**T.C.**
**YILDIZ TEKNİK ÜNİVERSİTESİ**
**SOSYAL BİLİMLER ENSTİTÜSÜ**
**İŞLETME ANA BİLİM DALI**
**SAVUNMA KAYNAKLARI YÖNETİMİ PROGRAMI**

**YÜKSEK LİSANS TEZİ**

# DEĞİŞEN PARADİGMALAR DOĞRULTUSUNDA SİBER TEHDİTLERİN SAVUNMA PLANLAMALARINDAKİ DÖNÜŞÜME ETKİLERİNİN İNCELENMESİ

**GÖRKEM KILINÇÇEKER**
**167A2003**

**TEZ DANIŞMANI**
**Doç. Dr. Fahri ERENEL**

**İSTANBUL**
**2018**

**T.C.**
**YILDIZ TEKNİK ÜNİVERSİTESİ**
**SOSYAL BİLİMLER ENSTİTÜSÜ**
**İŞLETME ANA BİLİM DALI**
**SAVUNMA KAYNAKLARI YÖNETİMİ PROGRAMI**

**YÜKSEK LİSANS TEZİ**

# DEĞİŞEN PARADİGMALAR DOĞRULTUSUNDA SİBER TEHDİTLERİN SAVUNMA PLANLAMALARINDAKİ DÖNÜŞÜME ETKİLERİNİN İNCELENMESİ

**GÖRKEM KILINÇÇEKER**
**167A2003**

**TEZ DANIŞMANI**
**Doç. Dr. Fahri ERENEL**

**İSTANBUL**
**2018**

T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANA BİLİM DALI
SAVUNMA KAYNAKLARI YÖNETİMİ PROGRAMI

YÜKSEK LİSANS TEZİ

# DEĞİŞEN PARADİGMALAR DOĞRULTUSUNDA SİBER TEHDİTLERİN SAVUNMA PLANLAMALARINDAKİ DÖNÜŞÜME ETKİLERİNİN İNCELENMESİ

GÖRKEM KILINÇÇEKER
167A2003

Tezin Enstitüye Verildiği Tarih:
Tezin Savunulduğu Tarih: 07.09.2018
Tez Oy Birliği / ~~Oy Çokluğu~~ ile Başarılı Bulunmuştur.

| | Unvan Ad Soyad | İmza |
|---|---|---|
| Tez Danışmanı | : Doç. Dr. Fahri ERENEL | |
| Jüri Üyeleri | : Prof.Dr. Halit KESKİN | |
| | Doç.Dr. Yasemin BAL | |

İSTANBUL
EYLÜL 2018

# ÖZ

## DEĞİŞEN PARADİGMALAR DOĞRULTUSUNDA SİBER TEHDİTLERİN SAVUNMA PLANLAMALARINDAKİ DÖNÜŞÜME ETKİLERİNİN İNCELENMESİ

**Görkem Kılınççeker**
**Eylül, 2018**

Günümüzün güvenlik ortamı, özellikle küresel boyutta bir dönüm noktası olarak kabul edilen Soğuk Savaş dönemi ile birlikte geleneksel tanımlamalarının ve çerçevesinin oldukça dışına çıkmış, farklı nitelikler kazanmıştır. Değişikliğe neden olan tehdit olguları da tamamen boyut değiştirmiş; amaçları, izlenen stratejisi, reaksiyonları, planlama usulleri, uygulama yöntemleri, aktörleri, teknolojinin kullanımı ve coğrafi çerçevesi gibi geçmiştekilerden çok daha farklı şekillerde karşılaşılır olmuş, simetrik düzlemden çıkarak asimetrik boyutlara ulaşmıştır. Bu bağlamda; günümüzün ve geleceğe yönelik yapılacak savunma planlamalarının temelinde "belirsizlik" kavramından bahsetmek mümkündür.

Uluslararası düzende yaşanan bu hızlı değişim ve dönüşüm süreci; sahip olunması gereken imkan ve kabiliyetleri başta olmak üzere barıştan itibaren sürecin tamamını etkilemeye başlamıştır. Farklı ve süratli düşünmeyi, ani ve beklenmedik durumlara, yeni tehdit türlerine süratle uyumlu olabilecek yetenekler geliştirmeyi gerektiren, alışılagelenin dışındaki savunma anlayışlarıyla birlikte paradigma değişimleri kaçınılmaz olmuştur.

Teknolojinin ve bilişim dünyasının süratli akışı içerisinde yaşanan değişim ve gelişmeler, paradigma değişimlerine esas teşkil eden asimetrik tehdit türlerine yeni bir boyut daha eklemiştir: Siber Tehditler. Siber uzaya olan bağımlılık gün geçtikçe artmaktadır. Bu yüzden siber tehditlerin çok geniş bir alanda faaliyet göstermesi ve klasik saldırılara nazaran daha yıkıcı etkilere ulaşabilmesi nedeniyle, savunma planlamalarında öncelik verilmesi gerekmektedir.

Belirtilen hususlar dahilinde çalışmanın amacı; savunma planlamalarındaki tarihsel süreç içerisinde meydana gelen paradigma değişimine sebep olan dönüm noktalarını ele almak suretiyle söz konusu değişikliklerin temelinde yatan ihtiyaçları açıklamak ve değişimlere ihtiyaç teşkil eden asimetrik tehdit türlerinden siber tehditleri, örnekleri ve etkileri üzerinden ele alarak, savunma planlamalarındaki yerlerini ortaya koyabilmektir. Ayrıca gerek Türkiye'nin gerekse ulaşılabilen veriler doğrultusunda örneklem olarak ele alınan diğer ülkelerin siber tehditlere yönelik; stratejilerini, planlamaya yönelik görev ve sorumluluklarını, teşkilatlanmaları çerçevesinde siber tehditlerin savunma planlama anlayışlarındaki dönüşüme etkilerine yönelik durum tespiti yapılmaya çalışılmıştır.

**Anahtar Kelimeler:** Soğuk Savaş, Savunma Anlayışı, Planlama, Belirsizlik, Paradigma Değişimi, Asimetrik Tehdit, Siber Uzay, Siber Tehdit.

## ABSTRACT

### EXAMINING THE EFFECTS OF CYBER THREATS TO TRANSFORMATION IN DEFENCE PLANNINGS IN LINE WITH THE CHANGING PARADIGMS

**Görkem Kılınççeker**
**September, 2018**

Today's security environment, especially with Cold War Era which is admitted a milestone on a global scale, has quietly gone beyond the conventional definitons and environments, has gained different qualifications. The threats that caused to change, completely replaced; iams, strategies, reactions, planning concepts, ipmlementation methods, actors, usage of technology and geographic environment has been different than past has been encountered with very different ways. It had also reached to asymmetrical dimensions by leaving from symmetrical plane. In this context, it's possible to mention that the "uncertainty" notion is in the basis of defence plannings of today and future.

The fast of change and transformation in international systemhas started to effect the whole process from peace time, mainly possibilities and capabilities that has been need to have. With the extraordinary, unconventional defence perceptions that has been required to develop the skills which is compatible to different and quick thinking, sudden and unexpected situations, new threat types, so the paradigm shifts have become inevitable.

The changes and transformations that was lived in the fast run of technology and world of information, had added a new dimension to the asymmetrical types which was a basis of the paradigm shifts: Cyber Threats. The addiction to the cyber space has increased day by day. So, since the Cyber Threats has been able to operate in a very wide area and reach to more devastating effects than the conventional attacks, it should be given a priority in defence plannings.

Within the stated issues, the aim of the study is to explain the needs in the basis of changes which was occured that caused to paradigm shifts by mentioning the milestones in historical process and to present the situation of the cyber threats in defence plannings which is a type of asymmetrical threats. Also it had been tried to make an assessment about the effects of cyber threats to the defence planning understandings in the scope of the strategies, missions and responsibilities about planning, organizations of Turkey and the other countries were choosen with accessible datas.



**Key Words:** Cold War, Notion of Defence, Planning, Uncertainity, Paradigm Shift, Asymmetric Threat, Cyber Space, Cyber Threat.

# ÖN SÖZ

Öncelikle Harp Akademileri Stratejik Araştırmalar Enstitüsü Savunma Kaynakları Yüksek Lisans bölümündeki öğretim süresince bilgi ve birikimlerini benimle paylaşarak tez çalışmamın temelini oluşturan değerli öğretim elemanlarına ve elimizde olmayan sebepler nedeniyle uzun bir müddet ara vermek zorunda kaldığımız öğretim sürecinin sonlandırılmasına yönelik teşvikleriyle bana destek olan değerli arkadaşlarıma;

Ders ve tez yazım süresi boyunca gerek akademik gerekse tecrübi olarak bana yol gösteren danışman hocam Sayın Doç.Dr. Fahri ERENEL ve yoğun programına rağmen tüm samimiyetiyle sormuş olduğum sorulara cevap verip, çalışmama ilişkin görüş ve önerilerini belirten Sayın Prof.Dr. Haluk KORKMAZYÜREK'e;

Yüksek lisans sürecimin son bölümünde dahil olduğum Yıldız Teknik Üniversitesi'nde yardımlarını esirgemeyen Sosyal Bilimler Enstitüsü ve İşletme Ana Bilim Dalı yönetimi ve personeline;

Son olarak; aldığım her kararda, attığım her adımda sabırla ve büyük bir heyecanla beni destekleyen canım aileme teşekkürü borç bilirim.

İstanbul; Eylül, 2018 Görkem Kılınççeker

## İÇİNDEKİLER

## TABLOLAR LİSTESİ

## ŞEKİLLER LİSTESİ

## KISALTMALAR

| | | |
|---|---|---|
| **ABD** | : | Amerika Birleşik Devletleri |
| **ARGE** | : | Araştırma Geliştirme |
| **ARPANET** | : | Gelişmiş Araştırma Projeleri Dairesi Ağı |
| **CIA** | : | Merkezi İstihbarat Teşkilatı |
| **DOD** | : | Department of Defense |
| **ENISA** | : | Avrupa Ağ ve Bilgi Güvenliği Kurumu |
| **EYP** | : | El Yapımı Patlayıcı |
| **KGB** | : | Sovyet Gizli Haber Alma Teşkilatı |
| **MSB** | : | Milli Savunma Bakanlığı |
| **MOSSAD** | : | İsrail Gizli Haber Alma Örgütü |
| **NATO** | : | North Atlantic Treaty Organisation |
| **PKK** | : | Kürdistan İşçi Partisi |
| **TSK** | : | Türk Silahlı Kuvvetleri |
| **USA** | : | United States of America |
| **USGS** | : | Ulusal Siber Güvenlik Stratejisi |
| **TÜMAS** | : | Türkiye Milli Askeri Stratejisi |
| **SHAPE** | : | Avrupa Müttefik Kuvvetler Komutanlığı |
| **SOME** | : | Siber Olaylara Müdahale Ekibi |
| **SSCB** | : | Sovyet Sosyalist Cumhuriyetler Birliği |
| **SSM** | : | Savunma Sanayii Müsteşarlığı |

# 1. GİRİŞ

Soğuk Savaş Dönemi'nin son bulmasıyla birlikte tüm dünya genelinde hissedilen güvenlik ve savunma anlayışındaki değişimler, özellikle 11 Eylül saldırıları sonucunda; tehdit algısı, savunma konsept ve anlayışında da köklü değişiklikler gereksinimini doğurmuştur. Bu bağlamda 11 Eylül saldırılarıyla birlikte bir terim olarak küresel manada kabul gören asimetrik tehdit kavramının, önceden bilinen savunma ve güvenlik stratejilerinin yeniden değerlendirilmesi ve değişen tehdit algısına göre şekillendirilmesine zemin oluşturması nedeniyle savunma ve güvenlik planlamaları açısından bir dönüm noktası olduğu varsayılmaktadır. Devletlerin tehdit algısındaki değişimi ve belirsizliği en aza indirme çabası; savunma planlamalarında bilinen paradigmalarının değişimine ve güvenlik ihtiyaçlarına cevap verebilecek, muhtemel tehdit algılarına karşı koyabilecek şekilde dönüşüme ayak uydurmalarını zorunlu kılmıştır[1].

Güvenlik stratejilerinin belirlenmesi esnasında temel araştırma konusu; tehdidin türü ve nasıl önleneceğine yönelik çabaların değerlendirilmesidir. Günümüz gerçekleri ve tecrübleri ışığında tehditlerin çeşitliliği ve belirsizliği etkin bir savunma mekanizması oluşturulmasına imkân vermemektedir. Bu durumda eldeki kaynakların en verimli şekilde kullanılması için öncelikler belirlenmelidir. Devletlerin uygulayacağı güvenlik stratejileri, doğası gereği sürekli değişim içerisindeki asimetrik tehditlere göre paralellik göstermeli ve ona uyumlu olarak önlemlerin alınması gerekmektedir.

Bilgi Çağındaki değişimler ve teknolojik gelişmeler, sürekli boyut değiştiren asimetrik tehdit türlerine yeni bir kavram daha eklemiştir: Siber Tehdit. Siber tehditlerin, uygulayana ne gibi avantajlar sağladığı, maruz kalanın ise hangi boyutlarda etkilendiği çalışmanın ilgili bölümlerinde anlatılmaya çalışılmıştır. Özellikle son yüzyılda meydana gelen siber saldırılar ve sonucunda elde edilen tecrübeler, asimetrik kavramın sınırlarının ne kadar öngörülemez olabileceğini doğrulamaktadır. Buna binaen, günümüz savunma ve güvenlik planlamalarında kendisine önemli yer edinen siber tehditleri minimize etme çabaları, teknolojik

[1] Francois Vrey, "Paradigm Shifts, South African Defence Policy And The South African National Defence Force: From Here To Where?", **Scientia Militaria: South African Journal of Military Studies**, c.32, s.2 (2004): 90.

gelişmelerden yararlanarak; yeni, daha karmaşık ve teknolojik sistemlere sahip olmakla eşdeğer tutulmaktadır.

Bilişimin sağladığı imkânların olumsuz yönde kullanımının çok ciddi bir tehdit haline dönüştüğü günümüz dünyasında devletler, sanal silah üretimine büyük önem vermektedirler. Bu nedenle ortaya çıkan bu yeni tehdit türünün şüphesiz tehdit kategorisinde ilk sıralara konulması gerekmektedir. Çok hızlı bir biçimde metot geliştiren ve değiştiren, teknolojinin imkânları sayesinde nerdeyse hiçbir emare bırakmayan, sonsuz bir siber boşlukta kaybolmasını sağlayan soyut bir düşmanla mücadelenin ne kadar zor olduğunu devletler, çok ciddi sonuçlara sebep olan tecrübelerle anlamaya başlamışlardır. Bu bağlamda siber tehditleri, bir asimetrik tehdit türü olarak günümüzün en sinsi savaş yöntemlerinden birisi olarak tanımlamak mümkündür.

Siber uzayın genişliği düşünüldüğünde tehdidin kaynağın sınırsız olabileceği unutulmamalıdır. Bu sebeple özel ve kamu sektörünün, devletlerin bu anlamdaki güvenlik yapılanmalarının ve uluslararası yapılanmaların, sürekli bilgi paylaşımında bulunması tehdidin kaynağını belirlemek için kullanılabilecek yöntemlerin esasını oluşturmaktadır. Siber uzayın her an gelişen bir yapıda olması sebebiyle güvenliğin ve kontrolün bir an bile bırakılmaması gerekmektedir[2].

Durum ve olgu tespiti odaklı olan bu çalışma, herhangi bir hipotez geliştirme amacı gütmemektedir. Araştırmanın konusu, savunma planlamalarındaki paradigma değişimleri ve değişen güvenlik anlayışı çerçevesinde bir asimetrik tehdit türü olan siber tehditlerin savunma planlamalarına etkilerinin incelenmesidir. Çalışma üç ana bölümden oluşmaktadır. Girişe müteakip birinci bölümde; savunma ve güvenlik anlayışlarındaki değişime temel dayanak olan üç dönemin (Soğuk Savaş öncesi, esnası ve sonrası) karşılaştırılması ve bu anlayışlar arasındaki farklara binaen savunma planlamalarında ortaya çıkan paradigma değişim ihtiyaçları ele alınmıştır. Bu bölümde temel amaç, araştırmanın ilerki safhalarında karşılaşılacak kavramlar için ön bilgilendirme yapmak ve müteakip bölümlerde ortaya çıkacak kavramlara zemin oluşturmaktır. Bu çerçevede, birbirleri ile yakın ilişkide oldukları değerlendirilen dönemler gruplandırılarak birlikte ele alınmışlardır. Bahse konu dönemlerin çok daha farklı boyutlarda ve çok daha ayrıntılı olarak ele alınmaları mümkün olsa da; çalışmanın genel çerçevesini oluşturan "savunma yaklaşımları" ve "paradigma değişimi" kavramları açısından değerlendirilerek aralarındaki ilişkilerin ortaya konulması amacıyla literatüre seçici yaklaşılmıştır. Bu kapsamda temel yaklaşım, belirli bir düşünceyi desteklemek ya da eleştirmek değil, ilgili kavramların

[2] Zafer Yener, “Siber Uzay Güvenliği: Ulusal Güvenlik ve Uluslararası Güvenliğe Etkileri” (Yüksek Lisans Tezi, Uludağ Üniversitesi, 2013), 1.

mümkün olduğunca konu kapsamındaki farklı yönlerinin ortaya konulması şeklinde olmuştur.

İkinci bölümde, asimetrik savaşların kavramı ve kapsamı ile tarihsel süreci ve çalışmanın odağında bulunan bir asimetrik tür olan siber tehdit kavramı, konuya ilişkin terimlerin yanı sıra siber tehditlerin boyutları ve ulaşılabilen kaynaklardan alınan mevcut veriler üzerinden siber tehditlerin etkileri açıklanmaya çalışılmıştır. Bu bölümde üzerinde durulan hususlardan amaçlanan, nihai bölümdeki ana resmin görülebilmesine zemin hazırlayabilmektir.

Çalışmanın son bölümünde ise, ulaşılabilen veriler doğrultusunda örneklem olarak ele alınan diğer ülkelerin siber tehditlere yönelik; stratejilerini, planlamaya yönelik görev ve sorumluluklarını, teşkilatlanmaları çerçevesinde siber tehditlerin savunma planlama anlayışlarındaki dönüşüme etkilerine yönelik durum tespiti yapılmaya çalışılmış, Türkiye örneği üzerinden şimdiye kadar yayımlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planları üzerinden ülkemizin siber güvenlik stratejisine yönelik bir değerlendirme yapılarak siber tehditlerin savunma planlamalarına etkileri inceleme amaçlanmıştır.

Araştırma konusuna yönelik metodoloji ile ilgili kavramlar şu şekilde açıklanmıştır;

**Çalışmanın Amacı:** Savunma planlamalarında tarihsel süreç içerisinde meydana gelen anlayış değişikliğine sebep olan dönüm noktalarını ele almak suretiyle söz konusu değişikliklerin temelinde yatan ihtiyaçları açıklamak, savunma yaklaşımlarında değişimlere dayanak oluşturan yeni tehdit türlerinden en belirsizi olduğu değerlendirilen Siber tehditlerin tarihsel süreci, örnekleri ve ulaşılabilen veriler üzerinden sonuçlarını ele alarak, söz konusu siber tehditlerin günümüz savunma planlamalarındaki yerlerini ortaya koyabilmektir. Ayrıca gerek Türkiye'nin gerekse ulaşılabilen veriler doğrultusunda diğer ülkelerin siber tehditlere yönelik stratejileri doğrultusunda; alınan tedbirleri, başta askeri olmak üzere teşkilatlanma çabaları, plan ve projeleri ile örneklem olarak ele alınan ülkelerdeki siber tehditlerin savunma anlayışlarına olan yansımalarına yönelik durum tespiti yapabilmek çalışmanın amacı olarak değerlendirilmiştir.

**Çalışmanın Önemi:** Çalışma;

a. Savunma anlayışları ve planlamalardaki değişikliğe sebep olan veya olabilecek esasları ortaya koyması,

b. Bir asimetrik savaş unsuru olan siber tehditlerin günümüz dünyası, ülke savunma planlamalarındaki yeri, geleceğe yönelik atılabilecek adımların değerlendirilmesi,

c. Siber tehditlerin savunma planlamalarına etkileri ile örnek olarak ele alınan diğer ülkelerin savunma planlama modellerini ortaya koyarak durum tespiti yapılabilmesini sağlamak, müteakip dönemlerde benzer konularda yapılabilecek olan yüksek lisans veya daha geniş kapsamlı bir doktora çalışması için bilgi paylaşımına imkan vermek, ortaya çıkan neticeler doğrultunda savunma planlayıcıları tarafından ilerde yapılacak olan çalışmalar için bir değerlendirme kriteri, belirlenecek yol haritalarına yönelik bir rehber kaynak olabileceği değerlendirildiğinden önemli olabileceği varsayılmaktadır.

**Çalışmanın Kapsamı ve Sınırlılıkları:** Bu çalışmanın evreni savunma planlamalarında görev alan ve milli gücün askeri boyutunu oluşturan Türk Silahlı Kuvvetleri ile konuya ilişkin çalışmalar yürüten ülkelerden bazılarıdır. Bununla birlikte, değerlendirilen unsurlardan TSK ve çalışmanın örneklem uzayında bulunan ülkeler ile ilgili verilere ulaşılabilen ölçülerde yer verilerek bir analiz yapılmaya çalışılmıştır. Söz konusu verilerin açık kaynaklarda yer aldığı kadarıyla ele alınması çalışmanın kapsamını belirleyen esas faktörü oluşturmaktadır. Savunma planlamalarında söz sahibi olan kurum olarak değerlendirilen TSK ve savunma alanında faaliyet gösteren kurum ve kuruluşların faaliyet alanlarının belirli kurallar dahilinde "gizlilik" prensibine dayanması ve bununla beraber siber saldırı eylemlerin tespitinin zor olması, çoğu zaman da saldırıya uğrayanlar tarafından açıklanmamasından dolayı verilen örneklerin alanı kısıtlı kalmıştır. Bunun yanı sıra siber tehditlere ilişkin tarihsel süreç çok gerilere dayanmamakla birlikte şimdiye kadar basılı, yayımlanan yayın miktarı çok fazla olmadığından verilerin kısıtlı olduğu görülmüştür.

Veri toplama sürecinde yapılan görüşmeler genelde; bilgisine başvurulan, veri toplamada çalışmaya katkıda bulunan kişi ve kurumlar ile elektronik posta ve telefon vasıtasıyla iletişime geçilmesi şeklinde icra edilmiş, alınan notlar ve geri bildirimler çalışmanın ilgili bölümlerinde kullanılmak üzere raporlama süreci yürütülmüştür.

Bunun yanı sıra, açık kaynak ve literatür taramasının haricinde özellikle görüşme yapılan yerlerin, konuya ilişkin bilgisine ulaşılan kişi ve kurumların genel olarak Ankara ve İstanbul'da yoğunlaşması ve raporlama yapılan yere uzak olması, söz konusu şahısların iş yoğunlukları nedeniyle planlanan verimli araştırma süresinin dışına çıkılması, elektronik posta ile istenen bilgilere ve sorulan sorular geç yanıt verilmesi çalışmanın zaman kısıtlamasına sebep olan faktörleri olarak öne çıkmıştır.

Siber uzay ve siber tehditlerin, bilişim dünyasındaki sürekli ve ani değişikliklere paralel olarak kendini güncellemesi nedeniyle yapılan araştırma süresi içinde bile

değişen veriler; erişildiği, çalışmanın yapıldığı zaman dilimi ile sınırlı olup gelecekte ulaşılabilecek, öngörülemeyen durumlara ilişkin verilere yönelik herhangi bir mutlak ifade veya tespit içermemektedir.

**Varsayımlar:** Araştırmada bilgisine başvurulan, çalışmaya kaynak oluşturulan kişi ve kurumların uzman görüşlerini samimi ve gerçeğe uygun yanıtladıkları varsayılmıştır. Ayrıca, siber tehditlere karşı kesin ve her daim bir savunma yöntemi bulunmadığından yapılan savunma planlama yaklaşımlarının genel olarak tehdide yönelik varsayımlara dayanan muhtemel hareket tarzlarını içerdiği görülmüştür.

**Veri Toplama Yöntemi:** Çalışmada verilerin toplanması iki aşamalı olarak gerçekleştirilmiştir. Öncelikle, belgesel tarama yöntemi ile savunma planlama yaklaşımlarındaki paradigma değişimleri ve bu değişim ihtiyacına sebep olan etmenler, asimetrik savaşlar ve onun bir türü olan siber tehditlere yönelik özellikle kavramsal bulgulara yönelik; basılı yayın ve dokümanlar ile bilimsel ve akademik veri tabanlarındaki kitap, makale, dergi, konularla ilişkin olabileceği değerlendirilen tezler, açık ağ üzerinden ilgili kurum ve organizasyonlar tarafından yayınlanan raporlar araştırılmıştır.

Nitel araştırma teknikleri arasında en çok kullanılmakta olan görüşme, bu çalışmaya yönelik kısmen uygulanmaya çalışılmış, yüz yüze görüşme imkanı sınırlı olduğundan genel olarak konuya ilişkin uzman kişilere önceden hazırlanmış sorular ile belli bir sistematik dâhilinde elektronik posta veya telefon görüşmesi yapmak suretiyle sorulmuş, edinilen bilgi ve veriler çalışmanın ilgili bölümlerine girdi yapılmak üzere kaydedilmiştir. Dolayısıyla çalışmayı yapana bir çok açıdan avantaj sağlayan kısmen yarı yapılandırılmış görüşme tekniği, çalışmanın sınırlılıkları bölümünde de belirtilen esaslar dahilinde uygulanmaya çalışılmıştır.

Belirtilen yöntemlerin yanı sıra ders ve araştırma süreci müddetince katılım sağlanan (geneli 2016 ve 2017 yılında icra edilen) eğitim ve konferanslar (Siber Tehditlere Yönelik Farkındalık Eğitimi, Müşterek Ağ Tabanlı Yapılar Kursu, Bilgi Güvenliği Eğitimi vb.), TSK Siber Savunma Komutanlığı'nda görevli uzman personeller ile yapılan görüşmeler, Kara Harp Akademisi Stratejik Araştırmalar Ensitüsü tarafından icra edilen gezilerde ilgili kişi ve kurumlarla yapılan görüşmeler sonucunda edinilen bilgi ve belgeler, çalışmanın veri toplama sürecini oluşturmuştur.

**Verilerin Analizi:** Veri toplama maksadıyla araştırma sürecinde kısmen yapılan yarı yapılandırılmış görüşme tekniği neticesinde elde edilen bilgi ve belgeler sistematik bir biçimde değerlendirilerek çalışmanın ilgili bölümlerine dahil edilmiştir.

## 2. KAVRAMSAL ÇERÇEVE

Savunma gereksinimi, tarih boyunca hem insanlar hem de devletler için mutlak bir ihtiyaç olarak yer almaktadır. Bu gereksinimi karşılamak için tehdidin ezeli ve ebedi olduğu insanlık tarihinde bireysel, ulusal veya uluslararası manada bazı tedbirlerin alınması zorunlu kılınmıştır. Alınan bu tedbirler planlama adı altında değerlendirilerek; tehdide yönelik en caydırıcı, en maliyetsiz, en süratli alınacak tedbirler planlama sürecinin esasını oluşturmuştur.

Milli güvenlik sistemi içerisinde, bir devletin milli değerlerini, milli çıkarlarını ve milli hedeflerini elde etmesine ya da korumasına engel olmak amacıyla başka bir devlet tarafından alınan tertip ve tedbirler[3] olarak tanımlanan tehdit algısındaki değişiklikler, devletlerin savunma ve güvenlik anlayışlarının da zaman içerisinde belirli evrimler geçirmesini zorunlu kılmıştır. Bu değişimler, ülkelerin savunma ve güvenlik anlayışlarına paralel olarak oluşturdukları üst politika belgelerinde de değişikliğe gidilmesine yol açmıştır[4].

Savunma planlaması ile ilgili olarak birçok tanım bulunsa da özet olarak; "Savunma gereksinimlerine yönelik mevcut kaynakların ihtiyaca cevap verebilecek hale getirilmesi süreci" olarak tanımlamak mümkündür. Savunma planlamalarından beklenenler; çevredeki belirsizliklerle başa çıkabilmek, harekât alanındaki beklenmeyen durumlara reaksiyon gösterebilmek, askeri görevi icra edebilecek askeri yetenekler oluşturmak ve değişen ihtiyaçları karşılayabilecek esnek kuvvet yapıları oluşturmaktır. Burada, belirsizliğin yoğun olduğu şeklinde bahsedilen çevre kavramı; teknoloji, politika, ekonomi, küreselleşme, değerlerdeki değişim, insan haklarına yönelik artan vurgu, terör, su kaynakları, sivil toplum kuruluşları ve çok uluslu şirketlerdir[5].

---

[3] Hünkar Karahan Türk, "Türk Savunma Sanayinin Ekonomik Etkileri ve Savunma Harcamaları-Ekonomik Büyüme İlişkisinin Ekonometrik Modellenmesi" (Yüksek Lisans Tezi, Çukurova Üniversitesi Sosyal Bilimler Enstitüsü, 2007), 21.

[4] Savunma Sanayii Müsteşarlığının 2010, 2011, 2012 Yıllarına İlişkin Faaliyet ve İşlemlerinin Denetimi, "Türkiye Cumhuriyeti Cumhurbaşkanlığı Denetleme Raporu", 2014, Ankara: 1411.

[5] 18-22 Eylül 2017 tarihleri arasında TSK BİOM (Barış İçin Ortaklık Merkezi) K.lığı/Ankara'da

Savunma planlamalarının, dönem içerisinde kendisini etkileyen faktörlere göre güncellenmesi gerekmekte olup, sürekli bir faaliyet olarak değerlendirilmelidir. Çünkü çevresel faktörler, küresel güvenlik algıları ve tehdit türleri sürekli değişmekte olup eskiye nazaran statik halden uzaklaşarak dinamik bir hale gelmiştir[6]. Tarihsel süreç içerisindeki değişimlerine göre genel olarak; kadro, tehdit ve yetenek temelli olmak üzere üç ana yaklaşım üzerinde durulmaktadır[7]. Ancak bunların dışında özellikle 11 Eylül sonrası dönem için artan belirsizlikle başa çıkmak için geliştirilen, literatürde belirtilen yaklaşımlara alternatif, destekleyici türde yaklaşımlara rastlamak mümkündür[8].

Değişen tehdide yönelik bir anlayış geliştirmek, ortaya çıkan yeni savunma ihtiyacına karşılık vermek bu üç ana yaklaşım arasındaki geçişin daha net anlaşılmasına imkân vermektedir. Savunma planlama yaklaşımlarındaki değişikliğe yönelik tarihteki en önemli geçiş noktası olarak kabul edilen Soğuk Savaş öncesi ve sonrası dönemi iyi değerlendirmek gerekmektedir. Çünkü hâlihazırda mevcut savunma planlama yaklaşımları, Soğuk Savaş ve 1990'lardaki evrimsel gelişmelerin bir sonucudur[9]. Soğuk Savaş dönemine ilave olarak 11 Eylül'de gerçekleştirilen ve çalışmanın ikinci bölümünde üzerinde ayrıntılarıyla durulacak olan asimetrik tehditler, eskinin savunma anlayışlarının köklü bir değişim içerisine girmesine sebebiyet vermiştir.

Siyasi, askeri ve teknoloji alanlarındaki gelişmelere göre her dönem için farklı bir yaklaşım benimsense de her yeni dönemle birlikte diğer yaklaşımların tamamen terk edildiğini söylemek güçtür. Dolayısıyla yeni yaklaşımların öncekilerin üzerine inşa edildiği ve onların eksik yönlerini tamamlamak üzere geliştirildikleri, planlamanın çeşitli safhalarında farklı yaklaşımların kullanılabileceği göz ardı edilmemelidir[10].

Bu bölümün amacı, savunma planlama yaklaşımları ve güvenlik algılarında köklü değişiklere neden olan, paradigma değişiminini etkileyen dinamikleri açıklamaktır. Bu maksatla, tarihsel dönüm noktalarından Soğuk Savaş ve Sonrası

---

icra edilen "Savunma Planlaması Kursunda", Prof.Dr.Haluk Korkmazyürek tarafından verilen "Savunma Planlamasının Tarihsel Gelişimi" konulu ders yansılarından alınmıştır.

[6] US Department of Defense, “Force Structure Plan”, **Base Closure And Realignment Report**, c.1, Chapter:2 (2005): 5.

[7] Taner Altunok ve diğ., **Stratejik Savunma Yönetimi**, (İstanbul: Bizim Büro Yayınevi, 2010), 15.

[8] Yunus Öztürk, “Savunma Planlamasında Yeni Yaklaşımlar ve Türk Silahlı Kuvvetlerinde Bir Senaryo Uzayı Çalışması” (Yüksek Lisans Tezi, Kara Harp Okulu Savunma Bilimleri Enstitüsü, 2006), 125.

[9] Allied Command Transformation Staff Element Europe, **The Beginners' Guide To The NATO Defence Planning Process** (2013), 10.

[10] Uğur Berk, “Stratejik Savunma ve Güvenlik Planlamasinda Ortak Bir Yaklaşım Olarak Senaryo Temelli Planlama”, **Güvenlik Bilimleri Dergisi**, c.4, s.2 (2015): 9.

dönemler üzerinden savunma anlayışları karşılaştırılarak Tehdit Temelli Savunma Anlayışından, Yetenek Temelli Anlayışa geçişe yönelik duyulan ihtiyaç ve paradigma değişimi sonucu yeni oluşan savunma planlama algıları incelenmiştir.

## 2.1. Soğuk Savaş Dönemi Öncesi Savunma Yaklaşımı

Bu dönemde savunma planlamasındaki temel düşünce belli bir arazi kesminin, hava veya deniz alanının elde tutulması olarak ön plana çıkmıştır. Özellikle dünya savaşları öncesi dönemde, savunulması planlanan alan ne kadar ise, o alanı kapatmak için gereken birlikler harita üzerinden hesaplanır, personel ve malzeme kadroları belirlenir ve bu kadroların doldurulmasıyla yeterli kuvvete ulaşıldığı kabul edilirdi[11]. Dönemin savunma planlama yaklaşımı "Karşımdakinde ne varsa, bende de en az o kadar olmalı" mantığı üzerine kurulmuştur. Bu maksatla silah, personel vb. konularda nicel üstünlüğün elde bulundurması esas alınmıştır. Bütün bu bilgiler ışığında, Soğuk Savaş Dönemi öncesi savunma planlama yaklaşımının her konuda sayısal üstünlüğün zaferin anahtarı olduğu ilkesine dayanan "Kadro Temelli Planlama Yaklaşımı" olduğu söylenebilir.

Kadro temelli planlama yaklaşımına göre; tehdidin tanımı gayet açık olup, gücü ve sınırları belirlidir. Daha çok I. ve II.Dünya Savaşları döneminde hakim olan bu anlayışa göre, çevresel şartların etkisi yok denecek kadar azdır. Düşmanın imkan ve kabiliyetlerine yönelik, "Kim olduğu, kuvveti (sayıca) ve aşağı yukarı ne yapabileceği" sorularına yanıt bulmak kolaydır. Teçhizat, malzeme ve silahlar standart olup, bilinenin dışında bir husus yoktur. Harakat hedefleri ve muharebenin gerçekleşeceği yerler kesindir. Bu nedenle tehdide yönelik planlamayı etkileyen faktörler gayet açık olduğundan, yapılacak olan planlama, nitelikten ziyade sayıca üstünlüğü öngörür[12].

İlerleyen dönem içerisinde nicel üstünlüğün sonucu olan kadrolardaki aşırılık, gerektiğinden fazla silah ve personele sahip olmak ciddi bir maddi israfa yol açmış, özellikle gelişen teknolojiyle birlikte daha az sayıda ancak etkili silah sistemleri ve daha az ancak nitelikli birlikler ile sonuca ulaşılabileceği[13] fikri "Kadro Temelli Planlama"nın sorgulanır hale gelmesine neden olmuştur. Kadro temelli planlama,

[11] Haluk Korkmazyürek ve Harun Şeşen, "Savunma Yönetiminde Yeni Planlama Yaklaşımları: Kavramsal Bir Analiz", **Kara Harp Okulu Bilim Dergisi**, c.18, s.1 (2008): 56.
[12] 18-22 Eylül 2017 tarihleri arasında TSK BİOM (Barış İçin Ortaklık Merkezi) K.lığı/Ankara'da icra edilen "Savunma Planlaması Kursunda", Prof.Dr.Haluk Korkmazyürek tarafından verilen "**Savunma Planlaması Stratejileri**" konulu dersin yansılarından alınmıştır.
[13] Çağdaş Akif Kahraman, "Tarihsel Süreçte Savunma Planlaması Yaklaşımları İle Savunma Tedarik Sistemleri Arasındaki İlişki", **Kara Harp Okulu Bilim Dergisi**, c.26, s.2 (2016): 104.

özellikle dünya savaşlarında öne çıkmış ancak zaman içerisinde getirdiği özellikle maliyet ve güç israfı kriterleri nedeniyle Soğuk Savaş ile birlikte yerini, çalışmanın ilerleyen bölümünde karşımıza çıkacak olan Tehdit Temelli Planlamaya bırakmıştır.

Belirtilen hususlar ışığında özetlemek gerekirse; kadro temelli savunma planlamasının esasını; belirli düşman ve tehdit durumu, ülkeden ülkeye önemli farklılık göstermeyen askeri teknoloji ve teşkilatlanma, düşük belirsizlik düzeyi ve sayısal üstünlüğü elde bulundurmak gibi basit ilkelerin oluşturduğunu söylemek mümkündür. Ancak savaş durumundaki iki ülkenin kıyaslanmasında halen önemli bir kriter olarak değerlendirildiği bir yaklaşım tarzı olduğu da göz önünde bulundurulmalıdır[14].

## 2.2. Soğuk Savaş Dönemi Savunma Yaklaşımı

II. Dünya Savaşı sonrasında oluşan uluslararası sistemi tanımlamak için kullanılmış olan "Soğuk Savaş" terimini kamu önünde ilk kez adlandıran kişi Amerikalı maliye uzmanı Bernard Baruch'tur[15]. Kutuplaşmış dünya düzeninde ABD ve SSCB liderliğindeki iki blok arasındaki gerginlik ve kısmi çatışma süreci olarak tanımlanmakla[16] birlikte temelinde 50 yıllık Sovyet-Amerikan güvensizliği ve karşılıklı korkuyu barındıran bir dönem[17] olarak tarihte yerini almaktadır. Bu düzende dünya devletleri ya iki bloktan birisini seçmiş ya da Bağlantısızlar Hareketine katılarak tarafsızlıklarını sürdürmeye yönelik bir strateji izlemiş olsalar da "Küreselleşme" olgusu ile birlikte dünyanın herhangi bir yerinde meydana gelen en küçük bir gelişme dahi bütün dünya ülkelerini doğrudan ya da dolaylı olarak etkilemiştir[18].

Bloklar arasındaki çatışmanın artan bir ivmeyle devam ettiği Soğuk Savaş döneminde tehdide yönelik çeşitli organizasyonların kurulduğu görülmüştür. NATO ve Varşova Paktı gibi iki merkezli olarak kurulan düzenin, taraflar arasındaki ilişkideki gerginlik ve korku üzerinde inşa edildiğini söylemek mümkündür[19].

---

[14] Taner Altunok ve diğ., **age**, 20.
[15] Şenol Sevim, "Soğuk Savaş Sonrası Avrupa Güvenlik Yapılanması ve Türkiye" (Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2006), 1.
[16] Ufuk Tepebaş, "Soğuk Savaş ve 11 Eylül Sonrası Uluslararsı Sistemdeki Değişimin Güvenlik Algılamalarına Etkisi ve Türkiye", http://www.tasam.org/tr-TR/Icerik/205/soguk_savas_ve_11_eylul_sonrasi_uluslararasi_sistemdeki_degisimin_guvenlik_algilamalarina_etkisi_ve_turkiye [22.12.2017].
[17] Oral Sander, **Siyasi Tarih (1918-1994)**, 20.bs., (Ankara: İmge Kitabevi, 2011), 225.
[18] Fahir Armaoğlu, "20.Yüzyıl Siyasi Tarihi (1914-1980)", **Türkiye İşbankası Kültür Yayınları**, Genel Yayın No:252, Tarih Dizisi:17 (1983): 419.
[19] Gökhan Bayraktar, **Siber Savaş ve Ulusal Güvenlik Stratejisi**, (İstanbul: Yeniyüzyıl Yayınları, 2015), 35.

Dünya savaşları dönemindeki savunma planlama yaklaşımlarının temelinde gayet açık ve net olarak tanımlanabilen bir tehdit, yer ve zamanı tahmin edilebilen ya da belirlenebilen savaş alanları yer almaktaydı. Dolayısıyla planlamaya etki edecek bu faktörlerde büyük değişiklikler beklenmemekteydi. 1980'li yıllarla birlikte gelişen teknoloji ve ekonomik kısıtlamalar "Tehdide Dayalı" bir anlayışın gelişmesine sebep olmuştur[20]. Belirsizlik seviyesinin az olduğu bu dönemde savunma planlamaları tehdit tabanlı olarak oluşturulmuş ve bu planlama anlayışı, az olan belirsizliğin karşılanmasında yeterli görülmüş,[21] var olan belirsizliğin ise, ayrıntılı planlama ve düşmana nazaran daha kısa zamanda tepki verebilen, daha etkin ve caydırıcılık gücü yüksek silah sistemleri (bilhassa Kitle İmha Silahları) ile azaltılabileceği düşünülmüştür[22].

Tehdide Dayalı Planlama; Soğuk Savaş süresince hakim olan, dost ve düşman arasındaki ayrımın gayet net olduğu, tarafların net çizgilerle birbirinden ayrıldığı[23], farklı kuvvet unsurlarının entegre bir yapı içinde teşkilatlandırıldığı ve müştereklik konseptine dayandığı bir yaklaşım olma özelliğini taşımaktaydı. Bu anlayışa göre, karşıt kuvvetin ne yapabileceğine odaklanmak ve tehdidin ne şekilde bertaraf edileceğine yönelik planlamalar yapmak önemliydi. Çünkü belirsizlik az, tehdidin kim ve nerede olduğu ile gücü hakkında hüküm vermek nispeten kolaydı. İmkân ve kabiliyetleri esas kriter olarak alan bu model, düşmanın kim olacağı ya da bir çatışmanın nerede olabileceğinden çok düşmanın nasıl savaşabileceği (hangi imkân ve kabiliyetlerle karşımıza çıkabileceği) ile ilgili husulara odaklanmaktaydı[24].

Bu döneme kadar savunma planlamacıları tarafından fazla dile getirilmemiş olan "etkinlik" kavramının özellikle Soğuk Savaşın ilerleyen zamanlarında ne kadar önemli olduğu tecrübe edilmiştir. Buna göre teknolojinin sayıya oranla daha üstün olduğu, belki de yüzlerce kişinin yapabileceği bir işi tek bir silah/silah sisteminin yapabileceği anlaşılmış ve planlamalarda yer verilmesi gerektiği fikri oluşmuştur. Söz konusu anlayışa örnek verilecek olursa; düşmanın sahip olduğu tankları imha etmek için sayıca fazla tanka sahip olmak yerine, tanksavar silahları kullanarak da düşman tanklarının imha edilebileceği, silah sayısından ziyade etkinliğin

[20] Haluk Korkmazyürek, **Stratejik Savunma Yöntemi ve Savunma Planlaması**, (Ankara: 2011), 12.
[21] Cem Harun Meydan ve Akif Demirel, "Savunma Planlamasında Belirsizlikle Başa Çıkmada Esnek Yaklaşımlar", **SAVBEN Dergisi**, c.9, s.1 (2010): 13.
[22] John Lewis Gaddis, **Strategies of Containment: A Critical Appraisal of American National Security Policy During the Cold War**, (USA: Oxford University Press, 2005), 76.
[23] Bojan Zrnic, "The New Trends in Defence Planning and Their Impact on the Defense Planning Systems in Transitional Countries", **Vojno Delo**, c. 60, s.1 (2008): 27.
[24] Mustafa Kemal Topçu, "Savunma Planlamasının Ekonomiye Etkileri ve Savunma Bütçeleri", **Savunma Bilimleri Dergisi,** c.9, s.1 (2010): 78.

değerlendirilmesinin önemli olacağı hususunu ön plana çıkarmış, söz konusu anlayışın da maliyet ve etkinlik olarak olumlu yansıyacağı anlaşılmıştır.

Soğuk Savaş dönemi, iç güvenlik ve iç tehdit algılarının geri plana atıldığı, ulus devlet anlayışıyla tarafların toprak bütünlüklerini koruma amacından hareketle iki blok arasındaki silahlanma yarışına dönen bir süreçtir. Soğuk Savaş döneminin sonlarına doğru; bilindik tehdit kavramının değişmesi, tüm savunma planlarının temel dayanağı olan belli başlı senaryolardaki bilinen tehdidin anlamını yitirmesi[25], özellikle nükleer silahlar alanında başlayan yarış neticesinde silahlanmanın ürkütücü boyutlara ulaşması ve fikirsel anlamda daha liberal söylemlerin ön plana çıkmasıyla birlikte mevcut anlayışın sürdürülebilir olmadığı ifade edilmeye başlanmıştır[26].

Savunma planlamacılarının tehdit temelli yaklaşıma karşı özellikle Soğuk Savaş Döneminin ilerleyen dönemlerinde yüzleşmek zorunda kaldıkları finansal kısıtlamalarla ilgili gerçeklikler, mevcut anlayışın giderek ihtiyaçları karşılamadığını göstermiştir[27]. Dolayısıyla yeni bir güvenlik anlayışının doğmasındaki en etkili itici güç olarak; Soğuk Savaş sonrası dönemde ivme kazanan, küreselleşme döneminde yaşanan değişim ve dönüşüm süreçlerinin ortaya çıkardığı yeni savunma ihtiyaçları[28] olduğunu söylemek mümkündür.

Tehdit Temelli Yaklaşımın değişen şartlara uymada yetersiz kaldığı görülmüş olsa da bazı yönlerden cazip yönleri de bulunmaktadır. Yaklaşım, kuvvetlerin yeterliliğini ölçmek üzere tek ve basit bir kıstas sunmaktadır: Tehdit. Bu nedenle, özellikle tehditlerin gerçek ve canlı olduğu durumlarda, kamuoyunun desteğini almanın oldukça kolay[29] olması özelliği ön plana çıkmaktadır.

Soğuk Savaş döneminin acil tehditlerinin artık bulunmadığı ve muhtemelen önümüzdeki çeyrek asır da olmayacağı bilinmektedir[30]. Dönemin sonuna kadar NATO ve Varşova Paktı ülkeleri kendi içlerinde benzer doktrinler benimseyip, benzer silah ve teçhizatları kullanıp, her an çıkabileceğini düşündükleri bir savaşa yönelik eğitimler yapmışlardır. Onlarca ülkenin birbirlerini tehdit olarak tanımlayıp bütün savunma planlamalarını üzerlerine inşa ettikleri dönemde beklenen küresel kriz/savaş (Küba Krizi, Kore ve Vietnam Savaşları hariç) hiç bir zaman

---

[25] Fikret Birdişli, "Ulusal Güvenlik Kavramının Tarihsel ve Düşünsel Temelleri", **Sosyal Bilimler Enstitüsü Dergisi**, c.31, s.2 (2011): 153.

[26] Özlem Kösedağ İçin, "Değişen Güvenlik Anlayışının Uluslararası Örgüt Dernekleri Üzerinden Analiz Edilmesi", **Güvenlik Stratejileri Dergisi**, c.13, s.25 (2017): 103.

[27] Tony Lawrence, "The Risk of Threat-Based Planning", http://www.businessofgoverment.org/bio/john-m-kamensky [25.12.2017].

[28] Bilal Karabulut, "Küreselleşme Sürecinde Güvenlik Alanında Değişimler: Karadeniz'in Güvenliğini Yeniden Düşünmek", **Karadeniz Araştırmaları Dergisi**, c.6, s.23 (2009): 2.

[29] Yunus Öztürk, **age**, 127.

[30] Hans Binnendijk ve diğ., **ABD Silahlı Kuvvetlerinin Dönüşümü**, (Washington DC: National Defence University Press, 2002), 21.

gerçeklememiş, SSCB'nin dağılıp Doğu Blokunun dağılma sürecine girmesiyle birlikte Soğuk Savaş dönemi kendiliğinden sonra ermiştir[31].

Soğuk Savaş Dönemi sona ermiş olsa da tehdit temelli yaklaşımın aslında tamamen terk edildiğini söylemek zordur. Çünkü günümüzde hala devletlerarası, özellikle bazı simetrik tehditlere yönelik planlamaların tehdit temelli yaklaşıma uygun düştüğü söylenebilir. Kuzey Kore-ABD ile Rusya-ABD ilişkilerini ve birbirlerine yönelik planlamalarını tehdit temelli yaklaşım düzlemine oturtmanın çok da yanlış olmayacağını söylemek mümkündür.

## 2.3. Soğuk Savaş Dönemi Sonrası Savunma Yaklaşımı

Soğuk Savaşın sona ermesiyle birlikte başlayan yeni dönem, uluslararası ilişkilerde önemli siyasi gelişmelerin ortaya çıktığı bir süreçtir. İki kutuplu dünya düzeninden tek kutupluluğa doğru geçişle birlikte; küreselleşme olgusunun tüm dünyada hissedilmeye başlandığı; belirtilen döneme kadar geçerli olan siyasi, ekonomik ve sosyo-kültürel tanımlarda anlam karmaşalarının veya değişikliklerin yaşandığı bu dönemde, Doğu Bloğuna bağlı Doğu Avrupa devletlerinde komünist sistem çökmüş ve SSCB'nin dağılma süreci başlamıştır[32].

Savunma planlama yaklaşımları açısından ise, Soğuk Savaş döneminin belirgin doğası, yerini belirsizliklerle dolu bir ortama bırakmış ve güvenlik literatürüne "alışılmadık, simetrik olmayan" tehdit ve riskler girmeye başlamıştır[33]. Soğuk Savaş döneminde de muhtemelen var olan ancak devletlerin sert ve katı tutumları nedeniyle sivrilemeyip ön plana çıkma fırsatı bulamayan, askeri odaklı olan veya olmayan birçok sorun yeni tehdit algılamaları olarak toplumsal ve uluslararası alana dahil olmuştur[34]. Uluslararası iç karışıklıklarından, bölgesel çatışmalara kadar uyuşmazlıklar artmaya başlamış, tehdidin öngörülmesi zorlu bir süreç haline gelmiştir. Buna bağlı olarak da Soğuk Savaş döneminin bölgesel savunma planlama anlayışı yerini küresel savunmaya bırakmıştır[35].

Tehdit tanımlamasının artık somut bir karşılığının olmadığı ve belirsizliğe karşılık gelen bir olgu olduğu kabul edilmiştir. Soğuk Savaş dönemi sonrasında;

---

[31] Emre Dikici, **Harbin Evrimi, Geleceğin Harekât Ortamı ve Harp Teknolojileri**, (İstanbul: Harp Akademileri Basımevi, 2013), 15.
[32] Bahadır Bumin Özarslan, "Soğuk Savaş Sonrası Karadeniz'de Güvenlik Politikaları ve Türk-Rus İliskileri", **Türk Dünyası İncelemeleri Dergisi**, c.12, s.1 (2012): 136.
[33] Yunus ÖZTÜRK, **age**, 25.
[34] Muharrem Aksu ve Faruk Turhan, "Yeni Tehditler, Güvenliğin Genişleme Boyutları ve İnsani Güvenlik", **Uluslararası Alanya İşletme Fakültesi Dergisi**, c.4, s.2 (2012): 73.
[35] Richard L.Kugler, **U.S. Defense Strategy and Force Posture for the 21st Century: Capabilities and Requirements**, (Santa Monica: RAND, 1994), 94.

devletler için karmaşık bir hale gelen savunma planlamaları, tek bir baskın tehdit üzerine yoğunlaşmaktan[36] ziyade gittikçe belirsizleşmeye başlayan ve artan tehdit kaynaklarına karşı, gelişen teknolojiyi de planlama süreçlerine dahil ederek yaklaşımlar oluşturma ihtiyacını doğurmuştur.

Yeni tehdit ortamının önceki döneme göre oldukça farklılık arz etmeye başlaması, savunma planlamalarında da değişimi zorunlu kılmıştır. Soğuk Savaş sonrası dönemde artan belirsizlikle birlikte ortaya çıkan yeni tehditlere karşı, geniş bir yelpazede yetenek geliştirmeyi esas alan ve söz konusu yetenek geliştirme sürecine ekonomik unsurları da dahil eden bu yeni anlayış[37] Soğuk Savaş dönemi sonrasına hakim olmuştur. Yetenek temelli planlama anlayışı olarak tanımlanan bu yaklaşımda; tehdidin silahı olan belirsizliğe karşı, mümkün olduğunca her şartta tedbirli olmayı ve tehdidin gelebileceği istikametlere süratle kanalize olabilmeyi öngören yeteneklerin oluşturulması amaçlanmıştır.

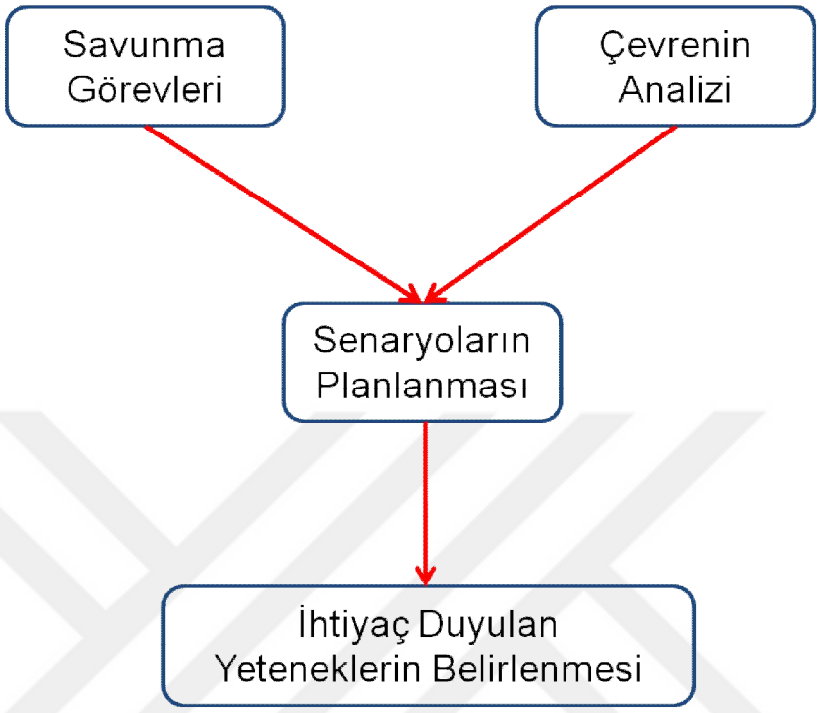
Küreselleşen dünyada tehditlerin de artık küreselleşmesi[38] ve özelikle Soğuk Savaş döneminin sonlarına doğru başlayan tehdit temelli yaklaşımdaki zaafiyetlerin, belirli dönemlerde farklı evrimlere uğrasa da genel olarak hala geçerliliğini koruyan bir anlayış olan Yetenek Temelli Yaklaşımın oluşmasına zemin hazırladığı kabul edilmektedir.

Yetenek temelli yaklaşım, kadro ve tehdit temelli yaklaşımlar üzerine inşa edilmiş bir yaklaşım olmakla birlikte günümüz dünyasının dinamik tehdit odaklarına karşı üretilen; artan risk, belirsizlik ve ekonomik sınırlamalar dahilinde geleceğe yönelik neye ihtiyaç duyulacağı sorusunu soran rasyonel bir savunma anlayışıdır[39]. Bu anlayışa sebep olan tehdit odaklarındaki değişime bakılacak olursa; çeşitli senaryolarda hasım olarak değerlendirilen ülkelerin yerlerini terör örgütleri, isyancılar, uluslararası suç şebekeleri gibi aktörler alırken temel değerlendirme kriterleri ise niceliksel verilere ilave olan "yetenekler"dir[40]. Buradaki yeteneklerden kasıt düşmanın yeteneklerine karşılık mevcut olan ve ihtiyaç duyulan yeteneklerdir[41]. Bu kapsamda yetenek temelli yaklaşımı özet olarak; ekonomik çerçeve dahilinde,

---

[36] NATO Research And Technology Organisation, **Handbook on Long Term Defence Planning** (France, 2003), 1.
[37] Paul Davis ve Russell D.Shaver, **Portfolio Analysis Methods for Assessing Capability Options**, (Santa Monica: RAND, 2008), 22.
[38] Çağrı Erhan, "NATO Niçin Küresel Bir Güvenlik Örgütü Haline Gelmelidir?" **Aylık Strateji ve Analiz Dergisi**, s.12 (Ocak 2004).
[39] Joint Systems and Analysis Group of Subcommıttee On Non-Atomıc Mılıtary Research And Development, "Guide To Capability Based Planning (TTCP Technical Report)", Technical Panel 3rd Of The Technical Cooperation Program, 2004, USA, 1-2.
[40] Lou Finch ve Paul K.Davis, **Defense Planning For The Post-Cold War Era**, (California: Naval Postgraduate School Press, 1993), 24.
[41] Michael Fitzsimmons, **"**Whither Capabilities-Based Planning?", **National Defense University**, Issue 44 (2007): 102.

belirsizlik çatısı altında, günümüzün geniş tehdit koşullarına karşı koyabilecek uygun yetenekler sağlamayı öngören bir planlama anlayışı[42] olarak tanımlamak mümkündür.




**Şekil 1: Yetenek Temelli Planlama Süreci**

Hari Bucur-Marcu, Philipp Fluri ve Todor Tagarev, "Defence Management: An Introduction", **Security And Defence Management Series**, s.1 (2009): 62.

Yetenek temelli planlama yaklaşımı, tehdit temelli planlama yaklaşıma benzer, fakat yukarda belirtilen Şekil 1'de de görüldüğü üzere kapsamlı ve bir proaktif yaklaşımla savunma görevleri ve çevresel faktörlerin analizi sonucunda gerçekleşmesi muhtemel, beklenen senaryolar planlanır. Müteakiben de senaryolara göre ihtiyaç duyulan yetenekler belirlenerek ve söz konusu ihtiyaçların karşılanmasına yönelik stratejilerin geliştirilmesi hedeflenir[43].

