T.C.

DÜZCE ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

TOPLAM KALİTE YÖNETİMİ

TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKALARI VE SİBER SALDIRILARIN ULUSLARARASI ETKİLERİ

YÜKSEK LİSANS

Özge ARSLAN

Düzce

Ekim, 2021

T.C.

DÜZCE ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

TOPLAM KALİTE YÖNETİMİ

TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKALARI VE SİBER SALDIRILARIN ULUSLARARASI ETKİLERİ

YÜKSEK LİSANS

Özge ARSLAN

Danışman: Zafer AKBAŞ

Düzce

Ekim, 2021

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün aşamalarda etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara kaynak gösterdiğimi ve bu kaynakları da kaynaklar listesine aldığımı, yine bu tezin çalışılması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığını beyan ederim.

Sosyal Bilimler Enstitüsü Müdürlüğüne;

Bu çalışma jürimiz tarafından Toplam Kalite Yönetimi Anabilim Dalında oy birliği / oy çokluğu ile YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Başkan

Üye

Üye

Üye

Onay

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

.. / .. / 2020

ÖZET

TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKALARI VE SİBER SALDIRILARIN ULUSLARARASI ETKİLERİ

Özge ARSLAN

Yüksek Lisans, Toplam Kalite Yönetimi Anabilim Dalı

Tez Danışmanı: Zafer AKBAŞ

Ekim 2021, 94 Sayfa

Siber güvenlik, her geçen gün daha büyük bir soruna dönüşen, yakın sayılabilecek bir geçmişe sahip bir olgudur. Teknolojik gelişmelerin geldiği nokta ve teknoloji kullanımının yaygınlaşması ile birlikte hem bireysel hem de ulusal bir önem taşımaya başlayan siber güvenlik olgusuna yönelik uluslararası arenada birçok çalışma gerçekleştirilmektedir. Çalışma kapsamında da siber saldırılardan etkilenen ülkeler olmak üzere önde gelen ülkelerin siber güvenlik politikaları ele alınacaktır. Bu amaçla ilk olarak güvenlik, ulusal güvenlik ve siber güvenlik olgularına yer verilecek alt başlıkları ile birlikte bu olgular ele alınacaktır. Bu başlıkların yanı sıra siber saldırı türleri, Türkiye'nin siber güvenlik politikalarına ve uluslararası siber güvenlik yaklaşımları ele alınarak yakın geçmişte yaşanmış saldırılar ve önde gelen ülkelerin siber güvenlik çalışmalarına yer verilecektir. Son olarak sonuç ve öneriler ile birlikte de çalışma tamamlanacaktır.

Anahtar Kelimeler: Siber güvenlik, Siber saldırı

ABSTRACT

TURKEY'S CYBER SECURITY POLICIES AND THE INTERNATIONAL EFFECTS OF CYBER ATTACKS

Özge ARSLAN

MSC, Department of Total Quality Management

Thesis Advisor: Zafer AKBAŞ

October 2021, 94 Page

Cyber security is a phenomenon with a relatively recent history, which is becoming a bigger problem day by day. With the point of technological developments and the wide spread use of technology, many studies are carried out in the international arena on the phenomenon of cyber security, which has started to have both in dividual and national importance. Within the scope of study ,upon leadıng countries, particularly those affected by cyber attacks will be discussed about cyber security policies. For this purpose, first of all, security, national security and cyber security phenomena will be discussed together with their sub-titles. In addition to these topics, types of cyber attacks,Dealt with Turkey's cyber security policies and international cyber security approachment, recent attacks and cyber security studies of leadıng countries will be debated. Finally, the study will be completed with conclusions and recommendations

Keywords: cybersecurity, cyberattack

İTHAF

Bu çalışmanın tüm aşamasında sonsuz desteği olan sabrıyla her zaman bana destek veren ve yol gösteren hocam Prof.Dr. ZaferAKBAŞ'a teşekkürlerimi sunarım. Ayrıca bana her zaman yardımcı olan ve yanımda olan eşim Hasan ARSLAN ve biricik oğlum Yiğit ARSLAN 'a ve tezimi son aşamaya getirmeye sağlamam için beni motive eden arkadaşım Ömer KARAKAŞ'a, eğitim hayatım boyunca maddi ve manevi desteklerini esirgemeyen aileme sonsuz teşekkürlerimi sunarım.

İÇİNDEKİLER

GİRİŞ

Teknolojik gelişmelerin artması ile birlikte internet, gündelik yaşamın bir parçası olmuş durumdadır. Bugün, bankacılık faaliyetlerinden mutfak alışverişine, eğitimden eğlenceye kadar hemen her alanda internet ortamına bir geçiş söz konusudur. Bu geçiş, insan hayatını kolaylaştırdığı ve hızlandırdığı gibi beraberinde çeşitli sorunları da getirmektedir. Bu sorunlardan birisi de güvenlik. Hemen her faaliyetin internet üzerinden gerçekleştirilebiliyor olması ve teknolojinin gündelik yaşamın bir parçası haline gelmiş olması bireysel ve ulusal neredeyse tüm bilgilerin internet ortamında yer almasına ve bu bilgilerin saklanmasına, hatta takip edilmesine olanak sağlamaktadır. Bu da hem bireysel bilgilerin hem de ulusal bilgilerin kötü niyetli kişi ya da kurumlar tarafından ele geçirilmesi riskini doğurmaktadır. Siber saldırı olarak adlandırılan bu kötü niyetli yaklaşımlar, doğrudan bilgileri ele geçirme, banka hesaplarına erişme ve benzeri birçok niyete bağlı olarak gerçekleştirilmektedir. Bu durum ülkelerin siber güvenlik tedbirleri almasını zorunlu hale getirirken, bir mücadeleyi de ortaya çıkartmaktadır. Çalışma kapsamında Türkiye'nin siber güvenlik politikaları nedir ve bu politikalar siber saldırılara karşı yeterli midir temel sorusu üzerinde durulmaktadır.

Çalışma kapsamında problem kısmında ifade edildiği üzere Türkiye'nin siber güvenlik politikaları ve bu politikaların siber saldırılara karşı yeterliliğinin belirlenmesi amaçlanmakta olup dünyanın önde gelen ülkelerinin siber güvenlik politikalarına ilişkin de incelemede bulunarak Türkiye'nin siber güvenlik politikalarını geliştirmesi adına öneriler getirilmesi hedeflenmektedir. Siber güvenlik, bugün gelinen noktada küresel bir sorun olup her ülke bu olgu üzerinde durarak politikalar geliştirmektedir. Çalışma kapsamında ortaya konulan bulgular küresel düzeyde verilen mücadeleye ve geliştirilen politikalara ilişkin bilgileri ortaya koymakla birlikte Türkiye'nin durumunu da tespit edecek, geliştirilebilir yanlara odaklanarak öneriler getirecektir.

Çalışma içerisinde karşılaştırmalı olarak geliştirilebilir yanların ortaya konulacak olması araştırmanın önemini oluştururken, bu çalışma ile birlikte literatürde konuya ilişkin çalışmalara çeşitlilik kazandırılacak olması, konuya ilişkin araştırmacılara yeni bir kaynak sunulacak olması ve gelecekte konuya ilişkin yapılan çalışmalara da fikir verecek olması araştırmanın önemini oluşturmaktadır.

Çalışma kapsamında konuya ilişkin literatür araştırması yapılmış olup konuya ilişkin kitap, makale, dergi vb. kaynaklardan yararlanılacaktır. Araştırma kapsamında elde yapılan araştırmalar ve faydalanılan kaynaklar araştırmanın sınırlılıklarını oluşturmaktadır.

BİRİNCİ BÖLÜM

KAVRAMSAL BOYUTUYLA GÜVENLİK

1.1. Güvenlik ve Ulusal Güvenlik

1.1.1. Güvenlik ve Ulusal Güvenlik Kavramı

Güvenlik kavramı Batı dillerinde kökeni Latinceye dayanan "securitas" (emniyet) kelimesinden türetilerek kullanılmaktadır. Bu kelimeden türeyen sécurité yani güvenlik kavramı ise; garanti, güven ve huzur temin etmek, barış, emniyet gibi çağrışımlara anlam itibariyle sahiptir (Bal, 2003: 115).

Kavramın ortaya çıkışı ve kullanımında dikkat çeken nokta zaman içerisinde yaşadığı dönüşümdür. Kavram XV. yüzyılda eski Fransızca seurte, seürte kelimelerinden türetilip; "sığınak, sözünü tutma, temin etme, korkunun olmayışı" gibi çeşitli anlamlarda kullanılır olmuştur. Ancak; XVI. yüzyıla gelindiğinde dönemin Fransa'sında, bir sosyal grubun getireceği tehlikeden korunmuş olmak halini ifade etmeye başlamıştır. Diğer taraftan polis kelimesi de orijinal Fransızca kullanımında policie kelimesinden türetilip Kıta Avrupa'sındaki diğer dillerde de benzer şekilde kullanılmıştır. Bunlardan bazıları "policei, pollicei, policey, pollizei"dır (Neocleous, 2006: 1).Kavram tıpkı güvenlik kelimesinde olduğu gibi XV. yüzyılda ortaya çıkmış, iyi düzenin ve refahın korunması adına bir topluluğun yasal ve idari olarak düzenlenmesi fikirlerine işaret etmiştir (Bauman, 1996: 112).

Birbirine fiili ve anlamsal olarak yakın olan bu iki kavramın aynı bölgede eş zamanlı olarak ortaya çıkması dilbilimde oluşmuş bir tesadüfün sonucu olamaz. Özellikle güvenlik kavramının içeriksel olarak yaşadığı farklılaşmanın gösterdiği, kavramın ortaya çıkışı, gelişimi ve kullanımı tarihsel ve toplumsal süreçlerin dâhilinde ve hatta belirleyiciliğinde meydana gelmiştir. Bu anlamıyla güvenlik alanına dair yapılacak bir çalışmada kullanılması gereken temel yol; güvenliğin ve onu çevreleyen kavramların tarihsel bir perspektifle ve sosyolojik bir bakış açısıyla değerlendirilmesi olmalıdır.

İnsanlık tarihinin güvenlik kaygılı geliştirdiği politikalar ya da uğraşlar da, maddeden ve toplumsal süreçlerden bağımsız bireysel olarak ele alınamaz (Harvey, 2003: 18).

Modern yani gelişmiş dünyanın ortaya çıkması ve kurumsallaşması insanlık tarihinde büyük altüst oluşlarla birlikte anılır. Kıta Avrupa'sında başlayan ve ardından tüm dünyayı etkisi altına alan değişim verili düzenin kurucu öğelerini ve yapısını değiştirmiştir. Emniyet, güvenlik, güvende olma hali gibi tanımlamalar açısından ise; bu sorunlar modern öncesi dönemde sosyal ilişkiler ve örgütlenmeler içinde anlam kazanmakta ve çözülmektedir. Modern dünyanın oluşumu bu durumu değiştirmiştir (Polanyi, 2000: 87).

Merkezi ve bürokratik devletin kurulması, mülkiyet esaslı toplumsal ilişkilerin oluşumu, yurttaş-devlet ilişkisinin asli belirleyen haline gelmesi, emeğin özgürleşmesi, şehirleşme gibi birçok bağımsız değişken kişinin ve toplumun güvenlik sorununda etkili olmaya başlamıştır. Modern dünyanın oluşumuna paralel olarak beliren bu ilişki ve süreçler güvenlik sorununu birey ve toplum açısından ne yönde etkileme düzeyinin araştırılması önem kazanmaktadır. Güvende olmaya dair geliştirilen temel kriterler, güvensizlik yaratan unsurlar, tabakalı toplumsal yapıdan sınıflı toplumsal yapıya geçişin sosyal güvence sorununu etkilemesi, sosyal güvencesizlik ile toplumsal tehlikeler arasındaki bağların kurulabilirliği, toplumsal yapıya yön veren siyasal ve ekonomik örgütlenmelerin güvenlik sorununu çözmek adına geliştirebileceği mekanizmalar, iç güvenlik sorununda, sorunun tarafı olan polisin ortaya çıkış nedeni, görev alanı incelenecektir.

Feodalizmin çözülüşüyle birlikte başlayan süreç en genel tanımıyla kapitalist iktisadi ilişkilerin ve modern ulus-devletin oluşumu şeklinde tanımlanabilir. Farklı öncüllerle ve farklı dönemlerde açığa çıkan, bir diğeri ötekine üstünlük sağlayarak değişen yeni toplumsal ve iktisadi ilişki biçimleri bugün modern dünya olarak anılan görünümün oluşumunu sağlamıştır. Bir önceki döneme ait olan tüm sosyal, siyasal ve ekonomik örgütlenişler modern dünyayla birlikte farklılaşmıştır.

Orta çağın sonuna kadar ekonomik ilişkilerde piyasalar önemli bir rol oynamamaktadır ve hatta ekonomik faaliyet ile tercihler ekonomi dışındaki nedenlere bağlı olarak şekillenmiştir. Bireysel ekonomik çıkarın yerine sosyal saygınlığı kazanmak; şef, despot ya da feodal bey gibi aktörlerle olan bağımlılık ilişkileri ve dışa kapalı ilişkiler ekonomik ve sosyal yaşamın başat unsurlarıdır (Polanyi, 2000: 90).

Karşılıklı güven ve kolektif sorumluluğa dayanan modern öncesi ilişkilerde toplumsal düzenin sağlayıcısı olarak bu karşılıklılık ilkesi esas alınmaktadır. Modern öncesi toplumda birey bürokratik ya da merkezi bir aidiyet tanımlaması içinde değildir. Dolayısıyla bireyin emniyeti sosyallikler ve statüler aracılığıyla sağlanmıştır. Bu karşılıklılık ilişkileri cemaatin her bir üyesinin birbiri üzerindeki sıkı denetimi sonucunu doğursa da, merkezi ve bürokratik bir denetim söz konusu değildir. Bahsedilen ilişkiler modern dünyanın ürünü olan ekonomik, sosyal ve siyasal farklılaşma ile çözülmüştür.

Modern dünyanın karşılıklılık ve tabiiyet ilişkileri farklı formlarda vücut bulmuştur. Modern toplumsal düzen iki ideal üzerine kurulmuştur. Toplumsal düzen, insanlar arasında kurulacak karşılıklı hak ve yükümlülüklerle sağlanacaktır. Burada herkese düşen temel görev; hayat ve mülkiyet hakkının korunmasıdır. Bu ise ancak müşterek güvenliğin sağlandığı bir toplumda kurulabilir. Bu yönüyle; güvenlik ve ekonomik refah modern toplumsal dünyanın temel idealleridir (Castel, 2004: 16).

XVII. yüzyılla birlikte piyasalara egemen olan aktörler ekonomik ve siyasal olanın yeniden tanımlanmasını istemişlerdir. Bu talep dönemin gündemini belirleyen temel kavramların özel, mülkiyet, yasa ve devlet olması sonucunu doğurmuştur. Geleneksel ilişkilerin köklü etkisinden ve gücünden kurtulmak isteyen aktörler aynı zamanda ekonomik aktivasyonların da sahipleridir. Bu bağlamda devletin yetkilerinin düzenlenmesi yasa ve yönetmelikler aracılığıyla toplumsal işleyişe müdahale edilmesi gündeme gelmiştir (Ercan, 2001: 102).

Kendi kendine işleyen bir piyasa düzeninin oluşturulması ve idari örgütlenmenin de bu işleyişi tamamlayıcı şekilde yeniden kurgulanması, piyasa mekanizmasının işleyişi açısından kaçınılmaz olmuştur. Bu yüzyıl ve bir sonraki yüzyıl aynı zamanda üretim ilişkilerindeki aktörlerin ve ilişkilerin köklü değişimler yaşadığı yüzyıldır. Emeğin özgürleşmesi ve özgür emek piyasasının oluşumu sanayi kapitalizminin ürünü olarak ortaya çıkmıştır. Çalışmanın ve emeğin bir önceki dönemden farklı olarak piyasa ilişkileri içerisinde değişim değeri ile ölçülebilir ve sınıflandırılabilir olması özgür emeğin ortaya çıkışını kısaca tanımlar.

İnsanın çalışmasına dair üretilen sosyal ve psikolojik olumsallıklar toplumsal ilişkilerde bir baskı unsuru olmuştur. Bunun ötesinde yasal olarak olmasa da fiili

olarak kişinin bu ilişkilerde yer alması zorunluluğu kapitalist serbestleşme ve zorunluluk ilişkilerini belirleyen temel dinamiktir (Aykut, 2006: 51).

Piyasanın görünmez eli ve işleyişi felsefesi dâhilinde, eşit ve özgür kabul edilen bireylerin birincil hak ve talepleri ise mülkiyet edinme ve onu koruyacak mekanizmalara sahip olabilme şeklinde tanımlanmıştır. Ortaya çıkan bu yeni durum uyarınca piyasada emeğini satma özgürlüğü olan bireyin mülkiyet edinme ve onun tasarrufunu sağlama özgürlüğü de olmalıdır. Bahsedilen bu hakların doğuştan eşit olan bireylerin doğal haklarıdır. Ancak bu kurgu birey, toplum ve piyasa açısından önemli bir problemi de ortaya çıkarmıştır. Bu problem ise edinilen mülkiyetin korunması ve emniyetine ilişkindir. Birey eksenli düşüncenin temel yaklaşımı ve argümanı olan insanın varoluşsal olarak güvenilmez bir varlık olduğuna ilişkin değerlendirmeler, güvenlik sorununun toplumsalın üstünde bir alanda çözülmesi önerisini beraberinde getirmiştir. Doğal durumunda çıkarcı, bencil ve menfaatlerinin peşinde olan hırslı bireyler her an birbirlerine zarar verme potansiyelini taşımaktadırlar dolayısıyla bir üst iradenin toplumsal denetimi kaçınılmazdır (Aykut, 2006: 52). Toplumun ortak çıkarı da ancak bu şekilde sağlanacaktır. Bireyci menfaat toplumunda her bireyin mülkiyet hakkının korunması toplumsal refahın ve huzurun sağlanmasını beraberinde getirecektir (Castel, 2004: 22).

Bu yaklaşıma göre devlet denilen organizasyonun temel işlevi ve hatta varlık nedeni, bireyin yaşam ve mülkiyet hakkını korumaktır. Yine aynı yaklaşımla kendisine tabi olan bireyler karşısında eşit olacağı varsayılan devletin temel müdahale alanı, bu doğal hakların korunması çerçevesinde uygun görülmüştür (Köker, 2003: 84).

Kapitalist toplumsal ilişkiler içindeki hukuk ve devlet fikrinin özel mülkiyetle olan ilişkisi bu yaklaşım çerçevesinde kurulmuştur. Devlet-yurttaş-özel mülkiyet ilişkileri çerçevesinde iktidarla kurulan yatay tabiiyet ilişkileri modern toplumda nesnellik nosyonu aracılığıyla, devlet-yurttaş ilişkilerinde de mutlak eşitlik ve hukuk kavramları aracılığıyla meşruluk kazanarak gizli bir duruma gelmiştir. Modern ulus-devletin tanımlanmasında sıklıkla rastlanan şiddet tekelini elinde tutan tek meşru güç olma niteliği kurulan bu sözleşmede belirlenmiştir. Devletin görevi huzurun, güvenin ve normun tayini olarak tanımlanmıştır (Schmitt, 2006: 65).

Bu doğrultuda devlet ya da onu temsilen oluşturulan yapılar toplumsal düzenin koruyucu unsurları olarak kabul edilmiştir. Modern toplumun güvenlik projelerini ve uygulamalarını oluşturan silahlı bürokrasi ordu ve polis olarak ortaya çıkmıştır.

Modern devletin oluşumuyla birlikte anılan güvenlik sorunu genel hatlarıyla yukarıda bahsedildiği şekliyle belirmiştir. Ancak modern dönemlerin bir diğer tanımlaması olan sınıflı toplumlarda güvenliğin oluşma ve gelişim koşulları, sınıflar arası hiyerarşik ilişkiler çerçevesinde de değerlendirilebilir. Emeğin özgürleşmesine koşut olarak oluşan ücretliler toplumunda emniyetin ya da emniyetsizliğin nasıl telakki edildiği ve yaşanan dönüşüme koşut olarak tehlikeli olarak addedilen süreç, durum ve aktörlerin neler olduğu bu bakış açısıyla da irdelenebilir. Bu doğrultuda kapitalist sistemin yarattığı yeni toplumsal ilişkiler, değerler ve tanımlamalar yol gösterici olabilir.

Egemen üretim ilişkileri ve bölüşüm mekanizmaları toplumsal yapının ana gövdesini belirlemektedir. Toplumsal yapıyı ve nitelendirmeyi belirleyen temel sıfatlandırmalar bu ilişkilerden yola çıkılarak geliştirilir. Bu anlamda statü ve geleneksel hiyerarşilere bağlı olarak gelişen tabakalı toplumlardan, sınıflı kapitalist topluma geçiş önemli toplumsal yapıda önemli bir kırılmayı doğurmuştur. Özellikle sanayi kapitalizminin gelişimiyle birlikte geleneksel üretim ilişkilerinde yaşanan değişim sadece ekonomik olanda değil, onun ötesinde sosyal ve siyasal olanda da radikal bir dönüşüme sebep olmuştur.

Toplumun tümü kendi kendini düzenleyen piyasalarca şekillenmeye başlamıştır. Kapitalizmin hızlı gelişmesine bağlı olarak şehirlerin sınırları da hızla büyümüştür. Şehirsel alan yeni toplumsal ilişkilerin belirleyici mekânı olmuş buna bağlı olarak şehirleşme denilen süreç bir ölçüt olarak kabul edilmeye başlamıştır. Bunun yanı sıra emeğin piyasada alınıp satılabilen bir ürüne dönüşmesiyle birlikte en genel haliyle ücretliler ve güvencesizler olarak tanımlanabilecek toplumsal kesimler ortaya çıkmıştır.

Bu kesimlerin varlığı en açık şekilde şehirsel alanda hissedilir olmuştur. Bu yönüyle kapitalist şehirleşme süreçleri toplumsal adalete ilişkin sorunların en çok yansıdığı ve temsil edildiği mekândır (Şengül, 2001: 9).

Geleneksel toplumsal ilişkilerin çözülmesi, yeni aidiyet ve tabiiyet ilişkilerinin kurulması, makineleşmeye bağlı olarak artan işsizlik ve toprak mülkiyetinin yeniden düzenlenmesi, kırsal alandaki nüfusun şehirlere gelişi, rekabete dayalı ilişkilerde koruyucu sosyal mekanizmaların olmaması gibi faktörler; şehirde emniyetsiz olduğu düşünülen yaşam biçimlerinin ve görünümlerin ortaya çıkmasına yol açmıştır. Formel olarak ücretli ekonomik ilişkiler içerisinde yer almayan, devletle kurdukları ilişkide de yurttaş olarak tanımlanamayacak kesimler toplumsal düzene ve refaha zarar verecek gruplar olarak belirlenmiştir.

Bireylerin toplumda iyi yurttaş olmaya dair kurulan durumlar haricinde marjinal olarak nitelendirilebilecek kesimlerin sayıca hızla artması toplumsal yaşamda iç güvensizlik kaynağı olarak görülmelerine yol açmıştır. İktisadi disiplinin içerisinde yer alamayan bu kesimler sosyal disiplinin de içinde yer almamaktadırlar.

Modern devletin ve piyasa ekonomisinin işleyişi açısından bilinir ve tanımlanabilir olma niteliğini taşıyamayan bu kesimler fabrika ya da bürokrasi tarafından denetime tabi tutulamadıkları ve geleneksel ilişkileri temsil ettikleri için iç tehdit olarak görülmüşlerdir. Ancak kapitalizm bu döneminde ayaklanmaya ve toplumsal düzensizliğe tahammül edemeyeceği için bu kesimlerin kontrol altında tutulması zaruri olmuştur. Sosyal ve siyasal olarak da piyasanın ihtiyaçlarına göre şekillenmiş yeni toplumsal tahayyülün düzensizlik, kabadayılık ve kontrolsüz şiddet gibi nizamı bozacak her türlü duruma karşı tahammülü bundan sonraki dönemde sınırlı olmuştur.

Sınıflı toplumlarda, mülkiyete dayalı toplumsal düzenin korunması kişilerin güvencelerinin ancak mülkiyetlerinin güvence altında olmasıyla sağlanır olması aslında güvencesizlik sorunu olarak yorumlanabilir. Çalışan yurttaşların bağımsız bireyler olabileceği idealinden hareketle bireylerin bağımsızlığını koruması ve sosyal risklere karşı güvence altında olması ancak mülkiyetin en yetkin güvence poliçesi olarak kabul edilmesini beraberinde getirmiştir (Castel, 2004: 23).

Ancak modern güvensizliğin işaret ettiği güvence yokluğu durumu, yani güvence arayışı tek başına güvencesizliği beraberinde getirmektedir. Emniyetsizlik korkusunu yaşayan özneler böylelikle nesneleştirilmektedir. Sonucunda sınıflı toplumlar toplumsal güvensizliği yaratan unsurları içinde barındırmaktadır, bunlar

ise sistemin çelişkileri ve çıkmazları olarak toplumsal yaşamda vücut bulmaktadır. Sanayi kapitalizminin şehirde yarattığı tüm çelişki ve çıkmazlara koşut olarak şehirsel mekân daha önce aktarıldığı üzere toplumsal adaletsizliğin ve eşitsizliğin fiziksel olarak yüzeyde ve açıkta olduğu alandır.

Ekonomik çıkarın tek başına geçerli olduğu toplumsal ilişkiler yoksulluk, işsizlik, informel iş ağlarında yer alma zorunluluğu, güvencesizlik gibi sorunları gündeme getirmiştir. Modern devletin iki güvenlik kurumu olan ordu ve polis görev tanımı anlamında birbirinden farklılaşmış modern güvenlik aktörleridir. Polis ordudan faklı olarak iç güvenlikten sorumlu garantör kurum olarak kurumsallaşmıştır. Polislik işi ise yoksulluğun ve marjinal kitlelerin idaresini içermiştir. Özellikle şehirsel alanda ortaya çıkan nizam dışı ve başıboş ilişkileri yani alt sınıfların yaşamlarının kontrol ve denetimini sağlamak niyetiyle polislik kurumu ve faaliyeti devlet-yurttaş-özel mülkiyet ilişkileri içerisinde olgunlaşmıştır. Bu anlamıyla özellikle kamu düzeni polisliği; toplumun üzerinde yükseldiği yeni sınıfsal ilişkilerin ve kültürün ürünüdür (Erkut, 2004: 18).

Feodalizmin çözülüşünden sonra; kapitalizmin sosyal, siyasal ve iktisadi süreçlerde egemen biçim olması geleneksel olarak tanımlanan tüm ilişki ağlarını ve tarzları farklılaştırmıştır. Şehrin bir mekân olmasının ötesinde içerdiği anlam ve ilişkiler yeni sisteme paralel olarak biçimlenmiştir.

Şehir denilen mekân sosyal ve siyasal süreçlerin ürünü olarak şekillenmiştir. Bu anlamıyla şehirselliğe dâhil edilerek tanımlanan birçok problem modern dünyanın, modern dünyaya ait birçok çelişkide birer şehir sorunu olarak görülmüştür. Şehrin güvenliğinin ve refahının sağlanması amacıyla kurulan polislik kurumu modern dünyada genel refah sisteminin merkezinde bulunmaktadır (Bedük, 2009: 62).

