**T.C.**
**FIRAT ÜNİVERSİTESİ**
**SOSYAL BİLİMLER ENSTİTÜSÜ**
**TEKNOLOJİ VE BİLGİ YÖNETİMİANABİLİM DALI**

# ULUSLARARASI İLİŞKİLERDE SİBER GÜVENLİK KAVRAMI VE UYGULAMALARI

**YÜKSEK LİSANS TEZİ**

**DANIŞMAN**
**Dr. Öğr. Üyesi Zülfükar Aytaç KİŞMAN**

**HAZIRLAYAN**
**Özge GÜLEÇ**

**ELAZIĞ-2021**

# ÖZET

**Yüksek Lisans Tezi**

**Uluslararası İlişkilerde Siber Güvenlik Kavramı ve Uygulamaları**

**Özge GÜLEÇ**

**Fırat Üniversitesi**
**Sosyal Bilimler Enstitüsü**
**İktisadi ve İdari Bilimler Anabilim Dalı**
**Elazığ 2021 Sayfa: IX+88**

Uluslararası ilişkiler sistemi özünde güç, aktör, güvenlik gibi unsurları içermektedir. Soğuk savaş sonrası dönemde teknolojik gelişmelerin hızlı bir şekilde ilerlediği yeni dönemde yeni bir alan olan siber uzay eklenmiştir. Siber uzayın kullanım oranı arttıkça eski güvenlik kavramı dönüşerek yeni modern güvenlik anlayışı hakim olmuştur. Bu bağlamda uluslararası sistemin üzerinde durduğu askeri güvenlik konusunun da alanı genişleyerek siber güvenlik kavramı uluslararası ilişkiler sistemine dâhil olmuştur. Siber güvenlik stratejilerinde önemli çalışmaları olan NATO, AB, Birleşmiş Milletler ve Avrupa Konseyi gibi uluslararası kuruluşlar siber saldırılar konusunda önemli çalışmalar yapmıştır.

Bu çalışmada uluslararası ilişkiler açısından görece yeni olan siber güvenlik kavramı üzerinde durularak çeşitli uluslararası kuruluşların bu alanda yaptığı çalışmalar, aldığı tedbirler, uygulama ve düzenlemeler irdelenecektir. Devletlerarası ilişki ve mücadelenin taşındığı bu yeni düzlemin bir işbirliği düzlemine dönüşmesinde uluslararası kuruluşların payı araştırılacaktır.

**Anahtar Kelimeler**: Siber Uzay, Siber Güvenlik, Uluslararası İlişkiler

# ABSTRACT

**Master's Thesis**

**The Cyber Security Concept and Applications in International Relations**

**Özge GÜLEÇ**

**Fırat University**
**Social Sciences Institute**
**Department of Faculty of Economics and Administrative Sciences**
**Elazig 2021 Page: IX + 88**

International relations system essentially includes elements such as power, actor and security. Cyber space, a new area, has been added in the new era where technological developments have progressed rapidly in the post-cold war era. As the rate of use of cyber space increases, the old security concept has transformed and the new modern security understanding has prevailed. In this context, the field of military security, which the international system emphasizes, has expanded and the concept of cyber security has been included in the international relations system. International organizations such as NATO, the EU, the United Nations and the Council of Europe, which have important works in cyber security strategies, have done important work on cyber attacks.

In this study, the concept of cyber security, which is relatively new in terms of international relations, will be emphasized, and the studies, measures, practices and regulations of various international organizations in this field will be examined. The role of international organizations in the transformation of this new plane of interstate relations and struggle into a cooperation plane will be investigated.

**Keywords:** Cyberspace, Cyber Security, International Relations

# İÇİNDEKİLER

## ÜÇÜNCÜ BÖLÜM

# TABLOLAR LİSTESİ

# ŞEKİLLER LİSTESİ

# ÖNSÖZ

Lisansüstü öğrenimim ve çalışmalarım boyunca tecrübelerini, bilgi birikimlerini ve desteklerini esirgemeyen kıymetli hocam, danışmanım Dr. Öğr. Üyesi Zülfükar Aytaç KİŞMAN'a ve her konuda desteğini esirgemeyen sevgili eşim Uğurcan GÜLEÇ'e teşekkürlerimi sunarım.

**ELAZIĞ-2021** **Özge GÜLEÇ**

# KISALTMALAR

**AB** : Avrupa Birliği

**ABD** : Amerika Birleşik Devletler

**AR-GE** : Araştırma ve Geliştirme

**BİLGEM** : Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi

**BM** : Birleşmiş Milletler

**BSI** : British Standarts Institute

**CCDCOE** : NATO Cooperative Cyber Defence Centre of Excellence

**CDMA** : Kod Bölmeli Çoklu Erişim

**DCSSI** : Central Information Systems Security Division

**DHS** : Amerika Birleşik Devletleri İç Güvenlik Bakanlığı

**DTC** : Delta Trade Company

**ENISA** : European Network and Information Security Agency

**GGE** : Group of Governmental Experts

**NATO** : North Atlantic Treaty Organization

**NIS** : The Network Information Service

**SSCB** : Sovyetler Birliği

# GİRİŞ

Küreselleşme sürecinde; güvenlik farklı bir boyut kazanarak "ulus devlet" anlayışı yerine, dünya ülkeleri arasında modern güvenlik anlayışı hâkim olmaktadır. Bu süreçte devletler, yeni ulus güvenliğin inşası için birçok adım atarak uluslararası kuruluşlarla ortak kararlar almaktadır. Bütünleşme çabası ortak hareketler yoluyla siyasi ilişkiler kavramı daha duyarlı bir hal alarak yeni bir karakter kazanmıştır. Devletlerarasındaki siyasal birleşmelerin boyutu küresel çapta sadece askeri kapasite kuvvetlerin birleşimi olarak değil; sınırların ötesindeki derin, yeni konular önem kazanmaktadır.

Evrensel boyutta oluşan tehditler ya da sorunlar soğuk savaş dönemi gibi tek yönlü değil, daha kapsamlı soğuk savaş döneminden farklı olarak askeri güvenlik sınırının ötesindedir. Devletlerin güvenliğini sarsacak askeri boyutta olmayan sorunlar, ancak devletlerin yine askeri olmayan boyutta işbirliği içinde ortak anlaşmalarıyla çözümlenir. Devletin kendi başına mutlak güç olduğu fikri tüm dünyada çok uzak bir anlayıştır.

Teknolojik gelişmeler ışığında ortaya çıkan "internet" günümüz dünyasının vazgeçilmez parçası olmuştur. Bilişim sistemlerinin yoğun olarak kullanımıyla yeni bir alan ortaya çıkmıştır. Bu alan "siber uzay" olarak adlandırılmaktadır. Ulusal ve uluslararası arenada birçok fayda ve kolaylık sağlayan internet kötü niyetli kişi veya örgütler tarafından kötüye kullanıldığı bilinmektedir. Siber uzayda yapılan her türlü saldırı girişimleri "siber tehdit" anlamına gelmektedir. Oluşan tehditleri minimum zararla atlatmak amacıyla uluslararası kuruluşlar ortak noktada buluşmaktadır. Son yıllarda gerçekleşen siber tehditlerin ve saldırılar basit bir yapıda olmadığı; organize edilmiş güçlü siber saldırılar olduğu görülmektedir. Bu bağlamda özellikle NATO, AB, Birleşmiş Milletler, Avrupa Konseyi, gibi güçlü kuruluşlar ortak hareketle siber yeteneklerini geliştirerek daha dirençli bir alt yapı oluşturdukları bilinmektedir.

Devletler siber güvenlik ile ulusal ve uluslararası düzeyde siber tehditlere ve saldırılara hazırlıklı olmayı amaçlamaktadır. Saldırı gerçekleştiği anda ise saldırı türünün tespit edilip, beraberinde koordinasyon sağlanmasıyla oluşturulmaktadır. Siber güvenlik sadece saldırı ihtimaline karşı değil; aynı zamanda devletlerin kendini, kritik altyapıların korunması için siber teröristlerden muhafaza etmeyi amaçlamaktadır. Uluslararası kuruluşlar da siber güvenliği sağlamak amacıyla birçok çalışma

hazırlamıştır. Bu çalışmaların ortak amacı uluslararası düzenin bozulmaması açısından, kuruluşlara üye olan devletlerin siber güvenliğini sağlamak buna paralel olarak da siber riskleri ortadan kaldırmaktır. Bu bağlamda en büyük örgütlenme olan Birleşmiş Milletler tarafından 2001 yılında, "Bilgi teknolojilerinin suç amaçlı kullanımı ile mücadele" kararı kabul edilmiştir. Siber güvenlik konusunda öncü olarak tanımlanan, uluslararası düzeydeki siber suçlara karşı ilk antlaşma Avrupa Konseyi tarafından hazırlanan "Siber Suç Sözleşmesi"dir. Kosova Krizi, Estonya'ya düzenlenen siber saldırı, Gürcistan siber savaşı sonucunda NATO ittifakı siber güvenlik adına önemli adımlar atmıştır. Avrupa Birliği tarafından siber güvenliği sağlama ve uygulama adına, Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA), ya görev verilmiştir. Ayrıca Avrupa Birliği siber güvenlik hakkında tavsiye kararı ve direktifler yayınlamıştır.

Siber uzayın sınırının olmaması; uluslararası sistemdeki güvenlik kavramının aktörler tarafından, önemli ölçüde etkilendiği ortadadır. Bu kapsamda Amerika Birleşik Devletleri, Almanya, Fransa, Singapur, Çin, Japonya, Avustralya, Birleşik Krallık, Estonya, Kanada, Rusya, İran, İsrail, Hindistan, Güney Kore siber güvenlik alanında kritik altyapılarını korumayı amaçlayan ciddi çalışmalar yapmaktadır.

Çalışmanın birinci bölümünde; uluslararası ilişkiler ve uluslararası ilişkilerde güvenlik kavramı başlığı altında ulus devlet anlayışı anlatılıp güvenlik kavramının uluslararası sistemdeki gelişimi ve yeni (modern) güvenlik anlayışı ele alınarak anlam birliği sağlanması adına ulus-devlet anlayışının ve yeni(modern) güvenlik anlayışının arasındaki temel farklar anlatılacaktır.

İkinci bölümde, siber ile ilgili temel kavramların tanımları yapılacaktır. Uluslararası alanda düzenlenen siber savaşlar hakkında örnekler verilecektir. Siber güvenlik kavramının özellikleri, siber güvenliğin istenilen düzeyde sağlanması amacıyla dikkat edilmesi gereken hususlar, siber güvenlik çalışmalarında bulunması gereken özellikler, uyulması gereken maddeler anlatılacaktır.

Üçüncü bölümde; Uluslararası ilişkilerde siber güvenlik taktikleri ve siber suçlarla mücadelede uluslararası işbirliği, uluslararası kuruluşların siber güvenliği sağlamak amacıyla oluşturduğu evrensel kurallar ele alınacaktır. NATO, Avrupa Birliği, Birleşmiş Milletler, Avrupa Konseyi gibi önemli kuruluşların tarihçesi, yapısı hakkında bilgi verilecektir. Bu kuruluşların siber güvenlik alanında yaptıkları faaliyetler, ilgili yapılanmaları, oluşturdukları politikalar ele alınacaktır. Bazı ülkelerin siber güvenlikle ilgili attığı önemli adımlar, aldığı önlemler hakkında bilgi verilecektir.

**Araştırmanın Amacı**

Tezin amacı, uluslararası ilişkilerde önemli yer tutan güvenlik kavramının, askeri savaşların bitmesiyle yeni bir boyut kazandığını ortaya koymak ve yeni güvenlik anlayışının önem kazandığını, pratikte gerçekleşen siber savaşlardan örneklerle desteklemektir. Ayrıca uluslararası örgütlerin, kritik altyapıların korunması amacıyla yaptığı çalışmalar, stratejileri inceleyerek siber güvenliğin uluslararası işbirliği ile daha yönetilebilir bir alan olduğunu ortaya koymaktır.

**Araştırmanın Önemi**

Siber alanda ve siber güvenlik konularında yapılanan araştırmalara bakıldığında uluslararası ilişkilerde siber güvenlik konusu, alt başlık olarak incelenmiştir. Bu tez çalışması siber güvenliğe ulusal ve uluslararası düzeyde verilen öneme katkı sağlaması, özellikle uluslararası kuruluşların yaptığı faaliyetler, oluşturduğu politikalar ve onayladığı sözleşmeler incelenerek ihtiyaç duyulan geniş kapsamlı bir çalışma olmuştur. Dolayısıyla bu tez çalışmasının devletlerin, uluslararası kuruluşların siber alanda, siber güvenlik konulu yapılacak yeni çalışmalara rehber kaynak olması beklenmektedir.

**Araştırmanın Yöntemi**

Bu çalışmada, siber güvenlik ve uluslararası sistemlerle ilgili yapılan araştırmaların yanı sıra siber güvenlikle ilişkili olan siber uzay, siber tehdit ve siber savaş gibi konulara ağırlık veren makalelerden, tezlerden, eserlerden, kurumlara ait resmi internet sitelerinden ve raporlardan yararlanılmıştır. Bu çalışmamızda, ayrıca bilgi ve teknoloji konulu makalelerden ve tezlerden yararlanılmıştır. Bilimsel makale, dergi ve kitapların yanı sıra AB, NATO, Birleşmiş Milletler, Avrupa Konseyi gibi uluslararası örgütlerin yayınladığı raporlardan faydalanılmıştır. Çalışmamızda siber güvenlik şirketlerinin verilerine de başvurulmuştur. Ayrıca çalışmamızın güncel gelişmeleri kapsaması sebebiyle internet odaklı açık kaynaklardan, gazete haberlerinden yararlanılmıştır. Bu şekilde tez ilgili literatür üzerinden çeşitli değerlendirmeler ve konu hakkında çeşitli tartışmalar yapılarak betimleyici bir biçimde ortaya koyulmuştur.

# BİRİNCİ BÖLÜM

## 1. ULUS DEVLET ANLAYIŞI

Tarihsel süreci incelediğimizde ulus-devlet anlayışı Fransa ve İngiltere kaynaklı olarak ortaya çıktığını görmekteyiz. On dokuzuncu yüzyıldan itibaren ise toplumun modernleşme sürecinde ulus-devlet anlayışının yeniden oluşturulmasında önemli bir araç olarak görüldü. Ulus kavramı, resmi bir alanda toplumun egemenliğini temsil eder. Bu bağlamda ulusun önemi, ortak kültürel değerlerinin yüksekliğine bağlıdır. Bu savın ortaya çıkardığı sonuç aynı kültürel kimliğe sahip olmayanlar yabancı olarak kabul edilir (Zabunoğlu, 2018: 537-541).

Devletlerin bazı değerlerine (fikirleri, kurumsal yapıları, fiziksel yapıları) yönelik her türlü saldırıya karşı devletlerin hürriyetini, egemenliğini ve bütünlüğünü korumak amacıyla yaptığı tüm çabalar ulus-devlet kavramı ile ilgilidir. Ülkeler ulusal politikada bu tehditlere öncelik vererek askeri politikasını bu şekilde oluşturmaktadır (Haser, 2018: 14).

Ulus devlet anlayışı, küreselleşmenin etkisiyle, ulus devlet ötesi durumuna gelmektedir. Ulus devlet anlayışını var olduğu dönemde devlet güvenliğin sağlayıcısı durumdayken, siber güvenlik ile ilgili olarak ortaya çıkan sorunlar (bireylerin kimlik bilgilerin öğrenilmesi, banka hesaplarına izinsiz giriş, hatta ulusal güvenlik sorunlarına kadar) hemen hemen her alanda güvenlik tehditleri devletlerin yeni güvenlik riskleriyle tek başlarına baş edemeyecekleri fikrinin ortaya çıkmasına neden olmuştur. Dünyanın herhangi bir yerinde oluşan sorun diğer ülkelerin güvenliğini de etkilemektedir. Yerel olarak güvenlik sorunlarıyla baş edebilmek mümkün değildir. Güvenliğin bölünmez bir bütün olarak görülmesi, özellikle 11 Eylül saldırı sonrası etkili olmuştur (Oğuzlu, 2007: 9-12).

Klasik sınırların ortadan kalkması ile birlikte, devletlerin karar alma sürecinde dolaylı ya da doğrudan, ulus-devletin yanında bazı uluslararası örgütler güç unsuru olarak yerini almıştır. Uluslararası örgütlerin bu şekilde aktör olması, ortak güvenlik politikaları oluşturmasını sağlamıştır (Yılmaz, Akbulut, 2016: 74).

### 1.1. Uluslararası Sistemin Gelişimi

Uluslararası hukuk nezdinde devletler Viyana Kongresi ve La Haye Konferanslarında sorunlarını barışçı yollarla çözmek maksadıyla bir araya gelmişlerdir. 1899'da yirmi altı devletin katılımıyla; silahlara sınırlandırma getirilmesi konusu ele alınmıştır. Ancak bu konu başarısız olmuştur. Konferansa katılanların oy birliğiyle problemleri barışçı yollarla çözmek ve bu paralelde barışın devamını sağlamak amaçlı bir Daimi Hakemlik Mahkemesinin kurulmasına karar verilmiştir. 1907 yılında İkinci La Haye Konferansı gerçekleşmiştir. Konferansa bazı Avrupa dışındaki ülkeler ve Latin Amerika devletlerinin katılmasıyla temsil edilen devlet sayısı kırk dört olmuştur. Bu Konferans kara ve deniz savaşı kuralları yönündeki düzenlemelerine paralel olarak tarafsızlık hukuku ile ilgili sözleşmeler onaylanmıştır. La Haye Konferansı'nın genel kurallarına bakacak olursak ilkine göre daha başarılı olduğu gözlemlenmektedir (Polat, 2020: 1952).

Çeşitli siyasi, tarihi faktörlere bağlı sorunlar devletlerarasında gittikçe yaygınlaşan siyasi krizler ve insanî felaketler meydana getirmiştir. Değişen uluslararası ilişkiler ve koşullarla, devletlerarasındaki sorunların barışçıl yollarla çözülmesi ihtiyacı devletlerarası ilişkilerin barışçıl işbirliği sağlama imkânı doğurmuştur. Yeni uluslararası sistemle büyük umutlarla kurulan ilk uluslararası örgüt olma özelliğini taşıyan Milletler Cemiyeti (MC) uluslararası barış ve güvenliği sağlamak maksadıyla Birinci Dünya Savaşından sonra kurulmuştur (Sur, 2013: 2536).

Uluslararasındaki örgütlenme savaş sonrası dönemde iki tür teşkilatlanmayla meydana gelmiştir. Birinci; uluslararası işbirliğini ilerletmek amacıyla evrensel özelliğe sahip örgütlenme girişimleridir. Tarihteki ilk evrensel uluslararası örgüt olan Milletler Cemiyeti'nin temel amacı; özellikle bölünmüşlüğün daha kolay kontrol edilmesi ve uluslararası politikanın müzakere temelinde yürütülmesidir. Milletler Cemiyeti'nin örgütsel çalışmaları incelendiğinde; kurumsal anlamda uluslararası ilişkilerde bir devrim niteliği taşıdığı kabul edilmektedir. Milletler Cemiyeti siyasî sorunlarda küçük ve orta boy devletlerarasındaki bazı uyuşmazlıkların çözümünde başarılı olmuştur ancak; daha ciddî uyuşmazlıklarda örgütün başarısız olduğu kabul edilmektedir. İkincisi; devletler birçok girişimler yoluyla belirli bir çerçeve içerisine girmeyi taahhüt ederek, dünyada iki büyük güç olan devletlerin etrafında örgütlenmişlerdir. Böylece; uluslararasında gruplaşma belirginleşerek, ikiye bölünmüş bu yapının her biri kendi

ulusal çıkarları için kendi bloklarının örgütlenmesini gerçekleştirmişlerdir (Arat, Solmaz vd. 2017: 5).

### 1.2. Uluslararası İlişkilerde Güvenlik Kavramı

Güvenlik, uluslararası ilişkileri belirleyen kavramların başında gelmektedir. Güvenlik kavramı, farklı dönem ve koşullarda var olan risklere göre şekillenmiştir. Böylece güvenlik kavramının tanımı, içeriği, unsurları da farklılık göstermiştir (Bakan, Şahin, 2018: 138).Ülkeler arasındaki büyük savaşlar, devletlerin kendi aralarındaçeşitli alanlarda yaptığı antlaşmalarla birlikte sonlanmıştır. Karşılıklı işbirliği ve antlaşmalara dayanan gelişim süreci küreselleşme faktörünü doğurmuştur. Küreselleşmeyle birlikte sorunlar da küreselleşmiştir. Bunlardan bir tanesi güvenliktir. Yaşamımızın her alanında kullandığımız güvenlik kavramı eskilerden günümüze içeriğini zenginleştirerek gelmiştir (Kaypak, 2012: 2). Ayrıca günümüzde devletlerin kendi başlarına baş edemeyecekleri türden çok çeşitli güvenlik problemleri bulunmaktadır. Bu sorunlar hiç şüphesiz bilişim teknolojilerinin gelişmesiyle beraber yaşamımızın her alanına giren internetle birlikte küresel bir hal almış ve böylece yeni suçları da beraberinde getirmiştir. Bunun sonucunda da yeni hukuk düzenlerine ihtiyaç artmıştır. Teknolojinin doğurduğu sorunlardan biri hiç şüphesiz siber suçlardır. Siber suçların doğurduğu sorunlara yönelik uluslararası işbirliği elzemdir (Önok, 2013:1230).

Tarihte her dönemde güvenliğin sürekli kılınması amacıyla hukuksal ve etik kurallar oluşturulmuştur. Devletler önceleri sadece kara, hava, deniz gibi alanlardan ülkelerini korumaya çalışmıştır. Ancak; internetin günlük yaşam akışına katkı sağlamasıyla, tüm sistemler ve temel hizmetler internete bağımlı olmuştur. Fiziki alan olmayan yeni alanda, devlet dışı aktörler kritik sistemlere uzaktan zarar verebilmektedir. Bu kapsamda fiziksel güvenlik kavramı sınırlayıcı özelikte değil; daha geniş ve kapsamlı olarak uluslararası politikada yerini almaktadır.

Dünyada teknolojik gelişmelerin yaşanmasıyla birlikte bireysel ve toplumsal yaşamda yeniliklerin yaşandığı döneme hızla girmektedir. Teknolojik yaşamla, kablolu ve kablosuz ağların insan yaşamını yönettiği dönemi yaşamaktadır. Bu bağlamda ortaya çıkan yeni güvenlik sorunlarıyla ulus devletler birtakım önlem almaktadır. Değişen yeni dünya düzeniyle ortaya çıkan güvenliğin tanım şekli de siber boyutta ele alınmaktadır.

### 1.3. Uluslararası İlişkiler Açısından Güvenlik

Uluslararası sistem, birden fazla ülkenin aralarında düzenli ilişkilerin olduğu ve meydana gelen değişiklerin diğer devletlerin kararlarını etkilediği yapıdır. Uluslararası sistemin temel nitelikleri bu tanımla ortaya çıkmaktadır. a) Güç dengesi sistemi, devletlerin gücü ne olursa olsun aralarında denge sistemin değişmeyeceği, b) Her devletin bir bütünün parçasıymış gibi ortak hareket edip karar verilmesi, c) Etkinlik boyutu ne olursa olsun ortak etkileşimi uluslararası sistemin ana özellikleridir (Demiray, İşcan, 2008: 144).

Bireyler üzerinde büyük öneme sahip olan güvenlik kavramı devletler açısından da aynı oranda önem taşımaktadır. Uluslararası ilişkilerin temel unsurlarından biri olan güvenlik kavramı ulusların da kendi toplumların güvenliği bakımından öncelik sırasının başında gelmektedir. Devletler ulus güvenliğini en büyük değer olarak gördüğünden güvenliği tehdit eden durumları yok etmek için mücadele ederler. Güvenlik ile ilgili uluslararası çalışmalar ikinci dünya savaşına kadar uzanmaktadır ancak yapılan ilk çalışmaların çerçevesi dar tutularak askeri açıdan incelenmiştir (Sancak, 2013: 124-125).Günümüzde ulusal güvenlik sorunlarını çözmek, ağır maliyet gerektiren çok çeşitli bir yapıdır. Devletler kendi başlarına baş edemediğinden uluslararası iş birliği yapmak zorundadır. Özellikle tüm dünyayı etkileyen, çevre kirliliği, yasadışı göç hareketleri, terörist örgütlenmeler gibi güvenlik sorunlarıyla mücadele uluslararası ölçekte incelemek zorunludur. Bu bağlamda saldırgan yaklaşımdan öte işbirlikçi yaklaşıma gidilmelidir. “Ulusal güvenliğin sağlanması, uluslararası güvenlik stratejisiyle bütün olarak görülmelidir. Bu durumun farkında olan Batılı devletler, kendi aralarında kolektif olarak güvenlik toplulukları (NATO, AB gibi) oluşturmuştur. Sözü edilen toplulukların üye devletlerarasındaki ilişkilere bakıldığında askerî güç kullanımı artık önemli bir rol oynamamaktadır. Bir arada hareket ederek, uyum içinde stratejiler üretip uygulama, örgütler açısından önem arz etmektedir (İşyar, 2008: 4-8).

Devlet, güvenliğin sağlanmasından mesul bir araçtır. Söz konusu güvenliğin sağlanmasından sorumlu devletin kendisi olmaktadır. Bu bağlamda uluslararası güvenlik kavramı; “ulus-devletlerden meydana gelen uluslararası sistemin, savaş tehdidinden uzak, küresel çatışma ve savaşlardan korunması olarak tanımlanabilir.” Bu tanımla uluslararası güvenlik kavramının iki boyutunun olduğu ortaya çıkmaktadır. Bunlardan ilki; bir ulus devletin, uluslararası sistemde ulusal güvenliğini oluşturmasına yönelik sağladığı uluslararası güvenlik anlayışı, İkincisi ise; uluslararası sistemin bir

bütün olarak güvenliği anlayışıdır" Bu bağlamda devletler güvenlik sorunlarını ele alırken sadece kendi güvenliğini düşünerek hareket etmemekte uluslararası güvenlik gibi kavramını da sıklıkla incelemektedir(Özcan, 2011: 449-450).Bu düşünceyle uluslararası güvenlik kavramı farklı boyutlarda ele alınmaktadır (Yorulmaz, 2014:109).

**Tablo 1.** Uluslararası Güvenlik Kavramının Farklı Boyutları

| **Bireysel boyutta** | **Ulusal boyutta;** | **Bölgesel boyutta** | **Küresel boyutta** |
|---|---|---|---|
| Bireylerin güvenliği. | Aynı ülke içinde yaşayan toplumun güvenliği, ulus-devlet güvenliği | Coğrafi ya da alt sistemlerin güvenliği. | Uluslararası sistemin güvenliği |

Fakat; günümüzde uluslararası ilişkilerde, bölgesel ve küresel açıdan güvenlik kavramı daha fazla ilgi gördüğünden, ulus-devlet anlayışına ek olarak güvenlik, global boyut olarak daha çok değer kazanmıştır (Yorulmaz, 2014:109).

Güvenlik olgusu genel olarak barış kavramıyla ilgilidir ve sadece bireysel olarak algılanmamalıdır. Ulus-devlet ya da ulus-devlet dışı aktörlerin yer aldığı büyük bir alan seviyesinde incelenmelidir (Brauch, 2008: 3).

- Sonuç olarak gelişen ve değişen dünyayla mücadele edebilmek ortak politikalar üretmekle mümkündür. 21. Yüzyıl için Robert Cooper ülkeler arası güvenlik işbirliği amacıyla beş madde belirlemiştir. Ülkelerin sahip olması gereken beş madde aşağıdaki gibidir (Terzi, 2018: 93):
- Yabancılara empati kurarak yaklaşılmalı.
- İç politikanın ne demek olduğu anlaşılmalı ve dış politika da buna göre oluşturulmalıdır.
- Yabancıları ikna ederken güç kavramı kenara bırakılıp değerler mevzusunda şuur oluşturma düşüncesi ön plana çıkarılmalıdır.
- Dış politika salt çıkar olarak algılanmamalı, ülkelerin kendileriyle alakalı çıkarları anlatma biçimi olabilir.
- Problem çözümünde karşı tarafa yenilme duygusu oluşturmak yerine farklı sahalarda da onların söz sahibi olmasına dikkat edilmelidir.

Güvenlik kavramı 1990'lardan itibaren bilgi teknolojilerinin hızlıca gelişmesiyle, küreselleşme olgusu da hız kazanarak "artık hiçbir şey eskisi gibi

olmayacak" sözünü onaylarcasına, her sahada "çok hızlı ve önüne geçilemez" bir "değişim süreci" başlamıştır. Dolayısıyla özellikle 1990'lardan önceki dönemlerde kabul gören askeri, ekonomik ve güvenlik politikaların temel alındığı stratejilerin çoğunun ortadan kalktığı bir döneme girilmiştir. O dönemdeki yani soğuk savaş dönemindeki klasik güvenlik algısını ele alıp; küreselleşmeyle birlikte yeni modern güvenlik algısı ve bu dönemde geleneksel güvenlik problemleri olarak görülen savaş, terör vb. kavramlar farklılaşarak yeni bir kavram olan bilgi, veri güvenliğine yönelen tehditlerin neler olduğu ve bu bağlamda güvenlik tanımlanması ve açıklanması "Soğuk Savaş öncesi ve sonrası" olarak incelemek gerekmektedir (Erdoğan, 2013: 266-267).

### 1.3.1. Soğuk Savaş Döneminde Güvenlik Algısı ( Klasik Güvenlik )

George Orwell tarafından ilk kez kullanılan "Soğuk savaş" terimi; ABD'nin ve Sovyet Birliğinin aralarındaki sosyal ilişkileri ve henüz açıklanmayan savaş halini göstermek için kullanılmıştır (Kolasi, 2013: 153).Tehdit, savaş, kriz gibi kavramların egemen olduğu soğuk savaş dönemi genel olarak en kanlı dönem olarak adlandırılmaktadır. Dönemi şekillendiren hiç kuşkusuz savaşlar olmuştur. Bu açıdan değerlendirildiğinde güvenlik; ulusal güvenliği ve kendi çıkarlarını sağlamak amacıyla devletin askeri gücünü kullanarak başarı elde etmesine bağlıdır. Devlet bu açıdan ulusal güvenlik sağlamanın ön koşulunu askeri güce bağlı olduğunu vurgulamaktadır (Sandıklı, Emeklier, 2012: 3, 6, 7).