Yetenek temelli planlama yaklaşımının üzerine inşa edildiği planlama yaklaşımlarından üstünlüğü, yetenek odaklı olması ve değişimle olan "uyum"udur. Yetenek temelli savunma anlayışı; düşmanın kim olduğundan ve savaşın nerede gerçekleşeceğinden bağımsız olarak düşmanın neler yapabileceğine ve bu tehditleri

[42] Paul K.Davis, **Analytic Architectures for Capabilities-Based Planning**, Mission-System Analysis and Transformation, (Santa Monica: RAND Publications, 2002), 1.
[43] Haluk Korkmazyürek, "Stratejik Yönetim Ders Notları" (Kara Harp Okulu Savunma Bilimleri Enstitüsü Savunma Yönetimi Doktora Programı, 2011), 3.

karşılamak için hangi yeteneklere ihtiyaç duyulduğuna odaklanmakta[44] ve tehdit temelli yaklaşımda net olarak belli olan tehdidin kim ve nerede olduğundan ziyade, yetenekleri ve gelecekteki muhtemel hamleleri ve bu hamlelere nasıl karşılık verilebileceği[45] üzerine kafa yormayı öngörmektedir. Bu kapsamda, tehdit olarak görülen ve planlamanın temelini oluşturan tehdit olgusu, yeteneklerin muhtemel senaryoların şekillenmesini ve bu senaryolar çerçevesinde yetenek ihtiyaçlarının "yetenek havuzu" ortaya çıkmasına sebep olmaktadır.

Yetenek temelli planlama ile ortaya çıkarılan yapılacaklar listesinin yerine getirilmesi için mevcut kaynaklar doğrultusunda, en uygun yetenek karması meydana getirilmeye çalışılmaktadır. Mevcut yetenekler ile var olan yetenekler karşılaştırılarak yetenek ihtiyaçları, bir ihtiyaç planlaması çerçevesinde maliyet-etkin bir şekilde ortaya konulabilmektedir. Gerekli yetenek ihtiyaçları listesi senaryoların birleşimi ile oluşturulmuş olan senaryo uzayı değerlendirilerek oluşturulmaktadır. Burada, temel yetenek ve ihtiyaçların planlamasının daha önce oluşturulmuş olan senaryo uzayı çerçevesinde meydana getirilmesi ve bu sayede belirsizliğin yarattığı risklerin en aza indirgenmesi için oluşturulmuş en muhtemel senaryo veya senaryolara göre savunma planlaması, yani kuvvet ve silahlanma planlaması yapılmasını ortaya koymaktadır[46].

Yetenek temelli anlayışa göre planlamalar yapılırken birlik veya silah sistemleri sayısı veya karşılaşılacak potansiyel tehditten ziyade, sahip olunan mevcut yeteneklerin geliştirilmesi göz önünde bulundurulmaktadır[47]. Dolayısıyla asıl mesele; sahip olunan kuvvetin, gücün büyüklüğü değil, gelecekte karşılaşılacak sorun sahalarına karşı çözüm bulabilecek yeteneklere duyulan ihtiyaçtır. Bu ihtiyaçlar sadece askeri değil aynı zamanda sivil yeteneklerin de birlikte düşünülerek[48], karma bir yetenek havuzu oluşturulmasıyla karşılanabilir. Belirlenecek stratejilerin temelini; detaylı bir çalışma sonucunda belirlenecek olan muhtemel tehdit kaynakları ve bunlara karşı mevcut durumdaki kuvvetli ve zayıf yönlerin belirlenmesi[49] ve bunlara göre sahip olunması gereken yetenek ihtiyaçları hususları oluşturmalıdır.

Özet olarak çalışmanın dönüm noktasını oluşturan Soğuk Savaş sonrası dönemden itibarenki süreçte, tehdit ve gücün artık tek merkezli olmadığı bilinmektedir. Tehdit kavramı artık dinamik bir yapıya sahiptir ve tehdit

[44] Taner Altunok ve diğ., **age**, 54.
[45] Jeremy Shapiro ve Lynn Davis, **The New National Security, The US Army and The New National Security Strategy**, (Santa Monica: RAND Publications, 2003), 17.
[46] Cem Harun Meydan ve Akif Demirel, **age**, 16-17.
[47] Kenneth R.Pennie, "Strategic Thinking in Defence", **Canadian Military Journal**, c.2, s.3 (2001): 25.
[48] Michèle A. Flournoy ve Tammy S. Schultz, **Shaping U.S. Ground Forces for the Future: Getting Expansion Right**, (Washington: Center For A New American Security, 2007), 3.
[49] Kenneth R.Pennie, **age,** 23.

algılamalarındaki değişim savunma planlama anlayışlarındaki dönüşümün de temelini oluşturmaktadır. Soğuk Savaş Döneminin önde gelen tehditlerinden biri olan nükleer silahlar, söz konusu dönemle birlikte önemini kaybetmiş, yerini birçok kaynaktan çıkan tehditler yelpazesine bırakmıştır[50]. Özellikle 11 Eylül saldırıları sonrası küresel manâda da kesin olarak kabul edilen, esas tehditlerin modern barbarlardan veya devlet dışı/askeri olmayan aktörlerden geleceği varsayımı günümüzde hala geçerliğini koruyan bir hükümdür. Gücün büyük devletlerarasında klasik manâda el değiştirip dönüşmesinden ziyade, bahse konu devlet dışı aktörlerin yükselişi savunma planlamacıları için daha büyük sorunlar teşkil etmektedir[51].

## 2.4. Savunma Planlamalarında Paradigma Değişim İhtiyacı

Türk Dil Kurumu tarafından "Değerler dizini"[52] olarak ifade edilen paradigma kavramı ilk olarak ünlü fizikçi Thomas Samuel Kuhn'un devrim niteliğindeki eseri olan "Bilimsel Devrimlerin Yapısı[53]"nda ayrıntılı olarak bahsedilmiştir. Kuhn, bilim adamları tarafından benimsenen inançlar bütününe veya problemlerin nasıl anlaşılması gerektiği konusuna ilişkin hemfikir olunan geleneklere paradigma adını vermiştir[54]. Tarihte; Kopernik astronomisinin, Newton dinamiğinin veya dalga optiğinin zamanında kabul görmüş gelenekler olduğunu ve bunların her birinin birer paradigma olduğunu ifade etmiştir. Kuhn'a göre, paradigmalar bir araştırma alanının belirli bir zaman periyodunda ortaya koyduğu meşru problemleri ve metotları ifade etmektedir[55].

Kuhn, bilimin gelişmesinde anahtar terimin paradigma olduğunu, paradigma kavramı ile bilimin iç içe bulunduğunu öne sürmüştür. Bilimin istikrarsız olduğunu ve kazanılmış bilgilerin toplamı olmadığını iddia etmiştir. Kuhn'a göre "Bilim süreklilik göstermez ve istikrar arz etmez, bilimsel süreç zaman zaman gerçekleşen devrimlerle kesintiye uğrar. Bilim bu devrimleri temel teamüllere ters düştüğü için başlangıçta kabul etmek istemez ve karşı koymaya çalışır. Ancak devrimler öyle bir

[50] Eray Akdemir, "Bir Arap Ülkesinde Bahar: Suriye'de Arap Baharı ve Türkiye'nin Güvenliğine Etkisi" (Yüksek Lisans Tezi, Kara Harp Okulu Savunma Bilimleri Enstitüsü, 2014), 184.
[51] Joseph S.Nye Jr., **The Future of Power**, (USA: Public Affairs Books, 2011), 30.
[52] Türk Dil Kurumu, **Büyük Türkçe Sözlük**, (Ankara: Türk Dil Kurumu Yayınları, 2011), 1782.
[53] Kuhn'un 1962 yılında yayımlanmış olan makalesi, daha sonradan kitap haline getirilmiştir. Kitabın orjinal adı "The Structure of Scientific Revolutions"dur.
[54] Bilal Güneş, "Paradigma Kavramı Işığında Bilimsel Devrimlerin Yapısı ve Bilim Savaşları: Cephelerdeki Fizikçilerden Thomas S.Kuhn ve Alan D.Sokal", **Türk Eğitim Bilimleri Dergisi**, c.1, s.1 (2003): 27.
[55] Taner Altunok ve diğ., **age**, 51.

hal alır ki bilim, bu devrimleri ve sonucunda gerçekleşen radikal değişimleri kabul etmek zorunda kalır[56].

Kuhn'a göre, hakim olan paradigma hem çözülmeye değer problemleri tanımlar hem de bu problemlere ilişkin çözüm yöntemlerinin nasıl bulunacağına dair yol gösterir. Paradigma bir alanda hâkim olduktan sonra bu paradigmanın dışına çıkılması pek mümkün olmamaktadır[57]. Ancak normal bilim sürecinde bilimsel istikrar sürerken araştırma sonuçları bilim adamlarını öyle bir noktaya getirebilir ki, araştırma bulguları sahip oldukları paradigmalarla çelişir. Başlangıçta paradigmaları tehdit eden bu bulgular kabul edilmek istenmez ve görmezlikten gelinir. Bu aşamaya 'kriz durumu' denir. Ancak araştırma safhaları ilerledikçe ve çeşitliliği arttıkça elde edilen bulguların kabul görmekte olan paradigma ile olan çelişkisi artar ve bilimin inatçılığı kırılmak zorunda kalır. Bu kriz durumunu aşmak için eski paradigmaların yeni bir paradigma ile değiştirilmesi[58] ihtiyacı doğar.

Paradigmalardaki değişimin; köklü anlayış, metot, yöntem farklılıklarına neden olduğu anlaşılmaktadır. Bilimsel devrimlerin sonunda paradigmadaki bir değişim, bilimsel araştırmanın temel esaslarını değiştirmekte ve kendisinden önceki paradigmalarla ilişkilendirilemeyen yeni standartların, çözüm teknik ve teorilerinin önünü açmaktadır.

Periyodik olarak bilimsel devrimler bu aşamalarla sürüp gider. Kuhn'un görüşleri doğrultusunda paradigmaları; yol gösterici, ayırt edici, sorunun çözümüne yönelik yöntemler bütünü olarak anlamlandırmak mümkündür. Başarılı uygulamanın herkes tarafından paylaşılan örneklerinin, grubun eksiğini kapattığı düşüncesine varıldığı (herkesçe kabul gördüğü) durumda söz konusu örnekler, örneklem grubun "paradigma"ları olarak tanımlanır[59]. Paradigma değişim sürecindeki geçişin en önemli noktası, işlerin yeni yol ve yöntemlerle yürütülmeye başlanması, eski metot ve anlayışlara "güle güle" denilebilmesidir[60]. Bu süreç kabullenilmesi ancak yeni paradigma anlayışının test edilerek, önceki paradigmanın karşılayamadığı ihtiyaçların, belirlenen açıkların kapatıldığının görülmesi halinde daha kolay hale gelmektedir.

---

[56] Thomas S.Kuhn, "The Structure of Scientific Revolutions", **International Encyclopedia of Unified Science**, c.2, s.2 (1970): 81-93.

[57] Ahmet Eyim ve Kamuran Uygar, "Thomas S. Kuhn'un Paradigma Görüşü ve Atwood Makinesi Üzerine Bir Tartışma", **Düşünme Dergisi**, c.1, s.8 (2016): 18.

[58] Thomas S.Kuhn, **age**, 62-66.

[59] Ümit Öztürk, "Thomas Kuhn'un Paradigma Kavrayışı Üzerine Analitik Bir İrdeleme", **Kaygı: Uludağ Üniversitesi Fen-Edebiyat Fakültesi Felsefe Dergisi**, c.19, s.19 (2012): 187.

[60] Laura R.Cleary ve Teri McConville, **Managing Defence In A Democracy**, (London/Routhledge: Cass Military Studies, 2006), 52.

Kuhn'un eserinde belirtmiş olduğu bilimsel devrimlere ilişkin paradigma anlayışı incelendiğinde, şimdiye kadar anlatılmaya çalışılan savunma planlama yaklaşımlarındaki değişimler ile paralellik gösterdiği anlaşılmaktadır. Soğuk savaş dönemi öncesi, sonrası ve özellikle 11 Eylül saldırıları ile birlikte değişen savunma anlayışlarındaki paradigma değişimlerini Kuhn'un teorisiyle açıklamak mümkündür. Kuhn'un teorisindeki en kritik nokta, radikal değişimdir[61].

Tarihsel süreç içerisinde değişen savunma anlayışları, başta sıkı sıkıya sahip çıkılmasına rağmen gelişen durumlar ve mevcut düzenin ihtiyaçlara karşılık verememesi nedeniyle yeni yaklaşımların doğmasına, dolayısıyla paradigmaların değişmesine sebebiyet vermiştir. 11 Eylül saldırıları başta olmak üzere Soğuk Savaş sonrası yaşanan gelişmeler, savunma planlama anlayışlarındaki paradigma değişimlerinin de kendisine ve öne sürdüğü temel niteliklere karşı ortaya çıkan tehdit neticesinde zorunlu hale geldiğini göstermektedir. Dolayısıyla yetenek temelli savunma yaklaşımına geçişin temelinde de savunma planlamalarındaki paradigma değişimleri olduğunu söylemek mümkündür[62].

Ülkelerin ve milli güç unsurları arasında önemli bir yere sahip olan askeri gücün mevcut değişimlere göre kendini uyarlamaları zaruridir. Aksi takdirde çağın gerisinde kalan sorunlu birimler haline gelme riski doğrultusunda, ihtiyaçlara cevap veremeyecek hale gelirler. Bu nedenle zaman içerisinde ortaya çıkan savunma konseptleri mevcut teşkilatlanmaları ve harp doktrinlerindeki dönüşümün zorunluluğuna işaret etmiştir[63]. Ancak bu düşünceye ilave olarak; paradigma değişimleri geçmişle olan bağların tamamen koparılması anlamına gelmemekte, aksine eskinin izlerini de içerecek şekilde yeninin olgunlaşmasını ve başarıya ulaşmasının beklendiği bir süreç olarak yorumlanmaktadır. Yani; gösterdiği dönemsel farklılıklara rağmen eski anlayışların tamamıyla terk edildiğini söylemek güçtür ancak ilerleyen dönemlerde dahi olsa artık mevcut durumdaki yeni yaklaşımın yerini alması da beklenmez. Örnek vermek gerekirse, halen günümüz savunma planlamalarına esas teşkil eden yetenek temelli savunma planlama anlayışının karşılaştığı her güçlükte yeniden eskiye, kadro temelli anlayışa dönülmesi fikri pek mümkün olmayacaktır[64].

Paradigma değişimi olarak tanımlanan süreci tetikleyen bir takım unsurlar bulunmaktadır. Burada esas üzerinde durulması gereken konu; paradigma değişim ihtiyacının kaynağı, yani mevcut paradigmanın değişen şartlar (çevre ve tehdide

[61] Francois Vrey, **age**, 89.
[62] Michael Fitzsimmons, **age**, 101.
[63] Erol Mütercimler, **Geleceği Yönetmek ve Kazanmak İçin Stratejik Düşünme** (İstanbul: Alfa Yayınları, 2011), 567.
[64] Taner Altunok (vd.), **age**, 57.

yönelik) karşısında cevap veremediği sorular ile yeni paradigmanın bu açıklara ve gelecekteki muhtemel ihtiyaçlara verebileceği değerlendirilen reaksiyonlardır. Çünkü Kuhn'un da bahsettiği paradigma anlayışına göre; "mevcut paradigma, ortaya çıkmasına neden olan sorulara yanıt vermekte yetersiz kalmaya başlandığında yaşanır"[65]. Dolayısıyla bir bakıma değişimden beklenen anahtar rol önceki anlayışın mevcut durumdaki zaafiyetlerini azaltarak avantaj sağlamaktır[66].

Soğuk Savaşın sona ermesi ve 11 Eylül saldırılarını takiben, uluslararası güvenliğe yönelik tehditler daha karmaşık ve yönetilmesi zor yapılar olarak şekillenmişlerdir. Eskiden birbirinden ayrı politikalarla yönetilmeye çalışılan bireysel, ulusal ve uluslararası güvenlik sorunları arasındaki sınırlar kalkmış durumdadır. Bu ortama yönelik mevcut durumun eskiye nazaran tamamen değiştiği söylenemezse de, değişimin beklenenden daha hızlı ve yoğun olduğu ortadadır[67].

Savunma planlama yaklaşımlarındaki paradigma değişimlerin yaşandığını daha net anlamak için eski ve yeni anlayışların karşılaştırılmasını yapmak önemlidir. Bu kapsamda eski ve yeni savunma yaklaşımları; değişen çevre, tehdit, varsayımlar ve savunma yöntemleri açısından incelenmelidir:

Eski savunma yaklaşımlarında temel varsayım, kaynağı ve gücü belli olan düşmanı bertaraf etmeye yönelik oluşturulan bir anlayış olarak belirmektedir. Tehdit gayet açık bir şekilde ifade edilebildiği için muhtemel senaryolar oluşturularak olası bir durumda önlem almak nispeten kolay gözükmekteydi[68]. Bu yaklaşıma göre düşman belli olduğu için nicel olarak en az onun kadar veya ondan fazla olunması başarının anahtarı olarak görülmekteydi. Ancak yeni yaklaşım belirsiz, potansiyel tehditlere odaklanmaktadır. Çünkü tehdit algısı çeşitli faktörlerin etkisiyle iyice bulanık bir hale gelmiştir. Bu nedenle belirsizliğe yönelik, yetenek temelli bir planlama anlayışı hakim olmaya başlamış, nicel üstünlüğün belirsiz bir tehdidin olduğu çevrede pek bir anlam ifade etmediği anlaşılmıştır.

Eski savunma yaklaşımları yüksek maliyet ve şişirilen kadrolar, silahlanma yarışına sahne olan bir süreci beraberinde getirmiştir. Ancak yeni anlayışa göre, değişen tehdit algılarına süratle müdahale edebilecek, daha esnek, hareket kabiliyeti yüksek, aynı anda birden fazla tehdide karşı koyabilecek ve düşük kadrolu yapılar tercih edilmektedir. Ayrıca yeni anlayışın teknolojik gelişmelerle desteklenelerek maliyet ve iş gücü konusunda önemli bir avantaj sağladığı da aşikardır. Bu

[65] Thomas S.Kuhn, **age,** 157.
[66] US DoD, **age**, 6.
[67] Ali L.Karaosmanoğlu, **NATO'nun Dönüşümü**, (İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2012), 10.
[68] Taner Altunok ve diğ., **age**, 74-75.

kapsamda, yeni paradigmaların askeri problemlerle teknolojik fırsatların dinamik ve sürekli olarak kesiştirilmesi ile elde edildiğini söylemek mümkündür.

Soğuk Savaş kanunları, güç kullanımı ve tahrip gücü yüksek saldırıları önlemeyi esas alan bir yaklaşımı esas almaktaydı. Önceki dönemlerde düşmanları alt edebilmek için büyük ordular ve gelişmiş bir askeri sanayi zaruriydi. Ancak günümüz dünyasında hüküm süren belirsiz ve karmaşık kaos ortamının yarattığı tehdit kaynakları bütün bu sayısal üstünlüklerin yaratabileceği etkinin çok daha azı bir maliyetle hedef ülkede ciddi acı verebilecek durumlara yol açabilmektedir. Özellikle asimetrinin hangi boyutlara ulaştığının en yakın örneği olan 11 Eylül saldırıları, zayıf tarafın güçlü olan karşısında ne kadar tehlikeli olabileceğini acı tecrübelerle tüm dünyaya göstermiştir. Bu nedenle tehdit ve çevresel faktörlerdeki değişim savunma yaklaşımlarında da paradigma değişimlerini kaçınılmaz hale getirmiştir.

Örgütsel savunma yaklaşımları açısından ise durum çok da farklı değildir. Sovyetler Birliği'nin çöküşü şüphesiz tüm dengelerde değişimler meydana getirmiş, devletlerin yanı sıra uluslararası örgütler de görevleri açısından, yeniden tanımlanma sürecine girmişlerdir. Soğuk Savaş süresince etkisini hissettiren belirgin tehdide karşı tasarlanan topyekün muharebe ordularının, Berlin duvarının yıkılışından sonra ne yapacağı merak konusu olmuştur. Bu noktada, ülkelerin güvenlik ve savunma politikalarında değişimler meydana gelirken, söz konusu değişimler örgütsel savunma anlayışları arasında da bir dönüşüm sürecine girilmesini zorunlu kılmıştır[69].

Soğuk Savaş dönemi (kadro/tehdit temelli) ve sonrası dönemde (yetenek temelli) benimsenen savunma planlama yaklaşımlarında ciddi bir paradigma değişiminin yaşandığı aşikar olup, Kuhn'un ortaya atmış olduğu paradigma anlayışıyla örtüştüğü görülmektedir. Küresel ortam, sürekli ihtiyaca yönelik güncellenen savunma yaklaşımları, var olan veya potandiyel tehdit odaklarının simetrik olmaktan uzaklaşması ve teknolojik gelişmeler zaman içerisinde var olan paradigmaların değişmesine sebebiyet vermiştir. Sürekli olarak bir değişim içerisinde olan çevresel faktörler ve buna bağlı olarak evrime uğrayan tehdit algısı, paradigma değişimlerinin bir sonu olmadığını adeta ispat eder niteliktedir. Belirtilen hususları destekler nitelikte, değişen savunma anlayışlarına yönelik olarak David A.Deptula; paradima değişikliklerinin şimdiye kadar olduğu gibi gelecekte de yaşanmaya devam edeceği ve bu muhtemel değişimlerin önceden kesitirilerek mutlaka kaynak ayrılması gerektiği, kara/hava/deniz harekat alanı kavramlarının

[69] Öner Akgül, "Soğuk Savaş Sonrası Dönemde NATO–AB İliskilerinde Rekabet-İşbirliği Analizi Ve Türkiye Faktörü", **Güvenlik Stratejileri Dergisi**, c.4, s.7 (2008): 118.

ortadan kalkarak bütünleştiği, askeri ve siyasi kanadın savunma planlama süreci esnasında birlikte hareket etmesinin önemli olduğunu belirtmiştir[70]. Bu kapsamda, ülkelerin savuma anlayışlarını belirlerken bu önemli noktaları göz ardı etmemeleri ve bunlara uygun olarak gelecekteki savunma planlamalarını oluşturmaları gerekmektedir[71].

## 2.5. Günümüz Dünyası Tehditleri ve Savunma Planlama Yaklaşımları

II.Dünya Savaşından bu yana savunma yaklaşımlarında köklü yapısal değişikliklerin gerçekleştiği yadsınamaz bir gerçektir. Günümüzde geçerliliğini koruyan yeni savunma konseptine göre; güvenliğe yönelik tehditler çok boyutlu ve genel olarak önceden tahmin edilmesi güç olarak nitelendirilmekte, caydırma ve savunma, önleyici diplomasi ve kriz yönetimi gibi kavramlar vurgulanır hale gelmektedir[72]. Bu kapsamda tehdidin saldırıya dönüşmeden önlenmesine yönelik ulusal ve uluslararası tedbirlerin alınması[73] hususunun günümüz savunma anlayışlarına temel oluşturduğu değerlendirilmektedir.

Savunma planlama yaklaşımlarındaki değişimin net bir şekilde küresel manada hissedildiği, kritik bir eşik olan Soğuk Savaş dönemi özelinde savunma planlama anlayışlarının tarihsel evrimi önceki bölümlerde anlatılmaya çalışılmıştır. Günümüz savunma planlama anlayışlarına belki de şu anki halini veren ve küresel anlamda bir anlayış değişikliği getiren 11 Eylül'de 2001'deki terör saldırıları, asimetrik savaş başlığı altında çalışmanın ikinci bölümünde ayrıca anlatılacaktır. Paradigma değişimlerini ve savunma yaklaşımlarındaki değişimi daha iyi anlayabilmek için aşağıda özet olarak verilen tablo üzerinden savunma planlama yaklaşımları arasında bir karşılaştırma yapmak mümkündür:

[70] Emekli Korgeneral David A.Deptula'nın 29 Mart 2013 tarihinde Hava Harp Akademisinde icra edilen Uluslararası Havacılık ve Uzay Gücü Paneli (ICAP)'nde yapmış olduğu konuşma notlarından alınmıştır.
[71] Taner Altunok ve diğ., **age**, 79.
[72] Fırat Purtaş, "Soğuk Savaş Sonrası NATO'nun Dönüşümü ve Genişlemesi Çerçevesinde Türk-Amerikan Askeri İlişkileri", **Güvenlik Stratejileri Dergisi**, c.2, s.1 (2005):10.
[73] Arif Bağbaşlıoğlu, "Transatlantik İlişkiler Bağlamında Küresel Ortaklar ve Akıllı Savunma", **Adam Akademi**, c.3, s.1 (2013): 80.

**Tablo 1: Savunma Planlamasının Gelişim Süreci**

| ***FAKTÖRLER*** | ***DÖNEMLER*** | | |
|---|---|---|---|
| | **I.Dünya Savaşları** | **Soğuk Savaş Dönemi** | **Soğuk Savaş Sonrası** |
| **Planlama** | Kadroya Dayalı Planlama | Tehdide Dayalı Planlama | Yeteneğe Dayalı Planlama |
| **Tehdit** | Tehdit çok iyi tanımlanmıştır. Kim/ne/nerede olduğu ve gücü bellidir. | Tehdit çok iyi tanımlanmıştır. Kim/ne/nerede olduğu ve gücü bellidir. | Tehdit ortadan kalkmıştır. Belirli ve tanımlı bir tehdit mevcut değildir. |
| **Çevre** | Harbin nerede yapılacağı bellidir. | Harbin nerede yapılacağı bellidir. | Tehdit kaynağı belirsizdir. Potansiyel tehditlerden söz edilebilir. |

Haluk Korkmazyürek, **Stratejik Savunma Yöntemi ve Savunma Planlaması**, (Ankara: 2011), 15.

Soğuk Savaş dönemi sonrası değişen şartlar ve bugünkü durum, pek çok ülke için spesifik bir düşman tanımını ortadan kaldırmıştır. Bu değişim sonucu savunma planlamalarını dayandırdıkları ana düşünce genel olarak, tüm tehditler içinden kendileri için en çok tehdit oluşturduğunu değerlendirdikleri ulusal tehdit değerlendirmeleri neticesinde yapılan tercihler haline gelmiştir[74]. Bu kapsamda devletlerin tehdit değerlendirmeleri; toplam güç, niyet algısı, savunma-saldırı dengesi ve coğrafi yakınlık gibi değişkenlere bağlı olarak değişmektedir[75]. Söz konusu hususların haricinde, savunma anlayışları oluştururken sadece spesifik tehditlere değil aynı zamanda tehdidin özünü oluşturan çevresel faktörlerin iyi bir

[74] Salih Akyürek, "Zorunlu Askerlik ve Profesyonel Ordu", **BİLGESAM Yayınları**, Rapor No:24 (2010): 1.
[75] Jürgen Haacke ve Paul D.Williams, "Regional Arrangements, Securitization, and Transnational Security Challenges", **Security Studies**, c.17, s.4 (2008): 776.

şekilde değerlendirimesine odaklanmak gerekmektedir[76]. Ne var ki tehdit algılamaları değiştikçe; yeni doktrin, silah sistemleri ve savunma anlayışlarının benimsenmesi için de uzun bir hazırlık sürecine ihtiyaç duyulmaktadır.

Tehditler ve kullandığı yöntemler ile bunları önlemeye yönelik üretilen tedbirlerin artık askeri yöntemlerin dışına çıktığı görülmektedir. Bu denli belirsizliğin bulunduğu tehdit havuzu, her geçen gün açık bir musluktan dolarcasına artan bir ivmeyle varlığını sürdürmekte, farklı maskelerle karşımıza çıkmaktadır. Dolayısıyla savunma planlamalarındaki dönüşümün asıl sebebi de olan ve günümüz stratejik çevre karakteristiğini en iyi şekilde tanımlayan kavram "belirsizlik" tir. Bu nedenle eski tehditlere göre oluşturulmuş askeri güçler, önceden tahmin edilemeyen ve önlem alınamayan değişen tehdit kaynakları karşısında etkisiz kalırken, bu tehditlere karşı ülkelerin savunma gereksinimleri Soğuk Savaştaki savunma konseptinden farklı olarak, tehdidin çıktığı yer ve zamanda önceden müdahale konseptini ortaya çıkarmıştır[77]. Diğer taraftan bu yeni tehditlerin neden olduğu çatışmalar uzamaya ve çatışmaların ağırlık merkezi savaş alanlarından toplumsal ve siyasal alana kaymaya başlamıştır[78].

Tehditlere yönelik bir kesin gelecek tahmini mevcut olmamakla[79] birlikte, savunma yaklaşımları açısından da devletlerarasında standart bir yaklaşım bulmak güçtür. Mevcut duruma ve muhatap olunan tehditlerin tip ve derecelerine göre, ülkeler zamansal ve bölgesel olarak çeşitli ulusal veya uluslararası stratejileri takip etmeye[80], sistem karşıtı anlamına gelen bir savunma algılamasıyla, kendi politikalarını ulusal çıkar ve tehdit değerlendirmeleri çerçevesinde tanımlamaya başlamışlardır[81]. Bu değişim, Soğuk Savaş döneminde geri plana atılan iç tehdit ve iç güvenlik algılamalarının devletlerin savunma planlamalarına etki edecek şekilde önem kazanmasına sebep olmuştur[82]. Bu bağlamda; muhtemel senaryolar ve öngörülebilir yetenekler, tehdidin doğasında bulunan belirsizlik ve karmaşıklığa yönelik çözümler üretilmesinin esasını oluşturmaktadır.

Birçok araştırmacının öngördüğü üzere gelecek; siyah ve beyaz ayrımı kadar

---

[76] UK Ministry of Defence, **Future Land Operating Concept**, **Joint Concept Note 2/12** (UK, 2012), 1-3.
[77] Cihangir Dumanlı, **Ulusal Güvenlik Sorunlarımız** (İstanbul: Bizim Kitaplar, 2007), 18-20.
[78] Gencer Özcan, "Doksanlı Yıllarda Türkiye'nin Değişen Güvenlik Ortamı", **En Uzun On Yıl: Türkiye'nin Ulusal Güvenlik ve Dış Politika Gündeminde Doksanlı Yıllar**, ed. Şule Kut (İstanbul: Büke Yayıncılık, 2000), 23.
[79] US Department of Defense, **age**, 5.
[80] Ömer Göksel İşyar, "Günümüzde Uluslararası Güvenlik Stratejileri: Kavramsal Çerçeve ve Uygulama", **Akademik Bakış Dergisi**, c.2, s.3 (2008): 37.
[81] Deniz Ülke Arıboğan, "Güvenliksiz Barıştan, Barışsız Güvenliğe", **ABD Dış Politikasında Yeni Yönelimler ve Dünya**, ed. Toktamış Ateş (İstanbul: Ümit Yayıncılık, 2004), 46.
[82] Burak Ülman, Gencer Özkan, "Türkiye'nin Yeni Güvenlik Algılamaları ve Bölücülük", **En Uzun On Yıl: Türkiye'nin Ulusal Güvenlik ve Dış Politika Gündeminde Doksanlı Yıllar**, ed. Şule Kut (İstanbul: Büke Yayıncılık, 2000), 99-102.

net olmayan, çok yönlü ve çok çeşitli bir karmaşa ortamına sahne olacaktır[83]. Bu kapsamda; gelecekte karşılaşılması muhtemel tehditlere karşı savunma anlayışları geliştirirken herşeyden önemlisi, planlamadan beklenen hususların net bir şekilde ortaya konulmasıdır[84]. Müteakip aşamada, nitel ve nicel etmenlerin ayrı ayrı değerlendirilerek çıkan ihtiyaçlara uygun planlamalar yapılması gerekmektedir. Nitel kriterler; eğitim, istihbarat, moral ve motivasyon, teknoloji, liderlik ve inisiyatif olarak sıralanırken, nicel kriterler ise; beka, ateş gücü, hareket kabiliyeti, atışlardaki isabet oranı, silahları menzili ve verimliliği gibi ölçülebilen hususlar[85] olarak değerlendirilmektedir. Bu hususlar ışığında savunma planlamacıları için yapılması gereken vazife; düşmanın yeteneklerine yönelik, nicel ve nitel verilerin değerlendirilmesi sonucunda belirlenecek olan senaryolar ve simülasyonların oluşturulmasıdır.

Günümüzde savunma alanında gelinen nokta; sayısal üstünlük elde etmekten ziyade vurucu gücü üst seviyede olan, ileri teknolojiye sahip, özgün, diğer ülkelerden izin almadan kullanılabilecek savunma sistem ve teçhizatına sahip olmayı gerektirmektedir[86]. Yaşanan çeşitli askeri operasyonlar, orduların güçlerini potansiyel tehdit odaklarına aynı çabuklukla dağıtabilmeleri gerektiğini göstermiştir. Tehdit yelpazesinin genişlemesi, elastikiyeti ön plana çıkarırken; tehditte belirsizliğin artması da, birlik yapısında hız ve çeviklik özelliklerine duyulan ihtiyacı artırmıştır. Taktik seviyede, böyle bir yeteneğin kazanılması, planlama ve uygulamanın her ikisinde de süreyi kısaltmaya bağlıdır. Planlamanın hızı, yetenekli askerlerin yanı sıra gelişmiş bilgi teknolojilerinin kullanıldığı karar destek sistemlerine bağlı iken; uygulamada hareket kabiliyeti geniş ve yüksek teknoloji harp silah ve araçlarına sahip küçük birlikleri gerektirmektedir[87]. Yani yapılacak planlamalarda, karşılaşılabilecek her türlü tehdide karşı hazır olmayı gerektirecek esnek kadro ve kuvvet yapılarına sahip olma hususu ön plana çıkmaktadır. Bu bağlamda, günümüzün savunma planlama yaklaşımlarında amaç; gelişen teknoloji ve yetenekleri birlikte kullanarak daha küçük ancak hareketli, esnek, tehdide karşı daha süratli reaksiyon gösterebilecek, görevin getirdiği ihtiyaca uygun birliklerle görev

---

[83] Frank G.Hoffman, "Hybrid Threats: Reconceptualizing The Evolving Character Of Modern Conflict", **Strategic Forum**, s.240 (2009): 5.

[84] Richmond M.Lloyd ve diğ., **Fundamentals Of Force Planning, Vol.1: Concepts**, (Newport: Naval War College Press, 1990), 134.

[85] P.H. Liotta ve Richmond M. Lloyd, "Here To There", **Naval War College Review**, c.58, s.2 (2005): 133.

[86] Ahmet Murat Köseoğlu, "Savunma Sanayi Stratejisinin Yeniden Belirlenmesi ve Türkiye'nin Güvenliğine Etkisi", **SAREM Stratejik Araştırmalar Dergisi**, c.9, s.17 (2011): 123.

[87] Serdar Genç, "Yetenek Temelli Stratejik Yönetim Anlayışının ABD Silahlı Kuvvetlerinin Teşkilat Yapısına Etkisi", **Güvenlik Stratejileri Dergisi**, c.11, s.21 (2015): 212.

etkinliğini artırmaktır.

21.yy. dünyasında savunma anlayışları artık bireysel, ulusal ve uluslararası yönleriyle iç içe geçmiş bir olguya işaret etmektedir. Bu karmaşık ortamda devletler; değişen şartlara, tehdit algılamalarına ve ihtiyaçlara uyum sağlayacak şekilde savunma planlamalarını düzenlemelidirler. Bunun yanı sıra geliştirilecek olan savunma yaklaşımlarına ilişkin ortak işbirlikleri, bölgesel tehditlere karşı birlikte hareket edilmesi hususu önem kazanmıştır. Devletlerin ve askeri güçlerin, gelecekte karşılaşılması muhtemel tehdit odaklarına karşı yakın işbirliği ve koordine içerisinde bulunmaları, kalıcı ve efektif çözümlere ulaşabilmesi açısından önemlidir[88]. Çünkü tehditler tek bir hedefe yöneleceği gibi birden fazla aktörü de güç durumda bırakmayı amaçlayabilirler.

Geleceğe yönelik yapılacak olan analiz ve beklentilerde gerçekçi öngörülerde bulunulmalı, işbirlikleri göz önünde bulundurulmalı, olası tehditlere uygun karşılıklar geliştirilebilmelidir[89]. Bu konudaki öngörüler öyle boyutlara ulaşmıştır ki, artık kara savaşlarının gerçekleşmeyeceği, dolayısıyla kara birliklerinin bulunmasına gerek olmadığı, orduların gittikçe küçülmesi gerektiği bile dile getirilmektedir[90]. Bu nedenle asıl zor sürecin bundan sonraki dönemde yaşanacağını söylemek mümkündür. Ancak geleceğe yönelik savunma yaklaşımları bütün bu kavram karmaşası ve boşluklara rağmen oluşturulmak zorundadır.

Soğuk Savaş Sonrası tehdidin artık tek ve belirgin olmadığı, değişimin artık kendisini iyiden iyiye hissettirmeye başladığı süreçte, özellikle çalışmanın ikinci bölümde ayrıntılı olarak bahsedilecek olan 11 Eylül saldırıları sonrası; bulanık ve iç içe geçmiş, bir kalıba sokulamayacak türde tehditler ortaya çıktığı kabul edilmiştir. Artık çok basitten karmaşığa uzanan bir yelpazede, eş zamanlı olarak uygulanabilen tehditlerle karşı karşıya olduğumuz bir gerçektir. Buradan hareketle 21. yüzyılda savunma planlamalarına dahil olan öğeler, sadece askeri tedbirleri değil daha ziyade siyasi, ekonomik ve sosyolojik tedbirleri de içerir hale gelmiştir[91]. Bu nedenle günümüz dünyası tarihi bir kırılma noktasında bulunmakta ve bir sonraki tehdidin nereden, ne zaman geleceği belli olmayan tehlikeli bir gelecek[92] ve ihtiyaçlara göre mutlaka süratle reaksiyon gösterilmesi gereken savunma anlayışları bizleri beklemektedir. Gelecekteki savaşlara hakim olacak öğeleri; savaşın doğasındaki

[88] Mieczysław Bieniek, "NATO's New Strategic Concept And The Military Transformation Of The Alliance", Ottawa Conference on Defence and Security, 2011, Ottawa, 7.
[89] Yaprak Gürsoy, **Türkiye'de Sivil-Asker İlişkilerinin Dönüşümü** (İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2012), 57.
[90] Gordon R.Sullivan, "America's Army: Movin Toward 2020", **Army** (October 2013): 12.
[91] Atilla Sandıklı ve Bilgehan Emeklier, "21. Yüzyılda Yeni Güvenlik Anlayışları ve Yaklaşımları", BİLGESAM, Uluslararası Balkan Kongresi, 28-29 Nisan 2011, Kocaeli, 38.
[92] Robert W.Cone, "The Future Army: Preparation and Readiness", **Military Review** (July-August 2013): 3-4.

sis, sürtüşme ve belirsizlik olarak sıralamak mümkündür. Tehlikenin ne şekilde ve nasıl ortaya çıkacağını kestirmek her zamankinden daha güç olacaktır. Dolayısıyla yüksek teknolojinin kansız zaferlere sebep olabileceği örneklerin yaşanacağı bir geleceğin[93] bütün dünyayı beklediğini söylemek artık çok da olasılık dışı değildir.

[93] Ali Bülent Uşaklı, **Savaşın Dönüşümü ve Teknoloji** (Ankara: Lalezar Kitabevi, 2008), 187.

# 3. ASİMETRİK SAVAŞ VE BİR ASİMETRİK SAVAŞ UNSURU OLARAK SİBER TEHDİTLER

Çalışmanın bu bölümünde değişen paradigmalar ışığında günümüz ve yakın gelecekteki muharebelerin asimetrik temele dayanacağı öngörüleri nedeniyle; asimetrik savaşın kapsamı, temel kavramsal açıklamaları ve tarihsel süreçteki örneklerine yer verilmiştir. Sonraki aşamada ise çalışmanın esasını oluşturan ve bir asimetrik savaş aracı olan siber tehditler ile ilgili bilgi ve veriler ele alınmıştır.

Önceki bölümde incelendiği üzere güvenlik kavramı ve savunma anlayışları tarihsel süreç içerisinde, temelinde aynı esası barındırsa da çeşitli paradigma değişimlerine sahne olmuştur. Bu değişimlerin en köklü yaşandığı zaman dilimi Soğuk Savaş dönemi sonrasıdır. Güvenlik algılamalarının değiştiği Soğuk Savaş sonrasındaki dönemde; özellikle 11 Eylül olayları, Ortadoğu'daki İsrail-Filistin çekişmesi, DEAŞ başta olmak üzere terör örgütlerinin eylemleri ile birlikte daha çok kullanılmaya başlanmıştır. Asimetrik savaş, değişik tanımlamalarla ifade edilse de kısaca; taraflar arasındaki güç dengesizliğinin, genellikle güçsüz olan tarafından yeri geldiğinde savaş hukuku ve etik değerleri de hiçe sayarak, farklı strateji ve taktikler kullanmak suretiyle giderilmeye çalışılması olarak ifade edilebilir. Bu tür girişimler, güçsüz olan tarafa geçici bile olsa belirli bir üstünlük sağlamaktadır.

Zamanı, mekânı ve öznesi açısından incelendiğine asimetrik tehditlere yönelik bir belirsizlikten söz etmek mümkündür. Bu yüzden asimetrik savaşlara karşı alınacak tedbirler ve savunma planlamaları konusunda mutlak bir doğru bulunmamaktadır. Teknolojinin gelişmesiyle birlikte, uyguladığı tekniklerde de her geçen gün değişimler meydana gelen asimetrik unsurlar; güç kullanımındaki orantısızlık, imkân ve kabiliyetlerinin öngörülemezliği, karşı tedbir alma güçlüğü bulunması, çok yönlü olması (askeri, ekonomik, sosyal, kültürel vb.), amaçlarına ulaşabilmek için hedef gözetmemesi, istismar odaklı olması, psikolojik etki yaratması, maliyet etkin olması, elastik bir yapıya sahip olup değişen durumlara süratle ayak uydurabilmesi ve eylemi gerçekleştirenin kimliğinin

belirlenmesi/doğrulanabilmesindeki zorluklar gibi özellikleri nedeniyle hem mevcut dönemi hem de gelecekteki gündemi en çok meşgul edeceği değerlendirilen bir kavram olarak ön plana çıkmaktadır.

Bu aşamada; asimetrik savaş kavramı, kapsamı, tarihsel süreci ve bu savaşın uygulama şekillerinden birisi olan siber saldırılara yönelik bilgi, veri ve değerlendirmelere yer verilmiştir. Bu bölümde anlatılanlara yönelik ulaşılmak istenen amaç; hem asimetrik savaş hem de öğelerinden biri olarak değerlendirilen siber savaşlara yönelik bir farkındalık yaratmak, siber tehditlerin etkilerini ve ulaşabileceği boyutlara dikkat çekmek ve bir sonraki bölümde anlatılacak olan siber tehditlerin savunma planlamalarına olan etkileri konusunda bir bilimsel düşünce altyapısı oluşmasını sağlamaktır.

## 3.1. Kavram ve Kapsam Olarak Asimetrik Savaş

İnsanlık tarihi boyunca savaş, uluslararası ilişkilerde tüm diplomatik yolların tıkandığı yerde nihai karar verme aracı olarak yer almıştır. Buna göre savaş, esasında kendisinin oluşmasına sebep olan öncesindeki ve sonrasındaki siyasi süreçten ayrı tutulmamalıdır. Aksine savaş, siyasetin son basamağıdır hatta farklı bir ifadeyle "politikanın devamıdır" [94]. Eski çağlardan beri her dönemin kendine özgü savaş konseptleri bulunduğu bilinmektedir. Bu konseptlerdeki değişiklikler içerik olarak genellikle; kadro yapıları, silah sistemleri, teçhizat ve malzemeler ile uygulanan strateji ve taktiklerden oluşmaktadır. Bu ayırt edici özelliklerdeki kısmen de olsa nicel üstünlükler galibin belirlenmesinde anahtar rolü oynamıştır. Söz konusu üstünlükleri ele geçiren taraf birçok seferde istediğini alarak masadan kalkmıştır.

Güvenlik kavramı, günümüzde eskiye kıyasla çok daha karmaşık hale gelmiştir. Uluslararası sisteme yeni aktörler, yeni tehditler, bunlara bağlı olarak da yeni güvenlik anlayışları egemen olmaya başlamıştır. Geçmişten gelen düşman kavramı ortadan kalkmış, onun yerine muhtemel tehditler doğrultusunda mücadele esasları belirlemek ön plana çıkmıştır. Bunun sebebi, tehdidin kaynağı olabilecek aktörlerin artık çok daha geniş bir yelpazede ve coğrafyada yer almasıdır[95]. Dolayısıyla eskinin potansiyel düşmanı kabul edilen komşu ülkeler yerine; bulunması, tanımlanması ve tedbir alınması gün geçtikçe daha da zor hale gelen, güçler arası asimetrinin hâkim

[94] Carl Von Clausewitz, **On War** (Princeton: Princeton University Press, 1976), 87.
[95] Ahmet Küçükşahin ve Tamer Akkan, "Değişen Güvenlik Algılamaları Işığında Tehdit ve Asimetrik Tehdit", **Güvenlik Stratejileri Dergisi**, s.5 (2007): 60.

olduğu küresel tehditler tarih sahnesinde yerini almaktadır.

Günümüzde esas amacın kesin sonuçlu bir zaferden ziyade, özellikle 11 Eylül saldırıları başta olmak üzere son yirmi yılda gerçekleşen olaylar göz önünde bulundurulduğunda, karşı tarafı; ekonomik, siyasi, askeri, psikolojik vb. mümkün olan her açıdan yıpratmak olduğu bilinmektedir. Bunu yaparken de amaca ulaşmak için nicel açıdan her zaman güçlü olmanın birinci şart olmadığı, karşı tarafa zarar vermek için bilinen geleneksel yöntemlerin ve üstünlüklerin yanı sıra farklı stratejiler belirleyip uygulamanın başarının anahtarı olabileceği tecrübe edilmektedir.

İki kutuplu sistemin çözülmesi ile birlikte güvenlik ve savunma kavramları güncellenmeye başlanmış ve bu köklü 'paradigma' (değerler dizini) değişiminin planlama, programlama ve tedarik süreçlerine kaçınılmaz yansımaları olmuştur. İki büyük dünya savaşının ardında bıraktığı toplumsal, ekonomik ve askerî yıkımlarla baş etmek durumunda kalan devletler, Soğuk Savaşın sona ermesi ile birlikte tehdit algılamalarını ve bu algılar üzerine inşa ettikleri güvenlik yapılanmalarını yeniden gözden geçirmeye koyulmuşlardır. Küreselleşmenin hız kazanması bu gayretlerin yoğunluğunu artırmıştır[96].

Soğuk Savaş dönemi incelendiğinde hem Doğu hem de Batı blokları için suni olarak aşılanmaya çalışılan korku ve tedirginlik[97] olgularının; teknolojik gelişmeler, farklı uluslararası işbirliklerinin ortaya çıkması, çıkar çatışmaları vb. nedenlerle tarihsel süreç içerisinde yeniden tanımlanmasına ihtiyaç duyulmuştur. Soğuk Savaşın sona ermesiyle birlikte küreselleşmenin yarattığı dinamik ortamda; terörizm, ayrılıkçı hareketler, etnik ve dini çatışmalar, kitle imha silahlarının yaygın hale gelmesi, uluslararası organize suçlar ve siber saldırılar gibi ulusal güvenliğe yönelik farklı tehdit algılamaları ortaya çıkmış, buna paralel olarak da güvenlik algılamalarında ve savunma planlama anlayışlarında değişiklikler olmuştur[98].

Soğuk Savaş sonrası dönemde, belirsizleşen ve asimetrik bir yapıya kavuşan tehditler savunma planlama süreçlerinin yeniden gözden geçirilmesini, farklı anlayış ve metotların benimsenmesini, yeni görevlerin ortaya çıkmasını ve kolluk kuvvetlerinin ortak güvenlik ortamının şekillendirilmesinde daha fazla rol almasını sağlamıştır[99].

Küreselleşme ve güvenlik bağlamı açısından güç dağılımının yeniden biçimlendirilmesi tam olarak mümkün olmamakta ve ortaya çıkan bu yeni savaş

---

[96] Yunus Öztürk, "Konvansiyonel Savaş Devri Geride mi Kaldı?", **Millî Güvenlik ve Askerî Bilimler Akademik Dergisi**, c.2, s.6 (2015): 26.
[97] Erol Mütercimler, **age**, 543.
[98] Gökhan Bayraktar, **age,** 15.
[99] Aslan Onur Nacak, "21'inci Yüzyıl Ortak Güvenlik Ortamı: Askerî Statülü Kolluk Kuvvetleri İçin Plânlama Önerileri", **Güvenlik Bilimleri Dergisi**, c.4, s.1 (2016): 1.

türünün aktörleri, kullandığı yöntemler ve sınırları gün geçtikçe daha belirsiz hale gelmektedir[100]. Bu kapsamda her yönüyle gün geçtikçe değişen bir asimetrik savaş olgusundan söz edilebilmektedir. Değişen güvenlik algılarına yönelik, uluslararası ortama en çok uyan tanımın asimetrik tehdit ve buna paralel olarak asimetrik savaşlar olduğu değerlendirilmektedir[101].

Soğuk Savaş döneminde, "gayri nizami harp" veya "gerilla savaşı" gibi geleneksel olmayan savaş konseptlerinin genel karakterlerini ifade etmek üzere kullanılan "asimetrik savaş" ve "asimetrik tehdit" terimleri; Soğuk Savaşın sona ermesinin ardından, özellikle terörizm ile bağlantılı olarak ortaya çıkan yeni tehditlerin ifade edilmesi için kullanılmaya başlanmıştır[102].

Küreselleşme sonrası tüm dünyada güvenlik bağlamında farkedilen değişim, özellikle 11 Eylül saldırısı sonrasında farklı boyutlara ulaşmıştır. Stratejik seviyede güvenlik konusunda meydana gelen bu zaafiyetin farklı şekillerde gözler önüne serilmesi; tehdidin herkes tarafından kabul edilen, klasik manada bir tehditten beklenen bir yapısının olmadığı gerçeğini kabul ettirmiştir. Genel tanım olarak asimetrik savaş şeklinde adlandırılan ve yarattığı farklı algılarla devletlerin genel kabul gören güvenlik stratejilerini geçersiz kılan bu yeni kavram, her yönüyle kapsamlı bir şekilde incelenmesi gereken bir olgu olmakla birlikte, özellikle ABD'ye yapılan saldırıyla birlikte küresel bir boyut kazanmış[103], bu nedenle 11 Eylül 2001'de Amerika Birleşik Devletleri'nde meydana gelen saldırılar hem siyasi hem de akademik çevrelerde dönüm noktası olarak kabul edilmiştir[104].Tartışmaların ve araştırmaların temelini; tehdidin nasıl önleneceği, tehdit önlemenin ve güvenliğin en önemli unsuru olarak kullanılan savunma planlamalarının, asimetrik koşullar altında nasıl yapılması gerektiği hususları oluşturmaktadır[105].

Asimetrik tehditlerin doğası gereği teknoloji ve çevresel faktörlerdeki değişim ve gelişim, yeni tehdit türlerinin doğuşuna zemin hazırlamaya her zaman müsaittir. Ancak en gelişmiş, sonucun kesin alınabileceği bir tehdit modeli yaratmak zordur.

---

[100] Muharrem Aksu ve Faruk Turhan, **age**, 69.
[101] Ahmet Küçükşahin ve Tamer Akkan, **age**, 45.
[102] Murat Demirel, "Asimetrik Tehdit Kavramı Bağlamında 11 Eylül 2001 Sonrası Dönemde Amerika Birleşik Devletleri'ndeki Siber Tehdit Algılamasının ve Geliştirilen Güvenlik Politikalarının İncelenmesi" (Yüksek Lisans Tezi, Kara Harp Okulu Savunma Bilimleri Enstitüsü, 2012), 23.
[103] Muzaffer Ünsaldı, "Asimetrik Tehdit ve Savunma Sanayisine Etkileri" (Yüksek Lisans Tezi, Kara Harp Akademisi Stratejik Araştırmalar Enstitüsü, 2013), 16.
[104] Behlül Özkan, "Soğuk Savaş Sonrası Amerikan Dış Politikası", **Stratejik Araştırmalar**, c.9, s.16 (2011): 53.
[105] Muzaffer Ünsaldı, **age**, 1.

Dolayısıyla her asimetrik tehdidin bir diğerinden bağımsız ve eşsiz[106] olduğunu ileri sürmek pek tabi mümkündür.

Geçmişten günümüze bakıldığında aslında bu yeni kavramın sadece yakın tarihe ait bir savaş stratejisi olmadığı bilinmektedir. Teknolojik gelişmelere paralel olarak kullanılan araçlar ve teknikler değişmesine rağmen, uygulama amacı aynı kalmıştır. Asimetrik savaş stratejilerine yönelik araştırmaların özellikle son yıllarda hız kazanmasının temel nedeni; eskiden devletler arasında sıkça kullanılan bir stratejiyken, günümüz şartlarında illegal kişi ve grupların da sıkça asimetrik yöntemleri kullanarak amaçlarını gerçekleştirmeye başvurmalarıdır. Bu nedenle; güçsüz devletlerin veya hükümet dışı organizasyonlardan doğan tehdit odaklarının gün geçtikçe büyümesiyle birlikte, coğrafi uzaklığa dayanan koruma kalkanı yok olmuş[107], tehdit artık zaman ve mesafe tanımayan yöntemlere sahip hale gelmiştir.

"Asimetri" terimi günümüzde sıkça kullanılan bir söylemdir. Ancak bu kavramın doğru olmayan yerlerde kullanımları bir çeşit kavram karmaşasına yol açmakta, gerçekte asimetrik özellik taşımayan birçok tehdit veya saldırı, asimetrik olarak nitelendirilmektedir[108]. Başka bir deyişle "asimetri" ve asimetrik kavramları modern bir slogan haline gelmiş ve her türlü durum için sıkça kullanılır olmuştur[109]. Bu nedenle asimetrik savaşın ne olduğunu daha iyi anlamak için öncelikle simetri ve asimetri kavramlarını ele almanın uygun olacağı değerlendirilmektedir.

Sözlük anlamı olarak incelendiğinde "simetri" kelimesi, "bakışım"; simetrik kelimesi "bakışımlı"; "asimetri" kelimesi, "bakışımsızlık"; "asimetrik" kelimesi ise "bakışımsız" anlamlarına gelmektedir. Yani görüldüğü üzere simetri, "iki veya daha çok şey arasında konum, biçim ve belirli bir eksene göre ölçü uygunluğu"; asimetri de, "aralarında bakışım (benzerlik) bulunmayan iki şey, simetrisiz" olarak tanımlanmaktadır[110].

Türkiye Cumhuriyeti Milli Güvenlik Kurulu'na göre asimetrik tehdit; "Yarattığı ani ve hazırlıksız durum nedeni ile ülkelerin siyasi, sosyal ve ekonomik sistemlerinde istikrarsızlıklarına neden olan, düşük seviyede kuvvet ve teknoloji kullanarak etkin olmayı amaçlayan tehdit algılamasıdır"[111]. Asimetrik savaşa ilişkin tanımda ise; "Normal savaş metotlarının tamamen dışında, çok küçük ama çok özel yetiştirilmiş

---

[106] John R.Davis, **age**, 24.
[107] US Department Of Army, **The Army Strategic Planning Guidance: 2006-2023** (US, 2003), 43.
[108] Ahmet Küçükşahin ve Tamer Akkan, **age**, 49.
[109] Stephen J.Blank, **Rethinking Asymmetric Threats** (Carlisle: U.S. Army War College Strategic Studies Institute Publications, 2003), 3.
[110] Türk Dil Kurumu resmi internet adresi, www.tdk.gov.tr [16.05.2016].
[111] MGK İnternet Sitesi, **Asimetrik Tehdit Nedir Sorusu**, http://www.mgk.gov.tr/turkce/sss.html#soru_13 [16.05.2016].

birliklerle, çok özel taktikler kullanılarak yapılan, nereden ve nasıl geldiğini belli etmeden büyük maddi ve manevi yıkımların yaşandığı, gayri nizami şartlarda yapılan savaş" olarak ifade edilmektedir[112].

Bu kapsamda, sınırları henüz keskin hatlarla belirli olmamakla birlikte, en geniş tanımıyla asimetrik savaş kavramı; güç açısından birbirine denk olmayan tarafların savaşı veya güçsüz tarafın güçlü olan tarafa beklenmeyen yer ve zamanda, teknolojik ve taktik avantaj sağlayan stratejileri uygulayarak, karşı tarafa zarar verip kendisine üstünlük sağlaması[113] olarak tanımlanabilir. Diğer bir ifadeyle ise güçlünün bilinen caydırıcı etkisini dengelemek için güçsüz olan tarafından uygulanan riski az, maliyeti az ve daha etkin neticeler verebilen uygulamalardır. Bu tanımlara paralel olarak belirtilen söz konusu özellikleri nedeniyle asimetrik yöntemlere olan ilgi gün geçtikçe artmaktadır.

Esasında asimetrik savaş yöntemleri, genel görüş itibariyle zayıfın güçlüye karşı bir kullandığı silahlar olarak algılansa da, yeri geldiğinde güçlünün güçlüye karşı kullandığı bir silah da olabilir[114]. Dolayısıyla asimetrik savaş kavramından bahsederken öncelikle vurgulanması gereken nokta; birbirine benzemeyen, birbirlerine denk olmayan unsurların mücadelesidir. Burada benzer olmama durumu yani asimetriden anlaşılması gereken; kuvvetler arasındaki teşkilat, teçhizat, doktrin, imkân ve kabiliyetlerden ortaya çıkan farklılıklardır[115].

Asimetrik tehditler rakibin kendisini savunamayacağı durumlar içerisinde bırakmaya yoğunlaşır[116]. Esasında, zayıflığı istismar ve kuvvetli taraftan kaçınmak yer almaktadır. Bu bakımdan asimetrik savaşı, hasmın zayıf tarafından faydalanarak dengesini bozmayı amaçlaması açısından güreş mücadelesine benzetmek mümkündür[117]. Bu benzetmeyle ilgili olarak, Sun Tzu da şu şekilde belirtmiştir: "Eğer düşman kuvvetli ise ondan kaç. Eğer düşman kuvvetleri birleşikse, onları parçala. Hazırlıksız olduğu yerden taarruz et. Beklenmediğin yerden ortaya çık"[118].