Devletin sokaktaki gücünü temsil eden polis; takdir ve erk yetkisiyle muhafızlık görevini üstlenmiştir ve gündelik düzeydeki koruma ya da denetleme yetkisiyle devleti birçok kurumdan daha fazla temsil etmiştir. Modern polisin gücü kamusallığından ve merkezi olarak atanan uzmanlaşmış bir yapıya sahip olmasından gelmektedir. Bu yüzden polise sokakta tanınan yetkiler oldukça manidardır. Sokağın

kamuyu temsil ettiği varsayılırsa; kamuya ait tüm girdi ve çıktıların hesabı polis tarafından tutulmaktadır.

1.1.2. Ulusal Güvenlik Faktörleri

Ulusal güvenlik faktörlerini etkileyen birçok faktörün varlığından söz etmek mümkündür. Özellikle günümüz küresel dünyasında ülkeler, içe kapanık bir yapıya sahip olamamaktadır. Bu da iç faktörlerin yanı sıra dış faktörlerin de ulusal güvenliği tehdit etmesine zemin hazırlamaktadır. Buna bağlı olarak birçok farklı isimlendirmede bulunmak mümkün olsa da ulusal güvenlik faktörlerini iki alt başlıkta ele almak mümkündür. Bu başlıklar şunlardır (Bedir, 2019: 30):

1. Ortam
2. Çevre

Bu faktörlerin kapsamlarını ve etkilerini anlayabilmek adına alt başlıklar halinde ele almakta fayda vardır.

1.1.2.1. Ortam

Ortam, en yalın hali ile ülkelerin içerisindeki bulundukları siyasal ve ekonomik durumdur. Siyasal ve ekonomik durum dinamik bir yapıya sahip olup, sürekli bir değişim içerisindedir. Bu doğrultuda ortamı kendi içerisinde ikiye ayırarak iç ortam ve dış ortam şeklinde ele almak mümkündür.

İç ortam, ülkelerin ulusal sınırları içerisinde meydana gelen değişimlere bağlı olarak ortaya çıkan siyasal ve ekonomik durum olarak özetlenebilmektedir. Her ne kadar siyasal ve ekonomik olgular ortamı oluşturan temel faktörler olmakla birlikte toplumsal olaylar, askeri gelişmeler ve benzeri unsurlar da ortamı oluşturmaktadır. Her ülke, içerisindeki bulunduğu koşullara bağlı olarak siyasal adımlar atmaktadır. Dolayısıyla ulusal sınırlar içerisinde meydana gelen değişimler yeni kararların alınmasına neden olduğu gibi mevcut düzenin de değişmesine yol açabilmektedir. Bu durumda mevcut düzende sağlanmış olan ulusal güvenlik, yeterliliğini yitirebilmekte ve yeni önlemler alınması zorunlu hale gelebilmektedir. Bu da nihayetinde ulusal güvenliğin etkilenmesine ve yeni adımlar atılmasına sebep olmaktadır (Arı, 1999: 183).

Devlet yönetimlerinin asli görevi toplumsal düzeni korumak, toplumun can ve mal güvenliğini sağlamaktır. Her devlet yönetimi, en yoğun mesaiyi ulusal

güvenlik konusuna ayırmaktadır. Ulusal güvenliğin sorun barındırmadığı bir yapı içerisinde ise yönetimler mesailerini dış siyaset, ekonomik gelişim, toplumsal refahın arttırılması gibi diğer önemli hususlara ayırabilmektedir. Dolayısıyla iç güvenliğin sağlanması temel öncelik olup diğer tüm unsurlar iç güvenlikten sonra gelmektedir. Bu denli önemli bir hususun da ihmal edilmesi ya da arka planda bırakılması mümkün olmamaktadır.

Toplumsal huzurun sağlandığı bir yapıda ulusal güvenliğin iç ortam nedeni ile tehdit edilmesi olası bir durum değildir. Devlet, asli görevlerinden olan toplumun huzur ve güvenliğini sağladığı, toplumsal düzeni koruduğu, ekonomik gelişmelerin pozitif bir seyirde ilerlediği, bireysel ve toplumsal özgürlüklerin genişletildiği ve diğer toplum refahını arttıran adımların atıldığı bir süreçte iç ortama bağlı ulusal güvenlik tehditlerinin ortaya çıkması için bir neden de kalmamaktadır.

Dış ortam ise ülkelerin ulusal sınırları dışında meydana gelen gelişmelerdir. Her ülke, birçok ülke ile sınır komşusu konumundadır. Dolayısıyla özellikle sınır komşularında meydana gelen gelişmeler, ülkelerin ulusal güvenliklerini tehdit edebilmektedir (Karakoç, 2008: 57). Günümüzde bu duruma verilebilecek en güncel örnek Suriye'deki gelişmelerdir. Türkiye ile Suriye sınır komşusu ülkeler olup, yıllardır süre gelen iç savaş neticesinde bugün Suriye'de ulusal güvenlikten söz etmek mümkün değildir. Buna bağlı olarak sınırın diğer tarafında meydana gelen gelişmeler, Türkiye'nin güvenliğine de tehdit unsuru konumundadır. Benzer şekilde Tunus'ta başlayan ve hızla diğer Arap ülkelerine de yayılan gösteriler sonucunda "Arap Baharı" adı verilen olaylar meydana gelmiştir. Dolayısıyla ulusal güvenliği tek başına bir iç mesele olarak ele almak mümkün değildir.

1.1.2.2. Çevre

Ulusal güvenliği tehdit eden bir diğer ana faktör çevredir. Çevre de tıpkı ortam gibi kendi içerisinde ikiye ayrılmakta olup fiziki çevre ve beşeri çevre şeklinde ele alınmaktadır.

Fiziki çevre faktörlerini de kendi içerisinde birçok alt başlığa ayırmak mümkündür. Bu faktörlerden ilki iklimdir. Her ülke, sahip olduğu iklim doğrultusunda tarım ve hayvancılık alanlarında gelişim göstermektedir. Bir ülkenin iklimi tarım ve hayvancılığa ne kadar uygun ise ülkenin gıda alanında dışa

bağımlılığı da o kadar azalmaktadır. Bu da ülkenin ulusal güvenlik alanında taşıdığı risklerin azalmasına neden olmaktadır. Her ne kadar teknolojik gelişmelerle birlikte doğal olmayan yollardan da tarım faaliyetlerinde bulunmak mümkün hale gelse de iklim hala ülkelerin tarım ve hayvancılık alanındaki temel belirleyici konumundadır (Sönmezoğlu, 2014: 634).

Fiziki çevre faktörleri içerisindeki bir diğer önemli faktör denizdir. Deniz ve beraberinde su günümüzdeki en önemli kaynakların başında gelmektedir. Dolayısıyla ülkenin coğrafi konumunun denize sınırının bulunması ya da denize ulaşım mesafesi, ülkelerin ulusal güvenliklerini etkileyen çevre faktörü olarak ön plana çıkmaktadır. Denize kıyısı bulunan ülkeler, kıta sahanlığı elde ederek uluslararası siyasette çok daha etkin bir hale gelmektedir. Bununla birlikte denize kıyının bulunması yaz turizmi, balıkçılık, deniz taşımacılığı gibi birçok yan unsuru da etkilemektedir. Denize kıyısı olan ülkeler denizden gelebilecek tehditlere karşı da tedbirini alma zorunluluğunu taşımanın yanı sıra sunduğu avantajlarla da gelişme kaydetmektedir (Bedir, 2019: 34).

Bir diğer fiziksel çevre faktörü mevkidir. Coğrafi konumun bir uzantısı olan mevki faktörü ülkelerin sahip oldukları jeopolitik öneme bağlıdır. Coğrafi konumdan farklı olarak jeopolitik konum daha dinamik bir yapıya sahiptir. Geçmişte ülkeler için büyük önem taşıyan bir bölge, yaşanan gelişmeler sonucunda eski önemini yitirebilmekte ya da önemsiz olan bir bölge çok daha önemli bir hale gelebilmektedir. Yaşanan bu değişim de doğrudan ulusal güvenlik tehditlerinin azalmasına ya da artmasına neden olmaktadır.

Ulusal güvenliği etkileyen bir diğer fiziksel çevre faktörü nehirlerdir. Nehirler de tıpkı denizler gibi önemli bir su kaynağı olmakla birlikte uluslararası rolü de bulunmaktadır. Aynı denize kıyısı olan birçok ülke bulunmaktadır. Karadeniz ve Akdeniz bu tanıma en uygun örnekler arasında yer almaktadır. Bu da beraberinde kıta sahanlığı sorununa neden olmaktadır. Nehirler ise bir ülkede doğup başka bir ülkede son bulabilmektedir. Bir başka ifade ile bir nehir birden fazla ülkenin ulusal sınırları içerisinde yer alabilmektedir. Bu da uluslararası sorunlara yol açabilmektedir. Almanya ve Hollanda sınırlarından geçen Ren Nehri, su taşımacılığına ilişkin birçok soruna neden olmuş ve uluslararası platforma da

taşınmıştır. Benzer şekilde Türkiye'nin komşuları olarak Irak ya da Suriye ile de benzer durumlardan söz etmek mümkündür (Külekçi, vd. 2002: 396).

Fiziksel çevre faktörlerinden bir diğeri doğal kaynaklardır. Doğal kaynaklar, ülkelerin gelişmişlik düzeyleri üzerinde doğrudan belirleyici olduğu gibi diğer ülkelerin o ülkeye bakış açısında da kilit rol oynamaktadır. Bugün Suriye'de ortaya çıkan sorunların temeline inildiğinde Suriye'nin sahip olduğu petrol yataklarının önemli bir yer tuttuğu görülmektedir. Benzer şekilde Venezuela'da yaşanan, ya da yakın geçmişte Irak'ta yaşanan sorunlar da yine ülkelerin sahip oldukları doğal kaynaklara dayanmaktadır. Ülkeler, şüphesiz doğal kaynaklarla birlikte ekonomik güçlerini arttırmakta ve hem ulusal güvenliklerini geliştirmekte hem de uluslararası siyasetteki etkinliklerini arttırmaktadır. Buna karşın ülkeler yeteri kadar gelişim gösteremediğinde, kendilerine göre daha gelişmiş ülkeler tarafından doğrudan hedef haline gelebilmektedir ki bu da ulusal güvenliğe yönelik tehditlerinin artmasına neden olmaktadır.

Fiziksel çevre faktörleri içerisindeki son faktör topogrofik yapıdır. Topografik yapı özünde ülke içerisindeki iletişim ve ulaşım kanalları üzerinde etkili olan bir faktördür. İletişim ve ulaşım kanallarının gelişimi düşük olan bir ülke içerisinde ulusal güvenlik tehditlerinin daha fazla olduğundan söz etmek mümkündür. Bir örnek vermek gerekir ise İngiltere, topografik yapı itibari ile son derece uygun bir konuma sahip iken Balkanlarda yer alan ülkeler topografik yapı itibari ile birçok zorlukla karşı karşıya kalmaktadır. Rusya'nın sahip olduğu topografik yapı da tıpkı Balkanlar gibi olumsuz duruma bir örnek oluşturmaktadır. Rusya, sahip olduğu coğrafi konum ve yüz ölçümü itibari ile son derece zorlayıcı bir ülkedir. Sahip olunan iklim koşulları da dikkate alındığında ulusal güvenliğin sağlanmasının ne denli güç olduğu çok daha net anlaşılmaktadır. Şüphesiz bu durumun Rusya açısından olumsuz yanıdır. Olumlu yönden bakıldığında ise özellikle İkinci Dünya Savaşı'nın kaybedilmemesinde sahip olunan bu topografik yapının rolü büyüktür. Askeri ve siyasi olarak Rusya'ya göre çok daha güçlü durumda olan Almanya, Rus askerleri kadar Rusya'nın fiziksel koşulları ile de mücadele etmek zorunda kalmıştır. Yürütülen yanlış stratejilerle de birlikte savaş kaybedilmiş, belki de dünya siyasetinde çok farklı bir senaryonun ortaya çıkması sağlanmıştır (Sönmezoğlu, 2014: 646).

Ulusal güvenliği tehdit eden çevre faktörleri fiziksel çevre ve beşeri çevre olarak ikiye ayrılmıştır. Beşeri çevre ise adından da anlaşılacağı üzere ülkelerin sahip oldukları topluma göre ortaya çıkan unsurlardır. Özellikle 18. yüzyılın sonlarından itibaren milliyetçilik akımı dünya siyasetinde belirleyici kavramlardan biri haline gelmiştir. Bugün de çok uluslu ülkelere sıkça rastlamak mümkündür. Nitekim Birinci Dünya Savaşı'nın temel nedenlerinden biri ülkelerin çok uluslu yapısı iken İkinci Dünya Savaşı'nın temel nedenlerinden biri de milliyetçilik akımının bir uzantısı olarak "üstün ırk" algısı olmuştur.

Bu genel girişin ardından beşeri çevre faktörlerini oluşturan unsurları tek tek ele almak gerekir ise ilk olarak nüfus ön plana çıkmaktadır. Nüfus, ülkeler için önemli bir güç olabilmektedir. Özellikle askeri yapı içerisinde kara gücü adına nüfusun fazlalığı ülkeler için bir güç haline dönüşmektedir. Örnek vermek gerekir ise 80 milyonun üzerinde nüfusa sahip olan Türkiye ile 3 milyonun üzerinde nüfusa sahip olan Gürcistan'ın eşit kara gücüne sahip olduğuna söz etmek mümkün değildir. İki ülkenin askere çağırabileceği nüfus arasında derin bir uçurum söz konusudur (Bedir, 2019: 37).

Beşeri çevre içerisindeki bir diğer faktör ülke nüfusunun etnik yapısıdır. Ülkelerin özellikle çok uluslu bir yapıya sahip olmalarındaki artış ile birlikte farklı etnik kesimden ya da farklı dini inanıştan nüfus yoğunluklarının aynı ülke sınırları içerisinde sıklıkla yer aldığı görülmektedir. Bu da ulusal birlik ve beraberlik duygusunun gelişimini olumsuz etkilediği gibi toplumsa çatışmaların gerçekleşme olasılığını da arttırmaktadır.

1.1.3. Ulusal Güvenlik Politikaları

Küreselleşen dünya ile birlikte ülkeler arası sınırlar da kâğıt üstünde olmasa da ortadan kalkmış bir durumdadır. Geçmiş dönemde ulusal güvenlik denildiğinde akla sınırlar içerisindeki toprak bütünlüğünün korunması gelirken, günümüzde siyasi gücün sahip olunan askeri güçten ziyade masa başında sahip olunan güce bağlı olmasından dolayı ulusal güvenlik olgusuna ilişkin algı da değişmiştir. Şüphesiz ulusal güvenlik, bugün hala iç güvenliğin sağlanması ve sınırların korunmasını içermektedir ancak kapsamı genişlemiş durumdadır. Ulusal güvenlik olgusu, temelinde can ve mal güvenliğinin sağlanmasını kapsamakla birlikte günümüzde

uluslararası itibar ve ekonomi olguları ile de yakından ilişkili bir hale gelmiştir (Tezkan, 2000: 19).

Günümüz toplumsal yaşamı ve siyasal ortamı içerisinde ulusal güvenlik olgusunun iç tehditler ve dış tehditler şeklinde sınıflandırılarak ayrı ayrı ele alınması mümkün görünmemektedir. Bugün gelinen noktada, kâğıt üstünde olmasa da küreselleşme ile birlikte sınırların ortadan kalkmış olması iç güvenlik ve dış güvenlik ya da iç tehdit ve dış tehdit kavramlarının bir arada ele alınmasına neden olmaktadır. Değişen koşullarla birlikte ulusal güvenlik olgusu askeri güçten ve iç tehditlerden koparak ekonomik ve siyasal tehditlerle de bir arada ele alınan bir olgu haline gelmiştir. Toplumun can ve mal güvenliğine yönelik bir tehdit olmamasına karşın siyasal ve ekonomik alanda ortaya çıkan tehditler de ulusal güvenliğin konusu olup ulusal güvenliği tehdit eden hususlardan biridir.

Ulusal güvenlik olgusunun kapsamının genişlemesi ile birlikte ulusal güvenlik politikaları içerisinde istihbarat sistemlerinin önemi ve rolü de genişlemiştir. Bugün çok daha geniş çaplı istihbarat sistemlerine ihtiyaç duyulurken, doğru analiz ve yorumlamaların önemi de çok daha kritik bir konumdadır (Tezkan, 2000: 20).

Elbette ulusal güvenlik olgusuna yönelik farklı algılar bulunmakla birlikte dünya genelinde ağırlıklı olarak askeri tehdit unsurlarının yanında siyasi ve ekonomik tehdit unsurlarının da ele alındığı, daha kapsamlı bir tanım üzerinde durulmaktadır.

Bir ülke yönetiminin temel önceliği toplumun can ve mal güvenliğini sağlamaktır. Yaşanan tüm gelişmeler, yürütülen tüm politikaların temelinde can ve mal güvenliğinin arttırılması bulunmaktadır. Ulusal ve uluslararası siyasetin, ekonomik gelişmelerin ve benzeri birçok unsurun temel dayanağı budur. Dolayısıyla ulusal güvenlik, ülke yönetimlerinin en çok üzerinde durduğu husus konumundadır. İstihbarat sistemleri de bu amaçla gelişim göstermekle olup, ulusal güvenliğin arttırılmasına katkı sağlamak ve ulusal güvenliğe tehdit oluşturacak iç ve dış unsurların ortadan kaldırılması, olası iç ve dış tehditlerin de önlenmesine yönelik faaliyetlerde bulunmaktadır. Ülke yönetimlerinin temelini ulusal güvenlik politikaları

oluştururken, ulusal güvenlik politikalarının oluşumunda da istihbarat sistemlerinin rolü bulunmaktadır (Yılmaz, 2007: 215).

İstihbarat sistemleri, istihbarat servislerinin oluşumunu sağlayıp istihbarat servislerinden aldıkları bilgileri kullanarak iç ve dış tehditlerin giderilmesine yönelik savunma mekanizmalarının geliştirilmesini sağlamaktadır. Tarih boyunca dünya genelinde hemen her gün farklı bölgelerde de olsa savaşlar meydana gelmiştir. Uluslararası tehditlerin bu denli yoğun ve yüksek olduğu bir ortamda değişen koşullarla birlikte bu tehditlerin arttığından söz etmek de mümkündür. Geçmiş dönemde sahip olunan teknolojik yetkinlikler ile birlikte ulusal ve uluslararası tehdit unsurları kara harekâtları ile sınırlıydı. Bu alan zamanla hava ve deniz harekâtları ile genişlemeye başlarken bugün internet kullanımının arttığı bir ortamda siber tehditlerle de en üst seviyeye ulaşmıştır. Ekonominin günümüz toplumlarının temelini oluşturması ve siyaset – ekonomi ilişkisinin üst düzeye çıkması ile birlikte tehdit unsurları da çok daha çeşitli bir hale gelmiştir. Özellikle Soğuk Savaş döneminde gelişim gösteren istihbarat sistemleri, 11 Eylül sonrası dönemde başta Amerika Birleşik Devletleri olmak üzere çok daha hızlı gelişimler göstermeye başlamıştır (Born ve Leigh, 2008: 71).

İstihbarat sistemleri, genel işlev olarak ulusal güç unsurlarının tespit edilmesi, bu unsurların geliştirilmesi ve doğru hedeflere yönlendirilmesi hususlarında belirleyici konumdadır. Bu noktada istihbarat sistemlerinin sürekli bir değişim ve gelişim içerisinde olduğundan söz etmek de mümkündür.Hem tehdit unsurları hem de toplumsal yaşam ihtiyaçları her geçen gün değişim göstermektedir. İstihbarat sistemleri de bu süreç içerisinde kendisini değiştirmek ve geliştirmek zorunda kalmaktadır (Andrew, 2004: 180).

Soğuk Savaşı dönemi istihbarat sistemlerinin zirve yaptığı dönem olarak ön plana çıksa da Sovyetler Birliği'nin dağılması ile birlikte uluslararası politikalarda yeni bir döneme girilmiştir. Uluslararası birliklerin siyasi ve ekonomik alandaki etkinliklerinin artması, uluslararası siyasetin ulusal siyaset üzerindeki etkinliğini arttırmıştır. Ülkeler, 1990 sonrası dönemde daha dışa dönük politikalar benimsemek zorunda kalmıştır. Sovyetler Birliği'nin dağılması ile birlikte Doğu – Batı ayrımının da bir nevi son bulması, yeni gruplaşmaları ortaya çıkartmıştır. Bu da hemen her

ülkenin oluşan yeni birlikler içerisinde kendi yerini belirlemek adına çaba içerisine girmesine neden olmuştur. Başta NATO olmak üzere uluslararası birliklerle birlikte bugün ülkeler ulusal güvenliklerini sağlamada diğer ülkelerle işbirliği içerisine girmektedir. Karşılıklı çıkarların korunarak gerçekleştiği bu işbirlikleri sonucunda, neredeyse hiçbir ülke kendi ulusal güvenliğini tek başına sağlayamaz hale gelmiştir (Yılmaz, 2008: 96).

Daha önce de ifade edildiği üzere ulusal güvenlik olgusu yalnızca askeri tehditler ile sınırlı kalmaktan çıkmış ekonomik tehditler, doğal afetlere, siyasi baskılardan, etnik ayrımlara kadar birçok farklı yönü ve tehdidi kapsayan bir olgu haline gelmiştir. Tehdit unsurlarının ve beraberinde tehditlerin boyutunun artması ile birlikte ulusal güvenlik ile uluslararası ilişkiler ayrılmaz bir bütün haline gelmiştir. Geçmiş dönemde bu iki olgunun daha keskin hatlarla ayrıldığından söz etmek mümkün olsa da bugün bu iki olguyu bir arada düşünmek bir tercihten ziyade zorunluluk haline gelmiştir.

Oluşan çeşitlilik, tehdidin artan boyutu ve bir arada ele alınması gereken olguların çoğalması sonucunda ulusal güvenlik olgusu çok daha karmaşık bir hale gelmiştir. Bu da ulusal güvenlik politikaların karmaşık ve kapsamlılığının artmasına neden olmaktadır. Ulusal güvenlik politikaları, birçok unsuru dikkate alarak geliştirilme zorunluluğunu taşımanın yanı sıra istihbarat sistemlerine de bağımlı hale gelmiştir. Bugün, dünya oldukça hızlı bir hale gelmiştir. Bu noktada istihbarat sistemleri ile birlikte olası tehdit unsurlarının mümkün olan en hızlı şekilde tespit edilmesi ve tehdide dönüşmeden önlem alınması hayati bir noktadadır (Yılmaz, 2008: 122).

Bugün hemen her ülkede terör olaylarına rastlamak mümkün hale gelmiştir. Özellikle 20. Yüzyılda ulusal sınırlar içerisinde terör örgütlerine rastlanırken, bugün uluslararası terör örgütleri hızla artmaktadır. Yaşanan bu değişim de özünde istihbarat sistemlerinin önemi ve işlevselliğine ilişkin bir kanıt niteliğindedir. Terör olaylarının ne zaman ve ne şekilde gerçekleşeceğini öngörmek çok daha zor bir hale gelmiştir. İstihbarat sistemlerindeki başarı, ülkelerin aynı zamanda ulusal güvenlik düzeylerinin de belirleyicisi konumundadır. Bu doğrultuda ulusal güvenlik düzeyi ile istihbarat sistemleri arasında pozitif yönlü doğrusal bir ilişki olduğundan söz etmek

mümkündür. Terör örgütlerin aynı zamanda suç unsurları ile finanse ediliyor olması terör örgütleri ile mücadelenin zorunluluğunu da artmaktadır. Günümüzde, terör örgütleri başta fuhuş, uyuşturucu ve silah kaçakçılığı olmak üzere yasa dışı yollarla örgütlerini finanse etmektedir. Terör örgütüne karşı verilen mücadele ulusal güvenliğin sağlamanın yanında toplumsal huzuru ve düzeni korumak adına da kazanımlar sağlamaktadır (Köseli, 2011: 159).

1.2. Siber Güvenlik ile İlgili Kavramlar

1.2.1. Siber Güvenlik

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

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

Siber güvenlik, siber ortamda kullanımda, dolaşımda ve depo halinde olan verilerin korunmasını, bu verileri korumayı amaçlayan politika ve prosedürleri, güvenliği sağlayacak olan her türlü teknolojiyi kapsamaktadır. Kuruluşların ve kişilerin siber ortamda barındırdığı varlıkların hepsini korumayı amaçlayan siber güvenlik, siber ortam tehditlerine karşı güncel teknik gelişmelerin takibi yapılması, politika ve prosedürlerin düzenli olarak gözden geçirilmesi ve uygulanması suretiyle sürekli mücadeleyi gerektirir.

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

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

Siber ortamda teknik kabiliyetleri gelişmiş kişi, kurum ve ülkeler ulusal veya uluslararası yasaların izin verdiği ölçüde, çoğu zaman ise illegal yollarla siber ortamdaki her türlü veriyi, ihtiyacı ve amacı doğrultusunda dilediği şekilde kullanabilme imkânına sahiptir. Dolayısıyla siber ortamda saklanan her veri anlamlı bir bilgiye dönüştüğünde veri sahibi /sahipleri, kurumlar, hatta ülkeler açısından güvenlik riski teşkil etmektedir. Tüm bu risklerin olabilecek en alt seviyeye indirgenmesi siber güvenliğin konusunu oluşturmaktadır. Gerçek dünyanın aynası olma yolunda ilerleyen siber ortam, siber güvenlik prensipleri temel alınarak atılan adımlarla, teknik envanterlerin iletişim ağlarına uygun konumlandırılmasıyla, kullanılan yazılımlarda güvenlik konusunda alınan önlemlerle ve siber tehditlere karşı organizasyonlar arası iş birliğiyle hem bireyler, hem de ülkeler için daha güvenli bir alan haline dönüşecektir.

1.2.2. Siber Alan

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

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

Siber uzayda güvenliğin tam anlamıyla sağlanması, alanın kontrol edilebilirliği bakımından günümüz şartlarında düşük bir ihtimal olarak görünmektedir. Ancak bir dizi önlem alınarak özellikle de organizasyonlar arasında iş birlikleri sağlanarak siber uzayın gerçek dünyaya yansıtacağı güvenlik risklerini minimize etmek mümkündür.

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

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

1.2.3. Siber Suç

Siber uzaydan, bilgi sistemlerine izinsiz olarak girişi hedefleyen, bu sistemlere uzun ya da kısa vadede zarar vermeyi amaçlayan, veri çalma veya iz sürme vb. niyetlerle ağdan sistemlere sızan her türlü kötü niyetli girişim siber saldırı kavramını oluşturur. Siber saldırıların birçok olumsuz etkisi olabilir. Bu durumun somut örnekleri, sermaye kaybı, hukuki süreçlerin doğuracağı cezai işlemlere maruz kalınması iken; soyut ve daha ciddi olarak düşünülebilecek etkileri ise güven ve itibar kaybıdır. Fikri mülkiyet hak ihlalleri ile doğan rekabet gücü kayıpları, müşteriler ve iş ortakları nezdinde itimat kaybı, dijital varlıklarda yaşanan tehlikeler ile zora girebilecek şirket yapısı ve hepsi bir araya konduğunda oluşması muhtemel marka ve kurum imajına yönelik güvensizlikler ve itibar kayıpları bir kurumun hisse fiyatını bir anda aşağı doğru çekebilmekte ve bazı uç durumlarda şirketleri iflasa dahi zorlayabilmektedir.

