Politik Psikoloji Dergisi

The Journal of Political Psychology

Araştırma Makalesi Research Article

21. YÜZYILDA SAVUNMA PLANLAMASI: GÜNCEL KONULAR VE TEHDİTLER

Fatma Nur Özkaya*

Öz: Savunma yönetimi, ülkenin bekasının ve menfaatlerinin sağlanması amacıyla hem bugünü hem de geleceği düşünerek mevcut kaynakların en etkin şekilde kullanılması ile ülkenin genel stratejik planlamasının yapılmasıdır. Savunma yönetimi uzun vadeli savunma planlaması ile stratejik yönlendirme ve savunma tedariki faaliyetlerinden oluşan bütünleşik bir sistemdir. Savunma planlamaları ülkelerin milli menfaatlerini gerçekleştirmek ve güvenliklerini sağlamak için mevcut kaynakların en etkin şekilde kullanılması ile uzun vadede silahlı kuvvetlerin nasıl bir yapıda olması gerektiği hususunda hazırlıklı olmayı ifade etmektedir. Tarihin belirli dönemlerinde farklı savunma yönetimi yaklaşımlarının varlığı yıllar içerisinde toplum ve devletlerin karşılaştıkları tehdit ve risklerin farklılık gösterdiğini gözler önüne sermektedir. Soğuk Savaş

* Doktora Öğrencisi, Milli Savunma Üniversitesi Alparslan Savunma Bilimleri ve Milli Güvenlik Enstitüsü-Savunma Yönetimi Programı, fatmanurkaya06@gmail.com, ORCID: 0000-0001- 9623-1433.
Doi: 10.5281/zenodo.16028428.

Geliş Tarihi: 15 Şubat 2025 Kabul Tarihi: 13 Mayıs 2025
Received: 15 February 2025 *Accepted: 13 May 2025*

Bu makaleye atıf için/ *To cite this article:* Özkaya, F. N., (2025*).* 21 Yüzyılda Savunma Planlaması: Güncel Konular ve Tehditler**.** *Politik Psikoloji Dergisi*, 5(1), 62-88.

döneminin bitimini takiben dünyanın daha farklı tehditler ve güvenlik sorunlarıyla karşılaşması savunma planlamacılarının daha karmaşık ve belirsiz bir süreçle karşı karşıya kalmalarına sebep olmuştur. Tehditlerin ne zaman ve nereden geleceğinin belirsizleşmesi savunma planlamalarının esnek ve birçok farklı senaryoya uygun yapılması gerekliliği sonucunu ortaya çıkarmıştır. Amerika Birleşik Devletleri'nde (ABD) 11 Eylül 2001 tarihli terör saldırısı devletlerin ve toplumların gündemine asimetrik savaş kavramını yerleştirmiş ve savunma planlaması üzerinde etki bırakan göç, hibrit savaş, siber savaş, asimetrik savaş gibi yeni durumlara uygun savunma planlamaları yapma gerekliliği hasıl olmuştur. Güncel tehditlerin savunma planlamaları üzerindeki etkisini ortaya koymayı amaçlayan bu çalışmada yeni tehditler ayrı başlıklar şeklinde ele alınarak savunma planlaması süreci kapsamında değerlendirilecektir. Ancak çalışma güncel tehditlerin tamamını çalışmaya dahil etmemesi nedeniyle bazı sınırlılıklara sahiptir.

Anahtar Kelimeler: Savunma Planlaması, Asimetrik Tehdit, Siber Tehdit, Hibrit Savaş, Göç

DEFENSE PLANNING IN THE 21ST CENTURY: CURRENT ISSUES AND THREATS

Abstract. *Defense management is the overall strategic planning of the country with the most effective use of available resources, considering both the present and the future in order to ensure the country's survival and interests. Defense management is an integrated system consisting of long-term defense planning, strategic guidance and defense procurement activities. Defense planning refers to the most effective use of existing resources in order to realize the national interests of countries and to ensure their security, and to be prepared for what kind of structure the armed forces should have in the long term. The existence of different defense management approaches in certain periods of history reveals that the threats and risks faced by societies and states have changed over the years. Since the end of the Cold War, the world has faced different threats and security problems, which has led defense planners to face a more complex and uncertain process. The uncertainty of when and where threats will come from has led to the necessity of making defense planning flexible and suitable for many different scenarios. The September 11, 2001 terrorist attack in the United States placed the concept of asymmetric warfare on the agenda of states and societies, and defense planning in accordance with new situations such as migration, hybrid warfare, cyber warfare, asymmetric warfare which have an impact on defense planning. This study, which aims to reveal the impact of*

current threats on defense planning, will address new threats separately and evaluate them within the context of the defense planning process. However, the study has some limitations because it does not include all current threats.

Keywords: *Defense Planning, Asymmetric Threat, Cyber Threat, Hybrid Warfare, Migration.*

GİRİŞ

"Bilgi ve Teknoloji Çağı" şeklinde nitelendirilen 21. yüzyılda, küreselleşen yeni bir dünya düzeni ve bu düzende ortaya çıkan terörizm, siber saldırılar, ekonomik krizler, doğal afetler ve salgın hastalıklar gibi yeni tehditlerden bahsedilebilir. Güvenlik olgusu tarihin her döneminde topluluklar ve devletler için yaşam için gerekli olan temel faaliyetlerin varlığı ve toplumsal yaşantının süreklilik göstermesi açısından vazgeçilmez nitelikte bir kavram olmuştur. Önemli bir motivasyon teorisi olarak kabul gören Maslow'un "İhtiyaçlar Hiyerarşisi" Kuramına göre de güvenlik kavramına ikinci basamakta yer verilmiştir. Bu durum, insanların fizyolojik ihtiyaçlarından sonra en temel ihtiyacının güvenlik olduğunu göstermektedir. Nitekim insanların toplu olarak yaşamasıyla birlikte gruplar arası mücadeleler başlamış ve kitlesel çatışmaların varlığı, bir güvenlik meselesi olarak, savaşları ortaya çıkarmıştır.

Tarih boyunca mücadele ve savaşların pek çok farklı amaç için yapıldığı ifade edilebilir. Örneğin nüfusun az olması ve kaynakların az olan nüfusa göre kıt olmaması nedeniyle tarihin ilk dönemlerinde insanlar arasında bir mücadeleden ziyade insanların doğaya karşı hayatta kalma mücadelesi verdiği ifade edilebilir. 1648 Westphalia Antlaşması ile ortaya çıkan ulus devlet kavramı (Özkaya, 2020: 331) sonrasında savaşlar önemli bir dönüşüm geçirmiş ve modern savaşlar dönemi başlamıştır. Modern savaşlarla birlikte daha çok dini amaçlarla yapılan savaşlar ulus devlet savaşına doğru evirilmiş ve savaşların topyekûn uluslar arasında gerçekleşiyor olması zorunlu askerlik sistemi gibi sistemlerin getirilmesine vesile olmuştur (Begenirbaş, 2022: 141). O halde günümüzde gerçekleşen savaşlarla ilgili olarak modern savaşların başlangıcı kabul edilen Westphalia Antlaşması önemli bir yer teşkil etmektedir.

Küreselleşen yeni dünya düzeni ile birlikte savunma anlayışı değişikliğe uğramıştır. Şöyle ki ülkeden ülkeye tehdit algısı olarak anlaşılan klasik savunma anlayışı yerine nitelik olarak daha asimetrik ve belirsiz olan yeni tehditler ortaya çıkmıştır. Bahsedilen bu yeni tehditlere örnek olarak kitle imha silahları, terörizm, siber tehditler, etnik çatışmalar, göçler, ekonomik yaptırım ve ambargolar, enerji mücadeleleri söylenebilir (Doğan, 2022: 52; Begenirbaş,

2022: 142). Ülkeler bir taraftan bu değişikler çerçevesinde savunma politikalarını yeni tehditlere uyumlu hale getirmeye çabalarken bir taraftan da toplumlar tarafından savunma harcamalarının maliyetlerinin sorgulanmaya başlanmasıyla birlikte savunma harcamalarını daha şeffaf ve etkin halde yapmaya gayret göstermektedirler. Savunma harcamalarının toplumların daha fazla ilgisini çekiyor olmasının şüphesiz birden fazla nedeni bulunmaktadır. Bu nedenlerden biri savunma için ayrılan kaynakların zaten sınırlı olan kaynaklar içerisinde toplumun refahını arttırmaya yönelik yatırımlara ayrılan kaynakların miktarını azaltıyor olması iken diğer bir neden ise politika, savunma, ekonomi, sağlık, güvenlik gibi ülkenin tamamını kapsayan ve ilgilendiren konuların birbirlerinden bağımsız şekilde değerlendirilmelerinin yanlış olacağı yönünde gelişen anlayıştır (Korkmazyürek, 2018: 17, 18).

Bu çalışmanın amacı 21. yüzyılda ortaya çıkan güncel tehditlerin savunma planlamaları üzerinde nasıl bir etkisi olduğunun ortaya çıkarılmasıdır. Bu amaçla öncelikle kavramsal çerçevenin oluşturulabilmesi adına savunma yönetimi ve savunma planlaması kavramlarının tanımı, kapsamı ve süreçlerinden bahsedilecektir. Bu açıklamaları takip eden bölümde ise savunma planlamasını etkileyen güncel tehditler; asimetrik savaş, hibrit savaş, siber tehdit ve göç başlıkları altında detaylandırılarak aktarılacaktır.

I. SAVUNMA YÖNTEMİ VE SAVUNMA PLANLAMASI

I.A.SAVUNMA YÖNETİMİ

Savunma, TDK sözlüğünde "*saldırıya karşı koyma, müdafaa*" şeklinde tanımlanmıştır (TDK, 2023). İnsanların ihtiyaç duyduğu temel gereksinimlerden biri olan ve savaşların nedenlerinden birini oluşturan savunma, bu eylemi başarılı şekilde gerçekleştirebilen devletlerin varlıklarını devam ettirebilmelerini sağlarken başarısız savunma gerçekleştirilen devletlerin ise mağlup olmalarına sebep olmaktadır. O halde devletlerin varlıklarının devamlılığının savunma yetenek ve kapasitelerine bağlı olduğu ifade edilebilir. Savunmanın önemini vurgulayan ünlü ekonomist Adam Smith savunmanın önemine vurgu yapmak için zenginlikten daha önemli olan tek şeyin savunma olduğunu dile getirmiştir (Çalış Yazgu & Bekmezci, 2023: 8, 9).