Asimetrik savaşa ilişkin tanımlar incelediğinde, asimetrinin ortak yönleri olarak;

- Düşmanın bir zayıflığına karşı gücü kullanmak,

---

[112] Tahir Tamer Kumkale, **Asimetrik Savaş**, http://kumkale.net/yazi.asp?id=599 [17.05.2016].
[113] Taner Altunok ve diğ., **age**, 117.
[114] Antulio J. Echevarria II, **Fourth-Generatıon War And Other Myths** (US: Strategic Studies Institute (SSI), 2005), 12.
[115] US Army, **FM 3-0 Operations, Chapter:4** (US, 2001), 4-2.
[116] James Mader, Tom Smith ve Dan Daley, **Asymmetric Warfare: The Only Thing New is The Tactic** (Washington DC: National Defense University National War College, 2000), 3.
[117] Hâkan Gunneriusson, "Nothing Is Taken Serious Until It Gets Serious: Countering Hybrid Threats", **Defence Against Terrorism Review**, c.4, s.1 (2012): 48.
[118] Sun Tzu, **Savaş Sanatı**, çev. Pulat Otkan ve Giray Fidan (İstanbul: Türkiye İş Bankası Yayınları, 2015), 34.

- Beklenmeyen, geleneksel olmayan ve yeni taarruz veya savunma metotları uygulamak,
- Askeri veya mali sonuçlar açısından harcanan güçle orantılı olmayan etkiler yaratmak,
- Teknolojik veya kültürel tehditleri kullanmak,
- Askeri veya askeri olmayan, ölümcül veya ölümcül olmayan teknikler kullanmak kavramları olduğu değerlendirilmektedir. Belirtilen hususlar dahilinde günümüz asimetrik harekât ortamının; kararlı ve her ortama uyum sağlayabilen düşmanları, çok yönlü aktörleri ve tüm bu aktörlerin birbirleriyle etkileşimlerinin doğurduğu kaotik, çok hızlı değişen ve öngörülemeyen şartları içeren tehdit ve risklerden oluştuğunu söylemek mümkündür[119].

Asimetrik Savaş yeni bir kavram gibi gözükse de aslında yeni bir strateji değil, tam aksine savaş tarihi kadar eskidir. Tarih boyunca genellikle zayıf olanın, kuvvetli olana karşı teknolojik ve sayısal zaafiyetini en aza indirmek veya tamamen ortadan kaldırmak için kullandığı yöntemler arayışıdır. 11 Eylül 2001'de bir grup teröristin, ABD'ye saldırmasıyla birlikte "Asimetrik Harp" yeni bir kavram olarak tarih sahnesine çıkmış gibi görünse de dünya tarihine bakıldığında bu stratejinin birçok örneği olduğu görülmektedir. Fatih Sultan Mehmet'in İstanbul'un fethi esnasında gemileri karadan Haliç'e indirerek asimetrik bir taktik izlediği ve bir çağın kapanıp yeni bir çağın başlamasına vesile olan büyük bir zafere ulaştığı bilinmektedir. Bu örneğin haricinde daha yakın bir tarih olan Çanakkale Savaşı esnasında Mustafa Kemal Atatürk'ün söylemiş olduğu "Merminiz yoksa süngünüz var emri de, asimetrinin psikolojik ve kültürel boyutunun en başarılı örneklerinden birisidir. Çünkü bu reaksiyon düşman kuvvetlerinin ve muharebe alanın hiç alışık olmadığı bir etki yaratmış ve taarruzlarını durdurmalarına neden olmuştur[120].

Asimetrik savaşların kökenin daha eskiye dayandığına dair farklı görüşler bulunmaktadır. Öyle ki M.Ö. 6.yy.da yaşamış ünlü Çinli komutan ve düşünür olan Sun Tzu, “Savaş Sanatı” adlı eserinde aslında tam olarak asimetrinin özünü oluşturan görüşlerini ifade etmiştir. Sun Tzu’ya göre; “Savaş kandırmacalı bir iştir. Vurabilecekken vurmayacakmış gibi göstermek, yaklaşıyorken uzaklaşıyormuş gibi göstermek gerekir. Bu nedenle yemle ve kandır, kargaşa çıkart ve ele geçir, dirençliyse ona göre hazırlan, sinirliyse onu kızdır, dinleniyorsa rahatsız et, ona hazırlanma fırsatı vermeden saldır, beklemediği anda ortaya çık. Bunlar savaş

[119] 1'inci Or.K.lığının 17 Mart 2017 tarihli "Hibrit Harekat Konsepti" konulu sunumunun yansılarından alınmıştır.
[120] Kara Harp Akademileri Komutanlığı, **Asimetrik Harp Yardımcı Yayını** (İstanbul: Harp Akademileri Basımevi, 2002), 7.

erbabının başarı sırlarıdır, önceden kestirilemez" [121].

Sun Tzu'nun söylemleriyle asimetrik savaşların özelliklerin büyük oranda benzeştiği görülmektedir. Bu nedenle asimetrinin temelinde yer alan zayıf olan tarafın söz konusu zaafiyetini dengelemek ve üstünlük sağlamak için farklı taktik ve teknikler üretmesinin oldukça eski bir yöntem olduğunu söylemek mümkündür[122]. Asimetrik savaşların süreç içerisindeki örnekleri ve insanlık tarihine yansımaları incelendiğinde, bahsedilen özelliklerin dönemler farklı olsa da benzer şekillerde kullanıldığı görülmektedir.

Asimetrik Savaş ortamının ortaya çıkmasına hiç şüphe yok ki, çeşitli bölgesel anlaşmazlıklar, küresel gelişmeler, etnik gruplar, dinler ve mezhepler arası anlaşmazlıklar kaynaklık etmektedir[123]. Bu bağlamda aşağıda verilecek olan yakın tarihte ön plana çıkan örnekler ışığında asimetrik savaşları değerlendirmek daha sağlıklı olacaktır:

- II. Dünya Savaşı sırasında Alman işgaline karşı koyan Sovyet Partizan Birliklerinin mücadelesi,
- Vietnam Savaşı sırasında Viet-Kong örgütünün Amerika'ya karşı yürüttüğü savaş,
- Eski Sovyet Sosyalist Cumhuriyetler Birliği'nin 1979 yılında Afganistan işgali sonrası "Mücahidin" olarak isimlendirilen Afgan halkının verdiği mücadele,
- Rusya'nın 1994 yılında Çeçenistan'ı işgali sonrası Çeçenlerin verdiği mücadele,
- 20 Mart 1995 tarihinde Japonya/Tokyo metrosuna sarin gazı saldırısı,
- İsrail-Filistin çatışmaları boyunca Filistinlilerin yapmış olduğu mücadele,
- Tüm dünyada korku ve kaosa neden olan şarbon (anthrax) virüsü,
- DEAŞ, Hizbullah vb. terör örgütleri tarihsel süreç içerisinde insanlığın karşılaştığı asimetrik savaş örneklerinden sadece bazılarıdır.

Başlı başına inceleme konusu olması gereken ve çalışmanın ana temasını oluşturarak ilerleyen bölümlerde çok daha ayrıntılı olarak anlatılacak olan, asimetrik savaşın bir diğer unsuru olan siber saldırılara ise Estonya ve Gürcistan'ın finans merkezlerini, hükümetini ve kritik kurumlarını hedef alan siber saldırılar ile 2010 yılında İran'ın nükleer enerji santrallerine yönelik olarak geliştirilen ve İran'a ciddi zararlar veren Stuxnet virüsü saldırısı örnek olarak verilebilir[124]. Verilen örneklerin

[121] Sun Tzu, **age**, 2.
[122] Metin Gürcan, "Savaşın Evrimi ve Teorik Yaklaşımlar", BİLSESAM, http://www.bilgesam.org/Images/Dokumanlar/0-163-201404072m_gurcan.pdf [22.05.2016].
[123] https://asimetriksavaslar.wordpress.com/2011/03/28/asimetrik-etki-nasil-yaratilir/ [Erişim Tarihi: 23.05.2016].
[124] Serdar Yıldız ve Onur Murat Köprülü, **Asimetrik Savaş** (2013), 7-8.

dışında asimetrik savaş ve asimetrik tehdit konusunda aslında milat olarak kabul edilen 11 Eylül saldırıları; dünyanın yöntemi bilinemeyen, önceden tahmin edilemeyen asimetrik bir savaşın içine girdiğinin en belirgin kanıtıdır.

Verilen örneklerden de görüldüğü üzere asimetrik tehditler oldukça yaygın bir haldedir ve gelişimini özellikle son yüzyılda gerçekleştirdiği kabul edilse de temeli daha öncelere dayanmaktadır. Ancak tehdidin "küresel" sözcüğü ile birlikte anılmaya başlanmasının milâdı, 11 Eylül 2001'de gerçekleşen terörist saldırılardır. ABD'nin uğradığı, hayal gücünü zorlayan bu saldırıya değin, pek çok terör örgütünün sınır aşan eylemlerine karşın, tehdidin küreselleştiği bir iddia ya da gerçeklik olarak çok fazla yüksek sese dile getirilmemiş[125]. 11 Eylül Saldırıları ayrıca, gerek tehdit algılarındaki değişimin daha net görülmesi ve somut hale getirilmesindeki rolü, gerekse de yeni hukuksal düzenlemelerin ve güvenlik politikalarının hayata geçirilmesi için açtığı "Fırsat Penceresi" ile bu doğrultuda oluşturulan küresel güvenlik politikalari[126] ve savunma planlama anlayışları açısından kritik bir eşiktir.

Asimetrik tehditlere küresel bir derece kazandırması açısından, "9/11 Saldınlan" olarak da anılan ve ABD hedeflerine yönelik olarak 11 Eylül 2001 tarihinde gerçekleştirilen terör saldırılarını, "New York'ta bulunan Dünya Ticaret Merkezi kulelerine ve Washington'un kalbinde yer alan Pentagon'a yapılmış bir dizi koordineli intihar saldırısı olarak özetlemek mümkündür. Saldırılar, teröristler tarafıdan kaçırılan yolcu uçaklarının belirtilen hedeflere intihar saldırısı şeklinde çarpması şeklinde gerçekleşmiştir. Kaçırılan bir diğer bir yolcu uçağı ise, Pennsylvania'nin kırsal kesminde bir alana düşmüştür. ABD hükümetinin, El Kaide'nin sorumlu oldugunu düşündüğü saldırılarda yaklaşık 3000 kişi hayatını kaybetmiştir"[127].

Asimetrik harp icra eden taraf, askeri açıdan denge haline (dönüm noktası) veya durgunluk noktasına gelindiğinde ya da askeri anlamda mağlup olsa bile, siyasi anlamda galipse savaçtan kazanan taraf olarak çıkar. Bu açıdan mücadelenin uzaması her zaman asimetrik unsurların yararınadır. Çünkü uzayan bir savaş büyük devletin ve onun kamuoyu nezdindeki azim ve kararlılığın ya da kazanma iradesinin yıpranması demektir[128]. Çabuk ve kesin sonuç alınamaması asimetrik unsurun başarısını arttırır, saldırıya uğrayan devletler açısından ise bu durumun kamuoyuna açıklanması gittikçe zor bir hale gelir[129]. Bunu sebebi olarak, kamuoyunda, tehdidin

---

[125] Ercan Çitlioğlu, "Terörizm ve Küreselleşme", **Stratejik Analiz** (Aralık 2007): 81.
[126] Murat Demirel, **age**, 165.
[127] Michael A.Turner, **Historical Dictionary of United States Intelligence** (Lanham: Scarecrow Press, 2006), 202.
[128] Kara Harp Akademileri Komutanlığı, **Asimetrik Harp Paneli Notları** (İstanbul: Harp Akademileri Basımevi, 2010), 28.
[129] John R.Davis, "Defeating Future Hybrid Threats", **Military Review** (September-October 2013): 25

önlenemeyeceğine ilişkin korku ve otoriteye karşı bir güvensizlik eğilimi doğmaya başlar. Tarih boyunca birçok güçlü ülke veya ordu asimetrik savaşın doğasındaki uzun süreç nedeniyle başarıya ulaşma konusunda zor duruma düşmüştür. Dolayısıyla asimetrik bir tehdidin yapmış olduğu girişimin sonucunda kaybetmediyse kazanmış sayılacağını ve hedefine ulaşmış olacağını söylemek nispeten mümkündür.

Asimetrik tehditle mücadele yüksek bir hayal gücü ve öngörü gerektirmektedir. Bu nedenle ülkelerin herhangi bir saldırıya hazır olmaları belki de paranoyaya kadar giden ve hayal gücüne bağlı olarak tehdidin bertaraf edilmesi için tedbir almayı gerektirebilmektedir. Bu tedbirler; alışveriş merkezlerinden havaalanlarına, sokaklardan iş yerlerine, telefon görüşmelerinin dinlenmesinden bilgisayar mesajlarının takibine hatta banka işlemlerine kadar giderek insan hürriyetini kısıtlayıcı bir hâl almaktadır. Mücadele için alınacak tedbirlerle toplumda tedirginlik ve rahatsızlığa neden olma arasında iyi bir dengenin kurulması şarttır[130].

Yakın tarih incelendiğinde Afganistan ve Irak'ta yaşanan savaş ve çatışmalar bunun en canlı örnekleridir. Teknoloji ve sayısal anlamda üstün olan güçler; düşük yoğunluklu çatışmalarla yorulmuş ve kazananı olmayan bir savaşın içine çekilmişlerdir. Meskûn mahallerde bir türlü istedikleri üstünlüğü kuramayan birlikler, asimetrik tehditler karşısında başarısız olmuşlardır. Bu örnekler, günümüzde konvansiyonel savaşlara yönelik yapılan hazırlıkların asimetrik tehditlere karşı çaresiz kaldığını[131] destekler niteliktedir.

Günümüz silahlı kuvvetlerinin en büyük açmazlarından birisi, belirtilen çıkmazlara karşı reaksiyon geliştirilmesi hususudur. Cephe savaşları için yetiştirilen birlikler özel savaş yöntemlerini ihtiva eden düşük yoğunluklu veya asimetrik savaşlarda başarılı olamamaktadır. Çünkü ülkeler askeri yapılarını ve savunma planlamalarını hala öncelikle eski nesil planlama anlayışlarını esas alan konvansiyonel savaşlara yönelik hazırlamaktadırlar. Ancak tarihteki birçok örnek, geleneksel savaş senaryolarına göre hazırlanmış olan teşkilatların ve planların asimetrik tehditlere karşı ne kadar zor durumlara düştüğünü tecrübe etmemize neden olmuştur. Eski bir Çin askeri stratejisti olan Zhuge LİANG, MÖ 3.yy.da; "Akıllılar dövüşmeden önce kazanır, cahiller ise kazanmak için dövüşür. Usta saldırı karşıtların nasıl savunacaklarını bilmedikleri saldırıdır. Bu nedenle yüksek surlar ve derin hendekler güvenliği, sağlam zırhlar ve etkin silahlar kuvveti sağlayamazlar"[132]

---

[130] Ali Bülent Uşaklı, **age**, 198.

[131] Gökhan Astan, "Gelişen Teknolojiler ve Değişen Muharebe Şartlarında Geleceğin Askerine Yönelik Teknoloji Öngörü Çalışması" (Yüksek Lisans Tezi, Kara Harp Okulu Savunma Bilimleri Enstitüsü, 2015), 185.

[132] Zhuge Liang, **Savaş Sanatında Ustalaşmak**, çev. Sibel Özbudun (İstanbul: Anahtar

demiştir. İşte bu nedenledir ki süper güç olarak bilinen ABD, 11 Eylül saldırılarını eli kolu bağlı olarak seyretmek zorunda kalmıştır.

Asimetrik saldırı türlerinin birçoğu için hukukun hiçe sayıldığını, etik düşünceden tamamen uzak olduğunu söylemek mümkündür. İnsanlık tarihi boyunca savaş kuralları ve bir savaş hukuku geliştirmeye çalışılmışken artık tüm bunlar tamamen rafa konmuş ve hiçbir asimetrik tehdit türünün dönük bakmadığı bir kavram haline gelmeye başlamıştır. Çünkü düşman adil savaşmayarak, çoğunlukla kirli bir oyun tarzı benimser hale gelmiştir. Tiyatrodan, evin salonuna kadar geniş bir yelpazedeki her yer asimetrik bir tehdidin hedefi olabilmektedir[133]. Dolayısıyla asimetrik savaş tehditleri, askeri tedbirlerin etkisini de önemli ölçüde azaltmaktadır. Çünkü bu tür eylemlerin çoğu halkın yoğun olarak yaşadığı yerler de dahil olmak üzere hedef gözetmeksizin, beklenmedik anlarda ortaya çıkmaktadırlar[134].

Dünyadaki savaşların geneline bakıldığında, savaşlarda güçlü olanın kazanması gerektiği çelişkisi bulunmaktadır. Savaşlar incelendiğinde 5'e 1 asimetrik güç dengesi bulunan savaşların, % 30'unun güçsüz olan tarafın kazandığı gözlemlenmektedir. Güçsüz tarafın kazanma sıklığının özellikle son yüzyıl içerisinde artan bir oranda ilerlediği görülmektedir. Günümüzde asimetrik tehdit unsurları ve ülkelerin askeri güçlerini karşılaştırdığımızda bu oranın çok daha ciddi bir artış gösterdiği görülmektedir[135].

Asimetrik tehditleri, simetrik tehditlerden ayıran hususlar şu şekilde sıralanabilir:

- Alışılmadık ve sıra dışı olması,
- Klasik savaş kanunlarıyla tanımlanmamış araçları kullanması nedeniyle kural tanımaması,
- Askeri veya sivil, özellik taşıyan varlıkları hedef alması,
- Yalnızca karşı tarafın sadece maddi çıkarlarına zarar vermek değil, aynı zamanda psikolojik alanda da gücünü zayıflatmak üzere planlanması,
- Yapılan saldırıya, tehdide karşılık verilmesinin zorluğu,
- Asimetrik tehdidin bilinmeyen gizemi onun ürkütücü yanını arttırır. En üst seviyedeki güvenlik makamları bile asimetrik tehditlere yönelik tam olarak neye bakacaklarını bilmiyorlarsa tehditlere karşı savunma mekanizmaları oluşturmak güçleşir[136].

---

Kitabevi, 1997), 42.

[133] Jack D.Kem, **Campaign Planning: Tools Of The Trade**, 3.bs (Kansas: US Army Command and General Staff College, 2009), 85.

[134] Sefer Yılmaz, "Türkiye'nin İç Güvenlik Yapılanmasında Değişim İhtiyacı", **Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, c.21, s.3 (2012): 33.

[135] Ivan Arreguin-Toft, "How the Weak Win Wars: A Theory of Asymmetric Conflict", **International Security**, c.26, s.1 (2001): 96.

[136] Colin S.Gray, "Thinking Asymmetrically in Times of Terror"**, US Army War College**, c.32,

Asimetrik savaşlar kapsam olarak incelendiğinde, kimilerine göre kavramın dinamik yapısı sebebiyle detaylı bir asimetrik tehdit listesi oluşturma girişimi bir hata olarak değerlendirilmektedir[137]. Ancak buna rağmen bahsedilen tehdit potansiyellerinin hangilerinin asimetrik olduğuna dair bir analiz yapmak, en azından tehdidin tanımlanabilmesi bakımından yararlı olacaktır. Bu kapsamda aşağıda sunulan unsurlar, asimetrik savaş yöntemleri olarak kullanılmaktadır[138]:

- Terör,
- Kitle imha silahları,
- Ekonomik tehditler,
- Bilişim (Siber) tehditler,
- Psikolojik harekât,
- Organize suçlar,
- Etnik ve dini çatışmalar,
- Bölgesel tehditler.

Yukarda bahsedilen asimetrik savaş yöntemleri şimdiye kadar karşılaşılan örnekler neticesinde sayılabilse de gelecekte bu unsurlara yenilerinin eklenebileceği değerlendirilmektedir. Bu yöntemler başta teknoloji olmak üzere çağa yön verebilen her türlü gelişmeye ve değişikliğe göre şekillenmekte, uygulayana göre de farklılık göstermektedir. Asimetrik tehdit tipleri değerlendirildiğinde sonuç olarak tehditteki anahtar noktalar; dengesiz etki elemanı, az kaynaklarla stratejik amaçlara ulaşmak ve psikolojik içeriğin önemini ortaya çıkarmaktır[139].

## 3.2. Asimetrik Tehditlere Yönelik Savunma Anlayışları

Geçmişte, sömürgeci istilalar bir yana bırakılırsa genellikle birbirine yakın güçlerin tırmanan gerilimlerinden kaynaklanan savaş olgusuna asıl anlamını veren "savaş meydanı" kavramı, İkinci Dünya Savaşı sonrasında büyük oranda ortadan kalkmıştır. Günümüzde savaşlarda düşman hedeflerine verilen zayiatın sınırları her geçen gün artmaktadır. Düşmanın giderek "görünür, bilinir" olmaktan çıkması ise, saldırgan ülke/devlette ölçülü ve merhametli olma ilkelerini ortadan kaldırmaktadır. Buna paralel olarak artık günümüzde taraflar artık birbirlerine savaş ilan etmemekte,

---

s. 1 (2002): 5.

[137] Steven Lambakis, James Kiras ve Kristin Kolet, "Understanding The Asymmetric Threats To The United States", **Comparative Strategy**, c.21, s.4 (2002): 253.

[138] Ahmet Küçükşahin ve Tamer Akkan, **age**, 4.

[139] Kenneth F. Mckenzie, **The Revenge Of The Melians: Asymmetric Threats And The Next QDR** (Washingon: Institute for National Strategic Studies, 2000), 3.

genel olarak beklenmedik anlarda sinsice saldırmaktadırlar[140].

Dünya çapında son yüzyıldaki çatışma ve anlaşmazlıklar incelendiğinde; sadece çok küçük bir kısmının (Azerbaycan-Ermenistan, Dağlık Karabağ; Çin-Japonya, Senkaku Adaları; Afganistan-Pakistan, Keşmir; Kuzey Kore-Güney Kore, ABD-Kuzey Kore) ulus devletlerin karşı karşıya geldiği çatışmalar olduğu, geriye kalan büyük çoğunluğun ise asimetrik güçlerin ve değişik tarzda aktörlerin rol aldığı düşük yoğunluklu ve uzun soluklu çatışmalar olduğu görülmektedir. Nijerya'da süren Boko Haram radikal dinci örgüt ve hükmet güçleri arasındaki çatışma, Filistin'de süregelen savaş, Suriye ve Irak topraklarında yaşanan bölgesel güçlerin, radikal dini terör örgütlerinin ve koalisyon güçlerinin arasında geçen çatışmalar ile Ukrayna'da dış güçlerin desteklediği ve taraf olduğu nihayetinde ülkenin parçalanmasına kadar varabilen çatışmalar da bu kapsamda sunulabilecek en güncel örneklerdir[141]. Ülkemiz açısından ise; PKK terör örgütünün, 1984 yılından itibaren başta terör faaliyetleri olmak üzere, güvenlik güçlerinin haricinde bölge insanı da dahil birçok hedefe yönelik uyguladığı şiddet içerikli taktikler[142], en yakından hissetmek zorunda kaldığımız asimetrik tehdit örnekleri olarak ön plana çıkmaktadır.

Asimetrik tehditler gelecekte de bugünkü duruma benzer, içinden çıkılması zor çatışmalara gebedir[143]. Asimetrik tehdidi algılayabilmek için sıralı üç yeteneğe ihtiyaç duyulduğu ortaya konmuştur: Dikkat, tanıma ve eyleme geçme.[144] Her ne kadar önlem almak ve kesin çözümlü güvenliği sağlamak mümkün olmasa da tarihsel süreç içerisinde karşılaşılan olaylar göz önünde bulundurularak dersler çıkarmak ve buna yönelik olarak muhtemel senaryoları da düşünerek farklı stratejiler geliştirmek önemlidir. Temel harekat tarzı; düşmanı ve durumu ortaya koymak, uygun stratejiyi uygulamak ve daima bir adım sonrasını görebilmektir.

Uzun vadeye yayılmış, düşük maliyetli, doğrudan çatışma riskini minimize eden asimetrik yöntemlerin terör örgütleri, illegal gruplar ve diğer aktörler vasıtasıyla uygulanmaya devam edileceği ve bu kapsamda kısa, orta ve uzun vadede kaos, güvensizlik, çatışma, şiddet ve korku ortamının artarak devam edeceği değerlendirilmektedir[145]. Güç mücadelesinde ekonomik ve teknolojik vasıtaların öncelikli araçlar olacağı, ekonomik ve sosyal olayların devletlerin geleceğini

---

[140] Berdal Aral, "Asimetrik Saldırı Savaşları, Siyaset ve Uluslararası Hukuk", **Uluslararası İlişkiler**, c.4, s.14 (2007): 60.
[141] Gökhan Astan, **age**, 20.
[142] Mehtap Yağ, "Türkiye Savunma Harcamalarının Karşılaştırmalı Analizi (1924-2010)" (Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi, 2014), 44.
[143] Ehsan Ahrari, Transformation of America's Military and Asymmetric War, **Comparative Strategy**, c.29, s.3 (2010): 223.
[144] Cristopher L.Wovels, "Asymmetric Attention Visualizing The Uncertain Threat", US Army Research Institute Research Report 2016, March 2010, Virginia, 1.
[145] 1'inci Or.K.lığı, **age**.

etkileyeceği, bölgedeki etnik ve mezhepsel zafiyetleri ve yönetim boşluklarını fırsat bilen tehdit odaklarının doğrudan çatışma yöntemi yerine asimetrik stratejiler izleyecekleri beklenmektedir.

Bahsedilen hususlar ışığında asimetrik unsurlara yönelik olarak hem bölüm içerisinde belirtilen hususları özetlemek hem de temel özelliklerinden bahsetmek suretiyle, asimetrik savaşın hangi boyutlara ulaşılabileceğini anlamada faydalı olabileceği değerlendirilmektedir. Bu kapsamda; orantısızlık, ön görülemezlik, karşı tedbir alma güçlüğü, çok yönlülük (askeri, ekonomik, sosyal, kültürel vb.), hedef gözetmezlik, istismar odaklı olmak, psikolojik yetki yaratmak, düşük maliyetli olmak, teknolojiyle yakın ilişkilide bulunmak, değişen durumlara süratle ayak uydurabilmek, failin kimliğinin belirlenmesinin zorluğu gibi özelliklerin asimetrik savaşın temelinde yatan hususlar olarak karşımıza çıkabileceğini söylemek mümkündür.

Savunma planlamacılarının esas vazifesi, planlamanın ayrılmaz özelliği olan stratejik belirsizliği azaltmaya ve yönetmeye çalışarak geleceğin güvenlik sorunlarını çözmektir. Asimetrik tehditlere yönelik savunma planlamalarında belirsizliği tamamen aydınlatmak imkânsıza yakın olsa da, bazı hususları dikkatlice gözden geçirip farklı yollar keşfetmek mümkündür[146].

Öncelikle savunma planlamasına başlarken atılacak ilk adım, değişen güvenlik algıları göz önünde bulundurularak, bir senaryo dahilinde; muhtemel tehditlere ve sahip olunan/olunması gereken yeteneklere yönelik olarak coğrafi, öznel ve nesnel boyutları içerecek şekilde bir durum değerlendirmesi yapmak olmalıdır[147]. Sonraki aşamalarda alınabilecek tedbirler ve savunma planlamalarına yön vermesi gereken unsurlar genel olarak şu şekilde olmalıdır:

- Gelişmiş bir istihbarat sistemi,
- Her türlü değişime süratle reaksiyon gösterebilecek bir kuvvet yapılanması,
- Asimetrik savaşlarda görev yapmak üzere özel olarak eğitilmiş birlikler,
- Etkin bir kurumsal altyapı tesis ederek özel eğitimli birlikler ile diğer askeri güç unsurlarının birlikte hareket edebilmesi,[148]
- Devletin tüm organlarıyla birlikte gelişen durumları sahiplenerek, gerektiğinde milli güç unsurlarının tamamının bütünleşik olarak kullanımını sağlayacak ulusal bir işbirliği mekanizması tesis etmektir.

Bu hususların önem durumları ve savunma planlamalarında yer alma gerekliliklerini daha kapsamlı olarak incelemek gerekirse; ulusal güvenliğin

---

[146] Ali L. Karaosmanoğlu, "Savunma Planlaması ve Stratejik Belirsizlik", **Bilge Strateji Dergisi**, c.7, s.12 (2015): 23.
[147] Ali L. Karaosmanoğlu, **age**, 35.
[148] Karl E.Reinhard, **A Paradigm for the System of Systems Countering Asymmetric Enemy Kinetic Attacks** (Pennyslvania: US Army War College, 2005), 10-14.

sağlanmasında istihbaratın yeri ve önemi kuşkusuzdur. Gerek düşman tanımlarındaki farklılık, gerekse dünyadaki güvenlik ve tehdit algılamalarındaki hızlı değişim; güvenliğin aktörlerini, güvenlik sağlama olanaklarını, niteliğini ve istihbaratını da önemli ölçüde sorgulamakta ve değişime zorlamaktadır[149]. Bu nedenle gelişmiş bir istihbarat sisteminin tesisi ve değişime ayak uydurarak kendini yenilemesi, asimetrik tehditlere karşı yapılacak savunma planlamalarında büyük rol oynamaktadır.

Asimetrik tehditler konusunda askeri planlamacıları bekleyen belirsizlikler; dost ve düşman unsurların, savaşın türünün ve zamanının belirlenememesidir. Tüm bu belirsizlikler içinde en zoru zamanlamanın kestirilememesidir. Dost ve düşman unsurların tanımlanması, diplomasinin görece yavaş gelişen/dönüşen seyri nedeniyle daha kolaydır. Ne tür bir savaş ile karşılaşılacağını belirleyen temel etmen ise çevresel faktörlerdeki değişim hızıdır[150]. Güvenlik ortamının doğasında var olan belirsizlik seviyesi, öngörüler neticesinde şekillenen hazırlık seviyelerine doğrudan etki etmektedir. Bu kapsamda, gelişmiş bir istihbarat ağının öngördüğü uygun senaryolara göre süratle harekete geçebilecek, değişime açık bir kuvvet yapılanmasının önemi büyüktür.

Modern savaşlar rakibi yenmek, zayıflatmak veya niyetinden vazgeçirmek amacına yönelik olarak pek çok stratejinin ortaya çıkmasına zemin hazırlamaktadır. Bu stratejiler, daha çok teknolojinin avantajlarını kullanan asimetrik saldırı yöntemlerini içermektedir[151]. Bu nedenle, asimetrik savaşta esas caydırıcı olarak ön plana çıkan faktör; özel eğitimli, asimetrik savaşa yönelik birliklerin yetiştirilmesidir. Özellikle 11 Eylül saldırısı sonrası oluşan güvenlik ortamında; kara, hava ve deniz kuvvetlerinin haricinde özel yetiştirilmiş birlikler ile bu kuvvetlerin özel birliklerle olan uyumu, müşterek hareket edebilme kabiliyetleri asimetrik savaşların kaderini belirlemektedir.

Sahip olunan askeri güç, asimetrik etkiler karşısında hiçbir zaman yeterli olmayabilir veya asimetrik etkiye maruz kaldığında devre dışı kalabilir.[152] Bu doğrultuda, savunma planlamalarının esasında odak noktasını oluşturması gereken husus, asimetrik savaşa kurulacak savunma mekanizmasını bir bütün halinde değerlendirerek; planlama ve uygulama sürecini sivil-asker işbirliği zeminine oturtup ulus olarak birlikte hareket etme yetisi kazandırmaktır. Oluşan bu yeni savaş

[149] İhsan Bal, "Küresel Çağ: Güvenlik, Tehdit ve İstihbaratın Değişen Seyri", **Cumhuriyet Strateji** (6 Ocak 2006): 1-2.
[150] Monica Toft ve Talbot Imlay, **The Fog of Peace and War Planning: Military and Strategic Planning Under Uncertainty** (New York: Routlegde, 2006), 1-2.
[151] Sait Yılmaz, "Modern Savaş ve Savunma Reformları", USAM Bülteni, www.academia.edu/7647876/Modern_Savaş_ve_Savunma_Reformları [27.05.2016].
[152] Taner Altunok, **age**, 138.

ortamında, planlama ve uygulama safhalarında, devletin sadece askeri yapısı ile değil tüm kademelerinde aynı dilin konuşulması, asimetrik tehditler konusundaki belirsizliklerin azaltılmasında önemli rol oynar.

Zafiyetlerin ve tehdit odaklarının belirlenmesi, alınabilecek önlemlerin ve yeteneklerin ortaya konmasıyla; potansiyel tehditlere karşı güvenlik konusunda, belirli ölçüde stratejiler geliştirebilme imkânı sağlamaktadır. Sonuç olarak asimetrik savaş durumuna karşı nelerin yapılabileceği, her devletin güvenlik stratejilerine ve gelecek vizyonlarına göre çeşitlilik gösterebilmektedir. Asimetrik tehditlere ilişkin mevcut olan stratejik belirsizlikler, hedeflerin belirlenmesi ve alınması gereken tedbirler konularında tutarsızlıklara yol açmaktadır. Bu kapsamda devletlerin asimetrik tehditlerle savaşabilmeleri; öncelikle kendisini tanıması, sahip oldukları yetenekler ve kendisine özgü geliştirdiği stratejilerle mümkün olabilir. Bu sayede asimetrik gücü tersine çevirerek kendi menfaatlerine uygun hale getirebilir[153].

Bu konuya ilişkin yine ünlü komutan ve düşünür Sun Tzu'nun sözleri aslında tam olarak bu bölümde anlatılanları özetlemektedir: "Karşısındakini ve kendini bilen hiçbir savaşta tehlikeye düşmez; karşısındakini bilmeyen, sadece kendini bilen bir kazanır, bir kaybeder; karşısındakini de, kendini de bilmeyen her savaşta mutlaka tehlikeye düşer". Asimetrik tehditlere ilişkin savunma planlamalarını yaparken "karşısındakini" bilmek, tahmin etmek her zaman ve her koşulda mümkün olmasa da "kendini bilmek" ve gerçekçi olarak değerlendirip ona göre stratejiler geliştirmek imkan dahilindedir. Asimetrik savaşta başarıya ulaşmaya, mevcut zafiyetleri azaltmaya zemin oluşturan temel faktör de budur[154].

Asimetrik tehdit kaynağının yaratacağı tehlikenin zararsız kılınması için bunların önceden algılanması ve bunlara karşı savunma tedbirlerinin mutlaka önceden planlanması gerekmektedir. Bu kapsamda; tehdidin doğru belirlenmesi ve risklerin oluşmadan tespit edilmesinde çözüm odaklı ve kapsamlı bir bakış açısı, yüksek sezgi ve öngörü, kendi imkân ve kabiliyetlerini doğru olarak tanımlayabilme, geleceği tahminde başarı, saplantı ve hayallere kapılmayan bir yaklaşım tarzı, özgür ve esnek bir düşünce sistemi mutlak suretle göz önünde bulundurulması gereken unsurlar olarak ön plana çıkmaktadır[155].

Giderek karmaşıklaşan dünya siyaseti, güce karşı tepki koymaya başlayan toplumsal hareketler ve bunlarla ilgili ekonomik koşulların, asimetrik savaşları

---

[153] Michael Breen ve Joshua A.Geltzer, "Asymmetric Strategies As Strategies Of The Strong", **Parameters**, c.41, s.1 (2011): 51-52.
[154] Sun Tzu, **age**, 7-8.
[155] Faruk Köksal, **Risk ve Tehdit Kavramında Yeni Paradigmalar ile Asimetrik Tehdit Analizi**, **Türkiye'ye Yönelik Dış Kaynakları Risk ve Tehditler** (İstanbul: Harp Akademileri Basımevi, 2007), 20.

bundan böyle daha çok gündeme getireceği aşikârdır. Uluslararası anlaşmalar ve insan hakları yasalarıyla, devletlerin asimetrik tehditlere karşı harekât yeteneği bir anlamda sınırlanırken, bu tür uluslararası anlaşmalar ve etik kuralların başta terör örgütleri olmak üzere asimetrik unsurlar nezdinde bağlayıcılığı olmaması nedeniyle, istediklerini kabul ettirmek ve küresel bir kaos ortamı yaratmak için asimetrik savaşı en kolay seçenek olarak kullanmaktadırlar[156].

Neticede karşılaşılan tabloda savaş kavramının klasik varsayımlarının çürüdüğü ve bilinen sınırlarının dışına çıktığı görülmektedir. Dolayısıyla buna bağlı olarak mutlak güvenliğin mümkün sayılmadığı çağımızda, özellikle güvenlik konusunda milat olarak kabul edilen Soğuk Savaş dönemi öncesi ve sonrasıyla incelendiğinde bir önceki bölümde de açıklanmaya çalışıldığı üzere hem gücün hem de güvenliğin tanımının ve buna bağlı olarak da oluşturulan savunma anlayışlarının değiştiğini hatta bundan sonra da değişebileceğini söylemek mümkündür.

Tarihin her dönemi kendi koşullarına uygun türde savaşlar yaratmıştır. Bir bakıma, her dönemin kendi savaş türünü ortaya çıkardığını söylemek mümkündür. 11 Eylül 2001'de yolcu uçakları ile New York'taki ikiz kulelerin patlatılmasıyla akıllara kazınan, son olarak da PKK ve DEAŞ terör örgütlerinin faaliyetleriyle iyice su yüzüne çıkan süreç de göstermektedir ki; tarafları, taktikleri, kullandığı vasıtaları, çıkış noktasındaki sebepleri açısından farklılık gösterse de içerisinde bulunduğumuz yüzyılın savaş türü “Asimetrik Savaş” olacaktır.

Buraya kadar anlatılan hususlar doğrultusunda, savunma planlama anlayışlarının tarihsel süreç içerisinde geçirdiği evrimler ve bunun sonucunda yaşanan paradigma dönüşüm ihtiyacına temel oluşturan "Asimetrik Tehditler" kavramsal yönleriyle ele alınmaya çalışılmıştır. Çalışmanın bundan sonraki ve özünü oluşturan "Siber Tehditler ve Savunma Planlamalarındaki Dönüşüme Olan Etkileri" konularına değinmeden önce; çalışma öncesinde ve esnasında gelişen durumlar neticesinde problem sahası olabileceği değerlendirilerek hazırlanan "Görüşme Soruları"na verilen yanıt ve değerlendirmeler, çalışmanın bu bölümüne dahil edilmiştir. Bu kapsamda, belirlenen temalar ve onlara ilişkin yapılan değerlendirmeler şu şekildedir[157]:

---

[156] Ali Külebi, “Asimetrik Savaş Kavramı ve Tehditler”, www.inadina.com/inadeski/sayi156/yazi9.htm [28.05.2018].

[157] Toros Ünüversitesi Rektörü Sayın Prof.Dr. Haluk KORKMAZYÜREK'le yapılan görüşme neticesinde şu ana kadar incelenen konulara ilişkin hazırlanan sorulara vermiş olduğu yanıtlar ve değerlendirmelerden alınmıştır. Görüşme sorularına, Kaynakça bölümünün sonunda ayrıca yer verilmiştir.

**<u>Birinci Tema:</u> Savunma Planlaması Anlayışının Stratejik Öngörü İhtiyacının Giderek Arttığı Günümüzde Gösterdiği Değişim.**

Stratejik öngörü, günümüzde, yüksek türbülans (çok hızlı değişen ortam şartları ve ilişkiler ağı) ve dolayısıyla belirsizlik ortamında yapılmak durumundadır. Böyle bir durumda, geleceği tam ve isabetli öngörmek kolay değildir. Öngörmek yerine "çevreyi şekillendirmek" yaklaşımı daha etkili olacaktır. Böyle bir ortamda, yeteneğe dayalı, etki odaklı planlamalar öne çıkmaktadır.

**<u>İkinci Tema:</u> Belirsizlikle Mücadele Edebilmek için Birçok Yöntemin Uygulanabilmesi Mümkün Olmakla Birlikte, Tehdit Boyutu ve Şeklinde Yaşanan Hızlı Değişim Karşısında Başarılı Olunup/Olunamamasına İlişkin Değerlendirmeler.**

Bu konuya ilişkin çevreyi şekillendirme stratejilerinin önem kazandığı değerlendirilmektedir. Bunlardan en öne çıkanı, koalisyonlar oluşturmak suretiyle riskleri paylaşmak, ama aynı zamanda faydaları da paylaşmak olmaktadır. Kuvvet Yapısı oluşturma açısından ise; esnek, küçük, ancak çeşitli yetenekleri, görevin gereklerine ve hedefte yaratılmak istenen etkilere bağlı olarak, kısa sürede bir araya getirip kullanabilen yapılar oluşturmak önem kazanmaktadır.

**<u>Üçüncü Tema:</u> Savunma Planlama Sürecinin Başarısı; Planlamacıları Yönlendirecek Açık ve Belirgin Bir Devlet Politikasının (Savunma Politikası) Varlığına Bağlıdır. Bu kapsamda "Asimetrik Tehdit" Ortamında Verilecek Kararların Politika Planlama Sürecini Yönlendirmedeki Yeterliliği.**

Özellikle uzun vadeli politik yönlendirmeler söz konusu olduğunda asimetrik tehdit ortamı ile politika arasındaki uyumsuzluk kaçınılmazdır. Böyle durumlarda önemli olan, sistemlerin ne kadar süratle yeni duruma uyum sağlayabileceğidir. Bu kapsamda, diplomasi ihtiyaç duyulan süreleri kazanmak için en güçlü enstrüman olmaktadır. Ülkenin savunma sanayii yetenekleri ve dışa bağımlılık düzeyleri de bu kapsamda çok önem kazanmaktadır. Bir başka konu da ekonomik güçtür. Aşırı borçlu ve borç ödeme yeteneği düşük olan ülkelerin "tabi" kalmaları (söyleneni yapmaları) ya da yeni ortaklar bulmaları kaçınılmazdır.

**<u>Dördüncü Tema:</u> Savunma Planlamalarındaki Esnekliğin Sağlanabilmesi.**

Kuvveti kullanmak ve verilecek askeri görevleri icra etmek zorunda olan askeri planlamacılar, belirsizlikten hoşlanmaz. Onlar için esas olan belirliliktir. Çünkü en büyük tehdit en yakın tehdittir. Esneklik sağlayacak başlıca uygulamaları şu şekilde sıralamak mümkündür:

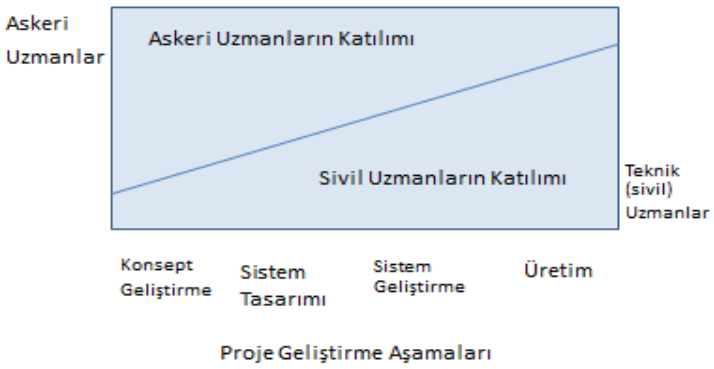
- Gözden geçirme süreçlerinin sıklığı ve gözden geçirme süresinin uzunluğu/kısalığı,
- Karar alma süreçlerinin etkinliği ve süresi,
- Yetenek temelli planlamada "Gelecekte icra edilecek" görevlerin gerektirdiği yeteneklere odaklanma,
- Müşterek harekât (hem kuvvet ve hem de komuta) yeteneklerinin geliştirilmesi.

**<u>Beşinci Tema:</u> Tehdit Değişiminin Hızlı Olduğu Günümüzde Savunma Planlamasında Sivil Yeteneklerden Yararlanabilme Olasılığı.**

Sivil yeteneklerin savunma planlamasına yönelik dahil edilmesi husus olmazsa olmazdır. Bu konuya ilişkin şu şekilde değerlendirmelerde bulunmak mümkündür:

- Stratejik analiz ve değerlendirme (bu konuda verilecek araştırma projeleri üzerinde çalışabilecek) yapabilecek sivil düşünce kuruluşları olmalı,

- Askeri (silah sistemleri vb.) projelerin oluşturulması sürecinde, teknik ve teknolojik dünya (akademi ve sanayi) daha yeteneğin tanımlanması aşamasından itibaren süreçlere dahil edilmelidir. Bu kapsamda aşağıdaki şöyle bir kadro yapılabilir:şekli öneriyorum: Aşamalara göre oranlamak gerekirse örneğin konsept aşamasında yer alan; 10 kişinin 8'i asker, 2'si sivil; üretim aşamasında ise ikisi asker sekizi sivil. Aşamalardaki katkı yapabilecekleri konulara ilişkin bu şekilde bir oranlamadan bahsetmek mümkündür. Bu birliktelik sadece silah sistemleri geliştirmede değil, askeri, politik vs her türlü analizde de kurulabilir, hatta kurulması zorunludur. Dolayısıyla asker ve sivil işbirliğinin proje/çalışmanın her aşamasında olması gerektiği değerlendirilmektedir.




**Şekil 2: Proje Geliştirme Aşamaları**

**<u>Altıncı Tema:</u> Yetenek Temelli Savunma Planlamasının Özünü Yetenek Havuzu Matrisinin Tam ve Doğru Bir Şekilde Oluşturulması Teşkil Etmektedir. Dolayısıyla Asimetrik Tehdit ve Özellikle DEAŞ Gibi Aniden Ortaya Çıkan Terör Grupları Dikkate Alındığında Yetenek Havuz Matrisinin Ne Kadar Gerçekçi Bir Şekilde Oluşturulabileceği.**

Yetenek temelli yaklaşımda esas olan gelecekteki yetenek ihtiyaçlarına odaklanmaktır. Çünkü günümüz zaten belirlidir, ihtiyaçlar tam tanımlanmıştır. Böyle yaklaşıldığında, gelecek bir gün olarak günümüz olarak baz alındığında yetenek hazır halde bulunacaktır. Burada önemli olan geleceğe iyi odaklanabilmek, bu kapsamdaki değerlendirmelerde hata yapmamaktır. Bu da bütünleşik bir çalışma gerektirmektedir. Örneğin günümüzün ciddi tehditlerinden birisi olan siber savaş tehditlerine ilişkin: Askeri hacker mı yetiştirilmeli yoksa mevcut hackerları planlama süreçlerine dahil edecek yol ve yöntemler mi bulunmalıdır? Hangisi daha etkin, süratli, ekonomik ve akılcı? Dolayısıyla ortak bir çalışma ve iradeyle amaçlar ve hedefler ortaya konarak, en akılcı, maliyeti düşük ve süratli reaksiyon gösterecek çözümlere ve ona uygun yeteneklere yönelmek esas olmalıdır.

**<u>Yedinci Tema:</u> Savunma Planlama Yaklaşımlarında Teknolojideki Gelişime Bağlı Olarak "Caydırıcılığın" Önem Kazandığı Görülmektedir. Söz Konusu Anlayışın Yetenek Temelli Planlama ile Birlikte Uygulanabilme İhtimali.**

Caydırıcılığa dayalı anlayışın temelinde; sayısal, olmuyorsa ya da sayısal üstünlük sağlamak akılcı değilse, teknolojik üstünlük sağlamak esastır. Teknolojinin her askeri fonksiyon alanında eşit hızda geliştiği ve caydırıcı bir üstünlük sağlayacağını iddia etmek pek olası değildir. Bazı durumlarda sayısal üstünlük kaçınılmaz olabilir. Ancak ikisi bir arada da olabilir. Buradaki temel fark şudur: Her askeri fonksiyon alanında mı, yoksa bazı fonksiyonlarda mı? Yani soru şu hali almaktadır: Hangi askeri fonksiyonlarda teknolojik üstünlüğe dayalı caydırıcılık, hangilerinde sayısal üstünlük? Bu nedenle burada yeni bir kavramdan bahsetmek mümkündür: Caydırıcılık Havuzu.

**<u>Sekizinci Tema:</u> Planlamacıları Bekleyen En Çetin Görevlerden Birinin, Sürprizlerin Kötü Sonuçlar Karşısında En Yüksek Korumayı Sağlayan Yaklaşımı/Yaklaşımları Bulabilmek" Olduğu İfade Edilmektedir. Bu İfadenin Günümüz Şartlarındaki Geçerliliği.**

Söz konusu yaklaşımın günümüz şartlarında da geçerli olduğu söylenebilir. Bu husus esnek planlamanın bir başka boyutunu ifade etmektedir. Yani askeri politik/ askeri stratejik esnekliği kaybetmemek. "Stratejiyi uygulayabilmenin iki temel koşulu

vardır: Hakim noktaları (araziyi vb.) ve inisiyatifi elde bulundurmak. Bunlardan biri bile eksikse stratejinin uygulanması güç hale gelir" ifadesi eski harekât ortamları için söylenen ancak günümüzde de geçerliliğini aynen koruduğu değerlendirilen bir hususdur. İnisiyatif kelimesi İngilizce “initiative, initiation” kelimesinin karşılığıdır. Bu da bir şeyi başlatabilme, girişimde bulunabilme gücünü ifade eder ve bir anlamda hareket serbestisini ifade etmektedir.

**Dokuzuncu Tema: Savunma Planlamasında Uzun Dönemli Planlama Sürecinin Sona Ermesi veya Devam Etme İhtimali.**

Savunma Planlamalarında uzun dönemli planlama sürecinin tamamen sona erdiğini söylemek yanlış olacağı değerlendirilmektedir. Bu kapsamda; uzun dönemli planlamanın sadece uzunluğu değişmiştir. Belirsizlik, türbülans ve asimetriden dolayı uzun dönemin uzunluğunu kısaltmak zorunda kalınmasının yarattığı eksiklik, Yetenek Temelli Yaklaşım ve bu yaklaşım üzerine bina edilen Etki ve Görev Odaklı Harekat türevi anlayışlarla kapatılmaya çalışılmaktadır.

**Onuncu Tema: Yetenek Temelli Savunma Planlama Yaklaşımında Yetenek Uyumsuzluğunun Söz Konusu Olması Halinde Yapılacak Hususlar.**

Yetenek temelli yaklaşımın esası; ortak bir çalışma ve iradeyle, amaçlar ve hedefler ortaya konarak, en rasyonel, en ekonomik ve en süratli çözümlere ve ona uygun yeteneklere yönelmektir. Bu kapsamda yetenek uyumsuzluğundan kasıt; planlamanın temelini oluşturan tehditlerin önlenebilmesi için belirecek olan ihtiyaçların, yeteneklerin yanlış veya eksik tespiti, yanlış temele oturtulması olduğu değerlendirilmektedir. Bu kapsamda; esnek planlama fikri ön plana çıkmaktadır. Planlamadaki esneklik ve daha önceden de belirtilen inisiyatif, uyumsuzluk konusunda da belirli bir hareket serbestisi sağlayacağından ortaya çıkan uyumsuzluk durumlarına daha akılcı ve seri bir şekilde reaksiyon gösterilmesini sağlayacağı değerlendirilmektedir. Dolayısıyla bütün planlamaların temelini oluşturan; planlamanın ilk safhadasındaki öngörülerin ve anlayışların mutlaka çok dikkatli, beklenmeyen durumlara veya ilerleyen safhalarda uyumsuzluğa neden olabilecek durumlara karşı belirli bir esneklik barındırması düşünülmelidir.

## 3.3. Bir Asimetrik Savaş Unsuru Olarak Siber Tehditler

Bilişim çağının bir lütfu olan ve günümüzde hayatın her alanına nüfuz etmiş olan internet, her açıdan fayda getirmiş ve sağladığı hizmetlerle ciddi anlamda

kolaylıklar sağlamıştır. Ancak bunun yanı sıra; toplumları, kurumları ve devletleri bu altyapılara bağımlı hale getirmiştir. Bu nedenle bilgi teknolojileri; zarar görmesi, saldırıya uğraması veya çalışmasında yaşanan aksaklıklardan dolayı hizmet verememesi durumunda çok ciddi sonuçlar doğurabilecek risklerle karşı karşıya bırakabilecek, toplum düzenini bozabilecek, ulusal hatta uluslararası güvenliği tehlikeye atabilecek altyapılar haline gelmiştir[158]. Bu ifade o kadar ciddi boyutlarda dile getirilmeye başlanmıştır ki; 11 Eylül saldırılarının cep telefonu ve internet kullanılarak gerçekleştirildiğini öne sürenler bile bulunmaktadır[159].

Geçmişte de değerli olan bilginin, elektronik hale gelmesi ve bilişim sistemleri ile yoğun bir şekilde paylaşılması maruz kaldığı tehdidi artırmakta, özellikle 11 Eylül sonrasında daha da çok dillendirilmeye başlanan asimetrik tehditler kavramına yeni bir boyut kazandırmaktadır[160].

Asimetrik savaşta en tehlikeli hasım olarak görebileceğimiz aktörler, genel olarak maliyeti ve riski az, doğrulanabilirliği zor olduğu için hukuki olarak da ciddi boşluklar bulunan saldırıları tercih ederler. Bunun da en önemlilerinden birisi hiç kuşkusuz siber saldırı yöntemleridir[161]. Çünkü siber ortam tamamen kendine özgü ve benzersiz bir çevre olup, anonim, asimetrik, çoğunlukla da gizlidir. Ülke sınırları olmayan siber ortamda saldırı hızlı, kolay ve ucuzdur[162].

### 3.3.1. Siber Uzay, Siber Savaş, Siber Tehdit ve Siber Saldırı

#### 3.3.1.1. Siber Uzay

İletişim sektöründe bir devrim yaratıp, küresel interneti oluşturan ARPANET'in tasarımı 1960'lara dayansa[163] da, bilişim teknolojilerinin gelişmesiyle birlikte hayatımıza iyice nüfuz eden internet, modern çağın en etkin kitle iletişim araçlarından biri haline gelmiştir. Kişisel kullanım araçlarından cep telefonları, televizyonlar vb. cihazlara kadar günlük hayatta kullandığımız en basit aygıtlar bile internet ortamına dahil olmuştur. Günümüzde çocuklardan yetişkinlere kadar, herkes

[158] Ercan Nurcan Yılmaz, Halil İbrahim Ulus ve Serkan Gönen, "Bilgi Toplumuna Geçiş ve Siber Güvenlik", **Bilişim Teknolojileri Dergisi**, c.8, s.3 (2015): 142.
[159] **Empires, Systems and States: Great Transformations in World Politics**, ed. Michael Cox, Ken Booth ve Tim Dunne, (Cambridge: Cambridge University Press, 2002), 94.
[160] Gökhan Bayraktar, **age**, 17.
[161] Muzaffer Ünsaldı, **age**, 39.
[162] Bradley K.Ashley, "Anatomy of Cyberterrorism: Is America Vulnerable?", United States Air Force (USAF) Air War College Seminar 10, A Research Paper www.au.af.mil/au/awc/awcgate/awc/ashley.pdf [26.01.2018].
[163] Katie Hafner ve Matthew Lyon, **İnternet Tarihi**, çev. Sinem Yazıcıoğlu (İstanbul: Güncel Yayıncılık, 2000), 8.

bilişim çağındaki gelişmelerin getirdiği imkânlardan azami istifade etmekte, hayatın her anında internetle içli dışlı olmaktadırlar. Soğuk Savaş sonrası dönemden beri artan internet kullanıcı sayısına yönelik olarak, 1990'larda 3 milyon civarında iken, 2015 yılında 3.2 milyara ulaşmış, 2025 yılı itibarıyla ise 4.7 milyara ulaşacağı[164] öngörülmüştür. En güncel haliyle 30 Haziran 2017 tarihli internet kullanıcısı sayılarına ilişkin verilerde belirtildiği üzere; 7.559.028.970'lik dünya nüfusunun, 3.885.567.619'unun yani % 51.7'lik kesminin internet kullanıcısı[165] olması; hem sayılara yönelik öngörüleri hem de her iki insandan birinin internet kullanıcısı olduğunu ve internet kullanımının günümüz şartlarında ihtiyaçtan ziyade artık neredeyse bir zorunluluk haline geldiğini ispatlar niteliktedir. Böylece internet, milyarlarca bilgiyi ve kullanıcıyı barındıran sanal bir ortam haline gelmiştir[166].

Değişim ve gelişimin bu hızla devam edeceği varsayıldığında; gelecekte bir bilgisayarla, internetle ya da başka herhangi bir siber sistemle çalışmanın, ışıkları veya suyu açmak kadar gerekli olacağını[167] ileri sürmek çok da olağan mantık dışı karşılanmamalıdır. Bu kapsamda bilişim teknolojilerindeki hızlı değişim, sistemlerin sayısallaşması, günlük hayatın önemli bir parçası haline gelmesinin yanı sıra bilgi paylaşımının zorunlu olması, kapsamın beklenmedik şekilde genişlemesi, tehditlerin gelişmesi ve artması[168] nedeniyle Siber Uzay terimi her geçen gün daha da yüksek sesle dile getirilen bir kavram haline gelmiştir.

Teknolojik, biyolojik, sosyolojik ve ekonomik sistemlerde, kumanda uç iletişim süreçlerini incelemeye dayanan bir amaca doğru yönlendirilmiş etki bilimi[169] olarak tanımlanan "Sibernetik" teriminden türeyen siber kelimesi ile uzay kelimelerinin bir araya gelmesinden oluşan "siber uzay" kavramı, ilk olarak William Gibson'un 1984 tarihli "Neuromancer" adlı bilimkurgu romanında kullanılmıştır[170]. "Siber Uzay" kavramına ilişkin özellikle konunun öneminin gün geçtikçe artması nedeniyle birçok tanım geliştirilmektedir. Bunların bazılarından; bilginin tanımlanması, kaydedilmesi, iletilmesi amacıyla ağ merkezli sistemler ve elektromanyetik spektrumun kullanılması suretiyle oluşturulan, internet ve benzeri haberleşme ağlarını da

---

[164] David Burt ve diğ., "Cyberspace 2025: Today's Decisions, Tomorrow's Terrain, Navigating the Future of Cybersecurity Policy", Microsoft Corporation (2014): 3-4.

[165] "Internet Usage Statistics: The Internet Big Picture", http://www.internetworldstats.com/stats.htm [25.01.2018].

[166] Mahzure Kara, "Siber Saldırılar-Siber Savaşlar ve Etkileri" (Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, 2013), 1.

[167] Lene Hansen ve Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School", **International Studies Quarterly**, c.53 (2009): 1167.

