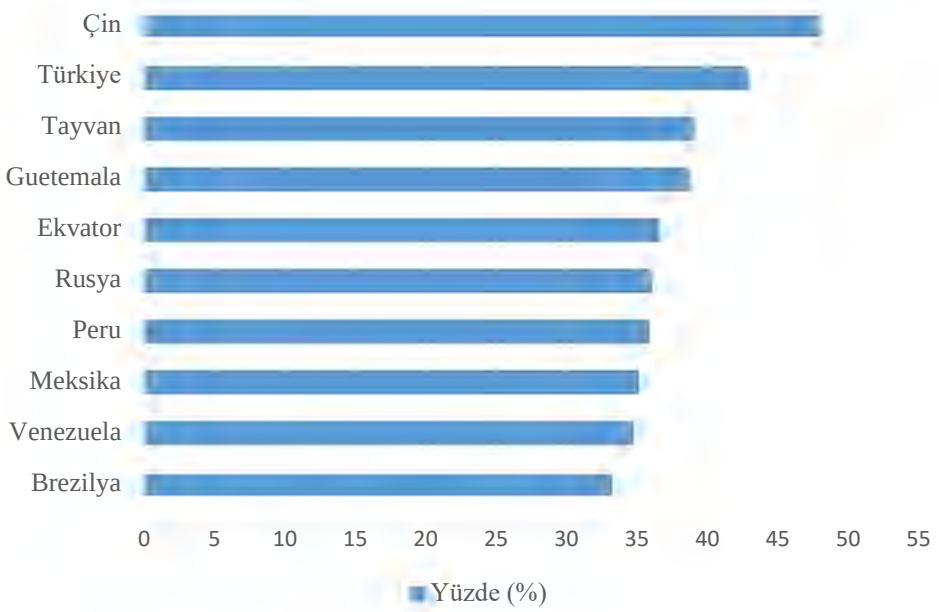
### 2.1.1. Zararlı yazılımlar:

Bilgisayar kullanıcılarının haberi olmadan, kullanılan bilgisayarlara sızmak ve söz konusu bilgisayarlara zarar vermek maksadıyla kodlanmış yazılımlara genel olarak zararlı yazılım denilmektedir. En geniş ifadeyle zararlı yazılımlar, bilişim ağlarına yetkisiz bir şekilde erişim sağlamak ve kullanıcıların iradesi dışında işlemlerde bulunmak

amacıyla yerleştirilmektedir (OECD, 2008). Zararlı yazılımlar küresel çapta bilişim sistemlerini etkilemektedir. Ancak etki alanları ülkelere göre değişiklik göstermektedir.

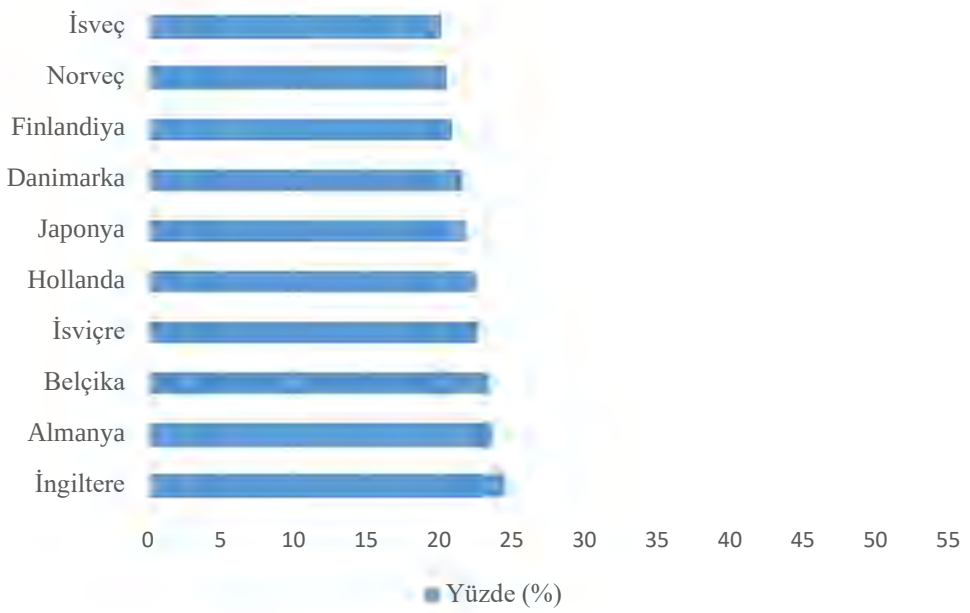
Aşağıdaki tablolarda zararlı yazılım bulaşan bilgisayarlar, ülkeler bazında ele alınarak en çok ve en az bulaşma yoğunluğuna sahip olanlar şeklinde gruplandırılmıştır.

**Tablo 2. 2.** *2016 yılında ülkelere göre en çok zararlı yazılım bulaşan bilgisayarlar (Statisca, 2016a)*




Tablo 2.2. 2016 yılında ülkelere göre en çok zararlı yazılım bulaşan bilgisayalarları ülkeler bazında ele almıştır. Aşağıda yer alan Tablo 2.3.'te ise aynı yılda en az zararlı yazılım bulaşan bilgisayarlar yine ülkeler bazında gösterilmiştir.

**Tablo 2. 3.** *2016 yılında ülkelere göre en az zararlı yazılım bulaşan bilgisayarlar (Statisca, 2016 b)*




Yukarıdaki tablolardan da anlaşılacağı üzere genel olarak Avrupa ülkelerinde zararlı yazlım bulaşan bilgisayar oranları nispeten daha düşükken, Çin başta olmak üzere Türkiye ve Tayvan gibi ülkelerde bu oran oldukça yüksektir. Zararlı yazılımların ülkelerdeki niceliğinin, siber alana dair hukuki alt yapılarının varlığı ve etkililiği, ayrıca söz konusu yazılımları önleme çalışmalarının yoğunluğu gibi farklı sebeplere bağlı olarak değiştiğini söylemek mümkündür (Eren, 2017, 39).

Bilişim sistemlerine bulaşan zararlı yazılımların gün geçtikçe hem çeşitliliği hem de bulaşma oranı artmaktadır. Başka bir deyişle, zararlı yazılımlar gün geçtikçe yatay ve dikey olarak artmaya devam etmektedir. Bu sebeple siber güvenlik çatısı altında hazırlanan bu çalışmada, zararlı yazılımları sınıflandırarak tanımlarına, teknik detaylarla karmaşık hale getirmeden, içeriğe uygun bir şekilde, işleyiş mantıklarına ve sebep olabilecekleri hasarlara yer verilmesi ilerleyen bölümlerin daha net bir şekilde anlaşılması için gerekli görülmüştür.

### 2.1.2. Bakteri ve solucan:

Başka bir programa bağımlı olmadan, kendi kendine çoğalabilen ve çoğalan versiyonlarını çalıştırırken daha fazla disk alanı ve işletim zamanı işgal ederek, kullanıcının bilgisayarında performans düşüklüğüne yol açan zararlı yazılımlara bakteri denilmektedir. Bakteriler, yapıları bakımından solucana, çalışma prensibi bakımından virüslere benzetildiği için, siber silahlara dair sınıflandırmalarda genel olarak kullanılmamakta ve virüs ya da solucanlar içinde tasnif edilmektedir (Çifçi, 2017, 169).

İşletim sistemleri ve programların güvenlik açıklarından faydalanarak bir bilgisayara girmesi halinde, ağdaki diğer bilgisayarlarla iletişim kurup kendini transfer ederek yayılan zararlı yazılımlara ise solucan denilmektedir. Solucanların saniyeler içinde milyonlarca bilgisayara bulaşma kabiliyeti bulunmaktadır (Çifçi, 2017, 169). Virüslerle karşılaştırıldığında daha zararsız bir yapıya sahip olan solucanlar, verilerde kayba ya da sistemde hasara sebep olmamaktadır. Fakat virüslere nazaran çok daha hızlı ve sistematik yayılma gücüne sahiptirler. Herhangi bir uygulamaya bağlı olmadan, kendi kendine çoğalabilir ve böylelikle bağlanılan ağ sayesinde diğer sistemlere kolayca bulaşabilmektedirler. Çoğalma ve yayılma süresince sistem ve ağın yavaşlamasına sebep olabilen solucanlar, doğrudan yayılma kapasitesine sahiptirler (Keleştemur, 2015, 227). e-postalar ya da dosyalar aracılığıyla son derece hızlı ve çok sayıda çoğalabilen solucanlar, hedef bilgisayarın kitlenmesine ve internet sayfalarının açılma sürelerinin uzamasına sebep olmaktadırlar (Ulaşanoğlu, 2010, 24).

1988'de ortaya çıkan ve Robert Tappan Morris'in yazılımını gerçekleştirdiği Morris solucanı, internete bağlı bilgisayarlardan 6000 tanesine bulaşarak, o zamana kadar en büyük hasara neden olan bilinen ilk solucan olmuştur (Nickolov, 2008, 37). Alanında etkin bilgisayar uzmanları bahsi geçen solucanı tespit etmek ve temizlemek için oldukça uzun zaman harcamış ve bu sürede çok sayıda askeri ve sivil araştırmacı bilgisayarından mahrum kalmıştır. Solucanın yarattığı maddi tahribatın boyutu ise 15 milyon dolar olarak hesaplanmıştır (Yıldırımoğlu, 2015).

TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) bünyesinde faaliyet gösteren Türkiye Bilgisayar Olayları Müdahale Ekibi (TR-BOME), 2009'da Conficker solucanı hakkında bir basın bülteni düzenlemiş ve solucanın dünya çapında 15 milyon bilgisayara bulaştığının tahmin edildiğini dile getirmiştir. Söz konusu

solucanın sisteme bulaştıktan sonra, bilgisayarın işletim sistemi ve anti-virüs programı güncellemelerini almasını engelleyerek başka zararlı yazılımların da bulaşması için uygun ortam hazırladığı belirtilmiştir (TÜBİTAK, 2009, 1).

### 2.1.3. Virüs:

Siber alanda uzun zamandır karşılaşılan virüs terimi, kimi zaman zararlı yazılımların bütününü ifade etmek için kullanılsa da bu yaklaşım yanlıştır. Virüsler, diğer bilişim sistemlerine bulaşarak yayılan ve çoğalan özel bir çeşit zararlı yazılım türünü ifade etmektedir (Graham, Howard, 2010, 198-199).

Virüslerin aktif hale gelip görevlerine başlayabilmeleri için virüslü program, dosya veya e-postaların kullanıcı tarafından çalıştırılması, okunması veya indirilmesi gerekmektedir (Canberk ve Sağıroğlu, 2006, 176-177). Tıpkı biyolojik virüsler gibi çalışan bilgisayar virüsleri diğer programlara bağımlıdırlar ve sızdıkları sistemlerde hızlı bir şekilde çoğalabilen zararlı yazılımlardır. Sızdığı sistem içinde kendi kendine çoğalabildikleri için mevcut yapıyı taşıyıcı olarak da kullanabilmekte, yazıldığı göreve göre hareket etmeye başladıktan sonra sistemleri kullanılamaz hale getirebilmeye kadar giden kabiliyetlere sahiptirler.

Genel olarak içine gizlendiği programın çalıştırılması ya da sistemdeki bir aksiyonun faaliyete geçirilmesiyle yayılmaya ve çoğalmaya başlayan virüsler, kendini kopyalamak için bilişim ağlarını kullanabilecekleri gibi CD, USB bellek, hard disk gibi harici depolama aygıtlarını da kullanabilmektedirler (Keleştemur, 2015, 222).

Virüsler, bulaştıkları bilgisayarların çalışma hızının yavaşlamasına, ya da bütünüyle çökmesine, bilgilerin kaybolmasına, bozulmasına ya da silinmesine neden olabilmektedirler. Virüslerin ne derece tehlikeli olabileceği yazılımcısının niyetine, zekasına ve yeteneğine göre değişiklik göstermektedir. Dolayısıyla, bazı virüsler ekrana sadece bir mesaj gönderirken diğeri bilişim sistemlerinde ciddi hasarlar meydana getirebilmektedir.

Virüslerin yazılımlarındaki görevlerini yerine getirebilmeleri için fark edilmeden sisteme girmeleri ve aynı şekilde faaliyetlerini sürdürmeleri gerekmektedir. Aksi takdirde yeterince yayılmadan ve yazılımlarını gerçekleştirmeden silinebilmektedir. Bu sebeple

her geçen gün karmaşıklaşan virüs yazılımları ile bu zararlı yazılımları tespit edip silmek için tasarlanan anti-virüs programları tam bir rekabet halindedir (Keleştemur, 2015, 222).

İlerleyen bölümlerde daha net anlaşılacağı üzere, virüs yazılımları siber alanda oldukça sık kullanılan saldırı yöntemlerinden biridir. Öyle ki 2009'da yapılan bir çalışmaya göre her 2.2 saniyede bir virüs siber alana dahil olmaktadır (Clarke ve Knake 50). Gelişen teknolojinin etkisi de dikkate alındığında bu sayının giderek attığını söylemek mümkündür. Ayrıca günümüzde neredeyse bütün verilerin bilişim sistemlerine aktarıldığı düşünüldüğünde, söz konusu sistemlere sızan bir virüsün sebep olabileceği hasarın son derece büyük boyutlara ulaşabileceği dile getirilebilmektedir. Nitekim son bölümde ele alınacak dünya çapında meydana gelmiş siber güvenliğe dair temel olaylarda virüslerle ilgili çok sayıda örneğe yer verilecektir.

### 2.1.4. Truva atı ve mantık bombası:

Tıpkı tarihte Yunanlıların Truva'ya hediye ettiği tahta at figürü gibi iyi niyetli, zararsız gibi görünen; ancak maskelenerek girdiği sistemlere gizli bir şekilde zarar vermek için programlanmış yazılımlara Truva atı denilmektedir. Truva atları, virüslerin aksine, bir bilgisayardan diğerine kendilerini kopyalayamazlar (Çifçi, 2017, 171). Yazılımcısı ile daima iletişim halinde olması Truva atlarının hedef sistem üzerinde her türlü erişim imkanına sahip olunmasını sağlamaktadır (Keleştemur, 2015, 223).

Çoğunlukla e-maillerin ya da ücretsiz uygulamaların içine yerleştirilen Truva atları, söz konusu program çalıştırılıncaya dek aktif hale geçemez. Kullanıcı sadece kendi faydası için ücretsiz bir uygulama indirdiğini düşünürken arka planda bir Truva atı da çoğu zaman kullanıcının haberi bile olmadan yüklenmiş olabilmektedir (Eren 2017,42). Aktif hale geçip, çalışmaya başladığındaysa, verilerin bozulmasına ya da silinmesine, kullanıcıya ait kişisel şifrelerin ele geçirilmesine veya sistemin uzaktan kontrolüne imkan veren erişime neden olabilmektedir (Yılmaz ve Salcan, 2008, 57).

Bir defa çalıştırıldıktan sonra sistemde yerini alan Truva atları, hedef bilgisayar çalıştığı ve internete bağlı kaldığı sürece yazılımcısı tarafından kontrol edilebilmektedir. Truva atları yazılımcıları, kimi zaman tek bir bilgisayarı hedef alabiliyorken kimi zaman da toplu saldırılar düzenleyebilmektedir. Bir Truva atının hedef aldığı sistem içinde yapabilecekleri, yazılımcısının istek ve yetenekleriyle doğru

orantılıdır (Keleştemur, 2015, 223). Ustalıkla yazılmış Truva atının hem kendisini gizleyebilmesi hem de hiçbir iz bırakmaması sebebiyle nerede olduğunu bulmak imkânsıza yakındır. Bu sebeple Truva atlarından korunmanın en iyi yolu kaynağı bilinmeyen program, uygulama ve yazılımların sisteme indirilmemesidir.

Kuluçka olarak adlandırılan dönemde, sistemlerde gizli bir şekilde zarar vermeden bekleyen, ancak belirli şartların oluşması ya da belirlenen zamanın geldiği durumlarda ortaya çıkarak, sistemleri tahrip edici şekilde hareket eden kodlar veya programlara mantık bombası denilmektedir (Keleştemur, 2015, 29). Belirlenen şartların oluşmasına ve istenilen zamanın gelmesine kadar zararlı bir program olarak görülmeyen mantık bombaları, bu yönleriyle Truva atlarına benzetilmektedir. Aktif hale geldiklerinde sistemleri çalışamaz duruma getirebilir veya yıkıcı etkiler yaratabilirler. Söz konusu sistemi kullanan bankalar, borsa ağları gibi kritik sistemlerin çökmesine sebep olabilirler (TSK, 1999, 12).

### 2.1.5. Arka kapı ve kök kullanıcı takımı:

Hedef bilişim sistemi üzerine yüklenen bir yazılım ya da işletim sisteminin kendisinde var olan bir açık veya sistemde mevcut bir yazılımda bırakılan bir açık aracılığıyla, normal kimlik kontrol mekanizmalarına takılmadan söz konusu sisteme gizli veya yetkisiz erişim sağlayan mekanizmalara arka kapı denilmektedir (Keleştemur, 2015, 289).

Arka kapılar, kimi zaman programcının herhangi bir portu bilerek ya da bilmeyerek açık bırakmasıyla oluşabileceği gibi kimi zaman da sisteme önceden sızmış kötü niyetli bir kişinin herhangi bir portu bilinçli bir şekilde açık bırakmasıyla da oluşabilmektedir.

Tespit edilmeleri son derece güç olan arka kapıların fark edilmesi durumunda, mümkün olan en kısa sürede açığı kapatan yama programlarla güvenlik yeniden sağlanmaya çalışılmaktadır. Sistemleri arka kapılardan korumanın en iyi yolu, kurulan uygulama ve eklentileri detaylı bir şekilde araştırmak ve kodlarını kontrol etmektir (Keleştemur, 2015, 289).

Kök kullanıcı takımları, çok kullanıcılı sistemlerde sıradan kullanıcıların yönetici haklarına dayanarak, yönetim uygulamaları ve sistem bilgilerine erişebilmeleri ve bahsi geçenleri gizleyebilmeleri için geliştirilmiş, ilk zamanlarda bu amaçlarla kullanılmıştır (Çifci, 2017, 173). Ancak yeni nesil kök kullanıcılar, sistemlere sızmış zararlı yazılımların rahatça gizli bir şekilde çalışabilmesi için kullanılmaktadır.

Genellikle işletim sistemlerinde, çekirdek düzeyde çalışıyor olmaları, tespit edilmelerini ve dolayısıyla temizlenmelerini güçleştirmektedir. Kök kullanıcıları bulup temizlemek için kullanılan özel araçların sahte anti-rootkit uygulaması olmadığından da emin olmak gerekmektedir. Zira bunların pek çoğu da işletim sistemine zarar vermektedir (Keleştemur, 2015, 226).

### 2.1.6. Casus yazılım ve köle bilgisayarlar:

İsminden de anlaşılacağı üzere, casus yazılımlar istihbarat amaçlı kullanılan yazılımlardır. Fakat ağırlıklı olarak firmaların reklam verme, istenmeyen mesaj gönderme gibi özel amaçlarına hizmet etmek için tasarlanmış casus yazılımlar da mevcuttur.

Kurulan casus yazılımlar; kullanıcı adı, şifre, kredi kartı bilgileri, e-posta bilgileri, webcam görüntüleri ve mikrofon kayıtları gibi son derece hassas kişisel verileri kaydedip, belirlenen hedeflere gönderebilmektedir. Ayrıca girilen web sitelerini, sosyal medyada yapılan yorumları kayıt altına alarak, kurbanın ilgi alanlarının da tespit edilmesinde kullanılmaktadır. Bunların dışında casus yazılımlar, arka planda çalışarak ziyaret edilmek istenenler yerine kullanıcıları sahte web sitelerine yönlendirebilmektedir (Keleştemur, 2015, 226). Casus yazılımlar aracılığıyla elde edilmiş özel ve hassas veriler tamamen farklı amaçlar için kullanılabilmektedir (Stafford ve Urbaczewski, 2004, 4597).

Bilgisayar kullanıcılarının haberi olmadan gizlice yüklenen ve sonrasında, saldırgana sistem üzerinde yönetici yetkileri vererek bilişim sistemini uzaktan, istediği şekilde kontrol etmesine olanak tanıyan zararlı yazılımlara bot, bu şekilde çok sayıda bilgisayarın ele geçirilmesiyle kurulan ağa ise botnet denilmektedir. Saldırganın her türlü amacına hizmet etmek için kullanılan bilgisayarlar da köle bilgisayar ya da zombi olarak adlandırılmaktadır (Keleştemur, 2015, 228).

Çok sayıda bilgisayar aynı anda tek bir saldırgan tarafından gelen komutlarla yönlendirilebilmektedir. Böylelikle saldırganlar, kullanıcısının haberi bile olmadan

dünyanın farklı yerlerindeki çok sayıda bilgisayarı kendi amaçları doğrultusunda yönetip, kontrol edebilmektedir (Eren, 2017, 48). Bu sebeple köle bilgisayarlar büyük çaplı siber saldırılarda da kullanılmaktadır (Güngör, 2015, 45). Nitekim Çifci de "bir milyon üyesi olan bir köle bilgisayar ağının Fortune 500'deki tüm şirketleri internet üzerinde çalışmaz hale getirebileceğini, on milyon üyesi olan bir köle bilgisayar ağının ise büyük bir Batılı devletin tüm iletişim alt yapısını felç edebileceğini" ifade etmiştir (Çifci, 2017, 173).

### 2.1.7. Gelişmiş siber tehditler (APT):

Gelişmiş siber tehditler, önceden belirlenmiş bir hedefe ısrarlı bir şekilde tekrarlanan saldırılar gerçekleştirebilen, son derece karmaşık yöntemler kullandıkları için oldukça etkili ve yıkıcı olan, aynı sebeple tespit edilmeleri ve önlenmeleri zor olan gelişmiş programlardır (Çifci, 2017, 174). Diğer yöntemlerden farklı olarak gelişmiş siber tehditler; savunma, imalat, finans, politika gibi değeri yüksek sektörleri hedef almaktadır (Chen, Desment, Huygens, 2014, 64).

Tek bir yönteme bağlı kalmadan; oltalama, sosyal mühendislik gibi siber saldırı teknikleri ile arka kapılar oluşturup hedefe yerleşerek saldırılar gerçekleştiren gelişmiş siber tehditler, hedef sisteme yavaşça ve fark edilmeden sızabilmektedir. Bu sayede hedef sistemde uzun süre kalmak amaçlanmaktadır (Virvilis,N., Gritzalis, D. 2013, 253-254).

Saldırının ilk hamlesi sisteme girişten sonra, sistem ve bağlı olduğu ağ keşfedilmektedir. Sonrasında sistemin açıkları belirlenip saldırıya geçilir. Gelişmiş siber tehdit programlarının sisteme girdikten sonraki süreçte aşama aşama neler yapcağı bütün alternatifleriyle birlikte önceden planlanarak saldırı kodlarına programlanmıştır (Robinson, N. vd., 2013, 30).

Knapp gelişmiş siber tehditleri diğer siber saldırılardan ayıran özellikleri aşağıdaki şekilde sıralamıştır (Knapp, E. D., Langill, J., 2014 44):

- Önceden belirlenmiş bir hedefe saldırmak için programlanmışlardır.
- Hedef sisteme sızdıktan sonra; yayılma, öğrenme, gizli verileri elde etme yeteneklerine sahiptirler.
- Herhangi bir ağa bağlı olmadan yani ağlardan bağımsız şekilde çalışan sistemlere de sızabilmektedirler.

Sistem içinde kendilerini gizleyebilme yetenekleri sayesinde uzun süre tespit edilmeden saldırılarını devam ettirebilmektedirler.

### 2.2. Siber Saldırı Türleri:

Siber uzayı konu alan uluslararası kurallara dair en kapsamlı çalışma olarak kabul edilen Tallinn El Kitabı siber saldırıyı, savunma ya da saldırıya yönelik olmasına bakılmaksızın, insanların yaralanmasına veya ölmesine, nesnelerin yok olmasına ya da zarar görmesine sebep olan siber faaliyetler olarak tanımlamıştır (Schmitt, 2013, 92). Lin'e göre siber saldırı; işletim sistemleri ve ağlarını ya da bu ağlarda bulunan veya iletilen bilgi ve/veya programlarını değiştirmek, bozmak, yok etmek veya geriletmek amacıyla kısa veya uzun vadeli olarak yapılan kasıtlı hareket ve operasyonlardır (Lin, 2010, 63). ABD Ulusal Araştırma Konseyi ise "bilgisayar sistemleri, ağlar veya bilgiyi ve/veya bunlarda yerleşik olan ya da bunları taşıya programları değiştirmek, bozmak, aldatmak, küçük düşürmek veya yok etmek içim yapılan kasıtlı hareketler" (Singer, Friedman, 2015, 29) şeklinde ifade etmiştir. 2016-2019 Türkiye Ulusal Siber Güvenlik Stratejisi de "ulusal siber uzayda bulunan bilgi ve iletişim teknolojilerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kişi veya sistemler tarafından yapılan işlemleri" siber saldırı olarak nitelendirmiştir (Ulusal Siber Güvenlik Stratejisi, 2016, 7).

Siber saldırılar bilişim sistemi kodlarını, işleyişini veya verilerini değiştirip kullanarak bu sistemlerin bozulmasına ve bazı siber suçlara sebep olarak yıkıcı sonuçlar doğurmaktadır (Andress, Winterfeld, 2011,3-5). Burada dikkat edilmesi gereken nokta bir saldırıyı, siber saldırı olarak nitelendirebilmek için saldırının siber ortamda gerçekleştirilmesi gerekmektedir. Örneğin; bir bilişim sistemini bombalayarak bozulmasına sebep olmak siber bir saldırı olarak değerlendirilmemektedir (Çifci, 2017, 6).

Bir siber saldırıda genel olarak aşağıdaki aşamalar izlenmektedir (Çifci, 2017, 153):

1- Bilişim sisteminden bilgi toplama
2- Bilişim sistemine sızma
3- Sıradan kullanıcı girişi

4- Ayrıcalıklı kullanıcı girişi
5- Bilişim sistemi kaynaklarının ele geçirilmesi
6- Bilişim sistemi kaynaklarının etkilenmesi

Siber alanda gerçekleşen ilerlemeler, gün geçtikçe siber bir saldırı için gerekli olan teknik bilgi ihtiyacını azaltmaktadır. Bu durum da kimi zaman sadece bir ağ bağlantısı ve tek bir bilgisayardan ibaret enstrümanla siber saldırı yapabilmeyi olanaklı hale getirmektedir. Böylelikle; teknik bilgiye duyulan ihtiyaçla ters orantılı bir şekilde siber saldırı sayısı artmaktadır. Üstelik siber saldırıya maruz kalan taraf açısından da giderek artan bedeller ortaya çıkmaktadır (Gürkaynak, İren, 2011, 273).

Gün geçtikçe daha sık hale gelen, daha organize ve doğurduğu sonuçlar açısından daha külfetli hale gelen siber saldırılar (Pernik, 2014, 1) sistemler üzerinde aşağıda verildiği şekilde etkiler yaratabilmektedir (Musman vd., 2011, 47-48):

- Verim Kaybı: Kullanılan verilerin parçalanması sistem hızını düşürür.
- Kesilme: Süreç, siber saldırı bitinceye dek kesintiye uğrar.
- Değiştirme: Veriler değiştirildiği için süreçler zarar görür.
- Aldatma: Sahte veriler yüklenerek sistemin etkin çalışması engellenir.
- Durdurma: Tüm süreç ya da yazılım ele geçirilir.
- Yetkisiz Kullanım: Tekrar siber saldırı yaşanması ihtimalini yükseltir ve beklenmeyen sonuçlara neden olur.

### 2.2.1. Hizmet dışı bırakma (DoS ve DDoS) saldırıları ve sosyal mühendislik:

Hizmet dışı bırakma saldırıları (DoS), bir bilgisayardan bir sunucu bilgisayara aynı anda ve mümkün olduğu kadar fazla istek ve paket göndererek, bu sunucunun yavaşlamasına sebep olan saldırılardır. Dağıtık hizmet dışı bırakma (DDoS) saldırıları ise DoS'ten farklı olarak, bir bilgisayardan değil çok sayıda bilgisayardan tek bir hedefe yapılan saldırılardır. Bu saldırılarda yüzlerce hatta binlerce bilgisayar aynı hedefe saldırabilmektedir. Saldırı bilgisayarları ele geçirilmiş olabileceği gibi anlaşmalı olarak da ayarlanabilmektedir. Eğer saldırı ele geçirilmiş bilgisayarlarla yapılmakta ise çalışmanın bir önceki bölümünde açıklanan zombi bilgisayarlar ve botnetler kullanılmaktadır (Keleştemur, 2015, 296).

DDoS saldırıları, DoS saldırılarına göre zombi bilgisayar sayısı kadar katlanan ölçüde büyük olduğu ve aynı oranda artan yıkıcı etkileri sebebiyle daha çok kullanılmaktadır (Ünal, 2015, 16).

DoS ve DDoS saldırılarında ortak amaç, hedef sistemle çok fazla sahte bağlantı kurarak sunucuya aşırı yük bindirmek ve nihayetinde sunucunun gerçek bağlantı taleplerine cevap veremez hale gelmesini sağlamaktır. Hedef alınmış sunucu hizmet bekleyen kullanıcılara ancak çok yavaş bir şekilde cevap verebilmekte ya da hiç cevap veremez hale gelmektedir (Douligeris, Mikrokotsa, 2004, 644).

Bu saldırılarda ağırlıklı olarak, devletlerin kritik alt yapıları hedef alınmaktadır (Hulme, 2018). Hizmetlerin yavaşlaması ya da tümüyle kesilmesi nihayetinde ciddi itibar kayıplarına ve maddi kayıplara sebep olmaktadır. En yıkıcı siber ataklar arasında olan DDoS saldırılarının, dünya ekonomisine en çok zarar veren siber atak çeşidi olduğu belirtilmiştir (Yihunie vd. 2018, 1-4).

Teknolojinin kullanılmasından ziyade, insan doğasının bir takım zafiyetlerinden yararlanarak, onlardan bilgi alma ya da istenilen işleri yapmasını sağlama faaliyetleri sosyal mühendislik olarak tanımlanmaktadır (Tombul 2015, 141). Sosyal mühendislik, kurbanlara güvenilir olduğunu hissettirme, onlarla ortak tanıdıklar vasıtasıyla yakınlık kurma, bir başkasını taklit etme, zor bir durum oluşturup yardım ediyormuş izlenimi verme, kurbanın çöp olarak attığı kişisel bilgileri karıştırarak elde etme (Gragner, 2001) gibi yöntemlerle hedef sisteme ait bilgilerin ele geçirilmesidir. Dolayısıyla sosyal mühendislik, diğer saldırılardan faklı olarak, teknik bilgiye ihtiyaç duymadan da yapılabilmektedir. Her siber saldırının araç, gereç ve sınırlamaları olsa da sosyal mühendislik, insanların kaçınılmaz olarak hatalara ve güvenlik duvarı ihlalalerine neden oldukları ve bu sebeplerle de siber güvenliğin en zayıf halkası oldukları tespit edilmiştir. Bu tespite dayanarak geliştirilen siber silahlar, herhangi bir sınırlama gerektirmeyen ve sınır tanımayan bir saldırı türüdür. İstismarcı, mağdura psikolojik olarak saldırır ve tuzağa düşürürse, kişi hakkında tüm bilgileri toplayabilmektedir (Maan ve Sharma, 2012: 557).

Sistem açığını bulmak, sisteme zararlı yazılımlarla saldırı yapmak gibi yöntemlerden çok daha kolay olması sebebiyle de sosyal mühendislik sıklıkla kullanılan saldırı yöntemi haline gelmiştir. Sosyal mühendislikte, siber güvenliğin en zayıf halkası

olan insan unsuru, kandırılarak gizli bilgilere ulaşıldığı için, alınan tüm siber güvenlik önlemleri etkisiz hale getirilebilmektedir (Akarslan 2015, 104-105).