Savunma yönetimi, ülkelerin bekası ile milli menfaatlerini gerçekleştirmek niyetiyle hem bugünü hem de gelecekte oluşabilecek riskleri düşünerek caydırıcılığı sağlamak maksadıyla stratejik planlar dahilinde yapılan faaliyetler bütünü olarak tanımlanabilir (Öz & Çalışkanlar, 2020: 311). Savunma yönetimi ayrıca savunmaya ayrılan her türlü kaynağın etkin şekilde kullanılması yönünde girişimlerde bulunmayı da gerektirmektedir (Begenirbaş & Bekmezci, 2023). Silahlı kuvvetlerin operasyonel performansını en üst düzeye çıkarmak savunma yönetiminin temel amaçları arasında yer alır (Çalış Yazgu & Bekmezci, 2023:

11). Yönetimin 5 fonksiyonu olan planlama, örgütleme, yöneltme, koordine etme ve kontrol savunma yönetim faaliyetleri için de temel teşkil etmektedir (Begenirbaş, 2022: 2-9). Yönetimin fonksiyonları ile savunma yönetimindeki yansıması Tablo 1'de yer almaktadır (Korkmazyürek, 2018:26).

Tablo 1: Türkiye'de Savunma Yönetimi Sürecinde Yönetim Fonksiyonları ve Savunma Yönetimi İlişkisi

Yönetim Fonksiyonları ve Savunma Yönetimi İlişkisi		
Yönetim Fonksiyonu	Savunma Yönetimindeki Yansıması	
	Faaliyet	Dokümanlar
Planlama	PPBS Faaliyetleri	MGSB, TÜMAS, SHP, OYTEP, Bütçe
Organize Etme	Kuvvet yapısı oluşturma, Kaynak tahsisi çalışmaları, Personel temin ve yerleştirme	Harbe hazırlık, Kuvvet yapısı, İnsangücü planı
Yönlendirme	MGSB, TÜMAS, PPD hazırlıkları, Konsept çalışmaları	MGSB, TÜMAS, PPD, Konseptler
Kontrol	SHP, OYTEP gözden geçirme süreci, Bütçe uygulama kontrol, Rutin dönemsel diğer kontroller	Gözden geçirme dokümanları

Kaynak: Korkmazyürek, 2018

Savunma yönetiminin ortaya çıkışında etkili olan temel faktörlerden biri savunma organizasyonlarıyla ilgili olarak insan kaynakları ve bütçe tahsisi ile savunmayı yönetme sürecinde ortaya çıkabilecek sorunları çözme gayretidir (Çalış Yazgu ve Bekmezci, 2023: 10). Stratejik savunma yönetimi stratejik yönlendirme, kuvvet planlaması, silahlanma planlaması şeklinde alt planlama faaliyetlerinden oluşmaktadır. Kuvvet planlaması, kuvvetlerin oluşturulması süreci ile ilgili olup şimdiki zaman ve gelecek zaman için kuvvetlerin hangi birliklerden oluşturulacağını ortaya koyar. Kuvvet planlaması sonucunda oluşturulan kuvvetlerin hangi silah ve malzeme ile donatılacağının belirlendiği süreç ise silahlanma planlamasını oluşturur. Silahlanma ve kuvvet planlamaları 'Savunma Tedarik Sistemi' ile bütüncül bir yapı içerisinde yer almaktadır (Korkmazyürek, 2018: 24).

Şekil 1: Stratejik Savunma Yönteminin Alt Grupları

Kaynak: Korkmazyürek, 2018

Türkiye'de uygulanan savunma yönetim süreci stratejik yönlendirme, savunma planlaması ve savunma tedariki şeklinde üç temel faaliyetten oluşmaktadır. Savunma planlaması savunma yönetimi sürecinin içerisinde yer alan temel bir faaliyet olarak yer almaktadır. Stratejik yönlendirme aşaması ile savunma yönetimi süreci başlamış olurken fiili olarak sürecin başlaması savunma planlaması ile gerçekleşir. Savunma politikaları bağlamında hangi yeteneklerin nasıl ve ne zaman kazanılacağının tespit edilmesi nedeniyle savunma planlaması oldukça kritik bir süreçtir (Begenirbaş, 2022: 13,14). Bir sonraki başlıkta savunma planlaması detaylı şekilde aktarılacaktır.

I.B. SAVUNMA PLANLAMASI

Savunma planlaması milli hedefleri elde etme, milli menfaatleri koruma ve ülkenin bekasını sağlamayı hedefleyen ve bu hedef ile beraber ülkenin sahip olduğu kaynakların etkin ve verimli kullanılmasını sağlayan bir süreç olarak ifade edilebilir (Korkmazyürek, 2018: 32). Savunma planlaması ülkelerin kısa ve uzun vadede silahlı kuvvetlerinin nasıl bir yapıda olması gerektiğiyle ilgili hazırlıklı olunmasını sağlar. Dolayısıyla savunma planlamasının odağında gelecek kabiliyetlerin de yer aldığı ifade edilebilir (Davis & Finch, 1993). Tehditlerin savunma planlamaları oluşturulurken öncelikli olarak göz önünde bulundurulması gerektiği ifade edilebilir (Çalış Yazgu ve Bekmezci, 2023: 10). Savunma planlaması ülkenin savunma kapasitesini arttırma gayesi ile çeşitli faaliyetleri içeren ve askeri tehditler yanı sıra terörizm, asimetrik tehditler, siber tehditler ve doğal afetler gibi farklı güvenlik tehditlerine hazır olmayı amaçlayan bir süreçtir. Görüldüğü üzere kapsamı oldukça geniş olan savunma planlamasının içerisinde tehdit değerlendirmesi, askeri doktrin geliştirme,

donanım tedariki ve personel eğitimleri şeklinde farklı nitelikte faaliyetler yer almaktadır (Gürbüz & Beyaz, 2023: 4)

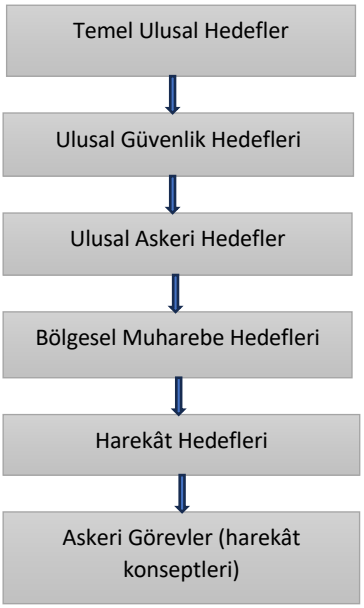
Ülkenin genel stratejik planlamasının bir bölümü olan stratejik savunma planlaması, tarihsel olarak değişen tehdit koşulları nedeniyle geçmişten bugüne kadar farklı yaklaşımlar şeklinde ortaya çıkmıştır (Tunca ve Özkil, 2020: 194). Nitekim 2. Dünya Savaşına kadar tehdidin belirsizlik düzeyinin çok az olması, düşmanın kim olduğunun ve gücünün bilinir olması, tehdidin çok iyi tanımlanmış olması, savaşın yapılacağı alanın belirgin olması vb. şeklindeki koşullar nedeniyle savunma planlama yaklaşımı olarak kadro temelli yaklaşım kabul edilmiş ve düşmanın sahip olduğu güçten nicelik olarak daha fazla güce sahip olmanın zafer kazanmak için yeterli olacağı kabul görmüştür (Kahraman, 2016: 104-105). Soğuk Savaş Döneminde ise savunma planlamasının temelini tehdide dayalı planlama anlayışı oluşturmuş ve bu anlayışta esas amaç caydırıcılığı sağlamak olmuştur. (Korkmazyürek, 2018: 48).

Tablo 2: Tarih Boyunca Uygulanan Planlama Yaklaşımları

Dönem	**Tehdit Özelliği**	**Planlama Yaklaşımı**
Soğuk Savaş Dönemi öncesi	Tehdit belirgin ve iyi tanımlanmış	Kadro Temelli
Soğuk Savaş Dönemi	Tehdit belirgin ve iyi tanımlanmış	Tehdit Temelli
Soğuk Savaş Sonrası Dönem	Tehdit belirgin değil ve tanımlanması zor	Yetenek Temelli
11 Eylül 201 sonrası	Asimetrik tehditler mevcut ve tehdit çok değişken	Yetenek Temelli (Senaryo Uzayı) Planlama

SSCB'nin dağılmasıyla birlikte terörizm, isyanlar, etnik çatışmalar, uluslararası suç örgütleri gibi tehditler yeni boyutlar kazanmıştır. Asimetrik tehditlerde yaşanan bu artışın yansıması olarak savunma planlaması yaklaşımında yetenek temelli planlama yaklaşımı öne çıkmıştır. Hayal gücündeki başarısızlıklar ifadesini meşhur hale getiren 11 Eylül terör saldırısından sonra ABD kendisini daha önce deneyimlemediği ancak yön verdiği bir savaşın içerisinde bulmuştur. Bu yeni savaş için benzer bir senaryo ve taktiği olmaması nedeniyle savaş ile mücadelesi esnasında askeri yetkililer anlık kararlarla hareket etmek durumunda

kalmışlardır. Dolayısıyla bu durum tüm ülkeler için farklı senaryolara ve tehditlere karşı yetenekler geliştirmiş olmanın gerekliliği hususunda önemli bir örnek teşkil etmiştir (Tunca ve Özkil, 2020: 195; Davis, 2018: 380). Açıkça ifade etmek gerekirse 11 Eylül terör saldırısından sonra dünya güvenlik, terörizm, insan hakları, özgürlük, savaş, siyaset, hukuk, ekonomi vb. pek çok alanda değişim ve dönüşümlerle yüzleşmeye başlamış ve geri dönülmez yeni bir sürece evirilmiştir (Arslan, 2022: 553).Ülkelerin kendi çıkarlarını koruyabilmeleri için milli güç unsurlarını oluşturan ekonomik, sosyal, coğrafi, politik, askeri yeteneklerini geliştirmesi ve muhafaza etmesi gerekmektedir. Milli güç unsurları ülkelerin gücünü ortaya koymaktadır. Milli güç unsurlarına ait yeteneklerin nasıl korunacağı ve geliştirileceği ülkede ilgili kurumların geliştirdiği stratejiler ile belirlenir. Sayılan bu yetenekler içerisinde "askeri yeteneklerin" oluşturulması ve korunması hususu stratejik savunma planlaması faaliyetlerine dahildir. Güvenlik politikalarının uygulanmasında büyük bir öneme sahip milli güç unsurlarından olan silahlı kuvvetlere verilen vazifelerin başarılması için gerekli askeri politikaları belirleyen temel dokümanlar savunma politikalarıdır. Stratejik savunma planlaması bu noktada en öncelikli konuları belirlemelidir. (Korkmazyürek, 2018: 31). Savunma planlaması sürecinin Kent ve Simons'ın değerlendirmesi ile bir amaçlar hiyerarşisini takip ettiği ifade edilebilir. Yazarların bahsettiği bu hiyerarşi, Şekil 2'de gösterilmiştir:



Şekil 2: Amaçlar Hiyerarşisi

Kaynak: Kent ve Simons, 1994

Türkiye'de uygulanan savunma planlama süreci ile ilgili olarak öncelikle Planlama Programlama ve Bütçeleme Sistemi (PPBS) 'den bahsedilecektir. Planlama Programlama ve Bütçeleme Sistemi (PPBS) çok uzun süredir başta ABD olmak üzere pek çok gelişmiş ülkenin temel planlama yaklaşımı olarak kullandığı bir sistemdir. Bu sistemde planlamacıların mali imkanlar ışığında planlama yapmasını sağlamak için bütçenin planlamayı desteklemesini sağlamak hedeflenmektedir. Türkiye'de PPBS süreci kapsamında Türkiye'nin Milli Askeri Stratejisi (TÜMAS), Harekât İhtiyaç Planları (HİP) ve Stratejik Harekât Planları (SHP) şeklinde hazırlıklar yapılmaktadır (Berk, 2015: 6). Bu planlardan önce Türkiye'nin ulusal savunma ile güvenlik stratejisi, MGK Genel Sekreterliği önderliğinde yürütülen ve beş yılda bir güncellenen Milli Güvenlik Siyaset Belgesi (MGSB) ile oluşturulmaktadır. Milli hedefler doğrultusunda izlenecek iç ve dış güvenlik ile savunma siyasetine ilişkin yol haritasını belirleyen MGSB doğrultusunda Türkiye'nin Milli Askeri Stratejisi (TÜMAS) belgesi hazırlanmaktadır. TÜMAS oluşturulurken MGSB doğrultusunda teknolojik, politik, tehdit, askeri durum ve politik askeri durum değerlendirmeleri yapılmaktadır. TÜMAS, askeri stratejik yönlendirmeyi sağlayan belge olarak ifade edilebilir (Korkmazyürek, 2018:86). TÜMAS'ı Stratejik Harekât Planları (SHP) ile On yıllık Tedarik Programı (OYTEP) takip eder ve bu planlar üç yılda bir tekrar gözden geçirilir (Çelik, 2020: 117, 118, 119).

