SOĞUK SAVAŞ SONRASI NATO VE TÜRKİYE'DE SİBER GÜVENLİK

Yüksek Lisans Tezi

İbrahim YALÇIN

Eskişehir 2019

SOĞUK SAVAŞ SONRASI NATO VE TÜRKİYE'DE SİBER GÜVENLİK

İbrahim YALÇIN

YÜKSEK LİSANS TEZİ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI
Danışman: Doç. Dr. Elif TOPRAK

Eskişehir
Anadolu Üniversitesi
Sosyal Bilimler Enstitüsü
Şubat 2019

JÜRİ VE ENSTİTÜ ONAYI

İbrahim YALÇIN 'ın "Soğuk Savaş Sonrası NATO Ve Türkiye'de Siber Güvenlik" başlıklı tezi **05 Mart 2019** tarihinde, aşağıdaki jüri tarafından Lisansüstü Eğitim Öğretim ve Sınav Yönetmeliğinin ilgili maddeleri uyarınca toplanan **Uluslararası İlişkiler** Anabilim Dalında, **yüksek lisans tezi** olarak değerlendirilerek kabul edilmiştir.

İmza

Üye (Tez Danışmanı) : **Doç.Dr.Elif TOPRAK**

Üye : **Dr.Öğr.Üyesi Erhan AKDEMİR**

Üye : **Dr.Öğr.Üyesi Ali Onur ÖZÇELİK**

Prof.Dr.Metin COŞKUN
Anadolu Üniversitesi
Sosyal Bilimler Enstitüsü Müdürü

FINAL APPROVAL FOR THESIS

This thesis titled "Post-Cold War Cyber Security in NATO and Turkey" has been prepared and submitted by İbrahim YALÇIN in partial fullfillment of the requirements in "Anadolu University Directive on Graduate Education and Examination" for the Degree of Master of Science in International Relations Department has been examined and approved on …../…../……..

Committee Members		Signature
Member (Supervisor)	:	.....
Member	:	.....
Member	:	.....

.....
Director Graduate School of
Social Sciences

ÖZET

SOĞUK SAVAŞ SONRASI NATO VE TÜRKİYE'DE SİBER GÜVENLİK

İbrahim YALÇIN
Uluslararası İlişkiler Anabilim Dalı
Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü, …../….
Danışman: Doç. Dr. Elif TOPRAK

Devletlerin güvenlik algıları son yıllarda büyük değişimlere uğramış ve uluslararası ilişkilerde güç mücadelesi yıllar içerisinde artarak devam etmiştir. Gelişen teknoloji ülkelerin tehdit algılarını etkilemiş ve güç mücadelesine yeni kulvarlar açmıştır. İnsanlık tarihinde güvenlik ihtiyacı, her zaman önceliğini korumuştur. Güvenlik, devlet bekası ve insan yaşamı için vazgeçilemeyecek bir ihtiyaçtır. Devletleri uluslararası sistemde temel aktör olarak gören realist kuramın gelişen teknoloji ışığında şekillendiği ve değiştiği, tehdit ve risklerin arttığı ortamda (siber tehdit), NATO'nun güvenlik anlayışında oluşan bu yeni tehditlere ve değişen koşullara bağlı olarak güncellendiği görülmektedir. Bu tez kapsamında internetin ortaya çıkışı, siber tehditler ve siber güvenlik unsurları ele alınarak, NATO'nun değişen güvenlik anlayışı ve stratejileri incelenmiştir. Bu çalışma, siber güvenliğin NATO ve diğer devletlerin ulusal güvenlikleri için ne kadar kritik bir konu olduğunu ortaya koyabilmek adına önem arz etmiştir. Askeri harekâtlarda kullanılan konvansiyonel silah sistemlerinin harp sahasına tesiri hesaplanabilmektedir fakat siber çatışmalarda sınırın nasıl şekilleneceğini tahmin etmek zordur. Teknoloji ile birlikte bilişim sistemlerinin kullanımının artması; askeri, siyasi, ekonomik vb. alanlarda bu sistemlerden etkin şekilde faydalanılması, ülkelerin beka algılarını etkilemiş ve savunma stratejilerinin değişimine sebep teşkil etmiştir. Bilişim sistemi araçlarında görülen siber tehdit unsurları; bireysel, ulusal ve uluslararası boyutta çeşitli güvenlik krizlerine sebep olmaktadır. Bu nedenle Soğuk Savaş'tan sonra ortaya çıkan siber tehditlere karşı devletlerin ve uluslararası örgütlerin gerekli önlemleri alması önem arz etmektedir.

Anahtar Sözcükler: NATO, Tehdit, Güvenlik, Siber Tehdit, Siber Güvenlik, Siber Savaş,

ABSTRACT

POST-COLD WAR CYBER SECURITY IN NATO AND TURKEY

İbrahim YALÇIN
Department of International Relations
Anadolu University, Graduate School of Social Sciences
Supervisor: Assoc. Prof. Dr. Elif TOPRAK

The security perceptions of states have undergone tremendous changes in recent years and the power struggle in international relations has continued to increase in years. Emerging technologies have affected the threat perceptions of states and opened new lanes to the struggle for power. The need for security since the known date of humanity has always existed and will continue to do so. Security is an indispensable need for state's survival and human life. It is seen that realist theory, which accept states as the main actors in the international system, is shaped and changed in the light of the developing technology; threats and risks are increased (cyber threat), NATO's security approach is updated according to new threats and changing conditions. In this thesis, the emergence of the Internet, cyber threats and cyber security are discussed and the changing structure of NATO is analyzed. This study is important to demonstrate how critical cyber security is to the national security of NATO and all states. The effect of conventional weapons systems used in conventional tactical military operations on the warfare field can be calculated, but it is difficult to predict the borders in cyber conflicts. Increasing use of information systems, the effective use of these systems in commercial, political, military etc fields, affect state perceptions and cause a change in their defense strategies. Cyber threat elements in information systems; cause various security crises at individual, national and international levels. For this reason, it is important for states and international organizations to take the necessary precautions against cyber threats in the post Cold War international system.

Keywords: NATO, Threat, Security, Cyber Threat, Cyber Security, Cyber War,

06/03/2019

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

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

İbrahim YALÇIN

TEŞEKKÜR

Bu çalışmanın gerçekleştirilmesinde, kıymetli bilgi, birikim ve tecrübeleri ile bana yol gösterici ve destek olan saygıdeğer danışman hocam Doç. Dr. Elif TOPRAK'a, çocukluğumdan bu yana desteklerini hiç esirgemeyen sevgili anne ve babama, her zaman yanımda olan değerli eşime teşekkür ve saygılarımı sunarım.

İÇİNDEKİLER

Sayfa

TABLOLARIN LİSTESİ

Tablo **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

RESİMLERİN LİSTESİ

Resim **Sayfa**

KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar ve açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	Açıklamalar
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AGİT	Avrupa Güvenlik ve İşbirliği Teşkilatı
AGSK	Avrupa Güvenlik ve Savunma Kimliği
AGSP	Avrupa Güvenlik ve Savunma Politikası
ARPA	Gelişmiş Savunma Araştırmaları Projeleri Birimi
ARPANET	Gelişmiş Savunma Araştırma Projeleri Dairesi Ağı
APT	Gelişmiş Paketleme Aracı
BAB	Batı Avrupa Birliği
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Araştırmalar Merkezi
BİO	Barış İçin Ortaklık
BM	Birleşmiş Milletler
CCDCOE	Siber Savunma Mükemmeliyet Merkezi
CERN	Avrupa Nükleer Araştırma Merkezi
CEO	İcra Kurulu Başkanı
CMDA	Siber Savunma Yönetim Makamı
COMECON	Karşılıklı Ekonomik Yardım Konseyi
DDOS	Dağıtık Hizmet Reddi Saldırıları
DOS	Disk İşletim Sistemi
DOK	Daimi Ortak Konsey
DPI-SSL	Derin Paket İnceleme Teknolojisi
HTML	Hiper Metin İşaretleme Dili

ID	Kullanıcı Adı
IOT	Nesnelerin İnterneti
IP	İnternet Protokolü
ISAF	Uluslararası Güvenlik Kuvveti (Afganistan)
ISP	İnternet Servis Sağlayıcıları
IXP	İnternet Değişim Noktaları
IŞID	Irak ve Şam İslam Devleti (Terör Örgütü)
İHA	İnsansız Hava Aracı
KAİK	Kuzey Atlantik İşbirliği Konseyi
KFOR	Çok Uluslu Barış Gücü (Kosova)
MEBS	Muhabere Entegre Bilgi Sistemi
M.Ö	Milattan Önce
MMS	Multimedya Mesaj Servisi
NATO	Kuzey Atlantik Antlaşması Örgütü
NGO	Sivil Toplum Örgütü
NRC	NATO-Rusya Konseyi
NUC	NATO-Ukrayna Komisyonu
OEEC	Avrupa Ekonomik İşbirliği Örgütü
OKTEM	Ortak Kriter Test Merkezi
PDF	Taşınabilir Belge Formatı
PKK	Kürdistan İşçi Partisi (Terör Örgütü)
RF	Rusya Federasyonu
SFOR	Uluslararası İstikrar Gücü (Bosna Hersek)
SGE	Siber Güvenlik Enstitüsü
SSCB	Sovyet Sosyalist Cumhuriyetler Birliği
SSL/TSL	Taşıma Katmanı Güvenliği/Güvenli Soket Katmanı
STK	Sivil Toplum Kuruluşları
STÖ	Sivil Toplum Örgütü
SQL	Programlama Dili
TİB	Telekomünikasyon İletişim Başkanlığı
TCP/IP	İnternet İletişim Kuralları Dizisi
TMD	Harekât Alanı Füze Savunması

TSK	Türk Silahlı Kuvvetleri
USB	Evrensel Seri Veri Yolu
WP	Varşova Paktı
WWW	Dünyayı Saran Ağ

I. BÖLÜM: GİRİŞ

Uluslararası İlişkilerde güvenlik algısı temelinde yaşanan en büyük değişimler yirminci yüzyılda meydana gelmiştir. Bu süre içerisinde dünya küresel çapta iki yıkım yaşamıştır. Birinci ve İkinci Dünya Savaşları, savaşa dâhil olan ülkeleri direkt dâhil olmayanları ise dolaylı yönden etkilemiştir. Soğuk Savaş ile birlikte nükleer silahların ön plana çıkması ve nükleer silahlanma yarışı sonucunda yaşanan dehşet dengesi güvenlik sorununun ülkelerin en önemli beka konusu olduğunu ortaya koymuştur. Bu zaman diliminde ülkelerin güvenliğinin sağlanmasının önceki yıllara nazaran daha zor ve daha maliyetli olduğu görülmektedir. Artan maliyetler ve gelişen yeni tehditler neticesinde ülkeler güvenliklerini sağlamak için güçlü devletlerin himayesinde kurulan organizasyonlara ve ittifaklara dâhil olmak istemişlerdir. Oluşan Doğu Bloğu ve Batı Bloğu rekabeti gün geçtikçe artmış ve sonucunda Batı Bloğunun güvenliğini sağlamak için Kuzey Atlantik Antlaşması Örgütü (NATO), Doğu Bloğunun güvenliğini sağlamak için ise Varşova Paktı (WP) kurulmuştur (Şahin, 2017: 60-61).

İnsanlığın bilinen tarihinden itibaren süregelen güvenlik ihtiyacı, her zaman var olmuştur, gelecek yıllarda da bu ihtiyaç artarak devam edecektir. Güvenlik, devlet bekası ve insan yaşamı için vazgeçilemeyecek bir ihtiyaçtır.

Bu çalışma; "sert güç kapsamında açıklanan ve realist teori bakış açısıyla devletin tartışılmaz ana oyuncu olduğu güvenlik anlayışının, gelişen teknoloji ışığında şekillendiği ve değiştiği, tehdit ve risklerin arttığı (örneğin siber tehdit), NATO'nun güvenlik anlayışının da oluşan yeni tehditlere (siber tehdit) ve değişen koşullara bağlı olarak güncellendiği" tezini savunmaktadır. Bu tez; güvenlik anlayışının teknolojik etmenler ile birlikte dönüşümünü ele alacak bu çerçevede realist bakış açısıyla konuyu inceleyecektir. Realizm temelinde incelenecek olan siber tehdit ve siber güvenlik konuları uluslararası ilişkiler alanında güç odaklı mücadeleye yeni bir başlık açmıştır. Bu inceleme için internetin ortaya çıkışı, siber tehditler ve siber güvenlik unsurları ele alınarak, NATO'nun değişen yapısı araştırılmıştır. Çalışma, siber güvenliğin NATO ve diğer ülkelerin ulusal güvenlikleri için ne kadar kritik bir konu olduğunu ortaya koyabilmek adına önem arz etmektedir. Çalışma için genel olarak NATO ve siber güvenlik kapsamında nitel araştırma tekniklerinden vaka incelemesi ile literatür ve belge taraması yoluyla elde edilen verilerin betimsel analizi yapılarak realist teori çerçevesinde tartışılmıştır.

Bu tezdeki en büyük sınırlılık siber güvenlik konusunun çok geniş kapsamlı ve teknik bilgi düzeyinin üst seviyede olması nedeniyle teknik terimlerin en aza indirgene-

rek verilmeye çalışılmış olmasıdır. Tez konusunu NATO ve Türkiye'yi müştereken ilgilendiren siber tehditler ve bunlara karşı geliştirilen siber güvenlik tedbirleri oluşturmaktadır.

Uluslararası İlişkiler alanında güvenlik konularında yapılan çalışmaların tamamını düşünürsek yazılan eserlerde (kitap, tez, makale, dergi vb.) realist teori ışığında yapılan incelemelerin ön sıralarda olduğu karşımıza çıkacaktır. Bu tez realist teorinin bakış açısıyla incelenecektir.

Bu çalışmanın araştırma soruları:

1. Uluslararası ilişkilerde güç odaklı mücadelede değişen koşullar nelerdir?
    a) Siber tehdit nedir?
    b) Siber güvenliğe neden ihtiyaç duyulmaktadır?
2. Değişen güvenlik tehditleri karşısında NATO'nun verdiği tepkiler nelerdir?
    a) NATO tarafından siber güvenlik için alınan tedbirler nelerdir?
    b) Türkiye'de siber güvenlik politikaları nelerdir? olarak belirlenmiştir.

Realist teori bakış açısıyla incelenen güvenlik kavramına göre, uluslararası sistemi kontrol edebilecek ve düzeni sağlayabilecek güçlü bir yapı olmamasından dolayı uluslararası sistem anarşik özellik taşır. Devletler merkezi bir otoritenin olmadığı bu anarşi ortamında hiçbir zaman kendilerini tam anlamıyla güvende hissedemeyecektir. Bu güvensizlik ortamı devletlerarasında artarak gelişen bir "güvenlik ikilemi" sorununu oluşturmaktadır. Ortaya çıkan güvenlik ikileminin aşılması için devletlerin yapacağı çalışmaların tek başına yeterli olmayacağı, devletlerarası statüde olan NATO ve WP benzeri kurumların da sistemin içine dâhil edilerek oluşturulacak "kolektif güvenlik" anlayışı ile sağlanabileceği görülmüştür (Şahin, 2017: 62).

Realizme göre devlet uluslararası ilişkiler sisteminin tartışmasız en güçlü unsurudur. Anarşinin hâkim olduğu uluslararası ilişkiler sisteminde devletlerarası menfaat mücadelelerinin çözümü ancak savaşla aşılabilmektedir. Bu ortamda devletlerin yegâne amacı kendi meşruiyetlerinin sürdürülmesidir (ulusal beka-national survival). Bu meşruiyeti sağlamak için gerekli en önemli unsur olan güç (power) devletler için vazgeçilemez bir niteliğe sahiptir. Çünkü uluslararası sistem "güç" üzerine kurulmuştur. Devletler her ne kadar ittifak kursalar ya da organizasyonların/kuruluşların içine dâhil olsalar da anarşinin hâkim olduğu uluslararası sistemde güvenliklerini sağlayabilmenin en temel yolu kendi öz kaynaklarından oluşan kendi güçleridir. Devletlerin üye olduğu uluslararası ittifak ve kuruluşlar devlet bekası için ikinci öncelikli konumdadır. Öncelikle

devletler uluslararası sistemde kendi öz güçlerine dayanarak ayakta kalmak zorundadır. Uluslararası ilişkiler alanında realist kuramı savunanların düşüncelerini özetlersek:

1. İnsanlar varlık olarak kötümser bir bakış açısına sahiptir.
2. Güç devlet için en önemli unsurdur.
3. Devletler kendi güvenliklerini (beka) öz kaynaklarıyla sağlamak zorundadır.
4. Uluslararası ilişkilere anarşi hâkimdir. Anlaşmazlıkların ve güç mücadelelerinin çözülebilmesinin tek yolu savaştır.
5. Uluslararası sistemde sabit ve kesinleşmiş bir yapı yoktur (Aydın, 2004: 37-39).

Uluslararası ilişkiler temelde devletlerarası ilişkilerin çalışılmasından ibarettir. Her ne kadar, realist gelenek, uluslararası ilişkilerde devlet-dışı aktörlerin (bireyler, uluslararası örgütler, STÖ'ler, çokuluslu şirketler, terör örgütleri vb.) varlığını yadsımasa da, diğer tüm aktörler ya önemsizdir ya da daha az önemlidir; devlet her hâlükârda diğerlerinin hareket sahasını belir1eyen birincil (primary) aktördür. Bu çerçevede ortaya çıkan evrensel devletin diğer ortak özellikleri şu şekilde ifade edilebilir:

1. Devlet bütüncül (unitary) bir aktördür.
2. Devlet rasyonel bir aktördür.
3. Devletlerin uluslararası arenada karşılaştıkları sorunlar hiyerarşisinde ulusal güvenlik en tepede yer alır (Aydın, 2004: 40-41).

Realizm anlayışının hâkimiyeti her ne kadar 2. Dünya Savaşından sonra başlasa da kökenleri M.Ö. kurulan devletler dönemlerinde de görülmektedir. Başlıca savunucuları ise; Thucydides, Machiavelli, Thomas Hobbes ve Hans J. Morgenthau'dur.

Özellikle Morgenthau insanların ve devletlerin hareket tarzları incelendiğinde güç sahibi olma uğraşının ne derece önemli olduğunu vurgulamıştır. Morgenthau'ya göre güç uluslararası sistemin yapı taşıdır. İnsanlar, devletler ve hatta uluslararası örgütler güç elde etmek için sürekli bir yarışma hali içindedirler. Doğal bir sonuç olarak bu yarış rakip konumundaki varlıkları savaşa sürükler. İnsanların bu anarşi halinden kurtulmalarının yolu bir araya gelip kendi ortak çıkarlarını savunacak bir devlet yapısı kurmaktır (Aydın, 2004: 46-47).

Bu çalışma kapsamında realizmin, 'savunmacı' ve 'saldırgan' realizm okullarından da bahsetmek gerekir. Savunmacı realist görüş, devletleri uluslararası sistemin temel unsuru olarak görmektedir. Anarşinin hâkim olduğu uluslararası sistemde devletler

kendi güvenliklerini sağlamak için güç unsuruna sahip olma ihtiyacı hissetmektedirler. Bu ihtiyaç hali devletleri güç bağlamında bir yarışa itmekle birlikte güce karşı bir bağımlılık durumu da yaratmaktadır. Savunmacı realizmin temel bakış açısı güvenlik ikilemi ile birlikte oluşan uluslararası istikrarsızlıktır. Savunmacı realizme göre uluslararası sistem toplamının sıfır olduğu büyük bir strateji oyunundan oluşmaktadır. Devletler arasında yaşanan bu güç mücadelesi askeri, ekonomik, politik ve teknolojik temelde yapılmaktadır. Yapılan mücadelenin sonucunda devletler arasında bir denge oluşumundan söz edilebilmektedir. Savunmacı realizme göre uluslararası sistemi anarşiden kurtarabilmenin ve kısmi de olsa güven ve istikrar sağlayabilmenin yegâne yolu bu dengenin devamlılığının ve korunmasının sağlanmasından geçmektedir (Tüysüzoğlu, 2013: 69).

Savunmacı realist görüş, uluslararası ilişkiler açısından genel olarak daha pozitif bir bakış açısına sahip olarak karşımıza çıkmaktadır. Savunmacı realizme göre, güç mücadelesi içinde olan devletler aslında rakiplerine karşı güçlerini arttırmaktan çok, uluslararası sistemin güvenliğini dengenin devamlılığı ile sağlamayı hedeflemektedirler. Bu bakış açısına göre uluslararası sistemde dengeyi bozabilecek devletlerin olma ihtimali her zaman vardır. Devletlerin kendilerine has olan iç ve dış politikalarında zaman zaman yaşanacak değişiklikler neticesinde üstün güç olmak, genişlemek ve sistemin dışına çıkıp sistem üstü bir konumda olmak gibi çatışmacı bir bakış açısının görülebileceği oldukça muhtemeldir. Savunmacı realizm, bu bakış açısının kısa sürede bastırılacağını öngörmektedir. Çünkü uluslararası sistem içerisinde yer alan bütün devletlerin yararına olan güvenliğin sürdürülebilmesi sadece devletlerin pozitif ve denge unsurunu gözeten dış politikalar oluşturması ile sağlanabilecektir. Savunmacı realist görüşün önemle bahsettiği bir konu daha vardır: Uluslararası sistemin temelinde görülebilecek bazı değişikliklerin yarattığı sonuçlarla devletler arasın da var olan dengenin bozularak güvenlik ikileminin artarak tırmanmasına sebep olma ihtimalidir (Tüysüzoğlu, 2013: 70).

Saldırgan realist görüşün bakış açısına göre, anarşinin egemen olduğu uluslararası sistemde devletler kendi bekalarını sağlamak ve politikalarını devam ettirmek için saldırgan bir tutum benimsemektedirler. Bu saldırgan tutum devletleri üstün güç olma arzusu içinde hareket ettirmektedir. Saldırgan realist görüşe sahip bir devlet için güç sınırı her zaman rakip devletlerin sahip olduğu güçten üstün olma hedefidir. Kısaca rakip devletten güçlü durumdaysa gerçekten üstün bir devlet konumunda demektir. Çünkü sadece güç sahibi devletler ayakta kalabilir ve meşruiyetlerini devam ettirebilirler. Tabi ki saldırgan realizmi benimseyen bir devlet politikasını oluşturmadan önce söz konusu devlet

hesap yapmak zorundadır. Oluşturduğu politikayı hayata geçirmek için mutlaka bu politikanın yararının zararından fazla olması gerekmektedir. Hâkim olan anarşi durumunun devletlerin saldırgan bir politika izleyerek coğrafi ve siyasal genişleme yönünde hareket geçmelerine neden olacağını belirtmektedir. Saldırgan realizme göre, tüm devletler kendi ulusal güçlerini diğerlerine oranla maksimize etmenin peşindedirler. Zira sadece en güçlü olan devletler kendi çıkarlarını koruyabilir ve siyasal varlıklarını garanti altına alabilir. Devletler saldırgan ve genişlemeci politika izlemeden önce, böyle bir politika izlemenin yarar-zarar hesabını yaparlar ve izlenecek olan politikanın yararları, zararlarına üstün çıktığı takdirde o politikayı benimsemektedirler. Saldırgan realist görüşün kullandığı en büyük argüman, uluslararası sisteme hakim olan anarşiyi durdurabilecek ya da dengeleyebilecek devletler üstü bir kuruluş olmamasıdır. Bu durumda tüm devletler bağımsız ve egemen birer yapı olarak güvenliklerini kendileri sağlamak zorunda kalmaktadırlar. Devletlerin bağımsız bir şekilde devamlılığı en önemli maksat ve niyetleridir. Bu dürtü devletlerin stratejilerini oluşturan birinci öncelikli unsurdur. Uluslararası sistem içerisinde yer alan devletler, rakip devletlere karşı sürekli olarak şüphe içerisindedirler. Kısaca belirtilmeye çalışılan konu, devletlerin sabit bir güvenlik görüşlerinin olmamasıdır. Devletlerin niyet ve hedefleri değişebileceği gibi, bu hedefleri gerçekleştirmek için izleyecekleri yollar da değişebilmektedir. Bunun sonucunda devletler kendilerine has güvenlik tedbirleri alarak çatışma ortamını besleyecek politikalar oluştururlar. Bu aşamada saldırgan realizme göre devletlerin güvenliklerini arttırmasının bir diğer yolu ise 'göreceli kazanç' unsurudur. Göreceli kazanç, uluslararası sistem içerisinde olan bir devletin diğer bir devlet ya da devletlere karşı ulusal gücünü arttırmasıdır. Silah teminleri, ulusal güç çerçevesinde yapılan diplomatik baskılar, ekonomik tedbirler ve ambargolar gibi tedbirler bu bağlamda saldırgan realizm anlayışını destekleyen unsurlardır (Tüysüzoğlu, 2013: 71-72).

Realist kuramın genel stratejisi "güç" temeline dayanmaktadır. Uluslararası sisteme hâkim olan anarşinin aşılabilmesinin tek yolu da güce sahip olmaktan geçer. İkinci Dünya Savaşı sonrasında güç elde etme isteği ve ortak çıkar mücadelesi sonucunda uluslararası sistem iki kutuplu bir hale gelmiştir. Devletlerin tehdit algısı artmış ve güvenlik ihtiyacı her zamankinden daha fazla olmuştur. Askeri ve politik olarak hissedilen bu güvenlik ihtiyacı neticesinde devletler uluslararası bir güç altında kendilerini garanti altına almak istemişlerdir. Sonuçta ABD'nin öncülüğünde NATO kurulmuş ve uluslararası sisteme bir güç unsuru olarak dâhil olmuştur. SSCB'nin öncülüğünde ise WP ku-

rulmuş ve uluslararası sistemde yerini almıştır. NATO ve WP uluslararası sisteme realist bakış açısıyla bakmış ve bu kuramın temel unsuru olan "güç" (özellikle askeri güç) konusunda çalışmalarını sürdürmüştür. Bu güç mücadelesi aynı zamanda bir silahlanma ve nükleer mücadeleye de sebep olmuştur (Şahin, 2017: 64).

NATO ve WP arasında realizm bağlamındaki bu güç mücadelesi artarak devam etmiş ve silahlı kuvvetler her zaman en etkin kuvvet çarpanı olmuştur. Çalışmada bahsedeceğimiz üzere gelişen teknoloji, internetin ortaya çıkması, siber tehditlerin oluşması neticesinde güç kavramı, tehdit durumu ve güvenlik algısı da tamamen değişmiştir. Değişen güvenlik algısı sebebiyle siber tehdit, siber güvenlik ve siber savaş konuları NATO ve diğer dünya devletlerinin de güvenlik stratejileri gündemine girmiştir.

II. BÖLÜM : SERT GÜÇ KAPSAMINDA NATO'NUN TEMEL GÜVENLİK STRATEJİLERİ

2.1. GÜVENLİK

Güvenlik, uluslararası ilişkiler disiplini içinde kullanılan temel kavramlardan biridir. Ne var ki, çoğu zaman sorun güvenlik değil güvensizlik algılamaları üzerine ortaya çıkmaktadır. "Neye" veya "kime" karşı "güvenlik" ve ne kadar "güvenlik" sorularına ise yanıt vermek hiçbir zaman kolay olmamıştır. Bu sorulara verilecek tek bir yanıt da bulunmamaktadır (Çelebi, 2007: 70). Güvenlik kelimesinin uluslararası alanda yaygın kabul görmüş karşılığı olarak ´security´ kullanılmaktadır. Kelimenin kökenine baktığımızda "securus" sözcüğünden türetilmiş ve "emniyet hali" anlamına gelmektedir. Uluslararası İlişkiler temelinde ele alınan güvenlik (security) kelimesinin de bu kökenle bağlantılı olduğu rahatlıkla gözlemlenmektedir (Birdişli, 2014: 15-16). Tehditler artsa bile devletlerin ve uluslararası örgütlerin güvenliği tesis edebilme adına mücadelelerine devam etmeleri öngörülmektedir (Şahin, 2016: 23).

Mustafa Aydın ve Fulya Ereker'e göre, Türkiye içinde yapılan çalışmalarda güvenlik, resmi çevrelerde "tehlikeye karşı korunma ya da tehlikeli bir duruma maruz kalma " şeklinde açıklanmaya çalışılmıştır (Şahin, 2016: 23).

"[…] *Bu üç boyut resmi kaynaklarda ' toplumun yaşamını devam ettirmesi, toprak bütünlüğünün korunması ulusun temel kimliğinin muhafaza edilmesi' şeklinde ifade edilmektedir. Ulusal kimlik kavramının tanım içinde yedirilmiş olması bir yana, askeri güvenliği önceleyen ve şiddet içeren tehditlerin caydırılması ile bu tehditlere karşı savunmanın sağlanmasında devletin askeri kabiliyetlerine odaklanan bu güvenlik kavramsallaştırması, 21. yüzyılın öne çıkan etnik ve dinsel aidiyetleri, farklılaşan siyasi meşruiyet koşulları ile ekonomik olanaklar ve çevresel sorunların değişen yapısına bağlı olarak, daha geniş ve karmaşık bir güvenlik kavramsallaştırmasının ortaya çıkma ihtiyacı karşısında zorlanmakta ve geleneksel yapıları uyuma zorlamaktadır*[…]" (Aydın ve Ereker, 2013: 2-3).

Mustafa Aydın, Fulya Ereker, ve Güngör Şahin'in güvenlik ile ilgili tanımlarına göre güvenlik konusunun eskisinden daha karmaşık bir hal aldığı görülmektedir. Soğuk Savaş döneminde realist kuramın klasik güç kullanımı, askeri üstünlük ve ulusal çıkarlar gibi söylem ve sembolleri ile ölçülüp sağlanabilecek olan güvenlik bugün yerini çok daha farklı beklentilere bırakmıştır. Daha önce dost ve düşman ayrımında; düşman başka bir devlet olarak topuyla tüfeğiyle askeriyle çok daha net seçilebilirken, bugün tehditlerin artışı nedeniyle bu mümkün olamamaktadır. Ayrıca küreselleşen dünya ile bir-

likte gelişen insan hakları, azınlık hakları, alt kimlik-üst kimlik tartışmaları, mikro milliyetçilik çabaları ve diğer yeni kavramlar, kimin dost kimin düşman görülmesi bağlamında ulus-devletlerin ve karar vericilerin işlerini zorlaştırmaktadır. Sadece karar verme sorumluluğu olan seçkinlerin değil, belli başlı doğrularla yetişen ulus-devlet vatandaşlarının da zihinlerini bulandırmaktadır. Dolayısıyla tüm bunlar, "neye" veya "kime karşı güvenlik" ve "ne kadar güvenlik" sorularını daha da karmaşık hale getirmektedir (Şahin, 2016: 23).

Uluslararası ilişkilerde güvenlik kavramını ilk kez, 1952 yılında kaleme alan Wolfers'ın tanımı Güngör Şahin tarafından "güvenlik, nesnel manada, elde edilen kazanımlara yönelen tehditleri; öznel manada ise, söz konusu kazanımların olası bir bunalıma neden olmasına yönelik duyulan korku eksikliğini göstermektedir" (http-11, Wolfers, E.T: 15.03.2018) şeklinde açıklanmıştır.

Uluslararası alanda askeri, siyasi, ekonomik, eğitim, ticari, sosyal ve bütün alanlarda güvenlik anlayışı değişerek yerini yeni güvenlik anlayışı ile internet üzerinde siber tehdit, siber güvenlik, siber saldırı, bilgi savaşları, bilgi kirliliği, kara propaganda vb. teknolojik olgulara bırakmaktadır.

2.1.1 Güç

Uluslararası İlişkiler için yapılan teorilerde ve devletlerin oluşturduğu uluslararası politikalarda ve uluslararası sistemde güç (power) kavramı en önemli unsur olarak karşımıza çıkmaktadır. Uluslararası İlişkiler bakış açısıyla güç kavramı, devletlerin öz kaynaklarından yararlanarak kullanabildiği fiziksel ve soyut kavramları içeren, çıkarları doğrultusundaki amaçlarını gerçekleştirebilmek için elinde bulunan tüm unsurların toplamıdır. Güç kavramı devletler için kendi amaçlarını elde etmede kullanılan bir yöntem olduğu kadar, rakip devletleri kendi isteği doğrultusunda yönlendirme yetisini de kapsamaktadır. Realist teori bakış açısıyla "güç" kavramı genel olarak askeri güç (sert güç) olarak akla gelmektedir. Gücün tanımı, kapsamı ve şekli konularında yaşanan bazı anlaşmazlıklar olsa da realist teorisyenlerin tamamı gücün önemi konusunda fikir birliğine sahiptirler. Devletlerin bekasının sağlanması ve güvenliğinin tesis edilmesinde "güç" vazgeçilmez bir unsurdur (Özdemir,2008:117).

Uluslararası İlişkilerde güç konusundan bahsedilirken ilk olarak "sert güç (hard power)" akla gelmektedir. Bunun sebebi sert gücün devletler nazarında caydırıcı bir etkisinin bulunmasıdır. Sert gücün yarattığı etki realist teorisyenlere göre içerik ve so-

nuç olarak farklı algılanabilmektedir. Devletlerin sahip olduğu fiziksel (doğal) kaynaklar birer güç unsuru olarak uluslararası sistemde karşımıza çıkmaktadır. Bu doğal unsurlar devletlerin gücünde olduğu kadar caydırıcılığında da büyük rol oynamaktadır. Fakat politik amaçlar doğrultusunda kullanılmamış kaynakların birer güç unsuru olarak tanımlanıp tanımlanamayacağı konusu yaşanan en önemli tartışma konularındandır. Bu konuda da kullanılmayan unsurların potansiyel şeklinde algılanabilecek bir güç unsuru olduğu düşünülebilir (Özdemir,2008:117).

2.1.2. Güç dengesi

Uluslararası İlişkiler konusunda düşünen, yazan ve teori üreten birçok insan bulunmaktadır. Çalışmalar bazen teori üzerine olmuş, bazen de sistem ve sistemi oluşturan unsurlar üzerine olmuştur. Bu çalışmalara katkısı olan araştırmacılardan birisi de A. Morton Kaplan'dır. Kaplan, Avrupa'da klasikleşmiş olan güç dengesinden esinlenerek yeni bir güç denge sistemi geliştirmek için çalışmıştır (Yılmaz, 2008; 29).

Kaplan'ın düşüncesine göre güç dengesinin belli başlı bazı kalıplara uyması gerekmektedir:

1. Güç seviyesini yükseltmek için çabalarken her zaman savaşmaktan ziyade karşılıklı görüşmeler ön planda olmalıdır.

2. Uluslararası sistemde oluşan dengeyi bozabilecek olan ülkelere ve ittifaklara engel olmak için çalışılmalıdır.

Güç dengesi anlayışının başlamasında Fransız İhtilali ve İkinci Dünya Savaşı arasında geçen zaman dilimindeki tarihsel gelişmeler katkı sağlamıştır. Bu dönemde milliyetçilik artmış, milliyetçiliğin sebep olduğu bölünmelerle devlet sayısı çoğalmış, teknolojinin gelişmesiyle birlikte silah sistemleri değişmiş, güç odaklı büyük ittifaklar kurulmuş, askeri güç her zamankinden daha fazla ön plana çıkmıştır. Günümüzde ise oluşan bu uluslararası güç dengesi sistemine askeri gücün yanında politik ve siyasi güç de eklenmiş, ekonomik güç ise önemini arttırmıştır. Bunun yanında nüfus gücü, uluslararası örgütler, sivil toplum örgütleri de etkin bir unsur olarak uluslararası güç dengesinde yer sahibi olmuştur(Yılmaz, 2008; 29-30).

2.1.3. Sert güç

Realizm kapsamında güç denilince ilk düşünülen genellikle askeri güç olmuştur. Gücün tanımı ve çeşitliliği değişse de askeri gücün yeri ve önemi tüm devletler için

vazgeçilmezdir. Türk Silahlı Kuvvetleri için klasikleşmiş bir cümle her yerde duyulmaktadır. 'Barışın güvercini, savaşın kartalı' şeklinde ifade edilen bu cümle aslında sert gücün bir devlet için anlamını özetlemektedir. Barışı sağlayan ve bunun teminatı olan bu güç aynı zamanda savaşta da devletin güvenliği konusunda etkin ve caydırıcı bir özelliğe sahiptir. Sert gücün caydırıcılığı için mutlaka kullanılması gerekmez, diğer devletler için varlığı da caydırıcı bir etkendir. Devletlerin güvenliği için askeri güç hayati bir öneme sahiptir. Her an hazır ve kullanılabilir durumda olan askeri bir güç oluşturmak ve devamlılığını sağlamak devlet yetkililerinin ülke güvenliği için alacakları birincil tedbirdir. Sert güç kapsamında değerlendirilen askeri güç mutlak suretle teknoloji ile desteklenmeli, nüfus gücüyle devamlılığı sağlanmalı ve ekonomik güç ile her türlü ihtiyacı karşılanmalıdır. Gelişmeyen ve teknolojik destek görmeyen bir askeri güç sadece kalabalık bir gruptan ibarettir (Yılmaz, 2008; 39).

Oluşturulan askeri gücün sert güç kapsamında olası tehditlere karşı saldırı maksatlı kullanılmasının yanında, aynı tehditlere karşı savunma nitelikli de kullanılabilmesi gerekmektedir. Askeri güç sadece saldırı nitelikli olmamalıdır. Elbette iki şekilde de kullanılabilmesinin yolu devleti yönetenler ile komuta kademesinin tamamıyla işbirliği esasları içinde çalışmalarına dayanmaktadır. ABD örneğinden yola çıkarak güçlü bir devlet olmanın temel yapı taşı güçlü bir askeri güce sahip olmaktan geçmektedir. Devletlerin uluslararası sistemde söz sahibi olmasını sağlayan askeri gücün niteliklerini maddeler halinde sıralarsak:

1. Teknolojik imkânlar dâhilinde nükleer silah sistemlerinin bulunması
2. Diğer ülkelerde kendine ait askeri birlik konuşlandırması (askeri üs kurma, deniz üssü kurma)
3. Elindeki askeri gücün MEBS (Muhabere Entegre Bilişim Sistemleri) imkânları
4. Etkin ateş gücüyle (teknolojik gelişmelerle güncellenen etkin silah sistemleri) donatılmış olması
5. Askeri gücün her türlü lojistik ve ulaştırma faaliyetleri ile kesintisiz desteklenmesi (stratejik ve taktik seviyede birlik kaydırma, ikmal malzemelerinin zamanında ve eksiksiz tedariki) kabiliyetleridir (Yılmaz, 2008; 39-40).

2.1.4. Yumuşak Güç

Yumuşak güç kavramı akademik olarak ilk kez Joseph S.Nye tarafından "Liderliğe Zorunluluk: Amerikan Gücünün Değişen Doğası" isimli eserinde bahsedilmiştir. Bu kavram genel olarak sert güç kapsamında kullanılan unsurların yerine kullanılması önerilen bir yöntemdir. Yumuşak gücün temeli, devletin sert güç kapsamında elde edebileceği hedeflerini yumuşak güç ile daha kolay ve daha kalıcı şekilde elde etmeye çalışmasıdır. İnsan hakları kavramı, ülke kültürü ve ülkenin demokrasi anlayışı yumuşak gücün öncelikli ihraç unsurlarıdır. Sert güç elde etmek istediği uluslararası amaçları kuvvet kullanarak (askeri, ekonomik tedbirler) elde ederken, yumuşak güç aynı amaçları diğer ülkelere karşı tehdit etmeden, baskı uygulamadan ve hatta o ülkelere cazip olacak şekilde gerçekleştirmektedir. Asıl amaç yumuşak gücü uygulayan devletin isteklerinin ve amaçlarının diğer devletler açısında da arzulanmasını temin ederek, uluslararası sistemde güç sahibi olmaktır. Bu yöntem güç kaydırma olarak da düşünülebilir (Rüşen, 2018: 340).

Devletler tehditlere karşı koymak, güvenliklerini temin etmek ve hedeflerine ulaşmak için bir seçenek olarak 'askeri güç' kullanırlar. Politik ve ekonomik güç unsurlarını kullanmak da sert güç kapsamında değerlendirilebilir. Ancak bu noktada değerlendirilmesi gereken konular; bu gücü kullanmanın zor olması, uzun süre alması ve etkisinin karşı tarafta bulunan devletin alınacak mesajı benimsemesine bağlı olmasıdır. Yumuşak gücün unsurları ile hareket etmek, sert gücün unsurları ile hareket etmeye göre fazla zaman gerektiren ve kısmen yavaş ilerleyen bir süreçtir (Nye, 2005:100-101).

Bu kuramı oluşturan Joseph S. Nye yumuşak gücü, zor kullanma ve ekonomik tedbirlerin haricinde cazibe oluşturarak hedeflere ulaşma yeteneği olarak sunmuştur. Diğer devletlerin yapması istenilen konular için mutlaka sert güç kullanma ve bunun için para harcama isteği olmaksızın da hedefler gerçekleştirebilir. Nye bir ülkenin askeri gücü ve bunu destekleyen ekonomik gücünün oluşturduğu ikna yönteminin sert güç olduğunu söylemektedir. Yumuşak güç ise aynı ülkenin kültür öğelerinin ve siyasi düşüncelerinin cazibesinden oluşmaktadır. Sonuç olarak uluslararası sistemde devletler sizin politik bakış açınızı benimseyip uygun buluyorlarsa sağlam bir yumuşak gücünüz var demektir. Yani yumuşak güç, diğer ülkelerin politikalarını kendi ülkenizin istediği şekilde oluşturma sanatıdır. Kısaca belirtmek gerekirse yumuşak gücü fazla olan ülkeler kendi amaçlarını gerçekleştirirken diğer devletlere göre daha az kaynak harcamakta-

dırlar. Fakat daha fazla zaman harcanacağı ise göz önünde bulundurulmalıdır (Yılmaz, 2008; 41).