Soğuk savaş döneminde nükleer tahribat devlet bekası için en büyük tehdit olarak görülmüştür. Bu yüzden askeri silahlanma en üst düzeye çıkarılmış ve güvenlik için sivil savunmaya önem verilmiştir. Bununla birlikte güvenlik anlayışı devlet odaklı olup, dış politikada ulusal çıkarlar ön plana alınmıştır (Şahin, 2015: 98).Askeri güvenlik kavramıyla birlikte bu dönemin güvenlik anlayışına ekonomik güvenlik kavramı eklemlenmeye çalışılmış ancak askeri-stratejik konular yine konunun ağırlık gündeminde olmuştur (Ayhan, 2016: 135).

Geleneksel güvenlik anlayışının temelinde savaş her zaman ihtimal olarak görülmektedir bu yüzden devletler savaş durumunun olması halinde, askeri güçlerini hazır bulundurmak isterler. Bu anlayıştan yola çıkarak ülkeler arasında ittifak kurmak karşılıklı güven sağlamanın en önemli yoludur (Haser, 2018: 14).

Klasik anlamda, uluslararası arenadaki tüm devletler, büyüklüklerine, bölgesel pozisyonlarına, sosyal, kültürel, dini, ekonomik, askeri, teknolojik, vb. yapılarına ve

çeşitli özelliklerine göre farklı güvenlik gereksinimlerine veya güvenlik anlayışına sahiptiler. Bu özellikler günümüzde de önemini yitirmemiştir ancak hızlı bir şekilde içerik değişikliğine uğramıştır (Özdemirci, Torunlar, 2018: 81).

Kısacası geleneksel güvenlik anlayışı askeri güç, askeri stratejiler olarak algılanmaktadır. Ana konuları askeri tehdit ve düşmanlardır. Devletlerin kendi güvenliğini tehdit altında görünce, karşıdaki devletin de güvenliğini sarsmak için gerekli tedbirlere başvurmasına neden olmakta bu da diğer tarafın aynı biçimde yanıt vermesine sebep olmaktadır. Yani güvenlik anlayışının temelinde askeri güç söz konusudur (Demiray ve İşcan, 2008: 152-153).

### 1.3.2. Modern Anlamda Güvenlik

Modern toplumların gelişmesiyle birlikte soğuk Savaş sonrası dönemde, bilgi teknolojilerinin unsurları olan veri akışı, teknoloji transferi vb. kavramlar gelişerek, farklı toplumlar arasındaki iletişimin hatta kültürel etkileşimin artmasına neden olmuştur. Bunun sonucunda yeni bir dönem başlamıştır (Erendor, 2017: 119). Yeni dönemim başlamasıyla uluslararası güvenlik anlayışı; soğuk savaşın sona ermesi ve küreselleşmenin etkisiyle askeri disiplin ve devlet odaklı olmaktan çıkıp yeni boyut kazanmıştır. Bu süreç ile birlikte "insan güvenliği", "toplumsal güvenlik" ve "dünyanın güvenliği" gibi birçok yeni kavram kendini göstermeye başlamıştır (Ağır, 2011: 99, 104). Klasik güvenlik anlayıştan modern güvenliğe geçişin en önemli nedeni kuşkusuz siber alanın artan kullanımı ve siber alandaki artan rekabetin önemidir ancak kendine has özelliği sınırsız bilgi teknoloji ağların oluşturduğu bilgi ortamındaki bir küresel alan olan siber uzay; siber saldırıya uğramış kişi kurum ya da devlet tarafından soğuk savaş döneminden farklı olarak saldırının kaynağını tanımlamasını zorlaştırmıştır (Tarhan, 2018: 52).

Eski savaş sistemlerin bitmesiyle birlikte her geçen gün büyüyen ve karmaşık hale gelen siber tehditler ve savaşlar daha zararlı hale gelmiştir. Kimilerine göre "kirli savaş" olarak görülen kimilerine göre ise "savaşanların her türlü şiddet ve suç eylemiyle beraber, medyanın ve bilgi akışının da silah olarak kullanılabileceği" bir kavram olarak gördüğü hibrit savaşlar; tarafların birbirleriyle sadece savaş alanında çatışmadığı, hedef kitlelerinin "zihinlerini kazanma savaşı" olarak görülen ve bu amaç için ellerinden geleni yaptığı çatışmadır. Hibrid Savaş'ın hedef kitleleri yalnızca halk değil, aynı zamanda uluslararası aktörlerdir. Askeri avantaj sağlamak gibi, "manevi güç ve zafer"

sağlamak amacıyla yapılan bu savaşlar hedef ülkenin stratejik internet noktalarını çökertme biçiminde gerçekleştirilir (Hibrid Savaş ve Siber Saldırılar, 2019).

Bugün artan nüfus, gelişen teknoloji, farklılaşan talep ile birlikte bilgi sistemlerinin güvenliği zorlaşmaktadır. Bu noktada yapılacak en büyük adım bilgi sistemlerin güvenliğini tehdit eden faktörlerin neler olduğunu belirlemek ve gerekli tedbirleri almaktır (Eroğlu, 2019: 1577). Tüm bu sıkıntılara rağmen devlet kendi kaynaklarıyla birlikte tehditlerle başa çıkmak zorundadır. Bu da ülkelerin, ulus devlet anlayışıyla siber uzay, siber tehdit, siber savaş, gibi kavramları algılama kabiliyeti, siber güvenlik önlemlerini alma biçimine bağlıdır (Bıçakçı, 2015: 29). Ulus-devlet anlayışının yerine ulus devlet ötesi kavramının hâkim olduğu bu dönemler de küreselleşme sürecine paralel olarak güvenliği tehdit edecek faktörlere karşı nasıl bir yol izleneceği, uluslararası sistemin yapısı incelenerek mücadele verilmelidir (Oğuzlu, 2007: 2).

Uluslararası ilişkilerde, küreselleşmenin etkisiyle şeklen değişen tehditlerle beraber askerî olmayan tehditlerin de dâhil olmasıyla uluslararası sistemin mücadele yöntemleri de güncellenmiştir. Bu bağlamda birçok stratejik mücadele ve işbirlikleri yapılmıştır (Dedemen, 2016: 143). Özellikle önemli altyapı ağlarına karşı gerçekleşme olanağı olabilecek siber saldırılara ve savaşlara karşı aktif savunma politikaları uluslararası arenada faaliyet gösteren kuruluşlarla oluşturulmuştur (Meral, 2015: 95).

**Tablo 2.** Klasik savaş ile Modern Savaş Arasındaki Farklar

| | **Klasik Savaş** | **Modern Savaş** |
|---|---|---|
| **Yararlanılan Araç** | Silah, Bomba, Füze vs. | Bilgisayar, Yazılım |
| **Amaç** | Toplumsal, siyasal, mesaj vermek. | Hükümet veya topluma zarar vermek |
| **Teknoloji** | İleri düzeyde teknolojiye ihtiyaç vardır. | Mevcut teknoloji saldırı için yeterlidir. |
| **Etkilediği Alan** | Saldırının gerçekleştiği bölge. | Ulusal veya uluslararası |
| **Risk Durumu** | Eylemi yapan kişi veya kişiler hayati risk altındadır. | Eylemi yapan kişi ya da kişiler hayati risk olmadan saldırı yapabilirler. |
| **Hız** | Savaşta kullanılan silahların hızındadır. | İnternetin hızına bağlıdır. |
| **Denetim** | Savaşa neden olanları gözlemek denetim altında tutmak, yok etmek nispi olarak mümkündür. | Siber savaşa neden olanları tespit etmek ya da yok etmek mümkün değildir. |
| **Saldırı Maliyeti** | Maliyeti yüksektir. | Maliyeti düşüktür. |
| **Zarar Tespiti** | Kolay yapılır. | Zor yapılır. |
| **Uygulanacak Ceza** | Suçun niteliğine, boyutuna göre uygulanacak ceza bellidir. | Siber suçların niteliğine göre uygulanacak ceza belli değildir. |

**Kaynak:** Karadağ, 2019: 20.

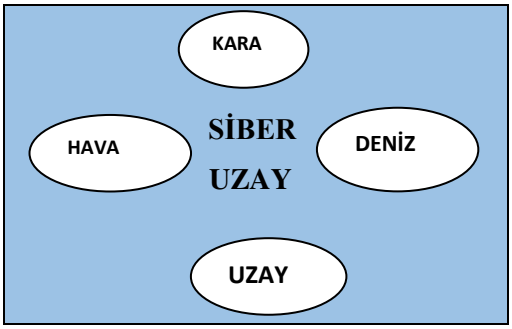
# İKİNCİ BÖLÜM

# 2. SİBER KAVRAMI VE SİBER GÜVENLİK KAVRAMI

Kara, hava, deniz, uzay alanlarına ek olarak internet kavramının ortaya çıkmasıyla dünyadaki fiziksel alanın dijital ortama aktarılmış yeni bir alan olan "siber" kavram meydana gelmiştir. Siber kavramları daha iyi anlayabilmek için kendi terimleri ile anlaşılmalıdır. Siber kavram İletişim sağlanırken zaman ve mekândan bağımsızdır. Siber uzayın varlığıyla, bilgi sistemlerinin sadece bireysel olarak kullanılmadığı, bilgisayar ağları sayesinde siber uzayın bir parçası olarak ortaya çıkmaktadır. Çalışmanın bu bölümünde siber kavramı ile ilgili çeşitli tanımlamalara yer verilecektir.

## 2.1. Siber Uzay

Akıllı telefon, bilgisayar gibi aletler sadece teknolojik nesne değil aynı zamanda kişisel bilgilerin ve verilerin yer aldığı sanal ortamdır. İnsanların ya da devletlerin teknoloji ağlarını kullandıkları yapay ortam olan siber uzay; siber alanın ana kavramıdır. Çünkü bilgiye ulaşmak, bilgiyi paylaşmak gibi temel döngüler siber uzayda gerçekleşir (Korhan, 2018: 5). Devletlerin güvenliği teknolojik gelişmelere bağlı olmasıyla birlikte siber uzayda olan teknolojik gelişmelere hakim olamayan devletler de ciddi güvenlik sorunlarıyla karşılaşırlar. Bu yüzden devletler güvenlik alanında klasik anlamda oluşturduğu stratejilerini yeniden şekillendirerek siber tehdit ve siber savaşlara karşı yeniden organize etmesi gerekmektedir (Çelik, 2018: 111).




**Şekil 1.** Siber Uzay

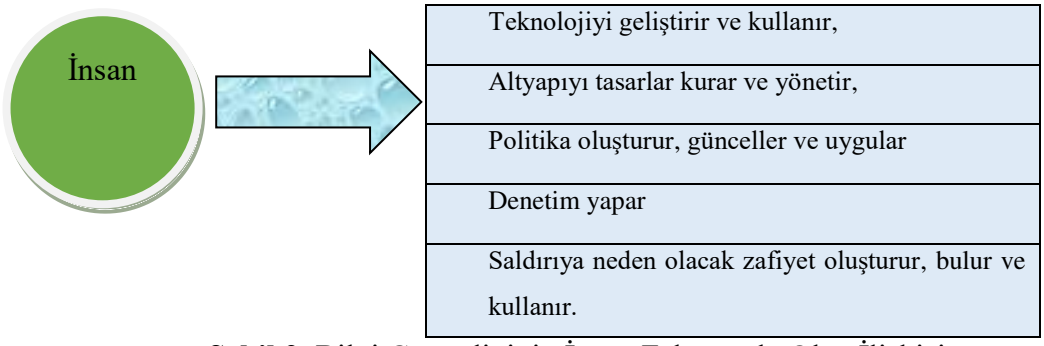
(Karadağ, 2019: 20).

Siber uzay belli bir fiziksel alan değildir. Dünyadaki fiziksel alanın dijital ortama aktarılmış biçimidir. İletişim sağlanırken zaman ve mekândan bağımsızdır. Siber uzayın varlığıyla, bilgi sistemlerinin sadece bireysel olarak kullanılmadığı, bilgisayar ağları sayesinde siber uzayın bir parçası olarak ortaya çıkmaktadır.

Alkan vd. (2018) eserinde ifade ettiği üzere siber uzay çok katmanlıdır ve dört ana öğeden oluşmaktadır (Alkan vd, 2018: 87-88):

1. Fiziksel altyapı (Havadan ve karadan geçen kablolar, yol boyunca haberleşmeyi sağlayan aygıtlar, yönlendiriciler, vb.)
2. Mantıksal yapılar (Genel olarak yazılımı ifade eder. Örneğin tarayıcılar, işletim sistemleri, cep telefonu yazılımları vb. Ayrıca yazılım, fiziksel birimlerin iletişimini, haberleşmesini ve görev yapabilmesine olanak sağlar.)
3. Bilgi(Sosyal medya ve internet ortamındaki tüm yazışmalar, e-postalar, fotoğraf, videolar vb.)
4. İnsan (Siber uzayın en önemli unsurudur. Çünkü iletişimi sağlayan yani bilgiyi kullanan, değiştiren, ileten, fiziksel ve mantıksal birimleri planlayan ve kullanan kişi insandır.)

Siber uzayı oluşturan insan katmanında oluşacak herhangi bir eksiklik ya da yanlışın diğer tüm katmanları da etkisiz hale getirecektir. Bilgi güvenliği ve siber güvenliğin insan faktörüyle olan ilişkisi şu şekildedir (Erol, 2016: 14).




**Şekil 2.** Bilgi Güvenliğinin İnsan Faktörüyle Olan İlişkisi

Yeni dünya güvenlik anlayışına göre birçok rapor, tasarı yayımlanmaktadır. Son zamanda yayımlanan Sophos 2021 Tehdit Raporu siber uzayın dünya genelinde nasıl etki etkileyeceği geniş bir bakış açısı sunmaktadır. Bu rapora göre:

- Tehdit oluşturabilecek gündelik bilgilere daha fazla dikkat etmek gerekmektedir.

- Siber hackerler tespite dair önlemlerden, ilişkilerden kaçınmak için güvenlik analizlerine engellemek maksadıyla bilinen yasal araçları, yardımcı sistemleri ve ortak ağ hedeflerini kullanacaktır.
- Siber saldırılar hız kesmeden devam edecektir
- Covid-19 salgınıyla artan internet kullanımı bilgi güvenliğini tehdit edecektir.

İstenmeyen reklamlar her yıl olduğu gibi bu yılda da sorun yaratacaktır (2021 Tehdit Raporu Önümüzdeki Yılın Siber Saldırı Eğilimlerine Işık Tutuyor, 2021).

### 2.2. Siber Tehdit

Günümüzde bilgi alanı, bilgi teknolojilerini kullanım oranı genişlemekte böylece siber uzayı oluşturan faktörlerin kullanım hızı da yaygınlaşmaktadır. Bunun sonucunda bilgi ya da iletişim teknolojilerine ve birçok sektöre düzenlenen saldırılar da artmaktadır. Siber uzayda yapılan her türlü yıkıcı, bozucu eylem ya da engelleyici ve ele geçirici özelliklere sahip girişimler ile siber saldırıların farklı araçlar ve unsurlar ile siber uzayda kullanılmasına siber tehdit denir (Çeliktaş, 2016: 8-9).

Siber tehditler, bilgi güvenliği sağlanması aşamasında gündemi belirlemektedir ve çoğunlukla üç ana başlık altında toplanmaktadır. (Henkoğlu, Yılmaz, 2013: 457).

1. Bilişim Sistemindeki bilgilere izinsiz erişim,
2. Sistemi bölme, bilgileri değiştirme ya da verileri yok etme, bilgi sistemini engelleme
3. Kimlik bilgilerini çalma ve bireysel bilgilerin kötüye kullanımıdır.

Siber tehditle beraber kötü niyetli kişiler; ulaştıkları sistemin ağ yapılarını bozmakta veya kullanılamaz hale getirmektedirler. Bu yüzden siber tehdidin ulusal olarak algılanması gerekmektedir.

Siber tehdidin ulusal olarak algılanması ve gerekli önlemlerin devlet tarafından alınması siber tehdidin boyutunu değiştirmektedir. Siber tehdit artık uluslararası düzeyde algılanmaktadır. Siber uzayın yapısı gereği boyut ve mekân algısının olmaması; devlet dışı aktörlerin, istediği zaman küresel olarak örgütlenerek farklı ülkelere ya da kurumlara siber saldırılar düzenleyebilmektedir (Yayla, 2014: 184). Özellikle soğuk savaş sonrası dönemde ülkeler arası savaş ekonomi ve teknoloji alanında olmuştur. Bir devletin ekonomisinin iyi olması ve teknolojisini sürekli geliştirmesi diğer ülkeler tarafından hedef tahtası durumuna gelmiştir. Düşman ülkeler

hedeflediği bu ülkelere her türlü elektronik saldırı düzenleyerek, sistemlerini çöktürmeyi, bilgilerini sızdırmayı, amaçlamaktadır(Ercan, 2015: 13).

Siber dünyada siber tehditler özellikle küresel çapta etkin olan şirketleri, devletleri hedef almaktadır. STM Ekim-Aralık 2020 Siber Tehdit Durum Raporuna göre gerçekleşen siber saldırılar şu şekildedir:

1. Kuzey Kore tarafından desteklenen Lazarus Grubu 2014- 2018 yılları arasında 13 ülkede 16'dan fazla kuruluşa siber saldırı düzenlemiştir. Bilinen son siber saldırısı ise Kuzey Kore tarafından 2020 yılında Güney Kore'nin verilerine erişim sağlamak amacıyla düzenlediği APT saldırısıdır.
2. COVID-19 Döneminde; Almanya'da Biontech şirketini tüm dünya tanıdı. Şirketin yaptığı çalışmalar sonucunda (COVID-19) aşısı deneklerin üzerinde yüzde 90 etkili oldu. Bu haberin tüm dünyada yayılması üzerine 2020 yılı Eylül ayında şirkete bilgisayar korsanları tarafından büyük bir siber saldırı düzenlendi. Ancak Biontech şirketinin koruyucu tedbirlerinin etkisiyle; yapmış olduğu incelemeler sonucunda saldırıların herhangi bir hasara yol açmadığı belirtilmiştir.
3. COVID-19 kriziyle çocukların sanal ortamda geçirdiği süre artmaktadır. Söz konusu artışla zamanın doğru kullanılmaması göze çarpmaktadır. Sokağa çıkma yasağının uygulandığı son dönemde online ortamda çocukların geçirdiği süre son yılların rekor seviyesine ulaşmıştır. Hayatımızdaki bu değişim çocuk istismarcıların çocukları kandırmak amacıyla birçok Web sitesinde anket doldurma linkleri göndererek ardından Whatsapp uygulamasından linklere devam edenlerin20 arkadaşına göndermesi gerektiği belirtilmektedir. Linkleri tanımlayan kullanıcıların ayda68 TL'lik bir hizmete üye olduğu gözlenmiştir (Thinktech STM Teknolojik Düşünce Merkezi: 8-10).

Şirketlerin ve ülkelerin siber saldırıya maruz kalmaması için;

- Siber güvenlik çalışmaları yapmaları ve güçlü uygulamalar kullanmaları,
- Siber tehditleri önceden belirlemek amacıyla siber tehdit modeli oluşturmaları,
- Şirkette siber güvenlik personelleri bulundurmaları,
- Firmaların birbirleriyle olan ilişkilerinde daha dikkatli davranmaları önerilmektedir (Thinktech STM Teknolojik Düşünce Merkezi: 8-10).

### 2.3. Siber Savaş

Siber savaş gizli veya gerçek bir biçimde düzenlenir ve etkileri hızlı bir şekilde görülür (Ercan, 2015: 13). Ancak siber savaş günümüzün en popüler konularından biri olmasına rağmen kavramsallaşma sürecini hala tamamlayamamıştır. Örneğin "kara harbi" ya da "hava harbi" nedir? diye soracak olursak uzlaşılan ortak cevap var iken, siber savaş için aynı durum söz konusu değildir. Bu noktada devlet düzeyindeki aktörlerin olabilecek siber savaşlara karşı meşru faktörlerin cevabını bilmesi gerekmektedir (Kasapoğlu, 2017: 1-3). Oysa siber savaşın tarihçesi Körfez savaşına kadar uzanmaktadır.1990 yılında ABD'nin Irak'a uygulamayı planladığı; Irak sistemlerini etkisiz hale getirmek istemesi, siber savaş tarihinin ne kadar eskilere dayandığını göstermektedir (Yayla, 2013: 186).

Savaşların harp meydanında değil de internet ortamında yani siber uzayda gerçekleşmesi, olabilecek 3. Dünya Savaşının da cephelerinden birinin siber uzay olacağı ihtimalini artırmaktadır. Böylece birçok ülke siber tehdit ve siber savaşlara karşı kendisini müdafaa etmek amacıyla kendi bünyesinde siber güvenlik kurumları oluşturmakta ve bu alanda birçok faaliyette bulunmaktadır (Önaçan, Atan, 2016: 15).

**Tablo 3.**Siber Tehdit ve Savaşın Ana Özellikleri.

| **Eylemler** | Siber Tehdit | Siber Savaş |
|---|---|---|
| **Eylemin Özelliği** | Doğrudan | Doğrudan, sembolik |
| **Eylemin Şiddeti** | Az yoğun | Çok yoğun |
| **Motivasyonu** | Siyasal, kişisel sebepler | Casusluk, politik nedenler ve doğrudan savaş yeteneğinien aza indirgemek, |
| **Suçluları** | Bireyler, suç teşkilatları, Anonim | Suçlular tam olarak öğrenilmese de hangi devletlerin neden olduğu bilinebilir. |
| **Amaçları** | Gözdağı vermek, güç elde etmek, kontrol sağlama, maddi kazanç sağlamak, sömürme, intikam | Kritik kuruluşlar, ekonomik ve endüstriyel altyapılar, Güvenlik Birimleri, Hükümet Temsilcilikleri, Askeri Altyapılarına Saldırı |
| **Kaynağı** | Ülke İçinden veya Dışından | Ülke Dışından |

Literatürde siber savaş ve siber saldırıları olaylarının birlikte bahsedildiği görülmektedir. Bu bağlamda incelenen örneklemler, siber saldırı ve siber savaş olaylarına yer vermektedir. Siber saldırı ve siber savaş olarak kabul gören bazı olaylar şu şekilde sıralanabilir:

2003 Yılında, İkinci Irak Savaşı'nda ABD, Irak askeri ağına bir şekilde sızarak, savaşa öncesinde "Irak Savunma Bakanlığı" ağı üzerinden binlerce Iraklı asker ve subayın savaş öncesinde ABD'ye boyun eğmelerini istedikleri e-posta göndermiştir. Yapılan bu saldırının, geleneksel savaşın hemen öncesinde olması bir siber savaş örneği olarak görülmüştür. Siber saldırı ile Iraklı asker ve subayların moralini bozmak amacıyla psikolojik savaş uygulanmış ve böylece düşmanın savunması etkin bir biçimde zayıflatılmıştır. Bilgi savaşın yanında bu mücadele psikolojik savaş olarak da adlandırılmaktadır (Çeliktaş, 2016: 54).

Siber savaşlar bazen geleneksel savaşlara göre daha etkin olabilmektedir. 2007'de Rusya kaynaklı Estonya'ya düzenlenen siber saldırı ülkenin parlamentosu, ekonomi merkezleri, ulaşım ve güvenlik sistemleri bir aya yakın süre iş yapamaz duruma getirilmiştir. Siber saldırıların sonucu bununla kalmayarak, Estonyadaki Rus askerleri tutuklanmış bunun sonucunda ise ülkede iç karışıklık meydana gelmiştir (Tarhan, 2018: 40).

2008 Yılında Gürcistan'a yapılan siber saldırı klasik savaşın siber uzayda, siber savaş cephesine geldiğinin göstergesidir. Rusya siber savaşçıları Gürcistan'a internet ağı trafiğini yöneten tüm aygıtları ele geçirerek, Gürcülerin başka ülkelerle olan iletişimini engellemiştir. Ülkedekiler böylece, başka ülkelere e-posta dahi gönderememiştir (Güngör, Güney, 2017: 142).

ABD tarafından 22 Haziran 2009'da ve 7 Temmuz 2009 Tarihinde İran'ın Natanz nükleer yakıt tesislerine karşı iki farklı saldırı düzenlenmiştir. Saldırı da tesisteki bilgisayar ağları hedef alınmıştır. ABD'nin saldırı da kullandığı virüs programları incelendiğinde; doğal gaz, su, kanalizasyon ağları gibi önemli altyapıların denetimi, enerji üretim ve dağıtımının kontrolü gibi kritik altyapıların izlenmesinde kullanıldığı ortaya çıkmıştır (Çelik, 2013: 146).

Farklı din ve ırka sahip birçok milletten insan ve malzeme taşıyan gemiler Gazze'ye yardım amaçlı malzeme götürmek için 2010 yılında İsrail tarafından uluslararası sularındayken saldırıya uğramıştır. "Saldırının öncesinde gemiden dünya medyasına yayın yapan uydu frekansı ve uydu telefonlarının iletişimi tamamen

kesilmiştir. Böylece; yardım gönüllüleri ile bağlantı kurulamamıştır.” İsrail askerlerin saldırısı sonucunda 9 gönüllü hayatını kaybetmiştir (Kara, 2013: 50).

2013 Yılında Rusya kaynaklı diğer bir saldırı ise, Ukrayna’ya yapılmıştır. Rusya Ukrayna Hükümeti’nin web sitelerine saldırarak, iletişim ağlarını çökertmiştir. Yaşanan siber kriz Rusya’ya olumlu etkisi olmuştur. Yaşanan bu siber saldırıdan sonra Rus siber güvenlik stratejisinde Putin’in isteği doğrultusunda yeni birçok çalışmalar yapılmaya başlanmıştır (Alizada, 2019: 99).

Rus uçağını Türkiye’nin 24 Kasım 2015 Tarihinde düşürmesinin ardından, 14-25 Aralık Tarihleri arasında Rus kaynaklı olduğu düşünülen birçok siber saldırı gerçekleşmiştir. İnternet faaliyetlerinin engellenmesi maksadıyla yapılan bu saldırılar sonucunda “edu.tr”, “gov.tr” “com.tr” gibi “tr” “uzantılı 400 bin siteye 1 hafta sürecince ya hiç girilememiş ya da bahsi geçen sitelere girişlerde çeşitli problemler yaşanmıştır (Çeliktaş, 2016: 59).

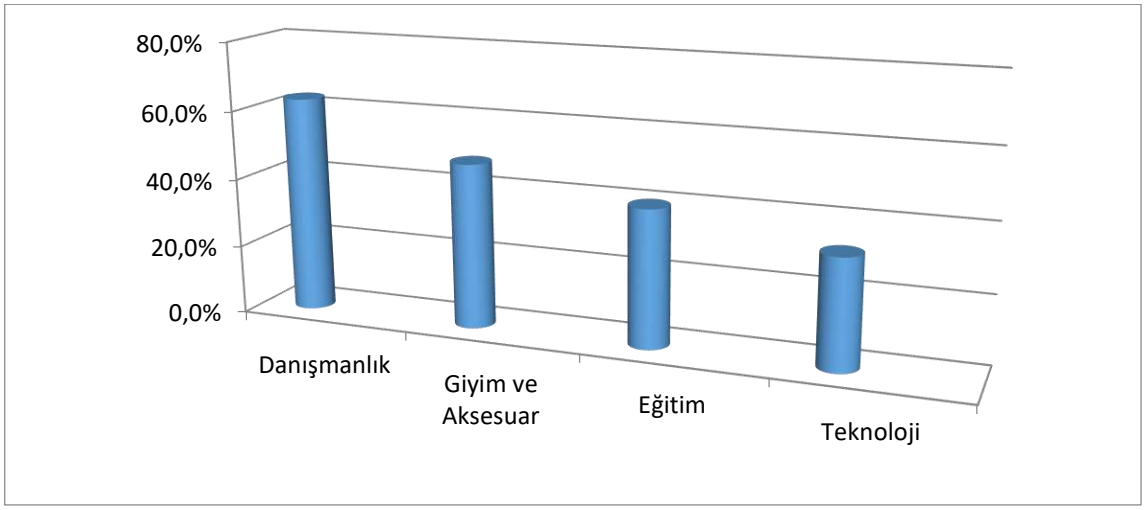
Dünyaca tanınan Siber güvenlik Şirketi Keepnet Labs, dünyada ve iş dünyasında gerçekleşen siber saldırılar hakkındaki verileri ortaya koymuştur. Bu verilere göre kötü amaçlı yazılımlarla en çok E-posta aracılığıyla saldırı düzenlenmektedir.

**Tablo 4.** Kötü amaçlı yazılımları tıklama yüzdesi

| **E-postayı Açan** | **E-postada Bulunan Bağlantıyı Tıklayan** | **Hassas Bilgilerini Veren** |
|---|---|---|
| %50.42 | %32.09 | %12.71 |

Siber güvenlik Şirketi Keepnet Labs firmasının yayımladığı rapora göre saldırılara karşı en savunmasız sektörler:

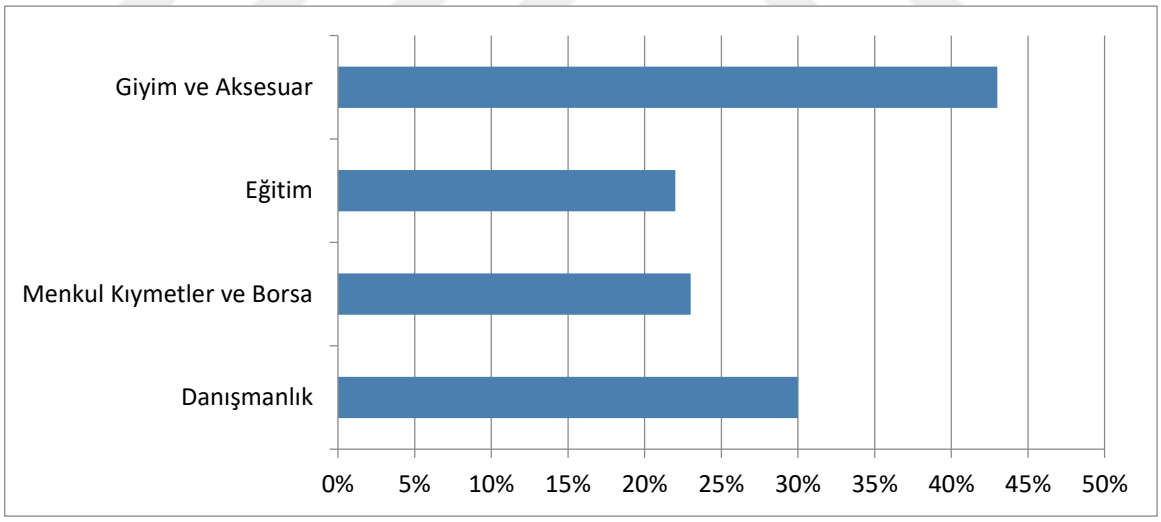
**Tablo 5.** Siber Saldırılara Karşı En Savunmasız Sektörler




**Kaynak:** (Siber Saldırılardan En çok Etkilenen Sektörler, 2020).

E-Postalardaki kötü amaçlı yazılımlara en çok tıklayan sektörler: Danışmanlık, Giyim ve Aksesuar, Eğitim, Teknoloji'dir.