Ağustos 2018 istatistiki verilerine göre siber saldırıların temelinde %77,5 oranıyla siber suçlar olduğu görülmektedir. Siber casusluk amaçlı saldırıların Ağustos 2018 itibariyle %18,8 oranında oluğu, hactivisim amaçlı saldırıların ise

%1.3 olarak kaydedildiği görülmektedir. Siber savaş amaçlı saldırılar ise bu araştırmaya göre önceki yıllarla kıyaslandığında artış göstermiş olup %2,5 oranındadır.

Siber saldırıların yasal olarak cezai yaptırımlarla karşılık görmesi siber suç kavramının hukuk sisteminde tanımlanmasını gerekli kılmıştır. Siber suçlar kimi zaman bilişim suçları, bilgisayar suçları, teknoloji suçu gibi farklı terimlerle ifade edilmektedir. Yasalarımızda, direkt olarak "siber suç" ifadesi olarak değil "bilişim suçları" olarak yer bulmaktadır. Siber suç, bilişim sistemlerinin güvenliğini tehlikeye sokmayı kasten veya kasıtsız olarak neden olabilecek eylemleri kapsar. Yetki olmaksızın, bir bilişim sisteminde var olan verilerin izinsiz bir şekilde kaydedilmesi taşınması, kasten bozulması, kopyalanması gibi eylemleri içeren bir dizi farklı durum da siber suç kapsamında düşünülmektedir. Siber suçlar, özel hayatın gizliliğini ihlal, müstehcenlik içeren yayınlar, terörün siber ortamlar vasıtasıyla propagandasının ve finansmanının yapılması gibi birçok farklı boyutta da ele alınabilmektedir. Siber suç işlenmesi için bir bilişim sisteminin kullanılmış olması gerekmektedir.

1.2.4. Siber İstihbarat

Siber güvenliğe ilişkin gelişmelerin arttığı günümüz teknolojisinde, istihbarat bilgilerinin edinilmesi, siber savaşlarda üstünlük göstergesi olarak kabul edilmektedir. İstihbarat konusunda güçlü olabilmek, güçlü teknolojik altyapıyı ve nitelikli insan kaynağını gerektirir. Olası zafiyetlere karşı korunma mekanizmalarının işletilmesi ve siber tehditlere karşı mücadelenin yürütülmesi için siber istihbarat bilgilerinin güvenilir olması şarttır. Öte yandan, paylaşıma açılmış her türlü veri doğru analizler yapılarak siber istihbarat bilgisine dönüşebilmektedir. Sosyal paylaşım sitelerinin güçlü ülkeler tarafından bu amaçlar için kullanıldığı yaygınlıkla gündeme gelen bir konudur. Bu nedenle bir ülkenin, salt teknolojik ilerleme kaydetmeye odaklanması, diğer ülkelerde olan teknik gelişmelere gözlerini kapatarak politikalar yürütmesi stratejik bir yanılgı olacaktır. Diğer ülkelerde olan teknik gelişmelerin takip edilmesi, edinilen bilgiler ışığında ülke içi değerlendirmelerin düzenli olarak yapılması, yeni politikaların geliştirilmesi hem siyasi hem teknik üstünlüğün elde edilmesine katkı sağlayacaktır. Tüm bu nedenlerle güvenilir siber istihbarat bilgilerinin edinilmesi ve bu bilgilerin doğru tasnifi ülkeler açısından önem teşkil etmektedir.

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

Siber uzayın harbin beşinci boyutu kabul edilmesi siber istihbaratı da önemli kılmaktadır. Siber harp alanında elde edilen galibiyetler, diğer savaş alanlarında düşman kabul edilen tarafların çatışma kararlığını kırabilecek güçtedir. Siber savaşın diğer savaş alanlarına olan bu etkisi, güçlü siber istihbarata ve güvenilir siber istihbarat kaynaklarına duyulan gereği göstermektedir. Ulusal istihbarat servisleri ve ulusal hükümetler kendi aralarında tartışma kanalları açmalı ve casusluk faaliyetinin aşırıya kaçırılmaması veya düşmanca niyet göstermek gibi yanlış anlaşılmaması sağlanmalıdır.

Türk istihbarat topluluğu, genel olarak askeri ve sivil istihbarat birimleri olarak gruplandırılabilir. Askeri istihbarat, Genelkurmay Başkanlığı'na, kolluk istihbaratı İçişleri Bakanlığı'na, dış istihbarat ise Başbakan'a bağlı teşkilatlandırılmıştır. 2937 sayılı Kanun'da 2017 yılında yapılan değişiklikler sonucu Milli İstihbarat Teşkilatı Cumhurbaşkanı'na bağlanmıştır. 2018 yılında ise devlet yapılanmasına ilişkin yeni düzenlemeler neticesinde teşkilatın adı Milli İstihbarat Teşkilatı Başkanlığı olarak değiştirilmiş, Başbakanlık makamı kaldırılmış ve Kamu Düzeni ve Güvenliği Müsteşarlığı görev ve yetkileri İçişleri Bakanlığı'na devredilmiştir.

1.2.5. Siber Savaş

Bilgisayar ağları kullanılarak devletlerin birbirlerinin sistemlerine yetkisiz ve izinsiz giriş yapması, verilerini değiştirmesi, çalması, kopyalaması, herhangi bir zarar vermesi, veri akışını veya hizmetleri kesintiye uğratması siber savaş olarak tanımlanabilmektedir. Clarke ve Knake, siber savaşların gizli varlığını çatışma amacında olan ülkelerin savaş hazırlıkları yaptığını öne sürerek vurgulamaktadır.

Bazı ülkeler, çeşitli tuzaklar ve dijital bombalar kurarak olası savaş tehditlerine ön savunma mekanizması kurmaktadırlar. Gelecekte fiziksel savaşların siber unsurlarla desteklenmesi mümkün görünmekte, hatta tek başına siber harplerin yaşanması ihtimali artmaktadır.

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

1.3. Siber Saldırı Türleri

1.3.1. Kötülümcül Yazılım (Malware)

Kötülümcül yazılımın İngilizce kısaltması olan malware (maliciousoftware) kullanıcının veya ağın bilgisi dışında sisteme ve bilgisayara erişmek veya zarar vermek üzere yaratılmış bir yazılım türü olarak tanımlanmaktadır. İnternet dünyasında birçok tehdit bu terim altında tanımlanabilir.

Kodlama ile yazılımlar yazıp tüm güvenlik duvarlarını aşabilen siber korsanlar bilgisayarlara ve iletişim ağlarına zarar verebilir. Bu saldırıların temel amacı bilgi kaynağını çalmak veya iletişim ağlarına zarar vermektir. Bu saldırı tipleri arasında virüs, Truva atı, solucanlar veya casus/fidye amaçlı yazılımlar sayılabilir (Lagouvardou, 2018: 45). Aşağıda bu saldırı tiplerinin kısaca açıklamaları yapılmıştır.

- **Virüs:** Biyolojik virüslerden esinlenerek adlandırılan ve bilgisayarla kolayca yapılan tehlikeli bir türdür. İnternet, email, usb/flaş tarzı harici ekipmanlar ile sisteme bulaşır. Makro, betik, ön yükleme ve dosya virüsleri olmak üzere dörde ayrılır (Canbek ve Sağıroğlu, 2006). 1948 yılında John VonNeuman tarafından ortaya atılmış olup ilk olarak kendisini kopyalayabilen bilgisayar programlarıdır. 1982'de ise RickSkrenta çalışan ilk virüsü ElkCloner ismiyle yazmıştır. Apple DOS 3.3 işletim sistemine disketler aracılığı ile bulaşmıştır. BLise öğrencisi olan RickSkrenta tarafından arkadaşlarına şaka maksadıyla hazırlanmış olan bu program kendini oyun dosyaları içerisinde gizlemekte ve her açıldığında kızdırmak amaçlı bir şiir olarak ekrana gelmekteydi (Demirer, 2009). Virüs kötülümcül yazılımların giderek yayılması teknolojini gelişmesi ile beraber ciddi bir tehdit haline gelmiştir. Bu durum virüs karşıtı (anti-virüs) veya güvenlik duvarları programlarının yaygınlaşmasına sebep olmuştur.

- **Truva Atı (TrojanHorse):** Yunan mitolojisindeki Truva'dan esinlenerek yaratılmıştır. Program içerisine eklenen tehlikeli kodlar ile kullanıcının talimatları dışında işlem yapıp zarar verebilir (Gürsoy, 2015: 81). Arka kapı açarak bilgisayarları uzaktan yönetir. Yasa dışı siteler, müzik veya oyun sitelerini ziyaret esnasında program indirirken istemsiz olarak kötü niyetli programlarda indirilir. Kurulumdan sonra arka plandan çalışıp korsana uzaktan erişim sağlar. Sisteme arka kapıdan (backdoor) erişen korsanlar, kişisel bilgilere, şifrelere ve sistemin yapısına kolayca erişebilir. Sisteme bulaşan Truva atı, belleğe yüklenip sistem açıkları dâhilinde korsanın tüm talimatlarını yerine getirmektedir (Değirmenci, 2002: 63).

- **Solucanlar (Worms):** Bilgisayar ağları arasında bir etkileşime ihtiyaç duymadan kendi kendine çoğalabilen ve herhangi bir programa ihtiyaç duymadan zarar verebilen kötülümcül yazılım türüdür. Solucanlar bilgisayara mail (spam) veya anlık mesajlara (ıms) tıklanarak bulaşır ve otomatik olarak bilgisayara yüklenir ve gizlenirler. Solucanlar dosyaları değiştirebilir, silebilir ve farklı yazılımları yükleyebilir. Bazı solucanları ise durmadan çoğalarak sistem kaynaklarını tüketir, (harici disk boş alanlar) ağır işleyiş ve çöküşlere sebebiyet verebilir. Aynı zamanda sistemden bilgi çalıp transfer edebilir ve korsanın bilgisayara erişimini sağlayabilir (Usnorton, 2019). "John Brunner tarafından 1975 yılında yazılan "ShockwaveRider" isimli romanda, ağ üzerinden yayılabilen programa verdiği isimden gelmektedir" (Canbek ve Sağıroğlu, 2006). Arpanet ağına yüklenen program ile tarihte ilk solucan olayı ABD'de 2 Kasım 1988'de görülmüştür. Yazılım hızlıca yayılarak bilim ve askeri sistemlerine bulaşmıştır. 2000 bilgisayar bu durumdan kötü etkilenerek yaklaşık 150.000 dolar zarar verilmiştir (Dülger, 2004: 212). 2010 yılında stuxnet adlı solucanın İran nükleer tesisine sızarak verdiği zararı da kısaca siber güvenlik tarihçesi kısmında da özetlemiştik.

- **Casus Yazılım (Spyware):** Bilgisayara sızdıktan sonra kullanıcın bilgi dışında 3.kişilere bilgi, şifre, kredi kartı bilgileri, internette sık ziyaret edilen sayfalar gibi önemli kişisel bilgileri aktaran yazılımlardır. Bu aktivitelerin hepsi sistem hızında ve ağlarda yavaşlamaya sebebiyet vermektedir.

Günümüzde internete bağlı her bilgisayara bulaşıp ciddi zararlar veren bir yazılım olup bu konuda tedbirli olmak oldukça önemlidir (Kaspersky, 2019).

- **Fidye Yazılım (Ransomware):** Bu yazılım sızdığı bilgisayarı kilitleyip şifreliyor ve ardından kullanıcının tekrar erişim sağlamasına izin vermek için de fidye talep etmektedir. Aynı zamanda yapılan ödemenin ardından tüm bilgileri sağlam bir şekilde geri alınacağının da garantisi yoktur. Genelde online oyunlar üzerinden bilgisayara bulaşmaktadır. Çeşitli saldırı tipleri olmakla beraber günümüzde oldukça aktif bir şekilde kullanılmaktadır. Dolaysıyla kurban olmadan önce güvenlik önemleri almak önemli bir yer tutmaktadır (Usnorton, 2019).

1.3.2. Oltalama (Phishing)

Oltalama (yemleme) saldırıları genelde kurbana sahte bağlantı (link) içeren elektronik postalar gönderme yöntemi olarak kullanılır. Gelen bu posta genellikle banka, resmi kurumlar ve benzeri yerlerden gelmiş gibi gözükerek linke tıklanması durumunda tüm kişisel ve diğer önemli bilgiler saldırgan tarafından ele geçirilir. Bu tip saldırılardan korunmanın en iyi yolu ise oltalama e-mail konusunda kullanıcının eğitimli olması ve bağlantılara tıklamadan kaçınmasıdır (Pajunen, 2017; 21). Oltalama saldırıları internet saldırıları arasında en yaygın ve en tehlikeli olanlarındandır. İngilizce balık tutma anlamına gelen ‘fishing’ sözcüğündeki ‘f ’ yerine ‘ ph ’ harflerini konulmasıyla türetilen terim, attığımız zaman en azından bir balık yakalayabileceğimiz düşüncesinden esinlenerek oluşturulmuştur.İstenmeyen E-Posta; İngilizce kelime olan ‘spicedporkand ham’ baharatlı domuz eti ve jambon anlamına gelip baş harflerinin birleştirilmesiyle oluşturulmuştur. Pazarlama, reklam veya sosyal içerikli olarak büyük kitlelere ulaştırılmak istenen mesajların kullanıcının isteği dışında kendisine yollanmasına dayanmaktadır (Turhan, 2006: 58).

1.3.3. Su Kaynağı Saldırısı (Watering Hole)

Su kaynağı saldırısı; yapılacak şirket veya kurum tarafından sıklıkla ziyaret edilen web siteleri tespit edilip, bunlardan biri veya daha fazlasına kötülümcül yazılımların veya zararlı kodların yerleştirilmesi ardından bu web sitelerine girilmesi neticesinde bu kötülümcül yazılımların sisteme bulaştırılması yoluyla yapılmaktadır

(Yaşar ve Çakır, 2015: 8). Bu saldırı türü diğer saldırılara göre daha stratejik ve hedef odaklıdır.

1.3.4. Hizmet Engelleme Saldırısı (Dos)

Hedef sistemin erişilebilirliğini engellemek için yapılan, bilişim sistemleri hakkında çok fazla teknik bilgiye sahip olunmasını gerektirmeyen saldırı çeşididir. Akşam trafiğinde trafiğin kilitlenerek durması DOS atak saldırısının çalışma yapısına benzetilebilir. Eğer yolun kapasitesinin üstünde araç bulunursa yollar tıkanır. Sistemin bant genişliğini aşacak şekilde paketlerin yollanmasıyla sistemin erişilebilirliği engellenir. Eğer gelen trafiğin bant genişliği saldırı alan sistemin bant genişliğinden daha fazla ise yapacak bir şey yoktur (Akyıldız, 2013: 36).

1.3.5. Botnet Saldırısı

"Robot" sözcüğü ile anlamlandırılan “BOT”, belirli bir görevi bir insandan daha hızlı gerçekleştiren ve tekrar eden bir uygulamadır. “BOTNET” ise, ağ yardımıyla birbirine bağlı birkaç BOT’un bir arada kullanılmasıdır. BOTNET saldırısının üç temel unsuru; Bot, Komuta ve Kontrol (C&C) Sunucusu ve Botmaster’dır (Dergi park, 2019).

Kötülümcül yazılım olup bilgisayara bulaşan botlar, botmaster tarafından komuta edilip spam mailler, önemli bilgiler, şifreleri karşı tarafa gönderebilir. Bunlara ek olarak rutin işleyişi de bozup kalıcı hasarlara sebebiyet verip ağları veya bilgisayarları kullanım dışı bırakarak ciddi ekonomik ve politik zararlar verebilir (Unibonn, 2019).

1.3.6. Ortadaki Adam Saldırısı (Man InTheMiddle)

Siber varlıklar iletişim kurabilmek amacıyla veri gönderme ve almak için çeşitli ağlarla bağlantı kurmaktadır. Kurulan iletişimlerin korsanlar tarafından manipüle edilmesine ortadaki adam saldırısı olarak tanımlanmaktadır (Bozgeyik, 2018: 54). Bu yöntem kurbanın bu durumdan haberi dahi olmadan bütün dijital verilerin çalınmasına sebebiyet verir.

1.3.7. Dns Saldırısı (Pharming)

Erişilmek istenen internet sayfası dışında başka bir sayfaya yönlendirilmesi metoduna dayanan saldırı tipidir. IP adresleri alan adı sunucusu (DNS) tarafından çözümlenmekte ve çözümlenme aşamasına korsanlar tarafından müdahale edilmektedir. DNS sunucusu veri tabanı olan bilgisayar sunucu olup, site ismini girilmek istenen sitenin IP adresine yönlendirir. İnternet adreslerinin listelendiği 'host' olarak adlandırılan veriye yazılımlar vasıtasıyla erişen korsanlar, bankasının web sitesine erişmek isteyen kullanıcıyı, doğru web adresi yazmasına rağmen yanlış adrese yönlendirmektedir. Bu yolla kullanıcının internet bankacılığına dair kullanmış olduğu tüm kişisel verileri korsanlar tarafından elde edilmektedir (Gürsoy, 2015: 99).

1.3.8. IP Aldatması (IP Spoofing)

Bilgisayara izinsiz bir şekilde erişim sağlayan saldırı türüdür. Saldırgan kullanıcı güvenilir bir IP den imiş gibi mesaj gönderir. Bu mesajın ardından saldırgan kullanıcın IP adresini ele geçirir ve internet üzerinden farklı paketler göndererek bilgi alışverişine başlar. Bu alışverişin ardından IP adresini değiştirerek güvenilir bir adres gibi gösterir. IP aldatması olarak bilinen bu aşamanın ardından saldırgan saldırılarına başlamaktadır (Abdul-Mumın, 2011: 31).

1.3.9. İnsan Faktörü (Sosyal Mühendislik)

Bilişim sistemleri günden güne gelişimini sürdürmekte güvenlik açısından her türlü açığı kapatmaya çalışmaktadır. Bunlara güvenlik duvarları, anti virüs ve koruma programlarını örnek verebiliriz. Her ne kadar gelişim sağlansa da en zayıf halka olarak insanın yer alması kaçınılmaz hataların yapılmasına ve güvenlik duvarlarının aşılmasına sebebiyet vermektedir. Sosyal mühendislik saldırganlar için en iyi saldırı biçimlerindendir. Her atak için bazı araç, gereçler ve sınırlamalar mevcut iken sosyal mühendislikte bunların hiçbirine ihtiyaç duymayıp sınır tanımayan bir saldırı tipidir. Saldırgan kurbana psikolojik yönden saldırıp ele geçirdiği için kişi ile alakalı tüm bilgileri ele geçirebilir (Maan ve Sharma, 2012: 557).

Sosyal mühendislik, insanların güven eğilimlerini manipüle edip kurban eden saldırı biçimidir. Gelişmiş güvenli bilişim sistemleri dahi kurbanları bu saldırılardan koruyamamaktadır. İnsanlar kolayca saldırıya uğramakta ve yaptıkları riskli sosyal

medya paylaşımları ile kendilerini kolayca hedefe koymaktadırlar. Güvenli olmayan internet sayfalarında gezinti yaparak, zararlı bağlantılara tıklayıp yüklenen kötülümcül yazılımlar sayesinde kullanıcı bilgisayarı kolayca enfekte olmaktadır (Conteh ve Scmick, 2016: 31).

Yukarda da saldırı tiplerinden bahsettiğimiz tüm siber saldırıların temelinde sosyal mühendislik yatmaktadır. İnsanları bir şekilde manipüle edip ele geçirilen bilgiler veya kontrollerle kurum veya şahıslara ciddi zararlar verilmektedir. Bu konuda farkındalığın artırılması ve eğitimlerin düzenlenmesi bu saldırıların önüne geçebilmek adına alınabilecek en önemli adımlardandır.

İKİNCİBÖLÜM

ULUSLARARASI SİBER GÜVENLİK ÇALIŞMALARI

2.1. Siber Güvenlik – Ulusal Güvenlik İlişkisi

Siber Alanın Uluslararası İlişkiler disiplini içerisine dâhil olması tamamen güvenlik odaklı bir yaklaşımdan dolayı olmuştur. Devletlerin son yıllarda ciddi şekilde güvenlik ikilemi içerisine düşmesi ve diğer devletlere yapılan siber saldırılar konunun önemini arttırarak disiplin içinde önemli bir noktaya ulaşmasını sağlamıştır (Tarhan, 2017: 111). Devletlerin önceden var olan risk durumunun tehdide dönüşmesi güvenlik politikalarını üretmesine neden olmuştur. Bir devletin, diğer devletlerin egemenliğini, istikrarını ve güvenliğini tehdit ettiği bir alan olarak görmesinden sonra Uluslararası İlişkiler için kritik bir noktaya gelmiştir. (Choucri, 2012: 5).

Uluslararası İlişkiler özü itibariyle modern devlet yapılanması ile ortaya çıktığı genel kabul görmüş bir ifadedir. Bundan dolayı araştırma, inceleme konusu ve temel aktörü daima devlet olmuştur. Devleti ilgilendiren meseleler disiplin içerisinde ele alınmaya başlanmıştır. Zamanla mesele ve sorunlarda değişikliğe uğrayarak çeşitlenmeye başlamıştır. Bir zamanlar lowpolitics olarak ifade edilen durumlar, bir süre sonra highpolitics haline dönüşmüştür. Siber uzayda bu evrelerden geçmiştir. Başlangıçta lowpolitics olarak görülen alan ki bunda realist teorinin önemi oldukça büyüktür. Zamanla devlet için kritik ve çok önemli bir nokta haline gelmiştir. Özellikle Siyasi liderlerin internetin dönüştürücü etkisini benimsemeye başlamaları alanın önemini arttırmıştır. İnternet uzun bir geçmişi olmasına rağmen 1990'ların başında kullanım oranı çok azdı güvenlik açıkları da yok denecek kadar önemsizdi. Ancak bugün milyarlara ulaşan kullanım oranının yaratmış olduğu karşılıklı bağımlılık ve fırsatların oluşması alanın disiplin içindeki önemini arttırmıştır (Nye, 2011:18).

Siber alanda güvenliği sağlamak devletlerin tek başına çabaları ile mümkün görülmemektedir. Nasıl I. Dünya Savaşı sonrası disiplin oluşurken, karşılıklı iş birliği vurgusu önemli bir meseleyse bugün de gelinen noktada devlet ve devlet dışı birçok aktörün birlikte hareket ettiği görülmektedir (Ünver, 2017: 108). Örneğin uluslararası alanda yapılan ilk önemli çalışma; Avrupa Konseyi tarafından 2001'de imzalanan Avrupa Siber Suç Sözleşmesi olmuştur. 23 Kasım 2001 tarihinde imzalanıp, 2004 yılında yürürlüğe giren temel metin olarak nitelendirebilecek sözleşmedir. Budapeşte'de imzalandığı için Budapeşte sözleşmesi olarak da anılmaktadır. Siber suçlara ilişkin imzalanan ilk sözleşme olan Budapeşte sözleşmesi içerik olarak; Siber suçlarla mücadeleyi, bilgisayarla bağlantılı sahtecilik ve telif haklarının ihlali gibi konular üzerinde yoğunlaşmıştır (Council of Europe, 2001). Sözleşmeden sonra diğer bir uluslararası çalışma ise Budapeşte sözleşmesinin referans alınarak AB tarafından imzalanan Şubat 2005 yılına ait 2005/222/JHA sayılı Çerçeve Kararı'dır. Bu karar daha sonra 14 Ağustos 2013 tarihinde Bilgi Sistemlerine Saldırılara Dair Yönerge şeklinde değiştirilmiştir (Mavzer, 2014). İmzalanan sözleşme de aynı şekilde AB için siber alanda imzalanmış ilk sözleşmedir.

Bir diğer uluslararası örgüt olan NATO bağlamında incelendiğinde ise siber güvenlik meselesinin 2000'li yılların başında gündeme geldiği görülmektedir. 1999 yılında NATO'nun Sırbistan'a düzenlediği askeri operasyonları protesto etmek için NATO ve üye devletlerine karşı yapılan siber saldırılar konunun NATO'nun gündemine girmesine neden olmuştur. Bundan dolayı NATO 2002 yılındaki Prag Zirvesi'nde Siber Savunma Programını kabul etmiştir. Amaç siber saldırılara karşı üye devletleri bilgilendirmek ve bu alanda güçlenmelerini sağlamaktır (Seren, 2016:16). Bu çalışmaların başlaması siber dünyanın devletler ve disiplin için önemli bir nokta haline dönüşmesini sağlamıştır. Sözleşmeler ilk halleri ile kalmamış, zaman geçtikçe yeni sözleşmeler, toplantılar ve konferanslar düzenlenmeye devam edilmiştir. Ayrıca her ülke kendisi için ulusal siber güvenlik stratejisi yayımlamaya başlamıştır. Bu da meselenin artık disiplinin içerisinde önemli bir kavram olmaktan öteye öncelikli alan olmasını sağlamıştır.

2.2. Siber İle İlgili NATO Zirvelerindeki Kararlar

NATO siber savunmada ana odak olarak daima kendi karargâhlarını, ajanslarını ve operasyonlarını korunmayı amaçlamıştır. 2014'te yapılan bir araştırmaya göre NATO üyesi olan 10 ülkeden 7'sine göre siber güvenlik en öncelikli konular arasına girmektedir. Bu araştırmaya göre; en çok oyu almış olan "İttifak hedefli saldırılar", ikincisi "uluslararası terörizm" ve üçüncü sırada da "siber güvenlik" konusu NATO için önem arz etmiştir (WickettandMcInnis, 2014: 8). 1990'dan bu yana İttifak bu alanda savunma yeteneklerini geliştirmeye devam etmiştir. NATO'ya karşı bilinen ilk siber olay olan Kosova saldırısından sonra örgüt ve üyeleri siber savunma konusunu gündem maddeleri arasına almıştır. 1999'da gerçekleşen bu saldırıdan birkaç yıl sonra üyeler Prag'da bir araya gelmiştir. 2002'de gerçekleştirilen Prag Zirvesi'nde, NATO'nun siyasi gündeminde ilk kez siber saldırılara karşı savunma kapasitesinin güçlendirilmesi ilan edilmiştir (Pernik, 2014: 4). Gerçekleştirilen bu zirvede NATO Siber Savunma Programı kabul edilmiştir. Aynı yıl Kuzey Atlantik Konseyi (NAC), Siber Savunma Programı'nın bir parçası olan ve siber olayları önleme, tespit etme ve bunlara müdahale etme amacıyla NATO Bilgisayar Olaylarına Müdahale Birimi'ni (NCIRC) kurmuştur.

2007 yılında meydana gelen, Estonya'nın hükümet, medya ve finans web sitelerine yapılan siber saldırı ve 2008'de Gürcistan- Rusya konvansiyonel savaşına siber saldırıların da dâhil olmasıyla birlikte, NATO İttifak'ının odak noktası kendi ağlarının güvenliğinden üye devlet ülkelerine doğru yayılmıştır. Estonya saldırısı sonrasında 2008 yılında Romanya'da, başkent Bükreş'te bir araya gelen ülkeler burada bir NATO zirvesi yapmışlardır. Bu zirvede siber savunma faaliyetlerinin önemi ve kritik altyapıların korunması konusu üzerinde durulurken, Bükreş Zirvesi Bildirisi'nin 47. Maddesinde de siber savunmaya dair birçok karar alınmıştır (Ada, 2018: 36).