Saldırgan, sosyal mühendislik sayesinde hedef sisteme ait tüm yetkilere sahip olmanın yanı sıra sadece bu kuruma ait verilere değil, kurumla iş yapan çözüm ortakları ve tedarikçiler gibi üçüncü taraflara ait verileri de ele geçirebilmektedir. İnsan ilişiklerinin kullanıldığı sosyal mühendislik, tarihin en eski ve en etkili siber saldırı yöntemi olarak nitelendirilmekte ve klasik donanım ve yazılımlarla engellenmesi mümkün olmayan bir saldırı çeşidi olduğu vurgulanmaktadır. (Keleştemur, 2015, 307). Böylesi bir saldırının devletin önemli kurumlarında görev yapan üst düzey yetkililere karşı yapılması durumunda ortaya çıkabilecek tehlikenin boyutları, sosyal mühendislik saldırılarının devletler için son derece kritik bir noktada olduğunu gözler önüne sermektedir.

Bilişim sistemleri her geçen gün gelişmekte ve bu konuda her türlü güvenlik açığın giderilmesi için çaba sarfedilmektedir. Kişileri bir biçimde suistimal edip elde edilen veriler ya da denetimlerle kişilere kurumlara önemli hasarlar verilmektedir. Bu hususta bilinçliliğin yükseltilmesi ve eğitimlerin sunulması bu saldırılara engel olabilmek amacıyla atılabilecek en fazla önem arz eden adımlar olarak nitelendirilmektedir (Conteh ve Scmick, 2016: 31).

### 2.2.2. Yemleme-oltalama saldırıları ve istem dışı yığın ileti (e-posta) gönderme:

Saldırganın, güvenilen kurum veya işletmelerin elektronik iletişim kaynaklarından birinin yerine geçerek, onlardan gönderilmiş izlenimi veren e-postalar veya mesajlarla kurbanın aslında sahte olan kaynakla kullanıcı adı, şifre, kredi kartı bilgileri gibi kapsamlı kişisel verilerini elde etme yöntemine yemleme-oltalama saldırısı denilmektedir (USOM, 2014). Saldırganlar genellikle bir kurumun temsilcisi veya yetkilisi gibi davranarak kurbanların bilgilerini ele geçirmektedir (Canbay, 2008: 17).

Yemleme-oltalama saldırıları, saldırgan tarafından güvenilen bir kurumdan gelmiş izlenimi veren bir e-posta aracılığıyla kurbanın, gerçeğine son derece yakın bir benzerliğe sahip sahte siteye yönlendirilmesiyle başlamaktadır. Siteyi gerçeğinden ayırt edemeyen kurbanın bilgilerini paylaşmasıyla birlikte saldırgan söz konusu bilgileri ele geçirmektedir. İnsan doğasının zafiyetlerinden faydalanarak yapılan bir saldırı çeşidi olması sebebiyle sosyal mühendislik içinde değerlendirilebileceği de dile getirilmiştir

(Hekim, 2015: 58). Ve tıpkı sosyal mühendislikte olduğu gibi devletin önemli kurumlarında görev yapan üst düzey yetkililere karşı yapılması durumunda ortaya çıkabilecek tehlikenin boyutları, bu saldırı çeşidinin de devletler için son derece kritik bir noktada olduğunu gözler önüne sermektedir.

Yemleme-oltalama saldırısı yoluyla kullanıcıları dolandırmak için sıklıkla popüler web siteleri, açık arttırma siteleri, alışveriş siteleri ve bankacılık siteleri gibi ağlar kullanılmaktadır (Çifci, 2017: 167). Bu saldırılar aracılığıyla son derce kapsamlı istihbarat operasyonları düzenlenebileceği gibi sıradan kullanıcılara ekonomik zararlar da verilebilmektedir. Bu bağlamda yemleme-oltalama saldırı kullanılarak binlerce kredi kartı bilgisi çalınmış, milyonlarca dolarlık vurgunlar yapılmıştır (Keleştemur, 2015, 308-309). Bu tür saldırılardan korumanın en etkili yolu, yemleme e-postaları hakkında bilgi edinmek ve bağlantılara tıklamaktan kaçınmaktır (Pajunen, 2017: 21).

Junk mail, spam mail ya da bulk mail gibi farklı isimlendirmeleri de bulunan istem dışı yığın iletiler, çok sayıda kullanıcıya benzer içeriğe sahip e-postaların gönderilmesiyle gerçekleştirilmektedir (Çifci, 2017, 164).

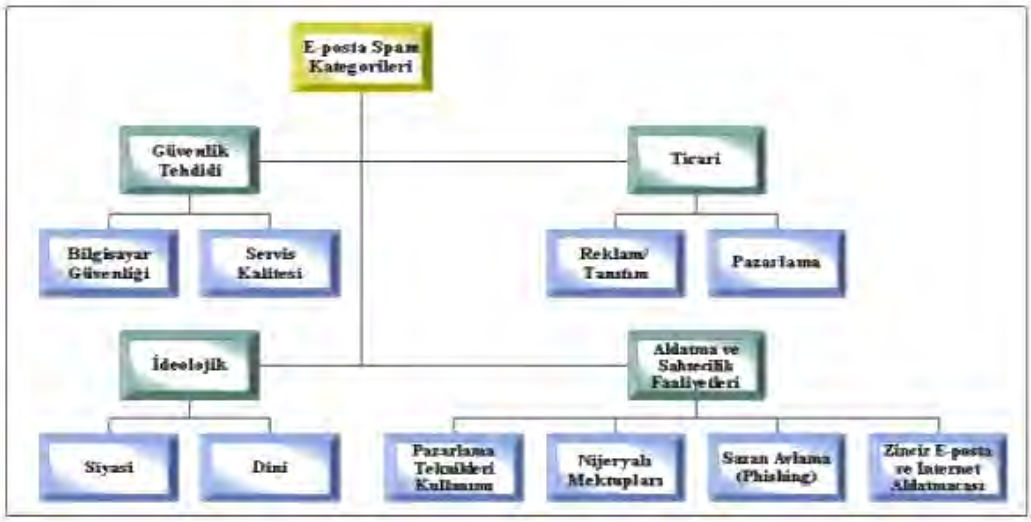
Saldırganlar, web sitelerinden, müşteri listelerinden, haber gruplarından, elektronik bültenlerden ve sosyal medyadan binlerce hatta yüzbinlerce e-posta adresini satın almakta ya da ele geçirmektedir. Ardından genellikle ticari kaygılarla veri tabanlarındaki kullanıcılara toplu olarak e-posta gönderilmektedir. İstenmeyen yığın iletiler ağırlıklı olarak reklam içerikli olsalar da kimi zaman zararlı yazılımlarla birlikte gönderilmektedir (Keleştemur 2015 310).

İstenmeyen toplu elektronik postalar, ticari nitelikte olması gerekli olmayan, tek seferde yüz binlerce e-posta hesabına gönderilen elektronik iletilerdir. Bu mesajlar ticari içerikli olabileceği gibi, bir konuda siyasi görüş yaymak veya kamuoyu oluşturmak amacıyla gönderilen elektronik iletiler de olabilmektedir (Şahinaslan, 2007: 19).

İstem dışı yığın iletiler, kişilerin gündelik yaşamda en fazla karşı karşıya kaldıkları ve sorun yaşadıkları zararlı yazılımların ilk sırasında yer almaktadır. İstem dışı yığın iletiler, reklam, ürün tanıtım ve satım ya da başka kötü maksatlarla insanların elektronik posta hesaplarına talep etmedikleri iletilerle meşgul etmektedir. Ferris Research tarafından yapılan çalışmada istem dışı yığın iletiler, 4 milyar dolarlık bir verim yitimine

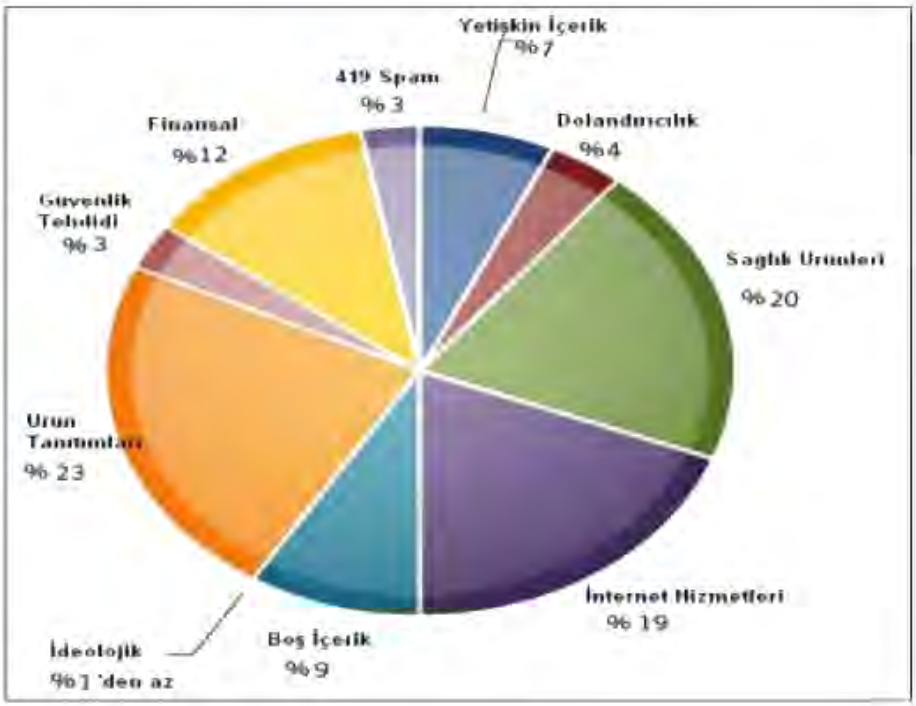
sebep olmaktadır (Canberk, Sağıroğlu, 2007; 126). Rasgele hesaplar açıp ileti gönderen bireyler, gerçek bir bireye ait olduklarını tespit ettikleri bu elektronik posta hesaplarını üçüncü bireylere vererek daha çok sağanağa yol açmaktadır (Öztürk, 2009: 34).

Şekil 2.1.'de spamlar kategorilere ayrılmıştır.




**Şekil 2. 1.** *Spam e-posta kategorileri (Öztürk, 2009: 34).*

Şekil 2.2.'de ise spamların oranları grafik üzerinde gösterilmiştir.




**Şekil 2. 2.** *Kategorilerine göre e-posta oranları (Öztürk, 2009: 36).*

### 2.2.3. Şebeke trafiğinin dinlenmesi ve kriptografik saldırılar:

Bir ağ üzerinde yer alan sunucu ve kullanıcılar arasındaki bilgi alışverişinin dinlenmesi "monitoring", bu sürede kullanılan kullanıcı adı, parola, kredi kartı bilgileri gibi kişisel verilerin elde edilmesi ise "sniffing" olarak tanımlanmaktadır (Ulaşanoğlu vd 2010, 21). Sniffer yazılımı veya donanımı, tüm paketleri dinleyen karışık moda giren tüm ağ trafiğini dinlemekte ve günlükte kayıt altına almaktadır. Bu paketlerde bulunan parola bilgileri gibi önem arz eden veriler paket içerikleri analiz edilerek elde edilebilmektedir (Şahinaslan vd., 2013: 1081). Bu saldırılarla saldırganlar tarafından daha sonra kullanılmak üzere birçok bilgi kaydedilebilmektedir. Günümüzde çok sayıda şirket, kamu kurumu ve üniversite sitelerinden elde edilmiş yüz binlerce kullanıcı adı ve parola saldırganlar tarafından ele geçirilmiştir (Yılmaz, Salcan 2008, 59).

Şifrelenmiş halde bulunan mesaj veya verilerin şifresinin çözülmesi amacıyla yapılan saldırılara kriptografik saldırı denilmektedir (Çifci 2017 161). Saldırı süresince kullanılmakta olan kriptografik sistem araştırılır ve sonrasında sistemin zayıf noktaları tespit edilerek herhangi bir zafiyet bulunması durumunda şifreler çözülmeye çalışılmaktadır.

Oldukça eski bir istihbarat faaliyeti olan kriptografik saldırılarla özellikle I. ve II. Dünya Savaşı dönemlerinde oldukça hassas pek çok bilgi ele geçirilmiş ve böylelikle savaşın gidişatını değiştiren operasyonlar düzenlenmiştir (Keleştemur, 2015, 303-304). Bu örnek göz önüne alındığında kriptografik saldırıların devletler için önemi ortaya daha net bir şekilde çıkmaktadır.

### 2.2.4. IP sahteciliği ve açık mikrofon dinleme:

Diğer adı IP Spoofing olan bu saldırıda kullanılan bilgisayarın gerçek IP (İnternet Potokolü) adresi gizlenmekte ya da başka biri yerine geçmek için değiştirilmektedir. Saldırganın kimliğini gizlemek adına önemli olan bu saldırı, ağırlıklı olarak hizmet dışı bırakma saldırılarında kullanılmaktadır (Keleştemur, 2015, 299). Bunun yanı sıra IP adresine dayanan kimlik doğrulama sistemlerinde de hedef bilgisayarı aldatıp, güvenilen ya da yetkili kişinin bilgisayarının yerine geçerek sistemin bir parçası olmak için veya söz konusu sisteme sızmak için de IP sahteciliği kullanılmaktadır (Çifci, 2017, 164).

Bilgisayar sahibinin haberi olmadan, bilgisayar mikrofonu açılarak canlı dinleme veya ortam dinlemesi yapılarak gerçekleştirilen saldırılar açık mikrofon dinleme olarak nitelendirilmektedir. Aynı şekilde bilgisayar kameraları da açılıp görüntüler gizlice kayıt altına alınabilmektedir (Çifci 2017 165).

2009 yılında GhostNet olarak adlandırılan bir casus yazılım ortaya çıkarılmıştır. Bu yazılımın, 103 ülkeden çok sayıda bilgisayarın mikrofon ve kameralarını açarak ses ve video kaydı aldığı, sonrasına topladığı bu verileri Çin'e gönderdiği iddia edilmiştir. Açık mikrofon dinleme saldırısı olan GhostNet'ten en çok devlet kurumları ve elçilikler etkilenmiştir (Keleştemur 2015 290).

### 2.2.5. Oturum çalma ve klavye kaydediciler:

İki bilgisayar arasındaki oturumun çeşitli yöntemlerle ele geçirilerek saldırgana yetkisiz erişim sağlama imkânı veren saldırılar oturum çalma olarak nitelendirilmektedir (Çifci, 2017, 165). Oturum çalma saldırısından sonra sisteme erişim sağlayan saldırgan, kendi isteği yönünde verileri elde edebilmekte ya da değiştirebilmektedir.

Açık mikrofon dinleme saldırısına benzer bir şekilde, saldırıya maruz kalan bilgisayarın klavyesine yapılan her vuruşu kaydeden ve bu verileri saldırgana gönderen programlara klavye kaydedici denilmektedir. Klavye kaydedici saldırısıyla kullanıcı adı, parola ve kredi kartı bilgiler gibi kritik kişisel veriler ele geçirilebilmektedir (Baraz vd. 2008 146-147).

### 2.2.6. Kabloya saplama yapma ve internet servis saldırıları:

Yeterli olduğu kadar emniyet önlemleri alınmamış iletişim ağı kablolarına çeşitli fiziksel teçhizatlar yardımıyla saplama yapılarak, bağlantı kurulması ve böylelikle her iki tarafın trafiğini ele geçiren faaliyetlere kabloya saplama yapma ismi verilmektedir. Kabloya sapma saldırısı ev telefonları, VoIP telefonlar ve mobil telefonların yanı sıra bilgisayar sistemlerine yönelik olarak da düzenlenebilmektedir (Keleştemur 2015 303).

Bu saldırı, ağa erişim sağlayarak veri paketlerine ve kişisel bilgilere erişmeyi hedeflemektedir. Saldırgan, sistemdeki zayıflıkları ve güvenlik açıklarını bulmak için gizli dinleme saldırıları da yapabilmektedir. VoIP teknolojisinde, IP ağına erişimi olan bir saldırgan, kolay erişim yoluyla iletilen paketleri görebilir ve bunlara müdahale

edebilmektedir. Bu saldırı bazı paket yakalama programlarıyla kolaylıkla uygulanabilmektedir (Sandilaç, 2021: 42).

İnternete bağlı tüm cihazlar bazı protokol ve servisler aracılığıyla birbirleriyle bağlanmakta ve bu sayede iletişim kurmaktadırlar. Söz konusu protokol ve hizmetlerin ise bazı zafiyetleri bulunmaktadır. İnternet servis saldırıları, kimi zaman doğrudan protokollerdeki zafiyetlerden kimi zamansa yazılımlardaki açıklardan faydalanarak düzenlenen saldırılar olarak tanımlanmaktadır (Keleştemur, 2015, 301-303).

### 2.3. Siber Savunma, Korunma Yöntem ve Sistemleri:

Siber uzayda yer alan yazılım, donanım ve iletişim ağı alt yapısından meydana gelen bilişim sistemlerini ve bu sistemleri içeren her türlü teçhizat, sistem ve alt yapıyı gelebilecek siber tehdit ve saldırılardan korumak için alınan önlemler ve uygulamaların tümüne siber savunma denilmektedir. Aynı zamanda tüm bu sistem parçalarının yazılımsal, donanımsal ve içerdiği verilere dair gizliliğinin sağlanması da sistemlerin siber saldırılar karşısında savunulmasında bir bütün olarak katkı sağlamaktadır (Çifci, 2017, 219). Siber savunmanın önemli kriterlerinden biri de gerekli bakımların yapılarak sistemi oluşturan öğelerin düzgün ve sorunsuz şekilde çalışmasını sağlamaktır. Bunların yanı sıra sistemin güvenlik açıklarının tespit edilerek varsa bunların kapatılması, sistem öğelerinin düzenli olarak güncellenmesi, bozuk ya da çalışmayan öğelerin doğrudan sistemden çıkarılması da son derece önemlidir. Siber savunma, bir saldırı olması halinde ne gibi operasyonların yapılması gerektiğini de içermektedir. Dolayısıyla siber güvenlik stratejileri genel olarak uzun vadede önem taşımaktadır (Keleştemur, 2015, 315-316).

Bilindiği üzere siber saldırıya hedef olabilecek sistemler içinde kamu kurum ve kuruluşlarının, bankacılık ve finans sektörlerinin kısaca devletler için hayati öneme sahip sektörlerin sistemleri de bulunmaktadır. Dolayısıyla siber savunma yalnızca bireysel ya da kurumsal bazda değil, ulusal ve uluslararası boyutta da son derece büyük bir öneme sahiptir. Siber saldırıların sebep olabileceği büyük ekonomik zararla birlikte kamusal düzen ve güvenlik de tehlikeye girebilmektedir. Bu sebeple siber saldırılara karşı bireyler, sivil toplum kuruluşları, kamu kurum ve kuruluşları ve özel sektör topyekûn bir şekilde ulusal ve uluslararası boyutta korunma yöntem ve sistemleri geliştirerek uygulamalıdır (Ünver ve Canbay, 2010, 99). Ancak bilişim sistemlerine dair güvenliğin en zayıf halkasının insan olduğu da kesinlikle unutulmamalıdır. En yüksek teknoloji ve güvenlik

önlemlerine sahip bir sisteme dahi sadece insan doğasının zafiyetinden faydalanılarak düzenlenen saldırılarla büyük çapta zarar vermek mümkündür. Bu sebeple kurum ve kuruluşların çalışanlarına eğitim vermek, siber saldırı ve tehditlere karşı bilinçlendirerek farkındalık yaratmak hat safhada önemlidir (Şahinaslan vd., 2009, 597-600).

Siber tehditlerle mücadele ederek etkin bir şekilde savunma yapabilmek ve bu çalışmanın ilerleyen bölümlerinde aktarılacak bazı konuların daha iyi anlaşılabilmesi için siber savunma yöntem ve sistemlerine yer vermek gerekli görülmüştür.

### 2.3.1. Zafiyet tarayıcılar ve güvenlik duvarı:

İletişim ağlarını, bilgisayarları, bilgisayar sistemlerini ve bu sistemler içindeki uygulamaları tarayarak herhangi bir zafiyet olup olmadığını inceleyerek, rapor veren yazılımlara zafiyet tarayıcı denilmektedir. Elde edilen raporlarda sistemin mevcut risklerini bertaraf etmek ve istenilen güvenlik düzeyine erişebilmek için gerekli görülen değişiklik tavsiyelerine de yer verilmektedir. Aynı zamanda şifrelerin güçlülüğünü de araştıran zafiyet tarayıcılar, sistemlere yapılan saldırıları ve bu saldırıların izlerini de araştırabilmektedir (Çifci, 2017, 227).

Zafiyet tarayıcılar bir taraftan yıkıcı olmayan, sadece zafiyetleri bularak sistemleri daha güvenli hale getirmek için kullanılırken diğer taraftan da saldırganlar tarafından hedef sistemlerin boşluklarını bulmak amacıyla kullanılmakta ve böylelikle yıkıcı bir araca da dönüştürülebilmektedir (Keleştemur, 2015, 323).

Temel olarak üzerinden geçen veri trafiğini belirlenmiş kurallara göre denetleyerek, gerektiği durumlarda bu trafiğin engellenmesini sağlayan programlara güvenlik duvarı denilmektedir. İçinden geçen trafikte erişim kurallarını tanımlamak ve uygulamak için kullanılan güvenlik duvarları içerisinde oluşturulan kurallar tablosu yardımıyla, belirli trafik türlerinin istenmeyen bir yere geçişini engellemeyi mümkün hale getirmektedir. Güvenlik duvarları, verilerin açık ağlardan geçerken gizliliğinin korunmasında da yardımcı olmaktadır (Tan ve Aktaş, 2011, 35). Ayrıca, güvenlik duvarları dış dünyayla bağlantı sağladığından, mobil kullanıcılar şifreli bağlantılar kurarak açık ağlarda dolaşırken veri gizliliğinin muhafaza edilmesine yardımcı olabilmektedir (Şahinaslan vd., 2013: 1083).

Güvenlik duvarları veri trafiğini; paket filtreleme, uygulama filtreleme, durumsal denetim ve tüm yöntemlerin birleştirilmesi gibi birçok güvenlik fonksiyonu vasıtasıyla kontrol edebilmektedirler (Çifci, 2017, 228).

### 2.3.2. Saldırı tespit/önleme ve veri kaçağı önleme sistemi:

Güvenliği sağlamak amacıyla veri ve ağ trafiğini sürekli olarak izleyerek şüpheli bir paket ya da zararlı bir davranışla karşılaştığında bunları kaydedip bir uyarı sinyali gönderen sistemlere saldırı tespit sistemleri denilmektedir. Saldırı önleme sistemleri ise ağ içinde güvenlik ihlali oluşturabilecek bir hareket tespit ettiğinde güvenlik duvarını yeniden programlayarak ağ trafiğini engelleyip, saldırıyı durduran sistemler olarak tanımlanmaktadır (Martin ve Strategy, 2016, 3). Ağ tabanlı saldırı tespit/önleme sistemleri ve bilgisayar tabanlı saldırı tespit/önleme sistemleri olarak temelde iki çeşidi bulunmaktadır (Çifci, 2017, 230).

Saldırı Tespit Sistemi, bilgisayar sistemi veya ağ sistemi üzerinde meydana gelen tüm faaliyetleri denetleyen, doğrulayan ve kontrol eden, güvenlik ihlali sorunları oluştuğunda sistem yetkililerine ve ilgili departmanlara bildirimde bulunmak için alarm gönderen güvenlik bileşenleridir. Saldırı Tespit Sistemi tarafından olası saldırı, bilgi toplama, inceleme ve yanıt analizi motoru olmak üzere üç öğede analiz edilmektedir. Saldırı Tespit Sistemi, istemci ve sunucu arasındaki veri alışverişinde anormal bir durum olup olmadığını belirlemek için İnternet ağ trafiğini ve sistemlerini incelemektedir. Saldırı Tespit Sistemi önleyici bir sistem değildir. Saldırganlar sisteme zarar vermeden önce uyarı görevi gören bir siber güvenlik önlemidir (Bace ve Mell, 2011: 29).

Bilgi güvenliği konusunda sıklıkla araştırılan Saldırı Tespit Sistemi, bir alarm sistemi görevi görmekte ve İnternet ağlarının son güvenli uç noktası olarak görev yapmaktadır. Başka bir deyişle, saldırgan bu saldırı tespit kalkanını kırarsa, neredeyse tüm sistemin kontrolünü ele geçirme gücüne erişebilmektedir.

Veri kaçağı önleme sistemi, belli bir sistem içindeki verilerin dışarıya sızdırılmasını engellemek için hem izleme hem önleme yöntemiyle çalışan yazılım ve donanımlara denilmektedir (Kanagasingham, 2008, 4-5). Bu sistemler, kritik bilgilerin dışarı sızdırılmasını önlemek için; dosyaların kime gönderildiğine, kimlerin harici sürücülere (CD/DVD) ne kaydettiğine, kimlerin dosya çıktısı aldığına dair bilgileri

kaydedebilmekte, belli dosya ve e-postaların kurum dışına gönderilmesini engelleyebilmekte veya kayıt altına alabilmektedir (Çifci, 2017, 232). Kurumlardan izinsiz olarak gizli sistem verilerinin alınmasını engellemektedir. Hem ağ düzeyinde hem de istemci düzeyinde çalışan modeller vardır. İstemci üzerinde çalışan sistemler, çıkarılabilir medya gibi kaynakların kaybını önlemek için aygıtları izleyen bileşenlere sahiptir. Örnekler arasında yazıcılar, CD-DVD yazıcılar ve sürücüler ve USB depolama aygıtları sayılabilir (Paşaoğlu vd., 2019: 82).

### 2.3.3. Antivirüsler ve yığın ileti engelleme sistemi:

Antivirüs koruma yazılımı, kötü amaçlı yazılımlara engel olmak, algılamak ve devre dışı bırakmak için tasarlanmış bilgisayar programları olarak tanımlanmaktadır. İlk başta bilgisayar virüslerine karşı koruma sağlamak için oluşturulan virüsten koruma yazılımının kapsamı, kötü amaçlı yazılımların oluşmasından bu yana genişlemektedir (Henry, 2013: 39). Gün geçtikçe daha kapsamlı hale getirilen antivirüs programları, tüm ağ trafiğini analiz edip gerekli tespit ve temizlikleri yapabilmekte, harici depolama cihazlarını tarayabilmekte, sisteme kopyalanan ya da indirilen dosyaları analiz edebilmekte ve bilinçli ya da yanlışlıkla çalıştırılan programları da tarayarak zararlı kod tespit edilmesi halinde bloke edebilmektedir (Keleştemur, 2015, 320).

Bir önceki bölümde aktarıldığı üzere, genellikle kullanıcıya zarar vermek ya da reklam amaçlı olarak gönderilen, bazı potansiyel tehlikeler içeren yığın iletilerin, doğrudan gelen kutusuna girmesini engelleyen sistemlere yığın ileti engelleme sistemi denilmektedir (Keleştrmur, 2015, 326) (Çifci, 2017, 231).

E-postalar sunucu tarafından gönderildiğinde bir dizi filtreden geçmektedirler. Bu filtrelerden bazıları, Bayes filtresi, gelişmiş buluşsal filtre, beyaz liste/kara liste ve URL filtresi olarak sıralanmaktadır. Bu bileşenler, az miktarda bellekle son derece hızlı taramalar gerçekleştirebilmektedir. Sezgisel filtre ile iletiler spam özellikleri açısından kontrol edilmektedir. WBL desteği ile güvenli olarak belirtilen adreslerden gelen e-postalara izin verilirken, kara listeye alınan adreslerden gelen e-postalar reddedilmektedir. URL filtresiyle, birçok spam e-posta genellikle reklamlarla ve bir şeyler satın alabileceğiniz çeşitli web sitelerine bağlantılarla doludur. Anti-spam etkinliği ile URL filtrelemeyi desteklemek için yeni bağlantılar eklenmekte veya kaldırılmaktadır (İkizler ve Başar, 2006: 91).

### 2.3.4. İçerik filtreleme sistemi ve bal küpü:

İletişim ağı ya da bilgisayara giren ve çıkan tüm trafiği izleyerek, istenmeyen trafiği engelleyen sistemlere içerik filtreleme sistemi denilmektedir (Çifci, 2017, 234). İçerik filtreleme sistemleri, bir kurum çalışanının fotoğraf paylaşmasını, sohbet programı çalıştırmasını, belirlenmiş kelime gruplarının gönderilmesini veya sosyal medya hesaplarının kullanılmasını engelleyebilmektedir (Keleştemur, 2015, 325).

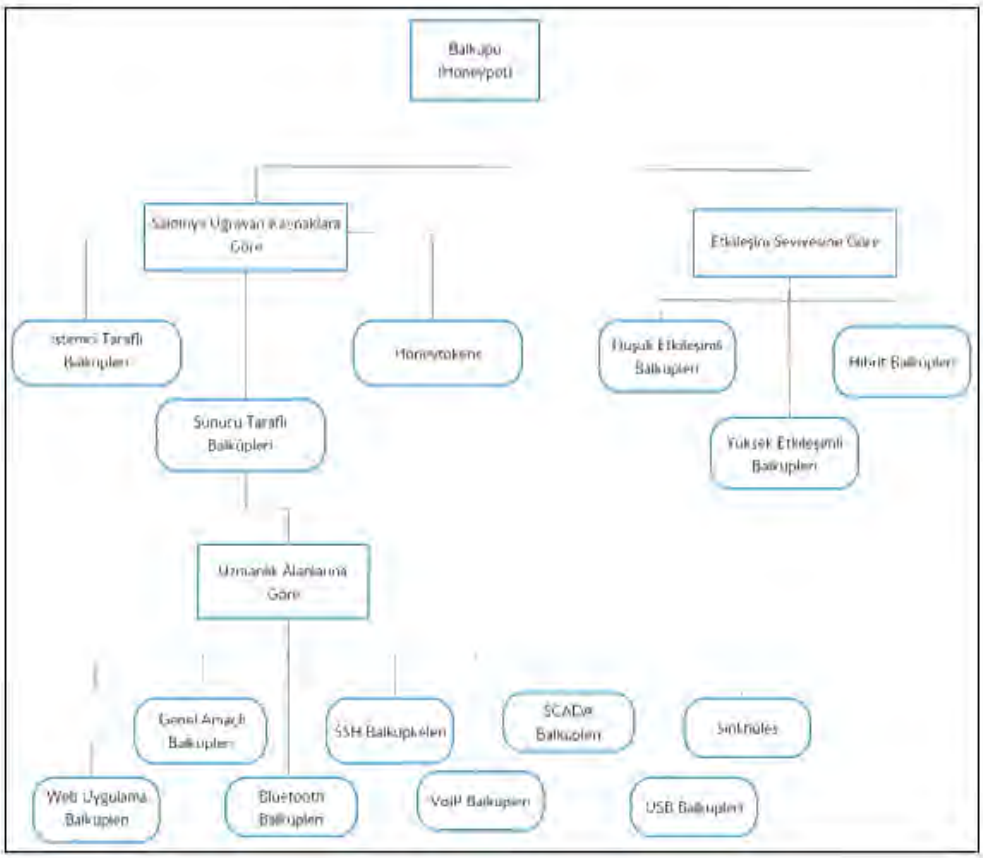
İçerik filtreleri, iç ağdan dış ağa doğru gerçekleşen bağlantıların tanımlanan kurallara uyup uymadığını kontrol eden ve istenmeyen web sunucularına bağlantıya engel olan sistemler olarak açıklanmaktadır. İçerik filtreleri, hedef sunucuya yoğunlaşmaktadır. Gelen paketlerin içeriğini analiz eden içerik filtrelerinin esas görevi, kullanıcıların güvenliği riske sokan web sunucularının erişimini önlemektedir. İçerik filtreleri güvenliği artırmaya yardımcı olsa da verilerin izinsiz olarak kuruluşun dışına iletimini engelleyememektedir. İyi niyetli olmayan kullanıcılar, başlattıkları web sunucularına kurum verilerini iletebilmektedir. İçerik filtreleri, hassas bilgilerin ağ üzerinden akışını engelleyememektedir (Arda, 2020: 48).