Soğuk Savaş döneminin bitimiyle beraber savunma planlaması yapılmasını güçleştiren tehdidin nereden ve ne zaman geleceğinin kestirilemediği belirsizlikler oldukça artış göstermiştir. Bu belirsizlikler hâlihazır tehditlerin içindeki belirsizlikler, muhtemel şoklar, savunmaya ayrılacak kaynakların miktarındaki belirsizlikler ile kullanılacak teknolojideki belirsizlikler şeklinde bir ayrıma tabi tutulabilir (Meydan ve Demirel, 2010: 15, 16). Bahsedilen belirsizlikler ülkelerin güvenlikleri için risk oluşturan yeni tehditleri beraberinde getirmiştir. Bir sonraki bölümde bu tehditler ve savunma planlamaları üzerindeki olası etkilerinden bahsedilecektir.

II. SAVUNMA PLANLAMASINI ETKİLEYEN GÜNCEL TEHDİTLER

1945-1991 yıllarını kapsayan Soğuk Savaş Dönemi iki kutuplu dünya düzeni şeklinde ifade edilmiştir bu şekilde ifade edilmesinde iki tarafın da nükleer güce sahip olması ve birbirlerine yönelik geliştirdikleri savunma stratejilerinin temelini caydırıcılığın oluşturması etkili olmuştur. Ancak SSCB ekonomisi caydırıcılık stratejisinin gerektirdiği mali yükü kaldıramamış ve SSCB'nin nihai olarak dağılması ile birlikte iki kutuplu dünya düzeni yerini tek kutuplu dünya düzenine bırakmıştır. ABD Başkanı George Bush bu dönem için "*yeni dünya düzeni*" ifadesini kullanmıştır. Dünyanın alışık olmadığı tek kutuplu dünya

düzenine geçilmesi ABD'de de bir şaşkınlıkla karşılanmış ve yeni stratejiler geliştirilmeye başlanmıştır (Coşkun, 2017: 112). Bu dönemde güvenlik inşasında yeni bir bakış açısının ortaya konduğu aşikâr olmakla beraber geleneksel güvenlik anlayışından tamamen uzaklaşıldığı söylenemez (Gül, 2016). 11 Eylül 2001 tarihinde ABD Dünya Ticaret Merkezi'ne yapılan terör saldırılarıyla da tehdit algısı ve bu tehditlere karşı geliştirilmesi gereken yetenekler değişikliğe uğramıştır (Begenirbaş ve Can Yalçın, 2020: 184). 'Yeni Dünya Düzeni' şeklinde tabir edilen dönem tehditlerin çeşitlenmesi, alışılmışın dışında tehditlerle karşılaşılması, belirsizliklerin artması şeklindeki nedenlerle aslında yeni dünya düzensizliğine evirilmiştir (Coşkun, 2017: 113). Bu dönem Clausewitz'in ifade ettiği "*her çağ kendi savaşını yaratır*" sözünü doğrular şekilde tehditler ve savunma yöntemleri yönünden önceki dönemlerden ciddi ölçüde farklılık göstermiştir (Özer, 2018: 30).

Avrupa Birliği'nin (AB) 2003 yılına ait olan Güvenlik Strateji Raporu'nda belirttiği üzere "*günümüz tehditleri açık askeri tehditler değildir ve bu nedenle de hiçbiri yalnızca askeri müdahale ile ortadan kaldırılamaz*". Raporda ayrıca Soğuk savaş sonrası iç ve dış güvenliğin ayrılmaz şekilde birbirine bağımlı hale geldiği ve küresel zorluklar nedeniyle uluslararası ilişkilerde devlet dışı grupların rollerinin arttığından bahsedilmiştir (European Union Committee, 2003). Benzer şekilde Kuzey Atlantik Antlaşması Örgütü (NATO)'nün yeni tehdit algılamasına uluslararası terörizm, kitle imha silahları, uluslararası suçlar, insan haklarının ihlali gibi unsurlar dahil edilmiştir (Korkmazyürek, 2018: 136). Önceki zamanlarda toprağını genişletmek için saldırıda bulunabilecek potansiyeli olan ülkeler tehdit unsuru olarak görülürken, artık nükleer silahlardan arınmayan, çevre kirliliğine neden olan, terör faaliyetlerine ve uluslararası suç örgütlerine destek olan ülkeler ve şiddeti artan ekonomik rekabet, insan hakkı ihlalleri, siber saldırılar, terörizm şeklindeki tehdit unsurları güvenlik riski olarak kabul edilmektedir (Coşkun, 2017: 114).

21. yüzyılda teknolojinin hızlı şekilde gelişmesi, Soğuk Savaş döneminin bitmesi ve yeni devletlerin ortaya çıkması, farklı savaş yaklaşımlarının ortaya çıkması tehdit algısını dönüştürmüş ve daha öncesinde alışık olunmayan güncel tehditlerin belirmesine yol açmıştır. Dolayısıyla savunma planlamacıları beliren bu yeni tehditlere uyumlu şekilde planlamalar yapmak ile meşgul hale gelmiştir (Begenirbaş, 2022: 142). Yaşanan küreselleşme ve hızlı teknolojik gelişmelerle birlikte yalnızca devletler arasında görülen az aktörlü savaşlar yerini çok aktörlü (terör örgütleri, yabancı savaşçılar, organize suç örgütleri vb.), daha az maliyetli ve daha kısa sürede sonlanması amaçlanan, savaş sahasının ve zamanının belirsizleştiği, sivil-asker ayrımının kalktığı bir hibrit savaş ortamına bırakmıştır (Aytuğ ve Pozan, 2023: 2). İzleyen bölümlerde savunma planlamasını etkileyen güncel tehditler olarak asimetrik tehditler, göç, siber tehditler, hibrit savaşlar incelenecektir.

II.A. ASİMETRİK SAVAŞ

Asimetrik savaş kavramının kökeninin "Savaş Sanatı" adlı eserinde "*tüm savaşların aldatma ve şaşırtmaya dayandığı*" yönündeki ifadesi nedeniyle Sun Tzu'ya dayandığı ifade edilebilir. Mao'nun "Savaş Sanatı" eserinde "sürekli saldırı" ve "düşmanı rahat bırakmamak" tekniklerine yapılan vurgu da asimetrik özelliğin anlaşılması yönünde kıymetlidir (Özdoğan, 2017: 1).

Savaşlarda taraflardan birinin zafer kazanmış olması için simetrik değil asimetrik niteliklere sahip olması ve böylece bir tarafın diğerine karşı bir üstünlük elde edebiliyor olması gerekmektedir. Simetrik savaş, savaş için düzenli orduların konuşlandırıldığı ve tarafların benzer silah ve teknolojilerle hareket ettiği savaş şeklidir (Karasoy, 2022a: 63). Asimetrik savaş kavramı ise, güç açısından birbirine denk olmayan taraflar arasındaki savaş olarak ifade edildiği gibi, bir başka tanımda güçsüz tarafın güçlü tarafa beklenmeyen, sürpriz bir zaman ve taktikle saldırarak küçük bir ordu ile daha büyük bir askeri güce karşı savaşta üstünlük sağlaması şeklindedir (Küçükşahin & Akkan, 2007: 50).

Asimetrik savaşların simetrik savaşlardan ayrıldığı yönleri aşağıda yer verildiği şekildedir (Küçükşahin & Akkan, 2007: 52);

- Asimetrik tehditler alışılmadık, kuralsız ve sıra dışıdır.
- Asimetrik tehditlerde amaç yalnızca saldırıda bulunmak değildir; diğer alanlarda gücün zayıflatılması ve bu şekilde dengeleme olması da amaçlar arasındadır.
- Asimetrik saldırılara orantılı ve aynı türde karşılık vermesi oldukça zordur.
- Asimetrik tehditler özellikle sivil ve elbette askeri varlıkları tehdit etmektedir.
- Asimetrik tehditler bilinmeyenin gizeminden yararlanarak korkutucudurlar ve güvenlik birimlerini tehdidin nereden geleceğini bilemedikleri için zor durumda bırakırlar.

Kavramsal olarak asimetrik savaş, ABD tarafından 1990'lı yıllarda ortaya atılmış ve 2001 yılında olgunlaşmış bir kavramdır. Asimetrik savaş ifadesi 11 Eylül saldırısına kadar daha çok düzensiz savaşları ifade etmek için kullanılırken bu tarihten sonra çoğunlukla terör faaliyetleri ile ilişkilendirilerek kullanılmıştır (Demirel, 2012: 24). 1941 yılındaki Pearl Harbour baskınından sonra ABD sınırları içerisinde ikinci saldırı olma özelliği taşıyan 11 Eylül 2001 terör saldırısı, sivil hava uçaklarının kaçırılarak Pentagon ve Dünya Ticaret Merkezi'ne çarpması nedeniyle 3000 civarında kişinin ölümüne ya da kaybolmasına yol açmıştır. Bu tarihten sonra başta Amerika'nın olmak üzere tüm dünyanın güvenlik paradigması değişmiş, kimileri terör olaylarındaki bu büyük değişimi ve yıkıcılığı Küresel Terör Dalgası' olarak nitelendirirken ABD

Başkanı George Bush tarafından 20 Eylül 2001 Perşembe gecesi, Temsilciler Meclisi ve Senato'nun ortak toplantısında yapılan konuşmada bu dalgaya karşı verilen mücadele de 'Teröre Karşı Savaş (*war on terror*)' şeklinde nitelendirilmiştir. En nihayetinde ülkelerin güvenlik ve savunma yaklaşımları değişikliğe uğramıştır (Yılmaz, 2011: 362; Arslan, 2023: 48). Bahsedilen terör saldırısı daha önceki zamanda ortaya çıkan bir kavram olan asimetrik savaş kamuoyunda kendisine yer edinmesi ve sıklıkla duyulur hale gelmesine neden olmuştur ((Begenirbaş, 2022: 148).