Bükreş'te alınan kararlara göre; İttifak, siber saldırılara karşı güvenliğini üst düzeye çıkarması için bilgi sistemlerini daha dayanıklı bir hale getirmesi gerekmektedir. Belirlenen birimlerce, kabul edilen siber savunma politikaları daha da geliştirilmektedir. Herhangi bir saldırı durumunda yardım talep eden üye devletlere siber savunma desteği verilmektedir. Siber savunma konusunda da üye ülkeler ve

ulusal otoriteler iş birliği yaparak ilişkilerini genişletmektedir (NATO CCDCOE, 2008). Bükreş Zirvesi siber güvenliğin detaylı bir şekilde işlenmesi ve bu konunun Sonuç Bildirisi'nde yer alması bakımından bir ilk olup önemli bir tarih olarak yer almıştır.

Bükreş Zirvesi sonrasında NATO sayesinde siber alanda önem arz eden iki gelişme yaşanmıştır. İlki siber savunmayı koordine edebilmek adına, kabiliyetleri incelemek ve risklere karşı uygun güvenlik sağlamak için NATO Siber Savunma Yönetimi Otoritesi'nin (CDMA) kurulmuş olmasıdır (Pernik, 2014: 4). CDMA, ihtiyaç olması halinde hızlı ve etkili bir siber savunmanın başlatılmasından ve koordine edilmesi açısından yetkilidir. NATO Siber Savunma Yönetim Kurulu (CDMB), Örgüt 'ün siber savunma politikasını hayata geçirmek ve üye ülkelerin herhangi birine karşı gerçekleştirilen siber saldırı durumunda gereken önlemleri almaktan sorumlu olarak oluşturulmuştur (Somuncu, 2018: 44). İkincisi ise; NATO'nun birlikte çalışabilirliğini geliştirmek ve siber farkındalık, eğitim ve öğretim çabalarını geliştirmek gibi ana hedeflerle Kooperatif Siber Savunma Merkezi (CCD COE) oluşturulmuştur.

2008'de yaşanan bu olayların tekrarlanmaması için ulusal ve uluslararası işbirliği ve uluslararası hukukun uygulanması için gerçekleştirilmek istenen analizleri de barındıran, NATO Siber Güvenlik Tatbikatları "NATO CyberCoalition" adıyla işleme konulmuştur. İttifak üyeleri 2009 yılında Strazburg/ Kehl'de yeniden bir araya gelmişler ve siber savunma için yeni bir strateji belirlenmesini istemişlerdir. Bu zirvede siber savunma NATO tatbikatlarına dâhil edilmiş ve böylece siber savunma NATO tatbikatlarının ayrılmaz bir parçası haline gelmiştir. Strazburg zirvesinde; 24 saat içinde görevlendirilebilecek altı uzmandan oluşan bir çekirdek ile iki siber Hızlı Tepki Ekibi (RRT) kurulmuştur. Üye devletlerin, siber savunma kapasitelerini en üst düzeye çıkarmak amacıyla çalışma başlatması, siber savunma konusunda hukuki boyutları araştırmak üzere NATO'da görevli olan uzmanların araştırma yapmasına karar verilmiştir (Darıcılı, 2016: 414). Siber Savunma Siyasası ile NATO'nun ağlarına ve saldırı durumunda üye devletlere yardım etme kararı teyit edilmiştir. NATO ve ilgili kurumlar genelinde siber savunma faaliyetlerini koordine etmek ve NATO'nun siber savunma politikalarının ve kabiliyetlerinin uygulanmasını

kolaylaştırmak amacıyla, 2011 yılında siyasi, askeri, operasyonel ve teknik seviyelerde NATO siber uzmanlarından oluşan Siber Savunma Yönetim Kurulu (CDMB, CDMA desteği) kurulmuştur (Pernik, 2014: 5).

2012 Chicago Zirvesi'nde gerçekleşen ve gerçekleşecek olan siber saldırıların yalnızca bilgi sistemlerini değil, siber alanla bağlantılı olan tüm kamu kurumlarının yanı sıra özel sektörü de etkileyebileceği üzerinde durulmuştur. Bu yüzden de kritik alt yapıları koruma anlayışı ve ortak hareket etme, dayanışma konuları önem arz etmiştir. Bu konuyu müteakiben de beş devlet (Danimarka, Hollanda, Kanada, Norveç ve Romanya) 2013 yılında Çokuluslu Siber Savunma Kapasitesi Geliştirme Projesini başlatmıştır (Darıcılı, 2016: 415).

Siber alana dair normların belirlenmesi ve uluslararası siber güvenliğin güçlendirilmesi amacıyla 2016 yılında NATO CCD COE tarafından "Siber normlar Dokümanı" yayımlanmıştır. Yine 2016 yılında siber için çok büyük bir adım, Varşova Zirvesi'nde atılmıştır. Bu zirvede siber alan operasyonel bir alan olarak devletler tarafından resmen tanınmıştır (Çelik, 2018: 115). Devlet Başkanları, Siber Savunma Taahhüdü 'nü imzalanmış ve Taahhüt kapsamında NATO tarafından ülkelerin siber güvenlik seviyelerini ölçme amacıyla öz denetim kriterleri belirlemiş ve ülkelerin kendilerini değerlendirmelerini talep etmiştir (Somuncu, 2018: 50). Bu taahhüt ile ulusal alt yapılar ve ağlarda siber savunmayı geliştirme ve güçlendirme konusunun kendileri için öncelikli bir konu olduğunu belirtmişlerdir.

2018 NATO Zirvesi yine Brüksel'de yapılmıştır. NATO'nun güvenliğine yönelik siber tehditlerin daha sık, karmaşık, yıkıcı ve zorlayıcı hale geldiği konusu üzerinde durulmuştur (Brent, 2019). Ekim 2018'de NATO'nun kurulacak Siber Uzay Operasyonları Merkezi ile ilgili ilk çalışmaların yapılacağı duyurulmuştur. Siber Uzay Operasyonları Merkezi'nin, siber uzay güvenliği konusunda farkındalık yaratmak, İttifak operasyon ve misyonlarının siber uzay boyutunun merkezî planlamasını ve siber uzay operasyonları ile ilgili koordinasyonu sağlamaktan sorumlu olacağı belirtilmiştir. Brüksel Zirvesi'nde müttefik ülkelerin gönüllü olarak sağladıkları kendi ulusal siber varlıklarının İttifak'ın operasyon ve misyonlarına ne şekilde entegre edileceği konusunda anlaşmaya varılmıştır (Brent, 2019). 2019'da ilk

siber uzay istasyonu projesinin müttefiklerce onaylanmasının ardından tamamlanması beklenmektedir.

Görüldüğü üzere NATO gerçekleştirdiği zirvelerde siber konusuna giderek genişleyecek şekilde değinmeye çalışmıştır. NATO, siber alanın belirsizliği ve sürekli değişen yapısı karşısında çeşitlenen tehditlere karşı bu sürece uyum sağlayıp sağlayamadığını ve tepkilerini devamlı olarak değerlendirmelidir.

2.3. Uluslararası Siber Güvenlik Olayları

2.3.1. Estonya'ya Yapılan 2007 Siber Saldırısı

Sovyetler Birliğinin dağılmasından sonra Rusya ve Estonya arasında sürekli bir anlaşmazlık mevcuttu. Anlaşmazlığın son noktası Estonya'nın 26 Nisan 2007 yılında Tallinn merkezinde bulunan eski Sovyet Asker Anıtını kaldırmasıyla ilişkiler iyice gerilmiştir. Gece tarih sahnesine Bronz Gece olarak geçmiştir. Tam bu süreçte yoğun Rus azınlığını da içinde bulunduran Estonya üç hafta süren yoğun siber saldırılara maruz kalmıştır. Avrupa'nın en güçlü kablo toplumu ve e-devlet uygulamasının en üst düzeyde olduğu ülkede siber saldırılar hayatı durdurma noktasına getirmiştir. Saldırıların hedef noktası; Estonya Cumhurbaşkanlığı ve Parlamentosu, Siyasi partiler, hükümete ait tüm bakanlıklar, ülkenin ün büyük üç haber kuruluşu, en büyük bankası ve iletişimde uzmanlaşmış firmalar vardı.

Saldırı sonrası Estonya Savunma Bakanı JaakAaviksoo yaptığı açıklamada; NATO'nun, açık bir askeri harekât olarak siber saldırıları tanımlamadığını ve bundan dolayı durumu Kuzey Atlantik Antlaşması'nın V. maddesinin hükümlerine göre veya başka bir deyişle toplu savunma mekanizmasının, saldırıya uğrayan ülkeye otomatik olarak uzatılmayacağı anlamına geldiğini ifade etmiştir (TheGuardian, 2007). Burada önemli nokta eğer bu saldırı savaş olarak tanımlansaydı, NATO kollektif şekilde Rusya ile karşı karşıya kalmak zorunda kalacaktı. Keza Estonya savunma bakanı ilk başta bunu bir savaş olarak kabul ettiğini ifade etmiştir ancak NATO'dan o şekilde bir geri dönüt asla sağlanmamıştır. Bundan dolayı yapılan açıklamalar daha ılımlı olarak bir saldırı şeklinde kabul edilip, araştırılacağı yönünde olmuştur. Aynı şekilde Kremlin sözcüsü Dimitri Peskov da iddiaları gerçek dışı olduğunu belirterek

Rusya'nın sorumlu olmadığını açıklamıştır(BBC Türkçe, 2007). Ancak uzmanların yapmış olduğu araştırmalar gösteriyor ki saldırıların DDos14(Distributed Denial of Service) olarak yöntemle gerçekleştirilmesidir. Pek çok bilgisayarın ele geçirilip zombi bilgisayar haline getirilerek yapıldığı ortaya çıkmıştır. Zombi bilgisayarların ise kullanıldığı ana bilgisayarların Rusya'da olup, programında Kril alfabesiyle yazıldığı tespit edilmiştir (Clarke, Kanke, 2011:15).

Estonya saldırısı Uluslararası alanda önemli bir soruyu ortaya çıkarmıştır. Böyle bir durumla karşılaşan devletin nasıl tepki vereceği veya saldırı karşısında nasıl bir savunma mekanizması oluşturacağını gündeme getirmiştir. Burada cevap niteliğinde kesinlikle devletlerin sahip oldukları göreceli güçlerinin önemine bağlı olduğu noktası dikkat çekmiştir. 2007'de meydana gelen olayda Rusya'nın saldırılarını başlatmasının ardından Estonya'nın doğrudan Rusya Hükümetini suçlaması iki devletin karşı karşıya gelmesine neden olmuştur. Estonya NATO üyeliğinden yararlanmak isteyerek kolektif öz savunmasını başlatmak istedi 5.madde gereği. Lakin NATO Rusya'yı silahlı saldırıyı suçlamaktan kaçındı. Estonya Savunma Bakanı yaşadığı hayal kırıklığı ile birlikte hizmet etkinliğinin reddedilmesini doğrudan terörist faaliyetlerle kıyasladı. Saldırının Rusya siber uzamının içinde yer alan bilgisayarlardan geldiğini ifade etmeye devam etti. Yaşanan olay NATO veya AB özelinde savaş olarak belirtilmeyip saldırı şeklinde ifade edilmiştir. Burada savaş olmayışı, önemli ölçüde maddi hasarın oluşmayıp veya insanların zarar görmemesi şeklinde ifade edildi. aviksoo, ne AB ne de NATO'nun siber savaş olarak nitelendirilebileceğini, ne de bu tür saldırıların başlatılması durumunda üye devletlerin hakları ile AB ve NATO'nun yükümlülüklerinin neler olduğunu tanımlayamadığını kabul etti. Siber saldırıların net bir askeri eylem olarak tanımlamanın zor olduğu açıkça ifade edilmiştir. Kısaca böyle durumlarda NATO'nun 5.maddesinin otomatik olarak hayata geçeceği anlamına gelmediği ifade edildi(Farwell, Rohozinski, 2011:32).

NATO ve AB'nin yaptığı açıklamalar gösteriyor ki böyle saldırılar karşısında devletlerin aslında Siber alanın yaratmış olduğu anarşik ortamdan dolayı yalnız olduklarını göstermiştir. Halkının yüzde 60'a yakınının günlük ihtiyaçlarının çoğunu internetten sağladığı, ülkedeki bankacılık işlemlerinin yaklaşık yüzde 96'sının internet üzerinden gerçekleşen Estonya gibi ülkelerin böyle saldırılar karşısında ne denli hezimete uğrayacağı açıkça anlaşılmıştır (Yener, 2015).

2.3.2. Gürcistan'a Yapılan 2008 Siber Saldırısı

Soğuk Savaşın sona ermesiyle dağılan SSCB toprakları içerisinde uzun yıllar bir takım etnik ve devlet içi sorunların yaşandığı görülmektedir. Bunlardan bir diğeri de Gürcistan içerisinde bulunan fiili olarak 1991'de bağımsızlaşan ancak uluslararası arenada halen Gürcistan'a bağlı olduğu kabul edilen Güney Osetya sorunudur. Her ne kadar Güney Osetya Gürcistan'a bağlı olsa da genel anlamda Rusya'dan oldukça önemli destek almaktaydı. 2008 ağustos ayına gelindiğinde Güney Osetya bölgesinde bir takım ayrılıkçı hareketlerin yaşandığı görülmüştür. Gürcistan hükümeti ise bu ayrılıkçı hareketleri durdurmak amacıyla Osetya bölgesine askeri operasyon düzenlemeye başlamıştır. Başlanan bu operasyon sonrasında ise Rusya Osetya'ya destek vererek Gürcistan'a hem askeri hem de siber alanda saldırılar düzenlemiştir (Tikk, vd., 2008:4).

Gürcistan-Rusya arasındaki savaşın önemli olmasını sağlayan ve diğer klasik anlamdaki savaşlardan ayıran bazı noktalar bulunmaktadır. Öncelikle Rusya başlatmış olduğu askeri operasyonları desteklemek için siber saldırılarda bulunmuştur. Hükümet siteleri ve ticari birçok web sitesine saldırarak savaşı sanal âleme de taşımıştır (The Sydney MorningHerald, 2008). Esasında askeri saldırılar başlamadan önce bu saldırılar başlamıştı. Daha savaşın ortaya çıkmasına 20 haftalık gibi çok uzun bir süre önce Rusya birçok ülkede binlerce bilgisayarı ele geçirerek Gürcistan'a karşı saldırıları başlatmıştı. Bu süre içinde de Abhazya ve Osetya sınırlarına yavaş yavaş asker konuşlandırmaya başladığı açık şekilde görülmüştür (Newsweek, 2008). Başlangıçtan beri Gürcistan hükümeti Rusya'yı suçlamıştır. Rusya tarafı bu durumu reddetmek yerine, 'ülkesi için bir şeyler yapmaya çalışan insanlar var' açıklaması ile suçlamaları kabul etme noktasına getirmiştir. Saldırılar ülkede günlerce internet ulaşımının kesilmesine neden olmuştur. Hatta elektrik

kesintileri de yaşanmış, ülkenin dış dünya ile bağlantısı kesilmeye çalışılmıştır (The New York Times, 2008).

Saldırıların uluslararası sistemde ve disiplin içerisindeki önemi; ilk kes siber alanda başlayan saldırıların, silahlı bir çatışmaya dönüşerek savaş şeklini almasıdır. Daha önce yaşanan birçok saldırı da bu durumun açık şekilde yaşanmadığı görülmektedir. Ancak Rusya-Gürcistan çatışması silahlı çatışmaya eşlik eden ilk önemli siber saldırıları temsil etmektedir (Nye, 2008). Rusya siber saldırılar alanında önemli derecede güçlü bir ülke konumunda bulunmaktaydı. Bu saldırılar Batı ve dünyanın geneline de açıkça verilmiş bir mesaj olarak algılanabilmektedir. Siber saldırıların, savaşa dönüşebileceğini kanıtlayan Rus Hükümeti, bunun yanı sıra caydırıcılık etkisi yaratmak istemiştir. Özellikle Soğuk Savaş sonrasında tekrardan büyük bir güç olduğunu kanıtlama çabasına girerek, kendi bölgesinde söz sahibi olduğunu vurgulamıştır. Buna benzer bir olayı da 2009 yılında ABD'nin Kırgızistan'da askeri üs kurma kararı aldıktan sonra ülkenin 4 önemli servis sağlayıcısının yoğun saldırılar altında kalması örnek verilebilir (TimeTurk, 2013). Tüm bunlar bir arada düşünüldüğünde Gürcistan saldırısı caydırıcılık için siber saldırıların potansiyel bir güç olduğunu göstermiş bulunmaktadır (Goodman, 2010:104).

2.3.3. İran'a Yapılan 2011 Stuxnet Siber Saldırısı

İnternetin yaygın kullanımı ile birlikte sanal dünya da birtakım değişiklikler ve risklerin ortaya çıktığı aşikârdır. Özünde 1988'de kötü yazılımlar ile bir takım Disk Operating System (DOS) ve başka kötü amaçlı yazılım sistemleri ile başlayan küçük boyuttaki kışkırtıcı saldırılar, 2009 yılına gelindiğinde daha önceki birçok virüs ve saldırıdan çok daha etkili bir boyutta ortaya çıkmıştır. Bir nevi siber alanda gerçekleştirilen saldırılar içerisinde bir evrim niteliği taşımaktadır (Collins, McCombie, 2012:80).

Stuxnet saldırısı ismini Stuxnet virüsünden almaktadır. 2009 yılında ABD tarafından İran nükleer santrallerine karşı yapıldığı belirtilmektedir. Her ne kadar ABD tarafı saldırıları üstlenmemiş olsa da verilen politik cevaplar ve analizler ABD üzerinden gerçekleştiği argümanını ortaya çıkarmaktadır (Çelik, 2014:144). Saldırı

esasında 2010 yılında fark edilmiştir. İran zenginleştirilmiş uranyum tesislerinde bir yıl boyunca değiştirilen santrifüjlerin %10'lara ulaşması, sistem içerisinde bir takım ters giden durumun olduğu fikrini ortaya çıkarmıştır. Ardından yapılan bir yıllık çalışma sonucu, değişen santrifüjlerin aslında bilgisayar sisteminden gelen bir arızadan dolayı olduğunu kanıtlamıştır. Bir yıl boyunca neredeyse dünyadaki birçok bilgisayar güvenliği araştırmacısının, dünyanın ilk yazılı sanal silahı olarak tarihe dönüşecek bir yazılım parçası olan, o güne kadarki yazılan en karmaşık kötü amaçlı yazılım olarak tarihe geçecek olan virüsün farkına varmışlardır(Zetter, 2011). Virüsün saldırı noktası tesisler de bulunan SimaticWinCC Step7 olarak bilinen enerji üretim ve dağıtımının kontrolü, su, doğal gaz, kanalizasyon sistemleri gibi kritik altyapıların kontrol edildiği ve izlendiği program olmuştur. Program SCADA15 (SupervisoryControlAnd Data Acquisition) denetleme kontrol ve veri toplama sistemi olarak bilinmektedir. Ve kritik alt yapılar içerisinde en önemlilerinden birisidir. Bu da siber alanda gerçekleştirilen bir saldırı ile normal gündelik hayatın çok ciddi boyutlarda aksayacağını göstermiştir.

Siber Saldırılar içerisinde en önemlisi olarak ifade edilen Stuxnet saldırısı, sistemi ele geçirme ve çökertme üzerine yazılmış virüsün, birçok kritik altyapı içerisinde kullanılan PLC devreleri üzerine yoğunlaşması diğer birçok devletinde böyle bir durumla karşılaşacağı riskini ortaya çıkarmıştır. Bu da Uluslararası İlişkiler içerisinde devletlerarasında süre gelen güvenlik ikilemi olgusunun halen geçerli olduğunu göstermektedir. Keza bu durumun klasik güvenlik anlayışında olduğundan öte bir duruma geçerek daha da güçlendiği şeklinde ifade edilebilir.

John Arquilla, günümüz teknolojisiyle kitlesel ölçekte saldırıların gerçekleşebileceğini ancak stuxnet ile birlikte sadece enformasyon savaşlarının olmayacağını bunun yanı sıra fiziki tahribatında verilebileceği vurgusunu yapmaktadır. Stuxneti diğer birçok program, yazılım veya virüsten ayıran özelliği ise, diğer birçok saldırı şekli için internete bağlı olmak koşulunun bu program için geçerli olmamasıdır. Yani herhangi bir veri girişinin bilgisayarı ele geçirip kendisi için kullanması mümkündür (Elektirik Port, 2011). Aslında siber alanda da meydana gelen yenilikler bir bakıma güvenlik olgusu içinde değişerek klasikleşmektedir. Stuxnet saldırının programın özelliği ve kodları yönünde bir inceleme ile ABD tarafından gerçekleştiği ihtimalini ortaya çıkarmaktadır. Ancak ABD hükümeti bu

iddiaları ne kabul etmiştir ne de açıkça yalanlamıştır. Edward Snowden yapmış olduğu röpartajda açıkça bunun İsrail ile ortak bir saldırı olduğunu ifade etmiştir (Snowden, 2013). Buna benzer bir açıklama da David E. Sanger tarafından gerçekleşmiştir. Sanger de aynı şekilde saldırının, Obama tarafından bizzat yürütülen ve İsrail ile işbirliği içinde hareket edilen bir program olduğunu belirtmiştir (Sanger, 2012).

Stuxnet'in güçlü teknik özellikleri siber tehditlerin daha da güçlenmeye başlayarak politik ve stratejik amaçlar için kullanılabileceğini göstermiştir. Devletlerin siber ortamı bir nevi caydırıcı etki sağlamak için kullanmaya başladığı ifade edilebilir. Caydırıcılık esasında güvenlik ikilemi içerisinde olan devletlerin gelebilecek saldırılara karşı kısıtlama getirmek için kullanılan bir araçtır (Korhan, 2016:154). Stuxnet saldırısı da modern anlamda caydırıcılığı en büyük saldırılardan biri olarak belirtilebilir. Program politik ve stratejik bağlamlarda yarattığı etkiler özelde caydırıcılık alanında oldukça önemli olmuştur. En önemli husus, siber suç ile devlet eylemi arasındaki yakınlaşmadır; Bu, devletin siber suç tarafından yönlendirilen teknoloji gelişiminden yararlandığı yerdir. Devletin bu teknolojiyi kullanma yeteneği olmasa bile, siber saldırıları yürütmek için üçüncü taraflara sözleşme yapma olasılığı her zaman vardır (Collins, McCombie, 2012:88).

Özetle yapılan saldırı çıkış kaynağı tam olarak belirlenmemiş olarak ifade edilse de programın bireyler bazında yapılamayacağı, arkasında devlet gibi önemli bir gücün olduğu apaçık ortadır. ABD tarafı suçlamaları kabul etmese de durum, büyük bir egemenlik ihlalini ortaya çıkarmaktadır. Uluslararası Sistemin anarşik doğası içinde klasik anlamda devletler saldırı kaynaklarını bilerek hareket ederken, günümüz dünyasında sistem içerisinden gelen saldırılar belirsiz olmaktadır. Bu da devletlerin önlem alma ve yaptırım uygulama veya saldırı şeklinde cevap vermesinin önüne geçmektedir. Zaten siber alnın en önemli problemi, gerçekleştirilmiş saldırının kaynağının nereden geldiği ve kim tarafından gerçekleştirildiğinin bilinmemesidir (Can, 2014). Bu durumda devletlerin daha fazla güvenlik ikilemi içerisine girmesine neden olurken, diğer bütün devletleri çıkarına ters düşen risk ve tehdit şeklinde algılamasına neden olmaktadır. Bundan dolayı da güvensiz bir dünya düzeni kurulmaya başlamıştır.

2.4. NATO Ve Siber Güvenlik

İkinci Dünya Savaşı'nın sona ermesi Avrupa'nın barış ve güvenliğe kavuşmasına yeterli olmamış yer yer ortaya çıkan huzursuzluklar Batı ile Doğu arasında her gün daha çokartan gerginliğin belirtilerini vermeye başlamıştı. İkinci Dünya Savaşı'ndan hemen sonra, Almanya konusunda Sovyetlerle Batılılar arasındaki koklu görüş ayrılıkları, Doğu Avrupa ülkelerinin teker teker Sovyet etki alanına girmesiyle ideolojik ve ekonomik örgütlenmenin başlaması, Japonya'da Müttefikler arasındaki ortak bir anlayışınkurulmaması, Yunan iç savası ortamında ilan edilen Truman Doktrini ile Marshall Planı ve İran ile Türkiye üzerindeki Sovyet baskısı, özellikle Avrupa'da soğuk savaşı doruknoktasına çıkarmaya başlamıştı (Sander, 2005: 263). Batı Avrupa Devletleri'ninSovyetler Birliği'ne karsı oluşturdukları ittifak ve bu ittifakta ABD'nin mali ve askeri desteğinin bulunmayışı Sovyet tehdit ve yayılmaları karsısında yeterli bir güç oluşturmamıştır. Bu nedenle Batı Avrupa Devletleri ABD'yi ittifaka dahil etmek için çalışmışlardır. Sovyetler Birliği'nin Avrupa'dan sonra Uzak Doğu'da da yayılma politikası izlemeye başlaması ve BM Teşkilatının dünya barısını tesis etme çabalarının Sovyetler Birliği vetoları ile etkisiz hale gelmesi karsısında ABD Sovyetler Birliği ile iş birliğinin güçleştiğini hatta imkânsız hale geldiğini görmeye başlamıştır. Bu olaylar karsısında, ABD Avrupa sorunları ile ilgilenmek zorunda kalmış ve çalışmalar başlamıştır. Vandenberg aceleyle hazırlanan bir planın Kongrede ret kararı ile karşılaşma ihtimalinin olduğunu tahmin ediyordu. Bu sebepledir ki bütün gün suren, iki aylık bir çalışma yapıldı. Tüm bu çalışmalar Marshall tarafından da takip edildi (Erkin, 1992: 28).

11 Nisan 1948 tarihinde ABD Dışişleri Bakanlığı yetkilileri ve Senatör Arthur H. Vandenberg Kuzey Atlantik bölgesinin güvenliği meselesi hakkında hazırlık görüşmelerine başlamışlardır. Görüşmeler neticesinde Vanderberg adını alan karar metni hazırlanmıştır. Bununla birlikte 28 Nisan 1948 tarihinde Kanada Dışişleri Bakanı St. Laurent Brüksel Antlaşmasını da içine alan ve ondan daha geniş kapsamlı bir Atlantik Antlaşmasının kurulması gerektiği fikrini ileri sürmüştür. 4 Mayıs 1948 tarihinde Brüksel Antlaşmasına taraf olan üyeler askeri planlarını ABD'ye sunacak bir komisyon kurulduğunu açıklamışlardır. Monroe Doktrini bu gelişmeler karsında engel teşkil etmiştir. Bu engeli ortadan kaldırmak amacıyla Senatör Vandenberg'in

hazırlayıp Amerikan Başkanına, ABD'nin güvenliğini ilgilendiren ve karşılıklı yardıma dayanan "bölgesel ve diğer ortak antlaşmalara" katılma yetkisi veren Vandenberg Kararı 42adını alan bu tasarı 11 Haziran 1948 tarihinde sekiz saat suren tartışmalardan sonra 4'ekarsı 64 oyla kabul edildi. "Vandenberg Kararı" denilen 289 sayılıkararla ABD, 1823'ten beri uygulamakta olduğu "Monreo Doktrinini" terk etmiş ve ittifakakatılması yolundaki engel kalkmış oluyordu (İsmay, 1956: 10). Çalışmalar esnasında Kuzey Atlantik Antlaşması'nın, ABD ve Brüksel Antlaşması'na taraf ülkeler dışında bazı ülkelerin de alınarak daha da genişletilmesi düşüncesi ve zarureti ortaya çıktı.