Bilişim sistemine ya da sistem içindeki verilere yetkisiz erişen saldırgan ya da uygulamaları tespit edebilmek amacıyla, sistemin bir parçası gibi görünen ancak aslında tuzak olarak tasarlanmış sistemlere bal küpü denilmektedir (Keleştemur, 2015, 325). Bal küpleri saldırganları öncelikle kendi üzerine çekmekte ve böylelikle kasıtlı olarak bırakılan açıklardan sızan saldırganları ve saldırı davranışlarını tespit etmeye yarayan yazılım çeşitleridir (Gökırmak vd, 2011, 1).

Saldırganları saptamak, saldırılarını incelemek ya da saldırganların hızını kesmek, yanlış bilgiye erişmek gibi kurulum amacına bağlı olarak yapısı farklılık gösteren ağ sistemlerine balküpü denmektedir. Balküpü, bilgi sistemlerine yönelik saldırıları tespit etmek için kurulan tuzaklar olarak da tanımlanmaktadır (Soysal vd., 2015:56).

Balküpü bir hile sistemi ağıdır. Açık kaynak kodlu yazılımlardan faydalanarak bu gibi sistemlerin kurulması ve yenilerini geliştirilmesi mümkün görülmektedir. Balküpleri organizasyon amaçlarına, saldırganla etkileşimlerine vb. göre gruplandırılmaktadır (Karaarslan vd., 2008).

Şekil 2.3.'te ENISA (European Union Agency for Network and Information Security) tarafından gerçekleştirilen grupalndırmanın şema üzerinde gösterimine yer verilmiştir.




**Şekil 2. 3**. *Balküplerinin gruplandırılması (Grudziecki vd., 2012).*

Etkileşim derecesine bağlı olarak balküpleri düşük ve yüksek etkileşimli iki alana ayrılmaktadır. Düşük etkileşimli bal küpleri, sunucu tarafı veya kullanıcı tarafı hizmetinizi taklit etmektedir. Düşük etkileşimli bal küplerinin kurulması ve idare edilmesi zor olmamaktadır. Fakat, keşifsel araştırma süreçleri için uygun görülmemektedir. Saldırganlar, düşük etkileşimli balküplerini basit bir şekilde saptayabilmektedir (Grudziecki vd., 2012: 71).

Yüksek düzeyde etkileşimli bal küpleri, gerçek sistemler ve kaynaklar sunan araçlar olarak nitelendirilmektedir. Bu sistemlerde taklitten ziyade gerçek sistemlerden yararlanılmaktadır. Fakat sanal sistemler sayesinde taklit de yapılabilmekte ve genel uygulamalarda sanal sistemler kullanılmaktadır. Bu konsept ile sanal sistemlerde

saldırgan etkileşim sınırı bulunmamaktadır. Bu, sızma ve enjeksiyon işlemlerinin eksiksiz bir analizini sağlamaktadır. Gerçek davranış, yüksek düzeyde etkileşimli bal küplerinin ana avantajıdır. Bu sistemler ile sıfır gün sapması gibi sapmaları tespit etmek mümkündür (Grudziecki vd., 2012: 71). Etkileşim arttıkça bal küpüne el konulma riski artarken diğer yandan saldırgan ve saldırı hakkında daha fazla bilgi saldırganın gerçek sistemle etkileşimi yoluyla elde edilmektedir (Gökırmak vd., 2009: 46).

Balküpü tasarımında özen gösterilmesi gerekli olan bir konuda da balküpünün saldırganlarca algılanmamasını sağlamak olarak ifade edilmiştir. Saldırgan, etkileşim kurduğu sistemi bir balküpü şeklinde değil gerçek bir servis biçiminde algılamaktadır. Balküpü olabildiğince genel görünmelidir. Genel olarak bakıldığında bal küpü kullanmanın amaçları; saldırganların sistemlere ulaşmak adına ne şekilde çalışma gerçekleştirdiğini ve giriştiğini öğrenmek olarak belirtilmiştir (Even, 2000: 64).

### 2.3.5. Hava boşluğu ve ağ erişim kontrol sistemi:

Farklı gizlilik derecesi olan iki ağ arasına yerleştirilen hava boşluğu sistemi, söz konusu ağlar arasında doğrudan fiziksel bir bağlantı kurulmadan, güvenli bir şekilde veri akışının yapılmasını sağlamaktadırlar. Gizlilik derecesi düşük olan ağ ile daha yüksek gizliliğe sahip ağ, fiziki olarak birbirine bağlanmadığı ve veriler hava boşluğu sistemi aracılığıyla sağlandığı için ağlar arası trafik güvenli hale getirilmektedir. Hava boşluğu sistemleri; askeri ağlar, havacılık ağları, nükleer santraller, finansal bilgisayar sistemleri, SCADA sistemleri gibi kritik alanlarda sıkça kullanılmaktadır (Kelestemur, 2015, 326).

Hava boşluğu sisteminin, yerel alan ağlarının güvenliğini sağlamak için en etkili yöntem olduğu ifade edilmiştir. Fakat, LAN'ın İnternet'e erişememesi, LAN'ın fonksiyonelliğini büyük oranda azaltmaktadır. Bu nedenle güvenlik düzeyi fazla olmasına karşın ağın fonksiyonelliğini düşmektedir. Hava boşluğu sistemleri gizlilik düzeyini artırsa da kullanıcıların kurumda işledikleri verileri dışarıya göndermeleri kolay olmadığı için tercih edilen bir yöntem olarak görülmemektedir. Hava boşluğu sistemleri kurumlara ilave yükler oluşturmaktadır. Bunlar şu şekilde sıralanmıştır (Kaya, 2013: 146):

- LAN ve İnternet için farklı ağlar kurma,
- Her ağ için ağ ekipman harcaması,
- Kullanıcıların LAN ve İnternet için farklı bilgisayarlara gereksinim duyması

Bir ağa bağlı olan bilgisayarın çalıştırılması durumunda devreye girerek, bilgisayarın ağa erişiminden önce, işletim sisteminin güncelliğini, yazılımların durumunu, antivirüs programı gibi güvenlik yazılımlarının güncelliğini, güvenlik için önceden belirlenmiş belirli dosyaların varlığını kontrol ederek bunların bir ya da birkaçının güvenlik için risk oluşturabilecek durumda olması halinde bilgisayarın ağa erişimini engelleyen sistemlere ağ erişim kontrol sistemleri denilmektedir. Bu sistemler, zararlı yazılımların ağ içine girmesini engellemenin yanında yetkisiz erişimleri de engellemektedir (Keleştemur, 2015, 324) (Çifci, 2017, 233-234). Ağ erişim kontrol sistemleri, kuruluş politikalarına uyumlu olmayan sistemlerin ağa eklenmesine engel olmak için kullanılmaktadır. Bu, üçüncü taraf sistemlerin ve yetersiz güvenlik koşullarına sahip sistemlerin iç ağı tehdit etmesini engellemektedir (Afacan, 2021: 2).

### 2.3.6. Adli bilişim ve uç nokta güvenliği sistemleri:

Bilgisayar ve yan donanımları, bilgi depolayan elektronik cihazlar, yönlendirici ve anahtar gibi iletişim ağı aktif cihazları, CD, DVD, harici bellekler gibi veri depolama cihazları gibi donanımlarda saklanan ya da bu donanımlar aracılığıyla iletilen ya da alınan ses, görüntü, veri, bilgi ya da bunların her türlü bileşiminden oluşan bilişim nesnesinin, mahkemede yasal olarak geçerli bir şekilde toplamaya ve analiz etmeye yarayan donanım ve yazılımlara adli bilişim sistemleri denilmektedir (Keleştemur, 2015, 326) (Çifci, 2017, 233). Bu sistemler ağ trafiğini pasif olarak yakalamakta ve trafiğin derin paket incelemesini gerçekleştirme yeteneği sağlamaktadır. Böylece sistemde oluşabilecek durumlar ve problemler detaylı şekilde analiz edilmektedir. Trafik günlüğe kaydedilirken, bir sızıntı durumunda verilerin doğası hakkında bilgi sağlayarak veri sızıntısı önleme sistemlerini desteklemektedir (Özen ve Özocak, 2015: 1). Bu sistemler sabit disklerden ve harici belleklerden imaj alabilmekte, verileri kurtarabilmekte, parolaları kırabilmekte ayrıca şifreleme analiz sistemi, imaj dönüştürme ve yazma engelleme gibi özellikler içerebilmektedir (Keleştemur, 2015, 326).

İçerisinde güvenlik duvarı, antivirüs programı, saldırı tespit/önleme yazılımı, cihaz kontrol yazılımı, ağ erişim kontrol sistemi, şifreleme yazılımı, veri kaçağı önleme ve uygulama kontrol yazılımı gibi çok sayıda güvenlik yazılımını barındıran (Çelik ve Çeliktaş, 2018: 105), böylelikle bilişim sistemlerinin bir kurum içinde tek bir merkezden

yönetilmesini ve kontrol edilmesini sağlayan bütünleşik güvenlik sistemlerine uç nokta güvenliği sistemi denilmektedir (Keleştemur, 2015, 321) (Çifci, 2017, 234-235).

### 2.3.7. Şifreleme sistemleri ve steganografi:

Veri güvenliğinin önemli bir parçası olan şifreleme sistemleri, kurumsal ya da bireysel hassas bilgilerin kötü amaçlı yazılımlardan ve erişim yetkisi olmayan kişilerden korunmasını sağlamaktadır. Bilgisayar ve bilişim sistemlerinde yer alan veri, dosya ve dizinler iletişim ağ trafiği, e-posta ve mesajlara güvenlik için yalnızca özel bir şifre anahtarı ile erişim yetkisi tanınmaktadır. Bu şifre anahtarı olmadan, verilerin orijinal içeriğine ulaşılamamakta ve böylelikle korunmak istenen belgeler yetkisiz ya da kötü amaçlı kişiler ve yazılımlarca elde edilememektedir (Keleştemur, 2015, 317-328).

Şifreleme, net bir mesajı anlamsız bir mesaja dönüştürme işlemi olarak tanımlanmaktadır. Başka bir deyişle, mesajın matematiksel yöntemlerle şifrelenmesini içermektedir. Verilerin gizliliğini, bütünlüğünü ve güvenliğini garanti etmektedir. Mesajın anlaşılır biçimi açık veya net mesaj olarak açıklanmaktadır. Açık mesajın matematiksel metıtlardan faydalanarak belirli işlemlere tabi tutulmasından sonra elde edilen mesajın anlamsız durumu şifreli mesaj şeklinde tanımlanmaktadır. Günümüze bakıldığında dijital iletişim kanallarından yararlanılmaktadır. Bu iletişim kanallarında özel bilgi ve sırlar paylaşılmaktadır. Esasen, bütün iletişimler güvenli olmamakta ve siber suçlular tarafından manipüle edilebilmektedir. Bu nedenle, modern kriptografi acil bir gereklilik halini almıştır. Hasas ya da gizlenmesi gereken bilgilerin muhafaza edilmesi mecburi duruma gelmiştir. Bu sebeple kimi zaman bilginin okunamaz bir formata çevrilmesi gerekmekte ve böylelikle söz konusu bilgiye sadece yetkili kişiler erişmektedir (Çelik, 2021: 53).

Eski Yunanca'da "gizlenmiş yazı" anlamına gelen steganografi, genel olarak bilgiyi gizleme işlemi olarak tanımlanmaktadır. Steganografide öncelikle elde edildiğinde dikkat çekmeyecek bir görsel seçilmektedir. Ardından gizlenmek istenen dosya ya da görsel veri, steganografi yazılımı aracılığıyla ana görsel içine saklanmaktadır. Steganografi yazılımı görsel içine veri saklama işini, seçilen orijinal görsel ile arasında insan gözünün ayırt edebileceği bir fark yaratmadan sağlamaktadır (Keleştemur, 2015, 328) (Çifci, 2017, 235). Bu tekniğin en önemli ve büyük avantajı bilgiyi gören ya da bir

şekilde elde eden saldırganın gördüğü şeyin önemli bir veri olduğunu fark edememesidir (Morkel vd., 2006, 3).

Steganografi artık verilerin çeşitli elektronik ortamlarda entegrasyonu ile ilişkilendirilmektedir. Steganografi ile daha yaygın olarak kullanılan şifreleme arasındaki fark, şifrelemenin verileri bulanıklaştırıp karartmasına karşın, steganografinin verileri tamamen bulanıklaştırmasıdır. Gizli ya da açık veriler, ana bilgisayar dosyasındaki küçük önemsiz bitlerin değiştirilmesiyle karıştırılmaktadır. Steganografi, bilgiyi diğer bilgilerle birlikte gizleme sanatı olarak nitelendirilmektedir. Şifreleme, verileri anlaşılmaz bir formata dönüştürerek gerçek verilere erişimi zorlaştırmakta, ancak iletişimin gizliliğini garanti etmemektedir. Steganografi bilginin varlığını gizlemek ya da bilgiyi fark edilmeden diğer verinin içerisine yerleştirmeyi hedeflemektedir. Steganografi, kriptografiye yakın olmasına karşın kriptografiden çok farklılık göstermektedir. Kriptografi iletinin içeriğinin muhafaza edilmesiyle alakadar olurken steganografi mesajın varlığının gizlenmesiyle de ilgilenmektedir. Bundan dolayı steganografi bir şifreleme yöntemi olmamakta, şifrelemeyi tamamlayıcı bir unsur olarak nitelendirilmektedir (Ocak, 2021: 61).

### 2.3.8. Elektronik imza ve eletromanyetik güvenlik:

Elektronik imza, elektronik ortamda taşınan verilerin, onu gönderen kurum veya kişiye ait olduğunu doğrulamakta ve verilerin başka bir kişi tarafından gönderilmemesini sağlamaktadır. Elektronik imza, gönderenin kimliğini, elektronik belgenin orijinalliğini ve güvenilirliğini kesin olarak teyit etmektedir. Elektronik olarak imzalanmış bir belgenin göndericisi, gönderildiğini ve alıcının belgeyi aldığını inkar edememektedir. İnternet üzerinden gönderilen verilerin güvenliği böylelikle elektronik imza kullanımıyla sağlanabilmektedir. Elektronik imza, bir veri bloğu ile ilgili hesaplanan özet bilgilere verilen isim olarak belirtilmiştir (Çiçek, 2008: 78). Elektronik imzaların; imza dosyaları, biyometri imzalar ve sayısal imzalar gibi çeşitleri bulunmaktadır (Ermiş, 2006, 123).

Bilgisayar klavyelerinde basılan tuşlar, ekrana yansıyan görüntüler, ağ üzerinden geçen veriler, modem kabloları ve daha çok sayıda cihaz ve teçhizattan birbiriyle bağlantılı elektromanyetik salınımlar yayılmaktadır. Yeterli donanım ve yeteneğe sahip olunduğu takdirde bahsi geçen tüm bu veriler yaklaşık 2 km gibi bir mesafeden

kaydedilerek, ele geçirilebilmekte ve uygun bir işleme evresinden geçirildikten sonra kullanılabilir hale getirilebilmektedir (Keleştemur, 2015, 356-357).

Güç hatları, bilişim sistemleri veya sinyal hatları aracılığıyla iletilen elektromanyetik sinyallerin ya da bilişim teçhizatlarından hava veya kablolar vasıtasıyla ışıma yoluyla sızan bu sinyallerin, kötü amaçlarla elde edilerek yakalanmasına ve yönlendirilmiş enerji saldırılarına karşı koruma sağlayan güvenlik tedbirlerine elektromanyetik güvenlik denilmektedir. Diğer adı TEMPEST karşı tedbirleri olan bu yazılımlar, fiziksel ya da elektromanyetik yakalama yoluyla verilerin yetkisiz kişilerce ele geçirilmesini önlemek amacıyla, saldırıya hedef olabilecek yollar boyunca zafiyetlere karşı koruma sağlamaktadır ( Çifci, 2017, 242-243).

Başka kişilerce erişilmesi arzulanmayan gizli verileri saklayan, taşıyan ve işleyen cihazlardan ortama yayılan ve kontrol edilemeyen elektromanyetik enerji, bu gizli verileri kapsayan sinyalleri çerçevelemektedir. Bu sinyaller başkalarınca erişilip, kapsadığı gizli bilgi çözülebilmekte ve bu yüzden de bir veri güvenliği sorunu oluşabilmektedir. Bundan dolayı bu durum bir TEMPEST problemi olarak nitelendirilmekte ve bu sorunun çözülmesinde TEMPEST çalışmalarından faydalanılmaktadır. TEMPEST konusundan belirlenecek tedbirlerde ilk başta gizlilik dereceli verinin hangi yöntemlerle istenmeyen alanlara gittiğini saptamaya gerek duyulmaktadır. Veri içeren bu istenmeyen kaçaklar iki çeşit istenmeyen alanlara gidebilmektedir. Bu alanlar, "*uzaysal ışıma ve elektriksel iletkenlik yolu*" şeklinde belirtilmektedir. Bu kaçaklara engel olunabilmesi adına belirlenmesi gerekli olan birtakım tedbirler vardır. Bu tedbirlerin tümü kırmızı ve siyah sistemlerin, cihazların ve kabloların bazı kurallar kapsamında birbirinden ayırt edilmesi ve oluşabilecek bütün kaçış yöntemlerinin düşürülmesini çerçevelemektedir. Bu ayrım yapılırken göz önünde bulundurulması gerekli olan birtakım durumlar vardır. Bu durumlar şöyle sıralanmıştır (Bayraktar, 2014: 20):

- Binaların muhtemel veri kaçaklarına yönelik ne denli bir muhafaza sağladığını tespit etmek,

- Gerekli durumlarda kırmızı bölgelerin elektromanyetiksel şekilde izolasyonunu sağlamak,

- Sistemin topraklamasını etkili bir şekilde gerçekleştirmek,

- Güç ve veri kablolarını doğru türde kullanarak uyumlu hatları çekmek,
- Gerekli durumlarda güç ve işaret hatları konusunda filtrelerden faydalanmak
- Cihazları teste sokarak uygun alanlarda kullanımını sağlamak.

## 2.4. Siber Aktörler:

Çalışmanın bu başlığı altında ele alınacak aktörler bilgi eksikliği olmaması amacıyla tek bir yaklaşıma bağlı kalmaksızın, geniş bir bakış açısıyla değerlendirilecektir.

### 2.4.1. Hackerlar:

Hack kavramı, genel olarak siber suçluların yaptığı tüm eylemleri karşılamak için kullanılıyor olsa da aslında bu yaklaşım gerçeği tam olarak ifade etmemekle birlikte toplumda yanlış bir algıya yol açmaktadır (Altınkaynak, 2017, 1). Doğru olmayan bu genel yaklaşım, hackerların da kendi amaçları doğrultusunda siber saldırı yapan, bilişim sistemlerine ve bu sistemler aracılığıyla insanlara zarar veren kişiler olarak bilinmesine sebep olmuştur. Nitekim birçok sözlükte de bu olumsuz anlamı ilk sırada vermiştir. Ancak hacker, kavram olarak ve köken itibariyle bilgisayar uzmanı anlamına gelmektedir (Akyeşilmen, 2018, 71). Elbette bu uzmanlar arasında kötü amaçlı hareket edenler de bulunmaktadır. Bu doğrultuda Ericson hackerı "hem kod (program) yazan hem de onu kötüye kullanan kişi" olarak tanımlamıştır (Ericson, 2008, 5).

Genellikle son derece yetenekli ve bilgili kişiler olan hackerlar; eğlenmek, gösteri yapmak, bilgi çalmak, para çalmak, bilişim sistemlerine zarar vermek ya da sistemin güvenlik testini yapmak, reklam yapmak veya siyasal içerikli eylemler amaçlayabilmektedir. Kimi zaman bireysel kimi zaman da topluluk halinde hareket edebilen hackerlar bu farklı amaçları sebebiyle farklı kategorilere ayrılmıştır. Aşağıdaki tabloda hackerlara türlerine göre kategorilerilere ayrılarak yer verilmiştir.

**Tablo 2. 4.** *Hacker türleri (Sandilaç, 2021: 61)*

| Hacker Türleri | Açıklamaları |
|---|---|
| **Beyaz Şapkalı Hackerlar** | Bilişim suçlusu olan kötü niyetli bireylerin kullandığı teknik ve yöntemleri etkin bir biçimde bilirler. Siber saldırganların faaliyetleri esnasında kullandıkları araçları ve yazılımları tanıyan, aynı bilgi ve beceriye sahip olmaktadırlar. Kötü niyetli olmayan siber güvenlik uzmanları olarak nitelendirilmektedir. |
| **Siyah Şapkalı Hackerlar** | Bilgisayar korsanları şeklinde de bilinen siyah şapkalı hackerlar, sisteme ve ağa ulaşmak, verileri çalmak, değiştirmek ya da silmek isteyen kötü niyetli kişilerdir. Saldırılarında ortak hackleme işlemlerinden faydalanmışlardır. Yasaları ihlal ederler ve suça yatkındırlar. |
| **Gri Şapkalı Hackerler** | Kullandığı yasadışı yollarla sistemin eksiklerini bulan fakat bulduğu açıkları zarar vermek için kullanmayan hackerlardır. Bunlar saptadıkları açıklar ile kullanıcılara hasar vermezler. |
| **Lamerler** | Tecrübe ve bilgiden mahrum olduklarından dolayı bilgisayar korsanlığı dünyasındaki en riskli bireyler şeklinde nitelendirilmektedir. İnternette yer alan herhangi bir kötü amaçlı aracın ya da yazılımın amacını bilmeden kullanırlar. |
| **Yeşil Şapkalı Hackerlar** | Bunlar bilgisayar korsanlığı dünyasının amatörler hackerlarıdır. Fakat bunlarla lamerler arasında bir fark bulunmaktadır. Hackleme hususunda çok az bilgiyi bulundurmaktadır. |
| **Kırmızı Şapkalı Hackerlar** | Bunlar da beyaz şapka korsanları gibi faaliyetlerini sürdürmektedir. Siyah şapka bilgisayar korsanlarının yaptığı saldırılara karşı durmak için çaba sarfetmektedirler. |

Tablodan da anlaşılacağı üzere hackerların bazıları kötü niyetliyken, bazıları da zararsız olmaktadır (Yegen, 2014: 119).

### 2.4.2. Siber ajanlar ve sosyal mühendisler:

Hackerların çoğundan faklı olarak girdikleri bilişim sistemine zarar vermeyen siber ajanlar, siber uzayda istihbarat yöntemleri kullanarak casusluk faaliyetleri gösteren kişilere denilmektedir. Diğer adı siber casus olan siber ajanlar, Truva atı, solucan, klavye kaydedici gibi programlar kullanarak sızdıkları sistem sahibinin kişisel bilgi ve verilerine ulaşmakta, ardından genellikler arkalarında iz bırakmadan topladıkları bilgiyi üst makamlarına raporlamaktadırlar.

Bir önceki bölümde sosyal mühendislik başlığı altında aktarıldığı üzere, ileri derece sosyoloji ve psikoloji bilgisine vakıf olan sosyal mühendisler, diğer adıyla toplum mühendisleri, aynı zamanda bilişim sistemleri hakkında da bilgi sahibi kişilerdir. Bazı sosyal mühendisler bir hacker kadar teknik bilgiye sahip olsa da saldırılarını yazılımsal ya da donanımsal olarak değil ağırlıklı olarak insan doğasının zafiyetlerine dayanarak gerçekleştirmektedir. Saldırılar kimi zaman sadece sosyal mühendislik aşamasında bırakılırken kimi zaman da sosyal mühendislerin elde ettiği bilgiler sayesinde daha büyük ölçekli saldırılara olanak sağlayacak zemin hazırlanmaktadır (Keleştemur, 2015, 212-213). Aynı durum siber ajanların ele geçirdiği bilgiler için de geçerli olmaktadır. Bu sebeple siber ajanlar ve sosyal mühendislerin faaliyetleri tüm aktörlerin siber güvenliklerini sağlamaları açısından son derece önemli bir hal almaktadır. Böylesi bir güvenlik soeunyla karşılaşmamanın yolu sisteme yüklenen her uygulamanın gerçek ve zararlı olup olmadığının kontrol edilmesinden geçmektedir (Bayraktar, 2014: 25).

### 2.4.3. Kriptocular ve kripto analizciler:

Tıpkı anahtar-kilit ilişkisinde gibi işleve sahip kriptocular ve kripto analizciler, bilgilerin şifrelenerek gizlenmesi ve gizlenen bilgilerin anahtar şifresinin bulunarak deşifre edilmesi üzerine çalışmaktadırlar. Özellikle devlet nezdinde korunması gereken bilgi ve verilerin kriptografi yöntemiyle şifrelenerek, düşman eline geçse dahi kullanılamaz hale gelmesini sağlayan kriptocular, bu açıdan büyük önem taşımaktadır. Aynı şekilde, ele geçirilen bilginin deşifre edilip istihbarat faaliyetlerinde kullanılması, daha büyük çapta siber saldırılar düzenlenmesi, sürmekte olan konvansiyonel ya da siber savaşta gelecek hamlelere yön verilmesi ve dolayısıyla, düşmanı yenilgiye uğratma noktasında kripto analizciler de son derece büyük bir rol oynamaktadırlar. Bu sebeple kriptografinin her iki tarafı da devletlerin güvenlikleri açısından hayati önem

taşımaktadır. Nitekim bu yöntemler II. Dünya Savaşı'ndan itibaren son derece etkin bir şekilde kullanılmaktadır.

### 2.4.4. Yazılımcılar ve siber tehdit analistleri:

Yazılımcılar ve siber güvenlik analistleri, siber risklere engel olmak, saptamak ve yönetmek için farklı teknolojiler ve işlemlerden faydalanarak bir kurumun korunmasına yardımcı olmaktadır. Bu koruma işleminde bilgisayarlar, veriler, ağlar ve programlar yer almaktadır. Genel olarak, müşterilerie danışmanlık hizmetlerinin sunulması ve kurum-kuruluşların güvenliğinin korunmasında rol üstlenmektedirler (Poyrazoğlu, 2022: 135).

Her türden siber silahlar geliştirerek düşmana saldırıda bulunmak ya da bilişim sistemlerinin korunmasını sağlayacak güvenlik yazılımları geliştirerek siber alandaki saldırıların önüne geçebilmek için yazılımcılara ihtiyaç duyulmaktadır. Bunlar dışında yazılımcılar, askeri ve istihbarat birimlerinin istediği özel amaçlara hizmet eden programlar da geliştirebilmektedir. Bu sebeplerle, tıpkı kriptocular ve kripto analizcilerde olduğu gibi bir devletin hem siber taarruz kabiliyet ve kapasitesini hem de siber güvenliğini arttırabilmesi açısından yazılımcılar büyük bir rol üstenmektedir.

Bilişim sistemlerini analiz ederek var olan ya da olası siber tehditleri tespit edip, siber saldırılara karşı sistemin korunmasını sağlayan siber tehdit analistleri de genellikle yazılımcılar gibi programlama bilgisine sahip olmaktadır. Gerçekleşen siber olayları tespit eden, sistem ve ağ açıklarını tespit ederek riskleri ortaya koyan, olası siber saldırılara karşı çözüm üreten ve gelişen olaylara anında müdahale ederek tehlikeyi bertaraf eden siber tehdit analistleri de siber alanda bu görevleriyle büyük rol oynayan aktörler arasında yer almaktadır. Üstelik siber risklerin tespit edilmesi ve olası ataklara karşı öngörü ve önleme önerileri, islenecek siber güvenlik politikalarına yön verilmesi açısından da büyük öneme sahiptir (Keleştemur, 2015, 218-220).

### 2.4.5. Ağ ve sistem uzmanları:

Ağ ve sistemlerin sorunsuz ve etkin bir şekilde çalışmasında görev alan bu kişiler, meydana gelen sorunların tespit edilmesi ve kaynağının bulunarak çözüm üretilmesi konusunda da rol üstlenmektedirler. İhtiyaç analizi yaparak sistem ve ağ alt yapısında kullanılacak doğru elemanları belirlemekte, planlamakta ve kurulumlarını gerçekleştirdikten sonra da test, güncelleme ve bakım gibi işlerden de sorumlu

tutulmaktadırlar. Üstlendikleri görevleri doğru ve etkin bir şekilde gerçekleştiremedikleri takdirde büyük çapta siber sorunların meydana gelmesi ihtimali yükselmektedir. Gelişen teknolojiden ve bu sayede artan güvenlik sorunlarının takibinden ve güvenlik politikalarından da sorumlu olmaları, ağ ve sistem uzmanlarının siber alandaki önemini artıran diğer faktörler arasında sayılmaktadır.

Ağ ve sistem uzmanlığı günümüzdeki teknolojik gelişmelerinin en üst düzey performans ile kullanımını hedeflemektedir. Artık işletmeler yenilenen teknolojiyi yakından gözeterek çalışma şartlarını ve bu normları kendilerince yeni bir sisteme yerleştirmektedir. Bu süreçte bilgisayar sistemleri, ağ sistemleri, güvenlik sistemleri konusunda bilgili ve uzman kişiler devreye girmektedir. Bu durum fiziksel çalışma ortamında değişiklik oluşturarak bilgiye zaman ve mekan farketmeksizin ulaşımı sağlayarak çalışma standartlarını üst seviyelere çekmektedir (Güntay, 2018: 82).

# ÜÇÜNCÜ BÖLÜM

## 3. SİBER AKTÖRLERİN SİBER DENGELEME YAPILANMALARI VE TEMEL OLAYLARDA SİBER DENGELEME POLİTİKALARI

Bu bölümde öncelikle siber alanda rol oynayan aktörlerin bu alanda oluşturduğu yapılanmalar ele alınacaktır. Ardından siber alanda meydana gelen temel olaylara yer verilecektir. Nihayetinde genel bir değerlenme ile siber dengeleme politikalarına dair bir sonuca ulaşılacaktır.

### 3.1. Ülkeler ve Uluslararası İşbirlikleri Çerçevesinde Siber Dengelemeye Yönelik Temel Yapılanmalar:

#### 3.1.1. NATO:

Siber güvenliğe ilişkin olarak gerçekleşen en ciddi nitelikteki inisiyatifin NCIRC (NATO Computer Incident Response Capability) projesi olduğu ifade edilmektedir. Söz konusu proje 2005 yılından itibaren fonksiyonel olarak faaliyetlerini yürütmektedir. Bu proje kapsamındaki faaliyetler şu şekilde sıralamak mümkündür (NATO, 2016, s. 1):

- NATO ağlarının korunması
- Siber güvenlik desteğinin sağlanması
- Bilgi güvenliğine ilişkin olayların incelenmesi
- Altyapılara ilişkin olayların incelenmesi
- Acil Reaksiyon Timlerinin görevlendirilmesi

Çalışmanın ilerleyen kısımlarında detaylı bir şekilde incelenecek olan Estonya bilgi sistemlerine yapılan siber saldırılar sonrasında 2008 yılında NATO "*Müşterek Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defence Enter of Exellence-CCD CoE)*"ni kurmuştur. Mükemmeliyet Merkezi tarafından birçok faaliyet gerçekleştirilmektedir. Bu faaliyetlerden bazıları şu şekilde sıralanabilmektedir:

- Eğitim
- Teknik destek
- ARGE
- Danışmanlık

Bununla birlikte 2013 yılında "Siber Savaşa Uygulanacak Uluslararası Hukuk Hakkında Tallinn El Kitabı-The Tallinn Manual on the International Law Applicable to Cyber Warfare" yayınlanmıştır. Bu el kitabının hazırlanmasına ilişkin çalışmaları Mükemmeliyet Merkezi koordine etmiştir (NATO Siber Savunma Mükemmeliyet Merkezi, 2019).

NATO siber güvenliğe ilişkin çalışmalarını daha sonra da sürdürmüştür. Bu kapsamda "NATO'nun Muhabere ve Bilgi Teşkilatı (NCI Agency)" kurumunun içinde "Siber Güvenlik Hizmet Hattı (CSSL)" kurulmuştur. Bu hizmet hattı ile hayati öneme sahip faaliyetlerin idare edilebileceği öngörülmüştür (Çeliktaş, 2016, s. 75).