[168] ASELSAN AŞ.de görevli Ali Yazıcı'nın "Siber Saldırıların Komuta-Kontrol Bilgi Sistemlerine Etkisi" konulu sunumunun yansılarından alınmıştır.

[169] **Büyük Larousse Ansiklopedi** (İstanbul: Gelişim Yayınları, 1986), 10470.

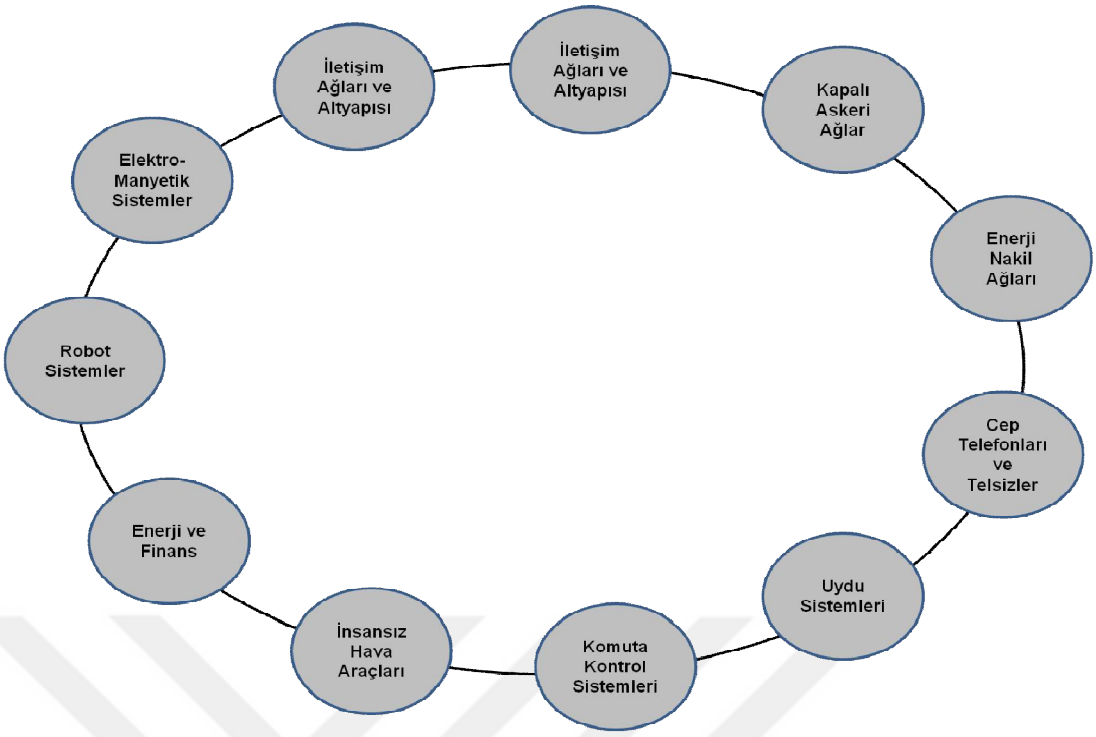
[170] Umay Türkeş Günay, "Folklor ve Siber Çağ", **Türk Dünyası İncelemeleri Dergisi**, c.13, s.1 (2013): 217.

kapsayan bir ortam[171], insan, yazılım ve hizmetlerin teknolojik ağ ve cihazlar aracılığıyla özellikle internet üzerinden etkileşimi ile ortaya çıkan fiziki olmayan sanal ortam[172], herhangi bir coğrafi sınırlamaya maruz kalmaksızın, internete bağlı bilgisayar ağlarının oluşturduğu elektronik ortam[173] tanımlarının yanı sıra siber uzayı daha soyut manada tanımlayan; bilgisayar destekli, etkileşimli sanal bir ortam, her gün dünya çağında milyarlarca insanın yaşadığı bir halüsinasyon[174] şeklinde ifadeler bulunmaktadır. ABD Savunma Bakanlığı ise siber uzayı; "İnternet, telekomünikasyon ağları, bilgisayar sistemleri, bunlara ilişkin işlemciler ve kontroller ile birbirleriyle bağlantılı bilişim teknolojisi altyapıları ağını içeren bilişim çevresinin içinde yer aldığı küresel alan" olarak tanımlamaktadır[175].

Siber uzay, siber alem ve sanal alem terimlerinin tamamı daha özel olarak internete karşılık olarak da kullanılmaktadır. Çünkü internet, iletişim yöntemi açısından siber olmakla birlikte meydana getirdiği ortam açısından sanaldır[176]. Ancak biraz daha geniş kapsamda değerlendirilecek olursa; siber uzay yalnız internete bağlı bilgisayar ve sistemlerini değil; yerel ağları, cep telefonu teknolojilerini, fiber altyapıları[177], açık ağdan bağımsız askeri ağları, yazılım tabanlı telsiz sistemlerini, elektronik harp ve elektronik komuta sistemlerini, insansız hava araçlarını ve uzay tabanlı iletişim sistemlerini[178] kapsayan oldukça karmaşık yapıya sahip bir ortamdır. Özetlemek gerekirse Şekil 3'te de belirtildiği şekilde; fiziksel cihaz ve donanımlardan, ağ sistemlerine, sisteme dahil olan kullanıcılardan, sunulan hizmetlere kadar bu bilişim ortamına bir şekilde dahil olan bütün unsurlar siber uzayın birer parçası olarak saymak mümkündür.

---

[171] Jason Whittaker, **The Cyberspace Handbook** (London: Routledge, 2003), 5.
[172] Gürol Canbek'in 07 Kasım 2016 tarihinde SATEM Komutanlığında verdiği "Siber Tehditlere Karşı Farkındalık Eğitimi"nin ders notlarından alınmıştır.
[173] Muharrem Gürkaynak ve Adem Ali İren, "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, c.16 (2011): 263.
[174] Nilgün Camgöz, "Siberuzay, Sanal Gerçeklik ve Müze", Bilim ve Teknik, www.biyolojiegitim.yyu.edu.tr/fizuzaypdf/Siberuzay199845.pdf [22.01.2018].
[175] The Joint Publication 1-02, "Department of Defence Dictionnary of Military and Associated Terms", http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf#search-"cyber%20space" [Erişim Tarihi: 21.01.2018].
[176] M.Emin Ulaşanoğlu, Ramazan Yılmaz ve M. Alper Tekin, "Bilgi Güvenliği: Riskler ve Öneriler", Bilgi Teknolojileri ve İletişim Kurumu, 2010, Ankara.
[177] Joseph S.Nye, "From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?", **Bulletin of The Atomic Scientists**, c.69, s.5 (2013): 8.
[178] Uğur Akyazı, "Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler", **6.Uluslararası Kriptoloji Konferansı Bildiriler Kitabı** (Ankara, 2013), 216.




**Şekil 3: Siber Uzayın Unsurları**

Uğur Akyazı, **Siber Harekat Ortamının Siber Güvenlik Tatbikatları Kapsamında Değerlendirilmesi** (İstanbul: Harp Akademileri Basımevi, 2012), 56.

Siber uzay; herhangi bir ülke coğrafyasıyla veya hukukuyla sınırlı olmayan, bağlanmak için herhangi bir kurum ya da yetkiliden izin almayı gerektirmeyen, kimlik tespitinin zor olduğu, zamanla tüm sosyal yaşamın aktarılacağı bir ortamdır. Birçok gözlemciye göre ise siber uzay; yeni taktiklerin ve görülmemiş bir formun değil, yeni bir mekan olarak kara, hava, deniz ve yörüngede kabaca benzer biçimlerde ortaya çıkacak bir tür olarak algılanmaktadır[179].

Siber uzayın getirdiği sınırsız özgürlük ortamında yaratılan sanal kavramlar, zamanla gerçek dünyayı, kişileri ve devletleri etkileyecek sonuçlar doğurmaya başlamıştır. İnsanlık adeta iki ayrı dünyada yaşar hale gelmiştir. Bir tarafta ülke sınırlarının, ulusal egemenliklerin, hukuki düzenlemelerin, ölçülü özgürlüklerin ve hakların bulunduğu, herkesin belirli bir kimlikle tanımlandığı gerçek dünya; diğer tarafta ise hem fiziksel hem de özgürlük anlamında sınırların, hukuksal düzenleme ve güvenlik tedbirlerinin bulunmadığı, kimliklerin gizlenebildiği siber uzay yer almaktadır[180].

[179] Michael Breen ve Joshua A.Geltzer, **age**, 48.
[180] Gökhan Bayraktar, **age**, 15.

Günümüz dünyasında hayatın akışının artık tamamıyla siber uzayda gerçekleştiğini söylemek çok da yanlış olmaz. Siber uzayın insanlığın faydasına birçok hizmeti sunduğu kabul edilmiş bir gerçektir. Bireylerin yanı sıra kamu ve özel kuruluşlar da hizmet alanı olarak siber uzaydan faydalanmaktadırlar[181]. Siber uzaydaki gelişmeler ışığında gün geçtikçe; uygulamalar artış göstermekte, tehdit, tehlike ve saldırılara yönelim artmakta ve doğal olarak buna yönelik sürekli yeni çözümler üretilmeye çalışılmakta, bilinmesi gereken konular giderek çoğalmakta, yapılacak ve kontrol edilecek parametreler artmaktadır[182].

Bilinmeyenin bilinenden daha çok olduğu siber uzay[183] faydalı birçok faaliyeti içinde barındırsa da, ilerleyen bölümlerde daha ayrıntılı belirtileceği üzere kötü niyetli amaçlar içinde kullanılabilmektedir. Bu açıklama dahilinde; bireysel veya grup halindeki suçlular, kötü niyetli kişiler, teröristler, kurum ve kuruluşlar, uluslararası örgütler, ülkelerin silahlı kuvvetleri ve istihbarat örgütleri, sanayi casusluğu yapmak veya rakiplerini zayıflatmak isteyen şirket/firmalar, casusluk ve istihbarat toplama amacı olan devletleri siber uzayın başlıca aktörleri[184] olarak saymak mümkündür.

Geçmişte, milli güç unsurları içerisinde adı sadece askeri güç içerisinde yer alan teknoloji ve siber uzaydaki kabiliyetler, artık başlı başına değerlendirilmesi gereken bir güç unsuru haline gelmiştir[185]. Bu kapsamda; siber uzayda etkin olmak; siber uzay icin daha kapsamlı operasyonlar geliştirmek, daha geniş siber deneyimi ve bilinci oluşturmak, siber operasyonların komutasını merkezileştirmek, diğer kurum ve devletlerle ortaklıklar yaratmak gibi yeteneklerin geliştirilmesi anlamına gelmektedir[186].

### 3.3.1.2. Siber Savaş

Tarih boyunca hep olumsuz bir çağrışım yapan ve şiddeti temsil eden savaş kavramı, dönemler içerisinde uygulama şekilleri ve kullanılan yöntemler açısından değişimlere uğrasa da günümüzde hala geçerliliğini koruyan, yıkıcı sonuçlara sebep olan birbirlerine hasım olan unsurların güç gösterisidir. İlk çağlardan itibaren ilkel silah, araç ve taktiklerle başlayan bu sonucu iki ihtimalli oyunun bugün geldiği nokta şaşırtıcı olmakla birlikte gelecekte ulaşabileceği boyutları tahmin etmek çok zordur.

---

[181] Mahzure Kara, **age**, 4.
[182] Prof.Dr. Şeref Sağıroğlu'nun "Siber Bilgi Güvenliği ve Savunma Yöntemleri" konulu sunumundan alınmıştır.
[183] Zafer Yener, **age**, 108.
[184] Richard O.Hundley ve Robert Anderson, **Emerging Challenge: Security and Safety in Cyberspace**, ed. John Arquilla and David Ronfeldt (Santa Monica: RAND Corporation, 1997), 232.
[185] Zafer Yener, **age**, 33.
[186] US Department of Defense, **Quadrennial Defense Review**, (US, 2010), .X.

Daha önceki bölümlerde de anlatılmaya çalışıldığı üzere değişen çevre, tehditler, yöntemler vb. gibi sebeplerle ciddi dönüşümlere uğrayan savaş artık klasik manada anlaşılan savaş kavramının çok dışına çıkmış ve siber uzay adı verilen ortamın da savaş alanı olarak kabul edilmesiyle gelecekte gerçekleşmesi muhtemel savaşların bambaşka boyutlarda cereyan edeceği üzerinde durulmaya başlanmıştır.

Siber savaşlar 5.boyut savaşları olarak da tabir edilmektedir. Bu görüş doğrultusunda, siber uzay diye adlandırılan söz konusu sanal ortam; kara, hava, deniz ve uzaydan sonra 5.savaş alanı olarak belirlenmiş[187], 14-15 Haziran 2016 tarihlerinde Brüksel'de icra edilen NATO Savunma Bakanları Toplantısında da siber uzayın, resmi olarak bir harekât alanı kabul edilmesine karar verildiği belirtilmiştir[188]. Bu görüşü destekler nitelikte; "19.yy.da ulusal güvenlik ve refahımız için denizlerimizin güvenliğini sağlamak zorundaydık, 20 yy.da ise buna hava dahil oldu, son olarak 21.yy.da ise ilaveten siber uzaydaki güvenliğimizi de sağlamak zorundayız"[189] açıklaması, 2009 yılında Birleşik Krallık Bakanlar Kurulunun hazırlamış olduğu "Birleşik Krallık'ın Siber Güvenlik Stratejisi" adlı raporunda tam olarak bu şekilde yer almış ve siber uzayın da artık bir savaş alanı olması görüşü ortak bir fikir haline gelmiştir.

Bugün güvenlik rekabetinin parçası olarak gelişen siber uzay, devletlerin ve grupların güç yarışını sürdürdükleri bir alana dönüşmüştür[190]. Devletler bir yandan ulusal ve uluslararası seviyede farklı tedbirler almanın güvenlikleri için gerekli olduğunu hissederken, diğer taraftan da siber uzayda meydan gelen gelişmeleri ve rekabeti yakından takip ederek, çıkabilecek bir dünya savaşının siber uzayda yaşanması ihtimali uluslararası politikayı da şekillendirmektedirler[191]. 2010 yılında Amerikan Hava Kuvvetlerinin hazırladığı bir reklam filminde geleceğin savaşlarının siber uzayda gerçekleşeceği ve elektrik şebekeleri, su sistemleri gibi kritik altyapıların askeri hedefler olacağı[192] vurgusu siber uzayın geleceğin muharebe alanlarına yönelik öngörüleri doğrular niteliktedir.

Asimetrik bir savaş olarak değerlendirilebilecek olan siber savaşlar, günümüzde klasik savaşlara destek olarak kullanılmakla birlikte başlı başına bir savaş olarak

---

[187] Genelkurmay MEBS Başkanlığının, "21'inci Yüzyılda Siber Savaş ve Hukuki Durum" konulu sunumunun yansılarından alınmıştır.

[188] https://www.nato.int [16 Haziran 2016].

[189] United Kingdom Cabinet Office, "Cyber Security Strategy of The United Kingdom", https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf [25.01.2018].

[190] Salih Bıçakçı, "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", **Uluslararası İlişkiler Dergisi**, c.10, s.40 (2014): 104.

[191] Nazlı Choucri, "Introduction: Cyber Politics in International Relations", **International Political Science Review**, c.21, s.3 (2000): 243.

[192] US Air Force, "Cyberspace", https://m.www.youtube.com/watch?v=amJI0xZA25c [29.01.2018].

uygulanması mümkün bir yöntemdir. Siber savaşların asimetrik özelliği nedeniyle bireyden, uluslararası örgütlere kadar geniş bir yelpazede olabilen tehdidin kaynağının tespit edilememesi ve düşük maliyetlerle çok ciddi sonuçlar doğurabilecek[193] potansiyele sahip olması siber savaşa yönelik artan bir ivmeyle her geçen gün daha da yoğunlaşan bir algının oluşmasına sebep olmuştur.

Uluslararası hukuk dilinde siber silahlarla çatışma durumu olarak tanımlanmasının[194] yanı sıra meydansız savaş olarak da nitelendirilen siber savaşların[195] esası; düşmanı psikolojik olarak çökertmek için bilgisayar kontrolü altındaki sistemlerine izinsiz, gizli ve görünmez olarak erişmektir[196]. En basit anlamıyla siber uzayda gerçekleştirilen "bilgi savaşı"[197] olarak özetlenebilecek olan siber savaş kavramını daha geniş bir ifadeyle; ekonomik, politik, askeri veya psikolojik amaçlar için seçilen hedefe yönelik bilgi ve iletişim sistemleri üzerinden gerçekleştirilen organize saldırılar bütünü[198] olarak tanımlamak mümkündür.

Siber savaşta amaç; kontrolü ele geçirerek bilgileri çalmak, değiştirmek, çökertmek ya da yanlış yönlendirmek üzere hareket etmek, kendi bilgi sistemlerimizi siber saldırılara karşı korurken, hedef ülke veya örgütlerin kritik altyapılarına veya silahlı kuvvetlerine ait bilgi ve komuta-kontrol merkezlerini işlemez ve kullanılamaz hale getirmek, istenilen şekilde yönlendirmek, aynı zamanda siber uzaydan istifade ederek istihbarat temin etmektir[199]. Bu tür sistemler artık günümüzde ciddi oranda siber uzayın bir öğesi haline geldiklerinden, siber saldırılara karşı hedef teşkil etmektedirler. Burada kritik altyapılardan kasıt; "işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda; can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar"[200] veya bir diğer tanımıyla "fonksiyonelliğini yitirmesi durumunda sağlık hizmetlerine, toplumsal ve güvenliğe, vatandaşların

---

[193] Gökhan Bayraktar, **age**, 18.

[194] Michael N. Schmitt ve Liis Vihul, "The Nature of International Law Cyber Norms", **International Cyber Norms**, ed. Anna-Maria Osula and Henry Rõigas (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publications, 2016), 29.

[195] Hakan Şentürk ve diğ., "Siber Güvenliğin Taarruzi Boyutu ve Uluslar arası Hukuk Kurallarının Uygulanabilirliği", **6.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı**, Ankara, 2013, 51.

[196] Cahit Karakuş, **Kritik Alt Yapılara Siber Saldırı**, http://www.ylt44.com/Security/Siber/siber.pdf [23.01.2018].

[197] Kartal Okan, "The Symmetrical Evolution Of (The Notion Of) State Security According To Asymmetrical Threats: From Sticks And Stones To Cyber Warfare" (Yüksek Lisans Tezi, 2015), 45.

[198] Tolga Mataracıoğlu, "Sayısal Ortamda Savaşın Tarihçesi", Sayısal Ortamda Savaş Sempozyumu (1), 2010.

[199] Richard A. Clarke ve Robert K. Knake, **Siber Savaş (Cyber War)**, çev. Murat Erduran (İstanbul: İstanbul Kültür Üniversitesi Yayınları, 2010), 8.

[200] T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, **Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı** (Ankara, 2012), 3.

ekonomik refahına veya hükümetin verimli çalışmasına ciddi yönde tesir eden bilgi ağları ve sistemleri"[201] olarak ifade edilmektedir. 11 Eylül saldırısının hemen ardından güvenlik vurgusunun öne çıktığı tanımlamalarda örnek olarak ABD tarafından kritik olduğu kabul edilen altyapılar Tablo 2'de, AB'ye göre kritik olduğu değerlendirilen altyapılar Tablo 3'te, Siber Güvenlik Kurulu tarafından ülkemiz için belirlenen kritik altyapılar ise Tablo 4'te gösterilmiştir.

**Tablo 2: ABD Kritik Altyapı Sektörleri**

| | | |
|---|---|---|
| Enerji | Savunma Endüstrisi | Kimya |
| Bankacılık ve Finans | Nükleer Reaktör, Madde, Atıklar | Tarım ve Gıda |
| Devlete ait Tesisler | Ticari Tesisler | Kargo ve Sevkiyat |
| Su | Bilgi Teknolojisi | Acil Sistemler |
| Barajlar | İletişim | Halk Sağlığı |
| Kritik Üretim | Nakliye Sistemleri | Milli Anıtlar |

Hasan Çiftçi, **Her Yönüyle Siber Savaş** (Ankara: Tübitak Yayınları, 2013), 9.

**Tablo 3: AB Kritik Altyapı Sektörleri**

| | | |
|---|---|---|
| Enerji | Sağlık | Kimyasal ve Nükleer Endüstri |
| Bilgi ve İletişim Teknolojileri | Finans | Ulaşım |
| Su | Nakliye | Uzay ve Araştırmalar |
| Gıda ve Tarım | Kamu-Hukuk Düzeni ve Emniyeti | |

Cristina Alcaraz and Zeadally Sherali, "Critical Infrastructure Protection: Requirements and Challenges For The 21st Century", **International Journal of Critical Infrastructure Protection**, Vol.18 (2015): 53.

**Tablo 4: Türkiye'de Kritik Altyapı Sektörleri**

| | | |
|---|---|---|
| Enerji | Elektronik Haberleşme | Ulaştırma |
| Su Yönetimi | Finans | Kritik Kamu Hizmetleri (Sağlık, Gıda, Acil Yardım gibi kritik veriler) |

Emine Yazıcı Altıntaş, "Ülkemizde Siber Güvenlik", www.icwcturkey.com/files/2014/54899f3052c8c.pptx [25.01.2018].

[201] Mehmet Kara ve Serdar Çelikkol, "Kritik Altyapılar: Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği", 4.Ağ ve Bilgi Güvenliği Sempozyumu, 2011, Kocaeli, 2.

Her ne kadar siber tehditlerin hedefi olabilecek kritik altyapılarının içerisinde yer alsalar da yüksek stratejik öneme sahip olan askeri sistemleri ayrıca sıralamak gerekmektedir. Bu kapsamda risk potansiyeli yüksek askeri sistemlerin şunlar olduğu değerlendirilmektedir:

- Askeri Haberleşme Ağları,
- Komuta Kontrol ve MEBS Sistemleri,
- Hedef Tespit ve Teşhis Sistemleri,
- Silah Sistemleri.

Siber savaşın mahiyetinde, düşmanın bilgi ve iletişim devreleri içerisine zorla veya izinsiz girerek yanlış/hatalı bilginin yayılmasını sağlamak ve elektronik olarak çökertmek de yer almaktadır. Saldırı amaçlı yapılan bu tür bir savaşta, bilgi savaşçıları düşmanın bilgi merkezlerine beklenmeyen saldırılar yaparlar[202]. Siber savaşların, bilinen klasik savaş yöntemlerine nazaran çok ciddi avantajları bulunmaktadır. Aşağıdaki tablo (Tablo 5) üzerinden siber savaşlar ile klasik savaşlar arasında bir değerlendirme yapmak mümkündür:

**Tablo 5: Klasik Savaş ile Siber Savaşın Karşılaştırılması**

| Kriterler | Klasik Savaş | Siber Savaş |
|---|---|---|
| **Saldırı Kaynağı** | Saldırının kaynağını bulmak nispeten kolaydır. | Saldırının kaynağını bulmak çok zordur. |
| **Hızı** | Kullanılan silah sisteminin hızı kadardır. | Işık hızındadır. |
| **Hasar Tespiti** | Fiziksel etkilerinden dolayı hasar tespiti nispeten kolaydır. | Hasarın tespiti ve boyutunu bulmak çok zordur. |
| **Silah Sistemleri** | Kara, hava ve deniz muharebe alanlarında kullanılan (tank, top, uçak, gemi, helikopter, tüfek, füze, bomba vb.) silahlar. | Bazen tek bir bilgisayar veya ağa bağlı basit bir cihaz bile yeterli olabilir. |
| **Teknoloji İhtiyacı** | İleri teknoloji ihtiyacı. | Teknolojiyle doğru orantılı. |
| **Maliyeti** | Kullanılan silah/sistemlerin maliyetine bağlı, ciddi maliyet gerektirebilir. | Maliyeti genelde ucuzdur. |
| **Etkisi** | Fiziksel alanda etkilidir. | Bilgi sistemleri ve iletişim sistemleri alanında etkili olarak hedef üzerinde çok ciddi sonuçlar doğurabilir. |

Hasan Çiftçi, **age**, 20.

[202] Mustafa Sağsan, "Bilgi Savaşı: Siperlerden Klavyelere Taşınan Savaşın Anatomisi", **Psikolojik Harp İstihbaratı Avrasya Dosyası Uluslararası İlişkiler ve Stratejik Araştırmalar Dergisi**, Fasikül:23, c.8, s.2 (2002): 110.

Tablo 5'ten de anlaşılacağı üzere; saldırının kaynağının tespiti, savaşın gelişme ve ilerleme hızı, sonuçlarına yönelik vereceği zararların tespiti, kullanılan silah/sistemler, ihtiyaç duyduğu teknolojik altyapı, maliyeti ve savaşın ekonomik boyutuna etkisi ve etki sahası kriterleri konusunda siber savaşların, klasik savaşlara nazaran çok ciddi avantajları bulunduğu görülmektedir. Ayrıca savaş sırasında fiziki cephe açma maliyeti ve insan kaybı göz önüne alınacak alındığında, elektronik saldırı ile sanal bir cephe açmak, birçok açıdan üstün bir strateji olarak kabul edilmektedir[203]. Belki de hepsinden daha önemlisi siber savaşın en büyük avantajı, güçlü ve gelişmiş olarak kabul edilen devletlerin bile siber savaşlar karşısında son derece çaresiz kalabildiği, dolayısıyla nicel ve nitel açısında üstünlüğün siber mücadelede zaferin anahtarı olamayacağının artık net bir şekilde anlaşılmasıdır.

Siber savaş ihtimallerine karşı geliştirilen savunma anlayışları doğrultusunda, özellikle son dönemde hemen hemen tüm güçlü yabancı silahlı kuvvetler siber savunma ve saldırı maksadıyla bir taraftan yeni teşkilatlar kurarken diğer taraftan da yetenek kazanma arayışları içerisindedirler. Çalışmanın üçüncü bölümünde ayrıntılı olarak bahsedilecek olan ve tezin de odak noktasını oluşturan siber savaş ve siber tehditlere karşı mevcut imkân ve kabiliyetler, hazırlık durumları konusunda özellikle ABD, Rusya ve Çin başta olmak üzere birçok devlet önemli taarruzi yetenekler geliştirmektedir. ABD Savunma Bakanlığının "21'inci Yüzyıl Savunma Öncelikleri" isimli resmi dokümanında siber uzayın öneminin bilhassa vurgulanması ve 21.yy.da bu alana verilen öncelik dikkat çekicidir[204].

Gelişmiş ülkeler başta olmak üzere savunma bütçelerindeki azalmanın bir sonucu olarak birlik ve personel sayılarında sayısal azalmalara gitmelerine rağmen, siber alan konusunda uzman ve eğitimli personele yönelik artış ve yatırım yapmaya öncelik vermektedirler. Yakın gelecekte savaşların kaderini; klasik cephelerin yerine, siber savaşların belirleyeceği[205], gelişmiş siber silahların kullanıldığı tam ölçekli bir siber savaşın gerçekleşmesi durumunda ise; dünyadaki askeri, ekonomik ve politik tüm dengelerin tamamıyla değişebileceği öngörülmektedir[206]. Bu nedenle ülkelerin bilgi sistemlerini ve kritik alt yapılarının esas alarak oluşturulacak olan savunma planlamalarının artık geri dönülmez derecede önemli olduğu değerlendirilmektedir.

---

[203] Cenk Ceylan, "Savaş Cephesi Olarak, Sanal Ortamda Savunma ve Saldırı", http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/savas-cephesi-olarak-sanal-ortamda-savunma-vesaldiri [25.01.2018].

[204] US Department of Defense, **Sustaining US Global Leadership: Priorities for 21st Century Defense**, 2012, 4-5.

[205] Gökhan Bayraktar, **age**, 60.

[206] Barış Çeliktaş, "Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme", (Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi, 2016), 59.

### 3.3.1.3. Siber Tehdit ve Siber Saldırı

İnternetin, kendisinin haberi olmayan kullanıcı ve sağlayıcılar tarafından silah olarak kullanmasından kaynaklanan durum, özellikle devlet dışı aktörlerin bu tip yöntemleri benimseyerek kullanmalarına neden olmuştur. Çoğu siber saldırı asimetrik bir yapı içermektedir. Gelişmiş ve bilgisayar sistemlerinin sık kullanıldığı ülkelerin altyapıları da bu tip saldırılara açık gelmektedir. Bunun nedeni, siber saldırılarda bilgisayar temelli sistemlerin kullanılmasıdır[207].

Siber saldırılar, daha çok 20.yüzyılda daha belirgin hale gelen asimetrik savaşın başka bir boyutudur. Bu tür saldırılar hem yapılması kolay ve hem de vereceği zarar hayal edilenin ötesinde olduğundan, karşı mücadele etmesi oldukça zordur[208]. Belirtilen faktörlerin yanı sıra, siber tehdidin kimliğinin belirlenmesine yönelik saldırı merkezleri yanıltıcı olabilmektedir. Siber saldırılarda, saldırıyı yapan ve saldırının kaynağı olan ülke veya örgüt farklı olabilmektedir. Bu nedenle beklenmeyen bir kaynaktan gelen saldırılar, aslında saldırının kaynağını şaşırtmak için yapılmış ya da söz konusu birimler arasındaki gerginlik ve çatışma durumu yaratmak amacıyla üçüncü bir taraf aracılığıyla yapılmış olabilir. Bu durumun ülkeler arasında kısa zamanda büyük krizlere neden olabileceğini[209] öngörmek çok da zor olmayacaktır.

Siber tehditlere ilişkin yapılan birçok değerlendirmede, geleceğe yönelik öngörülen saldırıların ya spesifik terör örgütlerinden ya da "siber tehditler" gibi kendine has özellikleri olan kaynaklardan geleceğinin belirtilmesi[210] konunun önemini ve uygulanabilirliğini vurgulamaktadır. Ayrıca geleceğe yönelik yapılan tehdit projeksiyonunda 2020 hatta 2030'ların en yüksek olasılıklı tehdit kaynaklarının "Siber Tehditler" olduğu belirtilmektedir[211].

Belirtilen hususlar dahilinde siber tehditler; siber uzayda bulunan bilginin bozulması, ifşa edilmesi, erişilebilirliğin kesintiye uğraması gibi istenmeyen durumlara neden olma potansiyeline sahip unsurlar olarak tanımlanabilir. Bu tehditler, bilgi ve iletişim teknolojilerinden faydalanılarak türetilmiş, tamamen yeni suç tanımları doğuran siber saldırıların yanı sıra; bilgi ve iletişim teknolojilerinin getirdiği imkanların araç olarak kullanıldığı, klasik saldırıların siber ortama

---

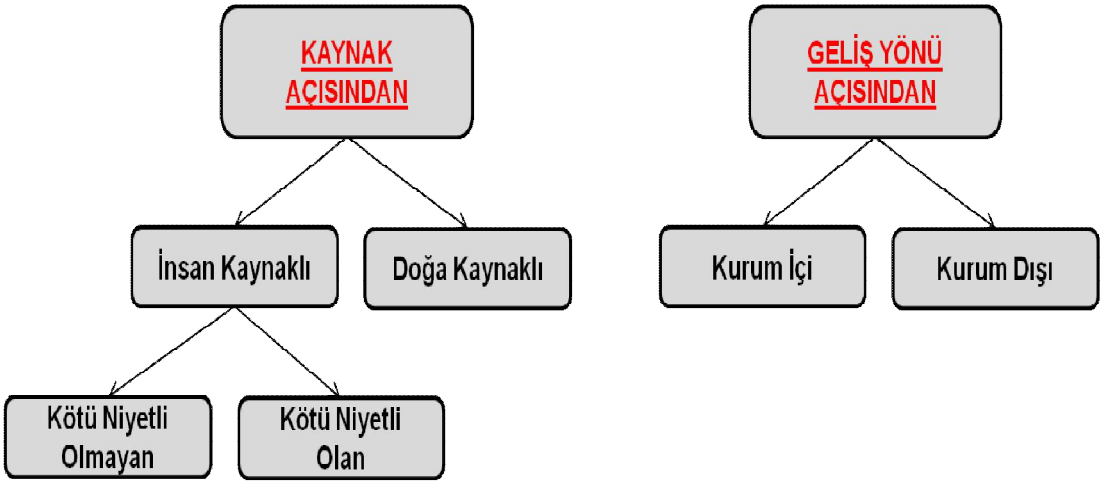
[207] Michael Breen ve Joshua A.Geltzer, **age**, 49.
[208] Sefer Yılmaz, **age**, 29.
[209] Mahzure Kara, **age**, 74.
[210] Robert Johnson, "Future Trends in Insurgency and Countering Strategies", Centre of Excellence Defence Against Terrorism, www.coedat.nato.int/publication/reaserches/04-FutureTrends.pdf [27.01.2018].
[211] Hasan Süzen'in, "Geleceğin Harekât Ortamında Kapsamlı Yaklaşım ve NATO'nun Komuta Kontrol Mimarisine İlişkin Görüş ve Çalışmalar" konulu sunumunun yansılarından alınmıştır.

uyarlanmış hallerini de kapsamaktadır[212]. Daha basit ve genel bir ifadeyle ise; bilgisayarlar, cep telefonları, oyun konsolları ve diğer internet bağlantılı cihazlarla karşımıza çıkan, çoğunlukla kimliği belirsiz kişilerce 24 saat boyunca yapılan ve yapılabilme ihtimali olan tacizler olarak açıklanabilmektedir[213].

Siber tehditlerin etkilerini kısa ve uzun vadeli olarak iki ayrı kategoride incelemek mümkündür. Kısa vadeli tehditler; hedef kişi, kurum, kuruluş ve devletlerin günlük faaliyetlerini etkileyen tehditlerdir. Dolandırıcılık olayları, veri ihlalleri, ATM'den usulsüz para çekilmesi vb. günlük faaliyetlerdir. Uzun vadeli tehditler ise; etkileri çok daha uzun süre devam eden ve çok daha geniş bir kitleyi etkileyebilen, ülkenin ve toplumun dengelerini değiştirebilen faaliyetleri içermektedir. Buna örnek olarak; endüstriyel ve askeri casusluk, sosyal hoşnutsuzluk ve huzursuzluk yaratma, ulusal güvenlik ihlali vb. tehditler verilebilir[214].

Siber tehditlerin kaynakları Şekil 4'te de görüldüğü üzere kaynağı ve geliş yönüne göre ikiye ayrılmaktadır. Bunların arasında en tehlikelisi kurum içindeki küskün ve art niyetliler ile kötü niyetli olmayan ancak eğitimsizlik, bilinçsizlik sonucunda istemeden de olsa zarar verenlerdir. Çünkü olası diğer teditlere karşı muhtemel hareket tarzları, potansiyel hedeflere bir tahmin ve tedbir geliştirme imkânı bulunması rağmen, biraz önce belirtilen tehdit kaynakları tamamen kapalı kutu olup, ne zaman, ne şekilde ve ne derece bir zarar verebileceklerine ilişkin bir öngörüde bulunmak ve tedbir almak çok zordur.

[212] Mustafa Ünver, Cafer Canbay ve Ayşe Gül Mirzaoğlu, "Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler", Bilgi Teknolojileri ve İletişim Kurumu, 2009, Ankara, 8.
[213] Jandarma Genel Komutanlığı MEBS Başkanlığı, **Siber Güvenlik El Kitabı** (Ankara, 2016), 60.
[214] Raymond Kim-Kwang Choo, "The Cyber Threat Landscape: Challenges and Future Research Directions", **Computers and Security**, c.30, s.8 (2011): 719-731.




**Şekil 4: Siber Tehdit Kaynakları**

Türksel Kaya Bensghir, "Kurumsal Bilgi Güvenliği Yönetim Süreci", Bilgi Yönetim Semineri, 2011, Antalya, strateji.deu.edu.tr/wp-content/uploads/2014/09/Kurumsal-Bilgi-Güvenliği-Yönetim-Süreci.pdf [05.02.2018].

Siber uzayla iç içe yaşamak aynı zamanda siber tehditlerin de hedefi haline gelmeyi beraberinde getirmiştir. Mevcut düzen, iki büyük dünya savaşındaki askeri ve jeopolitik üstünlüğün yerine, bilgi sistemleri üzerinden yapılan, siber uzayın sunduğu sınırsız özgürlük ortamı içinde daha kolay ve kısa sürede gerçekleştirilebilen saldırıları mümkün kılmaktadır[215]. Bu ortamda, bilişim teknolojisinin saldırı amacıyla kullanılmasına siber saldırı denilmektedir. Siber saldırılar, "Bilgi sistemleri doğrultusunda elektronik araçların bilgisayar programlarının ya da diğer elektronik iletişim biçimlerinin kullanılması aracılığıyla ulusal denge ve çıkarların tahrip edilmesini amaçlayan kişisel ve politik olarak motive olmuş, amaçlı eylem ve etkinlikler" [216] veya bir başka ifadeyle "Bilgisayarların siyasi olarak motive olmuş etnik gruplar, terör örgütleri veya gizli ajanlar tarafından şiddet, toplumun dikkatini çekme veya bir hükümetin politikalarını kendi amaçları doğrultusunda etkileme maksatlı olarak silah veya hedef olarak kullanılması"[217] şeklinde tanımlanmaktadır. Siber uzaya ilişkin en kapsamlı çalışma olarak kabul edilen Tallinn El Kitabı'nda ise siber saldırı; "Savunmaya veya saldırıya yönelik olmasına bakılmaksızın, insanların yaralanmasına ya da ölmesine, nesnelerin yok olmasına ya da zarar görmesine neden olan siber eylemler" olarak tanımlanmıştır[218].

[215] Gökhan Bayraktar, **age**, 24.
[216] Fatih Yamaç, **Siber Terörizm**, Emniyet Genel Müdürlüğü Terörle Mücadele Daire Başkanlığı Psikolojik Harekat Kurs Notları, 2001, Ankara, 5.
[217] Süleyman Özeren, **Responses to Cyber Terrorism**, ed. Terörizmle Mücadele Mükemmeliyet Merkezi (COEDAT)/Türkiye (Amsterdam: IOS Press, 2008), 71.
[218] Michael N.Schmitt, **Tallinn Manual on the International Law Applicable to Cyber**

Aynı çalışmada şiddet içermeyen psikolojik siber eylemlerin ve siber istihbarat faaliyetlerinin siber saldırı olarak kabul edilmeyeceği belirtilmiştir. Bu tanımların haricinde; ABD Savunma Bakanlığı tarafından "Bilgisayarda, bilgisayar ağlarında bulunan bilgilerin ya da bizzat bilgisayar ya da bilgisayar ağlarının kesintiye uğratılması, imha edilmesi"[219] şeklinde tanımlanan siber saldırı kavramının, ülkenin en üst askeri kurumu tarafından yapılan tanım neticesinde askeri açıdan da ne kadar dikkate alındığının bir göstergesidir.

Burada üzerinde durulması gereken en önemli nokta saldıranın kaynağını ayırt etmeksizin her siber saldırının siber savaş olarak değerlendirilemeyeceğidir. Savaşı tanımlarken dört farklı öğeden bahsedilmektedir. Bunlar; düşmanca tutum ve/veya eylem içermesi, kuvvet kullanmaya sebep olması, sonucunda hukuki bir durum yaratması ve en önemlisi faillerinin devletler olmasıdır[220]. Bu kapsamda değerlendirildiğinde siber savaş, bir ülkenin düşman ülkeye yönelik yapmış olduğu siber saldırıların çok daha ciddi bir boyutudur, yani savaşın aktörü devletlerdir[221]. Kötü niyetli bir hackerın banka hesaplarını ele geçirmesi veya bir bakanlığın web sayfasını kullanılamaz hale getirmesi bir siber savaş olarak değil ancak siber saldırı kapsamında değerlendirilmelidir. Dolayısıyla bu tür olayların savaş sebebi sayılmasının mümkün olmadığı değerlendirilmektedir.

Belirtilen ifadeler doğrultusunda, klasik savaş yöntemlerindeki taarruz ve savunma konseptlerine göre bir nevi siber tarruz olarak kategorilendirilebilecek olan siber saldırılar, teknolojik gelişmelere ve alınan tedbirlere karşı üretilen yeni yöntemler neticesinde bir takım araçları kullanarak hedef bilgi sistemlerine ve alt yapılarına yönelebilirler. Belirlenen hasma ait bilgi sistemlerine zarar vermek amacıyla fiziksel ya da yazılımsal olarak icra edilen bir siber harekat nevi olarak, uygulanma şekilleri açısından incelendiğinde;

- Kötücül yazılımlar (virüsler, kurtçuklar, truva atları, tavşanlar, mantık bombaları, bukalemun, klavye izleme, bilgi toplayan casus yazılımlar, istem dışı gönderilen ticari tanıtımlar),
- Mikroçipler,
- İstem dışı alınan elektronik postalar,
- Servis dışı bırakma saldırıları (Estonya ve Gürcistan saldırıları bu yöntemin en başarılı örnekleridir),

---

**Warfare** (Cambridge: Cambridge University Press, 2013), 92.

[219] Joint Chief of Staff, Joint Pub 3-13, Joint Doctrine for Information Operations GL-5, "Cyber Attacks: Unlawful Uses of Forces or Prohibited Interventions?", **Journal of Conflict and Security Law**, c.17, s.2 (2012): 220.

[220] Ali Bilgin Varlık, "Savaşı Tanımlamak: Terminolojik Bir Yaklaşım", **Avrasya Terim Dergisi**, c.1, s.2 (2013): 117-119.

[221] Kartal Okan, **age**, 45.

- Eşzamansız saldırılar,
- Süper darbe,
- Kaynak kod istismarı,
- Veri aldatmacası,
- Çöpe dalma,
- Web sayfası yönlendirmesi,
- Yemleme,
- Gizlice dinleme,
- Hackleme[222],
- Saplama yapma,
- Tuzak kapı (arka kapı),
- Trafik analizi,
- IP aldatmacası,
- Oturum çalma,
- Ağ tarama,
- Yerine geçme,
- Sosyal mühendislik[223] gibi yöntemlerin ön plana çıktığı görülmektedir.

Bilinçsiz kullanıcıların yarattığı riskler haricinde, siber tehdit olarak tanımlanan kötü niyetli kişi ve gruplar, teknolojinin gelişmesi ile birlikte her geçen gün farklı araçlara başvurarak söz konusu siber taarruz yöntemleri konusunda kendilerini geliştirmekte ve tedbir alınması daha zor yöntemler ortaya çıkarmaktadırlar. Dolayısıyla siber saldırı yöntemleri olarak yukarda belirtilen öğelere, çalışma son bulduğu andan itibaren bile yenilerinin eklenmiş olması olağan dışı sayılmamaktadır.

Bir çok siber saldırı senaryosunda, kritik alt yapıların ele geçirilmesi, kilitlenmesi ve yönlendirilmesiyle ülkede oluşacak kriz ortamının gözler önüne getirilmesine çalışılmaktadır. Şehrin elektrik şebekelerinin ele geçirilerek karanlığa bürünmesi, su şebekelerinin ele geçirilmesi, trafik ağının ele geçirilerek trafiğin felce uğratılması, telekomünikasyon ağının ele geçirilerek iletişimin durdurulması, telefonların çalışmaması, hastanelerde cihazların işlemez duruma getirilmesi, petrol boru hatlarının ele geçirilerek patlamalara sebep olunması, baraj kapaklarının açılması, karanlık gökyüzünde nereye gideceğini, nereye ineceğini bilmeden uçan uçaklara sebep olunması gibi birçok tehlikenin aynı anda gerçekleştirilmesi bilim kurgu olmaktan çıkmış ve gerçekleşmesi muhtemel[224] saldırılar olarak görülmeye

[222] Gökhan Bayraktar, **age**, 82-92.
[223] Abdullah Kör, **Siber Saldırılar İçin Dinamik Bir Çözüm Modeli** (Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, 2015), 6.
[224] Mahzure Kara, **age**, 32.

başlanmıştır. Dolayısıyla tehditlerin odağında hasmının omurgasını oluşturan birimler yer almaktadır.

Siber saldırının tarihi nispeten daha yeni olmakla beraber, 1982 tarihindeki "Farewell Dosyası" olayında ilk örneğine rastlandığı ileri sürülmektedir. KGB'nin teknoloji casusluğu yaptığını farkeden CIA, karşı istihbarat çalışması neticesinde SSCB'ne ait doğal gaz boru hattına ilişkin bir yazılıma zararlı kod yerleştirmiştir. Bu yazılımın kullanılması sonucunda uzaydan görülebilecek kadar büyük nükleer olmayan büyük bir patlamanın gerçekleştiği iddia edilmektedir[225].

Küresel manada değerlendirildiğinde ise, siber saldırıların ne zaman bir tehdit unsuru olarak öne çıktığını anlamak için çok da gerilere gitmeye gerek yoktur. Siber tehditlerin son yıllarda gelişmesi ve buna bağlı olarak siber saldırılara yönelmesi, kamuoyunda da bu tehlikenin varlığına yoğunlaşılmasına sebep olmuştur. Bir sonraki aşamada biraz daha ayrıntılı olarak anlatılacak olan üç kritik olay, siber saldırıların boyutuna yönelik dikkat çekilmesini zorunlu kılmıştır. Bunlar; 2007 yılında Estonya'nın maruz kaldığı siber saldırı[226], müteakiben Gürcistan'a yapılan saldırı[227] ve son olarak da İran'ın uranyum zenginleştirme programının "Stuxnet" adında bir virüsle çok ciddi şekilde zarara uğratılması[228] olaylarıdır.

Siber savaş ile klasik savaş arasındaki farklara yönelik bir önceki bölümde yapılan değerlendirmeye benzer şekilde, klasik saldırı ile siber saldırı arasındaki farkları da daha iyi anlayabilmek amacıyla şu şekilde bir tablo oluşturmak mümkündür:

**Tablo 6: Klasik Saldırı ile Siber Saldırının Karşılaştırılması**

| Kriterler | Klasik Saldırı | Siber Saldırı |
|---|---|---|
| **Kullanılan Araç** | Silah, bomba, EYP vb. silah ve düzenekler. | Bilgi sistem donanım ve yazılımları. |

[225] Dinnis Heather Harrison, **Cyber Warfare and The Laws of War** (Cambridge: Cambridge University Press, 2012), 6.
[226] Merve Yazıcı, "İlk Modern Siber-Atak: Estonya", www.tuicakademi.org/ilk-modern-siber-atak-estonya [22.01.2018].
[227] Lesley Swanson, "The Era of Cyber Warfare: Applying International Humanatarian Law To The 2008 Russian-Georgian Cyber Conflict", **Loyola of Los Angeles International & Comparative Law Review**, Vol.32 (2010): 303.
[228] David P.Fiddler, "Recent Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law", Vol.16, No.22, http://www.asil.org/insights/volume/16/issue/22/recent-developments-and-revelations-concerning-cybersecurity-and [23.01.2018].

**Tablo 6 - devam**

| | | |
|---|---|---|
| **Amacı** | Kamuoyunda korku ve baskı yaratmak, siyasi bir mesaj vermek. | Devletin kritik sistemlerine zarar vermek, hizmetleri kesintiye uğratmak, siyasi ve sosyal yönden etkilemek. |
| **Etki Alanı** | Saldırının yapıldığı bölge ya da alan ile sınırlıdır. | Ulusal veya uluslararası boyutlarda etkili olabilir. |
| **Risk** | Saldırıyı gerçekleştiren kişi ya da örgütler hayati açıdan risk altındadır. | Kimliğin belirlenmesi zor olduğundan, herhangi bir yaşamsal risk olmadan rahat hareket edip etkili saldırılar yapabilirler. |
| **Denetim** | Terörle mücadele konusunda kesin bir çözüm mümkün olmasa da etkin bir denetim mekanizması ile kısmi de olsa kontrol altında tutmak mümkün. | Siber saldırının kaynağını tespit etmek zor, yok etmek imkansıza yakın. |
| **Uygulanacak Ceza** | Suçun niteliğine göre hukuk kuralları çerçevesinde uygulanacak ceza bellidir. | Her gün yeni bir yöntem ve etki ile karşılaşılması sebebiyle mevcut kanunlarda hala bazı boşluklar mevcut. |

Oğuz Kara, Üzeyir Aydın ve Ahmet Oğuz, "Ağ Ekonomisinin Karanlık Yüzü: Siber Terör", //kisi.deu.edu.tr/oguz.kara/Ag%20Ekonomisinin%20karanlik%20yuzu%20siber%20teror.pdf [23.01.2018].

Tablo 6'da da görüldüğü üzere; saldırının yöntemlerinde kullanılan araçlar (silah, sistem vb.), saldırının amacı, saldırının uygulama ve etki alanının kapsamı, saldırının taşıdığı risk faktörü, saldırının denetimi ve kontrol ihtimali ve saldırının kaynağının tespiti durumunda uygulanacak yaptırımlar konularında siber saldırıların, klasik saldırılara nazaran çok ciddi farklılıkları barındırdığı görülmektedir. Tarih boyunca yaşanan örnekler de açıkça göstermiştir ki; artık saldırı yapacak unsurlar kendilerinin de ciddi manada zarar görebilecekleri, risk taşıyan, silah, malzeme ve teçhizat gerektiren, yüksek maliyetli, ter ve kan dökeceği saldırılardan kaçınmakta, bunların aksine oturduğu yerden sadece tek bir parmağını oynatarak klasik saldırı yöntemlerini kullanarak verebileceği etkinin misliyle fazlasını verebileceği, daha geniş ve uzak alanlara ulaşabileceği, yakalanma korkusu ve riskinin nispeten daha az olduğu siber saldırıları tercih etmeye başlamışlardır.

Riskin az olması konusunu biraz daha açmak gerekirse; henüz siber saldırının ne zaman başladığına ve meşru savunma hakkının ne zaman başlayıp ne zaman biteceğine bir cevap bulunamamıştır[229]. Bunun yanı sıra; siber saldırılarda

[229] Zafer Yener, **age**, 38.

saldırganın nadiren suç mahallinde bulunması nedeniyle, klasik saldırıların aksine hazırlık, icra ve kaçış esnasında yakalanma olasılığı da ortadan kalkmaktadır[230]. Böylece siber saldırganlar çok hızlı bir şekilde saldırıyı gerçekleştirmeyi müteakip, gerçek kimlik ve yer bilgilerini açığa vurmadan kaçabilmektedirler[231]. Bu nedenle siber tehdidin ve saldırının tespitine yönelik zorlukların, hukuki boşluklarla birleştiği de göz önününde bulundurulduğunda, kaynağın kendisini klasik saldırlara nazaran daha az risk altında hissetmesi ve yakalanma korkusu barındırması olağan gözükmektedir. Hepsinden önemlisi; hem medyanın hem de halkın bu tür ciddi sonuçlara yol açabilecek bir bilgisayar saldırısına duyacakları büyük ilgiden dolayı, bu olay çok dikkat çekecek ve basında kendine büyük bir yer bulacaktır[232]. Üstelik bu tür saldırılar için artık ileri seviyede bir teknik bilgi ve tecrübe sahibi olmaya ihtiyaç da bulunmamakta[233], geniş ve gelişmiş saldırı yöntemleri sayesinde neredeyse günümüzde herkes ağ sistemlerinin açıklarından faydalanabilmektedir[234]. Dolayısıyla belirtilen kriterlerdeki avantajları göz önünde bulundurulduğunda, siber saldırıların klasik bir saldırıyla kıyasla oldukça rasyonel bir yöntem olmasının yanında; Estonya, Gürcistan ve özellikle İran'daki Stuxnet krizlerinden sonra nükleer bir silahtan daha fazla zarar verebilecek bir etkiye neden olabileceğini[235] söylemek mümkündür.

Siber uzayda teknolojinin gelişimi açısından bakıldığında saldırı, savunmaya her zaman hükmeder[236]. Çünkü önce yeni saldırı yöntemleri geliştirilir, ardından tespit ve önlemeye yönelik savunma tedbirleri araştırılır[237]. Günümüz dünyasının ana çatışma temaları olan, siber saldırılarla devlet sırları ve devlet savunma sisteminin diğer ülkelerce ele geçirilmesi ve buna yönelik alınması gereken tedbirler devletlerin savunma planlama anlayışlarının esas düşüncesi haline gelmiştir[238]. Bu nedenle gizli sistemlere, sistem açıklarından faydalanarak sızan ve önemli sırları ele

---

[230] Susan W.Brenner, "Distributed Security: A New Model of Law Enforcement", **Journal of Internet Law**, c.8, s.5 (2004): 10.
[231] Ajmal Edappagath, "Cyber Law and Enforcements to Optimize Benefits of ICT", **I-Ways**, No. 3/4 (2004): 171.
[232] Dorothy E. Denning, "Activism, Hactivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", https://www.nautilius.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/ [26.01.2018].
[233] Hakan Hekim ve Oğuzhan Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", **Ulusal Güvenlik ve Terörizm Dergisi**, c.4, s.2 (2013): 143.
[234] Aleksandar Lazarevic, Vipin Kumar ve Jaideep Srivastava, "Intrusion Detectıon: A Survey, Managing Cyber Threats: Issues, Approaches and Challenges", **Springer Science and Business Media**, c.5 (2005): 20.
[235] Joseph S.Nye, **age**, 9.
[236] Mustafa Meral, "Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi" (Yüksek Lisans Tezi, Kara Harp Akademileri Stratejik Araştırmalar Enstitüsü, 2015), 13.
[237] Faruk Aydın, "Cyber Security In National Protection Of Turkey" (Yüksek Lisans Tezi, Çankaya Üniversitesi Fen Bilimleri Enstitüsü, 2012), 43.
[238] Mahzure Kara, **age**, 1.

geçiren kişi ya da gruplar artık birer siber savaşçı olarak devlet adına da çalıştırılmaktadır. Devletlerarası siber saldırıların kanunlarca önlenmeye çalışılması, pasif savunma tedbirleri kapsamında değerlendirilecek bir yöntem olsa da, gündeme yansıyanların yanında birçok siber saldırı, devlet eliyle konuda uzman birimlere yaptırılmaya devam edilmektedir[239].

### 3.3.2. Siber Tehditlerin Boyutları ve Etkileri

Bugün dünyada, bir diğer ülkenin büyük çaplı tehdidi altında bulunan çok az ülke bulunmaktadır. Terörizmin değişme ve gelişmesinin sebeplerinden birisi de budur. Özellikle bilgisayar sistemleri ve alt yapıya yönelik saldırılarla desteklenen konvansiyonel terörizm ve düşük yoğunluklu çatışmaların; hayati ulaştırma, bilgi ve haberleşme sistemlerinde ciddi hasarlara sebep olabildiği görülmektedir. 11 Eylül'den önce siber uzayın riskleri ve güvenlik sorunları sadece küçük uzman gruplarında tartışılan konular olsa da o tarihten ve ilerleyen zamanlardaki yaşanan büyük çaptaki küresel örneklerine tecrübe edilmesinden itibaren giderek birbirine bağımlı hale gelen toplumlar açısından siber dünyanın ciddi riskler yarattığı açıkça anlaşılmıştır. Çünkü siber tehdit yöntemleri her ne kadar sanal da olsa zararları gerçektir[240]. Tarihteki siber saldırı örneklerine bakılacak olursa, yarının teröristinin klavye ile bir bombadan daha yıkıcı zararlar verebileceğini söylemek mümkündür[241]. Dolayısıyla asimetrik tehditlerin, doğasında bulunan "güç dengesizliği" ile onun bir uzantısı olan siber tehditlerin getirdiği "bilinmezlik" faktörüyle birlikte gitgide derin[242] ve ürkütücü bir hal aldığını söylemek hiç de zor olmayacaktır.

Siber tehditler terörizmin yeni yüzü olarak tanımlanırken, bu aracın terör örgütleri tarafından kullanılması sonucunda ortaya çıkabilecek neticelerden bazılarını da şu şekilde sıralamak mümkündür: Buna göre siber saldırı yöntemini kullanan teröristlerin, elektronik bir saldırı yaparak bir barajın kapaklarını açabilecekleri, ordunun haberleşmesine girip yanıltıcı bilgiler bırakabilecekleri, kentin bütün trafik ışıklarını durdurabilecekleri, telefonları felç edebilecekleri, elektrik ve doğalgazı kapatabilecekleri, bilgisayar sistemlerini karmakarışık hale getirebilecekleri, ulaşım ve su sistemlerini allak bullak edebilecekleri, bankacılık ve

[239] Muzaffer Ünsaldı, **age**, 40.
[240] Mehmet Kabakoğlu, Fahri Koçuk ve Engin Vardar, **Siber Güvenlik El Kitabı** (Ankara: J.Gen.K.lığı MEBS Bşk.lığı, 2016), 61.
[241] Kara Harp Akademileri, **Asimetrik Harp Yardımcı Yayını** (İstanbul: Harp Akademileri Basımevi, 2002), 9-10.
[242] Vincent Wei-Cheng Wang ve Gwendolyn Stamper, "Asymmetric War? Implications For China's Information Warfare Strategies", **American Asian Review**, c.20, s.4 (2002): 167-207.

finans sektörünü çökertebilecekleri, acil yardım, polis, hastaneler ve itfaiyelerin çalışmasını engelleyebilecekleri, hükümet kurumlarını alt üst edebilecekleri, sistemin birden durmasına neden olabilecekleri ihtimaller dahilindedir[243].

Siber tehditlerlere değindikten sonra siber saldırı kavramının da belirtilmesi önemlidir. Siber saldırı, adından da anlaşılacağı üzere siber uzayın imkanlarını kullanarak düzenlenen bir saldırı türüdür. Özellike son 15 yıldaki tecrübeler ışığında; konvansiyonel bir silah olarak sayılmasa da siber saldırıların sonuçlarının çok ciddi can ve mal kaybına yol açabilme potansiyeli taşıdığı söylenebilir. Siber saldırıların askeri bir kavram olarak tanımı ise ABD Genelkurmayı tarafından şu şekilde yapılmıştır: "Bilgisayar, ilgili ağ ya da sistemleri kullanarak karşı tarafın kritik siber altyapılarını, varlıklarını ya da işlevlerini bozmak ve/veya imha etmek amacı taşıyan düşmanca eylemdir." [244]

Siber saldırının arzulanan etkileri sadece hedeflenen bilgisayar sistemleri veya verilerle sınırlı değildir; komuta-kontrol yeterliliği ya da altyapının bozulmuş olması ya da imha edilmesi amacıyla da bilgisayar sistemlerine saldırılabilir. Siber tehditler; çevresel cihazlar, elektronik vericiler, gömülü kodlar ya da canlı operatörler gibi ara dağıtım araçlarını kullanabilirler. Bir siber saldırının aktivasyonu ya da etkileri, zamansal ya da coğrafi olarak saldırının oluşmasından uzak olabilir[245].