Kanada hükümeti 13 Ekim 1948'de ittifaka katılabileceğini bildirdi. Antlaşmaya imza atan devletlerin aralarına almak istedikleri diğer ülkeler ise şunlardı: İrlanda Cumhuriyeti, İsveç, İzlanda, Norveç, Danimarka, Portekiz, ve İtalya idi. Ayrıca Fransa Cezayir'in üç vilayetinin de antlaşmanın tatbik sahası içine alınmasını istiyordu (İsmay, 1956: 11). Ancak sınır ilişkileri bu isteklerin hemen oluşmasına izin vermedi.

Norveç ve Danimarka'nın bu antlaşmaya katılma kararı bulundukları coğrafi konum itibariyle Sovyetler Birliği'ni tahrik edeceği düşüncesiyle hemen olmadı. Bu iki ülke önce İsveç'i de aralarına alarak bir İskandinav Antlaşması yapmak istedi. Fakat İsveç'in tam tarafsızlık siyaseti bu planın islemesini engelledi. 1 Şubat 1949 tarihli Ulus gazetesinde İskandinav antlaşmasını yapılamadığı belirtiliyor ve su şekilde izah ediliyordu:

"...İsveç'e göre silahlı tarafsızlık hiç şüphe yok ki hükümetin takip tasavvurunda olduğu siyasetin esasını teşkil etmektedir. Norveç'in müstakil Atlantik Paktı'na iltihaka karar vermesi beklenmektedir...

Norveç Dışişleri Bakanı Halvard M. Longe Atlantik Antlaşması hakkında bilgi almak ve görüşmek üzere 5 Şubat 1949'da Washington'a gitti. Dışişleri Bakanı'nın Washington'a hareketinden birkaç saat önce Rusya'nın vermiş olduğu nota 7 Şubat 1949 tarihli Ulus gazetesinde şöyle belirtiliyordu:

"Rusya notada Atlantik Paktı hakkındaki görüşünü açıklayarak, bunun tecavüz emelleri güden bir pakt olduğunu ve Norveç'le bir saldırmazlık paktı yapmağa hazır olduğunu bildiriyor.".

Norveç, Dışişleri Bakanı'nın Oslo ve Washington arasında birkaç defa gidip gelmesinden sonra Atlantik Paktı'na girmeyi tercih etti. Bu kararına en büyük etki ise Norveç'in Sovyetler Birliği'ne olan ortak sınırıydı. Sonuçta Norveç Parlamentosunda mevcut 400 delegeden 330'u Norveç'in güvenliğine ait meselelerin çözümünün Müttefik Devletlerle iş birliğinde aranması gerektiğine karar vererek Atlantik Paktı'na girme yolunu açtı (İsmay, 156: 11).

Norveç hükümeti bu kararıyla aynı zamanda Sovyetlerin vermiş olduğu notayı da cevaplamış oluyordu. Sovyetler notada ayrıca "Bu İttifaka katılmakla, Batı ülkelerinin saldırgan amaçlarına katılmayı ve bu ülkelere Norveç topraklarında us vermeyi mi tasarladığını" soruyordu. Norveç ise bu durumu; Birleşmiş Milletlerin barısı ve güvenliği korumakta yetersiz kaldığını, bu suretle güvenlik sistemini Atlantik ülkelerinden kurulu bir sistemde aradığını, toprağını hiçbir zaman saldırı politikası çerçevesinde kullandırmayacağını, saldırıya ve tehdide maruz kalmadıkça diğer ülke silahlı kuvvetlerine üs vermeyeceğini, acık bir dille izah etti (Erkin 1992: 28).

Norveç'in bu tavrı, Danimarka'nın Atlantik Paktı'na katılma kararını da tayin etmesinde kolaylık sağladı. Böylelikle iki ülke de art arda pakta katıldı. İrlanda Cumhuriyeti ise İngiltere ile aralarında toprak ihtilafı olduğundan pakta girmek istemiyordu.

Bu gelişmelerden sonra BAB'ı geniş bir ittifak sistemi haline sokmak amacı ile 6Temmuz 1948 tarihinde ABD, Kanada ve Brüksel Antlaşması'na taraf olan ülkelerin büyükelçileri arasında Kuzey Atlantik bölgesinin savunulması hakkında görüşmeler başlamıştır. 15 Mart 1949 tarihinde Danimarka, İzlanda, İtalya, Norveç ve Portekiz Kuzey Atlantik Antlaşmasına katılmaya davet edilmişler ve 18 Mart'ta Antlaşma metni yayımlanmıştır.19 Mart 1949 tarihli Ulus gazetesi "Antlaşmada hiçbir gizli hüküm yok. Paktı imza eden devletlerden birine tecavüz, hepsine tecavüz sayılacak" seklinde manşetle Türk halkına duyurdu ve antlaşmanın metnini yayınladı (Ulus, 19 Mart 1949).

31 Mart 1949'da Sovyetler Birliği Antlaşmayı imzalayacak olan 12 devlete bir memorandum göndererek antlaşma metninin BM Antlaşmasına ve Dışişleri Bakanları Konsey Kararlarına aykırı olduğunu bildirmiştir. Bunun üzerine 02 Nisan

1949 da 12 devlet müşterek bir nota vererek Sovyetler Birliği'nin bu iddialarını reddetmiştir.

Bunun üzerine ABD, Kanada ve Batı Avrupa Birliği'nin beş üyesi ile İtalya, Danimarka, Norveç, Portekiz ve İzlanda olmak üzere toplam 12 devlet temsilcileri tarafından 4 Nisan 1949 tarihinde Washington'da kısa adı NATO (North AtlanticTreatyOrganization) olan Kuzey Atlantik Antlaşması imzalanmıştır. Antlaşma, imza koyan devletlerin yasama organlarınca onaylandıktan sonrada 24 Ağustos 1949 tarihinde yürürlüğe girmiştir (İsmay, 1956: 15).

Kuzey Atlantik Antlaşması, antlaşmaya imza koyan devletlerarasında çok geniş bir iş birliğinin oluşturulması için gerekli bir çerçeve oluşturmuştur. NATO saldırıyı önlemeyi ve saldırıya karsı koymayı amaç edinmekle birlikte siyasal, ekonomik, askeri ve diğer alanlarda sürekli dayanışma ve iş birliğini öngörmektedir. Truman'ın ifadesiyle Marshall Planı ve NATO "bir elmanın iki yarısıydı."

Antlaşmaya imza koyan devletler BM Yasası ilkelerine bağlı olarak uluslararası barış ve güvenliği korumayı, Kuzey Atlantik bölgesinde istikrar ve refahı arttırmayı hedef almışlardır. Bu devletler ayrıca dış ekonomik politikaları arasındaki uyumsuzlukları gidermeyi ve aralarındaki ekonomik iş birliğini geliştirmeyi de taahhüt etmişlerdir.

NATO bir yandan ekonomik, sosyal, kültürel ve siyasi gelişmelerin önemini belirtirken, diğer taraftan da üye devletlerin kendilerini korumak için ortak bir savunma politikası izlemeleri zorunluluğunu vurgulamaktadır. Bu nedenle anlaşmanın iki yönlü olduğu söylenebilir. NATO, Birleşmiş Milletler Yasasının 51. maddesi çerçevesinde üye devletlerin savunmalarını ortaklaşa sağlamak ve birbirleriyle istikrarlı ilişkiler kurmak amacıyla imzaladıkları bir önsöz ve 14 maddeden oluşan bir belgedir (Soysal, 1991: 390). Önsözde askeri önlemlerle birlikte siyasal, sosyal, ekonomik ve kültürel alanlarda yapılacak olan iş birliğinin BM yasasına uygun olarak yapılacağı ifade edilip, antlaşmanın temel yapısı belirtilmiştir.

Birinci maddede; üye devletlerin uluslararası ilişkilerinde barısı ve dünya güvenliğini tehlikeye sokmamak için uymak zorunda oldukları temel ilkeler

tanımlanmıştır. Tarafların uluslararası uyuşmazlıkları barışçı yoldan çözmeyi istedikleri, tehditten uzak durarak zora başvurmak istemedikleri belirtilmiştir.

İkinci maddede; NATO'nun yalnız askeri amaç gütmediği belirtildikten sonra, üyelerin uluslararası her alanda iş birliği ve anlayışın egemen olmasına ve ekonomik politikalarında uyum sağlamaya çalışacakları belirtilmiş ve üye devletlerin uluslararası ilişkilerinde ve bu ilişkilerden doğan yükümlülüklerinde izlemeleri gereken yöntemler açıklanmıştır.

Üçüncü maddede; NATO'ya üye olan devletlerin silahlı bir saldırı karsısında tek tek ve toplu olarak karsı koyma esnasında güçlerinin korunması ve arttırılması gerektiği belirtilmiştir. Dördüncü maddede; üye olan devletlerden birinin toprak bütünlüğüne siyasal bağımsızlığına veya güvenliğine karsı bir tehdidin oluştuğuna inanması halinde tarafların birbirleriyle dayanışma içerisinde bulunacakları belirtilmiştir.

Antlaşmanın en önemli olan 5. maddesinde ise; üye devletlerin biri veya birkaçına karsı Atlantik'in her iki tarafında silahlı bir saldırı olması halinde bu saldırının bütün üye devletlere karsı yapılmış olacağının kabul edileceği açıklanmış ve bu durumda BM yasasının 51. maddesinde öngörülen bireysel ya da ortak savunma hakkı kullanılarak üye devletlerin bir saldırı durumundaki yükümlülükleri belirlenmiştir. Bu göre her üye devlet bu aşamada uygun gördüğü eyleme başvurmakta serbesttir ve durum BM Güvenlik Konseyi'ne de bildirilecektir.

Altıncı madde; savunulması gereken Atlantik bölgesiyle ilgilidir yani besinci madde hükümlerinin uygulanacağı bölgeyi saptamaktadır. 1949'da anlaşma imzalanırken tarafların Avrupa'daki ülkeleri, Kuzey Amerika (ABD, Kanada), Fransa'nın Cezayir eyaleti, üyelerin kimilerinin egemenliğinde bulunan belirli adalar öngörülmüştür. Daha sonra 1952'de Türkiye ile Yunanistan NATO'ya girerken imzalanan protokolün 2. maddesiyle, savunma alanı onların tüm sınırlarını koruyucu bicimde genişletilmiş arkasından 1962'de Cezayir bağımsızlığına kavuşunca bu ülke Atlantik bölgesinden çıkarılmış ve 1982'de İspanya NATO'ya katılınca da onun sınırları savunma bölgesi içine girmiştir.

Yedinci ve sekizinci maddelerde, üye ülkelerin mevcut uluslararası taahhütlerde hiçbirinin anlaşma hükümlerine aykırı olmadığı ve gelecekte anlaşma

ile ters düşecek yükümlülükler üstlenmemeyi kabul etmek zorunda oldukları açıklanmıştır. Ayrıca antlaşmanın BM'ye üye olmalarından kaynaklanan hak ve yükümlülükleri ile bağdaştığı ve BM Güvenlik Konseyinin uluslararası barış ve güvenliğin korumaktaki öncelikli rolünü etkilemediğini belirtmektedir.

Dokuzuncu maddede anlaşma hükümlerinin uygulanması için gerekli organların kurulmasını on germektedir. Onuncu madde üye devletlerin antlaşma ilkelerine uyabilecek diğer Avrupa devletlerinin pakta katılabilmesi için davette bulunabileceğini belirtmektedir.

On birinci madde üye devletlerin antlaşmayı anayasal usullerine göre onaylamaları ve antlaşmanın yürürlüğe girme surecini ortaya koymaktadır. On iki ve on üçüncü maddeler antlaşmanın on yıllık yürürlük suresinden sonra değiştirilebileceği ve yirmi yıllık bir üyelik suresinden sonra üye devletlerin istemeleri halinde üyelikten ayrılabileceğine dair hükümler içermektedir (Soysal, 1991: 391).

Tablo 1. NATO'nun Üyeleri

Amerika Birleşik Devletleri	Almanya	Arnavutluk
Belçika	Birleşik Krallık	Bulgaristan
Çekya	Danimarka	Estonya
Fransa	Hollanda	Hırvatistan
İtalya	İspanya	İzlanda
Kanada	Karadağ	Letonya
Litvanya	Lüksemburg	Macaristan
Kuzey Makedonya	Norveç	Portekiz
Polonya	Romanya	Slovakya
Slovenya	Türkiye	Yunanistan

NATO'nun21. yüzyılda gerçekleştirdiği zirveler şu şekildedir:

- Prag Zirvesi 21 – 22 Kasım 2002
- İstanbul Zirvesi 28 – 29 Haziran 2004
- Brüksel Zirvesi 22 Şubat 2005
- Riga Zirvesi 28 – 29 Kasım 2006
- Bükreş Zirvesi 2 – 4 Nisan 2008
- Strazburg – KehlZirvesi 3 – 4 Nisan 2009
- Lizbon Zirvesi 19 – 20 Kasım 2010
- Chicago Zirvesi 20 – 21 Mayıs 2012
- Galler Zirvesi 4 – 5 Eylül 2014
- Varşova Zirvesi 8 – 9 Temmuz 2016
- Brüksel Zirvesi 25 Mayıs 2017
- Brüksel Zirvesi 11 – 12 Temmuz 2018
- Londra Liderler Toplantısı 3 – 4 Aralık 2019

2.4.1. NATO'nun Siber Alanda Etkin Olma Nedenleri ve Siber Güvenlik Anlayışı

İnternetin hayatımıza girmesi ve teknolojik gelişmelerle birlikte siber alanın devletler ve öğütler bazında çok etkin bir alan olduğu ve giderek daha da etkinleşeceği tarihteki örneklerle görülmektedir. NATO üyeleri de siber arenada güvenliği artırmanın hayati önemini kavramış ve bu yönde ortak hareket etme kararı almıştır.

Üyeler bu ortak kararlarla hareket ederse NATO ulusal güvenlik için ek kaynaklar harcamak istemeyen üyelerden daha kolay "alım" yapabileceğini düşünmektedir. Küresel ticaret için siber iletişim yoluyla güvenli iletişim kesinlikle gerekli olduğundan, her büyük Avrupa ülkesinin ekonomisi için kritik öneme sahiptir. Siber alan üzerinde baskınlık olarak şu anda hiçbir devletin ezici yetenekleri

yoktur. NATO'nun, Avrupa üye ülkeleri tarafından göreceli etkisi daha yerleşik askeri arenalara yapılan yatırımlardan, çok daha büyük şekilde paranın karşılığını almayı sağlayacağı tahmin edilmektedir (Horowitz, 2010: 9).

Sabit bir coğrafi adresin bulunmadığı siber alan, doğal olarak ulusal sınırların ötesine geçerek, uluslararası hukuka ve uluslararası normların uygulanmasına ilgi duyan Avrupa devletlerinin dikkatini çekecek, uluslararası çözümler gerektirdiğini düşündürmüştür. Böylece bu alanda birlikte çalışarak, ABD ve NATO müttefikleri siber politikalarıyla norm koyucular haline gelebileceklerdir. Siber alanın ulusal güvenlik etkilerini ele almaya çalışırken, diğer Batılı müttefikler ve demokrasiler için rol modelleri olarak hizmet edebileceklerdir. Siber alan sayesinde de NATO için yeniden ortak noktalar doğmuş ve üyelerinin zaten ilgi gösterdiği, yenilenmiş bir NATO hareketi için büyük bir potansiyel olmuştur.

NATO, siber tehditler konusunda çok ciddi hazırlıkları yapan bir örgüt durumundadır. Siber Savunma Eylem Planı'na göre Siber Savunma Politikasının içine, siber alanda yapılmak istenen savunma faaliyetlerinin, 5. Madde kapsamındaki ortak savunma stratejisine alınmasında siber tehditler önemli bir paya sahiptir (Brent, 2019). Burada ortaya çıkan sorun 5. Maddede belirtilen ortak savunma koşulunun siber saldırıları kapsayıp kapsamayacağı durumu olmuştur. Yani İttifaktaki ülkelerden herhangi birinin siber saldırı türlerinden biriyle karşılaşması durumunda, anlaşma maddesinin bu durum için geçerliliği, saldıran ülkenin tespit edilmesi süresi ve saldırıyı yapan ülkeye karşı nasıl bir karşılık verileceği konusu belirsizliğini sürdürmektedir (Yayla, 2013: 207).

Ortak savunmanın olumlu yönü siber tehdit karşısında belirli bir harekât tarzı ve planlamaya sahip olmaktır. Siber saldırıya karşı hazırlıklı bir yapı oluşturulması ve riskleri önleyici çalışmalar yapılması önemli faydalar sağlamaktadır. Fakat bu şekilde yapılan bir belirleme, çizilen sınırların dışında gerçekleşen bir saldırının savunma kapsamına dâhil edilmemesine sebep olabilmektedir. Ayrıca net bir standardın getirilmesi üye devletleri gereksiz, istenmeyen ve standartları karşıladığı için ispatlanmamış, doğrulanmamış bir savaşın içine de sokabilmektedir (Horowitz, 2010: 7). Aynı zamanda siber saldırı durumlarında uygulanacak siber müdahalelerde,

gündemin belirlenmesinde İttifak üyeleri içindeki belli devletlerin baskınlığı, karar almalardaki temel sorunlardan birisi olmuştur (Güntay, 2016: 114).

2.4.2. NATO'nun Siber Güvenlik Politikaları

Asimetrik tehdit kavramının oluşması neticesinde ilk defa Münih kentinde yapılan toplantıda belirtilen akıllı savunma; uluslararası güvenlik stratejisi konuları arasına girerek bu tehditlerle mücadele kapsamında kullanılmaya başlanmıştır. Bu savunmanın temel amacı, ülkenin kaynaklarından en az biçimde yararlanarak en yüksek seviyede savunma gücü oluşturmaktır. Bu düşünce şekli 2012 yılından itibaren NATO'nun açıkladığı resmi stratejiye dâhil edilmiştir. Müteakiben, Galler'deki toplantıdan elde edilen sonuçla birlikte NATO bu konuyu kendi savunma stratejisinin yapı taşlarından biri olarak görmüştür (Bağbaşlıoğlu, 2016: 211).

NATO siber tehditler karşısında üye ülkelerin güvenliğini sağlamak için bazı konuları öncelikli olarak değerlendirmiştir. Ele aldığı ilk konu, NATO merkezinin bilişim sistemleri güvenliğinin sağlanmasıdır. SSCB'nin dağılmasını izleyen yıllardan itibaren NATO klasikleşmiş stratejisini bırakmış ve değişen koşullara göre yeni stratejiler üretmiştir. Asıl maksadını teşkil eden kolektif savunmanın gerçekleştirilmesiyle birlikte, örgütün uluslararası güç mücadelesinde etki sahasını büyüten ve NATO içerisinde yer almayan ülkelerle mevcut ilişkilerin arttırılması amacıyla sıkı bir koordinasyonu öngören güçlü ve işlevsel bir güvenlik stratejisi benimsenmiştir. Bu bakış açısıyla hazırlanan stratejilerde NATO'nun tehdit algısının miktarında ciddi bir artış olmuştur. Lizbon'da kararlaştırılan yeni güvenlik stratejisine göre nükleer silah sistemlerinin ve toplu imhayı sağlayacak diğer silahların artmasının, NATO hudutları haricinde gerçekleşen savaşların ve güvenlik krizlerinin, tüm dünya ülkelerini tehdit eden küresel terör örgütlerinin, uluslararası kanunlara aykırı olarak yapılan silah ticaretinin, kaçak narkotik maddelerin sevkiyatlarının, insanlığa karşı işlenen tüm suçların ve siber tehdit unsurlarının NATO için öncelikli güvenlik sorunları oldukları resmen açıklanmıştır (Bağbaşlıoğlu, 2016: 212).

NATO siber güvenlik kapsamında hem merkez teşkilatının hem de müttefik ülkelerin siber savunma ihtiyacını karşılaması gerekmektedir. Kullanılan bilişim

sistemi unsurlarının NATO tarafından aktif savunma anlayışı ile mutlak suretle savunulması için gerekli tedbirler alınmalıdır.

NATO'nun değerlendirdiği diğer konu, müttefiklerine kendilerine özgü siber savunma kabiliyetleri kazanmaları ve bunları geliştirmeleri konusunda destek vermektir. NATO söz konusu destek faaliyetlerini farklı yöntemlerle uygulamaktadır. Bu faaliyetlere örnek olarak; strateji oluşturmaya yardım etmek, eğitim süreçlerine destek sağlamak, tatbikatlar yardımıyla olası siber saldırılara hazırlık durumunu test etmek ve teknik konularda danışmanlık yapmak sayılabilmektedir.

Üyelerin karşılıklı beyanı ile onaylanan bu amaçlar NATO'nun sıralı birimlerince aşamalı olarak kontrol edilmektedir. Bununla birlikte, NATO'nun sağlamakta olduğu en iyi imkân Almanya'daki okul ve Portekiz'de bulunan Siber Akademi kurumu olmuştur. Bu kurumlar vasıtasıyla NATO, iyi eğitim almış, düzgün şekilde yetiştirilmiş, bilişim sistemlerine hâkim, gizlilik prensiplerine riayet eden, uygulamalarla kendini sürekli geliştiren, güncel teknolojiden en iyi şekilde yararlanan siber güvenlik personeli yetiştirmektedir.

Savunma zincirinin sağlamlığını en çürük halkanın belli edeceği düşüncesiyle, siber güvenlik unsurlarının tamamının birbirinin bütünleyicisi olması ve hepsinin tek başına da güçlü bir yapıya sahip olmaları şarttır. Dolayısıyla NATO'nun siber güvenliği için tümevarım yöntemi uygulanmaktadır. Öncelikle, her üye ülkenin ve NATO merkez teşkilatının kendi içinde siber güvenliği tesis etmesi gerekmektedir. Daha sonra, ortak kurumlar vasıtasıyla oluşturulacak genel bir stratejiyle NATO'nun genel siber güvenliği tesis edilmektedir. İşbirliği, diyalog ve koordinasyon bu çalışma faaliyetlerinde olması gereken en önemli konu olarak görülmektedir. Güç dengesinin önemli bir unsuru olan NATO, siber savunma faaliyetlerini uluslararası kamuoyuna şeffaflık içerisinde gerçek-eştirmeye devam etmektedir. BM ise, oluşturduğu bir kurul aracılığıyla uluslararası siber uzay sistemindeki hareketler için çalışmalar yapmaktadır.

Avrupa'daki başka bir güç unsuru olarak AGİT, siber güvenlik alanında savunma sistemini oluşturmak için bazı tedbirler almıştır. Alınan tedbirler

kapsamındaki kurallara uymayı onaylayan ülkeler arasındaki faaliyetlerde açıklık ve karşılıklı güven ilkesinin temel alınması kararlaştırılmıştır.

Değişen ve sürekli gelişen siber uzay her geçen gün daha çok ve daha güçlü siber tehditler içermektedir. NATO'nun siber savunmasını tam anlamıyla gerçekleştirmesi için, üyeleri arasındaki iş birliğini sağlaması, güncel teknolojik gelişmeleri takip etmesi, tehditlere karşı sürekli tatbikatlar vasıtasıyla hazırlık yapması, eğitim faaliyetlerine ağırlık vermesi, kurumlarını uygun kadro altında yeniden teşkil etmesiyle birlikte güçlü ve caydırıcı bir siber güvenlik stratejisi oluşturması bir gerekliliktir.

Bu şartlar altında NATO'nun Lizbon'daki toplantısında yeni şartlar altında güçlü bir siber savunma stratejisi oluşturulma kararı alınmıştır. NATO oluşan bu yeni tehdit karşısında savunması gerçekleştirmek maksadıyla hibrit tehditlerle mücadele edecek bir kurum kurmuştur. Bu merkezin kurulmasıyla birlikte NATO'nun müttefiki olan 9 devlet ve AB ortak bir çalışmaya dahil olmuş, siber güvenliğinin tesis edilmesi için müştereken planlanan projeyi 2017 yılında uygulamaya başlamışlardır. Merkeze ev sahipliği yapan Helsinki'de ABD, İngiltere, Fransa, Almanya, İsveç, Polonya, Letonya ve Litvanya, üyelik için bir niyet mektubuna imzalarını attılar. Bu oluşuma yeni NATO üyesi ülkelerin katılması beklenmektedir. Merkezin odaklanacağı hibrit tehditler olarak siber saldırı, propaganda ve dezenformasyon gibi, geleneksel savaştan daha az yıkıcı olduğu düşünülen ve bir ülkenin zayıf yönlerini hedefleyerek güvensizlik ortamını tetikleyen müdahaleler tanımlanmıştır.

Hibrit Merkezin kurulduğu Finlandiya'nın, Ukrayna krizinde 'hibrit kampanyalar' yürütmek ve 2016 ABD başkanlık seçimlerine karışmak ile suçlanan Rusya ile 1.300 kilometrelik bir sınırı bulunmaktadır. Rusya ABD'deki seçimlere karıştığı yönündeki iddiaları yalanlamıştır.

Helsinki'deki merkezde, üye ülkeler için uzmanların bir araya geldiği bir ağ teşkil edilmiştir. Merkezin AB ile NATO arasındaki iş birliğinin gerçek anlamda artırılması anlamına geldiğini kaydeden Finlandiya Dışişleri Bakanı Timo Soini, "hibrit faaliyetlerin Avrupa'nın güvenlik çabalarında sürekli rol oynayan bir etken haline geldiğini" belirtmiştir.

Finlandiya Dışişleri Bakanı Soini, kurulan yeni merkez ile hibrit tehditler ve toplumların hibrit operasyonlar ile vurulabilecek zayıf noktaları hakkındaki farkındalığın artırılmasının hedeflendiğini belirtmiştir. Bakan, "Hibrit stratejilerin kullanılması, toplumlarımızın iç tutarlılığını ve direncini test ediyor. Buna verilecek karşılığın, yalnızca devlet kaynaklı değil, aynı zamanda toplumsal bir direnç, güvenlik için kapsamlı bir yaklaşım olması gerekir" şeklinde demeç vermiştir.

Hibrit Merkezin yıllık bütçesi başlangıçta yaklaşık 1,5 milyon Euro olarak belirlenmiştir. Bu miktarın yarısı Finlandiya tarafından karşılanırken, diğer yarısı diğer üyeler tarafından üstlenilmiştir.

2.5. Siber Saldırıya Uğramış Seçili Ülkelerin Siber Güvenlik Çalışmaları

2.5.1. ABD

Kendisine yapılan siber saldırıları bir savaş sebebi olarak değerlendireceklerini açıklayan ABD dünyaya sunduğu siber ortamı ve icat ettiği 5.boyut silah karşısında kendisini bile korumaya çalışmakta ve bu sebeple yeni güvenlik stratejileri geliştirmektedir (Kara, 2013: 55).

ABD'nin siber güvenlikle ilgili ilk geniş ve kapsamlı belgesi 2003'te Beyaz Saray'ın yayınladığı Güvenli Siber Uzay (SecureCyberspace) belgesidir. Bu belgede "siber güvenlik" terimi sadece 3 defa kullanılmakta ve siber güvenlik yerine çoğunlukla güvenli siber uzay veya siber alan kelimelerine yer verilmektedir (WH, aktaran Göçoğlu, 2018: 102). Bu belgede, ulusal güvenliğin sağlanması için aşağıdaki önceliklere yer verilmiştir.