Asimetrik tehditler yalnızca terör örgütleri ile güçsüz, zayıf devletler tarafından kullanılan tehdit unsurları değildir. Esas amacı güçlü psikolojik etki yaratmak olan asimetrik tehditleri hem güçlü hem de zayıf taraf kullanabilir (Özdoğan, 2018:10, 11). Öyleyse güçlü devletler bu unsurları kullanarak stratejik planlarına yön verebilirler (Begenirbaş ve Can Yalçın, 2020: 185). Bu duruma yakın tarihten bir örnek verilebilir. 24 Şubat 2022 tarihinde Rus güçlerinin Ukrayna'ya saldırısı ile başlayan Rusya-Ukrayna Savaşı'nın [1] konvansiyonel savaş yanı sıra farklı yönleri ve nitelikleriyle birçok farklı savaş türünü barındırdığı söylenebilir. Rusya'nın Ukrayna'dan daha büyük bir güç olmasına rağmen Ukrayna'nın Rusya'nın zayıf yönlerinden yararlanarak başarı elde etmesi yönünden savaşın asimetrik savaş özelliği gösterdiği ifade edilebilir (Karasoy, 2022b: 45, 46, 50, 51). Asimetrik etki yaratmak için kullanılan stratejiler birbirlerinden farklılıklar göstermektedir. Ancak asimetrik bir etki ortaya çıkması için çoğunlukla terör ve teknolojiden yararlanıldığı ifade edilebilir (Begenirbaş, 2022: 148, 149).

Savunma planlamaları yapılırken asimetrik tehditlere ilişkin olarak dikkat edilmesi gereken önemli noktalardan biri mali yükle ilgilidir. Şöyle ki asimetrik etki yaratan unsurların varlığı savaşın çok uzun sürelere yayılmasına sebep olmaktadır. Uzun süreli savaşların ise ülke ekonomisine olumsuz etkisi olacaktır. Dolayısıyla savunma planlamalarının bu etki göz önüne alınarak yapılması gerekmektedir. Bir diğer önemli husus ise asimetrik tehditleri kullanan aktörlerle ilgilidir. Asimetrik tehdit yöntemlerinin yalnızca terör örgütleri tarafından kullanılmadığı daha önce vurgulanmıştı. O halde savunma planlamaları yapılırken devletlerin de asimetrik tehditte bulunabilen bir aktör olabileceği düşüncesinden hareket ederek strateji ve planları esnek hareket etme yeteneğine olanak verecek şekilde geliştirmek önemlidir (Begenirbaş, 2022: 151). Asimetrik tehditler, en başta klasik savunma anlayışını radikal bir şekilde dönüştürürler. Tehditlerin belirsizlik düzeyinin artması ve hangi aktörler

[1] Rusya-Ukrayna Savaşında savaşın başlatılması yönünde Rusya'yı cesaretlendiren iki husus olmuştur. Bunlardan ilki 2014 yılında Kırım'ı ilhak eden Rusya'ya karşı Batı'nın ciddi bir mukavemet göstermeyişi; diğer neden ise Rusya'nın bu savaşı başlattığı esnada Avrupa'nın içinde bulunduğu durum. 2020 yılında İngiltere'nin Brexit sistemine geçmesiyle resmen AB'den ayrılmış olması, ABD'nin Afganistan'da başarısız olduğunu kabullenerek geri çekilmiş olması gibi nedenlerle Rusya Batı'nın kendi meseleleriyle uğraşacağını ve kendisine bir mukavemet gösteremeyeceğini düşünmüştür (Karasoy, 2022: 45-46).

tarafından yöneleceğinin bilinmezliği savunma anlayışında esneklik ve dinamizm gerektirmekte ve klasik savunma anlayışının sınırlarını aşmaktadır. Ayrıca asimetrik savaşların yalnızca konvansiyonel savaş yöntemleri ile gerçekleşmemesi nedeniyle savunma planlarının konvansiyonel olmayan savaş yöntemlerine de hazırlıklı olması gerekmektedir. Savunma planlamalarının iç ve dış güvenliği sağlama noktasında birçok farklı tehdide karşı hazırlıklı olması yanı sıra bu tehditlere karşılık verecek birliklerin de asimetrik savaş unsurlarına karşı yetiştirilmiş özel birlikler şeklinde oluşturulması gerekmekledir. Dolayısıyla kuvvet planlaması ile silahlanma planlamasının asimetrik unsurlara uygun şekilde yapılması gerekmektedir. Asimetrik yöntemlerin sivil halka zarar verme maksadıyla yalnızca askeri alanlara değil kentlere yönelecek olması ihtimalinden hareketle sivil halkın korunması için planlama yapılması ve kentlerin güvenliğinin sağlanması gerekmektedir. Asimetrik savaşların temel özelliklerinden biri olan belirsizliğinin giderebilme noktasında istihbarat oldukça önemli hale gelmektedir.

II.B.HİBRİT SAVAŞ

Savaş kavramı TDK'de "*devletlerin diplomatik ilişkilerini keserek giriştikleri silahlı mücadele; harp (I), cenk, cidal, kıtal*" şeklinde tanımlanmıştır. Hibrit savaş konseptinde en az iki farklı muharebe çeşidi birlikte bulunmaktadır. Bu konsepti daha iyi anlamak için hibrit kelimesinin anlamına bakacak olursak bu sözcük TDK'de ilk anlam olarak "*melez*" ikinci anlam olarak ise "*iki farklı güç kaynağının bir arada bulunması*" şeklinde tanımlanmıştır (Türk Dil Kurumu Sözlükleri, 2023). Ülkelerin sahip oldukları jet motorları, uçak gemileri, drone teknolojileri, radar sistemleri vb. teknolojiler, silahlı mücadelelerini destekleyen temel muharebe araçları içerisinde yer almaktadır. Günümüz şartlarında savaş alanlarındaki mücadeleler sadece silahlı mücadeleler ile gerçekleşmemektedir. Bunun en temel sebebi yaşanan teknolojik ilerlemenin savaş olgusunda ortaya çıkardığı dönüşümdür (Doğan, 2022: 30). Günümüz savaşlarını ifade etmesi için birçok farklı terim kullanılmakta olsa da en çok kabul gören ve kullanılan ifade hibrit savaş ifadesidir (Aytuğ ve Pozan, 2023: 3; Bilal, 2021). Hibrit savaş yeni tür/nesil savaş çeşitlerinden birisi olarak kabul edilmektedir ve içinde pek çok unsuru, elementi, stratejiyi barındırmaktadır (Arslan, 2019: 934). Günümüzde konvansiyonel savaş araç ve gereçlerinin yıkıcılığının artması nedeniyle devletlerin doğrudan birbirlerine savaş ilan etme ihtimalleri azalmıştır. Bu durumda devletleri, daha ekonomik ve daha az risk içeren dolaylı savaş yöntemlerine başvurmaya yönlendirmiştir (Dedemen, 2016: 154).

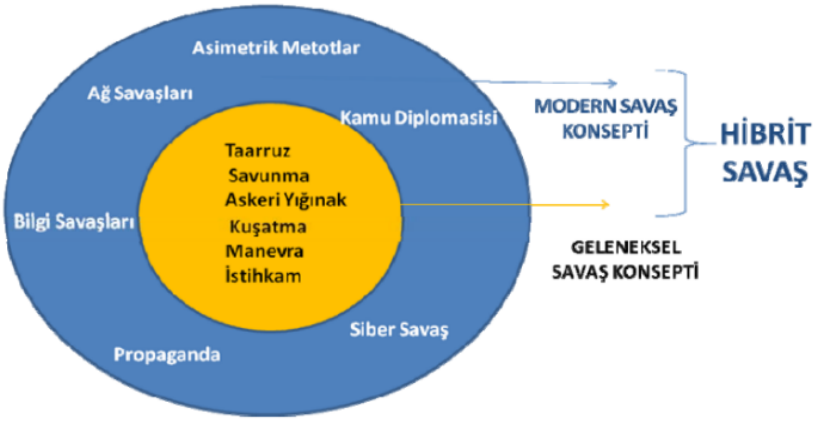
William J. Nemeth tarafından yazılan "*Gelecek Savaş ve Çeçenistan: Bir Hibrit Savaş Örneği*" başlıklı çalışmada Çeçen isyanının hibrit savaş için bir model olabileceği iddiasıyla kullanılmış olan hibrit savaş kavramı bugünkü anlamıyla ilk kez Frank Hoffman tarafından James Mattis ile yazdığı 2005 tarihli

"*Geleceğin Savaşı: Hibrit Savaşların Yükselişi*" (Mattis vd. 2005) adlı çalışmasında kullanılmıştır (Aytuğ ve Pozan, 2023: 3). Hoffman hibrit savaşı, düşmanın "*konvansiyonel silahlar, alışılagelmişin dışında taktikler, terörizm ve hukuk dışı faaliyetlerin amaca yönelik harmanlanmış şeklini kendi politik amaçlarına ulaşmak için aynı harekât ortamında ve zaman diliminde kullanması"* şeklinde tanımlamış *ve* hibrit savaşın çok çeşitli faaliyetlerden oluştuğunu dile getirmiştir (Karabulut, 2016: 27). Bu faaliyetlere geleneksel savaş yöntemleri, konvansiyonel olmayan taktikler, terör faaliyetleri, kriminal suçlar vb. faaliyetlerin dahil olduğunu vurgulamıştır. Bu faaliyetlere devlet ve devlet dışı aktörlerin başvurabileceğini ve farklı faaliyetlerin koordineli şekilde yürütülmesi ile başarılı bir sinerjinin oluşturulmasının amaçlandığını aktarmıştır (Gökçe ve Şengönül, 2017: 478). NATO da hibrit tehditlerin hem devlet hem devlet dışı aktörler tarafından kullanılabileceğine vurgu yapmaktadır. Devletleri hibrit tehditleri kullanma yönünde cezbeden husus hibrit tehditlerin yapılan eylemin sorumluluğunu inkâr etme olanağı tanıması ve atfedilememesi özellikleri taşımasıdır (Karasoy, 2022a: 40). Devlet dışı aktörler sıklıkla silahlı örgütler, milis grupları ve terör örgütleri ile özel şirketler olabilmektedir. Geleneksel orduların yanında bu gruplar da savaşların önemli unsurları haline gelmişlerdir (Yenal, 2020a: 62).