Tarih boyunca farklı örnekleri bulunsa da siber saldırıların ulaşabileceği boyutlar konusunda küresel manadaki en çarpıcı örneklerden ilki, 2007 yılında Estonya'nın finans merkezlerini, bankalarını, parlamentosunu, bakanlıklarını, medya kuruluşlarını, güvenlik ve ulaşım alt yapısını hedef alan saldırılardır. 19 gün süren söz konusu saldırılar ile ilk kez bir devletin hem kamu hem de özel sektör kuruluşları sistematik bir saldırıya maruz kalmış, Estonya'nın ülke dışında bilgi göndermesi engellenmiş, çok ciddi ekonomik zarara sebep olmuş, hayat felce uğratılmış ve devlet otoritesi ciddi şekilde sarsılmıştır[246]. Saldırıların Rusya kaynaklı olduğu bilinmesine ve bazı uzmanların saldırının boyutları sebebiyle olayın arkasında Rus hükümetinin olduğunu tahmin etmelerine rağmen[247] siber tehditlere yönelik kimlik

---

[243] Sedat Sertoğlu,"Büyük Tehlike", **Sabah Gazetesi**, 6 Aralık 1999, https://arsiv.sabah.com.tr./1999/12/06/y11.html [20.01.2017].

[244] Bleda Kurtdarcan ve Özgür Mumcu, **Geleceğin Savaşları ve Silahları** (Ankara, Uğur Mumcu Araştırmacı Gazetecilik Vakfı Yayınları, 2014), 169.

[245] James E.Cartright, "Joint Terminology For The Cyber Space Operations", Memorandum For Chiefs Of The Military Services Of The Combatting Commands Of The Directions Of The Joint Staff Directorates, 2011, 5.

[246] Eneken Tıkk, Kadri Kaska ve Liis Vihul, "International Cyber Incidents: Legal Considerations", Cooperative Cyber Defence of Excellence (CCD COE)/Estonia, 2010, 107.

[247] The Economist, "Cyber Warfare: Newly Nasty", http://www.economist.com/node/9228757 [22.01.2018].

tespitinin mevcut verilerle imkânsıza yakın olması nedeniyle sorumlunun Rusya olarak ispatı hiçbir zaman mümkün kılınamamıştır[248].

Dünya kamuoyun siber tehditler konusundaki bir sonraki tecrübesi Rusya-Gürcistan savaşıdır. Siber dünya bu kez de Rusya-Gürcistan çatışmalarının önemli bir cephesi haline gelmiş, finans, medya ve siyasi alanda yayın yapan pek çok Gürcü, Güney Osetya ve Azeri internet sitelerine siber saldırılar yapılmıştır[249]. Dış dünyayla bağlantısı tamamen kesilen Gürcistan, dışarıya eposta bile gönderememiştir. Bu olay tarihte ilk defa silahlı bir çatışmanın siber saldırılarla desteklenmesi şeklinde yorumlanmıştır[250]. Yine Estonya örneğinde yaşandığı gibi, sorumlunun Rusya olduğu bilinse de somut olarak hiçbir zaman ispat olanağı bulunamamıştır.

Söz konusu Estonya ve Gürcistan örnekleri incelendiğinde; olayın sadece siber saldırı yöntemlerini kullanarak hedef ülkelere çok ciddi zarar verme amacı gütmediği, aynı zamanda mevcut veya yeni geliştirilen siber silahların, araçların imkân ve kabiliyetlerinin test edilmesi ve etkilerinin görülmesi olduğundan da bahsedilmektedir. Dolayısıyla Estonya ve Gürcistan'ın, her ne kadar kimliği ispat edilememiş olsa da Rusya'nın siber yeteneklerini denemek için mükemmel birer deneme bölgeleri[251] olduğunu söylemek olasılık dahilindedir.

Siber tehditlerinin boyutlarının artık iyice tüm dünya çapında anlaşılmasını sağlayan daha yakın tarihli olay ise, 2010 yılındaki İran'ın uranyum zenginleştirme programına yönelik gerçekleştirilen siber saldırılardır. Adını artık herkesin ezbere bildiği "Stuxnet" virüsü, çalıştırıldığı anda kendisini aktive ederek komple bilgisayar ağına zarar verme özelliği taşıyan[252] ciddi bir siber tehdit silahıdır. Söz konusu virüs, bulaştığı andan itibaren sistemin işleyişini tamamen düzen dışı uygulamalar vasıtasıyla olağan ilerleyişini sekteye uğratmış ve sistemi kullanılamaz hale getirmiştir. Daha önceki olaylarda da görüldüğü üzere; perde arkasındaki aktörlere yönelik ciddi tahminler mevcut olmasına rağmen somut bir kaynağa ulaşılamamıştır.

Siber saldırılara ilişkin dünya kamuoyunu ciddi şekilde meşgul eden küresel olayların haricinde, gerek dünya genelinde gerekse ülkemizde basına yansıyan ve söz konusu saldırıların boyutları ve etkilerinin somut olarak anlatıldığı diğer siber

---

[248] Bleda Kurtdarcan ve Özgür Mumcu, **age**, 162.
[249] Eneken Tıkk, Kadri Kaska ve Liis Vihul, **age**, 109.
[250] Lesley Swanson, **age**, 304.
[251] Mustafa Alkan, "Siber Güvenlik ve Siber Savaşlar", Bilgi Güvenliği Derneği, 2012, https://www.tbmm.gov.tr/arastirma_komisyonlari/bilisim_internet/docs/sunumlar/BILGI%20GUVENLIGI%20DERNEGI/09_05%20-%20Bilgi%20/Guvenligi%20Dernegi.pptx [23.01.2018].
[252] Jeremy Richmond, "Evolving Battlefields: Does Stuxnet Demonstrates A Need For Modifications To The Law Of Armed Conflict", **Fordham Journal of International Law**, c.35, s.3 (2012): 850-852.

saldırı olaylarının, özellikle 2016-2017 yıllarını kapsayan güncel haline aşağıdaki örneklerle yer vermek mümkündür:

- Kuzey Kore'nin, Güney Kore'de 160 şirket ve resmi kurumun internet ağlarına girerek, 140.000 bilgisayara siber saldırı düzenlediği, saldırı sonucunda ele geçirilen bilgisayarlardan aralarında askeri belgelerin de bulunduğu 42.000 dokümanın silindiği belirtilmiştir[253].

- Terör örgütü DEAŞ'ın özellikle son yıllarda cihad çağrısı yapmak, örgüte üye toplamak, propaganda ve psikolojik etki yaratmak maksadıyla medya araçlarını ve dolayısıyla interneti son derece aktif olarak kullandığı bilinmektedir. Bu faaliyetler kapsamda söz konusu terör örgütü, tehdit ve gözdağı amacıyla 2015 yılında 100'den fazla Amerikan askerini fotoğraf ve kişisel bilgileriyle birlikte internete sızdırmış[254], bu nedenle ABD Siber Komutanlığının varlığı ve görevlerinin bile sorgulanır hale gelmesine neden olmuştur.

- Son dönemde artan ve coğrafi mesafe tanımayan siber saldırılardan Avusturalya da etkilenmiştir. Ülkenin kan haritası siber korsanlar tarafından ele geçirilmiştir. 1,3 milyon kan donörüne ait kayıtların internette yayımlandığı bu dosyanın boyutunun 1.74 GB olduğu ve donörlere ait kişisel verileri de içerdiği belirtilmiştir[255].

- ABD'nin 9 adet birleşik komutanlığından biri olan ve sorumluluk sahasında Ortadoğu ile Orta Asya'daki 20 ülkenin bulunduğu CENTCOM olarak isimlendirilen Merkez Kuvvetler K.lığının Twitter ve YouTube hesaplarının 12 Ocak 2015 tarihinde bilgisayar korsanlarınca ele geçirildiği bilgisi edinilmiştir[256].

- İngiltere'nin önde gelen banklarından Tesco Bank'tan yapılan açıklamada hackerların bankanın yaklaşık 20 bin müşterisinin hesaplarına girilerek para sızdırdığı bildirilmiştir[257].

- Alman Telekom devi Deutsche Telekom, internet, telefon ve televizyon abonelerinin siber saldırıya uğradığını açıkladığı olaya ilişkin internet abonelerine düzenlenen saldırıda 900 bin abonenin internet erişiminin kesildiği ifade edilmiştir[258].

- Yakın geçmişte önemli bir hacker saldırısına uğrayan kariyer sosyal ağı LinkedIn, 550 bin kullanıcısının şifrelerinin çalınmasına kadar varan bir siber

---

[253] www.trthaber.com/m/?news=kuzey-koreden-guney-koreye-sibersaldiri&news_id=255988&category_id=4 [15.06.2016].
[254] https://siberbulten/uluslararasi-iliskiler/abd-iside-karsi-siber-savas-ilan-etti/ [24.04.2016].
[255] https://www.btgunlugu.com/avusturalya-nin-kan-haritasi-calindi [29.01.2018].
[256] http://www.mynet.com/haber/guncel/centcomun-sosyal-medya-hesaplari-hacklendi-1655161 [29.01.2018].
[257] http://www.eurovizyon.co.uk/ekonomi/ingiliz-bankasinin-20-bin-musterisinin-hesabi-hacklendi-h47119.html [29.01.2018].
[258] http://tr.euronews.com/2016/11/29/deutsche-telekom-a-siber-saldiri-korkusu [29.01.2018].

saldırıya daha maruz kalmıştır. LinkedIn üzerinde online eğitimler vermesi için satın alınan Lynda.com'da ki bir açığı kullanan hackerların 550 bin kişinin bilgilerine ulaştığı açıklanmıştır[259].

- Güney Kore ve ABD'nin savaş planlarının yer aldığı 265 gigabyte'lık gizli askeri belgelerin Kuzey Koreli bilgisayar korsanları tarafından 2016 yılı içerisinde çalındığını belirtilmektedir[260].

- Son dönemlerde adından sıkça bahsedilen Anonymous siber korsan grubunun, Türkiye'ye yönelik "#opTurkey" adındaki operasyonun devam eden faaliyetlerinin son olarak siber saldırı yaptığı şirket İzmir Gaz olmuştur. İzmir'deki doğal gaz dağıtım ve tedarikini sağlayan İzmir Gaz İnternet sitesi, Temmuz 2016 ayının ikinci yarısındaki siber saldırı nedeniyle erişime kapatılarak bir süreliğine servis dışı bırakılmıştır[261].

- Eylül 2016 ayının sonlarına doğru, Yahoo tarafından yapılan açıklamada; 2014 yılında veri merkezlerine yapılan siber saldırı neticesinde, en az 500 milyon kullanıcının kimlik bilgileri, eposta adresi, telefon numarası ve hesap doğrulamak için gereken güvenlik soru ve cevaplarının bulunduğu verinin çalındığı belirtilmiştir[262]. Söz konusu çalındığı ifade edilen 500 milyon kişiye ait verinin şimdiye kadar gerçeşleştirilmiş en ciddi siber hırsızlıklardan birisi olduğu değerlendirilmektedir.

- 2016 yılında gerçekleşen en büyük siber saldırılardan biri de Bangladeş'te gerçekleşmiştir. Siber saldırılar sonrası Bangladeş Merkez Bankası soyulmuş, söz konusu saldırıya ilişkin yapılan açıklamalara göre saldırganlar başarılı bir şekilde savunma önlemlerini atlatarak 1 milyar doları hesaplarına aktarmışlardır. Saldırılar sonrasında banka yetkilileri yoğun bir çaba sarf etmelerine rağmen çalınan paranın 81 milyon doları hala kurtarılamamıştır[263].

- Enerji ve Tabii Kaynaklar Bakanı Berat ALBAYRAK, katıldığı bir televizyon programında 2017 yılının başında ülke çapında yaşanan ciddi elektrik kesintisinin sebebi olarak Amerika merkezli bir siber saldırıyı işaret etmiş ve birçok açıdan tedbirli olunmasının zorunlu olduğunu ifade etmiştir[264].

- Merkezi Rusya'da bulunan siber güvenlik ve Anti-Virüs yazılımı sağlayıcısı Kaspersky Lab'ın üst düzey yöneticisi Eugene Kaspersky; "Siber saldırıların

---

[259] http://www.hurriyet.com.tr/teknoloji/linkedin-hesaplari-yine-calindi-40310869 [29.01.2018].
[260] https://tr.sputniknews.com/asya/201712211031491296-kuzey-kore-abd-siber-saldiri-alakamiz-yok [29.01.2018].
[261] Savunma Teknolojileri Mühendislik ve Ticaret A.Ş., "İzmir Gaz'a Anonymous Saldırısı", 2016 Temmuz-Eylül Dönemi Siber Tehdit Durum Raporu, 6.
[262] STM, **age**, 7.
[263] http://www.ajansbt.com/2016-nin-en-buyuk-banka-soygunu.html [29.01.2018].
[264] http://www.gazetevatan.com/elektrik-hatlarina-sabotaj-var-mi-bakan-albayrak-yanitladi-1025710-gundem [29.01.2018].

büyüyen küresel bir tehdit haline dönüştüğünü ve bu alanda işlenen suçların dünya ekonomisine yıllık zararının 400 ile 500 milyar doları bulduğunu" belirtmiştir[265].

- Avusturya'da yayımlanan bir haberde, Parlemento'nun web sitesinin bir Hizmet Dışı Bırakma Saldırısı (DDoS) sonucu 20 dakika 7 boyunca erişilemez hale geldiği, siber saldırının Parlemento'da tartışılmakta olan kamusal alanda örtünme yasağına tepki olarak gerçekleştirildiği belirtilmiştir[266].

- İstanbul Siber Suçlarla Mücadele ekiplerinin, 0850'li VOIP (İnternet Üzerinden Sesli Görüşme) hatları üzerinden çok sayıda kişiyi çeşitli bankaların temsilcisi gibi arayıp dolandırdığı belirlenen şebekeye yönelik düzenlediği operasyonda, gözaltına alınan şüphelilerin bilgisayarında Türkiye genelinde 20 milyon kişinin kimlik ve banka hesap bilgilerinin bulunduğu ortaya çıkarılmıştır[267].

- Fortinet isimli firmanın siber suç dünyasındaki fiyatlarına yönelik yaptığı araştırmaya göre; kullanıcıların kredi kartı numaraları 0.50 dolara, PIN numaralı kredi kartları 2.5 dolara, e-posta hesapları 0.0003 dolara, banka hesap bilgileri 10 dolara, tıbbî kayıtlarının ise 10 ila 20 dolar arasında satışa çıkarıldığı belirtilmiştir[268].

- İranlı hackerların, aralarında Türkiye'nin de bulunduğu 16 ülkeye siber saldırı düzenlediği öğrenilmiştir. California merkezli güvenlik firması Cylance tarafından iki yıldır yapılan sanal takibe göre İran, 16 ülkede kritik öneme sahip enerji, ulaşım ve sağlık servislerinin de içinde olduğu 50 noktaya siber saldırı yapan. İranlı hackerların; Türkiye, ABD, Kanada, İsrail, Hindistan, Katar, Kuveyt, Meksika, Pakistan, Suudi Arabistan, Birleşik Arap Emirlikleri, Fransa, İngiltere, Çin ve Güney Kore'ye karşı siber saldırı düzenleyerek devletlerin gizli bilgilerini ele geçirmeye çalıştığı belirtilmiştir[269].

- Fidye yazılım (Ransomware) tehdidi neticesinde; 17 yaşında, otizmli ve İngiltere'de bir öğrenci olan Joseph Edwards, kendisinin polis olduğunu ve yasa dışı siteye giriş yaptığının tespit edildiğini ve bu yüzden 100 pound ceza kesildiğini, cezanın ödenmesi durumunda takibin bırakılacağını söyleyen sahte bir e-posta aldıktan sonra kendini asmıştır[270].

---

[265] http://www.bloomberght.com/haberler/haber/1983567-siber-suclarin-yillik-zarari-400-500-milyar-dolar [29.01.2018].

[266] https://tr.sputniknews.com/avrupa/201702071027104234-turk-hackerlar-avusturya-parlamentosunun-sitesine-saldirdi [29.01.2018].

[267] https://www.haberler.com/20-milyon-kisinin-kimlik-ve-banka-hesap-bilgileri-9546131-haberi [29.01.2018].

[268] http://digitalage.com.tr/arastirma-kisisel-bilgileriniz-siber-dunyada-ne-kadara-satiliyor [30.01.2018].

[269] http://www.hurriyet.com.tr/dunya/iranli-hackerlardan-turkiyeye-siber-saldiri-27709465 [30.01.2018].

[270] http://thehackernews.com/2015/01/police-ransomware-suicide.htm [30.01.2018].

- ABD'de bir güvenlik araştırmacısının, Nisan ayında bindiği bir yolcu uçağının kabin içi eğlence sistemini kullanarak uçağın elektronik sistemine girdiği ve uçuş esnasında uçağın rotasını değiştirmeyi başardığını bildirmiştir[271].

- 25 yaşında bir İngiliz vatandaşının, Amerikan ordusuna ait iletişim uydusundan 800 kullanıcıya ait verileri yasa dışı yollardan ele geçirdiği, İngiltere Ulusal Siber Suçlar Ajansı (NCA) tarafından duyurulmuştur[272].

- IBM Türk Güvenlik birimleri tarafından yapılan açıklamada; siber saldırıların dünyadaki maliyetinin 2.1 trilyon doları bulabileceği, artık internet üzerinden siber saldırılar üzerinden her şeye ulaşılabildiği, akıllı televizyonlardan, arabalara hatta buzdolaplarına kadar her alanda siber saldırıya maruz kalınabilecek bir döneme girildiği ifade edilmiştir[273].

- Ortadoğu'daki bir enerji santralini hedef alan siber korsanların, Triton isimli zararlı bir yazılım ile tesisin çalışmalarını durdurduğu, söz konusu saldırının endüstriyel güvenlik sistemlerine nasıl zarar verileceğini öğrenme amaçlı olduğu ve ilerde daha büyük bir saldırı başlatmak için kullanılacağı ifade edilmiştir[274].

Özellikle son yılları kapsayan süreçte çoğunluğu basında yer alan haberlerin kamuoyuna yansıması şeklinde cereyan eden siber saldırılar incelendiğinde; siber tehditlerin hedefleri, yöntemleri konusunda şimdiye kadar anlatılan hususların tamamına yakınını doğrular nitelikte örnekler göze çarpmaktadır. Hedef olarak belirlenen alanlar çoğunlukla; savunma sanayisinden, üretim sektörüne, sağlık sektöründen, finans, ulaşım ve haberleşme alanlarını içine alan kritik altyapılara yönelik olmakta ve belirlenen hedefin teknolojik, askeri ve ekonomik gücü ne olursa olsun ciddi kayıplara yol açabildiği yaşanan örneklerle görülmektedir. Bu açıklamaları destekler nitelikte, ABD Hava Kuvvetlerinden Tümgeneral William BENDERE'nin "Endüstri Çağının en güçlü hava kuvvetleri bizdik, ancak şu an Bilgi Çağındayız"[275] şeklindeki ifadeleri, Süper Güç olarak kabul edilen Amerika'nın bile çağın fenomen tehditleri ve saldırılarına karşı gücün pek bir anlam ifade etmediğini doğrulamaktadır.

Nedeni ne olursa olsun, siber saldırılar birçok zorluğu da beraberinde getirmektedir. Neredeyse hiçbir sanal kaynağı olmayan anonim ve izi sürülemez bir bireyin bile, hükümetin veya kurumun önemli operasyonlarını tehdit ederek

---

[271] http://www.gazetevatan.com/yolcu-ucagina-siber-saldiri-791885-dunya [30.01.2018].
[272] http://cybertoday.org/index.php/2017/05/18/amerikan-ordusuna-ait [30.01.2018].
[273] http://www.hurriyet.com.tr/ekonomi/siber-saldirilarin-maliyeti-2-1-trilyon-dolar-40486872 [30.01.2018].
[274] http://www.milliyet.com.tr/hackerlar-bir-enerji-santralinin-teknoloji-haber-2575449 [30.01.2018].
[275] Alan Brill'in "Terrorist Use of Cyberspace 2016: Is Digital Disruption The New Normal?" konulu sunumunun yansılarından alınmıştır.

vatandaşların emniyetini ve ekonomik güvenliğini risk altında bırakmasına olanak vermektedir[276]. Muhtemelen, internetin henüz başlangıç aşamasında olduğu ilk yıllarda bilgi sistemlerinde günümüzdeki gibi bu denli geniş ölçekli zararlara sebebiyet veren siber saldırıların olacağı hayal bile edilemezdi[277]. Ancak belirtilen örnekler, tamamen teknolojinin ve yetişmiş beyin gücünün kullanıldığı siber saldırıların tek bir damla kan akıtmadan, düşmana ekonomik, sosyal ve politik olarak ne denli zarar verilebileceğinin yaşanmış bir kanıtıdır[278].

Türkiye'de ve Dünyada ses getiren bu önemli siber saldırı örneklerinin haricinde her geçen gün yeni vakalar yaşanmaktadır. Nasıl ki deprem bölgesinde yer alan bir ülke için depremler günlük hayatın bir parçası haline geliyor ve etkilenmemek için gerekli tedbirler alınıyorsa, günlük hayatımızın bir vazgeçilmezi olan bilişim çağında da özellikle internete yönelik tehdit ve saldırılara sürekli hazır olunmalı ve bunlarla yaşama gerçeği kabul edilmelidir. Önemli olan bu tür saldırılardan zarar görmeden veya minimum zararla kurtulmak ve benzerlerine karşı gerekli tedbirleri süratle almaktır[279].

Siber tehditler bilişim teknolojilerinin kullanımının yaygınlaşması ile birlikte artarak devam etmekte ve siber saldırıların, geleneksel savaşlardan çok daha büyük sonuçlar doğurabileceği değerlendirilmektedir. Bu kapsamda siber tehditlere yönelik, siber uzaya bağımlılığı olan bütün birey veya devletlerin birer hedef olabileceğini söylemek mümkündür. Siber tehditlere ilişkin yakın geleceğe yönelik tahmin yapmak olasılık dahilinde olsa bile, siber uzaydaki değişimin hızı göz önünde bulundurulduğunda, devletlerin siber saldırılara karşı tam bir hazırlıkla ve anında reaksiyon göstermeleri şu an için çok da muhtemel gözükmemektedir[280]. Ancak yine de muhtemel siber saldırılara yönelik alınması gereken tedbirlerin, günümüzün ve geleceğin savunma anlayışlarına dahil edilmesinin, verilebilecek zararı minimuma indirmesi açısından hayati önem taşıdığı aşikardır.

---

[276] Tyson Storch, "Siber Güvenlik: Güvenli ve Bağlantılı Bir Toplumun Temel Taşı", Microsoft Corporations, 2012, 6.
[277] Murat Güngör, "Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma", T.C. Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı, Yayın No: 2919, 2015, 37.
[278] Gökhan Astan, **age**, 1.
[279] Adem Kaya, "Siber Güvenliğin Milli Güvenlik Açısından Önemi" (Yüksek Lisans Tezi, Kara Harp Okulu Savunma Bilimleri Enstitüsü, 2012), 60.
[280] P.Ewing, "The Cyber War After Next", https://www.military.com/dodbuzz/2012/03/22/the-cyber-war-after-next/amp [25.01.2018].

### 3.3.3. Güncel Verilerle Siber Tehditler

#### 3.3.3.1. Küresel Siber Tehdit Verileri

Teknolojiye ve internete olan bağımlılığın devasa boyutlara ulaştığı günümüzde, siber tehditler de sürekli artan bir ivmeyle seyretmekte ve sanal ortamdaki varlıklarımızı tehlikeye atmaktadır[281]. Dolayısıyla internet artık yönetilebilir olmaktan çıkmış, mücadele edilmesi zorunlu bir tehdit haline gelmiştir[282].

Bir ülke ne kadar gelişmiş ve teknolojik olarak ne kadar üstün durumdaysa o kadar siber tehdit altındadır[283]. Dolayısıyla siber tehditlere karşı "en iyi savunma" diye bir kavram yoktur. Aksine salgırganlar, özellikle en kuvvetli olduğu zannedilen, en çok ses getirecek ve zarar verecek noktaları kendilerine hedef seçmektedirler. Bu nedenle teknolojik anlamda güçlü olan devletlerin, bilişim sistemlerine bağlılıkları sebebiyle saldırıya daha açık olmaları ve daha fazla saldırıya uğramaları normal sayılmaktadır[284].

Siber tehditlerin gerçekleştirdiği siber saldırıların ne kadar ciddi boyutlara ulaşabileceği bundan önceki bölümde olarak anlatılmaya çalışılmıştır. Bu bölümde ise hem dünya genelindeki hem de Türkiye özelinde, daha çok tablo ve grafiklerle siber tehditlere ilişkin mümkün olduğunca güncel verilerle durum sayısal olarak açıklanmaya çalışılacaktır.

İnternet ve bilişim sistemlerinin getirdikleri şüphe götürmez kolaylıkların yanı sıra; kötü niyetli kişi ve gruplar ile bilinçsiz kullanıcıların hedefi olabileceği artık şüphe götürmez bir gerçektir. Konuya ilişkin güncel internet kullanım durumunun; internete olan bağımlılık, tehdit tarafından bakıldığında ise hedef kitlenin belirlenmesi açısından önemli olduğu değerlendirilmektedir. 30 Haziran 2017 tarihli internet kullanıcı sayılarının dünya nüfusu ve bölgelere göre dağılımının verildiği Tablo 7'de de belirtildiği üzere, artık dünya nüfusunun yarısından fazlası bir şekilde siber uzaya dahil olmuştur.

---

[281] Ahmet Küçük ve İbrahim Soğukpınar, “Siber Saldırılar ve Farkındalık Eğitimi İçin Bir Öneri”, cigicigi.com/CA.pdf [25.01.2018].

[282] Hilmi Özkök, "İnternet Silah Gibi", **Milliyet Gazetesi**, http://gazetearsivi.milliyet.com.tr/GununYayinlari/3cfulzH3qW3lu4zf6V4_x2B_5w_x3D_x3D_ [26.01.2018].

[283] Dan Verton, **Black Ice, The Invisible Threat of Cyber-Terrorism** (New York: McGraw-Hill, 2003), 203.

[284] Şeyda Türkay, “Siber Savaş Hukuku ve Uygulanma Sorunsalı”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, c.71, s.1 (2013): 1217.

**Tablo 7: İnternet Kullanım İstatistikleri**

| Bölgeler | Tahmini Nüfus | Dünya Nüfusuna Oranı | İnternet Kullanıcı Sayısı | Nüfusa Oranı |
|---|---|---|---|---|
| **Africa** | 1.246.504.865 | % 16.6 | 388.376.491 | % 31.2 |
| **Asya** | 4.148.177.672 | % 55.2 | 1.938.075.631 | % 46.7 |
| **Avrupa** | 822.710.362 | % 10.9 | 659.634.487 | % 80.2 |
| **Güney Amerika** | 647.604.645 | % 8.6 | 404.269.163 | % 62.4 |
| **Kuzey Amerika** | 363.224.006 | % 4.8 | 320.059.368 | % 88.1 |
| **Orta Doğu** | 250.327.574 | % 3.3 | 146.972.123 | % 58.7 |
| **Avustralya** | 40.479.846 | % 0.5 | 28.180.356 | % 69.6 |
| **TOPLAM** | 7.529.028.970 | % 100 | 3.885.567.619 | ***% 51.7*** |

"Internet Usage Statistics: The Internet Big Picture", http://www.internetworldstats.com/stats.htm [25.01.2018].

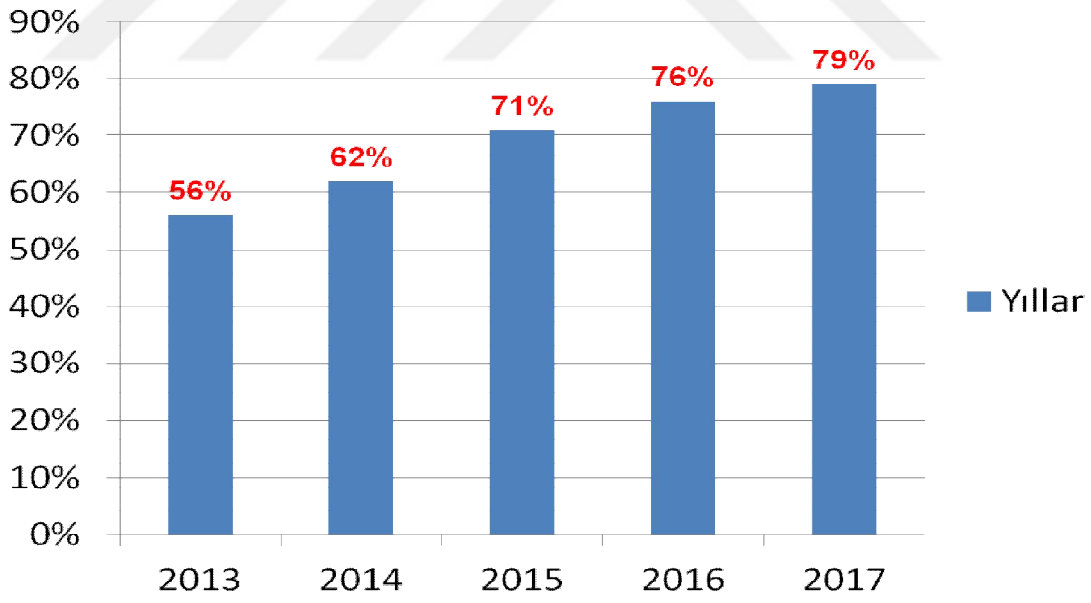
2012 yılından beri en büyük internet kullanıcı artışının gerçekleştiği ülkeler sırasıyla; Kamerun, Pakistan, Guatemala ve Cezayir olmuştur. Mevcut durumdaki internet kullanıcı sayısının, 2025 yılı için beklenen karşılığının ise 4.7 milyar civarında olacağı tahmin edilmektedir[285]. Belirtilen sayısal değerler kullanıcı bazında verilerdir. Bunun haricinde araştırma kuruluşu Gartner analistlerine göre "nesnelerin interneti" kapsamı da dahil olmak üzere internete dahil olan cihaz sayısının dünya genelinde 2018 itibarıyla 11.2 milyar, 2020'de ise 20.4 milyar olacağının öngörülmesi[286], siber uzayın insanlık için artık neredeyse su kadar vazgeçilmez ve hayati bir öğe haline geldiği değerlendirilmektedir.

Siber uzaya dahil olan kullanıcı sayısındaki yoğunluk siber tehditler için de bir nevi o kadar sayıda hedef anlamına gelmektedir. Yapılan çalışmalar neticesinde çeşitli siber güvenlik firmaları tarafından 2016 yılında yayınlanan küresel siber güvenlik raporlarında belirtildiği üzere; test edilen web uygulamalarının % 98'i siber saldırılara karşı zayıf durumda bulunmaktadır. Ayrıca büyük ölçekli şirketlerin % 90'ı, küçük ölçekli şirketlerde ise % 74'ünde yıl içerisinde en az bir defa da olsa güvenlik ihlali, zaafiyeti yaşandığı ve bunun bir önceki yıla göre % 81'lik bir artışa karşılık geldiği, siber saldırıların ticaret sektöründeki başarı oranının da bir önceki yıla nazaran % 144'lük bir artışla yoluna devam ettiği belirtilmektedir[287].

[285] David Burt ve diğ., **age**, 6.
[286] https://www.gartner.com/newsroom/id/3598917 [07.02.2018].
[287] Nazife Baykal'ın "Conceptual Perspective at Terrorist Use of Cyberspace" konulu sunumunun yansılarından alınmıştır.

Siber saldırıların, finansal kazançların daha çok olduğu alana yönelmesi tesadüf değildir. Önem derecesine göre, sistemlerin zayıf yanlarından faydalanılarak yapılan siber saldırıların kişisel ve kurumsal manada zararları ve ekonomik olarak maliyetlerinin her yıl katlanarak devam edeceği öngörülmektedir. 2017 yılında icra edilen Türkiye'de SOME'ler ve Siber Güvenlikte Yerli Milli Çözümler konulu seminerde; siber saldırıya uğrayan kişi sayısının toplam kullanıcı sayısının % 51'ini oluşturduğu ve siber saldırıların dünya genelindeki maliyetinin 2016 yılında 400 milyar doları aştığının[288] belirtilmesi ve 2020 itibarıyla da toplamda 1 trilyon dolara ulaşacağı öngörüleri[289] bu ifadeleri doğrular niteliktedir.

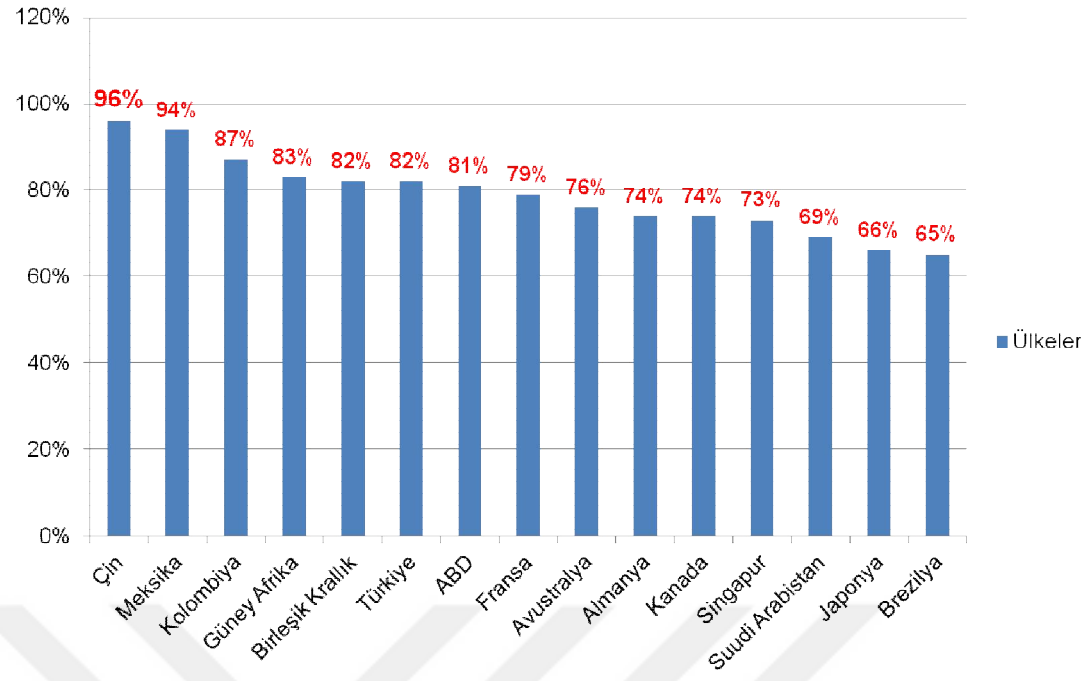
Cyber Edge Group tarafından yayımlanan "2017 Siber Tehdit Savunma Raporu"na göre; dünya çapında 15 ülkeden, 19 farklı alanda, 1.100 bilişim uzmanı tarafından yapılan değerlendirmeler sonucunda siber saldırılara karşı en zayıf olduğu düşünülen cihazlar sırasıyla; mobil cihazlar, dizüstü bilgisayarlar ve masaüstü bilgisayarlar olarak tespit edilmiştir. Siber saldırılara ilişkin söz konusu katılımcıların beyanlarına göre oluşturulan, son 5 yıl içerisinde maruz kalınan siber saldırıların başarı oranları Şekil 5'te, 2017 yılı içerisinde başarıyla sonuçlanan siber saldırılara maruz kalan ülkelerin istatistikleri ise Şekil-6'da verilmiştir.




**Şekil 5: Siber Saldırı Başarı Oranları**

[288] Tayfun Acarer, "Türkiye'de SOME'ler ve Siber Güvenlikte Yerli Milli Çözümler", www.teknokulis.com/haberler/guvenlik/2017/05/09/dunya-nufusunun-yuzde-51i-siber-saldiri-magduru [03.02.2018].

[289] Cybersecurity Ventures, "2017 Cybercrime Report", https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf [03.02.2018].




**Şekil 6: Siber Saldırıya Uğrayan Ülkeler**

Cyber Edge Group, "2017 CyberThreat Defence Report", https://www.sumologic.com/wp-content/uploads/CyberEdge-2017-CDR-2017-Report.pdf, [03.02.2018].

Dünyadaki internet servis sağlayıcıların % 90'ının siber güvenliğini sağlayan Arbor Networks'ün, Kasım 2016 - Ekim 2017 dönemine ilişkin hazırlamış olduğu 13.Yıllık Küresel Altyapı Güvenliği Raporuna göre; belirtilen dönem içerisinde çevrimiçi erişimi engellemeye yönelik 7,5 milyon saldırı kaydedildiği[290] ifade edilmektedir. Söz konusu raporla paralel bir görüşte, tüm dünya genelindeki siber saldırıların anlık olarak, canlı bir şekilde izlenebildiği Kaspersky, Norsecorp ve Threatcloud Intelligence gibi dev siber güvenlik firmalarının gerçek zamanlı siber tehdit haritalarından alınan verilere göre, örnek olarak incelenen bir gün (07 Şubat 2018) boyunca toplam gerçekleşen siber saldırının 8.191.912 olduğu[291] tespit edilmiştir. Söz konusu siber tehdit haritalarındaki veriler, Şekil-6'da belirtilen Türkiye'nin de en çok siber saldırı girişiminde bulununan ülkeler arasında üst sıralarda bulunduğu istatistiklerini doğrular niteliktedir[292].

[290] Arbor Networks, "13th Annual Worldwide Infrastructure Security Report", http://www.arbornetworks.com/report [07.02.2018].
[291] Threatcloud Intelligence, "Live Cyber Attack Threat Map", https://threatmap.checkpoint.com/ThreatPortal/livemap.html [08.02.2018].
[292] map.norsecorp.com/#/ ve https://cybermap.kaspersky.com [07.02.2018].

Günümüz kamuoyunu meşgul eden siber tehditlerin belki de en önemlisi; ilk olarak 2015 yılında ortaya çıkan[293] ve 2016-2017 yıllarında iyice popüler hale gelip, etkilerini tecrübe ettikçe daha her geçen gün kişi ve kurumları siber saldırılar konusunda daha karamsar hale getiren, tüm dünyaya adını WannaCry olarak tanıtan, fidye yazılımlardır. Kısaca bahsedilecek olursa; şifreleme ve kilitleme olmak üzere iki farklı fonksiyonu bulunan bu yazılım, söz konusu kilidi kaldırmak veya şifreyi vermek için fidye talep eden ve sadece yerleştirildiği bilgisayarı değil sisteme dahil olan bütün bilgi sistem araçlarını kullanılamaz, sistemi erişilemez hale getiren, çağın en tehlikeli siber tehditlerinden birisi olarak öne çıkmaktadır. Uzmanlara göre, kendi içerisinde yayılabilen ilk fidye yazılımı olup, şu an için mevcut siber güvenlik tedbirleri ve savunma imkânlarıyla karşı konulması pek mümkün değildir[294].

Fidye yazılımlara ilişkin veriler ve söz konusu tehdidin ulaştığı boyutlar, güvenlik yazılımları firması Kaspersky'nin hem 2016 hem de 2017 güvenlik bültenlerinde oldukça geniş bir şekilde yer almakta ve konunun önemine dikkat çekilmektedir. Bu kapsamda 2016 güvenlik bültenine göre; yılın ilk yarısında dünyanın herhangi yerinde bir kullanıcı her 20 saniyede bir fidye yazılımlara maruz kalırken, aynı yılın Eylül ayı verilerine göre ise bu sürenin 10 saniyeye düştüğü belirtilmektedir. Yine 2016 yılında küçük ve orta ölçekli işletmelerin % 42'si fidye yazılımlara maruz kalmış, bunlar arasından söz konusu fidyeyi ödeyen % 32'lik kesmin % 20'si bir daha hiçbir şekilde verilerine ulaşamamışlardır[295].

Ülke bazında fidye yazılımlarda en çok etkilenen ülkelerin; Rusya, Ukrayna ve Tayvan olarak öne çıktığı Kaspersky 2017 raporunda, firma bazında da; Renault, Alman nakliye devi Deutsche Bahn, İspanyol Telefonica, FedEx, Hitachi, Honda ve hatta Rusya İçişleri Bakanlığının bile söz konusu siber tehdidin popüler kurbanları arasında yer aldığı belirtilmektedir. Raporda dikkat çekici bir diğer husus da, 2020 yılına kadar günümüzdekinin 50 katı daha fazla veriyi siber tehditlerden korumak zorunda olacağımızdır[296]. Söz konusu verilere ilave olarak yine fidye yazılımlara ilişkin, tüketim malzemeleri firması Reckitt Benckiser'ın 2016 yıllık raporunda da; fidye yazılım nedeniyle 15.000 adet dizüstü bilgisayar, 2000 adet sunucu bilgisayar ve 500 adet de masaüstü bilgisayarın toplamda 45 dakika içerisinde tamamen sistem dışı kaldığı ve bu saldırının maliyetinin 300 milyon dolar olduğu[297] ifade

[293] Symantec, "Internet Security Threat Report", Vol.20 (2015): 93.
[294] **"Dikkat WannaCry Siber Saldırısı Tüm Dünyayı Etkisi Altına Aldı"** başlıklı haber, https://www.teknokulis.com/haberler/guvenlik/2017/05/13/dikkat-wannacry-siber-saldirisi-tum-dunyayı-etkisi-altina-aldi/amp [03.02.2018].
[295] Kaspersky Lab, "Kaspersky Cyber Security Bulletin: Story of the Year-2016", 23-24.
[296] Kaspersky Lab, "Kaspersky Cyber Security Bulletin: Story of the Year-2017", 6-13.
[297] Reckitt Benckiser Group, "Annual Report and Financial Statements 2016", https://www.rb.com/media/2473/rb-annual-report-2016-no-spine.pdf [05.02.2018].

edilmektedir. Ancak söz konusu siber saldırıların ekonomik zararından ziyade itibar zedelenmesi konusunda açtığı yaraların artık daha öncelikli hale geldiği ve bu nedenle dışardan siber güvenlik hizmeti alan kuruluşların oranının önceki yıla göre % 10 artmasını beraberinde getirdiği[298] belirtilmektedir.

2017 fidye yazılım raporuna göre; son bir yıl içerisinde, organizasyonların % 75'i 5 veya daha az, geri kalan % 25'lik bölümü ise 6 veya daha fazla fidye yazılım saldırısına maruz kalmışlardır. Konunun uzmanları tarafından oluşan bir örneklem uzayına yapılan ankette; % 79'luk kesim, fidye yazılımlarının ilerleyen dönemde daha da büyüyen bir tehdit haline geleceğini ifade etmişlerdir. Ayrıca yine aynı raporda, saldırı amaçlarının en başında % 86'lık bir oranla maddi kazanç elde etmek olduğunun belirtildiği[299] fidye yazılımlara ilişkin en tehlikeli yanın ise, 2016 türleriyle mukayese edildiğinde 2017 yılında karşılaşılan sayının nerdeyse iki katına çıkarak iyice yaygın hale gelmesi olduğu anlaşılmaktadır. Bu nedenle fidye yazılımların, özellikle finans ve hükümet faaliyetlerine ilişkin en hızlı gelişen siber tehditlerin başında geldiği değerlendirilmektedir.

### 3.3.3.2. Türkiye'ye Ait Siber Tehdit Verileri

Bir önceki bölümde verilen verilerden de anlaşılacağı üzere bilişim teknolojilerinin hızlı gelişimi neticesinde artan internet kullanımının; kişisel ve kurumsal anlamda hayatın vazgeçilmez bir parçası haline geldiği günümüzde, ülkemiz için de durum pek farklı değildir. Türkiye'nin bulunduğu coğrafya, bölgedeki sorunlar ve teknolojinin son süratle ilerlemesi bileşkesinde, fiziksel ortamdaki tehditlere ilave olarak siber tehditlerin de eklendiğini ve söz konusu siber tehditlerin hedefi olan ülkeler arasında üst sıralarda yer aldığımızı söylemek mümkündür.

Emniyet verilerine göre siber tehditlerin varlığına ve faaliyetlerine ilişkin ülkemizde kayıtlara giren ilk siber saldırı vakası, 1990 yılında işlenen 1 adet banka kartı dolandırıcılığıdır[300]. Bu olayla birlikte artan bir ivmeyle devam eden siber saldırılar bireysel hedeflerin yanı sıra kamusal alanlara ve kritik altyapılara yönelmiş ve verdiği zararlar ile potansiyel risk tehdidi açısından günümüzün başlıca ulusal güvenlik problemleri arasında yerini almıştır.

Fortinet firması tarafından Ağustos 2016 tarihinde yayımlanan 2016 ikinci çeyrek siber tehdit analiz raporunda, çeşitli siber tehdit yöntemlerinden (botnet,

---

[298] https://www.google.com.tr/amp/s/m.dunya.com/amp/sektorler/teknoloji/2017de-turkiyede-gunde-475-siber-saldiri-yasandi-haberi-401291 [07.02.2018].
[299] Cybersecurity Insiders, "Ransomware 2017 Report", 3-11.
[300] Ali Can ve Ufuk Taşçı, "Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014", **Fırat Üniversitesi Sosyal Bilimler Dergisi**, c.25, s.2 (2015): 236.

zararlı yazılım ve istismar kiti) etkilendiği tespit edilen ve Tablo 8'de verilen ülke istatistikleri içerisinde Türkiye'nin ilk 5 arasında, Şekil-6'da yer alan başarılı siber saldırıların ülkere göre dağılımlarında ise 6.sırada yer aldığı görülmektedir. Bu durum, siber tehditlere ilişkin problem sahasının ne kadar kritik bir seviyeye geldiğini gözler önüne sermektedir.

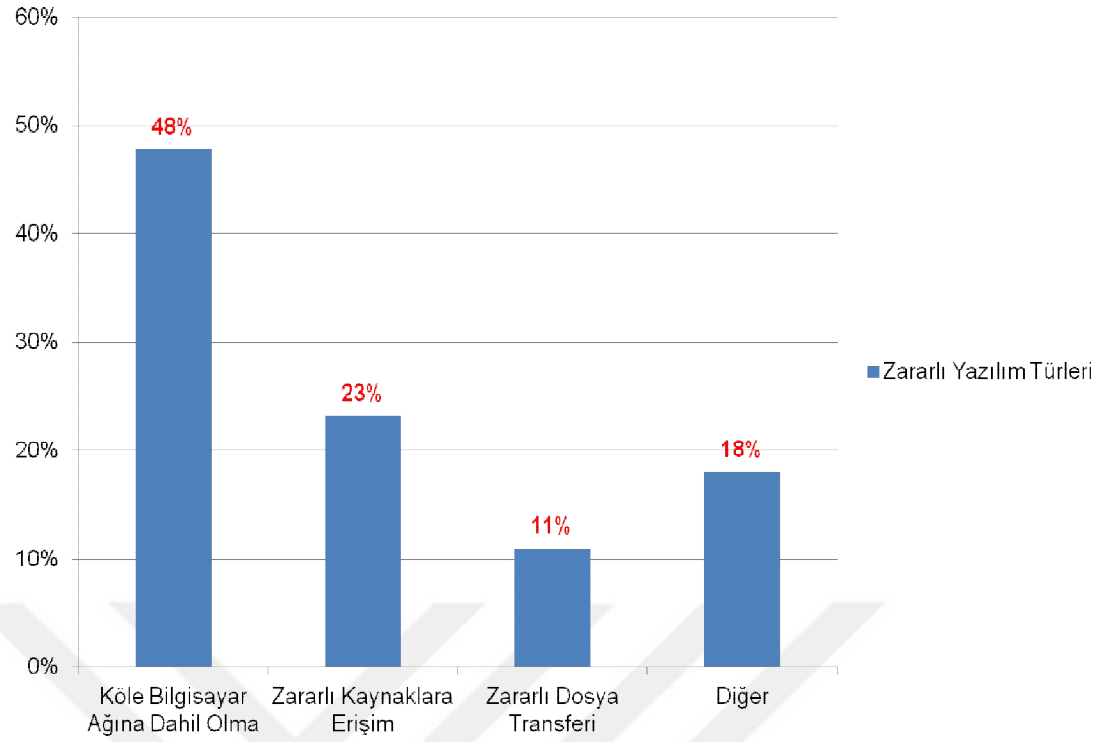
**Tablo 8: Siber Tehditlerin Hedefi Olan Ülkeler Sıralaması**

| Ülkeler | Siber Tehdit Türleri | | |
|---|---|---|---|
| | **Botnet** | **Zararlı Yazılım** | **İstismar Kiti** |
| **ABD** | 1 | 1 | 1 |
| **Japonya** | 2 | 2 | 2 |
| **Tayvan** | 3 | - | 3 |
| **Çin** | 4 | 6 | 4 |
| **Türkiye** | ***5*** | ***4*** | ***5*** |
| **Güney Kore** | 6 | 3 | 6 |
| **Macaristan** | 7 | - | 7 |
| **Kanada** | 8 | - | 8 |
| **Almanya** | 9 | 9 | 9 |
| **İsrail** | 10 | - | 10 |
| **Birleşik Krallık** | - | 5 | - |
| **Avusturya** | - | 7 | - |
| **Meksika** | - | 8 | - |
| **Hindistan** | - | 10 | - |

STM, **age**, 3.

Tablo 8'de Türkiye'nin 4.sırayı aldığı zararlı yazılım türünden siber tehditlere ilişkin Checkpoint firmasının yayımladığı aylık dünya siber tehdit haritasına göre, Aralık 2016-Aralık 2017 tarihlerine ait bulaşıcı zararlı yazılım tiplerinin ortalama değerlerinin büyük çoğunluğunu Şekil 7'de görüldüğü üzere "Köle bilgisayar ağına dahil olma" oluşturmaktadır. Yine aynı kaynağa göre, Türkiye'ye ait zararlı yazılım bulaştırılma yüzdesinin aylık olarak ortalama olarak % 4,74 olduğu belirtilmiştir[301].

[301] https://threatpoint.checkpoint.com/ThreatPortal/threat?threatType=publication&threatId=1561 [31.01.2018].




**Şekil 7: Yıllık Ortalama Siber Tehdit Oranları (Aralık 2016-Aralık 2017)**

https://threatpoint.checkpoint.com/ThreatPortal/threat?threatType=publication&threatId=1561 [31.01.2018]. Edge Group, "2017 CyberThreat Defence Report", https://www.sumologic.com/wp-content/uploads/CyberEdge-2017-CDR-2017-Report.pdf, [03.02.2018].

Günümüzün trend siber tehditlerinden olan fidye yazılımlara ilişkin Türkiye'nin verilerine baktığımızda ise; son yıllarda gittikçe artan fidye yazılım saldırılarını Avrupa bölgesinde en çok yaşayan ülke olduğu, dünyada ise yine ilk sıralarda bulunduğu Trend Micro tarafından yayımlanan raporda ifade edilmektedir. Raporun bir diğer dikkat çekici noktası, çevrimiçi bankacılığa yönelik artan tehditlere ilişkin verilerdir. Buna göre 2016 sonuna kadar olan dönemde, Türkiye 11.0516 siber saldırı ile Avrupa bölgesinde en fazla çevrimiçi bankacılık saldırısı yapılan ülke konumunda bulunmaktadır[302].

Çalışmanın ikinci bölümünde; savunma planlama anlayışlarındaki paradigma değişimlerinin esasını teşkil eden asimetrik savaşların doğuşu ve bir asimetrik savaş türü olan ve çalışmanın ana temasını teşkil eden siber tehditlere ilişkin kavramlar ve söz konusu tehditlerin boyutları güncel verilerle desteklenerek anlatılmaya çalışılmıştır. Teknoloji ve özellikle internetin zorunluluk haline geldiği ve kamuoyunun çoğunluğunun hem fikir olduğu Bilgi Çağı'nın getirdiği kolaylıkların,

[302] STM, **age**, 5.

siber tehditlerin de hedefi olduğu bir gerçektir. Özellikle son yıllarda artan siber saldırılar, söz konusu tehdidin muhtemel büyüme potansiyeline dikkat çekmektedir. Geleceğe dönük olarak siber tehditlere ilişkin bir değerlendirme yapmak gerekirse; finans, savunma, haberleşme, ulaşım ve sağlık sektörlerini de içinde barındıran kritik altyapılara yönelik saldırıların devam edeceği, kişisel ve kurumsal açıdan ise ciddi maddi zararları ve kişisel/kurumsal verilerin başkasının eline geçmesini beraberinde getirebilecek siber tehditlerin faaliyetlerine son süratle devam edeceği değerlendirilmektedir. 2017'de popülerliğin zirvesine oturan Bitcoin gibi sanal paralara karşı artan küresel ilgi ve WannaCry benzeri fidye yazılım saldırılarının da, siber tehditlerin 2018 yılı ve sonrasında da öncelikli hedeflerinden olacağı[303] tahmin edilmektedir.

Siyasi/politik, ekonomik, ego, eğlence, milli ve manevi duygular gibi farklı motivasyonlara sahip olan siber tehditlerin ortak gayesi; siber saldırı yapılacak olan hedeflerin özellikle sızması çok daha kolay olan açık ağda yer alan bilgilerine erişmektir. Devletler çeşitli hizmetler kapsamında verilerini internet ortamına açtıkça, siber uzayda saldırıya daha açık hale gelmektedirler[304]. Dolayısıyla siber tehditlerin bilgi ve becerileri ile her türlü imkân ve kabiliyete sahip olmalarının yanı sıra istedikleri ortam da mevcut bulunmaktadır[305].

Verilerden de görüldüğü üzere, rapor edilen saldırıların sayısı her geçen yıl daha da artmaktadır. Saldırı teknikleri daha fazla tahrip edici ve zarar verici olacak şekilde gelişmektedir. Ancak şu andaki çözümler, sadırıların artan hızı ve gelişimine ayak uyduramamaktadırlar[306]. Bu nedenle bilgi altyapılarının, her an her şeyle karşı karşıya olabileceği son derece tehlikeli bir tehdit havuzunun ortasında yüzmeye çalıştığını söylemek mümkündür. Buradan hareketle; siber tehditlerin artık kişisel, kurumsal, ulusal hatta uluslararası manada tedbir alınması, savunma mekanizması oluşturulması ve savunma planlamalarına mutlaka dahil edilmesi gereken bir kavram olduğu görülmektedir.

Çalışmanın bir sonraki bölümünde ayrıntılı olarak anlatılacak olan "Siber Tehditlerin Savunma Planlamalarına Olan Etkileri" ana temasına ilişkin; siber savunmanın kavramsal boyutu, Türkiye'nin siber güvenliğe ilişkin stratejisi, yürütülen projeler, yapılan faaliyetler, özellikle hükümet birimleri ve askeri alanlarda kurulan

---

[303] Funda Güleç Yalçın, "2018 Siber Tehdit Öngörüleri Raporu Yayınlandı", 02.01.2018, fintechtime.com/tr/2018/01/2018--siber-tehdit-ongoruleri-raporu-yayinlandi/?doing_wp_cron=1515812674.1795079708099365234375 [07.02.2018].

[304] Hüseyin Çakır, Nursel Yalçın ve Mehmet Serkan Kılıç, "İnternet Sitelerine Yapılan Siber Saldırılar: 2015 Yılı Türk Kamu Siteleri İncelemesi", **Güvenlik Stratejileri Dergisi**, c.13, s.25 (2017): 185.

[305] Sait Yılmaz ve Olay Salcan, **Siber Uzay'da Güvenlik ve Türkiye** (İstanbul: Milenyum Yayınları, 2008), 51.

[306] Sait Yılmaz ve Olay Salcan, **age**, s.13.

siber savunma birimlerinin kadro ve teşkilat yapısı ile ilgili hususlar, örneklem olarak ele alınan diğer ülkelerin siber saldırı ve savunma kabiliyetleri, kadro ve teşkilat yapılarının yanı sıra Türkiye ile kıyaslamalarının yapıldığı değerlendirmelere de yer verilecektir.

# 4. SİBER TEHDİTLERİN SAVUNMA PLANLAMALARINA ETKİLERİ

Cambridge Üniversitesinde 1837 yılında Prof. Charles BABBAGE tarafından "Akıllı Motor" adıyla ilk bilgisayar tasarlanırken çok büyük ihtimalle insanlık tarihinde bu kadar büyük bir devrim yaratacağı, hatta günümüz dünyasını savaşların eşiğine getirebileceği hiç düşünülmemişti[307]. Zaman içinde gelişen teknoloji, artık bilginin sadece saklandığı değil, işlendiği, kullanıldığı ve geliştirildiği en önemli ortam haline gelmiştir.

Teknolojik gelişimin beraberinde getirdiği avantajların yanı sıra birçok tehdidi de beraberinde getirdiği artık kabul edilen bir gerçektir. Değişen tehdit algısı, muharebe alanlarında ve savaş yöntemlerinde de değişikliğe sebep olmuştur. Günümüz savaşlarını önceki benzerlerinden ayıran ve yıkımları sanal dünyada gerçekleştiği için daha tehlikeli olduğunu net bir şekilde gösteren nedenlerin başında, savaşın bilgisayarlaşması ve rasyonelleşmesi gelmektedir[308].

Savaş konseptlerindeki değişimler doğrultusunda günümüzde "Ağ Merkezli Savaş" türüne doğru bir gidiş eğilimi bulunmaktadır. Ordular sistemlerini giderek sayısallaştırmakta ve herşeyi gerçek zamanlı olarak görüp derhal müdahale yeteneğini kazanmak istemektedirler. Bu konu esasen bir tercih konusu olmaktan çıkmış, büyük bir kesmin bu yola gittiği düşünüldüğünde artık geride kalınması düşünülemez bir hale gelmiştir. Ne var ki ağ merkezli savaşın inisiyatif üzerindeki kısıtlayıcı rolü, bu tür sistemlerin bilgisayar ve elektronik saldırılara açık oluşu, ağ merkezli sistemlerin ister siber saldırı isterse de başka nedenlerle çöktüğü takdirde bocalamamak için neler yapılacağı gibi devasa sorunlarını da beraberinde getirmektedir[309].

---

[307] Seda Yılmaz ve Şeref Sağıroğlu, "Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri", **6.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı**, Ankara, 2013, 158.

[308] Chris Hables Gray, **Postmodern Savaş: Yeni Çatışma Politikası**, çev. Derya Kömürcü (İstanbul: Alfa Yayınları, 2000), 54.