ABD 2003 yılında yayınladığı belge dışında siber güvenlik politikası üzerine, ulaşılabilir diğer bazı belgeler de yayınlamıştır (WH, aktaran Göçoğlu, 2018: 103). 2008 yılının ocak ayında eski Başkan George W. Bush'un imzaladığı Kapsamlı Ulusal Siber Güvenlik Girişimi (ComprehensiveNationalCybersecurityInitiative: CNCI) adlı ve bazı büyük çaplı politika değişikliklerini içeren bir belge ile siber politikasını yenilemiştir (Kara, 2013: 57). Bunlara ek olarak 2011'de yeni bir siber güvenlik strateji belgesi yayınlamıştır, bu belgede 5 stratejik öncelik bulunmaktadır (Göçoğlu, 2018: 103).

1. Savunma Departmanının (Department Of Defense: DOD) siber uzayın tüm potansiyeline hâkim olabilmesi için onu organize etmek, geliştirmek ve donatmak üzere operasyonel bir bağlam olarak ele alması.
2. DOD sistem ve ağlarını korumak için yeni operasyonel savunma içerikleri temin etmek.
3. Bütünsel bir siber güvenlik stratejisi oluşturmak üzere diğer devlet ve özel sektör kurumlarıyla iş birliği içinde olmak.
4. Kolektif siber güvenliği sağlamak için ABD müttefikleri ve uluslararası ortaklarla güçlü ilişkiler kurmak.
5. Daha iyi bir siber güç ve teknolojik inovasyon kabiliyeti için ulusun yaratıcılığını artırmak.

DOD 2013'te, "Savunma Bölümünün Ağları, Sistem ve Bilgiyi Savunma Stratejisi" adında bir belge yayınlamıştır. Bu belgede stratejinin temel amaçları yer almaktadır bunlar; Esnek bir siber savunma yapısı oluşturmak, Siber savunma operasyonlarını dönüştürmek, Siber olay farkındalığını geliştirmek ve çok geniş ve kapsamlı siber saldırılara karşı koyabilecek sistemler geliştirmektir (Göçoğlu, 2018: 107).

2003 yılında yayınlanan belgede yer alan ve siber güvenliğin sağlanmasından sorumlu olan İç Güvenlik Bakanlığı (Department of Homeland: DHS) siber savunmanın sağlanması için 2 taraflı bir yaklaşım ortaya koymuştur. Bilgisayar Acil Durum Hazır Ekibi Koordinasyon Merkezi ile DHS işbirliği yaparak federal sivil ağları kurumak için ABD Siber Acil Müdahale Ekibi (United StatesComputerEmergency Readiness Team: US/CERT) kurmuştur.

2.5.2. İsrail

Siber güvenlik konusu ile yakından ilgilenen ülkelerden biride İsrail'dir, ulusal güvenliğin ana yatırımlarına ek olarak, 82 milyar dolarlık bir siber güvenlik endüstri hacmi bulunmaktadır. Ülkede 2017'den bu yana siber güvenlik alanında çalışmakta olan 150 aktif firma mevcuttur (BVP, aktaran Göçoğlu, 2018: 105). İsrail'in siber güvenlik alanında en büyük imtihanı, 2014 yılında Gazze'ye gerçekleştirdiği saldırıdan sonra Filistin'in yanında olduklarını göstermek için

Türkiye dâhil bazı ülkelerden başlatılan çeşitli siber saldırılarla karşı karşıya kaldığı zaman olmuştur. Bu saldırılar İsrail'in devlet kurumları, iletişim altyapıları, Adalet Bakanlığı, Devletin Arşiv Portalı ve Ulusal Reklam Ajansı gibi birçok bakanlık ve kurum web sitelerini hedef almıştır (Aljareeza'dan, aktaran Göçoğlu, 2018: 105).

Çok sayıda siber saldırıya maruz kalmasına rağmen, İsrail siber güvenlik ve savunma stratejisi iyi olan ülkelerden biridir. Ülke siber güvenlikten sorumlu 4 temel kuruluşa sahiptir. Bunlar;

- İsrail Savunma Kuvvetlerine bağlı olarak, 1952'de kurulan Birim 8200, askeri personel ve subaylardan oluşmakta ve odak alanları ise İstihbarat toplamak, savunma yapmak ve saldırı gerçekleştirmektir.
- Shin Bet: Bu birim ülkedeki bilgisayar sistemlerinin güvenliğini sağlamak, ulusal altyapı ve devlet yöntemlerinin savunmasını sağlamak ile görevli olan iç istihbarat birimidir.
- Komuta, Kontrol, Haberleşme, Bilgisayar ve İstihbarat (Command, Control, Commonications, Computers, Intelligence: C4I): Bu birim tüm sistemlerden, kolordu haberleşme ve siber savunma çalışmalarından sorumludur,
- 2012'de kurulan ve görevi bilgisayar sistemlerindeki siber saldırılara karşı savunma yapmak olan İsrail Ulusal Siber Bürosu (IsraelNationalCyberBureau: INCB), bu birim aynı zamanda güvenlik sistemlerini, iş ve akademi dünyası ile işbirliği yaparak savunma sistemlerini organize etmeyi hedeflemektedir (Kara, 2013: 57).

İsrail, siber güvenliğini devlet içinde gerçekleştirdiği organizasyonlar ve uyguladığı politikalarla beraber uluslararası anlaşmalar ve iş birlikleri ile de sağlamaya gayret göstermektedir. Bu hususta en büyük müttefiki Amerika olmasına rağmen başka devletlerle de iş birliği yapmaktadır. Ülke, siber güvenlik ile ilgili yaptığı faaliyetlerden ötürü siber tehditlere karşı en hazırlıklı devletlerden biri olmanın yanı sıra ülkede siber güvenlik konusu devlet ve halkın ortak bir çalışma alanı ve sorumluluğu olarak kabul edilmektedir. Bu ülke, kritik işlemlerini internet ağından farklı bir Ethernet ağ üzerinde tutmakta ve böylece sistemlerini harici

tehditlere karşı korumaktadır (Yılmaz &Sağıroğlun'dan, aktaran, Göçoğlu, 2018: 110).

2.5.3. Çin

Çin siber güvenlik ve iletişim teknolojilerine 20. Yüzyılın sonlarından, yani bu teknolojilerin ortaya çıktığından beri önem vermektedir. İlk önce 1986'da ekonomik bilgilerin yönetimi ile ilişkin küçük bir ekip kurulmuş ve 2001 yılına kadar etkin olarak görev yapmıştır. 2003'te ise siber güvenlikle ilgili Belge 27 isminde ilk sivil belge yayınlanmıştır. BİT'lerin artmasından dolayı ülkede, siber suç ve siber saldırılar çoğalmış ve siber güvenlik konusu bu ülkenin de öncelik verdiği bir konu olmuştur. Çin'in Siber güvenlik konusunda bakış açısı da başka ülkelerle hemen, hemen aynıdır. Fakat tehditlere karşı ülkenin uyguladığı siber güvenlik yöntemi daha ulusal ve uluslararası platforma nispeten kapalı olduğundan dolayı batı ülkelerine göre farklılık göstermektedir. Bu ülkenin, başka ülkelerden farkı ise kendi ulusal siber ağlarını kullanarak ve dünyada yoğun olarak kullanılan birçok ağın kullanmasına yasak getirerek ya da kullanımını kısıtlayarak en etkili savunma sistemlerini geliştirmiş olmasıdır. Bu şekilde izlenen bir yöntem ülkeyi, siber güvenlik açısından batı ülkelerine göre daha güvenli kılmaktadır (Göçoğlu, 2018: 111).

Çin bir yandan Ulusal Kalkınma Stratejisi her alanda bilişim teknolojilerinin geliştirilmesini ve kullanılmasını önerirken, diğer yandan da temel bilgi ağlarının ve kritik alt yapılarının, güvenlik sistemlerini güçlendirilmesini göz önünde bulundurmuştur. Ülkenin siber güvenlik ve siber savunmasının sorumluluğu Halk Kurtuluş Ordusu (PeoplesLiberationArmy: PLA) tarafından sağlanmaktadır. Buna ek olarak, binlerce uzman personelden oluşan ve devlet tarafından desteklendiği düşünülen Çin 61398 nolu birliği 2006'dan beri faaliyet göstermektedir (Kara, 2013: 60).

Ülkede 2014 öncesi yapılan çalışmalarda siber güvenlik ve sistemsel altyapılara önem verilmiş, devletin oluşturduğu konsey bilgisayar bilgi güvenliği yöntemleri kurulmuş, Kamu Güvenliği Bakanlığı (Ministry of Public Security: MPS) tarafından zararlı yazılımlara karşı savunma ve internet için bazı standartlar geliştirilmiştir. 2014 yılında ise siber güvenlik grubu, Çin devlet başkanı XiJinping

önderliğinde kurulmuş ve yapılan çalışmalara aynı yılın hükümet raporunda yer verilmiştir. 2015'te Ulusal Halk Kongresi Daimî Komitesi (StandingCommittee of theNationalPeople'sCongress: SCNPC) kamu oy birliği ve vatandaşların fikirleri dikkate alınarak Siber Güvenlik Kanunu tasarlanmıştır. Kongre bu kanunu, 2016 yılının haziran ayında 2.defa tartışmaya açarken, temmuz ayında ise Siber Güvenlik Kanunun son halini resmi internet sayfasında yayınlayarak kamuoyunun ilgisine sunmuştur (Göçoğlu, 2018: 112).

2.5.4. Rusya

Siber güç alanında en önemli ülkelerden biri olan Rusya, 2000 yılının başlarından bu yana, siber uzay alanında etkisini göstermek niyetiyle plan ve strateji geliştirmektedir. 1979 ve 1989 yıllarında gerçekleşen Afganistan savaşı sırasında, Sovyet Ordusu psikolojik savaş tekniklerini kullanamamış ve Moskova Riyaseti Afganistan'daki bağlantıları ile etkili bir haberleşme sağlayamamıştır. Bunun yanı sıra 1994 ve 1996 yıllarında Çeçen Savaşında da internet üzerinden yapılan iletişimin başarısızlığından dolayı savaş sırasındaki gelişmeler Rusya açısından oldukça olumsuz olmuştur. Bu iki olayın olumsuz sonuçlanmasıyla, Rus devleti siber güvenlik ve askeri ağ teknolojilerini hızla geliştirmeye başlamıştır (Darıcılı, 2017: 420).

24 Ocak 2000 yılında Rusya Federasyonu Ulusal Güvenlik Konsepti (National Security Concept of the Russian Federation: NSCRF) belgesi yürürlüğe girmiştir. Bu belgede genel olarak, bilişim güvenliğinin önemi ve bu konuda ülke menfaatlerine yönelik harici ve dâhili tehditlere karşı alınacak önlemler ele alınmaktadır. Ayını yılın Eylül ayında belirlenen ve ülkenin siber güç olma yönündeki ilk ana belgesi olan Rusya Federasyonu Bilgi Güvenliği Doktrini (Information Security Doctrine of the Russian Federation: ISDRF) belirtilmiştir. Söz konusu belge, ülkenin bilgi güvenliği ile ilgili çalışmalarını, prensiplerini, hedeflerini ve konu ile ilgili resmi görüşlerini genel hatlarıyla kapsamaktadır. Belgede, biri ülkenin siyasi ve kültürel yapısına etki yaratabilecek psikolojik savaş diğer ise siber savaş olarak iki tehdit kaynağına odaklanılmıştır (Darıcılı, 2017: 420).

Rusya'nın 2015 yılında yayınladığı ulusal güvenlik stratejisinde güvenlikle ilgili kişisel, kamusal, çevresel, ekonomik, ulaştırma ve enerji güvenliği konuları

özel olarak ele alınırken, belgede "siber güvenlik" terimi hiç kullanılmamakla beraber ulusal güvenlik tehdidi, ulusal menfaatlere direk veya endirekt olarak hasar verebilecek tüm durumlar ve faktörler olarak tanımlanmıştır (Göçoğlu, 2018: 116).

2020'ye doğru Rus Ulusal Güvenlik Stratejisi (Russia'sNational Security Strategyto 2020) belgesine bakıldığında bütünüyle güvenlik konusuna odaklanmış bir belge olduğu görülmektedir. Bu belgede, öncelik ekonomi olmakla beraber, sağlık ve güvenlik stratejisi ile ilgili fikir ve düşünceler yer alırken, bilgi güvenliğinden dolaylı bir şekilde bahsedilerek belgenin hedefinin güven artırıcı ve iş birliği olduğu anlaşılmaktadır (Darıcılı, 2017: 420). Bu belge aynı zamanda, federal devletleriyle Rusya'nın uluslararası bilgi güvenliğini sağlamak için, devletlerarası amaçlarını, konu hakkında hukuki ve örgütsel fonksiyonlarını da içerecek şekilde, daha gelişmiş bir uluslararası bilgi güvenliği sistemi olarak hazırlanmıştır. Belge, bilgi güvenliği yönünden 2000 yılının belgesine göre daha geniş tanımları içermektedir (Göçoğlu, 2018: 120).

Ülkede; Federal Güvenlik Servisi (Federal Security Service: FSB), Dış İstihbarat Servisi (ForeignIntelligence Service: SVR) ve askeri Ana İstihbarat Direktörlüğü (Main IntelligenceDirectorate: GRU) siber güvenlik alanında görev yapan ve ülkenin siber savunma ve saldırı gücünü belirleyen kurumladır. Bunlardan GRU, Savunma Bakanlığı'na bağlı olarak Rus Silahlı Kuvvetlerinin (RSK) emrinde çalışırken FSB ve SVR, doğrudan Rusya Devlet Başkanı'na bağlı çalışmaktadır. FSB'nin görevi siber saldırılarla mücadele etmek ve ülke siber güvenliğini sağlamaktır (Darıcılı, 2017: 420). Diğer taraftan çalışmanın kayda değer bir konusu da Rusya'nın siber güvenliğe bakış açısı saldırıdan daha çok savunmaya yönelik olmasıdır. Fakat gelişim sürecinde saldırıya saldırı anlayışıyla güvenlik düşüncesini değiştirerek farklılaştırdığı görülmektedir (Göçoğlu, 2018: 113).

2.5.5. İngiltere

Bu ülke 2009 yılında kraliçenin buyruğu ile Siber Güvenlik Stratejisi Birleşik Krallık Güvenlik/Güvenlik ve Siber Alanda Dayanıklılık (Cyber Security Strategy Of The United KingdomSafety/Security AndResilience İn Cyber Space: CSSUKS/SRCS) adlı ilk siber güvenlik strateji belgesini yayımlanmıştır. Bu belgede bir yandan şirketler, devlet ve vatandaşların siber tehditlerle karşı karşıya olduğu

açıklanırken diğer yandan daha geniş bir şekilde hazırlanan Ulusal Siber Güvenlik strateji belgesi yayınlanmıştır. Bu belgede devleti, şirket ve halkın korunması gerektiği vurgulanırken, siber alandan gerçekleşebilen tüm siber suçlara karşı nasıl korunması gerektiğine dair açıklamalara yer verilmiştir. Aynı yılın Haziran ayında, stratejik liderliği sağlamak ve Birleşik Krallık Siber Güvenlik Stratejisini geliştirmek ve koordine etmek için Siber Güvenlik Ofisi Kurulmuştur. İngiltere 2010'da Siber Suç Stratejisi (CyberCrimeStrategy) belgesini yayımlanmıştır. Bu belgenin amacı, 2009'da ki Siber Güvenlik Strateji politikasını koordine etmek ve uygulamak, siber güvenlik ofisinin diğer bölümler ve ajanslarla birlikte hareket etmesini sağlamak, özellikle gelişen tehditlere karşı hazırlıklı olmak için Siber Suç Stratejisinin geliştirilmesini ve Siber Güvenlik Ofisi çatısı altında gelişen işlemlere uyumlu olmasını sağlamaktır (Alioğlu, 2019: 39).

2011 yılının Kasım ayında ülke; Dijitalleşen Dünya'ya Birleşik Krallığı Taşımak ve Korumak" adlı başka bir strateji dokümanı yayımlayarak Ulusal Siber Güvenlik planını detaylı olarak ele almış ve ülkenin siber güvenliği ile ilgili önemli değişikliklere gidilmiş ve bu çerçevede pek çok yeni kurum oluşturulması için faaliyetlere başlanmıştır. Bu strateji belgesine göre ülkenin 2015 yılının siber güvenlik vizyonunun dört temel amacı olacaktır.

Mart 2014'te kurulan ve ülkenin ulusal siber güvenlik vakalarına karşı tedbirli olmasından ve düzenlenmesinden sorumlu olan İngiltere Ulusal Bilgisayar Acil Müdahale Ekibi (United KingdomNationalComputerEmergencyResponse Team: UK/CERT), aynı zamanda hükümet kuruluşları ve endüstriyel ortaklarla tatbikatları yapmak, akademik kurumlar ve özel sektörle bilgi paylaşmakla görevlidir. Mayıs 2015'te ise güncellenen 2010 - 2015 İngiltere Devlet Siber Güvenlik Politikası (2010 To 2015 GovernmentPolicyCyber Security) adlı politika belgesini yayımlamıştır (Alioğlu, 2019: 39).

2016 yılının Kasım ayında ülkenin son Ulusal Siber Güvenlik Stratejisi (NationalCyber Security Strategy 2016 to 2021) yayınlanarak 5 senelik ulusal siber güvenlik strateji raporu açıklanmış ve siber güvenlikle ilgili alanlarda 1.9 milyar sterlin yatırım yapılmıştır. Aynı yılın Aralık ayında Siber Güvenlik Düzenlemesi ve Teşvikler İnceleme (Cyber Security RegulationsandIncentivesReview: CSRIR) adlı

bir inceleme belgesi daha yayınlanmıştır. Yine aynı yılın Ekim ayında ülkenin Ulusal Siber Güvenlik Merkezi (NationalCyber Security Center: NCSC) kurulmuş ve resmi açılışını 14 Şubat 2017'de Kraliçe yapmıştır. Kasım 2016'de yayınlanan belgede 2021 yılına kadar ülkenin siber güvenlik vizyonu siber tehditlere karşı güvenilir olmak, saldırılara karşı dayanıklı olmak ve güçlü durmak şeklinde ifade edilerek vizyonun sağlanması için Savunma, Caydırma ve Gelişme olarak 3 ana başlığı dikkatte almışlardır (Alioğlu, 2019: 42).

2.5.6. Almanya

Bu ülkede bilgi güvenliği için başlatılan faaliyetler siber güvenlik terimi meydana gelmeden çok daha eskilere dayanmaktadır. İkinci Dünya Savaşı esnasında Nazi Almanya'nın kullandığı Enigma isimli aygıt, Alman askerleri arasında gizli bilgiler için şifre kullanılması ve bu şifreleri tekrar çözülmesi için yararlanılan ve aynı zamanda başka devletlerin iletişim bilgilerini de deşifre edebilen bu aygıt tarih sayfalarında kendine yer bulmuştur. Ülkenin siber güvenlik stratejisini çoğunlukla Alman ordusu belirlemektedir. Fakat siber güvenliğin oldukça kapsamlı olması ve siber saldırıların nasıl, nerden gelebileceğinin ve hangi büyüklükte olduğunun bilinmediğinden dolayı birçok uluslararası kuruluşla da iş birliği yapmaktadır (Göçoğlu, 2018: 114).

Ülkenin siber güvenlikle ilgili düzenlediği belgelere bakıldığında ilk defa 1989'da Ulusal Politika belgesi yayınlanmıştır. Daha sonra 2005'te Bilgi Güvenliği ve Kritik Altyapıların Korunması ile ilgili Ulusal Strateji Belgesi yürürlüğe konulmuştur. Bu belgeden sonra 2011'de yayımlanan Alman Ulusal Siber Güvenlik Stratejisi, özellikle siber ortamdan gelebilecek risk ve tehditlere karşı koyabilmek için odaklanmıştır. Ülkenin siber güvenliğinin sağlanması için temel yapı olarak önemli katkılarda bulunan Alman Federal Bilgi Güvenliği Örgütünün birimlerine ise siber güvenlik ile ilgili uzmanlaşan bir politika takip etmektedirler. Bu örgüt, Siber Güvenlik Dairesi, Kriptoloji Dairesi, Güvenli Elektronik İşlemler Sertifikasyon ve Standardizasyon Dairesi, Profesyonel Ağ Savunma Birimi gibi birimleri içermektedir (Tuluk &Seferoğlun'dan, aktaran Göçoğlu, 2018: 114). Almanya'da gün geçtikçe karmaşıklaşan bilgi altyapılarına ve güvenlik zafiyetlerine bakıldığında, siber güvenlik durumu ilerleyen zamanlarda da kritik bir şekilde devam edecektir. Alınması gereken bazı stratejik amaçlar ve tedbirler vardır.

ÜÇÜNCÜ BÖLÜM

TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKALARI

3.1. Türkiye'nin Siber Güvenlik Politikaları

Hukuki Düzenlemeler Türkiye Cumhuriyeti Anayasası: Madde 20: Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir (TBMM, Ek fıkra: 12/9/2010-5982/2 md).

5070 sayılı Elektronik İmza Kanunu: Bir ve ikinci maddede amaç ve kapsam şu şekilde belirtilmiştir. "Bu Kanunun amacı, elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasları düzenlemektir." "Bu Kanun, elektronik imzanın hukukî yapısını, elektronik sertifika hizmet sağlayıcılarının faaliyetlerini ve her alanda elektronik imzanın kullanımına ilişkin işlemleri kapsar" (TBMM, 2004).

6 Haziran 1991 tarihli 3756 Sayılı Türk Ceza Kanunu'nun Bazı Maddelerinin Değiştirilmesine Dair Kanun ile Türk Ceza Kanunu'nda ilk defa siber suçlardan bahsedilmiştir (Bıçakcı vd. 2015: 4). Bu değişikliğin 20. maddesi ile "Bilişim Alanında Suçlar" başlığı altında; "bir bilgisayardan programların, verilerin veya diğer unsurların hukuka aykırı olarak ele geçirilmesi veya bunların başkasına zarar vermek üzere kullanılması, nakledilmesi veya çoğaltılması yasayla ceza unsuru" olarak kabul edilmiştir (TBMM, 1991). Eylül 2004 tarihli 5237 sayılı Türk Ceza Kanunu ile birlikte siber suç kavramı genişletilmiş ve üç adet bilişim suçu belirlenmiştir (Bıçakcıvd, 2015: 4).

Bu suçlar 243.maddeyle başlayıp bilişim sistemine girme fiilini tanımlamaktadır. Buna göre "bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye" ceza verileceğini hükme bağlamıştır. 244. Madde ile bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi, değiştirilmesi veya taşınması suçları hükme bağlanmaktadır. 245. madde kredi kartı ve banka dolandırıcılıklarına ilişkin ve son olarak 246. madde ise bu suçların işlenmesi suretiyle haksız menfaat sağlayan tüzel kişiler hakkında hükümler içermektedir (Hekim ve Başıbüyük, 2013: 149-150). Buna ek olarak TCK 9.Bölüm Kişilere Karşı Suçlar bölümünde özel hayata ve hayatın gizli alanına karşı suçlar başlığı altında 132.madde haberleşmenin gizliliğinin ihlal edilmesi, 133.madde kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması, 134.madde özel hayatın gizliliğinin ihlal edilmesi, 135.madde kişisel verileri kaydedilmesi, 136.madde verileri hukuka aykırı olarak verme veya ele geçirme ve son olarak 138.madde verileri yok etmeme suçlarını hükme bağlamıştır. Bunun dışında 124. Madde hürriyete karşı suçları, 125.madde şerefe karşı suçları, 142. ve 158. maddelerde malvarlığına karşı suçları, 226.maddede ise genel ahlaka karşı suçları işlemiştir (Aytekin, 2015: 112-120).

2000'li yıllarda, Türkiye, siber uzayın ülkenin milli güvenliği açısından önemine daha fazla ilgi göstermeye başlamış ve buna yönelik yapılan bir değişiklik ile siber suçlar 3713 sayılı Terörle Mücadele Kanunu'nda yerini almıştır. Devlet Planlama Teşkilatı (DPT), kamu hizmetlerinin sağlanması ve internet kullanımının düzenlenmesi ile ilgili olarak "e-Türkiye İnisiyatifi Eylem Planı 2002", "e-Dönüşüm Türkiye Projesi ve Kısa Dönem Eylem Planı (2003-2004)" ve "e-Dönüşüm Türkiye Projesi 2005 Eylem Planı" yayınlamıştır (Bıçakcıvd, 2015:4-5). E-Dönüşüm Türkiye Projesi ile e-devlet uygulaması sayesinde devletin vatandaşlara, vatandaşların da devlete karşı vazife ve hizmetlerini karşılıklı bir şekilde elektronik ortamda kurulacak iletişim yoluyla güvenli ve kesintisiz olarak yürütülmesi amaçlanmıştır (Önen ve Kurnaz, 2017: 745).

DPT tarafından 2005 yılında "Bilişim Toplumu Stratejisi" isimli bir çalışma ile 2006-2010 strateji belgesi ve eylem planı yayınlanmıştır; güvenlik ve kişisel bilgilerin gizliliği bu planın ana temalarından birini oluşturmuştur. Aynı zamanda Bilgisayar Olaylarına Acil Müdahale Merkezi (SOME) kurulacağı da belirtilmiştir.

Sorumlu kurum olarak da Türkiye Bilimsel ve Teknik Araştırma Kurumu (TÜBİTAK) altındaki Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) atanmıştır (Bıçakcıvd, 2015: 4-5). Siber uzayın güvenliğinin sağlanması ve siber uzayda işlenen suçlarla mücadele edebilmek adına atılan önemli adımlardan biri de internet ağlarıyla işlenen suçlara yönelik uluslararası bağlayıcılığı bulunan belki de ilk ve tek sözleşme olan "Sanal ortamda İşlenen Suçlar Sözleşmesi'dir. Budapeşte Sözleşmesi olarak da bilinen ve Avrupa Konseyi (AK) bünyesinde hazırlanan bu sözleşmenin amacı sanal ortamda işlenen suçların ortak tanımının yapılması ve uluslararası iş birliği rejiminin oluşturulmasıdır (Çeliktaş, 2016: 82-83).

Siber Güvenlik kavramının Türkiye'de de pek çok farklı tanımı yapılmıştır Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının tanımına göre siber güvenlik; "siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunması, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınması, saldırıların ve siber güvenlik olaylarının tespit edilmesi, bu tespitlere karşı tepki mekanizmalarının devreye alınması ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesidir. Siber saldırı ve tehditlerin sayısındaki ve etkilerindeki artış ile beraber, dünya ülkeleri ve uluslararası örgütlerin siber güvenlik ve güç kapasitelerini artırma çabalarına paralel olarak Türkiye de bu alandaki çalışmalarına yoğunluk vermiştir. Bu çalışmalar kapsamında da 2009 yılında siber güvenlik ile ilgili ilk resmi nitelikteki belgesi olan "Ulusal Sanal Ortam Güvenlik Politikası" hazırlanmıştır. Bu politikanın ana başlıkları arasında tehditler, açıklıklar, temel ilkeler ve siber güvenlik adımları yer almıştır. Ancak bu adımların uygulanmasına dair bir strateji veya eylem planı bulunmamaktadır (Çeliktaş, 2016: 77-78).