Nye tarafından yapılan yumuşak güç açıklaması uluslararası ilişkiler alanında çalışma yapan bazı teorisyenlere göre doğru kabul edilmemektedir. Bu bakış açılarından birine göre yumuşak güç kuramı her ülke için geçerli değildir. Yumuşak gücün geçerli sayılabilmesi ve uygulanabilmesi için söz konusu ülkede gelişmiş bir demokrasinin tesis edilmesi, teknolojik gelişmelere açık ve iyi bir eğitim sistemi ile birlikte haberleşme sistemi ve medya sistemi yönünden ulaşılabilir olması gerekmektedir. Bununla birlikte yumuşak gücü bahsedilen şekilde net olarak ayırmak doğal güç kaynakları bakımından bazı unsurların yeterli değerlendirmeye tabi olmaması sonucuna sebep olabilir. Nüfus gücü, teknolojik güç ve coğrafi güç yanlış değerlendirilebilecek başlıca konular arasında yer almaktadır. Ayrıca askeri gücü yanında hiçbir güç unsuru olmadan kendi kendine bir sert güç unsuru şeklinde düşünmek de imkânsızdır. Bu konuya kısa bir örnek verecek olursak, NATO vb. kuruluşların icra ettiği insani yardım görevleri bu kapsamda değerlendirilebilir (Yılmaz, 2008; 40-41).

Bilim insanlarının çoğu sert güç ile yumuşak güç arasında bir dengenin varlığından bahsetmektedir. Sert güç unsurlarının etkin ve fazla uygulanması, yumuşak güç unsurlarının uygulanabilme ihtimalini ortadan kaldırabilir. Aşırı derecede sert güç uygulanan bir ülkeye, belli bir süre sonra yumuşak güç uygulamanın bir verimliliği yoktur. Çünkü söz konusu ülkede, sert güç uygulayan ülkeye karşı nefret dürtüsü harekete geçecek ve yumuşak gücün benimsetmeye çalıştığı her türlü mesaja yararına ya da zararına olsun ön yargılı davranarak olumsuz cevap verecektir. Bu denge prensibinden hareketle "akıllı güç" kuramı ön plana çıkmaktadır. Günümüzdeki uluslararası ilişkiler sisteminde akıllı güç; sert güç ile yumuşak gücü birlikte uygulayabilme yeteneğidir. Sert güç kullanılarak alınan sonuçların çok kalıcı olmadığı görülmekte, bu yöntemi yeterli miktarda kullandıktan sonra yumuşak güç ile takviye etmenin gerekliliği ortaya çıkmaktadır (Yılmaz, 2008; 41).

2.1.5. Soğuk Savaşın Yarattığı Koşullar ve NATO

Soğuk Savaş, İkinci Dünya Savaşı'nın bitmesi ve SSCB'nin dağılma sürecine kadar ABD ve SSCB arasında gerçekleşen siyasi, askeri, ekonomik restleşmelerdir.

SSCB ve ABD'nin güç odaklı mücadelesi İkinci Dünya Savaşı'ndan itibaren artarak devam etmiştir. Realist teori odağında yaşanan bu güç mücadelesi dünyayı iki ku-

tuplu bir sistem içine sokmuştur. SSCB'nin yayılmacı politikasına karşı ABD bu yayılmayı durdurmaya yönelik tedbirler almaya başlamıştır. ABD, Sovyet yayılmacılığına karşı Avrupa ve Ortadoğu'da bazı tedbirler almak zorunda kalmıştır. Stratejik olarak planladığı Marshall Planı ile tedbirlerine başlamış, Truman Doktrini ile de bunu devam ettirmiştir.

Sert Güç'ün ön planda olduğu bu dönemde ABD'nin aldığı bu tedbirlerin askeri bir tedbir ile taçlandırılması gerekmekteydi. NATO bu güç mücadelesinin doğal bir sonucu olarak kurulmuştur. NATO'nun kurulmasıyla birlikte ABD-SSCB mücadelesi ağırlıklı olarak askeri güç yarışına doğru kaymıştır.

2.2. NATO'nun Kurulması

Birbirinden farklı dünya görüşüne sahip devletler, II. Dünya Savaşı yıllarında müttefik olmak zorunda kalmışlardır. Oluşturulan bu iyimser havayı savaş sonrasında da devam ettirmek niyetinde olan devletlerin öncülüğünde 50 devletin temsilcileri bir araya gelerek 1945 yılında ABD'nin San Francisco kentinde Birleşmiş Milletler (BM)'in kuruluşunu sağlamışlardır. Savaşın devam ettiği süreçte kurulan BM'ye barış ve güvenliğin uluslararası boyutta tesis edilmesi için güvenilmiştir. Fakat SSCB'nin uzlaşmak istememesi ve veto konusundaki tavrı münasebetiyle BM uluslararası güvenlik krizlerinin çözülmesinde üstüne düşen görevi yerine getirmekte yetersiz kalmıştır (Sarınay, 1988: 240). Birleşmiş Milletlerin kurulduğu tarih olan 1945'ten 1949'a kadar beş daimi üye kendilerine verilen veto hakkını otuz defa kullanmıştır (Gönlübol, 1969: 70).

Dolayısıyla uluslararası sorunların çözümü amacıyla kurulmuş olan Birleşmiş Milletler teşkilatı tam anlamıyla arzulanan sonuçları alamamakla birlikte, çözülmeyi bekleyen veto sorunlarını doğurmuştur.

Çözümlenemeyen bu sorunlar ile birlikte hali hazırda Sovyetler Birliği ile Batı Avrupa devletleri arasında gerek ideolojik gerekse ekonomik alanlarda ciddi görüş ayrılıkları mevcut idi. Üstelik savaşta Almanya ve Japonya'nın yenilmesi Sovyet Rusya'ya doğusunda ve batısında ciddi yayılma imkânı da vermişti. Sorunları çözmek amacıyla toplanan barış konferanslarından istenilen olumlu sonuçlar çıkmamıştır. 1947 Mart ayında Moskova'da toplanan Dışişleri Bakanları Konferansı'ndan sonra da Sovyet Rusya ile Batı Avrupa devletleri arasındaki savaş yıllarında görülen işbirliği yerini karşılıklı tedirginliğe bırakmıştır (Armaoğlu, 1949: 417-418).

İkinci Dünya Savaşı sonrasında Avrupa Devletleri'nin ekonomik ve askeri açıdan çökmüş olması ve bununla birlikte ABD'nin de kendi kıtası içinde kalma politikası neticesinde kuvvetler dengesi tamamıyla Sovyet Rusya'nın lehine dönmüş ve Sovyet Rusya Avrupa'nın en güçlü devleti olarak ortaya çıkmıştır. Oluşan SSCB hâkimiyeti bu zaman diliminde Avrupa'nın doğusuna kadar dayanmıştır. Avrupa'daki ülkeler, karşılaştıkları bu güvenlik krizini aşmak için uluslararası bir örgüt altında birleşme gereksinimi hissetmişlerdir (Peksarı, 2007: 1). Avrupa'nın ihtiyaçları ve yeniden yapılandırılması için ABD kendi hazırladığı Marshall Planını uygulamak için çalışmalara başladı.

Oluşan bu güvenlik krizi altında G. Marshall stratejik bir plan hazırladı. Marshall Planı adı altında oluşturulan söz konusu stratejik plan Avrupa devletlerinin ABD'den ekonomik yardımlar almasını öngörmekteydi. Aynı zamanda Avrupa devletlerinin de kendi içlerinde ekonomi alanında işbirliği gerçekleştirmeleri talep edilmekteydi.

Avrupa devletleri tarafından olumlu bir şekilde karşılanan Marshall Planı uygulanmaya başlandı. Fransa'nın başkenti Paris'te düzenlenen konferansa Türkiye ve 16 Avrupa ülkesi de katılmıştır. Toplantının ana konusunu Avrupa ülkeleri için alınacak ekonomik tedbirler oluşturmuştur. Yapılan bu çalışmaların neticesinde 4 yıl süre zarfında icra edilecek Avrupa Ekonomik Kalkınma Programı geliştirilmiştir. Yapılan bu programla birlikte ABD'de Ekonomik İşbirliği Kanunu hazırlamıştır. Bu tarihten sonra ise 18 Avrupa devleti işbirliği içerisinde "Avrupa Ekonomik İşbirliği Örgütü (OEEC)"nü kurmuşlardır. OEEC'nin asıl maksadı üye ülkelerin yapacağı işbirliği yöntemiyle Avrupa ülkelerin düzgün işleyen bir ekonomik sisteme kavuşturmaktı (Koyuncu, 2010: 12-13).

Marshall Planının uygulanmaya geçilmesi ile Avrupa devletlerinin durumları kısmen düzelme gösterse de, Sovyetler Birliğinin yayılmacı politikasının önünde set oluşturamamıştır. Sovyetler Birliğinin empoze ettiği ve desteklediği komünizm dalgası Doğu Avrupa'yı tamamıyla kuşatmıştı. Yugoslavya, Arnavutluk, Bulgaristan, Romanya, Macaristan, Polonya ve Doğu Almanya'da Sovyetler Birliğinin desteklediği komünist hükümetler iş başına geçmişti.

Stalin'in Çekoslovakya'daki komünistlere verdiği destek sayesinde gerçekleştirilen darbe NATO'nun kurulmasına zemin hazırlamıştır. Marshall Planı ortaya çıktıktan sonra SSCB komünist yayılmasına daha da hız vermiştir. Batı Bloğu ülkelerine bir gözdağı niteliğinde olan bu darbe SSCB'nin benzer girişimlere diğer ülkelerde rahatlıkla girişebileceğini göstermiştir. Yapılan bu darbeye karşı Batı Bloğu ülkelerinin ilk icraatı

Brüksel Antlaşması olmuştur. Bu antlaşmanın en önemli uluslararası neticesi Batı Avrupa Birliği (BAB)'nin kurulmasının sağlanmasıdır. Bu antlaşmayı imzalayan devletler; Belçika, Hollanda, Fransa, Lüksemburg ve İngiltere'dir. Antlaşmanın en önemli sonucu Avrupa ülkelerinin SSCB yayılması karşısında almış oldukları en önemli koruyucu ittifak tedbiridir. Alınan bu tedbir ile hem SSCB yayılmasına karşı birlemiş bir karşı tavır gösterilmiş hem de ülkeler arasında ekonomik bir işbirliği sağlanarak bundan sonraki dönemler için uluslararası sistemde söz sahibi olacak bir yapının da temelleri atılmıştır (Koyuncu, 2010: 12-13).

Böylece yalnızcılık politikası izlemeyi içeren ve "Avrupa işlerinden uzak durmayı" öngören 1823 Monroe Doktrini'ni II. Dünya Savaşına katılmakla terk etmiş olan ABD, Soğuk Savaş konjonktürüne bağlı olarak, Avrupa işlerine müdahale etme sürecini başlatmış oldu (NATO El Kitabı, 1995: 178).

Yaşanan tüm bu gelişmeler Sovyetler Birliği ve komünizm önünde set oluşturmak için yeterli değildi. Alınan sosyal, politik ve ekonomik önlemlerin caydırıcı hale getirilmesi için askeri tedbirlerle taçlandırılması gerekmekteydi. ABD tüm bu gelişmelerin ve işbirliğinin askeri bir çatı altında birleşmesinin uygun olacağı görüşündeydi. 1948 yılının Aralık ayında Washington'da politik temaslara başlanıldı. Görüşmelere Brüksel Antlaşması ülkeleri, Kanada ve ABD katıldı. SSCB'nin tüm politik ve askeri dayatmalarına karşın İskandinav coğrafyasındaki devletler de görüşmelere katılım sağlamıştır. 1949 yılında ABD'nin öncülüğünde gerçekleştirilen çalışmalarla Washington şehrinde North Atlantic Treaty Organisation (NATO)-Kuzey Atlantik İşbirliği Örgütü antlaşması imzalanmıştır. Bu yapılan antlaşmanın kurucu imzaya sahip ülkeleri ise; İzlanda, Fransa, Kanada, Lüksemburg, Belçika, İngiltere Norveç, Hollanda, İtalya, ABD, Portekiz ile Danimarka'dır (NATO El Kitabı, 1995: 204).

İmzalanan bu antlaşma 24 Ağustos 1949 tarihinde yürürlüğe girdi. ABD'nin, Sovyet Rusya yayılmacılığına karşı aldığı önlemler üç basamaktan oluşmuştur. Birinci basamak Marshall Planı ile uygulanan sosyal ve ekonomik tedbirlerdir. İkinci basamak Avrupa ülkeleri ile yapılan politik görüşmelerdir. Üçüncü basamak ise "caydırıcı bir güç" olarak kullanılabilecek olan NATO'nun kuruluşudur.

Soğuk Savaş'ın uluslararası ilişkiler sistemindeki güç dengesini değiştiren en büyük etkisi tartışmasız bir şekilde nükleer silahların keşfedilmesi ve bu alanda yapılan silahlanma faaliyetleri olmuştur. Nükleer silahların güç mücadelesine girmesiyle birlikte stratejik ve taktik seviyede bütün harp sahası taktikleri değişmiştir. Konvansiyonel si-

lahların düşman ordusu üzerindeki etkisi tahmin edilip risk analizleri rahatlıkla yapılabilirken, nükleer silahların birincil ve ikincil etkilerini hesaplamakta zorluklar yaşanmış ve topyekûn yok edici etkisi her zaman insani ve ahlaki bir tehdit olarak ülkelerin karşısına çıkmıştır. Harp sahasının temel kurallarını değiştiren bu keşif sadece bir balistik füze ile hem düşman birliklerini hem de birliklerin konuşlandıkları şehirleri tamamıyla yok etme imkânını sağlamıştır. Bununla birlikte iki kutuplu uluslararası sistem doğal olarak tehdit algısını değiştirmiş ve nükleer sistemler üzerine kurgulamıştır. Silahlanma yarışı hızlanmış ve bu yarış uluslararası sistemde dehşet dengesi olarak anlatılan topyekûn imha ihtimalinin oluşabileceği noktaya kadar gelmiştir. Güç temelinde yapılan bu silahlanma yarışında her ne kadar caydırıcı olma ilkesi benimsenmiş gözükse de gelinen nokta caydırıcılıktan çok toplu imha ihtimalinin artması olarak karşımıza çıkmıştır. "Caydırıcılık" her ne kadar nükleer silahlar bağlamında açıklanıyor olsa da, ilerleyen bölümlerde açıklayacağımız gelişen teknoloji ışığında ortaya çıkan siber güvenlik konusuyla da ilişkilidir (Mehmetçik, 2015; 34-35).

2.3. Doğu Bloğu'nun Kurulması ve Varşova Paktı

Marshall Planı'nın Batı Avrupa ülkelerinde uygulanmaya başlamasının ardından SSCB karşı bir plan olarak doğudaki eşdeğeri Karşılıklı Ekonomik Yardım Konseyi (COMECON)'ni hayata geçirdi (Bilgili, 2008: 19). Stalin'in amacı COMECON ile uydu devletleri ekonomik ve askeri alanda geliştirmek ve kendine bağlı kılmaktı. Ancak COMECON konusunda Stalin ve Kruşçev farklı görüşlere sahipti. Stalin COMECON'u ABD'nin Marshall Planına bir cevap olarak düşünüyordu. Fakat Kruşçev için COMECON kâğıt üzerinde atılmış önemsiz bir adımdı.

Kruşçev COMECON'u geliştirip gerçek güçlerden oluşan bir yapı haline getirmeyi düşündü. Bu dönüşümün askeri güçlerden yapılanarak başlaması gerektiğini düşünerek uydu ülkelerin silahlı kuvvetlerine yapmış olduğu bir takım antlaşmalarla etki etti.

Terfiler Moskova tarafından gerçekleştiriliyordu. Komutanların hemen hemen hepsi eğitiliyordu. Ordunun tüm ekipmanı Sovyetler tarafından karşılanıyordu. Kısacası Doğu Avrupa orduları tamamıyla SSCB birlikleri gibi görünmekteydi. Doğu Bloğu ülkeleri askeri ve ekonomik işbirliğini daha da arttırmak için Varşova şehrinde toplandı. Toplantının asıl amacı NATO karşıtı bir yapılanmaya gitmek ve uluslararası bir güç yaratmaktı. Toplantı neticesinde Varşova Paktı (WP) kuruldu. Nihai hedef hem NATO benzeri bir yapı oluşturup merkezi bir komuta sistemi tesis etmek, hem de bağlı devlet-

lerin içişlerine kadar nüfuz etmenin uluslararası hukuk açısından sorun oluşturmayacak sebebini yaratmaktı (Bilgili, 2008: 20).

NATO'ya karşı savunmacı realizm mantığıyla kurulan Varşova Paktı da caydırıcı güç kapsamında kurulmuştur.

Birinci Dünya Savaşından sonra Avrupa ekonomik, sosyal, insan kaynağı, askeri vb. alanlarda büyük kayıplar vermişti ve tam bir çöküş halindeydi. Savaşın sonunda iki büyük güç ortaya çıktı. ABD kendi çıkarları doğrultusunda Avrupa devletlerini yeniden yapılandırmak ve güçlendirmek için Marshall Planını oluşturarak devreye soktu ve sonrasında NATO'yu da kurarak askeri açıdan birlik sağladı. Bunun sonucunda; hem kendi küresel hedeflerine doğru yaklaştı hem de tek rakibi olan Sovyetler Birliğine karşı bir askeri bir güç ve coğrafi bir set oluşturdu.

Sovyetler Birliğinin ABD ve Batı Avrupa ülkelerine karşı kullandığı en büyük silah komünizm anlayışıydı. Sovyetler Birliğinin yapmış olduğu bütün icraatlar ABD'ye atılan karşı adımlardı. Yukarıda belirtildiği gibi Marshall Planına karşı COMECON, NATO'ya karşı ise Varşova Paktı oluşturuldu. Bu etkinlik ve nüfus yarışında ABD ilk adımı atan, Sovyetler Birliği ise 'savunmacı realizm' stratejisini benimseyen bir rakip görünümündeydi.

2.4. Soğuk Savaş Dönemi ve Yaşanan Gelişmeler

Tam manasıyla bir güç mücadelesi olan Soğuk Savaş dönemi NATO ve Varşova Paktı'nın da kurulmasıyla birlikte iki kutuplu askeri bir güç mücadelesi haline gelmiştir. ABD, NATO'yu hem SSCB yayılmacılığına karşı hem de küresel hedefleri ve çıkarları doğrultusunda yönlendirmiştir. Buna karşılık Varşova Paktı ise tamamen SSCB hegemonyasında NATO'ya karşı savunmacı realizm mantığı ile çalışmıştır. Realist teori odağında yaşanan bu "sert güç" mücadelesi ABD ve SSCB arasında çözülmesi zor ve savaşa kadar gidebilecek bazı krizlere yol açmıştır.

2.4.1. Avrupa'da Berlin bunalımı

1947'de Batılılar Almanya'nın kendi işgal bölgelerinin ekonomik bütünleşmesini başlattılar. 1948'de ise para reformu yaptılar ve bu bölgede bir Alman hükümetinin kurulmasını kararlaştırdılar. Buna Sovyetlerin tepkisi Batı Berlin'i abluka altına almak oldu. Sovyet bölgesinin 100 km. kadar içinde bulunan Berlin de dört işgal bölgesine ayrılmış ve bu bölgedeki Batılı birliklerin ve halkın ihtiyaçlarının karadan, havadan ve

demiryolu ile serbestçe sağlanması kararlaştırılmıştı. Bu abluka ile Sovyetler kara ve demiryolunu kestiler. Batılılar ya bir çatışmayı göze alacak ya da bölgenin ihtiyaçlarını havadan sağlamaya çalışacaklardı. İkinci yolu seçen Batılılar havadan ihtiyaçları karşılamayı başarınca Sovyetler ablukayı kaldırdı. Berlin Bunalımı, Batı Blokunun örgütlenme sürecini de hızlandırdı (Armaoğlu, 1949: 417-418).

2.4.2. Kore savaşı

1910 yılından beri Japonya'nın egemenliği altında bulunan Kore, Japonya'nın II. Dünya Savaşı'ndan yenik devlet olarak çıkması sonucu tartışılan büyük bir sorun haline geldi. 1945 yılında Sovyetler, Kore ülkesinin kuzey kısmını, ABD'de güney kısmını ele geçirdi. ABD ve SSCB'nin taktiksel manevraları Kore sorununun miladı olmuştur. Bunun üzerine ABD sorunu Birleşmiş Milletlere götürdü. Ancak Sovyet Birliği bu komisyonla işbirliğine yanaşmamış ve 38. enlemi geçmesine izin vermemiştir. Bu zıtlaşma sonucu 1948 yılında Kore'nin güney kısmında BM himayesinde ve Kore'nin kuzey kısmında ise SSCB himayesinde birbirinden farklı ülkeler kuruldu. BM daha sonra tek meşru hükümetin kendisinin desteklediği Kore'nin güneyinde kurulan ülke olması gerektiğini, kuzeyde ilan edilen ülkenin kabul edilmediğini ve tüm devletlerin Güney Kore'yi tanımasını gerektiğini belirtti. 1948'de Kuzey Kore'de 1949'da Güney Kore'de ordular kurulması çatışma derecesini arttırmıştı. Fazla zaman geçmeden iki ülke arasındaki çatışmalar başlamıştır (Acar, 1991'den aktaran Bilgili, 2008: 43).

Gerginliğin tırmandığı iki kesim arasındaki güven ortamının kaybolduğu bir dönemde ABD, Güney Kore Cumhuriyeti ile Sovyet Birliği ise Çin ve Kuzey Kore ile karşılıklı dostluk ve güvenlik antlaşması imzaladılar. Kısa bir süre sonra ise 1950 yılında Güney Kore askeri birliklerininsınırı ihlal ettiklerini iddia eden Kuzey Kore askeri harekâta başlayarak Güney Kore Cumhuriyeti'ne resmen savaş açtı.

Savaşın başlamasıyla birlikte Güney Kore'ye ABD yardımları başladı. ABD'nin etkisi altındaki Birleşmiş Milletler Güvenlik Konseyi önce savaşın sona erdirilmesini ve müteakiben Kuzey Kore'nin hemen birliklerini geri çekmesi gerektiğini duyurdu. Sonrasında ise Kuzey Kore'nin mevcut olan barış düzenini bozduğunu belirterek BM çatısı altındaki ülkelere Güney Kore'ye bu mücadele de destek verilmesi için talepte bulunmuştur. Birleşmiş Milletlere üye olan ülkelerin üç tanesi hariç (SSCB, Polonya, Çekoslovakya) tüm ülkeler bu kararları onaylamıştır. Geçen zaman süresinde Güney Kore'nin tamamı tehdit altına girmiştir (Alacakaptan, 1984'den aktaran Bilgili, 2008: 43).

BM'in çağrısıyla hareket eden üye devletlerin askeri güçlerinin savaşa katılmasıyla birlikte Kuzey Kore yeniden 38. enleme çekilmek zorunda kalmıştır. Denge sağlandıktan sonra ise Kuzey Kore masaya oturmak zorunda kalmıştır. Kuzey Kore ile BM görüşmeleri sonucunda anlaşma sağlanmıştır. Yapılan anlaşma neticesinde 38. Paralel iki ülkeyi ayıran yer olarak kabul edilmiştir. Ayrıca söz konusu yere iki ülkenin askeri birliklerinin girmesinin yasak olduğu da taraflara bildirilmiştir (Bilgili, 2008: 44).

Üç yıl süren Kore Savaşı sonrası Kore, 38. enlemde Güney Kore ve Kuzey Kore olmak üzere ikiye bölünmüştür. Gerçekleşen güç mücadelesiyle uluslararası sistemdeki iki blok resmen karşı karşıya gelerek mevcut güçlerini test etmişlerdir. Aslında burada şu söylem savaşın daha açık ve net bir özeti olacaktır. Kore Savaşı komünizm ile liberalizmin savaşıdır ve dolayısıyla bu Sovyetler Birliği ile Amerika Birleşik Devletlerinin küresel üstünlük kurma mücadelesidir (Angın, 1967'den aktaran Bilgili, 2008: 44).

2.4.3. Türkiye'nin NATO'ya dâhil olması

Türkiye Cumhuriyeti'nin politik ve askeri yetkilileri ülkenin NATO sistemine dâhil olmasını o dönemdeki tehdit algısı ve beka tedbirleri bakış açısıyla değerlendirmişlerdir. Farklı bir bakış açısı da, NATO'ya üye olmanın Türk demokrasisi ve siyasal hayatı için bir gereklilik olduğu yönünde olmuştur. Bu düşüncenin temeli, Türk devletinin küresel gelişmelere açık olmasının sağlanması, siyasi ilerlemenin önünün açılması, küresel ekonomik sistemden ayrı kalınmaması gerektiğine olan inançtır. Dolayısıyla Batının oluşturduğu askeri, politik ve ekonomik alanlardaki her türlü uluslararası ittifaklara katılmanın gelişmiş bir Türkiye için atılması gereken önemli bir adım olarak görülmüştür. Bu görüşler her ne kadar ülkedeki tüm insanların ortak düşüncesi olmasa da, medya ve siyasi destekle toplumun müşterek bir isteğiymiş gibi lanse edilmiştir (Şenyuva ve Üstün, 2013: 14).

1949 yılında oluşturulan NATO'ya Türkiye'nin davet edilmemesi dönemin hükümeti üzerinde olumsuz bir hava oluşturmuştu. Askeri kanat kendi yaptığı değerlendirmeler ve tehdit algısı sonucu Türkiye'nin NATO'ya üyeliğinin mutlaka olması gerektiğini düşünüyordu. Sovyetler Birliğinin uyguladığı yayılmacı politika ve oluşturduğu askeri tehdit halk ve kamuoyu nazarında derin bir tedirginlik yaratmaktaydı.

ABD'nin her ülkede kendilerine bağlı güçlerin iktidara getirilmesini desteklediği görüşünün kararnamelere, konsept belgelerine yazıldığı bu dönemde Türkiye seçimlere gidiyordu. Mayıs 1950'de gerçekleşen seçimlerde Menderes'in iktidara gelmesiyle Tür-

kiye'nin "komünizme karşı bir doğal kale" haline getirilme çabaları da yoğunlaştı (Hiçyılmaz,2004: 42). Sovyetler Birliğinin Türkiye'ye karşı tehdit ve istekleri ise her geçen gün artarak devam ediyordu, özellikle Sovyetler Birliği Türkiye'nin bu endişelerini artıran girişimlerde bulunup, Boğazlar sorununu bir kez daha alevlendirmeye çalışıyordu (Sander,1979: 64). Montreux'den beri Rusya boğazların kontrolünü ele geçirmek ve Karadeniz'e kıyısı olan devletleri egemenliği altına almak istemişti. Bu stratejisini, savaş sonrası yanına Yugoslavya'yı, Sosyalist bloka geçen Romanya ve Bulgaristan'ı da alarak devam etmek istemişti (Başyurt,1998: 68). Yaşanan tüm bu gelişmeler Türkiye'nin hem güvenlik kaygısını derinleştiriyor hem de Türkiye'yi Batı Bloğuna yakınlaştırıyordu.

Kore'de gerçekleşen güç mücadelesiyle Sovyetler Birliği etkisindeki komünizm yayılmacılığı en üst seviyesine çıkmış ve resmi bir savaşla tescillenmişti. Bu savaş neticesinde Avrupa'da Sovyetler Birliğine karşı duyulan endişe kat ve kat artmıştı.

İkinci Dünya Savaşı sonrasında, 1945-1953 yılları arasındaki dönem, Türkiye ve SSCB ilişkileri açısından sıkıntılı geçmiştir. O dönemde bir sinir harbi olarak tırmanan gerilim, Sovyetlerin Boğazlar rejimine yönelik iddiaları ve Doğu Anadolu illeri üzerinde(Ermenistan ve Gürcistan'a verilmek üzere) toprak talepleri ile tırmanmıştır. Türkiye, Soğuk Savaş açısından bir test alanı olmuş, yürütülen yoğun diplomasi de ABD'nin Truman Doktrini ile sınırlandırma politikasının gelişimine itici güç oluşturmuştur. Stalin döneminden sonra iki blok arasında uluslararası ilişkilerde genelde yaşanan yumuşama döneminin etkileri, NATO üyesi olan Türkiye ile SSCB arasındaki ilişkilerde de görülmüştür. Türkiye ve SSCB arasında ilişkiler 1960'lı yıllarda normale dönmeye başlamıştır (Hasanlı, 2012; 53).

Kore savaşında, Türkiye de kendini Batı ittifakı içine kabul ettirmek için çok daha fazla fedakârlıkta bulunmuştu. Türkler Kore'de gereğinden fazla sayıda kayıp vererek NATO üyeliğini garantilemişti. Türk birlikleri uzunca bir süre Kore'de kalarak yabancı askeri güçlerle çarpışmak zorunda kalmıştı. Türkiye, ABD'den gelen yardım çağrısına zaman kaybetmeden karşılık vermişti. Büyük bir Türk kuvvetini yollayarak Batı ittifakının içinde olduğunu kanıtlamış, sadakatini göstermiş ve bunu ispatlamıştır. Türkiye gelen baskılara aldırış etmeyerek; savaşa katılmakla kendi kaderini Amerika karşısında belirleyerek Amerikalıları sıkıntıdan kurtarmak istemiştir. ABD ise ihtiyaç duyduğu üsleri kullanmak ve Sovyetler Birliği'ni denetim altına almak istediğinden Türkiye'nin katılımını istemiştir (Ataöv,1970: 108).

ABD'li diplomatlar Türkiye'nin sistem içerisine dâhil edilerek müttefik yapılmasının iki taraf açısından da yararları olacağını belirtmişlerdir. SSCB'nin domine ettiği komünizm akımından korunmak ve olası askeri müdahale ihtimaline karşı destek sağlamak Türkiye'nin, Ortadoğu coğrafyası konusunda SSCB'nin elini zorlaştırarak bu bölgeye yakınlaşmak ve Türkiye'yi kendi ittifakları içinde tutmak ise NATO'nun elde edeceği kazançlar olacağını söylemişlerdir (Gözen, E.T: 20.01.2018).

Sonuçta yaşanan bu gelişmelerle Türkiye'nin İttifak'a girmesine ve alınmasına oybirliği ile karar verilmiş, iki ülke üyelik için davet edilmiştir. Böylece kuzey bölgesinin güvenliği için teminat sağlanırken; Türkiye'nin de uluslararası alanda güvenliği sağlanmıştır. Türkiye ve Yunanistan'ın NATO üyeliği böylece 2 Şubat 1952'de uzun bir maratonun ardından 73'e karşı 2 red oyuyla onaylanmıştır (Sander,1979: 80).

2.4.4. Küba füze krizi

1959'da Küba'da iktidara geçen Fidel Castro, SSCB ile sıkı işbirliği faaliyetlerine başlamıştır. Yaşanan gelişmeler sonrası Castro yönetimindeki Küba'da komünizmin etkisi artarak devam etmiştir. İşbirliği çalışmaları başlamış, Küba askeri birlikleri SSCB menşeli silahlarla donatılmıştır. Sonrasında SSCB, Küba'ya ABD tarafından yapılacak muhtemel bir askeri harekât neticesinde balistik silahların ve füze sistemlerinin de içinde olacağı askeri yardımın yapılacağını deklare etmiştir (Angın, 1967'den aktaran Bilgili, 2008: 44).

ABD kendi ülkesine bu kadar yakın ve komünizm etkisindeki bir yapı düşüncesine alışmaya çalışırken, Küba SSCB ile sıkı müttefiklik ilişkileri içerisindeydi. Hatta Küba kendisi için silah sevkiyatı konularında antlaşmalar da yapmıştır. Yaşanan gelişmeler sonucunda ABD Başkanı iki ülkeyi de silahlanma konusunda uyardı. Ayrıca Küba'nın antlaşma kapsamındaki füze sistemlerini SSCB'ye ivedi şekilde iade etmesini talep etti. Bunun karşılığında SSCB ülkesini tehdit eden ABD tarafından Türkiye'de kurulmuş olan balistik füze sistemlerinin kaldırılması gerektiğini belirtti. İki taraf ülkelerince gerçekleştirilen karşılıklı görüşmeler neticesinde bu mesele halledilmiştir. Füze krizi meselesi, ABD ve SSCB arasında yaşanan güç mücadelesinin zirve yaptığı yıllarda yaşanmıştır. Dehşet dengesinin içinde yaşanan bu kriz iki ülkeye de daha dikkatli olmaları konusunda somut bir örnek olmuştur. Çünkü iki ülke de bu sorun neticesinde nükleer bir yıkımın kapısından dönmüşlerdir (Angın, 1967'den aktaran Bilgili, 2008: 45).

2.4.5. U–2 uçağı krizi

Sovyetlerin Washington'la ilişkileri İncirlikten kalkan ABD keşif uçağının Rus devletinin toprakları içerisinde düşürülmesiyle birlikte iyice kötüleşmiştir. Amerika öncelikle söz konusu keşif uçağının silahsız olduğunu belirtmiştir. ABD hükümeti ilk olarak U2'nin silahsız bir uçak olduğunu beyan etti. Ancak Kruşçev ele geçirilen savaş pilotunu tüm ülkelerin görmesini sağlamış ve keşif uçağının silahlı şekilde görev yapıyor olduğu açıklamasını yapmaya zorlamıştır. Dahası Kruşçev, ABD'nin SSCB' ye karşı saldırgan ve düşmanca davrandığını itiraf etmesini, yapılan olay için de SSCB'ye özür dileyerek sorumluların cezalandırılmasını talep etmiştir. Kruşçev'in amacı ABD'yi köseye sıkıştırmaktı fakat yaptığı bu davranış sıkıntılı olan bir süreci çözmekten çok kopmaya yakın bir noktaya getirmiştir (Bilgili, 2008: 44).

NATO kurulduğu yıldan itibaren sürekli olarak SSCB ve Varşova Paktı ile bir güç mücadelesi içinde olmuştur. Kuruluş yıllarında oluşan güvenlik algısının temelini simetrik olan ve yoğunluğu giderek artan askeri tehditler oluşturmuştur. Yayılma ve silahlanma yarışının oluşturduğu bu tehditlere karşı, her geçen gün gelişen teknoloji ışığındaki güvenlik tedbirleri ile karşı koyulmaya çalışılmıştır. NATO'nun ve SSCB'nin güvenlik algıları ve stratejileri de bu simetrik tehditler neticesinde şekillenmiştir. Fakat gelişen teknoloji tehdit şeklini asimetrik bir hale getirmiştir. Dolayısıyla NATO'nun güvenlik algısı ve stratejileri sürekli olarak kendisini yenilemiştir.

2.5. NATO'nun Temel Stratejileri İle Sürece Dâhil Olması

2.5.1. NATO'nun Soğuk Savaş döneminde uyguladığı stratejiler

2.5.1.1. Topyekûn karşılık stratejisi

İkinci Dünya Savaşı'nın ardından NATO, tehdit algısı değişen uluslararası ortamda güvenlik planlarını güncellemiş ve farklı savunma perspektifleri geliştirmiştir. Bu stratejik gelişmelerin başında temelini konvansiyonel ve nükleer silah sistemlerinin oluşturduğu, rakip ülkeler tarafından algılanacak caydırıcı etkisi çok fazla olan Topyekûn Karşılık Stratejisi yer almaktadır (Peksarı, 2007: 34). NATO ilk zamanlarda, SSCB'ye karşı Avrupa'daki güç mücadelesinde geri planda kalmıştır. Bunun sebebi Avrupa ülkelerinin yeni bir yıkımdan çıkmaları, ABD'nin askeri gücünün büyük bir kısmının kendi ülkesinde ve söz konusu bölgeye uzak olması, SSCB'nin ise bölgeye yakınlığı olmuştur. Bu sebeple NATO aradaki farkı kapatmanın yolunu nükleer silah sistemlerinin gücünde bulmuştur (Özgöker, 2006: 115). Bu stratejinin amacı; olası bir

Sovyet tehdidi neticesinde, NATO üyelerinin ve onların askeri birliklerinin tehlike altında kalması halinde Sovyet harekâtının başlangıç zamanından mevcut zamana kadar caydırıcılık düşüncesi altında hareket ederek ve her türlü silah sistemlerini tam bir kararlılık içerisinde ivedi şekilde kullanarak yapılan saldırının tamamıyla bertaraf edilmesinin sağlanmasıdır. Bunun yanı sıra bu stratejide saldırgan ülkenin 2 farklı şekilde hareket edeceği öngörülmektedir. Birincisi, geniş kapsamlı bir askeri harekât ya da topyekûn taarruz, ikincisi ise gizli asimetrik savaş yöntemleri ya da küçük boyutlu taktik müdahale teknikleridir (Bilbilik, 2008: 26).

Amerika'nın Japonya'nın iki şehrinde kullandığı nükleer silahtan sonra SSCB de bu konuda başarılı bir test gerçekleştirmiştir. Nükleer silah sistemlerinin uluslararası alanda kullanılmaya başlamasıyla birlikte güvenlik anlamında köklü değişiklikler yaşanmaya başlamış ve ülkelerin tehdit algısı büyük değişimlere uğramıştır. Bu yeni silah sistemi aynı zamanda ülkelerin güvenlik konusundaki genel stratejik bakış açılarını da etkilemiş ve nükleer silahlanma yarışını hızlandırmıştır (Peksarı, 2007: 34).

Bu stratejik görüş neticesinde nükleer silahı olmayan ülkeler güvenliklerinin tehdit altında olduğunu düşünmeye başlamışlardır. Ayrıca yaşanabilecek büyük çaplı bir nükleer savaş insan ırkını yok olmanın eşiğine götürme ihtimali de taşımaktadır. Fakat bahse konu dönemde caydırıcı etkisi sebebiyle hem SSCB'nin hem de ABD ile birlikte NATO ülkelerinin güvenlik konusundaki temel yapı taşı olmuştur (Sander, 1979: 302).

2.5.1.2. Esnek karşılık stratejisi

SSCB'nin nükleer silah kabiliyetinin giderek yükselmesi, ülkelerin elindeki nükleer silahların gezegenin topluca imhasını defalarca kez gerçekleştirebilecek seviyeye ulaşması ve bu silah sistemlerinin yetkisinin bazı ülkelerde sadece ülkenin liderinin elinde olması Topyekûn Karşılık Stratejisinive onun tesis ettiği barış ve güvenlik ortamını sorgulanabilir hale getirmiştir. Sonuçta uluslararası sistem yeni bir güvenlik stratejisine ihtiyaç duymuştur (Çomak, 2005: 19). Topyekûn karşılık stratejisini sert ve aşırı tedbirli yapısı geliştirilerek, aklı ve yumuşak gücü ortaya çıkaran yeni bir müdahale stratejisi yaratmak için çalışılmıştır. Bunda asıl amaç topyekûn karşılık stratejisinin yıkıcı etkilerinden kaçınmaktır.

Stratejinin amacı, olası bir SSCB saldırısının kapsam ve nitelikleri değerlendirilerek benzer kapsamda icra edilecek bir harekât ile karşılık vermeyi önermektedir. Buradaki kritik nokta topyekûn bir savaşa başlamaktan ziyade benzer bir tepki ile yapılan

saldırıya karşılık vermektir. Bu kapsamda hasım ülkenin ya topyekûn bir saldırganlık içerisinde olacağı ya da taktik seviyede kalan kısmi bir saldırganlık halinde olabileceği düşünülmüştür. Bu stratejide nükleer silahlar kullanılacak en son silah konumundayken, Topyekûn Karşılık Stratejisinde duruma göre ilk kullanılacak silahlar içerisindedir (Bilbilik, 2008: 26).

Esnek Karşılık Stratejisi kapsamında NATO üyelerinin karşılaşacakları saldırılarda aşamalı bir şekilde karşı harekât icra edilecekti. Dolayısıyla SSCB'nin yapacağı bir fiili bir harekette aşamalı olarak silah kullanımı sağlanacaktı. Öncelikli olarak klasik silahlar kullanılacak, daha sonra tehdit durumuna göre konvansiyonel ve nükleer silah sistemleri icra edilecek operasyonlara dâhil edilecekti (Çalış, Akgün ve Kutlu, 2006: 183).

Bu stratejiye geçişin en önemli sebebi Amerika ile Sovyetlerin elinde bulunan nükleer silahlar ve kıtalararası füzeler olmuştur. Avrupa ülkelerinin Sovyetler Birliği'ne göre konvansiyonel silahlar bakımından seviyesinin çok düşük olduğu görülmüştür. Nükleer silahlar açısından kıyaslama ise neredeyse imkânsızdır. Aşırı derecede yapılan nükleer silahlanma yarışı ABD ve SSCB'yi dehşet dengesi noktasına kadar getirmiştir. İki ülkenin elinde bulunan nükleer silah stoğu tüm dünyayı defalarca kez yok etmeye yetecek seviyedeydi. İşte bu sebeplerden ötürü esnek karşılık stratejisine geçiş dünya güvenliği bakımından zaruri bir ihtiyaçtı.