2010 yılında NATO Stratejik Konsept'i yayınlamıştır. Bu Konsept'te siber güvenlik konusu ele alınmıştır. Söz konusu Konsept'te siber tehdide ilişkin olarak şu ifadelere yer verilmiştir (NATO, 2010, s. 4):

- Daha sık ve organize bir biçimde siber saldırılar düzenlenmektedir. Bu durum da iş dünyası, ekonomi, devlet kurumları, ulaştırma ve diğer altyapı hatları üzerinde yüksek maliyetlere yol açmaktadır.
- Siber saldırıların milli refahı, güvenliği ve istikrarı tehdit etmesi mümkün olabilmektedir.
- Yabancı istihbarat servisleri ya da silahlı kuvvetlerinin söz konusu saldırıları gerçekleştirebilecek suçluları organize etmesi mümkündür.

Söz konusu Konsept'te siber savunma hakkında ise şu ifadelere yer verilmiştir (NATO, 2010, s. 5):

- Siber saldırıların engellenmesi, belirlenmesi, saldırılara karşı savunma yapılması ve saldırılardan sonra toparlanma yeteneği daha da geliştirilecektir.
- NATO planlama süreci ulusal siber savunmaya ilişkin yeteneklerin geliştirilmesi ve koordine edilmesi için kullanılacaktır.
- Tüm NATO birimleri merkezi bir siber koruma altına alınacaktır.
- NATO'nun sahip olduğu siber farkındalık diğer üye ülkelerle de paylaşılacaktır.

NATO kapsamında gerçekleştirilen çalışmalar sonucunda 2011 yılında "Siber Savunma Eylem Planı" hazırlanmış ve milli irtibat noktaları üye ülkeler tarafından bildirilmiştir. Bu kapsamda TÜBİTAK UEKAE milli irtibat noktası olarak Türkiye tarafından bildirilmiştir (Şentürk vd., 2012, s. 118).

2012 yılında Chicago Zirvesi gerçekleştirilmiştir. Söz konusu zirvenin Sonuç Bildirisi'nde daha da karmaşıklaşan ve gelişimi sürmekte olan siber tehditlere karşı iş birliği içinde mücadelenin yürütülmesi gerektiği ifade edilmiştir (Chicago Zirve Bildirgesi, 2012).

Galler Zirvesi ise 2014 yılında gerçekleştirilmiştir. Söz konusu zirvede ciddi nitelikte bir adım atılmış ve siber saldırıların 5. Madde kapsamında değerlendirilebileceği yani taraf ülkelerin bir veya daha fazlasına karşı yapılacak bir saldırının hepsine karşı yapılmış sayılacağı hususu belirtilmiştir. Ancak üye ülkelerin siber saldırı ile karşı karşıya kalması durumunda saldırıyı gerçekleştiren kişi ya da kişilerin nasıl belirleneceği ve saldırıya karşılık olarak ne yapılacağı hususları söz konusu Zirve'de ele alınmamıştır (Galler Zirve Bildirgesi, 2014). Bununla birlikte Zirve'de NATO tarafından yürütülecek görevlerin yerine getirilmesini kolaylaştıracak yeni siber eylem planının da yürürlüğe girdiği ifade edilmektedir. Bu kapsamda siber risk ve tehditlere ilişkin olarak meydana gelebilecek problemlere karşı özel sektörle işbirliğinin tesis edilmesi öngörülmüş ve "NATO Endüstri Siber Ortaklığı (The NATO Industry Cyber Partnership (NICP))"nın sahip olduğu amaçlar tanıtılmıştır (NATO, 2014).

Varşova Zirvesi ise 2016 yılında gerçekleştirilmiştir. Bu Zirve'de de tıpkı diğer zirvelerde olduğu gibi güvenlik konusu önem arz etmiştir. Söz konusu zirvede şu hususlar ele alınmıştır (Varşova Zirve Bildirgesi, 2016):

- Siber güvenliğe ilişkin konularda işbirliği tesis edilmesi ve diyalogun artırılması
- Siber saldırıların da normal saldırılar kadar zararlı olması
- Siber uzayın harekât mekânı olarak tanımlanması gerektiği
- Siber uzayda istikrar ve barışın sağlanabilmesi için çaba harcanması gerektiği

Brüksel Zirvesi ise 2018 yılında gerçekleştirilmiştir. Söz konusu Zirve'de siber tehditlerin gün geçtikçe daha yıkıcı ve karmaşık bir hale geldikleri ve bu nedenle de güvenlik açısından önemli bir tehdit oldukları ifade edilmiştir. Ayrıca siber savunmanın da NATO'nun en önemli görevleri arasında olduğu bu nedenle de tıpkı kara, deniz ve havada olduğu gibi siber uzayda da harekât düzenleme yeteneğine sahip olunması gerektiği hususuna yer verilmiştir. Bununla birlikte Belçika'da Siber Güvenlik Harekât Merkezi kurulacağı ifade edilmiştir. Söz konusu Merkez'in kurulmasının amaçlarının ise NATO'nun durumsal farkındalığa sahip olmasının sağlanması ve siber uzayda gerçekleştirilecek NATO harekâtlarının koordinasyonunun sağlanması olduğu belirtilmiştir (Brüksel Zirve Bildirgesi, 2018).

### 3.1.2. Avrupa Birliği:

Avrupa Birliği'nin siber güvenliğe büyük bir önem verdiği ve bu konuyu toplumun önemli bir parçası olarak gördüğü ifade edilmektedir. Ayrıca Avrupa Birliği tarafından birçok konuda ARGE ve prosedür oluşturma çalışmaları yapıldığı belirtilmektedir. Bu konulardan bazıları şu şekilde sıralanabilir:

- Ağ güvenliği
- Kişisel verilerin korunması
- E-ticaret
- Siber suçlar

Bu çerçevede 2013 yılında Siber Güvenlik Strateji Belgesi, Avrupa Birliği Komisyonu tarafından hazırlanmıştır. Söz konusu belgede dünyanın en güvenli altyapısına sahip olunması amacıyla bireylerin haklarının korunacağı ifade edilmiştir. Ayrıca en güvenli altyapıya sahip olabilmek için tüm kurum ve kuruluşlarla koordinasyonun sağlanacağı belirtilmiştir (Avrupa Birliği Komisyonu, 2013: 19-20).

"Avrupa Şebeke ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency-ENISA)" Avrupa Birliği'nde siber güvenlik alanında faaliyet göstermektedir. Söz konusu kurumun merkezi Atina'da yer almaktadır (ENISA, 2019a). ENISA'nın 2014 yılında 2004/460/EC numaralı karar ile kurulduğu ifade edilmektedir. ENISA'nın başlıca görevlerini ise şu şekilde sıralamak mümkündür (ENISA, 2019b):

- Avrupa Birliği'ndeki ülkelere, iş çevrelerine ve tüm kurum ve kuruluşlara bilgi güvenliğine ilişkin önerilerde bulunmak
- Avrupa'da gerçekleşen olaylara ve tehditlerin artmasına ilişkin veri elde etmek ve bu verilerin analizini yapmak
- En iyi uygulamalara yönelik bilgi alışverişine olanak sağlamak
- Avrupa Birliği'ne karşı siber tehditlere dair risk yönetimi ve risk değerlendirme olanağını artırmak
- Bilgi güvenliğine ilişkin iş birliği tesis edilmesini ve bu konudaki bilinç seviyesinin artmasını sağlamak
- Bilgisayar Olaylarına Müdahale Ekiplerine (Computer Emergency Response Team-CERT) teknik destek sağlamak ve eğitim hizmeti vermek

Türkiye'de ise TÜBİTAK–UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) tarafından oluşturulmuş olan TR-BOME'nin ve ulusal akademik ağ kapsamında TÜBİTAK ULAKBİM'in kurmuş olduğu ULAK-CSIRT'nin, akreditasyonu ENISA tarafından sağlanmıştır.

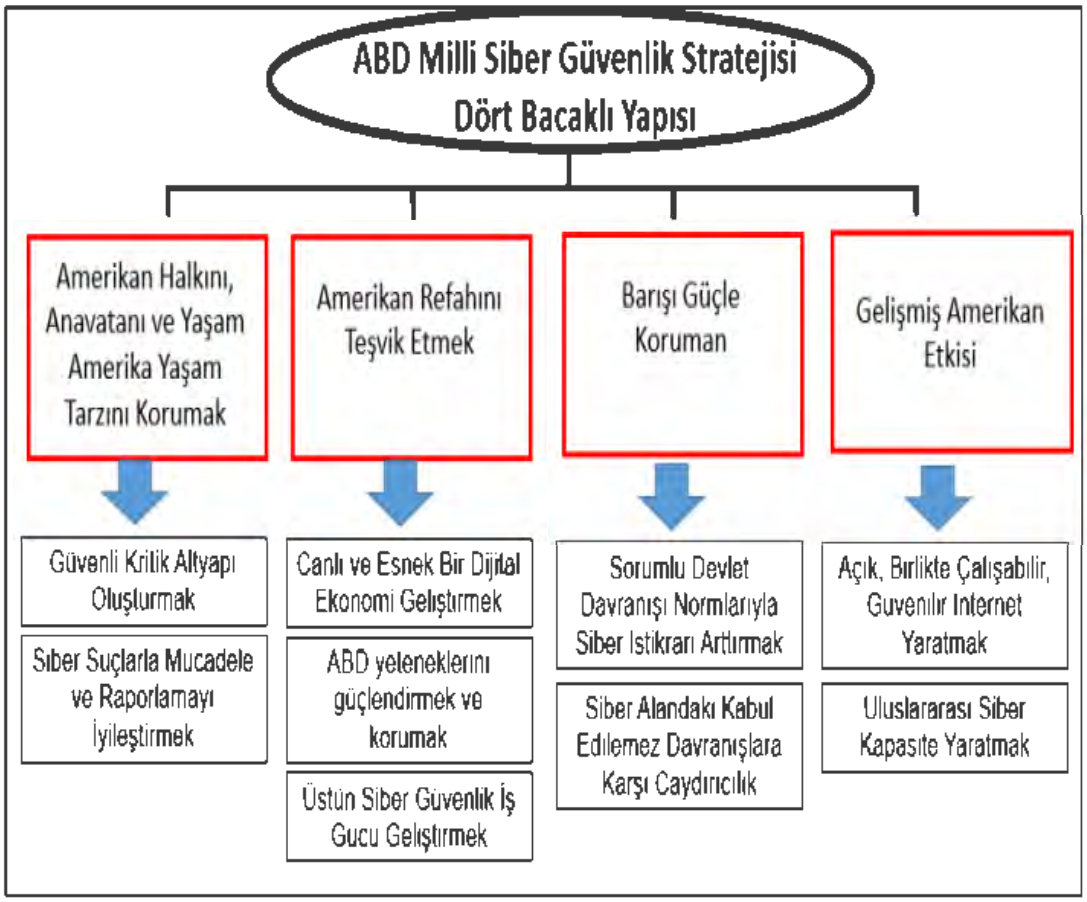
### 3.1.3. Amerika Birleşik Devletleri:

Amerika Birleşik Devletleri'nde siber güvenliğe ilişkin çalışmalar 90'lı yıllarda başlamıştır. Bu çalışmaların 2000'li yıllarla birlikte hızlandığı ifade edilmektedir (Wedermyer, 2012: 10). Bu konuya ilişkin olarak hazırlanan ilk kapsamlı belge "Siber Uzay Güvenliği İçin Ulusal Strateji (The National Strategy to Secure Cyberspace)"dir. Söz konusu strateji 2003 yılında hazırlanmıştır. Ayrıca belgede siber uzayda görev alması öngörülen kurumlar da belirtilmiştir. Sonraki süreçte de bu konuya ilişkin olarak çeşitli kurumların araştırmalar gerçekleştirdiği bilinmektedir (Korhan, 2018: 45).

ABD'nin karşı karşıya kaldığı en ciddi ekonomik ve milli güvenlik problemlerinden birinin siber güvenlik konusu olduğu eski ABD Başkanı Barack Obama tarafından da ifade edilmiştir. Bu durum siber güvenlik konusunun sahip olduğu önemi ortaya koymak açısından önemli görülmektedir (BBC, 2015). ABD'de siber güvenlik konusunda çeşitli faaliyetler gerçekleştiren üç temel kurum mevcuttur. Bu kurumları şu şekilde sıralamak mümkündür (Darıcılı, 2017a, s. 7):

- ABD Savunma Bakanlığı (United States Department of Defense)

- ABD İç Güvenlik Bakanlığı (The Department of Homeland Security)
- ABD Gizli Servisleri (FBI/CIA)




**Şekil 3. 1.** *ABD Milli Siber Güvenlik Stratejisi (ABD Ulusal Siber Güvenlik Stratejisi, 2018).*

ABD Savunma Bakanlığı 2008 yılında silahlı çatışma ya da savaş durumunda siber uzayın kontrolü görevini ABD Hava Kuvvetleri'ne vermiştir. Daha sonraki süreçte ise siber uzayın kontrolü görevinin yeni kurulacak olan Siber Komutanlığa (USCYBERCOM) verilmesi öngörülmüştür (Wedermyer, 2012). 2010 yılında söz konusu siber komutanlığın faaliyetlerine başladığı ifade edilmiştir (ABD Savunma Bakanlığı, 2010, s. 1).

ABD'nin dünya genelindeki en gelişmiş silah, araç ve gereçlere sahip olduğu bilinmektedir. Bu nedenle de ABD'nin siber tehditlerden en çok etkilenen ülkeler arasında ilk sıralarda geldiği belirtilmektedir. Dünya genelinde ABD'ye ait 88 ülkede 4.000 askeri üs bulunmaktadır. Bu üslerde 15.000 iletişim ağı ve 7.000.000'u aşkın bilgisayar bulunduğu ifade edilmektedir. Bununla birlikte bu altyapının tam ve doğru bir biçimde çalışabilmesi için yaklaşık olarak 90.000 personelin bulunduğu ve bunun için milyarlarca dolar kaynak kullanıldığı belirtilmektedir (Whitney, 2010). Bu büyüklükteki organizasyon, çeşitli ülkelerdeki ABD üstlerindeki iletişim ve bilgi altyapılarının korunması amacıyla ABD Stratejik Komutanlığı altında bir alt komutanlık şeklinde kurulmuştur.

Siber Komutanlığın görevleri ise şu şekilde sıralanabilmektedir:

- Bilgi ağlarının korunması
- Siber uzaydaki askeri faaliyetlerin idare edilmesi
- Siber uzayın sorunsuz bir biçimde kullanılmasının sağlaması

Siber güvenliğin sağlanması amacıyla, bilgi güvenliğine ilişkin konuların tek bir platformda toplanarak sinerji oluşturulması söz konusu Komutanlığın kuruluş amacını oluşturmaktadır (Jelinek, 2010). Siber Komutanlığın amaçları ise şu şekilde sıralanabilmektedir (ABD Savunma Bakanlığı, 2010: 1):

- Bakanlık sanal ağlarının güvenilir ve korumalı olmasının sağlanması
- Siber uzaydaki tehditlerin önlenmesinin sağlanması
- Siber uzay kapsamında gerçekleştirilecek harekâtların merkezi bir şekilde idare edilmesi

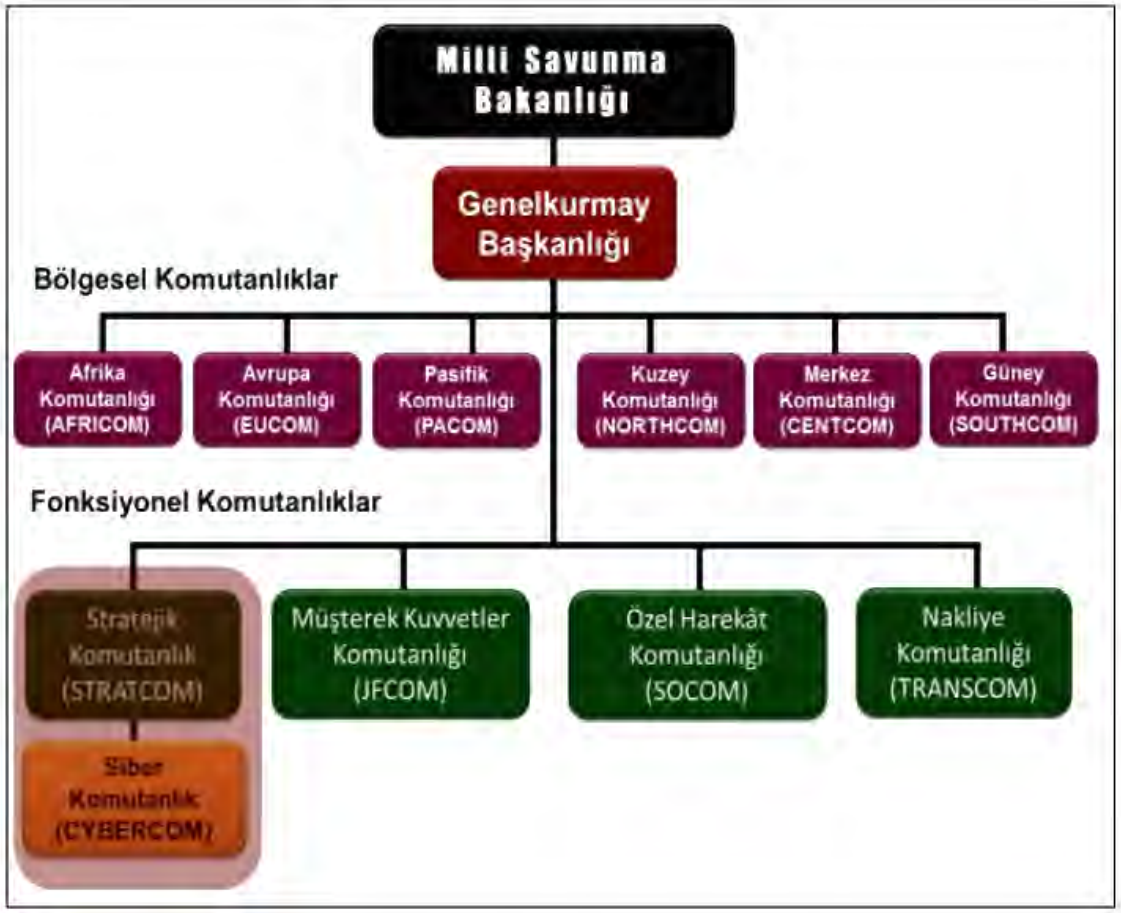
Bakanlığın .mil alanı sanal ağları Siber Komutanlık tarafından korunmaktadır. Bununla birlikte .gov alanı sivil ağların güvenliği ise İç Güvenlik Bakanlığı (Department of Homeland Security) tarafından korunmaktadır.

ABD'de 10 birleşik muharip komutanlığı bulunmaktadır. Söz konusu muharip komutanlıklardan 4'ü fonksiyonel ve 6'sı da bölgesel niteliktedir. Siber Komutanlık, ABD Stratejik Komutanlığı bünyesinde yer almaktadır. Söz konusu komutanlığın sorumluluk alanları ise şu şekilde sıralanabilir:

- Uzay harekâtı

- Füze savunması
- Komuta kontrol
- İstihbarat
- Keşif
- Gözetleme
- Nükleer silahlar

Savunma Bakanlığı Birleşik Muharip Komutanlıklar teşkilatı kapsamında Siber Komutanlığın konumu Şekil 3.2.'de gösterilmektedir.

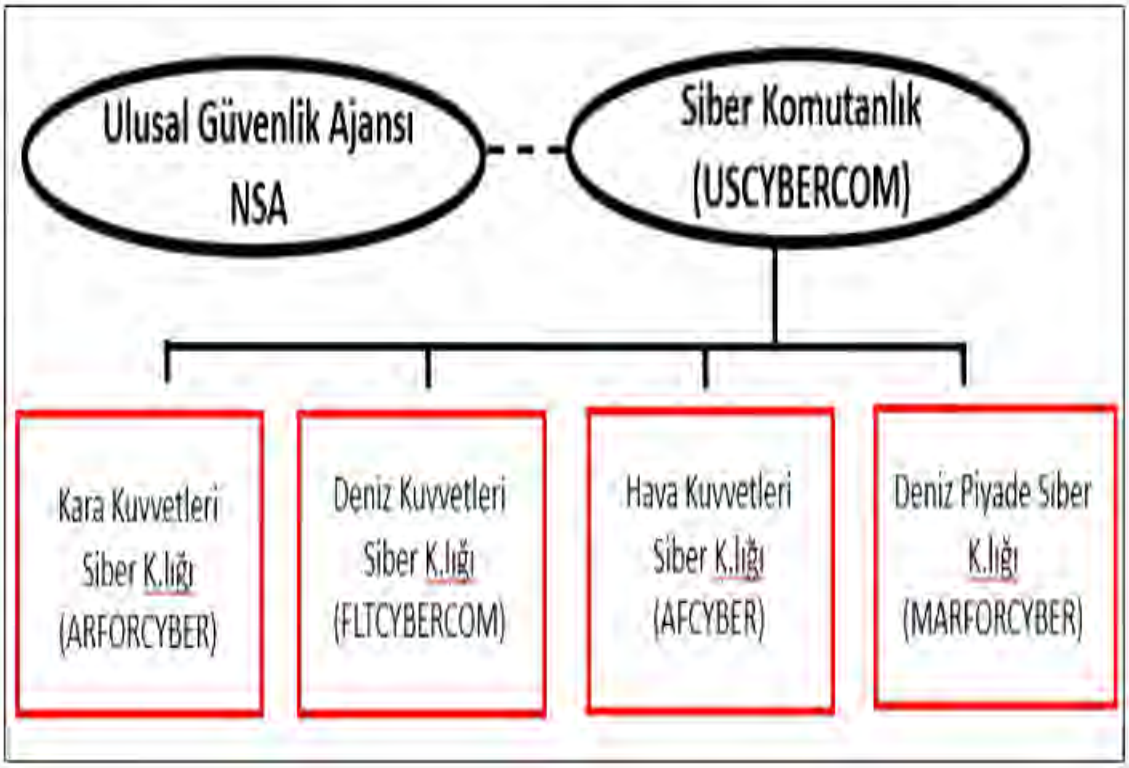



**Şekil 3. 2.** *ABD Siber Komutanlığı'nın teşkilat yapısındaki yeri (ABD Savunma Bakanlığı, 2019).*

Siber Komutanlığın 2010 yılında kurulduğu ifade edilmektedir. Siber Komutanlık faaliyetlerini Şekil 3.2.'de gösterilen hiyerarşik yapı içinde sürdürmektedir. Ancak siber güvenliğe ilişkin önemin artması ile birlikte Siber Komutanlık ile Stratejik Komutanlık

birbirinden ayrılmış ve ayrıca bir Birleşik Muharip Komutanlık oluşturulmuştur. 2018 yılında gerçekleştirilen törenden sonra ise Siber Komutanlığın 11. Birleşik Muharip Komutanlık olarak faaliyetlerine başladığı ifade edilmiştir (ABD Siber Komutanlığı, 2019a).

ABD Siber Komutanlığı'nı meydana getiren unsurlar ise Şekil 3.3.'te gösterilmektedir. Siber Komutanlığı yöneten komutanın çift şapkalı olduğu ve bununla birlikte yabancı sinyal istihbaratı ve ulusal güvenlik sistemlerinin korunmasından da sorumlu olan Ulusal Güvenli Ajansı'nı (NSA) bu komutan tarafından yönetilmektedir.




**Şekil 3. 3.** *ABD Siber Komutanlığı yapısı (ABD Siber Komutanlığı, 2019a).*

Siber Komutanlık ilk kurulduğu sırada kuvvet komutanlıklarının yalnızca bu komutanlığın talimatlarına göre kendi ağlarını işleteceği ve savunacağı öngörülmüştür. Fakat siber tehdidin askeri boyutunun çeşitlenmesi ile birlikte her kuvvete has güvenlik önlemleri alınması gerekli hale gelmiştir. Bu durum da her kuvvetin kendi siber yapılanmasını gerçekleştirmesine yol açmıştır. Siber Komutanlığın altında ve siber

uzayda faaliyetler gerçekleştirmek amacıyla şu komutanlıklar kurulmuş ve söz konusu yapının harekât kontrolüne bırakılmıştır (ABD Siber Komutanlığı, 2019b):

- Deniz Kuvvetleri Siber Filo Komutanlığı
- Deniz Piyade Siber Komutanlık
- Hava Kuvvetleri 16. Hava Komutanlık
- Kara Kuvvetleri Siber Komutanlık

### 3.1.4. Rusya Federasyonu:

Çin Halk Cumhuriyeti ve Amerika Birleşik Devletleri ile birlikte Rusya Federasyonu da günümüzde siber uzayı domine eden küresel güçlerden biridir. Siber uzayın sağladığı olanakların dış politik problemlerin ortadan kaldırılması için çözülmesi amacıyla kullanılması Rusya Federasyonu'nun siber kapasitesinin kapsamının diğerlerinden farklılaşmasına neden olmaktadır. Bununla birlikte siber uzayın sağladığı olanaklar Rusya Federasyonu tarafından komşularla ilişkiler kapsamında bir yaptırım ve baskı aracı olarak da kullanılmaktadır.

Her ne kadar Ulusal Güvenlik Strateji Belgesi'nde gerektiği kadar yer almasa da Rusya'nın siber güvenliğe ilişkin olan stratejiler oluşturduğu ve bu konudaki çalışmalara ABD'den daha erken başladığı söylenebilmektedir. Rusya'nın siber güvenliğe ilişkin politikaları üzerinde belirleyici olan belgelerin 2000'li yıllardan itibaren geliştirilmeye başlandığı Uluslararası İletişim Birliği tarafından ifade edilmektedir. Söz konusu belgeler şu şekilde sıralanabilir (Göçoğlu, 2017, s. 8):

- Rusya Federasyonu Bilgi Güvenliği Doktrini
- Uluslararası Bilgi Güvenliğinde Rusya Federasyonu Devlet Politikası Temel Prensipler Belgesi (Basic Principles for State Policy of the Russian Federation in the field of International Information Security)

1999 yılında Vladimir Putin Rusya Federasyonu'nun başına geçmiştir. Daha sonra 2000 yılında ulusal güvenlik politikası yeniden gözden geçirilmiş ve bilgi harekâtı konusu daha öncelikli hale getirilmiştir. Bu kapsamda Güvenlik Konseyi'ne ilk kez Rusya Federasyonu Bilgi Güvenliği Doktrini sunulduğu belirtilmektedir (Çiftçi, 2013, s. 44).

Gerçekleştirilen çalışmalar sonucunda saldırı ve savunmaya dair bilgi harekâtı olanakları Elektronik Harp Birlikleri kapsamına dahil edilmiştir. 2001 yılında da

"Voronezh Askeri Telsiz-Elektrik Elektronik Enstitüsü" faaliyet göstermeye başlamıştır. Bu Enstitü'nün Voronezh'da ileri düzeyde siber saldırı ve hackerlık eğitimleri verdiği ifade edilmektedir (Clarke ve Knake, 2011, s. 37).

Bilgi harekâtına ilişkin konulara odaklanılması amacıyla 15.000 personeli ve 6.000 öğrenci alma potansiyeli olan "Voronezh Askeri Havacılık Mühendisliği Üniversitesi" kurulmuştur (Özçoban, 2014, s. 97). Bununla birlikte "Stratejik Roket Kuvveti Akademisi" kapsamında faaliyetlerini yürüten "Elektronik ve Bilgi Harbi Teşkilatı" da bulunmaktadır. Bu bağlamda Rusya Federasyonu'nun eğitime oldukça büyük bir önem verdiği görülmektedir. Rusya Federasyonu'nda bilgi güvenliğine dair şu konularda dersler verildiği belirtilmektedir (Çiftçi, 2013, s. 45):

- Donanım güvenliği
- Bilgi güvenliği organizasyonu ve ileri teknolojileri
- BİT sistemleri
- Kriptoloji
- Yazılım güvenliği
- Bilgi sistemlerinin bütünleşik yapıda savunulması

Siber güvenlik alanında faaliyetlerini gerçekleştiren devlet kurumları şu şekilde sıralanmaktadır (Medvedev, 2015, s. 3):

- Federal Güvenlik Servisi (Federal Security Service)
- Dış İstihbarat Servisi (Foreign Intelligence Service)
- Ana İstihbarat Servisi (Mail Intelligence Directorate)

Bununla birlikte siber uzayın Rusya Federasyonu tarafından kullanım biçiminin savunmadan ziyade saldırıya daha yakın olduğu ve bu durumun da sadece gerçekleştirilecek yatırımların biçimlendirilmesi noktasında etkili olduğu ifade edilmektedir (Medvedev, 2015, s. 76-77).

Ülkenin bilgi ve siber güvenliğinin sağlanmasının Rusya Federasyonu'nun Siber Güvenlik Strateji Belgeleri'nin ana hedeflerinden biri olduğu ifade edilmektedir. Bununla birlikte Rusya Federasyonu'nun siber uzayın sunduğu olanaklardan olabildiğince yararlanılması ve teknolojik yeniliklerin elde edilmesi için bir siber espiyonaj sistemi de kurulması gibi amaçlarının olduğu ifade edilmektedir. Bu kapsamda birbirleri ile iş birliği

içinde çalışacak ve her biri ortak ama farklı hedeflere yöneltilmiş dört istihbarat servisi kurulmuştur. Bunlar şu şekilde sıralanabilir:

- Federal Güvenlik Servisi- Federal Security Service (FSB)
- Ana İstihbarat Servisi- Main Intelligence Directorate (GRU)
- Federal Koruma Servisi- Federal Protective Service (FSO)
- Dış İstihbarat Servisi- Foreign Intelligence Service (SVR)

ÇEKA, NVD ve KGB SSCB döneminde faaliyetler gerçekleştirmiştir. Bu kapsamda FSB'nin de SSCB döneminde faaliyetler gerçekleştiren bu kurumların yerini aldığı ifade edilmektedir. FSB'nin iç güvenlik servisi olarak faaliyetlerinin birden çok boyutunun olduğu belirtilmektedir. Ülke genelinde devletin güvenliği aleyhine yürütülen faaliyetlere ilişkin olarak istihbarat elde etmek FSB'nin başlıca görevini oluşturmaktadır (Gady vd., 2010, s. 5). Bu kapsamda FSB'nin görevinin ülkedeki bazı gruplara ilişkin olarak şu eylemlerde bulunmak olduğu söylenebilmektedir:

- Gerçekleştirilen faaliyetlerin izlenmesi
- Grupların takip edilmesi
- Gruplar hakkında istihbarat toplanması

Bununla birlikte Rusya Federasyonu'na karşı devam eden espiyonaj faaliyetlerine karşı koymanın da FSB'nin bir diğer görevi olduğu ifade edilmektedir. Söz konusu karşı koyma faaliyeti kont/espiyonaj çalışması olarak da nitelendirilmektedir. Bu faaliyetin amacının Rusya Federasyonu aleyhine dış istihbarat servisleri tarafından yürütülen yıkıcı ve bölücü nitelikteki bilgi operasyonlarının engellenmesi olduğu belirtilmektedir. Bu bağlamda siber saldırılara karşı mücadele edilmesi ve ülkenin siber güvenliğinin sağlanmasının FSB'nin görevi olduğu belirtilmektedir (http://www.cicentre.com/?page=191 , 2016). Yabancıların ve Rus vatandaşlarının telekomünikasyon iletişim bilgilerinin istihbari bilgiler kapsamında takip edilmesi de FSB'nin bir diğer görevini oluşturmaktadır. Söz konusu görev kapsamında FSB'nin "Operatif Denetleme Faaliyetleri Sistemi" (System for Operative Investigative Activities / SORM)'nin kontrol edilmesine ilişkin görevi de üstlendiği belirtilmektedir. Bu görev Rusya Federasyonun'daki analog ve internet haberleşmenin takip edilmesini sağlayan bir tür denetleme sistemi niteliğine sahiptir. Bilişim ve teknoloji sektörlerinin karşı karşıya

kalabileceği espiyonaj faaliyetlerinin önlenmesine ilişkin olarak da FSB'nin Rusya Teknik ve İhracat Kontrol Servisi (Federal Service for Technical and Export Control of Russia / FSTEC) ile oldukça yakın bir iş birliği içinde olduğu ifade edilmektedir. FSTEC 2004 yılında kurulmuş ve ihracat denetim rejiminin kontrol edilmesi görevini üstlenmiştir. Bu kapsamda bilişim, sanayi ve teknoloji alanlarına karşı gerçekleştirilebilecek espiyonaj faaliyetlerine karşı koyulması noktasında FSTEC'in oldukça önemli bir rol üstlendiği belirtilmektedir (Carr, 2001, s. 318). Bununla birlikte FSB tarafından yürütülen güvenliğe ilişkin çalışmalarla beraber diğer faaliyetlerin de SVR ile koordinasyon içinde gerçekleştirildiği ifade edilmektedir (Staar, 2010, s. 10).