[309] Mehmet Tanju Akad, **Tarihten Bugüne Gayrinizami Savaş** (İstanbul: Kastaş Yayınları, 2015), 82.

Günümüzün uluslararası çatışma ortamı aynı zamanda bir bilgi üstünlüğü ve bilgi savaşı konseptini de beraberinde getirmektedir. Operatif ve taktik alanlarda bilgi üstünlüğünün sağlanması ise büyük bir bilgi ve iletişim sistemleri altyapısı ile entegrasyonu gerektirmektedir. Ancak bu işler büyük avantaj potansiyelinin yanı sıra bir takım riskleri de barındırmaktadır. Bu risklerin en önemlisi, siber tehditlerden gerçekleştirilecek olan saldırılar olup, geleceğe yönelik oluşturulan tehdit projeksiyonunda ülkeleri bekleyen en yüksek olasıklıklı tehdit ihtimali olarak yer almaktadır[310]. Bugüne kadar olan deneyimler bu siber tehdit ve siber savaş risklerinin gerçek olduğunu göstermiştir[311]. Bu doğrultuda, yeni sayısal muharebe ortamını çok ciddi siber tehditlerle dolu bir geleceğin beklediğini[312] ve bu tehditlere karşı da son derece kırılgan bir yapıda olduğunu öngörmek gayet mümkündür.

Günümüz teknolojisi ile bir saldırının ne zaman yapılabileceğini kestirmek olanaksızdır. II. Dünya Savaşı yıllarındaki gibi, bir füzenin fırlatılması için 20 dakika gibi bir süre kullanma lüksü de günümüzde artık yoktur. Siber saldırıların ışık hızında gerçekleşmesi nedeniyle bu tür saldırılar anında reaksiyon göstermeyi gerektirmektedir[313].

Çalışmanın 4'üncü bölümünde; özellikle 3'üncü bölümde detaylı olarak anlatılan ve çağın en ciddi asimetrik tehditlerinden biri olan "Siber Tehditler"in savunma planlamalarına olan etkileri, ülkemizin siber savunma ve siber güvenlik stratejilerine ilişkin konsepti ve yürütülen faaliyetleri ile ulaşılabilen veriler doğrultusunda diğer ülkelerin özelikle askeri alandaki siber kabiliyetleri ve güçleri ile teşkilatlanma konusundaki gayretleri ve oluşturdukları organizasyonel yapılardan bahsedilerek siber tehditlerin savunma anlayışlarına olan etkileri açıklanmaya çalışılacaktır.

## 4.1. Siber Savunma

İnterneti ve bilişim ağlarını kontrol altında tutmak önemli bir mesele olarak gözükse de tehdidin geleceğini varsayarak tamamen yasaklamak veya erişimi kısıtlamak, milyarlarca insanın bilgiye ulaşmak için kullandığı günümüzde pek de

---

[310] Hasan Süzen tarafından hazırlanarak NATO Shape karargahında sunulan "Geleceğin Harekât Ortamında Kapsamlı Yaklaşım ve NATO'nun Komuta Kontrol Mimarisine İlişkin Görüş ve Çalışmalar" konulu sunumun yansılarından alınmıştır.

[311] Mehmet Tanju Akad, **age**, 83.

[312] Tim Mahon, "Cyber Defence: Welcome To The Next Level", **Naval Forces**, No:1 (2015): 40.

[313] Katharina VonKnop, "Institutionalization of a Web-Focused, Multinational Counter-Terrorism Campaign - Building a Collective Open Source Intelligent System", **A Discussion Paper, Responses to Cyber Terrorism**, ed. Centre of Exellence Defence Against Terrorism (Ankara: IOS Press, 2008): 9.

mantıklı bir çözüm olarak gözükmemektedir[314]. Bu nedenle bir önceki bölümde de ayrıntılı değinildiği üzere; teknoloji yarışının sonucunda devletlerin ulusal değerlerini, bireylerini, kaynaklarını, alt yapılarını, kaynaklarını hatta topraklarını diğer devletler veya devlet dışı aktörlerden gelebilecek olan siber saldırılara karşı savunma ihtiyacı doğmuştur[315]. Özellikle büyük çapta veriyi elde tutmalarından dolayı cazibe merkezi haline gelen gelişmiş ülkeler, bilgiye sahip olmanın yanında bunu korumanın da savaşını verme çabası içerisindedirler[316]. Bu amaçtan hareketle siber savunmayı, siber uzayda faaliyet gösteren yazılım, donanım, iletişim ağı altyapısından meydana gelen bilgi sistemlerini ve bu sistemleri içeren her türlü teçhizat, sistem ve altyapıyı siber tehditlere karşı korumak için alınan önlemlerin uygulanması[317] olarak tanımlamak mümkündür.

Basit manada siber savunma yöntemleri kapsamında değerlendirilen araçlar olarak; antivirüs yazılımları, güvenlik duvarları, network erişim kontrolleri, saldırı tespit ve önleme sistemleri, açıklık tarayıcı yazılımlar, geçerli kullanıcı ve şifre yönetimi, sanal özel ağ, kripto cihazları ve tuzak sistemlerini saymak mümkündür. Ancak siber savunma bir anlık veya saldırıya odaklı tedbirden ziyade, tedbirler bütünü ve uzun soluklu bir süreçtir. Bu kapsamda siber savunma sürecinin prensipleri şu şekilde sıralanabilir:

- Neleri savunacağız (Koruyacağız),
- Kimlerden koruyacağız (Tehdit kaynakları),
- Muhtemel riskler ve kayıplar,
- Zayıf ve güçlü yönlerimiz (En zayıf halka),
- Tehditlerin zayıf ve güçlü yönleri (Saldırganın analizi)
- Savunma ve saldırıya yönelik ihtiyaçlar[318],
- Hukuki boyutun değerlendirilmesi,
- Muhtemel hareket tarzları ve senaryoların hazırlanması,
- Planların (Alternatif planlar dahil) oluşturması,
- Deneme ve tatbikatlar ile yeteneklerin pekiştirilmesi, uygulama esnasında belirlenecek olan ihtiyaçlara yönelik plana girdi yapılması.

---

[314] Kristen E.Tullos, "From Cyber Attacks To Social Media Revolutions: Adapting Legal Frameworks To The Challenges and Opportunities Of New Technology", **Emory Internation Law Review**, c.26 (2012): 736.

[315] Anna-Maria Osula ve Henry Rõigas, "Outer Space and Cyberspace: A Tale of Two Security Realms", **International Cyber Norms**, ed. Paul Meyer (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publications, 2016), 155.

[316] Sait Yılmaz ve Olay Salcan, **age**, 151.

[317] Hasan Çiftçi, **age**, 191.

[318] İbrahim Soğukpınar'ın 2016 yılı içerisinde TASAM faaliyetleri kapsamında hazırlamış olduğu "Teknolojik Gelişmeler ve Siber Güvenlik" konulu sunumundan alınmıştır.

Siber savunma sürecinin ilk ayağı, görüldüğü üzere "Nelerin, kimlerden korunacağıdır". Çünkü bir varlığın korunabilmesi için öncelikle değerinin bilinmesi ve hangi muhtemel risklere maruz kaldığı/kalabileceğinin belirlenmesi gerekmektedir[319]. Bu kapsamda değerlendirilebilecek olan kişilerin ve kurumların sahip oldukları kritik verilerin, bilgilerin yer aldığı bilgi sistemlerinin; istihbarat, propaganda veya terör amaçlı yapılabilecek olan siber saldırılara karşı yüksek öncelikli olarak korunması zaruridir[320].

Siber savunma yöntemleri esasında, siber tehditlerden beklenen muhtemel taarruz şekillerine göre geliştirilmektedir. Dolayısıyla taarruz yöntemleri ve tehdit algılarındaki çeşitlilik ne kadar artarsa savunma yöntemlerine ilişkin yapılan çalışmalar da o yönde değerlendirilmekte, yeni savunma yöntemleri geliştirilmesine ihtiyaç duyulmaktadır. Özellikle küresel çapta gündeme gelen siber taarruzlar karşısında ne kadar aciz ve savunmasız olunduğu görülmüş ve nerdeyse bütün devletler tarafından artık bu konuda acil çözüm geliştirilmeye, savunma planlamalarına dahil edilmeye zorunlu hale gelindiği anlaşılmıştır. Çalışmanın bir sonraki aşamasında NATO başta olmak üzere ülkelerin erişilebilen veriler doğrultusunda siber teditlerin savunma planlamalarındaki yerleri ortaya konmaya çalışılacaktır.

## 4.2. Siber Savunma Durum Analizi ve Siber Tehditlerin Ülkelerin Savunma Planlamalarındaki Yerleri

Önemli kritik altyapı ve ağların açıklıklarını belirlemeden, olabilecek bir saldırı hakkında bilgi sahibi olmak için beklemek çok riskli ve kabul edilemez bir stratejidir. Siber saldırılar genellikle hiçbir ikaz olmaksızın ülke ağlarına sızmak suretiyle patlak verebilir ve bu saldırılardan zarar görenlerin hiçbirinin ikaz almasına vakit kalmaksızın süratle yayılabilirler. Hatta bir ikaz olsa bile korunma için ihtiyaç duyulan zamana, bilgiye ve araçlara sahip olma imkanı olmayabilir. Bazı durumlarda, bu tür saldırılara karşı bir savunma mekanizması oluşturmak, tedbir almak günlerce sürebilir[321].

Siber savunma stratejilerinde temas edilen ilk alan askeri siber operasyonlardır. Askeri siber operasyonlar denilince öncelikle akla gelen ülkenin sahip olduğu bilişim altyapısının korunmasına yönelik olan siber savunma faaliyetleri olmaktadır. Siber

[319] Seda Yılmaz ve Şeref Sağıroğlu, **age**, 160.
[320] Yılmaz Vural ve Şeref Sağıroğlu, "Ülke Bilgi Güvenliği", 3**.Ulusararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı**, Ankara, 2008, 3.
[321] Sait Yılmaz ve Olay Salcan, **age**, 65.

savunma istihbarat odaklı olup, acil durumlara hızlı müdahaleye imkân sağlayan bir organizasyonel yapıyı zorunlu kılmaktadır. Bunun yanı sıra pasif ve aktif savunma biçimlerini içermektedir. Aktif savunma yöntemleri saldırganın saldırı maliyetini arttırarak caydırıcılığı arttırmayı hedeflemektedir. İkinci önemli askeri beceri, düşman unsurların bilişim altyapılarına stratejik nitelikli siber operasyonlar yapabilmektir. Üçüncü önemli askeri beceri, ikinciyle yakından alakalı olarak, savaş halinde düşmanın sahip olduğu bilişim altyapılarına yönelik siber saldırı gerçekleştirebilmektir. Dördüncü ve son beceri ise geleneksel askeri yapıların, bilişim teknolojilerinin sunduğu imkânlardan yararlanılarak modernize edilmesi suretiyle kapasite ve etkinliğinin arttırılmasıdır[322].

Yüksek askeri bütçeli olanlar başta olmak üzere birçok ülke siber saldırı yeteneklerini arttırmaya çabalamaktadır[323]. Bunun yanı sıra siber saldırı araçlarını kullanmak istemelerine rağmen diğer yandan da aynı saldırı yöntemlerinin kendilerine karşı uygulanmasına doğal olarak müsamaha göstermemekte[324], aksine bunlara yönelik savunma tedbirleri de geliştirmeye yönelmektedirler. Ancak saldırı imkânları konusunda bir güçten bahsetmek mümkün olsa da savunma konusunda bir hüküm vermek pek mümkün değildir, çünkü daha önce de belirtildiği üzere siber tehditlere karşı en iyi savunma diye birşeyden bahsetmek mümkün değildir.

İnternet erişim ortamının, merkezi olmayan ve etkileşimli mimarisi, isteyen bütün herkesin çok düşük maliyetlerle erişim sağlayabiliyor olması, popülerliği ve anonimliği gibi özellikleri nedeniyle tehditler açısından çok büyük imkanlar sunmaktadır[325]. Bu nedenle özellikle internetin çok hızlı yayılımı, bağlantı hızlarının artması ve gizlilik dereceli bilgiler de dâhil birçok bilginin internet erişimli bilgisayar ve sunucular üzerinde bulunması, sanal ortamı da güvensizleştirmiştir. Bunun bir sonucu olarak ABD, Çin ve İngiltere gibi gelişmiş ülkelerin yanı sıra artık birçok ülke daha, savaş ortamına siber ortamı da bir boyut olarak ekleyerek siber kuvvetler oluşturma çabası içerisine girmişlerdir[326]. Siber ortamda savunma ve saldırı yapabilecek bir siber ordu oluşturan[327] ABD'de siber ordunun yedeklerinin dahi

---

[322] **National Cyber Security Framework Manual**, ed. Alexander Klimburg (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publications, 2012), 120, https://www.ccdoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf [ 01.02.2018].

[323] Kristen E.Tullos, **age**, 733.

[324] Kristen E.Tullos, **age**, 742.

[325] TSK Siber Savunma Komutanlığı, "Teröristlerin Siber Uzayı Kullanımı", **Siber Savunma Farkındalık Bülteni**, Bülten No: 2015-F-3 (2015): 1.

[326] Dennis P. Dias, **Partnering With Private Networks: The Dod Needs A Reserve Cyber Corps** (U.S. Army War College/Carlisle: PA, 2008), 2.

[327] Şener Çelik, "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, c.15, s.1 (2013): 137-175.

olması gerekliliğinin tartışılması, bir asimetrik tür olan siber tehditlerin savunma planlama anlayışlarında yaşanan dönüşüme ne denli etki ettiğini doğrular niteliktedir[328].

Çağımıza damga vuran bilişim teknolojilerindeki gelişim ve artan siber tehdit ihtimalleri doğrultusunda birçok devlet savunma planlamalarını, siber uzaya uyumlu hale getirmeye çalışmakta, orduları başta olmak üzere bütün kurumlarını bu modern tehditle mücadeleye uygun olarak teşkil etmeye yönelik gayret göstermektedir. İkinci bir güç gösterisi ve silahlanma yarışına sahne olunan bu dönem Siber Soğuk Savaş olarak adlandırılır hale gelmiştir[329]. Bu kapsamda, çalışmanın bu bölümünde elde edilebilen veriler doğrultusunda siber tehditlerin savunma planlamalarındaki etkilerinin daha iyi anlaşılmasını sağlayacak olan NATO'nun ve örneklem olarak ele alınan ülkelerin siber alandaki savunma tedbirleri, askeri kabiliyetleri ve teşkilatları ele alınmıştır.

### 4.2.1. NATO

1999 yılında Kosova Krizi sırasında uğradığı siber saldırılar neticesinde tedbirler almaya başlayan NATO, 2002 yılında Güvenlik Ofisi'ne bağlı NATO Bilgisayar Olayları Karşılama Kapasitesini (Computer Incident Response Capability) kurmuştur. 2007'de Estonya'da meydana gelen siber saldırılar ise siber güvenliğin daha etkin bir şekilde ele alınması gerektiğini ve siber saldırılara karşı önlemlerin yeni bir düzeye taşınması gerektiğini anlatan olay olmuştur.

NATO'nun 20 Kasım 2010 tarihinde yayınladığı Lizbon Zirve Bildirisinde siber tehditler öncelikli tehditler arasında sayılmıştır. Bildirinin siber güvenlikle ilgili işbirliğini ve atılacak adımları ele alan maddelerini şu şekilde özetlemek mümkündür:

- Siber savunma kapasitelerinin geliştirilmesi,
- Siber tehditlerin karmaşıklık ve ustalık bakımından hızla arttığı ve geliştiği,
- NATO'nun siber alana daimi ve kısıtlama olmaksızın erişimini sağlamak ve kritik sistemlerinin bütünlüğünü korumak için modern çatışmaların siber boyutlarının NATO doktrinleri içerisinde göz önünde bulundurulması ve tespit edilmesi, değerlendirilmesi ve engellenmesi, savunma ve Topluluğa karşı yapılacak siber saldırılar durumunda sistemleri iyileştirme kapasitelerinin geliştirilmesi,

[328] Dennis P. Dias, **age**, 3.
[329] https://www.nasdaq.com/article/so-who-has-the-most-advanced-cyber-warfare-technology-cm861979/amp [02.02.2018].

- Ortakların siber savunma kapasitelerini desteklemek, istekleri halinde NATO üyelerine yardım etmek, bilgi paylaşımını, işbirliğini ve ortak operasyon yapabilme kabiliyetini en iyi hale getirmek için NATO'nun savunma planlama süreçlerinin kullanılması,
- Siber alandan doğabilecek güvenlik risklerine karşılık verebilmek için BM ve AB gibi diğer aktörler ile anlaşmalar çerçevesinde sıkı işbirliği halinde çalışması gerektiği,
- NATO'nun mevcut savunma politikasının gözden geçirilerek derinlemesine bir siber savunma politikası oluşturulması ve bunun uygulanması için bir eylem planı hazırlanması,
- NATO'nun stratejik konsepti ve 2010 Lizbon Zirve Deklarasyonunun, giderek artan bir karmaşıklık ve uzmanlıkla gerçekleştirilen siber saldırılar; topluluğun bilgi ve iletişim sistemlerinin korunmasını NATO için birinci öncelik haline getirmiş ve NATO'nun güvenliğinin büyük oranda buna bağlı olduğu[330] konuları üzerinde durulmuştur.

Devam eden süreç içerisinde, 8 Haziran 2011 tarihinde NATO Siber Savunma Politikası kabul edilmiştir. Bu politika siber savunma konusunda gerçekleştirilecek olan topluluk bazındaki çabaları içermektedir. Ekim 2011'de ise Bakanlar tarafından Siber Savunma Eylem Planının detayları üzerinde görüş birliğine varılmıştır. Söz konusu NATO Siber Savunma Politikasına göre NATO kapsamında atılacak olan pratik adımları şu şekilde özetlemek mümkündür[331]:

- NATO'nun temel görevlerini yerine getirmesi konusunda kritik olan NATO ulusal bilgi sistemleri için asgari gereksinimler sağlanacak,
- NATO, zayıflıkları azaltmak maksadıyla gerekli olan asgari siber savunma seviyesinin gerçekleştirilebilmesi için ulusal kritik altyapılar konusunda müttefiklerini destekleyecek,
- Ayrıca bir siber saldırı durumunda müttefikler başka bir müttefiğe veya topluluğa yardım edebilecek,
- Siber savunma, NATO'nun Savunma Planlama Sürecine tam olarak dahil edilecek, siber savunma gereksinimleri belirlenerek NATO Savunma Planlama Süreci vasıtasıyla önceliklendirilecek,
- NATO Askeri Yetkilileri siber savunmanın NATO'nun temel görevlerinin yerine getirilmesini, askeri vazifelerin planlanmasını nasıl desteklediğini belirleyecek,

[330] https://www.nato.int/cps/en/natohq/official_texts_68828.htm [11.04.2018].
[331] https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf [11.04.2018].

- Ayrıca katkıda bulunan NATO üyesi olmayan milletlerin siber savunma gereksinimleri belirlenecek,
- Güçlü yetkilendirme gereksinimleri uygulanacak ve yetki elde etme süreci, tedarik zinciri risk yönetimi gereksinimleri akıcı hale getirilecek,
- Erken uyarı, durumsal farkındalık ve analiz kapasiteleri geliştirilecek,
- Farkındalık programları geliştirilecek ve NATO tatbikatlarının siber unsuru daha ileri düzeye taşınacak,
- NATO ve müttefikler Tallinn'deki Siber Savunma Mükemmeliyet Merkezi'nden faydalanarak uzmanlık kazanmaları konusunda teşvik edileceklerdir.

NATO Siber Savunma Politika Belgesi, esasen belirtilen hususların yanı sıra iki önemli kilometre taşının hayata geçirilmesi bakımından çok kritiktir. Bunlar; gerçek zamanlı operasyonel kabiliyeti olan Cyber Defence Management Authority (CDMA-Siber Savunma İdari Makamı) ve uzun vadeli, siber alandaki strateji ve doktrinlerin tartışıldığı, geliştirildiği bir fikir platformu olan Estonya temelli Cooperative Cyber Defence Centre of Excellence (CCDCoE-Siber Savunma İşbirliğine Ait Mükemmelliyet Merkezi)'dir[332].

NATO'nun siber savunma yeteneğini geliştirmek amacıyla 14 Mayıs 2008'de Estonya'da kurulan NATO Siber Savunma Mükemmeliyet Merkezi (NATO CCD COE), 28 Ekim 2008 tarihinde ise uluslararası askeri bir örgüt haline getirilmiştir[333]. Hali hazırda 11 NATO ülkesinin sponsor olduğu merkez; Siber Güvenliğin gerek teknik, gerekse hukuki ve uluslararası ilişkileri ilgilendiren konularında çok çeşitli faaliyetler yürütmektedir. NATO CCD COE'nin öne çıkan projeleri arasında; "The Tallinn Manual on the International Law Applicable to Cyber Warfare (Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı)" çalışması ve her yıl düzenlenmekte olan "International Conference on Cyber Conflict (Uluslararası Siber Anlaşmazlık Konferansı)" konferansı ile Locked Shields - Uluslararası Siber Savunma tatbikatını örnek olarak göstermek mümkündür[334].

Bir zincir ancak en zayıf halkası kadar güçlü olduğundan, bütün bu birimlerin bir araya geldiklerinde kendi kendilerini güçlendirmesi beklenmektedir. Bu nedenle ittifakın güvenliği ve toplu savunma, kriz yönetimi ve işbirliğine dayalı güvenlik gibi üzerinde anlaşmaya varılmış görevleri yerine getirme yeteneği; büyük çaptaki müttefiklerinin bireysel olarak siber savunma yeteneklerine ve kapasitelerine dayanmaktadır. Bu bağlamda, NATO bünyesindeki Siber Savunma Yönetim Ajansı CDMA (Cyber Defence Management Agency), NATO içerisinde siber savunma

[332] Mehmet Meral, "NATO ve Siber Savunma", https://mehmetmeral.wordpress.com/2015/01/17/nato-ve-siber-savunma [10.04.2018].
[333] Mahzure Kara, **age**, 58.
[334] http://sge.bilgem.tubitak.gov.tr/tr/nato-ccdcoe-daimi-temsilciligi [11.04.2018].

faaliyetlerini başlatan ve koordine eden birimdir. NATO'nun ele aldığı siber tehditler, politik veya askeri bir çatışma esnasında NATO ve üye ülkelere karşı gerçekleştirilen devlet destekli saldırılardır. Bu tür saldırılar, karşı konulması en zor ve etkileri en ciddi olanlardır[335].

NATO'nun temel bağlamda siber savunma rollerini iki çatı altında incelemek mümkündür. Buna göre birinci öncelik, 2014 yılındaki Galler Zirvesi'nde karara varıldığı gibi, kendi ağlarının korunmasıdır. İttifakın işi, Brüksel gibi şehirlerden zor şartlardaki çöllere kadar, bulunduğu değişik yerlerde bıraktığı ayak izleri ve operasyonel tesisler dikkate alındığında, bu bir hayli güç gözükmektedir. Bu nedenle NATO'nun siber savunmadaki rolünün bu bölümünü yerine getirebilmesi için ittifakın operasyonları ve misyonlarını yürütmek için dayandığı iletişim ve bilişim sistemlerinin siber uzaydan yayılan tehditlerden korunduğunu garanti etmesi gerekmektedir. NATO'nun ikincil önceliği ise üyelerine kendi siber savunma yetenekleri ve kapasitelerini oluşturmalarında yol göstermektir. Bunu çeşitli yollarla yerine getirmektedir. Bu yollardan birisi, her bir müttefikin toplu siber savunma hedeflerinin (örneğin siber savunma stratejisinin yaratılması) oluşturulması için katılacağı iki yıllık bir süreçtir[336].

Uluslararası aktörlerin arasında yer alan NATO, siber uzaya ilişkin faaliyetlerini kamuya açık olarak sürdürmektedir. Bu kapsamda, NATO'nun orta vadede siber alandaki rolünü güçlendirmeyi planladığı beş alan ise şunlardır:

- Siber savunmayı ana akım haline getirmek,
- Müttefikler arasında yeteneklerin geliştirilmesi,
- Uluslararası normlara destek,
- Kolluk kuvvetleri istihbarat alış-verişi,
- AB ile angajman[337].

Kabul edilen bu söz konusu müşterek hedefler konusundaki ilerlemeler sürekli olarak gözden geçirilmektedir. İlave olarak NATO, Oberammergau'daki NATO Okulu ve Portekiz'deki Siber Akademi vasıtasıyla geniş kapsamlı bir eğitim, öğrenim ve tatbikat fırsatı sunmaktadır. Estonya'daki NATO Siber Savunma Mükemmeliyet Merkezi de bu konuda önemli bir rol oynamaktadır. Bir diğer yandan NATO'nun bilgi güvenliği ve telekomünikasyon projelerini yürüten ajansı olan NCIA (NATO Communications and Information Agency) ise, siber savunma için ittifakı

[335] Süleyman Anıl, "Defending Against Cyber Attacks", **NATO CEP Perceptions**, s.8, https://www.nato.int/issues/cep/cep_newsletter_08e.pdf [11.04.2018].
[336] Neil Robinson, "NATO: Siber Savunmada Vites Değiştiriyor", **NATO Dergisi**, https://www.nato.int/docu/review/2016/Also-in-2016/cyber-defense-nato-securityrole/TR/index.htm [10.04.2018].
[337] Neil Robinson, **age.**

güçlendirmek, danışma, komuta-kontrol desteği ve istihbarat sağlamak, gözetleme ve keşif yeteneklerini artırmak amacıyla uygun maliyetli, birlikte çalışabilir iletişim, bilgi sistemleri ve hizmetleri sunmaktadır[338].

Siber uzayın yeni bir harekat alanı olarak tanınmasıyla birlikte üç yıllık bir Yol Haritası oluşturulmuştur. Söz konusu Yol Haritasındaki faaliyet alanlarından birisi de teşkilatlanma çalışmasıdır. Bu çalışma kapsamında SHAPE/Brüksel'de Siber Harekat Merkezi (Cyber Operations Center-CyOC) kurularak görev ve personel planlama çalışmalarının devam etmekte olduğu bildirilmiştir. Diğer bir faaliyet alanı olan Siber Etkiler kapsamında, Siber Savunma Komitesi tarafından ülkelerin siber imkân ve kabiliyetlerinin gönüllülük esasına göre kullanılmasına ilişkin ilkeler de belirlenmiş, devlet başkanları seviyesinde de ayrıca bir "Siber Savunma Taahhüdü" imzalanmıştır[339].

Siber savunmaya ilişkin NATO'da güçlü bir irade görülmektedir. Tehdidin önemine vurgu yapıldığı üzere, siber uzayın ve buradan gelebilecek saldırıların gerek tekil olarak devlet bazında gerekse birliğin geneline zarar vereceği düşüncesinden hareketle; savunmaya yönelik ciddi tedbirler geliştirilmekte, sürekli yenilenen konseptler, eğitim ve tatbikatlarla planlamalara yeni girdiler yapılmaktadır. Yürütülen bu çalışmalar neticesinde ilerleyen vadede bu işbirliklerinin artırılarak devam ettirileceği değerlendirilmektedir.

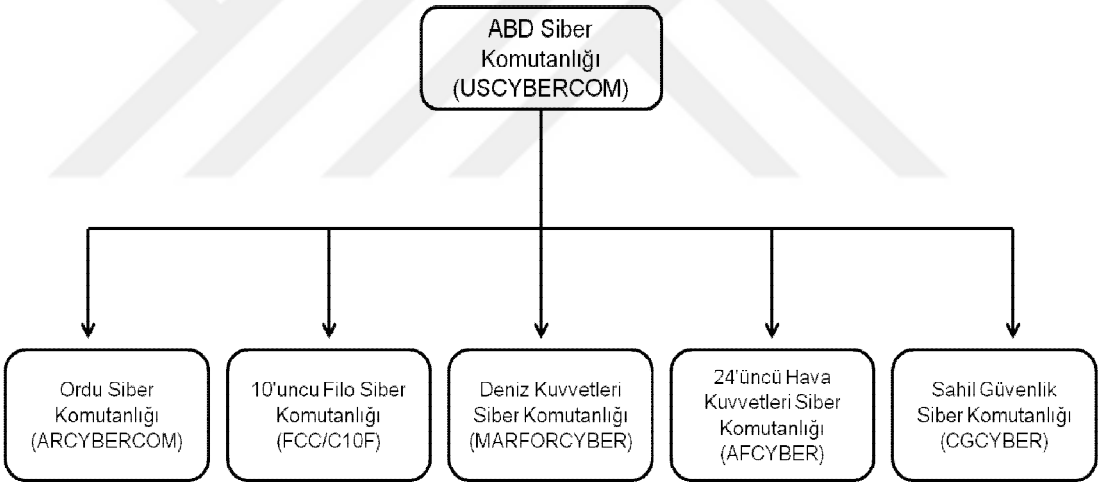
### 4.2.2. ABD

Siber tehditlerin önemli hedeflerinden birisi olan ABD'de artan dijital Pearl Harbour kaygısıyla[340] birlikte, 2002 yılında Siber Alanın Güvenliği için Ulusal Stratejinin (National Strategy to Secure Cyberspace) hazırlanmasıyla ilk adımın atıldığı ABD'nin siber savunma alanındaki faaliyetlerine ilişkin temel kaynağını 2013 Şubat tarihli "Siber Uzayı Koruma Ulusal Stratejisi" oluşturmaktadır. Federal yönetim, yerel makamlar ve özel sektörü de içermesi açısından ulusal değeri bulunan, geniş kapsamlı söz konusu belgede; görev ve sorumluluk alanları itibarıyla öncü olarak rolü bulunan kamu kurum ve kuruluşları da belirtilmektedir[341].

Askeri yapı bakımından değerlendirmek gerekirse, Amerikan ordusu, klasik savaş anlayışını kökünden değiştirmiştir. Bütün birimlerini siber uzayın bir parçası yapan Amerikan ordusu; iletişim, bilgisayar ve teknolojideki gelişmelerin, askeri

[338] Mahzure Kara, **age**, 58.
[339] https://www.nato.int/docu/review/2017/Also-in-2017/nato-priority-spending-success-cyber-defence/TR/index.htm [10.04.2018].
[340] http://bianet.org/biamag/toplum/130283-savaslar-siber-uzaya-tasiniyor [20.03.2018].
[341] Mehmet Meral, "Siber Savunma: Ülkeler ve Stratejiler", **3.Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı**, Ankara, 2008, 257.

yeteneklere dönüştürme çabalarının ilk olarak başlatıldığı askeri unsur olarak ön plana çıkmaktadır. Dünyanın en güçlü 5 siber kuvveti arasında gösterilen[342] ve "Süpergüç Hacker" olarak adlandırılan[343] ABD'nin Şekil 8'de belirtildiği üzere siber askeri teşkilatı incelendiğinde, en üst birimin ABD Siber Komutanlığı (USCYBERCOM) olduğu görülmektedir. ABD Stratejik Komutanlığı (USSTRAATCOM) altında Ordu seviyesinde, 2010 yılında Maryland eyaletindeki Fort Meade askeri tesislerinde kurulan ve aynı yıl ilk operasyonel yetenek kazanan bu birim[344], kendisine bağlı Ordu Siber Komutanlığı (ARCYBER), 10'uncu Filo Siber Komutanlığı (FCC/C10F), Deniz Kuvvetleri Siber Komutanlığı (MARFORCYBER), 24'üncü Hava Kuvvetleri Siber Komutanlığı (AFCYBER) ve Sahil Güvenlik Siber Komutanlığı (CGCYBER) gibi alt birimlerden oluşmaktadır. Aynı karargâhı paylaştığı ABD'nin en çok istihbarat toplayan teşkilatı olduğu kabul edilen Ulusal Güvenlik Dairesi (NSA)'in şefi/komutanı, aynı zamanda ABD Siber Komutanlığının da komutanıdır. Bu nedenle bu iki kurum sürekli koodinasyon ve işbirliği içerisinde çalışmalarını yürütmektedir[345].




**Şekil 8: ABD Askeri Siber Teşkilatı**

ABD Siber Komutanlığı; planlama, uygulama, birimler ve faaliyetler arasındaki senkronizasyon dahil olmak üzere siber harekat alanında yürütülen bütün

[342] https://www.google.com.tr/amp/s/safeandsavvy.f-secure.com/2017/03/20/top-5-countries-with-offensive-cyber-capabilities/amp [05.02.2018].
[343] Shannon Vavra, "The World's Top Cyber Powers", https://www.axios.com/the-worlds-top-cyber-powers-1513304669-4fa53675-b7e6-4276-a2bf-4a84b4986fe9.html [06.02.2018].
[344] www.stratcom.mil/Media/Factsheets/Factsheets-View/Article/960492/us-cyber-command-uscybercom [28.03.2018].
[345] Piret Pernik, Jesse Wojtkowiak ve Alexander Verschoor-Kirss, **National Cyber Security Organisation: United States** (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2016), 20.

faaliyetlerin birinci derece sorumlusu, emir komuta merkezidir. Savunma sistemlerine, ağlara, veritabanlarına yapılacak olan siber saldırılara yönelik 24 saat esasına göre savunma kalkanı oluşturmak ve görev verildiği takdirde siber uzayda harekat icra etmek, ana vazifeleri arasında yer almaktadır. Söz konusu birimin altında yer alan komutanlıkların her birinin görevleri birbirinden farklıdır. Ancak temel gayeleri ortaktır: Bilgi sistemleri altyapılarını savunmak, siber savaşa hazırlıklı olmak ve muhabere istihbaratı sağlamak[346].

Siber Komutanlık biriminin üzerinde durduğu 5 önemli husus bulunmaktadır. Bunlar; hali hazırdaki kuvvetleri eğitmek ve sürekli hazır durumda bulundurmak, siber harekat alanına ilişkin gerçek bir durumsal farkındalık yaratmak, verilecek görevlere ilişkin etkin bir komuta-kontrol ve operasyonel konseptleri oluşturmak, müşterek olarak savunulabilen bir ağ altyapısı inşa etmek ve siber uzayda geniş kapsamlı operasyonel faaliyetlerin icrasına izin veren doğru politika ve yetkilere sahip olunduğu konusunda komutana danışmanlık yapmaktır[347]. Bu kapsamda NATO bünyesindekiler de dahil olmak üzere her yıl birçok ulusal ve uluslararası tatbikatların planlama ve icra safhasında bulunarak siber savunma ve saldırı alanlarındaki imkan ve kabiliyetlerini test etme imkanı bulmakta, faaliyetlerin sonucuna göre planlamalarını gözden geçirerek gerektiğinde revize etmektedir.

"Saldır, Savun ve Faydalan (Açıklıklardan)" ilkeleri doğrultusunda faaliyetlerini yürüten alt birimlerin teşkilatanmalarına ilişkin konularında uzman ve nitelikli, sayıca yeterli sivil ve askerlerler birlikte görev yapmaktadır. Öyle ki bunlardan Ordu Siber Komutanlığı (ARCYBER)'nın 19.000[348], 10'uncu Filo Siber Komutanlığı (FCC/C10F)'nın ise yaklaşık 13.000 kişilik personel mevcutlarından teşkil edildiği[349] ifade edilmektedir.

ABD'de bilgisayarların, haberleşme altyapısının ve veri tabanlarının, askeri amaçlar için kullanılması esasına dayanan bilgi harbi üzerine yoğunlaşan gayretlerin iki ana sebebi bulunduğu ifade edilmektedir. Birincisi; ABD'nin siber saldırılar sonucunda kendi bilgi sistemlerinde oluşabilecek olan tahribat derecesinin tespiti, bir diğeri ise bilişim teknolojilerindeki gelişmeler neticesinde ortaya çıkacak olan yeni sistemlere yönelik olarak askeri stratejilerin geliştirilmesi fırsatlarının ortaya çıkaracağı hususlardır. Bu konudaki çeşitli sorular, senaryolar, tarihsel deneyimler ve güncel konular göz önüne alındığında siber uzayda gerçekleştirilecek olan

[346] Piret Pernik, Jesse Wojtkowiak ve Alexander Verschoor-Kirss, **age**, 20.
[347] Piret Pernik, Jesse Wojtkowiak ve Alexander Verschoor-Kirss, **age**, 20.
[348] http://www.arcyber.army.mil [28.03.2018].
[349] Deniz Kuvvetleri Komutanlığı MEBS Başkanlığının Mart 2018 tarihli "Siber Güvenlik" konulu sunumundan alınmıştır.

savunmanın zorluğunun haricinde caydırıcılık için etkili bir planın ortaya çıkarılmasının da çok zor olduğu değerlendirilmektedir[350].

Top, tank, tüfek gibi geleneksel yöntemlerle yapılan savaşların verdiği zararların siber saldırılarılar ile verilen zararlarla eşit tutulduğu ABD açısından, siber tehditler ulusal güvenliğin ve toplum hayatının devamlılığını tehlikeye atan bir faktördür. Bu nedenle ABD hükümeti, uğrayacağı siber saldırıları savaş sebebi olarak göreceklerini ifade etmektedir[351]. Bir önceki ABD Başkanı Obama'nın; "Artık birçok ülkenin çok ciddi kapasitelere sahip olduğu yeni bir çağa geçiş yapıyoruz ve açıkcası biz saldırı ve savunma açısından kimsenin sahip olmadığı kadar fazla kapasiteye sahibiz"[352] şeklinde ABD'nin siber harekat alanına ilişkin taarruz ve savunma gücüne vurgu yaptığı üzere, gerek bütçeden ayrılan pay gerek teşkilatlanma gerekse konuya ilişkin farkındalık yaratma konusunda hem siber saldırı hem de siber savunma konusunda çok ciddi çalışmalar yapıldığı görülmektedir[353].

Siber tehditlerin ekonomik ve ulusal güvenliğin karşı karşıya kaldığı en ciddi zorluk olduğununun benimsenmesi, hatta 21. yüzyılda Amerika'nın ekonomik refahının siber güvenliğe bağlı olduğunun ilan edilerek[354] ulusal ve uluslararası boyutta önemli bir sorun olarak görülmesi ve askeri teşkilatlanmadaki çabalarından da anlaşılacağı üzere, savunma planlama anlayışlarında siber tehditlerin ve siber harekat alanına yönelik faaliyetlerin ABD açısından önemli bir yer teşkil ettiğini söylemek mümkündür. Bilgisayar teknolojisinin sağladığı bütün olanakları kullanan Amerikan ordusu, herhangi bir savaşı sadece monitör, klavye ve mouse ile kazanmayı hedeflemektedir. Ancak Pentagon yetkilileri tarafından da belirtildiği üzere, bilgisayar savaşlarının en büyük zaafının, kendi sistemlerinin de başka ülkeler tarafından yok edilebilme ihtimali olması[355] her an tetikte olmayı zorunlu kılmaktadır.

---

[350] Zafer Yener, **age**, 82.

[351] Siobhan Gorman ve Julian E.Barnes, "Cyber Combat: Act Of War", https://www.wsj.com/articles/SB1i000142405270230456310457635562313578271 8 [02.04.2018].

[352] https://www.cybersecurityintelligence.com/blog/which-countries-are-ready-for-cyberwar-2763.html [01.02.2018].

[353] Keith Breene, "Who Are The Cyberwar Superpowers", https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers [01.02.2018].

[354] https://obamawhitehouse.archives.gov/the-press-office/2014/02/12/launch-cybersecurity-framework [02.04.2018].

[355] Douglas Waller, "Onward Cyber Soldiers", content.time.com/time/magazine/article/0,9171,983318,00.html [02.04.2018].

### 4.2.3. Çin

Modern halk savaşı ve eski manevra anlayışlarının bir araya gelmesi ile oluşturulan Çin'in savaş konsepti, savaşın nasıl kazanılabileceğine dair stratejik, operasyonel ve taktik seviyede fikirlerden meydana gelmektedir. Çin savaş anlayışının büyük kısmı aldatma, bilgi savaşı ve düşmana karşı asimetrik avantajlar kazanmak üzerinedir. Bu doğrultuda siber savaş konsepti klasik savaşlardan, aldatma ve kontrol anlayışına doğru kaymanın[356] en güncel örneklerinden birisidir.

Yapılan birçok araştırmaya göre siber güvenlik yapısı en zayıf ülkeler arasında yer alan ve siber savunma konusunda hazırlık durumu göz önünde bulundurulduğunda en son sıralarda bulunduğu belirtilen Çin[357]'in, birçok kullanıcısının korsan yazılım kullanması nedeniyle siber tehditlere karşı bu kadar zayıf olduğu değerlendirilmektedir. Bunun bir sonucu olarak, Çin kaynaklı olmasa bile birçok saldırı Çin'den yapılıyormuş gibi görünmektedir[358]. Ancak saldırı konusunda dünyanın lider siber tehdit kaynağı olarak kabul edilen Çin, agresif bir şekilde hızla siber savaşı askeri literatürüne, organizasyonuna, eğitimine ve doktrinine dâhil etmek için çaba sarf etmektedir. Çin'deki bir takım askeri gelişmelerin uzmanları endişelendirmesinin nedenlerinden en önde geleni, Çin'in siber saldırılar düzenlemek için sürekli yeni yollar keşfetme çabası ve niyetidir[359].

16 Nisan 2013 tarihinde yayınlanan Çin Halk Cumhuriyeti Beyaz Kitabına göre; Çin Silahlı Kuvvetlerinin Kullanım Çeşitliliği başlığıyla ilk defa kara, hava ve deniz kuvvetlerinin asker sayıları açıklanmıştır. Ancak askeri yapılanmadaki asker sayısını veren Beyaz Kitapta siber savaşçılardan bahsedilmemiş, yalnızca siber ve uluslar arası rekabette yüksek strateji zemini hazırlamak için ileri teknoloji ile askerin donatılmasının önemi vurgulanmıştır[360]. Ancak medyaya yansıyan haberlerde belirtildiği üzere Çin yapmış olduğu tarihi açıklamayla, ilk kez bir "süper elit siber savaşçı birliğine" sahip olduğunu belirtmiştir. Siber savaşçılardan oluşan ekibin, Çin Halk Kurtuluş Ordusu'nun (PLA) internet ağlarını dış saldırılardan korumak amacını taşıdığı ifade edilmektedir[361].

---

[356] Adem Kaya, **age**, 72.
[357] Dave Lee, "Israel Tops Cyber-Readiness Poll But China Lags Behind", www.bbc.com/news/technology-16787509 [02.04.2018].
[358] Jason Miks, "Israel, China and Cyber Security", https://thediplomat.com/2012/02/israel-china-and-cyber-security [02.04.2018].
[359] Steven A. Hildreth, "Cyberwarfare", **CRS Report for Congress**, Order Code: RL30735, 2001, https://fas.org/irp/crs/RL30735.pdf [04.04.2018].
[360] Mahzure Kara, **age**, 67.
[361] http://www.hurriyet.com.tr/gundem/cin-super-gizli-ordusunu-acikladi-17884879 [04.04.2018].

26 Mayıs 2015 tarihli Savunma Beyaz Kitabında ise; "Aktif Savunma" ilkesi ile belirlenen savunma stratejisinde siber savunma alanına odaklanılacağı belirtilmiş, askeri manada öncelik verilecek dört alan arasında siber savunmanın da (Diğer alanlar: Okyanus, uzay ve nükleer güç) yer aldığı, askeri gücünün gelişimini hızlandırmak için siber altyapısını güçlendirilmesi gerektiği ifade edilmiştir[362].

Görev ve sorumluluk alanının belirlenmesi açısından Çin'in siber güvenliği ve siber savunması görevi Çin Halk Kurtuluş Ordusuna (People's Liberation Army – PLA) verilmiştir[363]. Çin Kurtuluş Ordusunun içerisinde de daha çok teknik bir birim olarak bilinen 3'üncü Departman özellikle siber istihbarat olmak üzere ordunun siber faaliyetlerinin esas operasyonel kuvvetidir. Çünkü nerdeyse bütün faaliyetler söz konusu birim vasıtasıyla takip edilmektedir[364]. Diğer bir birim olan 4'üncü Departman ise, 3'üncü Departmanın savunmaya yönelik istihbarat toplama görevinin aksine en basitinden servis dışı bırakma, virüs ataklarının yanı sıra elektronik karşı taarruzu da içine dahil eden daha çok saldırı ve taarruzi faaliyetlerden sorumludur[365].

Çin Halk Kurtuluş Ordusunun siber birimlerinin haricinde siber uzayın savunulmasına yönelik çeşitli diğer örgütler de faaliyet göstermektedir. Bunlardan birisi olan ve "Siber Milisler" olarak bilinen; hackerlar, bilişim teknolojileri firmaları ve uzmanları, bilgisayar mühendisleri gibi personel yelpazesinden oluşan bu birimin esas görevi, direkt Çin Halk Kurtuluş Ordusuna bağlı olmadan Ulusal Acil Tatbikat Yapısının bir unsuru olarak askeri siber faaliyet alanlarında yer almaktır[366]. 8 milyondan daha fazla kişinin görev aldığının ifade edildiği ve bilinenin aksine daha çok savunmaya yönelik faaliyet yürüten söz konusu birim, siber savunma görevine ilişkin bir sivil-asker işbirliğinin bir parçası şeklinde görülmektedir[367].

### 4.2.4. Rusya

Estonya ve Gürcistan'daki küresel siber savaş olaylarının faili olarak ifade edilse de hiçbir zaman siber uzayın en büyük avantajlarından birisi olan kimliğin doğrulanamaması nedeniyle olaydan sorumlu tutulamayan Rusya, hem siber saldırı konusunda öncü ülkeler arasında yer almakta hem de siber tehditlerin hedefleri

---

[362] https://tr.sputniknews.com/savunma/201505261015665817 [04.04.2018].
[363] Mahzure Kara, **age**, 65.
[364] Nigel Inkster, "Chinese Intelligence Operations In The Cyber Age", **Survival Global Politics And Strategy**, c.55, s.1 (2013): 54.
[365] Mikk Raud, **China And Cyber: Attitudes, Strategies, Organisation** (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2016), 24.
[366] Mikk Raud, **age**, 26.
[367] Robert Sheldon ve Joe McReynolds, "Civil-Military Integration and Cybersecurity", **China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain** (Oxford: Oxford University Press, 2015), 196.

arasında üst sıralarda bulunmaktadır. Yapmış olduğu bu saldırılar, Rusya'nın aynı zamanda siber saldırı alanında ne kadar büyük bir tehdit olabileceğini tüm dünyaya göstermiştir. İlk siber savaşlar olarak kayıtlara geçen Estonya ve Gürcistan saldırılarının ardından birçok analist, Rus hükümetinin saldırıları gerçekleştirmek için suç örgütleri de dahil olmak üzere geniş bir siber gücü kullandığını öne sürmektedirler. Savaş sırasındaki saldırıların hedefleri, saldırganların Rus askeri gücü ile senkronizasyonu ele alındığında[368], bu hackerların devlet destekli olma ihtimalinden bahsetmek mümkündür.

Rusya, saldırıların arkasındaki faili ve siber saldırıların ülkeleri baskı altına alabileceğinin farkında olmasına rağmen siber savunma alanında bir faaliyette bulunmadığı izlenimi vermekte ve Savunma Bakanlığı sorumluluğu altında kurulması planlanan Siber Komutanlık için ağır davranmaktadır. Bunun nedeni Rusya'nın siber saldırı ve savunmaya ilişkin yeterli ve nitelikli personel veya faaliyet alanlarının bulunmaması değil; resmi olarak bunu kabul etmemesi[369], hatta belki de uluslararası platforma bu imajı vermek istememesidir. Bu görüşü doğrular nitelikte, Rusya'nın siber güvenlik doktirini saldırıdan ziyade savunmaya yönelik tedbirlere yoğunlaşmaktadır[370].

Rusya askeri anlamda siber savaşı, tarafların birbirlerine karşı bilgi elde etme üstünlüğü sağlama ve bu üstünlüğü elde bulundurma olarak görmektedir. Bu amaç, düşmanın bilgi sistemlerini, karar alma mekanizmalarını, komuta ve kontrol sistemlerini ve hatta toplumunu etkilemek üzere belirli seviyelerde bilgi teknolojileri kullanılarak gerçekleştirilmektedir[371].

Rusya'nın siber güvenlik konusundaki politik yaklaşımları ABD ve diğer Batı ülkelerinden farklıdır[372]. Uzmanlara göre ABD tarafından kullanılan "siber güvenlik" ve "siber uzay" kavramları yerine Rusya'da daha politik olduğu düşünülen "bilgi güvenliği" ve "bilgi alanı" terimleri kullanılmaktadır[373]. Teknoloji, Rusya'nın bilgi güvenliği anlayışının sadece bir parçasını oluşturmaktadır. 2016 tarihli Bilgi Güvenliği Doktrininde, "İnternet" kelimesi hiç yer almamaktadır. Rusya; bilgi güvenliğini, milletin bilgi ve kültürünün korunması ve bilginin serbest dolaşımı olarak tanımlamaktadır. Buna karşın, ABD'nin siber güvenlik politikası yerel teknolojileri,

---

[368] https://siberbulten.com/uluslararasi-iliskiler/rusya-siber-alanda-neden-saldiriyor [08.04.2018].
[369] Mahzure Kara, **age**, 69.
[370] https://www.rbth.com/defence/2017/01/12/russias-cyber-army-hacks-a-spot-in-the-top-5_679221 [08.04.2018].
[371] Steven A. Hildreth, **age**.
[372] https://www.jewishpolicycenter.org/2013/12/31/russian-cyber-capabilities [08.04.2018].
[373] Michael Connell ve Sarah Vogler, "Russia's Approach to Cyber Warfare", **CNA Analysis and Solutions**, https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf [08.04.2018].

aksamaya, yetkisiz erişime karşı veya başka herhangi bir tür müdahaleye karşı korumayı hedef almaktadır ki bu yaklaşım siber güvenliğin teknolojik boyutlarını vurgulamaktadır[374]. Söz konusu Rus Bilgi Güvenliği Doktrini; Rusya'nın ulusal stratejik öncelikleri doğrultusunda bilgi güvenliğine yönelik temel tehditlerin analizi, bilgi güvenliği durumuna yönelik değerlendirmeleri, stratejik hedeflerin belirlenmesi ve bilgi güvenliğinin idamesi için gerekli olan esasları içermekte, bilgi güvenliğine yönelik savunmanın da askeri ve politik gayretlerin ortak hareket etmesiyle sağlanabileceğine dikkat çekmektedir[375].

Teşkilatlanma açısından Rusya'nın siber faaliyet alanına ilişkin sorumlu olan organizasyonları şu şekildedir:

- Güvenlik Konseyi,
- Federal Güvenlik Hizmetleri,
- Federal Savunma Hizmetleri,
- Federal Teknik ve İhracat Hizmetleri,
- Bilgi Teknolojileri ve İletişim Bakanlığı[376].

Bir yandan siber güce ilişkin ordunun, medyanın ve akademik çevrenin etkisi tartışılırken diğer yandan da Rusya Federasyonu tarafından resmi olarak siber uzayın ulusal savunma planlaması ve askeri doktrin açısından ne kadar önemli olduğuna[377] vurgu yapılmaktadır. Her ne kadar siber savunma veya saldırıya ilişkin gizlilik veya devlet politikası gereği bu konuda kurulan askeri teşkilatlanmayla ilgili somut olarak bir bilgi açıklanmasa da, Savunma Bakanlığı adına çalıştığı bilinen hackerlara[378] ilave olarak 2017 yılında Savunma Bakanı tarafından Rus ordusu bünyesi içinde kurulduğu açıklanan siber ordunun; siber istihbarat da dahil olmak üzere siber alandaki operasyonel faaliyetlere yönelik olduğu ve özellikle propaganda amaçları için daha önce kullanılan her şeyden çok daha etkili bir araç olmasının beklendiği ifade edilmiştir[379]. Söz konusu birimin hedefleri veya teşkilatlanma esaslarına ilişkin herhangi bir ayrıntı verilmemesine rağmen[380] bu tür bir açıklama bile siber harekat alanına askeri yapılanmanın da dahil edildiğini ispatlamaktadır. Belirtilen hususlar dahilinde askeri yapılanmaya ilişkin çok tatmin edici somut verilere ulaşılamasa da savunma planlamaları açısından politika aracı olarak yer

---

374 Adem Kaya, **age**, 71.

375 The Securtiy Council Of Russian Federation, **Information Security Doctrine Of The Russian Federation**, https://toinformistoinfluence.com/2016/12/19/information-security-doctrine-of-the-russian-federation-6-december-2016 [08.04.2018].

376 Adem Kaya, **age**, 71.

377 Sergei A.Medvedev, **Offense-Defense Theory Analysis Of Russian Cyber Capability**, (Monterey/California: Dudley Knox Library, 2015), 55.

378 https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense [09.04.2018].

379 https://www.sabah.com.tr/aktuel/2017/02/23/rusya-yeni-bir-siber-ordu-kurdu [08.04.2018].

380 http://www.bbc.com/news/world-europe-39062663 [08.04.2018].

alan askeri gücün, siber saldırı ve savunma alanlarından ayrı olarak düşünülmesi pek de gerçekçi gözükmemektedir.

### 4.2.5. Ingiltere

İngiltere'nin özel olarak bir siber savunma stratejisi bulunmamasına paralel olarak, siber tehditler ne 2011 Ulusal Savunma Stratejisinde ne de 2010-2014 Savunma Planında öncelikli bir tehdit olarak tanımlanmamıştır. Ancak Ulusal Stratejik Savunma ve Güvenlik İncelemesinde, Savunma Bakanlığına yeni siber imkan ve kabiliyetlerin gelişimine öncülük etmek ve kritik altyapıların güvenliği için kendilerinin ve müttefiklerin siber faaliyetlerini destekleme görevi verilmiştir. Bu kapsamda, İngiltere Savunma Bakanlığı tarafından yürütülen askeri siber savunma faaliyet alanı; siber uzayın askeri amaçlarla kullanımının yanı sıra siber savunma politikası ve doktrini üzerine kurulmuştur[381].

Savunma ve Siber Güvenlik Raporuna göre silahlı kuvvetler, Savunma Bakanlığının siber alandaki hedeflerine ulaşması için belirlediği yol haritasının merkezinde bulunmaktadır. Özellikle son yıllarda askeri teşkilatlanma içerisinde siber savunmaya ilişkin yapılan düzenlemeler konunun öneminin her geçen gün daha da belirgin hale geldiğini göstermektedir. Bu kapsamda ulaşılan en güncel bilgilerden birisi olan hiç şüphesiz, Siber Savunma Okulu'nun açılışıdır. Siber savunmaya ilişkin büyüyen ilgisi ve gayretleri kapsamında, siber tehditlerden ulusal kaynaklara gelebilecek olan saldırılara karşı belirli bir mesafe kaydeden İngiltere, söz konusu gayretlere ilave olarak Shrivenham'daki Savunma Akademisi bünyesinde bir Siber Savunma Okulu açmıştır. Okulun açılışında konuşan Silahlı Kuvvetler Bakanı Mark Lancaster tarafından; İngiltere'ye yönelik siber tehditlerin sürekli arttmakta olduğu ve bu nedenle çok ciddiye alınması gerektiğini belirtilmiş, okulun açılış nedeninin de tam olarak bu tehditlere yönelik tedbirler geliştirebilecek, ulusal siber savunma sürecinde rol alabilecek çok daha fazla sayıda uzman personel yetiştirmek olduğunu ifade edilmiştir[382].

Belirtilen hususların yanı sıra Siber Savunma ve Güvenlik Programı için ayrılan 90 milyon sterlinlik bütçe[383] (2015 yılı için) siber tehditlerin savunma planlamalarına olan etkileri doğrular niteliktedir. Siber Savunma ve Güvenlik Programı 4 ana çalışma grubuna ayrılmıştır. Bunlar:

---

[381] Anna-Maria Osula, **National Cyber Security Organisation: United Kingdom** (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015), 13.
[382] https://www.gov.uk/government/news/uk-steps-up-cyber-defence [31.03.2018].
[383] Anna-Maria Osula, **age**, 13.

- Siber Farkındalık Grubu (Siber faaliyetlere yönelik planlama, eğitim, tatbikatların düzenlenmesi ve siber bilinci kazandırma),
- Siber Savunma Faaliyetleri Grubu,
- Siber İmkan ve Kabiliyetler Grubu (Siber alanda verilebilecek görevler için gerekli olan yetenekleri oluşturma),
- Geleceğin Siber Kuvvetleri Grubu (2020 ve sonrasına yönelik siber kuvvetlerin dizaynı) [384]. Söz konusu çalışma grupları arasında belki de en önemlisi olan, İngiltere'nin siber imkan ve kabiliyetlerinin daha esnek, ileri seviyede ve uygulanabilir hale dönüştürülmesi amacıyla kurulan Siber Savunma Faaliyetleri Grubunun, 2015 yılı itibarıyla tamamen operasyonel yeteneklere sahip hale geldiği belirtilmektedir[385].

### 4.2.6. Fransa

Günümüz dünyasında önemli bir risk olarak görülen siber saldırılara yönelik 2011 yılında 100 olan siber savunma uzmanı sayısını 2019 yılında 3 bine çıkarmak ve 4 bin 400 yardımcı uzman istihdam etmek için 1 milyar dolar ayıran Fransa'nın[386] bilgi sistemleri ve ağ altyapısının savunulmasına ilişkin görev ve sorumluluk Savunma Bakanlığına verilmiştir. Bu görevin yerine getirilebilmesi için Bakanlık bünyesinde yaklaşık 2000 personel görev yaptığı belirtilmektedir. Fransa'nın siber stratejisinin temel hedefleri; her şartta "Bilgiye hakim olma" konusunu garanti altına alabilmek ve ulusal savunma sistemlerini siber tehditlere ve siber saldırılara karşı korumaktır. Ancak Aralık 2017 tarihinde, Savunma Bakanı tarafından yapılan açıklamada; Genelkurmay Başkanlığına bağlı olarak Ocak 2018 ayından itibaren faaliyete geçecek olan ve yaklaşık 2.600 kişinin görev yapacağını bildirdiği Siber Operasyonlar Komutanlığının[387] kurulduğuna yönelik ifadeye rağmen çalışmanın son aşamasına kadar halen somut bilgiye ulaşılamamıştır.