**Tablo 6.** Sektörler arasında bilgi paylaşımı ve bilgi sızdırmada en yüksek oranlı sektörler:




**Kaynak**: (Siber Saldırılardan En çok Etkilenen Sektörler, 2020).

Yukarıda bahsedilen siber saldırı ve savaşları kategorilere ayırmak ve tanımlamak mümkündür (Erendor, 2017: 125-126):

1. Bilişim Saldırıları/Bilgi Saldırıları: Siber saldırıyla, elektronik ortamda bilgisayar sistemlerini etkisiz hale getirmeyi ya da içindeki bilgileri değiştirmeyi veya yok etmeyi amaçlamaktadır.
2. Altyapı Saldırıları: Bilgisayar ortamındaki programlamayı hedef alarak işletim sistemini bozmayı amaçlar.
3. Teknolojik Kolaylaştırma: Siber iletişimi, siber terörü sağlamak adına kullanıp, planlar göndermek ve siber savaşı kolaylaştırmak.

### 2.4. Siber Güvenlik

Güvenlik, insanoğlunun var oluşundan beri en temel ihtiyaçlarından biri olmuştur. Toplumların ve devletlerin temel taşı olan insan, güvenlik problemleriyle karşılaşmamak için gerekli tedbirler almıştır. Geçmişte uygulanan ilkel güvenlik tedbirleri teknolojinin gelişmesiyle, yerini modern uygulamalara bırakmıştır. Bilgisayarın yaşamımıza girmesiyle, insanlar ve kurumlar bilgisayarları aktif bir şekilde kullanmaya başlamıştır. Emniyet bilgilerinden, şirket sırlarına; ticari konulardan, milli istihbarata kadar birçok bilgi bilgisayarlarda bulunmaktadır. Dış dünyaya açık olan bu bilgisayarların ve kullanılan ağların korunması siber güvenlik alanını oluşturmaktadır. Siber güvenlik, teknolojinin gelişmesiyle daha da önem kazanmıştır. Hayatımızı kolaylaştıran teknolojik gelişmelerin insanoğluna sunduğu en önemli alet olan cep telefonları bugün cebimizde taşıdığımız telefon olmaktan çok hayatımızın kumandası durumundadır. Bu çerçevede 2018-2019-2020 yılları arasında internete bağlı olan hat sayılarından kullanım oranındaki durum Tablo 4'de gösterildiği gibidir.

**Tablo 7.** Global Dijital Raporu

| Yıllar | 2018 | 2019 | 2020 |
|---|---|---|---|
| **İnternet Kullanıcısı** | 4.02 milyar | 4.38 milyar. | 4.54 milyar |
| **Sosyal Medya Kullanıcısı** | 3.19 milyar | 3.48 milyar | 3.80 milyar |

**Kaynak:** Global Dijital Raporu, (2020).

Dijital 2020verilerine göre dünyada internet kullanıcısı ve sosyal medya kullanıcısı değerleri incelendiğinde sürekli olarak bu oranların artış eğiliminde olduğu

gözlenmektedir. Dünya nüfusunun 7.634.758.428 kişi olduğu düşünüldüğünde 2018 yılında internet kullanıcısı; dünya nüfusunun %53 iken, 2019 yılında %56'sı ve 2020 yılında yüzde 7 arttığı gözlemlenmektedir. 2018 yılında sosyal medya kullanıcısı, dünya nüfusunun %42'si iken, 2019 yılında dünya nüfusunun %45'i ve 2020 yılında yüzde 9 artmıştır.

Küresel anlamda bu denli internet kullanımın artması ve bu çerçevede internetin kullanım yoğunluğu düşünüldüğünde, internette geçirdiğimiz zaman ve internet aracılığıyla paylaştığımız bilgi miktarı hayal edilmeyecek boyutta olduğunu görmekteyiz. Bilgilerimizin içeriğini korumak ya da internet ortamında olan bilgilerimize gelebilecek her türlü tehdit veya zarardan korunmak önemli bir güvenlik sorunu şeklinde karşımıza çıkmaktadır. Yani teknolojik gelişmelerle kullanımı artan cep telefonu, tablet ve benzeri birçok elektronik alet, sunduğu kolaylıklarla birlikte, birçok güvenlik risklerini de taşımıştır. Siber güvenlik, özellikle son yıllarda çoğalan tehditler karşısında elektronik sistemlerin korunması için; en iyi metotları sunmayı hedefleyen, gelişmekte olan bir alandır (Siber güvenlik nedir). Bu bağlamda eski tedbirleri bırakmak zorunda kalan devletler ve toplumlar kritik bilgi altyapılarını korumak için siber güvenlik alanında çeşitli çalışmalar yapmaktadır.

Siber uzayın yaşamımıza entegre olmasıyla gerçek hayattaki gasp, hırsızlık gibi suçlar sanal ortamda da işlenmeye başlamıştır. Bunun sonucunda güvenlik endişeleri ortaya çıkmıştır. Uzun yıllar boyunca gündeme gelen siber güvenlik kavramı 2009 yılında Amerikan Başkanı Barrack Obama'nın Amerikan halkını siber güvenliğin farkına varılması ve ne gibi önlemler alınması gerektiği gibi konularda eğitimler düzenlemeye davetiyle siber güvenlik konusu popülerliği bir hayli artmıştır (Alp, 2018: 36).

Siber güvenlik; siber uzaydaki güvenlik zafiyetlerinin belirlenerek, kurum, kuruluş ya da devlet tarafından güvenlik risklerine karşı, çeşitli analizler yaparak sistemleri korumak demektir. Bilgi sisteminde işlenen, bilgi transferinde bilginin mahremiyeti ve gizliliğin korunması, verilerin aktarılırken hızının ve kalitesinin korunması, sistemin devamlılığı ve sürekliliğin sağlanması gibi temel amaçlar siber güvenliğin de prensiplerini oluşturmaktadır (Çeliktaş, 2016:19).

Siber güvenlik; bilgi, veri güvenliğinin alt yapıları olan bilgisayar ve bilişim sistemleri güvenliği kavramının internet kullanımının yaygınlaşması sonucu ortaya çıkan yeni kavramsal çevre olarak tanımlanabilir (Güngör, 2015: 19).

Siber Güvenlik, siber alan bilgi ağlarının her çeşit tehdit ve olabilecek saldırıya karşı korunması, siber uzayda işlenen bilgilerin gizliliğini ve erişilebilirliğini kontrol etmek ve emniyete almak, siber güvenlik olaylarını ve siber saldırıları saptama, otomatik kontrol yanıt mekanizmalarını tekrar ön plana koymak anlamına gelir (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı.2013: 9).Bugün, ağ üzerinden yapılabilecek bilgi hırsızlığı, siber saldırı gibi tüm entegre sistemlere zarar verebilecek bir noktaya gelmiştir. Dolayısıyla daha kapsamlı bir kurumsal boyutun yanı sıra siber güvenlik tehditleri siber istihbarat, siber suç gibi toplumsal, ulusal ve uluslararası boyutlara ulaşmıştır. Böylece devletler siber alanı bir egemenlik ögesi olarak değerlendirmeye başlamıştır ve siber güvenlik alanları daha bağımsız bir hale dönüşmüştür (Güngör ve Güney, 2017: 138).

Siber güvenlik çok boyutlu bir kavramdır. Ana özellikleri ise şunlardır(Ada, 2018: 11).

- *Gizliliğin sağlanması:* Bilgi ve verilere sadece yetkili kişilerin veya sistemlerin ulaşabilmesini ifade eder.
- *Bütünlük ilkesi:* Verilerin göndericiden çıktıktan sonra alıcıya ulaşırken herhangi bir değişime uğramaması olarak tanımlanır.
- *Erişebilirlik:* Yetkililerin istediği zaman verilere ulaşabilmesini ifade eder.
- *İzlenebilirlik:* Sistemlerde yapılan işlemlerin daha sonra incelenmek üzere kayıt altına alınmasını ifade eder.
- *Kimlik Doğrulama:* Alıcının, gönderdiği bilginin göndericinin kendini tanıttığı doğru kişi olmasıdır.
- *Güvenilirlik:* Sistemde gerçekleştirilen işlemlerle sonuçların aynı olması olarak tanımlanır.
- *İnkâr Edememe:* Göndericinin ve alıcının mesajları inkâr etmemesidir

Siber güvenliği sağlamak adına bazı hususlara dikkat ederek, siber güvenlik politikası oluştururken dikkat edilmesi gereken bazı hususlar şunlardır (Yılmaz ve Sağıroğlu, 2013: 159):

- Ulusal stratejilerin belirlenmesi ve ulusal politikaların geliştirilmesi
- Yasal çerçevenin belirlenerek oluşturulması ve düzenlenmesi
- Teknik anlamda önlemlerin belirlenmesi
- Kurumsal oluşumun belirlenmesi

- Ulusal işbirliğin sağlanması ve örgütlenmenin oluşturulması
- Yeteneklerin geliştirilmesi ve kapasitenin artırılması
- Farkındalığın artırılması
- Uluslararası işbirliğin oluşturularak, uzlaşmanın sağlanması

Siber güvenlik, global evrende artık, dünyanın temel taşıdır. Bu bağlamda, alt yapısı bilişim ağları olan tüm sistemler üzerinden bağlantı durumundaki tüm dünya, siber güvenlik konusunda uzlaşma sağlamaya çalışmaktadır. Yakın gelecekte yapay zekânın dünya genelinde robotik teknolojilerle gelişmesiyle, cihazların ve aygıtların sayısında eşi görülmemiş veri artışı sayesinde, büyük fırsatlarla birlikte çok büyük güvenlik kaygılarına ve zorluklara da neden olacaktır.

Siber güvenliğin sağlanabilmesi için aşağıda sıralanacak maddeleri bilmek ve uygulamak gerekir (İstanbul Bilgi Üniversitesi Bilgi ve Teknoloji Hukuku Enstitüsü, 2012: 4).

- Siber güvenlik stratejisinin belirlenmesi ve oluşturulması,
- Devletin bünyesinde siber güvenlik yapıların oluşturulması,
- Uyum içerisinde çalışabileceği akıllı bir alt yapının kurulması,
- Siber güvenlik alanındaki hukuki yapının oluşturulması
- Bu sahada çalışacak nitelikli personel ihtiyacının karşılayacak eğitim programlarının verilmesi
- Gelişimleri takip ederek bu alanda AR-GE merkezlerinin kurulması gerekir

Günümüzde siber saldırıların artışı nedeniyle siber güvenlik konusuna daha çok önem verilmektedir, bu bağlamda siber güvenlik çalışmaları artacaktır. Siber güvenlik çalışmalarında bulunması gereken özellikler aşağıdaki gibidir:(Arslan, 2016: 3).

- Siber güvenlik ile ilgili bütün çalışmaların ulusal politika ve stratejileri geliştirilmesi,
- Caydırıcılık faktörünün oluşturulması ve siber tehdit gibi konularda, ulusal mevzuattaki eksiklerin giderilmesi ve yasal çerçevenin oluşturulması,
- Geliştirilecek bütün hukuki düzenlemelere ek olarak teknik tedbirlerin (yazlım, donanım, iş süreçleri) geliştirilmesi,
- Siber güvenliğin başarılı ve bütüncül bir biçimde ilerlemesi için, belirli bir kurum belirlenip, bu kurumun görev ve yetkilerinin yanında diğer kurumlarla, paydaşlarla çalışma şeklinin yasal olarak belirlenmesi,

- Siber güvenliği sağlamak amacıyla ulusal ve uluslararası birimlerin sorumlulukları sağlanması adına koordinasyonun sağlanması
-

| |
|---|
| Engelleme |
| Erken İkaz |
| Müdahale |
| Kriz Yönetim |

**Şekil 3.** Kritik sistem ve bilgi alt yapıların korunmasını amaçlayan ulusal ve uluslararası politikalar

Siber dünyanın yaşamımızla bütün olması siber güvenlik mücadelesinin hem ulusal boyutta hem de uluslararası disiplin ve güvenlik çalışmalarının inceleme konusu şeklinde ele alınmaktadır. Bu bağlamda hiç olmadığı kadar son yıllarda uluslararası platformda siber güvenlik meseleleri ile ilgili yaklaşımların önemi artmaktadır (Çelik, 2018: 117).

Siber saldırıların dünya genelinde artmasıyla siber güvenlik alanına ve siber güvenlik sektöründe çalışanlara olan ihtiyaçta artmaktadır. 2014 yılı içinde 1 milyon boş siber güvenlik personeli pozisyonu varken siber güvenlik sektörünün küresel çapta büyümesiyle 2020 yılında bu oranın 3.5 milyona çıktığı görülmektedir. Ayrıca Microsoft verilerine göre; siber güvenliği sağlamak amacıyla Microsoft yıllık 1 milyar dolar bütçe harcamaktadır. Düzenli olarak her ay e-dolandırıcılık ve kötü amaçlı bilgisayar programlarının tespiti için 470 milyon e-posta incelenirken 1.2 milyar aygıtın güvenliği karşılamaya çalışmaktadır (Thinkteck STM Teknolojik Düşünce Merkezi).

Siber tehdit ve saldırılardan korunmak isteyen ülkeler ve uluslararası kuruluşlar siber güvenlik stratejileri ve politikaları oluşturmaktadır. Siber güvenlik alanında güçlü devletler sıralaması aşağıdaki şekildedir:

**Tablo 8.** Siber Alanda Güçlü Devletler

| Ülke Adı | Genel Güvenlik |
|---|---|
| ABD | 50.24 |
| Çin | 41.47 |
| Birleşik Krallık | 35.57 |
| Rusya | 28.38 |
| Hollanda | 24.18 |
| Fransa | 23.43 |
| Almanya | 22.42 |
| Kanada | 21.50 |
| Japonya | 21.03 |
| Avustralya | 20.04 |

**Kaynak:** Siber Bülten, (2020).

Uluslararası kuruluşlardan NATO, AB, Birleşmiş Milletler kurulduğu yıllardan itibaren kendi üye ülkeleri arasında eşsiz bir bağ oluşturarak NATO ittifak ülkelerini her türlü saldırıya karşı korumaya çalışmıştır ve uğradığı siber saldırılar sonrasında üye ülkelerinin güvenliğini korumak adına çeşitli siber güvenlik politikaları oluşturmuştur.

### 2.5. Uluslararası İlişkiler Açısından Siber Güvenlik

Uluslararası alanda askeri, siyasi, sosyal, ekonomik, eğitim, ticari, yani bütün alanlarda güvenlik kavramı değişerek yerini yeni güvenlik anlayışı ile birlikte ağ üzerinde siber tehdit, siber güvenlik, siber saldırı, bilgi kirliliği, kara propaganda vb. teknolojik kavramlara bırakmaktadır(Yalçın, 2019:8).Siber tehdit ve saldırılardaki artış nedeniyle, birçok ülke bu alanda güvenlik stratejilerine önem vermeye başlamıştır. Özel kurumlar ve bu alan hakkında görüşlerini verdikleri özel BT uzmanlarını yetiştirme ihtiyacı duymaktadır. Bu amaçla, ülkeler bireysel vatandaşların bilgi güvenliğini sağlamak için çeşitli altyapı, kamu bilgi ve dokümanları ve siber güvenlik politikaları oluşturur ve uygular (İstanbul Bilgi Üniversitesi Bilgi ve Teknoloji Hukuku Enstitüsü, 2012: 4).

Uluslararası ilişkilerin temeli olan güvenlik kavramı ve ulusal güvenlik anlayışları özellikle küreselleşmesinin etkisiyle toplumsal değer dizisi ve ulusal savunma stratejileri de değişmiştir. Bilgi toplumu olarak adlandırılan bu dönem, teknolojik zeminli gelişmelerin yaşandığı, ulusal ve uluslararası seviyesinde tehditlerin farklılaştığı ve yeni aktörlerin ortaya çıktığı bilgi zeminli dönemdir. Bu nedenle yeni aktörlere karşı yeni stratejiler oluşturarak, devletlerin savunma mekanizması oluşturması doğaldır (Güngör, Güney, 2017: 143).

Sınır ötesi ve çok uluslu özelliklerine sahip olan siber suçlar, deliller açısından siber sorunu ve suçluları bulma ancak işbirlik ve yardımlaşma ile mümkündür. Bu durumda da birçok ülkenin polis teşkilatlarına, ceza usul yasalarına ihtiyaç vardır. Küresel anlamda siber suçluları bulabilmek için klasik delillerin yerine çoğu dijital olan deliller toplanarak hukuka uygun biçimde hazırlanıp, ilgili ülke ceza usul yasalarının hukuki düzlemde insan haklarını düzenleyen uluslararası bazı sözleşmelere uygun hareket edilir". Bunun sonucunda bir ülkenin topladığı delil, diğer ülkenin mahkemesi tarafından hükme esas alınmak zorunda kalacaktır (Yetim, 2014: 184-185).Uluslararası örgütler ve devletler de bu bağlamda hazırlıklar yapmaktadır ve kendilerini siber savaşa karşı teşkilatlandırmaktadırlar. Uluslararası arenada savaş hukukuna dair uluslararası hukuk politikalarının olası siber savaşta uygulanıp uygulanamayacağı tartışılmaktadır (Yayla, 2013: 191).

Siber güvenliğin devletler arasındaki ilişkiler açısından önemli rol oynadığı konusunda birçok bilgi ve veri vardır. Siber alanının uluslararası ilişkiler çapında görüldüğü ve günümüzde "siber politikalar" ismiyle çalışmaların yapıldığı ve devletlerin güncel çalışmalarında ciddi bir artış görülmektedir. Değişen dünya açısından çıkar mücadelesinin ön planda olduğu, siber güvenlik ve temelindeki araçlarla siber saldırılara karşı, devletler siber saldırının nereden kaynaklı olduğuna dair tespitler yapabilmekte ve bu sorun uluslararası sistemi negatif yönde etkilemektedir. Siber tehditlerin varlığı ve olası siber saldırılar devletleri sıcak çatışmalara sürükleyecek hale gelmiştir (Güntay, 2018: 80-81).

Özellikle 2000'lerden sonra internetin getirdiği kolaylıklarla siber alanın kullanım oranının artması, siber uzayda güvenlik kavramı endişelere neden olmaktadır. Örneğin; 2020'de ABD'de yapılan seçimler için ABD Kongresi, bütçesini 425 milyon dolar artırarak 1.4 trilyona ulaştığını belirtmiştir (Thinktech STM Teknolojik Düşünce Merkezi).

Siber güvenliğin sağlanması ve siber savaşla mücadele, yalnızca devletlerin çabalarıyla mümkün değildir. Devlet ve devlet dışı birçok kurum, kuruluşların küreselleşen dünyada topyekün hareket ettiği görülmektedir. Örneğin, Avrupa Konseyi tarafından imzalanan ve 2004'te yürürlüğe giren Budapeşte Konvansiyonu ilk sözleşme ve bu sözleşmeyi ifade eden Şubat 2005'teki AB'nin 2005/222 / JHA hükmüdür. Hüküm daha sonra Ağustos 2013 tarihinde "Bilgi Sistemlerine Saldırı Yönergesi" olarak değiştirildi. İmzalanan anlaşma aynı zamanda AB için siber sahada yapılan ilk anlaşmadır (Tarhan, 2018: 47).

Birleşmiş Milletler (BM) Bilgi Güvenliği Devlet Uzmanları Grubu'na (GGE) liderlik etmektedir. İstikrar ve siber alandaki anlaşmazlıkların önlenmesi için gerekli adımları belirlemeyi amaçlayan çalışma grubunun, uluslararası normlar oluşturmak temel amaçları arasındadır. Sorumlu devlet davranışlarının ve siber uzayda devletlerin politikalarını sınırlayan norm, kural ve ilkelerin belirlenmesi konusunda bir rapor yayınlar ve o zamandan beri BM faaliyet göstermektedir (Dijital Türkiye, 2017: 14).

Dünyada gerçekleştirilen birçok saldırı sonucunda birçok ülke siber tehditleri dikkate almaya başladı ve uluslararası işbirliğin oluşturulması bu bağlamda hukuksal önlemler alınması gerektiği görüldü. NATO, Avrupa Birliği, Birleşmiş Milletler, Avrupa Konseyi ve bazı uluslararası kuruluşlar güvenlik politikalarını siber tehdit ve siber güvenliği göz onunda bulundurarak oluşturdu böylece aşağıda belirtilen evrensel kurallar oluşturuldu:

### 2.5.1. Bölgesellik Kuralı

Bir ülkenin kendi sınırları içinde olan tüm teknolojik altyapı ve sistemleri ulusal egemenliğin unsurudur. Evrensel hukuk özelliğine göre, her ülke kendi bütünlüğünü bozacak her türlü tehdit ve saldırıya karşı bilgi teknoloji alt yapısını iyileştirme yetkisine sahiptir (Yılmaz ve Sağıroğlu, 2013: 159).

### 2.5.2. Sorumluluk ve İşbirliği Kuralı

Bir ülkeye yapılan siber saldırının kaynağı olan ülkeye konuyu ile alakalı soruşturma yapılması, suçluların bulunması ve yakalanması, yargılama sürecine destek konusunda saldırı yapan ülke yardımcı olmalıdır. Uluslararası siber suçlar hukuk kurallarına göre taraflar elektronik kanıt toplama talep etme yetkisine sahiptir (Yılmaz ve Sağıroğlu, 2013: 159).

### 2.5.3. Öz-Savunma Kuralı

Uluslararası düzeyde gerçekleşen bireysel veya toplu saldırılar da devlet; güvenliğini tehlikede olduğunu düşündüğünde belirli yöntemlerle hatta silahlı güç olarak cevap verebilir. Örneğin; NATO antlaşmasının 5. Maddesinde NATO üyesi olan bir ülkeye yapılan saldırı diğer NATO üyesi ülkelere yapılmış gibi görülerek cevap verme yetkisine sahiptir (Yılmaz ve Sağıroğlu, 2013: 159).

### 2.5.4. Veri Koruma Kuralı

Bireylerin ağ üzerinde kendine ait hesaplarda bulunan bilgilerin, verilerin gizliliği kapsamına girip girmediği hukuk uzmanları arasında hala tartışma konusudur. Ancak "AB Veri Koruma Yönergesine" göre tanımlanmış ya da tanımlanmamış asıl bireylerin verileri kişi verileri olarak kabul edilir (Yılmaz ve Sağıroğlu, 2013: 159).

### 2.5.5. Bakım Kuralı

AB'nin Veri Koruma Yönergesi'ne göre, kişiler ağ üzerinden ya da yasal olmayan yollarla erişime karşı verilerin kasıtlı olarak veya yanlışlıkla yok edilmesini, değiştirilmesini, yetkisiz kişilere açıklanmasını önlemek amacıyla her türlü teknik önlemi almakla sorumludur. Aynı biçimde Avrupa Konseyi Sözleşmesi'nde kişilerin bilgi ve verilerinin her türlü veri kaybı, yetkisiz kişilerin erişimi ve verilerin üçüncü kişilere açıklanması ile değiştirilmesini önlemek için gerekli önlemleri alması zorunluluğu hükmü 7.Maddede açıkça belirtilmiştir. Bu kapsamda siber saldırıların siyasi boyutları arttıkça toplumsal, askeri ve bilgi hizmetleri açısından verilerin bakım ve korunmasına dair standartların geliştirilmesi gerekecektir (Yılmaz ve Sağıroğlu, 2013: 159-160).

### 2.5.6. Erken Uyarı Kuralı

E- servis sorumluları yasa dışı faaliyetleri üye ülkelere bildirmek zorundadır. Bu bağlamda E-servis yöneticileri tedbirleri almakla yükümlüdür ve her türlü eyleme karşı önlemleri koordine etmek zorundadır (Yılmaz ve Sağıroğlu, 2013: 160).

### 2.5.7. Bilgileri Kuralı

Halk yaşam, güvenlik vb konularda bilgi sahibi olmak ister. Günümüzde, toplumsal refah, güvenlik konularında devlet halka karşı daha şeffaf olmaya çalışır. Bu

bağlamda tehditlere karşı alınan kararlar kamuoyu bilgilendirilmeye çalışılır (Yılmaz ve Sağıroğlu, 2013: 160).

### 2.5.8. Suçluluk Kuralı

Her ulus yaygın olan siber suçları kendi ceza hukukuna dâhil etme sorumluluğu vardır. Uluslararası ceza kanuna göre bir durumun sonucu ulusal veya uluslararası yasalara göre bir suç olarak sayılmadığı sürece siber saldırı yapan bireye yönelik bir yaptırım uygulanması mümkün değildir. Bu durumlardaki karışıkların giderilmesi ve bir uyum için esas alınabilecek olan Avrupa Birliği Siber Suçlar Sözleşmesi'ne göre bir bilgisayar sisteminin tamamına ya da herhangi bir bölümüne yasadışı erişimler yasal yükümlülükler çerçevesinde değerlendirilmelidir (Yılmaz ve Sağıroğlu, 2013: 160).

# ÜÇÜNCÜ BÖLÜM

## 3. ULUSLARARASI KURULUŞLAR VE SİBER GÜVENLİK

Ülkelerin siber saldırılara ve olası siber tehditlere karşı tutumu değişmektedir. Bazı ülkeler siber alanı daha az kullanırken, bazıları da kendi çıkarları için sık sık kullanmakta ve yönetmektedir. Siber etkinlikleri fazla kullanan ülkelere baktığımızda, teknolojik anlamda ileri düzeydedirler. Küresel dünyada siber saldırıların kötü niyetli insanlar veya kuruluşlar tarafından gerçekleştirilmesi ve daha büyük devletlerin daha fazla acı çektiği gerçeği, siber alandaki gelişmelerin klasik uluslararası ilişkiler faaliyetlerinde bulunmasını gerektirmiştir. Çünkü siber uzaydaki gelişmeler uluslararası ilişkiler alanında yeni aktörler yaratmış ve yeni güvenlik riskleri oluşturmuştur (Gürkaynak ve İren, 2011: 265).

Uluslararası kuruluşların, belli devletlerin çıkar anlayışları üzerine bir araya geldiği ve belirgin faaliyete geçmesi amacıyla birer vesile olduğu, literatürde sıklıkla yer almaktadır. "Belli devletlerin, belirtilen kuruluşlar çerçevesinde, diğer devletlerin belli davranışlar içine girmelerini gerektiren kural ve maddeleri koyup, üye ülkelerin davranışlarını sınırlandırarak, bu kural ve maddeleri söz konusu devletlerin kendi davranışlarını da belli oranda sınırlandırdığı bilinmektedir. Yani uluslararası örgütlerin sınırlı olsa da belli bir düzenleme ve devlet davranışlarını yönlendirme gücü olduğunu söylemek mümkündür." Sınırlı bir etkiye sahip olan söz konusu kuruluşların, uluslararası sistemi değiştirecek kadar işlevi yoktur. Ancak "uluslararası sosyal bir düzenin belli fonksiyonlar icra edebilecek ve küresel seviyede gelir dağılımındaki büyük uçurumun kapatılmasına katkı sağlayabilecek" özelliklerine sahip olduğunu söyleyebiliriz (Büyükbaş, Ören, 2005: 111).

Ülkelerin ulusal çapta ya da uluslararası kuruluşlarla hazırladıkları siber alandaki çalışmaların ortak hedefi aynıdır. Bu çalışmaların amacı kuruluşa üye devletlerin ortak siber güvenliğini sağlamak, siber riskleri ortadan kaldırmaktır. Bu bağlamda uluslararası örgütler siber güvenlik konusunda birçok çalışma yapmaktadır ve devletler ordularını siber savaşlara karşı örgütlemektedirler. Siber alanda meydana gelen saldırılar, siber savaşlar ve siber güvenlik durumları bazı sonuçlar meydana getirmiştir. Bu sonuçlar aşağıdaki gibidir(Yayla, 2013: 191-192).

Siber uzayda gerçekleşen olaylar gösteriyor ki siber savaş durumu gerçektir. ABD, Rusya gibi güçlü ülkeler siber güçlerini kullanıp siber savaş açması durumunda bir ulusun yok olabileceği tahmin edilmektedir. Siber saldırının yapılma zamanıyla, etkisi aynı anda görülmektedir. Bu durum saldırıya uğrayan devleti, kriz yönetimi açısından zora sokmaktadır. Siber uzayın karmaşık olması ve kullanılan yöntemlerin çok fazla olması, herhangi bir siber anlaşmazlık durumunda anlaşmazlığın küresel bir hal alacağı ve birçok ülkeyi savaşa çekeceği görülmektedir (Yayla, 2013: 191-192).

Uluslararası kuruluşların işbirliğini sağlaması amacıyla oluşturacağı stratejilerin özellikleri şu şekilde olmalıdır (Aytekin, 2015: 60):

- Stratejiler uluslararası eşgüdümü teşvik etmeli ve desteklemelidir,
- Oluşturulan stratejiler koordinasyonu özendirmelidir,
- Ulusal kurum ve kuruluşlara uluslararası işbirliğini destekleyecek programlar verilmelidir,
- Bilgi güvenliği, bilgi ve istihbarat bölüşümü gibi mevzularda uluslararası kuruluş ve yetkin merkez işbirliği sağlamalıdır,
- Uluslararası antlaşmalara katılım sağlanarak desteklenmelidir.

Siber sorunlar daha önce hiç olmadığı kadar, günümüzde sorun hale gelmeye başlamaktadır. Bu durum etkin bir yargısal yardımlaşmayı gerekli kılmaktadır. Bu durum uluslararası işbirliğine ihtiyaç olduğunu göstermektedir. Bu bakımdan, geleneksel adli yardımlaşma sistemlerinin siber tehdit ve suçlarla mücadelede, eksik kaldığı konusuna dair şüphe yoktur. Siber suçlar mücadele ve siber güvenlik konularında, NATO, Avrupa Birliği, Avrupa Konseyi, Birleşmiş Milletler gibi uluslararası örgütler gözetiminde veya kuruluşların desteği ya da katılımıyla devam eden sayısız teşebbüs mevcuttur (Önok, 2013: 1238-1239).