Rusya Federasyonu'nun ülke dışında gerçekleştireceği espiyonaj faaliyetlerinin gerçekleştirilebilmesi için SVR kurulmuştur. SVR'nin KGB'nin devamı niteliğinde olduğu ifade edilmektedir. Bu kapsam SVR'nin bir dış istihbarat servisi olduğu söylenebilmektedir. GRU ve SVR'nin Rusya Federayonu'nun dış istihbarat faaliyetleri noktasında oldukça büyük önem arz ettiği belirtilmektedir. Hedef alınan ülkeye yönelik olarak SVR tarafından şu hususlarda istihbari nitelikte bilgi toplandığı ifade edilmektedir (Heickerö, 2015, s. 31):

- Siyasi
- Ekonomik
- Ulaştırma
- Bilim
- Askeri
- Biyografik
- Sosyal
- İletişim
- Teknoloji

Ülkelerin teknoloji ve bilim kapasitesini hedefleyen siber casusluk operasyonlarının planlanmasına ilişkin görevin de SVR'ye ait olduğu belirtilmektedir. SVR'nin birçok ülkede sinyal ve elektronik istibarat elde etmek için kullandığı merkezler de bulunmaktadır. Bu merkezlerden bazıları şu şekilde sıralanabilir (Heickerö, 2015, s. 32):

- Kazakistan
- Ermenistan
- Suriye
- Vietnam
- Abhazya
- Kırım
- Belarus
- Tacikistan
- Kırgızistan
- Küba
- Güney Osetya

GRU'nun bir askeri istihbarat teşkilatı olduğu ifade edilmektedir. Çünkü GRU, Rus Genelkurmayı'na bağlı bir biçimde faaliyetlerini gerçekleştirmektedir. Sovyetler Birliği döneminde GRU, Kızıl Ordu'ya bağlı olarak faaliyetlerini yürütmüştür. Bununla birlikte GRU'nun Rusya Federasyonu'ndaki en büyük kapasiteye sahip istihbarat teşkilatı olduğu belirtilmektedir. GRU askeri ve dış istihbarat konularında tam yetkiye sahiptir. Ayrıca GRU'nun ülkenin güvenliğine ilişkin olarak da istihbarat toplama yetkisine sahip olduğu ifade edilmektedir. Rus askeri kurumlarını hedefleyen siber operasyonlara karşı kontr/espiyonaj faaliyetlerinin yürütülmesi ve mümkün olması durumunda diğer ülkelerin askeri kapasitesine ilişkin siber casusluk operasyonlarının planlanması GRU'nun temel görevleri arasında gösterilmektedir (http://www.cicentre.com/?page=191, 2016). "Computer Emergency Response Team"leri Stratejik Füze Birliklerinin faaliyetlerinin devam ettirilmesi için kurulmuştur. Ayrıca bunların ülkenin karşı karşıya kalabileceği siber saldırılara ilişkin olarak da kurulduğu ifade edilmektedir. "Computer Emergency Response Team"lerinin kontrolünün de GRU ve diğer istihbarat kuruluşları ile birlikte sağlandığı belirtilmektedir (Heickerö, 2015, s. 27).

Siber güvenliğe ilişkin olarak Rusya Federasyonu'nun oldukça büyük bir çaba gösterdiği ifade edilmektedir. Bu nedenle özel sektörde konunun uzmanı olan akademik ve teknik personel ile iş birliği içinde faaliyetler yürütülmekte ve siber silahlar kullanılarak etkili bir siber savaş yaklaşımı benimsenmektedir (Schaap, 2009, s. 139).

Siber silahlar ve klasik nitelikteki yöntemlerin birlikte kullanılmasının gerçekleştirilecek harekâtın etkinliğini artıracağı ve bu şekilde de siber silahların etkinliğinin daha iyi anlaşılacağı düşüncesi benimsenmiştir. Bu düşüncenin Gürcistan ve Ukrayna olaylarında da fiilen uygulandığı ifade edilmektedir. Rusya Federasyonu'nun sahip olduğu siber olanakların diğer ülkelerin askeri, finans, kamu ve özel iletişim ağlarına zarar verebilecek nitelikte olduğu belirtilmektedir. Ayrıca gerçekleştirilecek bir askeri operasyon öncesinde de Rusya Federasyonu'nun sahip olduğu siber olanakların hedeflenen ülkenin altyapılarını devre dışı bırakabileceği belirtilmektedir (Billo ve Chang, 2004, s. 107).

Rusya Federasyonu'ndaki kritik internet ağlarının denetiminin hükümetin elinde olduğu ifade edilmektedir. Bununla birlikte yapılan yasal düzenlemeler ile internet sunucularının farklı bir ülkeye veri paylaşması engellenmiş ve bu şekilde de hükümetin desteği ile ya da isteği üzerine yapılan siber operasyonlara ilişkin bilgi edinilmesi engellenmiştir (Çeliktaş, 2016, s. 67).

### 3.1.5. Japonya:

2004 yılında siber güvenlik Japonya'da stratejik düzeyde ele alınmaya başlanmıştır. 2005 yılında ise Japonya'da Bilgi Güvenliği Politikası Komisyonu ile Ulusal Bilgi Güvenliği Merkezi'nin kurulduğu bilinmektedir (NISC, 2007).

Bilgi teknolojileri stratejik genel merkezinin ise Bakanlar Kurulu bünyesinde 2001 yılının ocak ayında kurulduğu ifade edilmektedir (Japan Cabinet, 2000). Söz konusu birimde bilgi teknolojilerine dair stratejik nitelikte kararlar alınmakta ve politikalar belirlenmektedir. Bu nedenle bu konuya ilişkin olarak bu merkezin ülkenin en üst seviyedeki oluşumu olduğu söylenebilmektedir.

2004 yılında kurumsal değerlendirmeye ilişkin yapılan çalışmalar neticesinde Bilgi Teknolojileri Stratejik Genel Merkezi bünyesinde bilgi güvenliği politikası komisyonu kurulmuştur. Bu komisyonun siber güvenliğe ilişkin olarak ulusal çapta stratejik kararların alınmasına ilişkin bir sorumluluk üstlendiği ifade edilmektedir. Bununla birlikte kamu kurumlarının bilgi güvenliğine ilişkin uyması gereken standartların oluşturulması görevinin de bu komisyona ait olduğu belirtilmektedir (NISC, 2007).

2004 yılında ise kurumsal nitelikte değerlendirme çalışmaları gerçekleştirilmiştir. Bu çalışmalar neticesinde Bilgi Teknolojileri Stratejik Genel Merkezi'nde bu ulusal bilgi güvenliği merkezi kurulmuştur. Üst düzeydeki politik kararların uygulanması ve koordine edilmesinden bu Merkez'in sorumlu olduğu belirtilmektedir. Söz konusu faaliyetler ise özel sektör ve kamudaki uzmanların geçici olarak görevlendirilmesi şeklinde yürütülmektedir. Merkez tarafından üstlenilen görevlerden bazıları ise şu şekilde sıralanabilir:

- Siber güvenliğe ilişkin olarak teknik düzeyde stratejiler üretilmesi
- Yeni teknolojilerin takip edilmesi
- AR-GE
- Kamu kurumlarında bilgi güvenliğine ilişkin değerlendirme ve analiz yapılması
- Kritik nitelikteki altyapıların korunması

Merkez tarafından gerçekleştirilen çalışmalar düzenli olarak Bilgi Güvenliği Politikası Komisyonuna sunulmaktadır. Ayrıca bu merkezden elde edilen verilere dayanılarak ulusal strateji belgeleri hazırlanmakta ve yıllık plan yapılmaktadır. Ayrıca kamu kurumlarının zorunlu olarak gerçekleştirilmesi gereken standartların takip ve denetimi de Merkez tarafından gerçekleştirilmektedir (NISC, 2007).

Ayrıca Japonya'da "Özellikli Kişisel Verileri Koruma Komisyonu"nun hem adı hem de kapsamı değiştirilerek "Kişisel Verileri Koruma Komisyonu" meydana getirilmiştir. Bununla birlikte Komisyon başkanı ve üyelerinin 5 yıl süresince meclis onayı ile Başbakan tarafından atandığı ifade edilmektedir. Ayrıca Komisyon üst kurul niteliğine de sahiptir. Bu nedenle Komisyon'un özerk bir yapıda olduğu ifade edilmektedir. Özel sektör kuruluşlarının kişisel verileri koruma organizasyonu olarak yetkilendirilmekte ve gelen şikâyetleri söz konusu yetkilendirilmiş üçüncü taraflar aracılığı ile çözmektedir (PPC, t.y.).

Kişisel Verilerin Korunması Kanunu kapsamındaki müeyyidelerin uygulanmasına ilişkin olarak merkezi otoritenin Müşteri İlişkileri Ajansı olduğu ifade edilmektedir. Ayrıca tüm bakanlıkların sorumlu olduğu sektörler hakkında yönlendirme ve yaptırım uygulama gücüne sahip olduğu da belirtilmektedir (Raul vd., 2014).

Siber alandaki yapılandırmalarda bir diğeri olan bilgi teknolojileri teşvik ajansının üç ana alanda faaliyetlerini gerçekleştirdiği ifade edilmektedir. Bu alanlar şu şekilde sıralanabilir:

- Bilgi güvenliği
- Bilgi sistemlerinin güvenilirliğinin artırılması
- İnsan kaynağının geliştirilmesi

Bilgi teknolojilerine bağlı olan ekonomik kalkınma ile etkili güvenlik önlemleri arasında oldukça sıkı bir ilişkinin mevcut olduğuna ilişkin inancın benimsenmiş olması bilgi güvenliğinin üç ana alandan biri olmasını gerektirmiştir. Bu kapsamda özel sektörün teşvik edilmesine dair bilgi teknolojileri politikaları üretilmesinin de kuruluş tarafından gerçekleştirildiği ifade edilmektedir (IPA, t.y.)

### 3.1.6. Çin:

Siber güvenliğe ilişkin olarak Çin'in iletişim ve bilgi teknolojilerin 1900'lü yıllarında sonlarından itibaren büyük bir önem verdiği ifade edilmektedir. Çin'de öncelikle 1986 yılında ekonomik nitelikteki bilgilerin yönetilmesine ilişkin olarak oldukça küçük bir grup kurulduğu belirtilmektedir. Siber güvenliğe ilişkin ilk sivil belge niteliği taşıyan Belge 27 ise 2003 yılında yayımlanmıştır. Söz konusu belge ile ulaşılmak istenen amaçlar ise şu şekilde sıralanabilir (Raud, 2016, s. 11):

- Kritik nitelikteki altyapıların korunmasına ilişkin aktif bir savunma politikası üretilmesi
- Dinamik gözlemleme
- Gelişimin desteklenmesi
- Ekonomik bilgilerin yönetimi grubu ve devlet organları ile iş birliği tesis edilerek siber güvenliğe ilişkin politikaların yönlendirilmesi

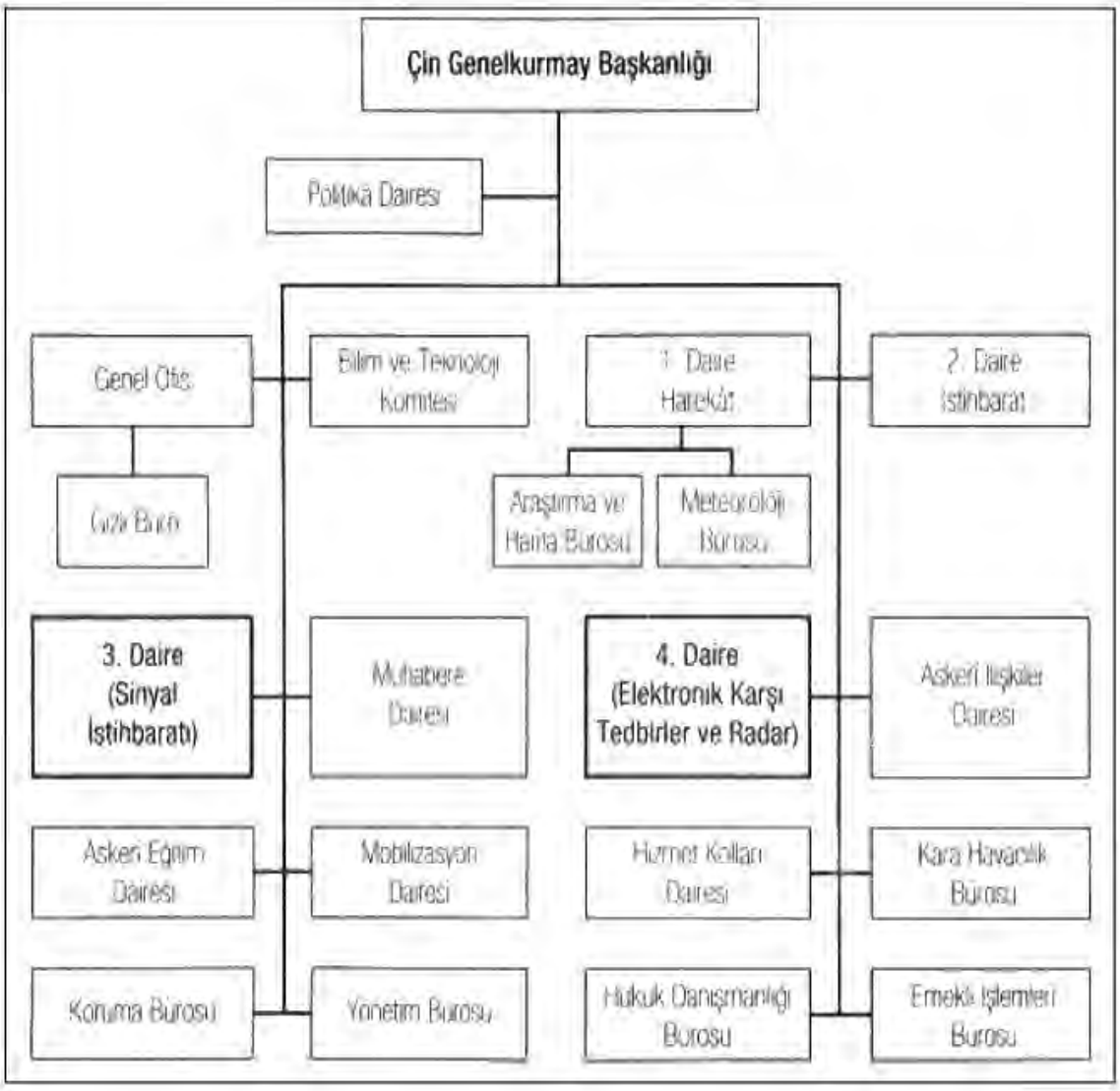
Siber güvenlik alanına ilişkin olarak Çin tarafından yapılan hukuki ve kurumsal nitelikteki düzenlemelerin ise 2014 yılında önce yapıldığı belirtilmektedir. Dünyada denetim alanındaki dört büyük şirketten biri olan KMPG tarafından yayınlanan raporda söz konusu düzenlemeler kronolojik olarak yer almaktadır. Yapılan düzenlemeler şu şekilde sıralanabilir (KMPG, 2016, s. 5):

- Siber güvenlik ve sistemsel nitelikteki altyapıların düzenlenmesi

- Bilgisayar bilgi güvenliğine ilişkin prosedürlerin devlet tarafından meydana getirilmesi
- Bilgisayar virüslerine karşı savunma ve internete ilişkin bazı standartların Kamu Güvenliği Bakanlığı tarafından geliştirilmesi
- Çin devlet başkanı olan Xi Jinping başkanlığında siber güvenlik grubunun kurulması
- Çin Ulusal Kongresi'nde (NPC) kamuoyu yoklaması yapılarak halkın bu konudaki görüşleri doğrultusunda Siber Güvenlik Kanun tasarısının oluşturulması

Siber güvenliğin Çin Halk Cumhuriyeti askeri konseptinde hakkında araştırmalar yürütülmesi ve oldukça büyük bir sermaye ayrılması gereken oldukça önemli bir konu olduğu belirtilmiştir. Siber olanakların savaş stratejileri kapsamında büyük katkılar sunduğu hususu da Çinli komutanlar ve idareciler tarafından dile getirilmiştir (Mulvenon, 2009, s. 257).

Siber savaş organizasyonuna ilişkin olarak Çin Halk Cumhuriyeti komuta kademesi tarafından 2011 yılında bazı açıklamalar yapılmıştır. Söz konusu açıklamalarda Çin Halk Cumhuriyeti'nde ilk kez süper elit siber savaşçı birliğinin mevcut olduğu ve bu birliğin "Mavi Ordu" olarak adlandırıldığı ifade edilmiştir. Ayrıca bu birliğin otuz kişiden meydana geldiği de belirtilmiştir. Bununla birlikte söz konusu açıklamalarda Çin Halk Kurtuluş Ordusu'nun sanal ağlarının muhtemel saldırılardan korunması amacıyla bu birliğin kurulduğu ifade edilmiştir (Hwang, 2012, s. 191). Şekil 3.4.'te Çin Halk Cumhuriyeti'nin Genel Kurmay Başkanlığı'ndaki siber teşkilat yapısına yer verilmiştir.




**Şekil 3. 4**. *ÇHC Genelkurmay Başkanlığı'ndaki siber teşkilat yapısı (Çifci, 2013: 42).*

Ülkenin politik yapısı ve ideolojisinden dolayı hem ülkenin savunması hem de siber güvenlik ülkenin silahlı kuvvetleri tarafından kontrol edilmektedir. Yukarıdaki şekilde gösterilen üçüncü ve dördüncü dairelerin iletişim ve bilgi altyapısının muhafaza edilmesinden sorumlu olduğu ifade edilmektedir. Söz konusu dairelerin tüm kuvvetler ile birlikte siber savaşa ilişkin unsurları koordineli olarak denetim altında tuttuğu belirtilmektedir (Corera, 2015, s. 232).

Çin Halk Kurtuluş Ordusu tarafından kullanılan tüm bilgi sistemleri ve sanal ağların korunması görevinin de Genelkurmay 3. Dairesi'ne ait olduğu ifade edilmektedir.

Ulusal düzeydeki faaliyetlerin gerçekleştirilmesi noktasında bu dairenin sorumlu olduğu ifade edilmektedir. Söz konusu daire 3 araştırma enstitüsü ve 12 operasyonel bürodan meydana gelmektedir. Ayrıca bu daire tarafından siber güvenliğin geliştirilmesi amacıyla sürekli araştırma ve geliştirme faaliyetleri yürütülmekte ve yüksek öğretim kurumları ile de birlikte hareket edilmektedir. Elektronik karşı önlemler ve radar konuları konusunda ise Genelkurmay 4. dairesinin görevli olduğu ifade edilmektedir. Bu dair klasik nitelikteki savaş mantığı kapsamında elektronik saldırı birimi olarak görevlerini yerine getirmektedir (Stokes vd., 2011, s. 5-7).

Çin Halk Kurtuluş Ordusu'nun dünyadaki en hızlı süper bilgisayarlara sahip olduğu ifade edilmektedir. Çin'deki en büyük ve köklü ARGE organizasyonunun Jiangnan Bilgisayar Teknolojileri Araştırma Enstitüsü olduğu belirtilmektedir. Burada oldukça önemli nitelikte süper bilgisayar yatırımları yapılmakta ve bu şekilde Çin'de bulunan diğer bilgisayar merkezlerine ve Çin Halk Kurtuluş Ordusu bünyesinde yer alan diğer organizasyonlara destek verilmektedir. Bununla birlikte söz konusu süper bilgisayarlar aracılığıyla diğer ülkelere ait olan kriptolar, karmaşık kodlar ve şifreleme sistemlerinin kırılmasına ilişkin çalışmalar gerçekleştirilmektedir (Stokes vd., 2011, s. 5).

1900'lü yıllardan itibaren Çin Halk Cumhuriyeti'nin siber alanda öncü olmak için birçok çalışma yürüttüğü ifade edilmektedir. Bu kapsamda birçok strateji belgesi ve doktrin Çin Halk Cumhuriyeti tarafından yayımlanmıştır. Çin Halk Kurtuluş Ordusu'nun "bilgileştirme" stratejisi kapsamında siber ortam ve bilgi iletişim teknolojileri alanlarında süper güç haline gelmeyi amaçladığı belirtilmektedir (Ventre, 2010).

Çin Halk Cumhuriyeti hackerlarının oldukça etkin ve geniş nitelikte bir siber saldırı tecrübesi ve yeteneğine sahip olduğu ifade edilmektedir. Oldukça geniş bir alanda faaliyetler gerçekleştiren ve uzmanlaşmış bir bilgisayar topluluğunun Çin Halk Cumhuriyeti'nde mevcut olduğu ifade edilmektedir. Bu topluluklar internet aracılığı ile birbirleri ile iletişim kurmakta ve siber saldırı silahları da birbirleri arasında sanal ağlar aracılığıyla paylaşılmaktadır. 2011 yılında Çin Halk Cumhuriyeti'nde Mavi Ordu'nun faaliyetlerine başladığı bilinmektedir. Ayrıca Mavi Ordu'nun söz konusu hackerların faaliyetlerinin kontrol edilmesi amacıyla kurulduğuna ilişkin iddialar da bulunmaktadır (Darıcılı ve Özdal, 2017).

Çin Halk Cumhuriyeti'nde "Altın Kalkan" şeklinde adlandırılmış olan bir filtreleme sistemi de bulunmaktadır. Bu sistem ile kritik bilgilerin Çin Halk Cumhuriyeti dışına çıkması ya da içeri girmesinin önlenmesi amaçlanmaktadır. Bununla birlikte bu sistem "Büyük Çin Güvenlik Duvarı" şeklinde de adlandırılmaktadır. Söz konusu sistemin muhtemel bir siber savaş durumunda Çin Halk Cumhuriyeti'ni koruyacağı ve ciddi nitelikte üstünlük elde etmesini sağlayacağı ifade edilmektedir (Clarke ve Knake, 2010, s. 35).

### 3.2. Temel Olaylarda Aktörlerin Siber Dengeleme Politikaları:

Günümüze kadar gelen süreçte uluslararası platformda sayılamayacak kadar çok sayıda siber olay gerçekleşmiştir. Her biri ayrı çalışma konusu olabilecek nitelikteki bu olayların tamamını ele almak elbette mümkün değildir. Söz konusu sebeple çalışmamızın bu başlığı altında literatür tarafından en önemli görülen siber olaylar ele alınacaktır.

#### 3.2.1. Stuxnet olayı:

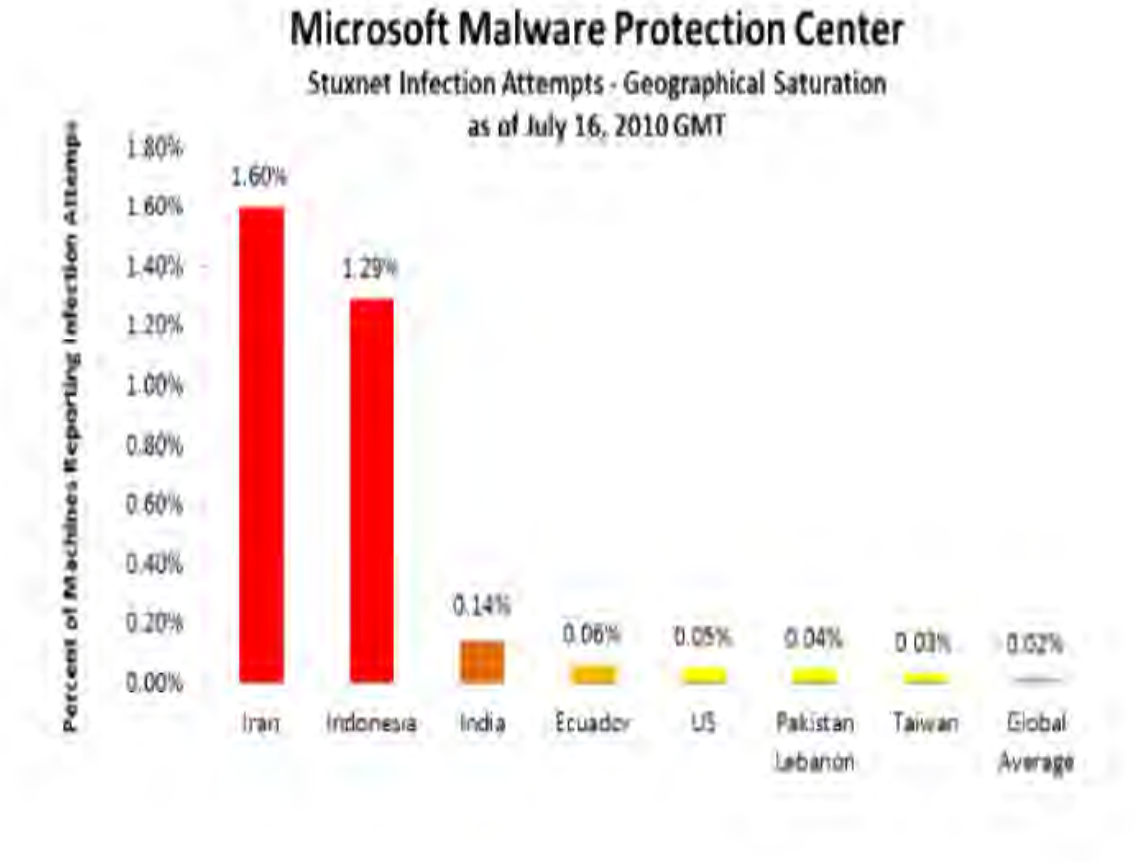
En çok gündeme gelen siber olaylardan birinin Stuxnet olarak adlandırılan bir yazılım ile gerçekleştirildiği ifade edilmektedir. Bazı araştırmacılar bu yazılımı sisteme giren ve dışarıya verilerin aktarılması için kapı açan bir truva atı olarak değerlendirmektedir. Bununla birlikte bazı araştırmacılar ise bu yazılımın sisteme girerek büyük yıkımlara neden olan bir solucan olduğunu ifade etmektedir. Stuxnet'in özellikle sanayii tesislerinin kontrol sistemlerini hedeflediği belirtilmektedir. Bu kapsamda Stuxnet'in İran'ın nükleer faaliyetlerini engellemek amacıyla Batılı ülkeler tarafından geliştirildiği ifade edilmektedir. Baraj, petrol platformu, enerji santrali, maden sahaları, sanayi tesisleri gibi yapıların kontrol edilebilmesi için SCADA sistemleri kullanılmaktadır:

Stuxnet'in de amacının SCADA sistemlerine girerek fiziksel kontrol sistemlerinin çalışma şeklini değiştirmek olduğu belirtilmektedir. Bu kontrol sistemlerinin çoğunlukla askeri üsler, kritik altyapılar, enerji santralleri, petrol boru hatları, havaalanları gibi bölgelerde kullanıldığı ifade edilmektedir (Yalçın, 2019, s. 64).

Yukarıda sıralanan bölgelerin ortak özelliği risk seviyesinin yüksek olması ve ayrıca güvenliğin ön planda tutulması gerektiğidir.

Stuxnet adlı yazılımın yalnızca görevlilerin bilgisayarlarına sızdığı ve yaklaşık 30.000 adet bilgisayarın zarar gördüğü İran tarafından ifade edilmiştir. Siber müdahalenin etkinliğini gösteren en temel olaylardan birinin Stuxnet saldırısı olduğu belirtilmektedir. Bu saldırı sonrasında İran tarafından üretilen 9.000'i aşkın santrifüjün yaklaşık 6.000 tanesi çalışamaz duruma gelmiştir (Ataç, 2019, s. 12).

Stuxnet üzerinde siber güvenlik uzmanları tarafından çeşitli araştırmalar gerçekleştirilmiştir. Bu araştırmalar sonucunda elde edilen bilgiler göz önünde bulundurulduğunda Stuxnet adlı yazılımın oldukça karmaşık bir yapıya sahip olduğu ifade edilmektedir. Bununla birlikte bu yazılımın konu hakkında uzman bir ekip tarafından oluşturulduğu ve SCADA teknolojisi hakkında oldukça kritik nitelikteki bilgilerin kullanıldığı belirtilmiştir. Bu nedenle bu yazılımın oluşturulması sürecinde birçok yerden destek alındığı görülmektedir. Stuxnet saldırısı hedefi ve saldırının gerçekleştiği coğrafya açısından basit bir saldırı özelliği göstermemektedir. Bu saldırıdan en çok etkilenen sistemlerin İran'da olduğu ifade edilmektedir (Industrial Ethernet Book, 2017). Ancak Şekil 3.5.'te görüleceği üzere Stuxnet virüsünden sadece İran etkilenmemiş; aksine çok sayıda ülkeye zarar vermiştir.




**Şekil 3. 5.** *Stuxnet virüsünden etkilenen ülkeler (Industrial Ethernet Book, 2017).*

Bugüne dek bilinen en gelişmiş siber saldırının Stuxnet olduğu ifade edilmektedir. Bu saldırının ABD tarafından 2009 yılında gerçekleştirildiği iddia edilmektedir. Bu saldırı ile İran'ın Natanz adlı şehrindeki nükleer zenginleştirme programının hedef alındığı belirtilmektedir. Bu kapsamda Stuxnet'in siber harekât ortamında tespit edilmiş hedeflerin etki altına alınması için özel olarak tasarlanan yeni nesil bir sistem olduğu ifade edilmektedir (Özbek, 2019, s. 16).

2011 yılında New York Times'ta çıkan bir makaleye göre Stuxnet'in İsrail ve ABD'li uzmanlar tarafından birlikte oluşturulduğu iddia edilmiştir. Bu iddiaları destekleyici nitelikte birçok neden bulunmaktadır. Bunlardan bazıları şu şekilde sıralanabilir (Broad vd., 2011):

- İran'ın nükleer program kapsamında kullanılmakta olan teknolojiye dair teknik istihbarat elde etmeye gereksinim duyulması
- Stuxnet'in oluşturulması sürecinde gelişmiş nitelikte test ve programlama yöntemlerinin kullanılması
- Yazılımın aktif hale geçebilmesi için tesislere bireysel olarak erişim sağlamanın gerekmesi

Daha önce de dile getirildiği üzere; barajlar, sanayi ve enerji tesisleri gibi kritik altyapı sistemlerini hedef alan ilk kötü amaçlı yazılım olan Stuxnet, ülke çapında 30.000'e yakın bilgisayarı etkilemiştir (Özçoban, 2014). New York Times'a göre Stuxnet, İran nükleer programının 1,5 ila 2 yıl ertelenmesine sebep olmuştur. Böylesine büyük sonuçlar doğuran bu virüs saldırısının ise hangi ülke tarafından yapıldığı kesin olarak bilinmemektedir. Dolayısıyla kaynak ülke sadece iddialar üzerine tartışmalar niteliğinde kalmıştır. Bu sebeple virüsten etkilenen ülkeler saldırıyı gerçekleştiren ülke ya da ülkelere karşı herhangi bir pozisyon alamamış, yaptırım talebinde bulunamamıştır.