2.5.1.3. Esnek karşılık ve ileri savunma stratejisi

Doğu Bloğu ile Batı Bloğu'nun güç odaklı mücadelesi uluslararası sistemin en önemli soru nu haline gelmişti. Öyle ki, NATO'nun savunma maksatlı olarak Avrupa'daki üye ülke topraklarına füze sistemlerini kurmasını müteakiben SSCB de yakın bölgelere kendi füze sistemlerini kurmuştur. Yaşanan bu silahlanma durumu bölgedeki güvenlik sorununu derinleştirmiştir (Uzgel, 2005: 306).

Aynı zamanda, Orta Doğu bölgesinde gerçekleşen krizlerden sonra (İran'daki devrim, İran-Irak savaşı) hammadde kaynaklarının ekonomik değerlerinin artması da büyük ülkelerin enerji maliyetlerinin aynı oranda artmasına sebep olmuştur. Petrol ihtiyacını bu bölgeden sağlayan Avrupalı devletler güvenliklerini sağlamak için en temel gereksinimleri olan enerji ihtiyacını temin etmekte çok zorlanmışlardır. Sonuç olarak Avrupalı devletlerin fark ettiği nokta; ülkelerinin güvenlikleri için sadece güçlü bir orduya sahip olmaları ve caydırıcı silah sistemlerini ellerinde bulundurmalarının yetmedi-

ği, aynı zamanda hammadde kaynaklarının bulunduğu coğrafyanın da güvenliğinin tesis edilmesi gerektiğidir (Peksarı, 2007: 45-46).

Bu stratejinin ana amacı çatışmayı ve anlaşmazlıkları üye ülkelerden uzak tutmaktı. Yani fiziki olarak üye ülkelerin sınırlarına gelmeden çatışmaları orada tutmak ya da sonlandırmaktı. Buradaki ana sebeplerden biri değişen nüfus yapısı, şehirlerde yaşayan insanların sosyo-kültürel yapıları, devletlerin değişen tehdit algısıydı. Diğeri ise mevcut konvansiyonel silahların gelişen teknoloji neticesinde etki alanının tahmin edilenden çok artmasıydı. Eski teknolojiye nazaran, yeni teknoloji ile üretilen bir balistik füze bile büyük bir şehri yerle bir etmeye yeterliydi.

Stratejinin en önemli hedefi; yaşanacak gerilimi ve harp ortamını üye ülkelerden ve stratejik öneme sahip olan coğrafyalardan olabildiğince uzaklaştırmaktı (Sander, 1979: 304).

2.5.2. Soğuk savaş sonrası 1999 yılına kadar uygulanan stratejik konseptler

Soğuk Savaş döneminde NATO'nun kurulduğu yıldan beri tüm stratejilerini belirleyen en önemli etken bir denge unsuru ve karşı gücün bulunmasıydı. SSCB'nin dağılmasıyla birlikte NATO'nun karşısında kendine denk, mücadele edebileceği, yarışıp gücünü kıyaslayabileceği bir unsur kalmadı. SSCB'den ayrılan devletlerin çoğunun elinde nükleer silah mevzi ve depoları bulunmaktaydı. Her ülkenin doğal olarak kendine has bir lideri, yönetim anlayışı ve tehdit algısı vardı. Bu zamana kadar NATO tüm tehdit algısını ve askeri yapılanmasını doğal olarak SSCB'ye karşı planlamıştı. SSCB'nin dağılması ve bahsedilen uluslararası ortamın oluşmasıyla birlikte NATO kendisini ve oluşturduğu stratejileri yeniden gözden geçirmek zorundaydı. Bu durum NATO'yu oluşan tehdit algılarına göre yeni bir strateji üretmeye zorladı.

Soğuk Savaş'ın bitmesiyle birlikte NATO'yu domine eden ABD'nin güvenlik konusundaki stratejileri uluslararası sisteme yön vermiştir. Uluslararası sistemdeki en büyük güç olan ABD hegemon devlet olma yolunda ilerlemiş ve güvenlik sistemini kendi menfaatleri doğrultusunda etkilemiştir. Karşısında kendisi kadar etkili bir rakip bulamayan ABD'nin uluslararası sistemden istekleri ve ülkeler üzerindeki nüfuzu her geçen gün artmıştır. Doğal bir sonuç olarak NATO'da bu durumdan etkilenmiş ve tamamıyla ABD güdümünde hareket eden bir organizasyon konumunda olduğu fark edilmiştir. ABD, kendi hedeflerini düşünerek planladığı senaryolarla NATO'yu gelişmeye ve büyümeye zorlamış, hatta NATO için farklı görevler tasarlamıştır (Kuloğlu,2009: 10).

NATO ülkeleri İngiltere'nin Londra şehrinde 1990 yılında yaptıkları toplantıda kendi ülkelerinde ve diğer Avrupalı ülkelerde yaşanan gelişmeleri konu alarak örgütün sistemiyle ilgili değerlendirmeler yapmışlardır. Toplantı sonucunda SSCB dayatmasıyla WP'ye geçmiş Avrupa ülkelerinin NATO'nun güvenliği için bir sorun teşkil etmediği belirtilmiştir. Bununla birlikte bu ülkelerin yapılacak görüşmelerle sisteme kazandırılmasının gerektiğine değinilmiş, hatta NATO'ya üyelik için ikna edilmelerinin de faydalı olacağı değerlendirilmiştir. NATO'nun bu yeni genişleme eksenindeki stratejisi ABD'nin güdümünde belirlenmiştir (Akgül, 2008: 4-2, 4-3).

Soğuk Savaş'ın bitmesiyle birlikte uluslararası güvenlik konsepti de değişmiştir. İki kutuplu sistem sona ermiş ve ABD hegemonyasında oluşan yeni bir yapı ön plana çıkmıştır. ABD ile birlikte NATO ülkeleri de oluşan yeni sistemde askeri gücün tek başına bir şey ifade etmeyeceğinin, bununla birlikte mutlaka ekonominin işin içinde olduğu, güçlü ve istikrarlı siyasal durumun sağlandığı, sosyo-kültürel etkenlerle desteklenen ve coğrafyanın ön plana çıktığı güncellenmiş ve düzgün şekilde çalışan güçlü bir stratejik planın yapılması gerektiğini fark etmişler ve bu doğrultuda gerekli adımları atmışlardır (Çalış, Akgün ve Kutlu, 2006: 183).

Soğuk Savaş'ın sona ermesiyle birlikte NATO'nun tehdit ve düşman algısı da değişime uğramıştır. Eski stratejide düşman SSCB ve WP olarak rahatlıkla tanımlanabilirken, SSCB'nin dağılmasıyla birlikte düşman olarak algılanan unsurlar ortadan kalkmıştır. Uluslararası sistemin genel güvenliğini tehdit eden unsurların tamamına karşı bir hassasiyet geliştirilmiştir. Özellikle WP'nin eski üyelerinin NATO bünyesine alınmasının düşünüldüğü bu dönemde güvenliğe yönelik risklerin ve tehditlerin bu şekilde azaltılabileceği de planlanmıştır. Geçmiş zamanlarda rakip devletlerin müzakere ve cazibe ile müttefik hale getirilmesi düşünülmüştür. Bununla birlikte yeni stratejik bakış açısı, silahlanma yarışının kontrol altına alınması, barışı tehdit eden unsurların engellenmesi ve diğer barışı destekleme görevlerinin yerine getirilmesini ilgi alanına almıştır (Wittmann, 2009: 14-15).

Bu aşamadan sonra İtalya'nın Roma şehrinde 1991 yılında yapılan toplantıdakararlaştırılan ortak stratejide NATO için önemli ilgi alanları oluşturulmuştur. NATO;

1. Avrupa ülkelerinin gelişmesinin ve modernleşmesinin teminini sağlamalı,
2. Üyelerinin her türlü güvenlik ihtiyacını karşılayarak NATO'ya olan güvenin devamlılığını temin etmeli,

3. Yapacağı güvenlik çalışmaları ile sadece üye ülkeler için değil uluslararası sistem için de NATO'nun çok önemli bir aktör olduğunu her platformda göstermeli,
4. Kendisini her koşula uyum sağlayabilecek bir yapıya dönüştürmeli ve modern silah sistemleri ile caydırıcı etkisini sürdürmeli,
5. Avrupa ülkeleri arasındaki ahengin kontrolünü ve devamlılığını sağlamalıdır (Davutoğlu, 2009: 230).

Yugoslavya'nın ortadan kalkması ve Avrupa kıtasında yaşanan aşırı milliyetçilik dalgasının yarattığı kriz neticesinde ABD'nin Washington şehrinde 1999 senesinde yapılan toplantıda NATO bazı kritik kararlar almıştır. Bu toplantıya temel teşkil eden sebepler arasında SSCB'nin dağılma sürecine yakınlaşması ve aşırı milliyetçilik hareketlerinin yarattığı krizler olmuştur. Bu toplantıda alınan kararların hayata geçirilmesiyle birlikte stratejik anlamda büyük gelişmeler yaşanmıştır. SSCB resmen dağılmış ve tarih sahnesinden silinmiştir. Balkan coğrafyasında yaşanan krizin çözümü için bölgeye askeri müdahale gerçekleştirilmiştir. Fakat bu operasyon taktik bir operasyon olarak görülse de gerçek manada güvenliği sağlama ve barış ortamını devam ettirmek için gerçekleştirilmiştir. NATO üye sayısını Doğu Avrupa ülkeleri ile arttırmıştır. Çek Cumhuriyeti, Polonya, Macaristan'ın NATO'ya üyelik işlemleri gerçekleştirilmiştir. Ayrıca Avrupa'nın genel güvenliği için stratejik kimlik oluşturma çalışmaları da yapılmıştır. Açıklanan ve icra edilen bu strateji NATO için bir görev tanım formu haline gelmiştir. Kısaca NATO'nun misyonunu özetleyen ve ilgi alanlarını deklare eden bir strateji olmuştur. NATO'nun yeni misyonu; güvenliğin sağlanması maksadıyla tavsiye vermek, yapısında bulunan savunma sistemleriyle caydırıcı güç oluşturmak, oluşacak kaosların giderilmesi için çalışmalar yapmak, üye ülkelerle sıkı bir ittifaklık anlayışı oluşturmaktır (Wittmann, 2009: 15).

2.5.3. Yeni stratejiler bağlamında NATO'nun devletler ve uluslararası örgütler ile ilişkileri

2.5.3.1. NATO ile Avrupa Birliği İlişkisi

Avrupa Birliği (AB) kurulduğu yıldan itibaren Avrupa Güvenlik ve İşbirliği Teşkilatını (AGİT) aktif halde tutmak istemiş, ortaya çıkan anlaşmazlıkları, politik krizleri ve askeri nitelikli çatışmaları bir nevi kendi çatısı altında çözümlemeyi hedeflemiştir. AB ülkelerinin yaptıkları toplantılar ve almış oldukları yaptırım kararlarına rağmen

önemli krizlerin üstesinden, ABD'nin ve özellikle NATO'nun katkısı olmadan gelememişlerdir. Bunun en bariz örnekleri Bosna-Hersek ve Kosova'da meydana gelen askeri nitelikli krizlerdir. AB bu iki krizden de edindiği tecrübe ile Avrupa'nın güvenliği konusunda NATO'ya şimdilik mahkûm olduğunu anlamıştır.

Bu süreçte, 1997–1998 yıllarında Fransa'nın NATO'nun askeri kanadına dönme eğiliminden vazgeçmesi; İngiltere'de iktidara gelen İşçi Partisi hükümetinin muhafazakârların aksine, Avrupa merkezli bir politikaya kayması ve BAB'ın etkin bir şekilde çalıştırılamaması etkili olmuştur. Bu amaçla 2 Ekim 1997'de imzalanan Amsterdam Antlaşmasıyla; "AB'nin küresel boyuttaki sorunlara etkili reaksiyon göstermesi" hedefi konulmuş, Avrupa liderlerinin, işbirliği çerçevesinde fikir birliğini sağlayarak stratejik ortaklığa uygun davranmaları gerektiği belirtilmiştir. Bu antlaşmayla, AB ülkelerinin birlikte hareket etmeleri sağlanırsa hem birliğin hedeflerine ulaşılmış olunacak hem de marjinal fayda sağlanacaktır. Bu antlaşmayı, 1998'de yapılan İngiliz-Fransız zirvesinde, Avrupa Birliği'nin NATO haricinde de stratejik konumda olması düşüncesi bağlamında Avrupa Güvenlik Savunma Politikası oluşturulmasına yönelik girişimler izlemiştir (Bilgili, 2008: 87).

AB'nin Helsinki'de gerçekleştirdiği toplantıda müttefik devletlerin herhangi bir kriz anında kullanılabilecek askeri bir birlik oluşturulması kararlaştırılmıştır. Taktik operasyonlarda da kullanılabilecek olan bu birliğin 50.000 mevcuda sahip olması, tam teçhizatlı ve göreve hazır şekilde bulundurulması kararlaştırılmıştır (http-6,4……, E.T: 31.01.2018).

2000 yılında gerçekleştirilen zirvede AB, BAB'da olduğu gibi somut bazı katılım mekanizmaları öngörmek yerine, ilgili 15 ülkeyle temelde yürütülecek bir ilişkiler manzumesi metni ortaya koymuştur. Bu çerçevede, AB'nin, NATO imkân ve yeteneklerinin veya müttefiklerin ulusal kuvvetlerinin kullanılacağı AB harekâtları için bile, sadece istişare nitelikte düzenlemeler yarattığı görülmüştür. Keza AB Nice Zirvesinde de; güvenlik ve savunma alanında öngördüğü yapılanmanın gerçekleştirilmesi kararlaştırılmış, BAB lağvedilmiş ve AB'nin sevk ve yönetiminde yürütülecek harekâtlar için örgütün birliklerine, stratejik veya taktik seviyedeki operasyonel kabiliyetlerine ve askeri planlama yeteneklerine "garantili ulaşım" (guaranteed access) konusu gündeme alınmış ve katılım bağlamındaki istişari düzenlemelerin ayrıntıları karara bağlanmıştır (Bilgili, 2008: 88).

Yapılan toplantıların sonrasında göze çarpan en önemli konu, eskiden NATO'nun Avrupa'ya bakış açısında hüviyet kavramı ön plana çıkarken yani AGSK'dan bahsedilirken, bu aşamada politik kavramlar ön plana çıkarak AGSP'den konuşulmaya başlanmıştır. Bu bakış açısı da ilerleyen yıllar içinde güvenlik stratejilerinin kapsamlı bir şekilde ele alınarak özelden genele doğru kayacağını göstermiştir (Çayhan, 2002: 49).

Avrupa Birliği'nin geleceğe yönelik en önemli güvenlik projelerinden biri olan AGSP hassas noktalar ihtiva etmektedir. Dünya'nın her noktasında askeri güvenlik tedbirleri ince ayrıntılarla planlanması gereken çok önemli konulardır. Coğrafi bölgelere ve stratejik hedeflere göre doğal olarak farklılık gösterebilecek bu güvenlik tedbirleri; geçmişi, yaşanan acı tecrübeleri, savaşlar ve yoğun bir rekabetin yaşandığı Avrupa coğrafyasında AB için hayati bir öneme sahiptir.

AB güvenlik sorunları ve işbirliği için NATO'yu her zaman yanında görmek istemekte fakat konu AB'nin iç meselesi olduğunda ise NATO'yu ve özelikle ABD'yi kapı dışında tutmaktadır. NATO ise kurumsal olarak baktığında çoğu meselede AB ülkelerini haklı görmektedir. ABD açısından NATO gözüyle bakıldığında ise meydana gelen tüm anlaşmazlık ve krizlerin ABD'nin dâhil olmasıyla ve NATO şemsiyesi altında çözülmesi gerektiği düşünülmektedir.

AB için bir başka sıkıntı yaratan husus ise AB coğrafyası içinde bulunan NATO askeri üsleri ve bu üslerin içinde konuşlanmış olan ABD askerlerinin mevcudiyetidir. AB, NATO üslerinde bulunan ABD asker sayılarının bazı noktalarda gereksiz olarak fazla olduğunu düşünmektedir. ABD ise her ne kadar NATO şemsiyesi altında askeri personelini AB coğrafyasına konuşlandırmış olsa da asıl maksat ve hedefi Rusya'nın önüne NATO'yu kullanarak askeri bir hat çekmek istemesidir.

Rusya NATO'nun üs bölgelerini, kendi coğrafyasına yakın bölgelerde NATO'nun konuşlandırmış olduğu füze bataryaları ve konvansiyonel silahları doğal olarak kendisine birinci dereceden asli tehdit unsuru olarak görmekte ve bu konuyu ele geçirdiği her fırsatta duyurmaktadır.

Rusya'nın bu tutumu karşısında ABD hedefini kısmen gerçekleştirmiş olsa da esas sıkıntı ve diplomatik krizleri AB ve AB ülkeleri yaşamaktadır. Karasal olarak AB ülkelerinin Rusya ile olan sınırı geçmişte olduğu gibi gelecekte de her türlü sıkıntılara, askeri operasyonlara ve politik krizlere sebep teşkil edebilir.

2.5.3.2. NATO ile Rusya ilişkisi

SSCB'nin dağılması ve Soğuk Savaşın bitmesiyle birlikte NATO için en büyük tehdit ve düşman ortadan kalmıştır. Bu olaydan sonra NATO kendisini ister istemez bazı tartışmaların içinde bulmuştur. Bu tartışmaların ana konusu NATO'nun misyonu, stratejisi ve oluşacak yeni tehdit algısı olmuştur.

Bununla birlikte Soğuk Savaş'ın sona ermesi sonucunda yaşanan hadiseler, meydana gelen krizler ve kaos ortamı uluslararası güvenlik sistemi için güçlü bir aktöre ihtiyaç duyulduğunu göstermiştir. NATO bu noktada güvenlik bağlamında öne çıkan en önemli örgüt olmuştur. Sonuçta Balkan coğrafyasında yaşanan etnik ve din temelli savaşlar, ortaya çıkan yeni devletlerin toprak paylaşım sorunları, özellikle Balkanlarda Yugoslavya'nın dağılması sürecinde soykırıma varan çatışmalar, SSCB'den ayrılmanın sonucunda eski üye ülkelerin politikalarındaki bilinmezlik, güçlü ve barışı tesis edebilecek bir unsurun eksikliğini göstermiştir (Kuloğlu, 2001: 586).

NATO bu aşamadaki temel stratejisini Roma'da yapılan toplantıda belirlemiştir. NATO yapılan bu toplantıda güvenlik durumunun değiştiğini kabul etmiş, gelişen yeni tehditler karşısında tavrını değiştirmiş ve yeni bir stratejik plan benimsediğini açıklamıştır. NATO ilan ettiği bu 'Yeni Stratejik Konsept'te ittifak anlayışıyla birlikte büyük çaplı güvenlik perspektifi ile hareket edeceğini belirtmiştir. Kuruluş yıllarındaki tehditlerin en önemlisi olan SSCB'nin ortadan kalktığı kabul edilmiş, uluslararası sistemde ortaya çıkan terör tehdidinin önemine vurgu yapılmış ve bazı hammadde kaynaklarına sahip coğrafyalardan gelebilecek tehditleri önceden engellemenin gerekli olduğunu ayrıca enerji ihtiyacının devamlılığını sağlamak için bu bölgelerin güvenliğinin kontrol altında tutulması gerektiğini savunmuştur. Bu stratejik mücadelede sadece askeri birliklerin kullanılmayacağını, bununla birlikte politik baskı unsurlarının ve ekonomik imkânların da seferber edileceği konusunda anlaşma sağlanmıştır. Ayrıca NATO askeri birliklerinin süratli, güçlü, mobilize olması ve en ileri silah sistemleriyle donatılmasının gerektiği üye ülkelerle karara bağlanmıştır. Belki de açıklanan en önemli konu gerektiğinde NATO birliklerinin konsept haricindeki konularda ve yerlerde de faaliyette bulunabileceği açıklanmıştır (Özkan, 2010: 114).

SSCB'nin dağılmasından itibaren NATO açıkça belirtmek istemese de Rusya ve Rusya'ya yakın devletlere karşı ilgisi ve tehdit algılaması devam etmiştir. Bu tehdit algılaması neticesinde Rusya'ya yakın ülkelere temas etmek istemiştir.

Geniş kapsamlı bir güvenlik anlayışı tesis etmek isteyen NATO, önceki dönemde düşman konumunda olan ülkelerle, başta Avrupalı ülkelerle ve ilgi alanındaki coğrafyalarda bulunan ülkelerle birtakım diplomatik temaslar kurarak ilişkileri düzeltmenin farklı yollarını aramıştır. İcra ettiği bu faaliyetlerin ilk meyvesi Kuzey Atlantik İşbirliği Konseyi (KAİK)'in hayata geçirilmesi olmuştur.

KAİK'in yaptığı toplantılar genel olarak ilişkilerin geliştirilmesi ve diyalog ortamının kurulması için düzenlenmiştir. Bu kapsamda NATO, direkt olarak temasta bulunmadan Avrupa'daki güvenlik sistemini sağlamlaştıracak ve denetimini sağlayacak kuruluşlar oluşturmaya çalışmıştır. Bu organizasyonun ana hedefi kalıcı bir güvenlik ortamının oluşturulması, silahlanma yarışının durdurulması, demokratik kurumların işler halde tutulması, teknolojinin sadece askeri konularda değil insani konularda da çalışmasının sağlanması, ordu mevcudunun belli bir seviyenin altında tutulması, diplomatik ilişkilerin iyileştirilmesi, vb. birçok konuda diyalog kurmak aynı zamanda müşterek faaliyetler icra etmek olmuştur (http-2,1 ……, E.T: 30.01.2018).

Soğuk Savaşın sonrasında icra edilen KAİK görüşmeleri genel olarak bireysel nitelikli değil tüm ülkeleri ilgilendiren politikalar üzerine odaklandı. Örneğin Rus askeri birliklerinin Baltık ülkelerinden çekilmesini sağlamıştır. Yapılan bu diyalog ve girişimlerin daha başarılı sonuçlar getirmesi için NATO'nun her ülke ile ayrı ayrı bireysel işbirliği ilişkileri geliştirmesi yönünde sağlam ve olumlu bir adım atılmamıştır. NATO'nun bu adımı atmasını sağlayan gelişme 1994 yılında kurulan Barış İçin Ortaklık (BİO) çalışmalarının başlatılmasıdır. Çalışmanın amacı, NATO ile çalışma dâhilindeki devletlerin koordineli şekilde faaliyetler icra etmesiydi.

Barış için Ortaklık'ın asıl hedefi, NATO'nun program dâhilindeki tüm ülkelerle samimi ve direkt olarak bağlantılı olmasının sağlanmasıdır. Önemli olan şey aktif halde tutulan diyaloglar sayesinde uyum halinde çalışmak ve çıkabilecek her türlü tehdide karşı birlikte hareket etme dürtüsünü programdaki devletlerin politikalarına entegre edebilmekti. Böylece müşterek bir güvenlik stratejisi ve savunma planı yaratılmış olacaktır. Bunun temini için program ülkelerinin hepsiyle ayrı ayrı ilgilenilmeli ve onların ihtiyaçlarına da değer verilmesi gerekmekteydi (http-3 ,2……,E.T: 30.01.2018).

Başlangıçta bu sürece karşı iyi niyetli davranan Rusya, NATO'nun amacının örgüte karşı sempati sağlamak ve üye sayısını arttırarak genişlemek olduğunu fark ettiğinde, programa karşı temkinli davranmış ve negatif yönde tutum göstermiştir (http-4,Pravda, E.T: 30.01.2018 :10).

NATO'nun Bosna'da uyguladığı strateji (Sırp askeri güçlerine karşı gerçekleştirdiği hava saldırısı), Kuzey Kore'ye karşı başlattığı yaptırımlar, birinci Çeçen savaşında Rusya'nın karşısında takındığı tavır ve Rusya'da yaşanan iç siyasal meseleler ve lider değişiklikleri karşısında izlediği politikalar; Rusya'yı ortaklık çemberinden sürekli olarak uzaklaştırmış ve Rusya'nın NATO konusundaki çekincelerini arttırmıştır.

Rus devleti, faaliyetlere aktif biçimde iştirak etmiş ve NATO ile büyük çaplı koordinasyon oluşturma konusunda kararlılığını göstermiştir. NATO ülkeleri ile Rus devleti kendi aralarında koordinasyon sağlamak, işbirliğini geliştirmek, güvenliği temin etmek, çevresel tehditler gibi alanlarda müşterek hareket edebilmek maksadıyla bürokratlarını görevlendirerek görüşmelere başlamışlardır (NATO Handbook, 2001: 81). Fakat Rusya bu programa katılmış olmasına rağmen Avrasya'da oluşacak güvenliğin ve istikrar ortamının icrasının AGİT (Avrupa Güvenlik ve İşbirliği Teşkilatı) aracılığıyla yapılmasını belirtmiştir. Rusya'nın NATO konusunda rahatsız olduğu başka bir konu ise genişleme stratejisidir. Rusya eline geçen her fırsatta NATO'nun genişlemesinden duyduğu rahatsızlığı belirtmiş ve bu konuda NATO'ya olan güvensizliğini iletmiştir. Rusya'ya göre başlatılan programların ve uygulanan stratejilerin hepsinin görünen amacı Avrupa'da genişletilmiş bir işbirliği kurma ve barışı tesis etme olarak açıklansa da; asıl amacı ABD'nin, Rusya'yı NATO vasıtasıyla kuşatmasıdır. Rusya'nın bu tezinde kullandığı en büyük argüman ise Rusya'ya yakın ve son dönemde NATO'ya üye olan ülkelere getirilen ABD askeri birlikleridir.

Bu programa ilaveten Rus devleti ve NATO; koordinasyonun artması, tesis edilen dayanışma ortamının devam ettirilmesi için 'İşbirliği ve Güvenliğe Dair Kurucu Senet' adı altında bir antlaşmayı imza altına almışlardır. Rus devletinin üzerinde durduğu konuların başında tarafların her alanda eşit olduğu vurgusu olmuştur. Yani, NATO'nun ya da üyelerinin Rus devletine karşı hiçbir üstünlüğünün olmadığı vurgulanmıştır. Bu antlaşmayla Rusya, fikir alışverişi ve koordinasyonun sağlanması maksadıyla oluşturulan Daimi Ortak Konsey (DOK) aracılığıyla NATO'ya stratejik konularda fiilen iştirak etmiştir. Bu antlaşma Rusya'nın Avrupa ülkeleriyle olan diyalogu ve NATO'nun büyümesi konularında stratejik seviyede destek vermiştir. Çünkü Rusya'ya, kendisinin halen önemli bir aktör olduğu hissi verilmiş ve güvenliğin tesis edilmesinde kendisine ihtiyaç duyulduğu mesajı gönderilerek ilişkilerin devam ettirilmesi gerektiğine vurgu yapılmıştır (Özdal, 2016: 71-72).

NATO, Balkanlardaki Kosova olaylarının çözülmesi için askeri birlik kullanma kararı alınca Rusya Federasyonu (RF) da antlaşmaları ve koordinasyon faaliyetlerini durdurmaya karar vermiştir. ABD'nin yaşadığı terör olaylarının (11 Eylül tarihinde İkiz Kulelere gerçekleştirilen saldırı) ardından Rusya Federasyonu (RF) ile NATO arasında gerçekleştirilen toplantı sonucunda NATO-Rusya Konseyi (NRC)'nin oluşturulması kararlaştırılmıştır. NRC, politik ilişkilerin ve koordinasyonun devamlılığı için faaliyet göstermiştir. NRC için, RF'nin Gürcistan'a müdahalesi ilişkilerin donma noktasına gelmesine sebep olmuştur. Gürcistan olayında ABD ve NATO açık şekilde RF karşıtı bir tutum almış ve kamuoyu yaratmaya çalışmıştır. Sonrasında kriz aşamalı bir şekilde aşılmış ve ilişkiler normalleşmiştir. Portekiz'in Lizbon şehrinde 2010 yılında yapılan toplantıyla ilişkiler doruk noktasına ulaşmıştır. Açıklanan bildiriyle uluslararası güvenlik krizlerinin müştereken değerlendirileceği, narkotik maddelerin ticaretinin durdurulması konusunda fikir birliğine varıldığı, füze sistemleri için diyalog sürecinin oluşturulacağı beyan edilmiştir. Bu açıdan genel güvenlik konularında müşterek hareket etmenin önemi üzerinde durulmuş, ilişkilerin devam ettirilmesinin uluslararası barışa ve güvenliğe büyük katkı sağlayacağı belirtilmiş, belirtilen konularda koordinasyonun devam ettirileceği açıklanmıştır (http-5,3……, E.T: 31.01.2018).

2.5.3.3. NATO'nun Orta Doğu ile ilişkisi

ABD'nin hegemon güç olma arzusu arttıkça ilgi alanları değişmiştir. Enerji kaynaklarının bulunduğu Ortadoğu coğrafyası da doğal olarak ABD'yi kendine doğru çekmiştir. Bunun sonucunda NATO da bölgeyle ilgilenmeye başlamış, Ortadoğu ülkeleriyle olan bireysel temaslarını arttırmanın yollarını aramıştır. Tarihsel süreci inceleyecek olursak NATO, SSCB ile mücadele edilen zamanlardan itibaren Ortadoğu ülkeleriyle temas halinde olmaya çalışmıştır. Geçmiş zamanlardaki strateji, bölge ülkelerini kullanarak SSCB'yi çevrelemek ve komünizm akımını engellemektir. Bu konudaki diğer bir amaç ise, enerji kaynaklarının güvenliğinin sağlanması ve SSCB'nin eline geçmesini engellemektir (Diriöz, 2012: 50).

SSCB'nin dağılması ve Soğuk Savaşın bitmesinden sonra NATO'nun tehdit algılaması her yerde olduğu gibi Ortadoğu coğrafyasında da değişti. Barış ve istikrarın sağlanması ve devam ettirilmesi için yapılan girişimlerin ve görüşmelerin yeterli olmadığı Balkanlarda yaşanan katliamlardan sonra açıkça görüldü (1992 Bosna Hersek ve 1999

Kosova olayları). NATO anlaşmazlık ve çatışma bölgelerine alan dışı ve direkt olarak müdahale edebilmesi için bir konsept ve yapılanma değişikliğine ihtiyaç duymaktaydı.

İşte bu ihtiyaçlar kapsamında, NATO kendi stratejisinde büyük değişikliklere gitmiştir. NATO güvenlik senaryolarını güncellemiş, oluşan yeni tehditlere karşı tedbirler geliştirmiş, misyonunu bu minvalde oluşturmuş ve yapısal görünümü gelişen şartlar altında tekrar oluşturmuştur. Bu çalışmaların sonucunda oluşan yeni stratejinin ilgi alanlarını maddeleyecek olursak;

- NATO, ilgi alanı dışındaki bir bölgeye güvenliği tesis etme maksatlı taktik seviyede birlik kullanabilecektir.
- NATO, insanlığı tehdit eden tüm silah sistemlerine (nükleer, biyolojik, kimyasal) karşı güç kullanımında bulunabilecektir. Bununla birlikte narkotik ve psikotrop madde ticaretini engellemek gibi uluslararası problemli alanlarda da uygulamalar yapabilecektir. Bu kararları ise BM'ye danışmaya gerek duymadan kendisi alabilecektir.
- NATO, üye ülkelerle işbirliği içerisinde Çokuluslu Görev Kuvvetleri kurabilecek ve kurulan birlikleri harp sahasında kullanabilecektir.
- NATO, sadece askeri boyutta değil uluslararası alanda yaşanacak siyasal krizlerde, ekonomi tabanlı sorunlarda da ilgilenebilecektir.
- NATO, Avrupa'daki devletler ile ABD'nin ortak menfaatlerini gözetecek bir yapı oluşturmalıdır.
- NATO, Avrupa ülkeleri arasındaki rekabetin olası krizlere sebep olmasını engellemelidir.

Kararlaştırılan bu konular NATO ve ABD'ye fazladan misyon eklemiştir. Aynı zamanda da müttefiklerin işbirliğinin arttırılmasını sağlayarak örgütün önümüzdeki yıllarda da etkinliğinin artarak devam edeceğini göstermiştir. NATO, bölgesel ve küresel her türlü tehdit karşısında kendi güvenliğini sağlamaya ve olası krizleri önceden tahmin ederek engellemeye çalışmıştır (Deniz, 2012: 363).

NATO'nun yeni konseptiyle Ortadoğu coğrafyasına müdahalesini Afganistan örneği ile anlatmak mümkündür.

11 Eylül terörünü yaşayan ABD'nin ve NATO'nun tehdit algısı değişti. Oluşan yeni tehdit algısı ve Washington Zirvesi'nde kabul edilen "Yeni NATO Konsepti" ile

NATO alan dışına askeri müdahale yapabilme ve muhtemel tehditleri her türlü tedbirleri alarak önceden engelleme anlayışını benimsemiştir.

ABD'nin başını çektiği NATO görev kuvveti (ISAF) 07 Ekim 2001 tarihinde Afganistan'a askeri müdahaleyi başlatmıştır. İcra edilen bu operasyonla birlikte NATO ilk kez görev sahasının dışında faaliyet göstermiştir. Bu operasyon her ne kadar yeni konsept ve 5. Madde işletilerek NATO açısından yasal görülerek icra edilse de ABD'nin etkisi ile yapıldığı bir gerçektir.

ABD'nin etkisiyle NATO, SSCB'nin dağılmasının ardından Ortadoğu coğrafyasıyla yakından ilgilenmiştir. Çünkü NATO bir güvenlik örgütü olarak oluşturulmuş olsa da aynı zamanda üye ülkelerin ortak menfaatleri için çalışan politik ve ekonomik bir organizasyondur. Aynı zamanda mevcut uluslararası güvenlik sisteminde gücü tartışılamayacak bir denge unsuru olarak yer almaktadır (Diriöz, 2012: 56).

2.5.3.4. NATO ile Birleşmiş Milletler İlişkisi

Birleşmiş Milletler, yapısı gereği neredeyse dünya üzerindeki tüm ülkeleri bünyesinde bulundurmaktadır. Örgütün amacı, küresel güvenliği tehdit eden konuları çözüme kavuşturmak ve küresel barışı tesis etmektir. Ancak kuruluş sisteminde yer alan veto yetkisi sayesinde küresel barışı sağlamaktan daha çok, büyük güçlerin stratejik mücadelelerinin bir aracı haline gelmiştir. Dünya genelindeki askeri, ekonomik, insani ve politik birçok sorun bu sebeple çözülememiştir. Öte yandan herhangi bir kriz konusunda karar çıksa bile, BM'nin bunu uygulayacak askeri ve operasyonel yeteneklere sahip olmaması BM'yi aciz kılmaktadır. Sonuçta, büyük bir hevesle kurulan BM; güvenlik alanında Soğuk Savaş döneminin etkisiz bir kuruluşu konumuna düşmüştür (Bilgili, 2008: 94).

SSCB'nin dağılmasıyla birlikte Avrupa coğrafyası ve Ortadoğu coğrafyası başta olmak üzere dünyanın birçok bölgesinde çatışmalar hızlı bir ivmeyle artmıştır. Başka bir dünya savaşının olmaması ve barışın, huzurun tüm dünyada tesis edilmesi ve bunun kontrol mekanizması görevini de üstlenmesi için kurulan BM kuruluş yapısı gereği hedeflediği vazifesini yerine getirmekte aciz kalmıştır. Bu acizliğin temel iki sebebinden biri; Güvenlik Konseyinin veto mekanizması, diğeri ise Birleşmiş Milletlerin elinde operasyonel bir birliğin olmamasıdır. Ayrıca her üye devletin kendine has sorunları ve tehdit algıları olması sonucunda güvenlik meselesi BM için, içinden çıkılmaz ve çözülemez bir hal almıştır.

BM'nin Somali ve Bosna'da yürüttüğü başarısız operasyonlar neticesinde ister istemez NATO bir adım öne çıkmıştır. Özellikle NATO'nun Bosna-Hersek operasyonunda BM'den sonra yer alması, kısmen de olsa başarı sağlaması, BM'nin durumunu sorgulamaya açmıştır. NATO'dan daha üst düzey bir kuruluş olan BM'nin etkisiz ve yetersiz kalması kuruma olan güveni zedelemiş ve birçok devletin BM'ye bakış açısını değiştirmiştir. 1999 yılında NATO'nun BM'den bağımsız ve habersiz bir şekilde Kosova'ya müdahale etmesi ise BM'nin askeri açıdan etkinliğinin ve caydırıcılığının olmadığını kanıtlamıştır.

Günümüzde BM Güvenlik Konseyinde yer alan beş devletin menfaat ve çıkarları doğrultusunda kararlar veren bir kurum haline gelmiştir. Kuruluş amacı gereği çatışmaları engelleme görevi olan BM, kararlarını dünya barışı için değil beş devletin çıkarları doğrultusunda vermektedir.

2.5.3.5. NATO ile Türkiye İlişkisi

Türkiye'nin NATO ile teması örgütün kuruluş yılına kadar dayanmaktadır. Yapılan politik görüşmeler ve SSCB tehdine 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 ordu'yu 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.

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 çatışmalarda 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 kendisinin 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'da 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).

Kıbrıs meselesi konusunda yaşanılan bu durumlar Türkiye ile NATO arasında bir güven bunalımını ortaya çıkardı. Türkiye, kendisinin NATO'ya bakış açısı ile NATO'nun Türkiye'ye bakış açısının farklı olduğunu gördü.

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'de 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 günümüzde dahi hala tartışılmaktadır. NATO, oluşturduğu SFOR vasıtasıyla barışı koruma faaliyeti icra edebileceğini ve kolektif güvenlik kabiliyetine sahip olduğunu da kanıtlamış oldu.

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 uçakları-

nın 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). Müdahale boyunca BM ve NATO arasında yaşanan anlaşmazlıklar girişimlerin gecikmesine ve sonuca ulaşmamasına sebebiyet vermiştir. Türkiye, NATO ile birlikte operasyon SFOR bünyesinde her aşamasına katılmasına rağmen çoğu yerde NATO ile aynı fikirde olmamıştır. Türkiye NATO'nun ve BM'nin bu operasyonda geç kaldıklarını ve operasyon esnasında çoğu zaman Sırpların lehine kararlar aldıklarını fark etmiştir. Bunun yanında ABD ve AB ülkeleri de bu operasyonda ortak bir strateji yaratamamışlardır.

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. Aynı zamanda alışılmadık tarzda bir faaliyet olarak, iki ülke arasındaki bir güvenlik sorunu için değil, aynı ülke sınırları içinde yaşayan insan topluluklarının birbirlerine karşı yaptığı katliamları engellemek maksadıyla operasyon yapılmıştır.

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 askeri 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 bakımından 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. Ortadoğu 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 üstesinden 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 süreçte çoğunlukla belirsizliklerin hakim 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: 01.02.2018).

Türkiye, 1952 yılında NATO'ya üye olmuştur. Üye olduğu tarihten itibaren NATO 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. Özellikle petrol ve doğalgaz gibi enerji hammaddeleri açısından dünya enerji arzını yönlendirecek bir yapıya 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.

2.6. NATO'nun Değişen Stratejisinde Önemli NATO Zirveleri

SSCB'nin dağılmasının ardından zamanın şartlarına ayak uydurmanın zorunlu olduğunu bilen NATO yeni stratejik hamlelerle kendisini bir değişime tabi tutmuştur. Yapılan değişimin amacı gelişen yeni tehdit algılarına karşı NATO'nun etkin halde kalmasını sağlamaktır. NATO bu süreci iki aşamalı olarak ilerletmiştir. Birinci aşamada

yapılan şey, taktiksel seviyede askeri birliklerin gelişen teknolojiyle yeniden modernizasyonunu sağlayarak sert güç kapsamındaki caydırıcı etkisinin devamlılığını sağlamaktır. İkinci aşamada ise, diyalog ve koordinasyonun arttırılması, ekonomik ilişkilerin devamlılığı ve kültürel konuların ön plana alınmasıyla yumuşak güç kapsamındaki konularla NATO'yu etkin kılmaktır. NATO'nun diğer Avrupa ülkeleri ve alan dışı ülkelerle gerçekleştirdiği temaslar gittikçe artmış ve Rusya ile iletişimini devam ettirerek gelişim konusundaki gayretleri görülmüştür (http-8 , 5 ……, E.T: 01.01.2018).

2.6.1. Washington zirvesi

Bu zirve üye ülkelerin katılımıyla 23 -24 Nisan 1999 tarihinde ABD'nin başkenti Washington'da gerçekleştirilmiştir. Çok önemli stratejik kararların alındığı Washington zirvesinin bildirgesinde aşağıda belirtilen konular ele alınarak deklare edilmiştir;

1. Uluslararası sistem tehdit algısı yönünden büyük değişimler yaşasa da aktörlerin güvenlik ihtiyacı devam ettiğinden NATO'nun üyelerinin güvenliğini sağlamasına aralıksız olarak devam edilecektir.
2. NATO sadece kendi ülkelerinin değil bölgesel ve küresel çaptaki güvenlik krizlerine de barışı sağlamak için müdahale edecektir.
3. NATO, uluslararası ve bölgesel örgütlerle dayanışmasını sürdürerek özellikle BM'nin faaliyetlerinde aktif rol alacaktır.
4. Terör örgütleriyle mücadeleye hız kesmeden devam edilecek, demokratik kurumların devamlılığı sağlanacak, barışı korumak için her türlü tedbir alınacaktır.
5. NATO, uluslararası sistemin talep ettiği güvenliği tesis etmek için alan dışı faaliyetlerde de bulunarak caydırıcı güç olmaya devam edecektir.
6. Silah yarışının durdurulması ve insanlığa karşı kullanılabilecek her türlü silah sistemlerinin (nükleer, kimyasal, biyolojik) yok edilmesi için çalışacaktır.
7. BİO faaliyetleri aralıksız şekilde sürdürülecek ve RF ile ilişkiler arttırılacaktır.
8. NATO, örgütün yapısını büyütmek için üye ülke kazandırma stratejisini sürdürecektir.
9. Çatışmaları ve krizleri başlamadan durdurmayı öngören bir anlayış benimseyecektir.
10. NATO için ABD'nin ve Avrupa kıtasının savunmasının müşterek bir şekilde yapılması gerektiği önemle belirtilmiştir (Gökçe, 2005: 19)

Bu kararların sonucunda NATO'nun kapsamlı bir değişikliğe gittiği açıktır. Bu zirvenin sonuçları sadece NATO'yu değil, üye ülkelerin hepsini ve hatta tüm Avrupa coğrafyasını etkilemiştir.