Siber tehditlerin varlığı ve olası siber saldırılar devletleri sıcak çatışmalara sürükleyecek hale gelmiştir (Güntay, 2018: 80-81).

Siber saldırıları engellemek için küresel bir işbirliğine ihtiyaç olduğu bilinmesinde yarar vardır. Bu alanda çok az uluslararası antlaşmalar imzalanabilmiştir. Sadece birkaç kuruluş siber saldırılarla mücadele etmeyi hedeflemiştir. Bazı Avrupa ülkelerine karşı düzenlenen siber saldırılar AB, BM, NATO, Avrupa Konseyi gibi uluslararası kuruluşları harekete geçirmiş ve siber saldırılara karşı birlikte hareket etmenin gerekliliği bir kez daha ortaya koymuştur (Gürkaynak ve İren, 2011: 275).

Siber güvenlik konusunda hukuki değerlendirmeler ve hükümler uluslararası kuruluşlar tarafından kabul görmektedir. BM, siber güvenlik konusunda anlaşmaların devletlerarasında olması nedeniyle suç failinin de "devlet olması ilgili fiilin kuvvet kullanımı ya da kuvvet kullanımı tehdidi olarak değerlendirilmesi gerekmektedir." Böylece, BM koşulu, siber saldırıların direkt kuvvet kullanımıyla birlikte, siber tehdit içerikli fiili müdahaleye varmayan durumları da yasaklamıştır. Siber güvenliği korumak adına devletlerin siber ordu kurduğu bilinen bir gerçektir. Siber orduda görev alan ajanlar ve çalışanlar devlet tarafından gizli tutulmaktadır. Bahsi geçen gizlilik, "devletin uluslararası hukuktan kaynaklanan yükümlülüklerine teknik olarak halel getirmeyeceğini, BM tarafından teamül hukukunun kodifiye edilmesiyle oluşturulan sorumluluğa ilişkin anlaşma taslağının 5. maddesi açık şekilde belirtilmiştir (Uluslararası Hukuk Komisyonu, 2001). İlgili maddede, devlet organı olmayan fakat kamu gücünü kullanarak haksız fiilleri işleyen kişi veya kişilerin yaptığı eylemlerin devlete isnat ettirilebileceği açıkça yer almıştır (Güreşci, 2019: 84-85).

NATO tarafından siber kavramlar olan; siber saldırı, siber savaş ile ilgili kavramları tanımlamak ve anlatmak üzere 2013 yılında Tallinn El Kitabı hazırlanmıştır. Siber güvenliği hukuki boyutlara tartışmak amacıyla, NATO'nun kurduğu "Ortak Siber Savunma Mükemmeliyet Merkezi" kurulmuştur. Uzmanlar grubun emeklerinin göstergesi olan El Kitabı'nın iki yorumunda da siber faaliyetlerle ilgili hukuk kuralları incelenmiş; siber çalışmalar için ve siber güvenlik adına uygulanabilecek ilkeler mevcut uluslararası kurallar ışığında hazırlanmıştır. Ayrıca uluslararası güvenlik ve siber faaliyetlerin ele alındığı El Kitabı'nın bölümünde yer alan ilkeler, uluslararası hukukta düzenlenen kuvvet kullanma, meşru müdafaa hakkı ve kolektif güvenlik sistemine ilişkin kuralların rehberliğinde hazırlanmıştır (Şafak, 2020: 146).

## 3.1. NATO

### 3.1.1. NATO Hakkında

Geniş alanları kontrolü altına almanın çabası içinde olan Sovyetler, 1940-1945 yılları arasında Avrupa'da yaklaşık 450.000 Km. alanı ve 24 milyon nüfusu sınırlarına almıştır. 1945-1948 yılları arasında 1 milyon Km. toprak ve 92 milyon nüfusu da himayesine almayı başaran Sovyet Birliğini, Amerika durdurmak için gerekli tedbirler almıştır. Bu tedbirlerin en büyüğü ve en etkilisi '4 Nisan 1949'da kurulan ABD ve 12 Batılı ülke arasında imzalanan kısaca NATO denilen Kuzey Atlantik Paktı'dır. NATO, Sovyet birliğine karşı kurulan askeri ittifaktır. Antlaşmanın ilk başlığında NATO ülkelerinin "demokrasi ilkeleri ile kişi hürriyetleri ve hukuk üstünlüğüne dayanan özgürlüklerini ve ortak savunmaları ile barış ve güvenliklerini korumak" amacıyla bir araya geldikleri belirtiliyordu. NATO ülkelerinden birine yapılan bir saldırı diğer ittifak ülkelerine yapılmış sayılacaktı(Armaoglu, 1989: 229-230). NATO zaman içerisinde üye sayısını ve etki alanını genişletmiştir. Günümüzde NATO'nun 29 üyesi bulunmaktadır. Yıllara göre NATO üyesi olan ülkeler ve üye oluş tarihleri Tablo 5'de gösterilmiştir.

**Tablo 9.** Yıllara göre NATO üyesi olan ülkeler ve üye oluş tarihleri (NATO, 2017).

| | | |
|---|---|---|
| Fransa (1949) | Lüksemburg (1949) | Bulgaristan (2004) |
| Belçika (1949) | Norveç (1949) | Estonya (2004) |
| BirleşikDevletleri (1949) | Türkiye (1952) | Letonya (2004) |
| Birleşik Krallık (1949) | Yunanistan (1952) | Litvanya (2004) |
| Danimarka (1949) | Almanya (1955) | Romanya (2004) |
| Hollanda (1949) | İspanya (1982) | Slovakya (2004) |
| İzlanda (1949) | Polonya (1999) | Arnavutluk (2009) |
| İtalya (1949) | Macaristan (1999) | Hırvatistan (2009) |
| Kanada (1949) | Çek Cumhuriyeti (1999) | Karadağ (2017) |
| Portekiz (1949) | Slovenya (2004) | Kuzey Makedonya (2020) |

NATO ilk kurulduğu zamanlarda, geleneksel ittifaklardan ayrı bir özellik göstermiyordu. Bu anlayış Haziran 1950'de Kuzey Kore'nin Güney Kore'ye karşı belirgin tehdidini artmasıyla değişti. Kore saldırısının ardından Batı Avrupa'ya da yönebileceğini düşünen üyeler; ortak genel bir harekât planı hazırlamaya başladılar. Bu andan itibaren NATO geleneksel ittifaklardan uzaklaşarak askeri bir ittifak haline gelmiş oldu. Çin'de komünistlerin başarıya ulaşmaları ve 1949 yılında Sovyetlerin

atom bombası patlatarak bu güçlü silahın ABD'nin tekelinde olamayacağını göstermesi de NATO'daki bu geçişi etkileyen diğer önemli unsurlardır (Sarınay, 1988: 76).

1960 sonlarına kadar SSCB ve ABD arasında uzun yıllar süren nükleer silahlarda ve gönderme araçlarında yarış olmuştur. Bu durumların yaşanmasıyla ekonomilerine getirilen yükler sonucunda 1970'lerin başında kutuplar arası yumuşama dönemine girilmiştir. Yaşanan barışçıl ortam sonucunda silahsızlanma görüşmeleri de yapılmaya başlanmıştır (Gürkaynak, 2005: 9).

NATO İttifakı temel hedefi olan güvenlik görevini yerine getirmek için aşağıda belirtilen belli başlı maddeleri yapmaya çalışır.

- NATO, siyasi ve askeri yollarla mükelleflerini korur. Ayrıca, savunma reformları, barışı koruma gibi konularda NATO üyesi olmayan ülkelerle işbirlik çağrısı yapar.
- NATO, üye ülkelerinin topraklarındaki ve topraklarının dışındaki çatışmaları engellemeye çalışır.
- NATO, çıkan anlaşmazlıkları barışçıl yollarla çözülmesini sağlar, barışçıl çabalar sonuç vermediğinde tek başına veya uluslararası örgütlerle işbirliği içine girer.
- NATO, üyelerinin doğal afetlerle mücadelesinde yardım eder ayrıca bilim ve çevre konularında işbirliğine teşvik edecek faaliyetlerde bulunur (NATO, Otan).

NATO üye ülkeleri, görevlerini yerine getirmek amacıyla siyasi, ekonomik ve askeri olmayan alanlarda da sürekli danışmanlık ve işbirliği sağlamaktadır. Bu faaliyetler, idari işler, bütçeleme ve planlama personelidir. Bunlara ek olarak uzmanlaşma gerektiren sahalardaki çalışmaların eşgüdümlenmesi maksadıyla, NATO üyesi ülkeler aracılığıyla kurulan ajansları da içinde bulunduran karmaşık bir sivil ve askeri yapı sayesinde olmaktadır. Uzmanlaşmaya gidilmiş söz konusu sahalara, askeri kuvvetlerin komuta ve kontrolünü, siyasi danışmanlığı ve kuvvetlerin devamını sağlamak amacıyla gerekli lojistik desteğin muhafazasını kolaylaştıran bir iletişim sistemi örnek olarak verilebilir (Ortaklık ve İş Birliği, 1995: 19).

NATO, demokrasiler ittifakıdır ve üyesi olan tüm ülkelerin parlamentoları NATO ülkelerinin halkı ile NATO liderleri arasındaki en önemli iletişim kanalıdır. NATO'nun aldığı tüm kararlar üye ülkeler arasında tartışma ve istişare sonrasında, oy

birliği sonucunda alınmaktadır (Ada, 2018:28).

### 3.1.2. NATO'nun Siber Güvenlik Stratejileri

Soğuk savaş sonrası İttifak'ın birliğini hedef alan yeni tehditler daha karmaşık bir hal almıştır. Özellikle son yıllarda meydana gelen siber tehditler İttifak'ın "havada, karada, denizde hangi biçimde çalışıyorsak, siber alanda da aynı biçimde çalışmalıyız" vizyonunu oluşturmasına neden olmuştur (NATO'nun siber uzaydaki rolü). NATO bu kapsamda siber uzayı dördüncü çalışma alanı hatta savaş sahası olarak görmüştür. 2011 yılında NATO, "merkezileştirilmiş siber savunma ihtiyaçlarının karşılandığı bir politika" ortaya koymuştur. 2012'de NATO tarafından 58 Milyon Avroluk bir kontrat imzalanmıştır. Amaç:

- ✓ "Bilgisayar Olayları Karşılama Kapasitesinin (NATO Cyber Incident Response Capability/NCIRC) yıl sonunda bütüncül olarak fonksiyonel duruma getirmeye çalışmaktır (Polat, 2020: 148).
- ✓ İttifak çalışmalarını artırarak 2016 yılında "Siber Savunma Sözleşmesini" imzalamıştır. NATO siber güvenliği sağlamak adına onayladığı sözleşmeyle, üye ülkelerin uygulama konusunda takibini gerçekleştirmektedir (Yenal, Akdemir, 2020:425).

NATO ittifakı da soğuk savaşların bitmesiyle birlikte hibrit savaşın parçası olarak görülen siber saldırılardan ciddi boyutta etkilenmiş ve çok çeşitli saldırılara uğramıştır. Bu saldırıların sonrasında da çeşitli stratejiler üretmiştir. NATO siber saldırılara karşı korunmak için son yirmi yıl içerisinde çeşitli yöntemler ve stratejiler oluşturmuştur. NATO'nun çalışmalar yaparak siber güvenlik konusunda ortak stratejiler oluşturmasına neden olan üç büyük siber savaş meydana gelmiştir.

### 3.1.3. NATO'nun Dâhil Olduğu Siber Kriz Örnekleri

NATO'nun siber güvenlik stratejileri oluşturmasında internetin gelişmesi ve yaygın kullanımıyla beraber artan siber tehditler ve saldırılar neden olmuştur. Bu bağlamda uluslararası güvenlik alanında siber güvenliğe dair çalışmalar yapılarak siber alan artık askeri güvenlik alanı olarak algılanmaya başlanmıştır. Özellikle; Kosova saldırısı, Estonya'ya yönelik siber saldırılar sonrası ve Gürcistan krizi gibi önemli üç saldırı NATO'nun siber güvenlik alanında; askeri bir uzlaşma sağlanmasına yönelik, uluslararası sahada strateji oluşturmasında ana nedenler olmuştur (Arı ve

Özdal, 2015: 411). Bu çerçevede NATO siber tehdit durumda siber savunma politikasıyla erken önlem almayı amaçlamaktadır

#### 3.1.3.1. NATO-Kosova Krizi (1999)

Yugoslav ordularının Kosova'dan çekilmemesi üzerine başlayan mücadele, NATO'nun krize dâhil olarak, 13 NATO üyesi Yugoslavya'yı vurmaya başlamıştır. Ayrıca, NATO uçaklarının vurma yetkisi NATO Genel Sekterinde olduğu belirtilmiştir. Bunun üzerine NATO, Yugoslavya'nın askeri gücü olan birçok tank ve topu hedef alarak, etkisiz bırakmıştır (Oduncu, 2019: 10).

Kosova krizi çıkmaz bir hal almışken, NATO savaş uçakları yanlışlıkla Çin elçiliğine çarpmıştır ve "Çin Kırmızı Hacker İttifakı"da karşılık vererek NATO ve ABD askeri web sitelerine saldırdı. Saldırıyla, NATO'nun özellikle resmi web sitelerinin sıkça kesintiye uğradığını ve NATO üye devletlerinin e-posta hesaplarının günlerce kapalı olduğunu tespit etti. Bu olay dünya tarihindeki ilk siber savaş olarak tanımlanmaktadır. NATO bu olaydan sonra siber güvenlik alanında ilk adımı attı. NATO ittifakı, Kosova Savaşı'nda hedefine varmış gibi anlaşılsada, savaş sırasında web sitelerinin ele geçirilmesi NATO'nun siber saldırılar karşısında yetersiz kaldığını göstermiştir. NATO ülkelerinin e-postalarına gönderilen mesajlar, saldırganların kim olduğunu ve neden yaptıklarını açıkça göstermektedir. Siber saldırı NATO'yu yeni bir stratejik önemli belge hazırlamaya zorlamıştır (Ada ve Çakır 2017: 638). Kosova krizinden sonra çıkarılan resmi NATO belgelerinin hemen hepsi siber güvenlik ve "bilgi sistemlerinin korunması" konularını içeriyordu, ancak bilgi sistemlerinin nasıl korunacağı, nasıl güvence altına alınacağı ve neyin güvenli olacağı gibi sorulara cevap vermediler. Bu belgelerde siber tehditlere nadiren değinilmiş olmasına rağmen, NATO'nun siber güvenlik konusundaki ilk basamağı bu şekilde oluşturulmuştur (Bıçakçı, 2012: 212).

Yapılan incelemelerde Çin'in Kosova Kriziyle ABD'nin ve NATO'nun web siteleri saldırması dünyada ilk siber saldırı olarak görülmüştür

### 3.1.3.2. Estonya Siber Savaşı (2007)

Estonya soğuk savaş döneminde Sovyetler Birliğinin bilişim merkezi olmuştur. Soğuk savaşın sona ermesiyle Estonya bağımsızlık kazanarak ayrı bir devlet olmuştur. Bunun üzerine Rusya Estonya'yla birlikteliğini güçlü tutmak istemiştir. Ancak 2002 yılında Prag zirvesiyle başlayan Estonya'nın NATO ya üye olma işlemleri 2004 yılında kabul edilmesiyle Rusya ile olan ilişkisini oldukça zayıflatmıştır. 2007 yılında ise Rusya ile Estonya arasındaki ilişkiler bitme noktasına gelmiştir (Yalçın, 2019: 61-62).

Nisan ve Mayıs 2007'de, Rusya Estonya'nın savunma sistemini felç eden kamu ve özel kuruluşların, özellikle devlet kurumlarının, bankaların ve medyaların web sitelerine büyük çapta siber saldırılar NATO'nun siber saldırılar tarafından yarattığı tehdit algısını tamamen değiştirdi. Bir başka deyişle, İttifak siber saldırıları "21. yüzyılda öncelik verilmesi gereken ekonomik, siyasal ve BT alanlarda güvenliğine hasar verebilecek bir problem olarak tanımlamıştır. Saldırıdan sonraki yıl yapılan 2008 Bükreş Zirvesi'nde, NATO' üyesi devletlerin siber saldırılara karşı mevcut kapasitelerinin büyütülmesi ve bu bağlamda savaş politikalarının oluşturulması ihtiyacı bir kere daha etkili bir biçimde onaylandı. Bu çerçevede "NATO, onayladığı siber savunma politikası kapsamında Sanal Savunma Yönetim Otoritesini" (CDMA) ve "Estonya merkezli Merkez Siber Savunma Mükemmeliyet Merkezini (CCD COE)" kurmuştur (Seren, 2016: 16-17).

Estonya krizinin ardından birçok siber saldırıya uğrayan NATO güçlü stratejiler oluşturularak siber güvenlik adına pek çok çalışma yapmıştır.

### 3.1.3.3. Gürcistan Siber Savaşı (2008)

Estonya'ya yapılan saldırıdan bir yıl kadar sonra Gürcistan devletine karşı siber saldırı düzenlendi. Saldırı hem Rusya hem de birçok ülke tarafından gerçekleştirildi.

Gürcistan'ın ayrılıkçı grubun provokasyonuna tepki verdiği Gürcistan güçlerinin 7 Ağustos 2008'de gerçekleşen olayların hızla artması, akşam saatlerinde Gürcistan'a siber saldırılarla sıcak bir çatışmaya dönüştü. Gürcistan'ın bilgi altyapısının Estonya kadar gelişmiş olmaması, saldırının yol açtığı zararın etkisini azalttığı, ancak olayların gelişmesi ve saldırı sırasında izlenen yöntemlerin Estonya'dakilerle neredeyse aynı olduğu görüldü (Bıçakcı, 2014: 101-130).

Gürcistan'a yapılan siber saldırıların en etkili sonucu mevcut bir melez savaş olmasıdır. Klasik savaş tarzlarını kullanarak, Rusya aynı anda siber saldırıları başlattı.

Bu savaşı, Rusya'nın karma savaşı olarak tanımlayabiliriz. Bu savaş NATO'nun melez savaşa olan inancını güçlendirdi (Bıçakçı, 2012: 205-226).

Gürcistan'daki siber saldırıların ardından Kasım 2008'de NATO Ortak "Siber Savunma Mükemmeliyet Merkezi (CCDCOE), Gürcistan'a Karşı Siber Saldırılar: Belirlenmiş Hukuki Dersler" başlıklı önemli açıklama yaptı. Rapor, Silahlı Çatışma Kanunu'nun SOO'nun Rusya-Gürcü Savaşı sırasındaki siber saldırılara karşı uygulanabilirliği hakkında fikir vermektedir (Ada ve Çakır, 2017: 639).

### 3.1.4. NATO Üyesi Ülkelerin Siber Güvenlik Çalışmaları

Bugün dünyadaki en önemli uluslararası kuruluşlardan biri olan Kuzey Atlantik Antlaşması Örgütü 30 ülkeyi bir araya getirir. NATO üye ülkelerine baktığımızda siber güvenlik alanına en çok önem veren devletlerin ABD ve Almanya olduğunu görmekteyiz. Çalışmanın bu bölümünde NATO üye ülkelerinden; ABD'nin Almanya'nın, Estonya'nın, Birleşik Krallık'ın, Kanada'nın, Fransa'nın ve Türkiye'nin siber güvenlik faaliyetleri kısaca incelenmiştir.

#### 3.1.4.1. ABD

ABD, siber güvenlik, siber uzay konularında diğer ülkelere önder konumundadır. Özellikle Avrupa ve Asya'daki ülkelere siber sorunlarla mücadele konusunda örnek olarak bir rol model durumuna gelmiştir.

Ulusal siber güvenlik stratejilerine 2001 yılında yaşanan olayların ardından 2003 yılında ABD Başkanı George Bush zamanında "Ulusal Siber Uzay Güvenliğini Sağlama Stratejisi" çıkarılmıştır. Stratejide; kamu-özel sektör işbirliğinin önemi belirtilerek, federal hükümet birimlerine yol gösterilmektedir. Ayrıca; siber uzayda var olan tüm aktörlere, siber güvenliği sağlama ve siber güvenliğin geliştirilmesi amacıyla oluşturulabilecek yöntemler ile ilgili bilgi verilmektedir (Aytekin, 2015: 85).

11 Eylül 2001'deki ABD'deki saldırıların ardından siber güvenlik ve kritik bilgi altyapılarının korunması alanlarında çeşitli değişiklikler yapıldı. Siber güvenliğin sağlanması için DHS bünyesinde Altyapı Koruması "(OIP) ve Siber Güvenlik ve İletişim Departmanı (CS&C) kurulmuştur." OIP, bazı mevcut altyapıların korunması konusundaki çalışmalarını koordine etmekten, mevcut altyapı sektörlerindeki güvenlik açığı değerlendirmesine yönelik çalışmaları desteklemekten ve uluslararası güvenlik kültürünün oluşturulmasını teşvik eden uluslararası programlar ve ilişkiler kurmak ve

sürdürmekten sorumludur. Kritik altyapıların korunması öte yandan CS&C, siber tehditler, risk yönetimi, acil durumlarda iletişim ve müdahale merkezlerinin kurulması gibi konularda özel sektör ile işbirliği kurmaya yetkilidir (Turhan, 2010: 103).

ABD, siber alanda Çin, Rusya ve İran gibi siber alanda kendini kanıtlamış güçlere karşı kendini savunmaya çalışmaktadır. 2012'de "ABD savunma stratejisi ile birlikte yayınlanan, savunma stratejisinin ana merkezine Çin'i oturtmuş böylece, ABD-Çin mücadelesini farklı bir boyuta taşımıştır." Bu çerçevede, siber uzay ilk kez bir çatışma sahası olarak görülmüştür (Korhan, 2018:46).

#### 3.1.4.2. Almanya

Almanya'nın İkinci Dünya Savaşında kullandığı şifre kırma makinesi olan Enigma, dönemin şartlarına bakıldığında makinenin, kırılması oldukça zor bir şifreleme algoritmasına sahip olduğu, Almanya devletinin bilgi güvenliği konusundaki çalışmalarına, İkinci Dünya Savaşı dönemine dayandığı kabul edilmektedir (Güngör, 2015: 26).

Almanya ikinci dünya savaşından sonra, özellikle dış politika anlayışında fazla değişime uğramamıştır. Kendi vatandaşlarının iç huzur ve güvenliğine önem vererek, iç politikada güvenlik politika çalışmalarına yönelmiştir (Kıratlı, 2016: 213). Fakat son yıllarda Almanya'nın dış politika anlayışı yapısal değişime uğrayarak, daha müdahaleci ve dışa açık bir rol üstlenmiştir. Bunun sonucunda da kendi ulusal güvenliğine gelebilecek dış tehditler olan siber tehdit, savaş ve terör gibi uluslararası tehdit ve problemler de artmıştır (Göçoğlu, 2018:145).

Almanya siber güvenlik yarışına ABD'den sonra başlamıştır. 2011 yılında ilk ulusal siber güvenlik stratejisini oluşturarako yıldan sonra büyük ve hızlı bir gelişme göstermiştir. Almanya, 2015 yılında stratejisini yenileyerek yolculuğunu sürdürdü. Stratejilerinde, Almanya kritik bilgi sistemi altyapılarının korunmasına önem vermektedir. Ek olarak, İnternetin her geçen gün artmasıyla, sadece her ülkenin kendi sistemlerinde değil; Diğer ülkelerin sistemlerindeki saldırılardan etkilenebilecek küresel bir dünya olduğundan, siber güvenlik ve siber savunma mekanizmalarının uluslararası düzeyde önemi vurgulamaktadır. Ayrıca, Almanya bir düzenlemenin yasa ile yapılması gerektiğini de belirtmektedir. Hem Birleşmiş Milletler, NATO, Avrupa Konseyi, Avrupa Birliği ve diğer uluslararası kuruluşların beraber çalışması ve faaliyette bulunması ihtiyacını vurgulamaktadır. Almanya'daki kritik altyapıların siber uzayda

meydana gelebilecek tehditlerden korunmasından ve bu konudaki çalışmaların koordinasyonundan yükümlü olan Federal Bilgi Güvenliği Ofisi (BSI), 2011 yılında hazırlanan stratejik planın ardından BSI'nin yetkisini arttırmıştır. Ancak günümüzde siber güvenlik çalışmalarında ABD tarafından yayınlanan siber konulu askeri yordamlarına bağlı kalmaya devam etmektedir (Sanalp, 2016: 28, 30).

#### 3.1.4.3. Estonya

Estonya'ya 2007 yılında yapılan siber saldırılar, siber kabiliyetler ve stratejiler açısından Estonya Hükümetinin ciddi bir biçimde incelemesine sebep oldu. Olaylar sonucunda ülkedeki siber savunma faaliyetleri "Savunma Bakanlığı" nezaretinde yürütülmektedir. Ayrıca, Estonya'daki Savunma Birliği adlı bir kuruluş ülkenin siber savunma kuvvetlerini iyileştirmek için çalışmaktadır. Savunma Birliğinin bir parçası olan Siber Güvenlik İttifakı, görevlerini üç ana başlık altında yerine getirmekle sorumludur. Bu görevler;

- Estonyalıların elektronik hayatlarını korumak,
- BT uzmanlarının eğitimi,
- Siber Savunma ile ilgili kamuoyu bilgilendirme faaliyetlerinde bulunmak

Şeklinde sıralanabilir. Bir NATO üyesi olan Estonya, NATO altındaki Bilgi Güvenliği alanında uluslararası işbirliğinin önemini bilen ve bu amaçla aktif bir rol oynayan ülkelerden biri. Bu işbirliğiyle savunma yetkinliğini arttırmanın yanı sıra NATO üyesi ülkelere de katkı sağlamaktadır. 2008 yılında Tallinn'de bir NATO kuruluşu olarak kurulan Siber Savunma Mükemmeliyet Merkezi, üye ülkeler arasındaki işbirliğini artırmak, bilgi paylaşmak ve siber güvenlik sahasında araştırma yapmak için harekete geçmektedir (İstanbul Bilgi Üniversitesi Bilgi ve Teknoloji Hukuku, 2012: 22, 23).

#### 3.1.4.4. Birleşik Krallık

İngiltere Hükümeti, İngiltere halkının siber uzayın sunduğu hizmetleri kullandığı ve siber uzayın sunduğu hizmetlere muhtaç olduğunu belirtmektedir. 2009 Haziran ayında Hükümet tarafından yayınlanan raporda "İngiltere'nin, dünyanın önde gelen dijital bilgi ekonomilerinden biri olma durumunun devamını sağlama" hedefine ulaşmanın gereği olarak bu rapor yayınlanmıştır. Doküman, İngiltere Devletinin siber uzayın sağladığı olanaklardan faydalanmak amacıyla neler yapacağını, siber uzayın

güvenliğini ve karşı koyabilme gücünü sağlamak için yapacağı çalışmaları bildirmektedir (Aytekin, 2015: 71).

Ekim 2010'da, İngiltere hükümeti Ulusal Güvenlik Strateji Raporunu meclise sundu ve yayınladı. Bu rapor, Birleşik Krallık'ın oluşabilecek tehditleri bölümlere ayırarak, siber saldırıları en güçlü tehdit grubu olarak kabul etmiştir. Raporda ayrıca siber saldırı alanındaki diğer ülkelerin siber saldırıları ve terörist grupların ve örgütlü ağların yönlendirdiği siber saldırıların da yapıldı. Ulusal Güvenlik Strateji Raporu, birçok ülkenin Birleşik Krallık'a siber alanda saldırılar gerçekleştirdiğini açıkça göstermektedir. Siber güvenlik konusunun, "rapor yılı boyunca takip eden beş yıl sürecince en yüksek kademeli ulusal güvenlik tehditlerinden" biri olarak görülmesi gerektiğini vurgulamaktadır (İstanbul Bilgi Üniversitesi Bilgi Teknolojisi ve Hukuk Enstitüsü, 2012: 30).

#### 3.1.4.5. Kanada

Kanada Hükümeti her alanda siber güvenliğin sağlanması amacıyla özel sektör, kamu kuruluşları ve uluslararası ortaklarla işbirliği yapmaktadır. Hükümet; siber güvenlik alanında bilgiler elde ederek, vatandaşların internet ortamında güvenliğini korumak amacıyla Siber Güvenlik Programı (Get Cyber Safe) yürütmektedir (Kama Güvenliği Kanada, 2020).

Siber güvenliğin sağlanması ve siber olaylarla mücadelede ulusal ve uluslararası mevzularda liderlik görevi üstlenen Kanada Siber Olaylara Müdahale Merkezidir (CCIRC).

CCIRC, 'nin birinci önceliği aralıksız olarak, herhangi bir tehdit, saldırı ya da tehlike olup olmadığını incelemektir. Bir tehlike veya olay olması durumunda ise ciddi tepki vererek; olaylara müdahale etmektedir. Ayrıca Kanada Hükümeti, 'nin kritik altyapı sektörlerine olaylara müdahale, koordinasyon ve destek sağlama, izleme ve siber güvenlik tehditleri analiz etme; bilgi teknolojileri alanlarında danışmanlık sağlama ve farkındalığın artırılması ile ilgili eğitim faaliyetleri yürütmektedir(Turhan, 2010:114-115).

#### 3.1.4.6. Türkiye

Günümüzde internet sadece iletişim ağı olarak görülmemektedir. Su, elektrik, sağlık gibi doğal gereksinimlerin karşılanmasında görev yapan güçlü bir aktör

durumuna gelmiştir. Örneğin, “SCADA yazılımlar vasıtasıyla elektrik şebekeleri kontrol edilmektedir.” Türkiye’de birçok ülkede olduğu gibi internet birçok hizmetin verildiği bir sistem haline gelmiştir. Bilişim alanının, hızlı gelişmesi, siber güvenlik kavramının hukuki alanda da çalışmalar yapılmasına neden olmuştur (Sarı, 2013: 65). Ancak; Türkiye'nin siber güvenlik stratejisi çalışma tarihi oldukça yenidir. Siber güvenlik açısından öne çıkan en önemli çalışmalardan biri, siber güvenlik alanı düzenleyen birtakım yasaların onaylanmasıdır. “2004 yılında kabul edilen 5070 sayılı Elektronik İmza Kanunu ile2008 yılında iletişim sektörünü düzenlemek üzere kabul edilen Elektronik İletişim Güvenliği Yönetmeliği bunlardan ilkidir.” Ayrıca, “Yüksek Planlama Kurulu kararında” yer alan “Bilgi Toplumu”. 2006/38, 2006’da 28242 sayılı “Resmi Gazete'de” yayımlanmıştır (Hekim ve Başıbüyük, 2013: 154-155).