### 3.2.2. ABD başkanlık seçimleri ve Rusya krizi:

2016 yılında ABD Başkanlığı'na aday olan Hillary Clinton'un kampanyasını yönetme görevini üstlenen John Podesta ile Clinton'a destek vere ABD'nin eski Dışişleri Bakanı Colin Powell'ın e-maillerinin Rusya Federasyonu tarafından ele geçirildiği ve ele geçirilen maillerin Rusya Federasyonu tarafından kendi çıkarları için sızdırıldığı iddia edilmiştir. Dahası 2012 yılındaki Rusya Federasyonu seçimlerinde Beyaz Saray yöneticileri tarafından Putin karşıtı kampanyalar yürütüldüğü için bu sızdırma olayının arkasında doğrudan Putin'in olduğu hususu öne sürülmüştür (Darıcılı, 2017a, s. 16).

Siber saldırıların 2015 yılında başladığı ve Rusya Federasyonu Askeri İstihbarat Örgütü ile İç İstihbarat Örgütü'nün söz konusu saldırıları gerçekleştirdiği ifade edilmiştir. Ayrıca bu kurumlar tarafından aşağıda sıralanan grupların desteklendiği ve saldırıların bu şekilde gerçekleştirildiği belirtilmiştir:

- Cozy Bear
- Fancy Bear
- The Dukes
- APT-28

- APT-29

Emaillerin ele geçirilmesi için yemleme tekniği kullanılmış ve ilgili olan kişi ve kuruluşların yaklaşık 60.000 emaili ele geçirilmiş ve bu mailler ilgili kaynaklar ile paylaşılmıştır. Meydana gelen gelişmeler şu sonuçların ortaya çıkmasına neden olmuştur (New York Times, 2016):

- Demokrat Parti tarafından yürütülen kampanya olumsuz olarak etkilenmiştir.
- Üst düzeydeki yöneticilerden bazıları görevlerinden ayrılmıştır.
- Demokrat Parti'nin diğer adayı bulunduğu konumu daha da güçlendirmiştir.
- Cumhuriyetçiler oldukça önemli bir argüman elde etmiştir.
- Seçim kampanyası boyunca Clinton ciddi anlamda yıpratılmıştır.

Söz konusu saldırılar hakkında Federal Araştırma Bürosu (FBI) ve ABD İç Güvenlik Bakanlığı bir çalışma gerçekleştirmiş ve çalışma sonucunda meydana gelen olayı sorumlusu olarak Rusya Federasyonu gösterilmiştir. Ayrıca konuya ilişkin olarak yapılan açıklamalarda ABD'deki kamu kuruluşları, firmalar ve üniversitelere yönelik olarak da Rusya Federasyonu tarafından saldırılar gerçekleştirilmesinin planlandığı ve bu saldırılara Rusya Federasyonu tarafından "Grizlly Steppe" adı verildiği belirtilmiştir (ABD İç Güvenlik Bakanlığı, 2016).

Ayrıca Ulusal Güvenlik Ajansı (NSA), Federal Araştırma Bürosu (FBI) ve ABD İç Güvenlik Bakanlığı'nın yürüttüğü ortak çalışmada 2016 yılındaki ABD Başkanlık seçim sürecinin manipüle edilmesine ilişkin emrin bizzat Putin tarafından verildiği de iddia edilmiştir (ABD Milli İstihbarat Direktör Ofisi, 2017, s. 7).

Meydana gelen tüm bu gelişmelerden sonra Rusya Federasyonu'nun diplomatlarından bazıları söz konusu saldırılarla ilişkilendirildiği için istenmeyen kişi ilan edilmiş ve ülkelerine gönderilmiştir. Bununla birlikte FBI'ın soruşturma açması gerektiği hususu da Obama tarafından dile getirilmiştir. Meydana gelen gelişmeler sonrasında 35 Rus diplomatının sınır dışı edildiği bilinmektedir (Darıcılı, 2017). Ayrıca New York ile Maryland'da yer alan iki adet Rusya Federasyonu temsilciliğinin de kapatılmasına ilişkin karar verilmiştir (Sputnik Haber Sitesi, 2017).

2016 yılındaki ABD Başkanlık seçimlerine Rusya Federasyonu tarafından müdahale edilmesine ilişkin gerçekleştirilen soruşturma için FBI Eski Başkanı olan James Brien Comey 2017 yılının Haziran ayında Kongre'de ifade vermiştir. Söz konusu ifade şu şekildedir (BBC, 2017):

"*Rusya'nın seçimlerle ilgili siber saldırı yaptığı konusunda şüphe duymuyorum, Trump benden konuyla ilgili yapılan 'FBI soruşturmasını durdurmasını istemiştir. Bu kapsamda Trump'a güvenmediğim için adı geçen ile yaptığı her görüşmeyi kayıt altına alma ihtiyacı hissettim.*"

Meydana gelen gelişmeler uluslararası hukuk göz önünde bulundurularak bir değerlendirme yapıldığında şu kavramlar ortaya çıkmaktadır:

- Siber casusluk
- Kuvvet kullanımı
- Meşru müdafaa
- İçişlerine müdahale edilmemesine ilişkin ilkenin ihlal edilmesi
- Özel hayatın gizliliğinin ihlal edilmesi

Bununla birlikte yukarıda sıralanan kavramların siber güvenlik kapsamında yoğun bir biçimde tartışıldığı ifade edilmektedir (Bülbül, 2018).

Yaşanan gelişmelerden sonra bu olayın öncesinde de bir sızıntı olup olmadığı hususu Demokratik Ulusal Komite tarafından dile getirilmiştir. Bu kapsamda bu olayın araştırılması için CrowdStrike adlı bir siber güvenlik şirketinden yardım talebinde bulunulmuştur. CrowdStrike tarafından gerçekleştirilen araştırmalar sonucunda iki farklı tarihte komiteye izinsiz bir biçimde giriş yapıldığı görülmüştür. Bu durum üzerine konuya ilişkin olarak FBI soruşturma başlatmıştır. 22 Temmuz'da gerçekleşen olaydan iki gün sonra ise Hillary Clinton'un kampanyasını yöneten Robby Mook söz konusu e-maillerin Donald Trump'a yardım edilmesi amacıyla Ruslarca sızdırıldığı hususu dile getirilmiştir. Mook tarafından dile getirilen söz konusu iddia hem Rusya hem de Trump tarafından kabul edilmemiştir. Fakat ele geçirilmiş olan dosyaların hepsinin halk ile paylaşılması gerektiği Donald Trump tarafından dile getirilmiştir (Inkster, 2016).

Rusya Federasyonu'nun Amerika Birleşik Devletleri'nde gerçekleştirilen seçimlere müdahalede bulunduğuna ilişkin deliller yeterli nitelik taşımamaktadır. Ancak

bu duruma rağmen kaynakların büyük bir kısmı Rusya Federasyonu'nun ABD seçimlerine müdahale ettiğini destekleyici nitelik taşımaktadır. Aşağıda sıralanan kurumlar tarafından Rusya'nın ABD'deki seçimleri etkileyebilmek için oldukça karmaşık bir kampanya yürüttüğünü dile getirmiştir:

- CIA
- NSA
- FBI

Bununla birlikte yukarıda sıralanan kurumlar tarafından bu iddianın sadece bir varsayım olduğu hususu da dile getirilmiştir. Kremlin'e bağlı olarak faaliyet gösteren kişilerin birçok eyalette seçimle ilgili bilgisayar sistemlerine sızmaya çalıştığının tespit edildiği Department of Homeland Security tarafından ifade edilmiştir. 2018 yılının şubat ayında ise özel yetkili savcı Robert Mueller ile yanındaki birçok federal savcı ABD'nin siyasi sistemine müdahale edilmesine ilişkin faaliyetlerde bulundukları gerekçesiyle Rus şirketlerinden bazılarını suçlamışlardır. ABD'deki hukukçular hem Demokrat Parti hem de Cumhuriyetçi Parti'nin sistemlerine sızıldığı inancına sahiptir. Bununla birlikte 2016 yılında Demokrat Parti'den çalınmış olan e-maillerden daha önce sisteme sızıldığı dile getirilmektedir. Fakat söz konusu müdahalelerin Rusya tarafından gerçekleştirilmiş olup olmadığı hususu ile birlikte bu müdahalelerin ABD'deki başkanlık seçimleri üzerinde ne derece etkili olduğu sorusu da sorulmaktadır (Masters, 2018).

### 3.2.3. Estonya siber savaş alanı:

2007 yılında Estonya'ya karşı Rusya Federasyonu tarafından gerçekleştirilen siber saldırı bir ülkenin diğer bir ülkeye karşı yaptığı ilk saldırı olarak nitelendirilmektedir. Bu yönüyle de bu saldırının tarihe geçtiği belirtilmektedir. Her ne kadar Rusya Federasyonu itiraz etmiş olsa da Estonya Parlamentosu'nun aldığı karara göre Talinn'de yer alan ve II. Dünya Savaşı'ndaki Sovyet askerlerini temsil eden "Meçhul Asker" adlı anıtın kaldırılması kararlaştırılmıştır. Bu kararın alınmasından sonra Rusya Federasyonu ve Estonya arasında gerginlik tırmanmış ve 2007 yılının Nisan ayında da siber saldırılar gerçekleştirilmeye başlanmıştır. İki ülke arasındaki gerginliğin yanı sıra NATO ittifakı ile Rusya Federasyonu arasındaki mücadelenin de söz konusu saldırıların gerçekleştirilmesi noktasında etkili olduğu ifade edilmektedir (Bıçakçı, 2014, s. 121).

Rusya Federasyonu tarafından gerçekleştirilen saldırılardan sonra Estonya'daki bilgisayarların büyük bir kısmı kullanılamayacak hale gelmiştir. Ayrıca şu hususlara ilişkin olarak da önemli ölçüde zarar verilmiştir:

- Siyasi partiler
- Devlet kurumları
- Bankacılık sistemi
- İnternet altyapısı

Her ne kadar söz konusu olaya ilişkin olarak Estonya tarafından Rusya Federasyonu suçlanmış olsa da Rusya Federasyonu söz konusu saldırıları asla kabullenmemiştir (Darıcılı, 2014, s. 6).

Şu kurum ve kuruluşlardaki bilgisayarlar gerçekleştirilen saldırı sonrasında kullanılamaz hale gelmiştir:

- Estonya devlet başkanlığı
- Estonya parlamentosu
- Bakanlıklar
- Siyasi partiler
- Ülkedeki haberleşme kuruluşlarının büyük bir kısmı
- En büyük iki banka
- İki iletişim kuruluşu

Bununla birlikte söz konusu saldırıdan sonra Estonya'da hayatın neredeyse durduğu ifade edilmektedir. Bu saldırı sonrasında NATO ve AB de teyakkuza geçmiştir. NATO tarafından siber güvenlik uzmanları Estonya'ya gönderilmiş ve söz konusu saldırının kapsamı tespit edilmeye çalışılmıştır (Çakmak ve Altunok, s. 121-122).

Meydana gelen bu olay neticesinde siber güvenlik kavramı ve siber saldırıların uluslararası ilişkiler kapsamında yeniden değerlendirilmesi gerekmiştir. Bu olay bu açıdan da oldukça büyük bir önem arz etmektedir. Meydana gelen saldırıdan sonraki süreçte siber uzay tıpkı soğuk savaş döneminde olduğu gibi yeniden bir rekabet alanı olarak görülmeye başlanmıştır (Roth, 2009, s. 14).

### 3.2.4. Gürcistan ve Rusya mücadelesi:

Güney Osetya bölgesinde meydana gelen problemlerden dolayı 2008 yılının Ağustos ayında Rusya ve Gürcistan arasında çatışmalar başladığı ifade edilmiştir. Hem askeri harekât gerçekleşmeden önce hem de askeri harekât sırasında Rusya'nın siber saldırılar gerçekleştirdiği iddia edilmektedir. Söz konusu siber saldırılar kapsamında Gürcistan Devlet Başkanlığı'nın resmi internet sitesindeki Başkan'ın resmi değiştirilip yerine Adolf Hitler'in resmi koyulmuştur. Daha sonra ise siber saldırılar ülkenin tamamına yayılmıştır. Sonraki süreçte Rusya tarafından gerçekleştirilen saldırıların servis dışı bırakma saldırısı (DDoS) olduğu belirlenmiştir. Gerçekleştirilen siber saldırılarda devlet internet sitelerine grafiti resimleri koyulmuştur. Bu kapsamda klasik biçimdeki saldırılar ile siber saldırılar birbiri ile koordineli olarak gerçekleştirilmiştir. Rusya tarafından gerçekleştirilen saldırılar incelendiğinde kullanılan kredi kartlarının ABD'den çalınmış olduğu ve kullanılan internet sitelerinin ise Rusya ve Türkiye'de açıldığı tespit edilmiştir (Bıçakçı, 2012, s. 219).

BBC ve CNN gibi birçok internet sitesine Gürcistan'ın girişi bu saldırılar ile engellenmiştir. Gürcistan'a trafik sağlayan tüm yönlendiricilerin Rusya siber güvenlik uzmanları tarafından ele geçirildiği ifade edilmektedir. Bu şekilde Gürcistan dışarıyla iletişim kuramamıştır. Bu kapsamda Gürcistan'dan dışarıya e-mail dahi yollanamadığı ifade edilmektedir. Bununla birlikte gelişmiş bilgisayar bilgisi olmayan kullanıcıların da köle bilgisayar yöntemiyle saldırıya destek vermesi sağlanarak yığın dosyaları dağıtılmıştır. Bu şekilde saldırıyı gerçekleştiren kaynakların artırılması amaçlanmıştır (Kara, 2013, s. 49).

Söz konusu müdahalenin en önemli özelliğinin ise kara operasyonu ile birlikte siber saldırıların birbirleri ile koordineli bir biçimde gerçekleştirilmesi olduğu belirtilmektedir. Diğer siber saldırıların büyük bir kısmı gibi söz konusu saldırının da Rusya Federasyonu ile bağlantısı açık bir biçimde ortaya koyulamamıştır. Fakat bu konuya ilgili olan çeşitli siber güvenlik şirketleri, Gürcistan'a karşı gerçekleştirilen siber saldırıların iki aşamadan meydana geldiğini belirlemiştir. Bu kapsamda ilk aşama 7 Ağustos'ta Rus hackerler tarafından Gürcistan haber ajanslarının hedeflenmesi olmuştur. Söz konusu saldırılar DDoS saldırısı olarak nitelendirilmektedir. Gürcistan haber sitelerine karşı saldırılar sürerken saldırı listeleri genişletilmiştir. Bu durum da ikinci

aşamayı meydana getirmektedir. Bu kapsamda saldırının şu kurum ve kuruluşlara yapıldığı belirtilmektedir (Shakarian, 2011):

- Finansal kurumlar
- İşletmeler
- Eğitim kurumları
- CNN
- BBC

Bununla birlikte söz konusu saldırıların yalnızca DDoS saldırılarından ibaret olmadığı ve söz konusu kurum ve kuruluşların internet sitelerinin de zarar gördüğü hususu ifade edilmektedir.

### 3.2.5. Hainan Adası olayı:

1 Nisan 2001'de, bir ABD gözetleme uçağı, Çin'in güney sahilinin yaklaşık 100 kilometre açığındaki Hainan Adası yakınlarında uçuyordu. Önlemek için iki Çin savaş uçağı gönderildi ve havada bir çarpışma meydana gelmiştir. ABD uçağına zarar vermiş ve 24 mürettebatın Çinliler tarafından gözaltına alındığı Hainan Adası'ndaki Lingshui askeri havaalanına acil iniş yapmasına neden olmuştur. Çin jeti Güney Çin Denizi'ne düşerek pilotu öldürmüştür. Artan gerilimler, 24 havacının serbest bırakılması ve uçağın geri dönüşü konusundaki müzakereleri karmaşıklaştırmıştır.

Olayın ilk gününde Çin sözcüsü Zhu Bangzao, Çin askeri jetlerinin Çin'in su alanları üzerinde ABD gözetleme uçaklarını izlemesinin normal ve uluslararası uygulamalara uygun olduğunu ve düşüşün doğrudan nedeninin ABD uçağının düşmesi olduğunu belirtmiştir. Üstelik ABD uçağının Çin hava sahasına girmiş ve izinsiz indiği ifade edilmiştir. Bu nedenle Birleşik Devletler'in tüm sorumluluğu üstlenmesi gerektiği belirtilmiştir (P.R.C. Embassy, 2001). Daha sonra yaklaşık olarak 80.000 Çinli tarafından ABD hükümetine karşı siber saldırılar başlatılmıştır. Sonraki süreçte bu olay Birinci İnternet Savaşı (World Wide Web War I) olarak adlandırılmıştır (Çeliktaş, 2016, s. 53-54).

ABD'nin resmi pozisyonu hiçbir suçlamada bulunmamıştır ("U.S. Aircraft Collides," 2001). Daha sonra basında çıkan haberlere göre, Çinli pilot Wang Wei'nin

ABD'li pilotlar tarafından özellikle ABD keşif uçaklarıyla karşılaştığında agresif olduğu ve Çin jetinin ABD uçağına çarptığı anlaşılmıştır. Ayrıca, inmeden önce, hasarlı uçağın mürettebatı, yanıtsız kalan birden fazla acil durum tehlike sinyali yayınlamıştır (Richter, 2001).

4 Nisan'da Beyaz Saray Basın Sözcüsü Ari Fleischer, "Kaza uluslararası hava sahasında, uluslararası sularda gerçekleşti ve özür dilemek için herhangi bir neden bulamıyoruz. Birleşik Devletler yanlış bir şey yapmadı" demiştir (Basın Sekreteri Ofisi, Beyaz Saray, 2001a). ABD'nin tutumu, Birleşmiş Milletler Deniz Hukuku Sözleşmesi'ne göre, ABD'nin bölgede askeri uçak uçurma hakkına sahip olduğuydu. Ancak 5 Nisan'da Başkan Bush, "Çinli bir pilotun kaybolmasına üzülüyorum ve uçaklarından birinin kaybolmasına üzülüyorum ve dualarımız pilot ve ailesi için" diyerek yanıtı yumuşatmıştır (Basın Sekreteri, Beyaz Saray, 2001b).

Olayın sonucu, karşılıklı olarak kabul edilebilir bir son olarak görülmüştür. Her iki taraf da istediklerini almıştır. ABD için 24 ABD mürettebatının özgürlüğü ve Çin ile yüzleşme. Her ikisi de diplomatik zaferlerini uluslararası alanda iddia ederken, vatandaşlarına farklı mesajlar vermiştir.

### 3.2.6. Kosova Savaşı:

1999 yılında NATO'nun Kosova operasyonunu gerçekleştirdiği bilinmektedir. Bu operasyon kapsamında siber saldırılar da gerçekleştirilmiştir. Bu saldırıların dünya genelinde gerçekleştirilmiş olan ilk geniş kapsamlı İnternet Savaşı olduğu belirtilmektedir (Geers, 2012).

Sırbistan'ın NATO uçakları tarafından bombalanmaya başlanmasından sonra Sırpları destekleyen birçok hacker grubu NATO'nun internet altyapısına saldırılar gerçekleştirmiştir (Geers, 2012).

Operasyon süresinde hacker gruplarının NATO'nun internet altyapısına virüslü e-mailler ve DDoS saldırıları ile saldırdığı ifade edilmektedir. Bu kapsamda ABD'deki Beyaz Saray'ın internet sitesinin ana sayfası değiştirilmiştir. Bununla birlikte İngiltere de veri kaybettiğini ifade etmiştir (Geers, 2012).

NATO tarafından gerçekleştirilen operasyon sırasında bir hata sonucunda Çin Elçiliği de bombalanmıştır. Bu olay üzerine siber saldırılara Çinli hackerler de destek

vermiş ve Amerikan resmi internet sitelerine saldırılar gerçekleştirilmiştir (Messmer, 1999).

Saldırganların bu saldırılar kapsamındaki en önemli başarısının NATO'nun halkla ilişkiler sitesi üzerinde elde ettiği ifade edilmektedir. Gerçekleştirilen saldırılar sonucunda söz konusu internet sitesi günlerce aktif olamamıştır (Geers, 2012).

### 3.3.7. Panama belgeleri:

Wikileaks belgelerinin sızdırılması ve "Panama Belgeleri" şeklinde yayımlanan belgeler siber güvenlik konusunun gündeme gelmesine neden olmuştur. Dünyanın dördüncü büyük offshore firması Mossack Fonseca'nın veri tabanından 11,5 milyon adet belge ele geçirilmiştir. Söz konusu belgeler Uluslararası Araştırmacı Gazeteciler Konsorsiyumu (International Consortium of Investigative Journalists-ICIJ) aracılığıyla dünya ile paylaşılmıştır. Söz konusu belgelerde birçok kişinin vergi kaçırma ve para aklama gibi illegal faaliyetlere giriştiği ortaya koyulmuştur. Söz konusu kişiler arasında şunlar da bulunmaktadır:

- Siyasi liderler
- Bürokratlar
- İş adamları
- Ünlüler

12 siyasi lider ve offshore vergi cennetlerini kullanan 143 siyasetçi ile aileleri söz konusu belgelerde bulunmaktadır (Erdurucan, 2017, s. 23-24). Panama Belgeleri'nin normal bir okuyucu için çok fazla bir anlam ifade etmeyeceği belirtilmektedir. Ancak söz konusu belgeler gazeteciler tarafından analiz edilmiş ve bu şekilde yankı uyandıran haberler yapılmıştır. Panama Belgeleri'nin kanuni ve siyasal olarak oldukça önemli etkilere sahip olduğu ifade edilmektedir. Bununla birlikte söz konusu belgelerin yayımlanmasının gazetecilik faaliyetleri bakımından da oldukça büyük önem arz ettiği bilinmektedir. Bu kapsamda yeni medyanın sunmuş olduğu imkânlardan yararlanılmış ve geniş bir iş birliği ile araştırmacı gazetecilik örneği sergilenmiştir. Günümüze kadar olan süreç göz önünde bulundurulduğunda söz konusu veri sızıntısının en geniş kapsamlısı olduğu belirtilmektedir. Panama ve Wikileaks belgeleri ile birlikte siber güvenlik konusu

da uluslararası siyasetin en önemli gündemlerinden biri olma özelliğine sahip olmuştur (Atalay, 2018, s. 143).

### 3.2.8. Rusya'nın Ukrayna'ya müdahalesi:

Ukrayna Devlet Başkanı olan Viktor Yanıkovich 2014 yılının Şubat ayında görevinden uzaklaştırılmıştır. Bu durum da Ukrayna ve Rusya Federasyonu arasındaki sıcak çatışma sürecinin başlangıcı olarak kabul edilmiştir (Medvedev, 2014).

Rusya Federasyonu'nun Gürcistan'a karşı gerçekleştirdiği askeri harekât sırasında görülen resmi nitelik taşımayan savaş doktrini Rus hibrit savaş konsepti olarak adlandırılmaktadır. Söz konusu stratejinin kapsamında şu hususlar yer almaktadır (Medvedev, 2014):

- Siber saldırı teknikleri kullanılması
- Mücadele edilen devletin askeri gücünün azaltılması
- Yerel ve küresel olarak enformasyon teknikleri kullanılarak Rusya Federasyonu lehine bir propaganda yapılması
- Karşı ülkede bulunan akraba ve dost topluluklar kullanılarak koordineli bir bircimde özel kuvvet operasyonları gerçekleştirilmesi

Rusya Federasyonu tarafından Ukrayna'ya ilk müdahale 2014 yılının şubat ve mart ayları arasında gerçekleştirilmiştir. Söz konusu müdahale kapsamında 150.000 asker görev almış ve bir şaşırtma tatbikatı yapılmıştır. Söz konusu tatbikat düşük bir tempoya sahip güç gösterisi biçiminde gerçekleştirilmiştir. Bununla birlikte Kırım'a karşı askeri güç kullanılmasına onay veren bir kanun da Rusya Federasyonu Parlamentosu tarafından çıkarılmıştır (Gürcan, 2014).

Ukrayna'nın İç Güvenlik Birimi'nin Başkanı olan Valenty Nalyvaichenko da 2014 yılının şubat ayından itibaren Ukrayna'nın internet ve mobil telefon altyapılarının saldırıya uğradığını ifade etmiştir. Bununla birlikte bilhassa Ukraynalı milletvekilleri ve bürokratlar tarafından kullanılan akıllı telefonların hacklendiği de dile getirilmiştir. Bununla birlikte CyberBerkut adlı Rusların yanında yer alan bir hacker grubu da şu kurum ve kuruluşlara yönelik DDoS saldırıları gerçekleştirmiştir (Lee, 2014):

- Ukrayna Silahlı Kuvvetleri
- Ukrayna resmi internet siteleri

- Ukrayna ile ilişkili olarak faaliyetler gerçekleştiren NATO'nun internet erişimi
- Ukrayna medya kuruluşları

Söz konusu siber saldırıların Gürcistan ve Estonya'ya karşı gerçekleştirilen siber saldırılara karşı daha etkili olduğu ve daha detaylı olarak planlandığı ifade edilmektedir. Saldırılarda "Snake/Uroboros" adlı yazılım kullanılmıştır. Söz konusu yazılımın Ukrayna'nın resmî kurumlarına karşı gerçekleştirilen siber saldırılarda oldukça etkili olduğu belirtilmektedir (Weedon vd., 2014).

Ukrayna'ya karşı gerçekleştirilen siber saldırıların etkili bir biçimde gerçekleştirilmesinin bir başka sebebi olarak ise Ukrayna'nın internet altyapısını özellikleri gösterilmektedir. Ukrayna hükümetleri tarafından sınırlandırıcı nitelikte çalışmalar yürütülse de Ukrayna'da liberal internet kullanımı politikasının hâkim olduğu bilinmektedir. Bununla birlikte Ukrayna'nın küresel internet sistemi ile ilgili hem uydu hem de karasal bir yapı aracılığıyla sağlanmaktadır. Bu sebeple internet kullanımına ilişkin politikalar serbestlik ilkesi kapsamında biçimlenmektedir. Ayrıca Ukrayna'nın global internet sistemi ile de iletişim içinde olduğu ifade edilmektedir. Bu nedenle Ukrayna her ne kadar internet sistemini dış dünyaya kapatmaya ilişkin girişimlerde bulunmuş ise de söz konusu girişimler başarısız olmuştur. Bu durum da siber saldırıların etkili olmasını ve yaygınlaşmasını sağlamıştır (Kelly, 2014).

Söz konusu siber saldırılar ile birlikte Rus taraftarı olan sivil protestocular da Sivastopol'da şiddet unsurunun kullanılmadığı sokak eylemleri gerçekleştirilmiştir. Söz konusu eylemlerde Rusya Federasyonu'na bağlanma isteği dile getirilmiştir. Ayrıca Kırım'da bulunan ve Rus taraftarı olan Russkoye Yedinstvo Partisi de Kırım Ruslarının güvenliğinin sağlanması amacıyla bir hafta içinde 10.000 kişiden meydana gelen silahlı bir güç oluşturduğunu ifade etmiştir. Söz konusu grupların bir hafta gibi oldukça kısa sayılabilecek bir sürede organize edildikleri göz önünde bulundurulduğunda Rus özel kuvvetlerinin bu gruplar ile doğrudan ilişki içinde oldukları görülebilmektedir.

Rusya Federasyonu tarafından gerçekleştirilen siber saldırılar sonucunda Ukrayna'nın direnme gücü oldukça azalmıştır. Bu durum da sıcak çatışmanın başlamasından önce Kırım'ın küresel sistemden ve Ukrayna'dan izole edilmesine ilişkin planlar yapılmasına yol açmıştır. Bu amaçla 2014 yılının mart ayında Ukrayna'nın resmi

mobil iletişim şirketi Ukrtelecom'un altyapısı çökertilmiştir. Bu şekilde Kırım'da bulunan cep telefonlarının sıcak çatışma başladıktan sonra kullanılması önlenmiştir. Ayrıca şunların da gerçekleştiği ifade edilmektedir (Gürcan, 2014):

- İnternet erişiminde de önemli ölçüde yavaşlama
- Kritik nitelikteki altyapıları kullanılamaz hale getiren siber saldırılar gerçekleştirilmesi
- Sivastopol limanında yer alan Rus savaş gemilerinden Kırım'daki radyo ve televizyon yayınlarını engelleyecek nitelikte elektronik karıştırmalar yapılması
- Kırım'daki fiber optik kablo altyapısının hasar görmesi

2014 yılının nisan ayına kadar olan süreçte ise Donetsk ve Lugansk bölgelerinin büyük bir kısmı Rus taraftarı olan isyancılar tarafından ele geçirilmiştir. Ayrıca söz konusu isyancıların Rus özel kuvvetleri tarafından yönlendirildiği, silahlandırıldığı ve eğitildiği de ifade edilmektedir. Bununla birlikte hükümet binaları ve karakollarda da Rusya Federasyonu'nun bayrağı göndere çekilmiştir. Lugansk ve Donetsk gibi oldukça büyük olarak nitelendirilebilecek olan şehirler de isyancılar tarafından ele geçirilmiştir.

### 3.3. Genel Değerlendirme ve sonuç:

Savaşla şiddetin ortadan kaldırılıp kaldırılamayacağına dair sorunsal, uluslararası ilişkilerin, Birinci Dünya Savaşı'ndan sonra sistemli bir bilimsel disiplin olmasından başlayarak, değişik araştırmaların merkezinde yer almıştır. Soğuk Savaş'tan sonraki dönemin getirmiş olduğu yenilik, uluslararası ilişkiler alan yazını üstünde ciddi bir etkisi olan güvenliğin tabiatına ilişkin yeni modeller ortaya çıkmıştır (Baylis, 2008: 71).

Bilhassa savaş teknolojilerindeki gelişim ve istihbarat yapısıyla alakalı genel değişim "siber güvenlik" terimiyle ilgili yaklaşımlarla uluslararası ilişkilerin bu yönüyle ilgili faaliyetleri süratlendirmiştir. Son yıllarda uluslararası güvenlikle ilgili olarak değişik ve kendine has bir perspektif geliştiren normatif uluslararası ilişkiler yaklaşımları ile siber güvenlikle ilgili kuramsal düzlem harmanlanmış ve "siber güvenlik" teriminin uluslararası sahadaki belirginliği daha da artmıştır.

Devletlerin menfaat amaçları, yeni savaşlar ve saldırı metotlarını beraberinde getirmiştir. Böylelikle "Siber Terörizm", "Siber Saldırılar", "Siber Caydırıcılık", "Siber

Güvenlik" gibi terimler değişik gelişmelerle uluslararası sahada da değişik bir çatışma sahasını ortaya çıkarmıştır.

Nükleer caydırıcılığın tersine siber caydırıcılıkta taarruz yeteneği, yer ve zamanı bilinmez iken; telafi edilemeyen iktisadi kayıplar ortaya çıkabilmektedir. Üstelik can kaybı da söz konusu olmamaktadır. Öte yandan saldırı ve savunmada daha etkili manevralar yapılabilmekte ve böylelikle zararlar minimuma indirilebilmektedir. Ancak siber saldırı ya da terörizmin caydırıcılığı, sadece somut olarak uygulandığı zaman söz konusu olabilmektedir (Güntay, 2015: 479). Caydırıcılığın yönünün ve boyutunun artması ile siber güvenlik uluslararası hale gelen bir terim olmuştur. Tartışılabildiği boyut Soğuk Savaş devrinin geleneksel caydırma teorileri ile izah edilmese de süper güçlerin yükselişi ile tesirini artırmış olan "siber güvenlik" terimi 1939 ile öncesindeki uluslararası sistemde kendine yer bulamamıştır (Zagare ve Kilgour, 2000: 4).

"Siber güvenlik" teriminin uluslararası ilişkilerde inceleme boyutunun bulunmasının başlangıç noktasında caydırıcılık ve uygulama alanıyla ilgili somut hadiselerin artışa geçmesi yer almaktadır. Nitekim Soğuk Savaş'ın bitişiyle söz konusu parametrelerdeki gelişmenin süratlenmesi daha önce değinilen "siber terörizm", "siber savaş" ile "siber güvenlik" gibi terimlerin uluslararası ilişkilerde incelenmesini mecburi duruma getirmiştir. Bir taraftan siber savaşın yönünün Soğuk Savaş'tan sonra hızla devam etmesi, diğer taraftan zararlı yazılımların ve siber suçların uluslararası çapta etki yaratmasıyla siber olayların artışı uluslararasında boyutta iş birliğini de gerekli hale getirmiştir.