2.6.2. İstanbul zirvesi

İstanbul'da gerçekleştirilen toplantıda diplomatlar seviyesinde bazı görüşmeler yapılmıştır. Toplantıya ittifak üyelerinin yanı sıra katılan diğer ülkeler bu zirvede dikkat çeken husus olmuştur. Toplantıda alınan kararlar kısaca aşağıdaki gibidir;

1. NATO'nun Bosna'da icra ettiği SFOR görevlerini bitirmesi ve yapılacak yeni bir düzenleme esaslarına göre taktik seviyede askeri birlik görevlendirilmesi gerektiği belirtilmiştir.
2. Bunun aksine Kosova bölgesinde görevli KFOR birliklerinin devamlılığına karar verilmiş ve demokratik kurumların desteklenmesi gerektiği açıklanmıştır.
3. NATO, Akdeniz bölgesinde yaptığı operasyonları terör örgütlerinin etkisiz hale getirilmesi maksadıyla devam ettireceği sinyalini vermiştir.
4. NATO üyeleri Irak ülkesinin askeri birliklerinin bölgesel güvenliği sağlamak için eğitime tabi tutulması konusunda fikir birliğine varmıştır.
5. Terör örgütleriyle yapılan mücadelenin üye ülkelerce uluslararası boyutta devam ettirilebilmesi maksadıyla alınacak bir takım yeni önlemler konusunda karar verilmiştir.
6. NATO birliklerinin her koşulda görev yapabilmeleri için teknolojik imkânlarla desteklenmiş, gelişmiş silah sistemleri ile donatılmış, düzgün ve işlevsel bir kadroyla dizayn edilmiş olmasının güvenliğin sağlanması için bir gereklilik olduğuna karar verilmiştir.
7. Jeostratejik bakımdan hassasiyet taşıyan Kafkaslar ve Ortadoğu coğrafyasındaki ülkelerle işbirliğinin devam ettirilmesi gerektiği belirtilmiştir.
8. NATO, Akdeniz bölgesindeki koordinasyonu arttırmak için farklı dayanışma ve diyalog organlarının kurulmasını tavsiye etmiştir (http-8 , 5 ……, E.T: 01.01.2018).

2.6.3. Bükreş zirvesi

NATO'nun Bükreş şehrinde yaptığı toplantıya üye ülkeler arasında olan Estonya'nın yaşadığı kriz damga vurmuştur. Bu zamana kadar hiçbir ülkede görülmeyen bo-

yutta bir dijital saldırıya maruz kalan Estonya'da büyük sorunlar yaşanmıştır. Devlet kurumlarının neredeyse tamamının dijitalleşmiş olması ve vatandaşların gündelik birçok işini internet üzerinden gerçekleştirmesi yaşanan bu saldırı sonucunda altyapının çökmesine sebep olmuştur. Durumun vahametini bu örnek olayla anlayan NATO, Bükreş'te yapılan toplantıda ilk kez siber saldırıları gündemine almış ve bu konuyu bir tehdit algısı olarak değerlendirmiştir (http-12,Boyraz, E.T: 17.03.2018).

Estonya'ya karşı sanal ortamda yapılan siber saldırı sonucu, Estonya da bilgisayar ve ağ sistemlerinin kritik alt yapılarında büyük çapta krizler meydana gelmiştir. Gerçekleşen siber saldırı sonucunda oluşan hasar boyutu Estonya'nın olduğu kadar diğer ülkelerin ve NATO'nun da dikkatini çekmiştir. Bu güvenlik açığı NATO'ya yeni bir güvenlik algısı oluşturmuştur. NATO'yu ve diğer Dünya ülkelerini ilgilendiren yeni tehdidin adı 'siber güvenlik'tir.

Bu yaşanan olay neticesinde NATO bazı tedbirler alma yoluna gitmiştir. İlk olarak böyle bir siber saldırının tekrar yaşanması ihtimaline karşı savunmanın ortak bir strateji ile yapılabilmesi için Siber Savunma Yönetimi Makamı (CDMA)'nı oluşturmuştur. Belli bir süre sonra da Estonya'da Siber Savunma Mükemmelliyet Merkezi (CCDCOE)'ni kurarak siber güvenlik konusunda bir koordinasyon makamı yaratmıştır (http-12, Boyraz, E.T: 17.03.2018).

NATO oluşan bu yeni tehdit konusunda da üye ülkelerin ihtiyacını karşılaması gerektiğinin farkında olarak faaliyete geçirdiği makamlarla birincil tedbirini almıştır. Bu kurumların temel amacı gelecek bir siber tehdidi önceden fark ederek gerekli tedbirleri almak ya da gerçekleşen bir siber saldırıda aktif savunma planları ile karşılık vermektir. Bununla birlikte bu kurumlar; üye ülkelerin siber güvenlik alanlarında ihtiyaç duyduğu teknik yardımı temin etmek, teknolojik işbirliği gerçekleştirmek, siber tehditlere karşı ortak bir savunma planı oluşturmak, yapılan bu çalışmaların yeterliliğini kontrol etmek için gerçeğe dayalı saldırı senaryoları düzenlemek, üye ülkelerin bu alanda çalışacak personelinin eğitimine gerekli desteği vermek gibi görevleri yapmakla yükümlüdür (http-12, Boyraz, E.T: 17.03.2018).

NATO bünyesinde Estonya'nın Tallinn şehrinde faaliyet gösteren CCDCOE, siber güvenlik konusunda önemli gelişmelere imzasını atmıştır. Birincisi, siber dünyanın genelini ilgilendiren konularda kanuni bir zemin oluşturmak için Tallinn El Klavuzu adı altında bir çalışma yapmıştır. İkincisi, NATO ülkelerinin katılımıyla siber güvenlik konusunda gerçekleştirdiği Uluslararası Siber İhtilaf Konferansları'dır. Üçüncüsü ise,

NATO üye ülkelerinin tamamının katıldığı ve müştereken icra edilen tatbikatlardır (http-12, Boyraz, E.T: 17.03.2018).

2.6.4. 60. Yıl zirvesi

NATO'nun kuruluş yıldönümünde gerçekleştirilen toplantıda ülke liderlerinin katılımıyla geniş çaplı bir görüşme yapılmış ve kritik konularda kararlar alınmıştır. NATO'nun genişlemesine ve gelişmesine vurgu yapılmış, Afganistan ve Kosova ülkelerinde icra edilen barışı destekleme faaliyetleri görüşülmüş, Sekreterlik makamı görevlendirmesi yapılmış ve daha birçok farklı konu gündeme getirilmiştir.

Zirvenin başlıca sonuçları aşağıdaki gibidir:

1. Rasmussen NATO'nun Genel Sekreterlik makamına getirilmiştir.
2. Fransa, NATO'nun askeri kanadına dönüş yapmıştır.
3. Balkanlardaki genişleme politikasının somut bir göstergesi olarak Hırvatistan ve Arnavutluk NATO'ya dâhil olmuştur.
4. NATO, çağın güvenlik gerekliliklerine uygun olarak misyonunu yeniden tanımlamış ve kuruluş amaçlarına sağdık kalacak şekilde bir strateji geliştireceğini belirtmiştir.
5. Bir sonraki toplantının Lizbon'da düzenleneceği bildirilmiştir (http-8, 5 ……, E.T: 01.01.2018).

2.6.5. Lizbon zirvesi

19-20 Kasım 2010 tarihin de üye ülkelerin katılımıyla Lizbon'da gerçekleştirilen zirvede alınana kararlar aşağıda belirtilmiştir.

1. Füze Kalkanı Projesine saldırıların İran ve Suriye'den geleceğine ilişkin Fransa'nın bildiriye konmasını istediği ifade konusunda ısrarı sonuçsuz kaldı. "Orta Doğu" ifadesini koydurtma isteği de kabul görmedi, sonuç olarak bildiriden Türk devletini tedirgin edebilecek cümleler çıkartıldı. Söz konusu füze savunma projesinin 10 yıl sonra kullanıma hazır olacağı düşünülmektedir.
2. Rusya ile NATO arasında ilk kez bu kadar samimi bir ilişki tesis edildi. NRC işbirliğinin devam etmesinin yanında savunma sistemleri konusunda da NATO ve Rusya birlikte hareket edeceklerini beyan etti.
3. Açıklanan bildiride Türkiye'nin NATO için değerli bir aktör olduğu vurgulandı.

4. Almanya'nın nükleer silah sistemlerinin en aza indirgenmesi konusundaki fikrine diğer üyeler (İngiltere ve Fransa başta olmak üzere) karşı çıkmışlardır. Yapılan görüşmeler neticesinde uluslararası sistemde nükleer silahların NATO dışındaki ülkelerde de bulunmasından dolayı örgüt ülkelerinin güvenliğinin sağlanması için bu sistemlerin bir ihtiyaç olduğu kararlaştırıldı.

5. Afganistan meselesinde ciddi görüşmeler yapıldı. Görüşülen maddeleri sıralayacak olursak;

i. NATO askeri birliklerinin ISAF'tan ayrılması bir yıl sonra başlayacaktır.

ii. Dört yıla kadar Afganistan ordusunun modernizasyonu ve eğitimi tamamlanarak kendi ülkelerini kendilerinin koruması sağlanacaktır.

iii. RF ile yapılan mutabakata göre askeri lojistik malzemeleri bundan sonra RF'nin demiryolu kullanılarak yapılabilecektir. Böylece ekonomi ve işgücü tasarrufu sağlanacaktır.

6. Terör örgütlerine karşı NATO'nun aktif bir strateji uygulayacağı ve gerekirse müştereken bir askeri operasyon dâhil her seçeneği uygulayabileceği üye ülkelerce karar bağlanmıştır (http-9, Çetin, E.T: 01.02.2018).

2.6.6. Chicago zirvesi

Gerçekleştirilen zirve ABD'de icra edilen ikinci NATO zirvesi olmuştur.

1. Yapılan bildiride özellikle Afganistan sorunu hakkında önemli bir mesafe kaydedildiği ve iki yıl sonra NATO'nun çekilmesiyle birlikte Afganistan ordusunun kendi ülkesini koruyabilecek hale getirileceği ifade edilmiştir. NATO, Afganistan devletinin terör örgütleriyle olan mücadelesinde desteğini devam ettirecektir. Bu aşamadan sonra da gerek askeri, gerek eğitim, gerekse diplomatik konularda işbirliği devam ettirilecektir. NATO, Afganistan'da barış, güvenlik ve huzur ortamı sağlanması için bölge ülkeleriyle de temasını sürdürecek ve bölgesel güvenliği sağlamak için çalışacaktır.

2. Ayrıca NATO'nun Balkan coğrafyası için de girişimlerde bulunmaya devam edeceği, KFOR bünyesinde gerçekleştirilen faaliyetlere iştirak edeceğini beyan etmiştir. Bununla birlikte Ortadoğu bölgesi ve Akdeniz havzası gibi yerlerde de güvenliğin tesisi için operasyonlarına devam edeceğini açıklamıştır.

3. Bildiride Türkiye'nin AB üyesi olmamasına rağmen müşterek askeri faaliyetlere katıldığı ve NATO bünyesindeki diğer faaliyetlere olan katkıları göz önüne

alındığında değerli bir müttefik olduğu belirtilmiştir. Ayrıca Türkiye'nin güvenlik kaygılarının da önemli ve dikkate alınmaya değer olduğu vurgulanmıştır

4. NATO, üye ülkelerin arasında koordinasyon sağlanmasının zorunluluğunu hatırlatmış, ilişkilerin iyi niyetli olarak sürdürülmesi gerektiğini belirterek ortak kaygıları paylaşan ve aynı konuları savunan her ülkenin NATO'ya katılabileceğini beyan etmiştir. Bu yaklaşım NATO'nun genişleme yanlısı tutumunu bir kez daha göstermiştir.

5. NRC faaliyetlerinin küresel barışa olan katkısı belirtilmiş, RF ile daha iyi ilişkiler kurma isteği özellikle beyan edilmiştir. Uluslararası barış ve güvenliğin sağlanmasında NATO-Rusya ile işbirliğinin önemine işaret edilmiş, iki taraf arasında gerçek anlamda bir stratejik ortaklık arzu edildiği vurgulanmıştır. Libya ülkesinin istemesi halinde NATO faaliyetlerine katılımcı şeklinde dâhil olabileceği iletilmiştir. Ortadoğu coğrafyasındaki çatışmaların ise dikkatle izlendiği BM'nin taleplerine olumlu bakılacağı açıklanmıştır.

6. NATO'nun tehdit algıları arasında özellikle siber saldırı konusundan bahsedilmiştir.

7. Nükleer silahlanma faaliyetleri açısından yapılan tüm uyarılara rağmen İran'ın faaliyetlerine devam etmesi ve iletişim taleplerine olumsuz cevap vermesi kınanmıştır. Ayrıca nükleer silah kapasitesi ve balistik füze sistemlerini arttırmayı planlayan ve bu yönde çalışan Kuzey Kore'nin faaliyetlerinin dikkatle takip edildiği belirtilmiştir

8. Kıtalararası balistik füze sistemlerinin artması sonucunda yeni bir savunma stratejisi üzerinde çalışan NATO kendi imkânlarını arttırmak için harekete geçmiştir. Bu kapsamda Türkiye (Kürecik)'de yeni nesil bir füze savunma sisteminin kurulacağı açıklanmıştır. Bu gelişmelerin RF ile diyalog içerisinde gerçekleştirildiği ve kesinlikle RF'ye yönelik bir tehdit unsuru içermediği özellikle belirtilmiştir.

9. Toplantıda NATO üye ülkelerince kararlaştırılan yeni stratejiye göre; NATO'nun emir-komuta düzeninin çabuk ve etkili karar verebilen bir yapıya dönüştürüleceği, yapılan faaliyetlerin parasal yükünün azaltılacağı, merkezi görev yapan askeri birlik durumunun minimum seviyelere getirileceği, yapısal bazı değişikliklere gidileceği, teknolojik sistemlerin güncelleneceği, üye ülkeler arasındaki iletişimin daha da arttırılacağı, yapılan tüm harcamaların üye ülkelerin kontrolüne açık olacağı bir yapı tesis edileceği açıklanmıştır (http-10, Akçadağ, E.T: 01.02.2018).

2.6.7. Newport zirvesi

4-5 Eylül 2014 tarihinde gerçekleştirilen bu toplantının ana konusu IŞİD olmuştur. Ukrayna'da yaşanan olaylar ve dini motifli terörist grupların yaptığı saldırılar nedeniyle gündemde olması gereken siber güvenlik konuları arzu edildiği kadar değerlendirilmemiştir (http-12, Boyraz, E.T: 17.03.2018).

NATO'nun terörle mücadele harekâtı görevlerinin arttığı bir dönemde siber savunma konusu daha önceden temel güvenlik konuları arasına alınan tehditler ile mücadele alanı içinde değerlendirilmiştir. NATO bu aşama da kendisine ait bir siber savunma politikası belirlemiş ve siber tehditlere karşı stratejik seviyede bir eylem planı geliştirmiştir. Bu kabul gören temel savunma stratejisinin bir gereği olarak bildiride siber güvenlikle ilgili olarak açıklanan maddeler şunlardır;

1. İlerleyen süreç içerisinde teknolojinin gelişmesine paralel olarak siber tehdit konuları da artacağından dolayı müttefikler arasındaki diyalog süreci ve koordinasyon devam ettirilmelidir.
2. Siber tehdit unsurları ile mücadele faydalanılabilecek hukuki bir dayanak olmadığı için bu kapsamda çalışmalar gerçekleştirilmelidir.
3. Siber tehditlere karşı kapsamlı siber savunma planlarının yapılması için müttefikler kendi ülkelerindeki kurumları sürekli olarak desteklemelidir.
4. Her müttefikin bünyesinde ve AB'nin her üye ülkesinde siber savunma kabiliyetlerinin yönetileceği kurumlar oluşturulmalıdır. Ayrıca bu sektördeki özel kuruluşlar da ülkeler tarafından desteklenmelidir (http-12, Boyraz, E.T: 17.03.2018).

2.7. Soğuk Savaş Sonrası Güç Dengesi

Genel olarak anarşinin hâkim olduğu uluslararası sistem son yıllarda meydana gelen olaylar neticesinde ciddi bir güvenlik bunalımı yaşamıştır. Yaşanan gelişmeler sistemin denge unsurlarını da etkilemiş ve tehdit algılamalarını değiştirmiştir. SSCB'nin dağılması sonrasındaki güç dağılımı, terör örgütlerinin küresel boyutta faaliyet göstermesi, Orta Doğu ve Balkanlarda yaşanan etnik temelli ve dini motifli çatışmalar, ülkelerin arasında yaşanan silahlanma mücadelesi, nükleer silah sistemlerinin artması ve teknolojinin gelişmesiyle birlikte hayatımıza giren siber tehditler kaos içindeki uluslararası sistemi daha da içinden çıkılmaz ve aşılması zor bir güvenlik ortamına sürüklemiştir (Yılmaz, 2008; 34).

SSCB'nin dağılmasının ardından güç dağılımındaki dengesizlik ve ulus devletlerin tehdit algısındaki değişim gücün tanımını da değiştirmiştir. Zor kullanma yerine işbirliği ve diyalog süreçlerinin öne çıkması, maliyet sorunları ve kitlesel imha tehditleri neticesinde sert gücün önemi yok olmamış olsa da başka güç kaynak arayışları artmıştır. Uluslararası sistemin en güçlü aktörü olan devlet, oluşan yeni tehditler karşısında kendi bekasını sağlamak için amacını, hedeflerini, kaynaklarını ve en önemlisi gücünü sorgulamıştır. Günümüz dünyasında ulusal devlet yapısının ayakta kalabilmesi için, donanımlı bir askeri güce sahip olması, mevcut tehditlere karşı aktif tedbirler alması, ekonomik düzeyini sağlam bir yapıya dayandırması gerekmektedir. Kısacası her türlü tehdit durumuna karşı kendi öz kaynaklarıyla savunma stratejileri geliştirip, bu planları hiçbir destek almadan kendisi uygulamak zorundadır (Yılmaz, 2008; 34-35).

SSCB dağıldıktan sonra küresel güç sisteminde büyük denge sorunu yaşanmıştır. Bunun sebebi uluslararası ilişkilerin temelini iki kutuplu düzenin sağlamasıdır. İki kutuplu sistemin ortadan kalkmasıyla birlikte yeni bir güç dengesi inşa edilememiştir. Klasik realizm anlayışına sahip olanlar, uluslararası sistemin dengesinin ne biçimde değişeceğini sorgularken; liberalizm akımından etkilenenler de, sistemin yaşadığı değişimi, küreselleşme kavramını ve başka güç unsurlarının sistemi ne şekilde etkileyeceği üzerinde düşünerek bu gelişmelerin kim tarafından ve nasıl bir etki faktörü olarak değerlendirileceği konusunda çalışma yaptılar. Fakat bu yapılan çalışmaların hepsi düşünce halinde kalmış ve strateji seviyesine getirilememiştir. Koşulların köklü olarak değiştiği uluslararası sistemde devletler kendi menfaatleri doğrultusunda bir işbirliği anlayışı ararken, müttefikleri ile müşterek çıkarları konusunda da ileriye dönük stratejiler oluşturma niyeti göstermektedirler. SSCB'nin dağılmasından sonra oluşan küresel ortamın güvenlik sisteminin dengesini, güçlü ve ulus devletlerce oluşturulacağını belirtmek mantıklı bir yaklaşım olacaktır (Efegil, Musaoğlu, 2009: 2-3).

Buzan'a göre SSCB'den sonraki uluslararası sistemde bazı temel yaklaşımlar oluşmuştur. Bunlar; küresel bakış açısı, neo-realist bakış açısı ve bölgesel bakış açısıdır. Neo-realizm bakış açısına göre, realist düzenin öngördüğü şekilde temel aktör devlettir ve uluslararası güvenliğin güç odaklı mücadelesinin bir hegemon devlet ya da birden çok devletin etkisinde gerçekleşeceğini tahmin etmektedir. Küresel bakış açısına göre, neo-realist bakışın karşıtı bir görüşle devletin yerini küresel şirketler almıştır. Ekonominin ön planda olduğu bir dönemde sınırların, kuralların ve ulusal devletlerin statik durumun yerine büyük ekonomik güce sahip, esnek yönetim tarzı olan ve sınırları olmayan

güçlerin denge sistemini oluşturacağını belirtmişlerdir. Hatta bu şirketlerin, ellerindeki büyük sermaye gücü sayesinde temel güç unsuru olarak ulus devletleri kendi amaçları doğrultusunda birer araç olarak kullanabileceklerini değerlendirmişlerdir. Bölgesel bakış açısında da SSCB'nin dağılmasıyla birlikte ilgi alanının uluslararası ortamdan ziyade bölgesel ortamlara kaydığını, hegemon güç olan ABD'nin dışındaki diğer ülkelerin kendi güvenlik sorunlarıyla ve dar kapsamlı konularla uğraştıkları, komşularının haricinde sınır ötesi bir güvenlik kriziyle ilgilenmediklerini öne sürmüştür (Yılmaz, 2008; 35-36).

SSCB'nin dağılmasının ardından uluslararası güvenlik ortamı şekillenmeyi halen sürdürmektedir. Güç dağılımı çok kutuplu yöne doğru kaymaktadır. Bu durumun sebepleri arasında şunlar söylenebilir:

1. Kontrol makamındaki kurumlar ve güç unsurları geçerliliklerini yitirmektedir.
2. Enerji kaynakları tükenirken elde olanları muhafaza edebilmek ve bu kaynakları birer güç unsuru haline getirmek önemli uluslararası krizler ve çatışmalar yaratacaktır.
3. Bu enerji kaynaklarına sahip olmak için hegemon güç olma niyetini sürdüren ABD ve sistemde güç unsuru olma yolunda olan ülkelerin yapacağı güç mücadelesi uluslararası güvenlik ortamını şekillendirecektir.
4. Güvenlik konularında terör örgütleri daha çok gündemde olacak, demokratik krizler, kültürel sorunlar ve dini meseleler ön plana çıkartılacaktır.
5. Ulus devletlerin önemini yitirmesini sağlayan küresel sistem devletlerarası krizleri ve güven bunalımını arttırmaktadır (Yılmaz, 2008; 36).

İkiz Kulelere yönelik olarak yapılan terör saldırıları hem ABD için hem de tüm dünya ülkeleri için güvenlik kapsamında bir dönüm noktası olmuştur. Yapılan bu saldırı ABD'nin terör örgütleri konusunda taktiksel seviyede reaksiyon göstermesine sebep olmuştur. ABD tarafından teröre yönelik olarak yapılan operasyonlar çoğu zaman amacını aşarak stratejik hedefler elde etme yolunda kullanılan bir bahane olmuştur. Bunun sonucunda RF de kendi stratejisini değiştirme yoluna gitmiştir. Aynı zamandan ABD'nin bu zamansız, mekânsız ve aşırı güç kullanımı içeren operasyonları Avrupa ülkeleri ile olan ilişkilerine de zarar vermiştir. Dönemin ABD Başkanı, kendi ülkesinin dışarıya olan stratejik bakışını örgütlerini etkisiz hale getirmek ve küresel sisteme hâkim

olmak şeklinde açıklamıştır. Aynı zamanda ABD yetkililerince yapılan açıklamalarda; ABD'nin terör örgütlerini ortadan kaldırmak için yaptığı operasyonların devam edeceği, bu taktik harekâttaki kararlılığın diğer düşman unsurlar için de caydırıcılık taşıyacağı ve ABD'nin tehdit nereden gelirse gelsin zaman, mekân ve koşul aramaksızın kendisine yönelen tehdit unsurlarını yok edeceği özellikle belirtilmiştir (Yılmaz, 2008; 36).

Bu yeni ortamda ABD'nin hegomonik bir güç olma isteği, kendi bekasını ve güvenliğini her türlü konudan üstün tutması, başta RF olmak üzere tüm dünya ülkelerine uyguladığı politik baskı unsurları ve silahlanmasıyla birlikte saldırgan realizm anlayışı içinde olduğu görülmektedir. ABD kendi ulusal gücünü sürekli olarak üstün tutma gayret ve çabası içerisindedir. ABD için önemli olan uluslararası sistemin güvenlik dengesi değil, kendi ulusal gücünü tartışılmaz üstün güç haline getirmektir. 11 Eylül saldırıları her ne kadar bu görüşü desteklese de aynı zamanda bu görüşün yapısal bir mazeretidir. Saldırgan realizm anlayışında, ülkelerde başka ülkelerin yarattığı sorunları ya da tehditleri, aktif bir savunma planıyla etkisiz hale getirme niyeti bulunmaktadır. Bu bakış açısı ABD'de yeterince mevcuttur. 'Esnek Karşılık ve İleri Savunma' stratejisi ABD tarafından kullanılan ve yukarıda bahsedilen konunun belirgin bir örneği sayılabilir.

RF ise her ne kadar üstün güç olma hedefini sürdürse de genellikle dengecilik arayışları sebebiyle savunmacı realizm anlayışıyla hareket etmektedir. Küresel ve bölgesel yapmış olduğu ittifaklarla (BRICS, ŞİO) ABD'nin oluşturmak istediği çemberi kırmaya çalışmaktadır. Şu an için bu bakış açısında olsa da yaşanabilecek olan yapısal değişimlerle saldırgan realizm anlayışını da benimsemesi mümkün görünmektedir.

III. BÖLÜM : SİBER GÜVENLİK KAVRAMI VE STRATEJİSİ

3.1. İnternetin Ortaya Çıkışı ve Gelişimi

İnternet günlük yaşamda yerini almaya başlamasıyla birlikte en yoğun kullanılan, en hızlı kitle iletişim ortamı olmaya başlamıştır. Mobil cihazların gelişmesi ve bilgisayarlar gibi yeni işlevleri olmasıyla birlikte (yöndeşme) internet yaygın olarak kullanılmaya başlanılmıştır.

Teknolojinin gelişmesi ile birlikte her geçen gün yeni birçok sosyal ağ uygulamaları çıkmaktadır. Yeni çıkan sosyal ağ uygulamaları akıllı telefonlara da uygulama olarak eklenmiştir. Akıllı telefonlar her yaştan kullanıcıya hitap etmektedir. İnternet ortamında yayımlanan yazılar sadece okumakla kalınmayıp, yazılanlara ve görüntülemelere yorum da yapılabilmektedir. İnternet, milyonlarca veya milyarlarca kullanıcı tarafından içeriklerine de katkı sağlanan sanal ve sosyal bir ortam halini almıştır. İnternet günlük yaşamımızı kolaylaştıran çok fazla özelliği barındırmaktadır. Kamu kurum kuruluşları tüzel ve özel kuruluşlara gitmeden dünyanın her hangi bir yerinden işlem yapma olanağı sağlamaktadır. İnternet üzerinden yapılacak olan işlemlerde zamandan etkin yararlanılmakta ve paranın elde dolaşımına gerek kalmadan bankacılık, alışveriş vb. işlemler yapılabilmektedir. İnternet, doğru veya yanlış birçok bilgiyi barındırmaktadır (Altuntas,2018:3-11).

İnternetin yaygınlaşan kullanımı ile birlikte birçok zararlı yönleri de ortaya çıkmıştır. İnterneti kullanan kötü niyetli düşünceler, faaliyetlerini yapabilmek için interneti bir araç olarak görmektedir. Örnek verecek olursak, terör örgütlerinin üyeleri tarafından kendi aralarındaki iletişimi ve eğitimi gerçekleştirdikleri bir ortam olarak kullanılmaktadır (Kara, 2013: 6-7).

SSCB'nin 1957 yılında ilk yapay uydusu Sputnik'i uzaya göndermesinin ardından ABD tarafından tepki göstermek amacıyla çalışmalara hız verilmiştir.

İnternet, ABD'nin 'ARPA' adlı projesini hayata geçirilmesiyle başlamıştır. Bu projenin ilk amacı; önemli bir bölümünün kesintiye uğraması veya saldırıya maruz kalması durumunda bile faaliyetine devam edebilecek bir ağ yaratmaktı. ARPANET, sorun olması halinde otomatik olarak ağ trafiğini diğer irtibatlı sistemlere yönlendirerek gerekli bilgiyi kesintisiz bir şekilde aktarmak üzere tasarlanmıştır. İnterneti servis dışı bırakma (Denial-Of-Service-DOS) saldırılarına karşı dayanıklı olarak tasarlanmıştı(Yılmaz ve Salcan,2008: 35).

Daha fazla bilgisayarın ARPANET'e katılımıyla, ağın işe yararlılığı daha da artmıştır. Önceleri ARPANET, başlıca üniversiteler ve kamu bilgisayarlarından oluşmaktaydı. Elektronik posta, elektronik haber grupları ve uzaktan irtibatlanma gibi basit uygulamaları içermekteydi. 1971'de ARPANET, yaklaşık yirmi dört kadar araştırma ve kamu sitesine de irtibatlanarak araştırmacıların daha fazla bilgi alışverişi yapmalarına imkân sağlamaya başlamıştır. Böylece, ARPANET müşterek araştırmalar için ilk adımını atmıştır. Bu yıllarda araştırmacılar ARPANET kullanarak kendi aralarında oyunlar oynamaya başlamışlardır. Kendi aralarında şakalar yapmaya, eğlendirici ve sinirlendirici mesajlar, ayrıca küçük güvenlik ihlallerini kapsamaktaydı. Ancak bu ihlaller çok seyrek olmaktaydı. Çünkü ARPANET kullanıcıları genellikle birbirlerini tanıyan ve birbirlerine güvenen kişilerden oluşan küçük bir grubu temsil etmekteydi (Yılmaz ve Salcan,2008: 35-36).

ARPANET geçmiş yıllar içerisinde ve 1974-1976 tarihleri arasında intranet adıyla kullanılmaya başlamıştır. ARPANET hızlı olarak büyümeye başlayarak askeri faaliyetlerde kullanılan bölümlerine milnet ismini almıştır. ARPANET gelişmeye başlayarak internet ismini almıştır. İnternet zamanla ağların birbirlerine bağlanmasıyla büyük ağlar oluşmuştur.

1 Ocak 1983 tarihinde bilgisayarların karşılıklı haberleşebilmesi ve internette ağa bağlı bilgisayarların birbirlerini tanımasını sağlayan Transmission Control Protocol and Internet Protocol (TCP/IP) protokolü kullanılarak, internetin bireysel ve ticari şekilde kullanılmaya başlanılmıştır.

İngiltere'nin 20. yüzyıldaki en önemli isimlerinin zirvesinde yer alan ünlü İngiliz fizikçisi Tim Berners- Lee, Avrupa Nükleer Araştırma Örgütü olan CERN'de görev yaptığı çalışmalarının en önemlileri arasında 1989 tarihinde CERN laboratuarlarında geliştirdiği HTML işaretleme dili sayılmaktadır.

HTML işaretleme dili Web'in temelini oluşturmaktadır. HTML işaretleme dili yani web'i geliştiren ve kurucusu olarak kabul edilen Tim Berners-Lee ilk ağ tarayıcısı world-wide-web'i (www) 1990 yılında geliştirmiştir. İnternetin ortay çıkışını ve gelişmesini sağlayan ARPANET'e 1990 yılında son verilmiştir. Tim Berners-Lee kendi yazmış olduğu ağ tarayıcısıyla ilgili olarak kendisinin belirlediği bazı standartları ortaya koymak için W3C'yi yaratmıştır. Tim Berners-Lee tarafından W3C ile web'in standartlarını ortaya koyan bu örgütün temel amacı HTML dilinin devamlılığının oluşturularak HTML verilerinin bütün ağ tarayıcılarında ve teknolojik cihazlarda (akıllı telefonlar ve

bilgisayar) aynı veriyi almasını sağlamaktır. İnternet üzerinden web arama motorlarında W3C ile web'in standartları yaratılmış ve web sitelerinin arama motorlarında üst sıraya çıkması sağlanmışdır.

İnternetin, coğrafi olarak bir mekânı ve çizilmiş bir sınırı yoktur. İnternet'te bilinen fiziksel kuralları uygulamak zor ve imkânsızdır. İnternet kullanımın her geçen gün toplumsal olarak sosyal hayata girmesi ve artmasıyla birlikte oluşan sanal ortamların kontrol altına alınması zor bir hale gelmiştir. Kontrol altında tutulamaması internette yararları, zararları ve güvenlik problemlerini de beraberinde getirmiştir. Kamu kurum ve kuruluşları, özel şirketler, üniversiteler, vatandaşlar internet ağından faydalanmaktadır. Vatandaş ve devlet ilişkisi internet üzerinden örneğin e-devlet uygulamaları vb. uygulamalar ile hızlı ve güvenli şekilde gerçekleştirilmeye çalışılmaktadır. Her ne kadar güvenlik sağlanılmaya çalışılsa da bu tam anlamıyla sağlanılamamaktadır.

3.1.1. Worm saldırıları

Worm İngilizce kelime olup Türkçe anlamı solucan'dır. Bilgisayar solucanı anlamında gelmektedir. Bilgisayar solucanı, kendini kopyalamak ve diğer bilgisayarlara yayılmak için kötü amaçlı bir yazılım programıdır. Virüs gibi solucanlar da kendilerini diğer cihazlara kopyalamak için tasarlanmışlardır, ancak bunu kendi başlarına yönetirler. Solucanlar kendini diğer ağlara ve bilgisayarlara taşıyabilmektedir. Uzmanlar worm yani solucanı bilgisayarlarda bulunan sürücüler, sistemler veya ağlarda kendi kopyalarını oluşturarak yayılan bir virüs olarak tanımlamaktadır. Code Red ve Nimda'ya göre worm'lar "solucan", işletim sistemleri ve uygulamaların açıklıklarını kullanarak sisteme sızabilir ve sızdıkları sistem üzerinden çoğalır. Solucan (worm) sızıntılarını önleyebilmek için sızıntının tespit edilebilmesi önemli olup, imkânlar dâhilinde sistemlerin güvenlik duvarları kullanılarak emniyet alınmalıdır.

3.1.2. DDoS atakları

DDoS (Distributed Denial of Service), saldırısı, kullanıcıların belirli bir sisteme ulaşmasını önlemeyi amaçlar. Amaçlanan kullanıcılara ulaşılamayacak bir bilgisayar veya ağ kaynağı yapmaya çalışmayı, çoğunlukla hedef makineyi, yasal trafiğe cevap verememesini veya etkin bir şekilde kullanılamayacak kadar yavaş yanıt vermesini sağlamak için harici iletişim istekleri ile doyurmak anlamına gelmektedir. Bir DDoS saldırısı, sistemi meşgul tutmak için kullanıcıların isteklerini karşılayamadığı ve sistemi kul-

lanamayacağı için sahte istekleri gönderir. Bir internet sitesinin, bir sunucunun veya yönlendiricinin, sitenin yanıt verebileceği veya işleyebileceğinden daha fazla veri talebi ile suçlandığı bireysel suçlular ve diğer devlet dışı aktörler tarafından kullanılan temel bir siber savaş tekniğidir. Kaspersky için bu tür saldırılar, herhangi bir ağ kaynağı için geçerli olan belirli kapasite limitlerinden faydalanır - örneğin bir şirketin web sitesine olanak tanıyan altyapı gibi. DDoS saldırısı, web sitesinin çoklu talepleri karşılama kapasitesini aşmak ve web sitesinin düzgün çalışmasını önlemek amacıyla saldırıya uğramış web kaynağına birden çok istek gönderir. DDoS saldırıları için tipik hedefler; internet alışveriş siteleri, çevrimiçi hizmet sunmaya dayalı iş veya organizasyonlardır.

Basit saldırı çeşidi olarak DDoS (Distrubuted Denial of Service) çok sık kullanılmaktadır. DDoS saldırılarının temel olarak ana teması, çalışan sistemleri iptal ederek maddi zararlara neden olmaktır. Siyah şapkalı hacker'ların veya çeşitli hactivist oluşumların zaman zaman kullandıkları yöntemlerdir. Siber saldırılarda siber savaşların en etkilisi olarak görülmese de rahatsızlık vericidir ve maddi kayıplara neden olmaktadır. Gürcistan ve Estonya'ya karşı Rusya tarafından yapılan saldırıda DDoS atakları kullanılmıştır. DDoS atakları veya saldırılarında temel prensip sistemi durdurmak ve geçici süre ile kullanılmaz hale getirmektir. Ancak DDoS ataklarının ekonomik finansal kuruluşlardan bankalara karşı yapılması durumunda sistemi geçici olarak devre dışı kalması halinde ortak kullanıma ait bankamatikten herhangi bir işlem yapılamaması ve para dahi çekilememesi durumunun sorun oluşturabileceği açıkça görülebilmektedir. Saldırıların uzun zaman alarak devam etmesi durumunda ise sorunlarında büyümesine neden olmaktadır. Saldırıların dağınık diye adlandırılmasının nedeni ise saldırıların aynı zaman dilimi içerisinde binlerce, yüz binlerce veya milyonlarca bilgisayarın aynı anda kullanılarak yapılmasıdır. Bu duruma "botnet" ismi verilmiştir. Ağ üzerinden daha önce virüs bulaştırılarak kötü niyetli kimselerin kontrolüne aldığı bilgisayarlara zombi bilgisayarlar denilmekte ve zombi bilgisayarların ise uzaktan otomatik olarak kontrol edilmesiyle botnet ağları oluşmaktadır (Kara, 2013: 38).

Bilgisayar kullanıcıları kendi kullanımında ve sorumluluğunda bulunan bilgisayarlarına virüsün bulaşmasına paralel olarak bilgisayarlarının zombi bilgisayar olduğunun farkında değillerdir. Bilgisayarlarının zombi bilgisayar olduğunun farkında olmayan kullanıcılar doğal olarak DDoS saldırılarına alet edildiğini de anlamamaktadırlar. Bilgisayar kullanıcılarının bunu anlamamasının nedeni ise virüs'le bulaşarak zombi olan bilgisayarın programların arka planda çalışması ve bilgisayarda herhangi bir belirti

vermemesinden kaynaklanmaktadır. E-posta aracılığıyla gönderilen virüsler e-posta açıldığı andan itibaren bilgisayara bulaşarak bilgisayarı zombi bilgisayar haline dönüştürebilmektedir. Virüsler veya solucanlar bilgisayara bulaştığı andan itibaren saatler içinde başka binlerce veya milyonlarca bilgisayara da bulaşarak çoğalabilir.

Zombi bilgisayarlar sayesinde büyük bir bilgisayar ordusu faaliyete geçmiş olacaktır. Kullanıcılar bilgisayarlarının bu kurulan bilgisayar ordusunun bir parçası olduğunu anlamayacaktır. Genel olarak kullanılan DDoS atakları veya saldırılarında kullanılan ataklar ise SYN Flood, UDP Flood, http Flood, DNS Flood'dur. DDoS atakları aslında alt yapı problemlerine işaret etmektedir. Alt yapının sağlam temeller üzerine oturtulması saldırılara karşı alınmış bir güvenlik önlemidir (Kara, 2013: 38).

Klasik savaşların sonrasında sessiz ve sinsice yapılan saldırılar masum gibi görünse de aslında çok tehlikeli ve yıkıcı etkileri bulunmaktadır. Siber saldırılara paralel olarak siber savaşlar ile birlikte insanların günlük yaşamlarını etkileyen ve yaşamlarını tehlike içerisine sürükleyen yıkıcı etkileri oluşmaktadır.

3.1.3. Virüs

Virüs, kişilerin bilgisi ve isteği dışında bilgisayarlarına yüklenen ve çalışan küçük ama etkili bir bilgisayar programı veya yazılım kodudur. Virüs terimi, kötü amaçla ve kendi kendini yöneten bilgisayar programlarının veya yazılımlarının eş anlamlısı olarak kullanılır. Kötü amaçlı oldukları ve bilgisayarlara zarar vererek hasta durumuna getirmeleri ve kendi kendini kopyalama aracıyla hızla yayıldıkları için virüs adıyla isimlendirilir. Web siteleri üzerinden bir dosyayı bilgisayara yüklerken, e-posta aracılığıyla gönderilen bir e-postanın eki yüklenirken, bir taşınabilir USB bellek, hafıza kartı vb. dijital medyalardan veri aktarımı veya kopyalama yapılırken virüs bulaşabilmektedir. Virüsler kodlanırken yani yazılırken yazılım içerisine başka yazılımlar gizlenmek suretiyle oluşturulurlar. Virüsler tek başlarına değil içerisindeki bulunan yazılımlarda aktif olarak çalışmaktadır. Bilgisayar virüsü, çalıştırıldığında aktif hale gelen zararlı bir programdır. Tarihte ilk ve yaygın olarak tanınan virüs, 1971'de bir akademik araştırmada ortaya çıkan "creeper" adındaki virüstür.