Türkiye siber güvenlik politikalarını daha çok siber suçlar üzerinden değerlendirmektedir. Ayrıca kritik alt yapıların güvenliği üzerine odaklaşarak AB uyum sürecince birçok politikalarında ABD ve AB’nin izlerine taşımaktadır. Türkiye’nin siber suçları önleme çalışmaları ABD’nin “karşı istihbarat” adlı yapının inceleme ve araştırmaya olanak sağlayan yapılanmasıyla paralellik göstermektedir (Ünal, 2016: 427).

Bunlardan ilki, bilgi güvenliği için yasal düzenlemeler; ikincisi, bilgisayar etkinlikleri ve kamu kurumlarının bilgi güvenliğini sağlamaya yönelik faaliyetler için acil bir müdahale merkezi kurulmasını planlamaktadır. Bu kapsamda, “Bilgisayar Olayları Müdahale Ekibi (TR-BOME), TÜBİTAK Bilgi ve Bilgi Güvenliği İleri Teknolojileri Araştırma Merkezi (BİLGEM)” kuruldu. Siber güvenlik konusunda en somut adım, “Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetimi ve Koordinasyonu Karar Kararı olan 2012/3842 Bakanlar Kurulu Kararı ile gerçekleştirildi.” En çok ses getiren kararı "siber güvenlikle ilgili kararları belirlemek, 155 Siber Suç ve Türkiye'nin Siber Güvenlik Politikası planlarını, programlarını, raporlarını hazırlamak, ilkeleri ve standartları onaylamak ve uygulamalarını ve koordinasyonlarını sağlamak için" Siber Güvenlik Konseyi kuruldu. “Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Dışişleri Bakanlığı Müsteşarlığı, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme Müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarlığı, Ulusal İstihbarat Teşkilatı Müsteşarlığı, Baş Genelkurmay Başkanlığı, Haberleşme Elektronik ve Bilişim Sistemleri Müdürü, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

(TÜBİTAK) Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ve Ulaştırma, Denizcilik ve Haberleşme Bakanı tarafından atanacak bakanlıkların ve kamu kurumlarının üst düzey yöneticileri ülkenin siber sorunlardan korunarak siber güvenliğin sağlanması amacıyla strateji, politik ve eylem planları hazırlama görevinin Ulaştırma Bakanlığına verildiği belirtildi." Böylece Ulaştırma Bakanlığı, mensup birlik ve yapıların görüşlerini alarak bir siber güvenlik eylem planı oluşturmuştur (Hekim ve Başıbüyük, 2013: 154-155).

#### 3.1.4.7. Fransa

Fransa Savunma Bakanlığı 2011 Yılının Şubat ayında "Fransa Siber Güvenlik Stratejisi" başlıklı resmi bir belge yayınlamıştır. Belgede Stratejik Hedefler (-Siber Savunma Konusunda Dünya Gücü Ol. ), İcraat Alanı ( -Analiz Et -İkaz Et- Karşılık Ver) başlıkları yer almıştır (Fransa Siber Güvenlik Stratejisi, 2011).

Fransa'nın siber alandaki ulusal stratejisi; siber güvenliği sağlamak ve bu alanda kararlı politikalar çizmektir. Fransa'nın bilgi güvenliği konusundaki çalışmaları, İkinci Dünya Savaşı'na kadar uzanmaktadır. 1943'te Fransız ulusal direnişi altındaki Fransız topraklarının çoğunluğu ile 1943'te Fransız ulusal direnişiyle kurulan Direction Techniquedu Chiffre (DTC), savaş sırasında Alman kodlu iletişimi önlemeye çalıştı ve böylece direnişin iletişiminin gizliliğini sağladı. Savaştan sonra, 1953 yılında, birim, Merkezi Teknik du Chiffre STC-CH oldu. 1977 yılında kurulan İletişim Güvenliği ve Parola Hizmetleri Merkezi (Service Central du Chiffre et Sécuritédes Télécommunications), 1986 yılında Bilgi Sistemleri Güvenliği Merkezi'ne ("Service Central de la Sécuritédes Systèmes D'information-SCSSI") dönüştürüldü. Merkez daha sonra Direction Centrale de la Sécuritédes Systèmes Bilgi Sistemleri Güvenlik Merkezine (DCSSI) dönüştürüldü. Fransa'da bilgi güvenliği politikalarının uygulanmasını koordine etmek amacıyla, DCSSI 2008'de Fransız Ulusal Bilgi Güvenliği Ajansı (ANSSI) ile değiştirildi. Fransa'ya yeni bir kavramsal güvenlik çerçevesi sağlayan Ulusal Güvenlik ve Savunma Hakkında Beyaz Kitap (Défense et Sécuriténationale: Le Livre Blanc), Fransa'nın siber ortamdaki savunma kapasitesinin arttırılması gerektiğini vurguladı. Devletin en önemli görevlerinden biri, ulusal bilgi sistemlerinin güvenliğini sağlamaktı ve hem ISS'ler hem de kritik altyapı sağlayıcıları ile kamu kurumları arasında etkin koordinasyona ihtiyaç duyulduğunu vurgulamaktı. Beyaz Kitap, Fransa'nın ulusal güvenlik tehdidinin başında siber saldırılar görüyor. Bu

riski en aza indirmek için bir koordinatör yapısı oluşturulması önerilmektedir. Beyaz Kitap ile oluşturulacak önerilen koordinatör yapı, kitabın yayınlanmasından sonra kurulmuş ve ANSSI olarak adlandırılmıştır. ANSSI'nin görevlerinden bazıları şunlardır:

- Siber Güvenlik Operasyon Merkezi ile işbirliği içinde, devlete yönelik siber saldırılara karşı zamanında hareket etmek ve kamu kurumlarının ve elektronik kamu hizmetlerinin sunulduğu ağların bu tür saldırılara hazırlanmak için gerekli önlemleri almasını sağlamak,

- Kamu ve özel sektör kuruluşlarının bilgi güvenliği risklerini önlemek,

- Kamu kurumlarının ağ ve ürün güvenliği alanında ihtiyaç duyduğu güvenlik ekipmanını sağlamak veya geliştirmek

- Devletin bilgi güvenliği politikalarının askeri kurumlarla işbirliği ve uyum içinde uygulanmasını sağlamak (Güngör, 2015: 85-86-87).

### 3.1.5. Avrupa Birliği ve Siber Güvenlik

#### 3.1.5.1. AB Hakkında

İkinci dünya savaşından sonra Avrupa'da mutlak barış sağlanması amacıyla Avrupalı devlet adamları birçok faaliyette bulundu. Almanya ve Fransa arasında yıllardır devam eden savaşın son bulması amacıyla barış oluşturma çabası hız kazandı. Ayrıca Marshall yardımı altında ABD ekonomik gelirlerin Avrupa'ya aktığını gören küçük Avrupa ülkeleri ortak kendilerinin ABD'ye bağımlı olacağını düşünceleri yüzünden yeni sermaye piyasası oluşturmaya karar verdiler. Ortak sermaye fikrine ilk olarak Fransa çağrıda bulunarak "Federal Almanya, İtalya, Belçika, Hollanda ve Lüksemburg" yanıtlamıştır ve bu ülkeler arasında 18 Nisan 1951 Tarihinde "Avrupa ve Kömür ve Çelik" Topluluğunu oluşturan sözleşme Paris'te imzalanmıştır. Savaş sanayisini otak kullanacak olan bu ülkeler birbirleriyle savaşacak imkânı bulamayacaklardı. Avrupa Birliği'nin ilk doğuşu bu antlaşmayla başlamıştır. "Avrupa Kömür ve Çelik Topluluğu'nun, " kurulmasının ispatlayan başarı yeni ekonomik görüşmelerin doğmasına ve ortak ekonomik sektör birleşmesi görüşüne yoğunlaşmıştır. Uzun süren çalışmaların ardından Avrupa Topluluğu 25 Mart 1957 yılında bu kez Roma'da imzalanan Avrupa Atom Enerjisi Topluluğu (EURATOM) ve Avrupa Ekonomik Topluluğu (AET) anlaşmaları ile kurulmuştur. Altı ülkenin göstermiş olduğu başarılar Danimarka, İrlanda ve Birleşik Krallık'ı üyeliğe başvurmasını sağladı. Böylece

bu ülkeler 1973 yılında topluluğa üye oldular. Avrupa topluluğu, "7 Şubat 1992 tarihli" Maastricht Sözleşmesiyle "Avrupa Birliği" adını almıştır (Avrupa Birliği'nin Tarihsel Gelişimi. 2012).

Tarihsel değişim kuşkusuz, Parlamento'nun doğrudan seçimiyle başlamıştır. Avrupa Parlamentosu, Strasbourg'da, 1952 Eylül ayında 78 üye olarak toplanan Avrupa Parlamenter Meclisi'ne dayanır. Bu isim daha sonra 1962 yılında "Avrupa Parlamento'su" olarak kullanılmaya başlanmıştır. Avrupa Parlamenter Meclisi, üye devletlerin halkların temsilcilerinden oluşmaktadır. 1960 yıllarından itibaren doğrudan seçimle ilgili olan projenin hayata geçirilmesi 20 yılı almıştır. İdeal olanın ise Avrupa Parlamentosu'nun tüm üye devletlere uygulanacak tek tip sistemle seçilmesidir. Fakat bu sistem henüz gerçekleşmemiştir. Avrupa Parlamento'su üyeleri; her üye devletin ulusal seçim biçimine göre seçilmektedir. Şu an geçerli olan duruma göre bu seçimler Belçika, İtalya ve İngiltere'de bölgesel çapta nisbi sisteme göre; Avusturya, İspanya, Danimarka, Fransa ve Lüksemburg ve diğer bazı üye ülkelerde ulusal çapta nisbi sisteme göre Almanya'da ise karma bir sisteme göre yapılmaktadır (Tezcan, 2005: 8-11).

Doğu Almanya'nın ve Batı Almanya'nın "3 Kasım 1990" yılında bir araya gelmesi, "Merkezi ve Doğu Avrupa ülkelerinin Sovyet gözetiminden kurtulmaları 1991 Aralık ayında Sovyetler Birliği'nin çözülmesi Avrupa'nın siyasi yapısını tamamen değiştirdi. Üye devletler bağlarını güçlü kılma kararıyla ana özellikleri 9-10 Aralık 1991'de Maastricht'te bir araya gelen Avrupa Birliği Zirvesi'nde kararlaştırılan yeni bir Antlaşmanın müzakerelerine başladılar. Maastricht Antlaşması, diğer ismiyle Avrupa Birliği Antlaşması, 1 Kasım 1993 yılında yürürlüğe girdi." Bu antlaşmayla "1999 yılına kadar parasal birliğin sağlanmasına, Avrupa vatandaşlığının oluşturulmasına ve ortak dış ve güvenlik ile adalet ve içişlerinde işbirliği politikalarının yaratılmasına" oy birliğiyle onaylandı (Avrupa Birliğinin Tarihçesi).

1993 Maastricht Antlaşmasıyla asıl hedef Avrupa halkları arasında her türlü engeli yok etmek, barış ve bağımsızlığı sağlayarak devamlı ve yakın bir işbirliği yaratarak aralarındaki bağı güçlendirmektir. Avrupa Birliği yerine getirilmesi gereken ortak politikaları Maastricht Antlaşması'yla belirlemiştir. Politikalarına baktığımızda rekabet, bütçe, sanayi ve ticaret, bölgesel, vergi, çevre, enerji, ulaşım, telekomünikasyon ve bilim-araştırma, tarım, balıkçılık başlıkları altında ayrı ayrı incelemek mümkündür (Kıraç ve İlhan, 2010: 188).

Altı ülkenin üyeliğiyle başlayan Avrupa Birliği bu gelişmeler sonucunda üye sayısını yirmi yediye yükseltmiştir.

**Tablo 10.** Yıllara göre AB üyesi olan ülkeler ve üye oluş tarihleri (Avrupa Birliği Üyesi Ülkeler).

| Devlet | Kabul |
|---|---|
| Almanya | Kurucu |
| Avusturya | 1995 |
| Belçika | Kurucu |
| Birleşik Krallık | 1973 |
| Bulgaristan | 2007 |
| Çek Cumhuriyeti | 2004 |
| Danimarka | 1973 |
| Estonya | 2004 |
| Finlandiya | 1995 |
| Fransa | Kurucu |
| Hırvatistan | 2013 |
| Hollanda | Kurucu |
| İrlanda | 1973 |
| İspanya | 1986 |
| İsveç | 1995 |
| İtalya | Kurucu |
| Kıbrıs Cumhuriyeti | 2004 |
| Letonya | 2004 |
| Litvanya | 2004 |
| Lüksemburg | Kurucu |
| Macaristan | 2004 |
| Malta | 2004 |
| Polonya | 2004 |
| Portekiz | 1986 |
| Romanya | 2007 |
| Slovakya | 2004 |
| Slovenya | 2004 |
| Yunanistan | 1981 |

#### 3.1.5.2. AB'nin Siber Güvenlik Stratejileri

Avrupa Birliği (AB), birçok alanda üye ülkelerine ve AB'ye üye olmaya aday olan ülkelere yol gösterici durumundadır. Bu alanlardan biri hiç şüphesiz siber

güvenliğin sağlanması amacıyla oluşturulan tedbirler olmuştur. Bu kapsamda oluşturulan çalışmalar, bilgi teknolojilerini siber güvenlik ve stratejilere uygun hale getirecek düzenlemelerle mümkündür (Kurnaz, Önen, 2019: 83).

İletişim teknolojilerinin gelişimi ve bilgi sistemlerinde oluşan tehditler AB'nin de siber güvenlik stratejiler oluşturmasına neden olmuştur. AB siber güvenlik hususunda uluslararası alanda ciddi çalışmaların yapıldığı en önemli aktördür. Bunun sonucu olarak siber güvenlik sağlanması konusu en önemli konu olarak görülmekte ve bu bağlamda politikalar geliştirilmektedir. "23 Kasım 1995" tarihinde "Verilerin Korunması Direktifi" ile bireysel bilgi ve verilerin akışı sırasında kişi hakları ile gizliliğin sağlanması gibi konular işlenmiştir. Bu konuların AB üyesi ülkelerin sınırları içinde güvenli bir biçimde dolaşımına ilişkin kurallar belirlenmiştir. Ayrıca "direktifin 25. ve 26. maddelerinde işlenen çeşitli verilerin AB üyesi olmayan devletlerle paylaşımın nasıl olabileceği" hususunda bilgiler verilmiştir (Eren, 2017: 25, 43, 44).AB'nin 1995 yılındaki "Verilerin Korunması Direktifi' destekler nitelikteki diğer temel direktifleri şunlardır (Ünver, Canbay ve Mirzaoğlu, 2011: 19, 20):

• 1999/93/EC sayılı Elektronik imza Direktifi

• 2000/31/EC sayılı Elektronik Ticaret Direktifi

• 2002/58/EC sayılı Elektronik Haberleşme Sektöründe Kişisel Gizliliğin Korunması Direktifi

• 2006/24/EC sayılı Kamusal Elektronik Haberleşme Hizmetlerinin Sunumu Sırasında veya Kamusal Haberleşme Şebekeleri Üzerinden Elde Edilen Verilerin Muhafazasına ilişkin Direktif "

AB' nin siber güvenlik hususundaki diğer temel adımları şöyledir:

| | |
|---|---|
| 2005 Eylül | ENISA tam anlamıyla faaliyete başladı. |
| 2007 Mayıs | "Webi (ağı) Kontrol Et"adlı portal oluşturuldu. |
| 2010 Nisan | AB bakanları, "merkezi siber suç ajansına gereksinimleri saptama ve araştırılması amacıyla Komisyon'a çağrıda bulundu." |

(Yıldız, 2014: 92-93).

"Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) 1 Eylül 2005" tarihinde tam olarak faaliyete geçmiştir. Mayıs 2007'de online olarak terörizm incelenmek üzere "Avrupa Polis Ofisi (Europol) tarafından Ağı kontrol et" adlı portalı oluşturuldu. Nisan 2010 Tarihinde AB bakanları siber suç merkezinin ihtiyaçlarının belirlenmesi amacıyla Komisyon'a çağrıda bulundu. Bu gelişmelerin sonucu olarak siber güvenlik ilgili

konularda Europol da aktif rol oynamaktadır. ENISA tarafından siber güvenlik alıştırılması yapılmış ve sonuç olarak hukuk birliğine gidilmesinin en büyük ihtiyaç olduğuna karar verilmiştir (Yıldız, 2014: 92-93).

Bu kapsamda ENISA'nın stratejik görevleri aşağıdaki gibidir(Kurnaz ve Önan, 2019: 93).

- Avrupa Birliği'ne üye devletler arasında bilgi sistemin ve güvenliğinin sağlanması konusunda danışmanlık yapmak,
- Avrupa'da var olan tehditleri belirlemek, tehditler konusunda veri toplayıp analiz etmek,
- AB'nin bilgi güvenliği konusunda risklerini analiz ederek, risk yönetiminin sağlanmasına teşvik etmek,
- Bilgi güvenliği konusunda farkındalık yaratarak, işbirliğini güçlendirmek.

ENISA, bu görevlerin sayesinde AB'ye üye ülkelerin siber tehditlere karşı öneriler hazırlamaktadır. Siber güvenlik seviyelerinin artırılmasında konusunda da aktif rol oynayarak siber güvenlik sistemine ciddi katkılar sağlamaktadır

ENISA 2012 ve 2013 yıllarında, olası siber krizlerle nasıl baş edilmesi gerektiği, acil durum planlarının ne zaman uygulanacağı gibi konuların uluslararası siber güvenlik bilirkişilerince konuşulduğu ve kararların verildiği Siber Kriz İşbirliği ve Tatbikatları Konferansları (International Conferences on Cyber Crisis Cooperation and Exercises) düzenlenmiştir (Çeliktaş, 2016: 73).

AB, 2016 Temmuz'da "Ağ ve Bilgi Güvenliği Direktifini(Network and Information Security Directive-NIS) kabul etmiştir." NIS Direktifi özelliği, üye devletlerin siber tehditlere karşı tüm hazırlıklarını uyumlu hale getirecek ve AB işbirliğini geliştirmeye yönelik, AB çapında ağ ve bilgi sistemlerinin eşit bir biçimde güvenliğini sağlamaktır." Ayrıca bu direktif, AB bünyesindeki siber güvenlik konusundaki ilk mevzuattır. NIS Direktifi, 2018 tarihinde üye ülkeler yasalarına yansıtmıştır (Korhan, 2018: 53).

Avrupa Birliği; bilgi güvenliği politikaları oluşturmasına etki eden unsurları direktif ve sözleşmelerde açıkça belirtmiştir. "Veri koruma ile ilgili sözleşmeler mevcut direktifler, yeni bilgi ve veri koruma direktifi taslağı (European Commission, 2012) da dikkate alınarak, AB bilgi güvenliği politikaları ile" varılması istenen ana amaçlar şu şekildedir (Henkoğlu, Yılmaz, 2013: 466-467):

- Veri öznesinin tam kontrol edilip idarenin sağlanması,
- Bilginin işlenmesi ile alakalı tüm basamaklarda (toplama, kaydetme, değiştirme, engelleme, çıkarma, yayma vs.) veri öznesinin bilgilendirilmesi,
- Veri öznesinin veriye ulaşımın kolaylaştırılması,
- Bireysel bilgilerin ve verilerin hizmet sağlayıcılar arasında aktarımın sağlanması,
- Bireysel veriler işlevinde kullanılan hizmet sağlayıcılar arasında rekabetin arttırılması,
- Verinin elde edilecek şeklinin ("özellikle çocuklar için 13 yaş sınırı ile ilgili olarak") açıklık getirilmesi,
- Veri öznesini negatif açıdan etkileyebilecek güvenlik tehditleri ya dasorunları ortaya çıktığında; verinin hizmet sağlayıcıların veri öznesini ve yetki merkezlerini (AB dışında işlenmesi halinde dahi) haberdar etmeleri,
- Veri koruma haklarının ihlali konusu ile ilgili idari ve hukuki birimin geliştirilmesi,
- Verinin işlenmesiyle alakalı işlemlerde kontrollerin arttırılması,
- Siber suçlara karşı uluslararası veri koruma standartlarının yaratılması amacıyla, Avrupa dışından devletlerin de katılımıyla uluslararası mücadelenin geliştirilmesi
- AB sözleşmelerine taraf ülkelerde ENISA ile eşgüdüm durumunda olan bir "Bilgisayar Olaylarına Müdahale Merkezi"(Computer Emergency Response Teams, CERT) oluşturulması,
- Kişilerin istedikleri bilgiyi bulma ve taşıma hakkının müdahale olmaksızın sağlanması,
- Kişisel veri güvenliğinin AB vatandaşlarına dünyanın her yerinde aynı güvenliğin sağlanması amacıyla AB normlarının AB pazarında faaliyet gösteren, ama bireysel verileri AB sahası içinde bulundurmayan firmalara da uygulanması,
- Ulusal veri koruma yetkilerinin kuvvetlendirilerek, AB veri koruma kurallarına uymayan firmaları cezalandırabilmelerinin sağlanması,

- Veri koruma kurallarının etkin olarak uygulanması ile AB pazarında ticaretin canlandırılması ve böylece (yıllık 2, 3 milyar Euro) tasarruf sağlanması,
- Hizmet sağlayıcıların sadece AB ülkelerinde bulunan ulusal veri koruma otoritesi/kuruluşu ile bağlantılı olması ve bireylerin kişisel verilerini işleyen şirket AB alanı dışında olsa dahi, ihtilaf halinde kendi ulusal veri koruma otoritelerine bağlı olmalarının sağlanması,
- Yasal düzenlemeler ile tüketicilerin bilgi ve verilerinin korunduğu güvencesini verebilen AB şirketlerinin küresel rekabette avantaj sağlamaları ve bu bağlamda AB sayısal ekonomisinin hızlı büyümesinin gerçekleşmesi,
- Yaşamı kolaylaştıran ayrıca maliyetleri düşüren, yeni iş alanları oluşturan, ekonomiyi canlandıran, sayısal tek pazarın oluşumuna katkı sağlayan, açık ve güçlü bir hukuki altyapının oluşturulması (Henkoğlu, Yılmaz, 2013: 466-467).

Avrupa Birliği, gün geçtikçe artan siber suçlarla ve siber savaşlarla baş edebilmek için Avrupa Birliğine üye olan devletlere gerekli araçları sağlamaya çalışmaktadır. Faaliyetler için gerekli finans, insan kaynaklarını temin edebilirse "Avrupa Siber-suç Merkezi, Avrupa'daki siber-suçla mücadelede merkez noktası" olarak faaliyet gösterecek; dolayısıyla da siber-suç kavramı karşısındaki farkındalığı birlik çapında artırmış olacaktır. Geliştirilmiş, yeni çözümlerle beraber siber-suç şebekelerinin ortadan kaldırılması da kolaylaşacaktır. Bu bağlamda cezai soruşturmaları destekleyip, Merkezin Avrupa vatandaşlarının ve işletmelerin korunmasına katkı sağlayacak ve Merkez sayesinde internet hizmetin ve sanal ekonominin temini kolaylaşacaktır. Konsey bu tasarının kabul edilip onaylanmasına çağrıda bulunmakta ve "Merkez'in gelişimine katkı sağlama noktasında" Avrupa Parlamentosu teşvik edilmektedir (Başbüyük, 2012: 1594).

### 3.1.6. Birleşmiş Milletler

#### 3.1.6.1. BM Hakkında

Birleşmiş Milletler, İkinci Dünya Savaşı sırasında kurulması planlanan ve 1945 yılında kurulan bir örgüttür. İlk kurulduğu yıllarda üye sayısı 51dir. Şimdi ise 193' e ulaşmıştır. Örgütün amacı ilk maddesinde belirtilen Uluslararası barış ve güvenliği

korumak; uluslararası dostça ilişkiler geliştirmek; ekonomik, sosyal, kültürel gelişmeyi sağlamak ve insan haklarını korumaktır (Sur, 2013: 2538-2539).

**Tablo 11.** Yıllara göre BM üyesi olan ülkeler ve üye oluş tarihleri

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Afganistan (1946) | Almanya (1973) | ABD 1945) | Andorra(1993) | Angola(1976) | Antigua ve Barbuda (1981) | Arjantin(1945) | Arnavutluk (1955) | Avustralya (1945) | Avusturya (1955) |
| Azerbeycan (1992) | Bahamalar (1973) | Bahreyn (1971) | Bangladeş(1974) | Barbados(1966) | Belçika (1945) | Belize(1981) | Benin(1960) | Belarus(1945) | Birleşik Arap Emirlikleri (1971) |
| Bolivya (1945) | Bosna-Hersek (1992) | Bostvana(1966) | Brezilya(1945) | Brunei(1984) | Bulgaristan (1955) | Burkina Faso (1960) | Brundi(1962) | Bhutan(1971) | Büyük Britanya ve Kuzey İrlanda Birleşik Krallığı (1945) |
| Cezayir (1962) | Cibuti (1977) | Çat (1960) | Çek Cumhuriyeti (1993) | Çin (1945) | Danimarka (1945) | Kongo Demokratik Cumhuriyeti(1960) | Doğu Timor (2002) | Dominika (1978) | Dominik Cumhuriyeti (1945) |
| Ekvador (1945) | Ekvador Ginesi (1968) | El Salvador(1945) | Endonezya1950) | Eritre(1993) | Ermenistan (1992) | Estonya(1991) | Etiyopya(1945) | Fas(1956) | Fiji(1970) |
| Fildişi Sahili (1960) | Filipinler (1945) | Finlandiya(1955) | Fransa(1945) | Gabon(1960) | Gambiya (1965) | Gana(1957) | Gine(1958) | Grenada (1974) | Guatemala(1945) |
| Guyana (1966) | Gine-Bissau (1974) | Güney Afrika(1945) | Güney Kore(1991) | Güney Sudan (2011) | Gürcistan (1992) | Haiti(1945) | Hırvatistan(1992) | Hindistan (1945) | Hollanda(1945) |
| Honduras (1945) | Irak (1945) | İran (1945) | İrlanda (1955) | İspanya (1955) | İsrail (1949) | İsveç(1946) | İsviçre(2002) | İtalya(1955) | İzlanda(1946) |
| Jamaika (1962) | Japonya (1956) | Kamboçya(1955) | Kamerun(1960) | Kanada(1945) | Karadağ (2006) | Katar(1971) | Kazakistan (1992) | Kenya (1963) | Kıbrıs(1960) |
| Kırgızistan (1992) | Kiribati (1999) | Kolombiya(1945) | Komorlar(1975) | Kongo Cumhuriyeti (1960) | Kosto Rika (1945) | Kuveyt(1963) | Kore Demokratik Halk Cumhuriyeti (1991) | Küba(1945) | Laos(1955) |
| Letonya (1991) | Lesotho (1966) | Liberya(1945) | Libya(1955) | Lihtenştayn (1990) | Litvanya (1991) | Lübnan (1945) | Lüksemburg (1945 | Macaristan (1955) | Madagaskar(1960) |
| Makedonya (1993) | Malavi (1964) | Maldivler(1965) | Malezya(1957) | Mali (1960) | Malta (1964) | Marşal Adaları (1991) | Mauritius1968 | Meksika(1945) | Mısır(1945) |
| Mikronezya Federal Devletleri (1991) | Moğolistan (1961) | Moldova(1992) | Monako(1993) | Moritanya (1961) | Mozambik (1975) | Myanmar (1948) | Namibya(1990) | Nauru(1999) | Nepal(1955) |
| Nikaragua (1945) | Nijer (1960) | Nijerya(1960) | Norveç(1945) | Orta Afrika Cumhuriyeti (1960) | Özbekistan (1992) | Pakistan (1947) | Palau(1994) | Panama1945) | Papua Yeni Gine(1975) |
| Paraguay (1945) | Peru (1945) | Polonya(1945) | Portekiz(1955) | Romanya ( 1955) | Ruanda (1962) | Rusya (1945) | Saint Kitts ve Nevis (1983) | Saint Lucia (1979) | Saint Vincent ve Grenadinler (1980) |
| Samoa (1976) | San Marino (1992) | São Tomé ve Príncipe (1975) | Senegal(1960) | Seyşel Adaları (1976) | Sırbistan (2000) | Sierra Leone (1961) | Singapur(1965) | Slovakya (1993) | Slovenya(1992) |
| Solomon Adaları (1978) | Somali(1960) | Sri Lanka(1955) | Sudan(1956) | Surinam (1975) | Suriye (1945) | Suudi Arabistan (1945) | Esvatini(1968) | Şili(1945) | Tacikistan(1992) |
| Tanzanya (1961) | Tayland(1946) | Togo(1960) | Tonga(1999) | Trinidad ve Tobago (1962) | Tunus (1956) | Tuvalu (2000) | Türkiye(1945) | Türkmenistan (1992) | Uganda(1962) |
| Yunanistan (1945) | Zambiya (1964) | Zimbabve (1980) | | | | | | | |

**Tablo 12.** Birleşmiş Milletler Teşkilatı

| Kuruluş Tarihi | Merkezi | Genel Sekreteri | Üye Sayısı | Ana Organları | Amaçları |
|---|---|---|---|---|---|
| 1945 | New York | Antonio Guterres | 193 | Genel Kurul,<br>Güvenlik Konseyi (BMGK),<br>Ekonomik ve Sosyal Konsey(EKOSOK),<br>Vesayet Konseyi,<br>Uluslararası Adalet Divanı,<br>BM Sekretaryası | Savaşları ve tehditleri önlemek,<br>Ülkeler arasında dostane ilişkiler kurmak,<br>Uluslararası sosyal ve ekonomik işbirliğini sağlamak |

Birleşmiş Milletler; "aralarında Türkiye' ninde bulunduğu 50 ülke tarafından 26 Haziran 1945' de San Francisco'da imzalanmıştır. Polonya'nın daha sonra Şartı imzalamasıyla kurucu üye devlet sayısı 51'e yükselmiştir." Şart'ın onay işlemlerinin tamamlanmasıyla, "24 Ekim 1945 gününde resmi olarak faaliyete geçmiştir. Her sene 24 Ekim'de BM Günü olarak kutlanmaktadır". BM seçimlerde eşitliği sağlamak adına, coğrafi gruplar tesis etmektedir. 1) Afrika Ülkeleri, 2) Asya- Pasifik Ülkeleri, 3) Doğu Avrupa Ülkeleri, 4) Latin Amerika ve Karayip Ülkeleri, 5) Batı Avrupa ve Diğer Ülkeler olmak üzere 5 coğrafi grup bulunmaktadır. Üye ülkeler gelişmiş ekonomilerine göre teşkilata zorunlu katkı sağlamaktadır (Türkiye Cumhuriyeti Dışişleri Bakanlığı).