Siber tehditlerin askeri yetenekler üzerindeki potansiyel etkileri ilk olarak 2009'da Fransız Deniz Kuvvetlerine ait sistemlere bulaşan Conficker virüsü ile tecrübe edilmiştir. Söz konusu olayın sonucunda Rafale jet uçakları, sistemdeki zaafiyetler çözülene kadar uçamamıştır[388]. Bu nedenlerden dolayı Fransa Savunma

[384] Anna-Maria Osula, **age**, 14.
[385] Anna-Maria Osula, **age**, 16.
[386] http://www.hurriyet.com.tr/dunya/fransadan-siber-ordu-icin-1-milyar-dolar-40421504, [04.04.2018].
[387] https://google.com.tr/amp/www.hurriyet.com.tr/amp/dunya/fransadan-siber-ordu-icin-1-milyar-dolar-40421504 [29.03.2018].
[388] Kim Willsher, "French Fighter Planes Grounded By Computer Virus", **The Telegraph**, 2009, https://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.htm [29.03.2018].

Bakanlığı, siber savunmaya ilişkin detaylı planlamaları içeren Müşterek Siber Savunma Doktrinini hazırlama gereği duymuştur. Ayrıca teşkilat olarak özellikle somut bir askeri nitelikte bir yapılanmaya rastlanılmamasına rağmen, Siber Savunma Hücresi adı altındaki birimin halihazırda, kurulduğu bildirilen Siber Operasyon Komutanlığı şeklinde görev yaptığı belirtilmektedir[389]. Söz konusu birimin ana vazifeleri şunlardır:

- Siber savunma çalışmalarını Savunma Bakanlığı ile koordine etmek,
- Planlama ve Operasyon Merkezi birimiyle birlikte siber operasyonları planlamak ve komuta etmektir. Söz konusu siber operasyonlar genel olarak savunmaya yönelik faaliyetleri içerse de sadece savunmadan ibaret değildir[390].

Siber savunma görevlerine yönelik olarak, askeri sistemlere yönelik bir siber tehdidi bertaraf etmek veya etkisini hafifletmek için operasyonel bir düzen kurulmuştur. Planlama ve Operasyon Merkezinin temel vazifesi siber faaliyetlerin planlama ve icra safhaları arasındaki entegrasyonun sağlanmasına öncülük etmektir. Fransa'nın siber savunma stratejisinde kilit rol oynayan bir diğer birim ise Savunma Tedarik Ajansıdır. 250 uzman personelden oluşan bu birim, gün geçtikçe Fransa'nın siber savunma mimarisinde daha önemli bir yere gelmektedir[391].

2014-2019 Siber Savunma Anlaşması ve Askeri Planlama Kanuna göre, siber harekat alanına ilişkin çalışmalar, gayretler muazzam boyutlara yönelmektedir. Bunun sonucu olarak, ilerleyen yıllarda karşılaşılabilecek yeni tehdit türlerine yönelik siber yeteneklerin geliştirilmesi ve askeri operasyonların verimli bir şekilde desteklenmesi amaçlanmaktadır[392].

### 4.2.7. Israil

İsrail'in siber savunmadan sorumlu dört kuruluşu bulunmaktadır. Bunlardan ilki olan İsrail Savunma Kuvvetlerine bağlı, “Birim 8200” adı verilen, askeri personelden oluşan teşkilatın, siber savaşa ilişkin belirlediği ve gayretlerini yönelttiği alanlar; istihbarat toplama, savunma ve saldırıdır[393]. “Birim 8200” aynı zamanda yetişmiş, donanımlı personel temin etme konusunda akademik bir rol de üstlenmekte, eğittiği

[389] Pascal Brangetto, **National Cyber Security Organisation: France** (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015), 11.
[390] Pascal Brangetto, **age**, 11.
[391] Pascal Brangetto, **age**, 12.
[392] Jean-Marie Bockel, "The State Of Europe's Defence Industrial Base", NATO Parliamentary Assembly, https://www.nato-pa.int/download-file?filename=sites/default/files/201711/2017%20%2016%20E%20bis%20%20EUROPE%20INDUSTRIAL%20DEFENSE%20BASE%20-%20BOCKEL%20REPORT.pdf [30.03.2018].
[393] James A. Lewis ve Katrina Timlin, **Cybersecurity and Cyberwarfare 2011** (Center for Strategic and International Studies/US: UNIDIR Resources, 2011), 14-15.

personeli istihbarat ve siber güvenlik alanlarında çeşitli birimlerde görevlendirmektedir[394].

İsrail'in siber güvenlik stratejisi içerisinde ülke içindeki bilgi sistem ağlarının güvenliği, ulusal altyapı ve hükümet sistemlerinin savunmasını sağlama görevi ise iç istihbarat kurumu Shin Bet'in görevidir. Başlangıçta İsrail Savunma Kuvvetlerinin (IDF) bir alt birimi olarak 1948 yılında kurulmuş olan Shin Bet, ilerleyen süreçte Başbakanlığa bağlanmıştır. Söz konusu birim; komuta, kontrol, haberleşme, bilgisayar ve istihbarat (C4I) sistemlerinin tamamı ile iletişim ve siber savunma faaliyetlerinden sorumludur[395].

2009 yılında askeri istihbarat ve C4I Müdürlüğü arasında işbirliğini geliştirmek için kurulan ve "Matzov" olarak bilinen üst düzey Kriptolama ve Bilgi Merkezi, teknolojik istihbarat sağlamak ile sorumludur. Bunun haricinde; hükümetin, ordunun ve büyük şirketlerin bilgi sistem ağlarını korumak da görevlerinin arasında yer almaktadır. Ayrıca IDF, Shin Bet, MOSSAD gibi kritik birimlerin ağlarının yanı sıra elektrik, su ve telefon gibi önemli alanlarda faaliyet gösteren büyük şirketlere destek vermek, kod yazmak ve şifreleme yapmak da Matzov'un görev ve sorumluluk alanına girmektedir.

Bu üç kurumun haricinde 2012 yılının başlarında kurulan İsrail Ulusal Siber Bürosu (Israel National Cyber Bureau-INCB), İsrail'in siber savunmaya ilişkin rolü bulunan bir diğer birimidir. Bilgisayar sistemlerindeki saldırılara karşı ülkeyi savunmak için kurulan INCB; güvenlik sisteminin, iş dünyasının ve akademi dünyasının işbirliğiyle savunma sistemini organize etmeyi amaçlamaktadır[396]. Buna ilave olarak, ülkenin uğradığı siber saldırılarda, kurumlar arasında koruyucu önlemler alarak, siber savunma faaliyetlerini koordine etmektedir. Tel Aviv Üniversitesi Ulusal Güvenlik Çalışmaları Enstitüsü de çalışmalarını; saldırı, savunma ve istihbarat alanında yürütmektedir[397].

İsrail'in avantaj sağladığı belki de önemli özelliği, kritik altyapı sistemlerinin siber tehditlerden etkilenmemesi için hassas ve gizli bilgilerini internetten bağımsız olarak, izole bir şekilde taşımasını sağlamasıdır. İnternet üzerinden gelebilecek siber tehditlere karşı kendini kapayarak kritik milli sistemlerinin güvenliğini sağlamayı hedeflemektedir. Yaptıkları saldırılarla ülkelerin güvenlik açıklarını tespit etme fırsatı

[394] İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, "Siber Güvenlik Raporu", İstanbul, 2012, 39.
[395] İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, **age**, 39.
[396] Cabinet Briefed On The Israel National Cyber Bureau, http://www.pmo.gov.il/English/MediaCenter/Spokesman/Pages/spokecyber111112.aspx [03.04.2018].
[397] İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, **age**, 39

bulan RedHack grubu, İsrail'in sızmalara karşı üst seviyede hazırlıklı olduğunu, herhangi bir girişime izin vermediğini ve güvenliğinin güçlü olduğunu belirtmiştir[398].

İsrail'in siber harekat alanına ilişkin faaliyetleri ve teşkilatlanması kapsamında, İsrail Savunma Kuvvetleri (IDF)'nin; siber faaliyetlerin komuta yetkisi ve altyapının kurulması süreci ile birlikte askeri siber stratejinin önemli bir parçası olarak ilişkilendirildiği belirtilmektedir[399]. 2015 yılında alınan kararla ayrı bir Siber Komutanlık kurulmasına yönelik hedefleri bulunsa da, 2017 yılı itibarıyla buna gerek görülmemiş ve ilerde tekrar görüşülmek üzere söz konusu teşkilat planı rafa kaldırılmış, müteakip dönemde ise yapılan yeniden sorgulama neticesinde IDF haricinde bağımsız bir siber komutanlık fikrinin gerekli olmadığı kanaatine varılmıştır[400]. Teşkilatlanma konusunun haricinde, İsrail'in askeri siber güvenliğe yönelik icra edilen birçok faaliyetlerine ilave olarak muhtelif zamanlarda, siber savunma kabiliyetlerini ve siber saldırılara hazırlık durumlarını test etme olanağı veren IDF Siber Savunma Tatbikatlarının icra edildiği[401] bilgisine ulaşılmıştır.

### 4.2.8. Estonya

Bilindiği üzere Estonya'nın dünya kamuoyunda yer alan ilk siber saldırılara maruz kalan ülkeler arasında yer alması nedeniyle çalışmanın bu bölümüne yönelik siber savunma tedbirleri ve teşkilat yapısına ilişkin özellikle incelenme gereği duyulmuştur. Bu kapsamda 2010 tarihli Ulusal Güvenlik Konseptine göre, siber tehditlerin toplumda çok ciddi tahribatlara yol açabilecek bir potansiyele sahip[402] olduğuna vurgu yapılmaktadır. Benzer şekilde, Estonya'nın Ulusal Güvenlik Politikası Temel Prensibi'nde, siber güvenliğin gelişimine ilişkin kilit hususların ülkeyi hedef alan yabancı kaynaklı istihbarat ile mücadele[403] olduğuna işaret edilmektedir.

Ulusal savunma konusunun bir alt başlığı olarak değerlendirilen siber savunmaya ilişkin koordine yetkisi Savunma Bakanlığına verilmiştir[404]. Savunma

---

[398] İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, **age**, 40.
[399] Meir Elran ve Gabi Siboni, "Establishing An IDF Cyber Command", **INSS**, Insight No: 719 (2015): 1.
[400] Anna Ahronheim, "IDF Decides Not To Have A Cyber Command Department", **Israel News**, 2017, https://www.google.com.tr/amp/m.jpost.com/Israel-News/IDF-decides-not-to-have-a-cyber-command-department-477169/amp [30.03.2018].
[401] Deborah Housen-Couriel, **National Cyber Security Organisation: Israel** (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2017), 14.
[402] Riigikogu, "National Security Concept Of Estonia", http://www.eda.europa.eu/docs/default-source/documents/estonia--national-security-concept-of-estonia-2010.pdf [31.03.2018].
[403] Riigikogu, Approval Of The Main Guidelines Of Estonia's Security Policy Until 2015, http://siseministeerium.ee/29744 [31.03.2018].
[404] Estonian Ministry Of Defence, "Estonian Defence Strategy" http://www.kmin.ee/files/img/files/KM_riigikaitse_strateegia_eng(2).pdf [31.03.2018].

Bakanlığının konuya ilişkin işlevi; ulusal savunma planlanmasına yönelik önerilerde bulunmak, planlanan faaliyetleri icra etmek ve askeri teşkilatlanmayı da içeren ulusal savunmayı organize etmektir. 2014 Şubat ayında yine Savunma Bakanlığı bünyesi altında özel olarak siber politika üzerine ayrı bir birim daha kurulmuştur. Söz konusu birim, siber güvenlik konusunun teknik ve siyasi hususlarını da içine dahil eden, bilgi sistemlerinin ve bilgi teknolojilerinin gelişimine ilave olarak Savunma Bakanlığınca alınan kararların uygulanması konularından sorumludur. Estonya, NATO Siber Koalisyonu gibi büyük çaplı, müşterek siber tatbikatların düzenlenmesinde de görev almaktadır[405].

Teşkilatlanma konusu incelendiğinde, Estonya Savunma Kuvvetlerinin yapısal bir birimi olan Muhabere Taburunun görevleri arasında; Savunma Kuvvetlerinin sabit ve hareketli halde stratejik haberleşme ihtiyacının karşılanması ve bilgi sistemlerinin işletilip idame edilmesi ve güvenliğinin sağlanması hususlarının yer aldığı görülmektedir. Estonya ayrıca, NATO'nun 2008'den beri her yıl icra edilen, uluslararası askeri bir faaliyeti olan ve NATO üye ülkelerin siber savunma kabiliyetlerini deneme imkanı buldukları siber savunma tatbikatlarına ev sahipliği yapması bakımından üye ülkelerden dahi siber savunma konusunda fayda sağlamaya gayret göstermekte, ciddi bilgi ve tecrübeler edinmektedir[406].

Savunma Bakanlığının ve bünyesindeki birimlerin gayretlerinin haricinde, ulusal siber savunma konusu 2007'deki olaydan sonra kurulan Estonya Savunma Ligi'nin Siber Savunma Birimi tarafından da önemli ölçüde desteklenmektedir[407]. Söz konusu organizasyon, özel ve kamudan gönüllü siber güvenlik uzmanlarından oluşan ve amaçları Estonya'nın kritik altyapılarını ve bilgi sistemlerini siber uzaydan gelebilecek olan saldırılara karşı korumak olan bir ulusal savunma örgütüdür. Katılımcıların askeri emir-komuta zincirine bağlı olarak hareket ettikleri, başında aktif olarak görevde bulunan tabur ve üstü seviyede komutanların bulunduğu ancak katı kuralları olmayan ve kendi işine ait günlük mesaisinin dışındaki zamanlarda söz konusu Savunma Ligi'nin bir üyesi olarak görev yapan gönüllülerden oluşan ve katılımcıların herhangi bir ücret almadığı, Estonya'ya özel bir savunma birimi olup[408] temel vazifeleri;

- Gönüllü siber güvenlik uzmanları arasındaki işbirliği ve dayanışmayı geliştirmek,

---

[405] Anna-Maria Osula, **National Cyber Security Organisation: Estonia** (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015), 9.
[406] Anna-Maria Osula, **age**, 10.
[407] Anna-Maria Osula, **age**, 10.
[408] Sharon L.Cardash and Frank J.Cilluffo, "Estonia's Cyber Defence League: A Model For The United States", **Studies in Conflict & Terrorism**, s.36 (2013): 778-779.

- Kritik bilgi altyapılarına yönelik siber güvenlik seviyesini arttırmak,
- Bilgi sistemleri güvenliğine yönelik eğitim ve tatbikatlar icra etmek,
- Uluslararası siber güvenlik faaliyetlerine (eğitim, tatbikat, yarışma vb.) katılım sağlamaktır[409].

Siber savunmaya ayrılan bütçenin boyutu somut olarak yeterli olmasa da Savunma Bakanlığı, Estonya Savunma Ligi'nin Siber Savunma Birimi ve NATO Müşterek Siber Savunma Mükemmeliyet Merkezi arasında kurulan sinerji ve ortak çalışma sayesinde siber savunmanın ulusal ve uluslararası boyutta öncelik taşımaya devam edeceğini belirtmektedir[410].

### 4.2.9. Türkiye

Siber Savunma Mükemmeliyet Merkezi tarafından açıklanan ülkelerin siber imkan ve kabiliyetlerinin, teşkilatlarının yer aldığı raporlarda Türkiye ile ilgili herhangi bir bilgiye rastlanılmamakla beraber söz konusu konuların gizlilik dereceli olması nedeniyle açık ağda yer alan bilgiler, konuya ilişkin önceden yapılan çalışmalar ve özellikle Ulaştırma, Denizcilik ve Haberleşme Bakanlığı sorumluluğunda hazırlanarak yürürlüğe giren ve siber tehditlerin planlamalara dahil edilmesine rehber olan Ulusal Siber Güvenlik Stratejileri ve Eylem Planları incelenerek Türkiye'nin bu konudaki durumu ortaya konmaya çalışılmıştır.

Yakın tarihteki örneklerinde yola çıkılarak etkilerinin görülmesiyle birlikte işin ciddiyeti daha da anlaşılmış, siber alanda oluşan bütün bu tehditlere karşı devlet, kurum ve bireylerin bilinç seviyesi arttıkça uluslararası kuruluşlar ve devletler bazında tedbire yönelik birtakım girişimler oluşmaya başlamıştır[411]. Ülkemiz adına ise bu yönde atılan yazılı alandaki ilk adım, 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planıdır. Söz konusu planın; gelişen süreç içerisindeki tespitler, geri bildirimler ve değişen tehdit çeşitleri neticesinde güncellenmesine ihtiyaç duyulmuş ve en son haliyle 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı olarak ulusal manadaki siber rehber olarak yürürlüğe girmesi sağlanmıştır. Bu kapsamda ülkemiz açısından siber tehditlere ilişkin adılan atımlar ve mevcut en güncel yazılı doküman olan 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem

[409] www.kaitseliit.ee/en/cyber-unit [31.03.2018].
[410] Estonian Ministry Of Defence, "National Defence Development Plan 2013-2022", http://www.kaitseministeerium.ee/sites/default/files/sisulehed/kaitse-eelarve/national_ defence_development_plan_2013.pdf [31.03.2018].
[411] Chris Connoll ve diğ., "An Overview of International Cyber-Security Awareness Raising and Educational Initiatives", www.galexia.com/public/research/assets/gc381_acma_ cybersecurity_publication_version_20110517_galexia_web/print-index.html [01.02.2018].

Planı üzerinden, bir tehdit olarak ulusal manada strateji oluşturulma ihtiyacı duyulan siber tehditlere ilişkin hususlardan bahsedilecektir.

#### 4.2.9.1 Türkiye'nin Siber Güvenlik Stratejisi

Bilgi ve iletişim teknolojilerinin toplumun ve ekonominin ayrılmaz bileşenleri olduğu ve kalkınmaya önemli katkılar sağladığı artık bir gerçektir. Ülkemizde bilgi ve iletişim sistemlerinin kullanımı kamu kurumlarında, özel sektörde ve vatandaşlara ilave olarak; enerji, su kaynakları, sağlık, ulaşım, haberleşme ve finansal hizmetler gibi kritik altyapı sektörlerinde faaliyet gösteren kurum ve kuruluşlarda da hızla yaygınlaşmaktadır. Bilgi ve iletişim teknolojileri, özellikle de internet kullanımı siber uzaydaki tüm bileşenlerin birbiriyle bağlantılı olması nedeniyle bir bakıma siber güvenlik risklerini ve belirsizlikleri de beraberinde getirmektedir[412].

Kurum ve kuruluşlarının hizmet sunumlarında bilgi ve iletişim sistemlerini her geçen gün daha fazla kullanmaları nedeniyle, söz konusu bilgi ve iletişim sistemlerinin güvenliğinin sağlanması hem ulusal güvenliğin, hem de rekabet gücünün önemli bir boyutu haline gelmiştir. Bilgi ve iletişim sistemlerindeki mevcut veya sonradan ortaya çıkan güvenlik zafiyetleri; bu sistemlerin hizmet dışı kalmasına veya kötüye kullanılmasına, can kaybına, büyük ölçekli ekonomik zarara, kamu düzeninin bozulmasına ve/veya ulusal güvenliğin ihlaline neden olmasına sebebiyet verebilmektedir. Siber saldırılar neticesinde ortaya çıkan maddi zararlar çok ciddi boyutlara ulaşmaktadır[413]. Öyle ki başarıya ulaşan bir siber saldırının verebileceği ekonomik zarar, önceki bölümlerde değinilen mevcut verilerden de görüldüğü üzere ulusal manada ciddi krizlere sebep olabilecek seviyelere gelebilmektedir.

Siber uzay bilişim sistemlerine ve bilgi/veriye yapılan saldırılar için anonimlik ve inkâr edilebilirlik gibi fırsatları sunmaktadır. Bilişim sistem ve verilerini hedef alan ısrarcı ve gelişmiş siber saldırıların kimler tarafından finanse ve organize edildiğinin, yani failinin tespiti nerdeyse imkânsızdır. Bu nitelikler siber uzaydaki risk ve tehditlerin asimetrik karakterini ortaya koymakta ve siber tehditlerle mücadeleyi de güçleştirmektedir.

Siber güvenliğin bu denli belirsizliklerle dolu bir ortamda kesin olarak sağlanmasından bahsedilememekte, bunun yerine siber güvenlik risklerinin yönetilebilir ve kabul edilebilir seviyelerde tutulması hedeflenmektedir. İnternet gibi

[412] Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, **2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı** (Ankara, 2016), 5-6.
[413] Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, **age**, 8.

açık bir ortamda bulunmanın artan erişilebilirlikle birlikte bazı riskleri de getireceği bir gerçektir. Bu risklerin topyekün katılımlı bir yaklaşımla yönetilerek siber olaylara karşı hazırlıklı olunması ve bu olaylardan en az zararla çıkılması amacını içeren ulusal siber güvenlik stratejisi gereğince; ulusal siber güvenliğin sağlanmasına ilişkin politika, strateji ve eylem planlarını hazırlama ve koordinasyonunu sağlama görevi Ulaştırma, Denizcilik ve Haberleşme Bakanlığına verilmiştir[414].

Bu kapsamda atılan başlangıç adımları tarih sırasıyla şu şekildedir:

- Temmuz 2012: Siber Güvenlik Enstitüsünün Kurulması,
- Ağustos 2012: Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ve TÜBİTAK işbirliği ile Siber Güvenlik Projeleri,
- Eylül 2012: TSK Siber Savunma Merkezinin Kurulması,
- Ekim 2012: Siber Güvenlik Kurulunun Kurulması,
- Aralık 2012: Siber Güvenlik Kurulu İlk toplantısının Yapılması,
- Ocak 2013: UDHB Siber Güvenlik Dairesinin Kurulması,
- Şubat 2013: Siber Güvenlik Değerlendirmesinin Yapılmasıdır[415].

Ülkemizde Siber Güvenliğe ilişkin sürecin çok yakın tarihli olduğu görülmektedir. Söz konusu başlangıç adımlarını neticesinde ortaya çıkarılan ve doküman bazında siber güvenliğe ilişkin ilk ulusal rehber olarak değerlendirilen, içeriğinde genel olarak 2013-2014 döneminde gerçekleştirilmesi planlanan hedeflere ilave olarak bu yılları aşan periyodik faaliyetler ile eğitim ve bilinçlendirme çalışmaları gibi sürekli yürütülmesi gereken faaliyetlere yer veren Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, Siber Güvenlik Kurulunu oluşturan üye kurumların çalışmaları ve fikir alışverişleri neticesinde 20/06/2013 tarih, 28683 sayılı Resmi Gazete'de yayınlanarak yürürlüğe girmiştir. Burada asıl dikkat edilmesi gereken husus, Siber Güvenlik Kurulunda bulunan makamlardır. Çünkü önceki bölümlerde de belirtildiği üzere savunma ve güvenlik planlamaları sadece askeri değil, devletin topyekün katılımları ve özellikle siyasi iradeyle ortaya çıkarılmalıdır. Bu kapsamda söz konusu kurulun;

- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB)
- Dışişleri Bakanlığı
- İçişleri Bakanlığı
- Milli Savunma Bakanlığı (MSB)

[414] Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, **age**, 9.
[415] M.Yasir Şentürk, "E-Devlet ve Siber Güvenlik: Uluslararası Değerlendirme", Türk Hava Kurumu Üniversitesi E-Devlet ve E-Dönüşüm Konulu Sunum Yansıları, afyonluoglu.org/PublicWebFiles/Lectures/ECE581/ECE581Siber%20Güvenlik%20ve%20Uluslararasi%20Degerlendirme.pdf [10.03.2018].

- Kamu Düzeni ve Güvenliği Müsteşarlığı
- Milli İstihbarat Teşkilatı (MİT)
- Genelkurmay Başkanlığı
- Bilgi Teknolojileri ve İletişim Kurumu (BTK)
- Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)
- Mali Suçları Araştırma Kurulu
- Telekomünikasyon İletişim Başkanlığı (TİB) temsilcilerinden oluşan[416] uzman bir heyet tarafından hazırlandığı görülmektedir.

Gelişen bilgi ve iletişim teknolojileri, artan güvenlik gereksinimi ve edinilen tecrübeler doğrultusunda, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından ulusal siber güvenlik stratejisinin güncellenmesi ve 2016-2019 dönemini kapsayan eylemlerin belirlenmesi ihtiyacı doğmuştur. Bu kapsamda öncelikle eski eylem planında sorumlu veya ilgili olarak yer alan kurumlarla (Siber Güvenlik Kurulunda görevli) 10 Mart - 7 Nisan 2015 tarihlerinde yedi adet değerlendirme toplantısı yapılmıştır. Toplantılarda eski eylem planında yer alan faaliyetlerin gerçekleştirilme durumları ile karşılaşılan güçlüklere ek olarak ileriye dönük değerlendirmeler ve siber güvenlik kapsamında gerçekleştirilmesi gereken faaliyetler de detaylı olarak belirlenmiş ve kaydedilmiştir. Toplantıların ardından kamu kurumları, kritik altyapı işletmecileri, bilişim sektörü, üniversiteler ve sivil toplum kurumlarını temsilen 73 kurum ve kuruluştan toplam 126 uzmanın katılımı ile Ortak Akıl Platformu gerçekleştirilmiştir. Söz konusu platform çalışmaları kapsamında; Türkiye'nin siber güvenlik boyutunda güçlü ve zayıf yönlerinden hareketle stratejik amaçları ve gerçekleştirmesi gereken eylemler belirlenmiştir[417].

Siber Güvenlik konusu özellikle 2008 yılından itibaren AB (Avrupa Birliği), OECD (Ekonomik İşbirliği ve Kalkınma Teşkilatı) ve NATO (Kuzey Atlantik İttifakı) gibi uluslararası kuruluşlara ilave olarak tüm gelişmiş ülkelerin de gündemine girmiştir. 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı hazırlanırken gerçekleştirilen çalışmalara ilave olarak arka planda detaylı bir kaynak taraması da yapılmış; Amerika, Avrupa ve Uzak Doğu'dan çok sayıda ülkenin siber güvenlik stratejileri gözden geçirilerek, ülkelerin siber güvenlik alanındaki, hedefleri, öncelikleri, teşkilatlanma esasları, kaynak tahsisleri, Ar-Ge (Araştırma ve Geliştirme), kamu-özel sektör işbirliği, eğitim gibi başlıklarda üretmeye çalıştığı çözümler değerlendirilmiştir[418]. Tüm bu çalışmalar kapsamında üretilen bilginin toplanması, incelenmesi ve değerlendirilmesi sonucunda "2016-2019 Ulusal Siber

[416] Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, **2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı** (Ankara, 2013), 1-2.
[417] Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, **age**, 10.
[418] Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, **age**, 11.

Güvenlik Stratejisi" ve "2016-2019 Ulusal Siber Güvenlik Eylem Planı" hazırlanmıştır.

"Ulusal siber güvenliğin sağlanması amacıyla, etkin ve sürdürülebilir politikaları belirlemek, koordinasyonu sağlamak ve uygulanmasını gerçekleştirmek" söz konusu dokümanın misyonu, "Toplumun refahı ve güvenliği ile ülke ekonomisinin büyümesine ve verimliliğine katkı sağlamak üzere bilgi ve iletişim teknolojilerinden en etkin şekilde faydalanılabilmesi için, siber güvenlikle ilgili tüm paydaşların işbirliği içinde siber uzaydaki riskleri yetkin bir biçimde yönettikleri, siber güvenlik alanında uluslararası rekabet gücüne sahip bir eko-sistemin oluşması" ise vizyonu olarak belirlenmiştir. 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planının ana amacı ise; siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olduğu anlayışının tüm kesimlerde yerleşmesi, ulusal siber uzayda bulunan sistem ve paydaşların tamamının güvenliğini sağlamak üzere idari ve teknolojik önlemlerin alınmasını sağlayacak yetkinliğin eksiksiz bir şekilde kazanılmasıdır[419].

Siber güvenliğin sağlanmasına ilişkin ilkeler, siber güvenlik riskleri, siber güvenlik amaçları ve eylemleri, siber savunmanın güçlendirilmesi ve kritik altyapıların korunması, siber suçlarla mücadele, farkındalık ve insan kaynağı geliştirme, siber güvenlik ekosisteminin geliştirilmesi ve son olarak da siber güvenliğin milli güvenliğe entegrasyonu ana ve alt başlıklarını içeren plan, ulusal manada siber güvenliğe ilişkin çok ayrıntıya inilmese de genel bir konsept belirlemesi açısından rehber niteliği taşımaktadır.

#### 4.2.9.2. Türkiye'nin Siber Güvenlik Stratejisinin Diğer Ülkelerle Kıyaslanması

Dokümanın hazırlanma sürecinde diğer ülkeler tarafından yayınlanan Siber Güvenlik Stratejileri de detaylı olarak incelendiği ve söz konusu dokümanlarda belirtilen hususlar ve risk olarak belirlenen hususların irdelenmesinin yapıldığı ve 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında yer bulduğu ifade edilmektedir. Bu kapsamda, diğer ülke strateji belgelerinde dikkat çekilen risklerden en önemlilerinin; kişisel ve kurumsal manada sosyal ağlara bağımlılığı, artan siber tehditler ve siber saldırılar, eğitimli ve nitelikli personel yetersizliği, kurumlar arası işbirliği ve koordine eksiklikleri ile ekonomik kaygılar olarak ön plana çıktığı görülmektedir.

[419] Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, **2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı** (Ankara, 2016), 5-6.

Konuya ilişkin olarak Tablo 9'da verilen ENISA (European Network and Information Security Agency) kriterlerine göre İngiltere, ABD ve Türkiye'nin Siber Güvenlik Stratejilerinin Karşılaştırılması ile Türkiye'nin Siber Güvenlik stratejisine yönelik olarak İngiltere ve ABD'nin Siber Güvenlik Stratejileri üzerinden bir kıyaslama yapmak suretiyle siber tehditlere ilişkin hazırlık durumumuz, konuya bakış açımız ve önem derecemiz hakkında daha elle tutulur değerlendirmeler yapmak mümkün olacaktır.

**Tablo 9: ENISA Kriterlerine Göre USGS'lerin Karşılaştırılması**

| S.No. | Görevler | İngiltere | ABD | Türkiye |
|---|---|---|---|---|
| 1 | Vizyonu, kapsamı, hedefleri ve öncelikleri belirleme | + | + | - |
| 2 | Ulusal risk değerlendirmesi yaklaşımını takip etme | + | + | - |
| 3 | Hâlihazırdaki politika, mevzuat ve kapasiteleri dikkate alma | + | + | + |
| 4 | Şeffaf bir yönetim yapısı geliştirme | + | + | - |
| 5 | Paydaşları belirleme | + | + | + |
| 6 | Güvenilir bilgi paylaşım ortamı sağlama | + | + | - |
| 7 | "Ulusal Siber Acil Durum Planları" oluşturma | + | + | + |
| 8 | Siber Güvenlik tatbikatları icra etme | + | + | + |
| 9 | Temel güvenlik gereksinimlerini oluşturma | + | + | - |
| 10 | Olay raporlama mekanizmalarını oluşturma | + | + | + |
| 11 | Kullanıcı farkındalığı | + | + | - |
| 12 | Ar-Ge'yi teşvik etme | + | + | - |
| 13 | Eğitim programlarını güçlendirme | + | + | - |
| 14 | Acil durum müdahale kapasitesini oluşturma | + | + | + |
| 15 | Siber suçu tespit edebilme | + | + | - |
| 16 | Uluslararası işbirliği sağlama | + | + | - |
| 17 | Kamu-özel sektör işbirliği sağlama | + | + | - |
| 18 | Güvenlik ve mahremiyeti dengeleme | + | + | + |
| 19 | Değerlendirme | + | + | - |

Akın Aytekin, "Türkiye'nin Siber Güvenlik Stratejisi ve Eylem Planının Değerlendirilmesi" (Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, 2015), 138.

Siber güvenliğin ve buna yönelik olarak yapılacak olan savunma planlamalarının ulusal güvenlik politikasının bir parçası olması sağlanmalıdır.

Tablo 9'da da görüldüğü üzere; her üç ülke de mevcut politikaların üzerine USGS'lerini inşa etmiştir[420]. Siber güvenlik stratejisi hazırlanırken kritik altyapılar öncelikli olarak dikkate alınmalıdır. Bu adımda yapılması gereken en önemli husus kritik sektör ve altyapıların tanımlanması ve bunlara yönelik planların hazırlanmasıdır. İngiltere'de kritik altyapı sektörleri tam anlamıyla tanımlanmış ve bunlarla ilgili sorumlu kurum teşkil edilmiştir. ABD'de kritik altyapılara ilişkin özel yasa çıkarılmış, ayrılan bütçe bu yasa ile belirlenmiş ve konunun sorumlu olduğu bakanlık tarafından diğer kuruluşlara görevler verilmiştir. Türkiye'de ise kritik altyapılarla ilgili somut olarak sorumlu bir kurum bulunmamakla birlikte, bu tesislerin neler olduğu yasal mevzuat kapsamına alınmamıştır[421].

2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında belirtilen eylem maddelerinde hangi kurum/bakanlık/kuruluşa hangi görevin verildiği açıkça belirtilmiştir fakat USGS'nin ekonomik boyutu ve bütçelendirmesi ile ilgili açıklanan hiçbir hususa rastlanılmamaktadır. İngiltere ve ABD'de ise sorumlu kurumlar tarafından, her sene bütçeden ne kadar payın hangi konu için ayrılacağı belirlenmiştir[422].

AFAD tarafından icra edilen Kritik Altyapılar ve Siber güvenlik grup çalışmasında; ulusal kritik altyapılarını korumak maksadıyla Kritik Altyapıları Koruma Planı geliştirilmesi ve Ulusal Kritik Altyapılar belirlenirken dikkate alınacak faktörlerin, kapsam ve riskin boyutu olduğu belirtilmiştir[423]. Bu kapsamda, kritik altyapılarla ilgili büyük siber saldırıların yaşanma ihtimaline karşı acil müdahale ve kurtarma sürecinde geçici tedbirler ve yapılar oluşturulması gerekmektedir. Her üç ülkenin de acil durum planları mevcuttur, fakat Türkiye'de pek çok kurumun felaket kurtarma merkezleri henüz teşkil edilmemiştir. Ayrıca, AFAD tarafından icra edilen Kritik Altyapılar ve Siber güvenlik grup çalışmasında; ulusal kritik altyapılarını korumak maksadıyla Kritik Altyapıları Koruma Planı geliştirilmesi ve Ulusal Kritik Altyapılar belirlenirken dikkate alınacak faktörlerin, kapsam ve riskin boyutu olduğu belirtilmiştir.

Farkındalığın artmasıyla kişi ve kurumlar siber uzaydaki hareketlerini ve kendilerini nasıl savunacaklarını, neyi, kimden ve ne tür yöntemlerle koruyacaklarını öğrenirler. Organizasyon içinde veya dışında güvenlik ile ilgili farkındalık yaratma aktivitelerinin gerçekleştirilmesi hususu önemlidir. Örneğin; İngiltere ve ABD'de her

[420] Akın Aytekin, **age**, 132.
[421] Akın Aytekin, **age**, 131.
[422] Akın Aytekin, **age**, 133.
[423] T.C. Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı, **2014-2023 Teknolojik Afetler Yol Haritası Belgesi** (Ankara, 2014), 69-70.

yılın Ekim ayı, siber güvenlik farkındalık ayı olarak kutlanmaktadır, fakat ülkemizde bu şekilde bir uygulama şu an için mevcut değildir[424].

Esasen 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında, belki de ilk yazılı doküman olması nedeniyle daha ayrıntılı olarak belirtilen görevler, hedefler ve bunlardan sorumlu kurum/kuruluşlardan, 2016-2019 planında bir önceki plana atıf yapılarak daha genel olarak belirtilmiştir. Aradan geçen dönem göz önünde bulundurulduğunda ilk planda belirlenen eylemlerin büyük bir bölümüne yönelik çalışmalar yapılmış ve somut olarak adımlar atılmıştır. Kurumsal ve Ulusal işbirliklerine önem verilmiş, eğitim programları planlanarak uygulamaya konulmuş, yarışma, tatbikat ve kamplar düzenlenmiş, çeşitli projeler/Ar-Ge faaliyetleri yürütülmüş, altyapılarla ilgili düzenlemelere gidilmiştir. Özetle; siber güvenliğin bir ulusal güvenlik unsuru olarak değerlendirilerek Milli güvenliğe entegre edilmesine yönelik birçok çalışma yapılmıştır. Ancak, bir önceki bölümde verilen sayısal veriler ile siber güvenliğe ilişkin yapılan faaliyetlerin tarihçesi ve Tablo-9 üzerinden İngiltere ve ABD Siber Güvenlik Stratejileri ile kıyaslanıldığı üzere, gerek ülkemizin siber tehditler için cazibe merkezi olarak görülmesi gerekse internete olan bağımlılığın son yıllarda ciddi şekilde artması nedeniyle hala ciddi eksikler olduğunu söylemek mümkündür. Bu kapsamda, 2016-2019 Siber Güvenlik Stratejisi ve Eylem Planı detaylı olarak incelenmesine rağmen somut olarak yer almadığı görülen, bir önceki hedeflere yönelik tespit edilen hedeflere hangi oranda ulaşılabildiği ve şu anki durumu ortaya koyan bir çalışmanın veya bir değerlendirme raporunun, aradan geçen süre içerisindeki değişimi ve gelişimi görmek açısından faydalı olabileceği değerlendirilmektedir.

#### 4.2.9.3. Diğer Hususlar

Çalışmanın şimdiye kadarki bölümünde incelenmiş olan diğer ülkelerin siber tehditlere karşı bakış açıları ve savunma planlamalarına olan etkilerinin haricinde; Türkiye'nin siber güvenliğe ilişkin stratejileri ve 2013-2014, müteakiben de 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı çatısı altında şekillenen hususlar, siber tehditlerin ülkemiz açısından savunma planlamalarında gerçekleşen dönüşümene ölçüde etkide bulunduğunun kanıtıdır. Kırmızı Kitap olarak bilinen Milli Güvenlik Siyaset Belgesi'ne (MGSB) de giren "Siber tehditlere"[425] karşı önemler her geçen gün geliştirilmekte, gerek kişi, kurum ve kuruluşlar bazında gerekse ulusal ve uluslararası işbirliği bazında yürütülmeye çalışılmaktadır. ABD, Çin, Rusya gibi bu

[424] Akın Aytekin, **age**, 134.
[425] https://www.memurlar.net/haber/621386/tsk-siber-saldiri-ordusu-kuruyor.html, [15.04.2018].

alandaki gelişmiş ülkelerin, gerek tarihsel süreç gerekse gelişmişlik olarak arkasında geliyor olsa da özellikle son 5 yıllık süreçte ilerlemeler kaydettiğini söylemek mümkündür.

Türk ordusunun yeni konseptini oluşturan en önemli başlıklardan biri olan siber savunma[426] konusuna ilişkin Eylül 2012'de kurulan TSK Siber Savunma Merkezi, özellikle askeri teşkilatlanma açısından kritik bir eşiktir. Müteakiben 30 Ağustos 2013 yılında TSK Siber Savunma Komutanlığına dönüştürülen merkez ile her ne kadar geç bile kalınmış olsa da siber savunma politikalarına yönelik ciddi bir aşama kaydedildiğini ispatlar niteliktedir. Öncelikli olarak TSK'nın kritik altyapıları ve bilgi sistemlerine tehdit eden potansiyel saldırılara karşı kurulmuş olsa da hem NATO ile olan işbirliği hem de diğer kamu kurumlarıyla olan ilişkileri nedeniyle, ulusal siber savunma sürecinde önemli bir rol oynamaktadır.

TSK Siber Savunma Komutanlığı; Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, TÜBİTAK ve diğer kamu kurumları ile koordineli olarak faaliyetlerini icra etmektedir. Ayrıca NATO ile eşgüdüm içerisinde ulusal ve uluslararası alanda görevler yürütülmektedir.

Bu kapsamda;

- TSK'nın kullandığı siber ortamda bulunan tüm sistemlerin siber savunması yapılmakta,
- Siber olaylara 7/24 esasına göre müdahale edilmekte,
- Ulusal olarak ve NATO tarafından icra edilen tatbikatlara iştirak edilmekte,
- TSK çapında bilinçlendirme ve eğitim faaliyetleri yürütülmekte,
- TSK tarafından kullanılan ağlarda düzenli olarak siber güvenlik denetlemeleri ve testleri yapılmaktadır[427].

Siber saldırılara karşı hazırlık ve gerektiğinde müdahale anlamında Türkiye'nin önemli güçlerinden birisi konumunda olan komutanlık, aynı zamanda "bütünleşik" ve "derinliğine siber güvenlik" anlayışı ile kuvvet komutanlıkları unsurlarıyla birlikte "olay yönetimi", "aktif savunma ve test faaliyetleri", "standart oluşturma", "kalite yönetimi", "ulusal ve uluslararası eğitim, tatbikatlar ve işbirliği", "proje, bilgi ve risk yönetimi ile denetim" faaliyetlerinden sorumlu bir role sahip bulunmaktadır[428].

TSK çapında siber savunma (aktif savunma dahil) faaliyetlerini merkezi olarak yürütmek, TSK bilgi sistem ağlarının siber güvenliğini sağlamak maksadıyla gerekli

---

[426] http://www.haberturk.com/gundem/haber/1048546-turk-ordusunun-yeni-konsepti-siber-savunma [15.04.2018].

[427] http://rewreward.blogspot.com/2013/01/turk-silahl-kuvvetleri-siber-savunma.html [24.04.2018].

[428] http://www.hurriyet.com.tr/teknoloji/turk-ordusunun-yeni-kuvveti-siber-savunma-40113652 [ 24.04.2018].

planlama, uygulama ve icra esaslarını belirlemek TSK Siber Savunma Komutanlığının vazifeleri arasındadır. Bilgi Teknolojileri Kurumu ve TÜBİTAK tarafından oluşturulan ve Türkiye'nin siber tehditlere karşı en üst mekanizması, siber kalkanı olarak görev yapan Ulusal Olaylara Müdahale Merkezinin askeri kanadını oluşturan TSK Siber Savunma Komutanlığı, kendi bünyesindeki alt birimler (SOME - Siber Olaylara Müdahale ekipleri) vasıtasıyla herhangi bir siber olay meydana gelmesi durumunda olaya müdahale etmek, olayın etkilerini azaltmak ve olayın nedenlerini tespit ederek önleyici tedbirler almak maksadıyla teşkil edilmiştir. Ayrıca; ulusal güvenlikte yeni bir "kuvvet çarpanı" anlayışıyla siber istihbarat, gerektiğinde aktif savunma yapabilme yeteneklerinin kazanılması ve siber caydırıcılığa yönelik milli teknoloji ile ürün geliştirme amaçlı Ar-Ge çalışmaları, TSK Siber Savunma Komutanlığının fonksiyon alanları arasında bulunmaktadır[429].

Siber Savunma Komutanlığı bünyesinde görev yapan ve TSK'ya ait bilgi sistemlerinin siber güvenliğini milli yazılımlarla sağlanacak şekidle geliştirilmesi ve TSK bünyesinde gerçekleştirilen siber savunma faaliyetlerinin tek merkezden kontrol edilmesi amacıyla kurulan Siber Savunma Harekât Merkezinde 7/24 esasına göre, TSK ve MSB'ye ait iç ve dış ağlar hizmet dışı bırakma ve yetkisiz içerik değişikliklerine karşı izlenmektedir[430].

Geleceğe dönük projeler açısından ise ulaşılabilen veriler ışığında, 2018 yılı içerisinde bitirilmesi planlanan, aslında şu an kurulu vaziyette 7/24 esasında göre faaliyet gösteren Siber Savunma Harekat Merkezinin de bir parçası olduğu TSK Siber Savunma Merkezi Projesi (SİSAMER) ile birlikte TSK Siber Savunma Komutanlığının mevcut yeteneklerinin geliştirilmesi ve kısa vadede yeni yeteneklerin kazanılması amaçlanmaktadır[431].

Mevcut duruma bakıldığında siber taarruz ile ilgili olarak herhangi bir bilgi veya çalışma olmadığı, teşkilatlanma da dahil olmak üzere yapılan çalışmaların savunma odaklı olduğu görülmektedir[432]. Ayrıca siber tehditlere ilişkin farkındalığın oluşması ve planlamalara dahil edilerek gerekli çalışmaların yürütülmeye başlanmasının çok da uzak bir geçmişi olmadığı dolayısıyla hem tecrübe hem de nitekli, uzman personel konusunda eksikler olduğu, kısacası umut vadeden atılımlar bulunmasına rağmen yolun başında olduğu değerlendirilmektedir.

[429] http://www.webtekno.com/internet/tsk-siber-savunma-komutanligi-h17616.html [16.04.2018].
[430] https://www.ssm.gov.tr/website/contentlist.aspx?PageID=1083&LangID=1 [16.04.2018].
[431] http://www.tsk.tr/TSKdanHaberler/Haber_234 [16.04.2018].
[432] Ümit Tatar, "Geleceğin Muharebelerinde Siber Savaş Boyutu", Harp Akademileri Komutanlığı Geleceğin Harekat Ortamı ve Harp Teknolojileri Paneli, 2013, İstanbul.

Teşkilatlanmanın ve buna bağlı olarak verilen görev ve sorumlulukların haricinde özellikle kurum içerisinde yapılan Siber Güvenlik Hazırlık Değerlendirmeleri, eğitim ve farkındalık çalışmaları, üniversiteler de dahil olmak üzere diğer kurum ve kuruluşlar ile bilgi ve Ar-Ge paylaşımları, yürütülen projeler, gerek ulusal gerekse uluslararası kapsamda başta NATO Kilitli Kalkan ve Siber Koalisyon Tatbikatlarına yapılan katılımlar, ülkemiz açısından savunma planlamaları açısından icra makamı olarak değerlendirilen ve milli gücün unsurlarından askeri gücü oluşturan ordu içerisinde siber tehditlerin yerini göstermekte ve savunma planlamalarında verilen öneme dikkat çekmektedir.

# 5. SONUÇ, DEĞERLENDİRME VE ÖNERİLER

Bilgi ve iletişim sistemlerinin kullanımı; kamu kurum ve kuruluşlarının, özel sektörde faaliyet gösteren birimlerin ve bireylerin sonu gözükmeyen bir siber denize dahil olmasını sağlamıştır. Buna bağlı olarak özellikle de internetin kullanımı, birbirleriyle bağlantılı olmayı, ancak bununla birlikte riskleri, belirsizlikle dolayısıyla da siber tehditlerin hedefi olmayı beraberinde getirmektedir.

Gün geçtikçe yaşanan tecrübeler ışığında; siber saldırılar artık sadece sistemlere sızma, bilgiye sızıp kendi amaçları için kullanma veya yanlış bilgi yerleştirerek mevcut bilginin bozulması ile sınırlı kalmayıp, bir ülkenin haberleşme sistemlerine, bilgi sistem altyapısına, enerji ağlarına, ulaşım ağlarına, askeri komuta ve kontrol sistemlerine kısacası kritik altyapılarına zarar verecek boyutlara ulaşan bir asimetrik harp türü olarak belirmektedir. Kaynağının belli olmaması, sınır tanımaması, düşük maliyetli olması, saldırganlar açısından düşük risk içermesi, doğrudan şiddet kullanımını barındırmaması, ulusal hatta uluslararası ölçekte uygulanabilir olması nedeniyle modern çağın en ciddi, bir o kadar da karmaşık tehdit türü olarak değerlendirilmektedir.

Her yıl bir önceki yılla kıyaslandığında siber uzay; ülkelerin, terör örgütlerinin ve siber tehditlerin güç gösterisine sahne olmaktadır. Buna bağlı olarak, siber tehdit aktörlerinin yetenekleri her yıl gelişmekte, kullanmış oldukları yöntemler de daha karmaşık hale gelmekte, saldırıların sayısı ve ekonomik etkileri de doğal olarak artmaktadır.

Şimdiye kadar belirtilen konular dahilinde; siber tehditlerin asimetrik tehditlerin bir kolu olarak siber savunma konusunda hem ulusal hem de küresel kamuoyunda farkındalığa neden olduğu, yeni savunma konseptlerini, teşkilatlanmalarını etkilediğini, misyon ve vizyonlarını güncellerken siber tehditlerin rolünü dikkate aldıklarını, bu kapsamda çalışmanın ana fikrini oluşturan paradigma değişimlerine neticesinde savunma planlama anlayışlarındaki dönüşüme önemli bir girdi teşkil ettiği değerlendirilmektedir.

Siber tehditlere karşı savunma konusunda tehdidin veya düşmanın tam ve kesin olarak tanımlanamaması ve siber saldırıların ne zaman gerçekleşeceğine yönelik bir öngörüde bulunulamaması nedeniyle, siber tehditle mücadele gerek kurum içinde gerekse bölgesel, ulusal hatta uluslararası boyutta bir bütünlük içinde, diğer savunma birimleri ile sürekli bir işbirliği içerisinde yürütülmesini gerektirmektedir. Kritik bilgi sistemleri ve iletişim altyapısını siber tehditlere karşı korumak, bir taarruz oluştuğunda bu taarruzun etkilerini en aza indirebilmek ve iz takibi yapabilmek için; öncelikle ulusal sonra da uluslararası manada koordinasyon, bilgi paylaşımı, ortak savunma anlayışı ve karşılıklı işbirliği çok önemlidir. Ülke içinde kurumlar hatta bireyler ve uluslararası işbirliği olmadan siber uzayın güvenliğinden ve buna bağlı olarak gelebilecek saldırılara karşı savunma yapabilmek imkansızdır. Çünkü küresel olan siber tehditlerle yerel yaklaşımlar yoluyla mücadele etmek gerçekten çok zordur; bu nedenle konuya ulusal yaklaşımlar getirilmeli, uluslararası kuruluşlar ile olan işbirliği de güçlendirilmelidir[433]. Dolayısıyla bu uçsuz bucaksız, karmakarışık bilgi boşluğunda müşterek siber savunma anlayışı/anlayışları geliştirmek öncelikli hareket tarzı olmalıdır.

Tehdidin tüm gelişmiş imkan ve kabiliyetlerine rağmen siber uzaydaki savunma anlayışlarının temelinde tehditten bir adım önde olmak yatmaktadır[434]. Tehdidi hazırlık safhasından itibaren takip etmek ve zarar vermesine müsaade etmeden etkisiz hale getirmek esas hedeftir. Siber tehditlerle mücadele yöntemleri şu şekilde olmalıdır:

1. Siber savunma konusunda günlük görevlere/tedbirlere odaklanılmamalı, tehdit iyi bir şekilde analiz edilerek savunmanın uzun soluklu bir süreç olduğu değerlendirilmelidir,
2. Siber savunma konusunda bütün birimler aynı duyarlılığa sahip olmalı, işin teknik yanına derinlemesine inilmese de siber saldırıların doğası ve potansiyeli konusunda neler olabileceği konusunda bilinçli olunmalıdır,
3. Öncelikler belirlenmeli ve kurumun en kritik sistemleri ne ise onların öncelikli olarak korunmasına yönelik tedbirler geliştirilmelidir. Çünkü her bilgiyi, sistemi, altyapıyı aynı anda, üstün bir koruma düzeyinde savunmayı hedeflemek rasyonellikten uzak bir hedeftir,
4. Her şeyden önce bireysel savunma gelmektedir. Çünkü bütün hackerler öncelikle kendileri için açması en kolay olan kapıya yönelirler: İnsanlar. Çünkü insan

[433] Mehmet Nesip Öğün ve Adem Kaya, "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", **Güvenlik Stratejileri Dergisi**, c.9, s.18 (2013): 172.
[434] Fulya Aslay, "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi", **International Journal of Multidisciplinary Studies and Innovative Technologies**, c.1, s.1 (2017): 27.

siber savunma sisteminin en zayıf halkasıdır ve tedbir alınması en zor aşamasıdır. Bu nedenle "Hiçbir savunma tedbiri eğitimden daha önemli değildir" mantığı esas alınarak planlama yapmak gerekmektedir,

5. Siber saldırılara karşı süratle reaksiyon verebilecek cevap hücreleri ve prosedürler belirlenerek farklı senaryolarla sürekli test edilmelidir. Roller ve sorumluluklar açık ve net bir şekilde belirlenmeli, eğitim ve tatbikatlarla desteklenmelidir[435].

Gün geçtikçe artan siber tehditlere karşı topyekün organize olacak şekilde bir plan çerçevesinde hareket edilmeli ve bu tehditleri bertaraf edecek önlemlerin nasıl alınacağını temel hatlarıyla belirleyecek ve bir çerçeve yaklaşımıyla tanımlayacak "Siber Güvenlik Gelecek Programı"na acilen ihtiyaç duyulduğu değerlendirilmektedir. Ülkelerin askeri ve ekonomik güçlerini temelden etkileyen ve gelecekte daha da çok etkileyeceği öngörülen siber tehditlere karşı planlı bir şekilde hareket edilmeli ve bu programa sadık kalınarak uygulanmalıdır. "Siber Güvenlik Gelecek Programı"nın bir parçası olarak Türkiye'nin önümüzdeki yıllarda askeri ve ekonomik gücünü yöneltmek zorunda kalacağı siber savaşlara karşı özel bir strateji geliştirilerek, olası siber savaşlara karşı savunma amaçlı çalışmalar yürütecek, bu bağlamda araştırma ve geliştirme yapacak özel bir birimlerin de kurulması[436] ve işbirliği içerisinde faaliyetlerini yürütmeleri hayati önemi haizdir.

Bir diğer husus, yine her ne kadar kesin bir çözüm olmasa da özellikle Soğuk Savaş döneminde de yakınen tecrübe edilen "Caydırıcılık"tır. Caydırıcılığı genel anlamda “karşı tarafın düşmanca eylemler yapmamasına yönelik gözdağı vermek” şeklinde açıklayan siber savaş araştırmalarıyla ünlü ABD’li bilim adamı Martin C. Libicki; siber caydırıcılığı, siber ortamda saldırganın eylemini boşa çıkarma veya cezalandırma (misilleme tehdidi) yoluyla saldırıdan vazgeçirme olarak açıklamaktadır[437]. Bu bağlamda, her ne kadar Soğuk Savaş Dönemi için caydırıcılığa esas olan hususlar nükleer silahlar ve silahlanma yarışı olsa da, siber uzaya ilişkin benzer hususun siber savunma ve saldırı konusunda imkan ve kabiliyetleri içeren "Siber Caydırıcılık" olduğunu belirtmek mümkündür. Söz konusu caydırılık da ancak; öncelikle ülkenin kritik altyapılarını koruyan etkin bir siber savunma sistemi, saldırı yapılması muhtemel hedeflere yönelik siber istihbarat, olası bir saldırı durumunda süratle reaksiyon gösterebilecek etkin bir siber taarruz gücü,

[435] Erin Nealy Cox, "Dealing With Cyber Threats", **Governance Newsletter**, Issue: 259 (2016): 10-11.
[436] Halil Öztürkçi, "Türkiye’nin Siber Güvenlik Geleceğine İlişkin Öneriler", http://www.gencmusiad.org.tr/blog-detay-turkiye%E2%80%99nin-siber-guvenlik-gelecegine-iliskin-oneriler-5.html [26.03.2018].
[437] Mustafa Şenol, "Türkiye’de Siber Saldırılara Karşı Caydırıcılık", **Uluslararası Bilgi Güvenliği Mühendisliği Dergisi**, c.3, s.2 (2017): 4.

ulusal ve uluslararası boyutta işbirliği ve koordinasyon, güçlü bir siber otorite ve komuta-kontrol kabiliyeti, siber caydırıcılığa yönelik propaganda faaliyetleri ve her alanda topyekün bir siber durumsal farkındalık ile sağlamak mümkündür[438]. Belirtilen hususlar doğrultusunda siber caydırıcılığın, siber savaşların önlenebilmesi konusunda önemli bir yere sahip olabileceği[439], dolayısıyla yapılacak savunma planlamalarında siber caydırıcılığın esaslarının da belirlenmesi gerektiği değerlendirilmektedir.

Ülkemizin ciddi bir siber saldırıya maruz kalmayacağını ve siber tehditlerin bize karşı saldırı potansiyeline sahip olmadığını söylemek iyimserliğin bile dışında kalan tamamen felakete davetiye çıkaran bir yaklaşımdır. Bu yüzden hem aktif hem de pasif savunma tedbirlerini içeren planlamalar yapılmalıdır. Ancak bunlar yapılırken de hukuki ve ekonomik boyutu başta olmak üzere değerlendirme kritlerinin düzgün bir şekilde ortaya konulması zaruridir.

Başarılı bir siber saldırının verdiği zarar, savunma için yapılan yatırımdan daha yüksek olabilir[440]. Bunun yanı sıra siber güvensizliğin getirebileceği maliyetin bu alanda yapılacak harcamalardan daha fazla olabileceği göz önüne alındığında siber savunmaya daha fazla nitelikli yatırım yapılması gerektiği açıkça görülmektedir[441].

Sonuç olarak, siber tehditler hedeflerinden hiçbir zaman vazgeçmeyecek, siber saldırılar da hiçbir zaman durdurulamayacaktır. Aksine gittikçe daha karmaşık hale gelecek ve nicel olarak artış gösterecektir. Bu nedenle en üst seviyedeki birimlerden en alt seviyedeki kullanıcıya kadar siber tehditlere yönelik farkındalığın arttırılmasının ve her seviyede yapılacak olan savunma planlamalarında önemli bir yer teşkil etmesinin gerektiğinin günümüz ve gelecek konseptleri açısından vazgeçilmez olduğu değerlendirilmektedir.

[438] Mustafa Şenol, **age**, 6-8.
[439] Ferhat Çalışkan, Talip Güler ve Yavuz İduğ, "Siber Caydırıcılık ve Türkiye'nin İmkan ve Kabiliyeti", **6.Uluslararası Bilgi Güvenliğive Kriptoloji Konferansı Bildiriler Kitabı** (Ankara, 2013), 287-288.
[440] Sait Yılmaz ve Olay Salcan, **age**, 14.
[441] Sait Yılmaz ve Olay Salcan, **age**, 14.

# KAYNAKÇA


Acarer, Tayfun. "Türkiye'de SOME'ler ve Siber Güvenlikte Yerli Milli Çözümler". www.teknokulis.com/haberler/guvenlik/2017/05/09/dunya-nufusunun-yuzde-51i-siber-saldiri-magduru [03.02.2018].

Ahrari, Ehsan. "Transformation of America's Military and Asymmetric War". **Comparative Strategy**. c.29. s.3 (2010): 223.

Ahronheim, Anna. "IDF Decides Not To Have A Cyber Command Department", **Israel News**, 2017, https://www.google.com.tr/amp/m.jpost.com/Israel-News/IDF-decides-not-to-have-a-cyber-command-department-477169/amp [30.03.2018].