MacAfee sözlüğünde virüs şu şekilde tanımlanmaktadır. Virüs, genellikle kullanıcı bilgisi veya izni olmadan disklere veya başka dosyalara bağlanabilen ve kendini tekrar eden bir bilgisayar programı dosyasıdır. Bazı virüsler dosyalara yapışır, böylece virüslü dosya yürütüldüğünde virüs de çalışır. Bir virüsün yayılması, günümüzde bilgisa-

yarlar ağ üzerinden birbirine bağlı olduğundan ve internetteki birçok dosya paylaşıldığından çok yaygın olarak görülmektedir. Ne yazık ki, tüm bu ağ çevre kontrolleri, güvenlik önlemlerine rağmen bilgisayar sistemlerinde virüslerin zarar vermelerini engelleyememiştir. Virüsler, disketlere dağıtılmış (yani, çıkarılabilir medya, evrensel seri veri yolu USB) ve bunlar kurumsal ve devlet İnternet kullanıcılarına bildirilen web sitelerine yerleştirilmiştir. Virüs örnekleri, güvenlik belgelerini yasa uygulamalarına yardımcı olan, dijital kanıtları tanımlayan siber adli bilişim uzmanları tarafından analiz edilmiştir. Her virüs için, değiştirdiği her dosyayı ve geride bıraktığı günlük türlerini tanımlayarak "dijital imza" yaratılabildi. Sektöre ve hükümete sattıkları "antivirüs" yazılımı oluşturuldu. Antivirüs sağlayıcıları, müşterilerine, İnternet'te tanıtılan her yeni virüsle ilgili imzalarını güncel tutacaklarını taahhüt etmişlerdir. Hali hazırda binlerce veya milyonlarca dolaşan virüs olduğu için, şirketler tüm kullanıcılarının tüm PC'lerine virüsten koruma yazılımı kurma araçlarını çabucak tasarladılar.

Bununla birlikte antivirüs yazılımcıları tarafından virüsten korunma çözümlerinde özellikle virüs yeni bir virüsse, bunu tanıyıp yakalayamadığı görülmüştür. Ayrıca yeni virüs antivirüs yazılımı tarafından çıkarılacak olan yamada yeni yazılım yazılana kadar geçen süre içerisinde virüs bilgisayar ağları üzerinden tüm bilgisayar sistemlerine yayılacaktır. Yani, bu neredeyse her gün güncellenmesi gereken sürekli değişen bir sektör halini almıştır.

3.2. SİBER GÜVENLİK VE SİBER SAVAŞ TERİMLERİ

Teknolojinin gelişmesiyle birlikte bilgi-iletişim-teknoloji alanlarında birçok gelişme yaşanmaya başlamıştır. İnternetin ortaya çıkışı ve gelişimiyle birlikte bilgisayarların özelliklerinin giderek artması, bilgisayar donanımlarının küçülmeye başlamasıyla bilgisayarlarda küçülme yaşanmıştır. Bilgisayarların yanı sıra mobil cihazlarında gelişmeye başlaması ve mobil cihaz donanım yapılarının değişmesiyle hafıza kapasitelerinin artması, birçok uygulamanın kullanılması, internet hızının artması sonucu, mobil cihazlar giderek bilgisayarların yerini almaya başlamıştır. İnternet'in gelişmesine paralel olarak internet üzerinden sosyal paylaşım ağlarının kullanımı ile birlikte sosyal paylaşım siteleri ulusal sınırları aşmaya başlamıştır.

Bilgisayarların küçük ve taşınabilir hale gelmesi ve 21. yüzyılda internetin yaygınlaşması ile birlikte dünya üzerinde küresel olarak internetin gelişmesi ticari, siyasi,

askeri, alanlarda kullanılmaya başlamasıyla siber güvenlik problemleri ortaya çıkmaya başlamıştır (Ada, Çakır, 2017).

3.2.1. Tehdit

Tehdit; korku yaratma, insanın gözünü korkutma veya gözdağı verme anlamları kullanılarak Türk dil kurumu sözlüğünde yer almıştır. Türk Silahlı Kuvvetleri askeri terimler sözlüğünde ise, milli güvenliğe karşı her çeşit faaliyetler anlamında belirtilmiştir. Tehdit terimi ayrıca tehdit eden tarafın talepte bulunduğu ve tehdit eden tarafın taleplerinin yerine getirilmediğinde ise diğer tarafı cezalandırması şeklinde de ifade edilmektedir.

Devletlerin dünya üzerindeki jeopolitik konumları, tarihleri, hedefleri, doğal zenginlikleri, ulusal hedefleri ve güvenlik anlayışlarına göre tehdit algıları değişmektedir. Örneğin ABD'ye yapılan 11 Eylül saldırılarından sonra ABD ve Avrupa Birliği'nin tehdide bakış açıları büyük oranda aynı olsa da tehdide karşı stratejileri farklılaşmıştır. ABD ve AB'nin tehdide karşı farklı bakmasının nedenleri ise güvenlik anlayışlarının, yeteneklerinin ve tehdidi değerlendirme şekillerinin değişmesidir. Devletlerin tehdit veya risk izlenimleri, devletin idarecilerinin elinde olan güçle veya imkân ve kabiliyetlerine göre değişiklikler göstermektedir. Devletler için bu normal bakış açısıdır (Küçükşahin, Akkan, 2007: 46-47).

Tehdit terimi ve kavramından anlaşıldığı üzere tehdit aynı zamanda siber dünya üzerinde de geçerliliğini sürdürmektedir. Uluslararası alanda ülkelerin birbirlerine yönelik tehditleri, internet üzerinden birbirlerine saldırma, casusluk faaliyetleri, sistemleri kullanılamaz hale getirme ve bilgi hırsızlığı vb. şekilde gerçekleştirilmektedir.

Siber tehditlere örnek verecek olursak ABD'de görülen "NIMDA" isimli saldırı, kritik altyapılarda yıkıcı bir tahribat olmamasına rağmen, siber saldırılardaki teknik gelişmeyi göstermesi açısından iyi bir örnektir. Ayrıca NIMDA, bu organize saldırganların kendilerini kabul ettirmeleri ve gerekli silahlara sahip olduklarını göstermeleri bakımında da dikkat çekicidir. NIMDA, bilgisayar solucan ve virüsünün karışımı olan bir otomatik siber saldırı olarak tasarlanmıştır. İnanılmaz bir hızla yayılmış, bilgisayar sistemlerine bulaşmak için çeşitli yollar denemiştir. Erişim kazanana ve dosyaları yok edene kadar işgali sürdürmüş, bir saat içinde tüm ülke çapına yayılmış, günlerce devam etmiş ve 86000 bilgisayara saldırıda bulunmuştur (Yılmaz ve Salcan, 2008: 35-43).

3.2.2. Siber uzay, siber ortam, siber savaş ve siber güvenlik

Herhangi bir devletin, başka bir devletin bilgisayar sistemlerine veya ağlarına hasar vermek ya da kesintiye uğratmak amacıyla yapılan sızma faaliyetine siber savaş denilmektedir. Siber savaş terimini açacak olursak, siber terimi 'sibernetik' kökünden gelmektedir. Sibernetik 1958 yılında canlılar ve makineler arasındaki iletişimi inceleyen bir bilim dalı olarak adını almıştır. Siber savaş İngilizce "cyber war" kelimesinden türeyerek dilimize çevrilerek yerini almıştır. Siber kelimesi İngilizce "cyber" ismine tekâmül etmekte ve "war" savaş anlamına gelmektedir (Yayla, 2013: 180).

Bilişim ve siber kavramları genellikle aynı anlamlarda kullanılmaktadır. Bilişim kavramından da bahsetmemiz gerekirse insanların teknik, ekonomik ve toplumsal iletişimlerinde kullandıkları ve bilimin dayanağı olan bilginin, düzenli ve akla uygun bir biçimde, özellikle bilgisayarlar vb. elektronik cihazlar aracılığıyla işlenmesidir. Bilişim, teknoloji ile bilgi kullanılarak üretilen ya da ortaya çıkan sonuçlar olarak da tanımlanabilir. Her türlü bilgisayar donanımı ve her çeşit yazılım ya da uygulama bilişimin bir parçasıdır. Sonuç olarak "bilişim", "siber" kavramından farklı bir anlamına işaret etmektedir. Bilişim ve siber kavramları çoğu yerde birbirinin yerine kullanılsa da, çok belirgin olmayan bir şekilde, "siber" kavramı ağ üzerinde elektronik sistemlerin bulunduğu ortam olarak görülmekteyken "bilişim" bu ortam vasıtasıyla bilgi üretilmesi anlamına gelmektedir. Siber uzay kavramı İngilizce de "cyberspace" olarak kullanılmakta ve Türkçe de ise siber ortam olarak adlandırılmaktadır. William Gibson'ın yazmış olduğu "Neuromancer" adlı kitabında siber uzay'ın bilgilerin elektromanyetik dosyada oluşturulması ile dünyanın her yanına farklı sistemler aracılığıyla dağıtılması ve bilgiye erişim sağlanılan sanal ortamların bütünü olarak tanımlanmıştır (Çakmak ve Altunok, 2009: 25-26).

Siber uzay BM'nin terimler sözlüğünde; internette, haberleşme altyapısına çevrimiçi (online) kuruluşlara, bilgi depolayan ve işleme cihazlarına karşılık gelen küresel bir sistem olarak adlandırılırken, ABD Savunma Bakanlığı'nın askeri terimler sözlüğünde; internet, telekomünikasyon ağları, bilgisayar sistemleri, gömülü işlemci ve kontrol sistemleri gibi birbirine bağlı teknoloji altyapılarını kapsayan ortam olarak tanımlanmaktadır. Fazla sayıda ve gün geçtikçe genişleyen her biri farklı sayısal iletişim yöntemleri sağlayan uzayların birleşmesidir. Siber uzay'ın sınırları belli olmayan ve ağ şeklindeki yapısı dünya üzerindeki herhangi bir devletin veya herhangi bir hukuk düzeni ile

tek egemenlikleri bünyesinde barındırmasına engel teşkil etmekte ve aynı zamanda hangi hareketlerin siber suç oluşturduğunun tanımını zor kılmaktadır. Yurttaşlık veya ulus benzeri kavramların çok da anlam taşımadığı siber uzayda, siber uzayın dünyadaki diğer devletler tarafından hukuk kuralları oluşturma ve bu kuralların uygulanmasının sağlam temeller üzerine atılmasına gereksinim duyulmuştur. Siber uzayın yeni bir hukuk alanı olarak ortaya çıkmasıyla birlikte en önemli problem hukuk kurallarının kimin tarafından hazırlanacağı ve uygulamasının ne şekilde olacağıdır. Siber uzay dijital bir dünyayı gösteriyorsa da her ülkenin ulusal alanlarını işgal edebilmektedir. Devletler geçmişten günümüze kadar hukuk kuralları ile yönetiliyor olmasına rağmen siber uzayın yapısından dolayı bu hukuk kuralları ile yönetilmesini zorlaştırmaktadır (Yayla, 2013: 181).

Savaş insanlık tarihi kadar eskidir. Ülkeler menfaatlerini korumak ve bulundukları alanları genişletmek için silahlı ordular kurmuşlardır. Devlet yöneticileri iktidarlarını elinde tutmak ve güçlendirmek için silahlı güç kullanmaktan hiç bir zaman çekinmemişlerdir. Uluslararası düzenin ilk konusu devletler açısından savaşa gereksinim duyulmasının temel amacı ulus olarak çıkarlarının korunmasıdır. Savaşı tanımlarsak savaş, devletlerin aralarındaki ekonomik ve siyasal anlaşmazlıklar vb. nedenlerle siyasal ilişkilerini keserek, birbirleri ile silahlı ordularıyla karşı karşıya kaldıkları silahlı eylemlerdir. Uluslararası hukuk alanında ise savaşın tam anlamıyla tanımı belirtilmemiştir. Bunun en önemli nedeni ise devletler arasında oluşan silahlı eylemlerin savaş olup olmayacağı konusunun hukuk alanında objektif şekilde belirtilmemiş olmasıdır. Bu nedenle devletler arasında oluşan silahlı eylemlerin savaş olup olmayacağı konusundaki temel ölçüt savaşa katılan taraflardan birinin savaş amacıyla hareket etmesidir. Savaş bir toplumun, bir ulusun veya devletin isteklerini diğer bir ulus veya devlete zorla kabul ettirmesi amacıyla gerçekleştirdiği bir mücadele olarak tanımlanabilir. Devletler arasında uluslararası hukuk kurallarına uygun olarak yürütülen silahlı bir çatışma olarak da tanımlanmaktadır. İnsanlığın tarihinden itibaren devletlerin silahlı güç kullanmak istemesinin haklı bir nedene dayanması büyük bir önem taşımıştır. Devletlerin uluslararası hukukta savaşa başvurmasının yasaklanmasıyla beraber, devletler silahlı güç kullanma haklarından hiçbir zaman vazgeçmiş değildir. İnsanlık tarihiyle birlikte toplumlar farklı özellikleri olan iki alanda savaşmışlardır. Bu alanlar önce "kara" ve "deniz" savaşları olmuştur. İnsan gökyüzünde uçma arzusuyla çalışmaya başlamış ve 1900'lu yıllardan sonra uçakların icat edilmesiyle birlikte hava teknolojisinde büyük gelişmeler ortaya çıkmış-

tır. Böylelikle üçüncü savaş ortamı yani "gökyüzü" oluşmuştur. 1957 yılından itibaren yavaş yavaş dördüncü savaş ortamı "uzay" olarak kabul edilmeye başlanılmıştır. 1980'li yıllardan sonra internetin ortaya çıkarak gelişmesiyle birlikte 21.yüzyıla gelindiğinde beşinci bir savaş ortamı "siber savaş" bunlara eklenmiştir (Yayla, 2013: 182-183).

Dünya genelinde bütün devletlerin bilgilerini, örneğin sağlık bilgileri, vatandaşlarına ait özel ve kişisel bilgilerini, bankacılık, gayrimenkul, haberleşme vb. bilgilerinin depolandığı ve işlendiği, cihazların siber ortamlarda bulunması ve yönetilmesiyle birlikte beşinci savaş ortamı olan siber ortamda bilgi güvenliği ön plana çıkmaktadır. Siber ortamda devletlerarası savunma strateji ve taktikleri her geçen gün teknolojinin gelişmesine paralel olarak geliştirilmeli ve yeni çözümler bulunmalıdır. Uluslararası ilişkilerde devletlerarası sorunların çözülmesinde orduların caydırıcı bir güç olması yanında siber ordularında caydırıcı bir güç olarak kullanılmasının bir zorunluluk halini aldığı bir zaman oluşmuştur.

20. yüzyıldan itibaren bilgisayarın icat edilmesiyle birlikte yavaş yavaş oluşmaya başlayan siber alan, 21. yüzyıldan itibaren bütün alanları etkiler hale gelmiştir. Bilgisayarın ortaya çıkması ve gelişmesi ile birlikte bilgisayarların yarattığı siber alana, günümüzde sağlık hizmetleri, bankacılık işlemleri, haberleşme ve elektronik devlet hizmetleri ile birlikte bağımlı hale gelinmiştir. Siber alanın gelişmesine paralel olarak uluslararası ilişkilerde bu konunun ele alınması bir zorunluluk halini almıştır (Kurnaz, 2016: 57).

ABD'ne 11 Eylül 2001 tarihinde yapılan terör saldırısı ile tehdit konusundaki geleneksel görüş yıkılmıştır. Yıllarca dünyaya hâkim olan Soğuk Savaş senaryosu değişmiştir. Tehdidin herhangi bir adresinin olmadığı, devletlerin toprak bütünlüklerinin yanı sıra mekân ve zaman kurallarının da anlaşılmaz bir şekle dönüştüğü görülmüştür. Sivil bir uçağın terör örgütü tarafından saldırı aracı olarak kullanılmasıyla birlikte her şeyin her an silaha dönüşerek zarar verebileceğine dikkat çekerek hiçbir şeyin imkânsız olmadığı açık şekilde görülmüştür. Siber saldırı ve tehditler ile bu durum oluşabilmektedir. Teknoloji ile birlikte yeni gelişmelerin ortaya çıkmasıyla siber uzaydaki siber ortamdaki faaliyetler devletleri tehdit etmekte ve bu tehditlerin en yıkıcısı ve önemlisi siber savaşlar olarak görülmektedir (Yayla, 2013: 184).

Siber güvenlik, siber tehdit, siber savaş vb. kavramlar 21. yüzyılda çok hızla gelişmiştir ve gelişmeye de hızla devam etmektedir. Bilişim ve teknolojideki hızlı gelişmelere paralel şekilde yeni kavramlarda hızlı bir şekilde üretilip çoğalmaktadır. İnternet üzerinden, internet ağları kullanılarak oluşan tehditler ise birbirlerinden farklıdır. İnter-

net ağları kullanılarak ağ ve şebeke trafiğinin dinlenilmesi, casus yazılımlar, istenmeyen e-postalar, virüsler, solucanlar, sistemleri servis dışı bırakma, botnet bilgisayarlar (köle anlamında) vb. siber ortamdaki siber saldırı araçlarıdır. Joseph Nye'a göre ulusların veya devletlerin siber güvenliğine ilişkin ana tehditler; ülkelerin birbirlerine karşı yapabilecekleri siber tehditler, diğer ülkeler veya farklı aktörler tarafından yapılabilecek tehditlerdir. Ayrıca siber savaş ortamında özellikle ülkeler ekonomik amaçlı ve istihbarat amaçlı tehditler ile karşı karşıya kalmaktadırlar. Ağ sistemleri aracılığıyla siber savaş, siber suçlar ve siber terörizm ise diğer aktörler tarafından gelmektedir (Kurnaz, 2016: 58).

Siber uzay tanımında da bahsettiğimiz gibi siber uzay çok karmaşık bir kavram olup kendine ait farklı özellikler barındırmaktadır. Siber güvenlik ile güvenlik bütün devletler açısından ön plana çıkan bir alan haline gelmiştir. Siber güvenlik için siber ortamdaki her türlü bilgi, belge vb. verilerin üretilmesi, depolanması, kullanılabilir olması ve gerektiği zamanda her an erişilebilir olması gerekmektedir. Bu açıdan bakıldığında genel olarak siber ortamda siber güvenlik, kurum, kuruluş ve toplumdaki kullanıcıların devamlılıklarını sağlamak amacıyla; siber güvenlik araçları, güvenlik kavramları, izlenecek politikalar, risk analizleri, diğer alanlardaki faaliyetler, eğitimler ve teknolojinin tamamı kapsayacak şekilde tanımlanabilir. Siber güvenlik alanında hedeflere ulaşabilmek için güvenlik alanında belirli kriter ve özelliklerin sağlanması gerekmektedir. Bu kriterler; verilere erişebilme, verilerin gizliliği, verilerin doğruluğu, verilerin bütünlüğü, verilerin güvenilirliği, verilerin tutarlılığı, verilerin sürekliliği ve verilerin ölçülebilirliği olmalıdır. Devletler açısından bilgi, belge ve verilerin sahip olduğu bu özellikler nedeniyle bilişim sistemlerinin alt yapısının açıklarından yararlanılarak yapılacak olan siber saldırılar sonucunda sistemlere büyük hasar verebilecek ve devletleri içinden çıkamayacakları kaos ortamlarına sürükleyecek ya da zor durumda bırakacaktır (Kurnaz, 2016: 58).

3.2.3. Estonya siber saldırısı (28 Nisan – 23 Mayıs 2007)

Estonya dünya üzerinde internet sistemini çevrimiçi (online) olarak kullanan devletlerin ön sıralarında yer almaktadır. Sovyetler Birliği'nin Soğuk Savaş dönemlerinde Estonya en önemli bilişim merkezlerinden biri olmuştur. Soğuk Savaşın sona ermesinin ardından Estonya bağımsızlığını kazanarak bağımsız bir devlet olduğunda, Rusya her zaman bu ülke ile arasındaki birlikteliği kuvvetli tutmaya çalışmıştır. Estonya NA-

TO'nun Prag zirvesine 2002 yılında katılarak üyelik müzakerelerine başlamış ve 2004 yılında NATO'ya üye olmuştur. Bunun sonucunda Rusya ile arasındaki birliktelik zayıflamış ve azalmıştır. Estonya ile Rusya arasındaki zayıflayan ilişkiler 2007 yılında ayrılma noktasına gelmiştir (http-12, Boyraz, E.T: 17.03.2018).

Sovyetler Birliği'nin dağılmasına müteakiben Rusya Federasyonu (RF) kurulmuştur. Rusya ile Estonya'nın bağının zayıflaması ile birlikte Estonya'nın Başkenti Tallinn'de bulunan ve SSCB döneminden kalan Bronz Asker Heykeli (Bronze Soldier Monument)'ni Estonya yöneticilerinin askeri mezarlığa taşımak istemelerine Rusya çok büyük bir tepki göstermiştir. Bununla kalmayıp 27 Nisan gece saatlerinden itibaren Estonya Devletinin bilişim sistemlerine siber saldırıda bulunarak bilişim sistemlerini devre dışı bırakmıştır. Rus devleti ve Estonya'lı Ruslar dünya genelinde aldıkları destekle hareket ederek dünya'nın birçok farklı noktasından siber saldırılarına yaklaşık bir ay süresince devam etmişlerdir. NATO'nun müttefiki Estonya'ya bir ay boyunca maruz kaldıkları siber saldırılarda NATO hazırlıklı olmaması nedeniyle anlık destek sağlayamamıştır. Yapılan bu siber saldırılar ile bir devletin kritik alt yapı sistemlerinin internet üzerinden gelebilecek siber tehditlere karşı ne kadar açık olabileceği ortaya çıkmıştır. Estonya tarafından bu siber tehdidin hayati bir öneme haiz olmasının nedeni ise devletin kamu kurum ve kuruluşlarının faaliyetlerinin ve özel sektörün faaliyetlerinin hepsinin internet vasıtasıyla yürütülüyor olmasıdır (http-12, Boyraz, E.T: 17.03.2018).

3.2.4. Gürcistan siber saldırısı (01 Ağustos – 01 Eylül 2008)

Estonya'ya devletine karşı 2007 yılında yapılan siber saldırının ardından bir yıl sonra 2008 yılında Gürcistan'ın bilişim sistemlerinin kritik alt yapısındaki açıklıklar kullanılarak aynı tarzda bir saldırı gerçekleştirilmiştir. DDOS (Distributed Denial of Service) dağınık servis dışı bırakma atakları ile sistem engellenerek durdurtmuştur. Siber saldırılar Gürcistan devletine karşı sadece Rusya devletinden değil dünyanın birçok ülkesinden eş zamanlı olarak gerçekleştirilmiştir. Gürcistan devleti bir NATO üyesi olmaması sebebiyle NATO tarafından anında yardım sağlayamamıştır. Siber saldırılan yoğun şekilde devam etmesi üzerine Estonya devletinin çabaları ile NATO da saldırıyı engellemek üzere Gürcistan devletine uzman göndermiştir.

Gürcistan'a gelen uzmanların katkılarıyla yoğun şekilde ve uzun süredir devam eden siber saldırılar engellenmiştir. Engellenen siber saldırıların bilişim sisteminin kritik alt yapılarına vermiş olduğu zarar ancak yakın zamanda normal şekline getirilmiştir.

Devletleri etkisi altına aldığı bu siber saldırılar sonucunda NATO tarafından 2010 yılında Lizbon zirvesinin siber güvenliğe ilişkin konu başlıkları ortaya çıkmıştır (http-12, Boyraz, E.T: 17.03.2018).

Bu yapılan siber saldırılar birbirinden farklı olsa da bu iki devlet, Rusya tarafından deneme tahtası olarak kullanılmıştır. Rusya bu iki devlete karşı yapmış olduğu siber saldırılar ile kamu kurum kuruluşları, özel sektör, ekonomi sektörü ve basın yayın kuruşlarının dünya ile bağlarının bir aya yakın süre ile aksamasına neden olmuştur. Başarılı olan bu siber saldırıları Rusya devleti kabul etmese de saldırıya uğrayan iki ülke bu siber saldırıların Rusya tarafından yapıldığını belirtmektedir. Estonya ve daha sonra Gürcistan'a karşı yapılan bu siber saldırılar sonucunda NATO tarafından 2008 yılı içerisinde Estonya'nın başkenti Talin şehrinde siber savunma merkezi kurularak faaliyete geçirilmiştir. Bu yaşanan siber saldırılar neticesinde ABD Savunma Bakanlığı da kendilerinin enerji boru hatlarına, basın yayın kuruluşlarına ve füze sistemlerine karşı yapılacak siber saldırıları savaş nedeni olarak kabul edeceğini ve klasik savaş kurallarıyla hareket edeceklerini söylemiştir. NATO üyesi olan Estonya'ya karşı yapılan siber saldırı ya da siber savaş ABD hükümetini çok kızdırmıştır. ABD hükümeti buna karşılık Rusya hükümeti için büyük önem taşıyan bir devlet olan İran'ı hedef alarak bu devletten intikam almak istemiştir. Rusya, İran nükleer programına mühendisleriyle destek vermiştir. ABD hükümeti İran nükleer tesislerini hedef alarak kendi kendine kopyalanarak çoğalabilen Stuxnet (solucan) yazılımını kullandı. Bu yazılım motorları ve sıcaklıkları kontrolü altına alarak merkezi ana kontrol birimi olan PLC'yi yani fabrika ve üretim tesislerindeki makinelerin kontrolü vb. işlevlerin yerine getirilmesini sağlayan özel bilgisayarı ele geçirdi. PLC'yi ele geçirmesiyle birlikte özel bilgisayarda çalışan diğer yazılımları da teker teker etkisiz hale getirmiştir. İran nükleer tesislerinin ele geçirilmesiyle nükleer yakıt zenginleştirme tesislerinin santrifüjlerinin kontrolsüz bir şekilde hızla dönmeye başlamasıyla tesise ciddi zararlar verdi. ABD hükümeti tarafından yapılan siber saldırıyı İran devleti tam olarak anlayamasa da daha sonra olayın ciddiyetini anladı ve İran hükümeti yöneticileri siber saldırıya uğradıklarını belirtmiştir (http-13, 6……, E.T: 18.03.2018).

John Arquilla tarafından enformasyon savaşları deyimi ortaya sürülmüştür. Teknolojinin gelişmesiyle birlikte kitlesel olarak siber saldırıların ya da siber savaşların yıkıcı etkilerinin yüksek olması yanısıra Stuxnet saldırısıyla sadece enformatik değil fiziki zararların da olabileceği görülmüştür. Siber saldırlar ile bir devletin elektrik şebe-

kelerinden trafik ışık sistemine kadar her şeyi durdurmak mümkündür. Stuxnet yazılımının farklı olmasını sağlayan en önemli unsur internet üzerinden sadece ağ sistemlerine bağlı bilgisayarları değil herhangi bir dijital cihaza veri girişi yapılabilen USB, CD, DVD, hafıza kartı vb. dijital cihazlarda kullanılarak bilgisayarları ele geçirerek kullanabilmesidir. İran'a yapılan bu saldırı sonucu 62.867 adet bilgisayara Stuxnet solucanı bulaştırılmıştır (http-13, 6……, E.T: 18.03.2018).

Dünya devletleri klasik savaş yöntemleri kullanıldığında ülkelerine ne gibi etkileri olacağını kestirebilmektedirler. Fakat siber savaşlarda menzilin veya mekânın ne olacağını kestirmeleri çok zordur. Stuxnet (solucan)'in hızla yayılma yeteneği ile bu solucan sadece İran ile sınırlı kalmayıp Avusturya'dan Kuzey Amerika'ya kadar büyük bir alanda etkili olmuştur. Stuxnet (solucan)'ı dünyadaki yeni savaş düzeni olan siber savaşları açıkça ortaya çıkartarak tüm dünyaya duyurmuştur. Bu yeni savaş düzeninde sadece iyi bir orduya sahip olmak yeterli gelmemektedir. Enformasyon ve bilgisayarların güçleri ülkeleri içine alabilecek kadar güçlü olmuştur. Teknoloji ile birlikte gelecekte siber savaşlara karşı siber ordular kurulması gerekliliği ortaya çıkacağı aşikârdır (http-13, 6……, E.T: 18.03.2018).

Siber güvenlik açısından güvenliğin tam anlamıyla sağlanabilmesi bilişim sistemlerindeki kritik altyapılar da bulunan uygulama ve yazılımların tamamının korunmasıyla mümkündür. Güvenliğin sağlanması için verilerin gizliliği, kontrolü, bütünlüğü, erişilebilirliği ve doğruluğu tesis edilmelidir. Ülkelerin siber tehdit ya da siber savaş ile karşı karşıya kaldıkları saldırıların boyutlarına bakıldığında bilişim sistemlerinin durdurulması, engellenmesi, verilerin yok edilmesi, verilerin şifrelenmesi, verilerin değiştirilmesi, verilerin ifşa edilmesi ile siber güvenliğin hassas noktaları ortaya çıkmıştır. Siber güvenliğin en önemli faktörleri ve devletlerin korumak zorunda oldukları bilginin gizliliği (bilişim sistemleri üzerinde bulunan verilerin gizliliğinin korunması), bütünlüğü (bilişim sistemleri içerisinde barındırdıkları verinin bütünlüğünün sağlanılması ve bilişim sistemleri üzerinden gönderilen, alınan, paylaşılan, depolanan verilerin hiçbir hasara uğramadan noksansız olarak depolanmasıdır) ve erişilebilirliğinin (verinin her zaman gereksinim olduğunda hazır bulunması ve herhangi bir saldırı karşısında işlevsel olmasıdır) sağlanması gereklidir. Bu açıdan bakıldığında siber tehdit veya saldırılara karşı, siber güvenliğin sağlanılması için bilişim sistemlerinin kritik altyapılarının açıklarının en alt seviyeye indirilmesi amaçlanmaktadır (Kurnaz, 2016: 58).

3.2.5. Siber terörizm

Terörizm kısaca; ulusal ya da uluslararası alanda ülkelere yönelik sert güç kullanarak (askeri, ekonomik, siyasi) gerçekleştirilemeyen hedeflerin baskı, korku ve cebir yoluyla, belli bir ideolojik temele dayanan ve asimetrik savaş yöntemlerinin planlı olarak hedef ülkeye karşı uygulanmasıdır. Siber terörizm terimi son yıllarda uluslar arası güvenlik sistemine dâhil edilen yeni bir tehdit unsurudur. Bu yeni tehdit unsurunun uluslararası sistemde halen tartışması devam etmektedir. Terör eylemlerindeki özelliklerin siber saldırılarda da benzer nitelikte görülüp görülmediği hususu ile sonuçlarındaki etkiler sürekli olarak karşılaştırılmaktadır. Aslında bu karmaşanın bir diğer sebebi de kavramların tanımlarının ve özelliklerinin değişen koşullar altında güncellenmesinde yatmaktadır. Çünkü klasik anlamda terörizm kavramı güncel şartlarda ve gelişen teknolojiyle daha da karmaşık bir yapıya dönüşmüştür. Uluslararası terör örgütlerinin ortaya çıkması ve sayılarının artması, kullandıkları yöntemlerin çeşitliliği, eylemlerin zaman ve mekânlarının öngörülememesi, gelişen teknolojinin terör örgütlerine sağladığı avantajlar, terörizm kavramının da yapısını değiştirmiştir. Artık terör örgütlerinin bilişim sistemlerini kullanabilme yeteneğine sahip oldukları rahatlıkla görülmektedir. Bu açıdan bakıldığında siber terörizm olgusu, hedef ülkenin bilişim sistemlerini etkisiz hale getirmek, altyapı faaliyetlerini bozmak, ekonomik tesislerine internet tabanlı sabotajlar düzenlemek, vatandaşların kişisel bilgilerini ele geçirerek toplumda korku yaratmak ve huzuru bozmak şeklindeki eylemler olarak tanımlanmaktadır. Vatandaşların bireysel yaşamlarını tehdit eden bu saldırılar aynı zamanda ülkelerin toplumsal yapısını da etkilemekte, ülke genelinde büyük infiallerle yol açabilecek gelişmelere de sebep olmaktadır. Siber terörizm her anlamda vatandaş ve devlet güvenliği için büyük bir tehdit oluşturmaktadır. Uluslararası sistemin güvenlik algısı siber terörizm olgusuyla yeniden değişim sürecine girmiştir. Siber tehdit unsurlarının terör örgütleri tarafından da kullanılmaya başlaması ülkeleri yeni stratejiler belirlemeye ve daha fazla tedbir almaya itmektedir (Güntay, 2017: 88).

Siber terörizm doğal olarak kaynağını siber tehdit unsurlarından sağlamaktadır. Dolayısıyla teknolojik gelişmeler ve bilişim sistemlerindeki her atılım, terör örgütleri tarafından birer tehdit ve saldırı unsuruna dönüştürülmektedir. Bilişim sistemlerinin imkânlarını kullanarak daha az maliyetli saldırılar gerçekleştirmek terör örgütlerine cazip gelmektedir. Ayrıca terör örgütleri sadece saldırı nitelikli eylemlerde değil, propaganda amacıyla da siber yeteneklerini kullanmaktadırlar. İnternetin ve sosyal medya

uygulamalarının hızla yayılması neticesinde bu örgütler, bahse konu uygulamaların alt-yapılarına yaptıkları saldırılar ile hem ideolojilerini geniş mecralara taşımak hem de kendi örgütlerinin propagandasını yapmaktadırlar. Bu açıdan incelendiğinde siber terörizm, ülkenin birlik ve bütünlüğünü birinci derecede etkileyen bir tehdit haline gelmektedir. Siber terörizm, maliyet açısından küçük fakat yarattığı etki açısından büyük çaplı güvenlik sorunları yaratmaktadır. Bazı örnekleri; sosyal medya uygulamaları kullanılarak ayrılıkçı kesimler tetiklenip bir ayaklanma girişimi başlatmak, ekonomik tesisleri sabote edip ülke mali sistemini çökertmek, gizli bilgilerin ifşa edilmesiyle toplumda infial oluşturmak, kamu kurum ve kuruluşlarının savunma sistemlerini etkisiz hale getirmek şeklinde saymak mümkündür. Siber terörizm saldırılarına karşı her türlü tedbir alınmalıdır. Ufak bir tehdit bile öngörülemeyecek hasarlara sebep olabilme özelliğine sahiptir. Tüm bu hususlar göz önüne alındığında siber terörizmin önemi ortaya çıkmaktadır. Sadece ülkeler özelinde değil uluslararası sistemin de güvenliğini tehdit etmektedir. Çünkü terörle mücadelede klasik yöntem değişmiştir. Silahlı mücadele devam ederken yeni bir çatışma ortamı daha oluşmuştur: siber ortam. Siber terörizm devletler açısından dikkatle ele alınması gereken bir konudur. Devletler bilişim sistemlerinin kullanıldığı her kurum, kuruluş ve özel şirketi ulusal bir stratejiyle tek bir çatı altında toplamalı ve ortak bir savunma planıyla işbirliği içerisinde çalışan siber güvenlik alanı yaratmalıdır. Her birimin kendine has ayrı bir siber güvenlik sisteminin olması sağlanmalı, bu sistemler de ülkenin genel siber savunma sistemine entegre edilerek bir çatı savunma oluşturulmalı, genel siber savunma sisteminin de profesyonel ekiplerin çalıştığı tek bir merkezden kontrol edilerek işlevsel halde tutulması gerekmektedir (Güntay, 2017: 88).

3.3. Siber Savaş Silahlarına Karşı Kritik Alt Yapının Korunması

Siber güvenlik, teknoloji ile birlikte bilişim sistemlerinin giderek yaygınlaşması ticari, politik, askeri vb. alanlarda farklı bir yöntem şeklinde uygulanması sonucunda ülkelerin güvenliği için yeni bir algı alanı yaratmıştır. Bilişim sistemlerini etkileyen siber tehdit unsurları hem vatandaşların hayatını hem de ülkenin güvenliğini tehlikeye atmaktadır. Örnek verilecek olursa, bankaların internet şubeleri aracığıyla internet üzerinden işlem yapan kişinin hesaplarında bir dolandırıcılık olayının meydana gelmesi sadece ilgili şahsın mali durumuna etki ederken; devletin bir biriminin bilgi sistemine yapılan saldırılar bütün birim çalışanlarını, bu birimle ilişkili kişilerin şahsi bilgileri

veya kredi kartı bilgileri gibi verilerin kötü niyetli kişiler tarafından kullanılmasına imkân sağlamaktadır.

Ülkenin ulusal güvenliğini ilgilendiren gizlilik derecesindeki belgelerin ya da verilerin başka ülkeler ya da şahıslarca elde edilmesi, ilgili ülkenin bütün hassas noktalarının bilinmesine ve güvenliğinin sorgulanmasına sebep teşkil edecektir. Siber tehdit unsurlarının artması, devletleri kendi güvenliklerini gözden geçirmeye ve yeni bir savunma stratejisi oluşturmaya sevk etmiştir. İkiz kulelere yapılan terör saldırısı sonrasında ABD kritik bir adım atmıştır. ABD'nin kendi ülkesi için hazırladığı ve uygulamaya koyduğu 'Siber Uzayın Güvenliği İçin Strateji Belgesi' uluslararası güvenlik sistemine siber güvenlik kapsamında yön göstermiştir. Bu belge ABD'nin siber güvenlik ihtiyaçları göz önüne alınarak oluşturulmuştur. Belgede kısaca;

a. Ülkenin bilişim sistemi altyapısını hedef alan siber tehditleri engellemek,

b. Siber güvenlik sisteminin eksik yönlerini tamamlamak,

c. Siber saldırılar sonrasında meydana gelebilecek zararları ve zararların düzeltme işlem sürelerini azaltmak, gibi konular temel alınmıştır.

Teknolojik gelişmeler neticesinde açığa çıkan siber tehditler karşısında ülkelerin güvenlik ihtiyaçlarının karşılanması ve menfaatlerinin devam ettirilmesi kapsamında önemli sıkıntılar yaşanmıştır. Bu sorunlardan yola çıkarak ülkelerin siber güvenlik konusunda uluslararası alanda bazı işbirliği faaliyetleri içine girmesi ve anlaşmalar düzenlemesi ihtiyaç haline gelmiştir. Siber saldırılara karşı ulusal çıkarların korunması ve siber uzayın sınır güvenliğinin sağlanması hususunda karşılaşılan zorluklar, devletlerin uluslararası anlaşmalar yapmasını kaçınılmaz hale getirmiştir. NATO yapılan bu çalışmalarda yerini almış ve oluşturduğu bazı kurumlarla müttefiklerinin güvenlik ihtiyaçlarını karşılamaya çalışmıştır. Kurduğu CCDCOE (NATO Cooperative Cyber Defence Center of Excellence-NATO Müşterek Siber Savunma Mükemmelliyet Merkezi) makamıyla üye ülkelerin siber tehditler karşısında güvenliğini sağlamakta ve siber güvenlik konusunda önemli faaliyetler icra etmektedir (Ada ve Çakır, 2017: 633).

Bilişim sistemlerinin içinde depolanan belge ve bilgilerin güvenli bir şekilde muhafaza edilmesi önem arz etmektedir. Söz konusu verilerin ele geçirilmesi hem vatandaşların hem de ülkenin genel güvenliğini tehlikeye düşürecektir. Ülkenin kurumları tarafından kullanılan bilişim sistemleri sayesinde altyapı hizmetleri yürütülmektedir. Enerji nakil sistemi, ulaştırma sistemi, eğitim sistemi, sağlık sistemi ve en önemlisi savunma sistemi bilişim sistemi unsurlarından faydalanmaktadır. Dolayısıyla ülkenin kri-

tik altyapı faaliyetlerinin çoğu bilişim sistemleri kullanılarak gerçekleştirilmektedir. Bundan dolayı siber tehdit unsurları ülkenin her kurumunu ve her alanını yakından ilgilendirmektedir. Kamu güvenliğinin ve toplumsal huzurun sağlanması için tüm altyapı sistemlerinin doğru, güçlü, güncel ve işlevsel bir siber güvenlik stratejisi ile desteklenmesi gerekmektedir (http-14, 7……, E.T: 19.03.2018).

Kritik altyapılar konusunda farklı değerlendirmeler yapılsa da ülkeler için önemi açısından varılan nokta aynı olmuştur. Uluslararası sistem içerisinde gerçekleştirilen siber saldırılara bakıldığında göze çarpan ortak nokta, tamamına yakınının altyapı sistemlerine karşı yapılmış olmasıdır. Devletlerin bu sistemlerinin saldırı odağı seçilmesinin amacı hedef devlete büyük zararlar vermektir. Kritik altyapı sistemleri bünyesinde çok sayıda bilişim sistemi unsuru barındırmaktadır. Aslında verilen hizmet dâhilindeki bilişim sistemi unsurlarının tamamına yakını bu altyapıyı oluşturmaktadır. Örnek verecek olursak; askeri birliklerin kullandığı iletişim ve silah sistemleri, kamusal hizmet sistemleri, ulaştırma ve havacılık sistemleri, enerji üretim ve nakil sistemleri, iletişim sistemleri, sağlık hizmeti sitemleri, ekonomik tesislerin işletim sistemleri, borsa, temiz ve atık su şebeke sistemleri, karayolları sinyalizasyon sistemleri, eğitim sistemleri, bankacılık sistemleri vb. olarak saymak mümkündür. Bu altyapı sistemlerinin işletilmesi ve denetimi aşamasında doğal olarak hem bilişim sistemlerinden hem de internet sisteminden aktif olarak faydalanılmaktadır. Dolayısıyla bilişim sistemlerini etkileyen her siber tehdit unsuru bu altyapı sistemlerini de rahatlıkla etkileyebilmektedir. Terör örgütlerinin ve düşman devletlerin stratejik ve taktik hedeflerinde her zaman hedef ülkenin kritik altyapısını ele geçirmek ya da çökertmek üzerine çalışmalar yapılmıştır. Çünkü hedef ülkede anarşi yaratmanın en kolay ve en ucuz yolu altyapı sistemini çökerterek ülkeyi savunmasız bırakmaktır. Ülkenin tamamının ya da belli bir bölgesinin enerji nakil sistemini çökertme, içme suyu sistemini sabote ederek vatandaşları susuz bırakma, iletişim sistemini kontrol ederek yasadışı dinleme yapmak ya da iletişim sistemini felç etme, trafik sinyalizasyon sistemini ele geçirerek büyük çapta kazalara sebep olma, sağlık sistemini destekleyen bilişim unsurlarına sızarak vatandaşların gizli bilgilerini çalma ya da sistemin çalışmasını engelleyerek vatandaşların ölümüne sebep olma, ülkenin silah sistemlerinin bir kısmının kontrolünü ele geçirerek aynı ülke ya da farklı ülkeye karşı uygulamak suretiyle çatışma ortamı yaratma gibi senaryolar günümüzde tahminden öteye geçerek birer gerçek eylem haline gelmiştir. Hatta bu siber saldırı senaryolarından

birden fazlasının eş zamanlı olarak uygulanması ihtimali de ülkelerin siber güvenlik gündemine girmiştir (Kara, 2013: 31).