Birleşmiş Milletler altı ana organdan oluşmaktadır.

**a) Genel Kurul**

İlk birleşimi 1946 yılında yapan Genel Kurul, uluslararası barışın sağlanması ve devamı, barışa gölge düşürecek durumları engellemek ve bu bağlamda uluslararası işbirliği konularında kararlar alırlar. Alınan kararlar tavsiye niteliğindedir.

**b) Güvenlik Konseyi**

Beş daimi üyeden oluşan konseyin karar alabilmesi için, daimi üyelerinden birinin aksi yönde oy kullanmaması gereklidir. Konseyin görev ve sorumlukları şöyle sıralanabilir (Altıner, 2014: 5).

- Uluslararası güven ve barış ortamın sürekliliğini sağlamak,

- Barışı engelleyen antlaşmazlıkları bulmak ve çözüm bulmaya çalışmak,
- Silahlanma düzenleyen kuruluşlar konusunda plan yapmak,
- Barışın engellenmesi konusunda tedbirler almak,
- Saldırganları engellemek amacıyla yaptırımda bulunmak,
- Genel Kurula yeni alınacak üyeler hakkında tavsiye de bulunmak,
- Uluslararası Adalet Divanına hâkim seçimine yardımcı olmak,
- Genel Kurula, Genel Sekreterin seçilmesi için tavsiye de bulunmak.

**c) Ekonomik ve Sosyal Konsey**

Bu organ eğitim, sosyal, sağlık, eğitim, ekonomi, kültürel gibi konularda uluslararası işbirliğini geliştirme ve ülkelere tavsiyeler de bulunma görevini üstlenmiştir**.**

**d) Vesayet Konseyi**

1994 yılında faaliyetleri durmuştur.

**e) Uluslararası Adalet Divanı**

1945 Yılında kurulan bu organ 15 yargıçtan oluşmaktadır. Yargıçların görev süresi 9 yıldır. Divanda bir devletten 2 yargıç bulunmamaktadır. Ayrıca, BM'deki bütün organların hukuki anlamda oluşabilecek sorularına cevap vererek ve bu konularda tavsiyelerde bulunur (Altıner, 2014: 5).

**f) Birleşmiş Milletler Genel Sekreterliği**

Diğer organların getirdiği program, planları ve politikaları yönetip yürütmeyle görevlidir. BM' nin üst yönetim görevlisi Genel Sekreterdir (Birleşmiş Milletler (BM))

Yukarıda sıralan ana organların dışında BM'ye bağlı olarak çalışan birçok kuruluş vardır:

**Tablo 13.** BM'ye bağlı kuruluşlar

| | |
|---|---|
| Gıda ve Tarım Örgütü (FAO) | Uluslararası Çalışma Örgütü (ILO) |
| Uluslararası Göç Örgütü (IOM) | BM Kalkınma Programı (UNDP) |
| BM Nüfus Fonu (UNFPA) | BM Mülteciler Yüksek Komiserliği (UNHCR) |
| BM Enformasyon Merkezi (UNIC) | BM Çocuklara Yardım Fonu (UNICEF) |
| BM Sanayi Kalkınma Teşkilatı (UNIDO) | Dünya Sağlık Örgütü **(DSÖ)** |
| BM Kadın Birimi **(UNWOMEN)** | Dünya Gıda Programı **(WFP)** |
| BM Gönüllüleri **(UNV)** | |

***Kaynak***: (T.C.Milli Eğitim Bakanlığı, 2018).

Birleşmiş Milletleri kuran güçler için (ABD, Sovyetler Birliği, Fransa, Çin ve İngiltere) önemli olan şey, her ne olursa olsun savaş olmayan bir evren planlamaktı.

Birleşmiş Milletler küreselleşmenin etkisiyle çıkabilecek sorunları grupları ayırmaktadır. Bu sorunlar şöyle sıralanabilir (Birdişli, 2010: 176):

1. Politik sorunlar,
2. Ekonomik sorunlar,
3. Ekolojik sorunlar,
4. Sağlıkla ilgili sorunlar,
5. İnsan hak ve hürriyetleri ile ilgili sorunlar,
6. Askeri veya güvenlikle ilgili sorunlar

Sorunlar her ne kadar ayrı gruplar halinde sıralansa da küreselleşmenin etkisiyle iç içe geçen problemler olarak ele alınmaktadır.

#### 3.1.6.2. BM veSiber Güvenlik

Birleşmiş Milletler (BM) kurulduğu yıldan itibaren aktif rol oynamaktadır. Kurulduğu ilk yıllar bozulan uluslararası ilişkileri; sürekliliği sağlamak ve barışı daha güçlü ve daha sağlam temel adımlar atarak istikrara kavuşturmak maksadıyla önemli rol üstlense de günümüzde bu faaliyetlerin yanında; insan hakları, çevre koruma, çocuk sağlığı, ekonomik ve tarımsal kalkınma, çocuk gelişimi, doğal afet yardımı, yoksullukla mücadele ve birçok önemli konularda aktif rol oynamaktadır. Siber güvenlik faaliyetlerine ise 1980'lerin sonunda başlamıştır. Söz konusu siber güvenlik faaliyetler; BM Genel Kurulu tarafından alınan kararların yanı sıra, BM Bilgi ve İletişim Teknolojileri (BDT) Görev Gücü ve BDT ile ilgili çalışmalar yürütmekle sorumlu ana BM ajansı olan Uluslararası Telekomünikasyon Birliği (International Telecommunications Union - ITU) tarafından yapılan çalışmaları kapsamaktadır (Ünver, Canbay ve Mirzaoğlu, 2011:1-2).

1985 Tarihinde hazırlanan "7.Suçtan Korunma Suçluların Rehabilitasyonu" kongresinin hemen ardından düzenlenen; "Milan Eylem Planında, " Birleşmiş Milletler bünyesinde bilgisayar suçları ile ilgili çalışma ve farklı türdeki suç ve ihlaller için, uluslararası eylem planındaki raporda; 42–44. paragrafları arasındateknolojik gelişimin" etkilerine dikkat çekilerekbu bağlamda işlenen ve işlenebilecek bilgisayar suçları vurgulanmıştır (Kara, Aydın ve Oğuz, 2006: 9).

"Örgüt, 1994 yılında, maddi ceza ve usul hukuku, bilgisayar bağlantılı suçların

önlenmesi ve uluslararası işbirliğine dair hazırlanan BM Bilgisayar Bağlantılı Suçların Önlenmesi ve Kontrol Altına Alınması Rehberi yayımlamıştır (Akpek, 2015: 12).

BM Genel Kurulu, 1990 yıllarından itibaren bilgi güvenlik konularını ağırlıklı olarak incelemeye başladıktan sonra, BM Birinci Komite 19 Aralık 2001 tarihli 56. Oturumunda "Bilgi teknolojilerinin suç amaçlı kullanımı ile mücadele "ilişkin kararında, devletler arasında işbirliğinin önemine kamu-özel bölüm iş birliğinin gerekliliğine değinmiştir. Kararda, "BM`nin 55/63 sayılı" kararıyla gösterilen amaçların yapılmasımaksadıyla çalışmaların artırılarak sürekliliği sonucuna varılmıştır (Turhan, 2010: 52-53).

"BM Silahsızlanma Araştırmaları Enstitüsü, " 2007'de bir dergiyi "uluslararası bilişim güvenliği" konusuna adayarak, uluslararası bilişim güvenliğinin yasal olarak dikkate alınarak, siber tehditlere ve siber saldırılara karşılık vermek üzere "NATO ve Avrupa Güvenlik ve İşbirliği Teşkilatı" gibi uluslararası kuruluşlarla, uluslararası bilişim güvenliği sağlayarak yasal tedbirlerin alınması amacıyla diyaloglar başlatmıştır (Türkay, 2013: 1215).

BM şartının meşru müdafaa hakkını düzenleyen 51. maddesi "Bu Antlaşmanın hiçbir hükmü, Birleşmiş Milletler üyelerinden birinin silahlı bir saldırıya uğraması halinde, Güvenlik Konseyi uluslararası barış ve güvenliğin korunması için gerekli tedbirleri alıncaya dek, bu üyenin doğal olan bireysel ya da ortak meşru savunma hakkına halel getirmez" hükmünü amirdir. Yani, üye devletler ancak bir "silahlı saldırı'nın merkezi oldukları zaman meşru müdafaa hakkına başvurabileceklerdir. Söz konusu hükmün gelişen internet ve bilgisayar kullanımın hayatımızın her anına girmesiyle, yeni siber tehditler konusunda da açıklanmasını isteyen "NATO Siber Savunma Mükemmeliyet Merkezi, Uluslararası Bağımsız Uzmanlar Grubuna, Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn Kılavuzu" isimli "yumuşak hukuk" özelliğinde bağlayıcı niteliği bulunmayan metin hazırlatmıştır. Buyazıda, siber tehdit ve saldırılar silahlı saldırı seviyesine ulaştığı taktirde, saldırıyı yapan devlete karşı meşru müdafaa hakkının tanınabileceği vurgulanmıştır (Gökçe, 2017: 26).

Siber saldırılar hatta siber savaş gibi durumlarda Güvenlik Konseyinin yukarıda bahsedilen maddeler doğrultusunda siyasal anlamda, kuvvet kullanma kararı alması oldukça zordur. Siber saldırıların, silahlı saldırı olup olmadığına kesin bir karar verilemezken Güvenlik Konseyinin buna karşı hareket etmesi beklenemez. Ancak dünyadaki en büyük krizler olan Estonya, Gürcistan saldırılarına baktığımızda bu

ülkelerin Güvenlik Konseyi üyesi olmadığını görmekteyiz. Ayrıca Güvenlik Konseyi üyesi devletlerden hiçbirisi, etkisi itibariyle yüksek seviyede bir siber savaşa hatta siber saldırıya maruz kalmamıştır. Güvenlik Konseyinin daha fazla harekete geçmesi içindevlet uygulamalarında siber alanla ilgili denetimlerin artırılması ve siber araçların etkilerini düzenleme ihtiyacının bir gereklilik haline dönüşmesi gerekmektedir (Bolat, 2020: 47).

2017 yılında yayınlanan "Küresel Siber Güvenlik Endeksi, " (Global Cybersecurity Index) "Birleşmiş Milletler bilgi ve iletişim teknolojileri özel ajansı Uluslararası Telekomünikasyon" tarafından yayınlanan raporda, ülkelerin siber tehdit ve terörlere karşı altyapı ve müdafaa güçleri incelenmiştir. Siber terörlere karşı altyapısı en güçlü olarak listenin başında Singapur ve ikinci sırada Amerika Birleşik Devletleri gelmektedir. Türkiye ise 43'üncü sırada bulunmaktadır (International Telecommunication Union: "Global Cybersecurity Index (GCI) 2017).

#### 3.2.6.3. BM Üyesi Ülkelerin Siber Güvenlik Çalışmaları

Hem BM hem de NATO üyesi olan ülkeler yukarıda NATO başlığı altında gösterilmiş olduğundan, çalışmanın bu başlığında BM üyesi olup NATO üyesi olmayan siber güvenlik alanında strateji ve çalışmaları bulunan bazı ülkelerin siber güvenlik stratejilerine yer verilmiştir.

**Singapur**

Singapur, dünyanın en gelişmiş internet ağına sahip ülkelerden biridir. E-devlet projelerini büyük oranda hayata geçirmiştir. Ayrıca ülkede erken uyarı sistemleri üzerinde yoğun çalışmalar yapılmaktadır. Ulusal düzeyde halkın bilinçlendirilmesi, siber saldırılara karşı, gerekli önlemlerin almak için kurumlar ve özel sektör arasında işbirlik sağlanmaktadır (Yılmaz& Sağıroğlu, 2013: 328).

2008 yılından beri siber güvenlik çalışmalarına başlayan ada devleti Singapur, ulusal düzeyde tren otomasyonları sistemleri, santraller gibi önemli bilgi sistemlerine oluşabilecek siber tehditlere karşı önlem almaya çalışmaktadır. Bu doğrultuda 1 Ekim 2009 yılında Ulusal Siber Güvenlik Merkezi (the Singapore Infocomm Tecnology Security Authority – SITSA) kurulmuştur.

SITSA'nın görevleri: (İstanbul Bilgi Üniversitesi Bilişim Ve Teknoloji Hukuku Enstitüsü, 2012: 41).

- Singapur Hükümeti'nin stratejik projelerinde bilişim güvenliği danışmalığı yapmak,
- Devletin bilgi teknolojilerini artırmaya yönelik etkili olan birim ve kuruluşlarla işbirliği yapmak,
- Singapur'un bilişim alt yapı güvenliğini sağlayarak, siber tehditler alanında teknoloji geliştirme faaliyetlerinde bulunmak,
- Singapur'un olası siber saldırılara karşı tedbirli olmayı, planlamayı, karşı uygulamasını sağlamak,
- Bilişim alt yapısında eksikleri inceleyerek mevcut kapasiteyi geliştirmek

**Güney Kore**

Dünyada teknolojik alt yapısı güçlü olan ülkeler arasında Güney Kore yer almaktadır. Güney Kore'nin 1960 yıllarından sonra hızla büyümesi tüm dünyada hayranlıkla gözlemlenmektedir. Son yıllarda siber güvenlik adına yaptığı çalışmalar uluslararası sistemde yer almasını sağlamıştır.

Güney Kore siber güvenliği sağlamak adına 5 önemli eylem planı oluşturmuştur:

- Özel, kamusal ve özel sektör ortak müdahale sisteminin oluşturulması
- Askeri sektörler Kritik altyapının güvenliğinin güçlendirilmesi ve sır korumasını arttırmak
- Ulusal düzeyde siber saldırıları tespit etmek ve engellemek
- Uluslararası işbirliği yoluyla caydırıcılık oluşturma
- Siber güvenlik altyapısının oluşturulması(National Cyber Security Masterplan, 2011).

Tablo 14.Güney Kore'nin 2011 Yılındaki siber güvenlik konusunda önemli adımları

| **Tarih** | **Etkinlik** |
|---|---|
| 11 Mayıs 2011 | Ulusal Siber Güvenlik Stratejisi Konseyi Masterplan'ın kurulması |
| 13 Mayıs- 5 Temmuz 2011 | Konuyla ilgili kuruluşlar tarafından uzmanlara danışılarak bir taslak hazırlanmıştır. |
| 6 Temmuz- 18 Temmuz 2011: | Ulusal Siber Güvenlik Karşı Tedbir Konseyi toplantısı. |
| 2 Ağustos 2011: | 50 çıktı alınarak, uygulandı. |

**Kaynak:** (National Cyber Security Masterplan, 2011).

Her geçen gün artan Kuzey Kore siber saldırıları, Güney Kore' yi siber anlamda daha fazla tedbir almaya zorlamıştır. Bu bağlamda Başkanlık bünyesinde 2015 Mart ayında siber güvenlik ofisi kurulmuştur. Ancak bu ofis incelendiğinde Kuzey Kore'nin saldırılarına geçici olarak çözüm olarak kurulduğu kalıcı bir yapısının olmadığı görülmektedir. Ülkenin önemli bir kuruluşu Kore İletişim Komisyonu'dur. Bu komisyonun siber anlamda en önemi görevi siber güvenlik konusunda stratejiler belirleyip uygulamaktır (Özdaş, 2017: 69-70).

**Hindistan**

Siber güvenlik kavramına önem vererek bu çerçevede çokça çalışmalar yapan Hindistan, siber güvenlik kavramıyla ilgili çalışmaları 1990'lı yıllara kadar uzanmaktadır. Devlete ait sistemleri korumaya yönelik kanunlar düzenlenmektedir. Hindistan Hükümeti vatandaşlarına yönelik "Bilgi Güvenliği Farkındalığı" kampanyaları düzenleyerek halkın bilinçlenmesi sağlamaktadır. Ülkede bilişim alanında çalışmalarda bulunan kuruluşlar "ISO/27001 Bilgi güvenliği Yönetim Sistemi Standartları Uygunluk" Sertifikasına sahip olma zorunluluğu vardır (Yılmaz ve Sağıroğlu, 2013: 327).

Hindistan devletine ait ve uluslararası boyutta olan "Bilgi Güvenliği Farkındalığı" kampanyasıyla siber uzayda etkin olan devlet bu bağlamda başlıca aşağıdaki hedefleri oluşturmuştur (İstanbul Bilgi Üniversitesi Bilgi Teknolojisi ve Teknolojisi Hukuk Enstitüsü, 2012: 6).

- Ülkenin bilişim ve ağlarını en üst düzeyde korumak, önemli alt yapıları siber tehdit ve saldırılara karşı koruyarak ve önlemek,
- Siber tehdit ve saldırılara karşı zafiyeti en aza indirgemek,
- Olabilecek siber saldırılara karşı, zararı en aza indirgemek ve müdahalenin hemen yapılmasını sağlamak Hindistan, bu çalışmaların yanında Ulusal Güvenlik Konseyi (National Security Council) oluşturarak artan siber tehditleri karşılamayı amaçlamıştır. Böylece geniş kapsamlı siber güvenlik politikasının inşasına başlanmıştır. Bu çerçevede "Hindistan Devleti Inter Departmental Information Security Task Force (ISTF)" adlı kurum oluşturulmuştur. ISTF'nin yaptığı önerilerle devlet düzeyinde çalışmalara gidilmiştir. Hindistan hükümetinin yapmış olduğu açıklamada, devlete ait gizli çalışmaların yapıldığı bilgisayarların internete bağlı olmadığını açıklamıştır. Bütün bu çalışmaların

yanında siber güvenlik ile ilgili çalışan uzman kişilerin listesi oluşturularak veri tabanı oluşturulmuştur (Yıldız, 2014: 74-77).

2005 Yılında ordunun internet ve kritik alt yapılarının güvenliğinin sağlanması ve koordineli olarak kontrol edilmesi maksadıyla Hindistan ordusu tarafından "Siber Güvenlik Kuruluşu (Cyber Security Establishment)"kurulmuştur. Ayrıca, 2010 Yılının Nisan Ayında "Hindistan Ordusu Askeri Telekomünikasyon Mühendisliği Üniversitesi bünyesinde, " siber güvenlik laboratuarı oluşturmuştur. Bütün bunların dışında "Ulusal Güvenlik Veri Tabanı (National Security Database-NSD) isimli bir oluşum kurulmuş ve siber güvenlik ile alakalı, ulusal kritik altyapıların ve sistemlerin, korunmasıyla ilgili çalışan güvenilir ve donanımlı uzmanların listesi oluşturulmuştur. Liste yardımıyla Hindistan'da önemli kritik bölümlerde yer almak isteyenlerin güvenlik soruşturmalarından ve belli testlerden geçmeleri sağlanmaktadır (İstanbul Bilgi Üniversitesi Bilgi Teknolojisi ve Teknolojisi Hukuk Enstitüsü, 2012: 8-10).

**Rusya**

Rusya, dünyada siber saldırı kapsamına giren faaliyetlerde en çok suçlanan ülkedir. Çalışmanın önceki bölümünde yer alan Estonya Gürcistan olayları gibi birçok siber savaşın Rusya kaynaklı olduğu bilinmektedir. Rusya siber saldırı olarak çıkan yeteneğinin yanında siber güvenlik kapsamında da çeşitli faaliyetlerde bulunmaktadır. Rusya siber güvenlik faaliyetlerin ulusal olarak değerlendirip, politika üretmeye 2000 yılında başlamıştır ve bu yılda belge yayınlamaya başlamıştır (Meral, 2015: 113).

Rusya'nın siber uzay ve siber güvelik ile ilgili kamuoyuyla paylaştığı birçok belge bulunmaktadır. Birincisi 2000'de yayınlanan "Rusya Federasyonu'nun Bilgi Güvenliği Doktrini" dir. Belgede bu doktrinin amacı Rusya Federasyonu'nun bilgi güvenliği politikasını biçimlendirmek, önerilerde bulunarak yasal, teknik ve kurumsal çerçevelerine Rusya Federasyonu'nun bilgi güvenliğini sağlamak için, bilgi güvenliği programlarını tasarlamaktır. 2011 yılında bilgi alanında askeri uzmanlara ihtiyaç duyulduğu belirtilerek bu konuyla ilgili "Rusya Federasyonu'nun Silahlı Kuvvetleri'nin Bilgi Alanındaki Aktiviteleri Hakkında Kavramsal Görüşler" adlı belge yayınlanmıştır. 2013'de yayınlanan "Rusya Federasyonu'nun 2020'ye Kadar Uluslararası Bilgi Güvenliği Alanındaki Devlet Politikasının Temel Prensipleri" adlı belge "Rusya Federasyonu'nun hedeflerinin uluslararası bilgi güvenliği sisteminin oluşturulması için" uluslararası yasal düzenin kurulmasını özendirmek ve uluslararası bilgi güvenliği

sistemini ikili, çoklu, bölgesel ve global düzeylerde oluşturmak olduğu konuları işlenmiştir (Özfındık, Kotik, 2015: 56-57).

Öte yandan siber güvenliği sağlamak ve siber savaşlara karşı koymak "Rus Federal Güvenlik Servisi (Federalnaya Slujba Bezopasnosti / FSB), " nin görevidir. Siber güvenliğe tamamen yöneldiği tarih 2008 yılıdır. Ayrıca "Rus İstihbarat Servisi (Sluzhba Vneshney Razvedki / SVR)" bir ülkenin teknoloji ya da bilim kapasitesine siber casusluk harekâtı planlaması, SVR'nin siber güvenlik stratejisi kapsamında yerini alır. Rus istihbarat servislerinin çalışma alanları ve operasyonları, siber kapasiteleri dünya kamuoyunda sıklıkla tartışılmasına karşın, bu servislerin gizli siber çalışmaları kavramlarıyla alakalı sınırlı kaynak verisi bulunmaktadır (Darıcılı, 2017: 14-16).

Rusya'nın siber güvenlik stratejileri incelendiğinde, siber güvenlik çalışmalarına önem verdiği görülmektedir. Geçmişte yaşanan siber saldırılara bakıldığında siber potansiyel anlamda gücünü ispatladığı diğer ülkelerin tarafından korkulması şart olan bir otorite olduğu açıktır.

**Japonya**

Japonya'nın teknolojiye olan yakın ilgisi ve sürekli takibin etkisiyle oluşabilecek siber saldırıları önceden farkına vararak; gerekli düzenlemeleri, ceza hukukunda erken bir zamanda yer vermiştir. Söz konusu düzenlemeler oluşturulmadan önce, doktrinlerde savunulmuş ve siber suçlarla baş edebilmede geleneksel ceza tiplerin kâfi olamayacağına karar verilmiştir. Böylece siber suçların yeni tip suç olduğu onaylanarak, ortak birantlaşmaya varılmıştır. Sonuç olarak, 22 Haziran 1987"tarihli yürürlükte "Ceza Hukuku Alanında Baz Hükümlerde Değişiklik Yapılmasına İlişkin Kanunla Ceza Kanununa siber suçlarla ilgili yeni suç tipleri eklenmiştir. 1990'lı yıllarda ise, cyber-pornografik fiiller Ceza Kanunu'nun 175'inci maddesi kapsamında kabul edilmiştir (Turhan, 2006: 95-96).

2000 Yılında Japonya "Kritik Altyapılara Karşı Siber Tehditler Üzerine Özel Eylem Planı" hazırlamıştır. Planın hedefi önemli ve kritik sistemlerin altyapılarını, "insanların ve iş dünyasının" finansal anlamda faaliyetlerini ciddi oranda etkiyebilecek her türlü siber tehdit ve terör saldırılarından korumaktır. 2005 ve 2009 Tarihlerinde "Kritik Altyapılar için Bilgi Güvenliği Önlemleri Üzerine Birinci ve İkinci Eylem Planları" oluşturulmuştur. Birinci Eylem Planındaki amaç; "kritik bilgi ve altyapıların aksamasını önlemek amacıyla temel adımlardan olan Koruma Mühendisliği

Yetenekleri, Teknik İşlemler, Analizler ve Karşılık (CEPTOAR) yapısının geliştirilmesi olmuştur". Bu bağlamda kurumlar arasında birçok uygulamalar dayapılmıştır."İkinci Eylem Planı Birinci Eylem Planının" amacıyla; Bilgi Teknoloji sorun ve arızaların insanların yaşamlarına, sosyal hayatlarına ve finansal çalışmalarına yüksek oranda etkilemesini önleme şeklinde saptanmıştır (Ünver, Canbay, Özkan, 2011: 26, 29).

**İsrail**

İsrail savunmasında siber güvenlik algısı öncelikle bilgi güvenliği ve verilerin, bilgisayarların korunması şeklinde örgütlenmiştir. Siber güvenlik konusunda küresel pazarda yerini almak isteyen İsrail, bu bağlamda İtalya, Japonya ve Hindistan'la işbirliği yapmaktadır (Özfındık, Kotik, 2015: 65).

İsrail siber güvenlik ve savunma stratejisine sahip en iyi ülkelerden biridir. İsrail'in siber müdafaadan mesul dört birimi vardır. İsrail Savunma Kuvvetlerine bağlı, "Birim 8200" adında, emekli askerler ve subaylardan meydana gelen personeller üç alana yoğunlaşmaktadır. "Birim 8200'ün siber savaşta belirlediği alanlar": İstihbarat toplama, savunma ve saldırıdır. İsrail siber güvenlik ve stratejisinden sorumlu, hükümet sistemlerinin korunmasıyla sorumlu iç istihbarat kurumu Shin Bet'in görevidir. İsrail'in bağımsızlık ilanı ile 1948 yılında IDF'nin bir kolu olarak kurulan, "Shin Bet faaliyet sorumluluğu daha sonra Başbakanlığa bağlanmıştır." C4ISR (Command, Control, Commonications, Computers, Intelligence Komuta, Kontrol, Haberleşme, Bilgisayar ve İstihbarat) "sistemler bütünü, kolordu iletişim ve siber savunma gibi çalışmalardan sorumludur." 18 Mayıs 2011'de yabancı devletler tarafından müdafaa ağlarına etkileyebilecek ya da zarar verebilecek siber savaşlara karşı "Ulusal Sibernetik Çalışma Grubu" kurulmuştur. İsrail "Ulusal Siber Bürosu"ise (Israel National Cyber Bureau-INCB), 2012 yılında kurulmuştur. INCB, bilgisayar sistemlerindeki meydana gelebilecek, savaşlara karşı İsrail devletini savunmak amacıyla kurulmuştur. INCB önem verdiği güvenlik sisteminin, iş yaşamın ve akademi dünyasının birliğiyle savunma sistemini örgütlemeyi hedeflemiştir. Ülkenin uğradığı siber tehdit ve siber saldırılarda, ülkedeki birçok sektör arasında önleyici tedbirler alarak, siber savunma çalışmalarını düzenlemiştir (Kara, 2013: 63-64).

Günümüzde sayısız ülke, önemli ulusal bilgi ve sistemlerini internet temelli merkezde saklamaktadır ve bundan dolayı internet aracılığıyla oluşabilecek birçok siber tehdit hatta siber savaşlara karşı açık haldedir. "İnternet güvenlik şirketi McAfee'nin"

yaptığı yoğun araştırma neticesinde; İsrail ise, “sanal saldırılara karşı en hazırlıklı ülkelerden biridir.” İsrail kritik alt yapı ve sistemlerini internet ağları üzerinde tutarak nispeten başka ülkelerden gelen tehdit ve savaşlara karşı kendini kapamış durumdadır (İstanbul Bilgi Üniversitesi Bilgi Teknolojisi ve Teknolojisi Hukuk Enstitüsü, 2012: 40).

**Avustralya**

Avustralya’da siber güvenliği sağlama hizmeti sunan iki önemli teşkilat merkezi vardır. Federal ve eyalet/bölge bilgi teknolojileri sistemleri için destek sağlayan ve DSD tarafından yönetilen Bilgi Güvenliği Olay Tespit Raporlama ve Analiz Programı (ISIDRAS) ve kritik altyapı ve sistem işletmecilerine benzer hizmetler sunan Avustralya Bilgisayar Acil Durum Müdahale Ekibidir (AusCERT) (Turhan, 2010: 89).

ISIDRAS: “DSD tarafından yönetilmektedir.” Temel hedefi, devletin bilgi ve iletişim sistemlerinin güvenliğini etkileyecek güvenlik olaylarıyla ilgili bilgilerin elde edilmesidir. ISIDRAS, “Avustralya`nın önemli bilgi sistemlerine karşı tehlikeler ve güvenlik açıklarıyla ilgili bilgileri sağlamak suretiyle, bu sistemlerin en üst düzeyde nasıl korunabileceğine ilişkin bilgi ve veriler sağlamaktadır. ISIDRAS olayları düzenli bir biçimde DSD’ye sunmaktadır (Turhan, 2010: 90).

AusCert: Avustralya ve Asya / Pasifik bölgesinde Siber Acil Müdahale Ekibi tarafından oluşturulmuştur. 2018'de CERT Avustralya, Avustralya Siber Güvenlik Merkezi'nin (ACSC) bir parçası oldu ve daha sonra Avustralya Sinyaller Direktörlüğü'nün (ASD) bir parçası olmuştur. AusCERT, ulusal bilgi altyapısını etkileyen acil konularda bağlantı merkezidir. Yabancı devletlerden bilgi ve veri almakta ve aldıkları verileri Avustralya kritik bilgi temelli işletmecilerine ve sahiplerine iletmektedir. Ancak bilgisayar gündelik kısımlara karışmamaktadır (AUSCERT).