Hibrit savaş, konvansiyonel savaş ile konvansiyonel olmayan savaş yöntemlerinin ve hedefe ulaşmak adına tüm yeteneklerin birlikte kullanıldığı savaş şeklidir (Karasoy, 2022b: 47). Konvansiyonel savaş Körpe'nin (2023) ifadesi ile devlet güvenliğini sağlamak maksadı ile eğitilen, teçhiz edilen, yönlendirilen silahlı kuvvetlerin dahli ile belirli hukuk kurallarına uygun şekilde gerçekleştirilen savaş olarak; konvansiyonel olmayan savaş ise özel harbin bir alt bölümü olarak hem askeri hem yarı askeri yöntemlerle hedef ülke ya da işgal altındaki bölgelerde hakim otoriteyi zayıflatmak ve bölgeye hakim olmak amacı ile yürütülen harp şekli olarak ifade edilebilir (Körpe, 2023). Hibrit savaşın iki ayırıcı özelliği vardır. Bunlardan ilki savaş ve barış zamanı arasındaki çizgiyi belirsizleştirmesidir. Diğeri ise belirsizlik ve dayandırma ilişkisiyle ilgili olup hibrit saldırıya hedef olan ülkenin saldırıyı gerçekleştiren devlet veya sponsoruyla saldırıyı ilişkilendirememesi ve bu nedenle bu saldırıya ilişkin bir politika ve mukabele geliştirmesinin zorlaşmasıdır (Bilal, 2021). John McCuen modern toplumların birbirine bağlı doğasını da düşünerek hibrit savaşın konvansiyonel savaş alanlarında, saldırılan ülkenin kamuoyunda ve saldıran ülkenin kendi kamuoyunda aynı anda gerçekleştirdiği mücadele ile ortaya çıktığını değerlendirmiştir (Gökçe ve Şengönül, 2017: 478).

Hibrit tehditler sınıflandırıldığında bu tehditler üç kapsamda değerlendirilebilir. Birincisi ekonomik yollarla toplumları baskılamayı amaçlayan devletlere yönelik gerçekleştirilen tehditlerdir. İkincisi, askeri metotlarla gerçekleştirilerek kurumları, ulaşım ağlarını, iletişim ağlarını, limanları vb. etkisizleştirmeye çalışan tehditlerdir. Üçüncüsü ise yasadışı teşebbüsler şeklinde

nitelendirilebilecek toplumları kutuplaştırmayı, ayrıştırmayı ve korkutma yoluyla baskılamayı amaçlayan en ucuz yöntemlerin kullanıldığı tehditlerdir (Ünal, Kanat, ve Gürkaynak, 2023: 394, 395). Bu yönüyle hibrit savaş hem düzenli askeri birlikler gibi konvansiyonel savaş metotlarını kullanırken; bilgi dezenformasyonu, karşı tarafın moralini, devlete duyduğu güvenini olumsuz etkileme, ekonomik yaptırımlar vb. düzensiz savaş enstrümanlarını da kullanabilmektedir. Hibrit savaşın sahip olduğu bu çok çeşitli enstrümanlar hedefler doğrultusunda eş zamanlı şekilde kullanılabilmektedir. Bu durum da savaş alanının oldukça genişlemesi sonucunu beraberinde getirmektedir (Karasoy, 2022b: 44, 55). Aşağıda yer alan şekilde hibrit savaşta hem taarruz, kuşatma, manevra vb. şeklindeki geleneksel savaş konseptlerinin hem de asimetrik metotlar, ağ savaşları, bilgi savaşları vb. şekildeki modern savaş konseptlerinin bir arada kullanıldığı görülmektedir. NATO Dönüşüm Komutanlığı tarafından yayımlanan 2011 tarihli bir raporda da "*terörizm, göç, korsanlık, yolsuzluk, etnik çatışma, vb. çok geniş alandaki düşmanca durum ve faaliyetleri kapsayan bir şemsiye terim"* olarak kendisine yer bulmuştur (Karabulut, 2016: 27, 28).



Şekil 1: Hibrit Savaş

Kaynak: Dedemen, 2016

Hibrit savaşlarda konvansiyonel ve konvansiyonel olmayan yöntemlerin bir arada olması tehdit algı ve düzeyini çoğaltmış olacaktır. Bu minvalde savunma planlamalarının çok yönlü, esnek, dinamik, hızlı adapte olabilen, farklı disiplinlere açık olması anlamında disiplinlerarası yaklaşımı içeren şekilde olması gerekmektedir. Kuvvet ve silahlanma planlamaları yapılırken asimetrik savaşlarda olduğu gibi konvansiyonel olmayan savaş unsurlarının göz önünde

bulundurulması gerekecektir. Hibrit savaşların çok yönlü tehdit unsurlarını içermesi nedeniyle bu tehditlere karşı koyma noktasında askeri otoriteler ile sivil otoritelerin bir aradalığı ve güçlü iletişim ve koordinasyon içerisinde olmaları faydalı olacaktır. Bu bakımdan hibrit tehditlerin öngörülemez ve ani gelişiyor olmaları savunma planlamasında yetkili otoritelerin hızlı karar alma yeteneğini geliştirmelerini gerektirmektedir. Hibrit tehditlerin uluslararası özellik taşıma ihtimalinden dolayı bu tehditlere karşı koyma noktasında uluslararası iş birlikleri de gerekebilir.

III. SİBER TEHDİT

Önceleri yalnızca şifre koyma, şifre çözme amaçlı ortaya çıkan bilgisayarlar günümüzde hem kişiler hem kurumlar bazında vazgeçilmez bir araca dönüşmüştür. İnternet kullanımı 1960'lı yıllarda ABD'nin savaş esnasında askeri iletişimin zarar görmemesi amacıyla bir bilgisayardaki verinin başka bilgisayara aktarılabilmesi için kurduğu ARPANET kullanımıyla başlamıştır. İnternette tıpkı bilgisayarlarda olduğu gibi hem kişiler hem kurumlar için vazgeçilmez unsur olmuş ve bir anda hızlı şekilde yaygınlaşmıştır. Öyle ki bilgisayarlar ve internet gibi yeni teknolojilere adapte olamayan oluşumların varlığını devam ettirmesi imkânsız hale gelmiştir. Ancak bu hızlı şekilde yaygınlaşma beraberinde bu sistemlerin kötü niyetle kullanılmasına sebep olan güvenlik açıklarını getirmiştir ancak bu hızlı şekilde yaygınlaşma beraberinde bu sistemlerin kötü niyetle kullanılmasına sebep olan güvenlik açıklarını getirmiştir (Aslay, 2017: 24).

Siber kavramı, bilgisayar ve ağlarını içeren varlığı tanımlamaktadır. Siber alanla ilgili en geniş kavram olan siber uzay, bilgisayar ağları ile bu ağlar vasıtasıyla ulaşılabilen tüm veri kaynaklarını kapsayan alan olarak ifade edilebilir (Yılmaz O. , 2017). "*Siber uzayın her türlü tehditten korunması*" (Doğan, 2022: 43) temeline dayanan siber güvenlik kavramı bilişim sistemlerinden oluşan siber ortamın muhtemel saldırılardan korunması, bu sistemde yer alan verilerin gizlilik, bütünlük ve erişebilirliğinin güvence altına alınması, saldırı yapılmakta ise bunun tespiti ve siber ortamın saldırı öncesi haline döndürülmesinin sağlanmasıdır (Gençoğlu, 2019: 23). Siber saldırıların hedefinde kişiler ya da kamu ve özel kurumlar olabilmektedir. Bu saldırılar hedeflenen yapıya ait bilgi ve iletişim altyapılarına yönelik olmakta ve ticari, askeri, politik vb. amaçlarla yapılmaktadır (Aslay, 2017: 25). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda siber ortam tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortam şeklinde tanımlanmıştır (T.C. Ulaştırma ve Altyapı Bakanlığı, 2024). Siber savaş, ulusal bir çıkar ya da sürdürülen bir savaşı destekleme gayesiyle tarafların askeri ve sivil bilişim alt yapılarına yönelik engelleme ya da yok etme niyetindeki eylemleri kullanma şeklindeki savaş yöntemi olarak tanımlanabilir.

1900'lü yılların sonuna kadar kara, deniz, hava ve uzayda cereyan eden savaşlara, 21. yüzyılın başlarından itibaren siber uzay boyutu da eklenmiş ve bu şekilde siber savaş kavramı ortaya çıkmıştır. Bu yeni boyutta yapılan savaşların ülkelerin kritik sistem ve bilgilerine yönelmesi, ekonomik, askeri, siyasi vb. pek çok farklı yönden ciddi boyutta zarar görmelerine neden olmaktadır (Eren, Gençoğlu, ve Yenal, 2020: 271,272).

Siber saldırıların mahiyeti yalnızca devletin güvenliği ile sınırlı olmayıp, tüm özel teşebbüsler ile bireyler de bu saldırıların hedefi olabilmektedir. O halde siber saldırıların yalnızca devletlere yönelik yapılmadığı, bu tehditlere karşı geliştirilecek olan siber savunmanın da tek aktör üzerinden gerçekleştirilemeyeceği aşikardır. Dolayısıyla etkili bir siber savunma için tüm paydaşların ortak bir strateji yürütmesi gerekmektedir. Şüphesiz çok paydaşlı gerçekleşecek olan bu strateji için koordinasyon ve etkili iletişim mühim olacaktır (Begenirbaş, 2022: 145, 146). Siber saldırıların ne zaman yapılacağını tahmin etmek mümkün olmadığı gibi bu saldırılar ışık hızında gerçekleşmektedir. Bu sebeple saldırılara hızlıca karşılık vermek mühimdir. Bu saldırıların önüne geçebilmek için açıkların bulunması ve korumanın geliştirilmesi için tatbikat yapılması ciddi önem arz etmektedir. Türkiye'de de gerçek saldırı ve savunma teknikleri kullanılarak tatbikat yapılmaktadır (Aslay, 2017: 25).

Donanım ile yazılımlardaki hatalar, kritik sistemlere çevrimiçi erişim imkânı ve internet tasarımındaki zafiyetler siber saldırıların gerçekleştirilmesinin önünü açmaktadır. Siber saldırılar; siber taarruz, mikroçipler, istem dışı e-posta, Dos-DDos truva atı, salam tekniği, bilgi ve veri aldatmacası, süper darbe, zararlı yazılımlar, kurtçuk, mantık bombaları, klavye izleme oltalama, bukalemun, çöpe dalma, casus yazılımlar, yerine geçme, siber sabotaj, sistem güvenliğinin kırılıp içeri sızılması, sosyal mühendislik, web sayfası hırsızlığı ve yönlendirme gibi teknikler ile yapılmaktadır (Aslay, 2017: 26; Begenirbaş, 2022: 145; Eren, Gençoğlu, ve Yenal, 2020:273-277; Yılmaz, 2017:29). Bu saldırı tekniklerine karşı savunma yöntemleri ise anti virüs yazılımları, güvenlik duvarı, network erişim kontrolleri, saldırı tespit ve önleme sistemleri, açıklık tarayıcı yazılımlar, sanal özel ağ, kripto cihazları, geçerli kullanıcı ve şifre yönetimi, tuzak sistemler şeklindedir (Eren, Gençoğlu, ve Yenal, 2020: 277-280).