Siber saldırı ve tehditler ülkemizde uzun bir süre siber suç ve terörle mücadele kapsamında değerlendirilmiştir. Ancak bu saldırı ve tehditlerin milli güvenliği etkilemesi üzerine Milli Güvenlik Kurulu'nun (MGK) 27 Ekim 2010 tarihinde gerçekleştirdiği olağan toplantısında siber güvenlik konusu ilk defa gündeme alınmış ve "Siber tehdidin küresel düzeyde ulaştığı boyut ve bu tehdidin ulusal güvenliğe etkileri kapsamlı olarak ele alınmıştır. Bu bağlamda, siber tehdidin engellenebilmesi acısından millî düzeyde yürütülen çalışmalar değerlendirilmiştir" açıklaması ile bundan sonra ulusal güvenlik politikası kapsamında, siber güvenlik

üzerine yapılan çalışmalara ağırlık verileceği ifade edilmiştir. Olağan toplantı sonrası yayınlanan basın bildirisinde ise siber saldırı ve tehditlerin kamuoyunda "Kırmızı Kitap" olarak adlandırılan Milli Güvenlik Siyaset Belgesi'ne girmesine karar verildiği açıklanmıştır. 2010 yılı sonrasında Türkiye de yapılan çalışmalar, hazırlanan strateji belgeleri ve kurumsal yapılanmalar ile birlikte siber savunma ve saldırı kapasitesini geliştirme yönünde adımlar atmaya başlamıştır (Darıcılı, 2019: 15).

3.1.1. Kurumsallaşma ve Kurumsal Faaliyetler

Türkiye'nin resmi siber güvenlik alanında kurumsallaşması üç temel hedef kapsamında gerçekleşmiştir. İlk grupta yer alan kurumlar kendi alanları dâhilinde istihbarat yoluyla siber suçlarla mücadele etmek amacıyla kurulmuşlardır. Bunlar İçişleri Bakanlığı bünyesinde oluşturulan Emniyet Genel Müdürlüğü (EGM) Siber Suçlarla Mücadele Daire Başkanlığı, Jandarma Genel Komutanlığı (JGK) Bilişim ve Teknik İstihbarat Başkanlığı, Sahil Güvenlik Komutanlığı İstihbarat Daire Başkanlığı Siber Suçlarla Mücadele Şube Müdürlüğü'dür. İkinci grupta yer alanlar kurumlar, kritik altyapıların korunması ve Türkiye'nin siber savunma ve saldırı kapasitesini genişletme amacıyla kurulmuş kurumlardır. Bunlar BTK, MİT Başkanlığı, Afet ve Acil Durum Yönetimi (AFAD) Başkanlığı, TSK Siber Savunma Komutanlığı ve TÜBİTAK'tır. Üçüncü grupta ise devlet destekli özel girişimler yer almaktadır. Savunma Teknolojileri Mühendislik, Hava Elektronik Sanayii (HAVELSAN) ve Askeri Elektronik Sanayii (ASELSAN) bu kurumlardandır. Siber Güvenlik Kurulu (SGK) ise Türkiye'nin politikalarının oluşturulması ve siber güvenlik hedeflerinin tespiti ve yönetiminden sorumlu üst kuruldur (Darıcılı, 2019: 20-23).

3.1.2. Bilgi Teknolojileri ve İletişim Kurumu

Ocak 2000'de 4502 sayılı Kanunla kurulan ve telekomünikasyon sektörünün düzen ve denetiminin yerine getirilmesi amacıyla bağımsız olarak kurulan Telekomünikasyon Kurumu, Kasım 2008'de 5809 sayılı Elektronik Haberleşme Kanunu ile birlikte getirilen bir düzenleme sonrası Teknolojileri ve İletişim Kurumu adını almıştır (BTK, 2017). BTK telekomünikasyon sektörünün düzenleyici kurumudur. Görevleri arasında Yetkilendirme, denetleme, uzlaştırma, tüketici

haklarını korunma, rekabetin tesisi ve korunması, teknik düzenlemeler, spektrum yönetimi ve denetimi yer almaktadır (BTK, 2017). "06.02.2014 tarihinde yayımlanan 6518 saylı kanun ile 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'na bazı maddeler eklenerek ilgili Bakanlar Kurulu kararı güncellenmiş, Bilgi Teknolojileri ve İletişim Kurumu'na siber güvenlik ile ilgili yeni görevler verilmiştir" (BTK, 2017). BTK aynı zamanda bilgi teknolojilerinden sorumlu otorite olarak bu görevi Telekomünikasyon İletişim Başkanlığı (TİB) vasıtasıyla yerine getirmektedir. Telekomünikasyon araçları vasıtasıyla yapılan iletişimin ve sinyal bilgisinin takibi, gözetlenmesi, değerlendirilmesi ve kayıt edilmesinden sorumlu olan TİB aynı zamanda internet hizmetinin emniyetinin sağlanması için sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcılarının denetlenmesinden de sorumludur (Bıçakcıvd, 2015: 7).

3.1.3. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı

Türkiye'de siber güvenliğin sağlanması ile ilgili gerekli kamu kurum ve kuruluşlarının, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB)'nin çıkardığı plan, program, esas ve standartlarına uyma zorunluluğu bulunmaktadır. 2012/3482 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" UDHB'nin ulusal siber güvenliğine ilişkin görev ve yetkileri; ilgili politikaların belirlenmesi, strateji ev eylem planlarının oluşturulması, ulusal ve uluslararası kuruluşlarla iş birliği yapılması, siber güvenlikle ilgili farkındalık ve bilinçlendirmelerin artırılması, SGK'nın sekretaryasını yapmak, uzman personelin yetiştirilmesi şeklinde özetlenebilir (Bıçakcıvd, 2015: 12).

Bilgi Güvenliği Derneği tarafından yayınlanan tavsiye niteliğindeki belgede de benzer bazı adımların atılması gerektiğinin altını çizmiştir; Bu adımlardan bazıları Siber Güvenlik Strateji Belgesinin yayınlanması, Siber Güvenlik Kurulu oluşturulması, uluslararası işbirliğinin sağlanması, siber güvenlik alanında bilimsel çalışmalar yapılması, gerekli yasal mevzuatın düzenlenmesi şeklinde sıralanabilir (Bıçakcıvd, 2015: 10).

Bu belge Bilgi Güvenliği Derneği'nin üyeleri tarafından Türkiye'nin belirlediği hedeflere ulaşmasında yol göstermek amacıyla oluşturulmuş "Siber

Güvenlik Ulusal Strateji Belgesi" taslak metninin ve 19 Haziran 2012'de düzenlediği "Ulusal Siber Güvenlik Strateji Çalıştayı" sonuçları ile şekillendirildiği bir öneri belgesidir (Bilgi Güvenliği Derneği, Ulusal Siber Güvenlik Stratejisi, 2012: 10).

3.1.4. Siber Güvenlik Kurulu

Bakanlar Kurulu tarafından 2012 yılında çıkarılan 3843 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" ile kurulmuştur (Önen ve Kurnaz, 2017: 742).

Siber Güvenlik Kurulu (SGK)'nın görevleri; siber güvenliği ilgilendiren politika, strateji ve eylem planlarının onaylamak, kritik altyapıların belirlenmesi kapsamında teklifleri karara bağlamak ve kanunla verilen diğer görevleri icra etmek şeklinde özetlenebilir (BTK, 2017).

SGK'nin kurulmasından sonra Türk Silahlı Kuvvetleri (TSK) da Haziran 2012'de kendi Siber Güvenlik Merkez Başkanlığı'nı kurmaya karar vermiş ve 2013'te Siber Savunma Komutanlığı'nın kuruluşunu ilan etmiştir. Görevlerini ise TSK'nın kullandığı sistemlerin savunulması, siber olaylara müdahale edilmesi, Ulusal ve NATO tarafından gerçekleştirilen tatbikatlara katılmak, TSK bünyesinde bilinçlendirme çalışmaları yapmak ve düzenli olarak TSK ağlarının güvenlik denetimlerinin yapılması şeklinde tanımlamıştır (Bıçakcıvd, 2015: 18).

3.1.5. TÜBİTAK

Siber Güvenlik Enstitüsü'nün (SGE) faaliyetleri 1997 yılında ulusal siber güvenlik kapasitesinin genişletilmesi amacıyla Bilişim Sistemleri Güvenliği Birimi (BSG) adı ile TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) çatısı altında faaliyetlerine başlamıştır. 2012 yılından bu yana ise TÜBİTAK BİLGEM bünyesinde ayrı bir enstitü olarak çalışmalarına devam etmektedir.

Siber Güvenlik Enstitüsü, gerçekleştirdiği başarılı projeler ile ülkemizde siber güvenlik alanında bilgi birikiminin oluşturulmasın açısından önemli bir katkıda bulunmuştur. SGE bünyesinde Ağ Güvenliği Grubu adı altında yürütülen çalışmalar kapsamında bir test laboratuvarı kurulmuş ve önemli bir bilgi birikimi sağlanmıştır. Bu bilgi birikimi Genelkurmay Başkanlığı'nın da desteğiyle gerçekleştirilen ve 2001

yılında Ortak Kriter Test Merkezi (OKTEM) kurulması ile uluslararası kabul gören standartların gerçekleşmesi için kullanılmıştır. 2005 yılında Devlet Planlama Teşkilatı tarafından başlatılan Bilgi Toplumu Stratejisi projesi bilişim sistemleri alanında önemli bir dönüm noktasıdır. Bu projenin bir ayağını da Bilgi Sistemleri Güvenlik programı oluşturuyordu. TÜBİTAK BİLGEM bünyesinde oluşturulan Bilgisayar Olaylarına Müdahale Ekibi de bu çalışmaların yürütülmesi amacıyla kurulmuştur. Günümüzde de çalışmalarına devam eden SGE, kamu kurumları ve özel sektör kuruluşları ile birlikte yurtiçi ve yurtdışında projeler gerçekleştirmektedir. Siber Güvenlik Enstitüsünün etkinlikleri, İleri Siber Güvenlik Araştırma-Geliştirme Çalışmaları, Siber Güvenlik Stratejisi Belirleme Çalışmaları, Siber Güvenlik Çözüm Projeleri şeklinde üç başlık altında sıralanabilir (Siber Güvenlik Enstitüsü, 2019).

3.1.6. Emniyet Genel Müdürlüğü

İlk bilgisayar Suçları ve Bilgi Güvenliği Kurulu'nu Nisan 1998'de kuran Emniyet Genel Müdürlüğü, bu kurul ile bilişim suçlarının belirlenmesi, gerekli mevzuatın incelenmesi ve EGM'deki birimlerin görevlendirilmesi amacıyla 1999'da kurulan Bilgi Suçları Çalışma Grubu'na öncülük etmiştir. 2011 yılında da Bilişim Suçlarıyla Mücadele Daire Başkanlığı'nı kurmuş ve siber suçlarla mücadele edilmesi için çalışmalar başlatmıştır (Bıçakcıvd, 2015: 19- 20).

3.1.7. Milli İstihbarat Teşkilatı

Türkiye'de ki siber güvenlik tehditlerinin önceden belirlenip bu tehditlere yönelik önlem almak ve istihbarat yoluyla gerekli işlemleri yapmaktan sorumlu kurumlardan biri de Millî İstihbarat Teşkilatı (MİT)'dir. TBMM tarafından 17 Nisan 2014'te yasalaştırılan ve 26 Nisan 2014'te yürürlüğe giren yasa ile MİT'in görev ve yetkileri şu şekilde tanımlanmıştır; "Dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak" (Bıçakcıvd, 2015: 20).

3.2. Türkiye ile NATO İlişkisi

Türkiye'nin NATO ile teması örgütün kuruluş yılına kadar dayanmaktadır. Yapılan politik görüşmeler ve SSCB tehdidine karşı NATO ile işbirliği sürekli olarak yapılmıştır. Türkiye'nin NATO'ya girmesinde pek çok önemli etken ve sebepler vardır. Bu sebeplerden en önemlisi Kore savaşıdır. SSCB ve ABD'nin askeri mücadele sahası olan Kore savaşına Türkiye Cumhuriyeti 25 Temmuz 1950 tarihinde 4500 kişilik tam teçhizatlı bir orduyu görevlendirmiştir. Türkiye'nin bu savaşa katılmaktaki asıl amacı NATO'ya üye olmaktı. Ayrıca Türkiye, Kore'ye ABD'den sonra askeri birlik gönderen ikinci ülke olmuştur. Bu olay Türkiye'ye özellikle Batı Bloğu nazarında büyük bir prestij kazandırmıştır.

Kore savaşı aynı zamanda Türkiye'nin uluslararası alanda büyük bir yankı uyandırmasını sağlamıştır (Kibaroğlu, 2017: 10). Kore Savaşı neticesinde, Türk devletinin gösterdiği üstün çabalar ve ABD'nin de desteği ile 18 Şubat 1952 tarihinde Türkiye Cumhuriyeti NATO'ya resmi olarak üyelik statüsü kazanmıştır.

Türkiye'nin NATO'ya girmesiyle birlikte üye ülkeler içinde farklı sesler çıkmaya başladı. İngiltere ve Fransa'nın başını çektiği birçok ülke Türkiye'nin NATO'ya üyeliğinin örgüte zarar vereceği görüşünü savunuyorlardı. Bu görüşlerindeki temel fikir tam üye olan bir Türkiye ile NATO'nun sınırının Ortadoğu ve SSCB'ye dayanmasıydı. Zaman içinde SSCB ve Türkiye'nin diğer komşuları ile yaşayacağı bir problemin ya da çatışmanın NATO'yu da içine çekme ihtimalinin bulunduğunu düşünüyorlardı. Hatta muhalifler bu sorunların giderek artacağı ve NATO ile Varşova Paktı'nın karşı karşıya geleceğini belirttiler. Bu yıllarda Türkiye'nin NATO üyesi ülkeler içinde ABD dışında iyi ilişki kurabildiği ülke neredeyse yoktu. Türk dış politikası genellikle ABD ve NATO ekseni etrafında yürütülmekteydi.

Durum NATO açısından ise o yıllarda Türkiye'nin düşündüğü şekilde değildi. NATO'nun ana düşüncesi her zamanki gibi SSCB'yi çepeçevre kuşatmak ve Varşova Paktı'nı etkisiz hale getirmeye çalışmaktı. NATO bu konularla alakalı Türkiye'ye bir bildirimde de bulundu bu bildirim anlaşmanın 5. ve 6. Maddesinin hatırlatılmasıyla ilgiliydi.

NATO'nun en büyük amacı olan ortak savuma planına göre, müttefik bir ülkenin tehdit edilmesi ya da aktif bir saldırıya uğraması halinde bu saldırı NATO'ya karşı yapılmış gibi algılanarak topyekûn reaksiyon gösterileceği garanti altına alınmıştır. Bu nokta da maalesef NATO ülkeleri Türkiye konusunda ikili davranmışlardır. NATO her türlü tehdit algısı altında savunma yapacak olmasına rağmen, Türkiye'nin sadece SSCB ve WP üyesi Bulgaristan devleti tarafından gelecek bir tehdit karşısında ortak savunma konusunda destek göreceğini resmi olmasa da diplomatlar seviyesinde belirtmiştir. Bu ayrımcılık Türkiye'nin NATO konusundaki tereddütlerinin artmasına sebep olmuştur (Kibaroğlu, 2012: 55-72).

NATO tarafında yapılan bu bildirimin Türk devletine verdiği mesaj; SSCB ve Varşova Paktı dâhilinde olan tüm anlaşmazlık ve çatışmalar için nükleer caydırıcılık imkânı sunulacağı fakat SSCB dâhil bireysel meselelerde ve özelikle Ortadoğu coğrafyasındaki diğer komşu devletler (Irak, İran, Suriye, İsrail vb.) ile yaşanacak çatışmalar-da NATO'nun taraf olmayacağı şeklindeydi. Bu bildirim Türk devleti ve dış politikası nazarında NATO'nun gerekliliğini tartışmaya açmıştır. Bu tarihe kadar ABD ve NATO ekseninde sevk edilen Türk dış politikasında bir değişim yaşanmıştır. Türkiye Cumhuriyeti iç ve dış meselelerinde ve komşularıyla olan ilişkilerinde kendi göbek bağını kendi-sinin kesmek zorunda olduğunu (self help, kendine yardım) net bir şekilde anlamıştır. Türkiye fazla bir zaman geçmeden benzer bir senaryoyla karşılaşmıştır.

1964 yılının haziran ayında gerçekleşen ABD Başkanı Johnson'ın kaleme aldığı metinde görülmüştür. Bir sene önce Kıbrıs adasında Türk kökenli yerleşim yerlerinde yapılan katliamların ardından Türk Hava Kuvvetleri'nin Kıbrıs'a görevlendirilmesi sonucunda yaşanan bir krizdir. Bu krizde ABD, Türk devletine NATO bünyesinde kullanılmak üzere verilen silah sistemlerinin bu görevler kapsamında kullanılması gerektiği, başka alanda ve maksatta kullanılamayacağını hatta bu şekilde kullanılmaya devam edilmesi halinde SSCB karşısında yaşanabilecek bir tehditte ortak savunma ilkesinin işletilmeyebileceğini söylemiştir. Müttefiklik doğasına aykırı olan bu tutum neticesinde Türkiye'nin NATO'ya kaşı güveni ciddi yara almıştır. NATO'nun Türkiye için gerekli olup olmadığı sorgulanmış ve ilerleyen yıllarda başka krizlerin de yaşanabileceği kamuoyu nezdinde gündeme gelmiştir. Nitekim tam da Türkiye'nin düşündüğü gibi olmuş,

Yunanistan'ın ve Kıbrıs'taki Rumların ortak olarak yaptıkları katliamlar neticesinde Türkiye Cumhuriyeti adaya askeri müdahalede bulunmak zorunda kalmış ve bu müdahalenin gerçekleştirilmesinin bir sonucu olarak da NATO'daki dostu ABD'nin silah sistemleri konusundaki satış ambargosunu yaşamıştır (Kibaroğlu, 2017: 10).

Soğuk Savaşın sona ermesi ve Varşova Paktı'nın çökmesiyle birlikte Türkiye ve NATO'nun tehdit değerlendirmesi ve stratejisi de değişti. NATO'nun karşısında denk olan bir yapılanma kalmadığı için düşman değerlendirmesi yeniden yapıldı. Balkanlar'da artan milliyetçilik, Kafkasya bölgesindeki belirsizlik, Ortadoğu bölgesinde yaşanan gelişmeler ve özellikle ABD'nin tek başına süper güç olma hedefi NATO'ya yeni stratejiler konusunda yön verdi.

NATO'nun ilan ettiği yeni stratejik konsepti ışığında icra ettiği ve Türkiye'nin de dâhil olduğu ilk askeri müdahale Bosna-Hersek'te oldu. Yugoslavya'nın parçalanma süreci içerisinde Bosna-Hersek'in bağımsızlığını ilan etmesi ile birlikte Sırpların askeri müdahalesi ve yaptıkları katliamlar neticesinde NATO müdahale etmek durumunda kalmıştır. NATO bünyesinde oluşturulan SFOR'un Bosna-Hersek'e müdahalesi kısmen de olsa barışı sağlamıştır. Müdahalenin zamanı, taraflara karşı kullanılan güç günümüz-de dahi hala tartışılmaktadır.

NATO'nun başarılı olarak kabul ettiği bu harekâtta birtakım uyuşmazlıklar da yaşanmıştır. Özellikle Türk devleti ve NATO üyelerinin aralarında çelişkiler gözlenmektedir. Bosna sorununda yaşanan bu çelişkiler, yapılan karşılıklı görüşmeler ile çözülse de sorun içten içe devam etmiştir. Örneğin, Türk devletinin Sırplar tarafından yapılan taarruzların başlamasının ardından bu tehdidin ortadan kaldırılması için savaş uçaklarının icra edilecek askeri harekâta dâhil edilmesi ve Bosna'nın kendisini savunabilmesi için uygulanan askeri ambargo durumunun iptal edilmesi fikri uygun bulunmamıştır. Hepsinden mühim olan, NATO'nun stratejisinin temelini oluşturan üyelerin mutlak koruması kuralının (NATO'nun 5. Maddesi) SSCB'nin dağılmasının ardından nerede, ne şekilde ve hangi koşullarda kullanılacağı durumu Türkiye ile NATO ilişkilerinin en kırılgan noktası olmuştur (Karaosmanoglu, 2001: 68).

Bosna-Hersek olayından sonra yaşanan Kosova krizinde de Türkiye NATO ile birlikte görev yapmıştır. Kosova krizini çözmek maksadıyla yaptığı askeri birlik operasyonları ile müdahaleyi meşrulaştıran NATO, kuruluşundan bu zamana kadar ilk kez BM'den bağımsız olarak güvenliğini tesis etmek için müşterek bir operasyon icra etmiştir.

Yıllar içerisinde Türkiye ile NATO arasındaki ilişki artarak devam etmiştir. Türkiye, NATO içerisinde ABD'nin ardından güçlü bir orduya sahip ve stratejik değeri yüksek bir ülke konumundadır. Bu da dolaylı olarak Türk devletini NATO açısından kuvvetli bir müttefik ve askerî açıdan boşluğunun doldurulması zor bir ülke yapmıştır. Bosna-Hersek ve Kosova müdahalelerinden sonra Türkiye NATO ile birlikte Afganistan operasyonunda da yer almıştır.

NATO, BM'nin görevlendirmesi üzerine, 11 Ağustos 2003'te Afganistan'daki müşterek birliklerin (ISAF) komutasını devralmış, taktik seviyedeki operasyonlara karar verecek bir konuma ulaşmıştır. Bunun sonucunda ISAF, NATO'nun kontrol ettiği bir harekât şeklini almış ve NATO birlikleri daha önce görülmemiş şekilde alan dışı bir faaliyette görev almışlardır. Bu faaliyet, jeostratejik konumunun yanı sıra, zamanın koşulları, ekonomik koşullar ve bölgeye demokrasinin kazandırılması açısından zorlu bir sınav olmuştur. Ayrıca söz konusu operasyon uluslararası sistemin güvenliği bakımın-dan NATO gibi bir unsurun gerekliliğini ve güvenirliğini ispat etmesi açısından son derece önemli bir faaliyet olarak görülmüştür. Afganistan'ın bu aşamadan sonra yaptığı olumlu açıklamalar da bu düşüncenin doğruluğu perçinlenmiştir (Peksarı, 2007: 179-180).

ISAF görevi Türkiye'nin NATO içerisindeki önemini ve değerini bir kez daha göstermiştir. Çünkü Türkiye'nin jeopolitik konumu, bölge halkı ve Afganistan devleti ile çok eski zamanlara dayanan köklü ilişkileri ve Afgan halkının Türk askerine karşı duyduğu sempati ve sevgi harekâtın icrasında fayda sağlamıştır. Türkiye ISAF komutasını dönemler halinde üç kez devralmıştır.

Afganistan operasyonu neticesinde NATO, Türkiye'nin potansiyelini, jeopolitik konumunu ve askeri kabiliyetini daha iyi anlama ve değerlendirme fırsatı buldu. Orta-doğu bölgesi için Türkiye NATO açısından vazgeçilemez bir müttefiktir.

Ortadoğu'daki tüm bölgelere konum olarak yakın olan Türkiye adeta ileri bir üs bölgesi niteliğindedir. Sahip olduğu imkânlar, ordu, lojistik destek faaliyetleri ile her türlü operasyonun üste-sinden tek başına bile rahatlıkla gelebilecek kabiliyettedir. Bu tarihten sonra Türkiye NATO ile birlikte Somali ve Libya operasyonlarına da katılmış ve harekât boyunca destek vermiştir.

Jeostratejik açıdan Türkiye Cumhuriyeti bölgede çok önemli bir yere sahiptir. Bu konumun avantajları ve dezavantajları mevcuttur. Avantajlarına bakıldığında, enerji kaynaklarına yakın olması, ulaşım güzergâhlarını kontrol edebilen bir yere sahip olması, ticaret yollarının çoğunun bu coğrafyadan geçmesi olarak saymak mümkündür. Dezavantajlarına bakıldığında ise, çatışmaların ve kaos ortamının sürdüğü Ortadoğu'ya yakın olması, etnik krizlerin devam ettiği Balkanlar'ın yanı başında bulunması, tarihsel süreç-te çoğunlukla belirsizliklerin hâkim olduğu Kafkaslara komşuluğu, enerji kaynakları ile dolu olan bölgenin içinde çıkabilecek güvenlik sorunlarının kendisine yansıyabilme ihtimalini belirtmek doğru olacaktır. Buradan yola çıkarak Türkiye'nin bölge güvenliği için ne kadar önemli bir aktör olduğu görülmektedir. Bu jeostratejik konumunun bir gereği olarak Türkiye, NATO içinde Kara Kuvvetleri mevcudu bakımından ABD'nin ardından ikinci sırada yer almakta (%17,5), orta boy muharip deniz unsurları katkısı bakımından ise NATO içinde beşinci konumda bulunmaktadır. Diğer yandan Türkiye NATO envanterindeki savaş uçaklarının %10,5'ine, keşif unsurlarının %22,5'ine, kargo uçaklarının %20'sine sahiptir. Türkiye bu kapasitesi ile NATO ve BM'nin gerçekleştirdiği her türlü operasyonel faaliyetlerde rahatlıkla yer alabilmekte ve bundan sonra da verilecek tüm görevleri gerçekleştirme kapasitesinin olduğunu göstermektedir (http-7, Rustamov, E.T: 01.02.2021).

Türkiye, 1952 yılında NATO'ya üye olmuştur. Üye olduğu tarihten itibaren NA-TO bünyesinde çeşitli operasyonlara katılmıştır. Katıldığı bu operasyonların sonucunda gerek NATO gerekse bölgedeki diğer ülkelerin (özellikle Avrupa ve Ortadoğu coğrafyası) güvenliğine büyük katkıda bulunmuştur. Son dönemde Türkiye'yi ve diğer devletleri yakından ilgilendiren pek çok terör örgütü ortaya çıkmıştır. Türk devletinin 30 yıldır mücadele ettiği PKK, Afganistan'da ISAF koordinesinde mücadele edilen El-Kaide ve Taliban, son yılların en büyük terör örgütü olan IŞİD (DEAŞ) bunların sadece başlıca olanlarıdır. Ülkelerin ve

NATO'nun değişen güvenlik konseptleri bu terör örgütlerini ana tehdit olarak değerlendirmektedir. Coğrafyamıza çok yakın ve iç içe faaliyet gösteren terör örgütleri, Türkiye'nin terörle mücadele kapsamında katma değeri yüksek bir NATO üyesi olacağını kanıtlamaktadır. 2000'li yılların yeni güvenlik konseptin de ve şartlarında NATO nazarında Türkiye'nin önemi azalmanın aksine artarak devam edecektir. Çünkü Türkiye'nin içinde bulunduğu coğrafya dini, etnik, ayrımcılıkların çoğunlukla yaşandığı Balkanlar, Ortadoğu, Kafkasya bölgelerinin merkezindedir. Bu bölgeler her türlü çatışmanın belirsizliğin ve kaosun her zaman hâkim olabileceği yerlerdir. Bu terör ve güvenlik tehditlerinin yanı sıra bahse konu bölgeler stratejik öneme sahip birçok yeraltı ve yerüstü ham madde kaynaklarına da sahiptir.

Sonuç olarak incelendiğinde Türkiye NATO açısından bölge güvenliğinin sağlanması, barışı destekleme operasyonlarının sürdürülmesi, terörizmle mücadele harekâtlarının devam ettirilmesi ve enerji sahalarının güvenliğinin temin edilmesi kapsamında vazgeçilemez bir konum ve yapıya sahiptir. Geçmişte olduğu gibi gelecekte de Türkiye NATO için önemli bir müttefik ve kilit bir ülke olan konumunu arttırarak devam ettirecektir.