**Çin**

Ülkenin özellikle kuruluşundan sonraki 30 yıllık döneminde dış politikası incelendiğinde, Çin Halk Cumhuriyeti’nin beraberliğin devam ettirmek ve dış tehditlere karşı önlem alarak işgallere önlemek olduğu görünmektedir. Bilgi toplumuna geçişin ardından sürekli kendini geliştiren Çin Halk Cumhuriyeti internetsiz hiçbir iş yapamayacak duruma gelmiştir. Artan internet kullanım ile birlikte siber suçlar yükselmiş ve siber güvenlik kavramı, Çin Halk Cumhuriyeti’nin de önem verdiği bir eğilim olmuştur. Çin diğer Batı ülkelerinden farklı bir politika oluşturarak, kendi bilişim

teknolojisini oluşturmuştur. Politikanın ana başlığı, "bağımsız internet teknolojisi olmadan siber güvenliğin" sağlanamayacağıdır (Göçoğlu, 2018: 124-125).

Çin'in siber güvenlik konusunda yaptığı çalışmalar1986 yılında başlamıştır. Ekonomik bilgilerin yer aldığı yönetim küçük bir grup halinde örgütlenmiştir. "2003 yılında ise ilk sivil belge" olma özelliğine sahip 27 maddelik siber güvenliği korumaya yönelik belge yayınlanmıştır. Belge kritik alt yapılara koruma özelliğine sahip aynı zamanda aktif savunma özelliğini de içermektedir. 2014 yılından önceki tüm çalışmalar siber güvenlik çalışmalar hukuki ve kurumsal anlamdadır. 2014 yılında ise devlet başkanı Xi Jinping öncülüğünde siber güvenlik grubu oluşturulmuştur ve 2014 yılındaki tüm siber güvenlik çalışmaları o yılda yayınlanan "hükümet raporunda" yer verilmiştir. "2015 yılında Çin'in ulusal kongresi olan NPC'de (Standing Committee of the National People's Congress) kamuoyu yoklaması yapmak suretiyle halkın da görüşlerini göz önüne alarak Siber Güvenlik Kanunu tasarısını oluşturmuştur" (Göçoğlu, Aydın, 2019: 244). Bu bağlamda 2015 yılında "Beyaz Belge" yayınlandı. Beyaz Belge'nin içeriğine göre hava, deniz, kara ve siber uzayın güvenliği bütün olarak görünen askeri bir bütündür. Ayrıca belgede Çin'in siber ordu kurmakta olduğu belirtilmiştir. Bu bağlamda Çin'in siber stratejiler konusunda çalışmalar yaptığı, savunma stratejileri geliştirerek; ulusal ve uluslararası gelişmeleri desteklediğini belirtip, uluslararası işbirliğine açık kapı bırakmıştır (Özfındık, Kotik, 2015: 62).

**İran**

Siber güvenlik uzmanları ABD, Çin, Rusya gibi siber orduları güçlü olan devletlerin yanında İran devletinin de güçlü bir siber donanım ve siber orduya sahip olduğunu ifade etmektedir. Ayrıca, İran'ın siber alanda zarar verme kapasitesinin oldukça yüksek olduğu belirtilmektedir. ABD ve İsrail kaynaklı siber saldırılar İran devletini dijital alanda güvenlik sağlayarak, önlemler almasına neden olmuştur (İran En Güçlü Siber Ordulardan Birine Sahip).https://tr.euronews.com/2019/03/07/iran-en-guclu-siber-ordularindan-birine-sahipİran'ın maruz kaldığı birçok siber saldırı, İran devletinin bilgisayarlardaki bilgilerinin hacklenmesi amaçlanmıştır. "İran savunma bakanı" İran devletin hiçbir devlet tarafından siber alanda yenemeyeceğini ifade ederek, İran devletinin dahi bilgisine ve gücüne güvendiğini belirtmiştir. Siber saldırıları kontrol etmek, önlemek amacıyla orduyla eşgüdümlü siber müdafaa organizasyonu oluşturulmuştur. Siber savunma organizasyonu bilgisayar ağlarını sürekli kontrol

etmektedir. Özellikle stuxnet saldırısından sonra savunma sistemlerini geliştirmeye yönelerek birçok tatbikat yapmıştır (Kara, 2013: 68).

Gelinen noktada İran tarafından, söz konusu saldırılarda; stratejilere yön verebilmek için Siber Güvenlik Yüksek Kurulu oluşturulmuştur. Kurul, önde gelen yetkililerin yanında güvenlik ve istihbarat görevliler ileiletişim ve kültür bakanlarından oluşmaktadır. Ayrıca 120.000 gönüllü hackerdan oluşana bartılı sayı olarak görülebilecek olsa da "Siber Ordu" oluşturulmuştur. Ordunun ilk çalışması ise İran'ın yakıt istasyonlarına düzenlenen siber saldırılara cevap vermek maksadıyla İran tarafından baş şüpheli olarak görülen Sudi Aramco and BM RasGas şirketlerine yapılan saldırılardır. Bu saldırılar sonucunda yaklaşık 30.000 bilgisayardaki bilgiler silinmiş ve şirketlerin rafineri kontrol sistemleri zarar görmüştür (Göçoğlu, 2018:131).

İran devleti tarafından 2011 yılında, sibere özgü görevleri yürütmek amacıyla İran'ın kolluk kuvvetleri siber birimi olan, Siber NAJA Polis birimi kurulmuştur (Ünver, Kim, 2016: 13). İran siber saldırılara karşı tatbikat yapmaktadır. En büyük örneği ise Ehlibeyt Haber Ajansı ABNA göre, "Velayet 91 uzmanlık saha tatbikatı sözcüsü tuğamiral Emir Rastegari, uluslararası Tensim haber ajansına dün verdiği demeçte tatbikatın ikinci günü gelişmelerini ele alırken, siber saldırının ilk kez Velayet 91 uzmanlık saha tatbikatında gerçekleştiğini ve başarıyla denendiğini belirtmiştir. Habere göre İran İslam cumhuriyeti deniz kuvvetleri Velayet 91 uzmanlık saha tatbikatı sözcüsü tuğamiral Emir Rastegar ayrıca tatbikatın ikinci gününde birçok saldırgan düşmana karşı harekâtın başarı ile gerçekleştiğini, Tarık deniz altısının da saldırgan güçlere karşı başarılı olduğunu belirtmiştir (Velayet 91 Uzmanlık Saha Tatbikatında Siber Saldırı Başarı İle Denendi, 2012).

### 3.1.7. Avrupa Konseyi ve Siber Güvenlik

Avrupa Konseyi Avrupa'yı bütün olarak görme arzusunun sonucu olarak meydana gelmiştir. 1948 yılında La Haye'de, önemli birçok şahsiyet öncülüğünde bir araya gelen Kongrede, özgür Avrupa'nın çeşitli ülkeleri arasındaki bağları kuvvetlendirecek bir kuruluşun oluşması talep edildi. Diplomasi alanında derhal görüşmeler başladı ve yoğun görüşmelerin sonucu olarak "5 Mayıs 1949'da"imzalanarak, "3 Ağustos 1949" tarihinde yürürlüğe girmiştir. Böylece "Avrupa Konseyi" kurulmuştur. Örgüt kendileri için seçilen merkez olan Strasbourg şehrinde toplanmıştır. Avrupa Konseyi'ni kuran antlaşma sırasında 10 ülke bulunuyordu: Fransa,

Büyük Britanya, Belçika, Hollanda, İtalya, Lüksemburg, İrlanda ve 3 İskandinav ülkesi; Danimarka, Norveç ve İsveç (Dehousse, 1958: 41).

Avrupa Konseyi'nin kurulma amacı; askeri ve güvenlik konuları dışında Avrupa'da görülen diktatörlüklere ve Sovyet geleneğine tepki, insan hakları ihlalleri ve soykırıma karşı demokrasi sağlayarak, ortak siyasi değerler ortaya çıkarmak ve insan haklarını savunma gayesiyle kurulmuştur. Konsey faaliyetlerine başladıktan sonra askeri ve güvenlik alanları dışında her türlü konuları çalışmalarına almıştır. Ayrıca Avrupa Konseyi, üye ülkelerin uyum ve ahengi en yüksek oranda, üye devletlerarasında ikili sorunları en düşük oranda, hatta hiç olmaması gerektiğini göstermeye çalışmaktadır (Öncü, Cevizliler, 2013: 23, 24).

| **Avrupa Konseyi'nin Organları** | **Avrupa Konseyi Sözleşmeleri Çerçevesindeki Mekanizmalar** | **Avrupa Konseyi'nin Amaçları** |
|---|---|---|
| **1. Bakanlar Komitesi**<br>**2. Avrupa Konseyi Parlamenter Meclisi (AKPM)**<br>**3. Yerel ve Bölgesel Yönetimler Kongresi** | • Avrupa İnsan Hakları Sözleşmesi (AİHS)<br>• İşkence ve İnsanlık dışı veya Küçültücü Ceza veya Muamelenin Önlenmesi Avrupa Sözleşmesi<br>• Avrupa Sosyal Şartı | • Üye ülkelerin vatandaşların yaşam koşullarını iyileştirmek,<br>• Avrupa kültürel benliğini oluşmasını sağlamak ve bu amaçla yapılan çalışmalara katkıda bulunmak,<br>• Düşmanlık, ırkçılık, çevre sorunları, uyuşturucu kullanımı vb. sorunlara çözüm yolu bulmak,<br>• Çoğulcu demokrasi, "insan hakları ve hukukun üstünlüğü ilkelerini benimsemek, korumak ve güçlendirmek" |

**Kaynak:** (*Türkiye Büyük Millet Meclisi, 2021).*

İkinci Dünya Savaşı sonrasında konseyin temel yapıtaşı olan insan hakları ve özgürlüklere saygı konusunda 3 temel belge çıkarmıştır. Bunlar:

1. Avrupa İnsan Hakları Sözleşmesi: 4 Kasım 1950 yılında imzalanmıştır. Amacı "insan hakları ve özgürlüklerinin" korunması maksadıyla kişisel başvurulara imkân vermektir. Bu çerçevede Kişisel başvurular Avrupa İnsan Hakları Komisyonu'na bireysel başvuru imkânı tanınmıştır (Altuğ, 1991: 2).

2. İşkencenin Ve Gayri İnsani Ya Da Küçültücü Ceza Veya Muamelelerin Önlenmesine Dair Avrupa Sözleşmesi: "Avrupa Konseyi üyesi devletler, İnsan Haklarının ve Temel Özgürlüklerin Korunmasına Dair Sözleşme hükümlerini dikkate alarak;" 1 Şubat 1989'da Aynı Sözleşmenin, 3 Maddesi "hiç kimse işkence veya gayri insani veya küçültücü ceza veya muameleye tabi tutulmayacaktır." "Hürriyetinden yoksun bırakılan kişilerin işkence ya da küçültücü ceza veya muameleye karşı korunmalarının önlenmesi amacıyla" Avrupa Konseyi sözleşmesi imzalanmıştır (İşkencenin Ve Gayriinsani Ya Da Küçültücü Ceza Veya Muamelenin Önlenmesine Dair Avrupa Sözleşmesi1987: 363).
3. Avrupa Kültür Sözleşmesi:19 Aralık 1954'deAvrupa Kültür Mirasının gelişmesi korunması amacıyla oluşturulmuştur (Altuğ, 1991: 2).

#### 3.1.7.1. Avrupa Konseyinin Siber Güvenlik Stratejileri

Avrupa Konseyi bilişim suçlarını engellemek amacıyla; bireylerin özel hayatının korunması, elektronik bilgi bankalarında işlenen bilgi ve verileri korumak için gerekli olabilecek ilkeleri belirlemek amacıyla 1970'li yıllarda çalışmalara başlamıştır. "Özel sektör ve kamu sektöründeki elektronik bilgi bankalarında uygulanacak ilkeleri gösteren iki tavsiye kararı Avrupa Konseyi Bakanlar Komitesi, 1973 ve 1974 yıllarında" onaylanmıştır. Böylece bilgi, verilerin korunması hususunda özel yasaları; Konsey üyesi ülkelerden Almanya, Avusturya, Danimarka, Fransa, Norveç kabul etmişlerdir. "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması'na ilişkin 108 sayılı sözleşme, "28 Ocak 1981 tarihinde imzaya açılmış" ve hemen ardından Avrupa Konseyine üye ülkeler imzalamıştır (İlbaş, 2009:7).

Avrupa Konseyi Bünyesinde 1997 yılında "Siber-uzay Suçları Uzman Komitesi" (Committee of Experts on Crime in Cyber-space) kurulmuştur. Avrupa Konseyi Bakanlar Komitesi onayı ile 08.11.2001 tarihinde kabul edilmiştir Avrupa Siber Suç Sözleşmesi, devletlerin imzasına 23.11.2001 tarihinde Budapeşte'de açılmıştır. Siber alanda ilk uluslararası sözleşme olan Avrupa Siber Suçlar Sözleşmesi 01.07.2004'te yürürlüğe girmiştir. Budapeşte'de açıldığı için sözleşme, sıklıkla "Budapeşte Sözleşmesi" şeklinde de söylenmektedir. Avrupa Konseyi üyesi devletlerin haricinde, Sözleşme ayrıca ABD, Japonya, Kanada gibi Avrupa Konseyi olmayan birçok ülke tarafından onay verilerek imzalamıştır (Aliusta, Benzer, 2018: 37).

Avrupa Siber Suçlar Sözleşmesinin 23. Maddesinde yer alan ilkelerle bu çalışmanın konusunu oluşturan uluslararası adli yardımlaşmanın çerçevesi çizilerek, siber güvenlik konusunda uluslararası işbirliğinin genel ilkeleri ortaya konmuştur. Bu ilkeler (Siber Suç Uzmanları Komitesi, 2008: 40).

1) Birinci Maddede, uluslararası işbirliğin, taraflar arasında olası en geniş yöntemle gerçekleşeceği alenen belirtilmiştir. Bu maddeyle uluslararası işbirliğin sürekliliği sağlanması amaçlanmıştır.
2) İkinci Maddeyle, 23 Madde de yer alan uluslararası işbirliğinin yükümlülükleri açıkça belirtilerek genel kapsamı da ortaya konmuştur.
3) Üçüncü Maddeyle, işbirliği 23. Bölüm çerçevesinde gerçekleştirileceği ayrıca "cezai meseleler de uluslararası işbirliğine ilişkin uluslararası belgelerin, tek taraflı ya da karşılıklı sözleşmelerin ve ulusal yasaların uygulanması yoluyla" gerçekleştirilecektir ifadeleri ortaya konmuştur.

Yukarıda sayılan ilkeler doğrultusunda raporda belirtilen önemli temel amaçlar şu şekilde sıralanabilir (Aliusta, Benzer, 2018: 38).

- Uluslararası yardım ve işbirliği sağlamak amacıyla hızlı bir ağ ve etkili bir sistem oluşturmak,
- Bilişim suçlarıyla ilgili, konsey üyesi ülkelerin yasal mevzuatlarını ve diğer hukuk düzenlemelerini uyumlu duruma getirmek.

Yukarıda sayılan maddeler doğrultusuna sözleşmenin hedefinin kısaca; toplumun bilişim yoluyla işlenen suçlara karşı korunarak, ortak bir ceza politikasının oluşturulması ve gerekli mevzuatın kabul edilerek uluslararası işbirliğinin geliştirilerek sürdürülmesi söylenebilir (Aköz, 2018: 50).

Ayrıca; Avrupa Konseyi tarafından sözleşmenin onaylandığı 28 Ocak tarihi "verilerin korunması günü" olarak 2007 yılından itibaren anılmaya ve kutlanmaya başlanmıştır ve bu kapsamda birçok etkinlik düzenlenmektedir (Turhan, 2010: 76).

Tabloya baktığımızda; hemen hemen tüm Avrupa Konseyi'ne üye ülkeler sözleşmeye onay verirken, İrlanda, İsveç, Rusya Siber Suç sözleşmesine onay vermemiştir. Terörle Mücadele Uzmanlar Komitesi (Committee of Experts on Terrorism- CODEXTER); uluslararası Yukarıdaki tabloya göre 2020 yılı itibariyle; 44 Avrupa Konseyi ülkesi tarafından onaylanmıştır. Bu alanda, terörizm ve hukuk üzerine yaptığı çalışmalarıyla bilinmektedir. Küreselleşmenin etkisiyle yeni bir alan olan internetin, özellikle terör amaçlı kullanımı üzerine yaptığı çalışmalara da ağırlık

vermiştir. Bu bağlamda Terörle Mücadele Uzmanlar Komitesi (Committee of Experts on Terrorism- Codexter)Avrupa Konseyiyle işbirliği içindesiber güvenlik konusunda yaptığı çalışmalardan söz etmek mümkündür. İşbirliği sağlanarak, Avrupa Konseyi'nin öneri olarak sunduğu; altyapıların korunarak, ulusal hukukların uyumlaştırılması, konularının siber alanda siber sorunları engelleyebilecek bir unsur olabileceğinden söz etmiştir (Tikk, Oorn, 2008: 93-94). Böylece kritik altyapıların kullanılması ve hukuksal uyumlaşma, siber güvenlik çalışmalarında atılan adımlarda kolaylık sağlamıştır.

**Tablo 15.** 23/11/2001 Siber Suç SözleşmesiÜye Devletlerin imzasına açık antlaşma

| | **İmza** | **Onay** | **Yürürlüğe Girme** |
|---|---|---|---|
| Arnavutluk | 23/11/2001 | 20/06/2002 | 2004/01/07 |
| Andorra | 23/04/2013 | 16/11/2016 | 2017/01/03 |
| Ermenistan | 23/11/2001 | 12.10.2006 | 01/02/2007 |
| Avusturya | 23/11/2001 | 13/06/2012 | 01/10/2012 |
| Azerbaycan | 30/06/2008 | 15/03/2010 | 01/07/2010 |
| Belçika | 23/11/2001 | 20/08/2012 | 01/12/2012 |
| Bosna Hersek | 09/02/2005 | 19/05/2006 | 01/09/2006 |
| Bulgaristan | 23/11/2001 | 07.04.2005 | 01.08.2005 |
| Hırvatistan | 23/11/2001 | 17/10/2002 | 2004/01/07 |
| Kıbrıs | 23/11/2001 | 19/01/2005 | 01/05/2005 |
| Çek Cumhuriyeti | 09/02/2005 | 22/08/2013 | 2013/01/12 |
| Danimarka | 22/04/2003 | 21/06/2005 | 2005/01/10 |
| Estonya | 23/11/2001 | 12/05/ 2003 | 01/07/2004 |
| Finlandiya | 23/11/2001 | 24/05/2007 | 01/09/2007 |
| Fransa | 23/11/2001 | 10/01/2006 | 01/05/2006 |
| Gürcistan | 01/04/2008 | 06.06.2012 | 01/10/2012 |
| Almanya | 23/11/2001 | 09/03/2009 | 01/07/2009 |
| Yunanistan | 23/11/2001 | 25/01/2017 | 01/05/2017 |
| Macaristan | 23/11/2001 | 04/12 /2003 | 01/07/2004 |
| İzlanda | 30/11/2001 | 29/01/2007 | 01/05/2007 |
| İrlanda | 28/02/2002 | | |
| İtalya | 23/11/2001 | 05/06/2008 | 01.10.2008 |
| Letonya | 05/05/2004 | 14.02.2007 | 01/06/2007 |
| Lihtenştayn | 17/11/2008 | 27/01/2016 | 01/05/2016 |
| Litvanya | 23/06/2003 | 18/03/2004 | 2004/01/07 |
| Lüksemburg | 28/01/2003 | 16/10/2014 | 2015/01/02 |
| Malta | 17/01/2002 | 12.04.2012 | 01/08/2012 |

| | | | |
|---|---|---|---|
| Monako | 2013/02/05 | 17/03/2017 | 01/07/2017 |
| Karadağ | 07.04.2005 | 03/03/2010 | 01/07/2010 |
| Hollanda | 23/11/2001 | 16/11/2006 | 01/03/2007 |
| Kuzey Makedonya | 23/11/2001 | 15/09/2004 | 01/01/2005 |
| Norveç | 23/11/2001 | 30/06/2006 | 01/10/2006 |
| Polonya | 23/11/2001 | 20/02/2015 | 01/06/2015 |
| Portekiz | 23/11/2001 | 24.03.2010 | 01/07/2010 |
| Moldova Cum. | 23/11/2001 | 12/05/2009 | 01/09/2009 |
| Romanya | 23/11/2001 | 12/05/2004 | 01/09/2004 |
| Rusya | | | |
| San Marino | 17/03/2017 | 08/03/2019 | 01/07/2019 |
| Sırbistan | 07.04.2005 | 14/04/2009 | 01/08/2009 |
| Slovak cumhuriyeti | 04.02.2005 | 08/01/2008 | 01/05/2008 |
| Slovenya | 24/07/2002 | 08/09/2004 | 01/01/2005 |
| İspanya | 23/11/2001 | 03/06/2010 | 01.10.2010 |
| İsveç | 23/11/2001 | | |
| İsviçre | 23/11/2001 | 21.09.2011 | 01/01/2012 |
| Türkiye | 10.11.2010 | 29/09/2014 | 01/01/2015 |
| Ukrayna | 23/11/2001 | 10/03/2006 | 01/07/2006 |
| Birleşik Krallık | 23/11/2001 | 25/05/2011 | 01.09.2011 |

**Kaynak:** (Antlaşmanın İmza ve Onay Tablosu.2021).

2003 yılında oluşturulan bu komite, 2017 yılında sona ermiştir. Ancak, 2018 yılında, Avrupa Konseyi Terörle Mücadele Komitesi (Council of Europe Counter-Terrorism Committee CDCT)'ne dönüşmüştür. Komiteyle beraber ayrıca siber alandaki suç ve tehditlerle ilgili belirli sözleşmeler yapılmıştır (Committee of Experts on Terrorism 2003-2017).

Avrupa Konseyi, belirli dönemlerde, başta Avrupa Konseyine üye ülkelerle olmak üzere çalışmalar yapmakta ve konferanslar düzenlemektedir. Bu faaliyet kapsamında; siber alanda, özellikle siber güvenlik konusunda eğitim amaçlı çalışmalara öncelik verilmesi gerektiğinden söz edilmektedir. Burada; bir siber tehdit durumunda ya da meydana gelebilecek siber savaş karşısında hazırlıklı olabilmek, zararı en aza indirmek için çalışmalar yapılmaktadır (Güryuva, 2019: 171).

# SONUÇ

Tablo 4'de Global Dijital Raporu bakıldığında (bkz:19).2018 Yılında İnternet Kullanıcısı: 4.02 Milyar, Sosyal Medya Kullanıcısı 3.19 Milyar, 2019 Yılında İnternet Kullanıcısı: 4.38.Milyar, Sosyal Medya Kullanıcısı 3.48 milyar. 2020 Yılında 4.54 Milyar, Sosyal Medya Kullanıcısı3.80 milyar olduğu verilerine ulaşılmaktadır. Küresel anlamda bu denli internet kullanımın artması ve bu çerçevede internetin kullanım yoğunluğu düşünüldüğünde, internette geçirdiğimiz zaman ve internet aracılığıyla paylaştığımız bilgi miktarı hayal edilmeyecek boyutta olduğunu görmekteyiz. Bunun yanı sıra teknolojinin kullanımının artmasıyla, insanlar, özel sektör ve devlet kurumları siber alana bağımlı hale gelmiştir. Bu çerçevede tüm kurum ve kuruluşlar hizmetlerinin bir kısmını internet ortamında da sunmaktadır. Bilgilerin internet ortamında sunulması, bilgi güvenliği konusunda ve birçok alanda önemli değişikliklere sebep olmuştur. Bu değişimlerden sadece ulusal kurum ve kuruluşlar değil devletler ve uluslararası kuruluşlar da önemli ölçüde etkilenmiştir.

Siber uzayın kullanımındaki artış avantajlar kadar bazı dezavantajları da beraberinde getirmektedir. Özellikle uluslararası ilişkiler açısından bakıldığında siber tehdit ve saldırılar, gerçekleşen siber savaşlar yaşanan en büyük dezavantajlardır. Siber sorunlardan korunmanın en iyi yolu etkili siber güvenlik stratejiler ve politikalar oluşturmaktır. Bu bağlamda günümüz dünyasında güçlü bir devlet olabilmenin önemli koşulları; ağ sistemlerine hâkim olma, bilgi güvenliğini sağlama, özellikle yasal mevzuatlara dayanan siber güvenlik stratejisiyle mücadele etme hem ulusal hem de uluslararası sistemde çok daha önemlidir. Siber güvenlik alanında geliştirilecek politikaların ulusal bazda kalmaması ve uluslararası boyutta da etkili ve işbirliğine açık bir şekilde olması son derece önemlidir.

Yeni dönemde değişen güvenlik anlayışı çerçevesinde, özellikle siber güvenlik alanında, devlet tekelciliği güç kaybetmiştir. Uluslararası aktörler NATO, AB, Birleşmiş Milletler, Avrupa Konseyi gibi kuruluşlar siber sorunlardan korunma kaygısıyla geleneksel güvenlik anlayışı yerine yeni (modern) güvenlik konular çerçevesinde uluslararası alanda bazı adımlar atmaya başlamıştır. Bunda siber uzayda meydana gelen saldırıların, siyasi ilişkiler açısından gerginliklere yol açabilmesi ve sadece bir ülkeyi değil tüm ülkeleri tehdit edebilme potansiyeline sahip olması etkili olmuştur. Özellikle NATO ülkelerine düzenlenen siber saldırılar bu tarz krizlere ve

gündelik hayatın devamı açısından aksaklıklara neden olmuştur. Yaşanan krizler sonrasında "güvenlik kavramının uluslararası ortamın şartlarına uyarlaması ihtiyacı" fikri önem kazanmıştır. Bu bağlamda siber saldırıları önleme girişimleri sadece ulusal sınırlar içinde değil; dünya çapında aktif çalışmalarla, etkin uygulamalarla anlam kazanmıştır. Günümüze kadar daha çok çeşitli saldırılardan sonra ortaya koyulan tedbir ve politikalar geliştirildiği gözlemlenmiştir. Ancak siber uzayda meydana gelecek gerginliklerin reel dünyadaki yansımaları düşünüldüğünde konuya daha proaktif bir yaklaşım sergilenmesi ve düzeltici tedbirlerden önce "önleyici" tedbirlerin alınması büyük önem arz etmektedir.

Ayrıca siber sorunların arttığı bu dönemde siber güvenlik çalışmalarına önem veren birçok devlet bu savaşı kazanırken; siber güvenliğe önem vermeyen devletler bu savaşı kaybetmeye mahkûmdur. Bu çerçevede uluslararası sisteme dâhil olan her devletin bireysel bazda bu alanda tedbirli olması gerekmektedir. Yaşanan ulusal ve/veya uluslararası siber saldırılar veri tabanlarına işlenerek gelecekte gerçekleşebilecek yeni sorunlara karşı bütüncül stratejilerle tedbir alınmalıdır. Devlet gereksinimleri kadar güvenlik gereksinimleri de dinamik yapıya kavuşturulmalıdır.

Dünyada ulusal siber güvenlik farkındalığı konusunda başrol olan ülkeler (ABD, Almanya, İsrail, Çin, Birleşik Krallık, Rusya, Güney Kore, Estonya, Kanada, Japonya, Avustralya, Singapur, Hindistan) yüksek performansla dünya ülkelerine örnek konumdadır. Bu ülkelerin siber güvenlik çalışmalarına hızlı bir şekilde göz atacak olursak. Özellikle ABD, sisteminde riski ortadan kaldırmak ve risk yaratabilecek kaynakları da etkisiz duruma getirmek gibi siber güvenlik anlayışıyla, diğer ülkelerden farklı olarak daha saldırgan bir stratejiye sahiptir. Almanya siber güvenlik yarışına ABD'den sonra başlamıştır. 2011 yılında ilk ulusal siber güvenlik stratejisini oluşturarak o yıldan sonra büyük ve hızlı bir gelişme göstermiştir. Stratejilerinde, Almanya kritik bilgi sistemi altyapılarının korunmasına önem vermektedir. Rusya, dünyada siber saldırı kapsamına giren faaliyetlerde en çok suçlanan ülkedir. Estonya ve Gürcistan olayları gibi birçok siber savaşın Rusya kaynaklı olduğu bilinmektedir. Rusya siber saldırı olarak ortaya çıkan etkinliğinin yanında siber güvenlik yeteneğiyle de uluslararası sistemde yerini almaktadır. Siber güvenlik kavramına önem vererek bu çerçevede çokça çalışmalar yapan Hindistan, siber güvenlik kavramıyla ilgili çalışmaları 1990'lı yıllara kadar gitmektedir. Çin diğer Batı ülkelerinden farklı bir politika oluşturarak, kendi bilişim teknolojisini oluşturmuştur. Fransız hükümeti ulusal güvenlik tehdidinin başında

siber saldırıları görmektedir. Dünyaya teknolojik alt yapısı ve sistemleriyle örnek konumunda olan Güney Kore siber güvenliği sağlamak adına 5 önemli eylem planı oluşturmuştur. Kanada Hükümeti, yapmış olduğu siber çalışmaların yanında kritik altyapı sektörlerine olaylara müdahale, koordinasyon ve destek sağlama, izleme ve siber güvenlik tehditleri analiz etme, bilgi teknolojileri alanlarında danışmanlık sağlama ve farkındalığın artırılması ile ilgili eğitim faaliyetleri de yürütmektedir. Japon Hükümeti'nin siber alanda oluşabilecek tehditleri farkına varması çok eskilere dayanmaktadır. "22 Haziran 1987" tarihli yürürlükte "Ceza Hukuku Alanında Baz Hükümlerde Değişiklik Yapılmasına İlişkin Kanunla Ceza Kanununa siber suçlarla ilgili yeni suç tipleri eklenmiştir.2008 yılından beri siber güvenlik çalışmalarına başlayan ada devleti Singapur, ulusal düzeyde tren otomasyonları sistemleri, santraller gibi önemli bilgi sistemlerine oluşabilecek siber tehditlere karşı önlem almaya çalışmaktadır. Bu doğrultuda 1 Ekim 2009 yılında Ulusal Siber Güvenlik Merkezi (Singapore Infocomm Tecnology Security Authority – SITSA) kurulmuştur. Birleşik Krallık Ekim 2010'da, İngiliz hükümeti Ulusal Güvenlik Strateji Raporunu meclise sunmuş ve yayınlamıştır. Bu raporda, Birleşik Krallık oluşabilecek tehditleri bölümlere ayırarak, siber saldırıları en güçlü tehdit grubu olarak kabul etmiştir. Avustralya'da siber güvenliği sağlama hizmeti sunan iki önemli teşkilat merkezi vardır. Federal ve eyalet/bölge bilgi teknolojileri sistemleri için destek sağlayan ve DSD tarafından yönetilen Bilgi Güvenliği Olay Tespit Raporlama ve Analiz Programı (ISIDRAS) ve kritik altyapı ve sistem işletmecilerine benzer hizmetler sunan Avustralya Bilgisayar Acil Durum Müdahale Ekibidir (AusCERT). İsrail siber güvenlik ve savunma stratejisine sahip en iyi ülkelerden biridir. Siber güvenlik alanında küresel pazarda yer almak isteyen İsrail, bu bağlamda İtalya, Japonya ve Hindistan'la işbirliği yapmaktadır. Türkiye'de ve İran'da ise yapılan çalışmalar başlangıç aşamasındadır. Ancak; bu ülkelerdeki siber güvenlik algısının diğer dünya ülkelerindeki gibi hızlı bir biçimde arttığı gözlemlenmektedir.