Altyapı sistemlerini kontrol etmek ve işletmek için bazı bilişim sistemi programları kullanılmaktadır. Bu programlardan biri olan SCADA (Supervisory Control and Data Acquisition-Danışmalı Kontrol ve Veri Toplama Sistemi/Uzaktan Kontrol ve Gözleme Sistemi) yazılımı vasıtasıyla bazı altyapı bilişim sistemlerinin verimliliği artırılmakta ve ilgili kurumlarca kamuya ya da müşterilere daha sağlıklı, hızlı ve erişilebilir hizmetler sunulmaktadır. İşlevsel olarak SCADA, altyapı hizmetlerinin yürütüldüğü bilişim sistemlerine uzaktan erişim sağlayarak, sistemin geneli üzerinde hem kontrol mekanizması vazifesini yerine getirir hem de işletim sistemlerini sürekli olarak gözetim altında tutmaktadır.

Teknolojinin gelişmesiyle birlikte bilişim sistemlerinin de kendisini hızla yenilemesiyle birçok hizmet sektöründe bu tür yazılımlar etkin olarak kullanılmaktadır. Bu yazılımlar zaman, mekân ve iş gücü yönünden tasarruf sağlarken, uygulamaya konuldukları altyapı sistemlerinde fazladan bir güvenlik açığı da oluşturmaktadır. SCADA yazılımları genellikle kamu kurumlarının verdikleri hizmetlerde (su, enerji, sağlık, doğalgaz, haberleşme, ulaştırma) kullanılmakla birlikte, özel iştirakli kuruluş ya da şirketlerde de kullanılmaktadır. Bilişim sistemlerinin ve yazılımların etkin kullanılması ile birlikte gerekli güvenlik tedbirlerin alınmaması halinde küçük çaplı siber saldırılar sistemin tamamen engellenmesine sebep olacaktır. Asıl amaç bu yazılım ve donanımlar kullanılarak verilecek hizmetlerin maliyetlerini azalmak, hizmet hızını ise artırmaktır. Benzer bir yazılım ile herhangi bir bölgenin enerji nakil ihtiyacı, temiz şebeke su sistemleri, ulaştırma ve iletişim sistemleri rahatlıkla desteklenmektedir. Bu noktada en önemli husus, bilişim sistemleri temelinde verilen bu hizmetlerin siber güvenliğinin temin edilmesidir. Güvenlik ihtiyacının karşılanması için alanında uzman kişilerin çalıştığı, işlevsel ve güçlü bir yapıya sahip, güncel teknolojik imkânlarla donatılmış, doğru planlanmış stratejiye sahip olan kurumların oluşturulması ve işbirliği içerisinde çalıştırılması ile mümkün olacaktır (Meral, 2015: 54-73).

APT (Advanced Persistent Threat-Gelişmiş Kalıcı Tehditler), devletlerin altyapı bilişim sistemlerini tehdit eden diğer önemli bir siber tehdit unsuru olarak karşımıza çıkmaktadır. APT kavram olarak saldırı yapılacak hedefin kesin olarak tespit edildiği ve bu tespit edilen hedef üzerinde uzun zaman aralığında ve geçici süreli tehditler oluşturan zararlı programlardır. Siber saldırılarda ülkelerin kritik altyapılarına zarar vermek-

tedir. APT'lerin en önemli özelliklerinden biri siber güvenlik unsurlarının rahatlıkla aşabilmesi ve sistem üzerinde kendisini kopyalayabilmesidir. Ayrıca kendi kapasitesi dâhilinde saldırılan sisteme karmaşık bir şekilde sızarak sistem içindeki varlığını gizlemektedir. Bu yazılımların sisteme sızması ve çoğalması farklı yöntemlerle gerçekleşmektedir. Zararlı yazılımların bulaşma yollarına bakıldığında genellikle bilişim sistemleri uygulamaları (microsoft office yazılımları, adobe yazılımları, internet üzerinden ücretsiz indirilen yazılımlar, sosyal medya uygulamaları, blog bağlantıları vb.) ve dijital veri depolama cihazları (hafıza kartı, harici bellek, blueray, cd, dvd vb.) vasıtasıyla kendilerini kopyaladıkları tespit edilmektedir. APT'ler genellikle en güncel yazılım sistemlerini kendilerine kamuflaj olarak kullanarak tespit edilmelerini geciktirmektedirler (Kara, 2013: 32).

Saldırgan tarafından APT zararlı yazılımı ile bilişim sistemine gizlice girilerek bilişim sisteminde uzun zaman kalınması ve sistemi kontrol altına almaya çalışması bu zararlı yazılımın temel hedefidir. Bu zararlı yazılım ile genellikle kritik öneme haiz kamu kurum ve kuruluşları, özel, tüzel kuruluşlar ile kamuoyunda itibarı zedelenecek kişiler seçilmektedir. APT zararlı yazılımı ile yapılan saldırıların diğer yazılımlardan farklı olmasının en önemli sebebi ise bilişim sistemine fark edilmeden girmek ve bilişim sistemi içerisinde uzun bir zaman kalarak toplayabildiği kadar veri toplamaktır. APT'nin (Advanced Persistent Threat) açılımını yaparsak, advanced; saldırganın bilişim sistemlerine girebilmek için elindeki bütün imkânları kullanması anlamında kullanılmaktadır. Advanced safhasında birçok yöntem bir arada kullanılarak saldırılır. Persistent; bilişim sistemine fark edilmeden çabucak girerek sistemdeki bilgileri almak yerine, sistemdeki sürekliliğini devam ettirmesini sağlamasıdır. Threat; ise saldırganın çok iyi bir şekilde organize edildiği anlamına gelmektedir. Bilişim sistemlerine girmeden önce sosyal mühendislik yöntemleri kullanılarak sızılacak sistemler hakkında bilgi, belge toplamak örnek olarak verilebilir. Saldırı yapılacak olan bilişim sistemleri ne kadar güvenli olursa olsun bu zararlı yazılımlar farklı yöntemler kullanarak sisteme girebilmektedirler. APT zararlı yazılımları internet aracılığıyla virüs bulaştırma ya da çevresel faktörler kullanılarak veri depolama cihazlarıyla da virüs bulaştırılarak sistemlere girebilmektedirler.

APT zararlı yazılımları tarafından yapılacak saldırılara karşı güvenlik önlemi olarak anti virüs yazılımları, internet sitelerinin filtrelenmesi, risklerin tespit edilmesi, tespit edilen risklerin analiz edilerek zararlı yazılımların tespit edilmesi sayılabilir.

Profesyonel olarak hazırlanan uygulamalar ya da yazılımlar normal insanlar tarafından yazılamayacak kadar zordur. Bu yazılımlar uzman kişiler tarafından takım halinde çalışılarak ortaya çıkabilmektedir. Profesyonel yazılımların büyük bütçeler ayrılarak hazırlanabilmektedir. Profesyonel yazılımlar devlet ve büyük şirketlerce desteklenmesi gerekmektedir. Kritik altyapıların ve korunmasının önemi siber saldırılar ile birlikte fark edilmeye başlanılmıştır. Avrupa Birliği tarafından hazırlanan önlem planlarında bilişim sistemlerinin güvenliği ve savunulması amaç edinilmiştir. Bilişim sistemlerinin kritik altyapılarının korunması için çalışmalara Avrupa Birliği tarafından 2004 yılında başlanılmıştır.

20.10.2004 tarih ve 2004/702 sayılı Avrupa Birliği Komisyon kararında Terörle Mücadele de kritik altyapıların korunması konusunda toplumun güvenliğinin sağlanılması, toplumun sağlığının korunması vb. konularda mücadele edilmesi gerekliliği belirtilmiştir.

3.4. Yeni Riskler: Mobil Cihazlar ve Akıllı Telefonlar

Mobil cihazların yaygın kullanımı ve bu cihazlardaki yöndeşme sonucunda pek çok farklı fonksiyona sahip cihazlar kişisel bilgileri kamuya açık hale getirebilmektedir. Teknolojinin gelişmesi ile birlikte günümüzde bilgisayarlara yetişen akıllı cep telefonlarının hafızalarının büyümesi ile metin mesajlaşmalarının yapılabilmesi, e-posta gönderilip alınabilmesi, resim, video, ses kaydı alınabilmesine imkân sağlayarak yeni birçok özelliğe kavuşmuştur. Mobil cihazlar ile haberleşmenin yanı sıra; sosyal medyaya bağlanılması, sosyal ağlarda yorum yapma, resim, video, ses kaydının paylaşılması internet üzerinden kolaylıkla yapılabilmektedir. Mobil cihazlar günlük yaşamımızın bir parçası halini alarak kullanımı esnasında herhangi bir mekân ve zamana bağlı kalmaksızın insanın hangi konumda olduğu bilgisi sağlanabilmektedir. Mobil cihazların gelişmesine paralel olarak diğer alanlarda olduğu gibi güvenlik problemleri ile yeni riskler ortaya çıkmıştır (Altuntaş, 2018: 21).

Akıllı cep telefonu yani mobil cihazlar sadece haberleşme için değil içerisinde barındırdığı telefon rehberi, mms, kısa mesajlar, arama kayıtları, resim, video, ses, takvim notları vb. kapasitesi düşük verilerin yanı sıra daha çok veri saklama alanına ihtiyaç duyan ve internet, e-posta iletişimi, bankacılık işlemleri, navigasyon ve eğitim-öğretim vb. birçok uygulama ile çalışmaktadır. Mobil cihazlarında bilgisayarlar gibi özelliklere

kavuşması ile birlikte bilgisayarlar için alınacak güvenlik önlemlerinin mobil cihazlar içinde alınması gerekliliği ortaya çıkmıştır (Altuntaş, 2018: 21).

Mobil cihazlara güvenlik açısından bakıldığında bilgisayarlara oranla aynı güvenlik önlemlerini yakalayamasa da, akıllı telefonlar için kendine has güvenlik önlemleri ile antivirüs uygulamaları, firewall (güvenlik duvarı) ve akıllı telefonları şifreleme vb. güvenlik önlemleri ile az da olsa sağlayabilmektedir. Akıllı telefonlar için güvenlik uygulamalarının güncellemeleri yeteri kadar sık yayınlanmaması nedeniyle bilgisayarlar kadar fazla güncelleme yapılamamaktadır. Akıllı telefon kullanıcıları mobil cihazlara karşı yapılacak güvenlik tehditleri ya da güvenlik risklerinin farkında değildir. Kullanıcılar kullandıkları akıllı telefonların güvenlik güncellemelerini aktif hale getirememektedir. Ayrıca akıllı telefonlar ile internette gezinti yapmanın bilgisayarlardan daha güvenli olduğu kanısına varmaktadırlar (Altuntaş, 2018: 22).

Mobil cihazların işletim sistemlerindeki açıkların tespit edilmesi için 2009 ve 2010 yılların da yapılan bir çalışma ile mobil cihaz güvenlik açıklarının yüzde kırk iki oranında arttığı ve gelecekte daha da artacağı değerlendirilmiştir (Altuntaş, 2018: 22).

Akıllı telefonlara karşı yapılan saldırıların sayısının her geçen gün arttığı ve bu saldırılara karşı önlem alınmasında geç kalındığı tespit edilmiştir. Akıllı telefonların kullanımın yaygınlaşması ve teknik özelliklerinin gelişmesi ile birlikte akıllı telefonları saldırganların hedefi haline getirmiştir (Altuntaş, 2018: 22).

Akıllı telefonların sadece haberleşme teknolojisi kullanımı için değil bütün alanlarda kullanılmasıyla birlikte bilgisayar sistemlerini arkada bırakarak kullanımı hızla yayılmaktadır. Mobil cihazlar artık sadece bir haberleşme aracı olmaktan çıkmıştır. Akıllı telefonların işletim sistemleri ve donanım yapıları hemen hemen bilgisayarlar ile benzer özelliklere ulaşarak mobil cihazlarda bilgisayarla yapılan birçok işlemin bu cihazlar ile yapılması sağlanılmıştır. Bu durum ise mobil cihazlarda yapılan işlemlerin sonucunda kişisel verilerin korunması ihtiyacı ortaya çıkmıştır (Altuntaş, 2018: 23).

Akıllı telefonlara karşı başlıca oluşabilecek tehditleri sıralayacak olursak en çok kullanılan yöntemler, kötücül zararlı yazılımlar, direkt atak, araya girme, zafiyet kullanma ve sosyal mühendislik olarak belirtilebilir. Akıllı telefon kullanıcılarının güvenlik zafiyetleri dışında teknolojik bilgi eksikliğinden güvenlik açıkları oluşmaktadır. İnternet ve ağ sistemlerinin gün geçtikçe gelişmesine paralel olarak teknolojik açıdan farklı ve karmaşık bir niteliğe sahip olması, internet ortamı, bluetooth veya kızılötesi "wifi" ile birbirleri arasında bağlantı sağlamasıyla kötücül yazılımların hızla yayılmasına zemin

hazırlanması bu riskleri artırmaktadır. Akıllı telefonların sistemlerine bulaşan bu zararlı yazılımlar tespit edilip etkisiz hale getirilmesine rağmen akıllı telefonlardaki verilerin kaybedilmesi ya da yok edilmesi kişisel ve kurumsal açıdan manevi, maddi zararlara yol açmaktadır (Altuntaş, 2018: 24).

Zararlı yazılım veya virüslere örnek olarak cabir, cardtrap, skulls gibi örnekler verilebilir. 2004 yılında ortaya çıkan ve o zamanın en yaygın zararlı yazılımı symbian işletim sistemine bluetooth aracılığıyla zarar vermiştir (Sağıroğlu ve Bulut, 2009: 501-505).

Akıllı telefonlar da kullanıcının kendi isteği ile hotspot özelliğini aktif hale getirerek wi-fi ağı üzerinden internete çıkış yapıyorsa, saldırgan tarafından ip adresi tespit edilebilir ve saldırganın hedefi haline gelebilir (Altuntaş, 2018: 25).

Mobil cihazların kullanımın hızla artmasıyla birlikte akıllı telefonlarda en çok kullanılan işletim sistemlerinin başını Android ve İOS işletim sistemleri çekmektedir. Bu işletim sistemlerine zarar verecek çok sayıda zararlı yazılım yani virüs vardır (Altuntaş, 2018: 24).

IV. BÖLÜM : NATO VE TÜRKİYE'DE SİBER GÜVENLİK

4.1. Siber Savaş ve NATO Üyeleri

Soğuk Savaş sonrası İkinci Dünya Savaşı'nın olumsuz etkilerinin sonucunda Avrupa'da politik açıdan büyük boşluk oluşmuştur. Oluşan politik belirsizlik ortamında dönemin en büyük iki güç faktörü olan ABD ve SSCB uluslararası ortamın güç dengesini şekillendirmiştir. ABD ve SSCB siyasetlerine yeni anlayış kazandırarak dünya düzenine şekil vermeye başlamıştır. Bu arada güç mücadelelerine devam etmişlerdir. 1989 yılında Almanya'da Berlin duvarının yıkılmasıyla birlikte gelişen olaylar sonucunda WP'nin varlığı sona ermiş, bir anda NATO'nun en büyük tehdit algısı yok olmuştur.

SSCB'nin dağılmasından sonra uluslararası güç sisteminin denge unsurları da değişmiştir. SSCB'nin yarattığı tehditsel durumların yok olmasına paralel olarak NATO uluslararası güç sistemi içerisindeki konumunu yeniden şekillendirmek için strateji çalışmalarına başlamıştır. SSCB'nin dağılmasıyla birlikte alışılmış askeri birlik yapılanması, muharebe sahası tahminleri, taktik ve stratejik seviyedeki harekât planları önemini yitirmiştir. Kısacası simetrik olan tüm harp yöntem ve unsurları geçerliliğini yitirmeye başlamış, yeni gelişen teknolojilerle birlikte asimetrik tehditler ve harp yöntemleri oluşmuştur. Kosova'daki askeri müdahale esnasında, NATO'nun yaptığı hava hücum harekâtına karşı Sırplar gerçekleştirdikleri taktik siber saldırı yöntemleriyle gündeme gelmiştir. Bunun bir sonucu olarak da NATO, gelişen yeni tehditler kapsamında farklı bir strateji geliştirme ihtiyacı hissetmiş ve siber tehditleri gündemine almıştır (Bıçakçı, 2012: 205).

Günümüzde ise ülkeler bilişim sistemlerini ve siber güvenlik unsurlarını sert güç kapsamında değerlendirmeye almış bulunmaktadır. Taktik askeri harekâtların başarısı, mali dengenin korunması, ülkenin savunma sistemi altyapısının desteklenmesi gibi konularda bilişim sistemleri gün geçtikçe daha fazla kullanılmaya başlamıştır. Buradan yola çıkarak önümüzdeki dönemlerde siber güvenlik unsurlarının karışacağı uluslararası bir çatışma yaşayabilme ihtimalimizin hiç de az olmadığı gündeme gelmektedir.

Ülkelerin siber imkân ve kabiliyetleri incelendiğinde, bu niteliklerin bir siber saldırı niyetiyle değil daha çok hedef ülkenin faaliyetlerini sabote etmek, engellemek ya da bilgi casusluğu yapmak maksadıyla yönlendirildiği görülmektedir. Bunu destekleyen verilerin rahatlıkla görülmesine rağmen, birtakım ülkeler söz konusu siber kabiliyetlerini hasım ülkelere karşı icra edecekleri taktik askeri harekâta dâhil edeceklerini resmi

olarak belirtmeseler de siber imkân ve kabiliyetlerini bu kapsamda seferber edecekleri açıkça görülmektedir. Bu kararlılığa örnek verecek olursak; 2010 yılında Lizbon'da açıklanan stratejinin faaliyete geçmesiyle NATO, kendi stratejisini geliştirmiş ve yükseltmiş olacaktır. Bunun sonucunda NATO her türlü tehdide karşı görev yapabileceğini kanıtlamıştır. Siber yeteneklerin kullanımındaki çeşitlilik ve farklı aktörlerin sayısı, NATO'nun siber savunmadaki rolünü belirlemesini zorlaştıran önemli sorunlardan biridir. Belirlenen senaryolarda NATO'yu test edebilmek için iki çeşit siber tehdit durumu öngörülmüştür. Bu senaryolardan ilki, taktik ya da stratejik seviyede siber tehdit unsurlarının gerçekleştireceği bilişim casusluğuyla; önemli bilgilerin deşifre edilmesi ihtimalidir. Diğer senaryo ise, ülkenin önemli altyapı tesislerinin ya da sistemlerinin saldırıya uğradığı durumlarda, siber savunma unsurları işlevsiz hale getirerek altyapı sistemlerine verilecek zararın en yüksek seviyelerde olması ihtimalidir. Ayrıca maddi kazanç sağlamak için NATO'nun çalışanları da siber tehdit kapsamında yapılacak saldırının mağduru olabilir. Akıllı telefonların kullanımının artması ve bu gibi yazılıma sahip cihazların internet erişimlerinin rahatlıkla sağlanıyor olması da siber güvenlik konusunun en büyük güvenlik açığı sorunları arasında yer almaktadır (http-15, 8……, E.T: 20.03.2018).

4.2. Akıllı Güç ve Akıllı Savunma

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. Bu savunma kapsamında NATO güçlü, işlevsel ve güncel planlarla müttefiklerine güven vermesi gerekir. Güvenlik açısından baktığımızda tehditlerden korunma zorunluluğu bir açıdan da savunmacı realizmin 'güvenlik ikilemi' bakış açısının ön plana çıktığını göstermektedir.

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 (http-15, 8……, E.T: 20.03.2018).

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.

NATO siber güvenlikle alakalı bütün faaliyetleri ortak bir noktadan kontrol etmek maksadıyla daha önce büyük çaplı bir siber saldırıya maruz kalmış Estonya'nın Tallinn şehrinde CCDCOE'yi kurmuştur. Ayrıca ABD siber savunmaya destek vermek için,

müttefiklerin balistik füze bataryalarına, enerji nakil sistemlerine ve iletişim sistemlerine gerçekleştirilecek siber saldırıları direkt askeri tehdit olarak algılayacağını belirtmiş ve tehdidi etkisiz hale getirmek için askeri birlik harekâtı icra edeceğini açıklamıştır. Bu konuda da NATO'nun tüm kurumlarının ve unsurlarının seferber edilmesi gerektiğini de ayrıca belirtmiştir.

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 gerçekleştirmeye devam etmektedir. BM ise, oluşturduğu bir kurul aracılığıyla uluslararası siber uzay sistemindeki hareketler için çalışmalar yapmaktadır. RF ve Çin'in girişimleriyle bu faaliyet hızlandırılmış ve uluslararası geçerliliği olacak bir sözleşmenin oluşturulması için teknik çalışmalar sürmektedir (http-15, 8……, E.T: 20.03.2018).

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 işbirliğini 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 (http-17, 10……, E.T: 02.04.2018). Merkeze ev sahipliği yapan Helsinki'de ABD, İngiltere, Fransa, Almanya, İsveç, Polonya, Letonya ve Litvanya, üyelik için bir niyet mektubuna imzalarını attılar (http-18, 12……, E.T: 03.04.2018). 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 (http-18, 32……, E.T: 05.04.2018).

Helsinki'deki merkezde, üye ülkeler için uzmanların bir araya geldiği bir ağ teşkil edilmiştir. Merkezin AB ile NATO arasındaki işbirliğinin 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 (http-18, 11……, E.T: 03.04.2018).

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 (http-18, 11……, E.T: 03.04.2018).

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

Siber saldırıların uluslararası düzeyde devletlere karşı etkilerinin yıkıcı olduğu anlaşılmaktadır. Siber saldırlar ve etkilerini birkaç örnek ile açıklayacak olursak, siber bilgi casusluğu ile devletlere ait gizli kalması gereken bilgi ve belgelerin internet ortamı üzerinden sosyal medyaya sızdırılması ya da devletlere ait kritik kamu kurumlarının alt yapılarının kullanılmaz hale getirilmesi veya durdurulması durumlarıyla karşı karşıya kalınabilmektedir.

Lizbon'da gerçekleştirilen toplantının ardından NATO, bilişim sistemlerinin güvenliğinin ve siber savunmanın tesisi maksadıyla, güçlü ve etkili bir strateji oluşturmuştur. Bununla birlikte NATO müttefiki 9 üye ve AB işbirliği içerisinde oluşacak siber tehdit unsurlarını etkisiz hale getirmek için müşterek planlamayla birlikte, hibrit merkezinin kurulması ve faaliyete geçirilmesi gibi NATO'nun aldığı tedbirler, dolaylı olarak diğer ülkeleri de etkilemiş ve kendilerine has tedbirler almaya yönlendirmiştir.

4.3. SİBER SAVAŞ İLE NATO'YA YÖNELİK YENİ TEHDİTLER

NATO, Rasmussen'in Genel Sekreter makamında olduğu yıllarda yeni bir birim açılmasını kararlaştırmıştır. Açılan bu yeni birimin adı 'Yeni Güvenlik Tehditleri Bölümü' olmuştur. NATO için, kurulan yeni birimin ayrı bir önemi bulunmaktadır. NATO bu bölümü kullanarak hem merkez teşkilatını hem de üye ülkeleri uluslararası terör örgütlerine, siber tehditlere, enerji hammadde bölgelerine ve nakil sistemlerine karşı yapılacak saldırılara karşı yeni yöntemlerle toplu ve kapsamlı bir şekilde savunmak istemiştir. Bakıldığında genel olarak belirtilen tehdit algılarının birbiriyle pek müşterek yanı yok gibi gözükse de, ayrıntılı olarak incelendiğinde, aynı tehdit algılarının sistemsel bir biçimde birbirleriyle yakından ilgili oldukları rahatlıkla görülecektir. Belirtilen tehdit algıları savunma açısından baktığımızda müşterek özellikleri kendilerinde barındırmaktadır. Bu bakış açısı da, NATO'yu müttefikleri arasındaki işbirliğini baştan ele almaya, kendinden başka uluslararası güç unsurları ile iletişimini arttırmaya, güncel ve güçlü stratejiler oluşturmaya zorlamaktadır (http-9, Çetin, E.T: 01.02.2018).

NATO klasik savaş prensiplerinin yanında teknolojinin gelişmesiyle birlikte internet üzerinden sanal ortamda oluşan yeni tehditlere karşı ve yeni dünya düzeni olan, siber tehditler ve saldırı unsurları, enerji nakil hatları ve hammaddelerine karşı yapılacak saldırı türleri ve nükleer silah sistemlerinin oluşturduğu yıkım tehdidi gibi saldırılara karşı önlemler almak zorunda kalmıştır. NATO'ya ve diğer ülkelere karşı yapılan saldırılar 2018 yılı SonicWall siber tehdit raporunda ele alınmıştır.

Nova BOLD Bilgi Teknolojileri Destek Merkezi'ni yöneten ve işleten tek yetkili Hizmet Merkezi tarafından (SonicWall Capture Labs) güncel ve anlık tehditleri izleyerek yıllık rapor yayınlamaktadır. SonicWall Global Müdahale Savunma İstihbaratı Tehdit Ağı üzerinden farklı noktalarda çok sayıda aktif siber tehdit algılama cihazı olan SonicWall sürekli güncel ve anlık tehditleri izlemektedir. Güncel ve anlık tehditleri aşa-

ğıdaki bazı yöntemleri kullanarak ve danışmalık ile cihaz kurulum hizmetlerini birlikte vermektedir.

- İleri seviye ağ altyapısı analizi,
- Güvenlik politikaları danışmanlığı,
- Yerinde ağ güvenliği cihazları/yazılımları kurulum ve yapılandırması,
- İhtiyaca özel yazılım ya da çözüm geliştirme,
- Sistem yönetim hizmetleri,
- TZ, NSA ve Super Massive serisi vb. Firewall cihazları,
- Mobil Cihaz Analizleri,
- Güvenli Uzaktan Erişim Çözümleri,
- Kablosuz Güvenlik Çözümleri.

Günümüzde siber saldırılar ülkelere, ticari işletmelere, ekonomik tesislere, şirketlere ve vatandaşlara yönelik olarak yapılmaktadır. Bu saldırıların geneli kolay kurgulanmış fakat etkili yazılım programları şeklinde görülmektedir. Sayıları az miktarda olan bazı saldırılar ise, en ileri bilişim sistemleri kullanılarak programlanmış, şifrelenmiş, sağlam bir teknolojik altyapı tarafından desteklenen yazılımlardır. Tüm siber saldırı unsurlarının dikkate alınması gerekir. Basit olarak görülen bir saldırı büyük yıkımlara yol açma kapasitesine sahip olabilmektedir. Bu saldırılara karşı, aynı şekilde güçlü, işlevsel ve kurumların işbirliği içerisinde oluşturulacak bir savunma sistemiyle hareket edilmesi gerekmektedir (http-16, 9……, E.T: 01.04.2018).

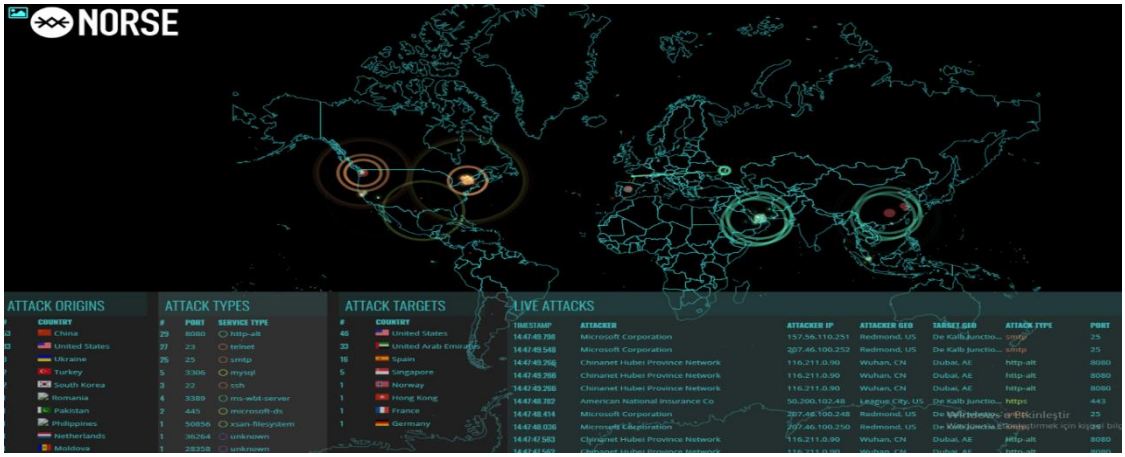
Bu konuda aslında bir ülkedeki en hassas nokta ekonomik tesisler ve şirketlerdir. Ülke sisteminin içinde olmalarına rağmen ilk önce kendi kurum güvenliklerini sağlamak zorunda oldukları bir gerçektir. Şirketlerin kar oranı ve mali yapısı ister istemez siber tehditler açısından kendilerini hedef yapmaktadır. Çünkü şirketlere yönelik olarak yapılacak siber saldırılar hem şirketin kendisine hem de ülke ekonomisine büyük zararlar verecektir. Bunun için şirketler tıpkı devlet kurumları gibi en son teknoloji ürünleri, güçlü bilişim sistemi unsurları, konusunda uzman siber güvenlik personeliyle çalışmak ve kendilerine has siber güvenlik stratejisi oluşturmak zorunda kalmaktadır. Güncel ve işlevsel olmayan bir siber savunma sisteminin, söz konusu şirketi olası bir siber saldırıda koruması mümkün değildir (http-16, 9……, E.T: 01.04.2018).

2018 yılı SonicWall Siber Tehdit Raporu'nda 2015-2017 yılları arasında kötü amaçlı yazılım atağı değerlendirildiğinde kötü amaçlı yazılım sayısının her geçen gün arttığı görülmektedir. Bu artış durumu Şekil 4.3.1'de sunulmuştur.

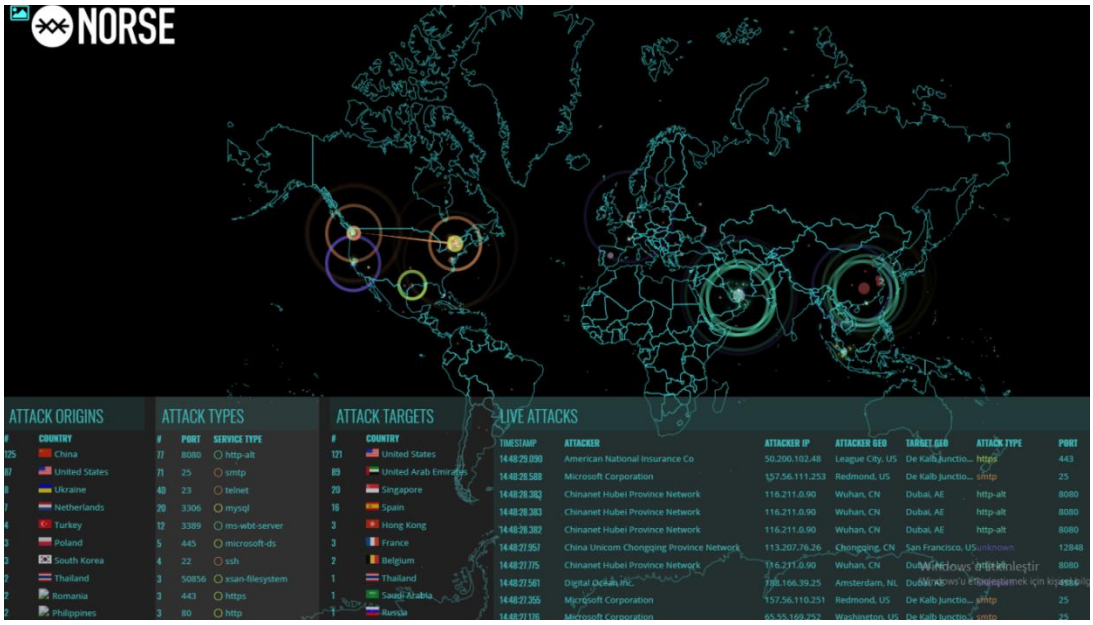
Şekil 4.3.1 Kötü Amaçlı Yazılım Atağı (2018 yılı SonicWall Siber Tehdit Raporu)

ABD'li bir siber güvenlik şirketi olan Norse'un kendine ait internet adresi (norse,map.ipviking.com) aracılığıyla ülkelerin maruz kaldığı siber saldırı miktarlarını ve bu saldırıların yerlerini anlık olarak üyelerine sunmaktadır. Anlık siber saldırı haritasında, Attack Origin Country (Saldırı Örneği Ülkeler), Attack Types (Saldırı Türleri), Attack Targets (Saldırı Hedefleri), Live Attack (Canlı Saldırı), Attacker (Saldırgan), Attacker IP (Saldırgan IP Adresi), Attack Type (Saldırı Tipleri), Port (Saldırı Port Numarası) vb. bilgiler görülmektedir.

Aşağıda Resim 4.3.1. ve Resim 4.3.2'de NorseMap Anlık Saldırı Ekran görüntüsü verilmiştir.



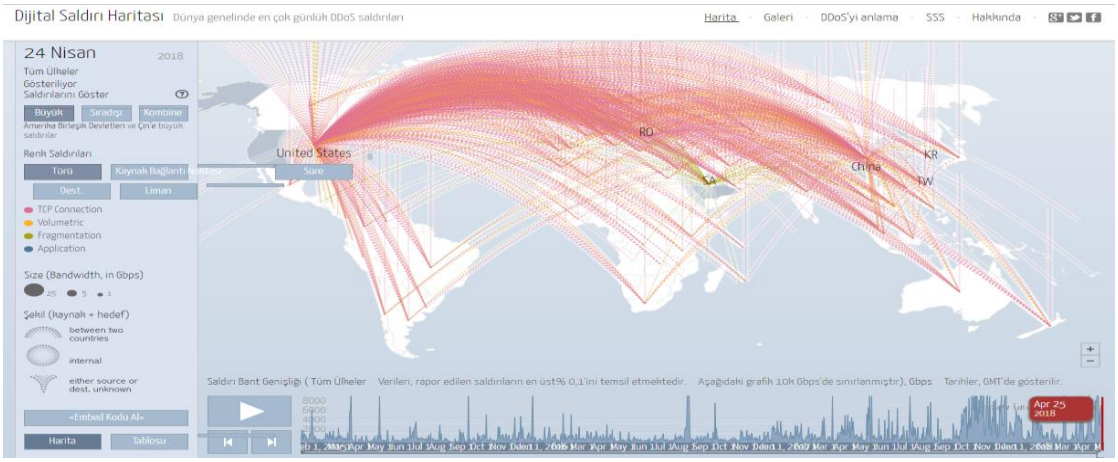
Resim 4.3.1.NorseMap Anlık Saldırı Ekran görüntüsü (http://www.norse-corp.com/)



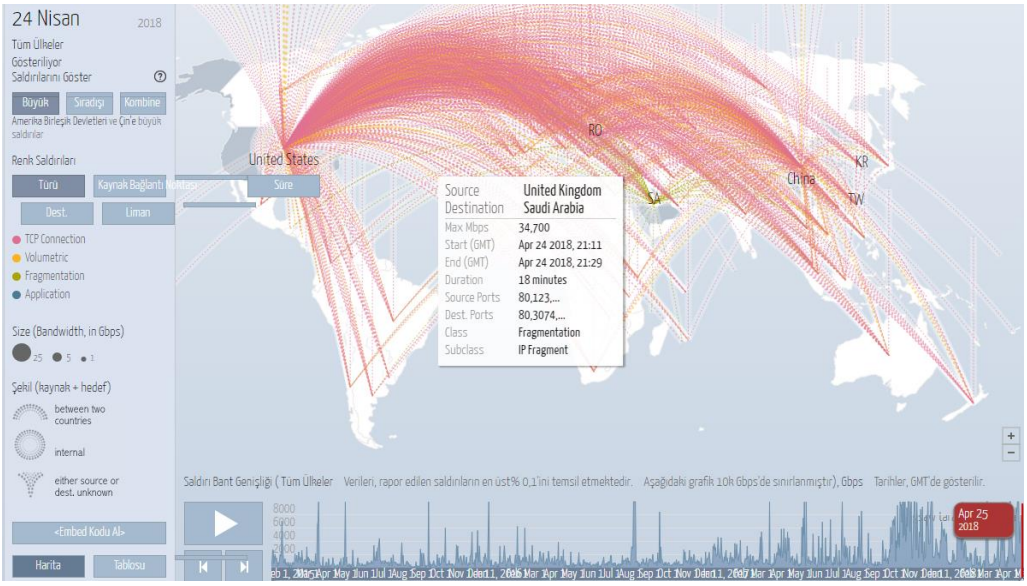
Resim 4.3.2. NorseMap Anlık Saldırı Ekran görüntüsü (http://www.norse-corp.com/)

Başka bir siber güvenlik firması olan Arbor Networks ise güncel ve gerçek zamanlı olarak DDoS Digital Attack Map (DDoS Dijital Saldırı Haritası) ile kendi internet adresi (digitalattackmap.com) aracılığıyla ülkelerin maruz kaldığı siber saldırı miktarlarını ve yerlerini anlık olacak şekilde ve geçmiş zamanlı olarak kullanıcılara sunmaktadır. Anlık DDoS siber saldırı haritasında, Web saldırıları, DNS saldırıları ve diğer saldırılar gibi vb. bilgiler görülmektedir.

Aşağıda Resim 4.3.3. ve Resim 4.3.4.'de Digital Attack Map Anlık Saldırı Ekran görüntüsü verilmiştir.



Resim 4.3.3. DDOS Digital Attack Map Anlık Saldırı Ekran görüntüsü



Resim 4.3.4. DDOS Digital Attack Map Anlık Saldırı Ekran görüntüsü

2018 yılı SonicWall Siber Tehdit Raporu'na göre milyonlarca insanın şahsi ve gizli verileri internet ortamında sızdırılmıştır. Bu sızıntıların geneline baktığımızda kötü amaçlı yazlımlar ve fidye uygulamaları aracılığıyla gerçekleştirildiği görülmektedir. Bu siber saldırı unsurlarından başlıcaları; BadRabbit, WannaCry, Petya zararlı yazılımları olduğu tespit edilmiştir. Aynı şirketin uzmanları bu türdeki yazılımların gün geçtikçe hızla arttığını belirtmişlerdir (http-16, 9……, E.T: 01.04.2018).

SonicWall Capture Labs firması 2016'da tespit ettiği zararlı yazılımların, 2017 yılı içerisinde sadece yüzde yirmi beşini tespit edebilmiştir. Tehdit miktarındaki artış oranına rağmen tespit miktarının azalması, siber saldırıları gerçekleştiren tüzel ya da özel kişilerin yeni yöntemler geliştirdiklerinin somut bir kanıtıdır (http-16, 9……, E.T: 01.04.2018).

SonicWall Capture Labs firmasının raporuna göre güvenlik duvarına karşı yapılan saldırıların gizlenerek ve şifrelenerek yapıldığı tespit edilmiştir. Yapılan zararlı yazılım saldırılarında internet trafiğinianaliz etme özelliği bulunmasaydı şirket zararlı yazılımların çoğunu tespit edemeyecekti (http-16, 9……, E.T: 01.04.2018).

Yazılım çeşitleri kullanılarak yapılan siber saldırılar önümüzdeki süreçte de siber güvenlik konusunda tartışılmaya devam edecektir. Genel olarak bu yazılımların temel amacı, hedef olarak seçtiği bilişim sistemlerinin alt yapısına zarar vermek, kontrol altına almak, casusluk ve istihbarat faaliyetlerine destek sağlamaktır (http-16, 9……, E.T: 01.04.2018).

SonicWall Capture Labs yöneticisi tarafından yapılan açıklamada, siber tehditlerin sadece ülkelere karşı yapılmadığı belirtilmiştir. Aynı tehditler insanları, kurumları, ekonomik tesisleri, şirketleri ve bilişim sistemlerini kullanan her birimi yakından ilgilendirmektedir. Siber tehditlere karşı alınacak önlemlerin maliyetleri de her geçen gün artmaktadır. Fakat siber güvenlik unsurları her geçen gün devletler, şirketler ve insanlar için vazgeçilmez nitelikte bir savunma aracı haline dönüşmüştür. Ekonomi endeksli fayda ve zarar durumuna bakıldığında, mali boyut başlangıç seviyesinde eksi yönünde görünse de Estonya benzeri bir saldırı durumunda tüm alt yapının çökebileceği göz önüne alınarak uzun vade de artı yönde etkileri görülecektir (http-16, 9……, E.T: 01.04.2018).