Son yıllarda büyük şirket ve kuruluşların elektronik belge ve verilerini en çok tehdit eden saldırılardan biri fidye yazılım saldırısıdır. Bu tehlikeli yazılımlar, e-postalardan, reklamlardan veya sosyal mühendislik saldırıları gibi farklı yöntemlerle kolayca bulaşabilmekte ve örgütlere büyük zararlar verebilmektedir. Saldırıya uğrayan taraf saldırganların talep ettiği ödemeyi yapmadığında elektronik verilerini kaybetmek vb. risklerle tehdit edilmektedir. Fidye yazılımlar 2010 yılı ve sonrasında saldırganlar için büyük bir kazanç kaynağı haline gelmiştir (Çelik ve Çeliktaş, 2018: 107). Nitekim Avrupa Birliği

de hibrit tehditler içerisinde en fazla siber tehditler vasıtasıyla saldırılarda bulunulduğundan hareketle ilk etapta bu saldırılara karşı önlem alınmasını elzem görmektedir. Başka bir deyişle Avrupa Birliği'nin yeni güvenlik konusu olarak belirttiği siber alem, hibrit tehditler içerisinde öncelikli tercih edilen saldırı alanını oluşturmaktadır (Ünal, Kanat, ve Gürkaynak, 2023: 393).

Kosova çatışması literatürde Yugoslavya Federal Cumhuriyeti'nin dağılma sürecine girmesiyle birlikte etnik unsurlar arasında yaşanan çatışmaları ifade etmek için kullanılmıştır. Bu çatışmalara NATO'nun 24 Mart 1999'da NATO Genel Sekreteri'nin direktifiyle Sırp mevzilerin bombalanması ile dahil olan NATO bu tarihten itibaren siber saldırılara maruz kalmıştır (Yılmaz O. , 2017). Bu saldırıları gerçekleştiren bilgisayar korsanlarının sitelere "*çok yaşa Sırbistan*" gibi ifadeler koydukları ve saldırıları yalnızca Sırpların değil, Çinliler ve Ruslarında gerçekleştirdikleri tespit edilmiştir. 1999 yılında bu şekilde başlayan siber saldırılar NATO'nun güvenlik konseptinde yeterince yer alamamış olsa da 1999 yılı NATO'nun güvenlik hedefleri yönünden önemli bir yıl olma özelliği taşımıştır (Bıçakcı, 2012: 210, 211). Yugoslavya'dan sonra bir Avrupa Birliği ülkesi olan Estonya'da siber saldırılara maruz kalmıştır (Köker, 2022: 61).

Siber saldırılarda kullanılan yöntemlerin maliyetinin ülkelerin savunma sistemlerinin daha altında bir maliyete sahip olması, savunmaya ayrılan kaynaklarının azaldığı ülkeler için siber saldırıları daha önemli hale getirmiştir. Ülkelerin finansal sistemlerden askeri sistemlere kadar sahip oldukları pek çok sistem küçük bir yazılımla zarara uğratılabilir. Günümüzde ülkelerin maruz kaldığı siber saldırılara ilişkin olarak birçok farklı örnek verilebilir. 2010 yılında ABD korsan bir yazılımla İran'ın nükleer santrallerine saldırı gerçekleştirmiştir. Bu saldırı santraldeki faaliyetlerin bir süre için durmasına sebep olmuştur. 13 Haziran 2025 tarihinde İsrail'in saldırıları ile başlayan ve 12 gün süren İsrail-İran savaşında da siber saldırılar karşılıklı olarak yaşanmıştır. İsrail'in İran'ın borsa ve bankacılık sistemlerine, İran'ın İsrail'in devlet televizyonuna saldırısı karşılıklı yaşanan siber saldırılara örnek gösterilebilir (Anadolu Ajansı, 2025).

Görüldüğü üzere ülkelerin birçok farklı sektör ve altyapısı siber saldırılan hedefi haline gelebilmektedir. Ülkelerin sahip oldukları pek çok sistemin dijitalleşmesi ve bu nedenle siber saldırılara açık hale gelmesi oldukça önemli bir güvenlik tehdidi̇dir. Siber saldırıların kritik alt yapı sistemlerine ve bilgi ağlarına yönelmesi, siber saldırıların çok hızlı ve etkili şekilde gerçekleşmesi, küçük bir yazılımın çok büyük zararlara neden olması geleneksel savaş alanlarına eklenen siber uzay alanının önemine işaret etmektedir. Siber saldırılara karşı koyabilmek için muhakkak önleyici mekanizmalara sahip olma, hızlı müdahale edebilme, zararın tespitini yapma ve hızlı şekilde yeniden toparlanma siber savunmanın kritik noktalarını oluşturmaktadır. Hızlı karşı koymayı sağlayabilmek için erken uyarı önlemleri, ikazlar ve elbette diğer

güncel tehditlerde olduğu gibi güçlü bir istihbarat ağı önemlidir. Elbette bu noktada savunmadan mesul olan askeri ve sivil tüm personellerin siber saldırılar ve siber savunma hususlarında bilgilendirilmiş olması gereklidir.

IV. GÖÇ

En yalın ifadeyle insanların iradi veya zorunlu olarak yaşadığı mekânı değiştirmesi (Kaygusuz, 2021: 61.) anlamına gelen göç, insan varlığının başlangıcına tarihlenebilen bir olgudur. Tarihin birçok dönemi, insanların güvenlik sebebiyle yaşadıkları yerlerden başka yerlere istekleri dışında göç etmelerine tanıklık etmiştir. Dolayısıyla göç, hemen her zaman güvenlik konusuyla yakın ilişki kurmuştur. Günümüz dünyasında da kitlesel göçlerin yoğun bir şekilde yaşandığına tanıklık edilmektedir. Aynı zamanda yakın gelecekte de küresel iklim değişikliği nedeniyle yoğun göçlerin yaşanacağı bilim insanları tarafından öngörülmektedir (Toktaş, vd.: 2023). Güvenlik anlayışının geleneksel anlamından sıyrılarak her türlü tehdidi içine alır şekilde genişlemesi de göç olgusunun güvenlikle ilişkisini artırmaktadır (Doğan, 2022: 52). Bu bakımdan göçün günümüzde önceki dönemlerde olduğundan daha yoğun bir şekilde güvenlik ile ilişkilendirildiğini ifade etmek gerekir.

Modern ulus devletlerin egemenlik ile iktidar alanını belirleyen ve iki devleti birbirinden ayırmaya yarayan hat şeklinde tanımlanabilecek olan sınır kavramı dendiğinde akla ilk önce devlet sınırları gelmektedir (Özkaya, 2020: 319, 329, 332). Devletlerin kara sınırları antlaşmalar ile belirlenmiş olup bu sınırlar içerisinde bireyler, semboller, taraflar ile uluslararası hukuk yer almaktadır. Bireyler ve devletlerin güvenliği en başta sınır güvenliğinin varlığı ile sağlanabilir (İstanbullu ve Emiroğlu, 2022: 227). Günümüzde kitlesel göç olgusu, devletlerin varlığını tehdit etmektedir (Özkaya & Efe, 2024: 263).

Günümüzde uluslararası güvenliği tehdit eden yeni hususlar beraberinde mülteci sorunu gibi yeni sorunları getirmiş ve sınır güvenliği kavramı daha geniş bir perspektiften değerlendirilmesi gereken bir olgu haline gelmiştir (İstanbullu & Emiroğlu, 2022: 229). 11 Eylül saldırısından sonra değişen paradigmalar, Soğuk Savaş döneminde devleti merkezine alan klasik güvenlik anlayışından, sınır ötesinde göçün önlenmesi ve kaynak mücadelesine doğru ciddi bir dönüşüm geçirmiştir. ABD'de 11 Eylül terör saldırısı sonrası gelişen "iç güvenlik yönetimi" anlayışı ile "*ülke içerisindeki terörist saldırıları önlemek, saldırı sonrası oluşan zararları azaltmak ve iyileştirmek*" bakış açısı baskın hale gelmiştir (Yılmaz S., 2011). Sınırların "teröristlerin" potansiyel geçiş noktası olduğu bakış açısı sınır güvenliği kavramını önemli hale getirmiş ve göçün sınır ötesinde önlenmesi gibi yeni mücadele yöntemlerini ortaya çıkarmıştır (Aras, 2023: 472). Güvenlikleştirme bakış açısı nedeniyle göç ile beraber elektronik gözetleme sistemleri, çok uluslu ve ulusal sınır güvenlik

timleri vb. şeklinde geniş bir güvenlik sektörü oluşmuştur (Özkaya & Efe, 2024: 166; Rumelili Bahar ve Karadağ, 2017: 86- 88).

Geleneksel sınır güvenliği politikalarının yerini daha korumacı bir sınır güvenliği anlayışına bırakmasıyla beraber devletler sınırlarından riskli grupların geçişini önlemeye yönelik mekanizmalar konusunda daha hassas davranır hale gelmişlerdir. AB 2005 yılında Operasyonel İş birliği Ajansı (FRONTEX) Sınır Güvenliği Birimi'ni kurmuştur (Aras, 2023: 474). Ancak AB göç-güvenlik ilişkisini 1980'li yılların ortalarından itibaren kademeli şekilde oluşturmuş ve Suriye Savaşı sonrasındaki mülteci meselesiyle birlikte zirve noktasına ulaştırmıştır (Rumelili Bahar ve Karadağ, 2017: 70). ABD ise 11 Eylül saldırısından sonra bir süre kara sınırını ve hava sahasını kapatmış, 2006 yılında Meksika Sınırını çit ile 2016 yılında duvar ile kapatma kararı almıştır. Çit ve duvar dışında sınırlar sınır karakolları, sınır gözetleme kuleleri, biyometrik tanımlama, uydu görüntüleri, hava araçları, termal kameralar gibi fiziki araç ve gereçler ile pasaport ve vize uygulamaları ile korunmaktadır (Deniz, 2020: 242).

Avrupa'da yakın zamanda aşırı sağın yükselişiyle birlikte göç olgusunun devlet güvenliğine tehdit boyutu daha da önemli bir hale gelmiştir. Nitekim Millî İstihbarat Akademisi'nin "Batılı Ülkelerde Aşırı Sağ Hareketler" 2023 yılı değerlendirme raporunda özellikle 2015 sonrasında Avrupa'da göçmenlerin terörle bağlantılı olarak bir güvenlik sorunu olarak değerlendirildikleri ifade edilmiştir (Milli İstihbarat Akademisi, 2024). Aslında bu durumun temeli 1990 sonrasında ortaya çıkan "Kale Avrupası" anlayışına dayanmaktadır. Kale Avrupası anlayışı, Schengen Bölgesi sınırlarının sert bir şekilde korunmasını ifade eden bir anlayıştır. Avrupa'da yükselen aşırı sağ, kalenin sınırlarının daha sağlam bir şekilde korunması düşüncesini desteklemektedir. Özellikle son 20 yılda İspanya, İngiltere, Fransa gibi Avrupa ülkelerinde yaşanan terör saldırıları göçü daha fazla güvenlikleştirmekte (Özkaya & Efe, 2024: 159, 166) ve savunma planlaması alanına çekmektedir.