Bu çalışmada siber güvenlik konusunda örnek konumdaki devletlerin ve uluslararası örgütlerin siber güvenlik strateji belgeleri, çalışmaları, potansiyel faaliyetleri incelenmiştir. Yapılan incelemeler sonucunda dünyadaki hemen hemen her devletin siber güvenlik konusunda altyapılarını geliştirilmesi amacıyla bu yönde çabaladığı ve bu doğrultuda birimler kurduğu görülmüştür. Bu çalışmayla dünyadaki ülkelerin siber güvenlik güç potansiyelleri, siber uzayda başrol oynayan ülkeler,

Uluslararası Kuruluşların Siber Güvenlik alanına bakış açıları, yaptıkları çalışmalar, yürüttükleri faaliyetler, antlaşmalar, eylem planları hakkında bilgiler verilmiştir. Ülkeler ulusal ve uluslararası düzeyde siber uzayda siber güvenlik alanında farkındalık oluşturarak bu doğrultuda bilinç seviyesi yükseltilmesi gerektiği sonucuna varılmıştır.

Sonuç olarak, siber suçlar dünya genelinde hızlı bir biçimde yayılırken, bu suçların tümünü yok etmek mümkün değildir. Ancak siber suçlarla mücadelede küresel çapta işbirliği sağlanarak ve bu bağlamda tüm ülkelerin imzalayacağı sözleşmeler geliştirilerek siber sorunların etkileri minimize edilebilir. Ayrıca etkin çalışmalarla standartlar hazırlanmalı ve siber saldırı savunma kapasiteleri artırılmalıdır.

Siber güvenlik eğitimi bütün bireyler tarafından alınmalıdır. Özellikle; ağ yöneticileri, güvenlik analistleri, güvenlik danışmanları, sistem uzmanları ve analistleri yüksek düzeyde siber güvenlik eğitimleri almalıdır. Bu bağlamda şirketler siber alanda dönüşüm başlatmalıdır ayrıca kapsamlı siber tehdit analizleri yaparak siber saldırı sırasında savunma mekanizması oluşturmalıdır.

Siber alanda eğitimsiz olarak teknoloji kullanımı daha büyük risklere neden olacaktır. Bilgi güvenliğinde oluşabilecek bir açık kötü niyetli kişiler tarafından kullanımı söz konusu olacaktır. Bu amaçla; siber uzayla ilgili düzenli programlar yapılarak risk tamamen kaldırılmasa da planlı eğitim tasarılarıyla en alt seviyeye indirilmesi sağlanmalıdır.

Akademik çalışmalarda son yıllarda siber güvenlik kavramı siber güvenliğin önemi gibi konular incelenmektedir. Siber alanda ve siber güvenlik konularında yapılanan araştırmalara bakıldığında uluslararası ilişkilerde siber güvenlik konusu, alt başlık olarak incelenmiştir. Dolayısıyla bu tez çalışmasının devletlerin, uluslararası kuruluşların siber alanda, siber güvenlik konulu yapılacak yeni çalışmalara katkı sağlaması beklenmektedir.

# KAYNAKÇA

## Makaleler


Ada, M., Çakır, H. (2017). Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, *5*(2), 632-656.

Aliusta, C., & Benzer, R. (2018). Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, *4*(2), 35-42.

Alizada, N. (2019). Ülke Dışı Politikalarda Siber Güvenlik Algısı: ABD, Rusya Ve İran Örneği. *Birinci Uluslararası Güvenlik ve Stratejik Araştırmalar Sempozyumu: Türkiye-Rusya Arasında Bilimsel, Teknolojik ve Ekonomik İşbirliği*, 92.

Altıner, B. (2014). Birleşmiş Milletler: Amacı, Gelişimi, Etkinliği, Uluslararası Güvenliğe Katkısı Ve Geleceği. *Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi*, *1*(1), 1-9.

Altuğ, Y. (1991).Türkiye ve Avrupa Konseyi. *Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni*, *11*(1-2), 1-4.

Arat, M., Solmaz, Ş., Ertuğrul G. Vd. (2017). Birleşmiş Milletler'in Tarihsel Gelişimi II. Dünya savaşı Sonrası Uluslararası Ortam ve Konferanslar. *Uluslararası İlişkiler Bülteni. Karabük Üniversitesi.(5).*

Arslan, M.E. (2016). Siber Güvenlik ve Siber Saldırı Türleri. 1-10.

Ayhan, U. (2016). Yeni Güvenlik Konsepti ve Güvenliği Sınır Ötesinde Karşılama. *Güvenlik çalışmaları Dergisi*, (3), 133-142.

Bakan, S., & Şahin, S. (2018). Uluslararası Güvenlik Yaklaşımlarının Tarihsel Dönüşümü ve Yeni Tehditler. *The Journal of International Lingual Social and Educational Sciences*, *4*(2), 135-152.

Başbüyük, İ. (2013). Dijital Çağda Suçla Mücadele: Bir Avrupa Siber-Suç Merkezinin Kurulması. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, *15*, 1583-1594.

Bıçakcı, S. (2012). Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu. *Uluslararası İlişkiler Dergisi*, *9*(34), 204-226.

Bıçakcı, S. (2014). NATO'nun Gelişen Tehdit Algısı: 21. yüzyılda siber güvenlik. *Uluslararası İlişkiler Dergisi*, *10*(40), 100-130.

Bıçakcı, S., Ergun, D., & Çelikpala, M. (2015). Türkiye'de siber güvenlik. *EDAM Siber Politika Kâğıtları Serisi*, (1).

Birdişli, F. (2010). Birleşmiş Milletler (BM)'in Uluslararası Sorunları Önleyebilme Yeteneği. *Journal of International Social Research*, *3*(11).

Brauch, H. G. (2008). Güvenliğin Yeniden Kavramsallaştırılması: Barış, Güvenlik, Kalkınma ve Çevre Kavramsal Dörtlüsü. *Uluslararası İlişkiler Dergisi*, *5*(18), 1-47.

Büyükbaş, H., & Ören, K. (2005). Küreselleşme, Birleşmiş Milletler ve Uluslararası Sosyal Düzen Arayışı. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (13), 103-121.

Çelik, Ş. (2013). Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Cilt: 15, Sayı: 1.*

Çelik, S. (2018). Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım. *Academic Review of Humanities and Social Sciences*, *1*(2), 110-119.

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

Dedemen, F. (2016). Geleceğin Güvenlik Ortamının Şekillenmesinde Hibrit Savaş Modelinin Değerlendirilmesi. *Güvenlik Bilimleri Dergisi*, *5*(1), 141-176.

Demiray, M., & İşcan, İ. H. (2008). Uluslararası Sistemde Güvenlik Kavramının Değişimi Ekonomik ve Jeopolitik Arka Planı.*Dumlupınar Üniversitesi Sosyal Bilimler Dergisi*, *1*(21), 141-170.

Erdoğan, İ. (2013). Küreselleşme Olgusu Bağlamında Yeni Güvenlik Algısı. *Gazi Akademik Bakış*, (12), 265-292.

Eren, M. Avrupa Birliği'nin Siber Güvenlik Stratejisi İçin Kuramsal Çerçeve ve Strateji Belgesi Öncesi AB'nin Eylemleri. *A Peer Review International E-Journal on Cyberpolitics, Cybersecurity and Human Rights Volume 2, Number 3, 2017*, 25-58

Eroğlu, H.T. (2019).Bilgi Yönetim Güvenliği Sistemi: Uygulamalar, Sorunlar ve Çözüm Önerileri. Uluslararası Kamu Yönetimi Sempozyumu (KAYSEM). *Uluslararası Siyaset ve Güvenlik Stratejileri Kamu Yönetimi Politikaları,* 18-

20 Nisan 2019, s.1576-1592.

Erendor, M. E. (2017). Risk Toplumu ve Refleksif Modernleşme Çerçevesinde Siber Terörizm: Tanımlama ve Tipoloji Sorunu. *Cyberpolitik Journal*, *1*(1), 114-133.

Göçoğlu, V., & Aydın, M. D. (2019). Siber Güvenlik Politikası: ABD, Rusya ve Çin Üzerine Karşılaştırmalı Bir Analiz. *Güvenlik Bilimleri Dergisi*, *8*(2), 229-252.

Gökçe, Y. (2017). Güç Kullanımı Olarak Siber Faaliyetler: Uluslararası Hukukun Siber Uzaya Uygulanabilirliği. *Yeditepe üniversitesi hukuk fakültesi dergisi*, 22.

Güngör, U., & Güney, O. (2017). Uluslararası İlişkilerde Güvenliğin Dönüşümü Çerçevesinde Bilgi Güvenliği ve Siber Savaş. *Karadeniz Araştırmaları*, (55), 131-146.

Güreşci, R. (2019). Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirmesi. *Savunma Bilimleri Dergisi*, *18*(1), 75-98.

Gürkaynak, M. (2005). Soğuk Savaş Sonrasında NATO ve Avrupa Güvenliği. *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (1), 7-27.

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

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

Henkoğlu, T., & Yılmaz, B. (2013). Avrupa Birliği (AB) Bilgi Güvenliği Politikaları. *Türk Kütüphaneciliği*, *27*(3), 451-471.

İşyar, Ö. G. (2008). Günümüzde Uluslararası Güvenlik Stratejileri: Kavramsal Çerçeve ve Uygulama. *Gazi Akademik Bakış,* (03), 1-42.

Kara, O., Aydın, Ü., &Oğuz, A. (2006). Ağ Ekonomisinin Karanlık Yüzü: Siber Terör.*V. Uluslararası Bilgi, Ekonomi ve Yönetim Kongresi*, Kocaeli, Turkey, (2), 156-170.

Kasapoğlu, C. (2017).Siber Savaş: Geleceğin Askeri Gerçekliği ve Günümüzün Bilimkurgusu Arasında. *EDAM Siber Politikalar Kâğıtları Serisi* 2017(2), 1-15.

Kaypak, Ş. (2012). Güvenlikte Yeni Bir Boyut; Çevresel Güvenlik. *International Journal of Economic & Social Research*, (8), 1-22.

Kıraç, S., & İlhan, B. (2010). Avrupa Birliği Oluşum Süreci ve Ortak Politikalar.

Kıratlı, O. S. (2016). Avrupa Dış İlişkiler ve Güvenlik Politikası ve Üç Büyükler: Almanya, Fransa ve İngiltere. Akademik İncelemeler Dergisi, 11(1): 207224 *Milli Eğitim Dergisi*, *40*(188), 191-201.

Kolasi, K. (2013). Soğuk Savaş'ın Barışçıl Olarak Sona Ermesi ve Uluslararası İlişkiler Teorileri. *Ankara Üniversitesi SBF Dergisi*, *68*(02), 149-179.

Kurnaz, S., & Önen, S. M. (2019). Avrupa Birliğine Uyum Sürecinde Türkiye'nin Siber Güvenlik Stratejileri. *International Journal of Politics and Security*, *1*(2), 82-103.

Oduncu, T. 1999 Kosova Krizi ve NATO'nun Kosova Müdahalesi. *Bucak İşletme Fakültesi Dergisi*, *2*(1), 1-15.

Oğuzlu, H. T. (2007). Dünya Düzenleri ve Güvenlik: Ulus-Devlet Güvenlik Anlayışı Aşılıyor mu? *Güvenlik Stratejileri Dergisi*, *3*(06), 1-35.

Önaçan, M. B. K., & Atan, H. (2016). Siber Güvenlikte Lisansüstü Eğitim: Deniz Harp Okulu Örneği. *Trakya Üniversitesi Mühendislik Bilimleri Dergisi*, *17*(1), 13-21.

Öncü, A. S., & Cevizliler, E. (2013). Avrupa Bütünleşmesi İçin Önemli Bir Adım:''Avrupa Konseyi''ve Türkiye'nin Konseye Üyeliği Meselesi. *Gazi Akademik Bakış*, *7*(13).

Önok, M. (2013). Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, *19*(2), 1229-1270.

Özcan, A. B. (2011). Uluslararası Güvenlik Sorunları ve ABD nin Güvenlik Stratejileri. *SÜ İİBF Sosyal ve Ekonomik Araştırmalar Dergisi,* 445-465.

Özdaş, M.R. (2017).Siber Güvenlik Kurumsal Yapılanması: Dünya Örnekleri ve Türkiye İçin Bir Kurumsal Yapılanma Önerisi. *A Peer Review International E-Journal on Cyberpolitics, Cybersecurity and Human Rights Volume 2, Number 3, 2017*, 59-85.

Özdemirci, F., &Torunlar, M. (2018). Bilgi-Değişim-Siber Güvenlik-Bağımsızlık. *Bilgi Yönetimi*, *1*(1), 78-83.

Polat, D. Ş, (2020). Nato'nun Yeni Operasyon Alanı: Siber Uzay. *Güvenlik Bilimleri Dergisi*, (International Security Congress Special Issue), 135-158.

Sancak, K. (2013). Güvenlik kavramı Etrafındaki Tartışmalar ve Uluslararası

Güvenliğin Dönüşümü. *Sosyal Bilimler Dergisi,* 123-134.

Sandıklı, A., &Emeklier, B. (2012). Güvenlik Yaklaşımlarında Değişim ve Dönüşüm. *Teoriler Işığında Güvenlik, Savaş, Barış ve Çatışma Çözümleri*, 1.

Sarper, A. B. (2011). Güvenlik Kavramını Yeniden Düşünmek: Küreselleşme, Kimlik ve Değişen Güvenlik Anlayışı. *Güvenlik Stratejileri*, (22), 109.

Sur, M. (2013). Birleşmiş Milletler Örgütünün Gelişimi ve Geleceği The Development and The Future of the United Nations. *Journal of Yaşar University*, *8*(Özel), 2535-2550.

Şafak, E.(2020). Uluslararası Hukukta Değişen Güvenlik Algısı ve Saldırı Suçu Bağlamında Siber Saldırılar. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, *28*(1), 127-160.

Terzi, M.(2018). Bilgi ve İletişim Teknolojilerine Dayalı Oluşumlar İle Bu Oluşumların Uluslararası İlişkilere Güvenlik Bağlamındaki Etkisi: Siber Terörizm. *Kara Harp Okulu Bilim Dergisi*, *28*(1), 73-108.

Ünal, S. (2016). Siber Uzamın Güvenlikleştirilmesi Söylemi Aracılığıyla Gözetim Ve Denetimin Meşrulaştırılması: Türkiye, ABD ve Avrupa Birliği Örnekleri. International Journal of Social Science, (42), 409-430.

Ünver, A, Kim, G. (2016). Türkiye'de Veri Gizliliği ve Gözetimi: Kişisel Verilerin Korunması Kanunu Tasarısının Değerlendirmesi. EDAM Siber Politika Kağıtları Serisi (2), 1-24.

Türkay, Ş. (2013). Siber Savaş Hukuku ve Uygulanma Sorunsalı. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, *71*(1), 1177-1227.

Yayla, M. (2013). Hukuki Bir Terim Olarak Siber Savaş. *TBB Dergisi*, *104*, 177-202.

Yayla, M. (2014). Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı. *Hacettepe Hukuk Fakültesi Dergisi*, *4*(2), 181-200.

Yenal, S., & Akdemir, N. (2020). Uluslararası İlişkilerde Yeni Bir Kuvvet Çarpanı: Siber Savaşlar Üzerine Bir Vaka Analizi. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *11*(1), 414-450.

Yetim, S. (2014). Siber Suçlar, Yargılama Yetkisi ve Yeni Bir Model Önerisi. *Türkiye Adalet Akademisi Dergisi*, 5(17). 177-230.

Yılmaz, E. A., & Akbulut, A. (2019). Küreselleşme Sürecinde Ulus-Devletin Rolü Ulus-Devletler Güçleniyor Mu? The Role Of The Natıon-States In Globalization Process Do The Nation States Gain Power?*Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *8*(16), 71-88.

Yılmaz, S., & Sağıroğlu, Ş. (2013). Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi.*6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı,* 20-21 Eylül, s.323-331.

Yılmaz, S., & Sağıroğlu, Ş. (2013). Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri. *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, 158-166.

Yorulmaz, M. (2014). Değişen Uluslararası Güvenlik Algılamaları Bağlamında Türkiye-Yunanistan İlişkilerinde Değişmeyen Güvenlik Paradoksu.*Balkan Araştırma Enstitüsü Dergisi-Trakya Üniversitesi*, *3*(1), 103-135.

Zabunoğlu, H. G. (2018). Günümüzde Ulus-Devlet. *Erciyes Üniversitesi Hukuk Fakültesi Dergisi*, *13*(1), 535-559.

## Tezler

Ada, M. (2018). NATO Üyesi Ülkelerin Siber Güvenlik Stratejileri Açısından İncelenmesi. *Yüksek Lisans Tezi. Ankara.*

Akpek, N. O. (2015). Siber Suçlar Sözleşmesinin Getirdikleri ve İç Hukuk Açısından Konuya Yaklaşım. *Doctoral dissertation, İstanbul Bilgi Üniversitesi.*

Aköz, B. C. (2018). Türk Ceza Kanunu Kapsamında Bilişim Suç ve Cezaları İle Örnek Yargısal Kararların Analizi ve Mevzuat Önerileri. *Bilgi Teknolojileri ve İletişim Kurumu, Bilişim Uzmanlığı Tezi. Ankara.*

Alp, Ö. (2018). Akıllı Şehirlerde Siber Güvenlik. *İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü. Yüksek Lisans Tezi. İstanbul.*

Aytekin, A. (2015). Türkiye'nin Siber Güvenlik Stratejisi ve Eylem Planının Değerlendirilmesi. *Yayımlanmamış Yüksek Lisans Tezi, Bilişim Sistemleri Anabilim Dalı, Gazi Üniversitesi*.

Bolat. C. (2020). Siber Saldırılara Karşı Meşru Müdafaa Hakkının Uluslararası Hukuk Açısından İncelenmesi. *Doktora Tezi. Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Anabilim Dalı, İstanbul Üniversitesi.*

Çeliktaş, B. (2016). Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir

Değerlendirme. *Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü. Trabzon*.

Dehousse, F., & Lütem, İ. Avrupa Konseyi. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, *15*(1), 41-49.

Ercan, M. (2015). Kritik Alt Yapıların Korunmasına İlişkin Belirlenen Siber Güvenlik Stratejileri. *Gebze Teknik Üniversitesi Sosyal Bilimler Enstitüsü. Kocaeli.*

Erol, S.E. (2016). Siber Güvenlik Farkındalığı İçin Yetenek Tabanlı Dinamik Model. Gazi Üniversitesi Fen Bilimleri Enstitüsü. Yüksek Lisans Tezi. Ankara.

Göçoğlu, V. (2018). Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi. *Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı. Ankara.*

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

Güryuva, Y. (2019). Uluslararası Siber Güvenlik ve Siber Ortamdaki Tehditlerin Fiziksel Bir Savaşa Dönüşme Olasılığı. *Çankaya Üniversitesi Sosyal Bilimler Enstitüsü. Siyaset Bilimi Ve Uluslararası İlişkiler Anabilim Dalı Yüksek Lisans Tezi.* Ankara.

Haser, D. (2018). Uluslararası İlişkilerde Güvenlik Kavramı: Soğuk Savaş Sonrası Dönem Güvenlik. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Enstitüsü. İstanbul.*

İlbaş, Ç. (2009).*B*ilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi. *Master's thesis, Başkent Üniversitesi Fen Bilimleri Enstitüsü.*

Kara, M. (2013). Siber Saldırılar Siber Savaşlar ve Etkileri. *İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim Ve Teknoloji Hukuku Yüksek Lisans Tezi. İstanbul.*

Karadağ, Ş. (2019). Siber Uzayın NATO'nun Güvenlik Anlayışına Etkisi. *Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü. Yüksek Lisans Tezi. Konya.*

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

Meral, M. (2015). Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi. *Harp Akademileri Stratejik Araştırmalar Enstitüsü Savunma Kaynakları Yönetimi Ana Bilim Dalı. İstanbul*.

Özfındık, Kotik Y. *(*2015).Uluslararası İlişkilerde Siber Güvenlik Algısı ve Ulus

Devletin Değişen Stratejisi. *Sosyal Bilimler Enstitüsü. Yüksek Lisans Tezi. Adana.*

Sanalp, S. (2016). *Çeşitli Ülkelerde Usom ve Some Yapılandırılması ve Türkiye Modeli Önerisi*. İstanbul: İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilgi Üniversitesi Doktora Tezi.

Sarı, O. (2013). Uluslararası Hukuk ve Türk Ceza Hukuku Bağlamında Siber Güvenlik Ve Bilişim Sistemine Yönelik Suçlar.*Harp/Harekât Hukuku Ana Bilim Dalı Yüksek Lisans Tezi.* İstanbul.

Şahin, G. (2015). Soğuk Savaş Sonrası Değişen Güvenlik Anlayışı Bağlamında NATO. *Trakya Üniversitesi, Sosyal Bilimler Enstitüsü. Doktora Tezi. Edirne.*

Tarhan, K. (2018). Uluslararası Güvenliğin Bir Bileşeni Olarak Siber Güvenlik. *Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü. Yüksek Lisans Tezi. Konya.*

Turhan, M. (2010).*Siber Güvenliğin Sağlanması Dünya Uygulamaları ve Ülkemiz İçin Çözüm Önerileri*. Ankara: Bilgi Teknolojileri ve İletişim Kurumu Uzmanlık Tezi.

Turhan, O. (2006). Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar).*T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği Planlama Uzmanlığı Tezi. Ankara.*

Yalçın, İ. (2019). Soğuk Savaş Sonrası NATO ve Türkiye'de Siber Güvenlik. *Anadolu Üniversitesi Sosyal Bilimler Enstitüsü. Eskişehir.*

Yıldız, M. (2014). Siber Suçlar ve Kurum Güvenliği. *Denizcilik Uzmanlık Tezi, TC Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Bilgi İşlem Dairesi Başkanlığı*.

**Raporlar**

Dijital Türkiye Platformu, (2017). *Türkiye'nin Siber Güvenlik Stratejisine Yönelik Değerlendirmeler.* İstanbul: Dijital Türkiye.

Fransa Siber Güvenlik Stratejisi, (2011). http://siberharp.blogspot.com/

İstanbul Bilgi Üniversitesi Bilişim Ve Teknoloji Hukuku Enstitüsü, (2012). *Siber Güvenlik Raporu.* İstanbul: İstanbul Bilgi Üniversitesi Bilişim Ve Teknoloji Hukuku Enstitüsü. İşkencenin ve Gayriinsani ya da Küçültücü Ceza Veya Muamelenin Önlenmesine Dair Avrupa Sözleşmesi (Strasbourg, 26 Kasım 1987), ve diğer sözleşme ve bildiriler... *Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni*, *8*(2), 363-370.

Seren, M. (2006). *Siber Tehditlerle Mücadelede Farkındalık ve Hazırlık*. Ankara: Siyaset, Ekonomi ve Toplum Araştırmaları Vakfı (SETA) Analiz, (183).

Thinktech STM Teknolojik Düşünce Merkezi, (2020). *2020'de Etkili Olacak 8 Siber Güvenlik Tehdidi.*

Thinktech STM Teknolojik Düşünce Merkezi, (2020). *Siber Tehdit Durum Raporu Ekim-Aralık 2020.*

Ulaştırma D. & Bakanlığı, H. (2013). *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı.* TC Ulaştırma, Denizcilik ve Haberleşme Bakanlığı*, Ankara*, *8*(2018), 2013-2014.

## Kitaplar

Alkan, M., Aslan Ö., Bostan, A., Doğru, İ., Dörterler, M., Efe, A., (2018). *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık.* BGD Siber Güvenlik ve Savunma Kitap Serisi 1. Ankara.

Siber Suç Uzmanları Komitesi (2008). *Avrupa Konseyi Siber Suçlar Sözleşmesi Taslağı*. Ankara 3. Baskı.

NATO. (1995).*NATO El Kitabı Ortaklık ve İşbirliği*. Brüksel: NATO Basın Yayın ve Enformasyon Bürosu.

Sarınay, Y. (1988).*Türkiye'nin Batı İttifakına Yönelişi ve NATO'ya Girişi*. Ankara: Kültür Ve Turizm Bakanlığı Yayınları Kültür Eserleri Dizisi.

Tezcan, E. (2005). *Avrupa Birliği Kurumlar Hukuku* (Vol. 8). USAK Books.
https://books.google.com.tr/books?id=BzpsncgNPh4C&lpg=PR5&ots=i6Oek8O8n6&dq=avrupa%20birli%C4%9Fi&lr&hl=tr&pg=PR5#v=onepage&q=avrupa%20birli%C4%9Fi&f=false

Ünver, M., Canbay, C., & Özkan, H. B. (2011). *Kritik altyapıların Korunması.* Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı, Mayıs. Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

Ünver, M., Canbay, C., Mirzaoğlu, A. G., Çetinkaya, E., & Teknolojileri, B. (2011). *Uluslararası Kuruluşların Siber Güvenlik Faaliyetleri*. Ankara:Bilgi Teknolojileri ve İletişim Kurumu.

Tikk, E ve Oorn, R "Legal and Policy Evaluation: International Coordination of Prosecution and Prevention of Cyber Terrorism, " içinde Responses to Cyber Terrorism, edit. Centre of Excellence Defence Against Terrorism (Ankara: IOS Yayınları, 2008), 90-91.

**İnternet Kaynakları**

*Avrupa Birliği Türkiye Delegasyonu (2021).*

https://www.avrupa.info.tr/tr/etkilesimli-avrupa-haritasi-9

Erişim Tarihi: 26.11.2019

*Avrupa Birliği'nin Tarihsel Gelişimi* (2012).

http://www.tuicakademi.org/avrupa-birliginin-tarihsel-gelisimi/

Erişim Tarihi: 26.11.2019

*Avrupa Birliğinin Tarihçesi (2019).*

https://www.ab.gov.tr/105.html

Erişim Tarihi: 26.11.2019

*Avrupa Birliği Üyesi Ülkeler*

http://www.etonet.org.tr/ABBilgiMerkezi/Uye.aspx

Erişim Tarihi: 09.11.2020

*Siber Güvenlik Nedir?*

https://www.kaspersky.com.tr/resource-center/definitions/what-is-cyber-security

Erişim Tarihi: 24.03.2019

*NATO. (2010). NATO'yu Keşfedin*

https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20111116_Discover_NATO_TUR.pdf

Erişim Tarihi: 12.02.2019

*Altınışık, H. Hibrid Savaş ve Siber Saldırılar*

http://webcache.googleusercontent.com/search?q=cache:bHvUyQuekg4J:www.siberteror.org/siberteror2017/files/HalimAltinisik.pdf+&cd=5&hl=tr&ct=clnk&gl=tr

Erişim Tarihi: 01.10.2019

*Türkiye Cumhuriyeti Dışişleri Bakanlığı*

http://www.mfa.gov.tr/birlesmis-milletler-teskilati-ve-turkiye.tr.mfa

Erişim Tarihi: 22.05.2020

*National Cyber Security Masterplan(Summary) (2011) 8. 2*

https://afyonluoglu.org/PublicWebFiles/strategies/Asia/South%20Korea%202011%20National%20Cyber%20Security%20Masterplan-EN.pdf

Erişim Tarihi: 22.05.2020

*AUSCERT*

https://www.cybersecurityintelligence.com/auscert-46.html

Erişim Tarihi: 23.05.2020

*Birleşmiş Milletler (BM) Tarihi Olaylar (2021).*

https://www.tarihiolaylar.com/tarihi-olaylar/birlesmis-milletler-bm-183

Erişim Tarihi: 24.05.2020

*Birleşmiş Milletler, (2018).*

https://abdigm.meb.gov.tr/www/birlesmis-milletler/icerik/1089

Erişim Tarihi: 24.05.2020

*International Telecommunication Union: "Global Cybersecurity Index (GCI) 2017*

https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Erişim Tarihi: 27.05.2020

*Council Of Europe*

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

Erişim Tarihi: 07.06.2020

Committee of Experts on Terrorism (2003-2017)

https://www.coe.int/en/web/counter-terrorism/codexterErişim Tarihi: 07.06.2020

*Türkiye Büyük Millet Meclisi (2021)*

https://www.tbmm.gov.tr/ul_kom/akpm/genel_bilgi.htm

Erişim Tarihi: 29.06.2020

*İran En Güçlü Siber Ordulardan Birine Sahip*

https://tr.euronews.com/2019/03/07/iran-en-guclu-siber-ordularindan-birine-sahip

Erişim Tarihi: 03.07.2020

*Velayet 91 Uzmanlık Saha Tatbikatında Siber Saldırı Başarı İle Denendi, (2012)*

https://tr.abna24.com/service/iran/archive/2012/12/30/376766/story.html

Erişim Tarihi: 03.07.2020

*Kamu Güvenliği Kanada (2020)*

*https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cbr-scrt-tl/index-en.aspx*

Erişim Tarihi: 03.03.2021

*NATO'nun Siber Uzaydaki Rolü (2019)*

https://www.nato.int/docu/review/tr/articles/2019/02/12/natonun-siber-uzaydaki-rolue

Erişim Tarihi: 05.03.2021

Siber Bülten (2020)

*https://siberbulten.com/sektorel/trky/harvard-30-ulkenin-siber-gucunu-hesapladi*

Erişim Tarihi: 05.04.2021

Siber saldırılardan en çok etkilenen sektörler (2020)
*https://digitalage.com.tr/siber-saldirilardan-en-cok-etkilenen-sektorler/*
Erişim Tarihi: 05.04.2021
Sophos 2021 Tehdit Raporu Önümüzdeki Yılın Siber Saldırı Eğilimlerine Işık Tutuyor (2020)
https://www.bthaber.com/sophos-2021-tehdit-raporu-onumuzdeki-yilin-siber-saldiri-egilimlerine-isik-tutuyor/
Erişim Tarihi: 24.04.2021