Akad, Mehmet Tanju. **Tarihten Bugüne Gayrinizami Savaş**. İstanbul: Kastaş Yayınları, 2015.

Akdemir, Eray. "Bir Arap Ülkesinde Bahar: Suriye'de Arap Baharı ve Türkiye'nin Güvenliğine Etkisi". Yüksek Lisans Tezi. Kara Harp Okulu Savunma Bilimleri Enstitüsü, 2014.

Akgül, Öner. "Soğuk Savaş Sonrası Dönemde NATO–AB İliskilerinde Rekabet-İşbirliği Analizi Ve Türkiye Faktörü". **Güvenlik Stratejileri Dergisi**. c.4. s.7 (2008): 118.

Aksu, Muharrem ve Faruk Turhan. "Yeni Tehditler, Güvenliğin Genişleme Boyutları ve İnsani Güvenlik". **Uluslararası Alanya İşletme Fakültesi Dergisi**. c.4. s.2 (2012): 73.

Akyazı, Uğur. "Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler". **6.Uluslararası Kriptoloji Konferansı Bildiriler Kitabı**. Ankara: 2013: 216.

_____. **Siber Harekat Ortamının Siber Güvenlik Tatbikatları Kapsamında Değerlendirilmesi**. İstanbul: Harp Akademileri Basımevi, 2012.

Akyürek, Salih. "Zorunlu Askerlik ve Profesyonel Ordu". **BİLGESAM Yayınları**. Rapor No:24 (2010): 1.

Alcaraz, Cristina ve Zeadally Sherali. "Critical Infrastructure Protection: Requirements and Challenges For The 21st Century". **International Journal of Critical Infrastructure Protection**. c.18 (2015): 53.

Alkan, Mustafa. "Siber Güvenlik ve Siber Savaşlar". Bilgi Güvenliği Derneği. 2012. https://www.tbmm.gov.tr/arastirma_komisyonlari/bilisim_internet/docs/sunumlar/BILGI%20GUVENLIGI%20DERNEGI/09_05%20%20Bilgi%20/Guvenligi%20Dernegi.pptx [23.01.2018].

Allied Command Transformation Staff Element Europe. **The Beginners' Guide To The NATO Defence Planning Process**. 2013.

Altunok, Taner ve diğ. **Stratejik Savunma Yönetimi**. İstanbul: Bizim Büro Yayınevi, 2010.

Altıntaş, Emine Yazıcı. "Ülkemizde Siber Güvenlik". www.icwcturkey.com/files/2014/54899f3052c8c.pptx [25.01.2018].

Anıl, Süleyman. "Defending Against Cyber Attacks". **NATO CEP Perceptions**. s. 8. https://www.nato.int/issues/cep/cep_newsletter_08e.pdf [11.04.2018].

Aral, Berdal. "Asimetrik Saldırı Savaşları, Siyaset ve Uluslararası Hukuk". **Uluslararası İlişkiler**. c.4. s.14 (2007): 60.

Arbor Networks. "13th Annual Worldwide Infrastructure Security Report". http://www.arbornetworks.com/report [07.02.2018].

Arıboğan, Deniz Ülke. "Güvenliksiz Barıştan, Barışsız Güvenliğe". **ABD Dış Politikasında Yeni Yönelimler ve Dünya**. ed. Toktamış Ateş. İstanbul: Ümit Yayıncılık, 2004.

Armaoğlu, Fahir. "20.Yüzyıl Siyasi Tarihi (1914-1980)". **Türkiye İşbankası Kültür Yayınları**. Genel Yayın No:252. Tarih Dizisi:17 (1983): 419.

Arreguin-Toft, Ivan. "How the Weak Win Wars: A Theory of Asymmetric Conflict". **International Security**. c.26. s.1 (2001): 96.

Ashley, Bradley K. "Anatomy of Cyberterrorism: Is America Vulnerable?". United States Air Force (USAF) Air War College Seminar 10. A Research Paper www.au.af.mil/au/awc/awcgate/awc/ashley.pdf [26.01.2018].

Aslay, Fulya. "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi". **International Journal of Multidisciplinary Studies and Innovative Technologies**. c.1. s.1 (2017): 27.

Astan, Gökhan. "Gelişen Teknolojiler ve Değişen Muharebe Şartlarında Geleceğin Askerine Yönelik Teknoloji Öngörü Çalışması". Yüksek Lisans Tezi. Kara Harp Okulu Savunma Bilimleri Enstitüsü, 2015.

Aydın, Faruk. "Cyber Security In National Protection Of Turkey". Yüksek Lisans Tezi. Çankaya Üniversitesi Fen Bilimleri Enstitüsü, 2012.

Aytekin, Akın. "Türkiye'nin Siber Güvenlik Stratejisi ve Eylem Planının Değerlendirilmesi". Yüksek Lisans Tezi. Gazi Üniversitesi Bilişim Enstitüsü, 2015.

Bağbaşlıoğlu, Arif. "Transatlantik İlişkiler Bağlamında Küresel Ortaklar ve Akıllı Savunma". **Adam Akademi**. c.3. s.1 (2013): 80.

Bal, İhsan. “Küresel Çağ: Güvenlik, Tehdit ve İstihbaratın Değişen Seyri”. **Cumhuriyet Strateji** (6 Ocak 2006): 1-2.

Bayraktar Gökhan. **Siber Savaş ve Ulusal Güvenlik Stratejisi**. İstanbul: Yeniyüzyıl Yayınları, İstanbul, 2015.

Bensghir, Türksel Kaya. “Kurumsal Bilgi Güvenliği Yönetim Süreci”. Bilgi Yönetim Semineri. 2011, Antalya, strateji.deu.edu.tr/wp-content/uploads/2014/09/Kurumsal-Bilgi-Güvenliği-Yönetim-Süreci.pdf [05.02.2018].

Berk, Uğur. “Stratejik Savunma ve Güvenlik Planlamasinda Ortak Bir Yaklaşım Olarak Senaryo Temelli Planlama”. **Güvenlik Bilimleri Dergisi.** c.4. s.2 (2015): 9.

Bıçakçı, Salih. “NATO’nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik”. **Uluslararası İlişkiler Dergisi**. c.10. s.40 (2014): 104.

Bieniek, Mieczysław. “NATO’s New Strategic Concept And The Military Transformation Of The Alliance”. Ottawa Conference on Defence and Security. 2011. Ottawa.

Binnendijk, Hans ve diğ. **ABD Silahlı Kuvvetlerinin Dönüşümü**. Washington DC: National Defence University Press, 2002.

Birdişli, Fikret. “Ulusal Güvenlik Kavramının Tarihsel ve Düşünsel Temelleri”. **Sosyal Bilimler Enstitüsü Dergisi**. c.31. s.2 (2011): 153.

Blank, Stephen J. **Rethinking Asymmetric Threats**. Carlisle: U.S. Army War College Strategic Studies Institute Publications, 2003.

Bockel, Jean-Marie. "The State Of Europe's Defence Industrial Base". NATO Parliamentary Assembly. https://www.nato-pa.int/download-file?filename-=sites/default/files/201711/2017%20%2016%20E%20bis%20%20EUROPE%20INDUSTRIAL%20DEFENSE%20BASE%20-%20BOCKEL%20REPORT.pdf [30.03.2018].

Brangetto, Pascal. **National Cyber Security Organisation: France.** Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015.

Breen, Michael ve Joshua A. Geltzer. “Asymmetric Strategies As Strategies Of The Strong”. **Parameters**. c.41.s.1 (2011): 51-52.

Breene, Keith, "Who Are The Cyberwar Superpowers". https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers [01.02.2018].

Brenner, Susan W. “Distributed Security: A New Model of Law Enforcement”. **Journal of Internet Law**. c.8. s.5 (2004): 10

Bucur-Marcu, Hari, Philipp Fluri ve Todor Tagarev, “Defence Management: An Introduction”. **Security And Defence Management Series**. s.1 (2009): 62.

Burt, David ve diğ. “Cyberspace 2025: Today’s Decisions, Tomorrow’s Terrain, Navigating the Future of Cybersecurity Policy. Microsoft Corporation (2014): 3-4.

**Büyük Larousse Ansiklopedi.** İstanbul: Gelişim Yayınları, 1986.

Cabinet Briefed On The Israel National Cyber Bureau. http://www.pmo.gov.il/English/MediaCenter/Spokesman/Pages/spokecyber111112.aspx [03.04.2018].

Can, Ali ve Ufuk Taşçı. "Türkiye’de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014". **Fırat Üniversitesi Sosyal Bilimler Dergisi**. c.25. s.2 (2015): 236.

Camgöz, Nilgün. “Siberuzay, Sanal Gerçeklik ve Müze”. Bilim ve Teknik. www.biyolojiegitim.yyu.edu.tr/fizuzaypdf/Siberuzay199845.pdf [22.01.2018].

Cardash, Sharon L. ve Frank J. Cilluffo. "Estonia's Cyber Defence League: A Model For The United States". **Studies in Conflict & Terrorism**. s.36 (2013): 778-779.

Cartright, James E. “Joint Terminology For The Cyber Space Operations”. Memorandum For Chiefs Of The Military Services Of The Combatting Commands Of The Directions Of The Joint Staff Directorates. 2011.

Ceylan, Cenk. “Savaş Cephesi Olarak, Sanal Ortamda Savunma ve Saldırı”. http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/savas-cephesi-olarak-sanal-ortamda-savunma-vesaldiri [25.01.2018].

Choo, Raymond Kim-Kwang. “The Cyber Threat Landscape: Challenges and Future Research Directions”. **Computers and Security**. Vol.30. No:8 (2011):719-731.

Choucri, Nazlı. “Introduction: Cyber Politics in International Relations”. **International Political Science Review**. c.21. s.3 (2000): 243.

Clarke, Richard A. ve Robert K. Knake. **Siber Savaş (Cyber War)**. çev. Murat Erduran. İstanbul: İstanbul Kültür Üniversitesi Yayınları, 2010.

Clausewitz, Carl Von. **On War**. **On War**. Princeton: Princeton University Press, 1976.

Cleary, Laura R. ve McConville, Teri. **Managing Defence In A Democracy**. London/Routhledge: Cass Military Studies, 2006.

Cone, Robert W. “The Future Army: Preparation and Readiness”. **Military Review** (July-August 2013): 3-4.

Connell, Michael ve Sarah Vogler. "Russia’s Approach to Cyber Warfare". **CNA Analysis and Solutions**. https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf [08.04.2018].

Connoll, Chris ve diğ. "An Overview of International Cyber-Security Awareness Raising and Educational Initiatives". www.galexia.com/public/research/assets/gc381_acmacybersecurity_publication

_version_20110517_galexia_web/print-index.html [01.02.2018].

Cox, Erin Nealy. "Dealing With Cyber Threats". **Governance Newsletter**. Issue: 259 (2016): 10-11.

Cox, Michael, Ken Booth ve Tim Dunne ed. **Empires, Systems and States: Great Transformations in World Politics.** Cambridge: Cambridge University Press, 2002.

Cyber Edge Group. "2017 CyberThreat Defence Report". https://www.sumologic.com/wp-content/uploads/CyberEdge-2017-CDR-2017-Report.pdf [03.02.2018].

Cybersecurity Ventures. "2017 Cybercrime Report".https://cybersecurityventures.com/2015-wp/wpcontent/uploads/2010/ 2017-Cybercrime-Report.pdf [03.02.2018].

Çalışkan, Ferhat, Talip Güler ve Yavuz İduğ. "Siber Caydırıcılık ve Türkiye'nin İmkan ve Kabiliyeti". **6.Uluslararası Bilgi Güvenliğive Kriptoloji Konferansı Bildiriler Kitabı.** Ankara, 2013: 287-288.

Çakır, Hüseyin, Nursel Yalçın ve Mehmet Serkan Kılıç. "İnternet Sitelerine Yapılan Siber Saldırılar: 2015 Yılı Türk Kamu Siteleri İncelemesi". **Güvenlik Stratejileri Dergisi.** c.13. s.25 (2017): 185.

Çelik, Şener. "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme". **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**. c.15. s.1 (2013): 137-175.

Çeliktaş, Barış. "Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme". Yüksek Lisans Tezi. Karadeniz Teknik Üniversitesi, 2016.

Çiftçi, Hasan. **Her Yönüyle Siber Savaş**. Ankara: Tübitak Yayınları, 2013.

Çitlioğlu, Ercan. "Terörizm ve Küreselleşme". **Stratejik Analiz** (Aralık 2007): 81.

Davis, John R. "Defeating Future Hybrid Threats". **Military Review** (September-October 2013): 25.

Davis, Paul K. **Analytic Architectures for Capabilities-Based Planning**. Mission-System Analysis and Transformation. Santa Monica: RAND Publications, 2002.

Davis, Paul ve Russell D. Shaver. **Portfolio Analysis Methods for Assessing Capability Options**. Santa Monica: RAND, 2008.

Denning, Dorothy E. "Activism, Hactivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy". https://www.nautilius.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/ [26.01.2018].

Demirel, Murat. "Asimetrik Tehdit Kavramı Bağlamında 11 Eylül 2001 Sonrası Dönemde Amerika Birleşik Devletleri'ndeki Siber Tehdit Algılamasının ve

Geliştirilen Güvenlik Politikalarının İncelenmesi". Yüksek Lisans Tezi. Kara Harp Okulu Savunma Bilimleri Enstitüsü, 2012.

Dias, Dennis P. **Partnering With Private Networks: The Dod Needs A Reserve Cyber Corps**. U.S. Army War College/Carlisle: PA, 2008.

Dikici, Emre. **Harbin Evrimi, Geleceğin Harekât Ortamı ve Harp Teknolojileri**. İstanbul: Harp Akademileri Basımevi, 2013.

Dumanlı, Cihangir. **Ulusal Güvenlik Sorunlarımız**. İstanbul: Bizim Kitaplar, 2007.

Echevarria II, Antulio J. **Fourth-Generatıon War And Other Myths**. US: Strategic Studies Institute (SSI). 2005.

Edappagath, Ajmal. , "Cyber Law and Enforcements to Optimize Benefits of ICT". **I-Ways**. No. 3/4 (2004): 171.

Elran, Meir ve Gabi Siboni. "Establishing An IDF Cyber Command". **INSS**. Insight No: 719 (2015): 1.

Erhan, Çağrı. "NATO Niçin Küresel Bir Güvenlik Örgütü Haline Gelmelidir?". **Aylık Strateji ve Analiz Dergisi**. s.12 (Ocak 2004).

Estonian Ministry Of Defence. "Estonian Defence Strategy". http://www.kmin.ee/files/img/files/KM_riigikaitse_strateegia_eng(2).pdf [31.03.2018].

_____. "National Defence Development Plan 2013-2022". http://www.kaitseministeerium.ee/sites/default/files/sisulehed/kaitseeelarve/national_defence_development_plan_2013.pdf [31.03.2018].

Ewing, P. "The Cyber War After Next". https://www.military.com/dodbuzz/2012/03/22/the-cyber-war-after-next/amp [25.01.2018].

Eyim, Ahmet ve Kamuran, Uygar. "Thomas S. Kuhn'un Paradigma Görüşü ve Atwood Makinesi Üzerine Bir Tartışma". **Düşünme Dergisi**. c.1. s.8 (2016): 18.

Fiddler, David P. "Recent Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law". c.16. s.22. http://www.asil.org/insights/volume/16/issue/22/recent-developments-and-revelations-concerning-cybersecurity-and [23.01.2018].

Finch, Lou ve Davis, Paul K. **Defense Planning For The Post-Cold War Era**. California: Naval Postgraduate School Press, 1993.

Fitzsimmons, Michael. "Whither Capabilities-Based Planning?". **National Defense University**. Issue 44 (2007): 102.

Flournoy, Michèle A. ve Tammy S. Schultz. **Shaping U.S. Ground Forces for the Future: Getting Expansion Right**. Washington: Center For A New American Security, 2007.

Gaddis, John Lewis. **Strategies of Containment: A Critical Appraisal of American National Security Policy During the Cold War**. USA: Oxford University Press, 2005.

Genç, Serdar. "Yetenek Temelli Stratejik Yönetim Anlayışının ABD Silahlı Kuvvetlerinin Teşkilat Yapısına Etkisi". **Güvenlik Stratejileri Dergisi**. c.11. s.21 (2015): 212.

Gorman, Siobhan ve Julian E. Barnes, "Cyber Combat: Act Of War". https://www.wsj.com/articles/SB1i0001424052702304563104576355623135782718 [02.04.2018].

Gray, Chris Hables. **Postmodern Savaş: Yeni Çatışma Politikası**. çev. Derya Kömürcü. İstanbul: Alfa Yayınları, 2000.

Gray, Colin S. "Thinking Asymmetrically in Times of Terror". **US Army War College**. c.32. s.1 (2002): 5.

Gunneriusson, Hâkan. "Nothing Is Taken Serious Until It Gets Serious: Countering Hybrid Threats". **Defence Against Terrorism Review**. Vol.4. No.1 (2012): 48.

Günay, Umay Türkeş. "Folklor ve Siber Çağ". **Türk Dünyası İncelemeleri Dergisi**. c.13. s.1 (2013): 217.

Güneş, Bilal. "Paradigma Kavramı Işığında Bilimsel Devrimlerin Yapısı ve Bilim Savaşları: Cephelerdeki Fizikçilerden Thomas S.Kuhn ve Alan D.Sokal". **Türk Eğitim Bilimleri Dergisi**. c.1. s.1 (2003): 27.

Güngör, Murat. "Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma". T.C. Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı. Yayın No: 2919, 2015.

Gürcan, Metin. "Savaşın Evrimi ve Teorik Yaklaşımlar". BİLSESAM. http://www.bilgesam.org/Images/Dokumanlar/0-163-201404072m_gurcan.pdf [22.05.2016].

Gürkaynak, Muharrem ve Adem Ali İren. "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler". **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**. c.16 (2011): 263.

Gürsoy, Yaprak. **Türkiye'de Sivil-Asker İlişkilerinin Dönüşümü**. İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2012.

Haacke, Jürgen ve Paul D. Williams. "Regional Arrangements, Securitization, and Transnational Security Challenges". **Security Studies**. c.17. s.4 (2008): 776.

Hafner, Katie ve Matthew Lyon. **İnternet Tarihi**. çev. Sinem Yazıcıoğlu. İstanbul: Güncel Yayıncılık, 2000.

Hansen, Lene ve Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School". **International Studies Quarterly**. c.53 (2009): 1167.

Harrison, Dinnis Heather. **Cyber Warfare and The Laws of War**. Cambridge: Cambridge University Press, 2012.

Hekim, Hakan ve Oğuzhan Başıbüyük. “Siber Suçlar ve Türkiye’nin Siber Güvenlik Politikaları”. **Ulusal Güvenlik ve Terörizm Dergisi**. c.4. s.2 (2013): 143.

Hildreth, Steven A. "Cyberwarfare". **CRS Report for Congress**. Order Code: RL30735. 2001. https://fas.org/irp/crs/RL30735.pdf [04.04.2018].

Hoffman, Frank G. “Hybrid Threats: Reconceptualizing The Evolving Character Of Modern Conflict”. **Strategic Forum**. s.240 (2009): 5.

Housen-Couriel, Deborah. **National Cyber Security Organisation: Israel.** Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2017.

Hundley, Richard O. ve Robert Anderson. **Emerging Challenge: Security and Safety in Cyberspace**. ed. John Arquilla and David Ronfeldt. Santa Monica: RAND Corporation, 1997.

Inkster, Nigel. "Chinese Intelligence Operations In The Cyber Age". **Survival Global Politics And Strategy**. c.55. s.1 (2013): 54.

İçin, Özlem Kösedağ. “Değişen Güvenlik Anlayışının Uluslararası Örgüt Dernekleri Üzerinden Analiz Edilmesi”. **Güvenlik Stratejileri Dergisi**. c.13. s.25 (2017): 103.

İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü. “Siber Güvenlik Raporu”. İstanbul, 2012.

İşyar, Ömer Göksel. “Günümüzde Uluslararası Güvenlik Stratejileri: Kavramsal Çerçeve Ve Uygulama”. **Akademik Bakış Dergisi**. c.2. s.3 (2008): 37.

Jandarma Genel Komutanlığı MEBS Başkanlığı. **Siber Güvenlik El Kitabı**. Ankara, 2016.

Johnson, Robert. “Future Trends in Insurgency and Countering Strategies”. Centre of Excellence Defence Against Terrorism. www.coedat.nato.int/publication/reaserches/04-FutureTrends.pdf [27.01.2018].

Joint Systems and Analysis Group of Subcommıttee On Non-Atomıc Mılıtary Research And Development. “Guide To Capability Based Planning (TTCP Technical Report)”. Technical Panel 3rd Of The Technical Cooperation Program. 2004, USA.

Joint Chief of Staff. Joint Pub 3-13, “Joint Doctrine for Information Operations GL-5, Cyber Attacks: Unlawful Uses of Forces or Prohibited Interventions?”. **Journal of Conflict and Security Law**. c.17. s.2 (2012): 220.

Kabakoğlu, Mehmet, Fahri Koçuk ve Engin Vardar. **Siber Güvenlik El Kitabı.** Ankara: J.Gen.K.lığı MEBS Bşk.lığı, 2016.

Kahraman, Çağdaş Akif. “Tarihsel Süreçte Savunma Planlaması Yaklaşımları İle Savunma Tedarik Sistemleri Arasındaki İlişki”. **Kara Harp Okulu Bilim Dergisi**. c.26. s.2 (2016): 104.

Kara, Mahzure. “Siber Saldırılar-Siber Savaşlar ve Etkileri”. Yüksek Lisans Tezi. İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, 2013.

Kara, Mehmet ve Serdar Çelikkol. “Kritik Altyapılar: Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği”. 4.Ağ ve Bilgi Güvenliği Sempozyumu. 2011, Kocaeli.

Kara, Oğuz, Üzeyir Aydın ve Ahmet Oğuz. “Ağ Ekonomisinin Karanlık Yüzü: Siber Terör”. kisi.deu.edu.tr/oguz.kara/Ag%20Ekonomisinin%20karanlik%20yuzu% 20siber%20teror.pdf [23.01.2018].

Kara Harp Akademileri. **Asimetrik Harp Yardımcı Yayını**. İstanbul: Harp Akademileri Basımevi, 2002.

_____. Kara Harp Akademileri Komutanlığı, **Asimetrik Harp Paneli Notları**. İstanbul: Harp Akademileri Basımevi, 2010.

Karabulut, Bilal. “Küreselleşme Sürecinde Güvenlik Alanında Değişimler: Karadeniz’in Güvenliğini Yeniden Düşünmek”. **Karadeniz Araştırmaları Dergisi**. c.6, s.23 (2009): 2.

Karahan Türk, Hünkar. “Türk Savunma Sanayinin Ekonomik Etkileri ve Savunma Harcamaları-Ekonomik Büyüme İlişkisinin Ekonometrik Modellenmesi”. Yüksek Lisans Tezi. Çukurova Üniversitesi Sosyal Bilimler Enstitüsü, 2007.

Karakuş, Cahit. **Kritik Alt Yapılara Siber Saldırı**. http://www.ylt44.com/Security/Siber/siber.pdf [23.01.2018].

Karaosmanoğlu, Ali L. **NATO'nun Dönüşümü**. İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2012.

_____. “Savunma Planlaması ve Stratejik Belirsizlik”. **Bilge Strateji Dergisi**. c.7. s.12 (2015): 23.

Kaspersky Lab. "Kaspersky Cyber Security Bulletin: Story of the Year-2016".

_____. “Kaspersky Cyber Security Bulletin: Story of the Year-2017”.

Kaya, Adem. “Siber Güvenliğin Milli Güvenlik Açısından Önemi”. Yüksek Lisans Tezi. Kara Harp Okulu Savunma Bilimleri Enstitüsü, 2012.

Kem, Jack D. **Campaign Planning: Tools Of The Trade**. 3.bs. Kansas: US Army Command and General Staff College, 2009.

Korkmazyürek, Haluk ve Harun Şeşen. “Savunma Yönetiminde Yeni Planlama Yaklaşımları: Kavramsal Bir Analiz”. **Kara Harp Okulu Bilim Dergisi**. c.18. s.1 (2008): 56.

Korkmazyürek, Haluk. **Stratejik Savunma Yöntemi ve Savunma Planlaması**. Ankara: 2011.

_____. “Stratejik Yönetim Ders Notları”. Kara Harp Okulu Savunma Bilimleri Enstitüsü Savunma Yönetimi Doktora Programı, 2011.

Köksal, Faruk. **Risk ve Tehdit Kavramında Yeni Paradigmalar ile Asimetrik Tehdit Analizi**, **Türkiye’ye Yönelik Dış Kaynakları Risk ve Tehditler**.

İstanbul: Harp Akademileri Basımevi, 2007.

Kör, Abdullah. **Siber Saldırılar İçin Dinamik Bir Çözüm Modeli**. Yüksek Lisans Tezi. Gazi Üniversitesi Bilişim Enstitüsü, 2015.

Köseoğlu, Ahmet Murat. "Savunma Sanayi Stratejisinin Yeniden Belirlenmesi ve Türkiye'nin Güvenliğine Etkisi". **SAREM Stratejik Araştırmalar Dergisi**. c.9. s.17 (2011): 123.

Kugler, Richard L. **U.S. Defense Strategy and Force Posture for the 21st Century: Capabilities and** Requirements. Santa Monica: RAND, 1994.

Kuhn, Thomas S. "The Structure of Scientific Revolutions". **International Encyclopedia of Unified Science**. c.2. s.2 (1970): 81-93.

Kumkale, Tahir Tamer. **Asimetrik Savaş**, **Asimetrik Savaş**. http://kumkale.net/yazi.asp?id=599 [17.05.2016].

Kurtdarcan, Bleda ve Özgür Mumcu. **Geleceğin Savaşları ve Silahları**. Ankara, Uğur Mumcu Araştırmacı Gazetecilik Vakfı Yayınları, 2014.

Küçük, Ahmet ve İbrahim Soğukpınar. "Siber Saldırılar ve Farkındalık Eğitimi İçin Bir Öneri". cigicigi.com/CA.pdf [25.01.2018].

Küçükşahin, Ahmet ve Tamer Akkan. "Değişen Güvenlik Algılamaları Işığında Tehdit ve Asimetrik Tehdit". **Güvenlik Stratejileri Dergisi.** s.5 (2007): 60.

Külebi, Ali. "Asimetrik Savaş Kavramı ve Tehditler". www.inadina.com/inadeski/sayi156/yazi9.htm [28.05.2018].

Lambakis, Steven ve diğ. "Understanding The Asymmetric Threats To The United States". **Comparative Strategy**. c.21. s.4 (2002): 253.

Lawrence, Tony. "The Risk of Threat-Based Planning". http://www.businessofgoverment.org/bio/john-m-kamensky [25.12.2017].

Lazarevic, Aleksandar, Vipin Kumar ve Jaideep Srivastava. "Intrusion Detectıon: A Survey, Managing Cyber Threats: Issues, Approaches and Challenges". **Springer Science and Business Media**. c.5 (2005): 20.

Lee, Dave. "Israel Tops Cyber-Readiness Poll But China Lags Behind". www.bbc.com/news/technology-16787509 [02.04.2018].

Lewis, James A. ve Katrina Timlin. **Cybersecurity and Cyberwarfare 2011**. Center for Strategic and International Studies/US: UNIDIR Resources, 2011.

Liang, Zhuge. **Savaş Sanatında Ustalaşmak**. çev. Sibel Özbudun. İstanbul: Anahtar Kitabevi, 1997.

Liotta, P.H. ve Richmond M. Lloyd. **Here To There**, Naval War College Review, 58 (2), 2005.

Lloyd M., Richmond ve diğ., **Fundamentals Of Force Planning, Vol.1: Concepts**.

Newport: Naval War College Press, 1990.

Mader, James, Tom Smith ve Dan Daley. **Asymmetric Warfare: The Only Thing New is The Tactic.**Washington DC: National Defense University National War College, 2000.

Mahon, Tim. "Cyber Defence: Welcome To The Next Level". **Naval Forces**. S.1 (2015): 40.

Mataracıoğlu, Tolga. "Sayısal Ortamda Savaşın Tarihçesi". Sayısal Ortamda Savaş Sempozyumu (1), 2010.

Mckenzie, Kenneth F. **The Revenge Of The Melians: Asymmetric Threats And The Next QDR**. Washingon: Institute for National Strategic Studies, 2000.

Medvedev, Sergei A. **Offense-Defense Theory Analysis Of Russian Cyber Capability**. Monterey/California, Dudley Knox Library, 2015.

Meral, Mehmet. "NATO ve Siber Savunma", https://mehmetmeral.wordpress.com/2015/01/17/nato-ve-siber-savunma [10.04.2018].

_____. "Siber Savunma: Ülkeler ve Stratejiler". **3.Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı**, Ankara, 2008: 257.

Meral, Mustafa. "Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi". Yüksek Lisans Tezi. Kara Harp Akademileri Stratejik Araştırmalar Enstitüsü, 2015.

Meydan, Cem Harun ve Akif Demirel. "Savunma Planlamasında Belirsizlikle Başa Çıkmada Esnek Yaklaşımlar". **SAVBEN Dergisi**. c.9. s.1 (2010): 13.

MGK İnternet Sitesi, **Asimetrik Tehdit Nedir Sorusu**. http://www.mgk.gov.tr/turkce/sss.html#soru_13 [16.05.2016].

Miks, Jason. "Israel, China and Cyber Security". https://thediplomat.com/2012/02/israel-china-and-cyber-security [02.04.2018].

Mütercimler, Erol. **Geleceği Yönetmek ve Kazanmak İçin Stratejik Düşünme**. İstanbul: Alfa Yayınları, 2011.

Nacak, Aslan Onur. "21'inci Yüzyıl Ortak Güvenlik Ortamı: Askerî Statülü Kolluk Kuvvetleri İçin Plânlama Önerileri". **Güvenlik Bilimleri Dergisi**. c.4. s.1 (2016): 1.

**National Cyber Security Framework Manual**. ed. Alexander Klimburg. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publications, 2012. https://www.ccdoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf [01.02.2018].

NATO Research and Technology Organisation. **Handbook on Long Term Defence Planning**. France, 2003.

Nye, Joseph S.Jr. **The Future of Power**. USA: Public Affairs Books, 2011.

_____. “From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?”. **Bulletin of The Atomic Scientists**. c.69. s.5 (2013): 8.

Okan, Kartal. “The Symmetrical Evolution Of (The Notion Of) State Security According To Asymmetrical Threats: From Sticks And Stones To Cyber Warfare”. Yüksek Lisans Tezi, 2015.

Osula, Anna-Maria. **National Cyber Security Organisation: Estonia.** Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015.

_____. **National Cyber Security Organisation: United Kingdom**. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015.

Osula, Anna-Maria ve Henry Rõigas. "Outer Space and Cyberspace: A Tale of Two Security Realms". **International Cyber Norms**. ed. Paul Meyer. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publications, 2016.

Öğün, Mehmet Nesip ve Adem Kaya. "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler". **Güvenlik Stratejileri Dergisi**. c.9. s.18 (2013): 172.

Özarslan, Bahadır Bumin. “Soğuk Savaş Sonrası Karadeniz'de Güvenlik Politikaları ve Türk-Rus İliskileri”. **Türk Dünyası İncelemeleri Dergisi**. c.12. s.1 (2012): 136.

Özcan, Gencer. “Doksanlı Yıllarda Türkiye'nin Değişen Güvenlik Ortamı”. **En Uzun On Yıl: Türkiye'nin Ulusal Güvenlik ve Dış Politika Gündeminde Doksanlı Yıllar**. ed. Şule Kut. İstanbul: Büke Yayıncılık, 2000.

Özeren, Süleyman. **Responses to Cyber Terrorism**. ed. Terörizmle Mücadele Mükemmeliyet Merkezi (COEDAT)/Türkiye. Amsterdam: IOS Press, 2008.

Özkan, Behlül. “Soğuk Savaş Sonrası Amerikan Dış Politikası”. **Stratejik Araştırmalar**. c.9. s.16 (2011): 53.

Özkök, Hilmi. "İnternet Silah Gibi", **Milliyet Gazetesi**, http://gazetearsivi.milliyet.com.tr/GununYayinlari/3cfulzH3qW3lu4zf6V4_x2B_5w_x3D_x3D_ [26.01.2018].

Öztürk, Yunus. “Konvansiyonel Savaş Devri Geride mi Kaldı?”. **Millî Güvenlik ve Askerî Bilimler Akademik Dergisi**. c.2. s.6 (2015): 26.

_____. “Savunma Planlamasında Yeni Yaklaşımlar ve Türk Silahlı Kuvvetlerinde Bir Senaryo Uzayı Çalışması”. Yüksek Lisans Tezi. Kara Harp Okulu Savunma Bilimleri Enstitüsü, 2006.

Öztürk, Ümit. “Thomas Kuhn’un Paradigma Kavrayışı Üzerine Analitik Bir İrdeleme”. **Kaygı: Uludağ Üniversitesi Fen-Edebiyat Fakültesi Felsefe Dergisi**. c.19. s.19 (2012): 187.

Öztürkçi, Halil. "Türkiye’nin Siber Güvenlik Geleceğine İlişkin Öneriler". http://www.gencmusiad.org.tr/blog-detay-turkiye%E2%80%99nin-siber-güvenlik-gelecegine-iliskin-oneriler-5.html [26.03.2018].

Pennie, Kenneth R. “Strategic Thinking in Defence”. **Canadian Military Journal**. c.2. s. 3 (2001): 25.

Pernik, Piret, **National Cyber Security Organisation: United States.** Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2016.

Purtaş, Fırat. “Soğuk Savaş Sonrası NATO’nun Dönüşümü ve Genişlemesi Çerçevesinde Türk-Amerikan Askeri İlişkileri”. **Güvenlik Stratejileri Dergisi**. c.2. s.1 (2005): 10.

Raud, Mikk. **China And Cyber: Attitudes, Strategies, Organisation**. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2016.

Reckitt Benckiser Group. "Annual Report and Financial Statements 2016". https://www.rb.com/media/2473/rb-annual-report-2016-no-spine.pdf [05.02.2018].

Reinhard, Karl E. **A Paradigm for the System of Systems Countering Asymmetric Enemy Kinetic Attacks**. Pennyslvania: US Army War College, 2005.

Richmond, Jeremy. “Evolving Battlefields: Does Stuxnet Demonstrates A Need For Modifications To The Law Of Armed Conflict”. **Fordham Journal of International Law**. c.35. s.3 (2012): 850-852.

Riigikogu. Approval Of The Main Guidelines Of Estonia's Security Policy Until 2015. http://siseministeerium.ee/29744 [31.03.2018].

_____. "National Security Concept Of Estonia". http://www.eda.europa.eu/docs/default-source/documents/estonia--national-security-concept-of-estonia-2010.pdf [31.03.2018].

Robinson, Neil. "NATO: Siber Savunmada Vites Değiştiriyor". **NATO Dergisi**. https://www.nato.int/docu/review/2016/Also-in-2016/cyber-defense-nato-securityrole/TR/index.htm [10.04.2018].

Sağsan, Mustafa. “Bilgi Savaşı: Siperlerden Klavyelere Taşınan Savaşın Anatomisi”. **Psikolojik Harp İstihbaratı Avrasya Dosyası Uluslararası İlişkiler ve Stratejik Araştırmalar Dergisi**. Fasikül:23. c.8. s.2 (2002): 110

Sander, Oral. **Siyasi Tarih (1918-1994)**. 20.bs. Ankara: İmge Kitabevi, 2011.

Sandıklı, Atilla ve Bilgehan Emeklier. “21. Yüzyılda Yeni Güvenlik Anlayışları ve Yaklaşımları”. BİLGESAM, Uluslararası Balkan Kongresi, 28-29 Nisan 2011, Kocaeli.

Savunma Sanayii Müsteşarlığı. “2010, 2011, 2012 Yıllarına İlişkin Faaliyet ve İşlemlerinin Denetimi”. **Türkiye Cumhuriyeti Cumhurbaşkanlığı Denetleme Raporu.** Ankara, 2014.

Savunma Teknolojileri Mühendislik ve Ticaret A.Ş., “İzmir Gaz’a Anonymous Saldırısı”. 2016 Temmuz-Eylül Dönemi Siber Tehdit Durum Raporu.

Schmitt, Michael N. **Tallinn Manual on the International Law Applicable to Cyber Warfare**. Cambridge: Cambridge University Press, 2013.

Schmitt, Michael N. ve Liis Vihul. “The Nature of International Law Cyber Norms”. **International Cyber Norms**. ed. Anna-Maria Osula and Henry Rõigas. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publications, 2016.

Sertoğlu, Sedat. "Büyük Tehlike". **Sabah Gazetesi**. 6 Aralık 1999. https://arsiv.sabah.com.tr./1999/12/06/y11.html [20.01.2017].

Sevim, Şenol. “Soğuk Savaş Sonrası Avrupa Güvenlik Yapılanması ve Türkiye”. Yüksek Lisans Tezi. Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2006.

Shapiro, Jeremy ve Lynn Davis. **The New National Security, The US Army and The New National Security Strategy**. Santa Monica: RAND Publications, 2003.

Sheldon, Robert and Joe McReynolds. "Civil-Military Integration and Cybersecurity". **China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain**. Oxford: Oxford University Press, 2015.

Soğukpınar, İbrahim. **Teknolojik Gelişmeler ve Siber Güvenlik**, TASAM, 2016.

Storch, Tyson. “Siber Güvenlik: Güvenli ve Bağlantılı Bir Toplumun Temel Taşı”. Microsoft Corporations, 2012, 6.

Sullivan, Gordon R. “America's Army: Movin Toward 2020”. **Army** (October 2013): 12.

Swanson, Lesley. “The Era of Cyber Warfare: Applying International Humanatarian Law To The 2008 Russian-Georgian Cyber Conflict”. **Loyola of Los Angeles International & Comparative Law Review**. Vol.32 (2010): 303.

Symantec. "Internet Security Threat Report". c.20 (2015): 93.

Şenol, Mustafa. "Türkiye’de Siber Saldırılara Karşı Caydırıcılık". **Uluslararası Bilgi Güvenliği Mühendisliği Dergisi**. c.3. s.2 (2017): 4.

Şentürk, Hakan ve diğ. “Siber Güvenliğin Taarruzi Boyutu ve Uluslar arası Hukuk Kurallarının Uygulanabilirliği”. **6.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı**, Ankara, 2013: 51.

Şentürk, M.Yasir. "E-Devlet ve Siber Güvenlik: Uluslararası Değerlendirme". Türk Hava Kurumu Üniversitesi E-Devlet ve E-Dönüşüm Konulu Sunum Yansıları, afyonluoglu.org/PublicWebFiles/Lectures/ECE581/ECE581Siber%20Güvenlik%20ve%20Uluslararasi%20Degerlendirme.pdf [10.03.2018].

Tatar, Ümit. "Geleceğin Muharebelerinde Siber Savaş Boyutu". Harp Akademileri Komutanlığı Geleceğin Harekat Ortamı ve Harp Teknolojileri Paneli. 2013, İstanbul.

Tepebaş, Ufuk. “Soğuk Savaş ve 11 Eylül Sonrası Uluslararsı Sistemdeki Değişimin Güvenlik Algılamalarına Etkisi ve Türkiye”. http://www.tasam.org/tr-TR/Icerik/205/soguk_savas_ve_11_eylul_sonrasi_uluslararasi_sistemdeki_degi

simin_guvenlik_algilamalarina_etkisi_ve_turkiye [22.12.2017].

T.C. Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı. **2014-2023 Teknolojik Afetler Yol Haritası Belgesi**. Ankara, 2014.

T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. **Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı**. Ankara, 2012.

____. **2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı**. Ankara, 2016.

The Joint Publication 1-02. "Department of Defence Dictionnary of Military and Associated Terms". http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf#search-"cyber%20space" [Erişim Tarihi: 21.01.2018].

The Securtiy Council Of Russian Federation. **Information Security Doctrine Of The Russian Federation**. https://toinformistoinfluence.com/2016/12/19/information-security-doctrine-of-the-russian-federation-6-december-2016 [08.04.2018].

Threatcloud Intelligence. "Live Cyber Attack Threat Map". https://threatmap.checkpoint.com/ThreatPortal/livemap.html [08.02.2018].

Tıkk, Eneken, Kadri Kaska ve Liis Vihul. "International Cyber Incidents: Legal Considerations". Cooperative Cyber Defence of Excellence (CCD COE)/Estonia, 2010.

Toft, Monica ve Talbot Imlay. **The Fog of Peace and War Planning: Military and Strategic Planning Under Uncertainty**. New York: Routlegde, 2006.

Topçu, Mustafa Kemal. "Savunma Planlamasının Ekonomiye Etkileri ve Savunma Bütçeleri". **Savunma Bilimleri Dergisi**. c.9. s.1 (2010): 78.

TSK Siber Savunma Komutanlığı. "Teröristlerin Siber Uzayı Kullanımı", **Siber Savunma Farkındalık Bülteni**, Bülten No: 2015-F-3 (2015): 1.

Tullos, Kristen E. "From Cyber Attacks To Social Media Revolutions: Adapting Legal Frameworks To The Challenges and Opportunities Of New Technology". **Emory Internation Law Review**. Vol.26 (2012): 736.

Turner, Michael A. **Historical Dictionary of United States Intelligence**. Lanham: Scarecrow Press, 2006.

Türk Dil Kurumu. **Büyük Türkçe Sözlük**. Ankara: Türk Dil Kurumu Yayınları, 2011.

Türk Dil Kurumu resmi internet adresi. www.tdk.gov.tr [16.05.2016].

Ulaşanoğlu, M.Emin, Ramazan Yılmaz ve M. Alper Tekin. "Bilgi Güvenliği: Riskler ve Öneriler", Bilgi Teknolojileri ve İletişim Kurumu, 2010, Ankara.

Türkay, Şeyda. "Siber Savaş Hukuku ve Uygulanma Sorunsalı". **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**. c.71. s.1 (2013): 1217.

Tzu, Sun. **Savaş Sanatı**, çev. Pulat Otkan ve Giray Fidan. İstanbul: Türkiye İş Bankası Yayınları, 2015.

United Kingdom Cabinet Office. “Cyber Security Strategy of The United Kingdom”, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf [25.01.2018].

UK Ministry of Defence. “Future Land Operating Concept”. **Joint Concept Note 2/12.** UK, 2012.

US Air Force, “Cyberspace”, https://m.www.youtube.com/watch?v=amJI0xZA25c [29.01.2018]

US Army. **FM 3-0 Operations**, Chapter:4. US, 2001.

USA Deparment Of Army. **The Army Strategic Planning Guidance: 2006-2023.** US, 2003.

US Department of Defense. “Force Structure Plan”. Base Closure And Realignment Report. Vol.1, Chapter:2, 2005: 5.

_____. **Quadrennial Defense Review**. US, 2010.

_____. **Sustaining US Global Leadership: Priorities for 21st Century Defense**, 2012.

Uşaklı, Ali Bülent. **Savaşın Dönüşümü ve Teknoloji**. Ankara: Lalezar Kitabevi, 2008.

Ülman, Burak. “Türkiye'nin Yeni Güvenlik Algılamaları ve Bölücülük”. **En Uzun On Yıl: Türkiye'nin Ulusal Güvenlik ve Dış Politika Gündeminde Doksanlı Yıllar**. ed. Şule Kut. İstanbul: Büke Yayıncılık, 2000.

Ünsaldı, Muzaffer. “Asimetrik Tehdit ve Savunma Sanayisine Etkileri”. Yüksek Lisans Tezi. Kara Harp Akademisi Stratejik Araştırmalar Enstitüsü, 2013.

Ünver, Mustafa, Cafer Canbay ve Ayşe Gül Mirzaoğlu. “Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler”. Bilgi Teknolojileri ve İletişim Kurumu, 2009, Ankara.

Varlık, Ali Bilgin. “Savaşı Tanımlamak: Terminolojik Bir Yaklaşım”. **Avrasya Terim Dergisi**. c.1. s.2 (2013): 117-119.

Vavra, Shannon. "The World's Top Cyber Powers". https://www.axios.com/the-worlds-top-cyber-powers-1513304669-4fa53675-b7e6-4276-a2bf-4a84b4986fe9.html [06.02.2018].

Verton, Dan. **Black Ice, The Invisible Threat of Cyber-Terrorism**. New York: McGraw-Hill, 2003.

VonKnop, Katharina. "Institutionalization of a Web-Focused, Multinational Counter-Terrorism Campaign - Building a Collective Open Source Intelligent System". **A Discussion Paper, Responses to Cyber Terrorism**, ed. Centre of Exellence Defence Against Terrorism.Ankara: IOS Press, 2008: 9.

Vrey, Francois. “Paradigm Shifts, South African Defence Policy And The South African National Defence Force: From Here To Where?”. **Scientia Militaria: South African Journal of Military Studies**. c.32. s.2 (2004): 90.

Vural, Yılmaz ve Şeref Sağıroğlu. "Ülke Bilgi Güvenliği". 3**.Ulularası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı**, Ankara, 2008: 3.

Waller, Douglas. "Onward Cyber Soldiers". content.time.com/time/magazine/article/0,9171,983318,00.html [02.04.2018].

Wang, Vincent Wei-Cheng ve Gwendolyn Stamper. “Asymmetric War? Implications For China's Information Warfare Strategies”. **American Asian Review**. c.20. s.4 (2002): 167-207.

Willsher, Kim. "French Fighter Planes Grounded By Computer Virus". **The Telegraph**. https://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.htm [29.03.2018].

Whittaker, Jason. **The Cyberspace Handbook**. London: Routledge, 2003.

Wovels, Cristopher L. “Asymmetric Attention Visualizing The Uncertain Threat”. US Army Research Institute Research Report 2016, March 2010, Virginia.

Yağ, Mehtap. “Türkiye Savunma Harcamalarının Karşılaştırmalı Analizi (1924-2010)”. Yüksek Lisans Tezi. Karadeniz Teknik Üniversitesi, 2014.

Yalçın, Funda Güleç. "2018 Siber Tehdit Öngörüleri Raporu Yayınlandı". 02.01.2018, fintechtime.com/tr/2018/01/2018--siber-tehdit-ongoruleri-raporu-yayinlandi/?doing_wp_cron=1515812674.1795079708099365234375 [07.02.2018].

Yamaç, Fatih. **Siber Terörizm**. Emniyet Genel Müdürlüğü Terörle Mücadele Daire Başkanlığı Psikolojik Harekat Kurs Notları. Ankara: 2001, 5.

Yazıcı, Merve. “İlk Modern Siber-Atak: Estonya”. www.tuicakademi.org/ilk-modern-siber-atak-estonya [22.01.2018].

Yener, Zafer. “Siber Uzay Güvenliği: Ulusal Güvenlik ve Uluslararası Güvenliğe Etkileri”. Yüksek Lisans Tezi. Uludağ Üniversitesi, 2013.

Yıldız, Serdar ve Onur Murat Köprülü. **Asimetrik Savaş**. 2013.

Yılmaz, Ercan Nurcan, Halil İbrahim Ulus ve Serkan Gönen. “Bilgi Toplumuna Geçiş ve Siber Güvenlik”. **Bilişim Teknolojileri Dergisi**. c.8. s.3 (2015): 142.

Yılmaz, Sait. “Modern Savaş ve Savunma Reformları”. USAM Bülteni. www.academia.edu/7647876/Modern_Savaş_ve_Savunma_Reformları [27.05.2016].

Yılmaz, Sait ve Olay Salcan. **Siber Uzay'da Güvenlik ve Türkiye**. İstanbul: Milenyum Yayınları, 2008).

Yılmaz, Seda ve Şeref Sağıroğlu. "Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri". **6.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı**. Ankara, 2013: 158.

Yılmaz, Sefer. "Türkiye'nin İç Güvenlik Yapılanmasında Değişim İhtiyacı". **Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**. c.21. s.3 (2012): 33.

Zrnic, Bojan. "The New Trends in Defence Planning and Their Impact on the Defense Planning Systems in Transitional Countries". **Vojno Delo**. c.60. s.1 (2008): 27.

https://www.memurlar.net/haber/621386/tsk-siber-saldiri-ordusu-kuruyor.html, [15.04.2018].

http://www.haberturk.com/gundem/haber/1048546-turk-ordusunun-yeni-konsepti-siber-savunma [15.04.2018].

http://rewreward.blogspot.com/2013/01/turk-silahl-kuvvetleri-siber-savunma.html [24.04.2018].

http://www.hurriyet.com.tr/teknoloji/turk-ordusunun-yeni-kuvveti-siber-savunma-40113652 [ 24.04.2018].

http://www.webtekno.com/internet/tsk-siber-savunma-komutanligi-h17616.html [16.04.2018].

https://www.ssm.gov.tr/website/contentlist.aspx?PageID=1083&LangID=1 [16.04.2018].

http://www.tsk.tr/TSKdanHaberler/Haber_234 [16.04.2018].

https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense [09.04.2018].

https://www.sabah.com.tr/aktuel/2017/02/23/rusya-yeni-bir-siber-ordu-kurdu [08.04.2018].

http://www.bbc.com/news/world-europe-39062663 [08.04.2018].

https://www.gov.uk/government/news/uk-steps-up-cyber-defence [31.03.2018].

https://google.com.tr/amp/www.hurriyet.com.tr/amp/dunya/fransadan-siber-ordu-icin-1-milyar-dolar-40421504 [29.03.2018].

https://siberbulten.com/uluslararasi-iliskiler/rusya-siber-alanda-neden-saldiriyor [08.04.2018].

https://www.rbth.com/defence/2017/01/12/russias-cyber-army-hacks-a-spot-in-the-top-5_679221 [08.04.2018].

https://www.jewishpolicycenter.org/2013/12/31/russian-cyber-capabilities [08.04.2018].

http://www.hurriyet.com.tr/gundem/cin-super-gizli-ordusunu-acikladi-17884879 [04.04.2018].

https://tr.sputniknews.com/savunma/201505261015665817 [04.04.2018].

https://www.nasdaq.com/article/so-who-has-the-most-advanced-cyber-warfare-technology-cm861979/amp [02.02.2018].

https://www.nato.int/cps/en/natohq/official_texts_68828.htm [11.04.2018].

www.kaitseliit.ee/en/cyber-unit [31.03.2018].

https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf [11.04.2018].

www.trthaber.com/m/?news=kuzey-koreden-guney-koreye-sibersaldiri&news_id=255988&category_id=4 [15.06.2016].

https://siberbulten/uluslararasi-iliskiler/abd-iside-karsi-siber-savas-ilan-etti/ [24.04.2016].

https://www.btgunlugu.com/avusturalya-nin-kan-haritasi-calindi [29.01.2018].

http://www.mynet.com/haber/guncel/centcomun-sosyal-medya-hesaplari-hacklendi-1655161 [29.01.2018].

http://www.eurovizyon.co.uk/ekonomi/ingiliz-bankasinin-20-bin-musterisinin-hesabi-hacklendi-h47119.html [29.01.2018].

http://tr.euronews.com/2016/11/29/deutsche-telekom-a-siber-saldiri-korkusu [29.01.2018].

http://www.hurriyet.com.tr/teknoloji/linkedin-hesaplari-yine-calindi-40310869 [29.01.2018].

https://tr.sputniknews.com/asya/201712211031491296-kuzey-kore-abd-siber-saldiri-alakamiz-yok [29.01.2018].

http://www.ajansbt.com/2016-nin-en-buyuk-banka-soygunu.html [29.01.2018].

http://www.gazetevatan.com/elektrik-hatlarina-sabotaj-var-mi-bakan-albayrak-yanitladi-1025710-gundem [29.01.2018].

http://www.bloomberght.com/haberler/haber/1983567-siber-suclarin-yillik-zarari-400-500-milyar-dolar [29.01.2018].

https://tr.sputniknews.com/avrupa/201702071027104234-turk-hackerlar-avusturya-parlamentosunun-sitesine-saldirdi [29.01.2018].

https://www.haberler.com/20-milyon-kisinin-kimlik-ve-banka-hesap-bilgileri-9546131-haberi [29.01.2018].

http://digitalage.com.tr/arastirma-kisisel-bilgileriniz-siber-dunyada-ne-kadara-satiliyor [30.01.2018].

http://www.hurriyet.com.tr/dunya/iranli-hackerlardan-turkiyeye-siber-saldiri-27709465 [30.01.2018].

http://thehackernews.com/2015/01/police-ransomware-suicide.htm [30.01.2018].

http://www.gazetevatan.com/yolcu-ucagina-siber-saldiri-791885-dunya [30.01.2018].

http://cybertoday.org/index.php/2017/05/18/amerikan-ordusuna-ait [30.01.2018].

http://www.hurriyet.com.tr/ekonomi/siber-saldirilarin-maliyeti-2-1-trilyon-dolar-40486872 [30.01.2018].

http://www.milliyet.com.tr/hackerlar-bir-enerji-santralinin-teknoloji-haber-2575449 [30.01.2018].

https://www.nato.int/docu/review/2017/Also-in-2017/nato-priority-spending-success-cyber-defence/TR/index.htm [10.04.2018].

http://bianet.org/biamag/toplum/130283-savaslar-siber-uzaya-tasiniyor [20.03.2018].

http://sge.bilgem.tubitak.gov.tr/tr/nato-ccdcoe-daimi-temsilciligi [11.04.2018].

https://www.google.com.tr/amp/s/safeandsavvy.f-secure.com/2017/03/20/top-5-countries-with-offensive-cyber-capabilities/amp [05.02.2018].

“Internet Usage Statistics: The Internet Big Picture”. http://www.internetworldstats.com/stats.htm [25.01.2018].

https://www.nato.int [16 Haziran 2016].

The Economist. “Cyber Warfare: Newly Nasty”. http://www.economist.com/node/9228757 [22.01.2018].

https://www.gartner.com/newsroom/id/3598917 [07.02.2018].

map.norsecorp.com/#/ [07.02.2018].

https://cybermap.kaspersky.com [07.02.2018].

https://www.google.com.tr/amp/s/m.dunya.com/amp/sektorler/teknoloji/2017de-turkiyede-gunde-475-siber-saldiri-yasandi-haberi-401291 [07.02.2018].

**"Dikkat WannaCry Siber Saldırısı Tüm Dünyayı Etkisi Altına Aldı"**. https://www.teknokulis.com/haberler/guvenlik/2017/05/13/dikkat-wannacry-siber-saldirisi-tum-dunyayı-etkisi-altina-aldi/amp [03.02.2018].

https://threatpoint.checkpoint.com/ThreatPortal/threat?threatType=publication&threatId=1561 [31.01.2018].

www.stratcom.mil/Media/Factsheets/Factsheets-View/Article/960492/us-cyber-command-uscybercom [28.03.2018].

http://www.arcyber.army.mil [28.03.2018].

https://obamawhitehouse.archives.gov/the-press-office/2014/02/12/launch-cybersecurity-framework [02.04.2018].

https://www.cybersecurityintelligence.com/blog/which-countries-are-ready-for-cyberwar-2763.html [01.02.2018].

# EKLER

## EK-1: Görüşme Soruları

### "Savunma Planlama Yaklaşımlarındaki Dönüşüm"
### Görüşme Soruları

1. Savunma Planlama Anlayışları, Stratejik Öngörü İhtiyacının Giderek Arttığı Günümüzde Nasıl Bir Değişim Göstermektedir?

2. Belirsizlikle Mücadele Edebilmek İçin Birçok Yöntemin Uygulanabilmesi Mümkün Olmakla Birlikte, Tehdit Boyut Ve Şeklinde Yaşanan Hızlı Değişim Karşısında Başarılı Olunduğu Söylenememektedir. Bu Konudaki Düşünceleriniz Nelerdir?

3. Savunma Planlama Sürecinin Başarısı; Planlamacıları Yönlendirecek Açık Ve Belirgin Bir Devlet Politikasının (Savunma Politikası) Varlığına Bağlıdır. Asimetrik Tehdit Ortaminda Verilecek Politika Planlama Sürecini Yönlendirmede Yeterli Olabilecek Midir?

4. Savunma Planlamasında Esneklik Nasil Sağlanabilir?

5. Tehdit Değişiminin Hızlı Olduğu Günümüzde Savunma Planlamasında Sivil Yeteneklerden Etkili Bir Şekilde Yararlanmak Mümkün Olabilir Mi?

6. Yetenek Temelli Savunma Planlamasının Özünü Yetenek Havuzu Matrisinin Tam Ve Doğru Bir Şekilde Oluşturulması Teşkil Etmektedir. Asimetrik Tehdit Ve Özellikle DEAŞ Gibi Aniden Ortaya Çikan Terör Grupları Dikkate Alındığında Yetenek Havuz Matrisi Gerçekçi Bir Şekilde Oluşturulabilir Mi?

7. Caydırıcılık Temelli Savunma Planlama Yaklaşımının Teknolojideki Gelişime Bağlı Olarak Önem Kazandığı Görülmektedir. Yetenek Temelli Planlama İle Birlikte Uygulanabilir Mi?

8. Gray, 1991 Yılındaki Çalışmasında: “Planlamacıları Bekleyen En Çetin Görevlerden Birinin, Sürprizlerin Kötü Sonuçlar Karşısında En Yüksek Korumayı Sağlayan Yaklaşımı/Yaklaşımları Bulabilmek” Olduğunu İfade Etmiştir. Bu İfade Günümüz Şartlarında da Geçerli Midir?

9. Savunma Planlamasinda Uzun Dönemli Planlama Sürecinin Sona Erdiğini Söylemek Mümkün Müdür?

10. Yetenek Temelli Savunma Planlama Yaklaşımında Yetenek Uyumsuzluğu Söz Konusu Olması Halinde Neler Yapilabilir?

# ÖZ GEÇMİŞ


**Adı Soyadı** : Görkem KILINÇÇEKER

**Doğum Yeri ve Tarihi** : İzmir / 04.01.1986

**Yabancı Dili** : İngilizce

**İletişim** :

**Tel** : 0530 693 01 10

**E-posta** : grkmklncckr@gmail.com


**Eğitim Durumu** :

**Lise** : Maltepe Askeri Lisesi

**Lisans** : Kara Harp Okulu

**Yüksek Lisans** : Kara Harp Akademisi ve Yıldız Teknik Üniversitesi

**Çalıştığı Kurumlar ve Yıl** : 2008-2014 54'üncü Mknz.P.Tug.K.lığı/Edirne
2014-2017 3'üncü Kor.K.lığı NRDC-T/İstanbul
2017-……. 7'nci Kor.K.lığı/Diyarbakır

**Diğer Konular** :