Tarihsel süreç içinde siber olayların güvenlik boyutuna dönüşmesi, 1960 ile 1970'li yıllarda tartışılmış olan bilgi devriminin kendi içindeki temel değişiklikler ve medya araçlarıyla inovasyon çerçevesindeki ögelerin etkilemesi ile de ilgilidir. Öyle ki kimi toplumsal hareketlerde ve verilerin sızdırılmasına yönelik olarak gerçekleşebilecek anlık iletişimde siber vasıtalar aktif olarak kullanılmakta ve bu tip hadiseler devletler tarafından yakın takibe alınmaktadır (Cavelty, 2008: 13). Söz konusu takip içerisinde devletlerin ismini tam koymadığı ve bazı bilim adamlarınca radikalleş(tir)me vasıtası şeklinde de kullanılmış olan, internetle medya etkileşimi yeni bir savaş aracı şeklinde görülmektedir. Söz konusu durum özellikle sosyal hareketlenmelerde daha da gözle görülür bir durum haline gelmektedir (Hoskins ve O'Loughlin, 2008: 31).

İkinci Dünya Savaşı'ndan sonra meydana gelen uluslararası sistemi tanımlamak üzere kullanılan "Soğuk Savaş" daha önce de dile getirildiği üzere, iki kutuplu dönemde Amerika ve Rusya'nın liderliğindeki Avrupa ile Doğu Bloku arasında gerginlikle kısmi çatışma şeklinde devam eden bir mücadele şeklinde kendini göstermektedir. Ulusal güvenlik, Soğuk Savaş aşamasındaki uluslararası sistemi biçimlendiren ve ulus devletler arasındaki ilişkileri tanzim eden ana öge şeklinde belirginleşmiştir.

Siber güvenliğin çağımızdaki boyutuna varmasında, Soğuk Savaş döneminin güvenlik modeli içinde yer alan önemli faktörler bulunmaktadır. Sönmezoğlu, bu durumun meydana gelmesinde güvenlik yaklaşımıyla ilgili üç belirleyici niteliği aşağıdaki şekilde ifade etmiştir (2014: 719):

> *"İlk olarak NATO ile Varşova paktı gibi, güvenliğe ilişkin kararların alındığı iki merkezde süreç çatışmaya dönük bir görünümde seyretmiş ve savaş teknolojilerine ilişkin gelişmeler karşılıklı olarak izlenmiş, geliştirilmiştir.*
>
> *İkincisi, bloklar ekonomik ve askeri yapılanmalarla üçüncü dünya ülkelerini kendi etki alanlarına sokmak adına uluslararası ilişkilerde çekişme içine girmişlerdir ve uzak coğrafyalara etki edebilme adına sibernetiğe ilişkin öz gelişim göstermiştir.*
>
> *Üçüncüsü ise silahların kitlesel yok edici özelliği savaşları önleyici bir hal almış ve bu da yine müdahele anlamında farklı araçların gelişimini hızlandırmıştır. Sisteme ilişkin stratejik denge farklı unsurlarla oluşturulmaya başlanmış ve arayış içine girilmiştir."* (Sönmezoğlu, 2014: 719).

İkinci Dünya Savaşı'ndan sonra bu özelliklerin yanı sıra istihbaratla ilgili teknolojik bilginin artması siber güvenliğin bu süreçte önemini arttırmıştır. Öncesinde istihbarat yalnızca savaşı kazanmak üzere gerekli görülür iken sinyalle görüntü istihbaratıyla ilgili önemin fark edilmesi teknolojideki arayışları siber güvenliğin uluslararası ilişkiler boyutuna itmiştir. Çok kısa bir süre içinde U-2 Keşif Uçakları, uzay programları, en eski bilgisayar örnekleriyle ve örtülü operasyonlarla alakalı özel araçların gelişmesi hususunda önemli girişimlerde bulunulmuştur (Yılmaz ve Salcan, 2008: 25).

Özellikle Amerika'nın, Rusya'nın uydusu Sputnik'e karşılık olarak, ileri bilimsel ve teknolojik projeleri yaşama dökmekle görevli ARPA'yı devreye sokması 1958 yılını bu anlamda bir milat haline getirmiştir. 1969 yılına gelindiğindeyse ABD'nin öncü üniversiteleriyle enstitüleri kendi aralarında bilgi alışverişi temin etmek için Amerika

Savunma Bakanlığınca desteklenmiş olan ve o zamana dek daha ziyade askeri amaçlarla kullanılmış olan ARPAnet ağına dahil olmuştur.

1974 yılına gelindiği zaman, Bob Kahn ile Vint Cerf isimli bilim insanları birbirlerinden bağımsız ağlarda bulunan kullanıcıların iletişime geçebilmesiyle data gönderimi yapabilen devrim özelliğindeki TCP protokolünü üretmiştir. Özellikle siber güvenliğin uluslararası sahaya sıçraması ve siber olayların bu sahayı etkilemesine dair hadiselerin yaşanması TCP'nin süratli bir biçimde gelişmesi ile başlamıştır.

SSCB 1980'li senelerin ortasına dek bilgisayar teknolojilerinin tamamını KGB vasıtasıyla Avrupa'dan çalmayı sürdürmüştür. SSCB'nin bilgi alma girişimleri 1981 senesinde Amerika ile Fransa'nın gerçekleştirdiği müşterek bir operasyon ile ortaya çıkarılmıştır. SSCB'nin bilhassa bugüne dek gelen bölgesel siber saldırganlığıyla hegemonik bir bölgesel siber güç şeklinde görülmesi 1980'li yıllarda bahsi geçen faaliyetlerine benzer olaylara uzanmaktadır (Hansen ve Nissenbaum, 2009: 1169).

Soğuk Savaş'ın bitmesine yakın dönemlerde ülkelerin kendi altyapılarının da önemli bir biçimde etkilendiği Morris virüsü, bilişim sisteminin karanlık tarafına geçen birçok yazılımcı için iştah açıcı bir durum olmuştur ve uluslararası sahada siber güvenlikle ilgili dataların önemiyle ilgili önemli bir gelişme olmuştur. Dijital saldırganlıkla yakın zamanlardaki boyutlar adına doneler veren, Soğuk Savaş'ın sonlarında yaşanan hadiseler siber güvenliğin bilgi çağında teknik boyutu ile kendisinden söz ettireceğini ve toplumsal bilimlerle uluslararası ilişkilerde de büyük bir yer edineceğini göstermiştir.

İkinci Dünya Savaşı'nın bitmesinden sonra Soğuk Savaşın başlaması ile beraber yeni bir güvenlik sistemi kurulmuştur. Sıcak çatışmalardan uzak kalınmış olan bu devirde, güvenlik endişesi ve dolayısıyla uluslararası sistemin tansiyonu sürekli yüksek seyretmiştir. 1989 senesinde Berlin Duvarı'nın yıkılmasının ardından, 25 Aralık 1991 tarihinde SSCB'nin dağılması ile beraber, uluslararası sistem için gerilimli bu iki kutuplu devir yavaşça bitmiştir (Bıçakçı, 2012: 206).

SSCB ve liderliğini gerçekleştirdiği Doğu Blokunun ortadan kalkması sonucunda karşısındaki simetrik somut bir düşmanı yitiren NATO'nun meşruluğu da sorgulanmıştır. NATO'nun görevinin artırılması ve ittifakların güvenlik sahasının genişletilmesine

yönelik olarak "1990 Londra Konferansı"nda yeni bir stratejinin geliştirilmesi kararı alınmıştır, "1991 Roma Zirvesi"yle yeni stratejik anlayış üretilmiştir (Bayraktar, 2015: 37). Siber güvenlikle ilgili siyasi düzlemde atılan yeni adımlar sayesinde NATO, kendisine önemli misyonlar edinmiştir. Birbirinin ardından gelen tatbikatlar ve zirveler ile siber güvenlikle ilgili tüm adımlar NATO'yu biraz daha öne çıkarmıştır (Healey ve Jordan, 2014: 3).

Soğuk Savaş döneminde simetrik bir düşmanı olan NATO'nun, Kosova Savaşı'nda karşı karşıya kaldığı siber saldırıların sonucunda söz konusu bakış açısını dönüştürerek, Soğuk Savaş'tan sonra en önemli atılımı gerçekleştiren örgütlenme olduğu dile getirilmektir. Özellikle sırası ile 11 Eylül saldırıları, NATO'nun bir müttefiki olan Estonya'ya dönük siber saldırılar sonrasında NATO ile üye devletleri siber tehditler ve siber güvenlik hususlarında daha da ihtiyatlı olmaya başlamıştır (Boyraz, 2015).

Soğuk Savaşta tartışılan ve uluslararası faaliyetlerde önemli bir yeri bulunan klasik ve nükleer caydırıcılığın yanına "siber caydırıcılık" teriminin eklenmesiyle devletler arasında yeni bir etkileşim oluşmuştur. Ayrıca siber caydırıcılığın da klasik ve nükleer caydırıcılık vb. fonksiyona sahip olacağına dair somut veriler ortaya konmuştur.

Siber caydırıcılıkla ilgili somut dataların Soğuk Savaştan sonra etkili olmasında ise askeri-stratejik ortamla ilgili değişimler etkilidir. Billhassa 2010 yılının başına dek geleneksel ögelerin etkili olduğu ve değişkenlerin yalnızca söz konusu silahların aktivitesinin artırılması üstüne kurulması, finans açısından da kaynakları bu tarafa yönlendirmiştir. Son yıllarda meydana gelen finans krizleri daha az maliyet ile caydırıcı olabilmesi sebebiyle siber kabiliyetlerin öne çıkarılmasını bir gereklilik olmaktan çıkarıp, mecburiyete dönüştürmüştür.

Siber kabiliyetlerin öne çıkarılması, gelişmiş devletler başta olmak üzere bütün devletlerin öncelikli sahası olmuştur. 1990'lı yılların ortasında ise Çin, Körfez Savaş'ından aldığı dersler çerçevesinde, stratejisini değiştiren devletlerin başında gelmiştir ve siber tesir bakımından Soğuk Savaş'tan sonra önemli düzeyde yükselen bir güç haline gelmiştir. Böylelikle Çin de ordusunu küçülterek, yeni teknolojiler için yatırım yapan devletler arasına dahil olmuştur (Clarke ve Knake, 2011: 33). Söz konusu gelişmelerle güvenlik ikileminin askeri döngüsü, siber savaş sahasına kaymıştır. Aynı zamanda ideolojik yakınlıklarla beraber daha güçsüz devletlerin birbirine olan

yaklaşımının yakın zamanda siber güvenliği dinamik tutacağı ve değişik siyasi birliktelikleri beraberinde getireceği de savunulmaktadır (Hare, 2010: 216).

Çalışmanın önceki bölümlerinde aktarıldığı üzere gerek uluslararası örgütler gerekse devletler, siber alanın giderek artan önemini göz önünde bulundurarak, kendi içlerinde siber yapılanmalar ve politikalar oluşturmuştur. Ele alınan siber olaylar da devletler için söz konusu alanın ne kadar önemli olduğunu göstermektedir. Gerek çizilen genel tablo gerekse ele alınan siber olaylar klasik güç dengesi sisteminde olduğu kadar net bir şekilde siber alanda aktörleri izleyebilmenin mümkün olmadığını göstermektedir. Bu sebeple siber alanda klasik güç dengesi sisteminden bahsedebilmek çok da mümkün görünmemektedir. Ancak uluslararası platformda süregelen bir güç dengesine paralel ilerleyen bir siber dengelemeden bahsedilebilmektedir. Bunun en önemli kanıtını örneklerde de üzerinde durulduğu üzere uluslararası ilişkileri yöneten aktörlerin klasik güçlerini siber güçleriyle destekleyerek aldıkları aksiyonlarda kullanmaları oluşturmaktadır.

## KAYNAKÇA


Abbate, J. (1999). *Inventing the Internet*. The MIT Press.

ABD İç Güvenlik Bakanlığı (2016). "*Executive Summary of Grizzly Steppe Findings from Homeland Security Assistant Secretary for Public Affairs Todd Breasseale*".

ABD Milli İstihbarat Direktör Ofisi (2017). *"Background to Assessing Russian Activities and Intentions in Recent US Elections"*: The Analytic Process and Cyber Incident Attribution. https://www.dni.gov/files/documents/ICA_2017_01.pdf (Erişim Tarihi: 18.04.2022).

ABD Savunma Bakanlığı (2010). *"U.S. Cyber Command Fact Sheet".* https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-038.pdf (Erişim Tarihi: 10.04.2022)

ABD Savunma Bakanlığı (2019). *"Combatant Commands".* https://www.defense.gov/Our-Story/Combatant-Commands/ (Erişim Tarihi: 10.04.2022).

ABD Siber Komutanlığı (2019a). *"U.S. Cyber Command History".* https://www.cybercom.mil/About/History/ (Erişim Tarihi: 10.04.2022).

ABD Siber Komutanlığı (2019b). "*Components".* https://www.cybercom.mil/Components/ (Erişim Tarihi: 10.04.2022)

ABD Ulusal Siber Güvenlik Stratejisi (2018). *"National Cyber Strategy".* https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (Erişim Tarihi: 10.04.2022).

Acton, L. (1907). *"Letter to Bishop Mandell Creighton, April 5, 1887"* published in Historical Essays and Studies, ed., J. N. Figgis ve R. V. Laurence Londra: Macmillan.

Afacan, E. (2021, June). Blockchain Based Network Access Control (Nac) Management Solution And Architecture. In *2021 29th Signal Processing And Communications Applications Conference (Siu)* (Pp. 1-4). Ieee.

Akarslan, H. (2015). *Bilişim suçları*. İstanbul: Seçkin Yayınları.

Aksar, Y. (2013), *Teoride ve Uygulamada Uluslararası Hukuk-I*, Ankara: Seçkin Yayınları.

Akyıldız, M. (2013). *Siber Güvenlik Sızma Test Uygulamları*. Yayımlanmamış Yüksek Lisans Tezi. Isparta: Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü.

Alcaraz, C. ve Zeadally, S. (2015), Critical infrastructure protection: Requirements And Challenges For The 21st Century, *International Journal of Critical Infrastructure Protection,* 8, 53-66.

Almaz, C. ve Sevi, M. (2021). Üniversitelerdeki Siber Güvenlik Sorunları Ve Farkındalık Eğitimleri. *Bilişim Teknolojileri Dergisi*, *14*(3), 229-238.

Alptekin, V., Metin, İ. ve Akcan, A. T. (2018). *Kripto Para Ekonomisi*. Eğitim Yayınevi.

Altınkaynak, M. (2017). *Uygulamalı Siber Güvenlik Ve Hacking*, 3, İstanbul: Abaküs Yayınları.

Altunok, T. ve Kaya, Z. (2009). Siber Tehditlerle Mücadele. Çakmak H. ve Altunok T. (Ed.), *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 1. Baskı İçinde (137-162), Ankara: Barış Platin Kitabevi.

Andress, J., Winterfeld, S., (2011). *Cyber Warfare : Techniques, Tactics and Tools for Security Practitioners*.

Antunes, Sadrina., Camisao, Isabel (2017). Realism, Stephen Mcglinchey et. al. Ed. *International Relations Theory*, Bristol: E-International Relations Publishing.

Aras, B. ve diğerleri (2010), *SETA Rapor, Araştırma Merkezlerinin Yükselişi: Türkiye'de Dış Politika ve Ulusal Güvenlik Kültürü*, Ankara: SETA Yayınları.

Arda, E. (2020). *Siber Uzay Ortamında Saldırı Tehditlerinin Farkındalığı, Tespiti Ve Önlenmesi Üzerine Bir Gerçek-Zaman Sistem Önerisi*. Yayımlanmamış Yüksek Lisans Tezi. Ankara: Başkent Üniversitesi Fen Bilimleri Enstitüsü.

Arı, T. (2004). *Uluslararası İlişkiler Teorisi, Hegemonya İşbirliği*, İstanbul: Marmara Kitap Merkezi

Arı, T. (2004). *Uluslararası İlişkiler Teorileri*, İstanbul: Alfa Basım Yayın.

Arimatsu, L. (2012), A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations. *4th International Conference on Cyber Conflict,* Talinn: NATO CCD COE Publications, 91-109.

Aslanlı, A., ve Memmedov, A. (2016). Neo-Realizm Kuramı Çerçevesinde Azerbaycan-İran İlişkilerinin Analizi. *İtobiad: İnsan ve Sosyal Bilimler Araştırmaları Dergisi*. 5 (6).

Ataç, C. (2019). *Ulusal Siber Güvenlik Stratejisi Oluşturma Sürecine Bir Bakış*. Yayımlanmamış Yüksek Lisans Tezi. Samsun: On Dokuz Mayıs Üniversitesi Fen Bilimleri Enstitüsü.

Atalay, A. H. (2012), Kurumsal Bilgi Güvenliği, *Siber Güvenlik, Mimar veMühendis Dergisi,* 68, 42-47.

Avrupa Birliği Komisyonu (2013). *Joint Communication to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (Erişim Tarihi: 10.04.2022).

Aydın, A., Bakıncak, E. (2016). Uluslararası Güç Dengesi ve İki Kutupluluk Arasındaki İlişki. *Cumhuriyet Üniversitesi İktisadi ve İdari Bilimler Dergisi*. 17(1), 102.

Aydoğan, B., Aydın, H. (2011). *Güç Kavramı, Kamu Diplomasisi ve Güvenlik*. İstanbul: Ekopolitik UİM Rapor.

Bace, R., ve Mell, P. (2011). Nıst Special Publication On Intrusion Detection Systems. *Publications Of National Institute Of Standards And Technology,* 1- 53.

Barış B. vd.,Büro Teknolojileri, Anadolu Üniversitesi Yayınları, Eskişehir, 2013.

Başaran, D. (2017). *Uluslararası Güç İlişkileri Bağlamında İkinci Dünya Savaşı Sonrası Hegemonik Mücadelelerin İncelenmesi*. Yayınlanmamış Yüksek Lisans Tezi. Giresun: Giresun Üniversitesi Sosyal Bilimler Enstitüsü.

Baykara, M., Daş, R. ve Karadoğan, İ. (2013, May). Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi. In *1st International Symposium On Digital Forensics And Security (Isdfs'13)* (Vol. 20, P. 21).

Baylis, J. (2008), Uluslararası İlişkilerde Güvenlik Kavramı. *Uluslararası İlişkiler Dergisi,* 5(18), 69-85.

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

Bayraktar, G. (2015), *Siber Savaş ve Ulusal Güvenlik Stratejisi*, İstanbul: YeniyüzyılYayınları.

BBC (2017). "Eski FBI Başkanı Comey: Trump Yönetimi Yalan Söyledi". http://www.bbc.com/turkce/haberlerdunya-40199389. (Erişim Tarihi: 18.04.2022).

Beckett, C. ve James B. (2012). *WikiLeaks*. John Wiley & Sons.

Bıçakcı, S., Ergun, D., ve Çelikpala, M. (2015). Türkiye'de Siber Güvenlik. *Ekonomi Ve Dış Politika Araştırma Merkezi (Edam) Siber Politika Kağıtları Serisi*, *1*, 1-35.

Bıçakçı, S. (2014). "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik". *Uluslararası İlişkiler*. 10 (40), ss. 101-130.

Bıçakçı, S. (2012), Yeni Savaş ve Siber Güvenlik Arasında NATO'nun YenidenDoğuşu. *Uluslararası İlişkiler Dergisi*, 9(34), 205-226.

Bıçakçı, S. (2014). Nato'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik. *Uluslararası İlişkiler Dergisi*, *10*(40), 100-130.

Bilgi Teknolojileri ve İletişim Kurumu (2009), *Siber Güvenliğin Sağlanması: Türkiye'de Mevcut Durum ve Alınması Gereken Tedbirler*. https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FSayfalar%2FSiberGuvenlik%2Fsg.pdf. (Erişim tarihi: 22.03.2022).

Billo, C. Ve Chang, W. (2004). *Cyber Warfare, An Analysis of the Means and Motivations of Selected Nation States*. U.S. Department of Homeland Security.

Birdişli, F. (2016), *Teori ve Pratikte Uluslararası Güvenlik: Kavram-Teori- Uygulama*, Ankara: Seçkin Yayıncılık.

Boyraz, M. (2015), NATO'nun Siber Güvenlik Politikası: Tarihsel Süreç ve Kırılma Noktaları. *Research Turkey, Türkiye Politika ve Araştırma Merkezi*.

Broad, W. J. Ve Markoff, J.-Sanger, D.E. (2011). *Israeli Test On Worm Called Crucial In Iran Nuclear Delay*. The New York Times. https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html (Erişim Tarihi: 18.04.2022).

Brown, C. (2009). Structural Realism, Classical Realism and Human Nature, *International Relations*, 23(2), 257-258.

Brown, Gary D. ve Metcalf, Andrew O. (2014), Easier Said Than Done: Legal Reviews of Cyber Weapons. *Journal of National Security Law and Policy*, 7(115), 115-138.

Brüksel Zirve Bildirgesi (2018). *Brussels Summit Declaration*. https://www.nato.int/cps/en/natohq/official_texts_156624.htm (Erişişm Tarihi: 10.04.2022).

BSA (2015a). *EU Cybersecurity Dashboard – Country Reports – Japan. The Software Alliance (BSA). Japan Section*. Cybersecurity Country Reports. 2015. http://cybersecurity.bsa.org/2015/apac/assets/PDFs/country_reports/cs_japan.pdf. (Erişim tarihi: 21.04.2022).

Bull, H. (2012). *The Anarchical Society: A Study of Order in World Politics*. 4th ed. Basingstoke: Palgrave Macmillan.

Buzan, B. ve Hansen, L. (2009), *The Evolution of Security Studies*, Cambridge: Cambridge University Press.

Bülbül, H.B. (2018). *2016 Amerika Birleşik Devletleri Başkanlık Seçimine Rusya'nın Siber Müdahalesi İddialarının Uluslararası Hukuk Açısından Analizi*. http://icil.org.tr/2016-amerika-birlesik-devletleri-baskanlik-seciminerusyanin-siber-mudahalesi-iddialarinin-uluslararasi-hukuk-acisindan-analizi/ (Erişim Tarihi: 18.04.2022)

Canbay C. B. (2008). *Siber Güvenliğin Sağlanması ve Kritik Bilgi ve Altyapıların Korunması: Gelişmekte Olan Ülkeler için Yol Haritası*. 17. ITS Konferansı, Montreal – Kanada.

Canbek, G., & Sağiroğlu, Ş. (2007). Kötücül Ve Casus Yazılımlar: Kapsamlı Bir Araştırma. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, *22*(1).

Carr, E. H. (1946), *Twenty Years Crisis*, 1919-1939, Palgrave Macmillan.

CARR, J. ve Lewis S. Inside (2010). *Cyber Warfare.* Sebastopol, Calif., O'Reilly Media, Inc.

Cassidy, J. (2003). *Dot.con: How America Lost Its Mind and Money in the Internet Era*. HarperCollins.

Cavelty, M. D. (2008), *Cyber-Security and Threat Politics: US Efforts to Secure The Information Age,* New York: Routledge Publishing.

Chicago Zirve Bildirgesi (2012). *Chicago Summit Declaration*. https://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en %20/(Erişim Tarihi: 10.04.2022).

Choucri, N. ve diğerleri (2013), Institutions for Cyber Security: International Responsesand Global Imperatives. *Information Technology for Development*, 20(2), 96- 121.

Clarke, R.A.-Knake R. K. (2011). *Siber Savaş*. Çev.Murat Enduran. İstanbul: İKÜ Yayınevi.

Clarke, R. A. ve Knake, R. K. (2010), *Cyber War – The Next Threat toNational Security and What to Do About It.* New York DC: HarperCollins.

Clarke, R. A. ve Knake, R. K. (2011), *Siber Savaş: Ulusal Güvenliğe Yönelik Yeni Tehdit.* (Çev. Murat Erduran), İstanbul, İKÜ Yayınevi.

Colarik, Andrew M. (2006), *Cyber Terrorism: Political and Economic Implications*. Hershey and London: Idea Group Publishing.

Collins, A. (Ed.). (2022). *Çağdaş Güvenlik Çalışmaları*. Oxford Üniversitesi Basım.

Conteh N. ve Schmick P. (2016). Cybersecurity: Risks, Vulnerabilities and Counter Measures to Prevent Social Engineering Attacks. *International Journal of Advanced Computer Research.* 6(23):31-38.

Corell, Hans (2000), The Challenge of Borderless Cyber-Crime, *Syposium On TheOccasion of The Signıng of The United Nations Convention Against TransnationalOrganized Crime*. Palermo.

Corera, G. (2015). *Secret History of Chinese Spies*. Paris: Nouveau Monde Editions.

Cox, R. W. (2019). Social Forces, States, and World Orders: Beyond International Relations Theory. In *Culture, Ideology, and World Order* (pp. 258-299). Routledge.

Çakmak, H., Altunok, T. (2009). *Suç Terör ve Savaş Üçgeninde Siber Dünya*. Ankara: Barış Platin Kitabevi

Çakmak, H. ve Demir, C. K. (2009), "Siber Dünyadaki Tehdit ve Kavramlar", Haydar Çakmak ve Taner Altunok (Ed.), *Suç, Terör ve Savaş Üçgeninde Siber Dünya,* 1. Baskı *İçinde* **(**23-54), Ankara: Barış Platin Kitabevi.

Çelik, S. (2021). Kuantum Kriptolojisi Ve Siber Güvenlik. *Bilişim Teknolojileri Dergisi*, *14*(1), 53-64.

Çelik, S., ve Çeliktaş, B. (2018). Güncel Siber Güvenlik Tehditleri: Fidye Yazılımlar. *Cyberpolitik Journal*, *3*(5), 105-132.

Çeliktaş, B. (2016). *Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme*. Yayımlanmamış Yüksek Lisans Tezi. Trabzon: Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü.

Çetin, H., Gundak, İ., ve Çetin, H. H. (2015). E-İşletme Güvenliği Ve Siber Saldırılar Üzerine Bir Araştırma. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *6*(2), 223-240.

Çetin, M. (2017). *Nükleer Tesislerde Siber Emniyet, Siber Saldırı Senaryoları, Sonuçları Ve Savunma Sistemleri*. Yayımlanmamış Uzmanlık Tezi. Ankara: Türkiye Atom Enerjisi Kurumu.

Çetinkaya, Ş. (2012). Güvenlik Algılaması ve Uluslararası İlişkiler Teorilerinin Güvenliğe Bakış Açıları. *21. Yüzyılda Sosyal Bilimler*, Sayı 2, 241-260.

Çıtak, E., ve Şen, O. (2014). *Uluslararası İlişkilerde Güvenlik, Teorik Değerlendirmeler*. Ankara: Röle Akademik Yayınları.

Çiçek, İ. (2008). *Ülkemizde Adli Bilişim Laboratuarlarının Kurulumu Ve Bilişim Suçlarıyla Mücadeleye Katkıları*. Yayımlanmamış Yüksek Lisans Tezi. İstanbul: Haliç Üniversitesi Fen Bilimleri Enstitüsü.

Çiçekçi, C. (2012). *Uluslararası Güvenlik Çalışmaları*, İstanbul: Kriter Yayınevi.

Çifçi, H. (2013). *Her Yönüyle Siber Savaş*, İstanbul: TÜBİTAK Popüler Bilim Kitapları.

Çitlioğlu, E. (2008). *Gri Tehdit Terörizm*, Ankara: Başak Matbaacılık ve Tanıtım Ltd.Şti.

Darıcılı, A. B., ve Özdal, B. (2017). Rusya Federasyonu'nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi. *Bilig*, (83), 121-146.

Darıcılı, B. (2014). Rusta Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıların Analizi. *Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*. 7 (2), ss.1-16.

Darıcılı, B. (2017a). Demokrat Parti Hack Skandalı Bağlamında ABD ve RF'nin Siber Güvenlik Stratejilerinin Analizi. *Uluslararası Çalışmalar Dergisi Özel Sayısı*. 1 (1), ss.1-24.

Dedeoğlu, B. (2003). *Uluslararası Güvenlik ve Strateji*, İstanbul: Derin Yayınları.

Denning, D. E., (1999). *Information Warfare and Security*, New York: Addison- Wesley.

Daniel, T. K. ve Jefferson C. (2011). Inside *Wikileaks : My Time With Julian Assange at The World's Most Dangerous Website*. New York: Crown Publishers.

Douligeris, C., ve Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks*, 44(5), 643-666.

Dunn, Myriam A. (2007), "Securing The Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory", Johan Eriksson and Giampiero Giacomello (Ed.), *International Relations and Security in the Digital Age*, içinde (85-106), New York: Routledge Publishing.

Efegil, E. E., ve Seyfettin, M. (2012). *Dış Politika Analizinde Teorik Yaklaşımlar: Türk Dış Politikası Örneği*. Ankara: Barış Kitap.

Elman, C. (2007). Realism. Martin Griffiths (Ed.), *International Relations Theory for The Twenty-First Century: An Introduction,* 1. Baskı *içinde* (11-21), New York: Routledge Publishing.

ENISA (2019a). *About ENISA*. https://www.enisa.europa.eu/about-enisa (Erişim Tarihi: 10.04.2022).

ENISA (2019b). *Mission and Objectives*. https://www.enisa.europa.eu/aboutenisa/mission-and-objectives (Erişim Tarihi: 10.04.2022).

Eren, M., (2017). *Avrupa Birliği'nin Siber Güvenlik Politikası*. İstanbul: Beta Yayınevi.

Ermiş, K. (2006). *Sayısal İmza ve Elektronik Belge Yönetimi*. Bilgi Dünyası, 7(1), 121-146.

Even, L. R. (2000, July 12). *Intrusion Detection Faq: What İs A Honeypot? Swansea*, Uk: Sans Institute.

F. Yihunie, E. Abdelfattah ve A. Odeh, (2018), Analysis of ping of death DoS and DDoS attacks. 2018 IEEE Long Island Systems, *Applications and Technology Conference (LISAT)*, Farmingdale, NY, 2018, pp. 1-4.

Gady, F. S. ve Austin G. (2010). Russia, The United States, And Cyber Diplomacy Opening the Doors. *East-West Enstitute Report*. New York: 1-32.

Galler Zirve Bildirgesi (2014). *Wales Summit Declaration*. https://www.nato.int/cps/ic/natohq/official_texts_112964.htm (Erişim Tarihi: 10.04.2022)

Gartzke, E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace back down toEarth. *International Security,* 38(2), 41-73.

Geers, K. (2012). Cyberspace and the Changing Nature of Warfare. *Centre of Excellence Tallinn*, Estonya.

Gibson, W. (1984). *Neuromancer*. The ACE Publications.

Gilpin, R. (1981). *War and Change in international Politics*. New York: Cambridge Press.

Göçoğlu, V. (2017). *Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi*. Yayımlanmamış Doktora Tezi. Ankara: Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü.

Gökırmak, Y., Yüce, E., Bektaş, O., Soysal, M., ve Orcan, S. (2009). Ipv6 Balküpü Tasarımı. *Emo Elektrik-Elektronik, Bilgisayar Ve Biyomedikal Mühendisliği Ulusal Kongresi*.

Gökırmak, Y., Yüce, E., Soysal, O. B. M., & Orcan, S. (2011). *IPv6 Balküpü Tasarımı*. Tübitak Ulakbim, Ankara.

Gragner, S. (2001). *Social Engineering Fundamentals, Part I: Hacker Tactics*. Security Focus.

Graham, J., Richard H. ve Ryan O. (2010). *Cyber Security Essentials*. Boca Raton: Auerbach Publications.

Griffiths, M. ve diğerleri (2011), *Uluslararası İlişkilerde Temel Düşünürler ve Teoriler,* (Çev. CESRAN), Ankara: Nobel Yayınevi.