1951 Cenevre Sözleşmesi ile kurulan uluslararası sığınma rejimi çerçevesinde sözleşmeye taraf ülkelerin sığınmacılar hususunda söylemleri ile eylemleri arasında farklılık olduğu ve ülkelerin çoğunlukla açık kapı politikasını uygulamaktan kaçındıkları görülmektedir. Avrupa kendisine gelecek göç akınından kurtulabilmek için Türkiye ile yaptığı anlaşma ile kendi ülkelerinde mültecileri istemediklerini ve mültecilere karşı geliştirdikleri politikaların "güvenlik" çerçevesinden oluşturulduğunu göstermektedir (Şimşek & İçduygu, 2017: 7, 8). Uluslararası göç literatüründe çokça kullanılan güvenlik kavramı daha çok devletlerin güvenliğinin korunması üzerinden kullanılmış ve ulusal güvenliği ifade etmiştir.

Göç olgusu çok boyutlu bir olgu olarak insani, ekonomik, toplumsal, güvenlik vb. birçok farklı boyutu içerisinde barındırmaktadır. Göç, farklı şekillerde

sınıflandırılabilmektedir. 20. yüzyılın son çeyreği itibarıyla gittikçe önem kazanan bir olgu olan düzensiz göçler (Şemşit, 2018) ülkelerin güvenlik politikaları açısından önemlidir. Göçün düzensiz göç niteliğinde olması ve kitlesel bir hareket olarak cereyan etmesi savunma planlamalarında bazı hususların yer alması sonucunu doğurabilir. Bireysel göçlerin en fazla kentsel güvenliği tehdit etme ihtimali varken, kitlesel göçlerin de ulusal güvenliği tehdit etme potansiyeli bulunmaktadır. Bu bakımdan devletler savunma planlamalarını yaparken var olan ve olması muhtemel düzensiz göç hareketlerini planlamak ve bu hareketlerin ülke savunmasına verebileceği muhtemel zararları öngörerek hareket etmek zorundadır. Göç olgusunun iç ve dış güvenlik için ortaya çıkardığı tehdit uluslararası nitelik taşıdığı için ülkelerin diğer ülkeler ve uluslararası örgütler ile ortak savunma anlayışı geliştirmesi gerekebilir. Bu nedenle uluslararası iş birlikleri göçün ortaya çıkardığı tehditler ile mücadelede önemlidir. Bir diğer önemli husus göç olgusunun insani yönü nedeniyle savunma planlamasının da insani öncelikleri ve insani yardım boyutunu da içerecek şekilde lojistik planlamasında bulunulmasıdır. Düzensiz göç hareketi nedeniyle sınır güvenliğinin en temel risk alanlarından biri haline gelmesi, savunma planlamalarında sınır güvenliğini sağlama noktasında hassas davranılmasını gerektirebilir. Sınır güvenliğini sağlamak adına sıkı kontrol önlemleri, biyometrik yüz tanıma sistemleri, dronlar, sensörler, duvarlar, radarlardan yararlanılabilir. Bu noktada ülkenin iç ve dış güvenliklerinden sorumlu birimlerin sıkı bir koordinasyon içerisinde hareket etmesi gerekmektedir. Göç olgusu hem iç güvenlik hem de sınır güvenliği ve dış güvenlik için ortak şekilde risk oluşturan bir olgudur. Dolayısıyla güvenlikten sorumlu tüm kurumların ortak ve bütüncül şekilde çalışmasını sağlayacak, esnek bir savunma planlaması gerekecektir.

SONUÇ

İnsanlık tarihi boyunca daima var olmuş olan savaş kavramı birçok düşünür tarafından devletin en önemli faaliyeti ve politikanın devamı şeklinde değerlendirilmiştir. Clausewitz her savaşın politik bir amaç taşıdığını ve her dönemin savaş doğasının ve koşullarının farklılaştığını ifade etmiştir. Günümüzde yaşanan savaşların da şüphesiz en temel sebebi politik gayeler güdülmesidir. Ancak günümüzdeki savaşların tanımı, aktörleri, araçları, tarafları gibi birçok özelliği geçmiş yıllarda yaşanan savaşlardan farklılık göstermektedir. İçinde bulunduğumuz yüzyılda savaşlar yalnızca konvansiyonel savaş yöntemler ile değil aynı zamanda konvansiyonel olmayan savaş yöntemlerinin de birlikte uygulanmasıyla gerçekleşmektedir. O halde günümüzde savaşan tarafların başarısı noktasında her iki savaş yöntemini bir arada kullanabiliyor olmasının oldukça elzem olduğu ifade edilebilir. Bilhassa gelişen teknolojilerle beraber ülkelerin savunma ve silah sistemlerinin

konfigürasyonu, yeni tehditlere karşılık verebilir hale gelmesi, kara, deniz, hava, uzay ve siber uzay alanında savunma yapabilir olması gerekmektedir. Ülkelerin savunma güçlerinin arttırılmasında önemli bir araç olan savunma planlamaları tarih boyunca ortaya çıkan güvenlik ve tehdit koşullarına göre değişim geçirmiştir. Farklılaşan her bir dönemde yeni bir savunma planlaması yöntemi uygulanmıştır. 11 Eylül terör saldırısı sonrasında yeni gelişen güncel tehditler ile beraber zaman ve mekânın belirsiz hale gelmesi ülkeleri savunma planlamaları noktasında bir belirsizlik ile mücadele etmek durumunda bırakmıştır. Bu kapsamda senaryo uzayı yöntemi uygulanmaya başlamıştır.

Günümüzde gerçekleşen bazı savaşlar birçok farklı savaş taktiği ve niteliği taşıması nedeniyle hibrit savaş özelliği göstermektedir. Simetrik ve asimetrik yöntemlerin bir arada yer aldığı hibrit savaşlar, hedefe ulaşabilmek adına farklı yeteneklerin birlikte kullanıldığı bir savaş türüdür. İnternet ve bilgisayar kullanımının ciddi şekilde yaygınlaşması çok hızlı ve ani bir şekilde gerçekleşebilen siber tehditlerin de yaygınlaşmasını beraberinde getirmiştir. Tüm bu yeni tehditler ülkelerin savunma planlamalarında ciddi değişimlerin yaşanmasına sebep olmuştur. Tarih boyunca ülkelerin karşılaştıkları tehditlerin niteliğinin değişmesi savunma planlaması yaklaşımlarının da değişmesini beraberinde getirmiştir. Asimetrik tehditlerin belirsiz olmasının yarattığı korku toplumlar üzerinde bir baskı unsuru olarak devam edecektir. Bu tehditlerin gündemimizden ve hayatlarımızdan bir anda silinme ihtimalinin olmadığı değerlendirilmektedir. Ayrıca çoğunlukla ülkeler arasında ve ülke içerisinde yaşanan çatışmaların ve ekonomik sıkıntıların sebep olduğu göç olgusu gelecek dönemlerde de sıklıkla rastlayacağımız bir olgu olacaktır.

Güncel tehditlerin varlıklarını devam ettirecek olmaları, savunma planlamacılarının bu belirsizlikler ve güncel tehditler karşısında esnek ve çeşitli senaryolara uyum sağlayabilecek kapasitede yeteneklere sahip planlamalar yapmalarını oldukça elzem hale getirmektedir. Ayrıca senaryoların çeşitlenmesi, her bir tehdit için önleyici tedbir alınması; var olan açıkların, eksik yeteneklerin tamamlanması saldırı anının belirsiz olduğu tehditlerin bertaraf edilebilmesi için önemli noktalardır. Her ülkenin karşılaştığı tehdit ve saldırıların farklılık göstermesi, ülkelerin savunma planlamaları için ayırdıkları bütçelerin de farklı olmasına sebep olmaktadır. Ülke yöneticilerinin kendi ülkelerinin koşulları, yetenekleri ve mali durumunu göz önünde bulundurarak günümüz değişen tehdit ve güvenlik algısına uygun şekilde savunma yönetimlerini yeniden tasarlamaları ve savunma planlamalarını değişen koşullara hızlı şekilde adapte olabilecek şekilde dizayn etmeleri önemli hususlar olarak değerlendirilebilir. Ülkelerin belirsizlik karşısında planlama yapabilmesi için istihbarat faaliyetlerinin başarısının oldukça önemli olduğu ifade edilebilir. Öyle ki tehdidin kaynağının, zamanlamasının, şeklinin, yönünün öngörülemediği noktada istihbarat faaliyetlerinin başarısı savunma

planlamacılarının elini kolaylaştıracak ve daha etkin bir savunma planlaması oluşturmasına katkı sağlayacaktır.

KAYNAKÇA

Anadolu Ajansı. (2025, Haziran 18). *İsrailli hacker grubunun İran'ın kripto borsasına siber saldırı düzenlediği iddia edildi*. Anadolu Ajansı: https://www.aa.com.tr/tr/dunya/israilli-hacker-grubunun-iranin-kripto-borsasina-siber-saldiri-duzenledigi-iddia-edildi/3602798 adresinden alındı

Aras, F. Ç. (2023). Türkiye'de Yeni Sınır Güvenliği Paradigması: Göç, Güvenlik ve Göç Yönetimi. *Van Yüzüncü Yıl Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, s. 469-487.

Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum. *International Journal of Multidisciplinary Studies and Innovative Tecnologies*, s. 24-28.

Aytuğ, H., & Pozan, İ. (2023). Gelişen Hibrit Savaş Ortamında NATO-AB İş Birliği. *Karadeniz Araştırmaları*, s. 1-27.

Begenirbaş, M. (2022). *Savunma Yönetimi ve Planlaması.* Ankara: Nobel.

Begenirbaş, M., & Bekmezci, M. (2023). *Savunma Tedarik Süreci ve Stratejileri.* Ankara: Nobel.

Begenirbaş, M., Can Yalçın, R., (2020). Savunma Yönetimine Stratejik Bakış, M. Begenirbaş, R. Can Yalçın, & S. Yenal içinde, *Strateji ve Güvenlik Alanında Temel ve Güncel Yaklaşımlar.* (s.157-187), Ankara: Nobel.

Berk, U. (2015). Stratejik Savunma ve Güvenlik Planlamasında Ortak Bir Yaklaşım Olarak Senaryo Temelli Planlama. *Güvenlik Bilimleri Dergisi*, s. 1-36.

Bıçakcı, S. (2012). Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu. *Uluslararası İlişkiler Dergisi*, s. 205 - 226.