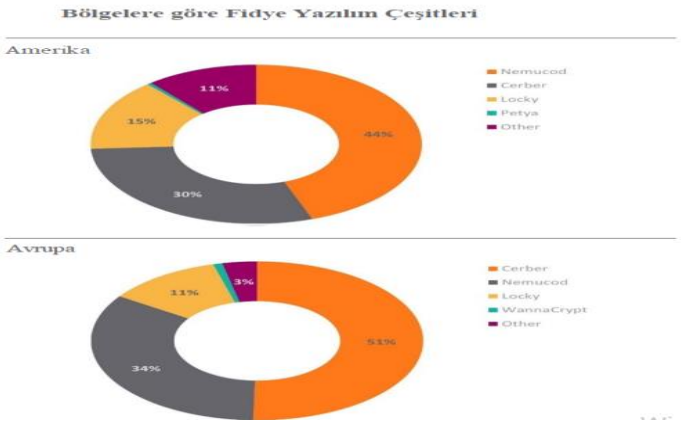
2017'nin en çok kullanılan Zararlı Yazılımları aşağıda belirtilen tablodaki yazılımlardan oluşmuştur.

Tablo 4.3.1. 2017'nin Zararlı Yazılımları

WannaCry	WannaCry bir yazılım ve solucan birleşmesi sonucu oluşmuştur. 2017 yılı başlarında ortaya çıkan bu yazılım ile dünya üzerindeki birçok ülkede kurum ve kuruluşlar etkilenmiştir. Bu saldırı dosya paylaşım protokolünün açıkları kullanılarak yapılmıştır.
Petya&NotPetya	2017 yılı içerisin de WannaCry'a benzeyen ve bilişim sistemi üzerindeki açıklar kullanılarak, Petya ve Notpetya solucanı ağ sistemlerine girerek ağ sistemleri üzerinden bulaşmaya başlamıştır. Bu zararlı yazılımın temel amacı girdiği bilişim sistemini ele geçirmek ve ele geçirdiği sistemini şifrelemek ve daha sonra bilişim sisteminde mavi bir ekran üzerinde kuru kafa resmi ile şifrelenmiş bilgilerin ödeme yapılması karşılığında verilmesini istemektir.

BadRabbit	BadRabbit yazılımı Adobe flash güncellemesi kullanılarak arka tarafta gizlenilmiştir. Bu zararlı yazılım ağ sistemleri üzerinden bilişim sistemlerine güç uygulayarak bilişim sistemlerine giren ve Microsoft Windows kimlik bilgilerinin listesini barındıran bir zararlı yazılımdır. Rusya ve Ukrayna'da ortaya çıkan zararlı bir fidye yazılımdır.
Cerber	2016 yılı içerisinde ortaya çıkmıştır. Bu zararlı yazılımın Rusya tarafından ortaya çıkarıldığı değerlendirilmiştir. 2017 yılında yayılmaya başlamıştır.
Nemucod	2016 yılı içerisinde ortaya çıkmıştır. Bu zararlı yazılımın içerisinde barındırdığı zararlı içeriklerin ortaya çıkmasını engellemek için şifreleme teknikleri arttırılmıştır.

Bölgelere göre zararlı yazılım çeşitleri Amerika ve Avrupa ülkeleri için Şekil 4.3.2'de gösterilmiştir.

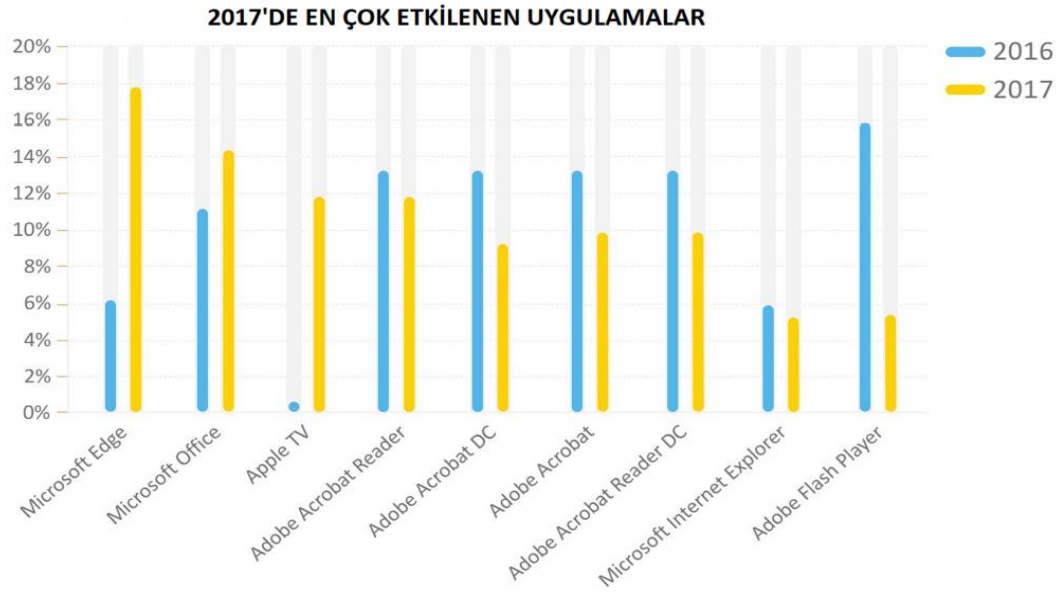


Şekil 4.3.2. Amerika ve Avrupa'da bölgelere göre zararlı yazılım çeşitleri

SonicWall şirketi 2016-2017 yılları arasında zararlı yazılımların %10-15 arasında büyüyerek arttığını tespit etmiştir. Siber saldırılar için saldırganların farklı yöntemler arayışında oldukları açıkça görülmüştür (http-16, 9……, E.T: 01.04.2018).

Bilgisayarlar ve mobil cihazlar da yoğun olarak kullanılan adobe ürünlerine karşı yapılan saldırılar azalırken, Microsoft işletim sistemlerinde kullanılan office yazılımlarına yapılan saldırılar artış göstermiştir (http-16, 9……, E.T: 01.04.2018).

2017 yılında en çok etkilenen uygulamalara bakıldığında, Şekil 4.3.3.'de belirtilen uygulamaların yaygın olduğu görülmektedir.



Şekil 4.3.3. 2017 yılında en çok etkilenen uygulamalar

Teknolojinin gelişmesiyle birlikte, internet aracılığıyla devletlerarası siber casusluk, siber terörizm, siber suçlar, siber saldırılar artmaktadır.

Bilgisayarlarda ve mobil cihazlarda kullanılan uygulamaların sahteleri, fidye yazılım vb. uygulama ve yazılımlar ortaya çıkmaktadır. NATO her yeni yılda siber silahlanma ve siber güvenlik konularının önem kazandığının farkına varmış ve bu konularda önlemler almaya başlamıştır. Siber tehditler sadece tehdit değil bir siber savaş ortamı oluşturmuştur. Siber savaş ortamında devletlerin tüzel ve özel kuruluşların ülkelerin ya da toplumun kişisel verilerini korumak için gerekli tedbirleri alması ve kendilerini teknolojinin ışığında geliştirmesi gerekmektedir.

4.4. TÜRKİYE'DE SİBER GÜVENLİK VE POLİTİKALARI

Teknolojinin gelişmesiyle birlikte bilgi ve iletişim teknolojisi ekonominin ve toplumun ayrılmaz bir parçası haline gelmiştir. Türkiye'nin kalkınmasında önemli katkılar sağlamaktadır. Türkiye'deki kamu kurumlarında, şirketlerde, vatandaşların kişisel hayatlarında, hastanelerde, ulaştırma hizmetlerinde, ekonomik tesislerde, enerji sağlayan santrallerde ve iletişim alanında yazılımlar, programlar ve bilgisayarlar birlikte internet sıkı bir şekilde kullanılmaya başlamıştır.

Dünya ülkelerinin siber yetenekleri her geçen gün teknolojinin gelişmesine paralel olarak artmaktadır. Doğal bir sonuç olarak siber tehditler de zaman, yer ve mekâna bağlı olarak artmaktadır. Bu tehditlerin sebep olduğu büyük ya da küçük güvenlik açıkları ile ortaya çıkan siber tehditlere örnek verecek olursak;

1. Stuxnet adlı virüsün İran'daki nükleer tesisin soğutma sistemini etkilemesi sonucunda oluşan büyük çaplı hasarlar (2010),
2. Wikileaks tarafından internet üzerinden açıklanan gizli bilgiler neticesinde oluşan diplomatik krizler (2010),
3. ABD'nin kullandığı bir İHA'nın kullanılan bir yazılımla İran tarafından etkisizleştirilerek ele geçirilmesi (2011),
4. Kuzey Kore Devlet Başkanı hakkında gösterime giren bir filmin, yapımcısı olan şirkete (Sony) yapılan büyük çaplı siber saldırılar neticesinde filmin yayınlanmasının durdurulması (2014),
5. ABD'de kamu hizmetlerini gerçekleştiren bilişim sistemlerine yapılan siber saldırılarla büyük çaplı krizlerin ortaya çıkması (2016) ve bunun neticesinde oluşan hasarların maddi değerinin ülke sisteminde yaptığı kriz etkisi gibi konular sayılabilmektedir.

Türkiye içerisinde de uluslararası sistemde görülenlerle benzer sıkıntılar yaşanmıştır. Bunu örneklendirecek olursak;

1. Bakü-Tiflis-Ceyhan enerji nakil hatlarına karşı yapılan siber saldırılarla sistemin belli noktalarda infilak etmesi (2008),
2. Gönderilen bir virüs neticesinde Atatürk Havalimanındaki havayolu ulaşım sistemlerinin kilitlenmesi (2009),
3. Ani gelişen siber saldırılar neticesinde Telekominikasyon İletişim Başkanlığı'nın bilgisayar sistemlerinin ve internet tabanlı programlarının belli bir süre işlevsiz bırakılması (2011),

4. Siber saldırılar sonucunda Türkiye'de iki il dışındaki tüm illeri etkisi altına alan elektrik kesintilerinin yaşanması (2015),

5. Yapılan toplu siber ataklarla ülkedeki kamu kurum ve kuruluşlarının altyapı sistemlerinin bir haftayı aşkın bir süre içerisinde vatandaşların ulaşımına sunulamaması (2015),

6. Türkiye'nin sağlık sistemine yapılan siber saldırılar neticesinde hastanelerin bilişim sistemlerindeki verilerin yok edilmesi (2016) ve ele geçirilmesi sayılabilir (Şenol, 2017:3).

Bilişim sistemleri ve özelliklede internetin her alanda aktif hizmet sağlaması siber ortam konularındaki bütün parçalarıyla birlikte siber güvenlik sorunların da oluşmasına yol açmaktadır.

Kamu iştirak ve kuruluşlarının vatandaşlara yönelik yaptıkları faaliyetlerin tamamına yakını internet üzerinden de verilmektedir. Bu konuda sistemin güvenliğinin sağlanabilmesi için özel gayretlerinin olması gerekmektedir. Çünkü genel siber güvenliğinin sağlanmasının yolu ülkedeki kuruluşların tek tek güvenliklerin sağlanmasıyla gerçekleştirilir. Siber güvenlik konusunda tümevarım yönteminin benimsenmesi gerekmektedir (http-21, 14……, E.T: 26.04.2018).

Bilişim sistemlerinin mevcut güvenlik açıkları, bu hizmetlerin yürütülememesine ya da kötü niyetli kişilerce ele geçirilmesine, vatandaşların hayatını kaybetmesine, geniş çaplı mali sorunlara, ülkenin genel güvenlik sisteminin tahrip edilmesine ve sonuçta kamu güvenliğinin ortadan kalmasına sebep olacaktır. Bu durumlar, yapılan siber tehdit senaryolarında devletler, şirketler ve uluslararası kuruluşlar tarafından tespit edilmiştir (http-21, 14……, E.T: 26.04.2018).

Gerçekleşen siber saldırılarda asıl dikkat çeken husus kaynağının bulunamaması yani kim tarafından, ne amaçla, hangi unsurların ya da ülkelerin desteğiyle yapıldığı sorularının çoğu zaman cevapsız kalmasıdır. Siber saldırıların gücü arttıkça arkasında bir destekçi bulunması ihtimali de aynı oranda artmaktadır. Çünkü bu saldırılar genellikle devletler tarafından bir taktik araç ya da baskılama yöntemi olarak da kullanılmaktadır. Verdiği zararlar göz önüne alındığında kullanan ülkeler için güçlü bir silah, maruz kalan ülkeler için ise büyük bir tehdit içermektedir. Bilinmezlik olgusu siber tehditlerin en güçlü yanını oluştururken, ülkeler için ise karşı tepki verilecek bir düşmanın olmamasına yol açmaktadır. Bu şartlar altında her türlü siber tehdit unsuru için tamamen korunan bir güvenlik sisteminin varlığını tesis etmek oldukça güçtür. Yapılması gereken

en önemli konu siber savunma araçlarının ya da sistemlerinin güncel teknolojik altyapıda olması, kurumlarla işbirliğini devamlı sürdürmesi, kendini sürekli olarak geliştirmesi ve gerçek senaryolarla düzenli olarak tatbikatlar gerçekleştirmesidir. İnternetin sağladığı faydalar kadar zararlarının da olması doğal bir sonuçtur. Çünkü tüm insanlığın faydasına kullanım serbestliği sağlayan bir yapı olmakla birlikte, aynı serbestlik kapsamında kötü niyetli ülkelere ve şahıslara müthiş imkânlar da sunmaktadır. Sonuçta ülkeler risk analizlerini yaparak hem bilişim sistemlerinin nimetlerinden faydalanmak, hem de siber güvenlik stratejilerini oluşturmak zorundadırlar (http-21, 14……, E.T: 26.04.2018).

Bu esaslar çerçevesinde Bakanlığın oluşturduğu stratejiye ve koyduğu kurallara tüm devlet kurumlarının, iştiraklerin, kamu görevlilerinin ve üretim tesislerinin uyması kanuni bir zorunluluk haline getirilmiştir. Ayrıca kendilerine tevdi edilen tüm görevleri de yerine getirmekle yükümlü kılınmışlardır. Bunu için oluşturulan Ulusal Siber Güvenlik Stratejisi 2013 yılında uygulanmaya başlamıştır. İçerisinde güvenlik tedbirleri, savunma planları, müşterek icra edilecek faaliyetler, eğitim-öğretim faaliyetleri, kurumlara ve vatandaşlara yönelik bilgilendirme faaliyetleri de yer almaktadır.

Teknolojinin gelişmesiyle aynı anda bilişim sistemleri de gelişmektedir. Doğal bir sonuç olarak bu gelişim siber tehdit konusunda da izlenmektedir. Oluşan yeni tehditler konusunda ülkenin de kendi sistemini gözden geçirmesi ve güncellemesi gerekmektedir. Bu amaçla mevcut sistemlerin değiştirilmesi gerektiğini anlayan Ulaştırma Bakanlığı yeni bir siber savunma stratejisi oluşturmuştur. İlgili kamu kurum ve kuruluşlarıyla birlikte bazı değerlendirme toplantıları yapmış ve önceki stratejinin eksik yanları ön plana çıkartılarak yeni oluşturulacak planda hangi noktalara daha fazla ağırlık verilmesi gerektiği konuları ele alınmıştır. Bu toplantılardan sonra, kamu yetkilileri, konusunda uzman şahıslar, siber güvenlik konusunda çalışan akademik personel ve STK'lardan gelen üyelerle kapsamlı araştırma çalışmaları da gerçekleştirilmiştir. Sonuçta ülkenin siber güvenliğini sağlamak ve yeni bir strateji oluşturmak konusundaki kararlılığını açıkça kamuoyuna beyan etmiştir. Yapılan çalışmalar neticesinde Ulaştırma Bakanlığı yeni bir strateji oluşturmayı başarmıştır. 2016-2019 Ulusal Siber Güvenlik Stratejisi adını alan bu genel strateji tüm ülkeye açıklanmış ve bu kapsamda uygulanacak Ulusal Siber Güvenlik Planı uygulamaya konulmuştur (http-21, 14……, E.T: 26.04.2018).

Bakanlık ayrıca bazı kurumlar kumuş ve bu kurumlara önemli görevler tevdi etmiştir. Kurulan Siber Güvenlik Konseyi, siber tehditlerin bertaraf edilebilmesi için stra-

teji oluşturmak, kanun teklifinde bulunmak, kurumlar arasında işbirliğini sağlamak, savunma planlarının uygulanması kontrol etmek ve sağlamakla yükümlüdür. Konseyin başında Ulusal Siber Güvenlik Koordinatörü bulunmaktadır. Bu makam tüm bu görevlerin yerine getirilmesinde birinci derecede Cumhurbaşkanına karşı sorumludur. NATO müttefiki olan ülkelerle birlikte Türkiye'de oluşturduğu bu strateji ve uygulamalarla siber savunma planı olan ülkeler arasında yer almaktadır.

Siber güvenlikte verilerin üç temel özelliğinin korunmasının önemi çok büyüktür.

(1) Verilerin gizliliği; verilerin ilgisiz şahıslar, kurumlar veya süreçler tarafından kullanılmaması ve açığa çıkarılmaması,

(2) Verilerin bütünlüğü; varlıkların doğruluğunun ve tamlığının koruması,

(3) Verilerin erişilebilirliği; yetki sahibi kurum ya da şahısların istekte bulunması halinde gerekli bilgilerin ulaşılabilir durumda bulunması anlamına gelmektedir.

Türkiye'de bu kritik hizmetlerin verilmemesi, vatandaşların hayatını kaybetmesine, geniş kapsamlı mali sorunlara ve tüm ülkeyi etkileyebilecek krizlere ya da devlet güvenliğinin tehditlere açık hale gelmesine sebep olabilecektir. Türkiye'de bilişim altyapısının bozulması halinde ise kritik hizmetin yanı sıra bilgi güvenliği sisteminin zarar görmesi neticesinde tüm kamu kuruluşlarının etkileneceği büyük bir güvenlik sorunu oluşacak ve mevcut altyapıların tekrar işletilebilir hale getirilmesi maliyet ve zaman alacaktır.

Türkiye'nin açıkladığı siber savunma planındaki misyonu; devletin siber güvenlik sisteminin tesis edilmesi maksadıyla, işlevsel ve caydırıcı bir bakış açısı yaratmak, işbirliğini temin etmek ve planın devamlılığını sağlamaktır. Vizyonu ise; halkın güvenliği ve ülkenin mali, siyasi, askeri ve beşeri tüm sistemlerinin sağlıklı büyüyerek gelişmesini temin etmek için bilgi iletişim sistemlerinden maksimum derecede yararlanarak etkin, güçlü, hızlı ve doğru üretilmiş bir genel strateji sayesinde caydırıcı ve güçlü bir siber güvenlik toplumu yaratmaktır. Ulaştırma Bakanlığının hazırladığı siber güvenlik eylem planının temel maksadı ise; bütün kamu kurum ve kuruluşlarına hatta özel şirketlerde dâhil olmak üzere siber savunmanın ülke savunmasının çok önemli bir ayağını oluşturduğu bilincini yerleştirmek, ülkenin tamamının siber tehditlere karşı savunulmasını sağlamak, bu konuda çalışacak etkin ve güçlü birimler oluşturmak, oluşturulan birimlerin çalışmasını denetlemek ve bu birimleri kullanarak ülkenin siber güvenliğini tesis etmektir (http-21, 14……, E.T: 26.04.2018).

Siber güvenlik hedeflerini gerçekleştirmek için;

• Ülkenin siber alanının tamamını içermek koşuluyla, bilişim sistemleri sayesinde yapılan bütün faaliyetlerin ve hizmetlerin oluşturulan siber güvenlik sistemleri ile korunmasının temini ve bu amaçla kullanılan sistemlerin bilgi havuzunun bilmesi gereken prensibine göre erişime açılmasını,

• Siber tehdit unsurlarının zararının minimum seviyede tutulmasına, saldırı sonrasında zarar gören uygulamaların bir an önce günlük faaliyetlerini yapabilecek hale getirilmesini sağlayan siber savunma tedbirlerinin oluşturulmasına ve gerçekleşen saldırının ilgili kurumlarca kovuşturulmasının yapılmasını,

• Siber savunma unsurlarının, sağlıklı ve güvenilir bir şekilde çalışabilmesi için ulusal kurumlarca oluşturulmasına, eğer bu imkân ve kabiliyet yoksa başka ülkelerden ya da şirketlerden temin edilen bu sistemlerin kontrolünü sağlayacak her türlü tedbirlerin alınmasına imkân sağlayacak tüm faktörler belirlenen plan dâhilinde mevcuttur. (http-21, 14……, E.T: 26.04.2018).

Türkiye'nin siber güvenlik savunma planındaki kapsamı ise, ülkedeki mevcut kamu kurum ve kuruluşlarının kullandığı bilgisayar sistemleri, devlet ya da özel girişimler tarafından sağlanan hizmet sektörünün yapısal faaliyetlerinin işletildiği elektronik sistemleri, ülke genelinde bunun dışında faaliyet gösteren ve bilişim sistem unsurlarını kullanan topluluğun oluşturduğu siber ortamdan oluşmaktadır.

Siber güvenlik savunma planı teknolojinin ilerlemesiyle, uluslararası siber tehditlerin gelişmesiyle, ihtiyaçların farklılaşmasıyla birlikte, ülkedeki unsurlar tarafından yapılacak istekler neticesinde ilgili kurumlar tarafından işbirliği içerisinde ve işlevsel olarak güncellenmektedir.

Ulaştırma Bakanlığı'nın siber güvenlik eylem planında bahsedildiği gibi başka devletlerin stratejik planlarında yer alan siber tehdit unsurları ve bu tehditlere karşı alınan tedbirler de dikkate alınarak plan dâhilinde yapılacak eylemler belirlenecektir. Sonuçta siber tehditlerin küresel nitelikte olduğu ve her ülke için tehdit unsuru olduğu belirlenmektedir (http-21, 14……, E.T: 26.04.2018).

Bu kapsamda alınacak tedbirlere aşağıdaki örnekler verilebilir:

1. Siber savunmanın oluşturulmasında şahıslar, kurumlar, topluluklar üzerlerine düşen tüm görevleri gerçekleştirmek zorundadır.

2. Kamusal kuruluşlar, eğitim kurumları, şirketler ve STK'lar siber güvenlik konusunda mutlak suretle koordinasyon içinde ve eşgüdümlü çalışmalar yapmaları gerekmektedir.

Diğer ülkeler ve uluslararası örgütlerle siber tehditler konusunda işbirliği içerisinde olmak gerekmektedir.

Gözden geçirilen belgelerde sıralanan önemli risk unsurları da aşağıdaki gibi özetlenebilir:

1. İnsanların sosyal ağlara karşı artan isteği,
2. Stratejik öneme sahip kurumları ve şirketlerin siber ortamdaki yerleri,
3. Bilişim sistemleri casusluğu ve belli bir amaca yönelmiş siber saldırılar,
4. Kurumlarda çalışan kişilerdeki bilgisizlik ve ilgisizlik,
5. Ülkedeki birimlerin işbirliği yapmaması ya da yapamaması,
6. Siber ortamlarda çalışan çeşitli firmalara yönelik mali kaygılardır.

Türkiye'nin siber savunma planı ile birlikte yukarıda bahsedilen konular da değerlendirilerek mevcutsiber savunma stratejisi güncellenmiştir (http-21, 14……, E.T: 26.04.2018).

Bu eylem planı belirlenirken sadece yurtiçi kurum ve kuruluşların değil, yurt dışı kurum ve kuruluşların da edindiği tecrübe ve fikirlerden faydalanılmıştır. Özellikle NATO bünyesinde faaliyet gösteren Estonya Talinn merkezli Müşterek Siber Savunma Mükemmelliyet Merkezi (CCDCOE)'nin çalışma sistemi ve ilgilendiği konular incelenmiştir.

CCDCOE tarafından açıklanan belgede NATO üyelerinin tatbik etmesinin zorunlu olduğu konular maddeler halinde belirtilmektedir:

1. Siber saldırıya uğrayan ülkenin altyapısını savunmak maksadıyla sert güç (özellikle askeri güç) uygulamak

2. Siber saldırıya uğrayan ülkenin savunulması ve ülkenin acil durum sistemini işletmek maksadıyla sert güç uygulamak

3. Yapılacak araştırmalarda destek sağlamak ve kovuşturmaya imkân vermek için adli makamların da soruşturmaya dâhil olmasını sağlamak

4. Konusunda uzmanlaşmış kişilerle siber tehdit altındaki ülke ile NATO arasındaki işbirliğini sağlamak

5. İnternet Servis Sağlayıcıları (ISP)'ler vasıtasıyla siber saldırıya maruz kalan ülkenin yapılacak işlemlerle saldırının akışını durdurmak

6. ISP'ler vasıtasıyla siber saldırıya maruz kalan ülkenin yapılacak işlemlerle bu işlemlere destek sağlayan ya da destek sağlamak ihtimali düşünülen ülkelerin veri akışını durdurmak

7. Siber saldırı unsurlarının keşfedilmesi halinde gerekli karşı uygulamalarla tehdidi bertaraf etmek

8. Siber güvenliği sağlayan unsurların kabiliyetini çoğaltmak için ek İnternet Değişim Noktaları (IXP) kurmak, aynı zamanda ulusal internetin gücünü arttırmak

9. Bilişim sistemleri üreten firmalarla icra edilecek işbirliği sonucunda kritik yerlere gerçekleştirecekleri lojistik desteklere önem vermelerinin sağlanması

10. NATO üyeleri, siber saldırı altındaki ülkeye destek vermek ve saldırıyı gerçekleştiren birimleri ya da kişileri engellemek için NATO'nun siber savunma birimlerini karşı hamleler için kullanmaktır (Ada, Çakır, 2017: 641).

Ulusal siber güvenliğin sağlanması maksadıyla TÜBİTAK'a bağlı olarak faaliyete geçirilen Bilişim ve Bilgi Güvenliği İleri Araştırmalar Merkezi (BİLGEM), 1997 yılından itibaren çeşitli çalışma ve gelişmelerle günümüze kadar siber güvenlik alanında devletin başlıca faaliyet gösteren bir kurumu olmuştur. Yaptığı çalışmalarla önemli bir bilgi birikimine ulaşan BİLGEM günümüzde halen faaliyet göstermektedir. Bu bilgi birikiminin uluslararası standartlarda kabul görmesi için 2001 yılında Genelkurmay Başkanlığı'nın da katkısıyla Ortak Kriter Test Merkezi (OKTEM) oluşturulması düşüncesi hayata geçirildi. 2006 yılındaki akıllı kart güvenliği programı ve 2010 yılındaki Ortak Kriterler belgelendirmesi gelişmeleri ile Türkiye 14. "sertifika üreticisi ülke" olarak ilan edildi. Kurum 2012 yılından itibaren Siber Güvenlik Enstitüsü (SGE) adı altında faaliyetlerine devam etmektedir. SGE devletimizin NATO bünyesinde gerçekleşen faaliyetler, taktik simülasyon uygulamaları ve strateji geliştirme işlemlerine iştirakini sağlayan bir kurumdur. Ayrıca siber güvenlik ve savunma politikalarından bilgi elde edilmesi, gelişen teknolojinin takip edilmesi, ulusal firmalarımızın reklamının yapılması ve ulusal gücümüzü sergilemesi maksadıyla NATO'nun koordinesinde çalışan kuruluşlara, organizasyonlara ve faaliyetlere ülkemizi temsilen katılmaktır (http-22, 15….. E.T: 04.12.2018).

Ayrıca TSK (Türk Silahlı Kuvvetleri) bünyesinde 1997 yılından itibaren Muhabere Entegre Bilgi Sistemi (MEBS) Başkanlığı altında faaliyet gösteren siber çalışma grupları 2012 yılından itibaren TSK Siber Savunma Merkezi Başkanlığı altında toplanmıştır. Bu birim ise 2013 yılında TSK Siber Savunma Komutanlığına dönüştürülmüştür.

TSK Siber Savunma Komutanlığı; Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Dışişleri Bakanlığı, TÜBİTAK ve diğer kamu kurumlarıyla işbirliği çerçevesinde çalışmaktadır. Aynı zamanda NATO ile koordinasyon halinde faaliyetlerini ülke içinde ve dışında devam ettirmektedir. Bu kapsamda NATO ile yapılan müşterek siber güvenlik tatbikatlarına da katılım sağlamaktadır. TSK, NATO tarafından icra edilen 2016 yılındaki 'Kilitli Kalkan' tatbikatına da aktif olarak katılım sağlamıştır.

SGE, TSK ile müştereken 2010'dan itibaren NATO'nun siber koalisyon faaliyetlerine hem planlayıcı hem de icracı olarak katılmaktadır. Ayrıca yine NATO'nun siber savunma kapasiteleri panellerine ve bu kapsamda uygulanan siber savunma kabiliyeti takımlarına da katılmakta ve önemli görevler almaktadır. NATO müttefiki ve NATO ile işbirliği içerinde olan devletlerin huzuru ve güvenliği için uygulamaya koyulan 'Güvenlik ve Barış için Bilim' faaliyetleri bünyesinde NATO modelleme ve simülasyon grupları ile ortak çalışmalar yürütmektedir. Bu çalışmaları koordine den CCDCOE'dir. Ayrıca NATO'nun bilgi ve teknoloji sistemleri panellerine de aktif olarak katılım sağlamaktadır (http-23, 16….. E.T: 04.12.2018).

Ülkemizde de 25-28 Ocak 2011'de 'I. Ulusal Siber Güvenlik Tatbikatı' yapılmıştır. Faaliyet sonrasında açıklanan sonuç raporunda Türkiye'nin siber tehditlere karşı savunmasının zayıf bulunduğu ve siber mücadelenin kamusal tüm kurum ve kuruluşlarda yeterli tedbirlerin uygulanmadığı belirtilmiştir. Bunun sonucunda 2011 yılında Emniyet teşkilatı içerisinde Bilişim Suçlarıyla Mücadele Daire Başkanlığı kurulmuştur. Aynı yıl içinde 8 aşamalı olan ve 61 kurumun katıldığı ikinci bir tatbikat yapılmış ve kuruluşlara gerçek siber saldırılar düzenlenmiştir. 29 Kasım 2017 tarihinde ise 'Ulusal Siber Savunma 2017 Tatbikatı' icra edilmiştir. Uygulamalar iki aşamada yapılmıştır. Birinci aşama, istekli olarak katılan 20 farklı kamu kuruluşuna üretilen kurgusal tehditlerle internet erişimi olan bilişim sistemlerine yönelik siber saldırılar gerçekleştirilmiş ve siber savunma unsurlarının işlevsellikleri test edilmiştir. Aynı zamanda bu uygulamalar sayesinde çalışanların da kabiliyetleri fiziken görülmüştür. Diğer aşamada da, internetin kullanılmadığı bilişim sistemlerinde kurumsal ağlar üstünden siber saldırılar tatbik edilmiş ve bu sistemlerin siber savunma gücü ve kapasitesi test edilmiştir. İcra edilen uygulamalı eğitim faaliyetleri tüm kurumların siber güvenlik seviyelerini tespit etmekte kullanılmış, eksik yanlar göz önüne çıkarılıp bu hususlara yönelik acil tedbirler alınarak güçlü bir siber savunma sistemi oluşturulması gerekliliği görülmüştür (Bıçakçı,2013; 45-46).

Gerçekleştirilen bu simülasyonların asıl maksadı;

(1) Kamu kurumlarının ve ülkedeki diğer bilişim sistemi kullanıcılarının siber tehditlere karşı güçlü siber savunma mekanizmaları oluşturmalarını sağlamak ve kabiliyetlerini arttırmak,

(2) Bu kuruluşların siber güvenlik açısından kendi içlerinde işbirliği yapmalarını temin etmek,

(3) Siber savunma tedbirlerinin gerekliliği ve önemi hususunda kamuoyu algısı oluşturmaktır.

Sonuçta ülkemiz 2015 yılına kadar 3'ü ulusal düzeyde, 1'i uluslararası düzeyde olmak üzere toplam 4 kez siber güvenlik ve savunma tatbikatları icra etmiştir. Uygulamalarda ilgili Bakanlık işbirliği kapsamındaki faaliyetlerde, TSK Siber Savunma Komutanlığı, TÜBİTAK ve TİB ile devamlı olarak irtibat halinde olmuştur.

Siber güvenlik kapsamında ülke savunmasının tesis edilmesi için dikkat edilecek hususlar aşağıda sıralanmıştır;

1. Siber güvenlik, her zaman olası tehditler göz önüne alınarak yeterli, güçlü ve gelişmeye yatkın sistemler ile yapılmalıdır. Ortaya çıkan tehdit unsurları için uygun hareket tarzları belirlenmeli, bunların fayda ve mahzurlarıyla incelenmesi sağlanmalı ve sonuçta en uygun şekilde mücadele edilmesi gerekmektedir.

2. Siber güvenlikte savunmanın başarılı olmasının temel kuralı, tüm kurumların tehdit algısının oluşturulması ve oluşan bu tehdit algısının siber güvenlik bilincine dönüştürülmesidir. Oluşturulacak farkındalık seviyesindeki en önemli husus, siber güvenliğin her kurum ve her iş sahası için bir ihtiyaç olduğunun bilinmesidir. Kendi tedbirlerini almayan kurum ve şahıslar sadece kendilerini değil bütün ulusal bilişim sistemi unsurlarını tehlikeye atma ihtimaline sebep olacaklarını bilmeleri gerekmektedir. Bunun sağlanması için ise, düzgün bir strateji oluşturulmalı, bu stratejinin bütün bilişim unsurlarınca kabul görmesi ve işlevsel olarak devam ettirilmesi sağlanmalı, iyi planlanmış bir eğitim programı ile kullanıcıların eğitimi desteklenmeli, hukuksal altyapı boşluklarının ise gerekli makamlarca giderilmesi sağlanmalıdır.

3. Oluşan risk faktörlerinin değerlendirilmesi, bilişim sistemlerinin zayıf yönlerinin tamamlanmasını, tehdit unsurlarının algılanmasını ve bertaraf edilmesini, bu mücadele sonucunda oluşabilecek hasarların azaltılmasını ihtiva eder. Hasarların azaltılması maksadıyla siber tehditlere karşı etkin, güçlü, işlevsel ve kararlı bir stratejinin oluşturulmuş olması gerekmektedir.

4. Siber ortamların savunulması ve işlevselliklerinin devam ettirilmesi için ülke içerinde yer alan tüm kurum, kuruluş, ekonomik iştirakler ve vatandaşların sıkı bir işbirliği ve koordinasyon içerisinde olmaları sağlanmalıdır.

5. Bütün bilişim sistemi unsurları, siber ortam savunmasını gerçekleştirmek için uğraşırken, hukuki bir bakış açısıyla hareket etmeli ve hiçbir vatandaşın ya da kurumun hakkını ihlal etmemesi gerekmektedir.

6. Kullanıcılar siber ortamdaki tehdit analizi ve değerlendirmesi konularında üzerlerine düşen görevleri yaparken açıklanabilir, hukuki değerlere uygun, toplumun değer yargılarına saygılı bir hareket tarzıyla çalışmalıdır.

7. Siber savunma tedbirlerinin tehdit unsurları ile alakalı olması, fayda zarar analizi yapılarak şekillendirilmesi uygun olacaktır.

8. Siber savunma unsurları ve araçlarının ulusal güce dayalı olması ve ülke içindeki birimlerce üretilmesi sağlanmalıdır. Bunun gerçekleştirilmesi için gerekli altyapı kurulmalı, mali destek sağlanmalı, eğitim ihtiyacına yönelik talepler karşılanmalı ve sistemin her türlü gereksinimi yerine getirilmelidir.

9. Vatandaşların sosyal medya uygulamalarını kullanma istek ve oranının artması, bilişim sistemleri ve siber ortam güvenliği ile ilgili yeterli bilgi donanımının olmaması, bilişim sistemi araçlarında (bilgisayar, tablet, cep telefonu, akıllı saat, vb.) gerekli emniyet tedbirlerini almamaları, kendilerinin ve diğer şahısların bilişim sistemi suçlarına karşı açık hale getirmektedir. Bu konu siber güvenlik için çok hassas bir nokta oluşturmakta, sebep olduğu hasarla çoğu zaman bireysel nitelikli başlayıp birden fazla şahsı hatta kurumları bile etkileyebilmektedir.

10. Ülke içindeki kuruluşlarda spam, virüs, kötü amaçlı yazılımlar ya da başka siber saldırı vasıtalarıyla yapılan siber saldırılarda adli suç çeşitleriyle karşılaşılması mümkün olmaktadır.

11. Ülke içindeki kuruluşlarda bilişim sistemini kullanan görevlilerin dikkatsiz davranması neticesinde altyapı sistemlerinin zarara uğraması ya da geçici süreyle hizmet dışı kalması görülebilmektedir. Bunun için gerekli duyarlılık oluşturulmalı ve eğitim faaliyetleri planlanmalıdır.

Yukarıda belirtilen maddeler her ne kadar ilke olarak belirtilmiş olsa da aynı zamanda birer risk faktörüdür.

Türkiye'nin 2016-2019 Ulusal Siber Güvenlik Stratejisi kapsamında oluşturduğu planlara ve yaptığı eylemlere bakıldığında, söz konusu zaman dilimindeki tehditleri

engellemek maksadıyla icra edilen faaliyetler aşağıda belirtilmiştir (http-21, 14……, E.T: 26.04.2018).

1. Ülkenin siber güvenliğini tesis etmek için gerekli olan altyapısal unsurların ivedi olarak oluşturulmasının temini ve bu unsurların görevli kurumlarca sık bir şekilde kontrol edilmesinin sağlanması,

2. Ulusal siber savunma için kontrol kurumlarının da dâhil olacağı bir çalışmayla hukuki açıkların kapatılması için yasal düzenlemelerin yapılması,

3. İlgili Bakanlık ve kontrol görevine sahip olan bütün kurumların ilgi seviyelerinin ve işlevselliklerinin arttırılması,

4. Ülke genelindeki tüm kuruluşların sahip olduğu siber güvenlik sistemlerinin siber tehditlerden alabileceği zararların yanında personelin kusurlu hareketlerinden ve yaşanacak doğal felaketlerden de etkilenmemesi için gerekli tedbirlerin alınması,

5. Siber tehditlerle mücadele eden tüm birimlerin kendilerine ait bilişim sistemleri güvenlik planının olması ve bu planı işletebilecek kapasitede bulunması,

6. Siber savunma görevinde bulunan kurum müdürlerinin farkındalık seviyesinin arttırılması ve personelini yönlendirebilecek öngörüde olmasının sağlanması,

7. Siber savunma birimlerinde çalışan personelin eğitilmesi ve eğitim almak isteyen diğer personellerin desteklenmesi,

8. Ülkenin her kesiminde siber güvenlik anlayışının yerleşmesinin temin edilmesi, bu kapsamda ulusal basının aktif olarak kullanılması,

9. Siber güvenlik birimlerinde çalışan personelin konusunda yetişmiş bireyler olmalarının sağlanması, bu kapsamdaki personel için güzel imkânlar sunulması,

10. Siber savunmanın bel kemiği olan siber olaylara müdahale ekiplerinin imkân ve kabiliyetlerini arttırmak için hukuki altyapının hazırlanarak kanun desteğinin sağlanması, ekonomik tedbirler ile ekiplerin güçlendirilmesi, düzgün bir altyapı imkânı verilmesi, modern bilişim sistemleri ile donatılması,

11. Siber güvenlik alanında faaliyet gösteren tüm birimlerin kontrolünü sağlayacak bir kurum oluşturulması ve bu kurum vasıtasıyla işbirliğinin arttırılması,

12. Ülkedeki tüm bilişim sistemi kullanıcılarının ve siber savunma unsurlarının katılımıyla genel bir siber güvenlik ortamının tesis edilmesi,

13. Oluşan genel siber güvenlik ortamının faaliyetleri incelenerek uygun hareket tarzlarının açıklanması, eğitim hizmetlerinin arttırılması,

14. Bilişim sistemlerinde siber güvenlik için aktif şekilde yararlanılan yazılım, donanım ve cihazların başka maksatlarda ülke aleyhine kullanılmalarının önüne geçebilmek için gerekli teknolojik ve bilimsel çalışmaların gerçekleştirilmesi,

15. Ulusal siber savunma unsurlarının geliştirilmesi,

16. Ulusal siber savunmada yabancı ürünlerin azaltılması, yerli firma ve kurumlara yapacaklarıaraştırmalar için gerekli mali desteğin sağlanması,

17. Siber tehditlerin daha saldırı başlamadan önce etkisiz hale getirilmesini sağlayacak siber savunma unsurlarının oluşturulması,

18. Siber tehditlerin siber uzay alanındaki güçlü yanları olan benzerliği engellemek maksadıyla düzenli ve sistemli bir kayıt imkânı sunan 6. Sürüm internet protokolünün kullanımının arttırılması temin etmek şeklinde belirtilmiştir.

V. BÖLÜM : SONUÇ VE DEĞERLENDİRME

NATO yıllar içinde farklı stratejiler planlayıp uygulamaya çalışsa da genel olarak iki ana strateji üzerinde yoğunlaşmıştır. Tehditlere karşı kademeli ve aynı ölçüde cevap vermek için esnek karşılık stratejisini kullanmış, önceden öngörüp tehdit oluşmadan engellemek için de ileri savunmayı temel strateji olarak ele almıştır.