Grudziecki, T., Jacewicz, P., Juszczyk, Ł., Kijewski, P., & Pawliński, P. (2012). *Proactive Detection Of Security Incidents*. Enısa.

Gündüz, M. Z. (2013). *Bilişim Suçlarına Yönelik Ip Tabanlı Delil Tespiti*. Yayımlanmamış Yüksek Lisans Tezi. Elazığ: Fırat Üniversitesi Fen Bilimleri Enstitüsü.

Güneştaş, M. ve diğerleri (2015). Siber Terörizm: Motivasyon ve Yöntem. Fatih Tombul ve diğerleri (Ed.), *Siber Suçlar, Tehditler, Farkındalık ve Mücadele* içinde (85-113), Ankara: Global Politika ve Strateji.

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

Güntay, V. (2018). Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi Ve Uluslararası Aktörler. *Güvenlik Stratejileri Dergisi*, *14*(27), 79-111.

Güntay, V. (2015), "Uluslararası İlişkiler Bağlamında Güvenlik Algısı ve Siber Güvenlik: Akdeniz, Karadeniz ve Avrupa Bölgeleri Üzerine Bir Değerlendirme", *The Journal of Academic Social Science Studies,* Number 37, 477-489.

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

Gürol C. ve Şeref S. (2006). *Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri*. Ankara: Şahsi Yayın.

Haley, C. (2013), "A Theory of Cyber Deterrence", *Georgetown Journal of International Affairs.* (75-88).

Hansen, L. ve Nissenbaum, H. (2009). Digital Disaster, Cyber Security and The Copenhagen School. *International Studies Quarterly,* Volume 53, 1155-1175.

Hare, F. (2010), The Cyber Threat to National Security: Why can't We Agree?. C. Czosseck ve K. Podins (Ed.). *Conference on Cyber Conflict Proceedings*. 1. Baskı*içinde* (211-225), Tallinn: CCD COE Publications.

Healey, J. ve Jordan, K. T. (2014). *NATO's Cyber Capabilities: Yesterday, Today and Tomorrow*, Atlantic Council.

Healy, B., Stein, A. (1973). The Balance of Power in International History Theory and Reality. *Journal of Conflict Resolution*. 17(1).

Heickerö, R. (2015). Industrial espionage and theft of information. In *ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security 2015: ECCWS 2015* (p. 86). Academic Conferences Limited.

Hekim, H., ve Başıbüyük, O. (2013). Siber Suçlar Ve Türkiye'nin Siber Güvenlik Politikalari. *Uluslararası Güvenlik Ve Terörizm Dergisi*, *4*(2), 135-158.

Hekim, H. (2015). Oltalama (Phishing) Saldırıları. Fatih Tombul ve diğerleri (Ed.), *Siber Suçlar, Tehditler, Farkındalık ve Mücadele* içinde (57-83), Ankara: Global Politika ve Strateji.

Henderson, Conway W. (2010). *Understanding International Law*. New Jersey: Wiley-Blackwell.

Henry, A. (2013). The Difference Between Antivirus And Anti-Malware (And Which To Use). In *Paper, Gw Juette And Le Zeffanella, "Radio Noise Currents İn Short Sections On Bundle Conductors (Presented Conference Paper Style*). Presented At.

Herbert S. L. (2010). Offensive Cyber Operations and the Use of Force. *Journal of National Security Law & Policy*. Vol.4, No.63, 63-86.

Hobbes, T. (2017). *Leviathan.* (Çev. Semih Lim). İstanbul: Yapı Kredi Yayınları.

Holsti, K. J. (1983). International Politics: A Framework for Analysis, Englewood Cliffs (NJ), Prentice-Hall, 1983, 494 p. *Études internationales*, *14*(2), 354-355.

Hornblower, S. (1992). Peloponez Savaşı'nın Dini Boyutu veya Thucydides'in Bize Söylemediği Şey. *Klasik Filolojide Harvard Çalışmaları*, 94, 169-197.

Hoskins, A. ve O'Loughlin, B. (2008). The Internet as a Weapon of War? Radicalisation, Publics and Legitimacy. Athina Karatzogiannni (Ed.), *Cyber Conflict and Global Politics*, 1. Baskı *içinde* (31-48), London: Routledge ChapmanHall.

Hulme, G. V. (2020). *DDoS explained: How distributed denial of service attacks are evolving. Csoonline. com*. https://www. csoonline. com/article/3222095/ddos-explained-how-denial-of-service-attacks-are-evolving. html. (Erişim tarihi: 15.10.2020).

Hwang, J. (2012). *China's Cyber Warfare: The Strategic Value of Cyberspace and the Legacy of People's War*. School of Geography, Politics and Sociology University ofNewcastle.https://pdfs.semanticscholar.org/3b69/1d2295dfc7161b27d395cda422c6e0730f08.pdf (Erişim Tarihi: 10.04.2022).

Industrial Ethernet Book (2017). *The Stuxnet Worm and Options for Remediation*. https://iebmedia.com/index.php?id=7409&parentid=63&themeid=255&hft=61&showdetail=true&bb= 1 (Erişim Tarihi: 18.04.2022).

İduğ, Y. ve diğerleri (2013). Siber Caydırıcılık ve Türkiye'nin İmkân ve Kabiliyeti. *6.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*. Ankara: Bildiriler Kitabı. 287-289.

İkizler, M., ve Başar, S. (2006). Spam'in Zararları Ve Spam İle Hukuki Mücadele: Abd Örneği Ve Türk Avrupa Birliği Hukukları İle Karşılaştırılması. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, *8*(2), 91-114.

Jabri, V. (2008). Reflections on the Study of International Relations. Trevor C. Salmon ve Mark F. Imber (Ed.), *Issues in International Relations*, 2. Baskı *içinde* (11-32), New York: Routledge Publishing.

Japan Cabinet (2000). *Basic Act on the Formation of an Advanced Information and Telecommunications Network Society*. Kanun No.144. Yayımlanma Yılı: 2000

Jelinek, P. (2010). *A Code You Can Hack: On CYBERCOM's Logo. Marine Corps Times*.https://web.archive.org/web/20100715055816/http://www.marinecorpstimes.com/news/2010/07/ap_military_cyber_command_logo_070810/ (Erişim Tarihi: 10.04.2022).

JNSA (t.y.). *Japan Network Security Association – About Us. Japan Network Security Association (JNSA)*. http://www.jnsa.org/en/aboutus/index.html. (Erişim tarihi: 14.05.2022).

Jones, R. W. (Ed.). (2001). *Critical theory and world politics*. Lynne Rienner Publishers.

JPCERT/CC (t.y.). *JPCERT Coordination Center within APCERT*. Japan Computer Emergency Response Team (JPCERT). Organizational Website. https://www.jpcert.or.jp/english/apcert. (Erişim tarihi: 16.07.2022).

Kanagasingham, P. (2008). *Data Loss Prevention*. https://www.sans.org/white-papers/32883/. (Erişim tarihi: 09.11.2021).

Kantarci, Ş. (2012). Soğuk Savaş Sonrası Uluslararası Sistem: Yeni Sürecin Adı Koalisyonlar Dönemi mi?. *Güvenlik Stratejileri Dergisi*, *8*(16), 47-84.

Kaplan, M. A. (2005). *System and process in international politics*. ecpr Press.

Kaplan, M. (1969). *Variants on Six Models of the International System: International Politics and Foreign Policy*. New York: The Free Press.

Kaplan, M. (2005). *System and Process in International Politics,* European Consortium for Political Research, Colchester.

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

Karaarslan, E., Akın, G., ve Fetah, V. (2008). *Kurumsal Ağlarda Zararlı Yazılımlarla Mücadele Kılavuzu*. Ulak-Csırt, Tübitak - Ulakbim .

Karabatak, S., Özmen, F., ve Karabatak, M. (2014). Üniversitelere Yapılan Siber Saldırılar Ve Üniversite Yönetimi Tarafından Yapılması Gerekenler. *Proceding Book*, 134.

Karabulut, B. (2015). *Güvenlik: Küreselleşme Sürecinde Güvenliği Yeniden Düşünmek,* Ankara: Barış Kitabevi.

Karakuş, C. (t.y.). *Kritik Altyapılara Siber Saldırı*. http://ckk.com.tr/bilimsel/siber.pdf. (Erişim tarihi: 09.08.2021).

Kaya, Ç. ve Yıldız, O., (2014). Makine Öğrenmesi İle Saldırı Tespiti: Karşılaştırmalı Analiz. *Marmara Fen Bilimleri Dergisi*, 3: 89-104.

Kaya, M. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi Ve Alınabilecek Tedbirler. *Güvenlik Stratejileri Dergisi*, *9*(18), 145-181.

Keleştemur, A. (2015), *Siber İstihbarat*,1. Baskı, İstanbul: Yazın Basın Yayınevi Matbaacılık Trz.Tic.Ltd.Şti.

Kim, Y., Kim, I., ve Park, N. (2014). Analysis of cyber attacks and security intelligence. In *Mobile, Ubiquitous, and Intelligent Computing* (pp. 489-494). Springer, Berlin, Heidelberg.

Kinsella, D., Russett, B., ve Starr, H. (2012). *World politics: The menu for choice*. Cengage Learning.

Kissinger, H. A., (1973). *At Pacem in Terris Conference. New Release, Bureau of Public Affairs*. Department of State.

Knapp, E. D., ve Langill, J. (2014). *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress.

Knutsen, T. L. (2006), *Uluslararası İlişkiler Teorisi Tarihi*, İstanbul: Açılım Kitap.

Korhan, S. (2018). *Siber Uzayda Uluslararası İlişkilerin Değişen Parametreleri*. Yayımlanmamış Yüksek Lisans Tezi. Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü.

KPMG 2016, *Outline of Financial Modelling Assumption for Local Government Merger Proposals – Technical Paper Prepared for the NSW Department of Premier and Cabinet, 19 January, 2016*, KPMG, Sydney.

Krippendorff, E. (1982). *Bruce Russett, Harvey Starr: Dünya Siyaseti*. Seçim Menüsü.

Kurki, M. (2008). *Causation in International Relations: Reclaiming Causal Analysis*, Cambridge, Cambridge University Press.

Libicki, M. C. (1996). *What Is Information Warfare?,* 3th Ed., Washinghton, DC: U.S. Government Printing Office.

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*, Santa Monica: Rand Corporation.

Lupovici, A. (2011). Cyber Warfare and Deterrence. *Military and Strategic Affairs*, 3(3), 49-62.

Maan P. ve Sharma M. (2012). *Socialengineering: A Partial Technical Attack*. Department of Information Technology DAV Institute of Engineering and Technology Punjab Technical University Jalandhar.

Martin, C., ve Strategy, S. D. P. (2016). Intrusion detection and prevention systems in the industrial automation and control systems environment. *In Process Control Systems*

*Industry Conference*, https://ics-cert. us-cert. gov/sites/default/files/pcsf-arc/intrusion_ detection_prevention_ systems-martin. pdf (25.01. 2016).

Mbanaso, U. M., ve Dandaura, E. S. (2015). The Cyberspace: Redefining A New World. *IOSR Journal of Computer Engineering*, *17*(3), 17–24.

McSweeney, B. (1999). *Security, Identity and Interests*. Cambridge: Cambridge University Press.

Mearsheimer, J. (2006). Structural Realism, Tim Dunne vd., der., *International Relations Theories: Discipline and Diversity*. Oxford: Oxford University Press.

Medvedev, S. A. (2015). *Offense-Defense Theory Analysis of Russian Cyber Capability*. Masters' Thesis. California: Naval Postgraduate School.

Mele, S. (2013). *Cyber-Weapons: Legal and Strategic Aspects, Version 2.0, Machiavelli Editions*, http://www.strategicstudies.it/wp-content/uploads/2013/07/ Machiavelli-Editions-Cyber-Weapons-Legal-and-Strategic-Aspects-V2.0.pdf (Erişim tarihi: 18.01.2016).

Messmer, E. (1999). *Kosovo Cyber-war Intensifies*. http://www.network-world.com/news/1999/0512kosovo.html. (Erişim tarihi: 18.04.2022).

Michael S. (2013). *Tallinn Manuel on the International Law Applicable to Cyberwarfare*. Rule 41. 141-142.

Miller, B. (2010). Explaining Changes in U.S. Grand Strategy: 9/11, The Rise of Offensive Liberalism, and the War in Iraq. *Security Studies*. 19:1, 26-65.

Morgenthau, H. J. (1973). *Politics Among Nations: The Struggle For Power And Peace*. Alfred A. Knoph. Inc., New York, 27.

Morgenthau, H. J. (2006). *Politics Among Nations The Struggle for Power and Peace*. New York: Mcgraw Hill Higher Education.

Morkel, T., Eloff J.H.P., Olivier M.S. (2005). An Overview of Image Steganography. *Proceedings of the Fifth Annual Information Security South Africa Conference.*

Mulvenon, J. (2009). *PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability*.

http://indianstrategicknowledgeonline.com/web/Ch_8-1.pdf (Erişim Tarihi: 10.04.2022).

Musman S. vd, (2011). *Computing the Impact of Cyber Attacks on Complex Missions*. IEEE International Systems Conference, Montreal.

NATO (2010). *Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation*. https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf . (Erişim Tarihi: 10.04.2022).

NATO (2014). *NATO Industry Cyber Partnership (NICP)*. https://www.ncia.nato.int/Industry/Pages/NATO-Industry-Cyber-Partnership.aspx (Erişim Tarihi: 10.04.2022).

NATO (2016). *NATO Cyber Defence Fact Sheet*. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf (Erişim Tarihi: 10.04.2022).

NATO Siber Savunma Mükemmeliyet Merkezi (2019). *About Us*. https://ccdcoe.org/about-us/ (Erişim Tarihi: 10.04.2022).

Naughton, J. (2016). The evolution of the Internet: from military experiment to General Purpose Technology. *Journal of Cyber Policy*, *1*(1), 5–28.

New York Times (2016). *Hackers to the U.S. Election*. https://www.nytimes.com/interactive/2016/07/27/us/politics/trail-of-dnc-emails-russia-hacking.html. (Erişim Tarihi: 18.04.2021).

NISC (2007). *Japanese Government's Efforts to Address Information Security Issues – Focusing on the Cabinet Secretariat's Efforts*. National Information Security Center (NISC). http://www.nisc.go.jp/eng/pdf/overview_eng.pdf. (Erişim tarihi: 23.04.2023).

O'Connell, M. E. (2012). Cyber Security without Cyber War. *Journal of Conflict & Security Law*, 17(2), 187-209.

Ocak, H. S. (2021). *İç Denetimin Gelişen Ve Değişen Dünyasında: Siber Güvenlik Ve Denetim*. Yayımlanmamış Doktora Tezi, İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü.

OECD, (2008), *Directorate for Science, Technology and Industry Committee for Information.* Computer and Communications Policy.

Office of the Press Secretary, White House. (2001a). *Press briefing by Ari Fleischer*. http://georgewbush-whitehouse.archives.gov/news/briefings /2001/04/20010404.html (Erişim Tarihi: 19.04.2022).

Office of the Press Secretary, White House. (2001b). *Remarks by the president at American Society of Newspaper Editors Annual Convention*. http://georgewbush-whitehouse.archives.gov/news/releases/2001/04/20010405-5.html (Erişim Tarihi: 19.04.2022).

Oğultekin, G., Tapan, M. ve Şener, S. M. (2009). Yüksek Teknoloji Yapılarında Biçim/Sentez İlişkisi. *İtüdergisi/A*, *7*(2).

Özbek, Y. (2019). *Öğretmen Adaylarının Siber Güvenlik Farkındalıklarının İncelenmesi*. Yayımlanmamış Yüksek Lisans Tezi. Konya: Necmettin Erbakan Üniversitesi Eğitim Bilimleri Enstitüsü.

Özçoban, C. (2014). *21.Yüzyılda Ulusal Güvenliğin Sağlanmasında Siber İstihbaratın Rolü*. Yayımlanmamış Yüksek Lisans Tezi. İstanbul: Harp Akademileri Stratejik Araştırmalar Enstitüsü.

Özdemir, H. (2008). Uluslararası İlişkilerde Güç: Çok Boyutlu Bir Değerlendirme. *Ankara Üniversitesi SBF Dergisi*, 63(3), 127-128.

Özen, M. ve Özocak, G. (2015). Adli Bilişim, Elektronik Deliller Ve Bilgisayarlarda Arama Ve El Koyma Tedbirinin Hukuki Rejimi (Cmk M. 134). *Ankara Barosu Dergisi*, (1).

Öztürk, Ö. (2009). *E-Postalarda Spam Sorunu Ve Çözüm Önerileri*. Yayımlanmamış Uzmanlık Tezi, Ankara: Bilgi Teknolojileri Ve İletişim Kurumu.

P.R.C. Embassy in the United States. (2001). *Chinese fighter bumped by U.S. military scout: FM*. http://www.china-embassy.org/eng/zmgx/zmgx/Military%20Relationship/t35745.htm (Erişim Tarihi: 19.04.2022).

Pajunen, N. (2017). *Overview Of Maritimecybersecurity*. South Easternfinlanduniversity: 21.

Paker, E. B. (2012). *Küresel Güvenlik Kompleksi: Uluslararası Siyaset ve Güvenlik,* İstanbul:

İletişim Yayıncılık.

Paşaoğlu, C., Güler, H. ve Jafari, M. (2019). Ağ Tabanlı Veri Sızıntısı Tespiti Ve Önlenmesi Üzerine Bir İnceleme. *Uluslararası Yönetim Bilişim Sistemleri Ve Bilgisayar Bilimleri Dergisi*, *3*(2), 79-92.

Peterson, D. (2013). Offensive Cyber Weapons: Construction, Development, and Employment. *The Journal of Strategic Studies*, 36(1), 120-124.

Pevehouse, J., Goldstein, J. (2017). *International Relations*. London: Pearson Education.

Ping C., Lieven D., and Christophe H. (2014). A Study on Advanced Persistent Threats. Communications and Multimedia Security, *15th IFIP TC 6/TC 11 International Conference, CMS 2014 Aveiro*, Portugal, September 25-26.

Piret, P. (2014). *Improving Cyber Security: NATO and The EU, International Centre for Defence Studies*. Talinn.

Ponemon Institute (2014). *Best Schools for Ciber Security 2014 Best Schools for Cybersecurity*. Ponemon.

Poyrazoğlu, G. B. A. (2022). *Geleceğin Meslekleri*. Kütüphane Kartı, 135.

PPC (t.y.a). (2022). *Japan Personal Information Protection Commission – About The Commission – Roles and Responsibilities*. Personal Information Protection Commission (PPC). http://www.ppc.go.jp/en/aboutus/roles. (Erişim tarihi: 23.07.2022).

Raud, M. (2016). *China and Cyber: Attitudes, Strategies and Organisation*. Tallinn: The NATO Cooperative Cyber Defence Centre of Excellence.

Raul, A. C. Manoranjan, T. ve Mohan, V. (2014). *The Privacy, Data Protection and Cybersecurity Law Review*. (Editor: Alan Charles Raul). Law Business Research.

Renard, T. (2014). *The Rise of Cyber-Diplomacy: The EU, Its Strategic Partners and Cyber-Security*, Working Paper 7, Madrid: European Strategic Partnerships Observatory.

Richter, P. (2001). *Chinese plane flew too close. LA Times*. http://www.taiwandc.org/latimes-2001-01.htm. (Erişim Tarihi: 19.04.2022).

Rid, T. ve McBurney, P. (2012). *Cyber-Weapons*. The RUSI Journal.

Robinson, N., Horvath, V., Cave, J., Roosendaal, A. P., ve Klaver, M. (2013). *Data and security breaches and cyber-security strategies in the EU and its international counterparts*. European Union.

Rosecrance, R. ve Steiner, Z. (2010). History and Neorealism Reconsidered, Ernest R. May ve diğerleri (Ed.), *History and Neorealism*, 1. Baskı *içinde* (341- 365). Cambridge: Cambridge University Press.

Roskin, M. G. ve Berry, N. O. (2014). *Uluslararası İlişkiler: Uİ'nin Yeni Dünyası,* (Çev: Özlem Şimşek), Ankara: Adres Yayınları.

Roth, M. (2009). *Bilateral Disputes Between EU Member States and Russia*. CEPS Working Document (Centre for European Policy Studies). https://www.ceps.eu/wp-content/uploads/2009/09/1900.pdf (Erişim Tarihi: 18.04.2022).

Rupert, M. (2007). Marxism. Martin Griffiths (Ed.), *International Relations Theory for The Twenty-First Century: An Introduction*, 1. Baskı içinde (35-47). New York: Routledge Publishing.

Sağıroğlu, Ş. (2013). Siber Güvenlik ve Savunma. *Harp Akademisi Geleceğin Harekât Ortamı ve Harp Teknolojileri Paneli,* İstanbul.

Sandıklı, A., Sandıklı, A., ve Güllü, İ. (2005). *Geleceğin Süper Gücü: Uzakdoğu'daki Entegrasyonlar ve Şangay İş Birliği Örgütü*. Ankara: Tasam.

Sandilaç, N. (2021). *Siber Dünyada Hacker Kültürü, Hacktivizm Ve Bilişim Suçları*. Yayınlanmamış Yüksek Lisans Tezi. Sakarya: Sakarya Üniversitesi Sosyal Bilimler Enstitüsü.

Scheuerman, W. E. (2007). Carl Schmitt and Hans Morgenthau: Realism and Beyond. Michael C. Williams (Ed.), *Realism Reconsidered: The Legacy of HansMorgenthau in International Relations*, 1. Baskı içinde (62-92), Oxford: Oxford University Press.

Sertçelik, A. (2015). Siber Olaylar Ekseninde Siber Güvenliği Anlamak. *Medeniyet Araştırmaları Dergisi, 2*(3), 25-42.

Sheehan, M. (2004). *The Balance of Power: History and Theory*. London: Routledge.

Singer, P.W. ve Friedman, A. (2015). *Siber Güvenlik ve Siber Savaş*. Ankara: Buzdağı Yayınevi.

Smith, T (1999). *History and International Relations*. New York: Routledge.

Soysal, M., Bektaş, O., ve Üçtop, K. (2015). *Ulak Csırt Balküpü Tuzağı Ve Kara Delik Çalışma Grubu*. Ankara: ULAKBİM.

Sönmezoğlu, F. (2009). *Uluslararası İlişkilere Giriş*. Ankara: Der Yayınları.

Sönmezoğlu, F. (2000). *Uluslararası Politika ve Dış Politika Analizi*, İstanbul: Filiz Kitabevi.

Sönmezoğlu, F. (2011). *İki Savaş Sırası ve Arasında Türk Dış Politikası*, İstanbul: Der Yayınları.

Sputnik Haber Sitesi (2017). *Beyaz Saray ABD, 35 Rus Diplomatı 72 Saat İçerisinde Sınır Dışı Edecek*. https://tr.sputniknews.com/abd/201612291026553306-abd-rusya-yaptirim-diplomat-sinir-disi (Erişim Tarihi: 19.04.2022).

Staar, R. T. (2010). Russia's Security Services. *Mediterranean Quarterly*. 15 (1): 1-10.

Stafford, T. and Urbaczewski, A. (2004). *Spyware: The Ghost in the Machine*. AMCIS. 2004 Proceedings.

Statisca, (2016 a). *Countries of the Highest Rate of Malware Infected Computers as of 4th Quarter 2016*.

Statisca, (2016 b). *Countries of the Lowest Rate of Malware Infected Computers as of 4th Quarter 2016*.

Stephen, M. W. (1987). *The Origins of Alliances*, Cornell University Press,New York.

Stokes, M.A., Lin, J. Ve Hsiao, L.C.R. (2011). *The Chinese People's Liberation Armay Signals Intelligence and Cyber Reconnaissance Infrastructure*. Project 2049 Institute. https://project2049.net/2011/11/11/the-chinese-peoples-liberation-army-signals-intelligence-and-cyber-reconnaissance-infrastructure/ (Erişim tarihi: 10.04.2022).

Stone, A. (1994), What is Supranational Constitution? An Essay in InternationalRelations Theory. *The Review of Politics*, 56(3), 441-474.

Şahinaslan E. (2009). Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri. *Harran Üniversitesi Akademik Bilişim Konferansı Bildirileri*. 597-602.

Şahinaslan, Ö. (2007). *Bilgisayar Ağlarında Açık Kaynak Kodlu Güvenlik Yazılımları İle Anti-Spam Modülünün Geliştirilmesi*. Yayınlanmamış Yüksek Lisans Tezi. İstanbul: Maltepe Üniversitesi, Fen Bilimleri Enstitüsü.

Şahinaslan, Ö., Şahinaslan, E., Borandağ, E., ve Şahinaslan, A. M. (2013). Güvenli Bir Toplumun İçin Son Kullanıcı Siber Güvenliği. *Xv. Akademik Bilişim Konferansı Bildirileri,* 1081-1085.

Şentürk, H., Çil, Z.C. ve Sağıroğlu, Ş. (2012). Cyber Secuirty Analysis of Turkey. *International Journal of Information Security Science*. 1 (4), ss.112-125.

T.C. Başbakanlık AFAD (2014), *2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi*, https://www.afad.gov.tr/Dokuman/TR/123-20141010111330-kritikaltyapi-son.pdf. (Erişim tarihi: 08.09.2022).

Tan, H. ve Aktaş A. Z. (2011). Bir Kuruluşun Bilgi Güvenliği İçin Bir Yaklaşım. *IV. Ağ ve Bilgi Güvenliği Sempozyumu Bildiriler Kitabı*, TMMOB Elektrik Mühendisleri Odası, Ankara, 34-39.

Tombul, F. (2015). Kamu Yönetiminde Siber Suçlara Karşı Kullanıcılarda Farkındalık Oluşturulmasının ve Kurumsal Bilişim Güvenlik Politikalarının Oluşturulmasının Önemi. Fatih Tombul ve diğerleri (Ed.). *Siber Suçlar, Tehditler, Farkındalık ve Mücadele* içinde (141-164), Ankara: Global Politika ve Strateji.

Turhan M. (2006). *Siber Güvenliğin Sağlanması, Dünya Uygulamaları Ve Ülkemiz İçin Çözüm Önerileri.* Ankara: Bilgi Teknolojileri Ve İletişim Kurumu.

TÜBİTAK (2009). *Basın Bülteni*.

Türk Silahlı Kuvvetleri (1999). *Türk Silahlı Kuvvetleri Bilgi Harbine Nasıl Hazırlanmalıdır?,* İstanbul: Harp Akademileri Basım Evi

CNN. (2001). *U.S. aircraft collides with Chinese fighter, forced to land*. http://archives.cnn.com/2001/US/04/01/us.china.plane.03/ (Erişim Tarihi: 19.04.2022)

Ulaşanoğlu, M. E. ve diğerleri (2010). *Bilgi Güvenliği: Riskler ve Öneriler*. Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

Ulaştırma Denizcilik ve Haberleşme Bakanlığı. 2016-2019 "*Ulusal Siber Güvenlik Stratejisi"*.

T.C. Resmi Gazete. (28683) (20 Haziran 2013). *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*.

USOM, 2014 T.C. Ulaştırma ve Denizcilik Bakanlığı. (2014). *Siber Güvenliğe ilişkin Temel Bilgiler*.

Ünal, A. (2015). Dağıtık Servis Dışı Bırakma (DDoS) Saldırıları: Güncel Yöntemler ve Mücadele. Fatih Tombul ve diğerleri (Ed.), *Siber Suçlar, Tehditler, Farkındalık ve Mücadele* içinde (11-36), Ankara: Global Politika ve Strateji.

Ünver, M. ve Canbay, C. (2010). Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik. *Elektrik Mühendisliği Dergisi*, 48(438), 94-103.

Valcourt, S.A. (2003). 1st International Workshop On Community Networks And P/X *Alphabet Soup: A Comparison Of The Current State Of Dsl Technologies Managing Director*, University Of New Hampshire Interoperability Laboratory, New Hampshire, S14-15.

Varşova Zirve Bildirgesi (2016). *Wales Summit Declaration*. https://www.nato.int/cps/en/natohq/official_texts_112964.htm (Erişim Tarihi: 10.04.2022).

Vasquez, J. A. (2015). *Savaş Bulmacası*. (Çev. Haluk Özdemir), İstanbul: Uluslararası İlişkiler Kütüphanesi Yayınları.

Ventre,C. (2010). *China's Strategy for Information Warfare: A Focus on Energy. Journal of Energy Security*. http://www.ensec.org/index.php?option=com_content&view=article&id=241:critical-energy-infrastructure-security-and-chinese-cyber-threats&catid=106:energysecuritycontent0510&Itemid=361 (Erişim Tarihi: 12.04.2022).

Viotti, Paul R Viotti, Mark V.Kauppi, (1999). *International Relations Theory, Realism, Pluralism, Globalism and Beyond*. London: Allyn and Bacon.

Virvilis,N., Gritzalis, D. (2013). The big four- what we did wrong in advanced persistent threat detection?. *International Conference on Availability, Reliabiliy and Security,* 248-254.

Wallerstein, I. (2004). The Rise and Future Demise of the World CapitalistSystem: Concepts for Comparative Analysis. Karen A. Mingst ve Jack L. Snyder (Ed.), *Essential Readings in World Politics*, 2. Baskı *içinde* (130-138), New York:Norton Publishing.

Waltz, K. (1979). *Theory of international politics. Reading*, MA: Addison-Wesley. Chapter, 4(5), 129.

Waltz, K. N. (2000). Structural realism after the Cold War. *International security*, *25*(1), 5-41.

Waltz, K. N. (2001). *Man, the state, and war: A theoretical analysis*. Columbia University Press.

Waltz, K. (1979). *Theory of International Politics*. Wesley Series in Political Science, Kanada.

Weber, C. (2010). *International Relations Theory: A Critical Introduction*, 3rdEdition, New York: Routledge Publishing.

Wedermyer, L.J. (2012). *The Changing Face of War: The Stuxnet Virus and the Need for International Regulation of Cyber Conflict*. https://www.law.msu.edu/king/2011-2012/Wedermyer.pdf. (Erişim Tarihi: 10.04.2022).

Weimann, G. (2004). Cyberterrorism, How Real Is The Threat?, *United States Institute of Peace***,** Special Report 119, Washinghton DC.

Whitney, L. (2010). *U.S. Cyber Command Prepped to Launch*. https://www.cnet.com/news/u-s-cyber-command-prepped-to-launch/ (Erişim Tarihi: 10.04.2022).

Yalçın, İ. (2019). *Soğuk Savaş Sonrası NATO ve Türkiye'de Siber Güvenlik*. Yayımlanmamış Yüksek Lisans Tezi. Eskişehir: Anadolu Üniversitesi Sosyal Bilimler Enstitüsü.

Yalçınkaya, M. A., ve Küçüksille, E. (2021). Web Uygulama Sızma Testlerinde Kapsam Genişletme İşlemi İçin Metodoloji Geliştirilmesi ve Uygulanması. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 25(1), 16-27.

Yazıcı, A. (2011). Siber Güvenlik ve SAHAB. http://www.emo.org.tr/ekler/fad64faae21db53_ek.pdf. (Erişim tarihi: 18.07.2022).

Yegen, C. (2014). Dijital Aktivizmin Bir Türü Olarak Hacktivizm Ve "Redhack". *Intermedia International E-Journal*, *1*(1), 118-132.

Yenal, S., ve Akdemir, N. (2020). Uluslararası İlişkilerde Yeni Bir Kuvvet Çarpanı: Siber Savaşlar Üzerine Bir Vaka Analizi. *Journal Of The Institute Of Social Sciences Cankiri Karatekin University/Cankiri Karatekin Üniversitesi Sosyal Bilimler Enstitusu Dergisi, 11*(1).

Yılmaz, S. (2014). *Uluslararası Politika ve Dış Poltiika Analizi*, 6. Baskı, Der İstanbul: Der Yayınları.

Yılmaz, Sait ve Salcan, Olay (2008). *Siber Uzay'da Güvenlik ve Türkiye*, İstanbul: Milenyum Yayınları.

Zagare, F. C. ve Kilgour, D. M. (2000). *Prefect Deterrence*. Cambridge, Cambridge University Press.