Bilal, A. (2021, Kasım 30). *Hibrid Savaş – Yeni Tehditler, Karmaşıklık ve Bunlara Çaresi olan 'Güven Duygusu.* NATO REVIEW: https://www.nato.int/docu/review/tr/articles/2021/11/30/hibrid-savas-yeni-tehditler-karmasiklik-ve-bunlara-caresi-olan-gueven-duygusu/index.html adresinden alındı

Birleşmiş Milletler Antlaşması ve Uluslararası Adalet Divanı Statüsü. (tarih yok). Kasım 2, 2023 tarihinde Birleşmiş Milletler Türkiye: https://turkiye.un.org/sites/default/files/2020-02/UN-charter-turkish_0.pdf adresinden alındı

BM. (2010, Haziran 26). *Birleşmiş Milletler Antlaşması.* BM: https://turkiye.un.org/sites/default/files/2020-02/UN-charter-turkish_0.pdf adresinden alındı

Coşkun, B. (2017). Türk Kamu Yönetimi Perspektifinde Soğuk Savaş Sonrası Oluşan Yeni Tehditler. *Alternatif Politika*, s. 109-130.

Çalış Yazgu, G., & Bekmezci, M. (2023). Savunma Yönetimi Öncesi ve Ötesi. M. Begenirbaş, & M. Topcu içinde, *Savunma Yönetiminde Güncel Yaklaşımlar* (s. 1-438). Ankara: Nobel.

Çalış Yazgu, G., & Bekmezci, M. (2023). Savunma Yönetimi Öncesi ve Ötesi. M. Begenirbaş, & M. Topcu içinde, *Savunma Yönetiminde Güncel Yaklaşımlar* (s. 7-25). Nobel.

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

Çelik, V. (2020). Stratejik Yönetim. Ö. Leblebici, A. Gürer, & S. Yenal içinde, *Savunma Yönetimi ve Uluslararası Güvenlik* (s. 101-125). Ankara: Nobel.

Davis, P. (2018). Defense planning when major changes are needed. *Defence Studies*, s. 374-390.

Davis, P., & Finch, L. (1993). *Defense Planning for the Post Cold War Era.* RAND National Defense Research Institute.

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

Demirel, M. (2012). Asimetrik Tehdit Kavramı Bağlamında, 11 Eylül 2001 Sonrası DönemdeAmerika Birleşik Devletleri'ndeki Siber Tehdit Algılamasının ve Geliştirilen Güvenlik Politikalarının İncelenmesi. Ankara: Kara Harp Okulu Savunma Bilimleri Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi.

Deniz, T. (2020). Sınırsız Dünya" Söylemleri Altında Sınırlar, Sınır Güvenliği ve Sınır İnsanları. *Doğu Coğrafya Dergisi*, s. 235-252.

Doğan, Z. (2022). Kavramsal, Tarihsel ve Kuramsal Bağlamda Güvenlik. Ö. Özkaya içinde, *Farklı Açılımlarla Hukuk Devleti ve Güvenlik* (s. 21-58). Ankara: Adalet Yayınevi.

Eren, H., Gençoğlu, M. T., & Yenal, S. (2020). Siber Savaş. M. Begenirbaş, R. Can Yalçın, & S. Yenal içinde, *Strateji ve Güvenlik Alanında Temel ve Güncel Yaklaşımlar.* (s.271-307), Ankara: Nobel.

European Union Committee. (2003). *EU Security Strategy.* Authority of the House of Lords.

Gençoğlu, M. (2019). Siber Güvenlik Matematiği. *Siber Güvenlik ve Savunma Standartlar ve Uygulamalar* (s. 23-46). Ankara: Grafiker Yayınları.

Gökçe, O., & Şengönül, A. (2017). Ukranya Krizi Işığında Hibrit Savaş. *International Vision University Ohrid*, s. 475-484.

Gül, M. (2016). Güvenlikteki Kavramsal Değişim ve Türkiye'nin Güvelik Yaklaşımı ve Politikalarına Etkileri. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 21*(1), s. 303-320.

Gürbüz, S., & Beyaz, B. (2023). Savunma Planlaması ve Savunma Tedariki İlişkisi. M. Begenirbaş, & M. Bekmezci içinde, *Savunma Tedarik Süreci ve Stratejileri* (s. 31-53). Ankara: Nobel.

İstanbullu, İ., & Emiroğlu, H. (2022). Sınır Güvenliği Mantığı. *Savunma Bilimleri Dergisi*, s. 223-249.

Kahraman, Ç. (2016). Tarihsel Süreçte Savunma Planlaması Yaklaşımları İle Savunma Tedarik Sistemleri Arasındaki İlişki. *Kara Harp Okulu Bilim Dergisi, 26*(2), s. 101-126.

Karabulut, A. (2016). Eski Savaş, Yeni Strateji: Rusya'nın Yirmibirinci Yüzyıldaki Hibrit Savaş Doktrini ve Ukrayna Krizi'ndeki Uygulaması. *Uluslararası İlişkiler AkademiK Dergi*, s. 25-42.

Karasoy, H. (2022). *Hibrit Savaş Asimetrik Savaş Vekalet Savaşı İstihbarat ve Terörle Mücadele.* Konya: Asatlas Akademi.

Karasoy, H. (2022). Hibrit, Asimetrik ve Vekâlet Savaşları: 2022 Rusya Ukrayna Savaşını Üçlü Sacayağı Üzerinde Bir İnceleme. *Medeniyet Araştırmaları Dergisi*, s. 44-56.

Kaygusuz, D. (2021). Uluslararası İlişkilerde Göç Olgusu ve Göçün Güvenlikleştirilmesi. *Akademik Düşünce Dergisi*(3), 60-76.

Kent, G., & Simons, W. (1994). Objective Based Planning. P. Davis içinde, *New Challenges for Defense Planning.* RAND.

Korkmazyürek, H. (2018). *Stratejik Savunma Yönetimi Temel Kavramları ve Esasları.* İstanbul: Hiperyayın.

Körpe, Ö. (2023). Eş Anlamlı Değil ama Eş Kullanımlı: Muharebe Sahası Fonksiyon Alanları Çerçevesinde Konvansiyonel, Asimetrik ve Hibrit Savaş. *Güvenlik Statejileri Dergisi*, s. 13-30.

Küçükşahin, A., & Akkan, T. (2007). Değişen Güvenlik Algılamaları Işığında Tehdit Ve Asimetrik Tehdit . *Güvenlik Stratejileri Dergisi*, s. 41-66.

Meydan, C., & Demirel, A. (2010). Savunma Planlamasında Belirsizlik Ve Belirsizlikle Başa Çıkmada Esnek Yaklaşımlar. *Savunma Bilimleri Dergisi*, s. 13-27.

Milli İstihbarat Akademisi. (2024). *Batılı Ülkelerde Aşırı Sağ Hareketler.* Ankara: Milli İstihbarat Akademisi.

Öz, T., & Çalışkanlar, T. M. (2020). Paralı Askerlerden Özel Askerî Şirketlere Savunma Yönetimi Teknolojileri Uygulamaları. *Güvenlik Stratejileri Dergisi, 16*(34), 309-339.

Özdemir, M., & Şahkulubey Baykal, N. (2022). Savunma Planlaması. F. Pirinçci , & M. Yeşiltaş içinde, *Savunma Politikaları* (s. 109-137). İstanbul: SETA.

Özdoğan, M. (2017, Mart). *Asimetrik Savaş Nedir? Tanımı, Özellikleri ve Geleceğ.* https://www.researchgate.net/publication/340233305_Asimetrik_Savas_Nedir_Tanimi_Ozellikleri_ve_Gelecegi adresinden alındı

Özdoğan, M. (2018). *Asimetrik Tehditlerle Mücadelede Stratejik Yönetim: Emniyet Genel Müdürlüğü Örneği.* Isparta: Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Yayımlanmamış Yüksek Lisans Tezi.

Özer, Y. (2018). Savaşın Değişen Karakteri: Teori ve Uygulamada Hibrit Savaş. *Güvenlik Bilimleri Dergisi*, s. 29-56.

Özkaya, Ö. (2020). Devlet Olgusu Üzerine Bir Değerlendirme. *Uyuşmazlık Mahkemesi Dergisi*, 317-352.

Özkaya, Ö., & Efe, S. (2024). Kentsel Politika ve Güvenlik Perspektifinden Göç ve Kentsel Direnç. *Altıncı Ulusal Yerel Yönetimler Sempozyumu Bildiriler Kitabı* (s. 159-172). Ankara: Ankara Üniversitesi.

Rumelili Bahar, & Karadağ, S. (2017). Göç ve güvenlik: Eleştirel yaklaşımlar. *Toplum ve Bilim*, s. 69-92.

Sehgal, I. (2023, Kasım). *What is hybrid warfare?* Global Vllage Space: https://www.globalvillagespace.com/what-is-hybrid-warfare-ikram-sehgal/ adresinden alındı

STM. (2022, Nisan 20). *Rusya ve Ukrayna Arasındaki Siber Saldırıları Analiz Ettik*. STM: https://www.stm.com.tr/tr/medya/haberler/rusya-ve-ukrayna-arasindaki-siber-saldirilari-analiz-ettik adresinden alındı

Şemşit, S. (2018). Avrupa Birliği Politikaları Bağlamında Uluslararası Göç Olgusu ve Türleri: Kavramsal Bakış. *Yönetim ve Ekonomi, 25*(1), s. 269-289.

Şimşek, D., & İçduygu, A. (2017). Uluslararası göç,politika ve güvenlik. *Toplum ve Bilim*, s. 6-26.

T.C. Ulaştırma ve Altyapı Bakanlığı. (2024). *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı.* Ekim 24, 2023 tarihinde T.C. Ulaştırma ve Altyapı Bakanlıığı: https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/some-2013-2014-eylemplani.pdf adresinden alındı

Toktaş, Ş., Çifçi, O., Baygeldi, M. R., Beşgül, B., Dinçel, Y., & Öztürk, E. (2023). *21. Yüzyılın İlk Yarısında Yeni Güvenlik Tehditler.* Ankara: Polis Akademisi.

Tunca, H.Ö., Özkil, A., (2020), Savunma Planlamasında Senaryo Analizi. M. Begenirbaş, R. Can Yalçın, & S. Yenal içinde, *Strateji ve Güvenlik Alanında Temel ve Güncel Yaklaşımlar.* (s.193-220) Ankara: Nobel.

Türk Dil Kurumu Sözlükleri. (2023, Aralık 23). TDK: https://sozluk.gov.tr/ adresinden alındı

Ünal, E., Kanat, S., & Gürkaynak, M. (2023). Hibrit Tehditler ve Avrupa Birliği. *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*(1), s. 391-412.

Yenal, S. (2020). *Asimetrik Savaş ve İstihbarat.* Ankara: Nobel.

Yenal, S. (2020). Savaş Kavramının Dönüşümü: 1. ve 2. Körfez Savaşı Örneğinde Hibrit Savaşların İncelenmesi. *Kara Harp Okulu Bilim Dergisi*, s. 85-110.

Yılmaz, O. (2017). Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik. *Cyberpolitik Journal, 2*(4), s. 22 - 43.

Yılmaz, S. (2011). 11 Eylül Sonrasında ABD ve Türkiye'deki İç Güvenlik Yeniden Yapılanmalarının Karşılaştırması. *Ç.Ü. Sosyal Bilimler Enstitüsü Dergisi, 20*(3), s. 361-380.