Örgütün kuruluş yılından itibaren 2000'li yıllara kadar strateji belirlemesinde ve savunma sisteminde askeri olarak etkin olan faktör, nükleer silahlar, balistik füzeler ve diğer konvansiyonel silahlar olmuştur. Askeri bir kuruluş olan NATO'nun doğal olarak gücünü konvansiyonel silahlara dayandırması tabi bir gerekliliktir.

Ancak 2000'li yıllardan sonra gelişen teknoloji ile birlikte NATO'nun da bu gelişmelere kayıtsız kalması mümkün değildi. Çünkü teknolojik gelişmeler sadece silah ve savunma sistemlerinde değil; hayatın her alanına etki etmeye başlamıştır. Özellikle internetin yayılması ve her alanda etkin halde kullanılmaya başlaması ile birlikte NATO için teknolojik gelişmelerin kapısının aralandığı kadar, öngörülemeyen birçok yeni tehdit unsuru da ortaya çıkmıştır. Bir savunma örgütü olarak kurulan NATO bu zamana kadar klasik savaş teknikleri ve konvansiyonel silahlar ile icra edilen mücadeleler için tedbir alıp strateji geliştirmiştir. İnternet ile birlikte NATO'nun yeni bir tehdit algısı daha oluşmuştur. Bu tehdit algısı ise siber savaş olmuştur.

İnsanlığın güç için mücadele etmeye başladığı ilkçağlardan bu yana, çatışmalar genel olarak ya toprak paylaşımı konunda olmuş ya da denizlere ve okyanuslara hâkim olma isteği sonucunda gerçekleşmiştir. Toprak ve su üzerinde gerçekleşen bu mücadele asırlar boyunca artarak devam etmiştir. Dünya Savaşlarıyla birlikte bu güç mücadelesi için yeni bir alan daha açılmıştır. Uçakların sisteme dâhil olmasıyla artık havada güç yarışında yerini almıştır. ABD ve SSCB'nin kendi aralarındaki kıyasıya mücadele konularından birisi olan Ay'a çıkmak ise, güç mücadelesi için yeni bir ortam yaratmıştır. Uzay boşluğunun da dâhil olmasıyla gerçekleştirilen stratejik hamleler gücün tanımını da değiştirmiştir. Ancak teknolojinin gelişmesine paralel olarak uluslararası güvenlik sisteminin tehdit algısı arasına giren siber tehditler, tüm bu yaşanan gelişmeleri derinden etkileyen ve ülkelerin bütün mücadele alanlarının ve savunma planlarının bir kişi tarafından bile tehdit altına girebilmesinin ortamını sağlayan bir unsur olmuştur.

SSCB'nin dağılmasının ardından zamana ayak uydurmak zorunda olduğunun farkında olan NATO, bu tarihten sonra gerçekleşen zirvelerde yapılan görüşmelerle yeni stratejiler oluşturmuştur. Koşulların ve tehdit algısının değişmesiyle, doğal bir sonuç

olarak NATO'nun da güvenlik algısı değişmiştir. Uluslararası sistemin anarşi özelliği devam ettiği sürece NATO kendi varlığını sürdürmek, güvenilirliğini devam ettirmek ve kuruluş amacını sağlamak için her türlü tehdit karşısında uygun stratejiyi oluşturmak ve uygulamak zorundadır.

Bu kapsamda şimdiye kadar tehditlerin neler olduğu ya da olabileceği öngörülebildiği için savunma sistemleri ve güvenlik senaryoları rahatlıkla belirlenebilmiştir. Siber tehditlerin ortaya çıkmasıyla birlikte NATO için öngörülmesi zor olan yeni bir asimetrik savaş tehdidi olarak 'siber savaş' konusu ön plana çıkmıştır.

ABD'nin yaşadığı 11 Eylül terör saldırısından sonra tehdidin nereden, ne zaman, ne şekilde geleceği konusundaki belirsizlik güvenlik ikilemini daha da arttırmıştır. Bu olaydan yola çıkarak terör örgütlerinin kullanacakları yöntemlerin klasik harp ortamıyla hiçbir alakasının olmaması ve örgüt mensuplarının hiçbir etik değere sahip olmaması, yapılacak eylemlerin öngörülememesine sebep olmaktadır. Sonuçta ülkeler genel güvenlik stratejilerini bilinen tehditlere karşı hazırlarken, terör eylemleri konusundaki öngörülmezlik, ülkeler için büyük çaplı güvenlik krizlerine sebebiyet vermektedir. Ortaya çıkan yeni güvenlik tehditleri ve aktörler nedeniyle literatüre genişletilmiş güvenlik kavramı girmiş ve bu kavram insan/vatandaş güvenliğini merkeze alarak incelenmektedir.

Güvenlik stratejileri konusunda benzer sıkıntılar siber tehditler konusunda da yaşanmaktadır. Hızla gelişen teknoloji siber tehdit kapasitesini arttırmakta, kurumları ve ülkeleri güvenlik krizlerine sürüklemektedir. Ortaya çıkabilecek en büyük kriz ise ülkelerin arasında gerçekleşebilecek bir siber çatışma ortamı oluşmasıdır.

İnternetin, coğrafi olarak bir mekânı ve çizilmiş bir sınırı yoktur. İnternette bilinen fiziksel kuralları uygulamak zor ve imkânsızdır. İnternetin kullanımın her geçen gün artan şekilde sosyal hayata girmesi ve artmasıyla birlikte kontrol altına alınması zor bir hale gelmiştir. Kontrol altında tutulamaması internette yararları, zararları ve güvenlik problemlerini de beraberinde getirmiştir.

NATO üyesi Estonya'da meydana gelen siber kriz, devlet kurumlarını ve güvenlik sistemini içinden çıkılması güç bir durumla karşı karşıya bırakmıştır. Oluşan siber saldırı süresince ittifak içerinde yer almasına rağmen, savunma açısından gereken yardımı alamamıştır. Çünkü NATO, bu zamana kadar böylesine bir tehdit algısı öngörmediği için bu koşullara uygun stratejik planlar da üretme gereği duymamıştır. Bu durum, NATO'nun Bükreş'te gerçekleştirdiği toplantının ana gündem maddesi haline getirilmiş ve

siber güvenliğin bir tehdit olarak görüldüğü belirtilerek stratejik ve taktik seviyede mücadele organları oluşturulması kararı alınmıştır.

NATO içerisinde yer alan ülkeler tarafından tasdik edilen amaçlar doğrultusunda gerçekleştirilen çalışmalar sürekli kontrol edilmektedir. Bununla birlikte, örgüt bünyesinde bulunan eğitim kurumları aracılığıyla yapılan çalışmalar ve birliklerin aktif katılımıyla icra edilen tatbikatlar ve simülasyonlar, siber güvenlik tedbirleri olarak sayılabilmektedir.

Bu kapsamda 2008'de kurulan siber savunma merkezi önemli görevler üstlenmektedir. Ayrıca bu merkezin Tallinn'de kurulmasının verdiği mesaj ise, kriz noktasında çözümün gerçekleştirilecek olmasıdır. Oluşturulan büyük stratejik yaklaşımda üyelerin stratejik kurumlarına ya da kaynaklarına yapılacak siber müdahalelerin direkt yapılan bir saldırı gibi muamele göreceği ve anında sert güç unsurları kullanılarak cevap verileceği açıklanmıştır.

Ülkeler tarafından siber tehditlerin kamu hizmetlerini ne derece etkileyebileceği ve altyapıya ne kadar zararı olabileceği Estonya örneğinde görüşmüştür. Fakat stuxnet-saldırısıyla bir nükleer santralin işleyişini bozarak kitlesel bir imhaya sebep olabileceğini görmek siber tehditlerin zararlarının hangi seviyelere kadar ulaşabileceğini göstermiştir. Bununla birlikte siber saldırıların ne kadar önemli bir güvenlik tehdidi olduğu tüm devletler tarafından fark edilmiştir.

NATO, Bükreş'te yaptığı toplantının sonucunda siber tehditlerin önlenmesi için bazı adımlar atmıştır. İlk adım olarak, merkezi teşkilatının bulunduğu Brüksel şehrinde bu konudaki çalışmaları tek elden yürütebilmek maksadıyla Siber Savunma Yönetim Makamını (CDMA) oluşturmuştur. İkinci adım olarak, ilk saldırının gerçekleştiği Tallinn şehrinde savunma planlarını oluşturacak olan Siber Savunma Mükemmeliyet Merkezini (CCDCOE) kurarak çalışmalarına devam etmiştir.

Esas olarak CCDCOE, NATO üyelerinin siber güvenlik planlarına destek vermek, bu kapsamda çalışan personelin eğitimine yardımcı olmak, üye ülkelerce müşterek yapılacak tatbikatları organize etmek, siber saldırılar konusunda genel bir strateji oluşturmak konularında görevlendirilmiştir. CDMA ise, olası bir siber saldırı durumunda CCDCOE'nin aktif bir şekilde çalışmasını sağlayarak, saldırıya uğrayan ülkenin isteği doğrultusunda gerekli tüm desteğin yapılmasını sağlamaktır.

Türkiye 2010 yılından itibaren NATO'nun Cyber Coalition tatbikatlarına aktif olarak katılmakta ve müşterek icra edilen faaliyetlerde aktif rol üstlenmektedir.

CCDCOE'nin siber savunma konusunda NATO üyesi ülkeler için yayınladığı yol gösterici ilkeler dikkate alınarak hazırlanan ulusal siber güvenlik planları uygulanmakta, yeni gelişen her türlü siber tehdide karşı NATO ile koordineli bir şekilde güncellenmektedir.

CCDCOE, NATO bünyesinde üye ülkelerin katılımıyla bazı faaliyetler düzenlemektedir. Birincisi, siber güvenlik konularında mücadelenin temelini teşkil edecek ve faaliyetlere zemin oluşturacak bir hukuksal taslak olan Tallinn El Kılavuzu'nun hazırlanmasıdır. İkicisi, bilgilendirme ve eğitim amacıyla müttefiklerin katılımıyla senede bir kere düzenlenen konferanslardır. Üçüncüsü ise, NATO ülkelerinin tamamının katılımıyla icra edilen siber savunma tatbikatlarıdır.

2010 tarihinde üye ülkelerin katılımıyla Lizbon'da gerçekleştirilen zirvede siber güvenlik sistemleri kapsamında güncel, işlevsel ve güçlü bir genel strateji oluşturulmasına karar verilmiştir. NATO, siber tehditlere karşı kapsamlı tedbirlerin bulunduğu güncellenmiş savunma planları hazırlamıştır. Bununla birlikte NATO, uluslararası güvenlik terminolojisine "hibrit" savaş terimini kazandırmıştır. Hazırlanan bu planlar Türkiye de dâhil olmak üzere bütün NATO üyelerinde uygulanmaya başlamıştır.

NATO, uluslararası sistemdeki diğer güvenlik sorunlarıyla (terör örgütleri, Afganistan, vb.)uğraşırken yine de siber güvenlik konusunu ihmal etmemiş ve yeni oluşan tehditler konusu içinde detaylı olarak değerlendirmeler yapmıştır. Newport toplantısında da konu kısmen de olsa görüşülmüş ve siber savunma politikası onaylanmıştır. Böylece NATO, örgütsel bir siber savunma stratejisinin imarı konusunda önemli bir aşama daha kaydetmiştir.

Önümüzdeki yıllarda siber saldırıların sayısının artması tahmin edilmektedir. NATO üyelerinin bu tehditleri engelleyebilmesi için çok iyi bir koordinasyon içerisinde olmaları, iyi eğitilmiş mücadele ekipleri oluşturmaları ve kurumlarının güncel teknoloji ile donatılmış olması bir zorunluluktur. Ayrıca tüm üyeler bireysel olarak kendi ülkelerinin siber güvenlik sistemlerini oluşturmak ve işlevsel halde tutmak mecburiyeti içindedirler. Çünkü NATO ikincil planda destek sağlayacak bir yapıdır. Tehditler öncelikli olarak ülkelerin kendi savunma planlarıyla engellenmeye çalışılmalıdır. Kısacası her üyenin kendi siber güvenlik stratejisi olmalı ve bu strateji odağında hazırlanacak savunma planı da NATO'nun planı ile müşterek şekilde çalışabilir halde olmalıdır. NATO, AB ve diğer güçlü aktörlerle siber savunma stratejileri konusunda işbirliğini mutlak suretle sürdürmelidir.

NATO siber güvenlik konusunda oluşturduğu sistemi temel önceliklerine göre planlamıştır. NATO'nun temel amacı, kendi kurumsal sisteminin savunulması ve güvenliğinin sağlanmasıdır. Üye ülkelerin savunma sistemlerine verilecek destek ise ikincil amacı olmuştur. Üye ülkelere verdiği destek faaliyetleri kapsamında, eğitim faaliyetleri, müşterek tatbikatlar, yapılan seminer ve konferanslar ve siber savunma stratejisi oluşturma konusundaki yardımlar sayılabilmektedir.

Harp sahasının klasik savaş prensiplerinin yanında teknolojinin gelişmesiyle birlikte internet üzerinden sanal ortamda oluşan yeni tehditlere karşı (küresel terör saldırıları, siber güvenlik tehditleri, nükleer silah tehditleri vb.) ya da başka tehdit unsurları tarafından gerçekleştirilecek saldırılar karşısında NATO da sürekli olarak yeni önlemler almak zorundadır.

İnternet ve bilişim sistemlerini kullanarak yayılan siber tehdit unsurları ülkelerde kamu kurumlarının altyapısında, vatandaşların yaşam alanlarında, ekonomik değer taşıyan şirket ya da tesislerde büyük güvenlik sorunlarına yol açmakta ve ülke güvenliğini yapısal olarak tehdit etmektedir.

Siber savunma sistemleri için güvenlik açıklarının sayısı çok fazladır. Bunun temel sebebi saldırı türlerinin çeşitliliğidir. Takipçi programlar, sistemleri kontrol eden yamalar, manipülasyon yaratıcı uygulamalar, kontrol dışındaki e-postalar, çeşitli amaçlar için üretilen virüsler, solucan yazılımlar ve botnetler, siber saldırı araçlarının çeşitleri arasında sayılmaktadır. Nye'ın yaptığı tanımlamaya göre, ülkelerin siber savunmalarını tehdit eden öncelikli konu diğer ülkelerin oluşturduğu siber tehditler ve ülkelerin dışındaki unsurlar tarafından oluşturulan tehditlerdir. Siber savaşlar ve ekonomi tabanlı siber saldırılar genellikle ülkeler tarafında yapılmaktadır. İnternet üzerinden gerçekleştirilen adli suç çeşitleri ve siber terör saldırıları ise ülkelerin dışında kalan unsurlar tarafından gerçekleştirilmektedir.

Dünya genelinde bütün devletlerin bilgilerini, örneğin sağlık bilgileri, vatandaşlarına ait özel ve kişisel bilgilerini, bankacılık bilgileri, gayrimenkul bilgileri, haberleşme bilgileri vb. bilgilerinin depolandığı ve işlendiği, cihazların siber ortamlarda bulunması ve yönetilmesiyle birlikte beşinci savaş ortamı olan siber ortamda bilginin güvenliği ön plana çıkmaktadır.

Siber saldırıların uluslararası düzeyde devletlere karşı etkilerinin yıkıcı olduğu anlaşılmaktadır. Siber saldırılar ve etkilerini birkaç örnek ile açıklayacak olursak, siber bilgi casusluğu ile devletlere ait gizli kalması gereken bilgi ve belgelerin internet ortamı

üzerinden sosyal medyaya sızdırılması ya da devletlere ait kritik kamu kurumlarının alt yapılarının kullanılmaz hale getirilmesi veya durdurulması krizleriyle karşı karşıya kalınabilmektedir.

Profesyonel programlar yüklü maliyetlerle hazırlanabilmektedir. Bu sebeple ülkeler ve ekonomik açıdan söz sahibi şirketlerce yaptırılması öngörülmektedir. Ulusal kurumların ve ekonomik tesislerin korunmasının önemi yapılan saldırılar ile birlikte fark edilmeye başlanılmıştır. Hazırlanan siber güvenlik strateji ve direktifleri, korunmaya ve savunmaya yöneliktir.

Bir ülkede ulusal güç denince akla ilk gelen genellikle sert güç kapsamında silahlı kuvvetler olmuştur. Bu kural sadece ülkeler için değil güvenlik anlayışı temelinde kurulan NATO gibi kuruluşlar için de geçerli olmuştur. Çalışmada belirtildiği gibi siber güvenlik konusu da sert güç kapsamında değerlendirilebilir. NATO'nun bu konuda geliştirdiği irade de bu yöndedir.

Bu tez kapsamında yapılan değerlendirme sonunda, NATO'nun yaklaşımının savunmacı realist görüşe daha yakın olduğu görülmektedir. NATO'nun siber tehditlere karşı Bükreş ve Lizbon zirvelerinden sonra geliştirdiği ve alt birimleri tarafından uygulamaya koyduğu stratejiler genellikle gelebilecek olan siber tehditlere karşı bir ortak savunma planı niteliğindedir. Dolayısıyla oluşan ya da oluşabilecek siber tehditlere karşı ortak savunmanın planlanması, NATO üyesi ülkelerin siber güvenlikleri konusunda iş birliği sağlama çalışmaları ve icra edilen müşterek tatbikatlar sürekli olarak planlanmış ortak savunma stratejileridir. Siber güvenlik NATO antlaşmasının temelini oluşturan üye ülkelerin korunması prensibi gereği doğal bir sonuç olarak varlığının meşruiyetini korumak maksadıyla NATO için bir gerekliliktir. NATO siber savunma planlarını güncel ve aktif halde tutma gayreti içerisindedir. Savunma odaklı bir 'güç' öğesi olarak elde bulundurulmak istenen siber güvenlik tedbirleri NATO için savunmacı realizmin araçları niteliğindedir. Gelebilecek olan siber tehditlerin yerinin, zamanının, kaynağının ve güç niteliğinin belirlenebilmesinin zor olması ve siber tehditlerin çeşitliliğinin hesaplanabilmesinin imkânsızlığı NATO'yu ister istemez savunma konumunda tutmaktadır.

ABD ise siber tehditler konusunda daha agresif bir tutum izlemektedir. Siber tehditler konusunda ön alma hatta karşı tehdit oluşturma ABD'nin öncelikli seçenekleri arasındadır. ABD'nin siber güvenlik konusunda saldırgan realizm anlayışına sahip olduğunu söylemek yanlış olmayacaktır. Genel olarak tehdidi yok etmek ve tehdit oluşturabilecek kaynakları da etkisiz hale getirmek gibi bir stratejiye sahiptir.

NATO üyesi olan Türkiye ise siber tehdit konusunda savunmacı realizm yapısına sahiptir. Türkiye'nin önceliği gelebilecek olan siber tehditlere karşı koymak, çıkabilecek olası bir siber savaşta kendisini korumaktır. Siber güvenlik için ulusal kurumları bulunan Türkiye güncel olarak tuttuğu siber savunma planlarıyla çalışmalarına devam etmekte olup NATO ile koordineli bir şekilde iletişimini sürdürmektedir.

Önümüzdeki yıllarda siber tehdit seviyesinin ne derece artacağı kesin olarak bilinmemektedir. NATO üyesi ülkelerin ortak bir çatı altında siber tehditlerden korunması, siber güvenliğin tamamıyla sağlandığı anlamına gelmemektedir. Tezde sunulan siber saldırı örneklerinde görüldüğü gibi, siber tehditlerin en güçlü yanı; zamana, mekâna ve kaynağa (askeri, politik, ekonomik güç) bağlı olmamasıdır. Hedef kuruma ya da ülkeye başka bir hasım ülke saldırabileceği gibi tek bir şahıs da kapsamlı bir saldırı düzenleyebilmektedir.

21. yüzyıldaki güç dengelerini realizmin bakış açısıyla inceleyecek olursak; sert güç, yumuşak güç ve her ikisinin kullanıldığı akıllı güç kavramlarının bulunduğu bir sisteme dayanacaktır. Türkiye'nin, uluslararası sistemde oluşacak yeni güç dengesinde yerini alabilmesi için her türlü tedbiri planlaması gerekmektedir. Ulusal devlet yapısını korumanın yolu askeri, politik, ekonomik bağımsızlıktan geçmektedir. Bu bağımsızlığı sürdürmenin tek yolu tüm tehditler için savunma planlarının yapılması, planlara ait tatbikatların icra edilmesi ve değişen koşullar gereği sürekli olarak güncellenmesidir. Askeri tehditler geçmişte olduğu gibi gelecekte de en büyük tehdit olacaktır. Türkiye, Türk Silahlı Kuvvetlerinin caydırıcılığına her zaman ihtiyaç duyacaktır. Unutulmaması gereken en önemli husus, gelişen teknoloji ışığında TSK'yı ve tüm savunma sistemlerini güncel halde tutmak ve gelebilecek tehditlere karşı korumaktır. 10.000 adet savaş uçağının bulunması bir ülke için büyük bir güçtür. Düzgün ve güncel bir siber savunma sistemi olmadan gerçekleşebilecek siber saldırı sonucu bu uçaklardan bir tanesinin bile havalanamayacak hale getirilmesi ihtimali siber tehditlerin önemini göstermek için verilebilecek tahmine dayalı ufak bir senaryodur.

Siber güvenlik Türkiye'nin en öncelikli konuları arasında yer almaktadır. Kesinlikle hafife alınmamalı, kurumlar siber tehditlere karşı daima hazır bulundurulmalı ve en önemlisi güncel, aktif ve güçlü bir siber savunma alt yapısının devamlılığı sağlanarak geliştirilmesi gerekmektedir.

KAYNAKÇA

Acar, C, (1991), Soğuk Savaş Dönemi Süper güçlerin Hâkimiyet Kavgası, Frapan Yayıncılık, Ankara: ACAR sayfa 214'ten aktaran BİLGİLİ, F, F, (2008), Geçmişten Günümüze NATO, Cumhuriyet Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, Sivas, s. 43.

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

Akgül, Ö, (2008), Soğuk Savaş Sonrası Dönemde NATO-AB İlişkileri ve Türkiye'ye Etkileri: Rekabet ve İşbirliğinin Jeopolitiği, Yayımlanmamış Yüksek Lisans Tezi, Harp Akademileri Komutanlığı Stratejik Araştırmalar Enstitüsü, İstanbul. s.4-3.

Alacakaptan, A, (1984). Türk Dış Politikasında NATO'nun Yeri, NATO Savunma ve Eğitimi Yönleri Sempozyumu,(Haz. Cahit Kavcar), AÜ. Basımevi, Ankara: Alacakaptan sayfa 40'tan aktaran Bilgili, F, F, (2008), Geçmişten Günümüze NATO, Cumhuriyet Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, Sivas, s. 43.

Altuntas, B, (2018), Adli Bilişim'de Mobil Cihazlar Ve Mobil Cihazlar Üzerinde Ekran Desen Kilidi ve Pin Kodunun Tespit Edilmesi, Yüksek Lisans Projesi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara. s.3-25

Angın, A, (1967), Küba ihtilâli, İstanbul: Kitapçılık Ticaret Limited Şirketi Yayınları, ANGIN sayfa.59'dan aktaran BİLGİLİ, F, F, (2008), Geçmişten Günümüze NATO, Cumhuriyet Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, Sivas: s. 44.

Armaoğlu, F, (1949). Sovyet Amerikan Münasebetlerinin Üç Yılı (1945-1948), A. Ü.S.B.F.D. C. 4, Ankara, , s.417-418.

Ataöv, T, (1970). NATO andTurkey, Ankara: Sevinç Printing House, s.108.

Aydın, M. ve Ereker, F, (2013), Türkiye'de Güvenlik: Algı, Politika, Yapı, İstanbul Bilgi Üniversitesi Yayınları, İstanbul: Aydın ve Ereker sayfa 2-3'den aktaran Şahin, G, (2016). Küresel Güvenlik ve NATO, 1. Baskı. Ankara: Detay Yayıncılık, s. 24.

Aydın, M, "Uluslararası İlişkilerin "Gerçekçi" Teorisi: Kökeni, Kapsamı, Kritiği", Uluslararası İlişkiler, Cilt 1, Sayı 1 (Bahar 2004), s. 33-60.

Bağbaşlıoğlu, A, (2016), Güncelliğini Yitirmeyen Bir Sorun Olan Yük Paylaşımına Yeni Bir Çözüm Arayışı: Akıllı Savunma ve NATO (A New Solution Seeking for a Timeless Issue Burden Sharing: Smart Defense and NATO), Akademik Bakış Dergisi, s. 3-8.

Başyurt, E, (1998). Ates Yolu: Boğazlarda Bitmeyen Kavga, İstanbul: Timas Yayınları, s.68.

Bıçakçı, S, (2012), Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu, Uluslararası İlişkiler, Cilt 9, Sayı 34, s. 205-226.

Bıçakçı, S, (2013), 21. Yüzyılda Siber Güvenlik, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, s. 45-46

Bilbilik, E, (2008). Kıskaç Harekâtı: NATO'nun Yeni Stratejik Konsepti, İstanbul, Profil Yayıncılık, , s.26.

Bilgili, F, F, (2008), Geçmişten Günümüze NATO, Cumhuriyet Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, Sivas, s.19-94,

Birdişli, F, (2014). Teori ve Pratikte Uluslararası Güvenlik: Kavram-Teori-Uygulama, Seçkin yayınevi, Ankara, s.15-16,

Coşkun, B, (2017), Türk Kamu Yönetimi Perspektifinde Soğuk Savaş Sonrası Oluşan Yeni Tehditler, Alternatif Politika,9 (1), s.109-115.

Çakmak, H ve Altunok, T, (2009), Suç, Terör ve Savaş Üçgeninde Siber Dünya, Ankara, Barış Platin Kitapevi yayınları, s.25

Çalış, Ş, Akgün, B, Kutlu, Ö, (2006), Uluslararası Örgütler veTürkiye, Konya, Çizgi Kitabevi Yayınları, s.183.

Çayhan Esra B. (2002), Avrupa Güvenlik Ve Savunma Politikası Ve Türkiye Akdeniz İ.İ.B.F. Dergisi (3),s.49.

Çelebi, Ö, (2007), Güvenlik, Uluslararası İlişkiler: Giriş, Kavram ve Teoriler, Çakmak, H, (Ed.), Ankara, Platin yayınları, s.70,

Çomak, H, (2005). Avrupa'da Yeni Güvenlik Anlayışları ve Türkiye: Soğuk SavaşSonrası Avrupa'da Güvenlik Yapılanması Sorunları, İstanbul, Tasam Yayınları, s.19.

Davutoğlu, A, (2009). Stratejik Derinlik, İstanbul, Küre Yayınları, s.230.

Deniz, T, (2012), Büyük Orta Doğu Projesi - Nato Ve G8 İlişkisi, e-Journal of New World Sciences Academy, Volume: 7, Number: 4, ArticleNumber: 4C0152, ISSN:1306-3111, s.363.

Diriöz, Ali O, (2012), NATO'nun Ortadoğu'ya Yönelik Politikası ve Kurumsal Programları, Ortadoğu Analiz Dergisi, Nisan- Cilt: 4 - Sayı: 40, s.50-56.

Efegil, E, Musaoğlu, N, Soğuk Savaş Sonrası Dönemde Uluslararası Sistemin Yapısına İlişkin Bir Model Çalışması, Gazi Akademik Bakış Dergisi, Cilt 2, Sayı 4, s. 1-25

Gökçe, A, (2005),Tarihi perspektifi ile 21.yy'da NATO, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası ilişkiler ana bilim dalı, Ankara, s 19.

Gönlübol, M. vd., (1969),Olaylarla Türk Dış Politikası 1919-1965, Sevinç Matbaası, Ankara, s.70.

Güntay, V, (2017), Uluslararası Sistem Ve Güvenlik Açısından Değişen Savaş Kurgusu; Siber Savaş Örneği, Trabzon, Güvenlik Bilimleri Dergisi, Kasım 2017, 6 (2), s. 81-108.

Hasanlı, C, (2012), Soğuk Savaş Dönemi Türkiye-Sovyetler Birliği İlişkileri, Toprak, E ve Kılıç, H (Ed.), Orta Asya ve Kafkaslarda Siyaset, Eskişehir, Anadolu Üniversitesi, s.53.

Hiçyılmaz, S, (2004). Halklara Karsı Bir Örgütlenme NATO Kurulusundan İstanbul Zirvesine, İstanbul: Sosyal Araştırmalar Vakfı, s.42.

Kara, M, (2013), Siber Saldırılar - Siber Savaşlar ve Etkileri, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, İstanbul, s.6-39

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, s.68.

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:, s. 55-72.

Kibaroğlu, M, (2017), Türkiye-NATO İlişkileri, ANALİZ Seta Siyaset, Ekonomi Ve Toplum Araştırmaları Vakfı, İstanbul, Mart 2017 Sayı: 191,s.10.

Koyuncu, H, NATO'nun Yeni Stratejik Konsepti İle Birlikte NATO İçerisinde Türkiye'nin Konumu, Atılım Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, Ankara, 2010:s.12 -13

Kuloğlu, A, (2001), "21. Yüzyıl Başlangıcında NATO, Avrupa ve Türkiye". İ. Bal (ed.) 21. Yüzyılın Eşiğinde Türk Dış Politikası. İstanbul Alfa Yayınları, s.586.

Kuloğlu, A, (2009). "60.Yılında NATO ve Türkiye İlişkileri", Ortadoğu Stratejik Araştırmalar Merkezi, Rapor 2, Ankara, s.10.

Kurnaz, İ, (2016), Siber Güvenlik Ve İlintili Kavramsal Çerçeve, Cyber Politik Journal (Siber Politikalar Dergisi),A Peer Review International E-Journal on Cyber politics, Cyber security and Human Rights, ISSN: 1769-6500, Vol.1, No.1, Winter 2016 www.cyberpolitikjournal.org, s.56-59.

Küçükşahin, A, Akkan, T, (2007), Değişen Güvenlik Algılamaları Işığında Tehdit Ve Asimetrik Tehdit, Dergi Pak Akademi, Sayı:5, s.46-47.

Mehmetçik, H, (2015), 21. Yüzyıl için Caydırıcılık: Teori ve Pratikte Neler Değişti?, Güvenlik Stratejileri Yıl: 11 Sayı: 22, http://dergipark.gov.tr/download/article-file/84600, s.31-59,

Meral, M, (2015), Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi, Harp Akademileri Stratejik Araştırmalar Enstitüsü Savunma Kaynakları Yönetimi Ana Bilim Dalı, İstanbul, s. 54-73

NATO El Kitabı, (1995). NATO Enformasyon Servisi, Brüksel: s. 178.

NATO Handbook, (2001), Brussels: NATO Office of Information and Press, s.81-83

Nye, J. S. (2005), Dünya Siyasetinde Başarının Yolu Yumuşak Güç, Çev: Aydın, R. İ. Elips, Ankara, s.100-101

Özdal, H, (2016), Sovyetler Birliğinin Dağılmasından Kırım'ın İlhakına Rus Dış Politikasında Ukrayna, Ankara, Uşak Yayınları, s.71-72.

Özdemir, H, Uluslararası İlişkilerde Güç: Çok Boyutlu Bir Değerlendirme Ankara Üniversitesi SBF Dergisi, Eylül 2008- Cilt 63, Sayı:3, s.113-144

Özgöker, U, (2006). Uluslararası Siyasi, Askerî ve Ekonomik Örgütler, İstanbul, Der Yayınları, s.115.

Özkan, G, (2010).Soğuk Savaş Sonrası Orta Asya Ve Kafkasya Ekseninde Türkiye-NATO-Rusya İlişkileri Ve Türk Dış Politikasına Yansımaları Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi 12/1 109-1322. s.114.

Peksarı, D. G, (2007). NATO'nun Değişen Konsepti, Ankara, Asil Yayınları, , s1-180.

Rüşen, S, 2018, Normatif Güç Bağlamında AB'nin Uluslararası Konumu Üzerine Tartışmalar, Sosyal Bilimler Dergisi Yıl: 5, Sayı: 23, Mayıs 2018, s. 336-354

Sağıroğlu, Ş ve Bulut, H, (2009), Mobil Ortamlarda Bilgi Ve Haberleşme Güvenliği Üzerine Bir İnceleme,Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, http://www.mmfdergi.gazi.edu.tr/article/viewFile/1061000183/106100015, Cilt 24, 3, s.501-505,

Sander, O, (1979). Türk-Amerikan İlişkileri 1947 - 1964, Ankara, Ankara Siyasal Bilgiler Fakültesi Yayınları, s.64-304

Sarınay, Y, (1988).Türkiye'nin Batı İttifakına Yönelişi ve NATO'ya Girişi, Kültür ve Turizm Bakanlığı, Ankara, s.240.

Şahin, G, (2016). Küresel Güvenlik ve NATO, 1. Baskı. Ankara: Detay Yayıncılık, s. 23.

Şahin, G, (2017), Küresel Güvenliğin Dönüşümü; NATO Bağlamında Kavramsal, Tarihsel ve Teorik Bir Analiz, Savunma Bilimleri Dergisi, Cilt 16, Sayı 2, s. 59-81

Şenol, M, (2017), Türkiye'de Siber Saldırılara Karşı Caydırıcılık, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:3, No:2, s.1-9.

Şenyuva, Ö ve Üstün, Ç, (2013). NATO-Türkiye İlişkileri Türkiye Kamuoyu ve Elit Algıları, İstanbul, İstanbul Bilgi Üniversitesi yayınları, s. 14.

Tüysüzoğlu, G., (2013),Savunmacı Realizm ve Saldırgan Realizm Bağlamında Karadeniz Havzası'ndaki Çatışma Gerçekliğinin Değerlendirilmesi, AVRASYA ETÜDLERİ, 44/2013-2, Ankara, s.57-85

Uzgel, İ, (2005). "ABD ve NATO'yla İlişkiler", Türk Dış Politikası: Kurtuluş Savaşından Bugüne Olgular, Belgeler, Yorumlar, ed. Baskın Oran, Cilt 2, 4. Baskı, İstanbul, İletişim Yayınları, s.306.

Wittmann, K,(2009). Towards A New Strategic Concept For NATO, Rome, NATO Defense College Research Division, , s.14-15.

Yayla, M, (2013), Hukuki bir terim olarak "siber savaş", Türkiye Barolar Birliği Dergisi, İstanbul, Sayı:104, s.179-181.

Yılmaz, S ve Salcan, O, (2008), Siber Uzayda Güvenlik ve Türkiye, İstanbul, Milenyum yayınları, s.35.

Yılmaz, S, (2008), Uluslararası İlişkilerde Güç ve Güç Dengesinin Evrimi, Beykent Üniversitesi Stratejik Araştırmalar Dergisi, İstanbul, Sayı 1 (01), 2008, 27-65

(http-1) Gözen R. Türkiye'nin Ortadoğu Politikası: Gelişimi ve Etkenleri, https://www.tarihtarih.com/?Syf=26&Syz=354821&/T%C3%BCrkiyenin Orta-do%C4%9Fu-Politikas%C4%B1:-Geli%C5%9Fimi-ve-Etkenleri-/-Do%C3%A7.-Dr. Ramazan-G%C3%B6zen- Erişim tarihi: 20.01.2018

(http-2) 1 …….(2014). Kuzey Atlantik İttifakı (NATO), http://www.bilgesam.org/Images/Dokumanlar/0-2-2014041722nato.ppt (Erişim tarihi: 30.01.2018)

(http-3) 2 ……..(2011) ,NATO Ortaklık Yoluyla Güvenlik, https://www.nato.int/docu/sec-partnership/sec-partner-turkish.pdf (Erişim tarihi: 30.01.2018)

(http-4) Pravda, A (2011), Russia And European Security: The Delicate Balance, https://www.nato.int/docu/review/1995/9503-4.htm, s.10. (Erişim tarihi: 30.01.2018)

(http-5) 3 …….. (2011) Türkiye Cumhuriyeti Dışişleri Bakanlığı, II. NATO ve Türkiye'nin Güncel NATO Konularına İlişkin Görüşleri, http://www.mfa.gov.tr/ii_-nato-ve-turkiye_nin-guncel-nato-konularina-iliskin-gorusleri.tr.mfa(Erişim tarihi: 31.01.2018)

(http-6) 4…….. (2011), Türkiye'nin NATO, BAB ile Avrupa Güvenlik Ve Savunma Kimliği'ne Bakış Açısı, http://www.tasam.org/trTR/Icerik/2318/turkiyenin_nato_bab_ile_avrupa_guvenlik_ve_savunma_kimligine_bakis_acisi (Erişim tarihi: 30.01.2018)

(http-7) Rustamov, E (2007),Türkiye'nin NATO İle Olan İlişkisi,http://www.tasam.org/tr-TR/Icerik/530/turkiyenin_nato_ile_olan_iliskisi (Erişim tarihi: 01.02.2018)

(http-8) 5…….. (2011), Türkiye Cumhuriyeti Dışişleri Bakanlığı ,II. NATO ve Türkiye'nin Güncel NATO Konularına İlişkin Görüşleri, http://www.mfa.gov.tr/ii_-nato-ve-turkiye_nin-guncel-nato-konularina-iliskin-gorusleri.tr.mfa(Erişim tarihi: 30.01.2018)

(http-9) Çetin, S (2010), NATO'nun 2010 Stratejik Konsepti Ve Lizbon Zirvesi, https://avrupanaliz.wordpress.com/tag/nato-lizbon-zirvesinde-alinan-kararlar/(Erişim tarihi: 01.02.2018)

(http-10) Akçadağ Alagöz, E, (2012), NATO'nun 2012 Chicago Zirvesi Üzerine Değerlendirme,http://www.bilgesam.org/incele/1208/-nato%E2%80%99nun-2012-chicago-zirvesi-uzerine-degerlendirme/#.WnMfTojFKUl(Erişim tarihi: 01.02.2018)

(http-11) Wolfers, A (1952), National Security as an AmbiguousSymbolhttp://files.janjires.webnode.cz/2000000143cb1e3daba/Arnold%20Wolfers%20%20National%20Security%20as%20an%20Ambiguous%20Symbol.pdfPoliticalScienceQuarterly, Vol. 67, No. 4. (Dec., 1952), pp. 484-485. (Erişim tarihi: 15.03.2018)

(http-12) Boyraz, H.M. (2015), NATO'nun Siber Güvenlik Politikası: Tarihsel Süreç ve Kırılma Noktaları, Cilt IV, Sayı 12, s.32-40, Türkiye Politika ve Araştırma Merkezi (Research Turkey), Londra: Research Turkey http://researchturkey.org/tr/natos-cyber-security-policy-the-historical-process-and-critical-junctures/ (Erişim tarihi: 17.03.2018)

(http-13) 6…….. (2011),, NATO'nun Siber Güvenlik Politikası: Tarihsel Süreç ve Kırılma Noktaları, http://www.elektrikport.com/teknik-kutuphane/siber-savaslar-stuxnet/4383#ad-image-0(Erişim tarihi: 18.03.2018)

(http-14) 7…….. (2013), T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, http://www.udhb.gov.tr/doc/siberg/SOME_2013-2014_EylemPlani.pdf (Erişim tarihi: 19.03.2018)

(http-15) 8…….. (2018), NATO: Siber Savunmada Vites Değiştiriyor, NATO Dergisi, https://www.nato.int/docu/review/2016/Also-in-2016/cyber-defense-nato-security-role/TR/index.htm(Erişim tarihi: 20.03.2018)

(http-16) 9…….. (2018), 2018 Sonıcwall Siber Tehdit Raporu, Küresel Siber Silahlanma Yarışı için Hazırlanan Tehdit İstihbarat, Endüstri Analiz ve Siber Güvenlik Kılavuzu http://www.m2s.com.tr/bulten/2018_Sonicwall_siber_tehdit_raporu-TR.pdf(Erişim tarihi: 01.04.2018)

(http-17) 10…….. (2017), http://www.hurriyet.com.tr/dunya/finlandiyaya-hibrit-tehdit-merkezi-kurulacak-40424860 (Erişim tarihi: 02.04.2018)

(http-18) 11…….. (2017), http://qha.com.ua/tr/siyaset/9-ulkeden-hibrit-tehditle-mucadele-icin-ortak-merkez/154565/ (Erişim tarihi: 03.04.2018)

(http-19) 12…….. (2017), https://www.ntv.com.tr/dunya/nato-hibrit-tehditle-mucadele-merkezi-kuruluyor,p7iwh-CpLUWL6ehyCwqC0w (Erişim tarihi: 03.04.2018)

(http-20) 13…….. (2018), https://www.ntv.com.tr/dunya/nato-hibrit-tehditle-mucadele-merkezi-kuruluyor,p7iwh-CpLUWL6ehyCwqC0w (Erişim tarihi: 05.04.2018)

(http-21) 14…….. (2016), 2016-2019 Ulusal Siber Güvenlik Stratejisi, Ulaştırma Denizcilik ve Haberleşme Bakanlığı, http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf (Erişim tarihi: 26.04.2018)

(http-22) 15…… (2018), TÜBİTAK Bilgem Tarihçesi, Ulaştırma Denizcilik ve Haberleşme Bakanlığı,http://sge.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce, (Erişim tarihi: 04.12.2018)

(http-23) 16…… (2018), TÜBİTAK Bilgem NATO Çalışma Gruplarına Katılım,Ulaştırma Denizcilik ve Haberleşme Bakanlığı,http://sge.bilgem.tubitak.gov.tr/tr/nato-calisma-gruplarina-katilim, (Erişim tarihi: 04.12.2018)