3.3. Siber Güvenlikte NATO – Türkiye İlişkisi

NATO'nun üye ülkelere sağladığı en büyük güvence, ulusal tehdit oluşturan bir unsurun ortak bir tehdit olarak algılanıyor oluşudur. Bir ülkeye yapılan siber saldırı, NATO'ya üye ülkelerin her birine yapılma riskini barındırdığı gibi anlayış olarak da her bir ülkeye yapılmış gibi değerlendirilmektedir. Bu sayede de sorunlar ortak görüldüğü gibi çözümler de ortak bir payda da sağlanmaya çalışılmaktadır. Yine siber güvenlik özelinde bu ilişkiye bakıldığında Türkiye'de 7 Nisan 2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu dikkat çekmektedir. NATO'ya üye her ülke siber güvenlik çalışmalarında kendi çalışmalarını yürütmüş ve yürürlüğe koymuştur.

Bu yaklaşımda şüphesiz toplumsal ihtiyaçların farklılığı gözetilmiştir. Bununla birlikte geliştirilen bu çalışmalarda ortak bir altyapı oluşturulmuş ve ilerleyen bölümde özelleştirilerek uygulamaya konulmuştur. Bu sebepledir ki Türkiye'de yürürlüğe giren kanun da NATO'ya üye ülkelerin yapmış olduğu

çalışmalardan faydalanılarak, geliştirilen altyapının üzerine inşa edilerek uygulamaya konulmuştur.

3.4. Siber Saldırıların Etkileri

Siber saldırılar, bir ulusun güvenliğine doğrudan etki etmekte olup var olan güven ortamının sarsılmasına ve sükûnetin korunamamasına neden olmaktadır. Bununla birlikte söz konusu etkilerini farklı açılardan değerlendirerek üç alt başlıkta ele almak mümkündür. Bu başlıklar;

1. Bireysel etkiler
2. Kurumsal etkiler
3. Küresel etkiler

Ölçekleri farklı olan bu etkilerin kapsamını incelemek hem etkiler arasındaki farkları ortaya koymak hem de sorunu çok daha iyi anlayabilmek adına önemlidir. Bu amaçla da alt başlıklar halinde incelemekte fayda vardır.

3.4.1. Bireysel Etkiler

Her geçen gün internet ve sanal işlemlere bağımlı hale gelen bir siber dünyada yaşamaktayız. Birey için; iletişim ve haberleşme, internet üzerinde reklam, alışveriş, araştırma, rezervasyon, bankacılık, kamu hizmetlerinden yararlanma, hukuk, sağlık güvenlik işlemleri ve bunların takibi temel birey ihtiyaç ve beklentisi haline gelmiştir. Nisan 2016 Türkiye İstatistik Kurumu araştırma verilerine göre hanelerin %76,3'ü internete erişim imkânına sahiptir. Finansal yatırımlar, başvuru ve üyelik formları, bankacılık işlemleri yaparken bir takım kişisel bilgiler karşı tarafa verilmek durumunda kalınmaktadır (TİK, 2016). Vatandaş kimlik numarası, doğum tarihi, nüfus cüzdan fotokopisi, kredi kartı bilgileri, iş ve aile bilgileri gibi bireye ait olan ve korunması gereken bilgiler çoğu zaman bilinçsizce bilinçsiz bir şekilde karşı tarafa verilebilmektedir. Bu durum tehditlere açık zafiyetin doğramasına da sebep vermektedir. Bu bilgilerin istenmeyen kişilerin eline geçmesi durumunda, birey siber saldırıların hedefi haline gelebilmektedir. Birey, bu saldırılar sonucunda gizlilik ihlali (mahremiyet) ve yasal bakımdan birtakım mağduriyetlere maruz kalmakta, maddi ve yaşamsal olarak yıpranmaktadır. Veri depolama ortamlarında tutulan bireye ait her türlü sır nitelikteki mahrem verilerin gizlilik, bütünlük ve erişilebilirlik niteliklerinin korunması gerekmektedir

3.4.2 Kurumsal Etkiler

Kurumsal yapılarda internet iş hayatının ayrılmaz bir parçasıdır. Ticari rekabet, hizmet sektöründeki çeşitlilik, müşteri memnuniyeti, alternatif on-line kanallar kurumsal yaşamla bütünleşik hale gelmiştir. Bu alandaki çatışmaların, rekabetin veya kasıtlı faaliyetlerin sonucu olarak siber saldırılara maruz kalınmaktadır. Tutulan müşteri, çalışan veya kurum verileri her geçen gün daha da kıymetli hale gelmekte, bunlar üzerinde siber suçların işlenme oranını da artırmaktadır. İş Sürekliliği Enstitüsü (BCI) tarafından 2013'de 62 ülkeden 730 kuruluş ile gerçekleştirilen geniş çaptaki bir araştırmaya göre kuruluşların %65'inin siber saldırı tehlikesi ile karşı karşıya kalma riski taşıdığı belirtilmektedir. Ülkemizden katılan 250 kurum üzerinden yapılan benzer araştırma sonucuna göre ticari kuruluşların %47'si, 2011 yılı itibarıyla maruz kalınanı siber saldırı sayısında artış olduğu görüşünde birleşmektedir.

Siber güvenlik sorunları kurumlar bazında ele alındığında tehditlerin daha karmaşık ve otomatik hale getirilmiş saldırı senaryolarıyla güvenliği atlatmada daha akıllı hale gelmektedir. DDOS saldırıları, bulut kaynaklarına yapılan saldırılar, kurum içi bilgilere yetkisiz erişim, zararlı yazılımlar kurumları tehdit eder öncelikli unsurlar olarak karşımıza çıkmaktadır. Kurumlar bu zorlu koşullarda iş ilişkisinde bulunduğu müşteri veya paydaşları nezdinde bir takım siber güvenlik ihlalleri sonucunda maddi, itibar, imaj, güven kayıtları, iş hukukunda birtakım zorluklar veya yasal yaptırımlarla karşı karşıya kalabilirler.

3.4.3. Küresel Etkiler

Toplumsal düzenin ve haberleşme, enerji, su, sağlık, güvenlik gibi kamu hizmetlerinin devamını sağlamada etkili olan kritik altyapılar ile bu altyapıları kullanan bilgi sistemlerinin korunması bir ülkenin ulusal güvenliğin sağlanması için önceliklidir. Avustralya kritik altyapı koruma stratejisinde uzun dönemde ulusun sosyal ve ekonomik sağlığı üzerinde olumsuz etki bırakabilecek, ulusal güvenliği sağlamada etkilenebilecek fiziksel tesisler, tedarik zincirleri, bilgi ve iletişim teknolojileri korunması gereken kritik varlıklar olarak ele alınır.

Uluslararası düzeyde devletler ekonomik gücü oranında askeri savunma kalkanı oluşturarak dış tehdit ve tehlikelere karşı ülke bütünlüğünü korumaktadır. Her devlet kendi ülke güvenlik ve menfaatleri doğrultusunda hareket etmekte ona göre güvenlik politikalarını oluşturmaktadır. İç ve dış siyasi, ekonomik ve sosyokültürel alanlarda güvenliğin sağlanması önemlidir. Ülke güvenliği birey, aile, toplum güvenliğinin üst şemsiyesini oluşturur. Fiziksel olmayan güvenlik kategorisine dâhil olan siber alan, küresel sonuçları bakımından 21. yüzyılın önemli güvenlik tehditlerindendir (Önen ve Kurnaz, 2017: 747).

Ülkemizde ise en son Ulaştırma ve Haberleşme Bakanlığının 2016-2019 Ulusal Siber Güvenlik Strateji Dokumanı yayımlanmıştır. 2007 yılında Estonya'ya yapılan siber saldırı ülkelerin siber saldırılara karşı bakış açısını değiştirmiştir. 2010 yılında İran'a karşı gerçekleştirilen Stuxnet saldırısıyla birlikte siber güvenliğin sağlanmasının devletler, toplumlar için ne kadar önemli olduğu bir kez daha görülmüş, toplumları kaygılandırmıştır. Bunun sonucu olarak ülkeler bir yandan siber güvenlik politikalarının oluşturmaya ya da revize etmeye öncelik verirken diğer taraftan siber saldırılara karşı siber ordular oluşturmaya bu tür sorunlarla başa çıkabilmenin yollarını aramaya ağırlık vermeye başlamıştır.

SONUÇ

Ülkeler arası rekabet tarih boyunca süre gelmiştir. Bu rekabetler geçmiş dönemlerde kara savaşları ile yaşanmış ve 20. Yüzyıla kadar dünya üzerinde sayısız savaş gerçekleşmiştir. 20. Yüzyılın başlarında önce Birinci Dünya Savaşı, ortalarında ise İkinci Dünya Savaşı yaşanmış ve dünya ağır bir yara almıştır. 20. Yüzyılın ikinci yarısından itibaren ise kara savaşları azalmış ve masa başı savaşları yoğunluk kazanmıştır. Nitekim Soğuk Savaş olarak adlandırılan süreç de masa başı savaşların temelini oluşturmuştur. Yaklaşık olarak yarım asır süren bu süreç nihayetinde savaşın taraflarından biri olan Sovyet Sosyalist Cumhuriyetler Birliği'nin dağılması ile son bulmuştur. 1990'lı yıllardan itibaren ise masa başı savaşları çok daha yoğun bir hal almış ve ekonomik yaptırımlar üzerinden bu savaşlar şekillendirilmeye başlanmıştır.

Aynı sürece bakıldığında teknolojik gelişmelerin de önü alınamaz bir hızla sürdüğü gözlemlenmektedir. Hayatın hemen her alanına dahil olan teknolojik gelişmeler, bugün gelinen noktada gündelik hayatın olmazsa olmazı haline gelmiş durumdadır. Bu durum şüphesiz büyük kazanımlar sağladığı gibi büyük riskleri de beraberinde getirmektedir. Siber güvenlik olgusu da bu risklerin bir uzantısı olarak karşımıza çıkmaktadır.

Hayatın her anında teknolojik aletleri kullanıyor oluşumuz bireylerin ardında siber iz bırakmasına yol açmaktadır. Her uygulamada, her işlemde bir iz bırakılıyor oluşu da bu bilgilerin geniş kitlelere ulaşmasını kolaylaştırmaktadır. Siber güvenlik, her ne kadar bireysel bir konuymuş gibi görünse de esasından ulusları yakından ilgilendiren temel bir sorun konumundadır. Bahsedildiği üzere ülkeler arası savaşlar artık masa başında yürütülmekte olup siber saldırılar da bu masa başı mücadelelerin bir parçası haline gelmiş durumdadır. Bu sebepledir ki siber güvenlik olgusunu yalnızca bireysel olarak ele almak doğru olmadığı gibi mümkün de değildir.

Dünyanın ekonomik ve gelişmişlik olarak önde gelen ülkeleri, siber güvenlik konusunda da ileri düzeyde ülkeler arasında yer almaktadır. Siber güvenlik olgusunun bireysel ya da toplumsal bir sorundan ziyade küresel bir sorun haline gelmiş olması Amerika Birleşik Devletleri başta olmak üzere NATO'ya bağlı ülkeler

bu sorunu ortak bir çaba ile ele almakla birlikte şüphesiz her ülke kendi tedbirlerini de geliştirmektedir. Ortak geliştirilen altyapıların yanında ülkeler ayrışarak toplumsal koşullara ve risklere bağlı olarak tedbirlerini geliştirmektedir. Bununla birlikte bahsi geçtiği zere siber güvenlik olgusu ortak bir paydada ele alınmakta ve NATO'ya bağlı ülkeler arasında ortak çalışmalar geliştirilmekte, geliştirilmiş olan fikirler karşılıklı paylaşılmaktadır. Türkiye de siber güvenlik tedbirlerini sürekli olarak arttıran ve bu konuda gelişim gösteren bir ülke konumundadır. Bugün gelinen noktada şüphesiz ekonomik ve gelişmişlik olarak belirli bir düzeye ulaşabilmiş olan Türkiye, siber güvenlik konusunda da belirli bir aşama kaydetmiş durumdadır ancak dünyanın bu alanda en iyi üç beş ülkesinden biri olduğunu iddia etmek de mümkün değildir. Türkiye zaman içerisinde siber uzaydaki mevcudiyetini ve kabiliyetlerini geliştirmiş olsa da, bu bütün alanlarda aynı seviyede olmamıştır; bunun neticesinde bazı alanlarda büyük aşamalar kaydedilse de diğer alanlarda beklenen ilerleme göstermemiştir. Yine de, son birkaç senede siber güvenlik ile ilgilenen devlet kurumlarının sayısı artmıştır ve Türk güvenlik güçleri siber tehditlerle mücadeleye önemli vurgu yapmışlardır. Tıpkı ekonomik ve gelişmişlik düzeylerinde olduğu gibi bu alanda da gelişmekte olan bir ülke olarak Türkiye'nin aşama kaydetmesi gerektiği tespitinde bulunmak mümkün olduğu gibi pozitif yönlü bir ilerleyişin varlığından söz etmek de mümkündür.

Siber güvenlik tedbirlerinin geliştirilmesi adına getirilebilecek başlıca öneriler de şunlardır:

- Öncelikli olarak bu alanda bireysel bir bilinçlenme ve çaba gerekmektedir. Elbette ülke yöneticilerinin bu alanda alması gereken tedbirler bulunmaktadır ancak bireysel olarak da bu konuda bilinçli olunması ve koruyucu önlemler alınması önemlidir.
- Bireysel çabanın yanı sıra kurumsal çaba da gösterilmeli ve kurumsal olarak da tedbirler alınmalıdır.
- Ulusal düzey ise bu alanda en çok sorumluluğun yüklendiği kesim olup, ulusal siber güvenlik tedbirlerinin alınması, bireysel ve toplumsal bilincin arttırılması, altyapı çalışmalarının tamamlanması gerekmektedir. Getirilebilecek öneriler de tarafların bu sorumluluklarının bilincinde olarak çabalarını arttırmaları yönündedir.

Sonuç olarak Siber güvenlik olgusu günümüzde bireyden çok uluslu şirketlere, çok uluslu şirketlerden uluslararası örgütlere ve devletlere varıncaya değin ve büyük bir yelpazede ve her uluslararası aktörü etkileyecek düzeyde ele alınması gereken bir hususdur. Siber güvenlik olgusu Her aktörü etkileyecek bir yapıya dolayısıyla mikrodan makro ölçeğe, bireyden uluslararası boyuta küresel boyuta varan düzeyde ekonomik, sosyal, siyasal, güvenlik ve benzeri boyutları ve sonuçları vardır. Günümüzde devletler düzeyinde düşünüldüğünde güçlü olmanın yolu ve rolü ancak ve ancak siber güvenlik tedbirlerinin iyi alınmasında, güçlü siber güvenlik sistemlerine sahip olunmasında ve siber alanda rakiplere karşılaştırmalı üstünlük sağlanmasında yatmaktadır. Bunu başaramayan ülkelerin kendi güvenliğini tam olarak sağlamaları mümkün olmadığı gibi güvenli bir geleceği inşa etmeleri mümkün değildir. Çalışmada elde edilen en temel sonuçlardan birinin siber güvenliğin tarihte hiç olmadığı kadar önemli olduğu ve öneminin giderek artan bir olgu olduğunu ortaya koymaktayız. Dijital dünyanın zorunlu hale getirdiği siber güvenlik artık geri dönülmez kaçınılmaz ve devletlerin içinde olduğu bir olgudur bu yüzden devletleri siber güvenlik anlamında tedbirler ve girişimler de bulunmayı zorunlu hale getirmiştir.

KAYNAKÇA

Abdul-Mumin S. (2011). *Detectıon of Man InTheMiddle Attack InIeee 802.11 Networks.* KwameNkrumahUniversity Of ScienceAndTechnology: 38.

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

Ateş, H. (2016). *İstihbarat Konferansları: Türk İstihbaratında Eğitim Süreci,* Detay Yayıncılık, Ankara.

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

Bağbaşlıoğlu, A, (2016).*Güncelliğini Yitirmeyen Bir Sorun Olan Yük Paylaşımına Yeni Bir Çözüm Arayışı: Akıllı Savunma ve NATO (A New Solution Seekingfor a TimelessIssueBurdenSharing: Smart Defenseand NATO),* Akademik Bakış Dergisi, s. 3-8.

Bal, M. A. (2003). *Modern DevletveGüvenlik,*IQSanatYayınları, İstanbul.

Bayraktar, G. (2015). *SiberSavaşveUlusalSiberGüvenlikStratejisi*,YeniyüzyılYayınevi.

BBC Türkçe (2007). Estonya'ya Siber Saldırı. Erişim Adresi: http://www.bbc.co.uk/turkish/news/story/2007/05/070517_estonia_cyber.shtml (Erişim Tarihi: 03.04.2021)

Bıçakçı, S. (2012). *YeniSavaşveSiberGüvenlikArasındaNATO'nunYenidenDoğuşu*. UluslararasıİlişkilerDergisi, 9 (34), 204-226.

Bıçakcı, S. Çelikpala, M. ve Ergun, D.(2015). *Türkiye'de Siber Güvenlik,* EDAM Siber Güvenlik Kağıtları Serisi. Sayı.1, ss.1-35.

Bilgi Güvenliği Derneği.(2012).Ulusal Siber Güvenlik Stratejisi. https://www.bilgiguvenligi.org.tr/wpcontent/uploads/2016/03/Ulusal_Siber_Guvenlik_Stratejisi.pdf (Erişim Tarihi: 21.02.2021)

Bozgeyik A. (2018). *Gaziantep'te Faaliyet Gösteren Orta Ve Büyük Ölçekli İşletmelerin Siber Güvenlik Yönetim Yaklaşımlarının Analizi*. Hasan Kalyoncu Üniversitesi Sosyal Bilimler Enstitüsü Doktora Tezi.

BTK.(2017).Siber Güvenlik Tatbikatları. https://www.btk.gov.tr/siber-guvenlik-tatbikatlari (Erişim Tarihi: 22.02.2021)

Can, M. (2014). *Stuxnet Ve Uluslararası Hukuk: Bir Siber Saldırının Anatomisi*. Bilim Ve Gelecek, Sayı 125.

Choucri, N. (2012). *Cyberpolitics in International Relations.*England: The MIT Press Cambridge, Massachusetts.

Clarke, R. A. andKanke, R. K. (2011). *Siber Savaş.* (Çeviren: Murat Erduran), İstanbul Kültür Üniversitesi.

Collins, S. andMcCombie, S. (2012). *Stuxnet: TheEmergence Of A New CyberWeaponAndİtsİmplications.*Journal of Policing, Intelligenceand Counter Terrorism, Vol 7, No 1, pp. 80-91.

Conteh N. ve Schmick P. (2016). *Cybersecurity: risks, vulnerabilitiesandcountermeasurestopreventsocialengineeringattacks*: 31.

Çelik, Ş. (2014). *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.

Çeliktaş, B. (2016). *SiberGüvenlikKavramınınGelişimiveTürkiyeÖzelindeBirDeğerlendirme.*Karadeniz TeknikÜniversitesi, SosyalBilimlerEnstitüsüUluslararasıİlişkilerAnabilim Dalı YüksekLisansTezi.

Darıcılı, A.B.(2018). *Askerileştirilen ve Siahlandırılan Siber Uzay*, Ali Acaravcı(ed.), Sosyal ve Beşeri Bilimlere Dair Örnekler, Nobel Yayıncılık, Ankara.

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

Dergipark. (2019). http://dergipark.gov.tr/download/article-file/465726(Erişim Tarihi: 21.02.2021).

DeutscheWelle (2008). Rusya, Gürcistan'ı Sanal Âlemde De Vurdu. Erişim Adresi: https://www.dw.com/tr/rusya-g%C3%BCrcistan%C4%B1-sanalalemde-de-vurdu/a-3575502 (Erişim Tarihi: 05.04.2021)

Farwell, J. P. andRohozinski, R. (2011). *StuxnetandtheFuture of CyberWar.*Survival, Vol 53, No 1 pp. 23-40.

Goodman, W. (2010). *CyberDeterrence: Tougher in Theorythan in Practice?,* Strategic StudiesQuarterly, Vol 4, No 3.

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

Gürsoy E. (2015). *Bilişim Yoluyla Dolandırıcılık Ve Korunma Yöntemleri*. Afyon Kocatepe Üniversitesi Yüksek Lisans Tezi.

Hekim, Y. D. ve Başıbüyük, D. D. (2014). *Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları- CyberCrimesandTurkey'sCyber Security Policies*, Uluslararası Güvenlik ve Terörizm Dergisi, 4(3), 143.

Karaosmanoglu, A, (2001). *Türkiye Açısından Avrupa Güvenlik Kimliği: Jeopolitik ve Demokratik Ufuk, Türkiye'nin Dış Politika Gündemi,* (Editörler: Saban H. Ç. - Dagı H. D.- Gözen R), Ankara: Liberte Yayınları.

Keleştemur, S. (2018). Siber İstihbaratın Kamu Güvenliği İçin Rolü ve Önemi. Gedik Üniversitesi Yüksek Lisans Tezi. İstanbul.

Kibaroğlu, M, (2012).*NATO'nun Nükleer Stratejisi ve Türkiye'deki Amerikan Nükleer Silahları,* Derleyen Seyfi Taşhan, Türkiye'nin NATO'da 60 Yılı: Güven Veren Bir Ortaklık, Dış Politika Enstitüsü, Ankara.

Kibaroğlu, M, (2017).*Türkiye-NATO İlişkileri,* ANALİZ Seta Siyaset, Ekonomi Ve Toplum Araştırmaları Vakfı, İstanbul, Mart 2017 Sayı: 191.

Korhan, S. (2016). *Uluslararası İlişkilerde Siber Caydırıcılık*, CyberpolitikJournal, Vol 1, No 1-2, pp:147-162.

Maan P. andSharma M. (2012). *SocialEngineering: A Partial Technical Attack*: 557.

Mavzer, Ş. (2014). *Siber Suçlarla Mücadelede Uluslararası İşbirliği.*

Mirzaoğlu, A. G., Ünver, M ve Canbay, C. (2009). *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler,* Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı.

Newsweek (2008). How Russia May HaveAttackedGeorgia's Internet. https://www.newsweek.com/how-russia-may-haveattacked-georgias-internet-88111 (Erişim Tarihi: 06.03.2021)

Nye, J. S. (2011). *NuclearLessonsforCyberSecurity?*.StrategicStudiesQuarterly, pp. 18-38.

Önen, M. ve Kurnaz, S.(2017). *Siber Güvenlik Politikalarının Kamu Yönetimine Yansıması,* Turgut Özal Uluslararası Ekonomi ve Siyaset Kongresi IV.

Özçoban, C. (2014). *21. Yüzyılda Ulusal Güvenliğin Sağlanmasında Siber İstihbaratın Rolü,* Harp Akademileri Stratejik Araştırma EnstitüsüYüksek Lisans Tezi, İstanbul.

Pajunen N. (2017). *Overview Of MaritimeCybersecurity*. South EasternFinlandUniversity: 21.

Peksarı, D. G, (2007). *NATO'nun Değişen Konsepti,*Asil Yayınları, Ankara.

Sander, O. (2005). *Siyasi Tarih (1918-1994),* İmge Kitabevi, Ankara.

Sanger, D. E. (2012). *Obama OrderSpedUpWave of CyberattacksAgainstIran.*The New York Times, Erişim Tarihi: 04.04.2021

Seçkin, O. (2010). *Devlet Güvenliği Kapsamında İstihbarat Alanında Karşılaşılan Sorunlar,* Beykent Üniversitesi Yüksek Lisans Tezi, İstanbul.

Seren, M. (2016). *Siber Tehditlerle Mücadelede Farkındalık Ve Hazırlık.* .SETA Analiz, Sayı 183, Ankara.

Siber Güvenlik Enstitüsü (2019).https://sge.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce (Erişim Tarihi:18.03.2021)

Snowden, Edward (2013). The NSA andItsWillingHelpers, Spıegelhttp://www.spiegel.de/international/world/interview-withwhistleblower-edward-snowden-on-global-spying-a-910006.html(Erişim Tarihi: 05.04.2021)

Tarhan, K. (2018). *Uluslararası İlişkilerde Yeni Bir Güvenlik Anlayışı: Siber Güvenlik ve Siber Politika.* 11-14 Mayıs, İstanbul: II. İstanbul Boğaziçi Uluslararası Siber Politika Ve Siber Güvenlik Konferansı Özet Kitapçığı.

TBMM.(2004).https://www.tbmm.gov.tr/kanunlar/k5070.html (Erişim Tarihi: 18.03.2021)

TBMM.(2007). https://www.tbmm.gov.tr/kanunlar/k5651.html (Erişim Tarihi: 18.03.2021)

T.C.Resmi Gazete.(2008).Elektronik Haberleşme Güvenliği Yönetmeliği. https://www.resmigazete.gov.tr/eskiler/2008/07/20080720-1.htm (Erişim Tarihi: 27.02.2021)

Tezsever, S. (2009).*Millî Güvenliğimiz İçinde İstihbarat-Türkiye Cumhuriyeti ve İstihbarat Olgusu,* İstanbul Üniversitesi Basımevi, İstanbul.

TheGuardian (2007). RussiaAccused Of UnleashingCyberwarToDisableEstonia, Erişim Adresi: https://www.theguardian.com/world/2007/may/17/topstories3.russia (Erişim Tarihi: 06.04.2021)

The New York Times (2008). BeforetheGunfire, Cyberattacks.https://www.nytimes.com/2008/08/13/technology/13cyber.html (Erişim Tarihi: 05.04.2021)

The Sydney MorningHerhald (2008). GeorgianWebsitesForced Offline İn 'CyberWar' https://www.smh.com.au/technology/georgian-websites-forced-offline-in-cyberwar-20080812-gdsqac.html (Erişim Tarihi: 05.04.2021)

Tikk, E. vd. (2008). *CyberAttacksAgainst Georgia: Legal LessonsIdentified.* Tallinn: CooperativeCyberDefenceCentre of Excellence.

TimeTurk (2013). *Siber Âlemin 'Kanlı' Savaşları.* https://www.timeturk.com/tr/2013/01/17/siber-alemin-kanli-savaslari.html (Erişim Tarihi: 05.04.2021)

Turhan M. (2006). *Siber Güvenliğin Sağlanması, Dünya Uygulamaları Ve Ülkemiz İçin Çözüm Önerileri.* Bilgi Teknolojileri ve İletişim Kurumu, Ankara.

Ulaşanoğlu, M. E., Yılmaz, R., ve Tekin, M. A. (2010). *Bilgi Güvenliği: Riskler ve Öneriler,* Bilgi Teknolojileri ve İletişim Kurumu, Ankara.

Unibonn. (2019). *ProtectiveBotnet Counter Measure.* http://four.cs.unibonn.de/fileadmin/user_upload/leder/proactivebotnetcountermeasures.pdf (23.02.2021).

Ünver, H. A. (2017). *Bilişimsel Diplomasi, Siber Politikalar ve Dijital Demokrasi,* Ekonomi ve Dış Politika Araştırmalar Merkezi, Sayı 3.

Yalçın, H. B. (2017). *Ulusal Güvenlik Stratejisi: ABD, İngiltere, Fransa, Rusya, Çin.* SETA Kitapları, Ankara.

Yalman, Y. (2018). *Siber Terör, Terörizm ve Mücadele,* Grafiker Yayınları, Ankara.

Yaşar H. ve Çakır H. (2015). *Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemler*: 8.

Yener, Y. (2015). *8. Yılında Estonya Saldırılarına Çok Boyutlu Bir Bakış.* Siber Bülten.

Zetter, Kım (2011). *How DigitalDetectivesDecipheredStuxnet, theMostMenacingMalware in History.* Erişim Adresi: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/ Erişim Tarihi: 03.04.2021